P3NK-3262-01Z0

IPアクセスルータ

Si-R シリーズ

Si-R 130B 取扱説明書

FUJITSU

変更履歴

安全上のご注意 ■警告表示について	■警告表示について（P14～16）の情報を「■警告表示について」に追加しました。
安全上のご注意 ■セキュリティの確保について	■セキュリティの確保について（P19）を「■セキュリティの確保について」に更新しました。
装置を保護する	「装置を保護する」の設定事例を追加しました。

はじめに

このたびは、本装置をお買い上げいただき、まことにありがとうございます。

本取扱説明書には、本装置を安全に使用していただくための重要な情報が記載されています。

本装置を使用する前に本書を熟読してください。特に本書に記載されている「安全上のご注意」をよく読み、理解されたうえで本装置を使用してください。また、本書は本装置の使用中、いつでも参照できるように大切に保管してください。

お客様の生命、身体、財産に被害をおよぼすことなく弊社製品を安全に使っていただくために細心の注意を払っています。本装置を使用する際には、本書の説明に従ってください。

本装置は、INSネット64などのISDN回線や、DA64／128などのディジタル専用線を使用して、インターネットサービスプロバイダやルータとのLAN-WAN通信を行うための小型ルータです。

本装置ではWWWブラウザを使用して、各種設定を簡単に行うことができます。また、設定画面はWWWのホームページと同じハイパーテキスト形式になっているので、設定方法や設定項目の説明をクリックひとつで参照できます。

インターネットやLANをさらに活用するために、本装置をご利用ください。

2008年10月

■回線料金に関するご注意■

従量制の回線（ISDN回線など）に接続して本装置をご利用になる場合には、下記のことを必ず守ってください。下記内容をご理解せずに本装置をご使用された場合、お客様のご利用環境によっては、予期しない高額な通信料金が請求される可能性があります。

本装置のB1またはB2ランプが、緑色で点灯または点滅しているときは、通信料金が加算されています。本装置ご利用の際は、ランプ表示により、回線の接続状態を必ず確認してください。

本装置は、10BASE-Tポートに接続したパソコンからの要求により、自動的にダイヤル発信を行い回線を接続します。そのため、お客様がご使用になられる機器、ソフトウェア、またはLANの利用条件により、不要なダイヤル発信が行われ、回線が接続されてしまう場合があります。ご使用の際は、本書の指示に従い、定期的に（1日最低1回）ログ情報を採取し、不要なダイヤル発信が行われていないかどうかを確認してください。詳細は、「課金情報を確認する」（P.650）を参照してください。

何もしていないのに、一定周期にダイヤル発信が行われて回線が接続される、一度接続された回線が自動的に切断されないなど、異常な現象が見受けられた場合には、ただちに本装置からISDN回線ケーブルを引き抜き、本書の指示に従い、原因の調査を行ってください。詳細は、「トラブルシューティング」（P.643）を参照してください。

本装置には通信に対し、上限金額／上限時間が設定でき、月々の回線料金がお客様の意図しない金額にならないよう、上限を超えた場合に新たなダイヤル発信を行わない（着信は可能）設定がされています。お客様のご利用計画に沿って必要があれば累計金額の上限を変更することもできます。詳細は、「課金制御機能を設定する」（P.533）を参照してください。

フレームリレーに接続してご利用になる場合には、統計情報を採取し、不要な通信が行われていないかどうか確認してください。

本ドキュメントには「外国為替及び外国貿易管理法」に基づく特定技術が含まれています。

従って本ドキュメントを輸出または非居住者に提供するとき、同法に基づく許可が必要となります。

Microsoft Corporation のガイドラインに従って画面写真を使用しています。

目次

コピーライトについて

In the following statement, the phrase "this text" refers to portions of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE Standard Portable Operating System Interface for Computer Environments (POSIX), copyright C 1988 by the Institute of Electrical and Electronics Engineers, Inc. In the event of any discrepancy between these versions and the original IEEE Standard, the original IEEE Standard is the referee document.

In the following statement, the phrase "This material" refers to portions of the system documentation. This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

本製品には、WIDEのKAMEプロジェクトによって開発され、下記の使用条件とともに配付されているソフトウェアが含まれています。

安全上のご注意

■ 警告表示について

取扱説明書では、使用者および周囲の方々や財産に損害を与えないための警告表示をしています。警告表示は、警告レベルの記号と警告文の組み合わせになっています。

⚠警告　正しく使用しない場合、死亡または重傷のおそれがあることを示します。

⚠注意　正しく使用しない場合、軽傷または中程度の傷害を負うおそれがあることを示します。
また、当該製品自体またはほかの使用者の財産に対して損害を与えるおそれがあることを示します。

⚠警告　本装置を安全にお使いいただくために、必ずお守りください。正しく使用しない場合、死亡または重傷のおそれがあることを示します。

作業区分	警告事項
感電・火災について	本装置の分解・解体・改造・再生を行わないでください。 また、本装置の上には絶対に物をのせないでください。感電・火災・故障の原因となります。
	直射日光の当たる場所や暖房機の近く、湿気、ホコリの多い場所には置かないでください。 感電や火災のおそれがあります。
	装置内部が高温になるため通気孔をふさがないでください。火災のおそれがあります。
	万一装置から発熱・発煙・異臭が発生したときは、「｜／⏻」スイッチ（電源スイッチ）を「⏻」側へ押して、電源プラグをコンセントから抜いてください。 電源を切断したら、富士通の技術員に連絡してください。そのまま使用すると、感電や火災のおそれがあります。なお、この場合、通信中のデータは保証されません。
	感電のおそれがあります。必ずアース線を接続してください。 アース接続は、必ず電源プラグをコンセントに接続する前に行ってください。 アース接続を外すときは、必ず電源プラグをコンセントから抜いてから行ってください。
	異常発生時は、ただちに「｜／⏻」スイッチ（電源スイッチ）を「⏻」側へ押して、電源プラグをコンセントから抜いてください。 アース線は、電源プラグを抜くまで外さないでください。
	アース線は、ガス管や水道管にはつながないでください。感電や火災のおそれがあります。
	電源ケーブルを傷つけたり、加工したりしないでください。 電源ケーブルの上に物をのせたり、絡みつけたり、足を引っかけたりしないようにしてください。感電や火災のおそれがあります。その他のケーブル類も同様です。
	本装置の電源ケーブルは、タコ足配線にしないでください。 コンセントが過熱し、火災の原因となることがあります。

作業区分	警告事項
感電・火災について	電源プラグの金属部分およびその周辺に、ほこりが付着している場合は、乾いた布でよくふき取ってください。 そのまま使用すると、火災の原因になります。
	電源ケーブルは、プラグ部分を持ってコンセントから抜いてください。 プラグが傷んで感電や火災のおそれがあります。
	電源プラグは、電源コンセントに確実に奥まで差し込んでください。 差し込みが不十分な場合、感電・発煙・火災の原因となります。
	ぬれた手で電源プラグを抜き差ししないでください。感電のおそれがあります。
	電源ケーブルや電源プラグが傷んだり、コンセントの差し込み口がゆるいときは使用しないでください。 そのまま使用すると、感電・火災の原因となります。
	使用中の装置を布でおおったり、包んだりしないでください。熱がこもり、火災の原因となることがあります。
	電源ケーブルを束ねて使用しないでください。発熱して、火災の原因となることがあります。
	雷が鳴りだしたら、電源ケーブルやケーブル類に触れないでください。感電の原因となります。
	コーヒーなどの液体やクリップなどの金属片が装置内部に入らないように気をつけてください。また、装置内部に異物が入るのを防ぐため、装置の上には物を置かないでください。 感電や火災のおそれがあります。
	モジュラジャックには指などを入れないでください。感電の原因となります。
	清掃の際、清掃用スプレー（可燃性物質を含むもの）を使用しないでください。 火災・故障の原因となります。
破損・負傷について	本装置を縦置きおよび段積みで使用しないでください。 落下や発熱による負傷・破損・故障・変形の原因となります。
	振動の激しい場所や傾いた場所など、不安定な場所に置かないでください。 落下したりして、けがの原因となることがあります。
	装置の上に物を置いたり、装置の上で作業したりしないでください。 装置が破損したり、作業者が負傷したりするおそれがあります。
	梱包に使用しているビニール袋は、お子様が口に入れたり、かぶって遊んだりしないよう、注意してください。窒息の原因となります。
	本装置を廃棄するときは、ほかのゴミと一緒に捨てないでください。火中に投じると破裂するおそれがあります。
	電源が入っている状態で本装置に長時間（1分以上）触れないでください。低温火傷の原因となることがあります。

⚠注意　正しく使用しない場合、軽傷または中程度の傷害を負うおそれがあることを示します。また、当該製品自体またはほかの使用者の財産に対して損害を与えるおそれがあることを示します。

作業区分	注意事項
故障について	条件を守って設置してください。条件以外の環境で本装置を使用すると、故障の原因となります。
	本装置は、屋内に設置してください。屋外で使用すると故障の原因となります。
	極端な高温、または低温状態や温度変化の激しい場所で使用しないでください。故障の原因となります。
	塩害地域では使用しないでください。故障の原因となります。
	衝撃や振動の加わる場所で使用しないでください。故障の原因となります。
	薬品の噴霧気中や、薬品にふれる場所で使用しないでください。故障の原因となります。
	電子レンジなど、強い磁界を発生する装置のそばで使用しないでください。故障の原因となります。
	本装置を並べて使用する場合、側面に3cm以上の間隔をあけてください。故障の原因となります。
	国内でだけ使用してください。本装置は国内仕様になっているので、海外ではご使用になれません。
	内部に液体や金属類などの異物が入った状態で使用しないでください。故障の原因となります。
	本装置を移動するときは、必ず電源ケーブルを抜いてください。故障の原因となります。
電波障害について	ラジオやテレビジョン受信機のそばで使用しないでください。 ラジオやテレビジョン受信機に雑音が入る場合があります。
感電について	感電するおそれがありますのでサービスマン以外はカバーを開けないでください。 また、保守時には必ず電源コードを抜いてください。

■ 電池に関するご注意

下記のことを必ず守ってください。電池の使い方を間違えますと、液もれや装置の破損、破壊がおこり、装置の故障やけがの原因となります。

⚠警告

- **電池の ⊕・⊖を正しく入れてください。⊕・⊖を間違えると電池が破損および破裂、液もれするおそれがあります。**
- **電池は、幼児の手の届かないところに置いてください。万一飲み込んだ場合は、ただちに医師に相談してください。**
- **電池をショートさせたり、分解、加熱、火に入れるなどしないでください。アルカリ性溶液がもれて目に入ったり、発熱、破裂の原因となります。**
- **アルカリ性溶液が衣服に付着した場合は、きれいな水で洗い流してください。万一目に入ったり、皮膚に付着した場合は、きれいな水で洗ったあと、医師に相談してください。**
- **電池がもれを起こした場合、もれた液を絶対にさわったり、なめたりしないでください。**

⚠注意

電池について

- **本装置に使用する乾電池には、必ず単3のアルカリ乾電池（LR6）をご使用ください。**
- **古い電池、種類の違う電池、異なるメーカーの電池を新しい電池と混ぜて使わないでください。**
- **電池に直接ハンダ付けをしないでください。**
- **使い切った電池はすぐに装置から取り外してください。**
- **電池を保管する場合は、直射日光、高温、多湿の場所を避けてください。**
- **落下などによって変形した電池を使用しないでください。**

電池交換について

- **電池を交換する場合は、必ず電源スイッチを「⏻」側にして、ケーブル類（電源ケーブル、10BASE-Tケーブル、ISDN回線ケーブル、モジュラケーブル）をすべて取り外してから作業を行ってください。**
- **電池を交換する場合は、装置底面を上にして、机の上など安定した場所に置いて作業してください。装置を立てたり持ち上げて作業すると、電池が飛び出したり、装置が落下するなどして、破損やけがの原因になります。**
- **必ずすべての電池を新しいものと交換してください。**
- **電池を装置に装着したまま停電がない場合でも、1年に1度の割合で新しい電池と交換してください。**
- **停電発生後は、新しい乾電池と交換することをお勧めします。**

■ メンテナンスに関するご注意

- 決してご自身では修理を行わないでください。故障の際は、富士通の技術員または富士通が認定した技術員によるメンテナンスを受けてください。
- 本装置をご自身で分解したり改造したりしないでください。本装置の内部には、高電圧の部分および高温の部分があり危険です。

■ 使用上のご注意

- 本製品を安定した状態でご使用になれる期間は5年が目安です。これは使用環境温度が25℃、湿度15～85%（RH）を想定した数値です。
- 本製品として提供される取扱説明書、装置本体およびファームウェアは、お客様の責任でご使用ください。
- 本製品の使用によって発生する損失やデータの損失については、富士通株式会社では一切責任を負いかねます。また、本製品の障害の保証範囲はいかなる場合も、本製品の代金としてお支払いいただいた金額を超えることはありません。あらかじめご了承ください。
- 本製品で提供されるファームウェアおよび本製品用として富士通株式会社より提供される更新用ファームウェアを、本製品に組み込んで使用する以外の方法で使用すること、また、改変や分解を行うことは一切許可しておりません。
- ISDN U ポートにケーブルを接続する場合は、接続相手がISDN 基本インタフェースであることを確認してください。異なるインタフェースを接続した場合、故障・焼損することがあります。
  コネクタ形状（RJ-11、2ピンモジューラーコネクタ）が同じでも、ISDN回線でないことがあります。アナログ回線やビジネス電話など宅内交換機との接続コネクタである可能性がありますので、配線工事を行った業者などに事前にご使用になるコネクタがISDNであることを確認してください。
- S/T ポートをご使用の場合は、接続相手がISDN機器のS/T ポートであることを確認してください。接続される機器の取扱説明書などをご確認のうえ、接続してください。
  ※ 正しい接続相手でもB1/B2 ランプが橙色点滅している場合は、底面のDSU の極性反転スイッチやDSU切り離しスイッチ＝ ONの設定を確認して接続してください。

■ ツイストペアケーブルの除電について

ツイストペアケーブルは、ご使用の環境などによって、静電気が帯電することがあります。静電気が帯電したツイストペアケーブルをそのまま機器に接続すると、機器または機器の接続ポート（LAN/BRIなど）が誤動作したり、壊れたりすることがあります。
機器に接続する直前に静電気除去ツール（注）などをご使用いただき、ツイストペアケーブルに帯電している静電気をアース線などに放電して接続してください。
また、静電気を放電したあと、接続しないまま長時間放置すると、放電効果が失われますのでご注意ください。

注）静電気除去ツールについて

当社では、以下のツールを提供しています。詳しくは当社担当営業にご確認ください。

品名：LANケーブル ESD除去ツール
型名：TS2002-001

■ 避雷対策について

本装置には避雷対策回路が内蔵されております。また、アース処理を行うことにより効果を高めることができます。

■ セキュリティの確保について

- 管理者パスワードを設定しない場合、ネットワーク上のだれからでも本装置の設定を行うことができます。セキュリティの面からは非常に危険なため、管理者パスワードを設定することを強くお勧めします。

☛ 参照 「ログインパスワードを設定する」（P.179）

- ご購入時の状態では、オンラインサポートを受け付ける設定になっています。この場合、オンラインサポート機能の暗証番号としてMACアドレスを使用します。MACアドレスは容易に知ることができるため、オンラインサポート機能を使用しない場合は、設定を変更してください。

■ 清掃について

本装置を清掃する場合、布に水（または水で薄めた中性洗剤）を含ませ、固く絞ってからふいてください。

ふき取りのときに、本装置のスイッチ類やすきまなどに、水が入らないように十分にご注意ください。

■ 電波障害自主規制について

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをしてください。

■ ハイセイフティについて

本製品は、一般事務用、パーソナル用、家庭用、通常の産業用等の一般的用途を想定して設計・製造されているものであり、原子力施設における核反応制御、航空機自動飛行制御、航空交通管制、大量輸送システムにおける運行制御、生命維持のための医療用機器、兵器システムにおけるミサイル発射制御など、極めて高度な安全性が要求され、仮に当該安全性が確保されない場合、直接生命・身体に対する重大な危険性を伴う用途（以下「ハイセイフティ用途」という）に使用されるよう設計・製造されたものではありません。

お客様は、当該ハイセイフティ用途に要する安全性を確保する措置を施すことなく、本製品を使用しないでください。ハイセイフティ用途に使用される場合は、弊社の担当営業までご相談ください。

■ 事業系の使用済み製品の引き取りとリサイクルについて

法人のお客様から排出される弊社製品は「事業系 IT 製品リサイクルサービス」（有料）にて回収、リサイクルし、資源の有効利用に取り組んでいます。

本製品の廃棄については、以下の富士通ホームページをご覧ください。

URL： https://www.fujitsu.com/jp/services/infrastructure/maintenance/lcm/service-phase4/recycle/

■ グリーン製品について

弊社の厳しい環境評価基準をクリアした地球に優しい、環境への負荷の少ない「グリーン製品」です。

- 主な特長
  - 小型／省資源化
  - 節電機能保有
  - 再資源化率が高い

このマークは富士通株式会社のグリーン製品の評価基準に適合したグリーン製品に表示しています。

富士通の環境についての取り組みの詳細は、以下の富士通ホームページをご覧ください。

URL : https://www.fujitsu.com/jp/about/environment/「環境活動」

取扱説明書の構成と使いかた

本書では、本装置をお使いになる前に知っておいていただきたいこと、接続する方法、インターネットやLANへ接続するための設定など、基本的な導入方法について説明しています。

本装置の機能をもっと知りたい場合、本装置を使って複雑な運用をする場合は、必要に応じてリファレンス編を参照してください。また、付録では補足情報を載せています。

- チュートリアル編　：　本装置の基本的な使い方を載せています。本装置を接続して設定を行い、通信ができるようになるまでを説明しています。また、本書を読みながら作業を進めることができるようになっています。
- リファレンス編　：　本装置の多様な機能の詳細を載せています。本装置の機能を活用していただくためにお読みください。

本装置のトップページと取扱説明書の記載内容とが異なる場合は、各ページの指示に従って設定を行ってください。

また、CD-ROMの中のREADMEファイルには大切な情報が記載されていますので、併せてお読みください。

第1部　チュートリアル編の構成

チュートリアル編の構成と各章の内容を示します。

章タイトル	内　容
第1章　準備	本装置の各部名称や、利用するパソコンの準備、回線や機器の接続方法を説明しています。
第2章　設定	基本的な設定方法を説明しています。
第3章　導入例	いろいろな接続形態の運用例を説明しています。

第2部　リファレンス編の構成

リファレンス編の構成と各章の内容を示します。

章タイトル	内　容
第4章　設定ページリファレンス	設定する項目をページごとに説明しています。
第5章　活用例（アナログ設定）	アナログ設定の便利な機能を活用した設定例を説明しています。
第6章　活用例（ルータ設定）	ルータ設定の便利な機能を活用した設定例を説明しています。
第7章　運用管理とメンテナンス	操作メニュー、表示メニュー、メンテナンスメニューなどを使って、本装置の運用を管理する方法を説明しています。
第8章　トラブルシューティング	本装置を使用して、通信料金が正常かどうかを確認する方法、および異常が発生した場合の対処方法を説明しています。

マークについて

本書で使用しているマーク類は、以下のような内容を表しています。

ヒント	本装置をお使いになるうえで役に立つ知識を、コラム形式で説明しています。
こんな事に気をつけて	本装置をご使用になる際に、注意していただきたいことを説明しています。
補足	操作手順で説明しているもののほかに、補足情報を説明しています。
☛ 参照	操作方法など関連事項を説明している箇所を示します。
⚠警告	製造物責任法（PL）関連の警告事項を表しています。本装置をお使いの際は必ず守ってください。
⚠注意	製造物責任法（PL）関連の注意事項を表しています。本装置をお使いの際は必ず守ってください。

■ 本書での商標の表記について

Microsoft、Windows、Windows NTおよびWindows Vistaは、米国Microsoft Corporationの米国およびその他の国における登録商標です。

AMD、AMD社ロゴマーク、ならびにその組み合わせは、Advanced Micro Devices, Inc.の登録商標です。

Magic Packet、PCnetは Advanced Micro Devices, Inc.の商標です。

AMD and the AMD Logo are registered trademarks and Magic Packet and PCnet are trademarks of Advanced Micro Devices, Inc.

AdobeおよびReaderは、Adobe Systems Incorporated（アドビシステムズ社）の米国ならびに他の国における商標または登録商標です。

UNIXは、米国およびその他の国におけるオープン・グループの登録商標です。

Hifn
Intelligent Secure Networking

LZSは、Hifn社の登録商標です。

本書に記載されているその他の会社名および製品名は、各社の商標または登録商標です。

製品名の略称について

本書で使用している製品名は、以下のように略して表記します。

製品名称	本文中の表記
Microsoft® Windows® XP Professional operating system	Windows® XP
Microsoft® Windows® XP Home Edition operating system	
Microsoft® Windows® Millennium Edition operating system	Windows® Me
Microsoft® Windows® 98 operating system	Windows® 98
Microsoft® Windows® 95 operating system	Windows® 95
Microsoft® Windows® 2000 Server Network operating system	Windows® 2000
Microsoft® Windows® 2000 Professional operating system	
Microsoft® Windows NT® Server network operating system Version 4.0	Windows NT® 4.0
Microsoft® Windows NT® Workstation operating system Version 4.0	
Microsoft® Windows Vista® Ultimate operating system	Windows Vista®
Microsoft® Windows Vista® Business operating system	
Microsoft® Windows Vista® Home Premium operating system	
Microsoft® Windows Vista® Home Basic operating system	
Microsoft® Windows Vista® Enterprise operating system	

第1部
チュートリアル編

第1章　準備

1

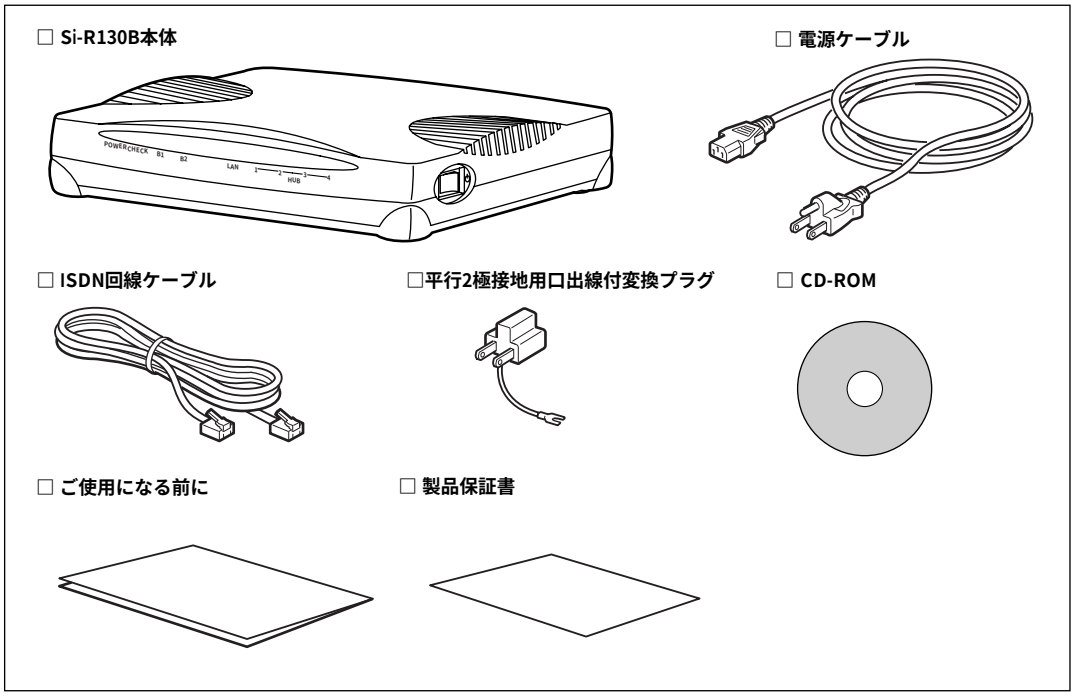
この章では、
本装置を使う前に必要な準備などを説明します。

梱包内容／各部の名称と働き

本装置をお使いになる前に、梱包内容を確認してください。

■ 梱包内容

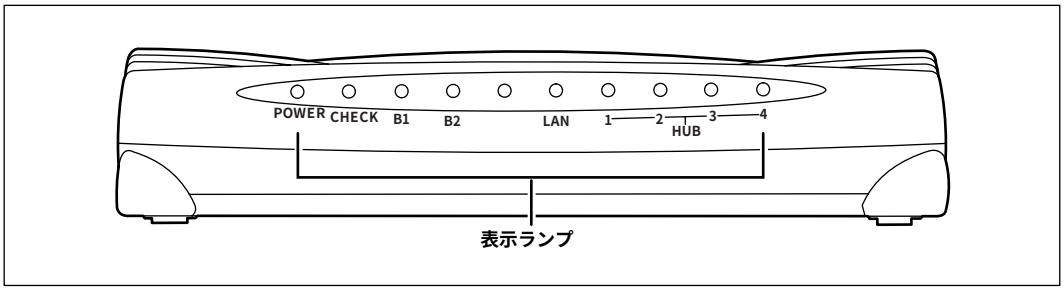
下記製品には、それぞれ以下のものが同梱されています。すべてそろっていることを確認してください。



- Si-R130B 本体　　本装置のことです。
- 電源ケーブル　　本装置とコンセントをつなぐケーブルです。
- ISDN回線ケーブル　　本装置をISDN回線またはディジタル専用線につなぐためのケーブルです。両端に6ピンのモジュラプラグがついています。
- 平行2極接地用口出線付変換プラグ
  本装置の3ピンの電源ケーブルを2穴のコンセントに差し込むためのアダプタです。
- CD-ROM　　CD-ROMの中には、ファームウェアおよび取扱説明書（PDF形式）が入っています。ご覧になる場合は、PDF閲覧ソフトAdobe Readerが必要になります。
- ご使用になる前に　　ファームウェアのインストール方法、梱包内容、使用許諾の契約内容などについて記載されています。
- 製品保証書

補足 本製品には、RS232C ケーブルは同梱されていません。
ケーブルについては、以下の富士通ホームページをご覧ください。
URL : http://fenics.fujitsu.com/products/manual/cable/

■ 本装置 前面



- 表示ランプ　　表示ランプの動作を以下に示します。

正常に動作しているときの表示ランプ

- POWER ランプ　　電源の状態を示します。電源を投入すると緑色で点灯し、切断すると消灯します。バックアップ電池で動作しているとき（「停電モード」）および「スタンバイモード」で動作しているときは、緑色で点滅します。

☛ 参照 「停電時の動作について」（P.670）、「スタンバイモードで使用する」（P.355）

- CHECK ランプ　　構成定義を書き込んでいる場合に、緑色で点滅します。

⚠注意
CHECK ランプが緑色で点滅しているとき、電源の切断およびリセットを行わないでください。構成定義が破壊される場合があります。

- B1 ／ B2 ランプ　　回線の状態を表示します。

  [データ通信を行う場合]
  相手側との接続が完了して通信可能な状態になったとき、緑色で点灯します。通信が行われている間は緑色で点滅します。

  [アナログ通信を行う場合]
  接続中および通話中は緑色で点滅します。ただし、2つのアナログポートで内線通話を行っている場合は、アナログポートの通信状況は表示されません。

⚠注意
B1／B2ランプが緑色で点灯または点滅している場合、通信料金が加算されています。

- LAN ランプ　　LANの状態を表示します。通信可能な状態は緑色で点灯し、通信が行われている（データがやり取りされている）間は緑色で点滅します。
- HUB PORT ランプ　　10BASE-T ポート（1～4）の状態を表示します。ポートにパソコンを接続しているときは、緑色で点灯します。データを受信している間は緑色で点滅します。

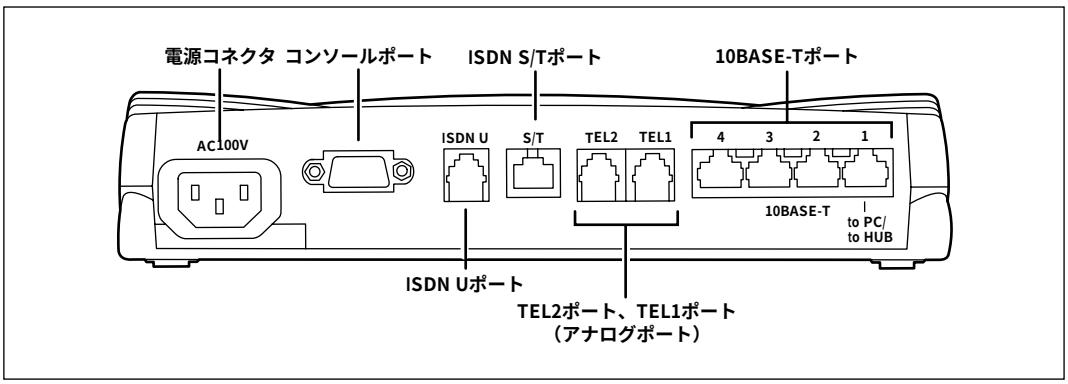
動作が異常なときの表示ランプ

- CHECK ランプ　　エラー発生時に、橙色で点灯します。
- B1 ／ B2 ランプ　　ISDN ポートでの通信が不可能な場合に、橙色で点滅します。ケーブルが正しく接続されていない、または極性が反転している可能性があります。
- HUB PORT ランプ　　状態が異常な場合、ランプは点灯しません。

☛ 参照 「起動時の動作に関するトラブル」（P.653）

- すべてのランプが消灯　　本装置の電源異常を検出したときは、すべてのランプが消灯し、電源が切れます。このような場合には、すぐに電源スイッチを「⏻」側へ押したうえで、富士通の技術員にご連絡ください。

■ 本装置 背面



- 電源コネクタ　　同梱の電源ケーブルをここに差し込みます。
- コンソールポート　　装置に対する設定・操作を行うために、コンソールケーブルとD-SUB9ピンのクロスケーブルでパソコンと接続します。
- ISDN U ポート　　ISDN 回線またはディジタル専用線に接続するときに使います。本装置に内蔵されたDSUを使用する場合は、同梱のISDN 回線ケーブルをここに差し込みます。

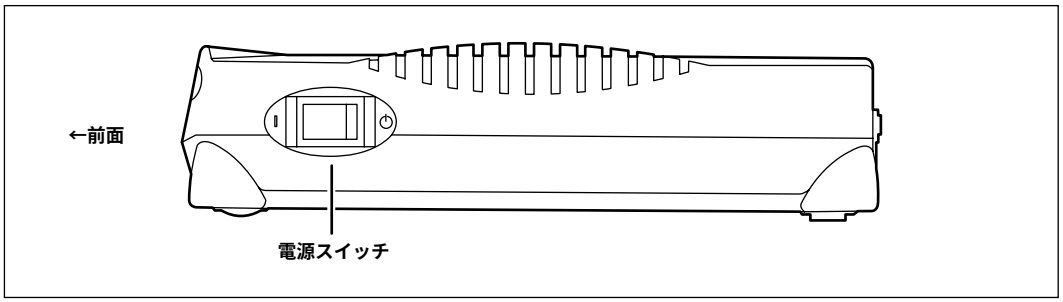
- ISDN S／Tポート　本装置にディジタル電話機、ディジタル回線用ファックスなどのISDN機器やTA（ターミナルアダプタ）をつなぐときに使います。ISDN機器などにつないだモジュラケーブルをここに差し込みます。外付けDSUをつなぐときに使います。DSUにつないだモジュラケーブルをここに差し込みます。

補足 外付けのDSUを使用する場合：ISDN S／Tポートに外付けのDSUをつなぎます。市販の8ピンISDN回線ケーブルをお使いください。

- アナログポート（TEL1、TEL2）　本装置に電話機やFAX、モデムなどのアナログ機器をつなぐときに使います。アナログ機器につないだモジュラケーブルをここに差し込みます。
- 10BASE-Tポート（1～4）　本装置をパソコンやワークステーションとつなぐときに使います。パソコンなどをつないだ10BASE-Tケーブルをここに差し込みます。

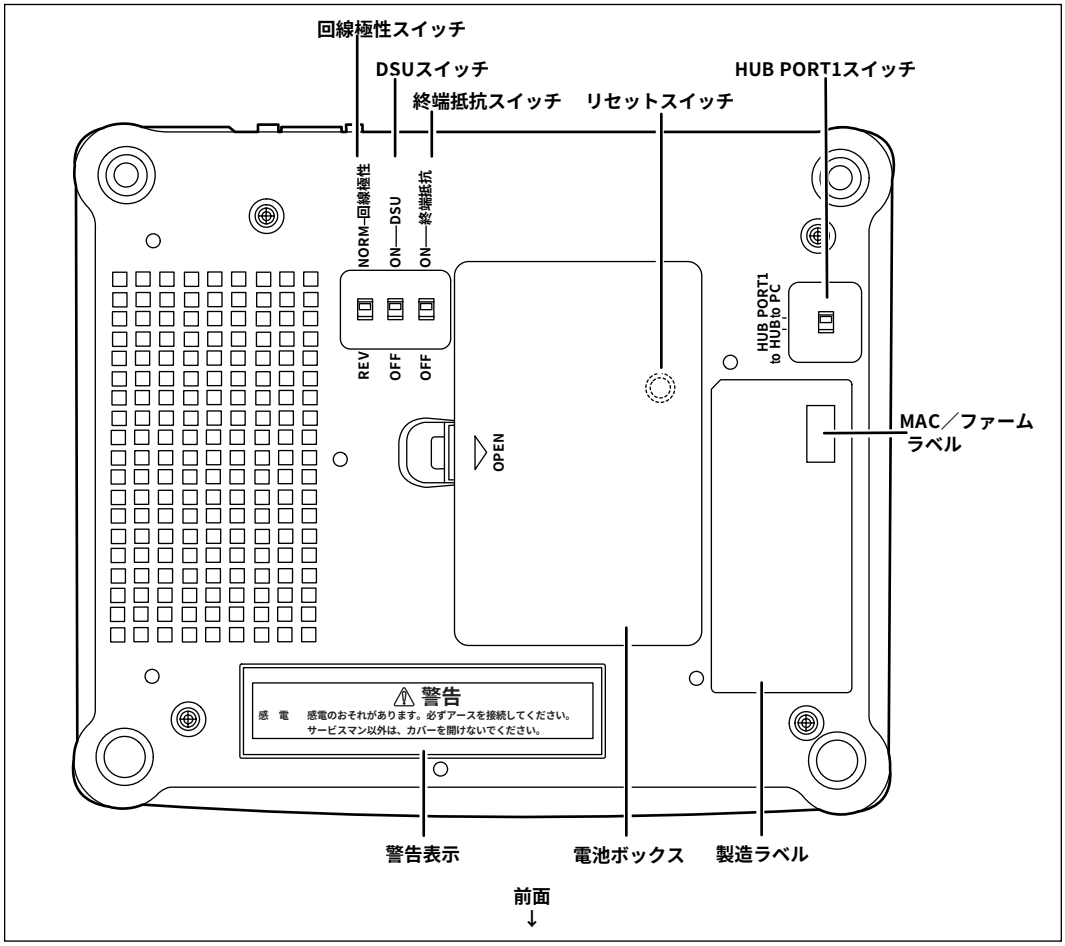
補足 10BASE-Tポートにパソコンなどをつなぐ場合は、市販の10BASE-Tケーブル（LANケーブル）をお使いください。

■ 本装置 側面

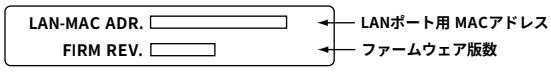


- 電源スイッチ　「｜」側へ押すと、電源が入ります。
「⏻」側へ押すと、電源が切れます。

■ 本装置 底面



- 回線極性スイッチ　　ISDN 回線の極性切り替えを行います。
- DSU スイッチ　　内蔵DSUの使用有無の設定を行います。
- 終端抵抗スイッチ　　終端抵抗の使用有無の設定を行います。
- リセットスイッチ　　電池ボックスの中にあります。
  スイッチを押すと、再起動を行います。
- HUB PORT1 スイッチ　　10BASE-T ポート 1 の接続先を、パソコンまたはHUB に切り替える設定を行います。
- MAC ／ファームラベル



  ご購入時の状態では、オンラインサポートの暗証番号に LAN ポート用のMAC アドレスが設定されています。
- 製造ラベル　　型名、製造号機、製造日などが記載されています。
- 電池ボックス　　停電時バックアップ用の電池をここに入れます。
- 警告表示　　本装置の取り扱いについて注意していただきたいことが記載されています。

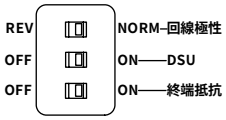
スイッチの設定

[HUB PORT1スイッチ]

10BASE-Tポート1の接続先に合わせてスイッチを切り替えます。

10BASE-Tポート1に接続する機器	スイッチの設定
パソコン	HUB PORT1スイッチを「to PC」にします。
HUB	HUB PORT1スイッチを「to HUB」にします。

[終端抵抗スイッチ、DSUスイッチ、回線極性スイッチ]



出荷時には、イラストのように設定されています。この場合、設定条件は以下のようになります。

- 回線の極性を反転させない
- 内蔵のDSUを使用する
- 内蔵の終端抵抗を使用する

☛ 参照　上記以外の条件で通信する場合→「スイッチ設定例」（P.671）

スイッチは以下のように設定します。

設定条件	スイッチの設定
回線の極性を反転させる場合	回線極性スイッチを「REV」にします。
回線の極性を反転させない場合	回線極性スイッチを「NORM」にします。
本装置の内蔵DSUを使用する場合	DSUスイッチを「ON」にしてから、両端が6ピンモジュラの形状のISDN回線ケーブル（本体に同梱されています）をISDN Uポートに接続します。
外付けのDSUを使用する場合 （本装置の内蔵DSUを使用しない）	DSUスイッチを「OFF」にしてから、両端が8ピンモジュラの形状のISDN回線ケーブル（別途購入が必要です）をISDN S／Tポートに接続します。
S／Tポート内蔵の終端抵抗を使用する場合	終端抵抗スイッチを「ON」にします。
S／Tポート内蔵の終端抵抗を使用しない場合	終端抵抗スイッチを「OFF」にします。

⚠注意

外付けのDSUを使用する場合は、「内蔵DSUを使用しない」ように、DSUスイッチの設定を「OFF」に必ず変更してください。

補足 外付けのDSUを使用する場合：ISDN S／Tポートに外付けのDSUをつなぎます。市販の8ピンISDN回線ケーブルをお使いください。

ヒント

◆ ISDN回線の極性

NTTの局線には極性があります。通常はストレートタイプのISDN回線ケーブルを差し込めば、通信ができるようになっていますが、まれにこの極性が反転している場合があり、ストレートタイプのISDN回線ケーブルではISDN機器がまったく動作しないことがあります。このような場合は、本装置の回線極性スイッチの設定を変更して、極性を反転させることができます。

設置環境を確認する

設置する前に、本装置の梱包内容がすべてそろっていることを確認してください。

☛ 参照 「梱包内容」(P.29)

本装置では、以下の環境を確保して設置してください。

■ 設置条件を確認する

⚠注意

以下の条件を守って設置してください。条件以外の環境で本装置を使用すると、故障の原因となります。

湿温度条件

	温度（℃）	湿度（%RH）
動作時	0～40	15～85
休止時	0～50	8～90

電源条件

項目	条件
電圧	AC100V ± 10%
周波数	50Hz／60Hz ＋2%、－4%
アース	空調アース、建屋アースと同一でないこと、D種接地（第三種接地）以上
最大消費電力	11W

設置条件

項目	可否
縦置き	×
平置き	○
段積み	×

チェックリスト

条件が守られているかを以下のチェックリストで確認してください。

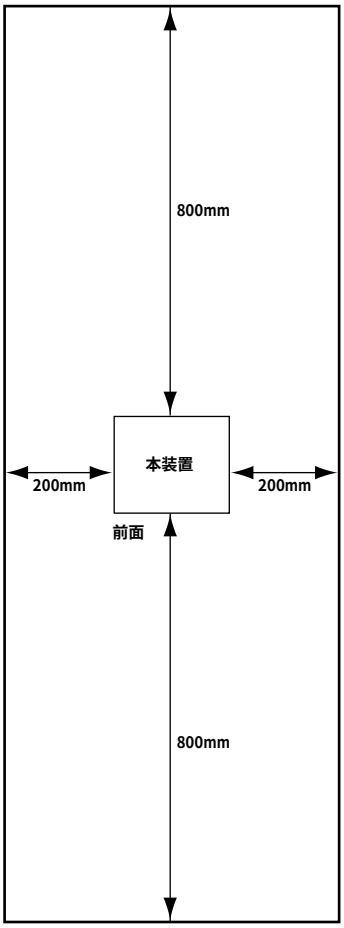
チェック内容	チェック結果
本装置の上に物をのせていない	
本装置の通気孔をふさいでいない	
本装置を縦置きおよび段積みにしていない	
本装置の設置場所は直射日光の当たる場所や暖房機の近く、湿気、ホコリの多い場所ではない	
本装置の設置場所は振動の激しい場所や傾いた場所などの不安定な場所ではない	
本書の「安全上のご注意」を読みました　☛ 参照 （P.14）	

■ 設置（保守）スペースを確保する

本装置の設置および保守を行う場合は、以下のスペースを確保してください。

保守スペースを確保する

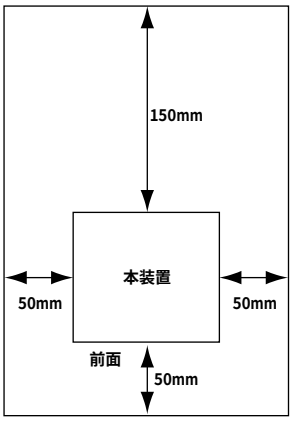
保守する場合は、以下の保守スペース（サービスエリア）を確保してください。



設置スペースを確保する

設置する場合は、以下の設置スペースを確保してください。

卓上に設置する



契約の内容を確認する

本装置をご使用になる場合には、回線に関するさまざまな契約が必要になります。ご利用になる回線に応じて契約内容を確認してください。

■ ISDN回線を利用する場合は

ここでは、もっとも一般的なNTT回線のINSネット64の場合について説明します。

INSネット64またはINSネット64・ライトを新規に申し込む場合や、アナログ回線からINSネット64に切り替える場合は、NTT各店に備え付けの「INSネット64／INSネット64・ライトお申込票」に必要事項を記入します。詳しくは、NTT窓口にお問い合わせください。

ご利用方法などに応じて、申込書の記入項目には、以下のように選択してください。

「ご確認項目（必須項目）」

- インタフェース形態およびレイヤ起動種別
  ：「P-MP呼毎」または「P-MP常時」を選びます。「P-MP呼毎」をお勧めします。「P-P」では動作しないので注意してください。
- 発信者番号通知サービス　：接続先に自分の電話番号を通知するかを選択します。本装置どうしでコールバック機能（無課金コールバック機能）を利用する場合や、アナログの発信者番号通知機能を利用する場合は、「通常通知」を選びます。
- ユーザ間情報通知サービス：本装置でオンラインサポート機能を利用する場合は、「着信許可」を選びます。

こんな事に気をつけて

すでにINSネットに加入済みで発信者通知サービスを「常時通知拒否」とされている場合、正常にデータ通信を行えないことがあります。

「ご確認項目（付加機能項目）」

- 通信中着信通知サービス　：本装置のBOD機能を使用してアナログ着信時にチャネル縮退する場合や、フレックスホンを利用する場合に選びます。

ヒント

◆ 本装置の BOD 機能とは？

本装置では MultilinkPPP（MP 機能）を利用して 2 つの B チャネルを束ねて 128Kbps でデータ通信することができます。BOD 機能を使うと MP で通信中にも通信量に応じて B チャネルを増減させたり、アナログ機器を使用してダイヤル発信したり、着信する場合も B チャネルを減らすことができます。

☛ 参照 「NTT との契約が必要な機能」（P.676）

「通信機器」

- 通信機器の名称　：Si-R130B
- メーカ名　：他社を選びます。
- 認定番号　：本装置底面の製造ラベルに記載されている「認定番号」

補足 お申し込み票によっては、認定番号の欄がない場合があります。

「配線工事等」

- 「回線接続装置 DSU」および「機器配線」
  ：お客様工事

■ 専用線を利用する場合は

スーパーディジタルインタフェース 64 または 128Kbps を指定してください。

■ フレームリレーを利用する場合は

フレームリレーは多数の拠点と接続し、各拠点に発生するバースト的な高トラフィックが 1 箇所に同時集中しないネットワーク形態に適しています。複数の論理的な通信路（論理チャネル）を 1 本のアクセス回線（物理回線）上に設定して、あらかじめ登録されている相手とだけ接続できます。

NTT コミュニケーションズでは「スーパーリレー FR」という名称でサービスを行っています。

ご利用方法に応じて、申し込み時に以下のように選択してください。

- フレームリレーサービス 64 または 128Kbps を選びます。
- PVC 状態確認手順（LMI）を使用する場合は、ITU-T:Q.933AnnexA を指定します。
- DLCI 番号は 16～991 で指定します。

■ IP-VPNを利用する場合は

IP-VPNは、複数のプロバイダのネットワークを経由する必要があるインターネットとは異なり、専用線接続のようなセキュリティ、回線品質が確保されたデータ通信ができます。必要に応じて、当社のFENICSビジネスIPネットワークサービスをはじめ、ULTINA IP-VPN（ソフトバンクテレコム）、Arcstar IP-VPN（NTTコミュニケーションズ）、KDDI IP-VPN（KDDI）などの通信会社にご相談ください。

■ プロバイダとの契約内容を確認する

本装置でインターネットに接続する場合、インターネットサービスプロバイダ（以降プロバイダと略します）との契約が必要です。この場合、「端末型ダイヤルアップ接続」「ネットワーク型ダイヤルアップ接続」「専用線IP接続」から、ご利用方法に応じて接続形態を選びます。

すでにプロバイダと契約している場合は、以下の各項目を確認してください。

●「端末型ダイヤルアップ接続」（フレッツ・ISDN接続を含む）の場合

- ユーザ認証ID
- ユーザ認証パスワード
- アクセスポイントの電話番号

●「ネットワーク型ダイヤルアップ接続」の場合

- DNSサーバのIPアドレス
- ユーザ認証ID
- ユーザ認証パスワード
- ネットワークアドレス
- アクセスポイントの電話番号
- ドメイン名

●「専用線IP接続」の場合

- DNSサーバのIPアドレス
- ネットワークアドレス
- 通信速度

ヒント

◆ユーザ認証ID／パスワード

端末型ダイヤルアップ接続の場合、プロバイダとの接続には一般の公衆回線を使います。当然、パソコンとモデム（またはTA）さえあれば、だれでも接続できてしまいます。これでは困るのでプロバイダ側では、正規契約者からの接続要求とそうでない要求とを識別するために、ユーザ認証IDとパスワードを発行するのです。このIDとパスワードが一致して初めて、インターネットへの接続が許可されるわけです。

ユーザ認証IDという呼び名は、「PPPユーザアカウント」とか「アカウント」などと呼ばれることがあり、プロバイダによって異なります（このマニュアルでは「ユーザ認証ID」「ユーザ認証パスワード」と呼びます）。

フレッツ・ISDN接続の場合は、ユーザ認証IDに「xxx@xxx.ne.jp」や「xxx@xxx.com」などの形式を使用しています。詳しくは、契約しているプロバイダに確認してください。

■ プロバイダと新規に契約する場合は

まず、プロバイダを選びます。インターネット関連の雑誌などに掲載された情報を参考に、以下のような基準でプロバイダを選んでください。

- 会社や自宅と同じ局番の地域にアクセスポイントがある
- 上位プロバイダと高度な回線で接続されている

こんな事に気をつけて

プロバイダによっては、NAT（Network Address Translation）を禁止しているところがあるので、あらかじめ確認しておく必要があります。その際は、プロバイダの指示に従ってください。

ヒント

◆ プロバイダとの接続形態

プロバイダとの接続形態は、一般的に「端末型ダイヤルアップ接続」「ネットワーク型ダイヤルアップ接続」「専用線IP接続」の3つがあります。

- 端末型ダイヤルアップ接続（フレッツ・ISDN接続を含む）

  1台のパソコンからインターネットに接続するときには、端末型ダイヤルアップ接続を選択します。この場合は、接続するたびに異なるIPアドレスが1つ割り当てられます。

  ただし本装置のマルチNAT機能を使用すると、端末型ダイヤルアップ接続で契約していても、本装置につながったパソコンの設定を変更しないで複数台のパソコンからインターネットに接続できます。

- ネットワーク型ダイヤルアップ接続

  ネットワーク上の複数台のパソコンからインターネットに接続するときには、ネットワーク型ダイヤルアップ接続を選択します。申し込み台数に応じてIPアドレスが割り当てられます。

- 専用線IP接続

  プロバイダとの間を専用回線でつないでインターネットに常時接続するときには、専用線IP接続を選択します。通常プロバイダが専用回線の手配を行います。インターネットを常時接続で利用する場合は、以下の2つの方法が一般的です。用途に合ったものを選択してください。

  - プロバイダと専用線IP接続契約を結ぶ：利用回線はDA64／DA128またはHSD
  - 各通信会社が提供している専用線接続サービスを利用する

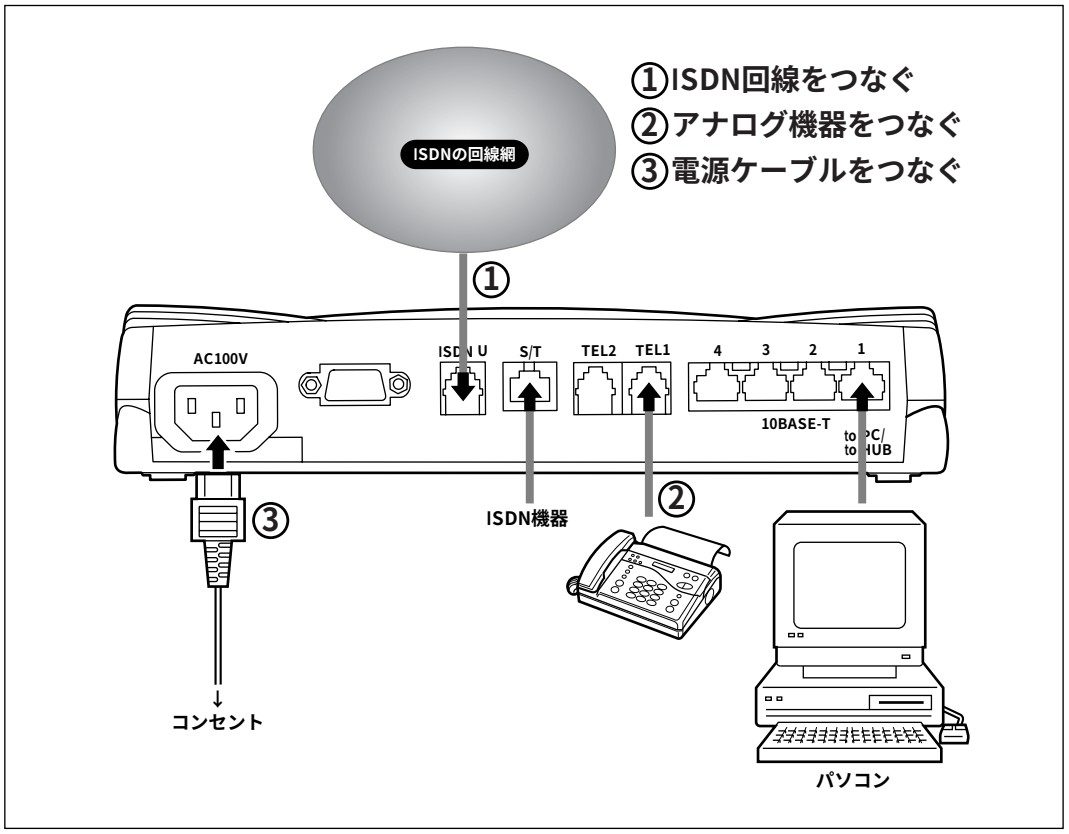
ISDN回線をつなぐ

■ 本装置の接続手順

以下に示す手順で、本装置を接続します。

⚠警告

本装置および接続する機器の電源を切断してから、つないでください。

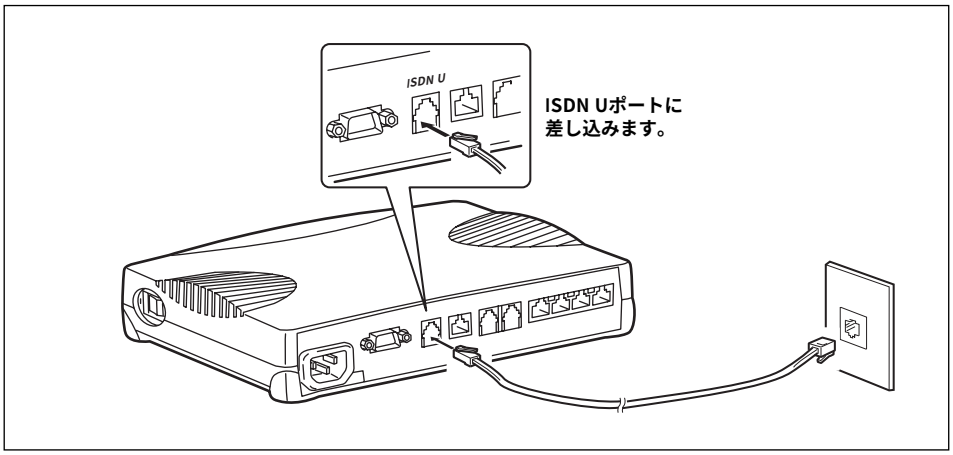


☛ 参照　パソコンのつなぎ方→「パソコンを設定する」（P.52）、「パソコンをつなぐ」（P.61）

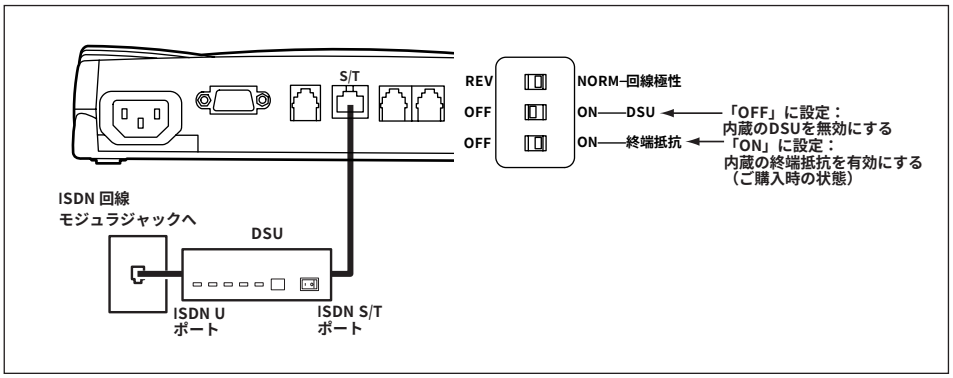
■ ISDN回線をつなぐ

1. ISDN回線ケーブルの一方を本装置のISDN Uポートに差し込みます。

2. ケーブルのもう一方をISDN回線のモジュラジャックに差し込みます。



補足 本装置の内蔵DSUを使用しない場合は、下図のように本装置のISDN S／Tポートと既設DSUのISDN S／Tポートをつなぎます。スイッチの設定を右下の図のように変更してください。



■ アナログ機器をつなぐ

アナログポート（TEL1、TEL2）にアナログ機器のモジュラを差し込むだけでアナログ機器を使うことができます。本装置でアナログ機能の設定を行うと、さらに便利な使い方ができます。

停電時にも、本装置にバックアップ電池が入っている場合、TEL1 ポートに接続された電話機は使うことができます。

☛ 参照 「停電時の動作について」（P.670）

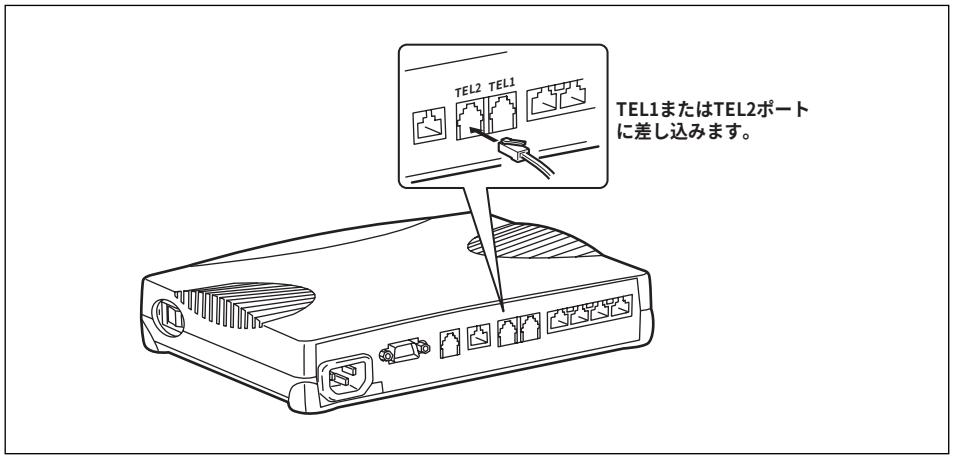
こんな事に気をつけて

- **アナログポート 1 つにアナログ機器 1 台だけをつないでください。2 分岐モジュラコネクタなどを使って 1 つのポートに複数の機器をつなぐと、誤動作の原因になります。**
- **アナログポートにつなぐことができるのは、プッシュ式のアナログ回線用の電話機、FAX、モデムなどです。パルス式の機器やディジタル電話機、ディジタル回線用の FAX は、このポートにつなぐことができません。**

補足
- 受話器を取ってダイヤルボタンを押したときに、受話器からピッポッパという音（PB 音と言います）がする電話機が使えます。PB 音が聞こえない場合でも、電話機にトーン／パルス切り替えスイッチがついているものであれば、トーン側にスイッチを切り替えれば使うことができるようになります（トーン／パルス切り替えスイッチについては電話機の取扱説明書をご覧ください）。
- PB 音を発信できる電話機でも、機種によっては使用できない場合があります。

1.　モジュラケーブルの一方の端をアナログ機器に差し込みます。

2.　モジュラケーブルのもう一方の端を本装置の TEL1、TEL2 ポートに差し込みます。



■ ISDN 機器をつなぐ

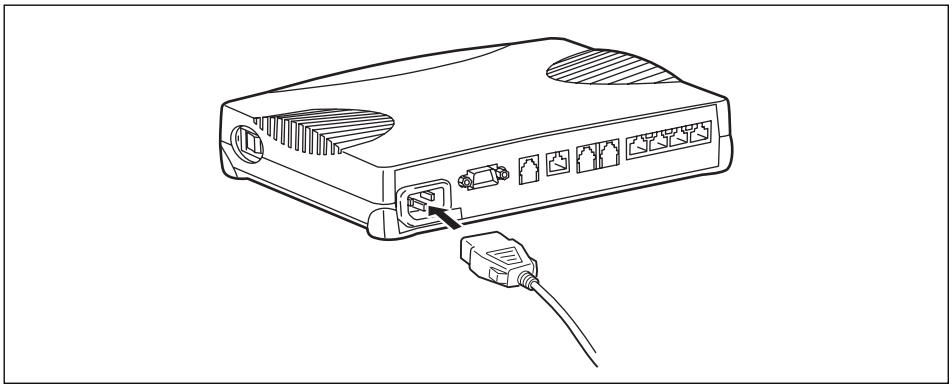
ISDN 機器をつなぐ場合は、「アナログ機器をつなぐ」を参考にして、ISDN S／T ポートに ISDN 機器のケーブルを差し込んでください。

■ 電源ケーブルをつなぐ

⚠警告

本装置の電源スイッチが「⏻」側へ押されていることを確認してから、電源コンセントに差し込んでください。

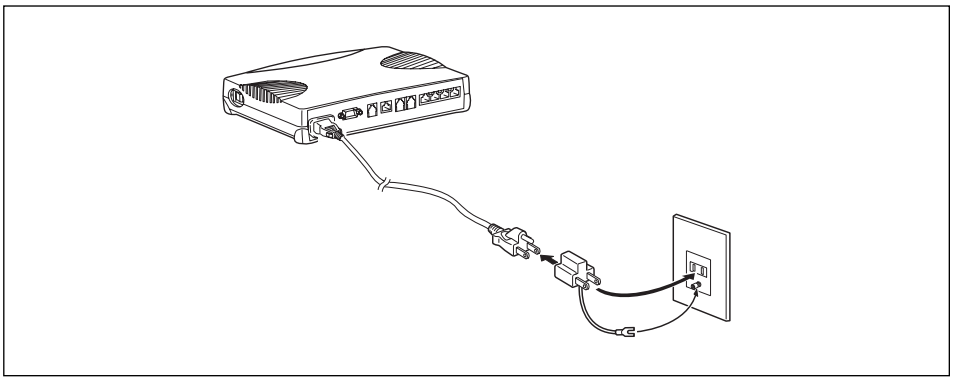
1. 本体背面に電源ケーブルを差し込みます。



2. 電源ケーブルの先に平行2極接地用口出線付変換プラグを取り付けます。
3. 平行2極接地用口出線付変換プラグを取り付けた電源ケーブルを、電源コンセントに差し込みます。
4. アース線の先についているFG端子をコンセントのFGネジに取り付けます。

⚠警告

アース線は必ず接続してください。感電のおそれがあります。



こんな事に気をつけて

本装置は電源ケーブルを差し込むコンセントの近傍に設置し、電源ケーブルを容易に抜くことができるスペースを確保してください。

■ 電源を投入する

1.　本装置の電源を投入します。（「 I 」側へ押します。）

2.　本装置が起動したことを確認します。

補足 電源を投入すると、本装置は自動的に装置の状態を診断します。このとき、CHECK／B1／B2／LANランプが点滅します。次にHUB以外のランプが同時に緑色で約2秒間点灯します。装置に異常がない場合は、CHECKランプが消灯して、起動が完了します。

■ 電話が利用できることを確認する

本装置のアナログポートにつないだ電話機は、アナログの回線につないだときと同様に利用できます。本装置に接続された電話機から電話をかけて、ISDN回線が正常に接続されていることを確認してください。

1.　受話器を上げ、ツーという音が聞こえることを確認します。

2.　相手先の電話番号をダイヤルすると、呼び出し音が鳴ります。

3.　通話が終わったら、受話器を置きます。

こんな事に気をつけて

受話器を置いてから、すぐに受話器を上げてしまうと、通話が切れません。続けてほかに電話をかける場合は、2秒以上置いてから受話器を上げてください。

ヒント

◆ リダイヤルするときには

最後に電話をかけた番号にもう一度電話をかける場合は、リダイヤル機能を使うと便利です。上の操作と同様な操作で、手順2.で ✱ 8 を押します。

◆ すぐに発信するには

ご購入時の設定では、番号をダイヤルして # を1回押すと、すぐに発信するようになっています。

☛ 参照 「ダイヤル操作早見表」（P.674）

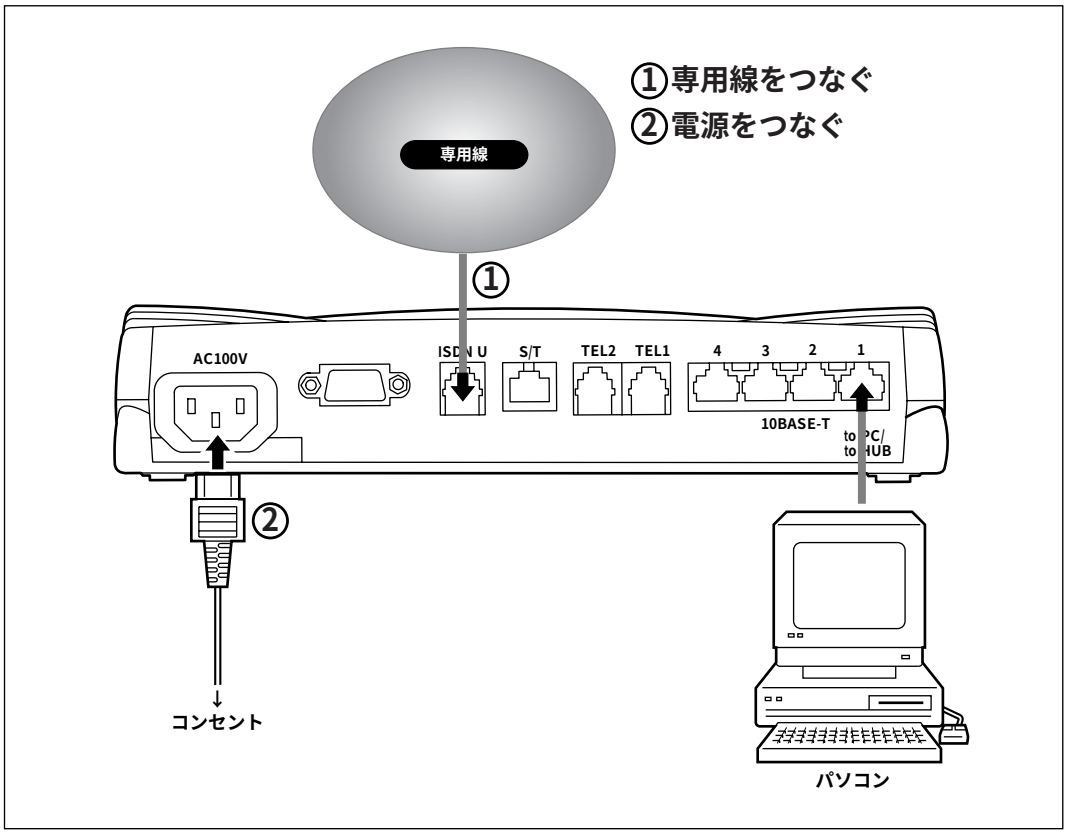
専用線をつなぐ

■ 本装置の接続手順

以下に示す手順で、本装置を接続します。

⚠警告

本装置および接続する機器の電源を切断してから、つないでください。

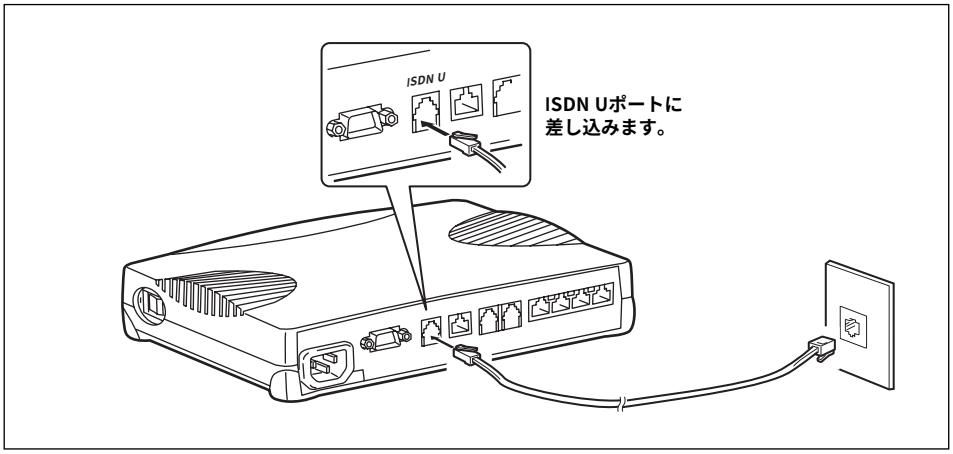


☛ 参照　パソコンのつなぎ方→「パソコンを設定する」（P.52）、「パソコンをつなぐ」（P.61）

■ 専用線をつなぐ

1. ISDN 回線ケーブルの一方を本装置のISDN U ポートに差し込みます。

2. ケーブルのもう一方を専用線のモジュラジャックに差し込みます。

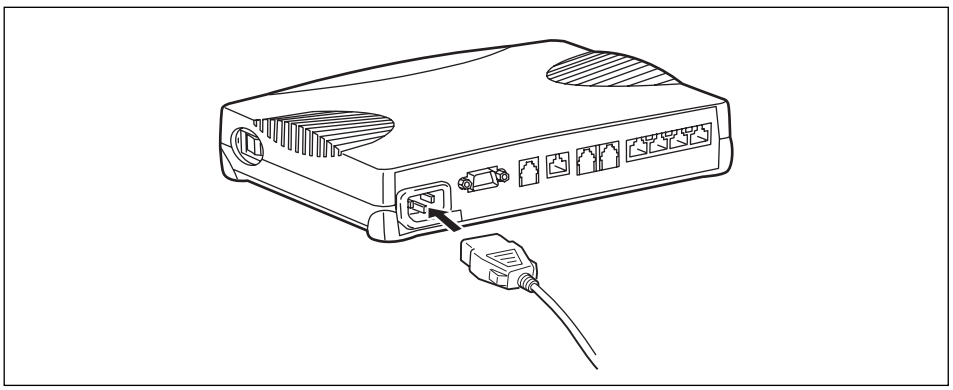


■ 電源ケーブルをつなぐ

⚠警告

本装置の電源スイッチが「⏻」側へ押されていることを確認してから、電源コンセントに差し込んでください。

1. 本体背面に電源ケーブルを差し込みます。



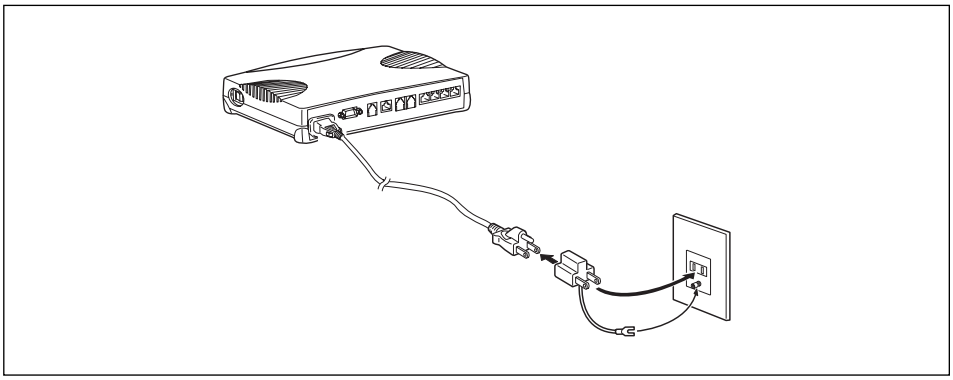
2. 電源ケーブルの先に平行2極接地用口出線付変換プラグを取り付けます。

3. 平行2極接地用口出線付変換プラグを取り付けた電源ケーブルを、電源コンセントに差し込みます。

4.　アース線の先についているFG端子をコンセントのFGネジに取り付けます。

⚠警告

アース線は必ず接続してください。感電のおそれがあります。



こんな事に気をつけて

本装置は電源ケーブルを差し込むコンセントの近傍に設置し、電源ケーブルを容易に抜くことができるスペースを確保してください。

■ 電源を投入する

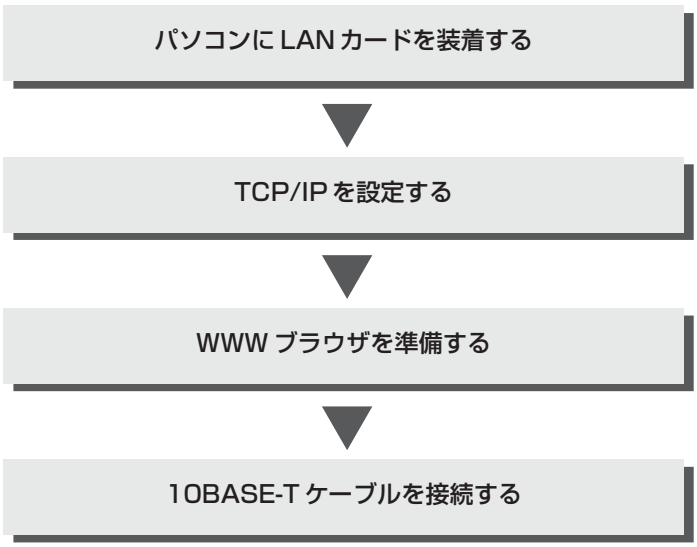
1.　本装置の電源を投入します。（「｜」側へ押します。）

2.　本装置が起動したことを確認します。

補足　電源を投入すると、本装置は自動的に装置の状態を診断します。このとき、CHECK／B1／B2／LANランプが点滅します。次にHUB以外のランプが同時に緑色で約2秒間点灯します。装置に異常がない場合は、CHECKランプが消灯して、起動が完了します。

パソコンを設定する

本装置の10BASE-Tポートにパソコンを接続して使用するための準備について説明します。



■ パソコンにLANカードを装着する

お使いのパソコンにLANポートがあることを確認してください。

LANポートがないパソコンの場合は、LANカードを取り付ける必要があります。パソコンやLANカードに添付されたマニュアルに従って、正しく設定をしてください。

■ TCP/IPを設定する

本装置を使うには、パソコンに「TCP/IP」というネットワークプロトコルモジュールをインストールしておく必要があります。

また、実際に通信するためには、パソコン側で以下の設定が必要です。

- IPアドレス
- ネットマスク
- DNSサーバアドレス
- デフォルトゲートウェイ
- ドメイン名

なお、本装置のDHCPサーバ機能を使用して、パソコン側で上記の設定を不要にすることもできます。

ただし、本装置のDHCPサーバ機能を使用し、UNIX®系OSをインストールしたパソコンをDHCPクライアントとして使用する場合に、本装置の詳細設定で設定反映後にパソコンの経路情報を変更しても、パソコン側に古い経路情報が残り、正しく通信できない場合があります。この場合、パソコンを再起動し、新しい経路情報をパソコンに反映させるか、パソコンのIPアドレスを固定にして使用してください。

ヒント

◆「TCP/IP」って何？

インターネットで利用されている標準の通信規約（プロトコル）をまとめて、TCP/IPと呼びます。

ここでは、Windows® 2000、Windows® XPおよびWindows Vista®のパソコンを設定する手順について説明します。

ほかのOSをお使いの場合は、パソコンまたはOSをご購入時に同梱のマニュアルを参照してください。

Windows®デスクトップの設定で「Webスタイル」を指定してある場合は、「ダブルクリック」と記載してあるところは「シングルクリック」で操作することができます。

パソコンの設定（Windows® 2000）

1.　［スタート］－［設定］－［コントロールパネル］をクリックします。

2.　［ネットワークとダイヤルアップ接続］をダブルクリックして開きます。

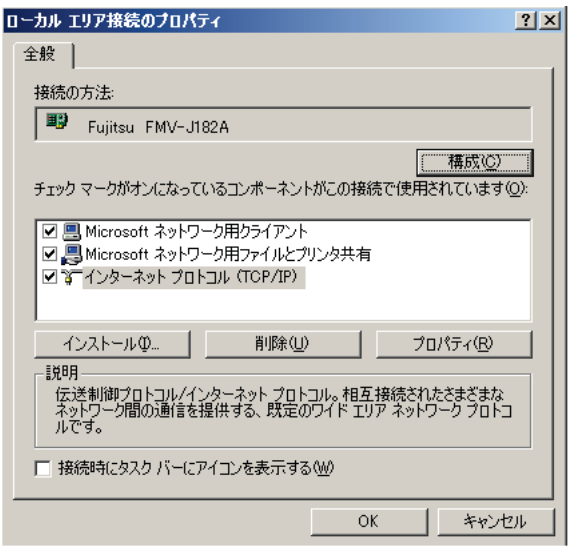
3.　［ローカルエリア接続］を右クリックし、［プロパティ］を選択します。

［ローカルエリア接続のプロパティ］ダイアログボックスが表示されます。

4.　一覧にインターネットプロトコル（TCP/IP）が存在していることを確認します。

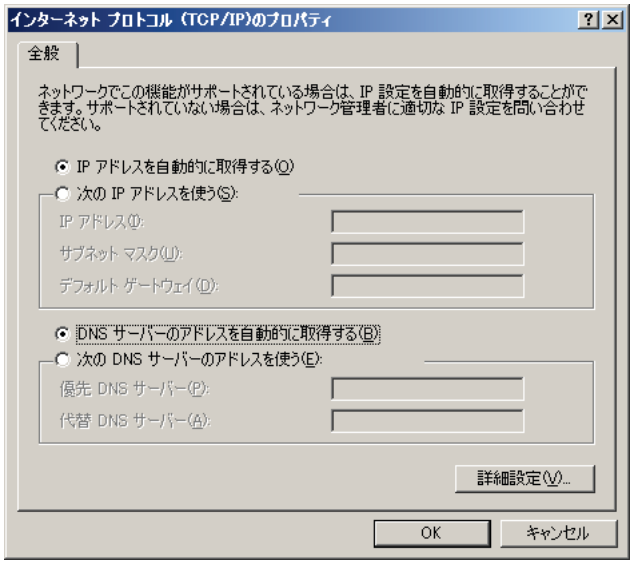
補足　一覧にTCP/IPが見つからない場合は、TCP/IPのインストールが必要です。Windows® 2000のマニュアルを参照して、インストールしてください。

5.　一覧から「インターネットプロトコル（TCP/IP）」を選択します。



6.　［プロパティ］ボタンをクリックします。

［インターネットプロトコル（TCP/IP）のプロパティ］ダイアログボックスが表示されます。



7.　パソコンのIPアドレスを指定します。

「次のIPアドレスを使う」を選択します。

IPアドレスを「192.168.1.2」、サブネットマスクを「255.255.255.0」、デフォルトゲートウェイを「192.168.1.1」に指定します。

8.　DNSサーバのIPアドレスを指定します。

「次のDNSサーバーのアドレスを使う」を選択します。

「優先DNSサーバー」に本装置のIPアドレス「192.168.1.1」を指定します。

9.　［OK］ボタンをクリックします。

［ローカルエリア接続のプロパティ］ダイアログボックスに戻ります。

10.　［OK］ボタンをクリックします。

パソコンを再起動するかを確認するメッセージが表示されます。

11.　［はい］ボタンをクリックし、パソコンを再起動します。

設定した内容は、再起動後に有効になります。

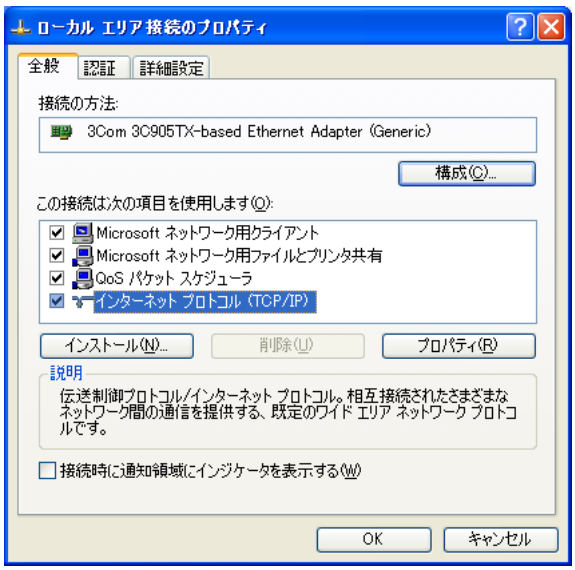
パソコンの設定（Windows® XP）

1. ［スタート］－［コントロールパネル］をクリックします。
2. ［ネットワーク接続とインターネット接続］をクリックします。
3. ［ネットワーク接続］をクリックします。
4. ［ローカルエリア接続］アイコンを右クリックし、［プロパティ］をクリックします。

   ［ローカルエリア接続のプロパティ］ダイアログボックスが表示されます。
5. 一覧にインターネットプロトコル（TCP/IP）が含まれていることを確認します。

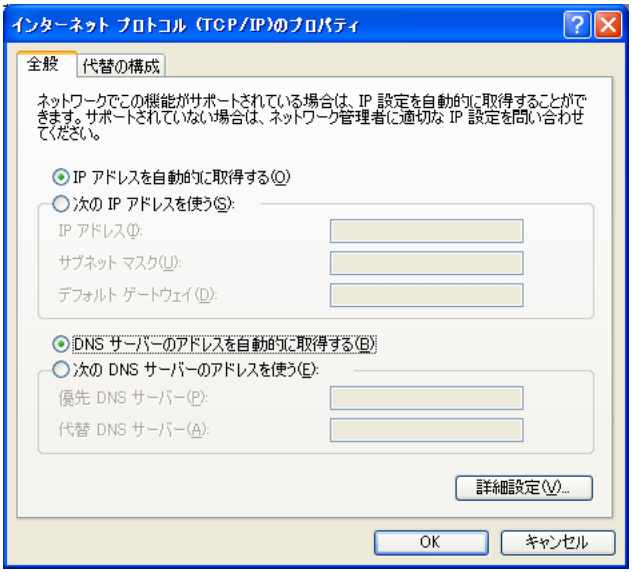
補足　一覧にTCP/IPが見つからない場合は、TCP/IPのインストールが必要です。Windows® XPのマニュアルを参照して、インストールしてください。

6. 一覧から「インターネットプロトコル（TCP/IP）」を選択します。



7.　［プロパティ］ボタンをクリックします。

［インターネットプロトコル（TCP/IP）のプロパティ］ダイアログボックスが表示されます。



8.　パソコンのIPアドレスを指定します。

「次のIPアドレスを使う」を選択します。

IPアドレスを「192.168.1.2」、サブネットマスクを「255.255.255.0」、デフォルトゲートウェイを「192.168.1.1」に指定します。

9.　DNSサーバのIPアドレスを指定します。

「次のDNSサーバーのアドレスを使う」を選択します。

「優先DNSサーバー」に本装置のIPアドレス「192.168.1.1」を指定します。

10.　［OK］ボタンをクリックします。

［ローカルエリア接続のプロパティ］ダイアログボックスに戻ります。

11.　［OK］ボタンをクリックします。

パソコンを再起動するかを確認するメッセージが表示されます。

12.　［はい］ボタンをクリックし、パソコンを再起動します。

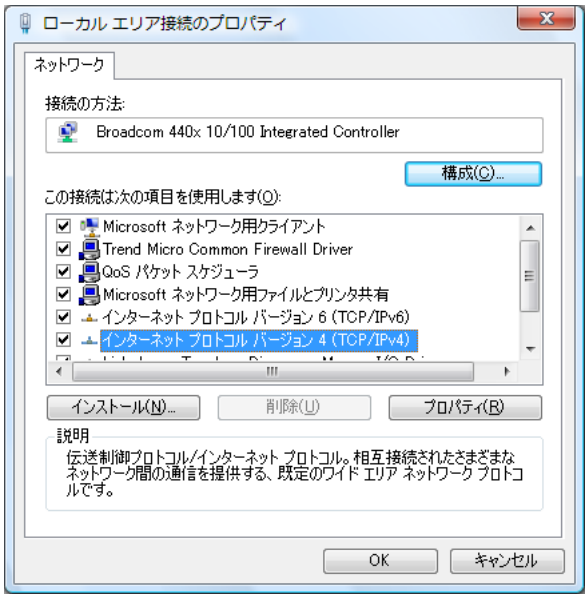
設定した内容は、再起動後に有効になります。

パソコンの設定（Windows Vista®）

1. ［スタート］－［コントロールパネル］をクリックします。
2. ［ネットワーク接続とインターネット接続］をクリックします。
3. ［ネットワークと共有センター］をクリックします。
4. ［ネットワーク接続の管理］をクリックします。
5. ［ローカルエリア接続］アイコンを右クリックし、［プロパティ］をクリックします。

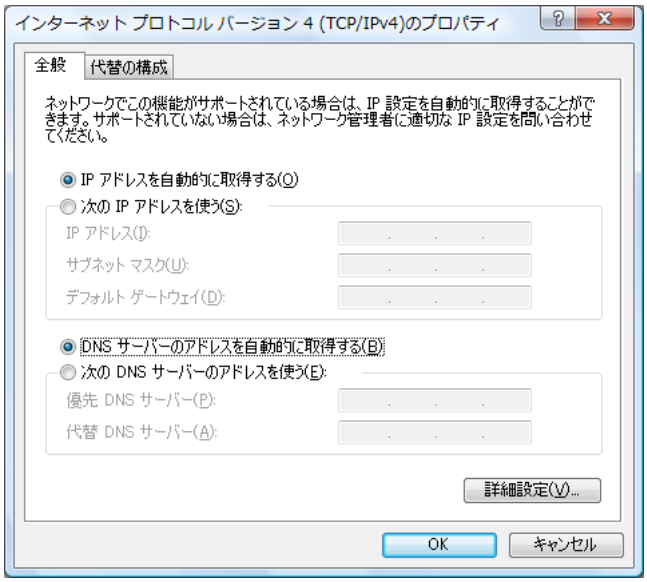
   ［ローカルエリア接続のプロパティ］ダイアログボックスが表示されます。
6. 一覧にインターネットプロトコルバージョン4（TCP/IPv4）が含まれていることを確認します。

   補足　一覧にTCP/IPが見つからない場合は、TCP/IPのインストールが必要です。Windows Vista®のマニュアルを参照して、インストールしてください。
7. 一覧から「インターネットプロトコルバージョン4（TCP/IPv4）」を選択します。



8.　［プロパティ］ボタンをクリックします。

［インターネットプロトコルバージョン4（TCP/IPv4）のプロパティ］ダイアログボックスが表示されます。



9.　パソコンのIPアドレスを指定します。

「次のIPアドレスを使う」を選択します。

IPアドレスを「192.168.1.2」、サブネットマスクを「255.255.255.0」、デフォルトゲートウェイを「192.168.1.1」に指定します。

10.　DNSサーバのIPアドレスを指定します。

「次のDNSサーバーのアドレスを使う」を選択します。

「優先DNSサーバー」に本装置のIPアドレス「192.168.1.1」を指定します。

11.　［OK］ボタンをクリックします。

［ローカルエリア接続のプロパティ］ダイアログボックスに戻ります。

12.　［OK］ボタンをクリックします。

パソコンを再起動するかを確認するメッセージが表示されます。

13.　［はい］ボタンをクリックし、パソコンを再起動します。

設定した内容は、再起動後に有効になります。

補足 IPアドレスなどの設定を確認する

IPアドレスやアダプタアドレス（MACアドレス）など現在のIP設定情報を確認できるコマンドがあります。

以下のように操作します。

• Windows® 95／98／Meの場合

1.［スタート］-［ファイル名を指定して実行］を選択します。

2.「winipcfg.exe」を指定します。

• Windows NT®、Windows® 2000 ／XP、Windows Vista®の場合

1.［スタート］-［アクセサリ］-［コマンドプロンプト］を選択します。

2.「ipconfig」を指定します。

■ WWWブラウザを準備する

本装置を利用するには、以下のWWWブラウザを使用してください。

- Microsoft® Internet Explorer Version 6.0
- Microsoft® Internet Explorer Version 7.0

ブラウザの設定が、「Proxy（プロキシ）サーバ機能」を利用しないようになっていることを確認してください。

以下のように確認します。

1.　Microsoft® Internet Explorerを起動します。

2.　「インターネットオプション」をクリックします。

- Microsoft® Internet Explorer 6.0の場合
  メニューバーの［ツール］をクリックします。
- Microsoft® Internet Explorer 7.0の場合
  ツールバーまたはメニューバーの［ツール］をクリックします。

3.　インターネットオプション画面の「接続」タブで、［LANの設定］ボタンをクリックします。

4.　プロキシサーバーの「LANにプロキシサーバーを使用する」が選択されていないことを確認します。

補足　Proxyサーバを使用する場合は、以下を参考にして本装置だけをProxyの対象外にしてください。

1.Microsoft® Internet Explorerを起動します。

2.「インターネットオプション」をクリックします。

- Microsoft® Internet Explorer 6.0の場合
  メニューバーの［ツール］をクリックします。
- Microsoft® Internet Explorer 7.0の場合
  ツールバーまたはメニューバーの［ツール］をクリックします。

3. インターネットオプション画面の「接続」タブで、［LANの設定］ボタンをクリックします。

4. プロキシサーバーの「LANにプロキシサーバーを使用する」が選択されていることを確認し、［詳細設定］ボタンをクリックします。

5.「HTTP」にプロバイダのProxyサーバを指定します。

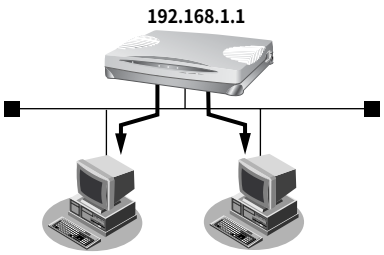
6. 例外の「次で始まるアドレスにはプロキシを使用しない」に本装置のIPアドレス（192.168.1.1）を指定します。

■ 10BASE-Tケーブルを接続する

「新規にLANを構築する場合」（P.61）と「既存のLANに組み込む場合」（P.63）を参考にして10BASE-Tケーブルを接続します。

新規にLANを構築する場合

新規にLANを構築する場合は、本装置のDHCPサーバ機能を利用してIPアドレスを割り当てることをお勧めします。



パソコンの起動時にアドレスを割り当てる

■ パソコンをつなぐ

本装置とパソコンを10BASE-Tケーブルでつなぎます。

補足　10BASE-Tポートにパソコンなどをつなぐ場合は、市販の10BASE-Tケーブル（LANケーブル）をお使いください。

⚠警告

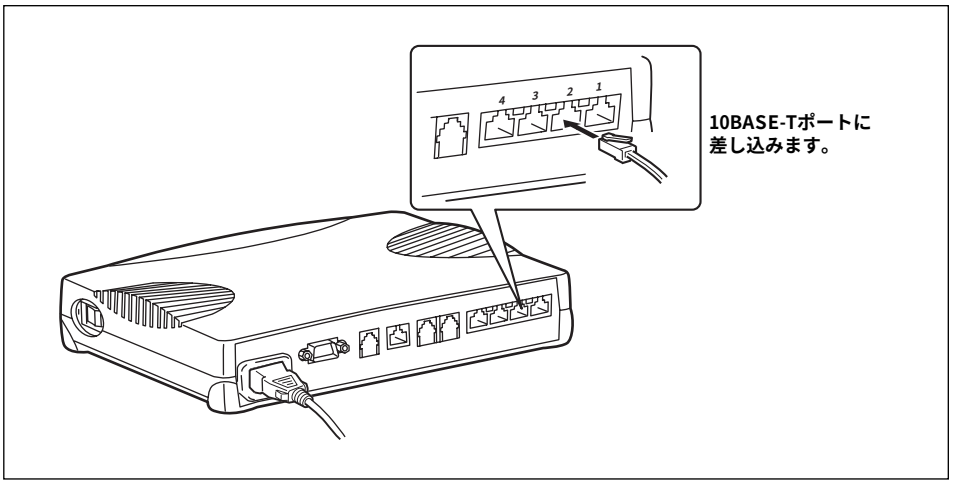
本装置および接続する機器の電源を切断してから、つないでください。

こんな事に気をつけて

- **本製品の10BASE-T（HUB）ポートに10／100BASE-TX機器（パソコン、ワークステーション、HUBなど）を接続してお使いになる場合は、接続機器のポートを“10Mbps／半二重（Half-Duplex）”にしてお使いになることをお勧めします。**
- **速度（10M／100M）および全二重／半二重（Full-Duplex／Half-Duplex）自動検出モードでお使いになると、正しく接続できないことがあります。万一、速度自動検出モードで正しく接続できない場合は、一度LANケーブルを抜き、機器の設定を“10Mbps／半二重（Half-Duplex）”に変更後、再度接続を行ってください。**

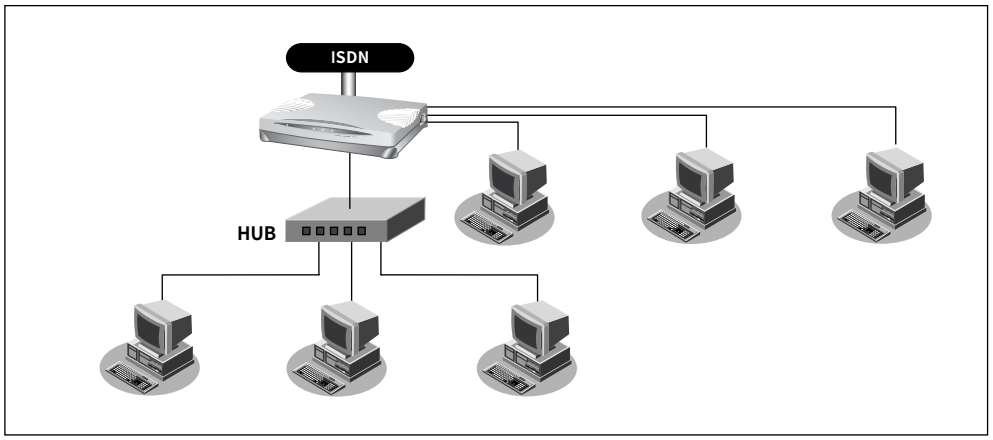
本装置にパソコンを1台だけつなぐ方法を説明します。本装置をネットワーク上の複数のパソコンで利用する場合も、1台のパソコンを一時的にネットワークから切り離し、本装置につないでから設定します。

1. パソコンの 10BASE-T ポートに 10BASE-T ケーブルの一方の端を差し込みます。
2. 本装置の 10BASE-T ポートに 10BASE-T ケーブルのもう一方の端を差し込みます。



■ HUB を使って LAN を構築する

HUB を使って LAN につなぐ場合は、以下のようにつなぎます。



⚠警告

本装置および接続する機器の電源を切断してから、つないでください。

1. 10BASE-T ケーブルで本装置の 10BASE-T ポート 1 と HUB のポートをつなぎます。
2. 本装置底面の HUB PORT1 スイッチを「to HUB」に切り替えます。
3. パソコンと HUB を 10BASE-T ケーブルでつなぎます。

既存のLANに組み込む場合

既存のLANに本装置を組み込む場合は、LAN内のIPアドレス割り当て方法に従って、本装置にIPアドレスを割り当てる必要があります。

☛ 参照 「DHCP機能を使う」（P.479）

■ ネットワークの状況を確認する

すでにネットワークを構築している場合は、ネットワーク上のホストのIPアドレスに注意して確認してください。

TCP/IPでは、ネットワーク上の各コンピュータ（慣例的にホストと言います）のIPアドレスと本装置のIPアドレスが重複すると、ホストと本装置間の通信ができなくなります。また、ネットワーク全体にも影響を与える場合がありますので、LAN上のほかのホストとIPアドレスが重複しないように、適切なIPアドレスに設定を変更する必要があります。本装置のご購入時のIPアドレスは「192.168.1.1」が設定されています。

各ホストのIPアドレスなどを静的に割り当てる場合は、IPアドレスが重複しないように設定してください。動的に割り当てる場合でも、DHCPサーバが割り当てるIPアドレスと本装置のIPアドレスが重複しないように設定を変更する必要があります。また、ブロードキャストアドレスは設定できません。

☛ 参照　使ってはいけないIPアドレス、ブロードキャストアドレス→「Q&A」（P.762）

ヒント

◆ TCP/IPによるネットワークでは、各ホストを識別するため、「IPアドレス」などの割り当てが必要です。

インターネットなどでたびたび出てくる「IPアドレス」は「ネットワーク部」と「ホスト部」の2つの要素から成り立っています。たとえば「192.168.1.10」というIPアドレスの場合、最初の「192.168.1.」までを「ネットワーク部」と言い、最後の「10」を「ホスト部」と言います（クラスCの場合）。

ネットワーク部が同じIPアドレスを持つホストは、同じネットワーク上にあると認識されます。さらに、ホスト部によって同一ネットワーク上の各ホストが識別されます。

したがって、「IPアドレス」を各ホストに割り当てるときは、以下のことを考慮しなければなりません。

- **同一ネットワークに含めるホストに対して、同じネットワーク部を与える**
- **ネットワーク部内では、ホスト部を重複させてはいけない**

■ IPアドレスを設定する

ここでは、電話機を使ってIPアドレスを設定する操作方法を説明します。

本装置のアナログポート（ポート1、ポート2）に接続したアナログ機器からIPアドレスの設定を行います。

☛ 参照 「アナログ機器をつなぐ」（P.46）

1.　本装置の電源を投入します。

2.　受話器を上げ、ツーという音が聞こえることを確認します。

3.　✱0✱810＋✱IPアドレス ✱ネットマスク ✱ブロードキャストアドレスをダイヤルします。

IPアドレス、ネットマスク、ブロードキャストアドレスの数字の区切りに✱を使います。

ブロードキャストアドレスは、指定するブロードキャストアドレスに対応する数値を以下の表から選択します。

選択値	ブロードキャストアドレスの設定
0	0.0.0.0
1	255.255.255.255
2	IPアドレス／ネットマスクから求められる ネットワークアドレス＋オール0
3	IPアドレス／ネットマスクから求められる ネットワークアドレス＋オール1

例）IPアドレスを「192.168.2.1」、ネットマスクを「24」、ブロードキャストアドレスを「3（ネットワークアドレス＋オール1）」に設定する場合

✱0✱810✱192✱168✱2✱1✱24✱3 をダイヤルします。

4.　ピッという音が2回とビジートーン（プープープーという話中の音）が聞こえます。

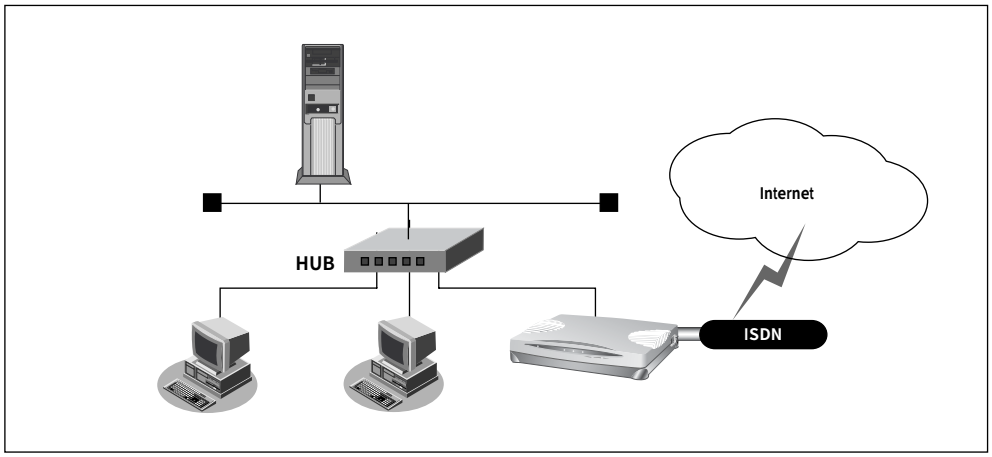
補足 正常に設定できなかった場合は、ビジートーン（プープープーという話中の音）だけが聞こえます。

5.　受話器を置きます。

■ 本装置をつなぐ

既存のLANに本装置を組み込みます。本装置とHUBを10BASE-Tケーブルでつなぎます。

補足 10BASE-Tポートにパソコンなどをつなぐ場合は、市販の10BASE-Tケーブル（LANケーブル）をお使いください。



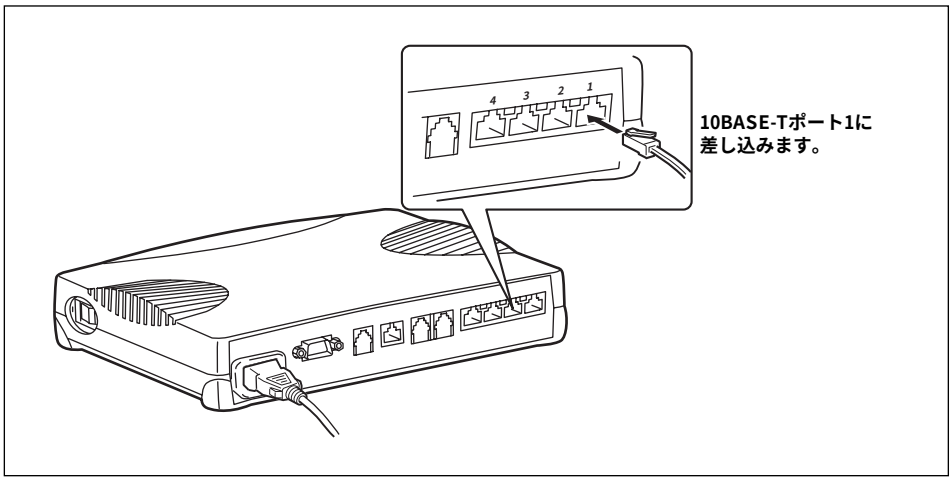
⚠警告

本装置および接続する機器の電源を切断してから、つないでください。

こんな事に気をつけて

- **本製品の10BASE-T（HUB）ポートに10／100BASE-TX機器（パソコン、ワークステーション、HUBなど）を接続してお使いになる場合は、接続機器のポートを“10Mbps／半二重（Half-Duplex）”にしてお使いになることをお勧めします。**
- **速度（10M／100M）および全二重／半二重（Full-Duplex／Half-Duplex）自動検出モードで使用すると、正しく接続できないことがあります。速度自動検出モードで正しく接続できない場合は、一度LANケーブルを抜き、機器の設定を“10Mbps／半二重（Half-Duplex）”に変更後、再度接続を行ってください。**

1.　10BASE-Tケーブルで本装置の10BASE-Tポート1とHUBのポートをつなぎます。



2.　本装置底面のHUB PORT1スイッチを「to HUB」に切り替えます。

第2章　設定

2

この章では、

本装置での基本的な設定方法を説明します。

設定を始める

■ 本装置とパソコンの電源を入れる

1.　本装置の電源を入れます。

2.　本装置が起動したことを確認します。

補足　電源が入ると、本装置は自動的に装置の状態を診断します。このとき、CHECK／B1／B2／LAN ランプが点滅します。次に HUB 以外のランプが同時に緑色で約 2 秒間点灯します。装置に異常がない場合は、CHECK ランプが消灯して、起動が完了します。

3.　パソコンの電源を入れます。

補足　IP アドレスなどの設定を確認する

IP アドレスやアダプタアドレス（MAC アドレス）など現在の IP 設定情報を確認できるコマンドがあります。

以下のように操作します。

• Windows® 95／98／Me の場合

1.［スタート］-［ファイル名を指定して実行］を選択します。

2.「winipcfg.exe」を指定します。

• Windows NT®、Windows® 2000 ／XP、Windows Vista®の場合

1.［スタート］-［アクセサリ］-［コマンドプロンプト］を選択します。

2.「ipconfig」を指定します。

⚠注意

本装置は、10BASE-T ポートに接続したパソコンからの要求によって、自動的にダイヤル発信を行い、回線を接続します。そのため、お客様がお使いになる機器、ソフトウェア、または LAN の利用条件によって、不要なダイヤル発信が行われ、回線が接続されてしまう場合があります。

すでに設定されている内容から、本装置が関係するネットワークの一部、またはすべてが変更になった場合は、本装置をいったんご購入時の状態に戻してから、設定し直してください。以前の設定が残っていると、お客様の意図しないダイヤル発信が行われたり、回線が接続できなかったりすることがあります。

■ WWW ブラウザを起動して本装置のトップページを表示させる

こんな事に気をつけて

本装置は IPv4 でだけ設定できます。

☛ 参照　WWW ブラウザの設定→「WWW ブラウザを準備する」(P.59)

1.　WWW ブラウザを起動します。

2.　本装置の URL「http://192.168.1.1/」を指定します。

本装置のトップページが表示されます。

画面上部のフレームに表示されるアイコンをクリックすると、ブラウザの表示が変わります。

（1）Si-Rロゴ	クリックすると、かんたんメニューが表示されます。
（2）［トップ］アイコン	クリックすると、かんたんメニューが表示されます。 かんたんメニューには「かんたん設定」と「かんたん操作」があります。 「かんたん設定」では、インターネットに接続するための基本設定ができます。 「かんたん操作」では、テレホーダイの開始／停止などができます。
（3）［詳細設定］アイコン	クリックすると、詳細設定メニューが表示されます。 詳細設定メニューには「ルータ設定」と「アナログ設定」があります。 「詳細設定」では、「かんたん設定」より詳細な情報を設定できます。 「アナログ設定」では、本装置に接続したアナログ機器の設定ができます。
（4）［操作］アイコン	クリックすると、操作メニューが表示されます。
（5）［表示］アイコン	クリックすると、表示メニューが表示されます。
（6）［メンテナンス］アイコン	クリックすると、メンテナンスメニューが表示されます。
（7）［編集終了］アイコン	クリックすると、すぐに設定操作を終了できます（ログインパスワードが設定されている場合だけ有効）。

☛ 参照 「操作メニューを使う」（P.603）、「表示メニューを使う」（P.611）、「メンテナンスメニューを使う」（P.628）

時計を設定する

本装置の設定を行う前に、必ず時計を設定してください。時計を設定する方法は、以下の2通りです。

- WWWブラウザで設定する
- 電話機を使って設定する（P.104）

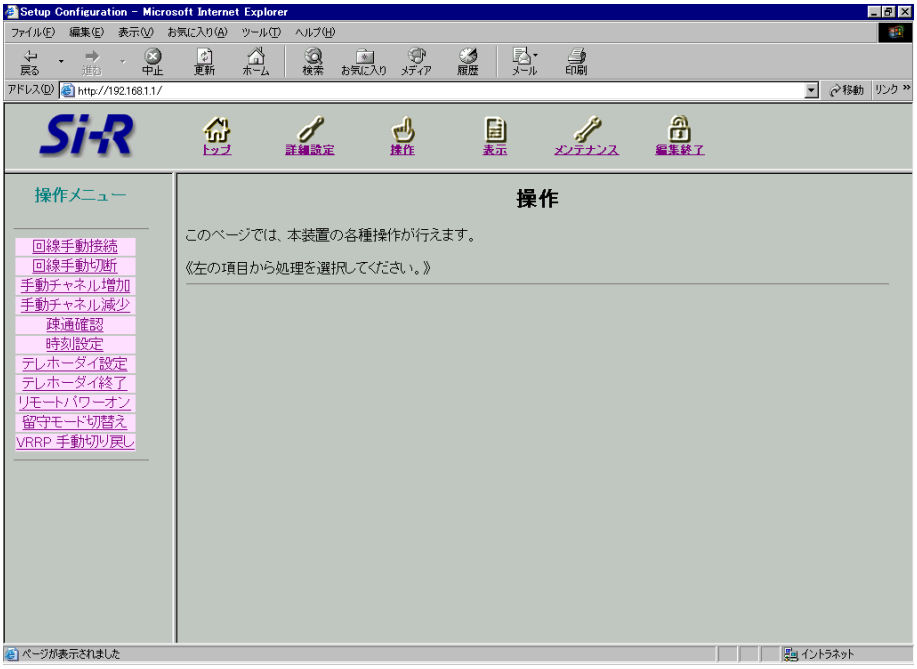
ここでは、WWWブラウザで設定する方法を説明します。操作メニューを使って、本装置の内部時計の時刻を設定します。

こんな事に気をつけて

24時間以上、電源を切ったままにすると時刻情報が失われます。

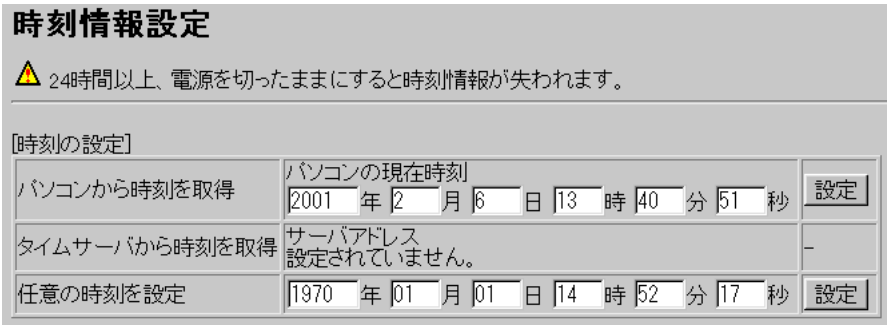
1.　本装置のトップページで、画面上部の［操作］アイコンをクリックします。

操作メニューが表示されます。



2.　操作メニューで「時刻設定」をクリックします。

「時刻情報設定」ページが表示されます。



3.　時計を設定する方法を以下の3つの中から選択します。

- パソコンから時刻を取得　→WWW ブラウザを利用しているパソコンの時刻を取得する
- タイムサーバから時刻を取得　→ネットワーク上のTIME サーバまたはNTP サーバから時刻を取得する
- 任意の時刻を設定　→現在の日時を入力する

4.　指定する時刻の設定方法の［設定］ボタンをクリックします。

「時刻を○○○○に設定しました。」というメッセージが表示されます。

設定方法を選ぶ

設定方法には「かんたん設定」と「詳細設定」の2つがあります。

通常のご利用では、「かんたん設定」で十分です。「かんたん設定」で設定したあとで、必要な設定に関しては「詳細設定」で設定を追加する方法をお勧めします。

補足 IPアドレスや時計の設定などは、アナログ機器でも行えます。

■「かんたん設定」で設定する場合

「かんたん設定」では、1つの画面で最小限の情報を設定するだけで本装置を使用できるようになります。『ルータ設定』と『アナログ設定』の2つがあります。

『ルータ設定』は、データ通信の設定ができます。以下の2つの接続形態があります。

(1)インターネット接続

プロバイダとの接続方法によって、以下を選択します。

- 端末型ダイヤルアップ接続の場合　→インターネットへ「ISDN接続」
  →インターネットへ「フレッツ・ISDN接続」
- 専用線接続の場合　→インターネットへ「専用線接続」

(2)事業所LANどうしを接続

接続方法によって、以下を選択します。

- ISDN接続の場合　→オフィスへ「ISDN接続」
- 専用線接続の場合　→オフィスへ「専用線接続」
- フレームリレー接続の場合　→オフィスへ「フレームリレー接続」

『アナログ設定』は、基本的なアナログ機器の設定ができます。

「かんたん設定」で設定する場合は、設定終了時に［設定終了］ボタンをクリックする必要があります。この場合、本装置が再起動され、通話中やデータ通信中の場合は通話およびデータ通信は切断されます。

■「詳細設定」で設定する場合

詳細設定は本装置のすべての定義が設定できます。

「詳細設定」で設定する場合は、「設定ページリファレンス」（P.183）を参照してください。

こんな事に気をつけて

- **「かんたん設定」を行ったあとに「詳細設定」を行うと、「かんたん設定」で設定した内容が変更されます。**
- **「詳細設定」を行ったあとに「かんたん設定」を行うと、「詳細設定」で設定した内容が変更されます。ただし、パスワード情報、アナログ情報、ファームウェア更新情報は有効です。**
- **詳細設定で設定した内容は、かんたん設定で確認できません。**

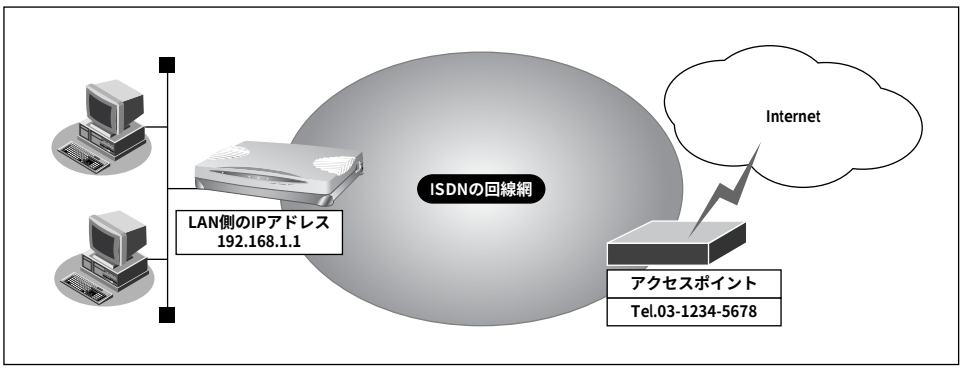
「かんたん設定」で設定する（インターネットへISDN接続のとき）

インターネットへISDN接続するときは、「かんたん設定」で［必須設定］の情報を設定するだけで接続できます。また、［オプション設定］の情報を設定すると、以下のことができます。

- 本装置のIPアドレスとLAN側のネットマスクの変更
- DNSサーバの設定
- 同一プロバイダのアクセスポイントを複数指定（マルチダイヤル）
- ISDN回線を自動切断するまでの時間の変更（無通信監視タイマ）
- 回線の切断タイミングの調整（課金単位時間）
- 接続ネットワーク名と接続先名の設定
- データの転送速度を早くする（MP-Multilink PPP）
- テレホーダイを手動で設定
- むだな通信料金の抑止（かんたんフィルタ）

☛ 参照 「用語集」（P.755）

ここでは、以下の条件を例に説明します。



● 設定条件

- 端末型ダイヤルアップ接続を行う
- 新規にLANを構築する
- 接続先の電話番号　：03-1234-5678
- ユーザ認証ID　：userid
- ユーザ認証パスワード　：userpass

こんな事に気をつけて

文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。
詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

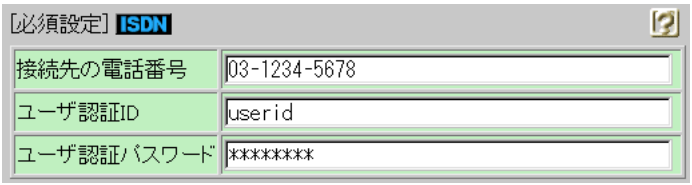
1. かんたん設定でインターネットへの「ISDN 接続」をクリックします。

「かんたん設定（インターネットへISDN 接続）」ページが表示されます。

補足 かんたんメニューは、本装置のトップページで画面上部の［トップ］アイコンをクリックして表示させることができます。

2. ［必須設定］で以下の項目を指定します。

- 接続先の電話番号　→03-1234-5678（プロバイダから提示された内容）
- ユーザ認証 ID　→userid（プロバイダから提示された内容）
- ユーザ認証パスワード　→userpass（プロバイダから提示された内容）



3. 必要に応じて、［オプション設定］で以下の項目を指定します。

- 本装置の IP アドレス　→192.168.1.1
- ネットマスク　→24
- DNS サーバ　→DNS サーバの IP アドレスが公開されていない場合、または DNS サーバアドレスの自動取得機能を利用する場合は「自動取得」を選択します。
  ただし、「自動取得」はプロバイダが DNS 自動取得に対応している場合だけ使用できます。
- 接続先の電話番号 2　→プロバイダのほかのアクセスポイントの電話番号 2
- 接続先の電話番号 3　→プロバイダのほかのアクセスポイントの電話番号 3

補足 「接続先の電話番号 2」、「接続先の電話番号 3」は、マルチダイヤル機能を利用する場合に設定します。

- 無通信監視タイマ　→初期設定値は 60 秒。必要に応じて変更します（0～3600 秒）。

補足 0 を指定した場合、回線の自動切断は行いません。

- 課金単位時間　→初期設定値は0秒。必要に応じて変更します（0～3600秒）。

補足 接続先までの課金単位に合わせて指定します。なお、0を設定した場合、課金単位の調整は行いません。たとえば、接続先までの電話料金が3分10円の場合、180秒をお勧めします。

- 接続ネットワーク名　→internet（接続するネットワークの名称を半角英数字8文字以内で入力します。接続先を区別するための任意の名称を指定します。）
- 接続先名　→ISP-1（プロバイダの名称を半角英数字8文字以内で入力します。接続先を区別するための任意の名称を指定します。）
- MP　→初期設定は「使用しない」。プロバイダがMPをサポートしていて、MPを使用する場合は「使用する」を選択します。
  - 使用する（手動）：操作メニューで「手動チャネル増加」を選択した場合にMPを使用
  - 使用する（自動）：通信量が多くなった場合に自動的にMPを使用

こんな事に気をつけて

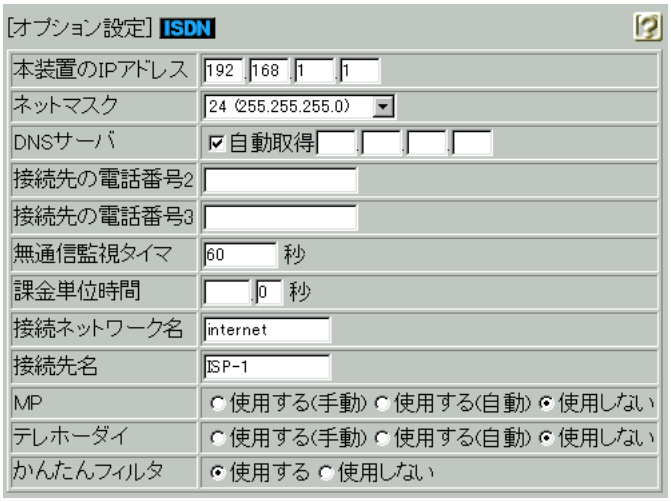
接続先のプロバイダがMPに対応していない場合は、MPでは通信できません。

- テレホーダイ　→初期設定は「使用しない」。テレホーダイを契約していて、テレホーダイを使用する場合は、「使用する」を選択します。
  - 使用する（手動）：操作メニューで「テレホーダイの設定」「テレホーダイ終了」で設定した時間帯にテレホーダイを使用
  - 使用する（自動）：毎日夜11:00～翌朝8:00の時間帯に自動的にテレホーダイを使用

補足 使用する（自動）を指定した場合、必ず装置の時刻を正しく設定してください。

- かんたんフィルタ　→初期設定は「使用する」。

補足 Windows® 環境でネットワークを構成している場合は、むだな課金が発生する場合があるため、「かんたんフィルタ」で「使用する」を選択することをお勧めします。



4.　設定が終了したら、［設定終了］ボタンをクリックします。

再起動後に、通信できる状態になります。

こんな事に気をつけて

- **本装置のIPアドレスを変更した場合、再起動後に本装置にアクセスするためには、パソコンのIPアドレスの変更（再起動）およびURLを変更する必要があります。**
- **本装置を既存のLANに接続する場合には、LAN上のほかのホストとIPアドレスが重複しないように適切なIPアドレスを設定してください。本装置のご購入時のIPアドレスは「192.168.1.1」が設定されています。**

⚠注意

本装置は、10BASE-Tポートに接続したパソコンからの要求によって、自動的にダイヤル発信を行い、回線を接続します。そのため、お客様がお使いになる機器、ソフトウェア、またはLANの利用条件によって、不要なダイヤル発信が行われ、回線が接続されてしまう場合があります。

インターネットに接続できることを確認する

設定が終わったら、インターネットに接続できるかどうかを確認します。

1.　WWWブラウザでURL「http://www.fujitsu.com」を入力します。

インターネットに接続できた場合は、富士通のページが表示されます。

ヒント

◆省略値について

かんたん設定時に適用される主な省略値を示します。

○：変更可能、×：変更不可

項　　目	適用される省略値	オプション設定での設定変更
自動ダイヤル	使用する	×
すべてのデータ通信の着信	許可しない	×
無通信監視タイマ	60秒	○
課金単位時間	なし	○
接続ネットワーク名	internet	○
接続先名	ISP-1	○
接続先のサブアドレス	なし	×
DHCP サーバ機能 ・割り当て先頭IPアドレス ・割り当てアドレス数 ・DNS サーバのIP アドレス	使用する 本装置のIP アドレス、ネットマスクから求めたネットワークアドレス＋2 64 「自動取得（※1）」指定時は、本装置のIP アドレス	×
NAT 機能	マルチ NAT を使用 アドレス割り当てタイマ：5分	×
MP 機能（※2）	使用しない	○
テレホーダイ	使用しない	○
かんたんフィルタ（※3）	使用する	○
ダイナミックルーティング ・RIP 送信（LAN 側） ・RIP 受信（LAN 側） ・RIP 送信（WAN 側） ・RIP 受信（WAN 側）	 送信しない 受信しない 送信しない 受信しない	×
スタティックルーティング ・LAN 側 ・WAN 側	 なし デフォルトルートを設定する（メトリック値：1）	×
データ圧縮	LZS：なし	×
ヘッダ圧縮	VJ-Compression：使用する IPヘッダ圧縮：使用しない	×
IPv6 ルーティング	使用しない	×
ブリッジ	使用しない	×
課金制御	上限　3,000 円	×
スケジュール	毎週金曜日 00:00 に課金情報クリア	×

※1）DNSサーバのIPアドレスを「自動取得」にした場合には、ProxyDNS情報が以下のように設定されます。

[順引き情報一覧]

優先順位	ドメイン名 タイプ 送信元IPアドレス／マスク	動　　作	ネットワーク名
1	＊ すべて any	接続先のDNSサーバへ問い合わせる	internet

[逆引き情報一覧]

優先順位	ネットワークアドレス	動　　作	ネットワーク名
1	any	接続先のDNSサーバへ問い合わせる	internet

※2）MP機能を「使用する（自動）」にした場合には、以下のように設定されます。

- アナログ使用時縮退　　：する
- トラフィックによる増減　　：する
- 回線増加条件　　：回線使用率（90%）、猶予時間（10秒）
- 回線削除条件　　：回線使用率（40%）、猶予時間（60秒）

※3）かんたんフィルタを「使用する」にした場合には、以下のように設定されます。

- Windows® 95／98／Me／2000、Windows NT® でMicrosoft Networkを使用する場合に、NetBIOS over TCPが使用するTCPおよびUDPのサービスポート137から139を遮断するフィルタを設定します。
- ping（ICMP echo）やsyslog、time、SNTPで使用するプロトコルを抑止するフィルタを設定します。なお、回線が接続状態の場合はそれぞれのパケットを通過させます。
- Windows® 2000から本装置を経由してインターネットへ接続する場合、Windows® 2000が送信する予期しないDNSパケットによって自動発信してしまう場合があります。この問題を回避するために、ProxyDNS情報に問い合わせタイプがSOA（6）、SRV（33）のDNSパケットを破棄するフィルタ、およびホストデータベース情報にIPアドレス「127.0.0.1」でホスト名「localhost」の情報を設定します。

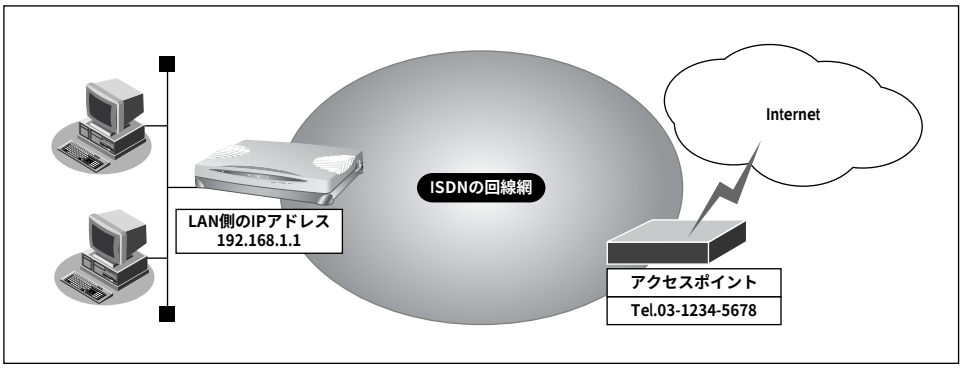
「かんたん設定」で設定する（インターネットへフレッツ・ISDN接続のとき）

インターネットへフレッツ・ISDN接続するときは、「かんたん設定」で［必須設定］の情報を設定するだけで接続できます。また、［オプション設定］の情報を設定すると、以下のことができます。

- 本装置のIPアドレスとLAN側のネットマスクの変更
- DNSサーバの設定
- ISDN回線を自動切断するまでの時間を変更（無通信監視タイマ）
- 接続ネットワーク名と接続先名の設定
- むだな通信料金の抑止（かんたんフィルタ）

☛参照 「用語集」（P.755）

ここでは、以下の条件を例に説明します。



● 設定条件

- 端末型ダイヤルアップ接続を行う
- 新規にLANを構築する
- 接続先の電話番号　：03-1234-5678
- ユーザ認証ID　：userid@nifty.com
- ユーザ認証パスワード　：userpass

こんな事に気をつけて

- **フレッツ・ISDNとは、NTTが提供するサービスです。定額料金でインターネットが使えます。フレッツ・ISDNを使用する場合は、NTTとの契約とフレッツ・ISDNに対応しているプロバイダとの契約が必要です。**
  フレッツ・ISDNでは、プロバイダのアクセスポイントに接続するのではなく、お申し込み後にNTTから通知された電話番号に接続します。
  またユーザ認証IDは「xxx@xxx.ne.jp」や「xxx@xxx.com」などの形式を使用しています。詳しくは、契約しているプロバイダに確認してください。
- **文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。**
  詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

1. かんたん設定でインターネットへの「フレッツ・ISDN接続」をクリックします。

「かんたん設定（インターネットへフレッツ・ISDN接続）」ページが表示されます。

補足 かんたんメニューは、本装置のトップページで画面上部の［トップ］アイコンをクリックして表示させることができます。

2. ［必須設定］で以下の項目を指定します。

- 接続先の電話番号　→03-1234-5678（NTTから通知された電話番号）
- ユーザ認証ID　→userid@nifty.com（プロバイダから提示された内容）
- ユーザ認証パスワード　→userpass（プロバイダから提示された内容）

3. 必要に応じて、［オプション設定］で以下の項目を指定します。

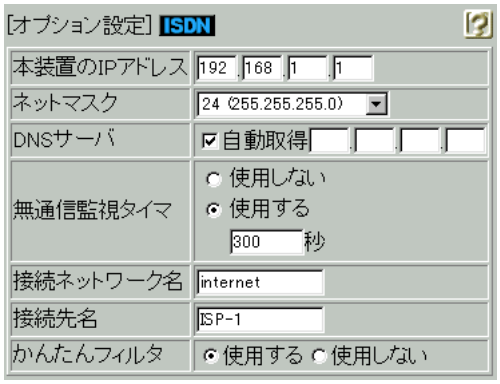
- 本装置のIPアドレス　→192.168.1.1
- ネットマスク　→24
- DNSサーバ　→DNSサーバのIPアドレスが公開されていない場合、またはDNSサーバアドレスの自動取得機能を利用する場合は「自動取得」を選択します。
  ただし、「自動取得」はプロバイダがDNS自動取得に対応している場合だけ使用できます。
- 無通信監視タイマ　→初期設定値は「使用する」、時間は300秒。必要に応じて変更します（0～3600秒）。

こんな事に気をつけて

0を指定した場合、回線の自動切断は行いません。

- 接続ネットワーク名　→internet（接続するネットワークの名称を半角英数字8文字以内で入力します。接続先を区別するための任意の名称を指定します。）
- 接続先名　→ISP-1（プロバイダの名称を半角英数字8文字以内で入力します。接続先を区別するための任意の名称を指定します。）
- かんたんフィルタ　→初期設定は「使用する」。

補足 Windows® 環境でネットワークを構成している場合は、むだな通信が発生する場合があるため、「かんたんフィルタ」で「使用する」を選択することをお勧めします。



4.　設定が終了したら、［設定終了］ボタンをクリックします。

再起動後に、通信できる状態になります。

こんな事に気をつけて

- **本装置のIPアドレスを変更した場合、再起動後に本装置にアクセスするためには、パソコンのIPアドレスの変更（再起動）およびURLを変更する必要があります。**
- **本装置を既存のLANに接続する場合には、LAN上のほかのホストとIPアドレスが重複しないように適切なIPアドレスを設定してください。本装置のご購入時のIPアドレスは「192.168.1.1」が設定されています。**

⚠注意

本装置は、10BASE-Tポートに接続したパソコンからの要求によって、自動的にダイヤル発信を行い、回線を接続します。そのため、お客様がお使いになる機器、ソフトウェア、またはLANの利用条件によって、不要なダイヤル発信が行われ、回線が接続されてしまう場合があります。

インターネットに接続できることを確認する

設定が終わったら、インターネットに接続できるかどうかを確認します。

1.　WWW ブラウザで URL「http://www.fujitsu.com」を入力します。

インターネットに接続できた場合は、富士通のページが表示されます。

ヒント

◆ 省略値について

かんたん設定時に適用される主な省略値を示します。

○：変更可能、×：変更不可

項　　目	適用される省略値	オプション設定での設定変更
自動ダイヤル	使用する	×
すべてのデータ通信の着信	許可しない	×
無通信監視タイマ	300 秒	○
接続ネットワーク名	internet	○
接続先名	ISP-1	○
接続先のサブアドレス	なし	×
DHCP サーバ機能 ・割り当て先頭 IP アドレス ・割り当てアドレス数 ・DNS サーバの IP アドレス	使用する 本装置の IP アドレス、ネットマスクから求めたネットワークアドレス＋2 64 「自動取得（※ 1）」指定時は、本装置の IP アドレス	×
NAT 機能	マルチ NAT を使用 アドレス割り当てタイマ：5 分	×
かんたんフィルタ（※ 2）	使用する	○
ダイナミックルーティング ・RIP 送信（LAN 側） ・RIP 受信（LAN 側） ・RIP 送信（WAN 側） ・RIP 受信（WAN 側）	 送信しない 受信しない 送信しない 受信しない	×
スタティックルーティング ・LAN 側 ・WAN 側	 なし デフォルトルートを設定する（メトリック値：1）	×
データ圧縮	LZS：なし	×
ヘッダ圧縮	VJ-Compression：使用する IP ヘッダ圧縮：使用しない	×
IPv6 ルーティング	使用しない	×
ブリッジ	使用しない	×
課金制御	なし	×
スケジュール	毎週金曜日 00:00 に課金情報クリア	×

※1）DNSサーバのIPアドレスを「自動取得」にした場合には、ProxyDNS情報が以下のように設定されます。

[順引き情報一覧]

優先順位	ドメイン名 タイプ 送信元IPアドレス／マスク	動　　作	ネットワーク名
1	＊ すべて any	接続先のDNSサーバへ問い合わせる	internet

[逆引き情報一覧]

優先順位	ネットワークアドレス	動　　作	ネットワーク名
1	any	接続先のDNSサーバへ問い合わせる	internet

※2）かんたんフィルタを「使用する」にした場合には、以下のように設定されます。

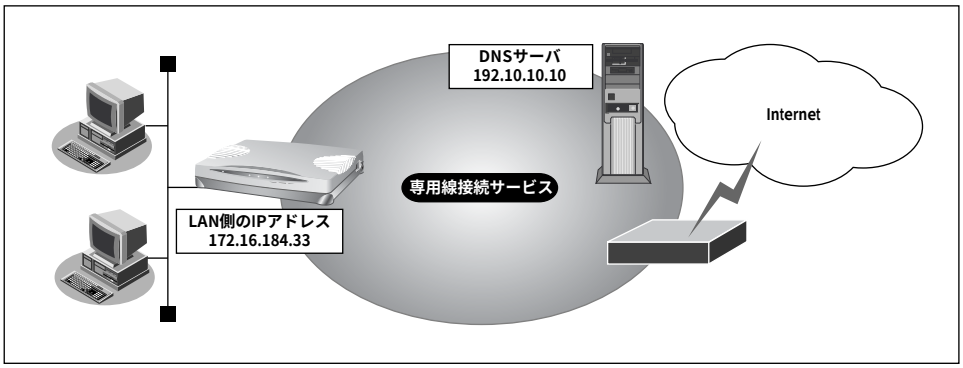
- Windows® 95／98／Me／2000、Windows NT®でMicrosoft Networkを使用する場合に、NetBIOS over TCPが使用するTCPおよびUDPのサービスポート137から139を遮断するフィルタを設定します。
- ping（ICMP echo）やsyslog、time、SNTPで使用するプロトコルを抑止するフィルタを設定します。なお、回線が接続状態の場合はそれぞれのパケットを通過させます。
- Windows® 2000から本装置を経由してインターネットへ接続する場合、Windows® 2000が送信する予期しないDNSパケットによって自動発信してしまう場合があります。この問題を回避するために、ProxyDNS情報に問い合わせタイプがSOA（6）、SRV（33）のDNSパケットを破棄するフィルタ、およびホストデータベース情報にIPアドレス「127.0.0.1」でホスト名「localhost」の情報を設定します。

「かんたん設定」で設定する（インターネットへ専用線接続のとき）

インターネットへ専用線接続するときは、「かんたん設定」で［必須設定］の情報を設定するだけで接続できます。また、［オプション設定］の情報を設定すると、以下のことができます。

- 接続ネットワーク名称の設定
- 契約時に指示されたドメイン名の設定
- アドレス変換の設定

ここでは、以下の設定条件で通信会社提供の専用線接続サービスを利用する場合を例に説明します。



● 設定条件

- 専用線（128Kbps）を使用する
- 新規にLANを構築する
- 通信会社側のDNSサーバを使用　：192.10.10.10
- 通信会社より提示されたドメイン名　：domain.carrier.ne.jp
- 接続するパソコンの台数は通信会社より割り当てられたIPアドレスよりも少ない
- 割当てIPアドレス
  ネットワークアドレス　：172.16.184.32/29
  本装置のIPアドレス　：172.16.184.33
  ホストアドレス　：172.16.184.34～172.16.184.38
  ブロードキャストアドレス　：172.16.184.39

こんな事に気をつけて

文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。
詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

1.　かんたん設定でインターネットへの「専用線接続」をクリックします。

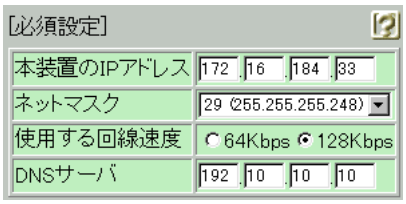
「かんたん設定（インターネットへ専用線接続）」ページが表示されます。

2.　［必須設定］で以下の項目を指定します。

こんな事に気をつけて

本装置のIPアドレスにネットワークアドレス、またはブロードキャストアドレスを指定しないでください。

- 本装置のIPアドレス　→172.16.184.33（割り当てられたホストアドレスの先頭）
- ネットマスク　→29（ネットマスクのビット数）
- 使用する回線速度　→128Kbps
- DNSサーバ　→192.10.10.10（通信会社から提示されたIPアドレス）



3.　必要に応じて、［オプション設定］で以下の項目を指定します。

- 接続ネットワーク名　→internet（接続するネットワークの名称を半角英数字8文字以内で入力します。接続先を区別するため任意の名称を指定します。）
- ドメイン名　→domain.carrier.ne.jp（通信会社より提示されたドメイン名）
- アドレス変換　→初期値は「使用しない」。
- アドレス個数　→アドレス変換で「マルチNAT」を指定した場合は、グローバルアドレスの個数を指定します。

補足　この例のように割り当てられたIPアドレスよりも接続するパソコンの台数が同数または少ない場合、「使用しない」を選択します。割り当てられたIPアドレスより接続するパソコンの台数が多い場合は、「マルチNAT」を選択すると、すべてのパソコンがインターネットを利用できます。その際は、「グローバルアドレス」と「アドレス個数」を設定します。

4.　設定が終了したら、［設定終了］ボタンをクリックします。

再起動後に、通信できる状態になります。

こんな事に気をつけて

- **本装置のIPアドレスを変更した場合、再起動後に本装置にアクセスするためには、パソコンのIPアドレスの変更（再起動）およびURLを変更する必要があります。**
- **本装置を既存のLANに接続する場合には、LAN上のほかのホストとIPアドレスが重複しないように適切なIPアドレスを設定してください。本装置のご購入時のIPアドレスは「192.168.1.1」が設定されています。**

ヒント

◆「マルチNAT」機能が便利

専用線接続サービスの契約時に割り当てられたIPアドレスの個数より、パソコンの台数が多い場合は、本装置の「マルチNAT機能」が便利です。「マルチNAT機能」によって、実際に割り当てられたIPアドレスの数を上回る台数のLAN上のパソコンでインターネットを利用できるようになります。

◆マルチNAT

本装置では、インターネットを利用する際に、プロバイダより割り当てられたIPアドレス（グローバルアドレス）と、ネットワーク上で設定したIPアドレス（プライベートアドレス）を対応付けることによって、従来のネットワークの設定を変更することなくインターネット接続ができるアドレス変換（NAT）機能をサポートしています。

NAT機能は、プライベートアドレスとグローバルアドレスを1対1に対応付けるもので、NAT機能を介して通信できるパソコンの台数は割り当てられるIPアドレスと同じになります。このため、プロバイダと端末型ダイヤルアップ契約の場合、1つしかIPアドレスが割り当てられないので、同時接続台数が1台に制限されます。

マルチNATは、この問題を解決するために1対1の対応付けから、多対1の対応付けを実現した機能です。IPアドレスとポート番号を組み合わせたIP情報の割り当てを行うことによって、プライベートアドレスとグローバルアドレスとを多対1に対応付け、同時に複数のパソコンからの利用が可能となります。

☛ 参照 「マルチNAT機能（アドレス変換機能）を使う」（P.490）

インターネットに接続できることを確認する

設定が終わったら、インターネットに接続できるかどうかを確認します。

1. WWW ブラウザで URL「http://www.fujitsu.com」を入力します。

インターネットに接続できた場合は、富士通のページが表示されます。

ヒント

◆ 省略値について

かんたん設定時に適用される主な省略値を示します。

○：変更可能、×：変更不可

項　　目	適用される省略値	オプション設定での設定変更
ブロードキャストアドレス	ネットワークドレス＋オール 1	×
接続ネットワーク名	internet	○
DHCP サーバ機能 ・割り当て先頭IPアドレス ・割り当てアドレス数	使用する 本装置の IP アドレス、ネットマスクから求めたネットワークアドレス＋ 2 64	×
NAT 機能	使用しない（※ 1）	○
かんたんフィルタ	使用しない	×
ダイナミックルーティング ・RIP 送信（LAN 側） ・RIP 受信（LAN 側） ・RIP 送信（WAN 側） ・RIP 受信（WAN 側）	 送信しない 受信しない 送信しない 受信しない	×
スタティックルーティング ・LAN 側 ・WAN 側	 なし デフォルトルートを設定する（メトリック値：1）	×
データ圧縮	LZS：なし	×
ヘッダ圧縮	VJ-Compression：使用する IP ヘッダ圧縮：使用しない	×
IPv6 ルーティング	使用しない	×
ブリッジ	使用しない	×

※ 1）マルチ NAT 使用時のアドレス割り当てタイマは 5 分を設定します。

「かんたん設定」で設定する（オフィスへISDN接続のとき）

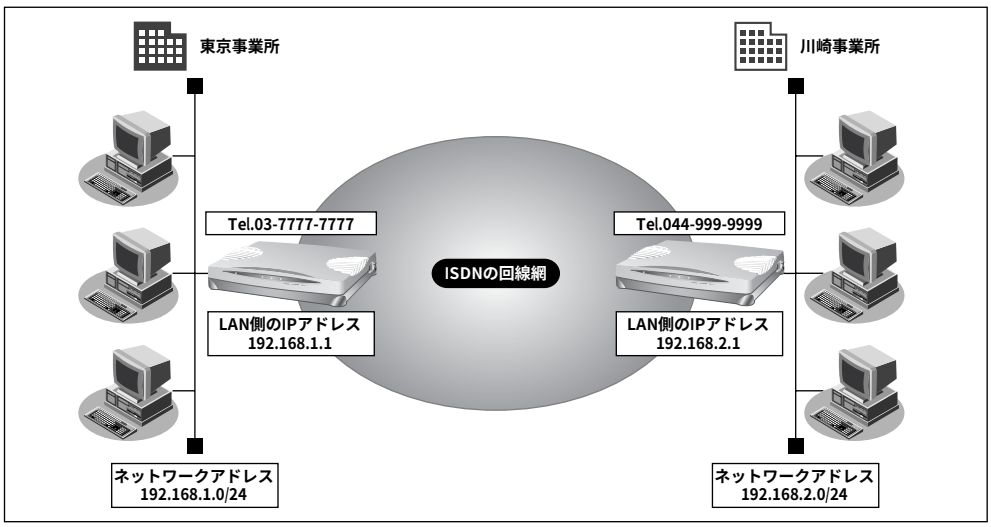
事業所LANどうしをISDNで接続するときは、「かんたん設定」で［必須設定］の情報を設定するだけで接続できます。また、［オプション設定］の情報を設定すると、以下のことができます。

- DHCPサーバ機能の設定
- ISDN回線を自動切断するまでの時間の変更（無通信監視タイマ）
- 回線の切断タイミングの調整（課金単位時間）
- 接続ネットワーク名と接続先名の設定
- データの転送速度を早くする（MP-Multilink PPP）
- 送受信するヘッダの圧縮

☛ 参照 「用語集」（P.755）

ここでは、ISDN回線を介して2つの事業所（東京、川崎）のネットワークを接続する場合を例に説明します。

補足 「詳細設定」で設定する場合や基幹ネットワーク（大規模ネットワーク）に接続する場合は、「事業所LANをISDNで接続する」（P.115）を参照してください。



● 設定条件

- DHCP サーバ機能は使用しない

[東京事業所]

- 電話番号　：03-7777-7777
- ユーザ認証 ID とユーザ認証パスワード
  発信　：tokyo、tokyopass
  着信　：kawasaki、kawapass
- LAN 側のネットワークアドレス／ネットマスク
  ：192.168.1.0/24
  （本装置の IP アドレス：192.168.1.1）

[川崎事業所]

- 電話番号　：044-999-9999
- ユーザ認証 ID とユーザ認証パスワード
  発信　：kawasaki、kawapass
  着信　：tokyo、tokyopass
- LAN 側のネットワークアドレス／ネットマスク
  ：192.168.2.0/24
  （本装置の IP アドレス：192.168.2.1）

こんな事に気をつけて

文字入力フィールドでは半角文字（0 ～ 9、A ～ Z、a ～ z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。
詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

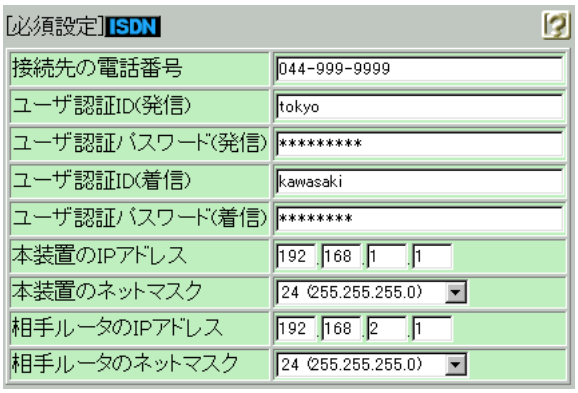
東京事業所の本装置を設定する

1.　かんたん設定でオフィスへの「ISDN 接続」をクリックします。

「かんたん設定（オフィスへISDN 接続）」ページが表示されます。

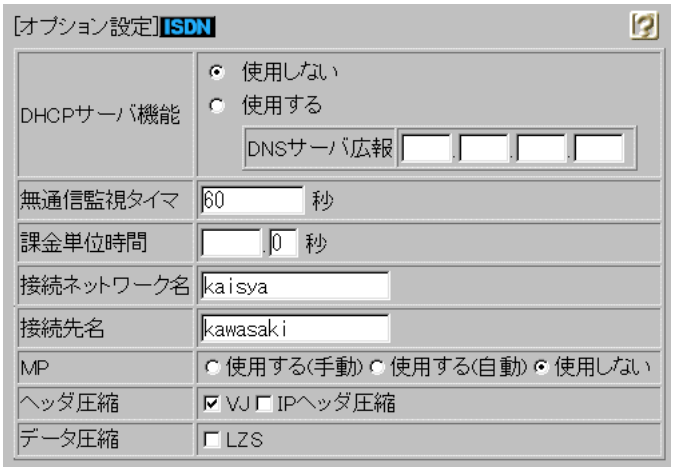
2.　［必須設定］で以下の項目を指定します。

- 接続先の電話番号　→044-999-9999
- ユーザ認証 ID（発信）　→tokyo
- ユーザ認証パスワード（発信）　→tokyopass
- ユーザ認証 ID（着信）　→kawasaki
- ユーザ認証パスワード（着信）　→kawapass
- 本装置の IP アドレス　→192.168.1.1（既存の LAN につなぐときは適宜変更）
- 本装置のネットマスク　→24（既存の LAN につなぐときは適宜変更）
- 相手ルータの IP アドレス　→192.168.2.1（接続先となる本装置のネットワークアドレス）
- 相手ルータのネットマスク　→24（接続先となる本装置のネットマスク）



3.　［オプション設定］で以下の項目を指定します。

- DHCP サーバ機能　→使用しない
- 接続ネットワーク名　→kaisya（接続するネットワークの名称を半角英数字8文字以内で入力します。接続先を区別するため任意の名称を指定します。）
- 接続先名　→kawasaki（接続先の名称を半角英数字 8 文字以内で入力します。接続先を区別するための任意の名称を指定します。）



4.　設定が終了したら、［設定終了］ボタンをクリックします。

再起動後に、通信できる状態になります。

こんな事に気をつけて

- **本装置の IP アドレスを変更した場合、再起動後に本装置にアクセスするためには、パソコンの IP アドレスの変更（再起動）および URL を変更する必要があります。**
- **本装置を既存の LAN に接続する場合には、LAN 上のほかのホストと IP アドレスが重複しないように適切な IP アドレスを設定してください。本装置のご購入時の IP アドレスは「192.168.1.1」が設定されています。**

川崎事業所の本装置を設定する

「東京事業所の本装置を設定する」を参考に、川崎事業所の本装置を設定します。その際、特に指定のないものは、東京事業所と同じ設定にします。

補足　設定が終わったら、［設定終了］ボタンをクリックします。

［必須設定］

- 接続先の電話番号　→03-7777-7777
- ユーザ認証ID（発信）　→kawasaki
- ユーザ認証パスワード（発信）　→kawapass
- ユーザ認証ID（着信）　→tokyo
- ユーザ認証パスワード（着信）　→tokyopass
- 本装置のIPアドレス　→192.168.2.1（本装置のLAN側のIPアドレス）
- 本装置のネットマスク　→24
- 相手ルータのIPアドレス　→192.168.1.1（接続先となる本装置のネットワークアドレス）
- 相手ルータのネットマスク　→24（接続先となる本装置のネットマスク）

［オプション設定］

- 接続ネットワーク名　→kaisya（接続するネットワークの名称）
- 接続先名　→tokyo

通信する

WWWブラウザや電子メールソフトなどの通信用アプリケーションを起動しておきます。通信が必要な状態になると、本装置が自動的に回線を接続します。

⚠注意

本装置は、10BASE-Tポートに接続したパソコンからの要求によって、自動的にダイヤル発信を行い、回線を接続します。そのため、お客様がお使いになる機器、ソフトウェア、またはLANの利用条件により、不要なダイヤル発信が行われ、回線が接続されてしまう場合があります。本装置の表示メニューで、課金情報を定期的にチェックしてください。

補足　「かんたん設定」で設定した初期設定の状態では、約60秒間データの送受信が行われない場合、自動的に回線を切断します。

ヒント

◆省略値について

かんたん設定時に適用される主な省略値を示します。

○：変更可能、×：変更不可

項　　目	適用される省略値	オプション設定での設定変更
自動ダイヤル	使用する	×
サブアドレス	なし	×
不特定相手着信	許可しない	×
無通信監視タイマ	60秒	○
課金単位時間	なし	○
接続ネットワーク名	localnet	○
接続先名	OFFICE-1	○
該当接続先への着信許可	許可する	×
DHCPサーバ機能 ・割り当て先頭IPアドレス ・割り当てアドレス数	使用する 本装置のIPアドレス、ネットマスクから求めたネットワークアドレス＋2 64	○
NAT機能	使用しない	×
MP機能	使用しない	○
かんたんフィルタ	使用しない	×
ダイナミックルーティング ・RIP送信（LAN側） ・RIP受信（LAN側） ・RIP送信（WAN側） ・RIP受信（WAN側）	 送信しない 受信しない 送信しない 受信しない	×
スタティックルーティング ・LAN側 ・WAN側	 なし 相手ルータのIPアドレス、ネットマスクを元にスタティックルートを設定する	×
データ圧縮	LZS：なし	○
ヘッダ圧縮	VJ-Compression：使用する IPヘッダ圧縮：使用しない	○
IPv6ルーティング	使用しない	×
ブリッジ	使用しない	×
課金制御	上限　3,000円	×
スケジュール	毎週金曜日 00:00 に課金情報クリア	×

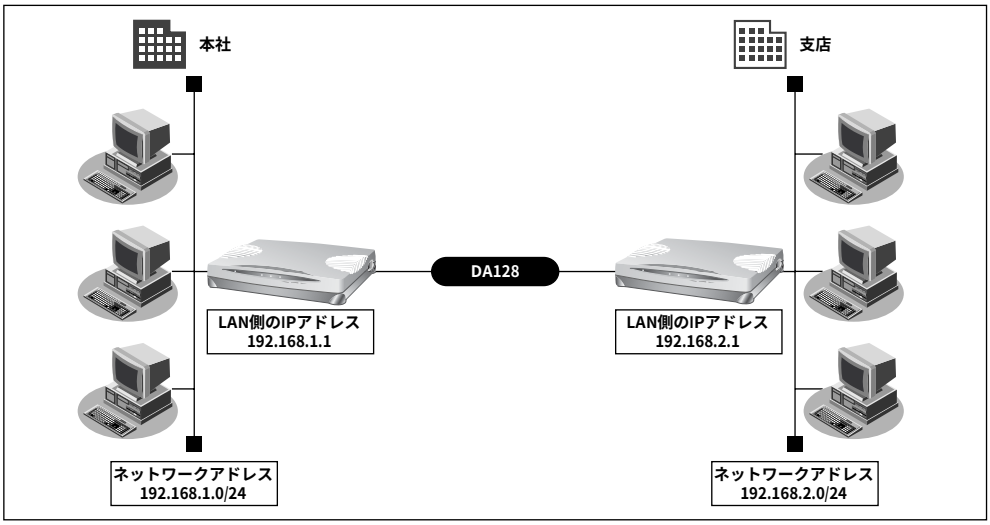
「かんたん設定」で設定する（オフィスへ専用線接続のとき）

事業所LANどうしを専用線で接続するときは、「かんたん設定」で［必須設定］の情報を設定するだけで接続できます。また、［オプション設定］の情報を設定すると、以下のことができます。

- 接続ネットワーク名の設定
- DHCPサーバ機能の設定
- 送受信するヘッダの圧縮

ここでは、専用線（HSD128Kbps）を介して2つの事業所（本社、支店）のネットワークを接続する場合を例に説明します。

補足 「詳細設定」で設定する場合や基幹ネットワーク（大規模ネットワーク）に接続する場合は、「事業所LANを専用線で接続する」（P.135）を参照してください。



● 設定条件

［本社］

- 専用線（128Kbps）を使用する
- DHCPサーバ機能は使用しない
- アドレス変換は使用しない
- LAN側のネットワークアドレス／ネットマスク　：192.168.1.0/24
- 本装置のIPアドレス　：192.168.1.1

［支店］

- LAN側のネットワークアドレス／ネットマスク　：192.168.2.0/24
- 本装置のIPアドレス　：192.168.2.1

こんな事に気をつけて

文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。
詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

本社の本装置を設定する

1. かんたん設定でオフィスへの「専用線接続」をクリックします。

「かんたん設定（オフィスへ専用線接続）」ページが表示されます。

2. ［必須設定］で以下の項目を指定します。

- 本装置のIPアドレス　→192.168.1.1（既存のLANにつなぐときは適宜変更）
- 本装置のネットマスク　→24（既存のLANにつなぐときは適宜変更）
- 相手ルータのIPアドレス　→192.168.2.1（接続先となる本装置のIPアドレス）
- 相手ルータのネットマスク　→24（接続先となる本装置のネットマスク）
- 使用する回線速度　→128Kbps

3. ［オプション設定］で以下の項目を指定します。

- 接続ネットワーク名　→kaisya（接続するネットワークの名称を半角英数字8文字以内で入力します。接続先を区別するため任意の名称を指定します。）
- DHCPサーバ機能　→使用しない

4. 設定が終了したら、［設定終了］ボタンをクリックします。

再起動後に、通信できる状態になります。

こんな事に気をつけて

- **本装置のIPアドレスを変更した場合、再起動後に本装置にアクセスするためには、パソコンのIPアドレスの変更（再起動）およびURLを変更する必要があります。**
- **本装置を既存のLANに接続する場合には、LAN上のほかのホストとIPアドレスが重複しないように適切なIPアドレスを設定してください。本装置のご購入時のIPアドレスは「192.168.1.1」が設定されています。**

支店の本装置を設定する

「本社の本装置を設定する」を参考に、支店の本装置を設定します。その際、特に指定のないものは、本社と同じ設定にします。

補足　設定が終わったら、［設定終了］ボタンをクリックします。

［必須設定］

- 本装置のIPアドレス　→192.168.2.1（本装置のLAN側のIPアドレス）
- 本装置のネットマスク　→24
- 相手ルータのIPアドレス　→192.168.1.1（接続先となる本装置のIPアドレス）
- 相手ルータのネットマスク　→24（接続先となる本装置のネットマスク）
- 使用する回線速度　→128Kbps

［オプション設定］

- 接続ネットワーク名　→kaisya（接続するネットワークの名称）
- DHCPサーバ機能　→使用しない

ヒント

◆省略値について

かんたん設定時に適用される主な省略値を示します。

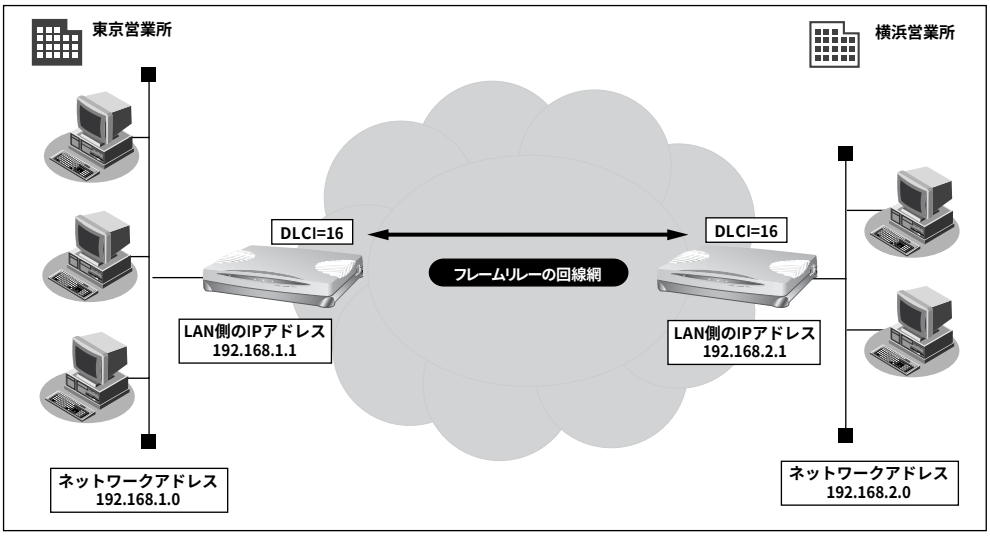
○：変更可能、×：変更不可

項　　目	適用される省略値	オプション設定での設定変更
接続ネットワーク名	localnet	○
DHCP サーバ機能 ・割り当て先頭アドレス ・割り当てアドレス数	使用する 本装置の IP アドレス、ネットマスクから求めたネットワークアドレス＋ 2 64	○
NAT 機能	使用しない	×
かんたんフィルタ	使用しない	×
ダイナミックルーティング ・RIP 送信（LAN 側） ・RIP 受信（LAN 側） ・RIP 送信（WAN 側） ・RIP 受信（WAN 側）	 送信しない 受信しない 送信しない 受信しない	×
スタティックルーティング ・LAN 側 ・WAN 側	 なし 相手ルータの IP アドレス、ネットマスクを元にスタティックルートを設定する	×
データ圧縮	LZS：なし	○
ヘッダ圧縮	VJ-Compression：使用する IP ヘッダ圧縮：使用しない	○
IPv6 ルーティング	使用しない	×
ブリッジ	使用しない	×

「かんたん設定」で設定する（オフィスへフレームリレー接続のとき）

事業所LANどうしをフレームリレーで接続する場合の設定方法を説明します。

フレームリレーを利用すると複数の事業所のLANと接続が可能になり、高速にデータの転送が行えます。また、相手先ごとに固定的な回線を接続するので、公衆網であるフレームリレー網に閉域ネットワークを構築することができ、セキュリティの確保にも適しています。



● 設定条件

[東京営業所]

- DLCI　：16
- CIR　：32Kbps
- DHCPサーバ機能は使用しない
- LAN側のネットワークアドレス／ネットマスク　：192.168.1.0/24
- 本装置のIPアドレス　：192.168.1.1

[横浜営業所]

- DLCI　：16
- CIR　：32Kbps
- DHCPサーバ機能は使用しない
- LAN側のネットワークアドレス／ネットマスク　：192.168.2.0/24
- 本装置のIPアドレス　：192.168.2.1

こんな事に気をつけて

文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。
詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

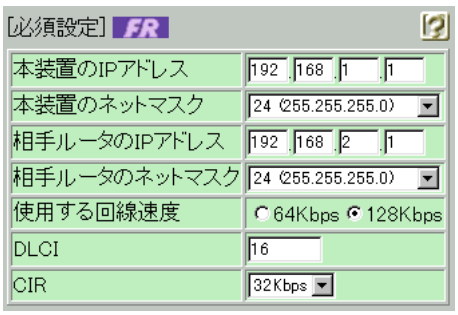
東京営業所の本装置を設定する

1. かんたん設定でオフィスへの「フレームリレー接続」をクリックします。

「かんたん設定（オフィスへフレームリレー接続）」ページが表示されます。

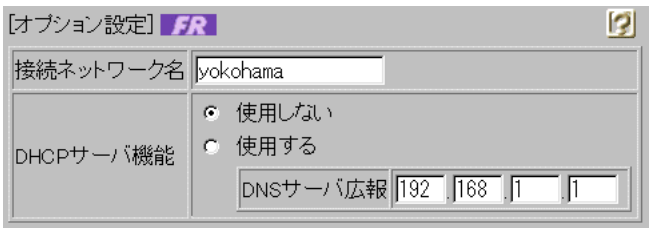
2. ［必須設定］で以下の項目を指定します。

- 本装置のIPアドレス　→192.168.1.1（既存のLANにつなぐときは適宜変更）
- 本装置のネットマスク　→24（既存のLANにつなぐときは適宜変更）
- 相手ルータのIPアドレス　→192.168.2.1（接続先となる本装置のIPアドレス）
- 相手ルータのネットマスク　→24（接続先となる本装置のネットマスク）
- 使用する回線速度　→128Kbps
- DLCI　→16
- CIR　→32Kbps



3. ［オプション設定］で以下の項目を指定します。

- 接続ネットワーク名　→yokohama（接続するネットワークの名称を半角英数字8文字以内で入力します。接続先を区別するため任意の名称を指定します。）
- DHCPサーバ機能　→使用しない



4.　設定が終了したら、［設定終了］ボタンをクリックします。

再起動後に、通信できる状態になります。

横浜営業所の本装置を設定する

「東京営業所の本装置を設定する」を参考に、横浜営業所の本装置を設定します。その際、特に指定のないものは、東京営業所と同じ設定にします。

補足　設定が終わったら、［設定終了］ボタンをクリックします。

［必須設定］

- 本装置のIPアドレス　→192.168.2.1（本装置のLAN側のIPアドレス）
- 本装置のネットマスク　→24
- 相手ルータのIPアドレス　→192.168.1.1（接続先となる本装置のIPアドレス）
- 相手ルータのネットマスク　→24（接続先となる本装置のネットマスク）
- 使用する回線速度　→128Kbps
- DLCI　→16
- CIR　→32Kbps

［オプション設定］

- 接続ネットワーク名　→tokyo（接続するネットワークの名称）
- DHCPサーバ機能　→使用しない

ヒント

◆省略値について

かんたん設定時に適用される主な省略値を示します。

○：変更可能、×：変更不可

項　　目	適用される省略値	オプション設定での設定変更
接続ネットワーク名	localnet	○
DHCP サーバ機能 ・割り当て先頭 IP アドレス ・割り当てアドレス数	使用する 本装置の IP アドレス、ネットマスクから求めたネットワークアドレス＋ 2 64	○
NAT 機能	使用しない	×
かんたんフィルタ	使用しない	×
ダイナミックルーティング ・RIP 送信（LAN 側） ・RIP 受信（LAN 側） ・RIP 送信（WAN 側） ・RIP 受信（WAN 側）	 送信しない 受信しない 送信しない 受信しない	×
スタティックルーティング ・LAN 側 ・WAN 側	 なし 相手ルータの IP アドレス、ネットマスクを元にスタティックルートを設定する	×
PVC 確認手順	使用する	×
CLLM メッセージ	使用する	×
輻輳通知ビット	FECN および BECN	×
IPv6 ルーティング	使用しない	×
ブリッジ	使用しない	×

「かんたん設定」で設定する（アナログ設定）

「かんたん設定」の「アナログ設定」では、本装置のアナログポートに接続する接続機器の設定、およびナンバー・ディスプレイの使用の有無を設定できます。

ここでは、以下の条件を設定する場合を例に説明します。

- アナログポート1には、電話を接続する
- アナログポート1に接続した電話には、ナンバー・ディスプレイを使用する
- アナログポート2には、なにも接続しない

補足 電話以外のアナログ機器を接続する場合は、詳細設定で設定してください。

1.　かんたんメニューで「アナログ設定」をクリックします。

「かんたん設定（アナログポート）」ページが表示されます。

2.　以下の項目を指定します。

- アナログポート1
  接続機器　→電話
  ナンバー・ディスプレイ　→使用する
- アナログポート2
  接続機器　→なし

アナログポート1	接続機器	◉電話 ○なし
	ナンバー・ディスプレイ	◉使用する ○使用しない
アナログポート2	接続機器	○電話 ◉なし
	ナンバー・ディスプレイ	○使用する ◉使用しない

3.　［設定終了］ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

- **「INS ナンバー・ディスプレイ」はNTT が提供するサービスです。利用の際はNTT との契約が必要です。**
- **アナログポートに接続したアナログ機器に発信者番号を表示させるには、本装置のアナログポートにナンバー・ディスプレイ対応のアナログ機器を接続し、アナログ機器のナンバー・ディスプレイ機能を「使用する」に設定する必要があります。**
- **アナログポート2に機器を接続しない場合は、必ず「接続機器」に「なし」を指定してください。ご購入時の状態では、アナログポート1、2共に「接続機器」は「電話」となっています。この場合、アナログポート1に接続された電話で通話中に電話がかかってくると、相手の方は呼び出し中のままとなります。**
- **ナンバー・ディスプレイ対応アナログ機器の機種によっては、発信者番号が正常に表示されない場合があります。**
- **詳細設定後にかんたん設定（アナログ設定）を行うと、詳細設定のアナログポート1／2情報で指定した「接続機器」と「通信前情報通知」の設定は無効となります。**

電話機を使って設定する

本装置のアナログポート（ポート1、ポート2）に接続したアナログ機器から設定できる項目を以下に示します。

- 時計の設定
- IPアドレスの設定
- アナログ機能の設定
  スタンバイモードの設定
  着信転送の設定
  アナログポートの接続機器の設定
  ナンバー・ディスプレイの設定
  ｉ・ナンバーの設定
  鳴り分け番号の動作モードの設定
- 着信転送先の設定
- TEL メールの設定
- メールチェックの実行
- 留守状態の設定
- 留守モードの設定

こんな事に気をつけて

データ通信中に電話機を利用して設定を変更するとデータ通信が切断されます。
ただし、「時計の設定」、「メールチェックの実行」の場合は切断されません。

■ 時計を設定する

電話機を使って本装置の内部時計を設定する方法を説明します。時計の設定方法は、ほかにもWWW ブラウザで設定する方法があります。

1.　受話器を上げ、ツーという音が聞こえることを確認します。

2.　✱0✱820 ＋✱日付＋時刻（yymmddHHMMSS）をダイヤルします。

- yy　→西暦の下2桁を指定します。00～36の場合は西暦2000年以降とみなします。
- mm　→月を01～12までの数字で指定します。
- dd　→日付を01～31までの数字で指定します。
- HH　→時間を00～23までの数字で指定します。
- MM　→分を00～59までの数字で指定します。
- SS　→秒を00～59までの数字で指定します。

例）時刻を2008年1月1日午後2時30分00秒に設定する場合

✱0✱8201✱0801011430000をダイヤルします。

3.　ピピッという音が2回とビジートーン（プープープーという話中の音）が聞こえます。

補足 正常に設定できなかった場合は、ビジートーン（プープープーという話中の音）だけが聞こえます。

4.　受話器を置きます。

■ IPアドレスを設定する

本装置のアナログポート（ポート1、ポート2）に接続したアナログ機器からIPアドレスを設定します。

こんな事に気をつけて

- **本装置のIPアドレスを変更するとLAN間通信やISDNでのデータ通信ができなくなる場合があります。**
- **DHCPサーバ機能を利用する場合には、WWWブラウザから設定を変更してください。**
- **DHCPサーバ機能を利用している場合は、本装置のIPアドレスを変更しないでください。IPアドレスを変更すると、DHCPサーバ機能は利用できません。**

1.　受話器を上げ、ツーという音が聞こえることを確認します。

2.　✱0✱810＋✱ IPアドレス✱ ネットマスク✱ ブロードキャストアドレスをダイヤルします。

IPアドレス、ネットマスク、ブロードキャストアドレスの数字の区切りに✱を使います。

ブロードキャストアドレスは、指定するブロードキャストアドレスに対応する数値を以下の表から選択します。

選択値	ブロードキャストアドレスの設定
0	0.0.0.0
1	255.255.255.255
2	IPアドレス／ネットマスクから求められる ネットワークアドレス＋オール0
3	IPアドレス／ネットマスクから求められる ネットワークアドレス＋オール1

例）IPアドレスを「192.168.2.1」、ネットマスクを「24」、ブロードキャストアドレスを「3（ネットワークアドレス＋オール1）」に設定する場合

✱0✱810✱192✱168✱2✱1✱24✱3 をダイヤルします。

3.　ピピッという音が2回とビジートーン（プープープーという話中の音）が聞こえます。

補足　正常に設定できなかった場合は、ビジートーン（プープープーという話中の音）だけが聞こえます。

4.　受話器を置きます。

ヒント

◆ ブロードキャストアドレス

ブロードキャストとは、LANに接続するすべての端末に同報発信することで、むだなトラフィックを軽減させるために使用します。たとえば、ネットワーク全体に同じデータを同時に送信する場合、送り先の端末分のパケットを送信する必要があります。しかし、ブロードキャストアドレスを指定するとパケットを1個送信するだけでネットワーク全体に送信することが可能です。ブロードキャストには、宛先アドレスとして特定のアドレスを使います。接続するネットワークの、ブロードキャストとして運用しているアドレスによって、ブロードキャストの設定を切り替える必要があります。

■ アナログ機能を設定する

アナログポートに接続したアナログ機器から、以下のアナログ機能を設定できます。

- スタンバイモードの設定（通常モード／スタンバイモード）
- 着信転送の設定（しない／する／疑似着信転送）
- 接続機器の設定（なし／電話／モデム／FAX／FAX（無鳴動強制着信／無鳴動識別着信／キャッチホン着信））
- ナンバー・ディスプレイの設定（使用しない／使用する（モード1）／使用する（モード2））
- ｉ・ナンバーの設定（使用する／使用しない）
- 鳴り分け番号の動作モードの設定（ポート1のみ着信／ポート2のみ着信／両ポート着信／着信拒否）

1.　受話器を上げ、ツーという音が聞こえることを確認します。

2.　ダイヤル操作で設定を変更します。

✱0✱ に続けて操作番号をダイヤルします。

機能		操作番号
スタンバイモード	通常モード	8001
	スタンバイモード	8002
着信転送	しない	6001
	する	6002
	疑似着信転送	6003
接続機器の設定	なし	40P1
	電話	40P2
	モデム	40P3
	FAX	40P4
	FAX（無鳴動強制着信）	40P5
	FAX（無鳴動識別着信）	40P6
	FAX（キャッチホン着信）	40P7
ナンバー・ディスプレイ	使用しない	41P1
	使用する（モード1）	41P2
	使用する（モード2）	41P3
ｉ・ナンバーの設定	使用しない	2201
	使用する	2202
鳴り分け番号の動作モード	ポート1のみ着信	22i1
	ポート2のみ着信	22i2
	両ポート着信	22i3
	着信拒否	22i4

Pには、設定を変更するアナログポートのポート番号（1または2）を入れます。

ｉには、鳴り分け番号1～3の番号（1、2または3）を入れます。

例）ポート2の接続機器を「なし」にする場合

[*][0][*][4][0][2][1] をダイヤルします。

3.　ピピッという音とビジートーン（プープープーという話中の音）が聞こえます。

補足　ピピッという音の鳴る回数は設定した機能によって異なります（操作で入力した最後の数字の回数です）。
例）「接続機器」の設定を「なし」に設定した場合、ピピッ（1回）プープープー
正常に設定できなかった場合は、ビジートーン（プープープーという話中の音）だけが聞こえます。

4.　受話器を置きます。

■ 着信転送先を設定する

アナログポートに接続したアナログ機器から、着信転送および疑似着信転送の転送先を設定できます。

☛ 参照 「着信転送の設定を行う」（P.376）、「疑似着信転送を使う」（P.370）

1.　受話器を上げ、ツーという音が聞こえることを確認します。

2.　ダイヤル操作で設定を変更します。

✱0✱に続けて操作番号＋転送先電話番号をダイヤルします。

機能	操作番号
契約者回線番号の転送先	610
ポート1のダイヤルインの転送先	611
ポート2のダイヤルインの転送先	612
鳴り分け番号1の転送先	613
鳴り分け番号2の転送先	614
鳴り分け番号3の転送先	615

例）契約者回線番号を「03-1111-2222」に着信転送する設定を行う場合

✱0✱6103111122222をダイヤルします。

3.　ピピッという音とビジートーン（プープープーという話中の音）が聞こえます。

補足 ピピッという音の鳴る回数は設定した機能によって異なります。

- 契約者回線番号の転送先を設定した場合　：1回
- ポート1のダイヤルイン番号の転送先を設定した場合：2回
- ポート2のダイヤルイン番号の転送先を設定した場合：3回
- 鳴り分け番号1の転送先を設定した場合　：4回
- 鳴り分け番号2の転送先を設定した場合　：5回
- 鳴り分け番号3の転送先を設定した場合　：6回

正常に設定できなかった場合は、ビジートーン（プープープーという話中の音）だけが聞こえます。

4.　受話器を置きます。

■ TELメールを設定する

アナログポートに接続したアナログ機器から、TELメールを設定できます。

☛ 参照 「TELメール機能」（P.547）

1.　受話器を上げ、ツーという音が聞こえることを確認します。

2.　ダイヤル操作で設定を変更します。

[*][0][*]に続けて操作番号をダイヤルします。

機能		操作番号
TELメール機能の設定	使用しない	2101
	使用する	2102

3.　ピピッという音とビジートーン（プープープーという話中の音）が聞こえます。

補足 ピピッという音の鳴る回数は設定した機能によって異なります（操作で入力した最後の数字の回数です）。
正常に設定できなかった場合は、ビジートーン（プープープーという話中の音）だけが聞こえます。

4.　受話器を置きます。

■ メールチェックを実行する

アナログポートに接続したアナログ機器から、メールチェックを実行できます。

☛ 参照 「メールチェック機能」（P.536）

1.　受話器を上げ、ツーという音が聞こえることを確認します。

2.　[*][0][*][8][3][0][0]をダイヤルします。

3.　ピピッという音が2回とビジートーン（プープープーという話中の音）が聞こえます。

補足 正常に設定できなかった場合は、ビジートーン（プープープーという話中の音）だけが聞こえます。

4.　受話器を置きます。

■ 留守状態を設定する

アナログポートに接続したアナログ機器から、留守確認機能の留守状態を設定できます。

☛ 参照 「留守状態を確認する（無課金）」（P.425）

1.　受話器を上げ、ツーという音が聞こえることを確認します。

2.　ダイヤル操作で設定を変更します。

✱0✱に続けて操作番号をダイヤルします。

機能		操作番号
留守状態の設定	在宅	2001
	留守	2002

3.　ピピッという音とビジートーン（プープープーという話中の音）が聞こえます。

補足 ピピッという音の鳴る回数は設定した機能によって異なります（操作で入力した最後の数字の回数です）。
正常に設定できなかった場合は、ビジートーン（プープープーという話中の音）だけが聞こえます。

4.　受話器を置きます。

■ 留守モードを設定する

アナログポートに接続したアナログ機器から、留守モードを設定できます。

☛ 参照 「留守モードの動作を設定する」（P.586）

1.　受話器を上げ、ツーという音が聞こえることを確認します。

2.　ダイヤル操作で設定を変更します。

✱0✱に続けて操作番号をダイヤルします。

機能		操作番号
留守モードの設定	解除	8401
	実行	8402

3.　ピピッという音とビジートーン（プープープーという話中の音）が聞こえます。

補足 ピピッという音の鳴る回数は設定した機能によって異なります（操作で入力した最後の数字の回数です）。
正常に設定できなかった場合は、ビジートーン（プープープーという話中の音）だけが聞こえます。

4.　受話器を置きます。

第3章　導入例

3

この章では、
本装置の代表的な接続形態のいくつかを紹介します。

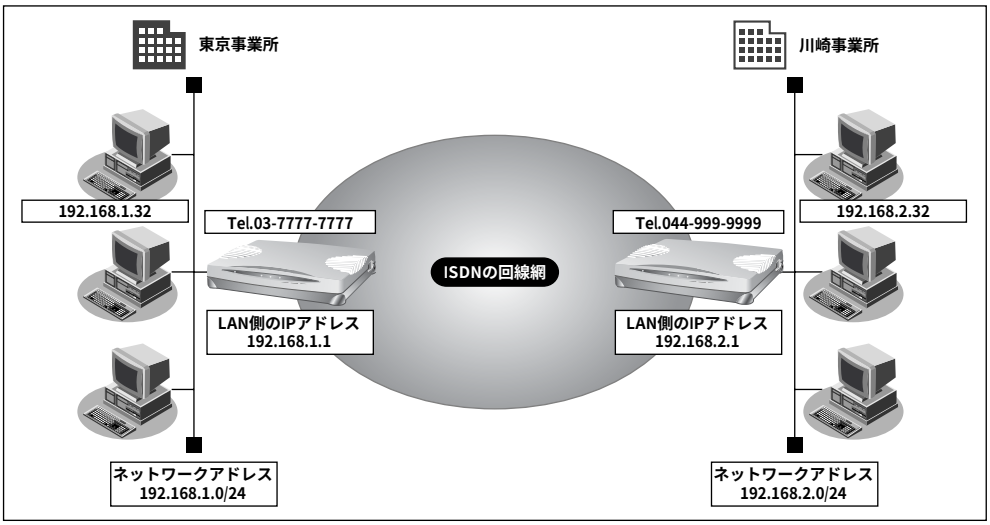
事業所LANをISDNで接続する

ここでは、ISDN回線を介して2つの事業所（東京、川崎）のネットワークを接続する場合を例に説明します。

こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。

☛ 参照 「ご購入時の状態に戻すには」（P.665）



● 設定条件

- ISDN回線を使用する
- DHCPサーバ機能は使用する
- アドレス変換機能を使用しない
- スタティックルーティング機能を使用する

[東京事業所]

- 電話番号　：03-7777-7777
- ユーザ認証IDとユーザ認証パスワード
  発信　：tokyo、tokyopass
  着信　：kawasaki、kawapass
- 本装置のLAN側のネットワークアドレス／ネットマスク
  ：192.168.1.0/24

[川崎事業所]

- 電話番号　：044-999-9999
- ユーザ認証IDとユーザ認証パスワード
  発信　：kawasaki、kawapass
  着信　：tokyo、tokyopass
- 本装置のLAN側のネットワークアドレス／ネットマスク
  ：192.168.2.0/24

こんな事に気をつけて

文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。
詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

■ 東京事業所の設定をする

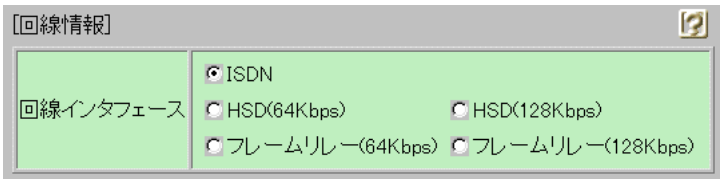
回線情報（東京事業所）を設定する

1.　詳細設定メニューのルータ設定で「回線情報」をクリックします。

「回線情報設定」ページが表示されます。

2.　[回線情報] で以下の項目を指定します。

- 回線インタフェース　→ISDN



必要に応じて上記以外の項目を指定します。

3.　[更新] ボタンをクリックします。

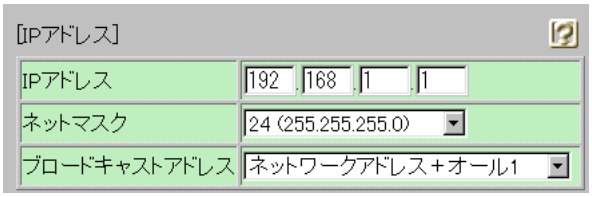
LAN情報（東京事業所）を設定する

1.　詳細設定メニューのルータ設定で「LAN情報」をクリックします。

「LAN情報設定」ページが表示されます。

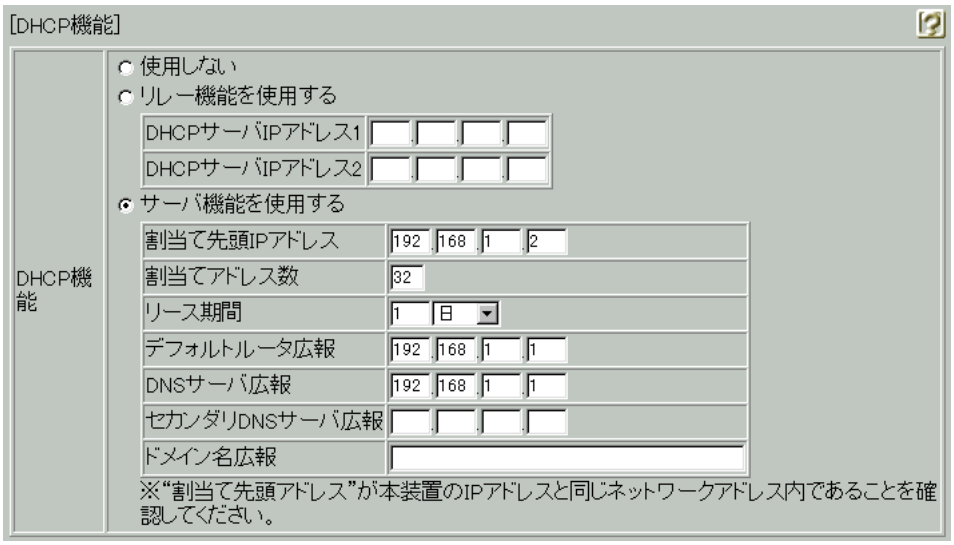
2.　［IPアドレス］で以下の項目を指定します。

- IPアドレス　→192.168.1.1（本装置のLAN側のIPアドレス）
- ネットマスク　→24
- ブロードキャストアドレス　→ネットワークアドレス＋オール1



［DHCP機能］で以下の項目を指定します。

- DHCP機能　→サーバ機能を使用する



必要に応じて上記以外の項目を指定します。

3.　［更新］ボタンをクリックします。

接続先の情報（川崎事業所）を設定する

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］で［追加］ボタンをクリックします。

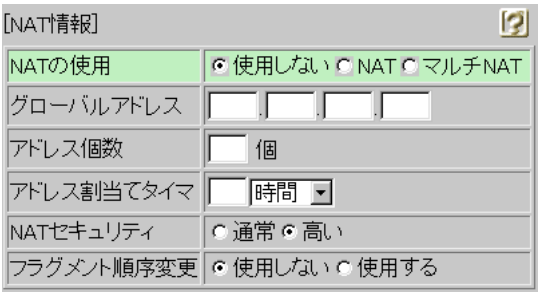
「ネットワーク情報設定」ページが表示されます。

3.　［基本情報］で以下の項目を指定します。

- ネットワーク名　→kaisya（接続するネットワークの名称）
- 自動ダイヤル　→する

［NAT 情報］で以下の項目を指定します。

- NAT の使用　→使用しない



必要に応じて上記以外の項目を指定します。

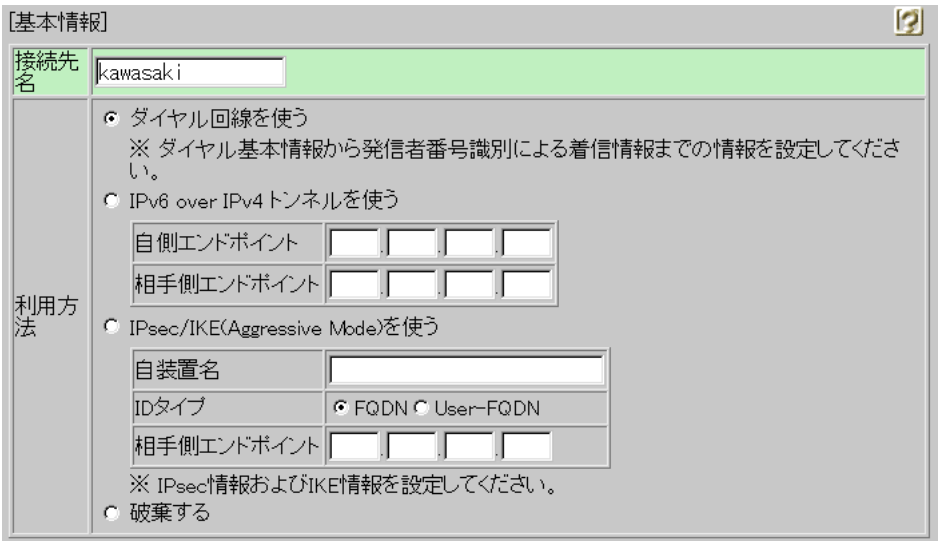
4.　［接続先情報一覧］で［追加］ボタンをクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

「接続先情報設定」ページが表示されます。

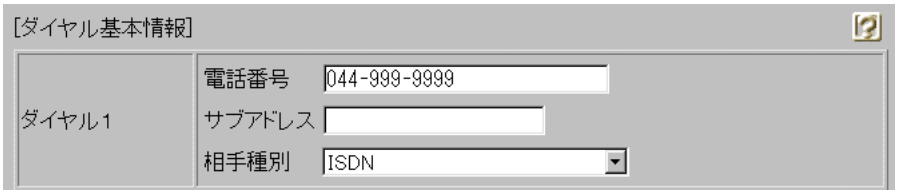
5.　［基本情報］で以下の項目を指定します。

- 接続先名　→kawasaki
- 利用方法　→ダイヤル回線を使う



［ダイヤル基本情報］で以下の項目を指定します。

- ダイヤル1
  電話番号　→044-999-9999

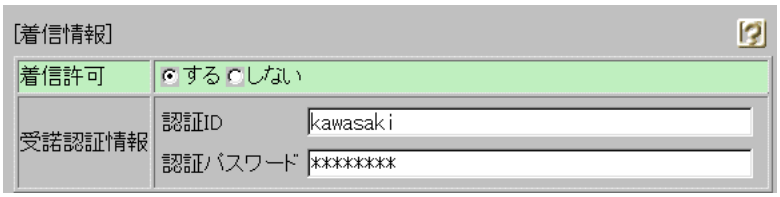


［発信情報］で以下の項目を指定します。

- 送信認証情報
  送信認証ID　→tokyo
  認証パスワード　→tokyopass

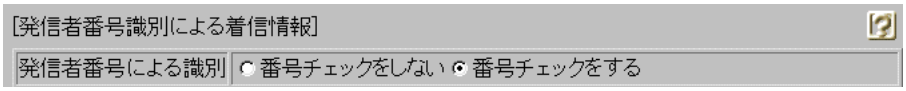
［着信情報］で以下の項目を指定します。

- 着信許可　→する
- 受諾認証情報
  認証 ID　→ kawasaki
  認証パスワード　→ kawapass



［発信者番号識別による着信情報］で以下の項目を指定します。

- 発信者番号による識別　→番号チェックをする



必要に応じて上記以外の項目を指定します。

6.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

7.　［スタティックルーティング情報一覧］で［追加］ボタンをクリックします。

「ルーティング情報設定」ページが表示されます。

8.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  宛先 IP アドレス　→ 192.168.2.1（接続先となる本装置の IP アドレス）
  宛先アドレスマスク　→ 24（接続先となる本装置のアドレスマスク）
- メトリック値　→ 1

9.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

10.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

11.　［更新］ボタンをクリックします。

12.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

■ 川崎事業所の設定をする

「東京事業所の設定をする」を参考に、川崎事業所の設定をします。その際、特に指定のないものは、東京事業所と同じ設定にします。

回線情報（川崎事業所）を設定する

［回線情報］

- 回線インタフェース　→ISDN

LAN情報（川崎事業所）を設定する

［IPアドレス］

- IPアドレス　→192.168.2.1（本装置のLAN側のIPアドレス）
- ネットマスク　→24
- ブロードキャストアドレス　→ネットワークアドレス＋オール1

［DHCP機能］

- DHCPサーバ機能　→使用する

接続先の情報（東京事業所）を設定する

「ネットワーク情報設定」

［基本情報］

- ネットワーク名　→kaisya（接続するネットワークの名称）
- 自動ダイヤル　→する

［NAT情報］

- NATの使用　→使用しない

「接続先情報設定」

［基本情報］

- 接続先名　→tokyo
- 利用方法　→ダイヤル回線を使う

［ダイヤル基本情報］

- ダイヤル1
  電話番号　→03-7777-7777

［発信情報］

- 送信認証情報
  送信認証ID　→kawasaki
  認証パスワード　→kawapass

［着信情報］

- 着信許可　→する
- 受諾認証情報
  認証ID　→tokyo
  認証パスワード　→tokyopass

「ルーティング情報設定」

- ネットワーク　→ネットワーク指定
  宛先IPアドレス　→192.168.1.1（接続先となる本装置のIPアドレス）
  宛先アドレスマスク　→24（接続先となる本装置のアドレスマスク）
- メトリック値　→1

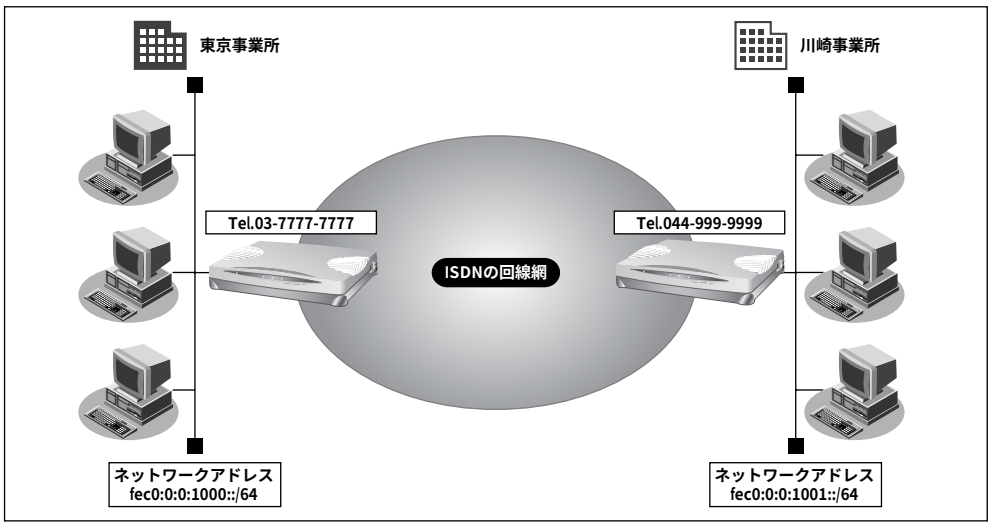
IPv6の事業所LANをISDNで接続する

ここでは、ISDN回線を介して2つの事業所（東京、川崎）のIPv6ネットワークを接続する場合を例に説明します。

こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。

☛ 参照 「ご購入時の状態に戻すには」（P.665）



● 設定条件

- ISDN回線を使用する
- スタティックルーティング機能を使用する

[東京事業所]

- 本装置のLAN側のプレフィックス／プレフィックス長
  ：fec0:0:0:1000::/64
- 電話番号　：03-7777-7777
- ユーザ認証IDとユーザ認証パスワード
  送信時　：kawasaki、kawapass
  受諾時　：tokyo、tokyopass

[川崎事業所]

- 本装置のLAN側のプレフィックス／プレフィックス長
  ：fec0:0:0:1001::/64
- 電話番号　：044-999-9999

- ユーザ認証IDとユーザ認証パスワード
  送信時　　：tokyo、tokyopass
  受諾時　　：kawasaki、kawapass

こんな事に気をつけて

文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。
詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

■ 東京事業所の設定をする

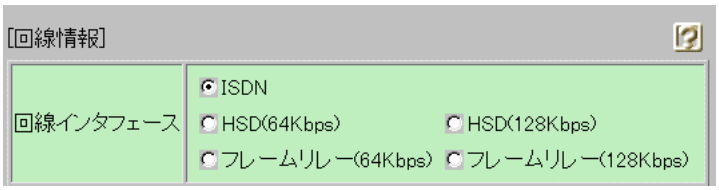
回線情報（東京事業所）を設定する

1.　詳細設定メニューのルータ設定で「回線情報」をクリックします。

「回線情報設定」ページが表示されます。

2.　［回線情報］で以下の項目を指定します。

- 回線インタフェース　　→ISDN



必要に応じて上記以外の項目を指定します。

3.　［更新］ボタンをクリックします。

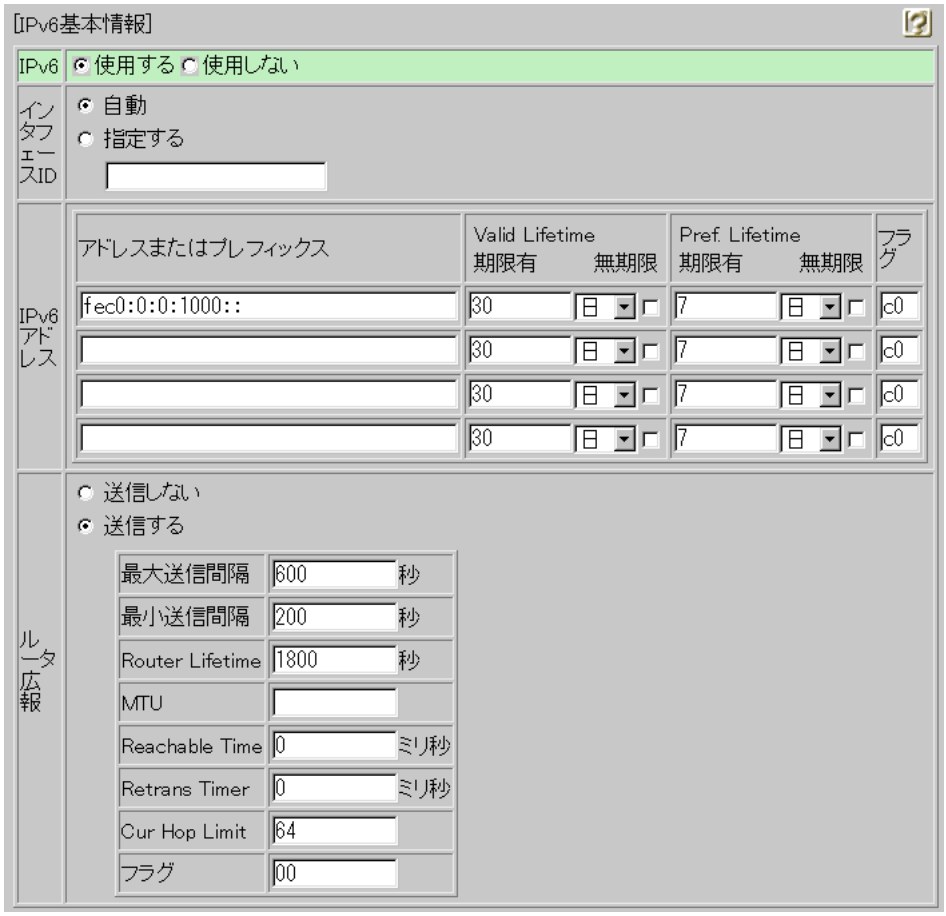
LAN情報（東京事業所）を設定する

1.　詳細設定メニューのルータ設定で「LAN情報」をクリックします。

「LAN情報設定」ページが表示されます。

2.　［IPv6基本情報］で以下の項目を指定します。

- IPv6　→使用する
- インタフェースID　→自動
- IPv6アドレス　→fec0:0:0:1000::
- ルータ広報　→送信する



必要に応じて上記以外の項目を指定します。

3.　［更新］ボタンをクリックします。

接続先の情報（川崎事業所）を設定する

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］で［追加］ボタンをクリックします。

「ネットワーク情報設定」ページが表示されます。

3.　［基本情報］で以下の項目を指定します。

- ネットワーク名　→kaisya（接続するネットワークの名称）
- 自動ダイヤル　→する

必要に応じて上記以外の項目を指定します。

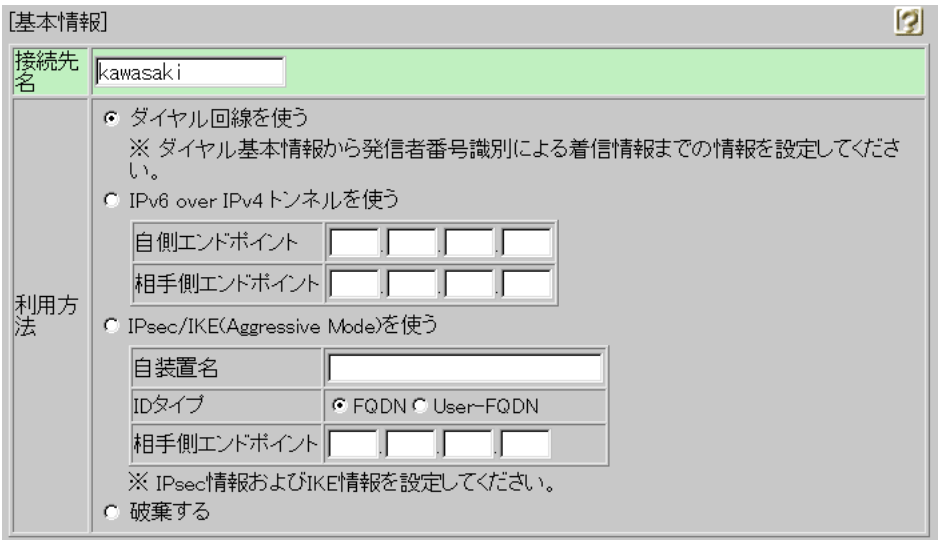
4.　［接続先情報一覧］で［追加］ボタンをクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

「接続先情報設定」ページが表示されます。

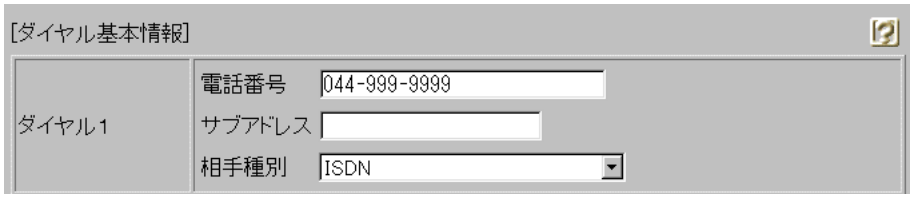
5.　［基本情報］で以下の項目を指定します。

- 接続先名　→kawasaki
- 利用方法　→ダイヤル回線を使う



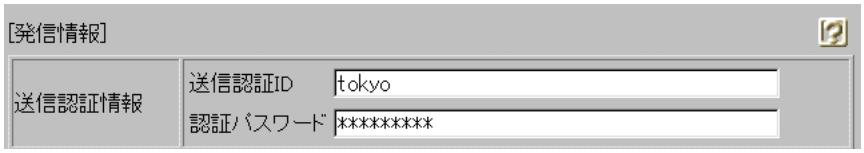
［ダイヤル基本情報］で以下の項目を指定します。

- ダイヤル1
  電話番号　→044-999-9999



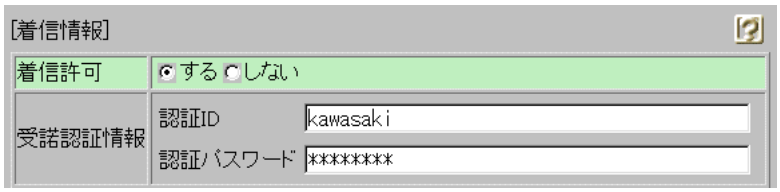
［発信情報］で以下の項目を指定します。

- 送信認証情報
  送信認証ID　→tokyo
  認証パスワード　→tokyopass



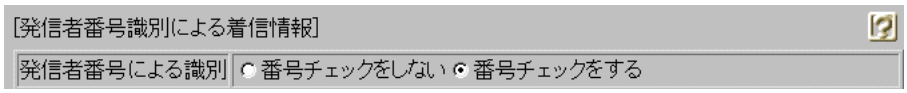
［着信情報］で以下の項目を指定します。

- 着信許可　→する
- 受諾認証情報
  認証ID　→kawasaki
  認証パスワード　→kawapass



［発信者番号識別による着信情報］で以下の項目を指定します。

- 発信者番号による識別　→番号チェックをする



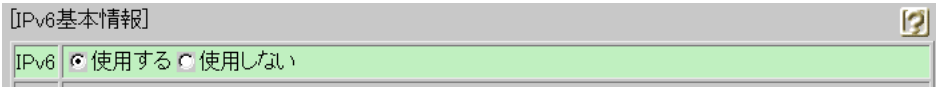
必要に応じて上記以外の項目を指定します。

6.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

7.　［IPv6基本情報］で以下の項目を指定します。

- IPv6　→使用する



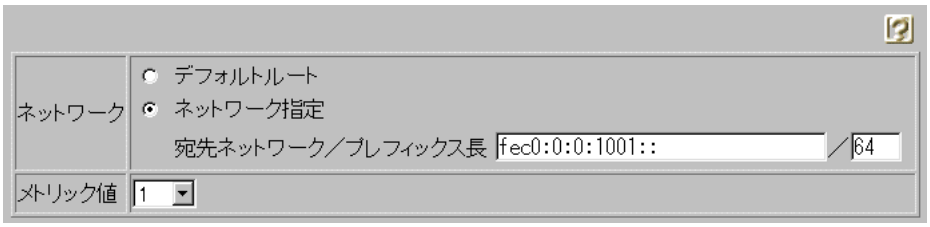
8.　［IPv6スタティックルーティング情報一覧］で［追加］ボタンをクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

「IPv6ルーティング情報設定」ページが表示されます。

9.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  宛先ネットワーク／プレフィックス長　→fec0:0:0:1001::/64
- メトリック値　→1



⚠注意

ISDNまたはフレームリレーの場合［IPv6ダイナミックルーティング機能］で「RIPng送信」が「送信しない」になっていることを確認してください。RIPngを送信すると思いもしない課金（定期発信または長時間接続）が発生します。

10.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

11.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

12.　［更新］ボタンをクリックします。

13.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

■ 川崎事業所の設定をする

「東京事業所の設定をする」を参考に、川崎事業所の設定をします。その際、特に指定のないものは、東京事業所と同じ設定にします。

回線情報（川崎事業所）を設定する

［回線情報］

- 回線インタフェース　→ISDN

LAN情報（川崎事業所）を設定する

［IPv6基本情報］

- IPv6　→使用する
- インタフェースID　→自動
- IPv6アドレス　→fec0:0:0:1001::
- ルータ広報　→送信する

接続先の情報（東京事業所）を設定する

「ネットワーク情報設定」

［基本情報］

- ネットワーク名　→kaisya（接続するネットワークの名称）
- 自動ダイヤル　→する

［IPv6基本情報］

- IPv6　→使用する

「接続先情報設定」

［基本情報］

- 接続先名　→tokyo

［ダイヤル基本情報］

- ダイヤル1
  電話番号　→03-7777-7777

［発信情報］

- 送信認証情報
  送信認証ID　→kawasaki
  認証パスワード　→kawapass

［着信情報］

- 着信許可　→する
- 受諾認証情報
  認証ID　→tokyo
  認証パスワード　→tokyopass

［発信者番号識別による着信情報］

- 発信者番号による識別　→番号チェックをする

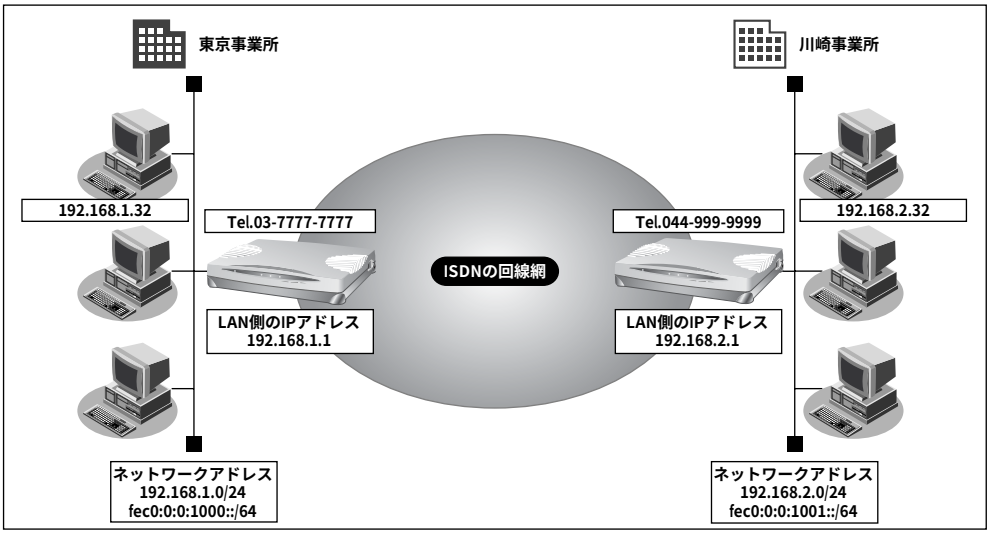
「IPv6スタティックルーティング情報設定」

- ネットワーク　→ネットワーク指定
  宛先ネットワーク／プレフィックス長
  →fec0:0:0:1000::/64
- メトリック値　→1

IPv4の事業所LANにIPv6ネットワークを追加する

ここでは、IPv4で通信を行っているネットワーク環境にIPv6通信設定を追加する場合の例を説明します。

「事業所LANをISDNで接続する」（P.115）を元に「IPv6の事業所LANをISDNで接続する」（P.123）で使用する設定条件のIPv6ネットワークを追加します。



● 設定条件

- ISDN回線を使用する

[東京事業所]

- 本装置のLAN側のプレフィックス／プレフィックス長：fec0:0:0:1000::/64

[川崎事業所]

- 本装置のLAN側のプレフィックス／プレフィックス長：fec0:0:0:1001::/64

こんな事に気をつけて

文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。
詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

■ 東京事業所の設定をする

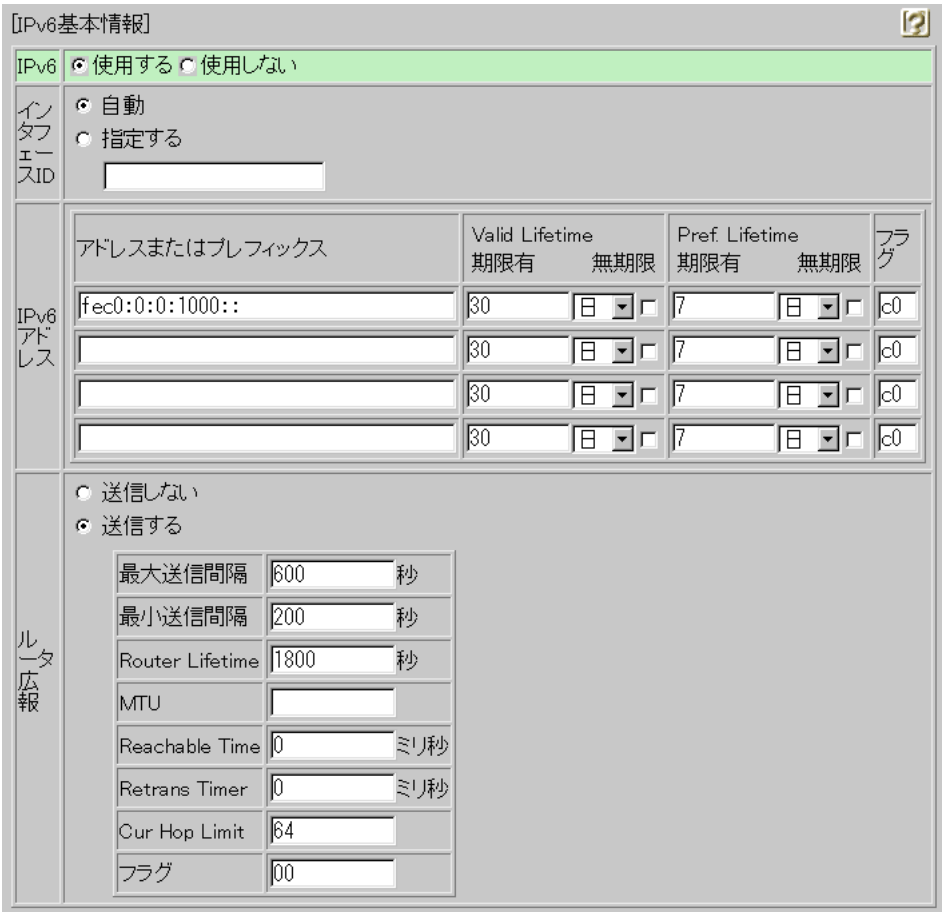
LAN情報（東京事業所）を設定する

1.　詳細設定メニューのルータ設定で「LAN情報」をクリックします。

「LAN情報設定」ページが表示されます。

2.　［IPv6基本情報］で以下の項目を指定します。

- IPv6　→使用する
- インタフェースID　→自動
- IPv6アドレス　→fec0:0:0:1000::
- ルータ広報　→送信する



必要に応じて上記以外の項目を指定します。

3.　［更新］ボタンをクリックします。

接続先の情報（東京事業所）を設定する

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

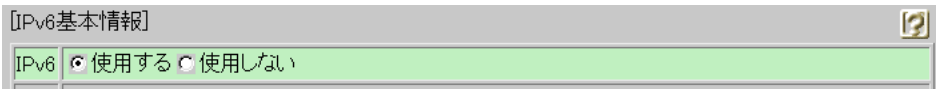
「相手情報設定」ページが表示されます。

2.　「ネットワーク情報一覧」でIPv6通信を追加するIPv4通信ネットワーク情報の［修正］ボタンをクリックします。

「ネットワーク情報設定」ページが表示されます。

3.　［IPv6基本情報］で以下の項目を指定します。

- IPv6　→使用する



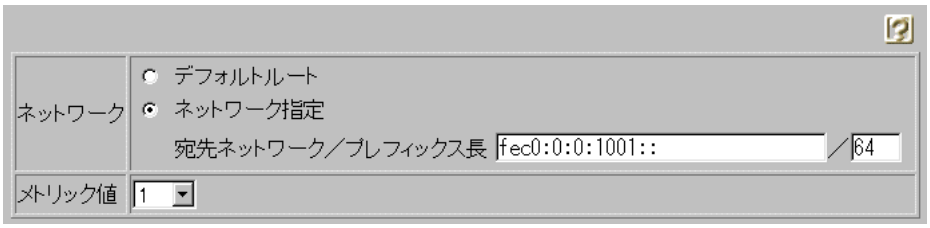
4.　［IPv6スタティックルーティング情報一覧］で［追加］ボタンをクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

「IPv6ルーティング情報設定」ページが表示されます。

5.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  宛先ネットワーク／プレフィックス長　→fec0:0:0:1001::/64
- メトリック値　→1



6.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

7.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

8.　［更新］ボタンをクリックします。

9.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

■ 川崎事業所の設定をする

LAN情報（川崎事業所）を設定する

［IPv6基本情報］

- IPv6　→使用する
- インタフェースID　→自動
- IPv6アドレス　→fec0:0:0:1001::
- ルータ広報　→送信する

接続先の情報（川崎事業所）を設定する

「ネットワーク情報設定」

［IPv6基本情報］

- IPv6　→使用する

「IPv6スタティックルーティング情報設定」

- ネットワーク　→ネットワーク指定
  宛先ネットワーク／プレフィックス長
  →fec0:0:0:1000::/64
- メトリック値　→1

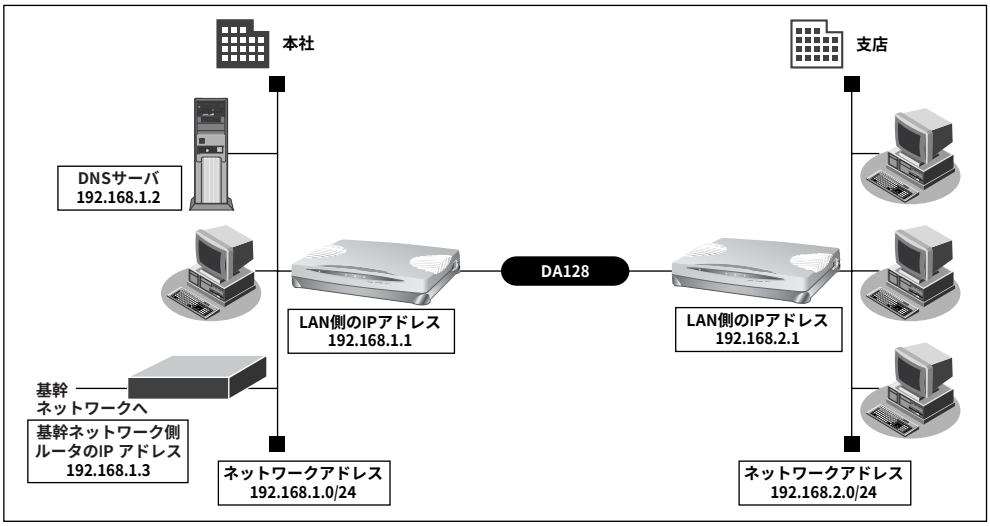
事業所LANを専用線で接続する

ここでは、高速ディジタル専用線（DA128）を介して2つの事業所（本社、支店）のネットワークを接続する場合を例に説明します。

こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。

☛ 参照 「ご購入時の状態に戻すには」（P.665）



● 設定条件

- 専用線（128Kbps）を使用する

[本社]

- 本装置のIPアドレス　：192.168.1.1
- LAN側のネットワークアドレス／ネットマスク　：192.168.1.0/24
- DHCPサーバ機能は使用しない
- アドレス変換機能は使用しない
- DNSサーバ　：192.168.1.2
- 基幹ネットワーク側ルータIPアドレス　：192.168.1.3

[支店]

- 本装置のIPアドレス　：192.168.2.1
- LAN側のネットワークアドレス／ネットマスク　：192.168.2.0/24

補足 この例では、本社にDNSサーバが存在しIPアドレスを固定にする必要があるので、本社側ではDHCPサーバ機能は使用しない条件にしました。

こんな事に気をつけて

文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。
詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

■ 本社の設定をする

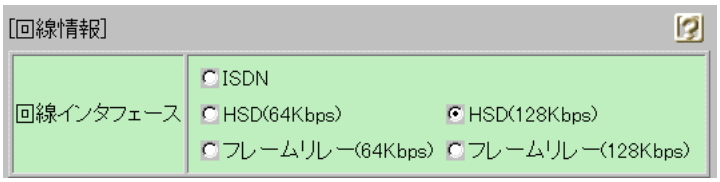
回線情報（本社）を設定する

1.　詳細設定メニューのルータ設定で「回線情報」をクリックします。

「回線情報設定」ページが表示されます。

2.　［回線情報］で以下の項目を指定します。

- 回線インタフェース　→HSD（128Kbps）



3.　［更新］ボタンをクリックします。

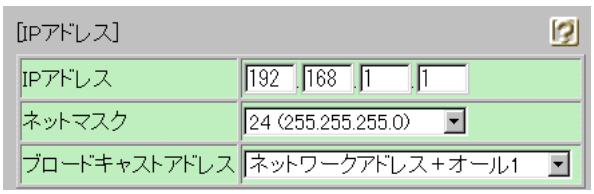
LAN情報（本社）を設定する

1.　詳細設定メニューのルータ設定で「LAN情報」をクリックします。

「LAN情報設定」ページが表示されます。

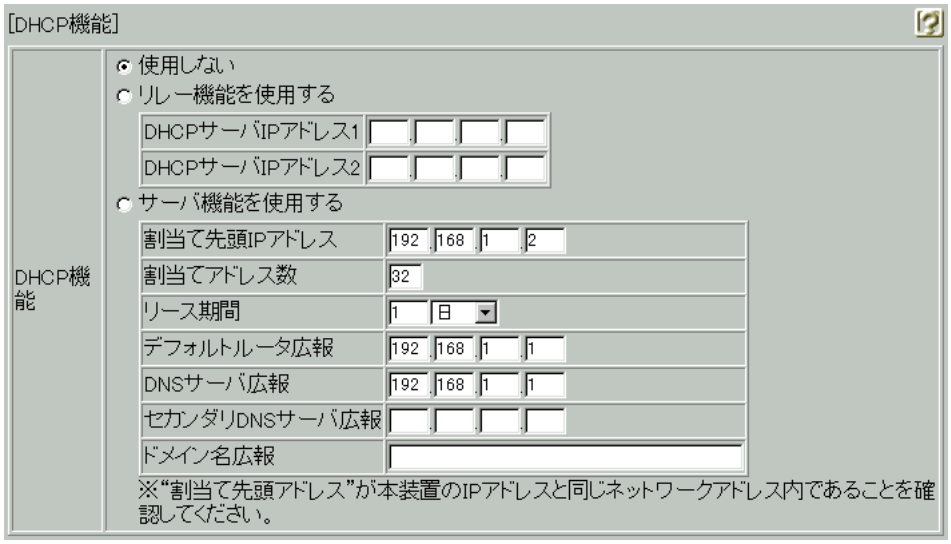
2.　［IPアドレス］で以下の項目を指定します。

- IPアドレス　→192.168.1.1（本装置のLAN側のIPアドレス）
- ネットマスク　→24
- ブロードキャストアドレス　→ネットワークアドレス＋オール1



［DHCP 機能］で以下の項目を指定します。

- DHCP 機能　→使用しない



必要に応じて上記以外の項目を指定します。

3.　［スタティックルーティング情報一覧］で［追加］ボタンをクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

「ルーティング情報設定」ページが表示されます。

4.　以下の項目を指定します。

- ネットワーク　→デフォルトルート
  中継ルータアドレス　→192.168.1.3（基幹ネットワーク側 IP アドレス）
- メトリック値　→1

5.　［更新］ボタンをクリックします。

接続先の情報を設定する

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］で［追加］ボタンをクリックします。

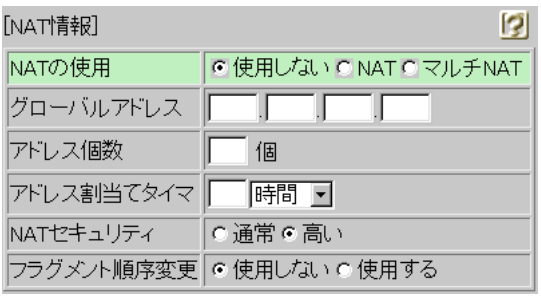
「ネットワーク情報設定」ページが表示されます。

3.　［基本情報］で以下の項目を指定します。

- ネットワーク名　→Siten1（接続するネットワークの名称）

［NAT 情報］で以下の項目を指定します。

- NAT の使用　→使用しない



必要に応じて上記以外の項目を指定します。

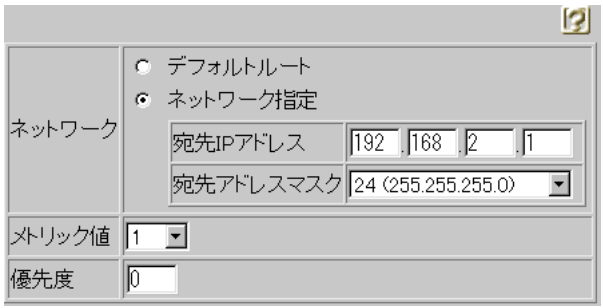
4.　［スタティックルーティング情報一覧］で［追加］ボタンをクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

「ルーティング情報設定」ページが表示されます。

5.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  宛先IPアドレス　→192.168.2.1（接続先のIPアドレス）
  宛先アドレスマスク　→24（接続先のアドレスマスク）
- メトリック値　→1



6.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

7.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

8.　［更新］ボタンをクリックします。

9.　［再起動］ボタンをクリックします。

設定した内容が有効になります。

■ 支店の設定をする

「かんたん設定（インターネットへ専用線接続）」で設定する

［必須設定］

- 本装置のIPアドレス　→192.168.2.1（本装置のLAN側のIPアドレス）
- ネットマスク　→24
- 使用する回線速度　→128Kbps
- DNSサーバ　→192.168.1.2

［オプション設定］

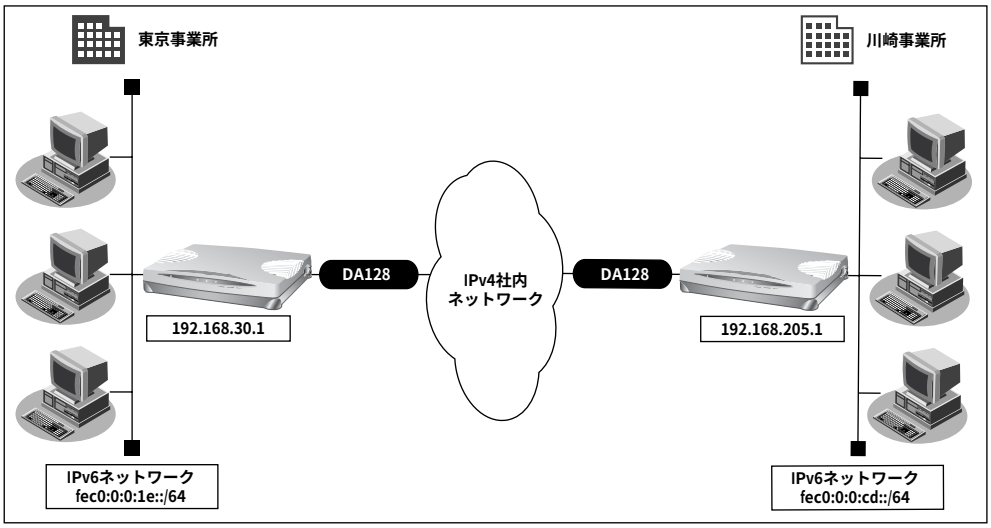
- 接続ネットワーク名　→kaisya（接続するネットワークの名称）
- アドレス変換　→使用しない

補足 「かんたん設定（インターネットへ専用線接続）」の省略値ではデフォルトルートを設定します。また、「かんたん設定（オフィスへ専用線接続）」の省略値では相手ルータのIPアドレスとネットマスクを元にスタティックルートを設定します。この設定例では本社のネットワーク内に基幹ネットワークにつながるルータが存在します。このため本社側への経路をデフォルトルートとする必要があります。それでここでは「かんたん設定（インターネットへ専用線接続）」を使用しています。ただし、この場合DHCPサーバが動作するので、DHCPサーバ機能を使用しない場合は「詳細設定」で設定を変更してください。本社のネットワークに基幹ネットワークにつながるルータが存在しない場合は、「かんたん設定（オフィスへ専用線接続する）」で設定できます。

☛ 参照 「かんたん設定（インターネットへ専用線接続）」の省略値について（P.85）
「かんたん設定（オフィスへ専用線接続）」の省略値について（P.95）

IPv6事業所間を接続する（IPv6トンネル）

ここでは、IPv4で構築されたイントラネットを介して、2つの事業所（東京、川崎）のIPv6ネットワークどうしをトンネリングによって接続する場合を例に説明します。



● 設定条件

- 専用線（128Kbps）を使用する

[東京事業所]

- 本装置のLAN側のIPv4アドレス　：192.168.30.1
- 本装置のWAN側のIPv4アドレス　：なし（unnumbered）
- 本装置のLAN側のIPv6プレフィックス／プレフィックス長
  ：fec0:0:0:1e::/64（※1）

[川崎事業所]

- 本装置のLAN側のIPv4アドレス　：192.168.205.1
- 本装置のWAN側のIPv4アドレス　：なし（unnumbered）
- 本装置のLAN側のIPv6プレフィックス／プレフィックス長
  ：fec0:0:0:cd::/64（※1）

※1）この例では、プライベートアドレス（IPv4）／サイトローカルアドレス（IPv6）を使用しています。

こんな事に気をつけて

- **文字入力フィールドでは半角文字（0 ～9、A ～Z、a ～ z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。**
  詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。
- **IPv6 over IPv4 トンネルを利用する場合は、カプセル化されたIPv4 パケットのフラグメントを防ぐため、トンネルに利用する相手情報の MTU に 1280 を設定してください。**

社内IPv4ネットワークへ専用線接続する

この例では、社内ネットワークを経由したIPv4通信ができていることを前提として説明します。

☛ 参照 「「かんたん設定」で設定する （オフィスへ専用線接続のとき）」（P.95）

■ 東京事業所の設定をする

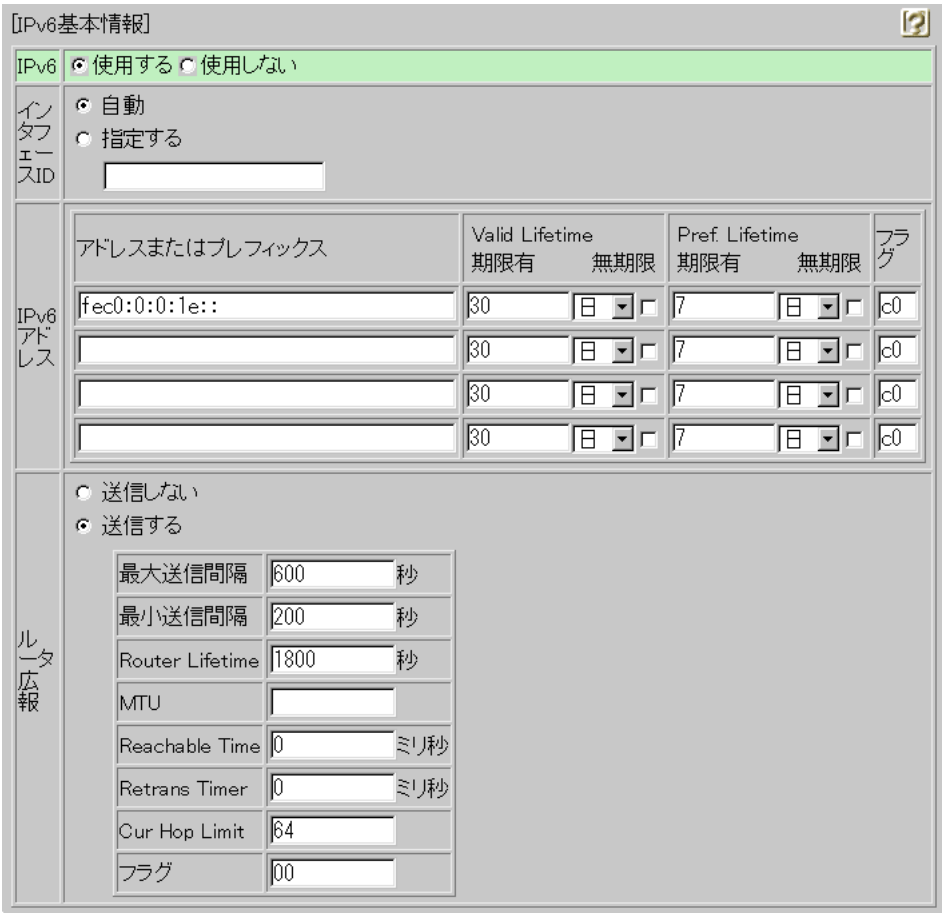
LAN情報（東京事業所）を設定する

1.　詳細設定メニューのルータ設定で「LAN情報」をクリックします。

「LAN情報設定」ページが表示されます。

2.　［IPv6基本情報］で以下の項目を指定します。

- IPv6　→使用する
- インタフェースID　→自動
- IPv6アドレス
  アドレスまたはプレフィックス　→fec0:0:0:1e::
- ルータ広報　→送信する



3.　［更新］ボタンをクリックします。

トンネル接続先の情報（川崎事業所）を設定する

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

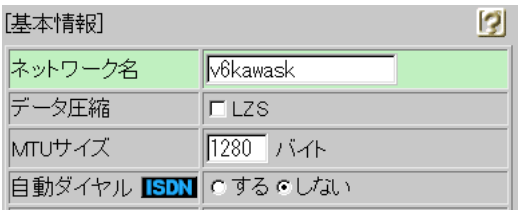
「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］で［追加］ボタンをクリックします。

「ネットワーク情報設定」ページが表示されます。

3.　［基本情報］で以下の項目を指定します。

- ネットワーク名　→v6kawask（接続するネットワークの名称）
- MTUサイズ　→1280



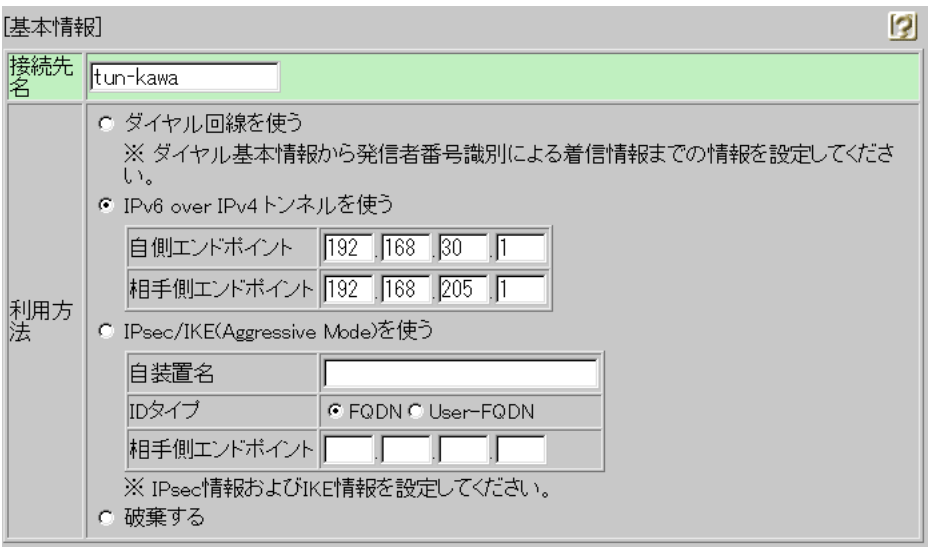
4.　［接続先情報一覧］で［追加］ボタンをクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

「接続先情報設定」ページが表示されます。

5.　［基本情報］で以下の項目を指定します。

- 接続先名　→tun-kawa
- 利用方法　→IPv6 over IPv4 トンネルを使う
  自側エンドポイント　→192.168.30.1
  相手側エンドポイント　→192.168.205.1

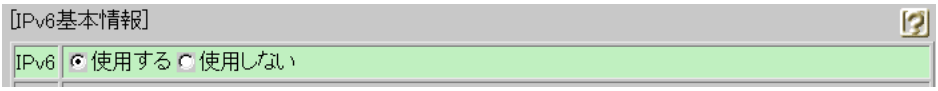


6.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

7.　［IPv6基本情報］で以下の項目を指定します。

- IPv6　→使用する



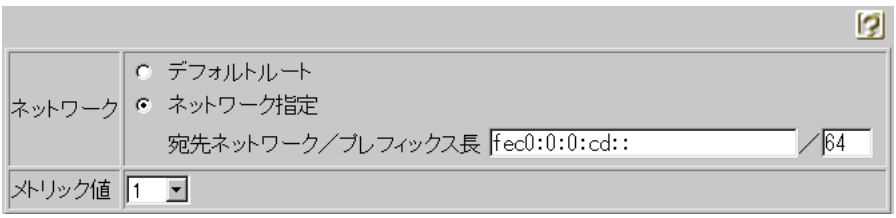
8.　［IPv6スタティックルーティング情報一覧］で［追加］ボタンをクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

「IPv6ルーティング情報設定」ページが表示されます。

9.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  宛先ネットワーク／プレフィックス長　→fec0:0:0:cd::/64
- メトリック値　→1



10.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

11.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

12.　［更新］ボタンをクリックします。

13.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

■ 川崎事業所の設定をする

「東京事業所の設定をする」を参考に、川崎事業所の設定をします。その際、特に指定のないものは、東京事業所と同じ設定にします。

LAN情報（川崎事業所）を設定する

［IPv6基本情報］

- IPv6　→使用する
- インタフェースID　→自動
- IPv6アドレス
  アドレスまたはプレフィックス　→fec0:0:0:cd::
- ルータ広報　→送信する

トンネル接続先の情報（東京事業所）を設定する

「ネットワーク情報設定」

［基本情報］

- ネットワーク名　→v6tokyo（接続するネットワークの名称）
- MTUサイズ　→1280

［IPv6基本情報］

- IPv6　→使用する

「接続先情報設定」

［基本情報］

- 接続先名　→tun-tkyo
- 利用方法　→IPv6 over IPv4 トンネルを使う
  自側エンドポイント　→192.168.205.1
  相手側エンドポイント　→192.168.30.1

「IPv6スタティックルーティング情報設定」

- ネットワーク　→ネットワーク指定
  宛先ネットワーク／プレフィックス長
  →fec0:0:0:1e::/64
- メトリック値　→1

ヒント

◆ NATとIPv6 over IPv4トンネルを併用する

IPv4環境のNATと、IPv6 over IPv4トンネルを利用したIPv6通信環境を併用する場合は、IPv4環境のNATの処理によって、IPv4アドレスがどのように変換処理されるかを判断してIPv6 over IPv4トンネル通信の設定を行う必要があります。

本装置では、トンネル処理はNAT処理の内側（プライベートアドレス側）で行われますので、以下のように設定します。

設定項目	設定内容
自側エンドポイント	以下のIPアドレスのどれかを設定します。 ・LANに設定されたIPアドレスまたはセカンダリIPアドレス ・相手情報→ネットワーク情報の自側IPアドレスに設定されたIPアドレス ※ PPPで割り当てられるIPアドレスは利用できません。
相手側エンドポイント	相手トンネルGWのIPアドレス
静的NAT	IPv6 over IPv4トンネル通信が相手トンネルGW側から開始されることがある場合は、静的NATの設定が必要となります。 ・プライベートIP情報 IPアドレス　自側エンドポイントに設定したアドレス ポート番号　すべて ・グローバルIP情報 IPアドレス　相手トンネルGWに設定された、本装置側のアドレス ポート番号　すべて ・プロトコル　IPv6 over IPv4

具体例を以下に示します。

条件：

- 本装置のNAT変換で利用するグローバルアドレスに172.16.0.1を利用
- 本装置のプライベートLAN側に192.168.1.1を利用
- 相手トンネルGWのIPアドレスに172.31.0.1を利用

トンネル設定：

- 本装置のトンネル通信の設定：
  192.168.1.1と172.31.0.1の間でトンネル通信を行うことを前提に、以下のとおり設定します。
  自側エンドポイント　：192.168.1.1
  相手側エンドポイント　：172.31.0.1

静的NAT設定：

- プライベートIP情報
  IPアドレス　192.168.1.1
  ポート番号　すべて
- グローバルIP情報
  IPアドレス　172.16.0.1
  ポート番号　すべて
- プロトコル　IPv6 over IPv4

なお、この具体例において、相手トンネルGWの設定は、以下のとおりです。

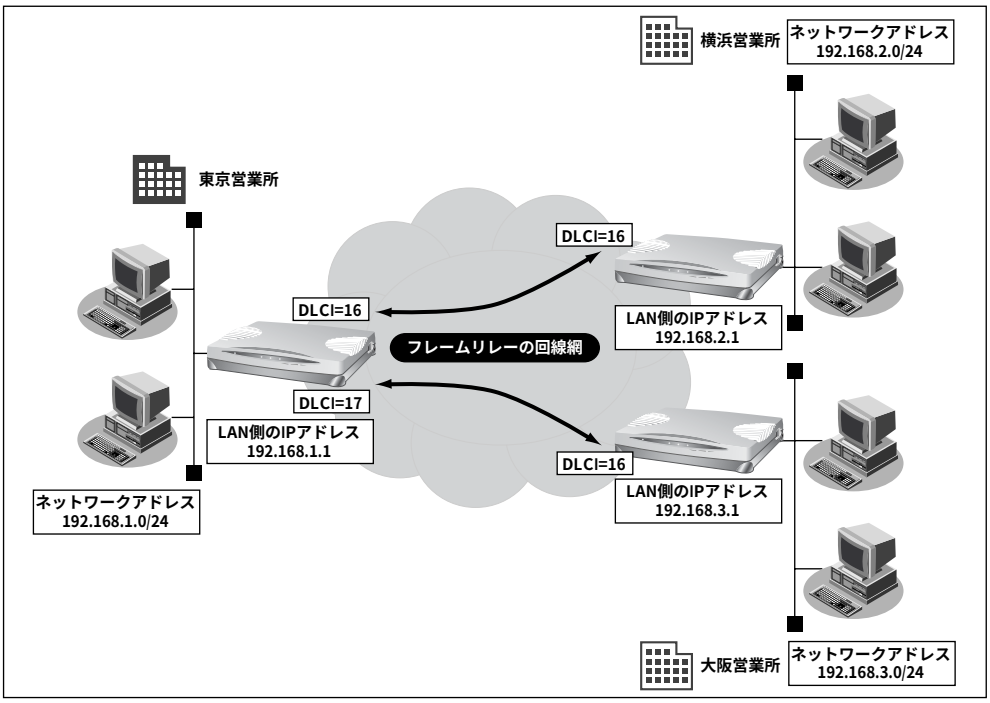
172.16.0.1と172.31.0.1の間でトンネル通信を行うことを前提とします。

相手トンネルGWにSi-Rシリーズ（NAT未使用）を利用する場合は、相手側のSi-Rに以下を設定します。

自側エンドポイント　：172.31.0.1
相手側エンドポイント　：172.16.0.1

複数の事業所LANをフレームリレーで接続する

ここでは、フレームリレーで複数の事業所を接続する場合を例に説明します。この例では、「「かんたん設定」で設定する （オフィスへフレームリレー接続のとき)」(P.99）で東京と横浜間を設定したあとに、接続先の数だけ接続先（この例では、東京と大阪間）を追加します。



● 設定条件

- フレームリレーを使用する
- 各回線の回線速度は128Kbps、CIRはそれぞれ32Kbpsとする

[東京営業所]

- DLCI　：16（横浜)、17（大阪）
- LAN側のネットワークアドレス／ネットマスク　：192.168.1.0/24
- 本装置のIPアドレス　：192.168.1.1

[横浜営業所]

- DLCI　：16
- LAN側のネットワークアドレス／ネットマスク　：192.168.2.0/24
- 本装置のIPアドレス　：192.168.2.1

[大阪営業所]

- DLCI　：16
- LAN側のネットワークアドレス／ネットマスク　：192.168.3.0/24
- 本装置のIPアドレス　：192.168.3.1

こんな事に気をつけて

文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。
詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

■ 東京営業所の設定をする

この例では、フレームリレーで東京と横浜間が接続されていることを前提として説明します。

☛ 参照 「「かんたん設定」で設定する （オフィスへフレームリレー接続のとき）」（P.99）

接続先の情報（大阪営業所）を設定する

1.　ルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］で［追加］ボタンをクリックします。

「ネットワーク情報設定」ページが表示されます。

3.　［基本情報］で以下の項目を指定します。

- ネットワーク名　→osaka（接続するネットワークの名称）
- DLCI　→17
- CIR　→32Kbps

必要に応じて上記以外の項目を指定します。

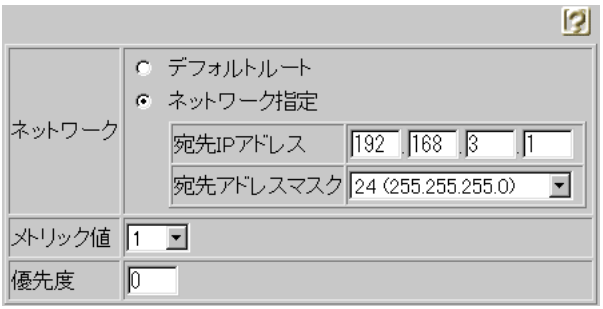
4.　［スタティックルーティング情報一覧］で［追加］ボタンをクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

「ルーティング情報設定」ページが表示されます。

5.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  宛先IPアドレス　→192.168.3.1（接続先のIPアドレス）
  宛先アドレスマスク　→24（接続先のアドレスマスク）
- メトリック値　→1



6.　[更新] ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

7.　[更新] ボタンをクリックします。

「相手情報設定」ページに戻ります。

8.　[更新] ボタンをクリックします。

9.　[設定反映] ボタンをクリックします。

設定した内容が有効になります。

■ 大阪営業所の設定をする

かんたん設定で設定する

[必須設定]

- 本装置のIPアドレス　→192.168.3.1（本装置のLAN側のIPアドレス）
- 本装置のネットマスク　→24
- 相手ルータのIPアドレス　→192.168.1.1（本装置のLAN側のIPアドレス）
- 相手ルータのネットマスク　→24
- 使用する回線速度　→128Kbps
- DLCI　→16
- CIR　→32Kbps

[オプション設定]

- ネットワーク名　→tokyo（接続するネットワークの名称）
- DHCPサーバ機能　→使用しない

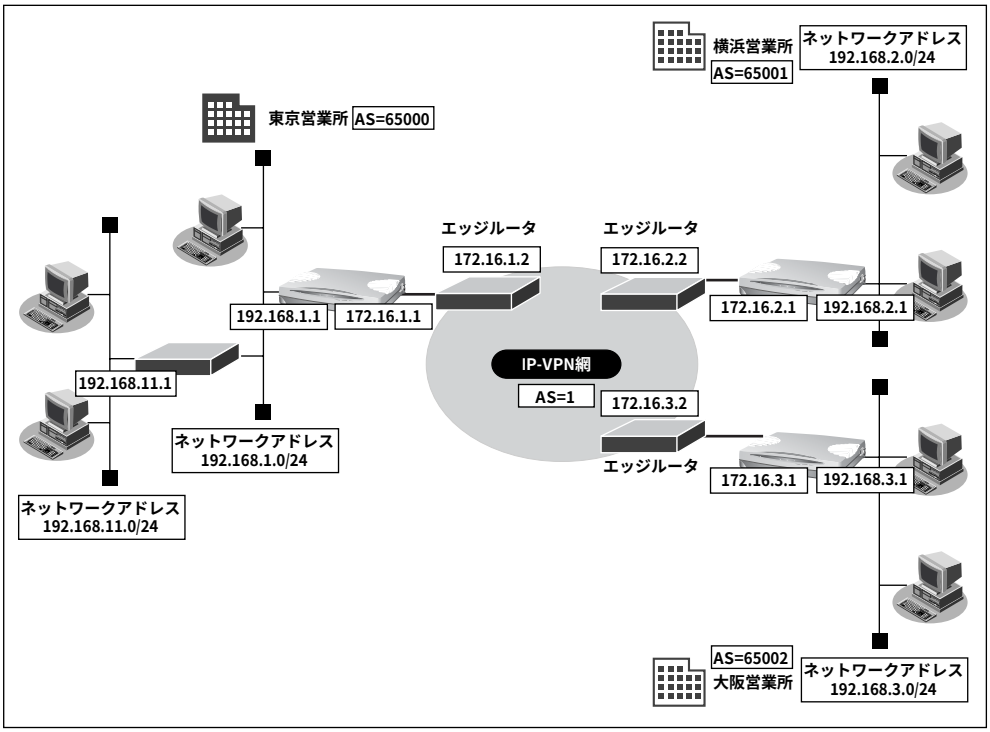
複数の事業所LANをIP-VPN網を利用して接続する

ここでは、高速ディジタル専用線（DA128）を介して、IP-VPN網で、プロトコルBGP4を使用して複数の事業所を接続する場合を例に説明します。

こんな事に気をつけて

- **この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。**
- **本装置では、IP-VPNサービスへのアクセスプロトコルでだけBGPが使用できます。**
- **BGP使用中にenableを行った場合、接続中のセッションが切断され、BGPの再起動が行われます。**

☛ 参照 「ご購入時の状態に戻すには」（P.665）



● 設定条件

- 専用線（128Kbps）を使用する

[IP-VPN網]

- 東京営業所向けIPアドレス　：172.16.1.2
- 横浜営業所向けIPアドレス　：172.16.2.2
- 大阪営業所向けIPアドレス　：172.16.3.2
- AS番号　：1

[東京営業所]

- 本装置のLAN側のIPアドレス　：192.168.1.1
- LAN側のネットワークアドレス／ネットマスク　：192.168.1.0/24
- サブLAN側のネットワークアドレス／ネットマスク　：192.168.11.0/24
- 本装置のWAN側のIPアドレス　：172.16.1.1
- AS番号　：65000
- 営業所内ルーティング　：RIPv2

[横浜営業所]

- 本装置のLAN側のIPアドレス　：192.168.2.1
- LAN側のネットワークアドレス／ネットマスク　：192.168.2.0/24
- 本装置のWAN側のIPアドレス　：172.16.2.1
- AS番号　：65001

[大阪営業所]

- 本装置のLAN側のIPアドレス　：192.168.3.1
- LAN側のネットワークアドレス／ネットマスク　：192.168.3.0/24
- 本装置のWAN側のIPアドレス　：172.16.3.1
- AS番号　：65002

こんな事に気をつけて

文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。
詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

■ 東京営業所の設定をする

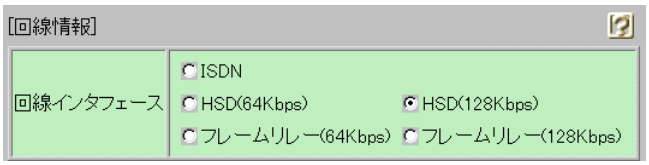
回線情報（東京営業所）を設定する

1.　詳細設定メニューのルータ設定で「回線情報」をクリックします。

「回線情報設定」ページが表示されます。

2.　［回線情報］で以下の項目を指定します。

- 回線インタフェース　→HSD（128Kbps）



3.　［更新］ボタンをクリックします。

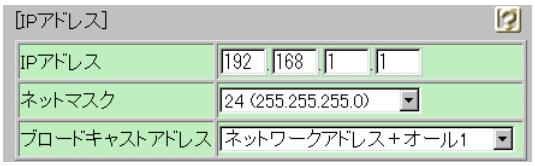
LAN情報（東京営業所）を設定する

1.　詳細設定メニューのルータ設定で「LAN情報」をクリックします。

「LAN情報設定」ページが表示されます。

2.　［IPアドレス］で以下の項目を指定します。

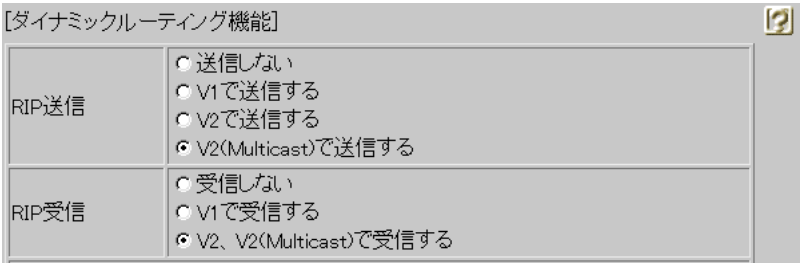
- IPアドレス　→192.168.1.1（本装置のLAN側のIPアドレス）
- ネットマスク　→24
- ブロードキャストアドレス　→ネットワークアドレス＋オール1



必要に応じて上記以外の項目を指定します。

3.　［ダイナミックルーティング機能］で以下の項目を指定します。

- RIP送信　→V2（Multicast）で送信する
- RIP受信　→V2、V2（Multicast）で受信する



4.　［更新］ボタンをクリックします。

接続先の情報（IP-VPN網）を設定する

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］で［追加］ボタンをクリックします。

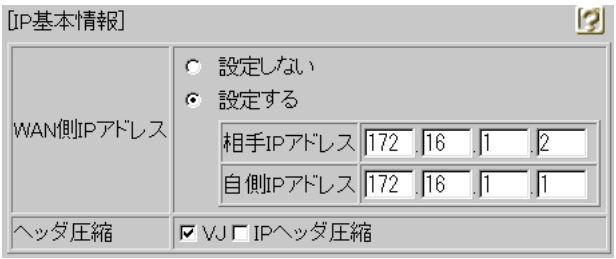
「ネットワーク情報設定」ページが表示されます。

3.　［基本情報］で以下の項目を指定します。

- ネットワーク名　→IP-VPN（接続するネットワークの名称）

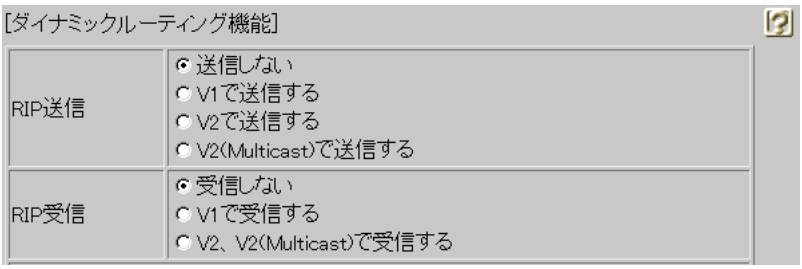
4.　［IP基本情報］で以下の項目を指定します。

- WAN側のIPアドレス　→設定する
  相手IPアドレス　→172.16.1.2
  自側IPアドレス　→172.16.1.1



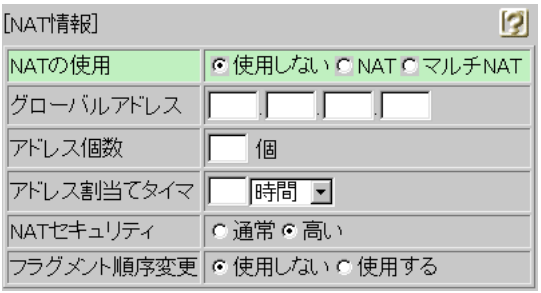
5.　［ダイナミックルーティング機能］で以下の項目を指定します。

- RIP送信　→送信しない
- RIP受信　→受信しない



6.　［NAT 情報］で以下の項目を指定します。

- NATの使用　→使用しない



必要に応じて上記以外の項目を指定します。

7.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

8.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

9.　［更新］ボタンをクリックします。

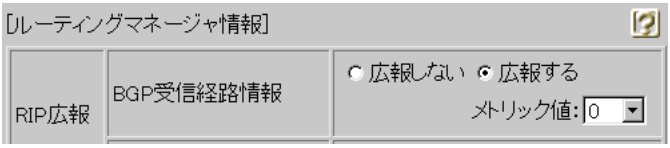
ルーティングプロトコル情報（東京営業所）を設定する

1.　詳細設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報設定」ページが表示されます。

2.　［ルーティングマネージャ情報］で以下の項目を指定します。

- RIP広報　→BGP受信経路を広報する



3.　［BGP 情報］で以下の項目を指定します。

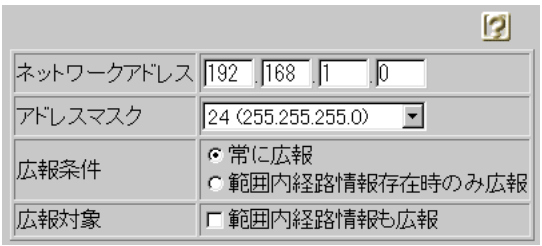
- BGP機能　→使用する
- 自AS番号　→65000

4.　［BGP 広報ネットワーク一覧］で［追加］ボタンをクリックします。

「BGP広報ネットワーク設定」ページが表示されます。

5.　以下の項目を指定します。

- ネットワークアドレス　→192.168.1.0
- アドレスマスク　→24（255.255.255.0）



6.　［更新］ボタンをクリックします。

「ルーティングプロトコル情報設定」ページに戻ります。

補足　IP-VPN網の申し込みで、東京営業所のネットワークとして複数申請している場合は、4.～6.の処理を繰り返します。

7.　手順4.～6.を参考に、以下の項目を指定します。

- ネットワークアドレス　→192.168.11.0
- アドレスマスク　→24（255.255.255.0）

8.　［BGP相手情報］で、［修正］ボタンをクリックします。

「BGP相手情報設定」ページが表示されます。

9.　以下の項目を指定します。

- 相手IPアドレス　→172.16.1.2
- 相手AS番号　→1

必要に応じて上記以外の項目を指定します。

10.　［更新］ボタンをクリックします。

「ルーティングプロトコル情報設定」ページに戻ります。

11.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

■ 横浜営業所の設定をする

「東京営業所の設定をする」を参考に、横浜営業所の設定をします。

回線情報設定（横浜営業所）を設定する

［回線情報］

- 回線インタフェース　→HSD（128Kbps）

LAN情報設定（横浜営業所）を設定する

［IPアドレス］

- IPアドレス　→192.168.2.1（本装置のLAN側のIPアドレス）
- ネットマスク　→24
- ブロードキャスト　→ネットワークアドレス＋オール1

相手情報設定（IP-VPN網）を設定する

［基本情報］

- ネットワーク名　→IP-VPN

［IP基本情報］

- WAN側のIPアドレス　→設定する
  相手IPアドレス　→172.16.2.2
  自側IPアドレス　→172.16.2.1

［ダイナミックルーティング機能］

- RIP送信　→送信しない
- RIP受信　→受信しない

［NAT情報］

- NATの使用　→使用しない

ルーティングプロトコル情報設定（横浜営業所）を設定する

［BGP情報］

- BGP機能　→使用する
- 自AS番号　→65001

［BGP広報ネットワーク設定］

- ネットワークアドレス　→192.168.2.0
- アドレスマスク　→24（255.255.255.0）

［BGP相手情報設定］

- 相手IPアドレス　→172.16.2.2
- 相手AS番号　→1

■ 大阪営業所の設定をする

「東京営業所の設定をする」を参考に、大阪営業所の設定をします。

回線情報設定（大阪営業所）を設定する

［回線情報］

- 回線インタフェース　→HSD（128Kbps）

LAN情報設定（大阪営業所）を設定する

［IPアドレス］

- IPアドレス　→192.168.3.1（本装置のLAN側のIPアドレス）
- ネットマスク　→24
- ブロードキャスト　→ネットワークアドレス＋オール1

相手情報設定（IP-VPN網）を設定する

［基本情報］

- ネットワーク名　→IP-VPN

［IP基本情報］

- WAN側のIPアドレス　→設定する
  相手IPアドレス　→172.16.3.2
  自側IPアドレス　→172.16.3.1

［ダイナミックルーティング機能］

- RIP送信　→送信しない
- RIP受信　→受信しない

［NAT情報］

- NATの使用　→使用しない

ルーティングプロトコル情報設定（大阪営業所）を設定する

［BGP情報］

- BGP機能　→使用する
- 自AS番号　→65002

［BGP広報ネットワーク設定］

- ネットワークアドレス　→192.168.3.0
- アドレスマスク　→24（255.255.255.0）

［BGP相手情報設定］

- 相手IPアドレス　→172.16.3.2
- 相手AS番号　→1

複数プロバイダと端末型接続する

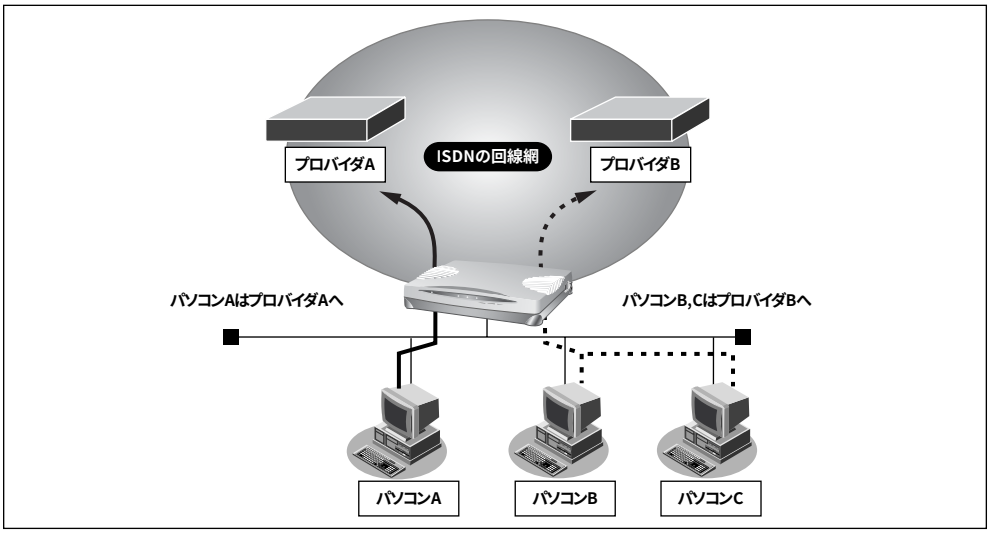
「マルチルーティング（ソースアドレスルーティング）機能」を使うと、パソコンのIPアドレスごとに接続先を変えることができます。

ここでは、パソコンが複数あって、それぞれのパソコンが別のプロバイダに加入しているような場合、本装置の「マルチルーティング（ソースアドレスルーティング）機能」を使って、それぞれ自分が加入するプロバイダに接続する場合を例に説明します。

こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。

☛ 参照 「ご購入時の状態に戻すには」（P.665）



● 設定条件

- ISDN回線を使用する
- パソコンAはプロバイダA（ISP-A）へ接続する
- パソコンA以外はプロバイダB（ISP-B）へ接続する
- プロバイダA（ISP-A）の接続先　：03-2222-1111
- パソコンAのIPアドレス　：192.168.1.2/32
- マルチNATを使用する

こんな事に気をつけて

文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。
詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

かんたん設定で基本的な設定を行う

1.　かんたん設定のインターネットへの「ISDN接続」でプロバイダBの設定を行います。

☛ 参照 「「かんたん設定」で設定する（インターネットへISDN接続のとき）」（P.74）

詳細設定でプロバイダAの情報を追加する

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］で「internet」欄の［修正］ボタンをクリックします。

「ネットワーク情報設定」ページが表示されます。

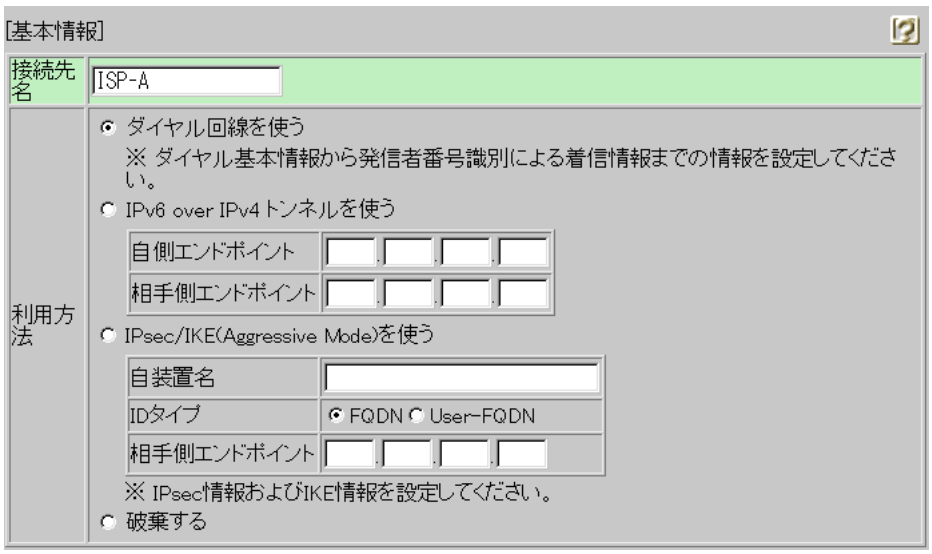
3.　［接続先情報一覧］で［追加］ボタンをクリックします。

「接続先情報設定」ページが表示されます。

4.　プロバイダAの情報を指定します。

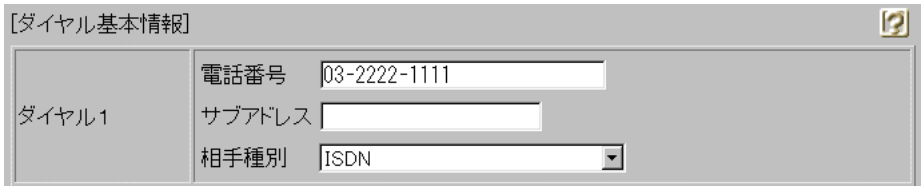
［基本情報］で以下の項目を指定します。

- 接続先名　→ISP-A（プロバイダAの名称）
- 利用方法　→ダイヤル回線を使う



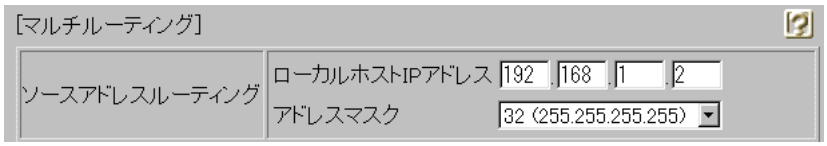
［ダイヤル基本情報］で以下の項目を指定します。

- ダイヤル1
  電話番号　→03-2222-1111（プロバイダAより提示された接続先の電話番号）



［マルチルーティング］で以下の項目を指定します。

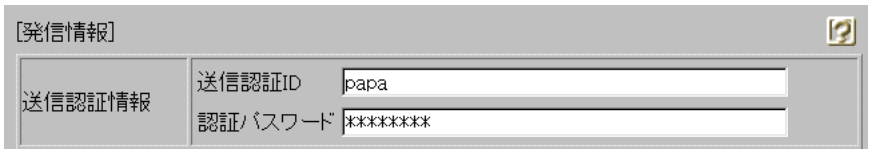
- ソースアドレスルーティング
  ローカルホストIPアドレス　→192.168.1.2（パソコンAのIPアドレス）
  アドレスマスク　→32



補足　この例では対象となるパソコンが1台のため、255.255.255.255となります。IPアドレスとアドレスマスクを組み合わせることにより、複数のIPアドレスを対象とすることができます。

［発信情報］で以下の項目を指定します。

- 送信認証情報
  送信認証ID　→papa（プロバイダAから提示された内容）
  認証パスワード　→papapass（プロバイダAから提示された内容）



必要に応じて上記以外の項目を指定します。

5.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

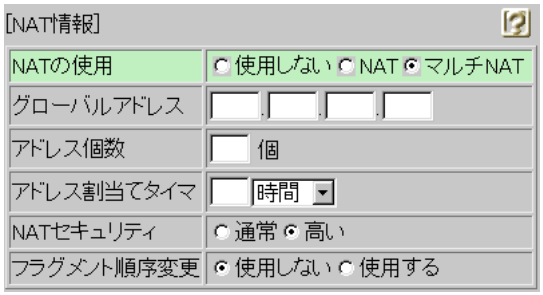
6.　ISP-Aの優先順位が「1」でない場合は、移動先の優先順位に「1」を入力し［移動］ボタンをクリックします。すでに優先順位が「1」になっている場合は、手順8.へお進みください。

こんな事に気をつけて

接続先には優先度があるため、マルチルーティングの設定をしない接続先の優先度を高くすると、優先度の低いマルチルーティング設定は無効となります。接続先の優先順位に気をつけてください。

7.　［NAT 情報］で以下の項目を指定します。

- NAT の使用　→マルチ NAT



補足 このマルチ NAT は、動的 NAT を意味します。

☛ 参照 「マルチ NAT 機能（アドレス変換機能）を使う」（P.490）

8.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

9.　［更新］ボタンをクリックします。

10.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

ヒント

◆「ソースアドレスルーティング機能」を使うとき、IP アドレスの割り当てはどうするの？

「DHCP サーバ機能」を利用すると、DHCP サーバは未使用の IP アドレスを要求のあったパソコンに順次割り当てていきます。このため、パソコンの IP アドレスが変わることがあります。

本装置がサポートしている「IP フィルタリング機能」、「静的 NAT 機能」、「マルチルーティング機能」などは、パソコンの IP アドレスが常に固定されていないと使いにくい場合があります。そこで、これらの機能を使用しながら本装置の DHCP サーバも利用できるように、「DHCP スタティック機能」が用意されています。

LAN（Ethernet）で通信する機器には MAC アドレスという固有のアドレスが設定されています。MAC アドレスは世界中で重複しないように管理されているため、この値から機器を特定できるのです。

☛ 参照 「DHCP スタティック機能を使う」（P.482）

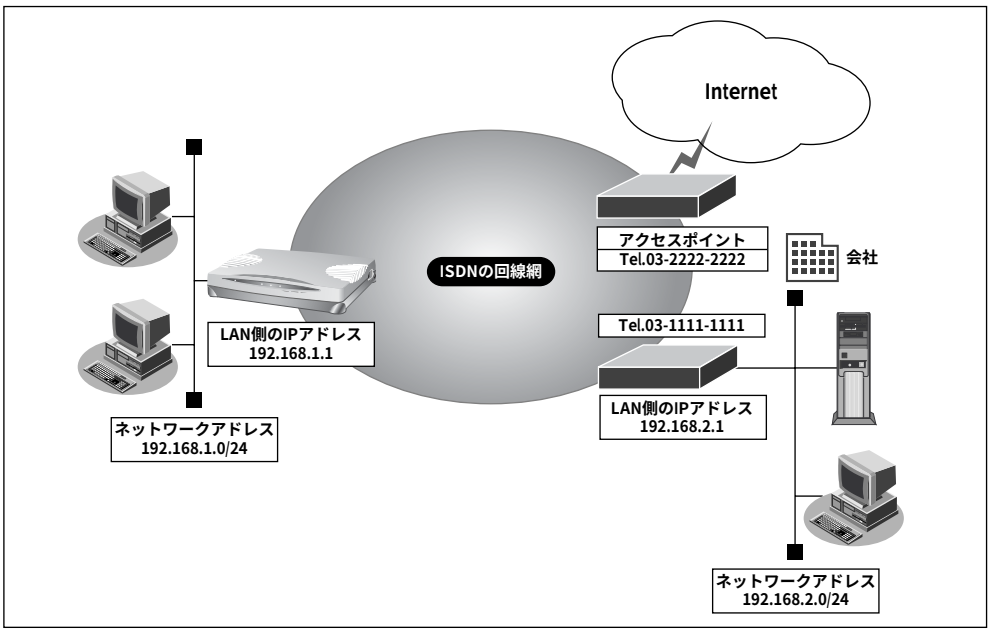
インターネットとLANに同時接続する

ISDNのBチャネルを2つ使うと、インターネットとLANをシームレスに使うことができます。ここでは、インターネットでWWWを利用しながら会社のLANにも接続する場合を例に説明します。

こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。

☛ 参照 「ご購入時の状態に戻すには」（P.665）



● 設定条件

- ISDN回線を使用する
- 新規にLANを構築する
- プロバイダには端末型ダイヤルアップ接続する

接続先の電話番号	：03-2222-2222
ユーザ認証ID	：tokyoid
ユーザ認証パスワード	：tokyopass
DNSサーバ	：192.10.10.10

- 会社にはネットワーク型ダイヤルアップ接続を行う

会社のルータが接続されている電話番号	：03-1111-1111
送信認証ID／送信認証パスワード	：officeid、officepass

こんな事に気をつけて

文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。
詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

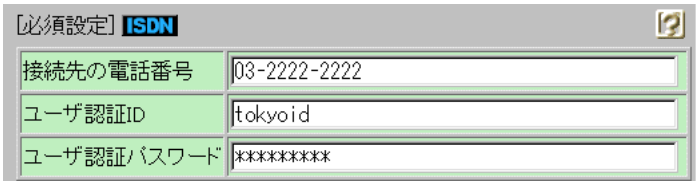
かんたん設定でインターネット接続の設定を行う

1. かんたん設定でインターネットへの「ISDN 接続」をクリックします。

「かんたん設定（インターネットへISDN 接続）」ページが表示されます。

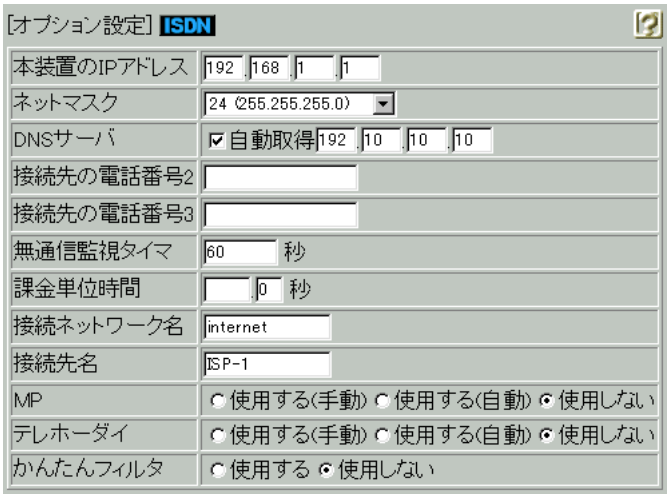
2. ［必須設定］で以下の項目を指定します。

- 接続先の電話番号　→03-2222-2222（プロバイダから提示された内容）
- ユーザ認証 ID　→tokyoid（プロバイダから提示された内容）
- ユーザ認証パスワード　→tokyopass（プロバイダから提示された内容）



［オプション設定］で以下の項目を指定します。

- DNS サーバ　→192.10.10.10（プロバイダから提示されたDNS サーバのIPアドレス）
- 接続ネットワーク名　→internet（接続するネットワークの名称）
- 接続先名　→ISP-1（プロバイダの名称）



3.　［設定終了］ボタンをクリックします。

再起動後に、通信できる状態になります。

接続先の情報を設定する

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］で［追加］ボタンをクリックします。

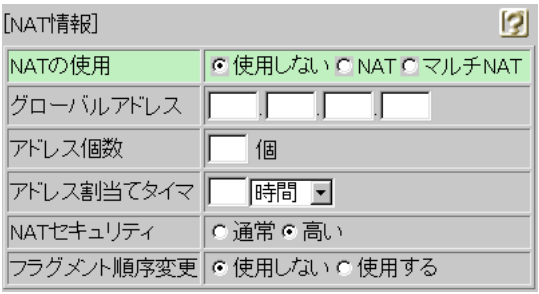
「ネットワーク情報設定」ページが表示されます。

3.　［基本情報］で以下の項目を指定します。

- ネットワーク名　→kaisya（接続するネットワークの名称）
- 自動ダイヤル　→する

［NAT 情報］で以下の項目を指定します。

- NAT の使用　→使用しない



必要に応じて上記以外の項目を指定します。

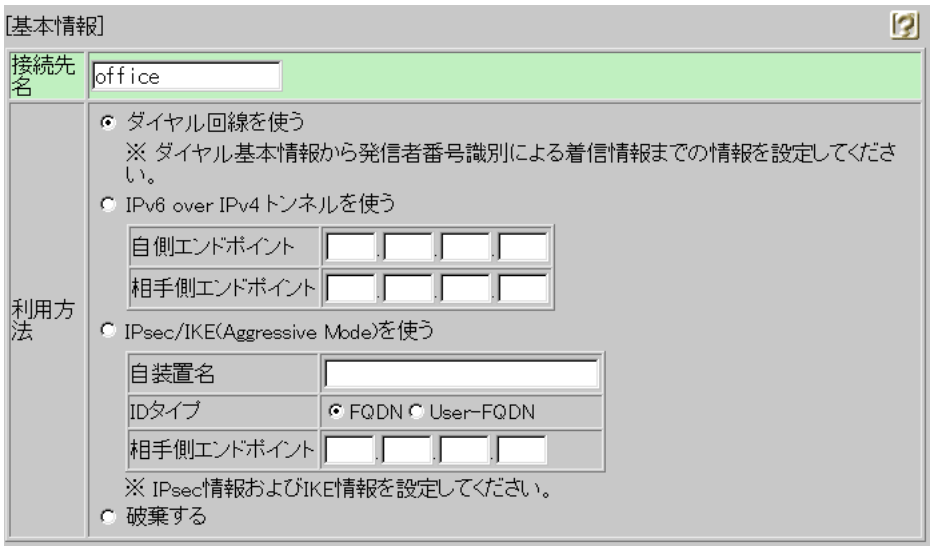
4.　［接続先情報一覧］で［追加］ボタンをクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

「接続先情報設定」ページが表示されます。

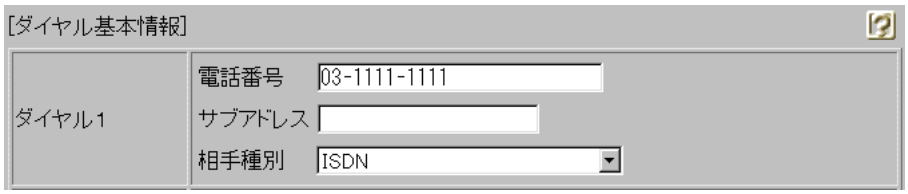
5.　［基本情報］で以下の項目を指定します。

- 接続先名　→office（接続先の名称）
- 利用方法　→ダイヤル回線を使う



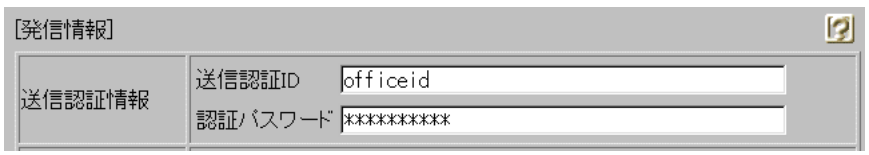
［ダイヤル基本情報］で以下の項目を指定します。

- ダイヤル1
  電話番号　→03-1111-1111（接続先の電話番号）



［発信情報］で以下の項目を指定します。

- 送信認証情報
  送信認証ID　→officeid
  認証パスワード　→officepass



必要に応じて上記以外の項目を指定します。

6.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

7.　［スタティックルーティング情報一覧］で［追加］ボタンをクリックします。

「ルーティング情報設定」ページが表示されます。

8.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  宛先IPアドレス　→192.168.2.0（接続先のネットワークアドレス）
  宛先アドレスマスク　→24（接続先のアドレスマスク）
- メトリック値　→1

9.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

10.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

11.　［更新］ボタンをクリックします。

12.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

- **本装置のIPアドレスを変更した場合、再起動後に本装置にアクセスするためには、URLを変更する必要があります。また、パソコン側の設定変更および再起動を行ってください。**
- **会社LAN上のホスト名の名前解決を行う場合は、ProxyDNSの設定が必要です。**

☛ 参照 「DNSサーバを使いこなす（ProxyDNS）」（P.471）

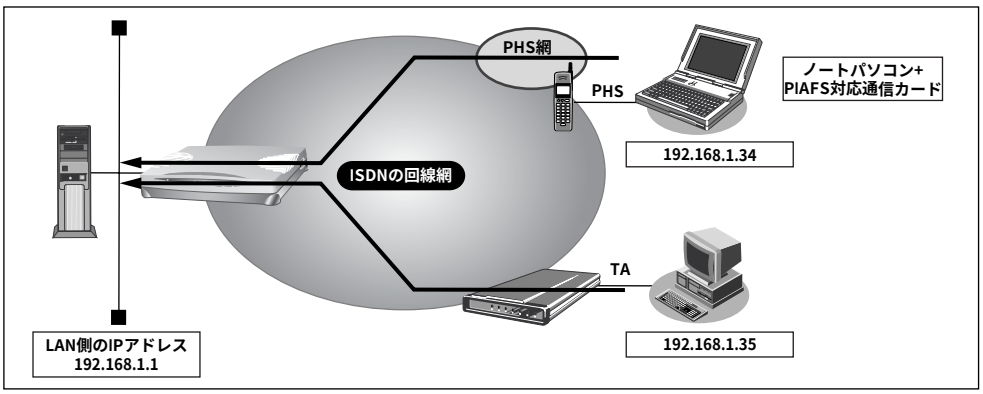
外部のパソコンと接続する（TA&PHS）

ここでは、ISDN回線経由で外部から本装置へ着信接続する例を説明します。

こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。

☛ 参照 「ご購入時の状態に戻すには」（P.665）



● 設定条件

- 本装置のLAN側のネットワークアドレス／ネットマスク　：192.168.1.0/24

[ノートパソコン+PHS]

- 割り当てIPアドレス　：192.168.1.34
- 電話番号　：070-1234-5678
- PHS通信速度　：64Kbps
- 受諾認証ID　：mobileid
- 受諾認証パスワード　：mobilepass

[パソコン+TA]

- 割り当てIPアドレス　：192.168.1.35
- 電話番号　：03-1234-5678
- 受諾認証ID　：sohoid
- 受諾認証パスワード　：sohopass

☛ 参照 「外部のパソコンから着信接続する （アクセスサーバ機能）」（P.497）

補足 本装置のLAN側のネットワークと同一のネットワークアドレスを別ネットワークのパソコンに割り当てることによって、Proxy ARPが自動的に動作し、ISDN回線経由で接続されたパソコンがLAN上に存在するように扱えます。

ヒント

◆ Proxy ARPとは

Ethernet上で通信する場合、相手を識別するためにMACアドレスが使用されます。このとき、IPアドレスとMACアドレスの対応付けを行う手段としてARP（Address Resolution Protocol）が使用されます。

ブロードキャストでARP要求を発行することにより、LAN上で自分のIPアドレスに関連するARP要求であると認識したパソコンは、自分のMACアドレスを送り返します。

Proxy ARPとは、パソコンから送られてくるARP要求に対して、実際のパソコンの代わりに応答する機能です。

こんな事に気をつけて

文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。
詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

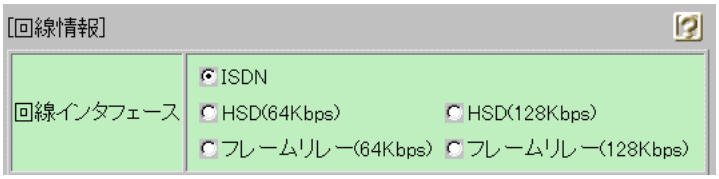
回線情報を設定する

1.　詳細設定メニューのルータ設定で「回線情報」をクリックします。

「回線情報設定」ページが表示されます。

2.　［回線情報］で以下の項目を指定します。

- 回線インタフェース　→ISDN



3.　［更新］ボタンをクリックします。

接続先情報（ノートパソコン＋ PHS）を設定する

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］で［追加］ボタンをクリックします。

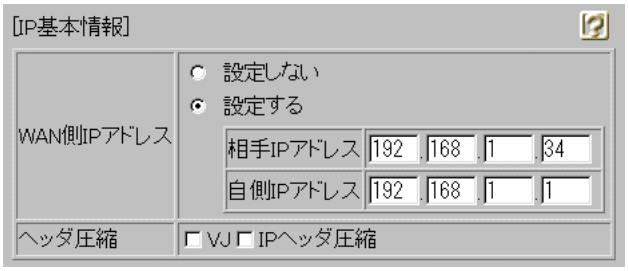
「ネットワーク情報設定」ページが表示されます。

3.　［基本情報］で以下の項目を指定します。

- ネットワーク名　→outside（接続するネットワークの名称）
- 自動ダイヤル　→しない

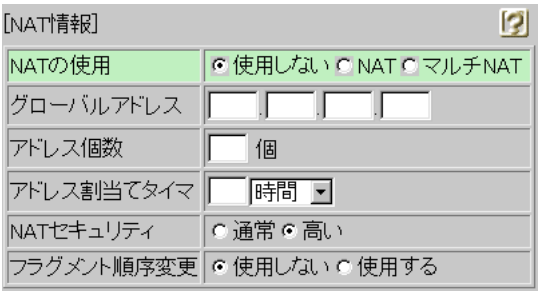
［IP 基本情報］で以下の項目を指定します。

- WAN側 IPアドレス　→設定する
  相手 IPアドレス　→192.168.1.34
  自側 IPアドレス　→192.168.1.1



［NAT 情報］で以下の項目を指定します。

- NATの使用　→使用しない



必要に応じて上記以外の項目を指定します。

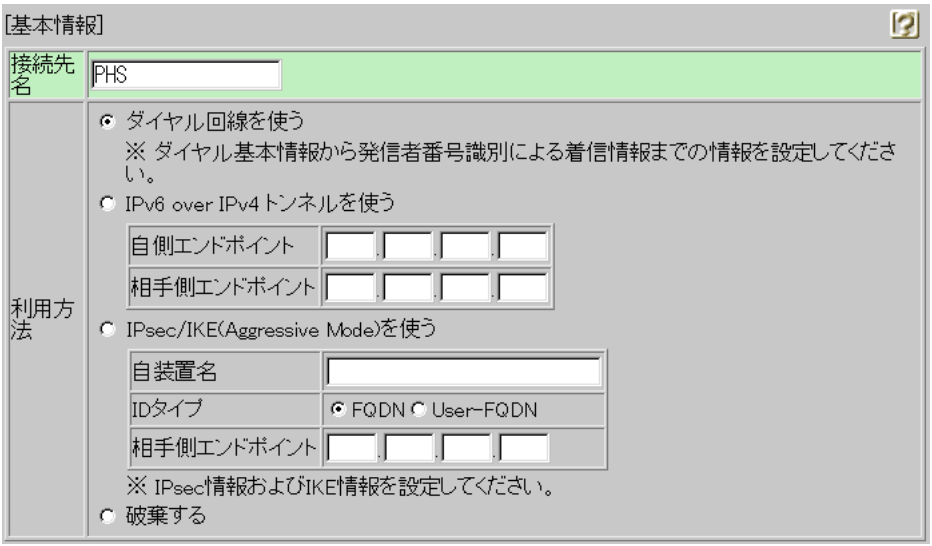
4.　［接続先情報一覧］で［追加］ボタンをクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

「接続先情報設定」ページが表示されます。

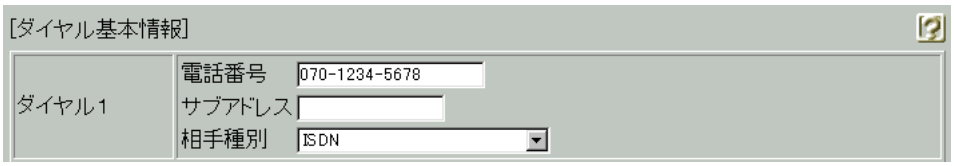
5.　［基本情報］で以下の項目を指定します。

- 接続先名　→PHS（接続先の名称）
- 利用方法　→ダイヤル回線を使う



［ダイヤル基本情報］で以下の項目を指定します。

- ダイヤル1
  電話番号　→070-1234-5678
  相手種別　→指定しない（デフォルト：ISDN）

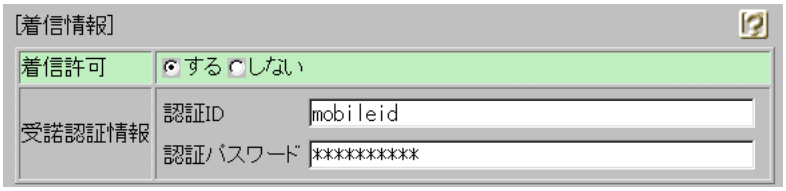


こんな事に気をつけて

PIAFS 64Kbpsを使用する場合、発信側からサブアドレスを発信しても通知されないため、着信時の接続先情報でサブアドレスを指定しても無効となります。

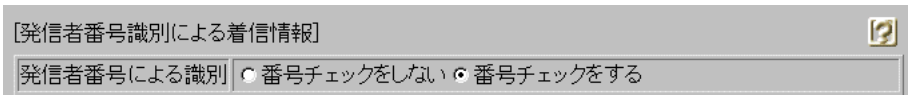
[着信情報] で以下の項目を指定します。

- 着信許可　→する
- 受諾認証情報
  認証 ID　→mobileid
  認証パスワード　→mobilepass



[発信者番号識別による着信情報] で以下の項目を指定します。

- 発信者番号による識別　→番号チェックをする



必要に応じて上記以外の項目を指定します。

6.　[更新] ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

接続先情報（パソコン＋ TA）を設定する

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　[ネットワーク情報一覧] で [追加] ボタンをクリックします。

「ネットワーク情報設定」ページが表示されます。

3.　[基本情報] で以下の項目を指定します。

- ネットワーク名　→home（接続するネットワークの名称）
- 自動ダイヤル　→しない

[IP 基本情報] で以下の項目を指定します。

- WAN 側 IP アドレス　→設定する
  相手 IP アドレス　→192.168.1.35
  自側 IP アドレス　→192.168.1.1

[NAT 情報] で以下の項目を指定します。

- NAT の使用　→使用しない

必要に応じて上記以外の項目を指定します。

4.　［接続先情報一覧］で［追加］ボタンをクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

「接続先情報設定」ページが表示されます。

5.　［基本情報］で以下の項目を指定します。

- 接続先名　→TA（接続先の名称）
- 利用方法　→ダイヤル回線を使う

［ダイヤル基本情報］で以下の項目を指定します。

- ダイヤル1
  電話番号　→03-1234-5678
  相手種別　→指定しない（デフォルト：ISDN）

［着信情報］で以下の項目を指定します。

- 着信許可　→する
- 受諾認証情報
  認証ID　→sohoid
  認証パスワード　→sohopass

［発信者番号による着信識別］で以下の項目を指定します。

- 発信者番号による識別　→番号チェックをする

必要に応じて上記以外の項目を指定します。

6.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

7.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

8.　［更新］ボタンをクリックします。

9.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

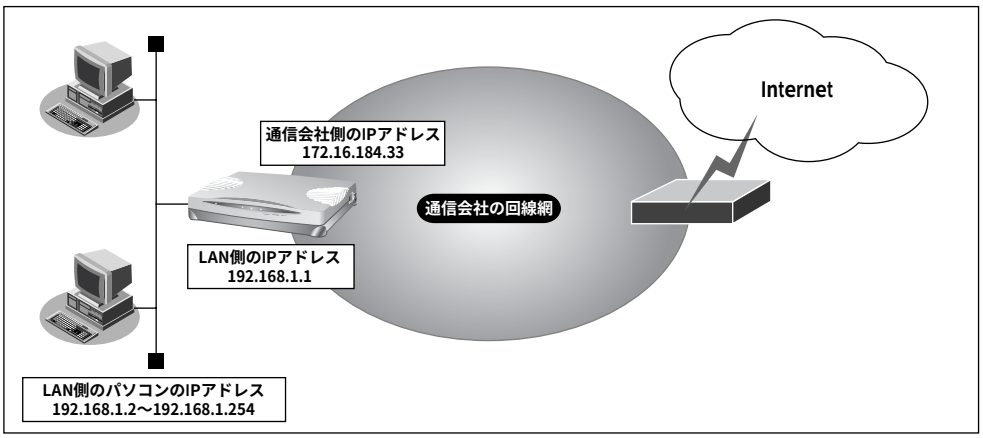
通信会社提供の専用線接続サービスと接続する

ここでは、通信会社提供の専用線接続サービスと接続する際に、LAN側に接続されたパソコンの台数が割り当てられたIPアドレスより多い場合を例に説明します。パソコンの台数が割り当てIPアドレス以下の場合については、「「かんたん設定」で設定する （インターネットへ専用線接続のとき）」（P.85）を参照してください。

こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。

☛ 参照 「ご購入時の状態に戻すには」（P.665）



● 設定条件

- 専用線（128Kbps）を使用する
- 通信会社側のDNSサーバを使用する　：192.10.10.10
- 通信会社より提示されたドメイン名　：domain.carrier.ne.jp
- 接続されたパソコンの台数が割り当てられたIPアドレス（5+1）よりも多い（253+1）

[通信会社側]

- ネットワークアドレス　：172.16.184.32/29
- 本装置のIPアドレス　：172.16.184.33
- ホストアドレス　：172.16.184.34～172.16.184.38
- ブロードキャストアドレス　：172.16.184.39

[LAN側]

- ネットワークアドレス　：192.168.1.0/24
- 本装置のIPアドレス　：192.168.1.1
- パソコンのIPアドレス　：192.168.1.2～192.168.1.254

こんな事に気をつけて

文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。
詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

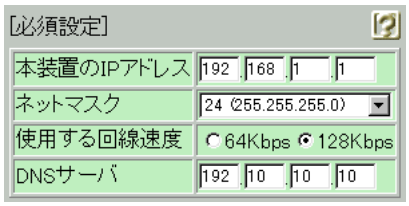
かんたん設定で専用線接続の設定を行う

1.　かんたん設定でインターネットへの「専用線接続」をクリックします。

「かんたん設定（インターネットへ専用線接続）」ページが表示されます。

2.　［必須設定］で以下の項目を指定します。

- 本装置のIPアドレス　→192.168.1.1
- ネットマスク　→24
- 使用する回線速度　→128Kbps
- DNSサーバ　→192.10.10.10（通信会社より提示された内容）



［オプション設定］で以下の項目を指定します。

- 接続ネットワーク名　→internet（接続するネットワークの名称）
- ドメイン名　→domain.carrier.ne.jp（通信会社より提示されたドメイン名）
- アドレス変換　→マルチNAT
  グローバルアドレス　→172.16.184.34（アドレス変換でパソコンに割り当てる連続したIPアドレスの先頭）
  アドレス個数　→5（連続したグローバルアドレスの個数）

補足　この例では通信会社より割り当てられるIPアドレスは8個です。そのうちネットワークアドレス（1個）、ブロードキャストアドレス（1個）、本装置のIPアドレス（1個）を除いた5個がパソコンに割り当てることのできるIPアドレスとなります。

3.　［設定終了］ボタンをクリックします。

再起動後に、通信できる状態になります。

アドレス変換情報を設定する

補足　通信会社から本装置に向かってPINGのテストを行う場合があるため、本装置にはグローバルアドレスを割り当てておく必要があります。

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］でかんたん設定で設定したネットワーク名の欄の［修正］ボタンをクリックします。

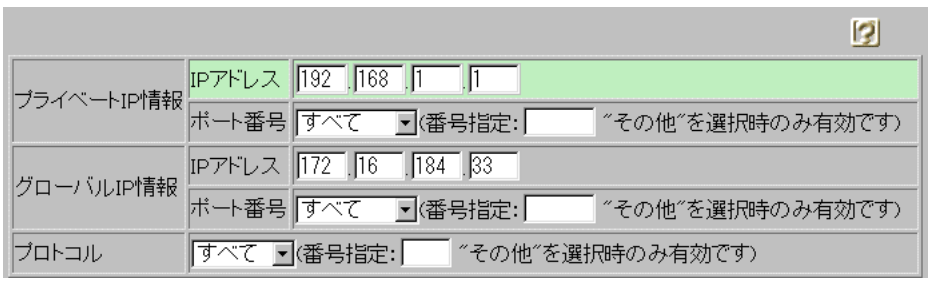
「ネットワーク情報設定」ページが表示されます。

3.　「静的NAT情報一覧」で［追加］ボタンをクリックします。

「静的NAT情報設定」ページが表示されます。

4.　以下の項目を指定します。

- プライベートIP情報
  IPアドレス　→192.168.1.1
  ポート番号　→すべて
- グローバルIP情報
  IPアドレス　→172.16.184.33
  ポート番号　→すべて



こんな事に気をつけて

- **本装置のIPアドレスを変更した場合、再起動後に本装置にアクセスするためには、パソコンの再起動およびURLを変更する必要があります。**
- **動的NATと静的NATが混在する場合、動的NATで使用するIPアドレスと静的NATで使用するIPアドレスは重複しないようにしてください。**

5.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

6.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

7.　［更新］ボタンをクリックします。

8.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

ネットワーク型接続でマルチNATを使用する際には、グローバルアドレスの設定が必須となります。なお、端末型接続では、接続時にグローバルアドレスが割り当てられるため、設定は不要です。

ログインパスワードを設定する

こんな事に気をつけて

本装置にグローバルアドレスが割り振られた場合、telnetなどで接続可能となるため、ログインパスワードを設定してアクセスを制限しなくてはなりません。

1.　詳細設定メニューのルータ設定で「パスワード情報」をクリックします。

「パスワード情報設定」ページが表示されます。

2.　以下の項目を指定します。

- 新しいログインパスワード　→himitu
- ログインパスワードの確認　→himitu

必要に応じて上記以外の項目を指定します。

3.　［更新］ボタンをクリックします。

設定した内容が有効になります。

第2部
リファレンス編

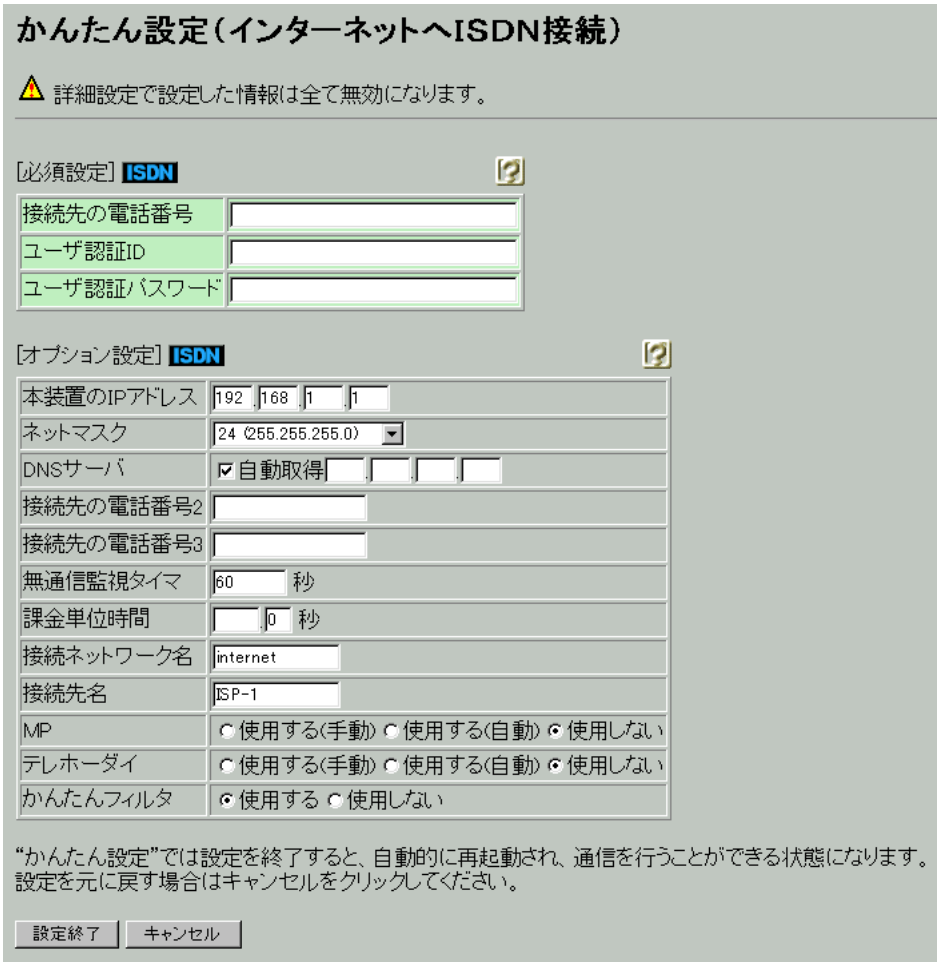
第4章　設定ページリファレンス

4

この章では、

本装置で設定できる項目をページごとに紹介します。

かんたん設定（インターネットへISDN接続）



[必須設定]

接続先の電話番号

半角数字32桁以内で指定します。－、(、)、が区切り文字として使えます。

《指定例》

01-2345-6789

01(2345)6789

ユーザ認証ID

接続先より通知されたIDを半角英数字64文字以内で指定します。

ユーザ認証パスワード

接続先より通知されたパスワードを半角英数字64文字以内で指定します。

[オプション設定]

本装置のIPアドレス／ネットマスク

本装置のIPアドレスとネットマスクを指定します。ただし、既存のネットワークに接続するのでなければ、修正は不要です。
IPアドレスに0.0.0.0を指定すると通信ができなくなります。

DNSサーバ

必要に応じて接続先、またはネットワーク管理者に指示されたDNSサーバのIPアドレスを指定します。指定する値はDHCPサーバ機能により広報されます。省略、または0.0.0.0を指定する場合は、広報を行いません。また、“自動取得”をチェックする場合は、本装置のIPアドレスをDNSサーバアドレスとして広報します。実際のDNSサーバアドレスは回線接続時に相手システムより取得し、ProxyDNS機能が名前解決を行います。自動取得は相手システムがDNSサーバアドレスの広報機能（RFC1877）をサポートしている場合にだけ使用できます。

接続先の電話番号2／3

マルチダイヤルを行う場合に指定します。記述方法は、接続先の電話番号と同じです。

無通信監視タイマ

ISDN回線の無通信監視タイマを0～3600秒の範囲で指定します。その時間を超えても、通信が行われなかった場合は、ISDN回線を自動的に切断します。なお、0を指定した場合は、自動切断を行いません。

課金単位時間

課金単位時間を0.0～3600.0秒の範囲で指定します。ここで指定する時間は無通信監視による回線切断のときに参照され、同一料金で最大の接続時間を得るよう回線切断タイミングを調整します。なお、0を指定した場合は、課金単位の調整を行いません。

接続ネットワーク名

ネットワークを識別する名称を半角英数字8文字以内で指定します。

接続先名

接続先を識別する名称を半角英数字8文字以内で指定します。

MP

MP接続をするかどうかを選択します。“自動”の場合は、データ通信量に応じて適宜増減します。“手動”の場合は、「操作メニュー」の「手動チャネル増加」「手動チャネル減少」を用いてチャネルの増減を行います。

テレホーダイ

テレホーダイなどのサービスを利用する場合に回線接続保持機能を使用するかどうかを選択します。“自動”の場合は、毎日夜11:00～翌朝8:00の時間帯は無通信監視タイマによる回線の自動切断を行いません。“手動”の場合は「操作メニュー」の「テレホーダイ設定」「テレホーダイ終了」を用いて開始／終了を行います。“自動”の場合には、必ず装置の時刻を正しく設定します。

かんたんフィルタ

かんたんフィルタは、通常の使用方法で起こりやすい以下の問題を回避するためのIPフィルタを簡単に設定できます。

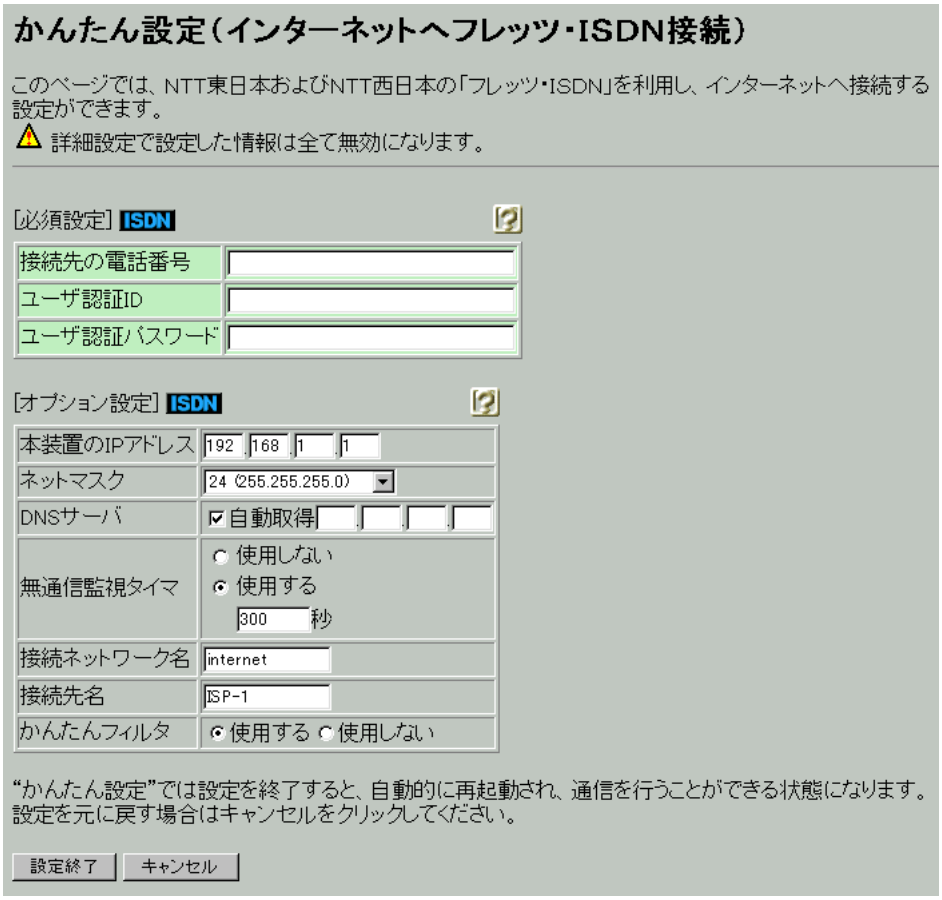
Windows NT®、Windows® 95などによるMicrosoft Networkを使用している場合、お客様のネットワーク設定によっては、NetBIOS over TCPによって定期的に送出されるパケットにより自動発信してしまう場合があります。この問題を回避するために、NetBIOS over TCPが使用するTCPおよびUDPのサービスポートの137から139を遮断するフィルタを設定します。

ping（ICMP echo）などのコマンドにより自動発信してしまう場合があります。この問題を回避するために、ICMPプロトコルによる自動発信を抑止するフィルタを設定します。なお、回線が接続状態にある時にはICMPパケットを通過させます。

syslog、TIME、NTP（SNTP）により自動発信してしまう場合があります。この問題を回避するために、それぞれのプロトコルによる自動発信を抑止するフィルタを設定します。なお、回線が接続状態にある時にはそれぞれのパケットを通過させます。

Windows® 2000から本装置を経由してインターネットへ接続する場合、Windows® 2000が送信する予期しないDNSパケットにより自動発信してしまう場合があります。この問題を回避するために、ProxyDNS情報に問い合わせタイプがSOA（6）、SRV（33）のDNSパケットを破棄するフィルタ、ホストデータベース情報にIPアドレスが「127.0.0.1」のホスト名は「localhost」を設定します。

かんたん設定（インターネットへフレッツ・ISDN接続）



[必須設定]

接続先の電話番号

半角数字を32桁以内で指定します。－、(、)、が区切り文字として使えます。

《指定例》
01-2345-6789
01(2345)6789

ユーザ認証ID

接続先より通知されたIDを半角英数字64文字以内で指定します。

ユーザ認証パスワード

接続先より通知されたパスワードを半角英数字64文字以内で指定します。

[オプション設定]

本装置のIPアドレス／ネットマスク

本装置のIPアドレスとネットマスクを指定します。ただし、既存のネットワークに接続するのでなければ、修正は不要です。
IPアドレスに0.0.0.0を指定すると通信ができなくなります。

DNSサーバ

必要に応じて接続先、またはネットワーク管理者に指示されたDNSサーバのIPアドレスを指定します。指定する値はDHCPサーバ機能により広報されます。省略、または0.0.0.0を指定する場合は広報を行いません。また、“自動取得”をチェックする場合は、本装置のIPアドレスをDNSサーバアドレスとして広報します。実際のDNSサーバアドレスは回線接続時に相手システムより取得し、ProxyDNS機能が名前解決を行います。自動取得は相手システムがDNSサーバアドレスの広報機能（RFC1877）をサポートしている場合にだけ使用できます。

無通信監視タイマ

ISDN回線の無通信監視タイマを0～3600秒の範囲で指定します。その時間を超えても、通信が行われない場合は、ISDN回線を自動的に切断します。なお、0を指定した場合は、自動切断を行いません。

接続ネットワーク名

ネットワークを識別する名称を半角英数字8文字以内で指定します。

接続先名

接続先を識別する名称を半角英数字8文字以内で指定します。

かんたんフィルタ

かんたんフィルタは、通常の使用方法で起こりやすい以下の問題を回避するためのIPフィルタを簡単に設定できます。

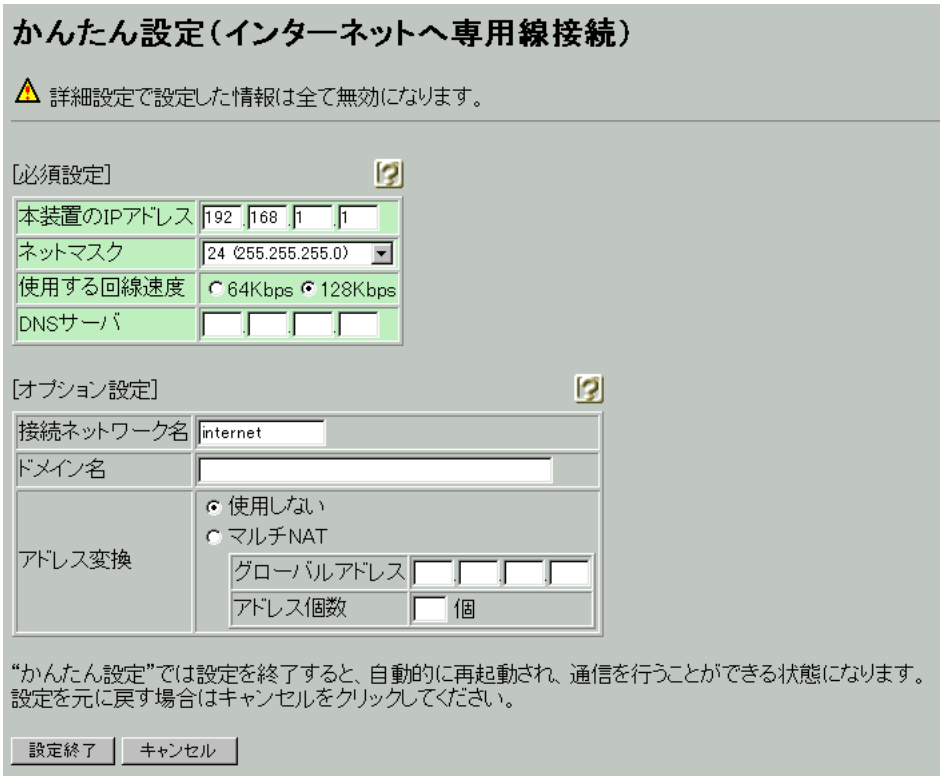
Windows NT®、Windows® 95などによるMicrosoft Networkを使用している場合、お客様のネットワーク設定によっては、NetBIOS over TCPによって定期的に送出されるパケットにより自動発信してしまう場合があります。この問題を回避するために、NetBIOS over TCPが使用するTCPおよびUDPのサービスポートの137から139を遮断するフィルタを設定します。

ping（ICMP echo）などのコマンドにより自動発信してしまう場合があります。この問題を回避するために、ICMPプロトコルによる自動発信を抑止するフィルタを設定します。なお、回線が接続状態にある時にはICMPパケットを通過させます。

syslog、TIME、NTP（SNTP）により自動発信してしまう場合があります。この問題を回避するために、それぞれのプロトコルによる自動発信を抑止するフィルタを設定します。なお、回線が接続状態にある時にはそれぞれのパケットを通過させます。

Windows® 2000から本装置を経由してインターネットへ接続する場合、Windows® 2000が送信する予期しないDNSパケットにより自動発信してしまう場合があります。この問題を回避するために、ProxyDNS情報に問い合わせタイプがSOA（6）、SRV（33）のDNSパケットを破棄するフィルタ、ホストデータベース情報にIPアドレスが「127.0.0.1」のホスト名は「localhost」を設定します。

かんたん設定（インターネットへ専用線接続）



[必須設定]

本装置のIPアドレス／ネットマスク

本装置のIPアドレスとネットマスクを指定します。マルチNATを使用する場合は、ローカルなIPアドレス、使用しない場合は、プロバイダから割り当てられたIPアドレスを指定します。IPアドレスに0.0.0.0を指定すると通信ができなくなります。

使用する回線速度

使用する回線速度を選択します。

DNSサーバ

接続先、またはネットワーク管理者に指示されたDNSサーバのIPアドレスを指定します。指定する値はDHCPサーバ機能により広報されます。0.0.0.0を指定した場合は、広報を行いません。

[オプション設定]

接続ネットワーク名

ネットワークを識別する名称を半角英数字8文字以内で指定します。

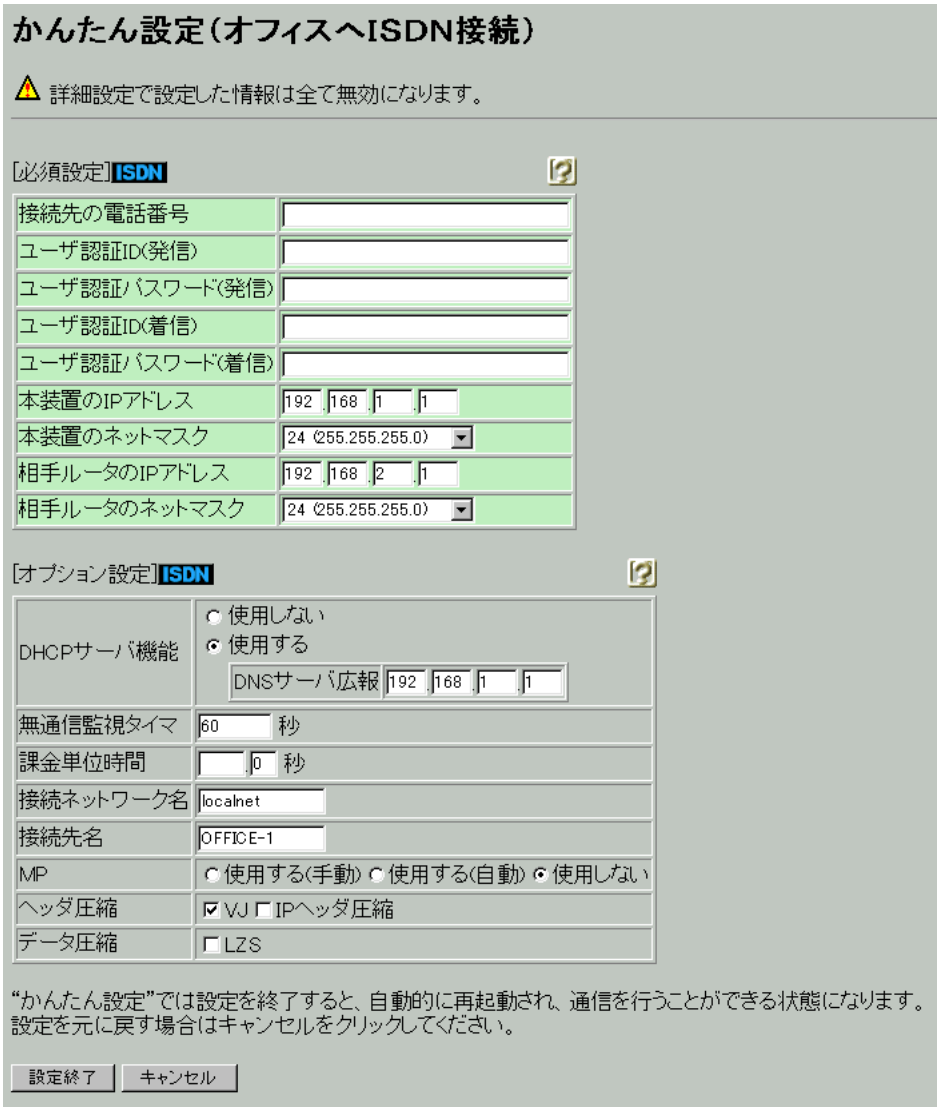
ドメイン名

必要に応じて接続先、またはネットワーク管理者に指示されたドメイン名を半角英数字80文字以内で指定します。省略する場合は、DHCPサーバによる広報を行いません。

アドレス変換

マルチNATを使うとプロバイダから取得しているIPアドレス個数以上の端末を使用できます。使用する場合は、“マルチNAT”を選択します。WAN側に固定のアドレスを1つ、または複数持っている場合は、“グローバルアドレス”と“アドレス個数”を指定します。“アドレス個数”は1～16の範囲で指定できます。“グローバルアドレス”を先頭とする“アドレス個数”分のアドレスが本装置のWAN IPアドレスとなります。

かんたん設定（オフィスへISDN接続）



[必須設定]

接続先の電話番号

半角数字32桁以内で指定します。－、(、)、が区切り文字として使えます。

《指定例》
01-2345-6789
01(2345)6789

ユーザ認証ID／パスワード（発信）

本装置から発信接続するときに使用する認証IDとパスワードを半角英数字64文字以内で指定します。

ユーザ認証パスワード／パスワード（着信）

本装置から着信接続するときに使用する認証IDとパスワードを半角英数字64文字以内で指定します。

本装置のIPアドレス／ネットマスク

本装置のIPアドレスとネットマスクを指定します。ただし、既存のネットワークに接続するのでなければ、修正は不要です。
IPアドレスに0.0.0.0を指定すると通信ができなくなります。

相手ルータのIPアドレス／ネットマスク

相手ルータのIPアドレスとネットマスクを指定します。本装置はこの指定で得られるネットワークに対してスタティックルートを指定します。

[オプション設定]

DHCPサーバ機能

DHCPサーバ機能を使用するかどうかを選択します。

DNSサーバ広報

必要に応じて接続先、またはネットワーク管理者に指示されたDNSサーバのIPアドレスを指定します。指定する値はDHCPサーバ機能により広報されます。省略、または0.0.0.0を指定する場合は、広報を行いません。

無通信監視タイマ

ISDN回線の無通信監視タイマを0～3600秒の範囲で指定します。その時間を超えても、通信が行われない場合は、ISDN回線を自動的に切断します。なお、0を指定した場合は、自動切断を行いません。

課金単位時間

課金単位時間を0.0～3600.0秒の範囲で指定します。ここで指定する時間は無通信監視による回線切断のときに参照され、同一料金で最大の接続時間を得るよう回線切断タイミングを調整します。なお、0を指定した場合は、課金単位の調整を行いません。

接続ネットワーク名

ネットワークを識別する名称を半角英数字8文字以内で指定します。

接続先名

接続先を識別する名称を半角英数字8文字以内で指定します。

MP

MP接続をするかどうかを選択します。“自動”の場合は、データ通信量に応じて適宜増減します。“手動”の場合は、「操作メニュー」の「手動チャネル増加」「手動チャネル減少」を用いてチャネルの増減を行います。

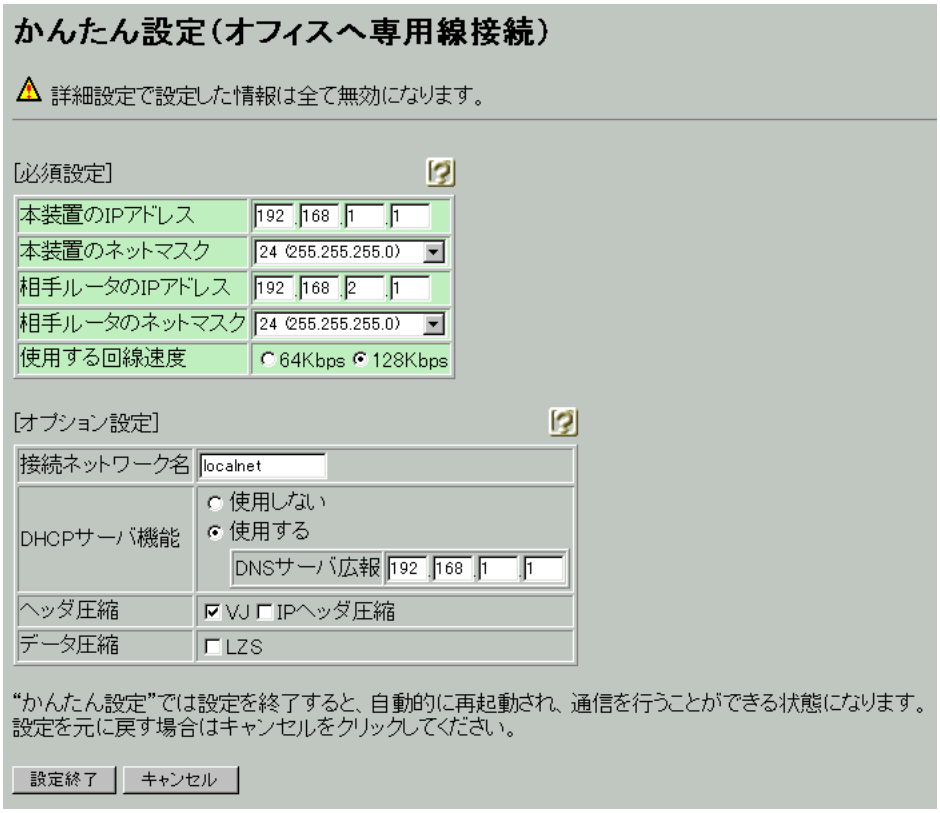
ヘッダ圧縮

送受信するヘッダを圧縮します。ヘッダ圧縮のアルゴリズムは、VJヘッダ圧縮（RFC1144に準拠）およびIPヘッダ圧縮（RFC2507／RFC2508に準拠）をサポートします。使用する指定の場合も、実際にヘッダ圧縮を行うかどうかは、相手ホストとのネゴシエーションで決まります。

データ圧縮

送受信するデータを圧縮します。データ圧縮のアルゴリズムは、LZSをサポートします。使用する指定の場合も、実際にデータ圧縮を行うかどうかは、相手ホストとのネゴシエーションで決まります。

かんたん設定（オフィスへ専用線接続）



[必須設定]

本装置のIPアドレス／ネットマスク

本装置のIPアドレスとネットマスクを指定します。マルチNATを使用する場合は、ローカルなIPアドレス、使用しない場合は、プロバイダから割り当てられたIPアドレスを指定します。IPアドレスに0.0.0.0を指定すると通信ができなくなります。

相手ルータのIPアドレス／ネットマスク

相手ルータのIPアドレスとネットマスクを指定します。本装置は、この指定で得られるネットワークに対してスタティックルートを指定します。

使用する回線速度

使用する回線速度を選択します。

[オプション設定]

接続ネットワーク名

ネットワークを識別する名称を半角英数字8文字以内で指定します。

DHCP サーバ機能

DHCP サーバ機能を使用するかどうかを指定します。

DNS サーバ広報

必要に応じて接続先、またはネットワーク管理者に指示されたDNSサーバのIPアドレスを指定します。指定する値はDHCPサーバ機能により広報されます。省略、または0.0.0.0を指定する場合は、広報を行いません。

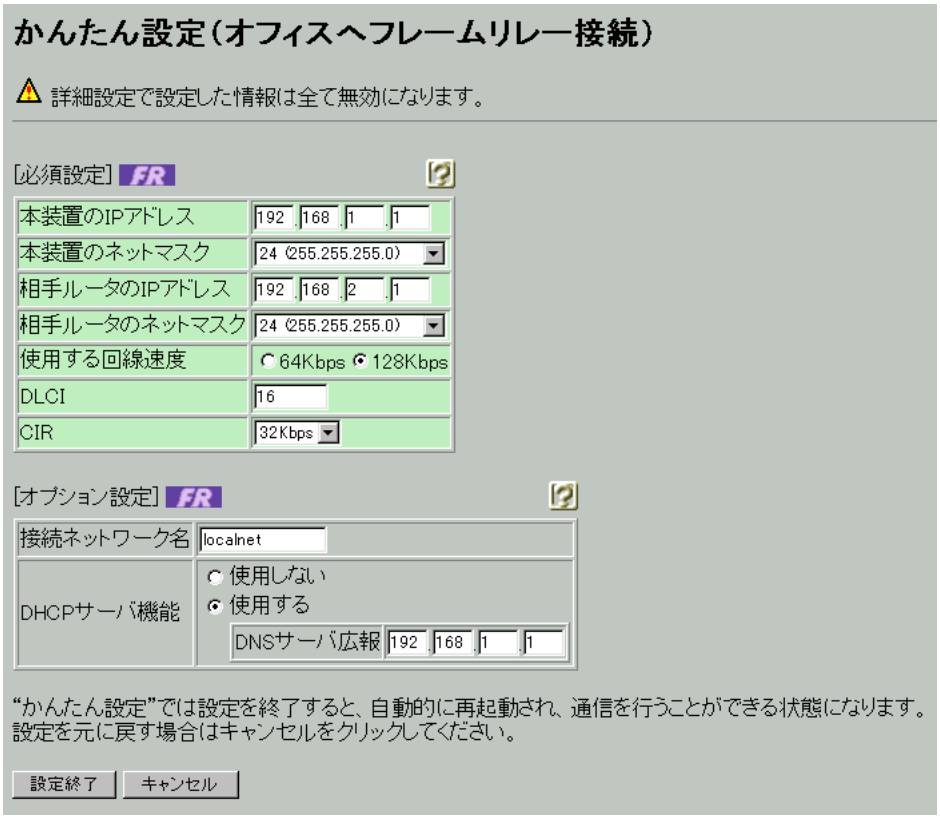
ヘッダ圧縮

送受信するヘッダを圧縮します。ヘッダ圧縮のアルゴリズムは、VJヘッダ圧縮（RFC1144に準拠）およびIPヘッダ圧縮（RFC2507／RFC2508に準拠）をサポートします。使用する指定の場合も、実際にヘッダ圧縮を行うかどうかは、相手ホストとのネゴシエーションで決まります。

データ圧縮

送受信するデータを圧縮します。データ圧縮のアルゴリズムは、LZSをサポートします。使用する指定の場合も、実際にデータ圧縮を行うかどうかは、相手ホストとのネゴシエーションで決まります。

かんたん設定（オフィスへフレームリレー接続）



[必須設定]

本装置のIPアドレス／ネットマスク

本装置のIPアドレスとネットマスクを指定します。0.0.0.0を指定すると通信ができなくなります。

相手ルータのIPアドレス／ネットマスク

相手ルータのIPアドレスとネットマスクを指定します。本装置は、この指定で得られるネットワークに対してスタティックルートを指定します。

使用する回線速度

使用する回線速度を選択します。

DLCI

DLCIを16～991の範囲で指定します。DLCIを指定できるネットワークは32個までです。DLCIはフレームリレーを使用するときに、一本の物理回線上に設定される複数の論理的な通信路（データリンク）を識別する識別子です。

CIR

CIRを指定します。CIRは網が正常な状態で保証されるスループットです。本装置が輻輳制御動作を行う場合は、CIRを基準としてスループットを制御します。

[オプション設定]

接続ネットワーク名

ネットワークを識別する名称を半角英数字8文字以内で指定します。

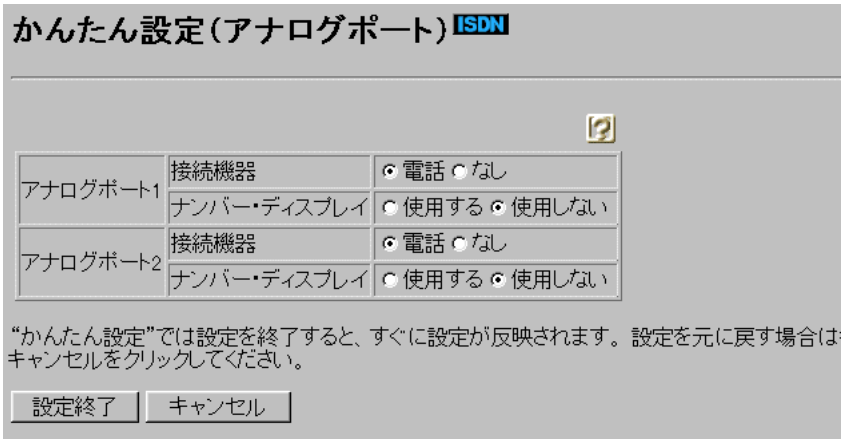
DHCPサーバ機能

DHCPサーバ機能を使用するかどうかを指定します。

DNSサーバ広報

必要に応じて接続先、またはネットワーク管理者に指示されたDNSサーバのIPアドレスを指定します。指定する値はDHCPサーバ機能により広報されます。省略するか、0.0.0.0を指定した場合は、広報を行いません。

かんたん設定（アナログポート）



接続機器

アナログポートに電話を接続するかどうかを指定します。

ナンバー・ディスプレイ

ナンバー・ディスプレイ対応機器を使用するかどうかを指定します。

「詳細設定」で設定する

「かんたん設定」の場合とは異なり、「詳細設定」では設定項目を個別に設定し、各項目を組み合わせて通信できる状態にします。詳細設定メニューでは、「ルータ設定」および「アナログ設定」の設定ができます。

こんな事に気をつけて

- **「詳細設定」だけで設定する場合、「回線情報」「LAN 情報」「相手情報」は必ず設定します。**
- **「詳細設定」で設定したあとで「かんたん設定」を行うと、「詳細設定」で設定した内容が無効になります。ただし、パスワード情報、アナログ情報、ファームウェア更新情報は有効です。**

「詳細設定」で設定する場合は、更新する内容により、再起動が必要となる場合があります。

ただし、複数のページで設定が必要な場合、それぞれのページで設定した情報を［更新］ボタンをクリックして更新しておき、最後に［再起動］ボタン、または［設定反映］ボタンをクリックすると設定したすべての内容が有効になります。

再起動が必要な場合は、［再起動］ボタンが表示され、再起動なしに設定情報を反映できる場合は、［設定反映］ボタンが表示されます。

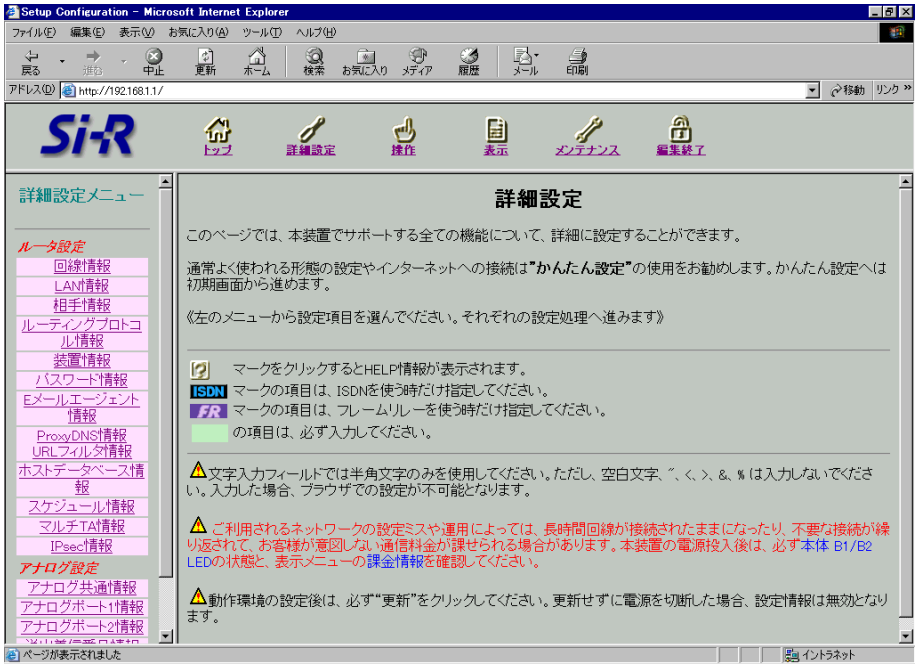
どちらのボタンが必要かについては、更新情報により、ブラウザ画面に必要なボタンが表示されますので、メッセージに従って処理を進めます。

なお、クリックするボタンにより、本装置は以下のように動作します。

- ［再起動］ボタン　：通話中やデータ通信中の場合、通話およびデータ通信は切断されます。
- ［設定反映］ボタン　：通話中やデータ通信中の場合、通話は切断されません。データ通信は切断されます。ただし、マルチ TA 機能を利用したデータ通信は切断されません。

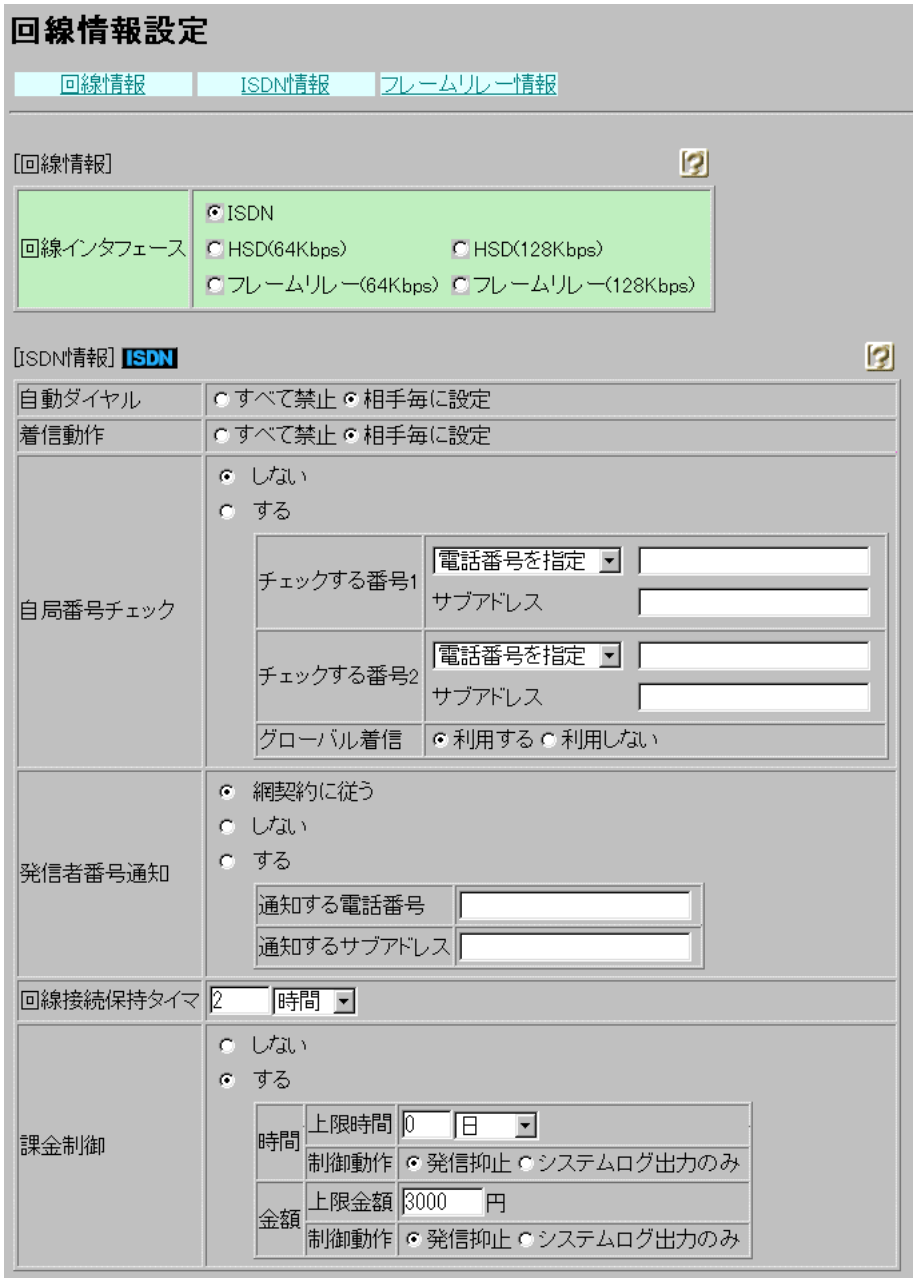
■ 詳細設定メニューを表示する

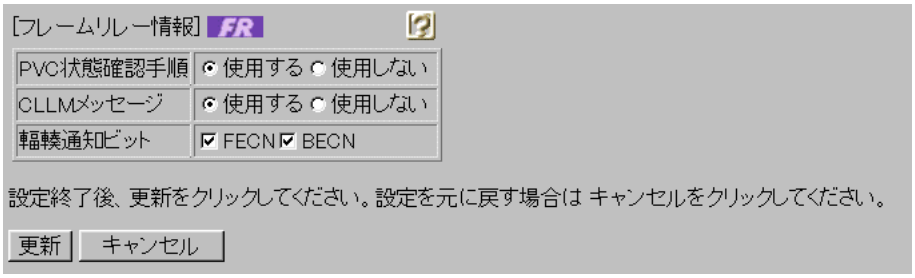
本装置のトップページで画面上部の［詳細設定］アイコンをクリックすると、詳細設定メニューが表示されます。



回線情報設定

【操作】「詳細設定メニュー」→ルータ設定「回線情報」





[回線情報]

使用する回線の種類を設定します。

回線インタフェース

以下の5つから使用する回線を選択します。

ISDN

INSネット64などのISDN接続の場合に選択します。

HSD（64Kbps）

ハイ・スーパー・ディジタル（HSD）やDA64などの専用線の場合に選択します。

HSD（128Kbps）

ハイ・スーパー・ディジタル（HSD）やDA128などの専用線の場合に選択します。

フレームリレー（64Kbps）

64Kbpsのアクセス回線でフレームリレーを使用する場合に選択します。

フレームリレー（128Kbps）

128Kbpsのアクセス回線でフレームリレーを使用する場合に選択します。

[ISDN情報]

ISDNを選択する場合だけ、以下の項目を設定します。

自動ダイヤル

データ通信が発生したときに自動的にダイヤルするかどうかを選択します。本装置からの自動ダイヤルを禁止するときに“すべて禁止”を選択します。いかなる通信データ発生時にも自動的にダイヤルしません。“相手毎に設定”を選択した場合は、相手情報のネットワーク情報設定で対象を設定します。

着信動作

外から本装置に着信を要求してきたときの動作を選択します。着信を装置全体として禁止するときは“すべて禁止”を選択します。データ通信の着信をすべて拒否し、発信専用となります。“相手毎に設定”を選択した場合は、相手情報のネットワーク情報の接続先情報設定で設定します。

自局番号チェック

ダイヤルイン番号やｉ・ナンバー、サブアドレスを利用して着信機器を識別するかどうかを選択します。識別する場合は、“する”を選択します。チェックする番号は2つまで指定でき、以下の中から選択します。

・電話番号を指定

・i・ナンバー情報1（契約者回線番号）

・i・ナンバー情報2（追加の番号）

・i・ナンバー情報3（追加の番号）

“電話番号を指定”を選択する場合、右の記入欄に電話番号を32桁以内で指定します。

また、どれを選択する場合もサブアドレスを19桁以内で指定します。

“電話番号を指定”を選択し、右の記入欄に電話番号を記述しないで、サブアドレスだけを指定する場合、電話番号は任意となります。

グローバル着信を行う場合は、“利用する”を選択します。

☛ 参照 「ダイヤルイン／グローバル着信機能を使う」（P.397）

発信者番号通知

発信者番号通知の内容を変更する場合に設定します。通常は“網契約に従う”の状態で問題ありません。この場合、回線の加入契約で選択した内容の設定になります。“する”を選択する場合は、通知する電話番号とサブアドレスを指定します。電話番号を32桁以内、サブアドレスを19桁以内で指定します。なお、PIAFS（64Kbps）発信時には、指定したサブアドレスは無視され、相手に通知されません。

回線接続保持タイマ

回線接続保持タイマは、操作メニューでテレホーダイ開始をクリックと有効になります。無通信監視タイマによる切断を無効とする時間を0～24時間の範囲で指定します。通信時間監視タイマを指定した時刻から指定時間が経過するまでの間、無通信状態が続いても、無通信監視タイマによる切断は行れません。

課金制御

通信総時間と課金合計金額による自動発信制限を行うかどうかを選択します。“する”を選択した場合は、時間による制御と課金による制御が行え、両方を同時に使うこともできます。上限時間は0～999時間、上限金額は0～999999円の範囲で指定します。なお、0、または空白を指定する場合は、その機能は無効となります。

[フレームリレー情報]

フレームリレーを選択する場合だけ、以下の項目を設定します。

PVC状態確認手順

PVC状態確認手順を使用するかどうかを選択します。PVC状態確認手順には以下の機能があります。

・ユーザー網間のリンクの正常性を確認する機能

・ユーザーユーザ間のPVC状態を通知する機能

こんな事に気をつけて

- **この機能を使用する場合は、通信事業者と契約する必要があります。**
- **PVC状態確認手順の双方向手順はサポートしておりません。**

CLLMメッセージ

CLLMメッセージ受信時に輻輳制御を行うかどうかを選択します。CLLMメッセージとは網が網状態（輻輳、故障）を通知するメッセージです。本装置はこの通知内容に合わせて動作します。

こんな事に気をつけて

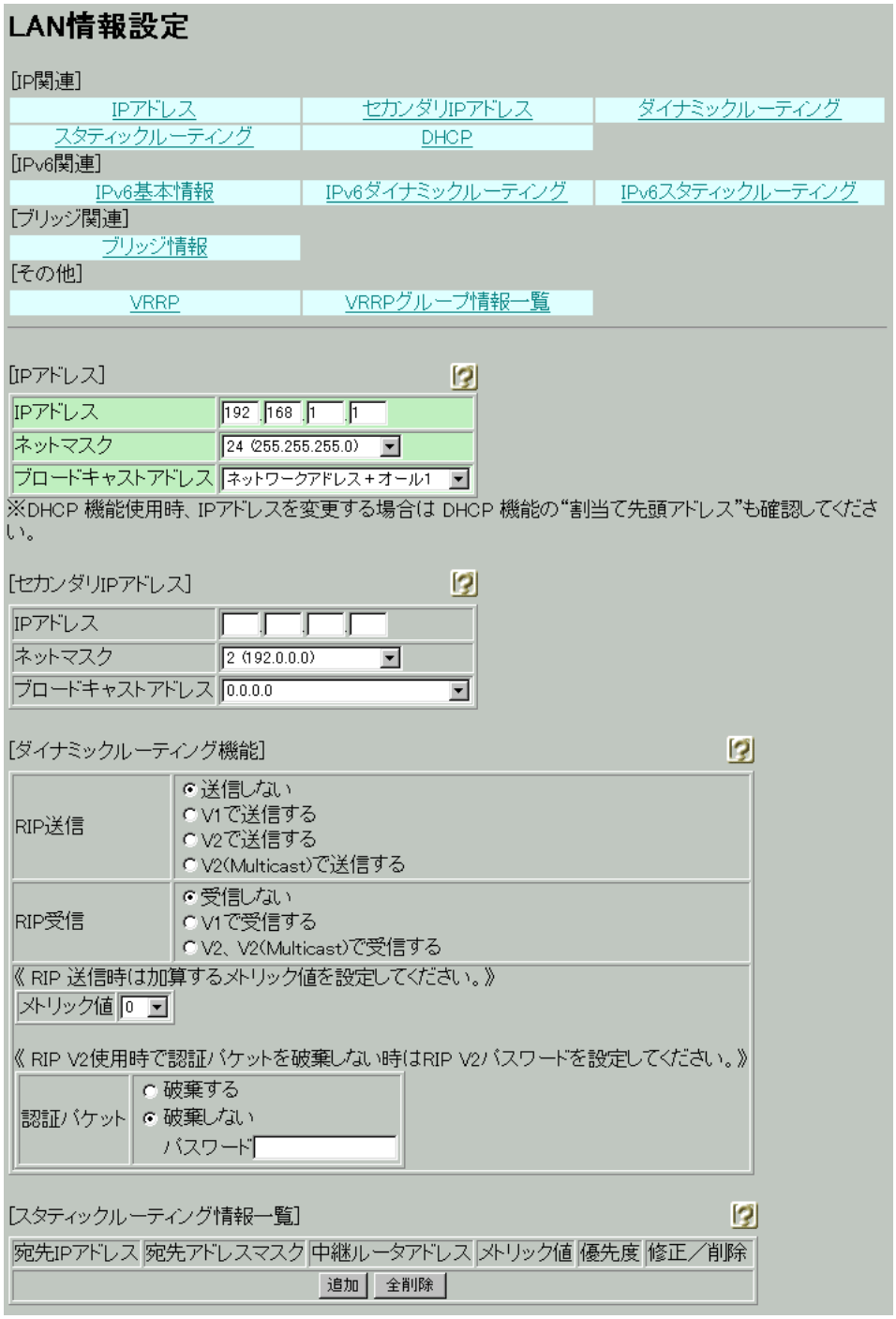
この機能を使用する場合は、通信事業者と契約する必要があります。

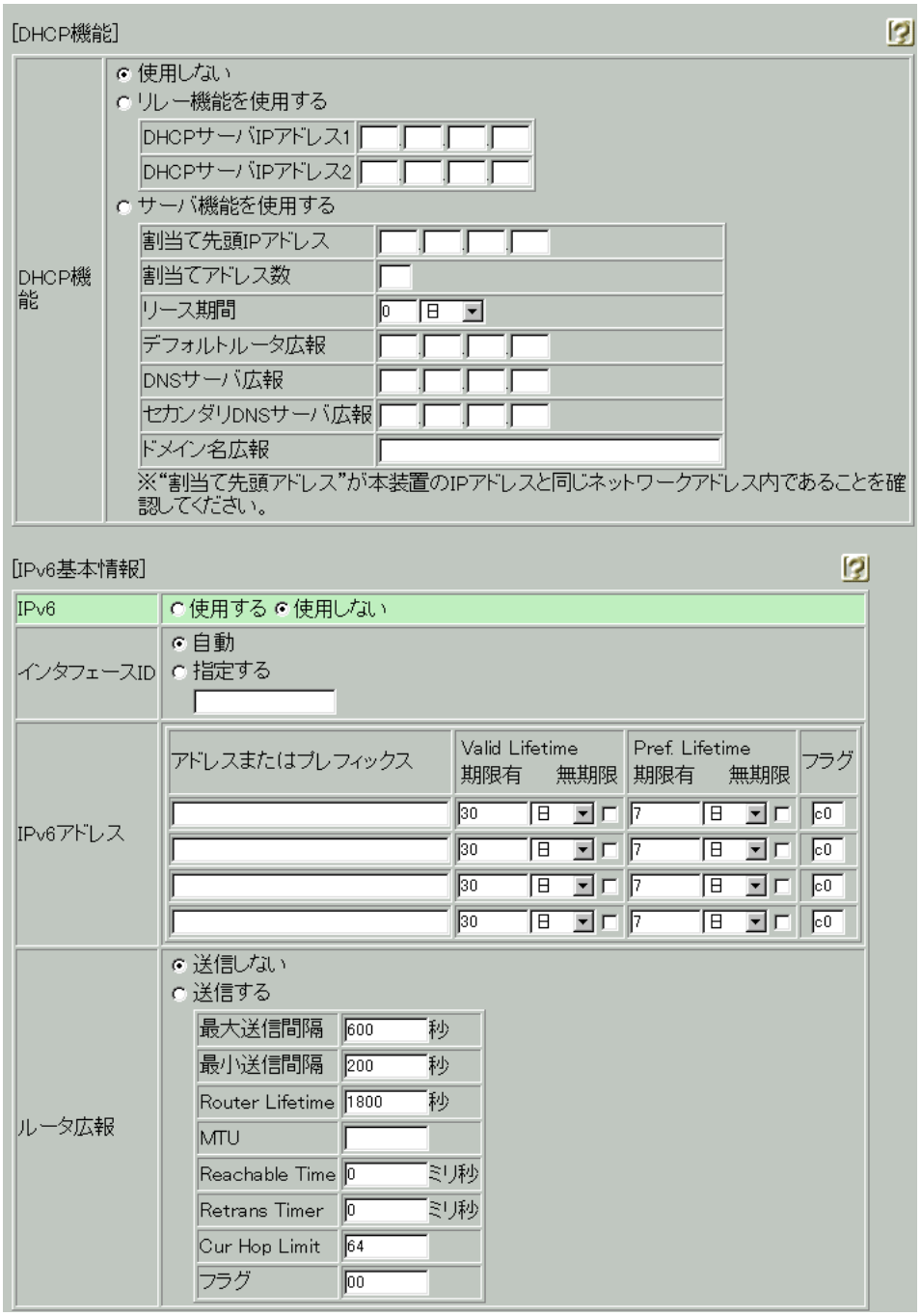
輻輳通知ビット

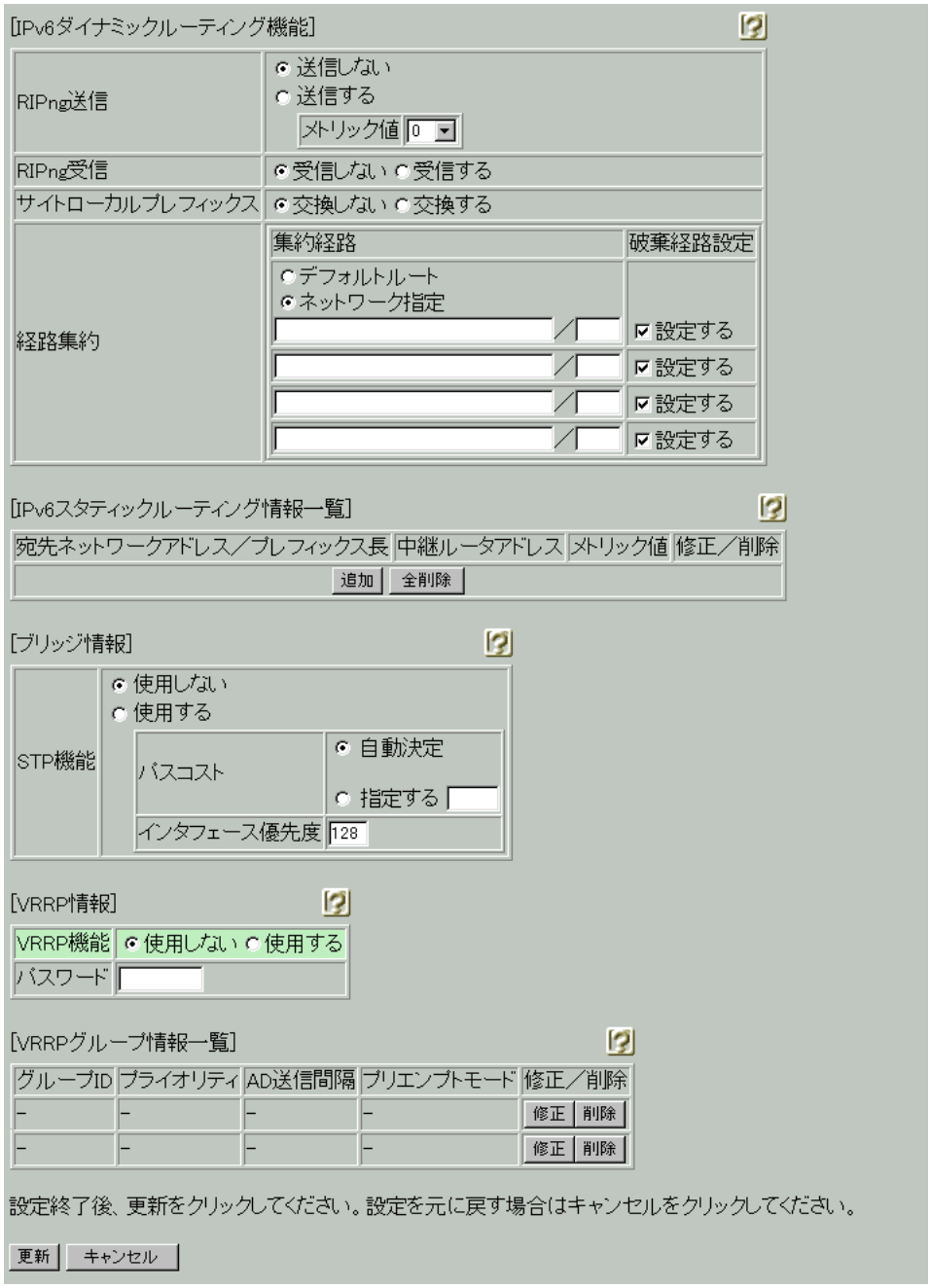
輻輳制御に利用するビットを指定します。指定したビットがセットされたパケットを受信した場合、本装置は網を正常な状態に戻すためにパケットの送信を抑制します。

LAN情報設定

【操作】「詳細設定メニュー」→ルータ設定「LAN情報」




[DHCP機能]
DHCP機能
使用しない
リレー機能を使用する
DHCPサーバIPアドレス1
DHCPサーバIPアドレス2
サーバ機能を使用する
割当て先頭IPアドレス
割当てアドレス数
リース期間
0
日
デフォルトルータ広報
DNSサーバ広報
セカンダリDNSサーバ広報
ドメイン名広報
※“割当て先頭アドレス”が本装置のIPアドレスと同じネットワークアドレス内であることを確認してください。
[IPv6基本情報]
IPv6
使用する
使用しない
インタフェースID
自動
指定する
IPv6アドレス
アドレスまたはプレフィックス
Valid Lifetime
期限有
無期限
Pref. Lifetime
期限有
無期限
フラグ
30
日
7
日
c0
ルータ広報
送信しない
送信する
最大送信間隔
600
秒
最小送信間隔
200
秒
Router Lifetime
1800
秒
MTU
Reachable Time
0
ミリ秒
Retrans Timer
0
ミリ秒
Cur Hop Limit
64
フラグ
00


[IPv6ダイナミックルーティング機能]
RIPng送信
送信しない
送信する
メトリック値 0
RIPng受信
受信しない 受信する
サイトローカルプレフィックス
交換しない 交換する
経路集約
集約経路
破棄経路設定
デフォルトルート
ネットワーク指定
設定する
[IPv6スタティックルーティング情報一覧]
宛先ネットワークアドレス／プレフィックス長
中継ルータアドレス
メトリック値
修正／削除
追加
全削除
[ブリッジ情報]
STP機能
使用しない
使用する
パスコスト
自動決定
指定する
インタフェース優先度
128
[VRRP情報]
VRRP機能
使用しない 使用する
パスワード
[VRRPグループ情報一覧]
グループID
プライオリティ
AD送信間隔
プリエンプトモード
修正／削除
修正
削除
設定終了後、更新をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
更新
キャンセル

[IPアドレス]

本装置のIPアドレスを設定します。

IPアドレス／ネットマスク

本装置のLAN側のIPアドレスとネットマスクを指定します。

こんな事に気をつけて

IPアドレスに0.0.0.0を指定すると通信ができなくなります。

ブロードキャストアドレス

本装置のLAN側のブロードキャストアドレスを以下の中から選択します。

・0.0.0.0

・255.255.255.255

・ネットワークアドレスのホスト部をオール0にしたもの

・ネットワークアドレスのホスト部をオール1にしたもの

通常は“ネットワークアドレス＋オール1”から変更する必要はありません。

[セカンダリIPアドレス]

本装置はLAN側に複数のIPアドレスを持つことができます。複数のIPアドレスを使用する場合に設定します。

こんな事に気をつけて

セカンダリIPアドレスの属するネットワークには、以下のサービスは行いません。

・RIPの送受信

・DHCP機能

[ダイナミックルーティング機能]

ダイナミックルーティングを行うためのルーティング情報を設定します。

本装置がサポートしているダイナミックルーティング機能はRIPとBGPです。RIPを使用する場合は、各インタフェース単位で設定する必要があります。BGPを使用する場合は、「ルーティングプロトコル情報設定」（P.281）を参考にしてください。

RIP送信

RIP情報を送信するかどうかを選択します。送信する設定にした場合、15～45秒ごとにRIP情報を送信します。RIP送信を行う場合は、RIPの種類を選択します。

- V1
  ルーティングプロトコルにRIP V1を使用し、ブロードキャストで送信します。

- V2
  ルーティングプロトコルにRIP V2を使用し、ブロードキャストで送信します。
- V2（Multicast）
  ルーティングプロトコルにRIP V2を使用し、マルチキャストで送信します。

RIP受信

RIP情報を受信するかどうかを選択します。RIP受信を行う場合は、RIPの種類を選択します。

- V1
  ルーティングプロトコルにRIP V1を使用し、受信します。
- V2、V2（Multicast）
  ルーティングプロトコルにRIP V2を使用し、ブロードキャストおよびマルチキャストを受信します。

メトリック値

RIP送信時に加算するメトリック値を選択します。

認証パケット

RIP V2使用時にだけ有効な設定です。RIP V2では、同一パスワードグループでだけ、RIP情報の交換を行うことができます。パスワード認証によるRIP情報の交換を行う場合は、“破棄しない”を選択し、パスワードを半角英数字16文字以内で指定します。“破棄する”を選択する場合は、パスワード認証によるRIP情報の交換は行いません。

[スタティックルーティング情報一覧]

現在LAN側に設定されているスタティックルーティング情報の一覧です。スタティックルーティングの定義は装置全体で64個まで設定できます。処理するボタンをクリックし、次のページに進みます。

ヒント

◆ダイナミックルーティングとスタティックルーティング

スタティックルーティングとは、目的とする接続先へ到達するまでのルートをあらかじめ設定しておき、常に固定的なルートを選択してデータ通信を行います。それに対して、ダイナミックルーティングはルータ間でルーティング情報をやりとりすることで、そのつどネットワークに応じて最適なルートを選択してデータ通信を行うものです。

[DHCP 機能]

DHCP 機能

本装置をLAN 側ネットワークのDHCP サーバとして使用するかどうかを選択します。使用する場合は、“サーバ機能を使用する”を選択し、以下の項目を設定します。また、ほかのネットワークに置いてあるDHCP サーバを、本装置のネットワークのDHCP サーバとして使用する場合は、“リレー機能を使用する”を選択し、利用するDHCP サーバのIPアドレスを指定します。

割当て先頭IPアドレス

DHCP サーバ機能により、割り当てる連続したアドレス群の先頭のIP アドレスを指定します。

割当てアドレス数

DHCP サーバ機能で割り当てるアドレス数を1 ～64 の範囲で指定します。

こんな事に気をつけて

ホストデータベース機能を使用すると特定のDHCP クライアントに対して固有のIP アドレスを割り当てることができます。この場合のIP アドレスは、割当て先頭IPアドレスと割当てアドレス数によって規定される動的割り当て範囲である必要はありません。

リース期間

DHCP サーバ機能により割り当てたIP アドレスを貸し出す期間を、1 時間以上、365 日未満の範囲で指定します。0 を指定すると無期限を意味します。

デフォルトルータ広報

DHCP サーバで広報するデフォルトルータのIP アドレスを指定します。省略、または0.0.0.0 を指定する場合は、DHCP サーバによる広報を行いません。

DNS サーバ広報

DNS サーバのIPアドレスを指定します。省略、または0.0.0.0 を指定する場合は、DHCP サーバによる広報を行いません。ProxyDNS を使用する場合は、本装置のIP アドレスを指定します。

セカンダリDNSサーバ広報

セカンダリDNS サーバのIP アドレスを指定します。省略、または0.0.0.0 を指定する場合は、DHCP サーバによる広報を行いません。

広報ドメイン名

ドメイン名を半角英数字80 文字以内で指定します。省略する場合は、DHCP サーバによる広報を行いません。

[IPv6基本情報]

IPv6

LAN上でIPv6通信を使用するかどうかを選択します。

インタフェースID

“自動”を選択する場合は、装置のMACアドレスから自動生成されるインタフェースIDを使用します。通常はこの設定を使用します。

“指定する”を選択する場合は、16ビットごとに区切り文字（:）を入れて、16桁の16進数でインタフェースIDを指定します。このとき、ほかの装置と違うインタフェースIDを指定します。

記述例）

fedc:ba98:7654:3210

IPv6アドレス

本装置のLAN側のIPv6アドレスを標準的なIPv6アドレスで指定します。本装置ではprefix lengthは64に固定されます。インタフェースID部分がすべて0の場合は、指定するアドレスはprefixとして解釈されます。実際に利用するアドレスは、そのアドレスにインタフェースIDを付与したものとなります。

記述例）

fec0::1000:200:fffc:1111:1111

完全なIPv6アドレスとして解釈されます。

fec0:0:0:1000::

prefixとして解釈され、インタフェースID部分にはインタフェースIDが付与されます。

Valid Lifetime

通常は奨励値“30日”を使用します。

有効範囲）

0 ～ 365日

0 ～ 8760時

0 ～ 525600分

0 ～ 31536000秒

期限を定めない（無期限）の場合は、チェックボックスをチェックします。

Pref. Lifetime

通常は奨励値“7日”を使用します。

有効範囲）

0 ～ 365日

0 ～ 8760時

0 ～ 525600分

0 ～ 31536000秒

期限を定めない（無期限）の場合は、チェックボックスをチェックします。

フラグ

ルータ広報のプレフィックス情報ごとに設定するフラグフィールドの内容を2桁の16進数で指定します。この領域の値として、RFC2461 で以下の値が定義されています。必要に応じて以下の値の論理和を設定してください。

・on-link flag　80

・autonomous address-configuration flag　40

特に問題がない場合は“c0”を使用します。

ルータ広報

ルータ広報メッセージ（router advertisement message）を送信する場合は“送信する”を選択し、以下の項目を設定します。

最大送信間隔

ルータ広報メッセージの最大送信間隔を指定します。

有効範囲）4 ～ 1800

最小送信間隔

ルータ広報メッセージの最小送信間隔を指定します。

有効範囲）3 ～ 最大送信間隔の3/4

Router Lifetime

ルータ広報で送信するRouter Lifetimeの内容を指定します。

有効範囲）0または最大送信間隔 ～ 9000

MTU

ルータ広報で送信するMTU optionの内容を指定します。無指定の場合にはMTU optionを含めません。

有効範囲）1280 ～ 1500

Reachable Time

ルータ広報で送信するReachable Timeの内容を指定します。

有効範囲）0 ～ 3600000

Retrans Timer

ルータ広報で送信するRetrans Timerの内容を指定します。

有効範囲）0 ～ 4294967295

Cur Hop Limit

ルータ広報で送信するCur Hop Limitの内容を指定します。

有効範囲）0 ～ 255

フラグ

ルータ広報の本体部分に設定するフラグフィールドの内容を2桁の16進数値で指定します。この領域の値として、RFC2461 で以下の値が定義されています。必要に応じて以下の値の論理和を設定してください。

・Managed address configuration flag　80

・Other stateful configuration flag　40

[IPv6ダイナミックルーティング機能]

RIPng送信

RIPng送信を行うかどうかを選択します。

メトリック値

加算するメトリック値を選択します。“RIPng送信する”を選択した場合だけ有効です。

RIPng受信

RIPng受信を行うかどうかを選択します。

サイトローカルプレフィックス

サイトローカルプレフィックスを交換するかどうかを選択します。

経路集約

RIPngで集約経路を送信する場合に、集約して広報する経路を設定します。

集約経路

デフォルトルートまたはネットワーク指定を選択し、集約して広報する経路を指定します。

破棄経路設定

集約経路に対する破棄経路を設定するかどうかを選択します。破棄経路を設定すると、転送先にこの経路を選択したパケットは破棄され、パケット送信元にICMPv6エラーメッセージが送信されます。

[IPv6スタティックルーティング情報一覧]

現在LAN側に設定されているIPv6のスタティックルーティング情報の一覧です。IPv6スタティックルーティングの定義は装置全体で64個まで設定できます。処理するボタンをクリックし、次のページに進みます。

[ブリッジ情報]

相手情報でSTP機能を有効に設定するネットワーク情報がない場合は、STP機能は動作しません。

STP機能

STP機能を利用して経路制御を行うかどうかを選択します。行う場合は、“使用する”を選択して、以下の項目を指定します。

パスコスト

STPで利用するパスコストを選択します。“指定する”を選択する場合は、1～65535の範囲で指定します。パスコストの適性値が不明な場合は、“自動決定”を選択すると、自動的にパスコストが決定されます。

インタフェース優先度

STPで使用するインタフェースごとの優先度を0～255の範囲で指定します。値が小さい方が優先となります。

[VRRP情報]

VRRP機能

VRRPを使用するかどうかを選択します。VRRPを使用するとルータの冗長構成を組むことができます。VRRPを使用しない場合は、以下の設定は無効です。

パスワード

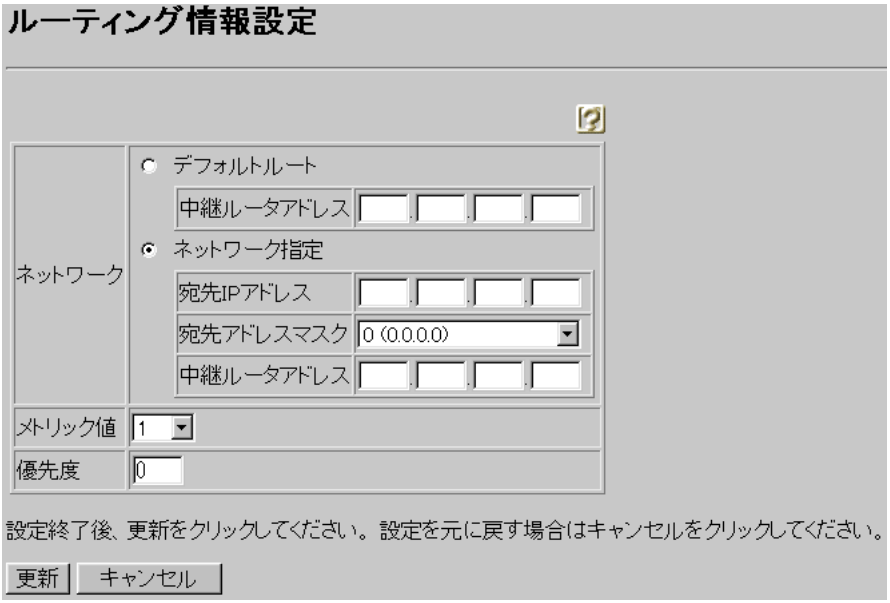
マスタから送信されるAdvertisementパケットに、認証情報を含める場合に設定します。インタフェースから送信される、すべてのAdvertisementパケットに適用します。

[VRRPグループ情報一覧]

現在このインタフェースに設定されているVRRPグループ情報の一覧です。VRRPグループは、インタフェースに2個まで設定できます。処理するボタンをクリックし、次のページに進みます。

ルーティング情報設定（LAN情報）

【操作】「詳細設定メニュー」→ルータ設定「LAN情報」→［スタティックルーティング情報一覧］



このページでは、ルーティング情報を固定で設定できます。ただし、デフォルトルート指定は装置に1つしか設定できません。

ネットワーク

デフォルトルート、またはネットワーク指定を選択し、宛先および中継先のネットワークを指定します。ネットワーク指定は、指定するネットワークを宛先に持つパケットの転送先を指定するもの、デフォルトルートは、ネットワーク指定されていない宛先を持つパケットの転送先を指定するものです。

メトリック値

メトリック値を選択します。これは、ここで設定するルーティング情報をRIPで送信するときに加算されます。

優先度

ここで設定したルーティング情報の優先度を0～254の範囲で指定します。省略時は0が設定されます。優先度は小さい値がより高い優先度を示します。指定した優先度はルーティングプロトコルの経路情報の優先度と比較され、優先度の高い経路が使用されます。

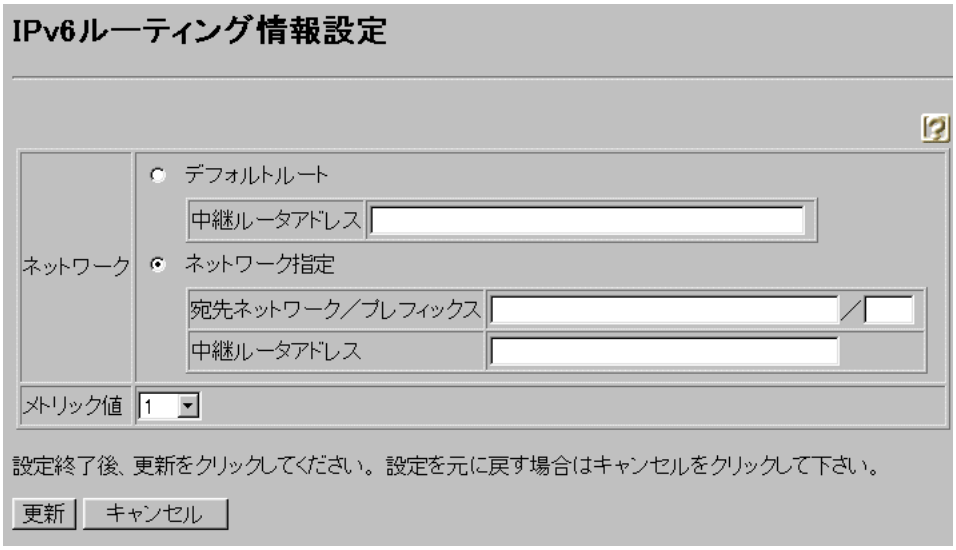
ルーティングプロトコルの優先度のデフォルトは以下のとおりです。ルーティングプロトコルに設定されている優先度と同じ値は設定しないでください。

BGP：20

RIP：120

IPv6ルーティング情報設定（LAN情報）

【操作】「詳細設定メニュー」→ルータ設定「LAN情報」→［IPv6スタティックルーティング情報一覧］



このページでは、IPv6ルーティング情報を固定で設定できます。ただし、デフォルトルート指定は装置に1つしか設定できません。

ネットワーク

デフォルトルートまたはネットワーク指定を選択し、宛先および中継先のネットワークを指定します。ネットワーク指定は、指定するネットワークを宛先に持つパケットの転送先を指定するもの、デフォルトルートは、ネットワーク指定されていない宛先を持つパケットの転送先を指定するものです。

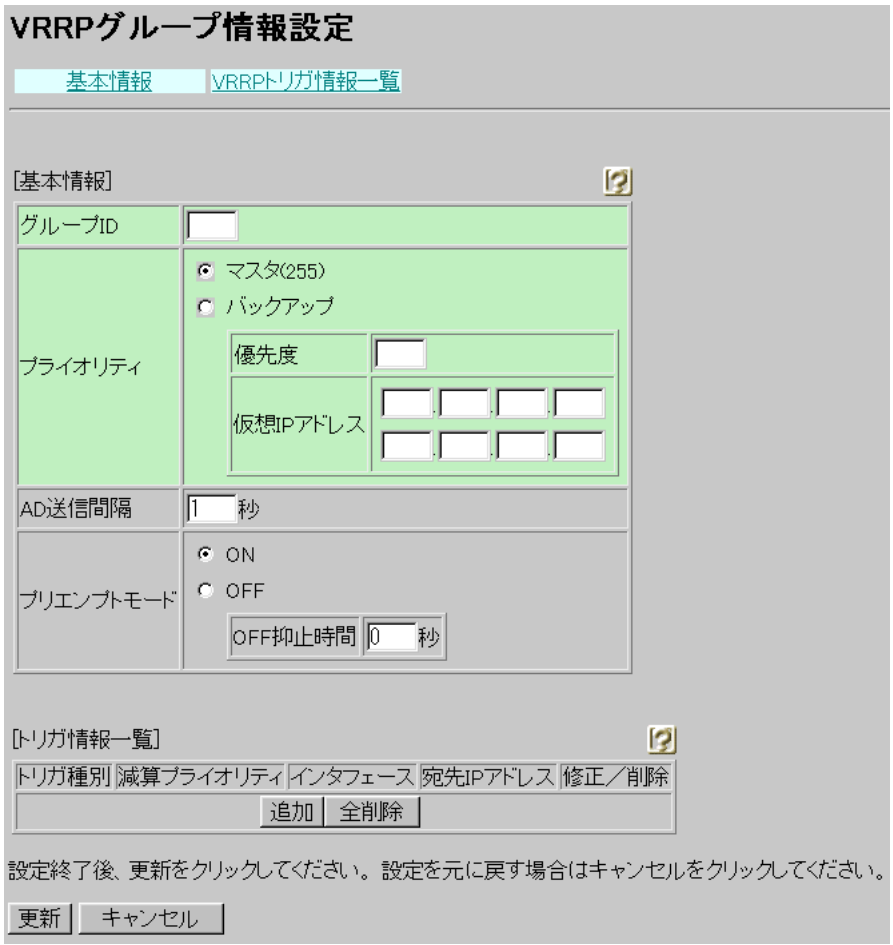
なお、ICMPv6 Redirectを正常に動作させるために、中継ルータアドレスはリンクローカルアドレスで設定する必要があります。

メトリック値

メトリック値を選択します。これは、ここで設定するルーティング情報をRIPngで送信するときに加算されます。

VRRPグループ情報設定

【操作】「詳細設定メニュー」→ルータ設定「LAN情報」→［VRRPグループ情報一覧］



設定するVRRPグループのメンバとして動作します。

[基本情報]

グループID

VRRPグループのグループIDを1～255の範囲で指定します。VRRPグループは、指定したグループIDで識別（グループ化）されます。グループIDは、装置内で重複しないように指定してください。

プライオリティ

マスタまたはバックアップを選択します。“マスタ”を選択した場合は、プライオリティが255のVRRPグループメンバとして動作します。また、仮想IPは、このインタフェースのIPアドレスとなります。“バックアップ”を選択した場合は、以下の項目を指定します。VRRPグループ内で、プライオリティが1番高いVRRPグループメンバがマスタとなります。プライオリティは、数値が大きいほど高くなります。プライオリティは、なるべくVRRPグループ内で差をつけてください。トリガを使用する場合は、プライオリティに1を指定しないでください。また、トリガを使用する場合は、“バックアップ”を選択してください。“マスタ”を選択すると、該当グループがバックアップ状態となった場合にVRRPを設定したLANが通信できなくなります。グループ内でもっとも優先度が高いグループがマスタになります。

優先度

プライオリティを1～254の範囲で指定します。

仮想IPアドレス

VRRPグループ内では、同じ仮想IPアドレスを指定します。VRRPグループ内にマスタを設定されたVRRPグループメンバが存在する場合は、その設定されたインタフェースのIPアドレスを指定します。自装置のインタフェースに設定されたIPアドレスを指定しないでください。

AD送信間隔

マスタが送信するAdvertisementパケットの送信間隔を1～254（秒）の範囲で指定します。VRRPグループ内では同じ値を使用してください。本装置とVRRPを構成する他装置にも同じ値を指定してください。省略した場合は、1秒に設定されます。

プリエンプトモード

通常は“ON”を選択することをお勧めします。

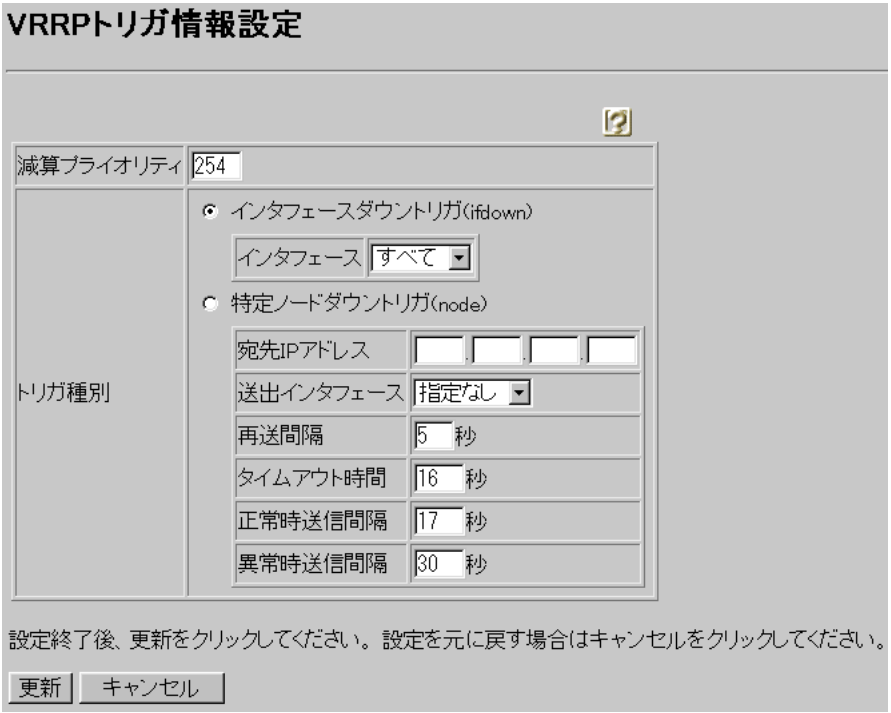
“OFF”を選択した場合、自装置VRRPグループメンバの優先度が高くても、マスタである他装置のVRRPグループメンバがすでに存在すると、マスタになることはできません。“OFF”の選択は、ネットワークの状態が不安定で、マスタの交替が頻繁に発生する場合に有効です。OFF抑止時間（秒）は、システムの立ち上がりからプリエンプトモードOFF状態を抑止する時間です。マスタより先にバックアップのシステムが立ち上がり、本来マスタになるべきVRRPグループに制御が移らないのを防ぎます。0～900（秒）の範囲で指定します。省略した場合は、0秒に設定されます。

[トリガ情報一覧]

現在このVRRPグループメンバに設定されているトリガ情報の一覧です。VRRPトリガの定義は装置全体で50個まで設定できます。処理するボタンをクリックし、次のページに進みます。

VRRP トリガ情報設定

【操作】「詳細設定メニュー」→ルータ設定「LAN 情報」→［VRRP グループ情報一覧］→［トリガ情報一覧］



設定した条件が発生した場合に、該当する VRRP グループメンバの優先度を下げます。条件に当てはまるすべてのトリガが適用されます。このインタフェースに異常が発生しない限り、減算されるプライオリティの最大は 1 です。

減算プライオリティ

設定した条件が発生した場合、「VRRP グループ情報設定」で設定したプライオリティを減算する値を 1 ～ 254 の範囲で指定します（プライオリティ 1 より低い値までは減算されません）。省略した場合は、254 秒に設定されます。

トリガ種別

トリガとなる種別を選択します。

インタフェースダウントリガ（ifdown）

指定されたインタフェースがダウンした場合にトリガを適用します。有効ではないインタフェースは動作上、無視されます。

インタフェース

トリガの対象となるインタフェースを選択します。“すべて”を選択した場合は、有効なすべてのインタフェースが対象です。

特定ノードダウントリガ（node）

設定したノードに対してICMP ECHOパケットを送信します。応答がタイムアウトした場合にトリガを適用します。ICMP ECHOパケットの送信元IPアドレスは、VRRPが設定されたLANインタフェースのIPアドレスとなります。応答を受診するための経路情報が正しくない場合は、不当に異常を検出することがあります。

宛先IPアドレス

ICMP ECHOパケットの送出先IPアドレスを指定します。

送出インタフェース

ICMP ECHOパケットを送出するインタフェースを指定します。“指定なし”の場合は送出時の経路情報によって決定されます。

再送間隔

ICMP ECHOパケットの応答が受信されない場合に、再送する時間を1～60（秒）の範囲で指定します。送信から指定した再送間隔まで応答がない場合に、ICMP ECHOパケットを再送します。省略した場合は、5秒に設定されます。

タイムアウト時間

ICMP ECHOパケットの再送を繰り返しても応答が受信されず、タイムアウトするまでの時間を、［再送間隔+1］～240（秒）の範囲で指定します。タイムアウトによって、トリガが適用されます。省略した場合は、再送間隔×3+1秒に設定されます。

正常時送信間隔

ICMP ECHOパケットの応答が正常に受信されている状態で、次にICMP ECHOパケットを送信する時間を、［タイムアウト時間+1］～255（秒）の範囲で指定します。正常に受信されている状態での周期送信間隔です。省略した場合は、タイムアウト時間+1秒に設定されます。

異常時送信間隔

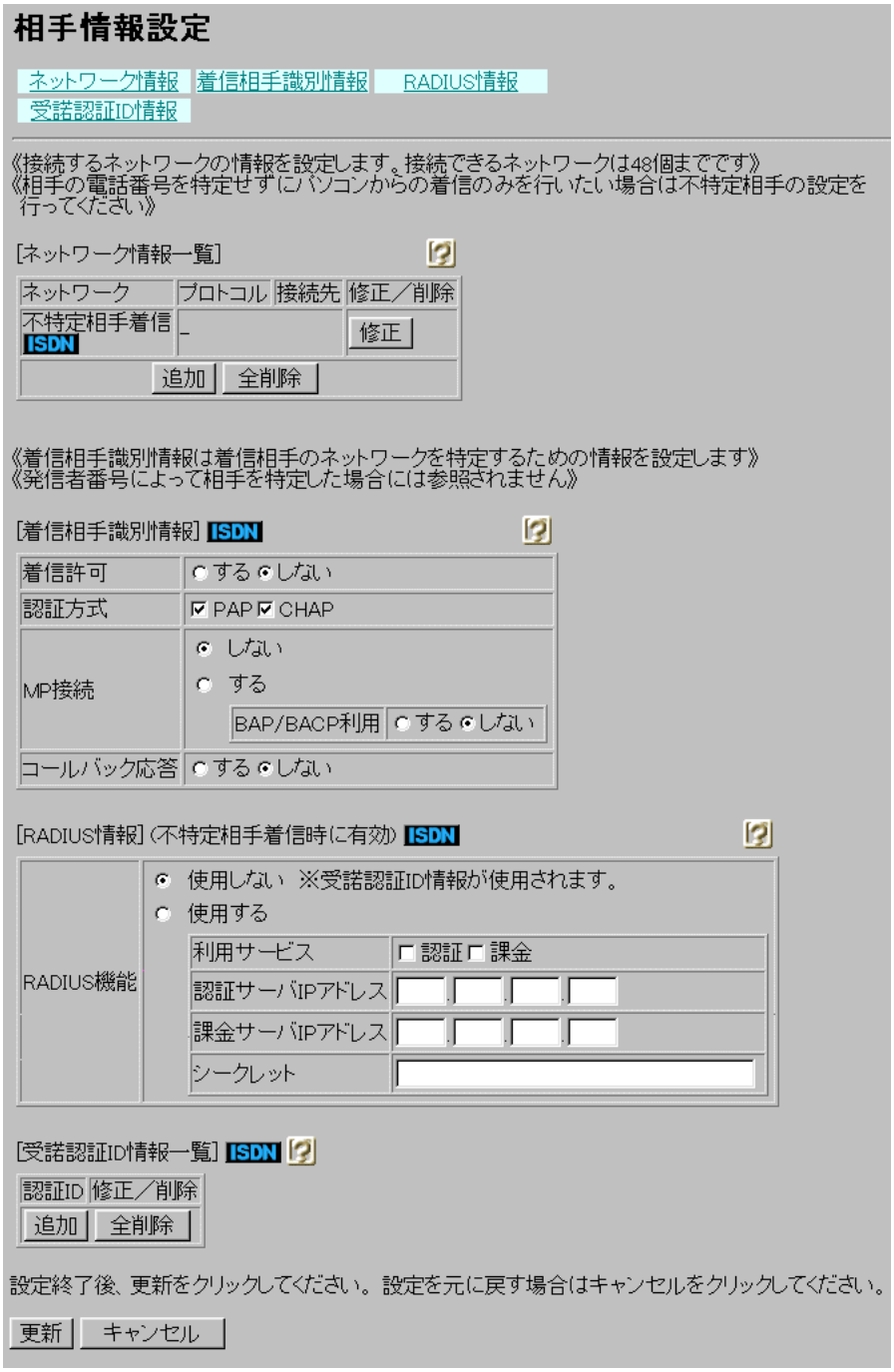
ICMP ECHOパケットのタイムアウトが発生してから応答が受信されるまでの、周期送信する間隔を1～255（秒）の範囲で指定します。応答が受信された場合は、トリガを適用せずに正常状態に戻ります。省略した場合は、30秒に設定されます。

こんな事に気をつけて

特定ノードダウントリガ機能を使用する場合は、本装置から宛先IPアドレスに対してICMP ECHOパケットを定期的に送出します。そのため、定額制でない回線を使用している場合は、超過課金の原因となることがあります。このような環境では、特定ノードダウントリガ機能を使用しないでください。

相手情報設定

【操作】「詳細設定メニュー」→ルータ設定「相手情報」



[ネットワーク情報一覧]

接続相手のネットワーク情報の一覧です。ネットワークの定義は48個まで設定できます。処理するボタンをクリックし、次のページに進みます。

「不特定相手着信」欄の［修正］ボタンをクリックすると、「不特定相手情報設定」ページに進みます。

[着信相手識別情報]

発信者番号で識別されない相手から着信がある場合に利用する情報です。

着信許可

発信者番号で識別されない相手からの着信を許可するかどうかを選択します。

認証方式

着信時に利用する認証プロトコルを選択します。どちらのプロトコルも選択しない場合は、認証を行いません。

MP接続

着信時にMP接続を受け付けるかどうかを選択します。“する”を選択する場合は、BAP／BACPの利用可否も選択します。

コールバック応答

着信時にコールバック応答を行うかどうかを選択します。

[RADIUS情報]

RADIUS情報

不特定相手着信の場合だけRADIUSクライアント機能を使用できます。RADIUSサーバに認証を問い合わせたり、課金情報を通知します。“使用しない”を選択する場合は、［受諾認証ID情報一覧］で表示される情報をもとに認証を行います。“使用する”を選択する場合は、以下の項目を設定します。

利用サービス

RADIUS機能で利用するサービスを選択します。“認証”を選択するとRADIUS認証を行います。“課金”を選択するとRADIUS Accountingを行います。どちらも選択しない場合は、RADIUS機能は使用しません。

認証サーバIPアドレス

RADIUS認証サーバのIPアドレスを指定します。

課金サーバIPアドレス

RADIUS Accountingサーバの IPアドレスを指定します。RADIUS Accounting サーバと認証サーバが同じシステムの場合は、認証サーバと同じ IPアドレスを指定します。

シークレット

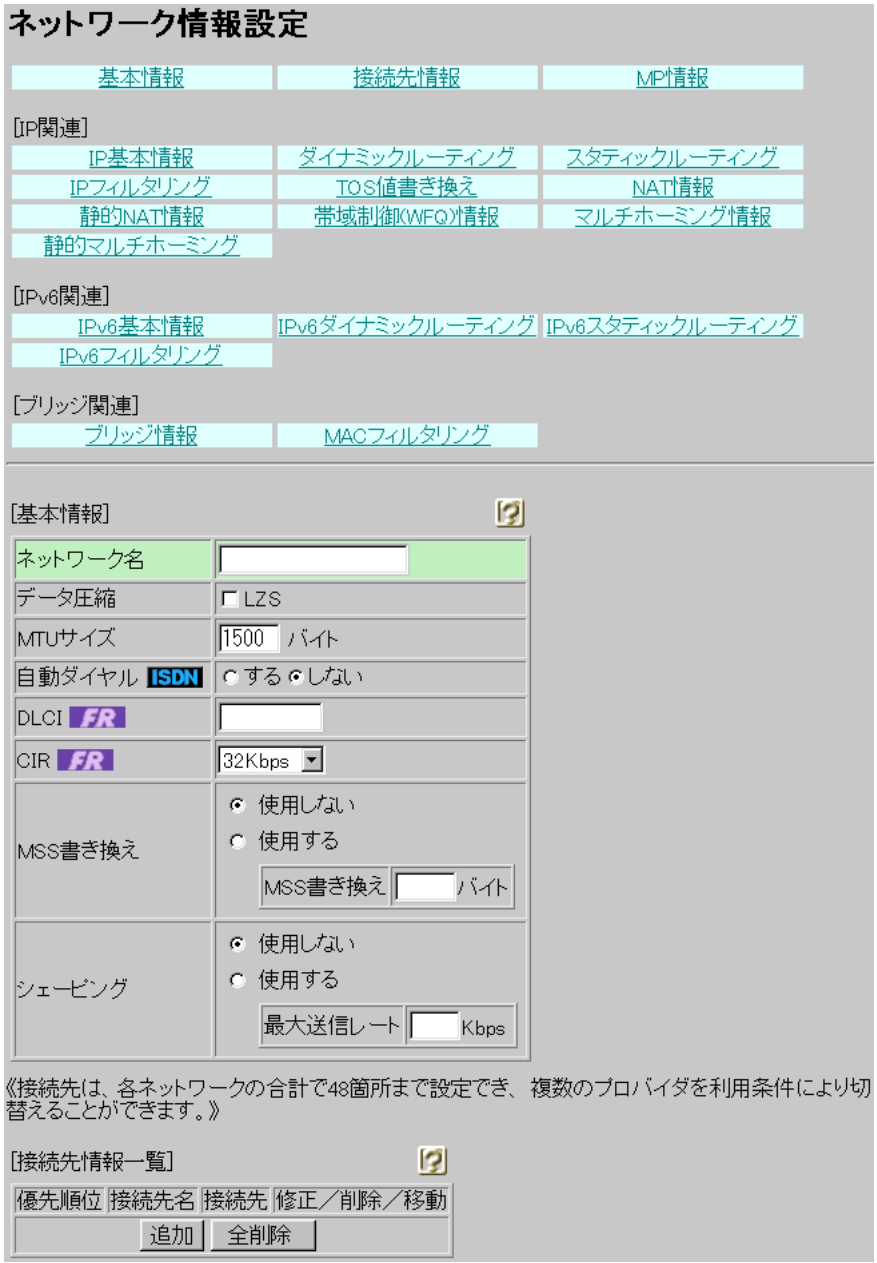
RADIUS認証／課金サーバの間で共有するシークレット文字列を半角英数字 64 文字以内で指定します。ここで指定するシークレットはサーバでも登録する必要があります。

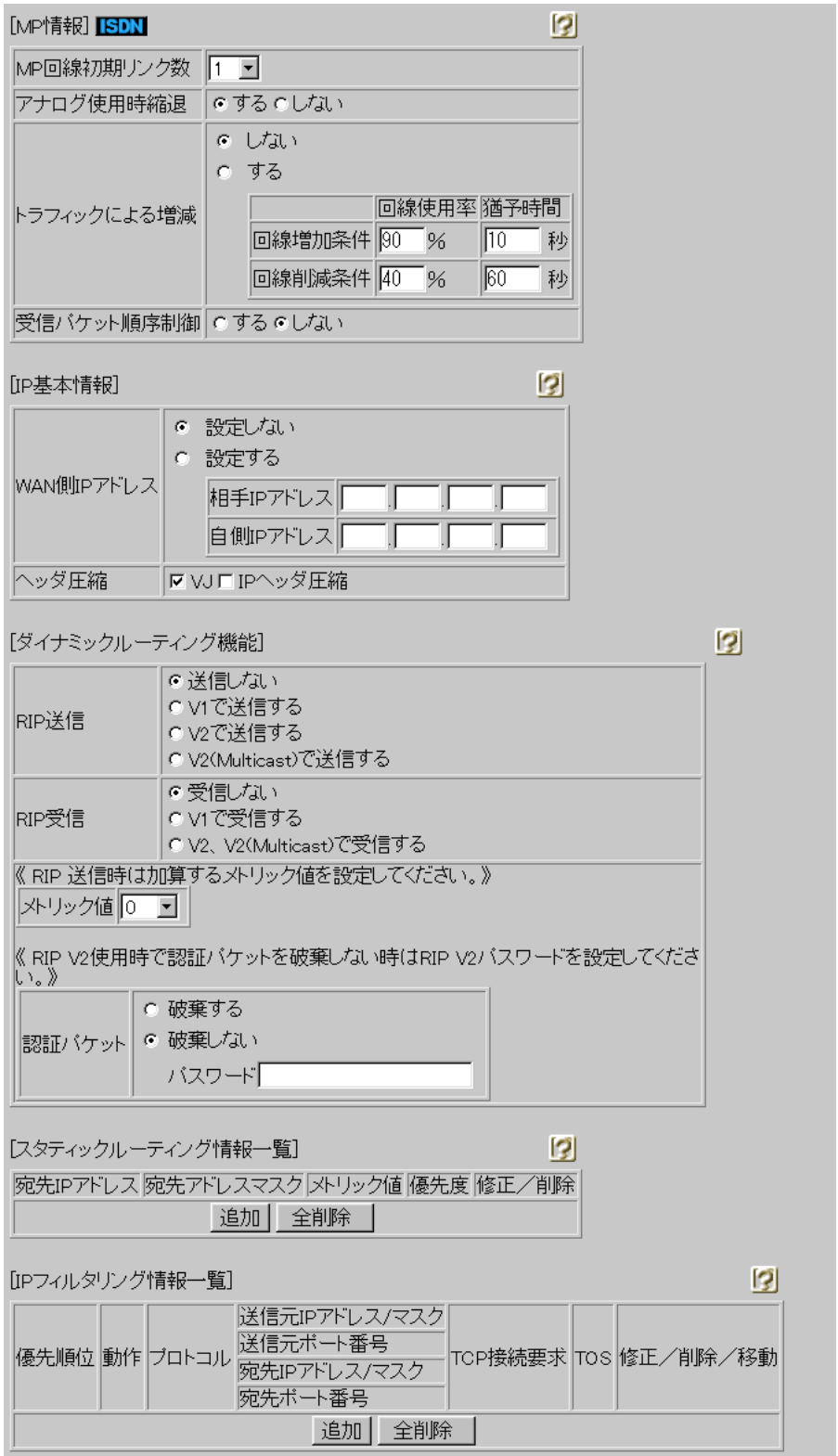
[受諾認証 ID 情報一覧]

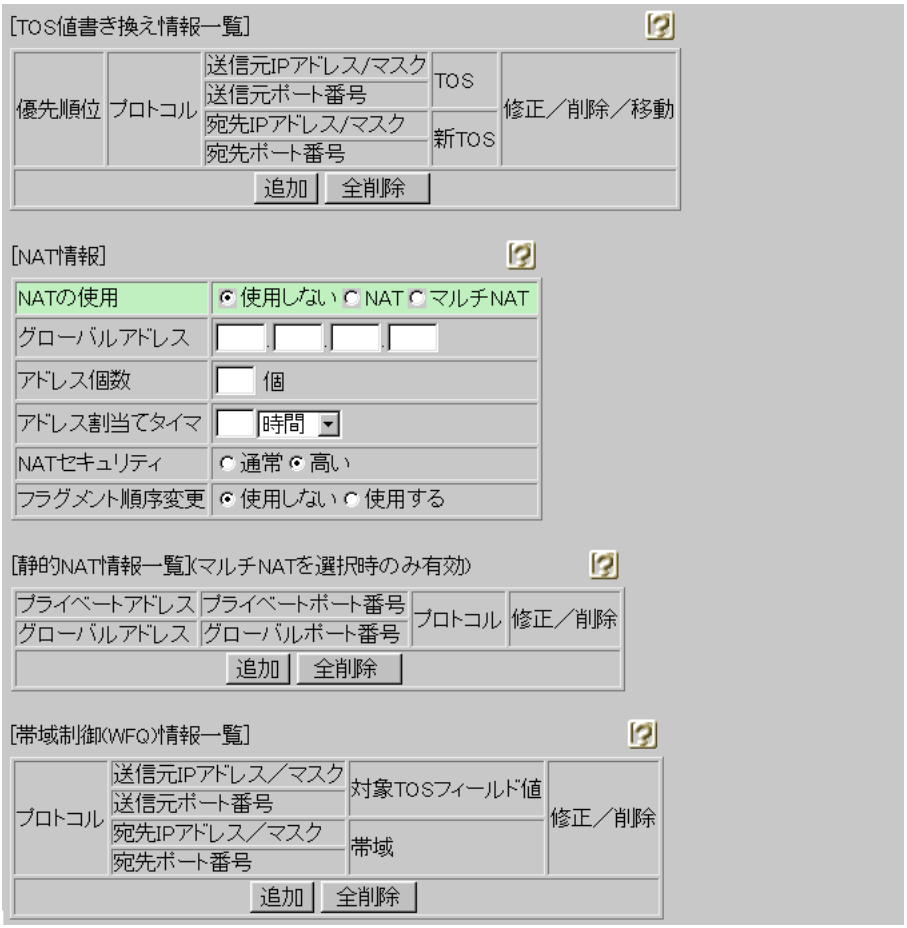
着信時に受け付ける認証 ID 情報の一覧です。64 個まで設定できます。ここにないID でも、各接続先情報の受諾認証情報に記述されている ID であれば、着信を受け付けます。処理するボタンをクリックし、次のページに進みます。

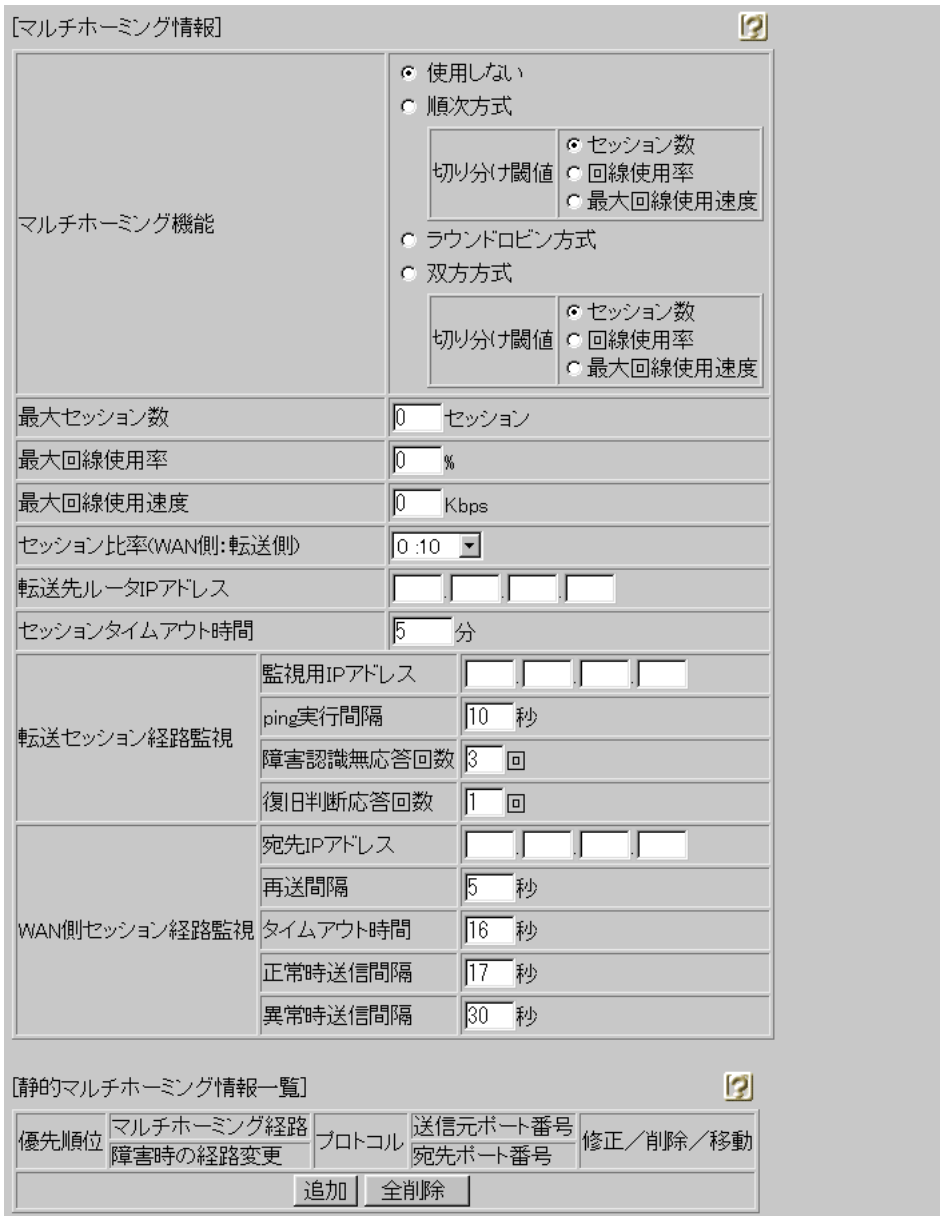
ネットワーク情報設定

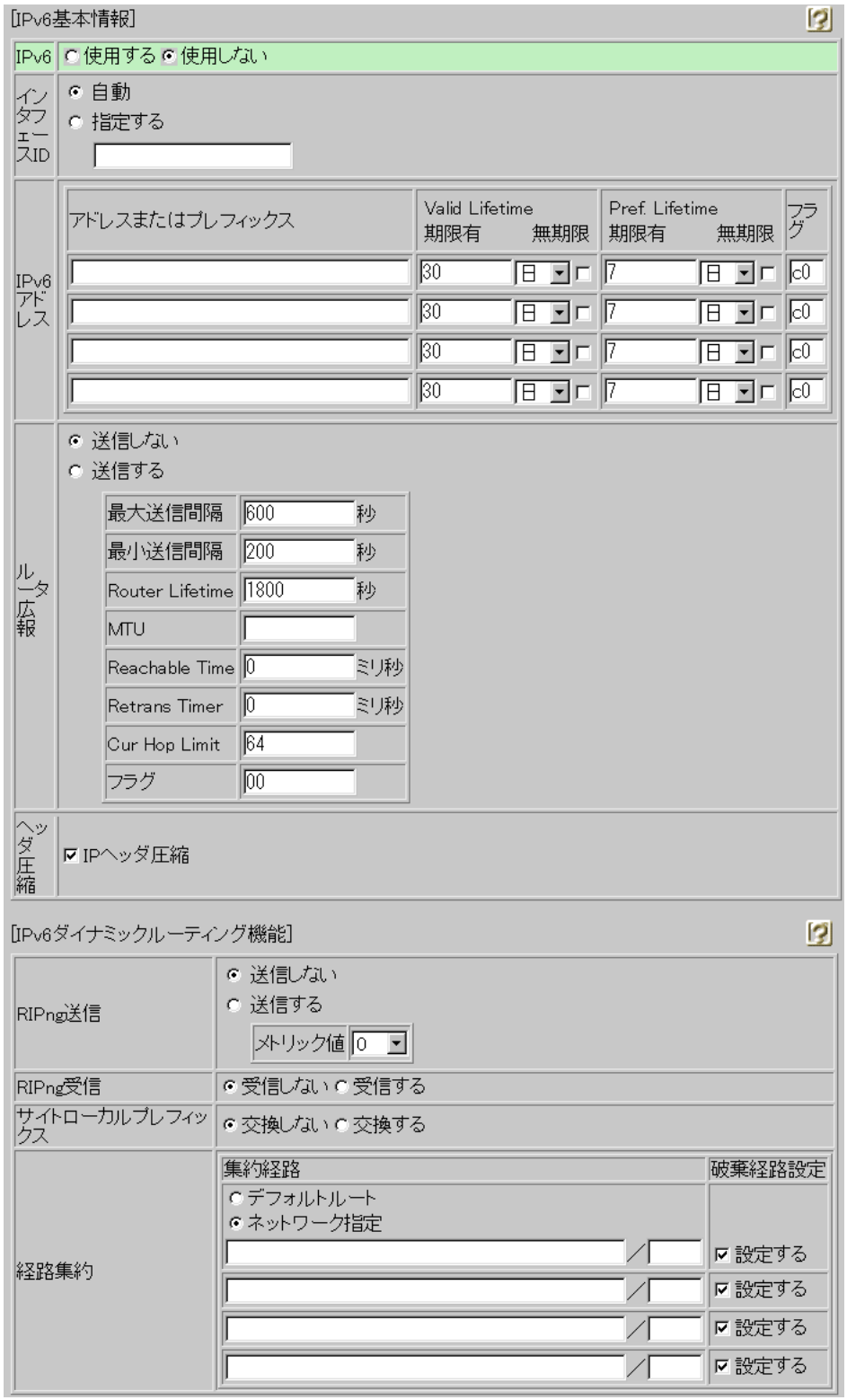
【操作】「詳細設定メニュー」→ルータ設定「相手情報」→［ネットワーク情報一覧］

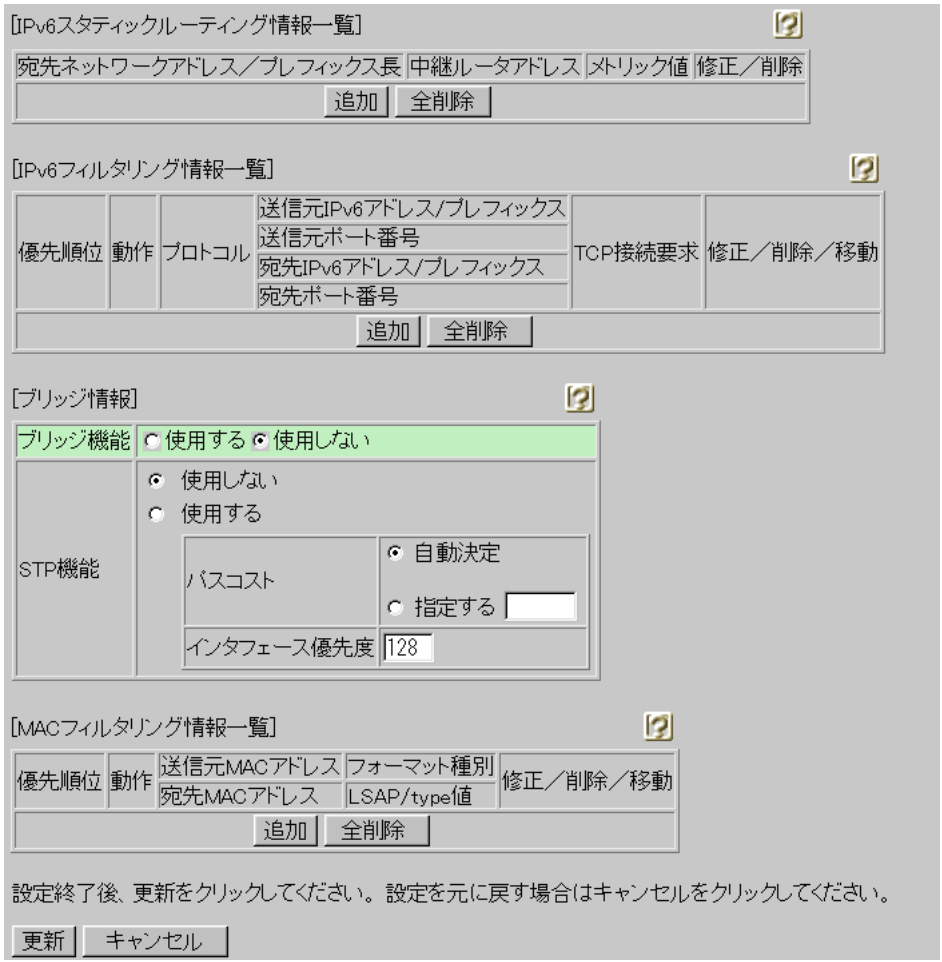



[MP情報] ISDN
MP回線初期リンク数
1
アナログ使用時縮退
する しない
トラフィックによる増減
しない
する
回線使用率
猶予時間
回線増加条件
90 %
10 秒
回線削減条件
40 %
60 秒
受信パケット順序制御
する しない
[IP基本情報]
WAN側IPアドレス
設定しない
設定する
相手IPアドレス
自側IPアドレス
ヘッダ圧縮
VJ IPヘッダ圧縮
[ダイナミックルーティング機能]
RIP送信
送信しない
V1で送信する
V2で送信する
V2(Multicast)で送信する
RIP受信
受信しない
V1で受信する
V2、V2(Multicast)で受信する
《 RIP 送信時は加算するメトリック値を設定してください。》
メトリック値
0
《 RIP V2使用時で認証パケットを破棄しない時はRIP V2パスワードを設定してください。》
認証パケット
破棄する
破棄しない
パスワード
[スタティックルーティング情報一覧]
宛先IPアドレス
宛先アドレスマスク
メトリック値
優先度
修正／削除
追加
全削除
[IPフィルタリング情報一覧]
優先順位
動作
プロトコル
送信元IPアドレス/マスク
送信元ポート番号
宛先IPアドレス/マスク
宛先ポート番号
TCP接続要求
TOS
修正／削除／移動
追加
全削除


[TOS値書き換え情報一覧]
優先順位
プロトコル
送信元IPアドレス/マスク
送信元ポート番号
宛先IPアドレス/マスク
宛先ポート番号
TOS
新TOS
修正／削除／移動
追加
全削除
[NAT情報]
NATの使用
使用しない NAT マルチNAT
グローバルアドレス
アドレス個数
個
アドレス割当てタイマ
時間
NATセキュリティ
通常 高い
フラグメント順序変更
使用しない 使用する
[静的NAT情報一覧](マルチNATを選択時のみ有効)
プライベートアドレス
グローバルアドレス
プライベートポート番号
グローバルポート番号
プロトコル
修正／削除
追加
全削除
[帯域制御(WFQ)情報一覧]
プロトコル
送信元IPアドレス／マスク
送信元ポート番号
宛先IPアドレス／マスク
宛先ポート番号
対象TOSフィールド値
帯域
修正／削除
追加
全削除


[マルチホーミング情報]
マルチホーミング機能
使用しない
順次方式
切り分け閾値
セッション数
回線使用率
最大回線使用速度
ラウンドロビン方式
双方方式
切り分け閾値
セッション数
回線使用率
最大回線使用速度
最大セッション数
0 セッション
最大回線使用率
0 %
最大回線使用速度
0 Kbps
セッション比率(WAN側:転送側)
0 :10
転送先ルータIPアドレス
セッションタイムアウト時間
5 分
転送セッション経路監視
監視用IPアドレス
ping実行間隔
10 秒
障害認識無応答回数
3 回
復旧判断応答回数
1 回
WAN側セッション経路監視
宛先IPアドレス
再送間隔
5 秒
タイムアウト時間
16 秒
正常時送信間隔
17 秒
異常時送信間隔
30 秒
[静的マルチホーミング情報一覧]
優先順位
マルチホーミング経路
障害時の経路変更
プロトコル
送信元ポート番号
宛先ポート番号
修正／削除／移動
追加
全削除


[IPv6基本情報]
IPv6
使用する
使用しない
インタフェースID
自動
指定する
アドレスまたはプレフィックス
Valid Lifetime
期限有
無期限
Pref. Lifetime
期限有
無期限
フラグ
IPv6アドレス
30
日
7
日
c0
ルータ広報
送信しない
送信する
最大送信間隔
600
秒
最小送信間隔
200
秒
Router Lifetime
1800
秒
MTU
Reachable Time
0
ミリ秒
Retrans Timer
0
ミリ秒
Cur Hop Limit
64
フラグ
00
ヘッダ圧縮
IPヘッダ圧縮
[IPv6ダイナミックルーティング機能]
RIPng送信
送信しない
送信する
メトリック値
0
RIPng受信
受信しない
受信する
サイトローカルプレフィックス
交換しない
交換する
経路集約
集約経路
破棄経路設定
デフォルトルート
ネットワーク指定
設定する



[基本情報]

ルーティングの対象となるネットワークの情報を設定します。

ネットワーク名

このネットワークを識別する名称を半角英数字８文字以内で指定します。

データ圧縮

送受信するデータを圧縮します。データ圧縮のアルゴリズムは、LZSをサポートします。使用する指定をした場合でも、実際にデータ圧縮を行うかどうかは相手ホストとのネゴシエーションで決まります。

MTUサイズ

最大パケット送信サイズ（Maximum Transmission Unit）を200～1500バイトの範囲で指定します。IPv6通信で利用する場合は、1280バイト以上の値を指定します。
IPv6トンネル（IPv6 over IPv4）を利用する場合は、1280を指定します。
ブリッジ通信する場合は、1500バイトを指定します。1500バイト未満のMTUを指定すると、正しくブリッジ通信ができない場合があります。
RIPを利用する場合は、576バイト以上を指定します。576バイト未満のMTUを指定すると、RIPパケットが送信されない場合があります。

自動ダイヤル

通信データ発生時に自動的にダイヤルするかどうかを選択します。使用する場合は、通信データ発生時に自動的にダイヤルします。

こんな事に気をつけて

回線情報で自動ダイヤルを“すべて禁止”としている場合は、自動ダイヤルを行いません。自動ダイヤルを行う場合は、回線情報の自動ダイヤルを“相手毎に設定”とします。

DLCI

16～991の範囲で指定します。DLCIを設定できるネットワークは32個まで指定できます。

CIR

CIRを選択します。

MSS書き換え

MSS書き換え機能を使用するかどうか選択します。使用する場合“使用する”を選択し、書き換えサイズを0または160～1460の範囲で指定します。0を指定する場合はMSS書き換え機能が無効となります。

シェーピング

シェーピング機能を使用するかどうか選択します。使用する場合は、最大送信レートを1～128の範囲で指定します。

補足 シェーピング機能とは、相手装置にデータを送信する際に回線速度より低い転送速度で通信する場合に使用する機能です。

本装置は回線種別が専用線（HSD）の場合だけ使用することができます。本機能を使用する場合は、以下のように設定してください。

1. 詳細設定メニューから「相手情報設定」→［ネットワーク情報一覧］でシェーピング機能を使用するネットワーク情報の［修正］ボタン（追加の場合は、［追加］ボタン）をクリックします。
2.「基本情報」の「シェーピング」で“使用する”をチェックし、“最大送信レート”に送信する速度を1～128の範囲で設定し、［更新］ボタンをクリックします。

ただし、64Kbps専用線を使用する場合に、64～128の範囲で“最大送信レート”を設定しても、本機能は動作しませんので注意してください。

［接続先情報一覧］

現在設定されている接続先の情報の一覧です。マルチルーティングを行う場合は、優先順位の1から順に評価され、最初に条件が成立した接続先にデータが流れます。接続先の定義は装置全体で48個まで設定できます。処理するボタンをクリックし、次のページに進みます。

［MP情報］

MP（MultilinkPPP）の情報を指定します。

MP回線初期リンク数

回線接続時に接続するチャネル数を選択します。

アナログ使用時縮退

アナログ使用時縮退を行うかどうかを選択します。アナログ使用時縮退は、MPで2本のチャネルを使用している時に、アナログ電話がかかってきたり、アナログ電話の受話器を上げたりする場合に、チャネルを1本に減らしてアナログ機器を使用することができます。

トラフィックによる増減

回線負荷に応じて帯域幅（1B、2B）を自動的にコントロールする機能（BOD）を使用するかどうかを選択します。“する”を選択する場合は、回線増減の条件も指定します。指定した回線使用率を超える（削減の場合は下回った）状態が“猶予時間”以上続く時点で、回線の接続（削減の場合は切断）を行います。回線使用率は0～100%、猶予時間は0～3600秒の範囲で指定します。

この機能を利用する場合は、主に発信側となる装置のBOD機能を有効にし、着信側となる装置のBOD機能を無効にしてください。発信側および着信側の両装置でBOD機能を有効にすると、両装置の仕様差により、着信側から発呼する場合があり、着信側に課金が発生する場合がありますので注意してください。なお、BAP／BACP機能をサポートする相手装置と接続する場合は、接続先情報のMP接続でBAP／BACP利用を必ず“する”にしてください。

受信パケット順序制御

MPを使用する場合は、必ず“する”をチェックします。“しない”をチェックすると、MPとヘッダ圧縮を併用する場合にヘッダ圧縮が無効になります。また、データ圧縮を使用している場合は、受信パケット順序制御の“しない”を選択すると圧縮効率が下がります。ブリッジを使用する場合は、有効にしてください。

[IP基本情報]

WAN側IPアドレス

WAN側のIPアドレスを固定で設定するかどうかを選択します。設定する場合に、“相手IPアドレス”、または“自側IPアドレス”の一方だけを指定し、他方を省略することもできます。なお、WAN側でRIPを使用する場合は、どちらか一方を省略することはできません。両方とも指定するか、両方とも省略してください。BGPを使用する場合は、両方とも指定してください。

ヘッダ圧縮

送受信するパケットのヘッダ部分を圧縮します。圧縮アルゴリズムは、VJヘッダ圧縮（RFC1144に準拠）およびIPヘッダ圧縮（圧縮方法：RFC2507／RFC2508、ネゴシエーション方法：RFC2509に準拠）をサポートします。使用する指定の場合も、実際にヘッダ圧縮を行うかどうかは、相手ホストとのネゴシエーションで決まります。

[ダイナミックルーティング機能]

ダイナミックルーティングを行うためのルーティング情報を設定します。

本装置がサポートしているダイナミックルーティング機能はRIPとBGPです。RIPを使用する場合は、各インタフェース単位で設定する必要があります。BGPを使用する場合は、「ルーティングプロトコル情報設定」（P.281）を参考にしてください。

RIP送信

RIP情報を送信するかどうかを選択します。送信する設定にした場合、15～45秒ごとにRIP情報を送信します。RIP送信を行う場合は、RIPの種類を選択します。

- V1
  ルーティングプロトコルにRIP V1を使用し、送信します。
  WAN側IPアドレスの自側IPアドレスが設定されている場合はユニキャストで、設定されていない場合はブロードキャストで送信します。
- V2
  ルーティングプロトコルにRIP V2を使用し、送信します。
  WAN側IPアドレスの自側IPアドレスが設定されている場合はユニキャストで、設定されていない場合はブロードキャストで送信します。
- V2（Multicast）
  ルーティングプロトコルにRIP V2を使用し、マルチキャストで送信します。

⚠注意

ISDNの場合、RIP情報を送信すると思わぬ課金（定期発信、または長時間接続）が発生します。

RIP受信

RIP情報を受信するかどうかを選択します。RIP受信を行う場合は、RIPの種類を選択します。

- V1
  ルーティングプロトコルにRIP V1を使用し、受信します。
- V2、V2（Multicast）
  ルーティングプロトコルにRIP V2を使用し、ブロードキャストおよびマルチキャストを受信します。

メトリック値

RIP送信時に加算するメトリック値を選択します。

認証パケット

RIP V2使用時にだけ有効な設定です。RIP V2では、同一パスワードグループでだけ、RIP情報の交換を行うことができます。パスワード認証によるRIP情報の交換を行う場合は、“破棄しない”を選択し、パスワードを半角英数字16文字以内で指定します。“破棄する”を選択する場合は、パスワード認証によるRIP情報の交換は行いません。

[スタティックルーティング情報一覧]

現在、このネットワークに設定されているスタティックルーティング情報の一覧です。スタティックルーティングの定義は装置全体で64個まで設定できます。処理するボタンをクリックし、次のページに進みます。

[IPフィルタリング情報一覧]

現在、このネットワークに設定されているIPフィルタリング情報の一覧です。処理は優先順位1から順に行います。IPフィルタリングの定義は装置全体で64個まで設定できます。処理するボタンをクリックし、次のページに進みます。

[TOS値書き換え情報一覧]

現在、このネットワークに設定されているTOS値書き換え情報の一覧です。処理は優先順位1から順に行います。TOS値書き換えの定義は装置全体で32個まで設定できます。処理するボタンをクリックし、次のページに進みます。

[NAT情報]

NATに関する情報を設定します。

NATの使用

NATを使用するかどうかを選択します。マルチNATを使うと複数の端末を同時に使用できます。NATを使用しない場合は、以下の設定は無効です。

グローバルアドレス

特定のグローバルアドレスを使用する場合に指定します。指定しない場合は、自動で割り当てられます。

アドレス個数

複数個のグローバルアドレスを使用する場合は、上述のグローバルアドレスを先頭とし、連続した複数のアドレスを指定します。その個数を1～16の範囲で指定します。

アドレス割当てタイマ

アドレス変換情報は一定の時間に該当する通信を行わないと、自動的に解放されます。解放するための猶予時間を0～24時間の範囲で指定します。0を指定すると、回線が切断するまで情報は解放されません。

NATセキュリティ

“高い”を選択する場合、ftpやdnsの要求する相手からの応答かどうかをチェックします。相手サーバがNATを使用している際など、要求先とは別のアドレスから応答する場合は、“通常”を選択します。

フラグメント順序変更

NATは、フラグメントされたパケットの順序が前後逆転して受信した場合、そのパケットを破棄します。フラグメントされたパケットの順序が逆転しないように、あらかじめパケットを整列させる機能を使う場合は、“使用する”を選択します。

[静的NAT情報一覧]

NATを使用すると、アドレス変換情報は固定で持つことができます。現在設定されている固定のアドレス変換情報の一覧です。

静的NATの定義は装置全体で64個まで設定できます。処理するボタンをクリックし、次のページに進みます。

[帯域制御（WFQ）情報一覧]

現在、このネットワークに設定されている帯域制御の定義の一覧です。帯域制御の定義は装置全体で64個まで設定できます。処理するボタンをクリックし、次のページに進みます。

[マルチホーミング情報]

マルチホーミング機能

マルチホーミング機能はWANに送信されるパケットの一部をLAN上のほかのルータに転送することによりWAN回線を負荷分散します。また本装置のWANインタフェースのケーブル抜けや前述のLAN上のほかのルータを経由する経路に障害が発生した場合に、障害が発生した経路を通過しないようにパケットを送信して高信頼性を実現します。

マルチホーミング情報の説明でのセッションとは送信元IPアドレスと宛先IPアドレスの組のことであり、TCPのセッションとは異なります。また、静的マルチホーミング情報で設定した通信とFTPのデータ送受信の通信はここには含まれません。表示メニューのマルチホーミング情報ではtypeがdynamicである情報がこのセッションにあたります。セッションは順次方式・双方方式のセッション数切り分けとラウンドロビン方式で使用されます。

マルチホーミング情報でtypeがFTPである情報はFTPのデータの送受信であり、切り分けには使用されません。

静的マルチホーミング情報が設定されている場合、マルチホーミング情報より静的マルチホーミング情報が優先されます。

マルチホーミング機能でのパケットの切り分け方式を設定します。

使用しない

マルチホーミング機能を使用しません。以下のマルチホーミング情報の設定は無視されます。

順次方式

切り分け閾値が“セッション数”の場合、指定した「最大セッション数」を超えるWAN向きのセッションはLAN上の転送先ルータを経由します。

切り分け閾値が“回線使用率”の場合、WANの回線使用率が指定した「最大回線使用率」を超えているときに始まった新しいセッションは、LAN側の転送先ルータを経由します。

切り分け閾値が“最大回線使用速度”の場合、「最大回線使用速度」に指定した速度を超えているときに始まったセッションは、LAN側の転送先ルータを経由します。

この方式を使用する場合は以下を設定します。

- 「切り分け閾値」
- 「最大セッション数」、「最大回線使用率」、または「最大回線使用速度」
  切り分け閾値に“セッション数”を選択した場合は「最大セッション数」を、“回線使用率”を選択した場合は「最大回線使用率」を、“最大回線使用速度”を選択した場合は「最大回線使用速度」をそれぞれ指定します。
- 「転送先ルータIPアドレス」
- 「転送セッション経路監視用IPアドレス」

ラウンドロビン方式

本装置のWANを経由するWAN側セッションとLAN側の転送先ルータを経由する転送セッションの比率が一定になるようにパケットを振り分けます。

この方式を使用する場合は以下を設定します。

- 「セッション比率（WAN側：転送側）」

- 「転送先ルータIPアドレス」
- 「転送セッション経路監視用IPアドレス」

双方方式

切り分け閾値を超えるまでは「順次方式」と同様に動作し、切り分け閾値を超えている間は「ラウンドロビン方式」と同じ動作をします。

この方式を使用する場合は以下を設定します。

- 「切り分け閾値」
- 「最大セッション数」、「最大回線使用率」、または「最大回線使用速度」
  切り分け閾値に“セッション数”を選択した場合は「最大セッション数」を、“回線使用率”を選択した場合は「最大回線使用率」を、“最大回線使用速度”を選択した場合は「最大回線使用速度」をそれぞれ指定します。
- 「セッション比率（WAN側：転送側）」
- 「転送先ルータIPアドレス」
- 「転送セッション経路監視用IPアドレス」

最大セッション数

順次方式または双方方式で閾値に使用する最大セッション数を0～256の範囲で指定します。

このセッション数を超えた分のセッションは転送セッションとなります。順次方式または双方方式の切り分け閾値に回線使用率または最大回線使用速度を使用する場合は指定する必要はありません。

最大回線使用率

順次方式または双方方式で閾値に使用する最大回線使用率を0～100の範囲で指定します。

回線使用率がこの指定値を超えている時に新しいセッションが発生すると、そのセッションは転送セッションとなります。順次方式または双方方式の切り分け閾値にセッション数または最大回線使用速度を使用する場合は指定する必要はありません。

最大回線使用速度

順次方式または双方方式にで閾値に使用する最大回線使用速度を0～128の範囲で指定します。順次方式または双方方式の切り分け閾値にセッション数または回線使用率を使用する場合は指定する必要はありません。

セッション比率（WAN側：転送側）

ラウンドロビン方式または双方方式を使用する場合、WAN側と転送側の経路を通るセッションの割合を選択します。セッションとは送信元IPアドレスと宛先IPアドレスの組のことであり、TCPのセッションとは異なります。順次方式を使用する場合は選択する必要はありません。

転送先ルータIPアドレス

転送セッションのパケットを転送する先のルータのアドレスを指定します。

セッションタイムアウト時間

動的なセッション管理一覧に記録されたセッションが、ここで指定した時間を超えても無通信状態が続くと、そのセッションは一覧から削除されます。1～1440分の範囲で指定します。

転送セッション経路監視

監視用IPアドレス

転送セッションの経路の状態を監視するために実行するpingの宛先IPアドレスを指定します。

ping実行間隔

前記のpingの実行間隔を1～255の範囲で指定します。

障害認識無応答回数

前記のpingの応答をここで指定する回数で連続して受信できない場合に、転送セッションの経路に障害が発生したと認識します。1～16の範囲で指定します。

復旧判断応答回数

転送セッションの経路に障害があると認識されている状態で、前記のpingの応答をここで指定した回数を連続して受信した場合に障害から復旧したと認識します。1～16の範囲で指定します。

WAN側セッション経路監視

WAN側セッションの経路の状態を監視するために実行するICMP ECHOパケットの宛先IPアドレスを指定します。ICMP ECHOパケットの宛先IPアドレスを指定しない場合は、WAN側セッションが使用する回線の状態によって、WAN側に障害が発生、または障害から復旧したと認識します。

宛先IPアドレス

WAN側セッションの経路の状態を監視するために実行するICMP ECHOパケットの宛先IPアドレスを指定します。0.0.0.0を指定した場合は、ICMP ECHOパケットによる監視は行わず、使用する回線の状態によって、WAN側に障害が発生、または障害から復旧したと認識します。

再送間隔

ICMP ECHOパケットの再送間隔を1～60秒の範囲で指定します。省略した場合は、5秒に設定されます。

タイムアウト時間

ICMP ECHOパケットの応答を待つ時間を［再送間隔+1］～240秒で指定します。省略した場合は、再送間隔×3＋1秒に設定されます。

正常時送信間隔

WAN側の回線に障害が発生していない、または障害から復旧して正常とみなしているときのICMP ECHOパケットの送信間隔を［タイムアウト時間+1］～255秒の範囲で指定します。省略した場合は、タイムアウト時間＋1秒に設定されます。

異常時送信間隔

WAN側の回線に障害が発生し、異常とみなしているときのICMP ECHOパケットの送信間隔を1～255秒の範囲で指定します。省略した場合は、30秒に設定されます。

こんな事に気をつけて

WAN側セッション経路監視の宛先IPアドレスを指定した場合は、本装置から宛先IPアドレスの監視ホストに対してICMP ECHOパケットを定期的に送出します。そのため、定額制でない回線を使用する場合は、超過課金の原因となることがあります。このような環境では、WAN側セッション経路監視の宛先IPアドレスを指定しないでください。

［静的マルチホーミング情報一覧］

現在、このネットワークに設定されている静的マルチホーミング情報の一覧です。特定のアプリケーションに属するパケットのマルチホーミング経路を固定するために使用する情報で64個まで設定できます。処理は優先順位1から順に行います。処理するボタンをクリックし、次のページに進みます。静的マルチホーミング情報で設定した通信はマルチホーミング情報には表示されません。

［IPv6基本情報］

IPv6

WAN回線上でIPv6の通信を使用するかどうかを選択します。

インタフェースID

“自動”を選択する場合は、装置のMACアドレスから自動生成されるインタフェースIDを使用します。通常はこの設定を使用します。

“指定する”を選択する場合は、16ビットごとに区切り文字（:）を入れて、16桁の16進数でインタフェースIDを指定します。このとき、ほかの装置と違うインタフェースIDを指定します。

記述例）

fedc:ba98:7654:3210

IPv6アドレス

本装置のLAN側のIPv6アドレスを標準的なIPv6アドレスで指定します。本装置ではprefix lengthは64に固定されます。インタフェースID部分がすべて0の場合は、指定するアドレスはprefixとして解釈されます。実際に利用するアドレスは、そのアドレスにインタフェースIDを付与したものとなります。

記述例）

fec0::1000:200:fffc:1111:1111

完全なIPv6アドレスとして解釈されます。

fec0:0:0:1000::

prefixとして解釈され、インタフェースID部分にはインタフェースIDが付与されます。

Valid Lifetime

通常は奨励値“30日”を使用します。

有効範囲）

0 ～ 365日

0 ～ 8760時

0 ～ 525600分

0 ～ 31536000秒

期限を定めない（無期限）の場合は、チェックボックスをチェックします。

Pref. Lifetime

通常は奨励値“7日”を使用します。

有効範囲）

0 ～ 365日

0 ～ 8760時

0 ～ 525600分

0 ～ 31536000秒

期限を定めない（無期限）の場合は、チェックボックスをチェックします。

フラグ

ルータ広報のプレフィックス情報ごとに設定するフラグフィールドの内容を2桁の16進数で指定します。この領域の値として、RFC2461で以下の値が定義されています。必要に応じて以下の値の論理和を設定してください。

・on-link flag　80

・autonomous address-configuration flag　40

特に問題がない場合は“c0”を使用します。

ルータ広報

ルータ広報メッセージ（router advertisement message）を送信する場合は“送信する”を選択し、以下の項目を設定します。

最大送信間隔

ルータ広報メッセージの最大送信間隔を指定します。

有効範囲）4 ～ 1800

最小送信間隔

ルータ広報メッセージの最小送信間隔を指定します。

有効範囲）3 ～ 最大送信間隔の 3／4

Router Lifetime

ルータ広報で送信する Router Lifetime の内容を指定します。

有効範囲）0 または 最大送信間隔 ～ 9000

MTU

ルータ広報で送信する MTU option の内容を指定します。無指定の場合には MTU option を含めません。

有効範囲）1280 ～ 1500

Reachable Time

ルータ広報で送信する Reachable Time の内容を指定します。

有効範囲）0 ～ 3600000

Retrans Timer

ルータ広報で送信する Retrans Timer の内容を指定します。

有効範囲）0 ～ 4294967295

Cur Hop Limit

ルータ広報で送信する Cur Hop Limit の内容を指定します。

有効範囲）0 ～ 255

フラグ

ルータ広報の本体部分に設定するフラグフィールドの内容を 2 桁の 16 進数値で指定します。この領域の値として、RFC2461 で以下の値が定義されています。必要に応じて以下の値の論理和を設定してください。

・Managed address configuration flag　80

・Other stateful configuration flag　40

ヘッダ圧縮

送受信するパケットのヘッダ部分を圧縮します。圧縮アルゴリズムは、IP ヘッダ圧縮（RFC2507／RFC2508 に準拠）をサポートします。使用する指定の場合も、実際にヘッダ圧縮を行うかどうかは、相手ホストとのネゴシエーションで決まります。

[IPv6ダイナミックルーティング機能]

RIPng送信

RIPngを送信するかどうかを選択します。

メトリック値

加算するメトリック値を選択します。“RIPng送信する”を選択した場合だけ有効です。

RIPng受信

RIPngを受信するかどうかを選択します。

サイトローカルプレフィックス

サイトローカルプレフィックスを交換するかどうかを選択します。

経路集約

RIPngで集約経路を送信する場合に、集約して広報する経路を設定します。

集約経路

デフォルトルートまたはネットワーク指定を選択し、集約して広報する経路を指定します。

破棄経路設定

集約経路に対する破棄経路を設定するかどうかを選択します。破棄経路を設定すると、転送先にこの経路を選択したパケットは破棄され、パケット送信元にICMPv6エラーメッセージが送信されます。

[IPv6スタティックルーティング情報一覧]

現在、WAN側に設定されているIPv6のスタティックルーティング情報の一覧です。IPv6スタティックルーティングの定義は装置全体で64個まで設定できます。処理するボタンをクリックし、次のページに進みます。

[IPv6フィルタリング情報一覧]

現在、このネットワークに設定されているIPv6フィルタリング情報の一覧です。処理は優先順位1から順に行います。IPv6フィルタリングの定義は装置全体で64個まで設定できます。処理するボタンをクリックし、次のページに進みます。

[ブリッジ情報]

ブリッジ機能

接続相手とブリッジ機能を使用して通信するかどうかを選択します。

STP機能

STP機能を利用して経路制御を行うかどうかを選択します。行う場合は、“使用する”を選択して、以下の項目を指定します。この設定項目はブリッジ機能を使用する場合だけ有効です。

パスコスト

STPで利用するパスコストを選択します。“指定する”を選択する場合は、1～65535の範囲で指定します。パスコストの適性値が不明な場合は、“自動決定”を選択すると、自動的にパスコストが決定されます。

インタフェース優先度

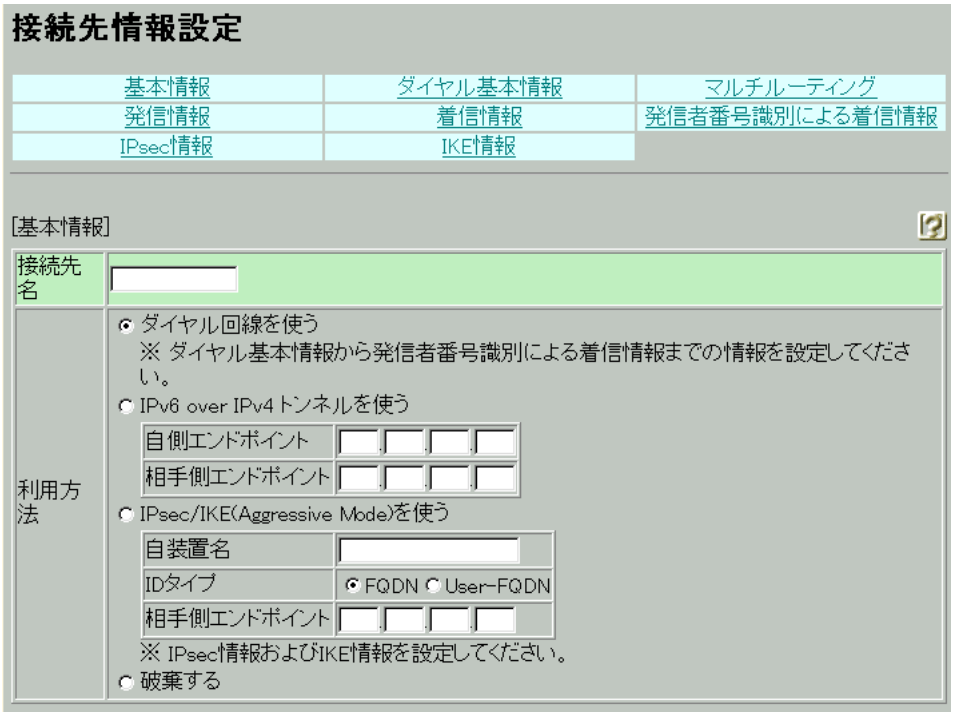
STPで使用するインタフェースごとの優先度を0～255の範囲で指定します。値が小さい方が優先となります。

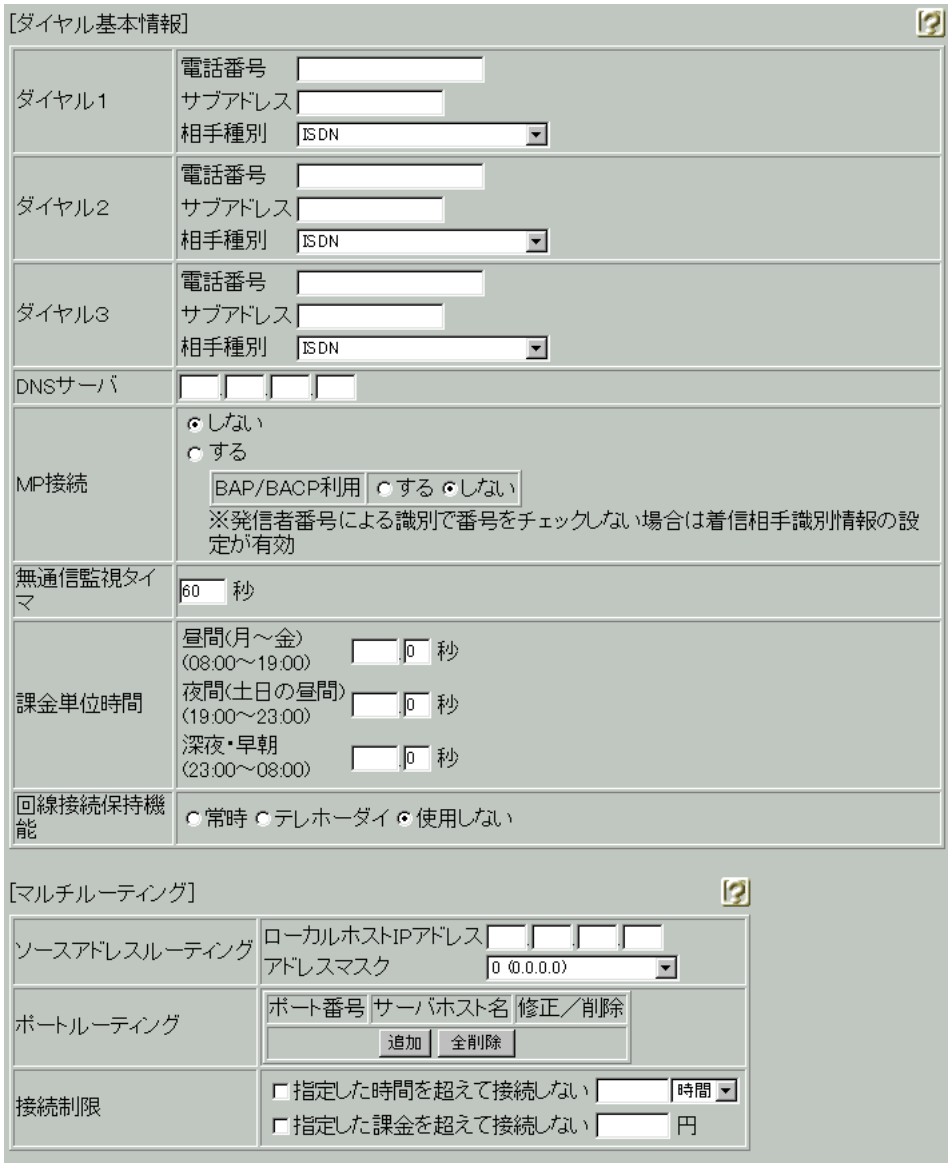
[MACフィルタリング情報一覧]

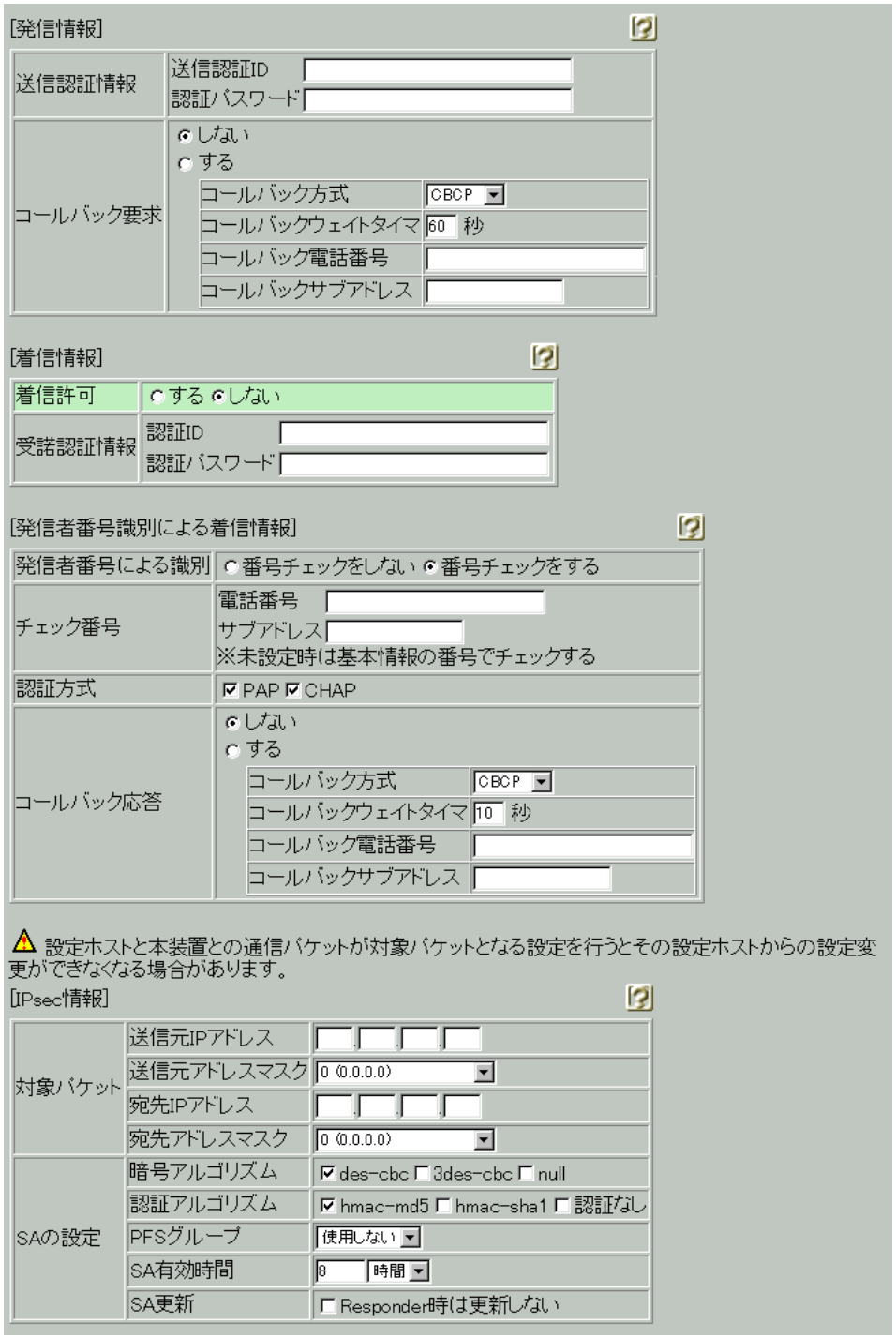
現在のWAN回線接続のMACフィルタリング情報の一覧です。MACフィルタリングの定義は装置全体で128個まで設定できます。処理するボタンをクリックし、次のページに進みます。

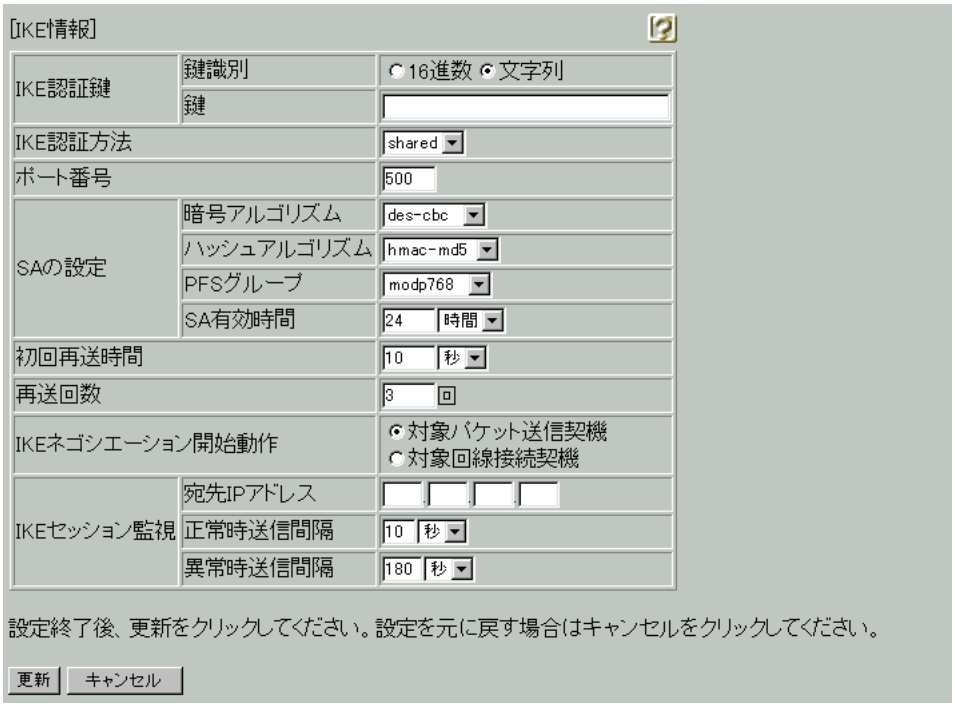
接続先情報設定

【操作】「詳細設定メニュー」→ルータ設定「相手情報」→［ネットワーク情報一覧］→［接続先情報一覧］




[ダイヤル基本情報]
ダイヤル1
電話番号
サブアドレス
相手種別
ISDN
ダイヤル2
電話番号
サブアドレス
相手種別
ISDN
ダイヤル3
電話番号
サブアドレス
相手種別
ISDN
DNSサーバ
MP接続
しない
する
BAP/BACP利用
する
しない
※発信者番号による識別で番号をチェックしない場合は着信相手識別情報の設定が有効
無通信監視タイマ
60
秒
課金単位時間
昼間(月～金)
(08:00～19:00)
0
秒
夜間(土日の昼間)
(19:00～23:00)
0
秒
深夜・早朝
(23:00～08:00)
0
秒
回線接続保持機能
常時
テレホーダイ
使用しない
[マルチルーティング]
ソースアドレスルーティング
ローカルホストIPアドレス
アドレスマスク
0 (0.0.0.0)
ポートルーティング
ポート番号
サーバホスト名
修正／削除
追加
全削除
接続制限
指定した時間を超えて接続しない
時間
指定した課金を超えて接続しない
円


[発信情報]
送信認証情報
送信認証ID
認証パスワード
コールバック要求
しない
する
コールバック方式
CBCP
コールバックウェイトタイマ
60
秒
コールバック電話番号
コールバックサブアドレス
[着信情報]
着信許可
する
しない
受諾認証情報
認証ID
認証パスワード
[発信者番号識別による着信情報]
発信者番号による識別
番号チェックをしない
番号チェックをする
チェック番号
電話番号
サブアドレス
※未設定時は基本情報の番号でチェックする
認証方式
PAP
CHAP
コールバック応答
しない
する
コールバック方式
CBCP
コールバックウェイトタイマ
10
秒
コールバック電話番号
コールバックサブアドレス
設定ホストと本装置との通信パケットが対象パケットとなる設定を行うとその設定ホストからの設定変更ができなくなる場合があります。
[IPsec情報]
対象パケット
送信元IPアドレス
送信元アドレスマスク
0 (0.0.0.0)
宛先IPアドレス
宛先アドレスマスク
0 (0.0.0.0)
SAの設定
暗号アルゴリズム
des-cbc
3des-cbc
null
認証アルゴリズム
hmac-md5
hmac-sha1
認証なし
PFSグループ
使用しない
SA有効時間
8
時間
SA更新
Responder時は更新しない



[基本情報]

接続先名

この接続先を識別するための名称を半角英数字８文字以内で指定します。この接続名は手動接続の際にも使用されます。

利用方法

この接続先との通信で利用する方法（通信方式）を以下の４つから選択します。

ダイヤル回線を使う

ISDN回線を利用して通信する場合に選択します。

IPv6 over IPv4 トンネルを使う

IPv6 over IPv4 トンネルを利用して通信する場合に選択します。

自側（相手側）エンドポイントの指定

IPv4形式のアドレスを指定します。

IPsec/IKE（Aggressive Mode）を使う

IPsec/IKE（Aggressive Modeの発側）を利用して通信する場合に選択します。
固定IPアドレスでIPsecによる暗号化通信を行う場合は、「詳細設定メニュー」の「IPsec情報」を設定してください。

自側装置名
自装置を識別する名前を64文字以内で指定します。

IDタイプ
ネゴシエーションの交換タイプを選択します。

相手側エンドポイント
IPv4形式のアドレスを指定します。

破棄する
送信するパケットをすべて破棄する場合に選択します。

[ダイヤル基本情報]

ダイヤル1／2／3

接続に用いる電話番号は3つまで指定できます。ダイヤル1の電話がかからない場合はダイヤル2に、ダイヤル2がかからない場合はダイヤル3にダイヤルします。相手種別は送信時にだけ参照されます。着信時は自動認識します。

電話番号
電話番号を32桁以内で指定します。電話番号には、0～9、*、#を使用できます。

サブアドレス
サブアドレスを19桁以内で指定します。
PIAFS（64Kbps）着信時は、指定したサブアドレスは無視されます。

相手種別
相手の種別をISDN、32kPIAFS、64kPIAFS（NTT DoCoMo方式）、64kPIAFS（DDI Pocket方式）の中から選択します。

DNSサーバ

接続するときに使用するDNSサーバのIPアドレスを指定します。ProxyDNSを使用するときに必要です。省略、または0.0.0.0を指定する場合は、自動取得となります。
255.255.255.255を指定する場合は使用しません。また、このアドレスはPPPのネゴシエーションの中で相手から要求がある場合、相手に受け渡すDNSサーバアドレスとしても使用します。

MP接続

MP接続を行うかどうかを選択します。“する”を選択する場合は、BAP／BACPの利用可否も選択します。ただし、発信者番号では識別されない相手から着信がある場合、相手情報の着信相手識別情報の設定を参照します。

無通信監視タイマ

ISDN回線の無通信監視タイマを0～3600秒の範囲で指定します。その時間を超えても、通信が行われない場合は、ISDN回線を自動的に切断します。なお、0を指定した場合、自動切断を行いません。

課金単位時間

各時間帯の課金単位時間を0.0～3600.0秒の範囲で指定します。ここで指定する時間は無通信監視による回線切断のときに参照し、同一料金で最大の接続時間を得るよう回線切断タイミングを調整します。なお、昼間時間帯に0を指定した場合、課金単位の調整は行いません。また、夜間時間帯や深夜・早朝時間帯に0を指定した場合は、その前の時間帯の指定を利用します。

こんな事に気をつけて

この機能を使用するときは、操作メニューの時刻設定を用いて本装置の内部時計を正しく設定してください。また、祝日の料金体系には対応していません。

回線接続保持機能

“常時”を選択すると、ほかの設定や通信の有無にかかわらず接続状態を保持します。また、相手から切断された場合や回線エラーによる切断が行われた場合は自動で再接続を行います。ただし､本装置で手動切断を行うと､次に手動接続が行われるまで自動接続動作は行いません。

⚠注意

フレッツ・ISDNなどの通信料定額サービス以外で“常時”を選択すると、高額な通信料金が課せられます。

“テレホーダイ”を選択すると、テレホーダイ機能の動作中に、この接続先が回線接続保持の対象となります。テレホーダイ契約されている電話番号向けの機能です。

[マルチルーティング]

従来のIPルーティングに加え、ローカルホストIPアドレス、ポート番号、および接続制限の組み合わせによるルーティングを行います。

ソースアドレスルーティング

ローカルホストIPアドレスによるルーティングを行います。この接続先に送信するパケットをローカルホストIPアドレスによって定義します。

ローカルホストIPアドレス、アドレスマスクの組み合わせにより、対象となるローカルホストIPアドレスを決定します。

こんな事に気をつけて

すべての接続先に対してソースアドレスルーティングを設定している状態で、本装置のファームウェア更新や通信確認（ping）などを行うことはできません。必ず1つはソースアドレスルーティングを行わない接続先を定義します。

ポートルーティング

ポート番号を使用して、ルーティングを行います。この接続先に送信するパケットをポート番号（サービス）によって定義します。ポートルーティングの定義は装置全体で32個まで設定できます。

接続制限

この接続先を接続時間と課金によって発信抑制します。時間は0～999時間、金額は0～999,999円の範囲で指定できます。

[発信情報]

接続先への発信に関する情報を設定します。

送信認証情報

発信時に使用する認証IDとパスワードをそれぞれ64桁以内で指定します。

コールバック要求

コールバック要求を行うかどうかを選択します。コールバック要求とは、いったん接続して認証を行ったあとに回線を切断して、相手から電話をかけ直してもらう機能です。

要求する場合は、“する”を選択し、以下の項目を設定します。

コールバック方式

コールバックを行う場合の方式をCBCP、または無課金の中から選択します。Microsoft® 製品やCBCP方式をサポートしている装置とのコールバックを行う場合は、“CBCP”を選択します。本装置どうしのコールバックを行う場合には“無課金”も選択できます。“無課金”ではコールバック要求側には電話料金はかかりません。

コールバックウェイトタイマ

コールバック要求後の着信待ち時間を0～60秒の範囲で指定します（推奨時間60秒）。コールバックがうまくいかないときは、この時間を長くします。

コールバック電話番号

コールバックで相手側にダイヤルしてもらう電話番号を32桁以内で指定します。この電話番号は、CBCP方式によるコールバックにだけ有効です。

コールバックサブアドレス

コールバックで相手側にダイヤルしてもらう電話番号のサブアドレスを半角英数字19文字以内で指定します。このサブアドレスは、CBCP方式によるコールバックにだけ有効です。

[着信情報]

接続先からの着信に関する情報を設定します。接続先の特定に使用します。

着信許可

この接続先から着信を許可するかどうかを選択します。

受諾認証情報

着信時に受け付ける認証IDとパスワードをそれぞれ64桁以内で指定します。発信者番号で接続先を識別できる場合は、この情報を省略し、代わりに相手情報の受諾認証ID情報を使用できます。

[発信者番号識別による着信情報]

発信者番号で識別する相手の着信に関する情報を設定します。

着信時の相手識別の方法は2つあります。発信者番号通知を用いる方法と、認証IDを用いる方法です。

発信者番号による識別

発信者番号通知で相手を識別するかどうかを選択します。識別する場合は、“番号をチェックする”を選択し、以下の項目を設定します。識別しない場合は、以下の項目を設定する必要はありません。

チェックする番号

相手識別に使用する電話番号を32桁以内、サブアドレスを19桁以内で指定します。省略時は基本情報の値を使用します。なお、PIAFS（64Kbps）着信時には、指定したサブアドレスは無視されます。

認証方式

着信時に利用する認証プロトコルを選択します。どちらも選択しない場合は、その相手からの着信は認証しません。

コールバック応答

相手からのコールバック要求に応答するかどうかを選択します。応答する場合は、“する”を選択し、以下の項目を設定します。

コールバック方式

コールバックを行う場合の方式をCBCP、または無課金の中から選択します。Microsoft® 製品やCBCP方式をサポートしている装置とのコールバックを行う場合は、“CBCP”を選択します。本装置どうしのコールバックを行う場合には“無課金”も選択できます。“無課金”ではコールバック要求側には電話料金はかかりません。

コールバックウェイトタイマ

コールバック要求を受け、回線切断後、発信を行うまでの待ち時間を0～60秒の範囲で指定します（推奨10秒）。コールバックがうまくいかないときは、この時間を長くします。

コールバック電話番号

コールバック要求を受け、自側がダイヤルする電話番号を32桁以内で指定します。

コールバックサブアドレス

コールバック要求を受け、自側がダイヤルする電話番号のサブアドレスを半角英数字19文字以内で指定します。

［IPsec情報］

対象パケット

送信元（宛先）IPアドレス／アドレスマスク

IPsecを適用するセッションの送信元IPアドレスおよびアドレスマスクと、宛先IPアドレスおよびアドレスマスクを指定します。

SAの設定

暗号アルゴリズム

トンネリングするパケットの暗号アルゴリズムを使用する場合に選択します。3des-cbc、des-cbc、nullの順に比較されます。

認証アルゴリズム

トンネリングするパケットの認証アルゴリズムを選択します。hmac-md5、hmac-sha1、認証なしの順に比較されます。“認証なし”だけを選択した場合は、パケットの認証を行いません。

PFSグループ

自動鍵交換の鍵を生成するための鍵素材です。値が大きい程セキュリティ強度は高くなります。ただし、装置の負荷が高くなる場合があります。使用しない場合は、“使用しない”を選択します。

SA有効時間

SAの有効期限を時間で指定します。指定した時間が経過した時点で、SAの有効期限が切れ、IKEによってSA情報や鍵情報が自動的に更新されます。

SA更新

SAの更新時間を選択します。initiator SAは有効時間満了の90秒前、responder SAは有効時間満了の30秒前に設定されます。“Responder時は更新しない”を選択した場合は、Responder側からのSA更新は行いません。

[IKE情報]

SAの設定

暗号アルゴリズム

IKEセッションの送受信パケットを暗号化／複号化するためのアルゴリズムを選択します。

ハッシュアルゴリズム

IKEセッションのネゴシエーションパケットを認証するためのアルゴリズムを選択します。

PFSグループ

値が大きい程セキュリティ強度は高くなります。ただし、装置の負荷も高くなる場合があります。

SA有効時間

IKE SAの有効期限を時間で指定します。指定した時間が経過した時点で、IKEによってSAの設定は自動的に更新されます。

以下の範囲でSA有効時間を指定します。

単位）

1～24時

10～1440分

600～86400秒

初回再送時間

IKEの初回再送時間を10進数を使用して、1～10秒の範囲で指定します。

再送回数

IKEの再送回数を10進数を使用して、1～10回の範囲で指定します。

IKEネゴシエーション開始動作

IKEネゴシエーション開始動作を指定します。対象回線接続契機を指定した場合は、対象パケット送信契機も含まれます。

IKEセッション監視

指定された宛先IPアドレスに対してICMP ECHOパケットを送信します。応答がタイムアウトした場合にISAKMP/IPsec SAを解放します。

宛先IPアドレス

ICMP ECHOパケットの送出先IPアドレス指定します。宛先IPアドレスに0.0.0.0または省略した場合、IKEセッション監視をしません。また、正常時送信間隔、異常時送信間隔は初期値になります。

正常時送信間隔

ICMP ECHO パケットの応答が正常に受信されている状態で、次にICMP ECHO パケットを送信する間隔を1～60秒の範囲で指定します。省略した場合は10秒に設定されます。

異常時送信間隔

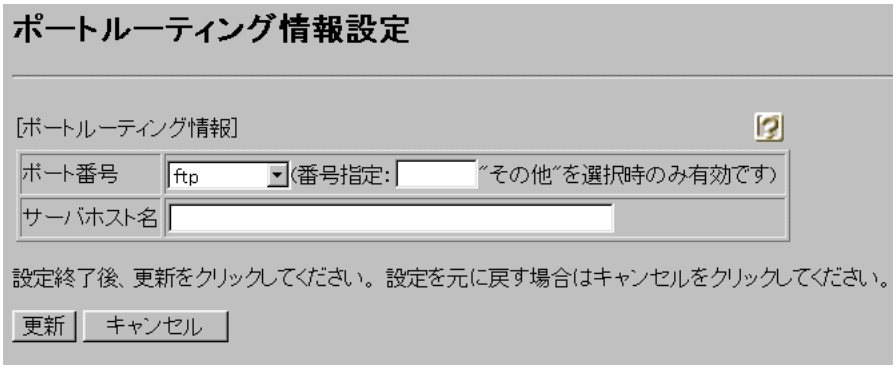
ICMP ECHO パケットのタイムアウトが発生してから応答が受信されるまでの周期送信する間隔を、60～600秒の範囲で指定します。応答が受信された場合は正常時送信間隔状態に戻ります。省略した場合は3分に設定されます。

こんな事に気をつけて

IKE セッション監視機能を使用すると、本装置から宛先IP アドレスのホストに対してICMP ECHO パケットを定期的に送出します。そのため、定額制でない回線を使用している場合は、超過課金の原因となることがあります。このような環境では、IKE セッション監視機能を使用しないでください。

ポートルーティング情報設定

【操作】「詳細設定メニュー」→ルータ設定「相手情報」→［ネットワーク情報一覧］→［接続先情報一覧］→［マルチルーティング］



[ポートルーティング情報]

ポート番号を使用して、ルーティングを行います。この接続先に送信するパケットをポート番号（サービス）によって定義します。この機能はProxyDNSを使用する場合だけ有効です。

ポート番号

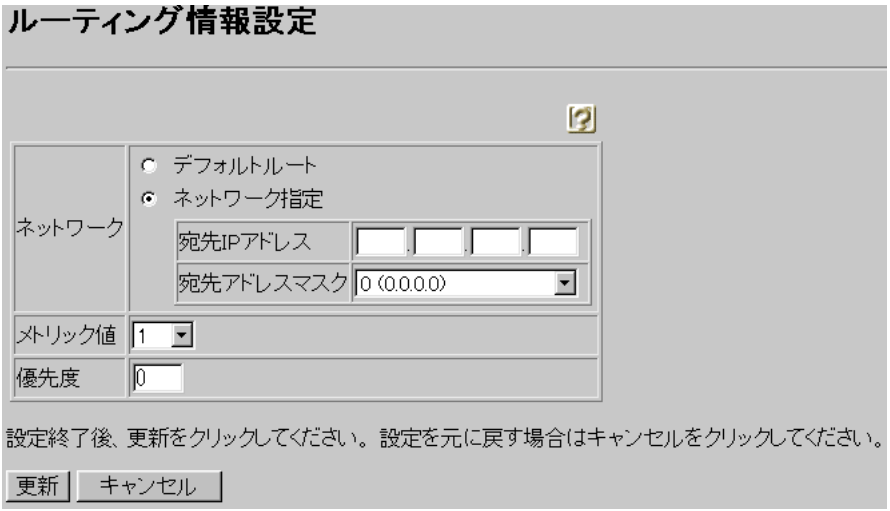
ポートルーティングの対象となるサービスを選択します。ポート番号を指定する場合は、“その他”を選択し、10進数を使用して、1～65535の範囲で指定します。

サーバホスト名

ポートルーティングの対象となるホスト名を半角英数字80文字以内で指定します。

ルーティング情報設定（ネットワーク情報）

【操作】「詳細設定メニュー」→ルータ設定「相手情報」→［ネットワーク情報一覧］→［スタティックルーティング情報一覧］



このページでは、ルーティング情報を固定で設定できます。ただし、デフォルトルート指定は装置に1つしか設定できません。

ネットワーク

デフォルトルート、またはネットワーク指定を選択し、宛先のネットワークを指定します。ネットワーク指定は、指定するネットワークを宛先に持つパケットの転送先を指定するもの、デフォルトルートは、ネットワーク指定されていない宛先を持つパケットの転送先を指定するものです。

メトリック値

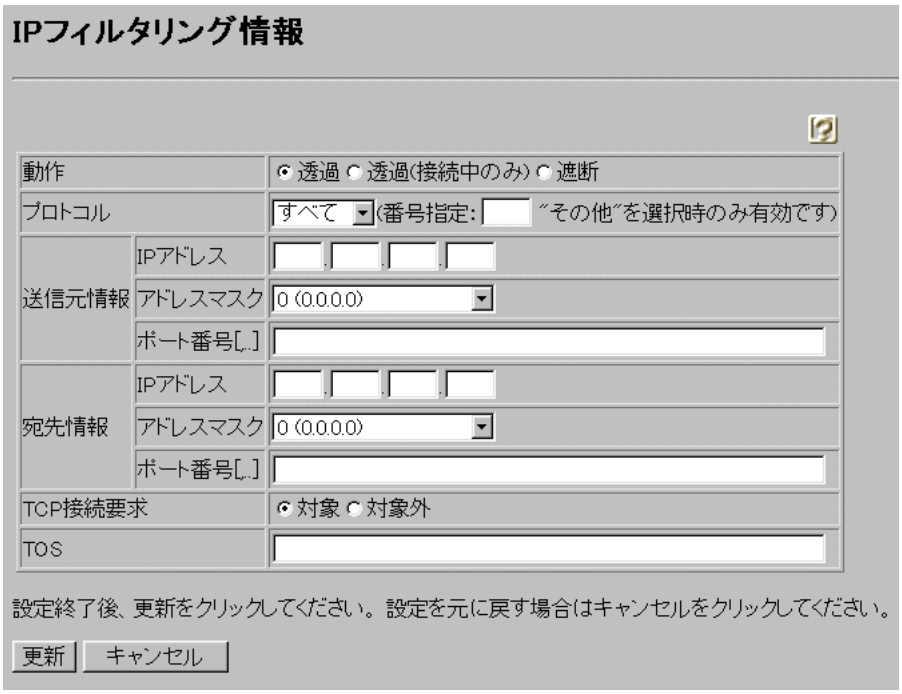
メトリック値を選択します。これは、ここで設定するルーティング情報をRIPで送信するときに加算されます。

優先度

ここで設定したルーティング情報の優先度を0～254の範囲で指定します。省略時は0が設定されます。優先度は小さい値がより高い優先度を示します。指定した優先度はルーティングプロトコルの経路情報の優先度と比較され、優先度の高い経路が使用されます。
ルーティングプロトコルの優先度のデフォルトは以下のとおりです。ルーティングプロトコルに設定されている優先度と同じ値は設定しないでください。
BGP　：20
RIP　：120

IPフィルタリング情報（ネットワーク情報）

【操作】「詳細設定メニュー」→ルータ設定「相手情報」→［ネットワーク情報一覧］→［IPフィルタリング情報一覧］



優先順位の高い定義より順にパケットのチェックを行い、すべての条件が一致する場合に定義する動作を行います。ただし、分割されたパケットに対しては正しく扱えません。

動作

IPフィルタリングの動作を以下の3つから選択します。

透過

条件と一致する場合にパケットを透過します。

透過（接続中のみ）

条件と一致する場合に、ISDN回線が接続しているときはパケットを透過します。切断しているときは遮断します。

遮断

条件と一致する場合にパケットを遮断します。

プロトコル

フィルタリング条件としてプロトコルを以下の6つから選択します。

・すべて　（0）

・TCP　（6）

・UDP　（17）

・ICMP　（1）

・IPv6 over IPv4　（41）

・その他

プロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、0～255の範囲で指定します。

送信元／宛先情報

IPアドレス／アドレスマスク

フィルタリング条件としてのIPアドレス、およびアドレスマスクを指定します。

チェック対象となるパケットのIPアドレスと、定義するIPアドレスとアドレスマスクの論理積が等しい場合に条件に一致します。

ポート番号

フィルタリング条件としてポート番号を10進数を使用して、1～65535の範囲、または'any'で指定します。'any'を指定する場合は、すべてのポート番号をフィルタリングの対象とします。また、ポート番号を複数指定する場合は、','で区切ります。範囲指定の場合は、'-'で区切ります。送信元情報と宛先情報を合わせて10組まで設定できます。

TCP接続要求

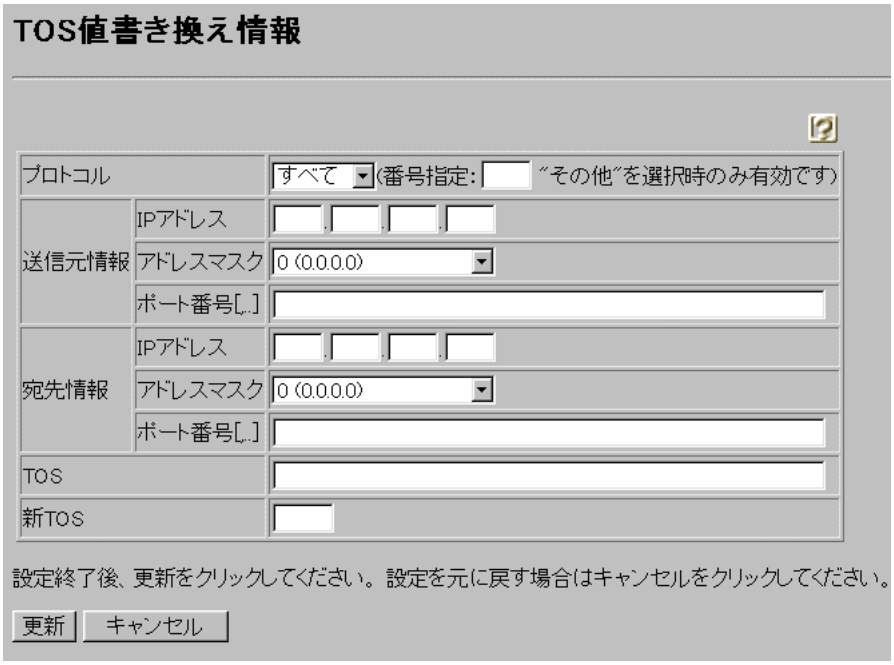
TCPプロトコルでのコネクション接続要求をフィルタリングの対象に含めるかどうかを選択します。

TOS

IPパケットのTOSフィールド値を16進数を使用して、0～ffの範囲、または'any'で指定します。TOSフィールド値を複数指定する場合は、','で区切ります。範囲指定の場合は、'-'で区切ります。10組まで設定できます。何も設定しない場合は、すべてのTOSフィールド値をフィルタリングの対象とします。

TOS値書き換え情報（ネットワーク情報）

【操作】「詳細設定メニュー」→ルータ設定「相手情報」→［ネットワーク情報一覧］→［TOS書き換え情報一覧］



［TOS値書き換え情報］

優先順位の高い定義より順にパケットのチェックを行い、すべての条件が一致する場合に定義するTOS値書き換えを行います。ただし、分割されたパケットに対しては正しく扱えません。

プロトコル

TOS値書き換えの条件としてプロトコルを以下の6つから選択します。

・すべて　(0)
・TCP　(6)
・UDP　(17)
・ICMP　(1)
・IPv6 over IPv4　(41)
・その他

プロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、0～255の範囲で指定します。

送信元／宛先情報

IPアドレス／アドレスマスク

TOS値書き換え条件としてのIPアドレス、およびアドレスマスクを指定します。

チェック対象となるパケットのIPアドレスと、定義するIPアドレスとアドレスマスクの論理積が等しい場合に条件に一致します。

送信元（宛先）情報のポート番号

TOS値書き換え条件としてポート番号を10進数を使用して、1～65535の範囲、または'any'で指定します。'any'を指定する場合は、すべてのポート番号がTOS書き換えの対象となります。また、ポート番号を複数指定する場合は、','で区切ります。範囲指定の場合は、'-'で区切ります。送信元情報と宛先情報で合わせて10組まで設定できます。

TOS

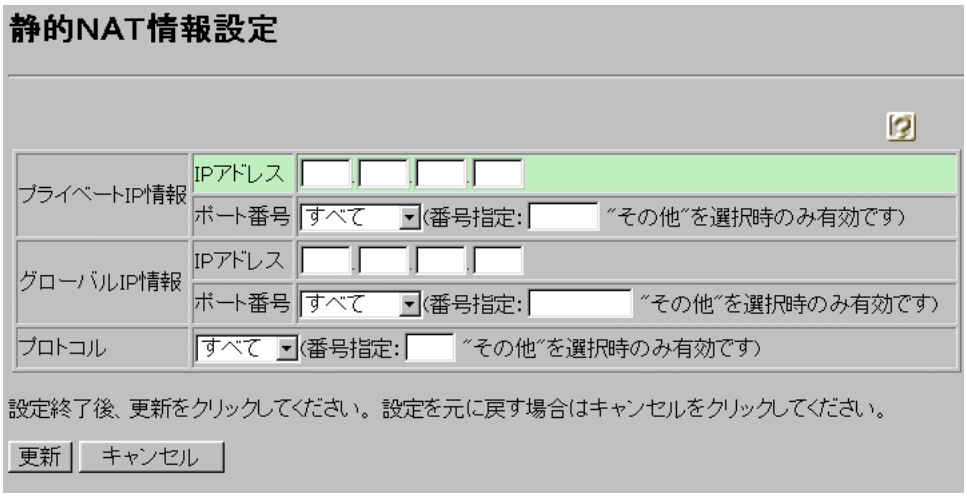
TOS値書き換えの条件としてIPパケットのTOSフィールド値を16進数を使用して、0～ffの範囲、または'any'で指定します。TOSフィールド値を複数指定する場合は、','で区切ります。範囲指定の場合は、'-'で区切ります。10組まで設定できます。何も設定しない場合は、すべてのTOSフィールド値を書き換えの対象とします。

新TOS

IPパケットに新しく設定するTOSフィールド値を16進数を使用して、0～ffの範囲で指定します。

静的NAT情報設定

【操作】「詳細設定メニュー」→ルータ設定「相手情報」→［ネットワーク情報一覧］→［静的NAT情報一覧］



プライベートIP情報

固定でアドレス変換を行う場合にローカルネットワーク側のIPアドレスとポート番号を指定します。IPアドレスは省略できません。

ポート番号を指定する場合は、“その他”を選択し、1～65535の範囲で指定します。グローバルポート番号を範囲指定する場合は、その範囲のグローバルポート番号が、指定するプライベートポート番号を先頭とする範囲へ変換されます。たとえば、プライベートポート番号に1000を指定し、グローバルポート番号に10000-11000を指定すると、グローバルポート番号の10000～11000はプライベートポート番号の1000～2000に変換されます。

グローバルIP情報

固定でアドレス変換を行う場合は、WAN側のIPアドレスとポート番号を指定します。IPアドレスは省略できます。省略する場合は、すべてのグローバルアドレスに対して有効な設定となります。ポート番号を指定する場合は、1～65535の範囲で1つ、または'-'で区切った1組の範囲を指定します。

プロトコル

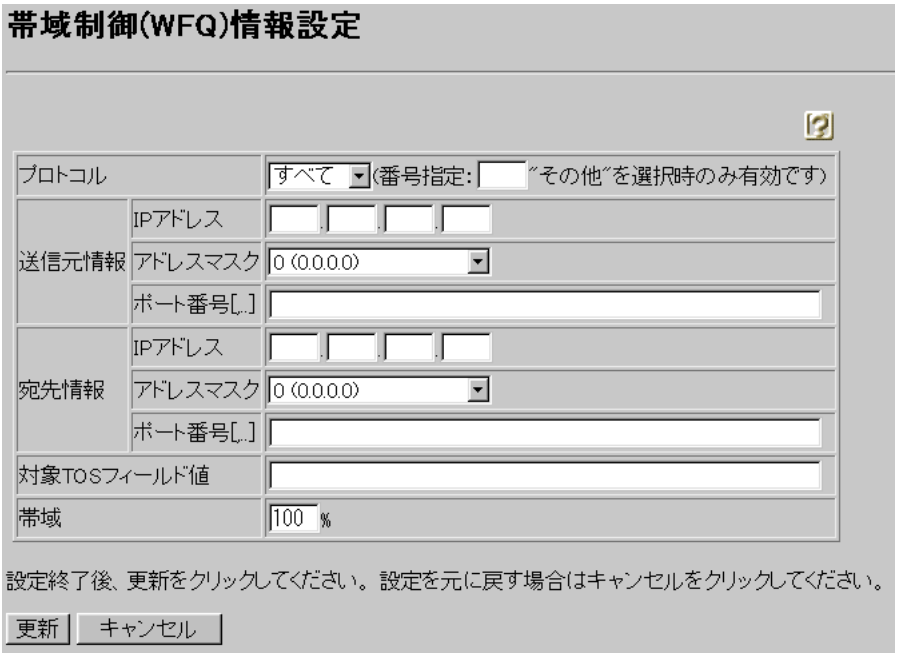
固定でアドレス変換を行う場合は、対象となるプロトコルを以下の8つから選択します。

・すべて　(0)
・TCP　(6)
・UDP　(17)
・ICMP　(1)
・IPv6 over IPv4　(41)
・ESP　(50)
・AH　(51)
・その他

プロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、0～255の範囲で指定します。

帯域制御（WFQ）情報設定

【操作】「詳細設定メニュー」→ルータ設定「相手情報」→［ネットワーク情報一覧］→［帯域制御（WFQ）情報一覧］



設定する任意のプロトコル、IPアドレス、ポート番号、TOSフィールド値の条件を元に、帯域を割り当てます。

プロトコル

帯域制御の対象となるプロトコルを以下の6つから選択します。

・すべて　(0)
・TCP　(6)
・UDP　(17)
・ICMP　(1)
・IPv6 over IPv4　(41)
・その他

プロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、0～255の範囲で指定します。

送信元／宛先情報

IPアドレス／アドレスマスク

帯域制御の対象となるIPアドレス、およびアドレスマスクを指定します。対象となるパケットのIPアドレスと定義するアドレスマスクの論理積と、定義するIPアドレスとアドレスマスクの論理積が等しい場合に条件に一致することになります。

ポート番号

帯域制御の対象となるポート番号を10進数を使用して、1～65535の範囲、または'any'で指定します。'any'を指定する場合は、すべてのポート番号が対象となります。また、ポート番号を複数指定する場合は、','で区切ります。範囲指定の場合は、'-'で区切ります。送信元情報と宛先情報を合わせて10組まで設定できます。

対象TOSフィールド値

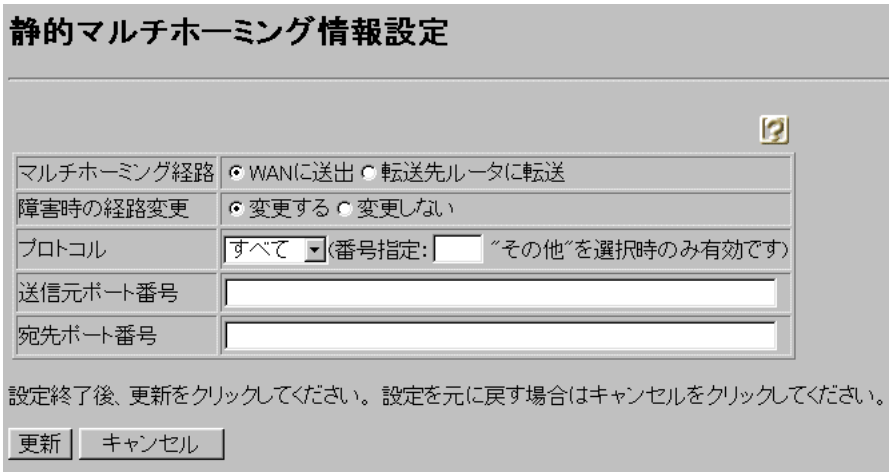
帯域制御の対象となるTOSフィールド値を16進数を使用して、0～ffの範囲で指定します。TOSフィールド値を複数指定する場合は、','で区切ります。範囲指定の場合は、'-'で区切ります。10組まで設定できます。何も設定しない場合は、すべてのTOSフィールド値を帯域制御の対象とします。

帯域

割り当てる帯域（%）を10進数を使用して、0～100の範囲で指定できます。0は非優先（ベストエフォート）、100は最優先を表します。同じ相手ネットワーク中で、0のものと100のものを除いたものの帯域トータルが100を超える場合には、それらの比率に従って帯域を割り当てます。

静的マルチホーミング情報設定

【操作】「詳細設定メニュー」→ルータ設定「相手情報」→［ネットワーク情報一覧］→［静的マルチホーミング情報］



特定のアプリケーションに属するパケットのマルチホーミング経路を固定するために使用します。その情報に従って、一致するパケットをWANに送出するか、またはLAN側の転送先ルータに転送します。

マルチホーミング経路

プロトコルとポート番号が一致するパケットをWANとLANのどちらに送信するかを選択します。“WANに送出”を選択する場合は、パケットをWANに送出します。“転送先ルータに転送”を選択する場合は、LAN側にある転送先ルータに転送します。転送先ルータは「マルチホーミング情報」で設定します。

障害時の経路変更

上記の「マルチホーミング経路」で設定した経路に障害が発生して不通となった場合にどうするかを選択します。“変更する”を選択する場合は、パケットを破棄しないで、上記の「マルチホーミング経路」で設定した経路とは異なる経路にパケットを転送します。“変更しない”を選択する場合は、マルチホーミング経路を変更しないでパケットを破棄します。

プロトコル

パケットのトランスポートプロトコルを以下の6つから選択します。

・すべて　（0）

・TCP　（6）

・UDP　（17）

・ICMP　（1）

・IPv6 over IPv4　（41）

・その他

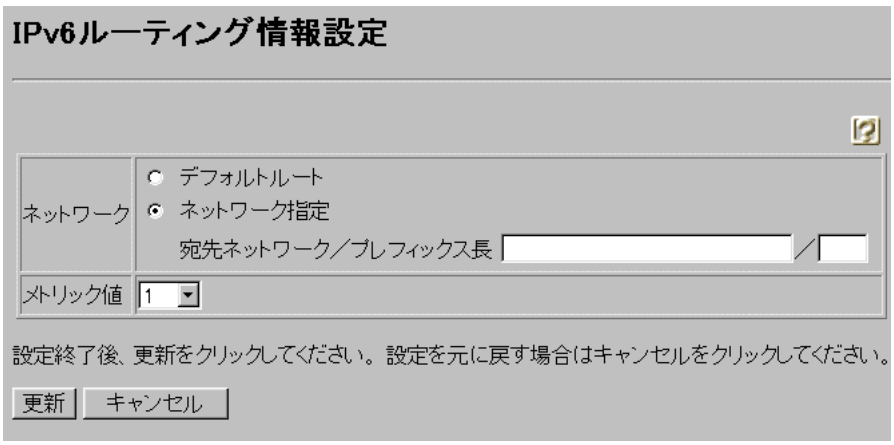
プロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、0～255の範囲で指定します。

送信元ポート番号、宛先ポート番号

ポート番号を10進数を使用して、1～65535の範囲、または'any'で指定します。'any'を指定する場合は、すべてのポート番号がフィルタリングの対象となります。また、ポート番号を複数指定する場合は、','で区切ります。範囲指定の場合は、'-'で区切ります。送信元ポートと宛先ポートを合わせて10組まで設定できます。

IPv6ルーティング情報設定（ネットワーク情報）

【操作】「詳細設定メニュー」→ルータ設定「相手情報」→［ネットワーク情報一覧］→［IPv6スタティックルーティング情報一覧］



IPv6ルーティング情報を固定で設定できます。ただし、デフォルトルート指定は装置に1つしか設定できません。

ネットワーク

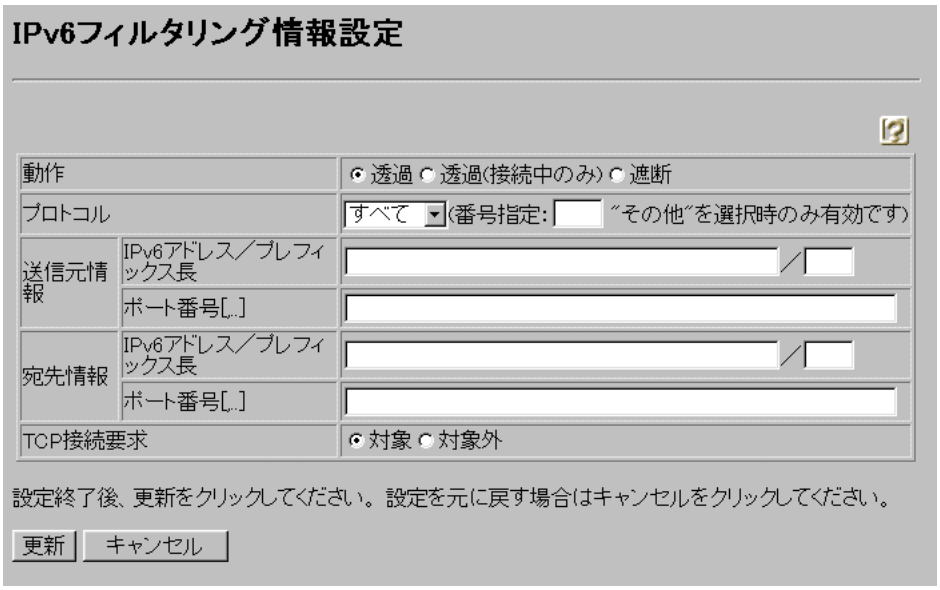
デフォルトルート、またはネットワーク指定を選択し、宛先および中継先のネットワークを指定します。ネットワーク指定は、指定するネットワークを宛先に持つパケットの転送先を指定するもの、デフォルトルートは、ネットワーク指定されていない宛先を持つパケットの転送先を指定するものです。

メトリック値

メトリック値を選択します。これは、ここで設定するルーティング情報をRIPngで送信するときに加算されます。

IPv6フィルタリング情報

【操作】「詳細設定メニュー」→ルータ設定「相手情報」→［ネットワーク情報一覧］→［IPv6フィルタリング情報一覧］



優先順位の高い定義より順にパケットのチェックを行い、すべての条件が一致する場合に定義する動作を行います。

動作

IPv6フィルタリングの動作を以下の3つから選択します。

透過

条件と一致する場合にパケットを透過します。

透過（接続中のみ）

条件と一致する場合に、ISDN回線が接続しているときはパケットを透過します。切断しているときは遮断します。

遮断

条件と一致する場合にパケットを遮断します。

プロトコル

プロトコルを以下の5つから選択します。

・TCP　（6）

・UDP　（17）

・ICMPv6（58）

・すべて　（255）

・その他

プロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、0～255の範囲で指定します。

送信元／宛先情報

IPv6アドレス／プレフィックス長

IPv6アドレス、およびプレフィックス長を指定します。チェック対象となるパケットのIPv6アドレスと、定義するIPv6アドレスとプレフィックス長の論理積が等しい場合に条件に一致します。

ポート番号

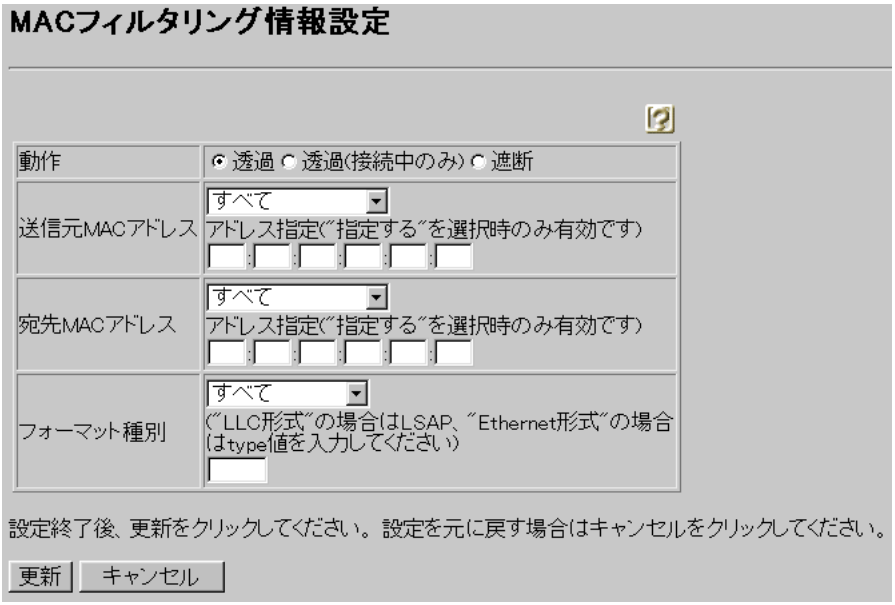
ポート番号を10進数を使用して、1～65535の範囲、または'any'で指定します。'any'を指定する場合は、すべてのポート番号がフィルタリングの対象となります。また、ポート番号を複数指定する場合は、','で区切ります。範囲指定の場合は、'-'で区切ります。送信元情報と宛先情報を合わせて10組まで設定できます。

TCP接続要求

TCPプロトコルでのコネクション接続要求をフィルタリングの対象に含めるかどうかを選択します。

MACフィルタリング情報設定

【操作】「詳細設定メニュー」→ルータ設定「相手情報」→［ネットワーク情報一覧］→［MACフィルタリング情報一覧］



WANモジュールで送受信するときにフィルタリング処理をします。優先順位の高い定義より、順にパケットをチェックします。フィルタリング条件が一致する場合に定義する動作を行います。

動作

フィルタリング条件に一致するときのMACフィルタリングの動作を以下の3つから選択します。

透過

フィルタリング条件と一致する場合に、透過します。

透過（接続中のみ）

フィルタリング条件と一致する場合に、回線が接続しているときは、透過します。切断しているときは、破棄します。

遮断

フィルタリング条件と一致する場合に、遮断します。

送信元／宛先MACアドレス

MACアドレスを以下の項目から選択します。“指定する”を選択する場合は、アドレス指定にMACアドレスを16進数で指定します。

すべて
すべてのMACアドレスを対象とします。

ブロードキャスト
ブロードキャストMACアドレスを対象とします。

マルチキャスト
ブロードキャストMACアドレスおよびマルチキャストMACアドレスを対象とします。

指定する
アドレス指定に指定するMACアドレスを対象とします。

フォーマット種別
フィルタリング対象のフォーマットを以下の項目から選択します。LLC形式の場合は、LSAPを16進数を使用して、0～ffffの範囲で指定し、“Ethernet形式”の場合は、type値を16進数を使用して、5dd～ffffの範囲で指定します。

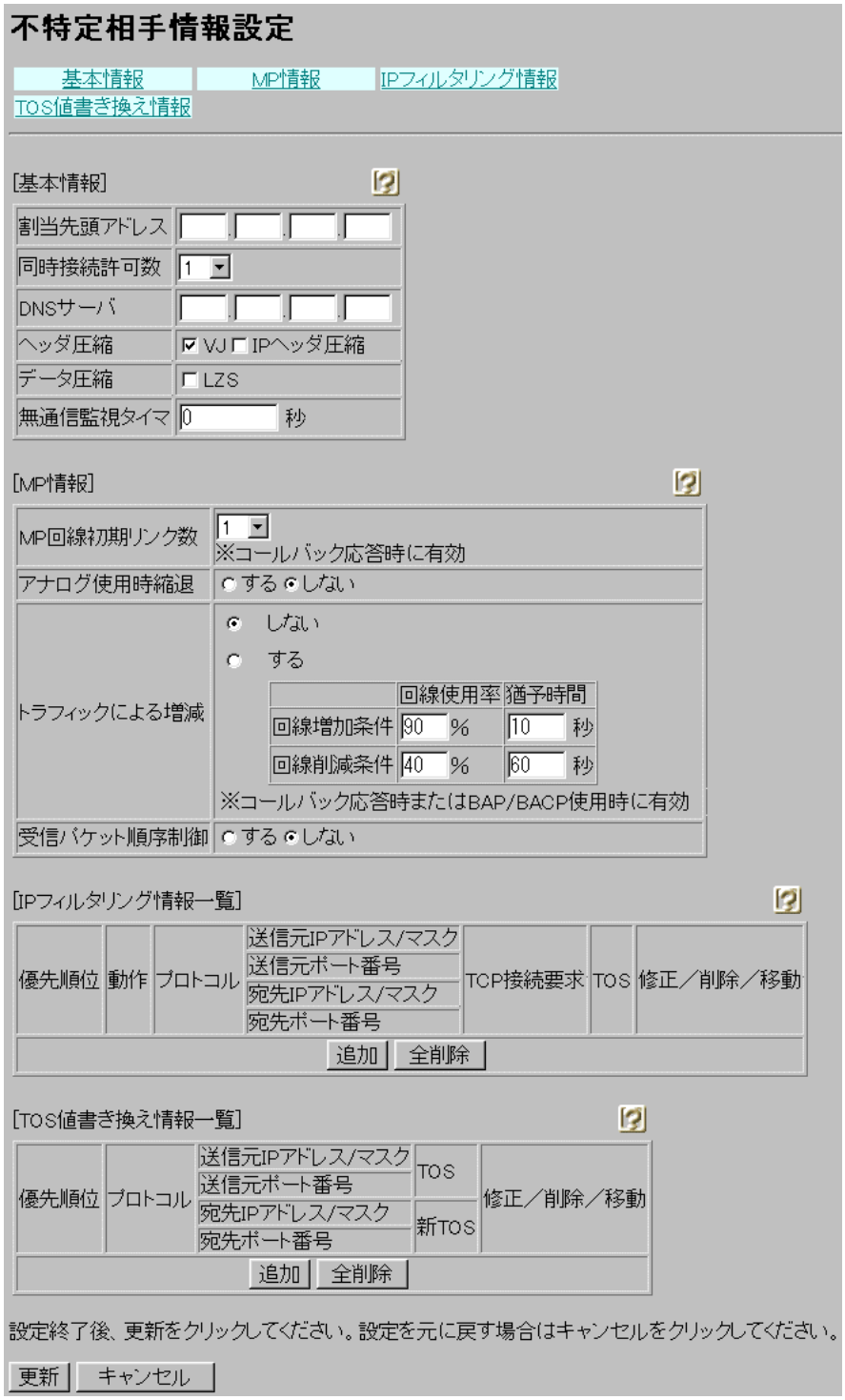
LLC形式
LLC形式のパケットを対象とします。

Ethernet形式
Ethernet形式のパケットを対象とします。

すべて
すべてのパケットを対象とします。

不特定相手情報設定

【操作】「詳細設定メニュー」→ルータ設定「相手情報」→［ネットワーク情報一覧］



[基本情報]

相手情報で定義したどの相手とも判断できない着信相手に対する動作に関する情報を設定します。

割当先頭アドレス

着信相手に対して、割り当てる先頭のIPアドレスを指定します。同時接続許可数と組み合わせて範囲（許可数）を指定します。

割当先頭アドレスを省略する場合は、不特定相手からの着信は行われません。

同時接続許可数

割当先頭アドレスを先頭に、相手に割り当てる同時接続許可数を選択します。

DNSサーバ

相手から要求がある場合に、通知するDNSサーバのIPアドレスを指定します。

ヘッダ圧縮

送受信するヘッダを圧縮します。ヘッダ圧縮のアルゴリズムは、VJヘッダ圧縮（RFC1144に準拠）およびIPヘッダ圧縮（RFC2507／RFC2508に準拠）をサポートします。使用する指定の場合も、実際にヘッダ圧縮を行うかどうかは、相手ホストとのネゴシエーションで決まります。

データ圧縮

送受信するデータを圧縮します。データ圧縮のアルゴリズムは、LZSをサポートします。使用する指定の場合も、実際にデータ圧縮を行うかどうかは、相手ホストとのネゴシエーションで決まります。

無通信監視タイマ

ISDN回線の無通信監視タイマを0～3600秒の範囲で指定します。その時間を超えても、通信が行われない場合は、ISDN回線を自動的に切断します。なお、0を指定した場合は、自動切断を行いません。

[MP情報]

MP（MultilinkPPP）の情報を設定します。

MP回線初期リンク数

回線接続時に接続するチャネル数を選択します。

アナログ使用時縮退

アナログ使用時縮退を行うかどうかを選択します。

アナログ使用時縮退は、MPで2本のチャネルを使用している時に、アナログ電話がかかってきたり、アナログ電話の受話器を上げたりする場合に、チャネルを1本に減らしてアナログ機器を使用することができます。

トラフィックによる増減

回線負荷に応じて帯域幅（1B、2B）を自動的にコントロールする機能を使用するかどうかを選択します。使用する場合は、回線増減の条件も指定します。指定する回線使用率を超える（削減の場合は下回った）状態が“猶予時間”以上続く時点で、回線の接続（削減の場合は切断）を行います。回線使用率は0～100%、猶予時間は0～3600秒の範囲で指定します。

受信パケット順序制御

MPを使用する場合は、必ず“する”をチェックします。しない”をチェックすると、MPとヘッダ圧縮（VJ）を併用する場合にヘッダ圧縮（VJ）が無効になります。

[IPフィルタリング情報一覧]

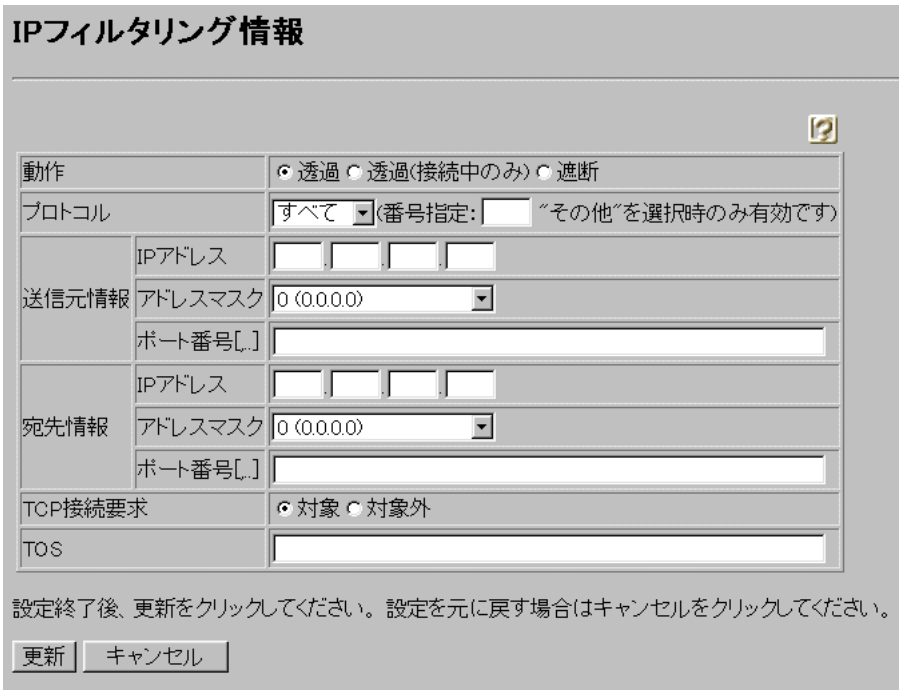
現在、設定されているIPフィルタリング情報の一覧です。処理は優先順位1から順に行います。IPフィルタリングの定義は装置全体で64個まで設定できます。処理するボタンをクリックし、次のページに進みます。

[TOS値書き換え情報一覧]

現在、設定されているTOS値書き換え情報の一覧です。処理は優先順位1から順に行います。TOS値書き換えの定義は装置全体で32個まで設定できます。処理するボタンをクリックし、次のページに進みます。

IPフィルタリング情報（不特定相手情報）

【操作】「詳細設定メニュー」→ルータ設定「相手情報」→［ネットワーク情報一覧］→［IPフィルタリング情報］



優先順位の高い定義より順にパケットのチェックを行い、すべての条件が一致する場合に定義する動作を行います。ただし、分割されたパケットに対しては正しく扱えません。

動作

IPフィルタリングの動作を以下の3つから選択します。

透過

条件と一致する場合にパケットを透過します。

透過（接続中のみ）

条件と一致する場合に、ISDN回線が接続しているときは、パケットを透過します。切断しているときは、遮断します。

遮断

条件と一致する場合にパケットを遮断します。

プロトコル

フィルタリング条件としてプロトコルを以下の6つから選択します。

・すべて　（0）

・TCP　（6）

・UDP　（17）

・ICMP　（1）

・IPv6 over IPv4　（41）

・その他

プロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、0～255の範囲で指定します。

送信元／宛先情報

IPアドレス／アドレスマスク

フィルタリング条件としてのIPアドレス、およびアドレスマスクを指定します。

チェック対象となるパケットのIPアドレスと、定義するIPアドレスとアドレスマスクの論理積が等しい場合に条件に一致します。

ポート番号

フィルタリング条件としてポート番号を10進数を使用して、1～65535の範囲、または'any'で指定します。'any'を指定する場合は、すべてのポート番号をフィルタリングの対象とします。また、ポート番号を複数指定する場合は、','で区切ります。範囲指定の場合は、'-'で区切ります。送信元情報と宛先情報を合わせて10組まで設定できます。

TCP接続要求

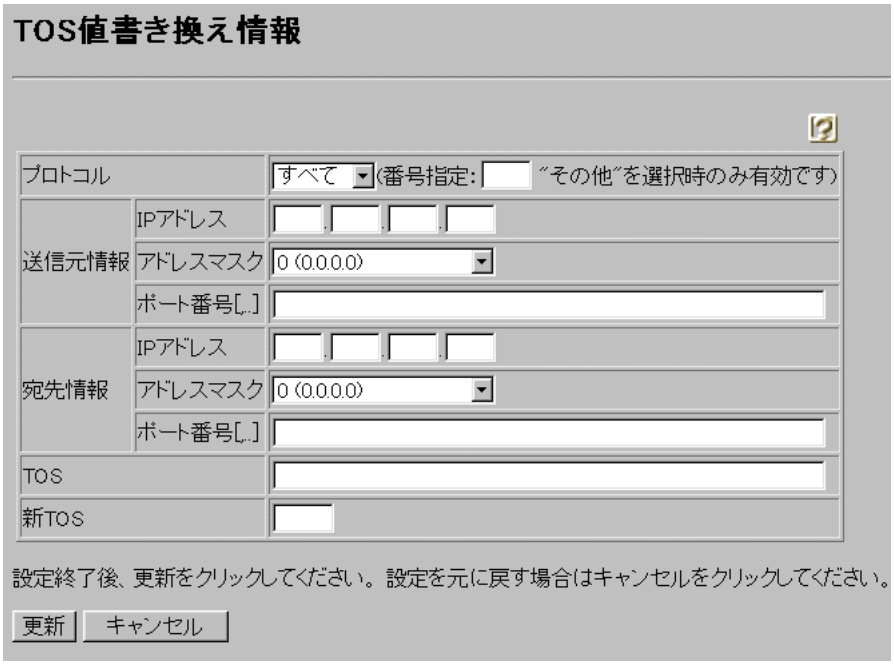
TCPプロトコルでのコネクション接続要求をフィルタリングの対象に含めるかどうかを選択します。

TOS

IPパケットのTOSフィールド値を16進数を使用して、0～ffの範囲、または'any'で指定します。TOSフィールド値を複数指定する場合は、','で区切ります。範囲指定の場合は、'-'で区切ります。10組まで設定できます。何も設定しない場合は、すべてのTOSフィールド値をフィルタリングの対象とします。

TOS値書き換え情報（不特定相手情報）

【操作】「詳細設定メニュー」→ルータ設定「相手情報」→［ネットワーク情報一覧］→［TOS書き換え情報一覧］



［TOS値書き換え情報］

優先順位の高い定義より順にパケットのチェックを行い、すべての条件が一致する場合に定義するTOS値書き換えを行います。ただし、分割されたパケットに対しては正しく扱えません。

プロトコル

TOS値書き換えの条件としてプロトコルを以下の6つから選択します。

・すべて　(0)
・TCP　(6)
・UDP　(17)
・ICMP　(1)
・IPv6 over IPv4　(41)
・その他

プロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、0～255の範囲で指定します。

送信元／宛先情報

IPアドレス／アドレスマスク

TOS値書き換え条件としてのIPアドレス、およびアドレスマスクを指定します。

チェック対象となるパケットのIPアドレスと、定義するIPアドレスとアドレスマスクの論理積が等しい場合に条件に一致します。

ポート番号

TOS値書き換え条件としてポート番号を10進数を使用して、1～65535の範囲、または'any'で指定します。'any'を指定する場合は、すべてのポート番号がTOS書き換えの対象となります。また、ポート番号を複数指定する場合は、','で区切ります。範囲指定の場合は、'-'で区切ります。送信元情報と宛先情報で合わせて10組まで設定できます。

TOS

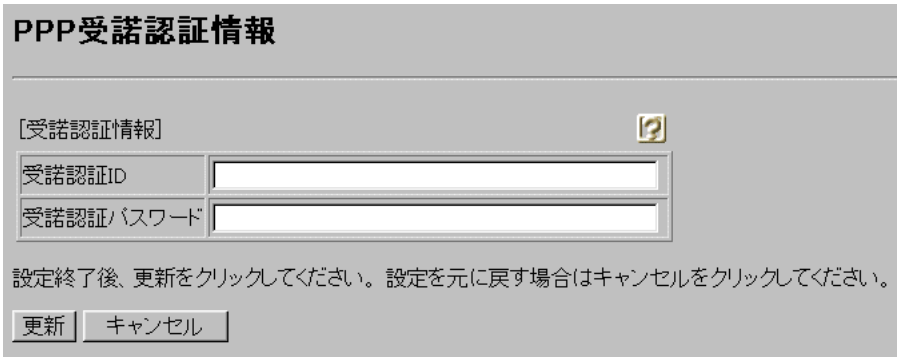
TOS値書き換えの条件としてIPパケットのTOSフィールド値を16進数を使用して、0～ffの範囲、または'any'で指定します。TOSフィールド値を複数指定する場合は、','で区切ります。範囲指定の場合は、'-'で区切ります。10組まで設定できます。何も設定しない場合は、すべてのTOSフィールド値を書き換えの対象とします。

新TOS

IPパケットに新しく設定するTOSフィールド値を16進数を使用して、0～ffの範囲で指定します。

PPP受諾認証情報

【操作】「詳細設定メニュー」→ルータ設定「相手情報」→［受諾認証ID情報一覧］



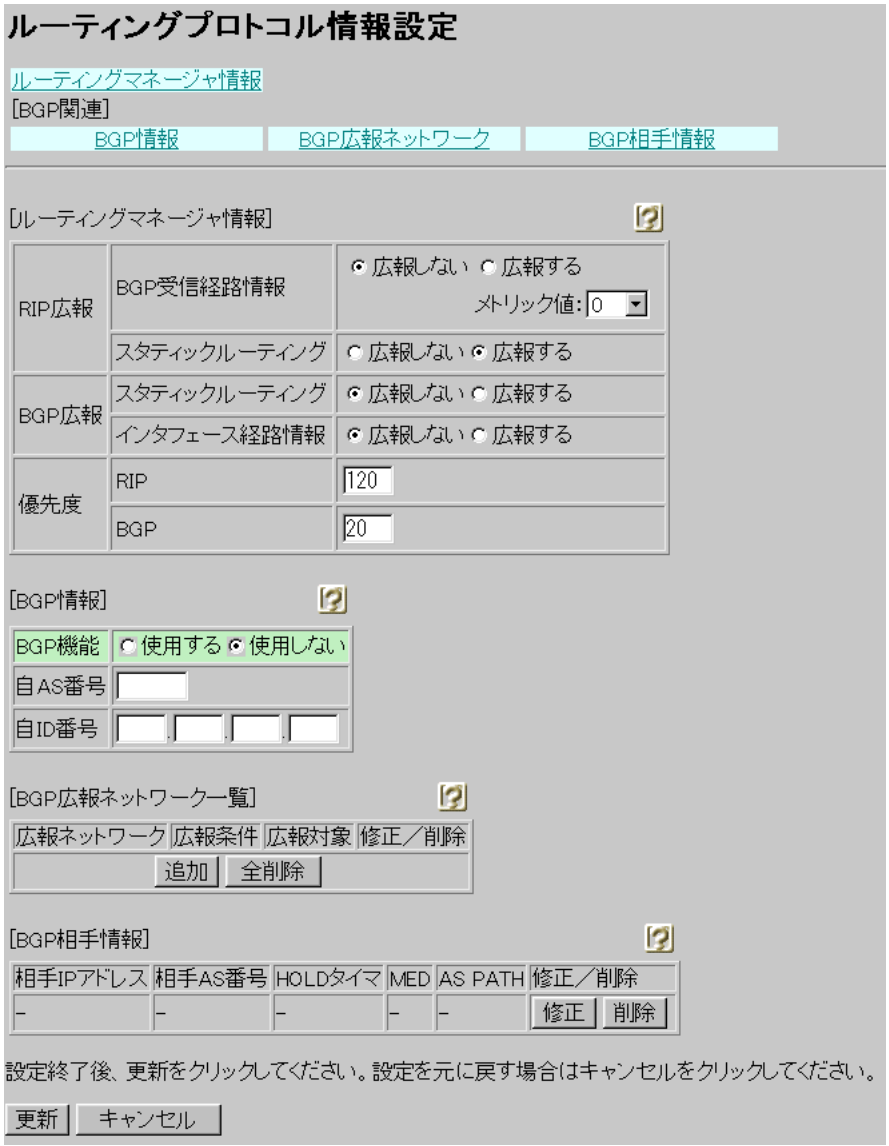
［受諾認証情報］

主に不特定相手からの着信時の認証に使用する情報です。

着信時に受け付ける相手の認証IDとパスワードをそれぞれ64桁以内で指定します。

ルーティングプロトコル情報設定

【操作】「詳細設定メニュー」→ルータ設定「ルーティングプロトコル情報」



[ルーティングマネージャ情報]

RIP広報

RIPで広報する経路情報を選択します。

BGP受信経路情報

BGPの持つ経路情報を広報します。

メトリック値

BGPの経路情報に設定するメトリック値を0～16の範囲で選択します。

スタティックルーティング情報

本装置に設定されているスタティックルーティングの経路情報を広報します。

こんな事に気をつけて

RIPでは、インタフェースが接続されているネットワークの経路情報は常に広報され、広報しないようにすることはできません。

BGP広報

BGPで広報する経路情報を選択します。

スタティックルーティング情報

本装置に設定されているスタティックルーティングの経路情報を広報します。

こんな事に気をつけて

- **スタティックルーティングの経路情報を広報する場合は、同じ宛先の経路情報をBGPで受信するとスタティックルーティングの経路情報を優先します。**
- **デフォルトルートをBGPで広報する場合は、BGP相手情報設定でデフォルトルートを“広報する”に設定してください。**

インタフェース経路情報

インタフェースが接続されているネットワークの経路情報を広報します。

優先度

複数のルーティングプロトコルで同じ経路情報を受信した場合や受信した経路情報がスタティックルーティングで設定している経路情報と同じだった場合、どの経路情報を優先的に使用するかを優先度で判断します。

優先度を10進数を使用して、1～254の範囲で指定します。なお、優先度は小さい方が高い優先度を示します。

こんな事に気をつけて

- **優先度はほかのプロトコルやスタティックルーティングに設定されている値と同じ値は指定しないでください。**
- **各ルーティングプロトコルで受信する経路、およびスタティック経路には優先度（distance）があり、初期値はスタティック経路が0、BGP（EBGP）が20、RIPが120です。**
  Geostream Rシリーズ・LR-Xシリーズの初期値と異なっており、優先度の変更を行う場合、初期値に違いがあることに注意してください。
  ルーティングプロトコル情報設定画面、ルーティング情報設定（LAN情報）画面、ルーティング情報設定（ネットワーク情報）画面、およびroutemanage distanceコマンド、lan ip route, remote ip routeコマンドで優先度をGeostream Rシリーズ・LR-Xシリーズに合わせることができます。

[BGP情報]

BGPを使って経路広報を行うかどうかを選択します。

こんな事に気をつけて

- **本装置では、IP-VPNサービスへのアクセスプロトコルでだけBGPが使用できます。**
- **バージョン4だけをサポートしています。**
- **BGPの認証機能はサポートしていません。**
- **利用できるセッションはE-BGPとして1つだけです。I-BGPは使用できません。**
- **WAN側IPアドレスを必ず設定してください。**
- **BGPでは、インタフェースの状態にかかわらず、経路情報を広報します。たとえば、BGPで、広報用にスタティック経路情報やインタフェースの経路情報を設定しておくと、ケーブル抜けなどが発生した場合にも、経路情報を広報します。**
- **経路情報を、ルーティング情報の最大値まで保持している場合、受信したBGPパケットは破棄されます。破棄されたBGPパケットの経路情報は、その後、ルーティング情報に空きができた場合でも、ルーティング情報に反映されません。**
- **NATは同時に使用できません。**

⚠注意

WAN回線で使用する場合は、専用回線でだけ使用することができます。ISDN（回線交換）でBGPを使用した場合、思わぬ課金（定期発信または長時間接続）が発生します。

自AS番号

本装置の属するAS番号を10進数を使用して、1～65535の範囲で指定します。

自ID番号

本装置を一意に示すIDを指定します。指定するIDはほかのルータと重複しないIDをドット形式で指定します。一般的には自装置のIPアドレス（IPv4）を指定します。

省略時または0.0.0.0を指定する場合、自装置のインタフェースに指定したIPアドレスの中でもっとも大きい値をIDとして使用します。

[BGP広報ネットワーク一覧]

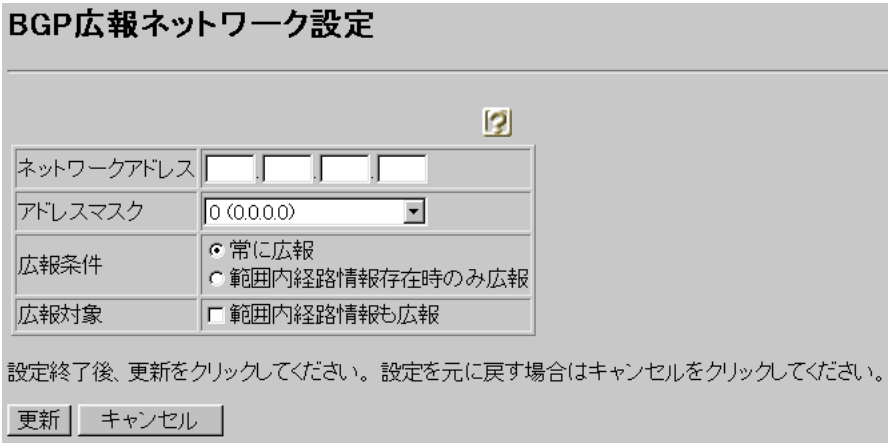
現在、設定されている相手装置に広報するネットワークと広報する形態の一覧です。広報ネットワークの定義は装置全体で16個まで設定できます。処理するボタンをクリックし、次のページに進みます。

[BGP相手情報]

現在、設定されているBGPの相手情報です。BGPの相手情報の定義は装置全体で1個設定できます。処理するボタンをクリックし、次のページに進みます。

BGP広報ネットワーク設定

【操作】「詳細設定メニュー」→ルータ設定「ルーティングプロトコル情報」→［BGP広報ネットワーク一覧］



このページでは、BGP相手装置に広報するネットワーク情報と広報する形態を設定できます。

ネットワークアドレス／アドレスマスク

BGPを使用して広報するネットワークのアドレスとアドレスマスクを指定します。

ネットワークアドレスにデフォルトルートを示す0.0.0.0は設定できません。

こんな事に気をつけて

指定したネットワークアドレス／アドレスマスクよりも長いサブネットマスクの経路情報は、受信することができません。

広報条件

指定したネットワークアドレス／アドレスマスクを広報する条件を以下から選択します。

常に広報

指定したネットワークアドレス／アドレスマスクを常に広報します。

範囲内経路情報存在時のみ広報

BGPで広報する経路情報の中に、指定したネットワークアドレス／アドレスマスクの範囲内のものがある場合だけ、指定したネットワークアドレス／アドレスマスクを広報します。

広報対象

BGPで広報する経路情報の中に、指定したネットワークアドレス／アドレスマスクの範囲内のものがある場合、その経路情報も合わせて広報するかどうかを選択します。

チェックボックスをチェックしていない場合

指定したネットワークアドレス／アドレスマスクを広報します。BGPで広報する経路情報の中に、指定したネットワークアドレス／アドレスマスクの範囲内のものがあっても、その経路情報は広報しません。

チェックボックスをチェックした場合

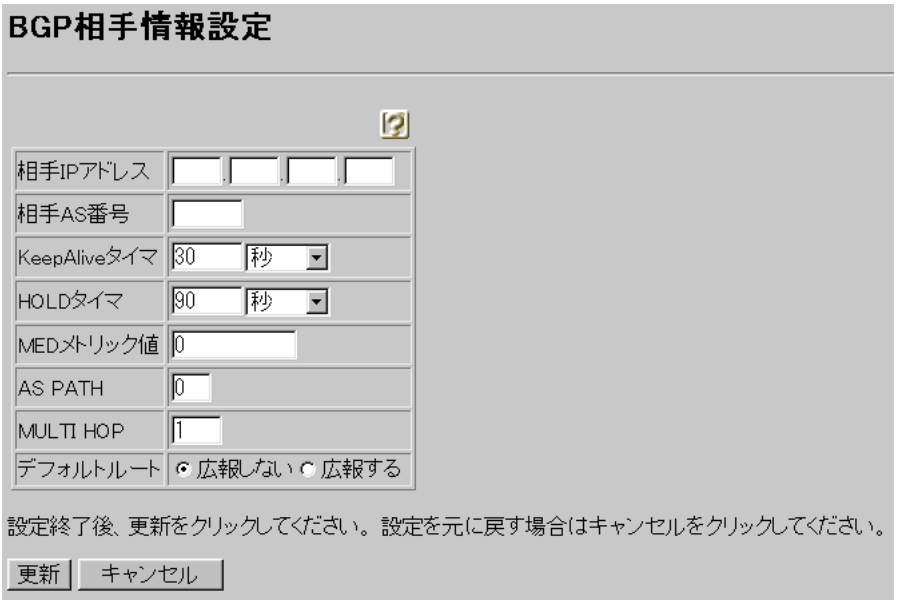
指定したネットワークアドレス／アドレスマスクを広報します。BGPで広報する経路情報の中に、指定したネットワークアドレス／アドレスマスクの範囲内のものがあった場合、その経路情報も広報します。

こんな事に気をつけて

BGPで広報する経路情報は、「ルーティングプロトコル情報設定」の［ルーティングマネージャ情報］のBGP広報で“広報する”を設定したものが対象となります。RIPの経路情報は対象にはなりません。

BGP相手情報設定

【操作】「詳細設定メニュー」→ルータ設定「ルーティングプロトコル情報」→［BGP相手情報］



このページでは、BGP広報を行う相手装置の情報を設定できます。

相手IPアドレス

BGP広報する相手装置のIPアドレスを指定します。BGP相手装置とルータを経由して接続する場合は、経由するルータの数をMULTI HOPに加算して指定します。また、WAN側のIPアドレスにLAN側のIPアドレスを指定している場合は、MULTI HOPを1加算して指定します。

相手AS番号

BGP広報する相手装置のAS番号を10進数を使用して、1～65535の範囲で指定します。指定するAS番号は、自AS番号と異なる番号を指定します。

KeepAliveタイマ

無通信状態のとき、相手装置との通信可否を確認するために送信するKeep Aliveメッセージのタイマを設定します。

以下の範囲でKeep Aliveタイマ値を指定します。

有効範囲）
1～18時間
1～1092分
1～65535秒

こんな事に気をつけて

Keep Alive タイマの値は、HOLD タイマより小さい値を指定してください。

HOLDタイマ

相手装置との間で、通信異常と判断する無通信状態の時間（タイマ）を指定します。このタイマ値は、相手装置とのネゴシエーションで決まり、装置間でより小さな値が使用されます。以下の範囲でHOLDタイマ値を指定します。

有効範囲）
1～18時間
1～1092分
3～65535秒

こんな事に気をつけて

相手装置とのネゴシエーションによって、相手装置のHoldタイマ値が使用された場合は、その値の3分の1の値がKeepAliveタイマとして使用されます。

MEDメトリック値

相手装置へ広報する経路情報に付加するMEDメトリック値を10進数を使用して、0～4294967295の範囲で指定します。

AS PATH

BGPで広報する経路情報に付加するAS番号の個数を10進数を使用して、0～4の範囲で指定します。

MULTI HOP

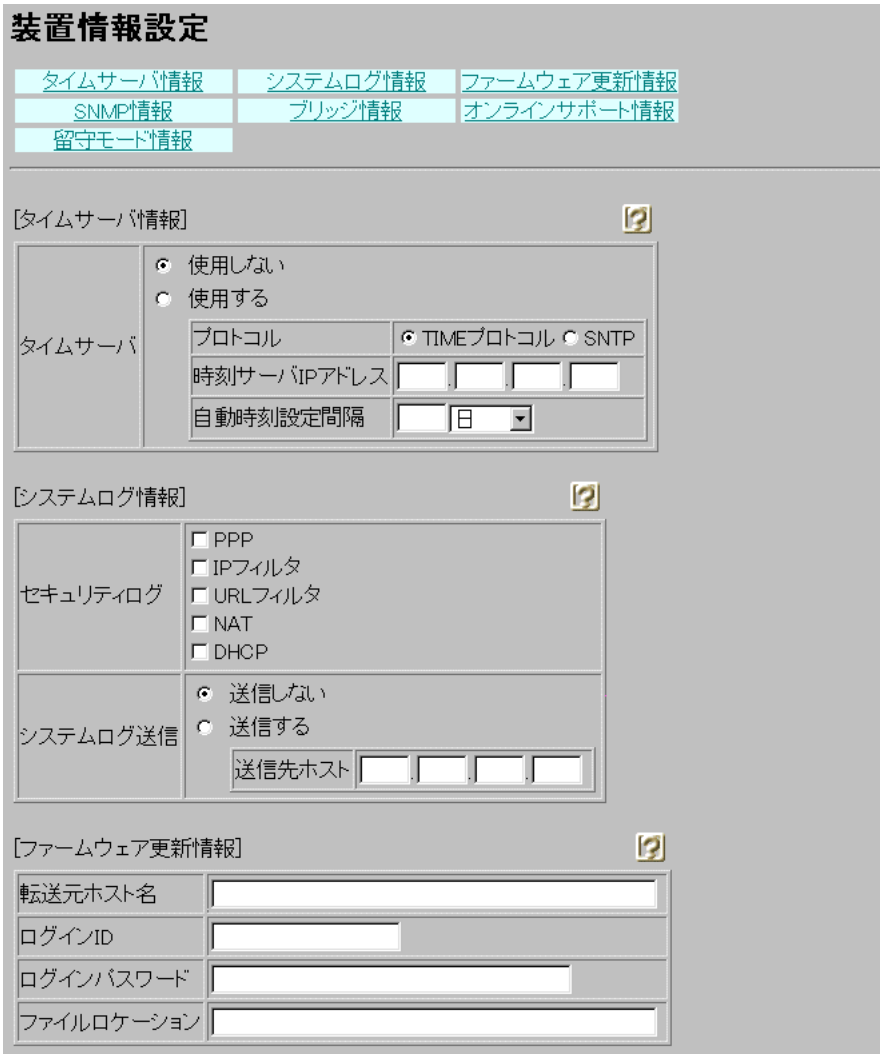
相手装置とBGP接続する場合のIPパケットのTTL値を10進数を使用して、1～255の範囲で指定します。

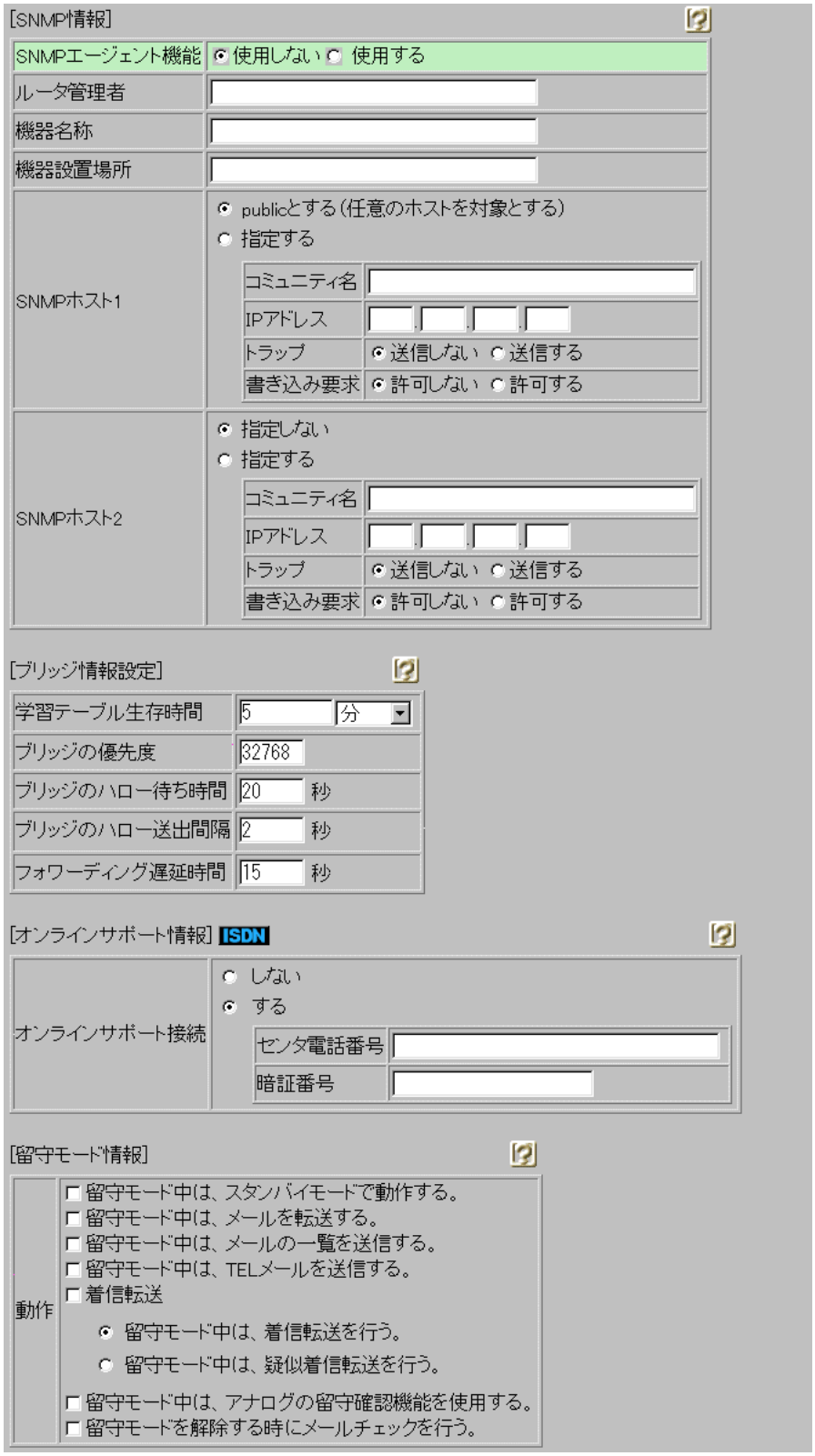
デフォルトルート

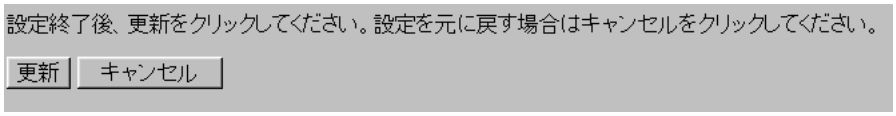
BGPでデフォルトルートの広報を許可するかどうかを選択します。対象となるデフォルトルートにはスタティックルーティング情報があります。

装置情報設定

【操作】「詳細設定メニュー」→ルータ設定「装置情報」




[SNMP情報]
SNMPエージェント機能
使用しない
使用する
ルータ管理者
機器名称
機器設置場所
SNMPホスト1
publicとする（任意のホストを対象とする）
指定する
コミュニティ名
IPアドレス
トラップ
送信しない
送信する
書き込み要求
許可しない
許可する
SNMPホスト2
指定しない
指定する
コミュニティ名
IPアドレス
トラップ
送信しない
送信する
書き込み要求
許可しない
許可する
[ブリッジ情報設定]
学習テーブル生存時間
5
分
ブリッジの優先度
32768
ブリッジのハロー待ち時間
20
秒
ブリッジのハロー送出間隔
2
秒
フォワーディング遅延時間
15
秒
[オンラインサポート情報]
ISDN
オンラインサポート接続
しない
する
センタ電話番号
暗証番号
[留守モード情報]
動作
留守モード中は、スタンバイモードで動作する。
留守モード中は、メールを転送する。
留守モード中は、メールの一覧を送信する。
留守モード中は、TELメールを送信する。
着信転送
留守モード中は、着信転送を行う。
留守モード中は、疑似着信転送を行う。
留守モード中は、アナログの留守確認機能を使用する。
留守モードを解除する時にメールチェックを行う。



[タイムサーバ情報]

本装置は、ネットワーク上のタイムサーバから時刻情報を取得し、内部時計を自動的に設定できます。

タイムサーバ

タイムサーバから時刻情報を取得する場合は、“使用する”を選択し、以下の情報を設定します。

プロトコル

使用するプロトコルを選択します。

時刻サーバのIPアドレス

タイムサーバのIPアドレスを指定します。

自動時刻設定間隔

タイムサーバから定期的に時刻情報を取得するときの取得周期を0～10日の範囲で指定します。0を指定すると、起動（再起動）時だけ時刻情報を取得します。

[システムログ情報]

セキュリティログ

不正アクセスのログ情報やIPフィルタ、URLフィルタ、NATにより遮断されるパケットのログ情報、DHCPサーバが割り当てるIPアドレスログを採取します。採取する項目を指定します。

システムログ送信

本装置は、syslog形式でシステムログサーバにシステムログ情報を送信します。送信する場合は、“送信する”を選択し、システムログサーバにシステムログ情報を送信する送信先のIPアドレスを指定します。

[ファームウェア更新情報]

ファームウェアを入れ替えたり、レベルアップを行うときに、転送元となるホストに接続するための情報を設定します。ファームウェアの更新操作はメンテナンスメニューから行うことができます。

転送元ホスト名

更新用ファームウェアが存在するホスト名を半角英数字128文字以内で指定します。

ドット形式のIPアドレスを指定することもできます。

こんな事に気をつけて

ProxyDNSが設定されていない場合、ホスト名指定によるファームウェア更新はできません。

ログインID

更新用ファームウェアのログインIDを16文字以内で指定します。

ログインパスワード

更新用ファームウェアのパスワードを32文字以内で指定します。

ファイルロケーション

更新用ファームウェアのロケーションを80文字以内で指定します。

[SNMP情報]

SNMPエージェント機能

SNMPエージェント機能を使用すると、SNMPマネージャの動作しているほかのシステムから本装置の状態を監視することができます。SNMPエージェント機能を使用する場合は、“使用する”を選択し、以下の項目を設定します。

ルータ管理者

本装置の管理者名を半角英数字40文字以内で指定します。ただし、空白文字は使用できません。区切り文字は“_”や“.”を使用します。

機器名称

本装置の名称を半角英数字32文字以内で指定します。ただし、空白文字は使用できません。

機器設置場所

本装置の設置場所を半角英数字72文字以内で指定します。ただし、空白文字は使用できません。

SNMPホスト

SNMPによるアクセスを許可するホストを指定します。ホストは2つまで指定できます。“publicとする”を選択すると、コミュニティ名“public”で任意のホストからのアクセスを許可します。コミュニティ名を変更する場合やホストを限定する場合は、“指定する”を選択し、コミュニティ名・IPアドレス・トラップ送信可否を指定します。

コミュニティ名

SNMPにより情報交換するグループのコミュニティ名を半角英数字32文字以内で指定します。

IPアドレス

SNMPによるアクセスを許可するホストのIPアドレスを指定します。“0.0.0.0”を指定すると、任意のホストのアクセスを許可します。

トラップ

このSNMPホストにトラップを送信するかどうかを選択します。ただし、任意のホスト（0.0.0.0）を指定している場合は、トラップの送信は行われません。

書き込み要求

このSNMPホストから書き込み要求を許可するかどうかを選択します。ただし、任意のホスト（0.0.0.0）を指定する場合は、書き込み要求は許可されません。

[ブリッジ情報設定]

ブリッジ情報設定項目はブリッジ機能を使用する場合だけ有効です。

学習テーブル生存時間

以下の範囲で学習テーブル生存時間を指定します。

有効範囲）
1～11日
1～277時間
1～16666分
10～1000000秒

ブリッジの優先度

ルートブリッジ決定アルゴリズムで使用するブリッジの優先度を0～65535の範囲で指定します。ブリッジの優先度は値の小さい方が優先となります。この設定はSTPを使用する場合だけ有効です。

ブリッジのハロー待ち時間

ルートブリッジ、または代表ブリッジが送出する構成情報BPDUの待ち時間を6～40秒の範囲で指定します。この設定はSTPを使用する場合だけ有効です。

ブリッジのハロー送出間隔

ルートブリッジになった時に送出する構成情報BPDUの送出間隔を1～10秒の範囲で指定します。この設定はSTPを使用する場合と本装置がルートブリッジとして動作する場合だけ有効です。

フォワーディング遅延時間

構成情報BPDUが一番時間のかかる経路に届く時間を指定します。フォワーディング遅延時間を4～30秒の範囲で指定します。この設定はSTPを使用する場合と本装置がルートブリッジとして動作する場合だけ有効です。

[オンラインサポート情報]

オンラインサポート接続

オンラインサポート接続をするかどうかを選択します。センタ側からのオンラインサポート接続を許可する場合には“する”を選択し、拒否する場合には“しない”を選択します。オンラインサポート接続を許可するときにセンタ電話番号と暗証番号のどちらも指定していない場合、LANポート用のMACアドレスを認証に使用されます。

センタ電話番号

オンラインサポートを受け付ける相手電話番号を32桁以内で指定します。

暗証番号

オンラインサポートを受け付ける相手との暗証番号を半角英数字19桁以内で指定します。

ヒント

◆ オンラインサポートとは

ISDN回線に接続した遠隔地（リモート側）の本装置を、管理者側（センタ側）の本装置を使用して直接設定する機能です。本機能ではPPPによるIP接続を必要としないので、ご購入時の状態のまま、本装置を設定することができます。ただし、専用線（HSD）では使用できません。

以下の手順で設定を行うことができます。

1）WWWブラウザを使用してセンタ側の本装置のトップメニューを開きます。

2）「メンテナンスメニュー」の「オンラインサポート」で、リモート側の電話番号と暗証番号を指定し、[オンラインサポート開始] ボタンをクリックします。

3）正常に接続したあとは、センタ側の本装置を設定するのと同様の手順でリモート側の設定を行うことができます。

4）「メンテナンスメニュー」の「オンラインサポート」で、[オンラインサポート終了] ボタンをクリックしてオンラインサポートを終了します。

⚠注意

本機能を使用して発信するにはINSネット64の「ユーザ間情報通知サービス」を使用するため、1回の発信につき1メッセージ分の料金が通信料金とは別にかかります。

こんな事に気をつけて

- **オンラインサポート中は、ISDN 回線は接続されたままとなります。無通信監視タイマによる自動切断は行われません。設定終了後は必ずオンラインサポートを終了し回線が切断されたことを確認します。**
- **暗証番号にはリモート側の本装置に設定された暗証番号を指定します。一致しない場合は、接続できません。なお、リモート側の本装置がご購入時の状態、またはオンラインサポート情報未設定の場合は、暗証番号として MAC アドレスを指定することにより接続できます。MAC アドレスは装置底面に表記されているとおり半角小文字の英数字で指定します。**
- **本機能を利用する際には、センタ側とリモート側に同一機種の本装置を使用します。ただし、バージョンが異なる場合、設定できない項目もあります。**

[留守モード情報]

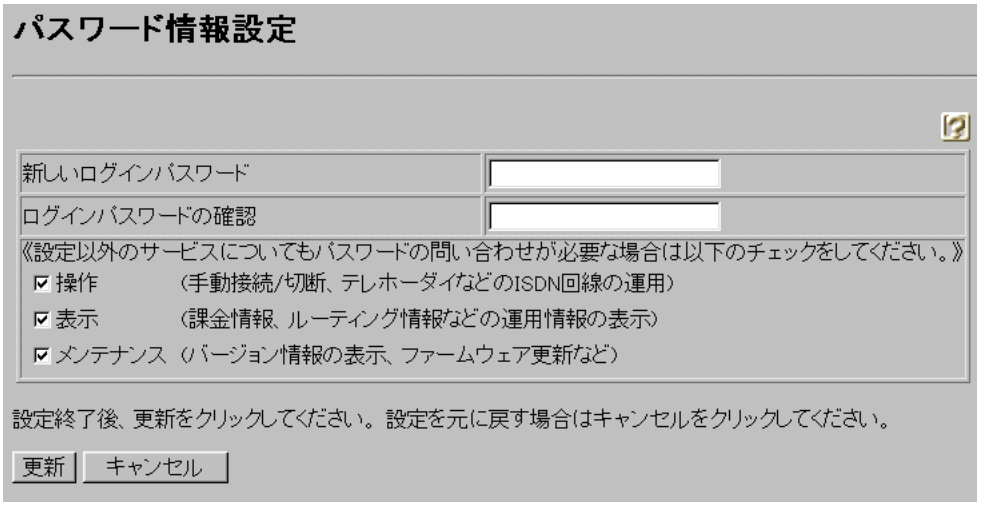
留守モードに割り当てる動作を選択します。装置のアナログポートに接続されている電話機、操作メニュー、またはスケジュール機能により、留守モードの切り替えができます。

こんな事に気をつけて

- **留守モード中に電源を切ると留守モードが解除された状態になります。**
- **留守モード中に設定変更を行った場合、留守モードで設定された内容と違う動作をする場合があります。**
- **回線情報の回線インタフェースが ISDN 以外で動作している場合は、「留守モード中は、スタンバイモードで動作する」は、無効になります。**

パスワード情報設定

【操作】「詳細設定メニュー」→ルータ設定「パスワード情報」



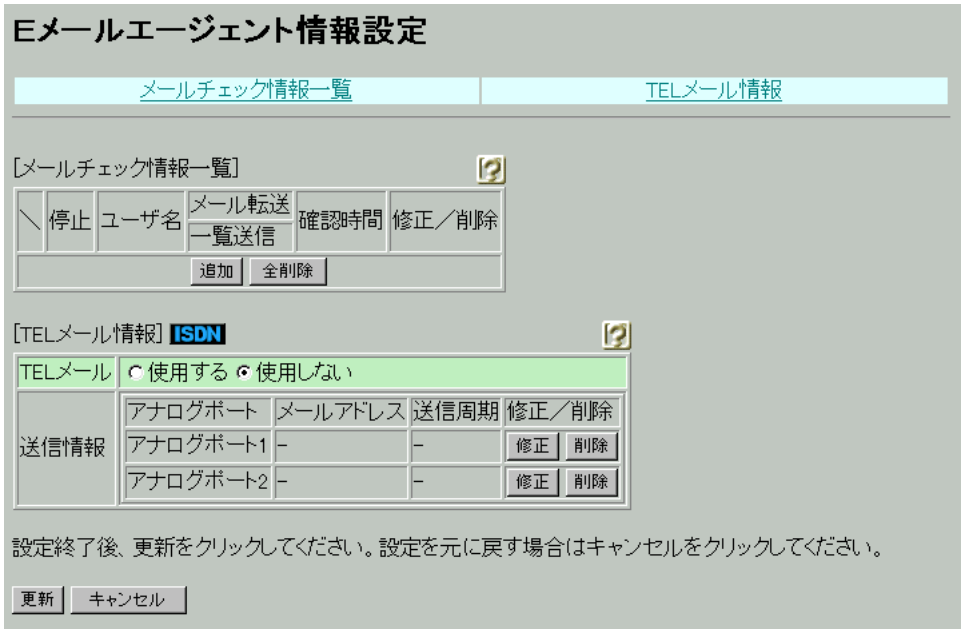
本装置を操作するときのパスワードを半角英数字16文字以内で指定します。パスワード入力によって操作の制限が解除される時間は10分間です。それ以降の操作では再びパスワードが要求されます。

なお、パスワードは更新直後から有効になります。

操作メニュー、表示メニュー、メンテナンスメニューの操作に関しても、パスワードが必要な場合は、必要な項目を選択します。

Eメールエージェント情報設定

【操作】「詳細設定メニュー」→ルータ設定「Eメールエージェント情報」



4

ヒント

◆Eメールエージェント機能には以下の機能があります。

・メールチェック機能

メールチェックとは、POP3プロトコルを使用して、指定時間にPOP3サーバにメールが到着しているかどうかを確認する機能です。メールが到着していれば、メールの件数、差出人、題名、送信時刻を取得します。

・メール転送機能

指定時刻になるとPOP3サーバに到着しているメールを指定したメールアドレスに転送する機能です。

・メール一覧送信機能

指定時刻になるとPOP3サーバに到着しているメールの一覧情報を指定したメールアドレスに転送する機能です。

・TELメール機能

アナログポートの着信履歴を着信ごと、または一定時間ごとにメールで送信する機能です。

[メールチェック情報一覧]

現在、設定されているメールチェック情報の一覧です。メールチェック情報は10個まで設定できます。処理するボタンをクリックし、次のページに進みます。

こんな事に気をつけて

同時刻に複数のメールチェックを実行した場合、メールチェックの実行がずれる場合があります。

停止

メールチェックを一時的に停止する場合は、“停止”をチェックします。

[TEL メール情報]

TEL メール

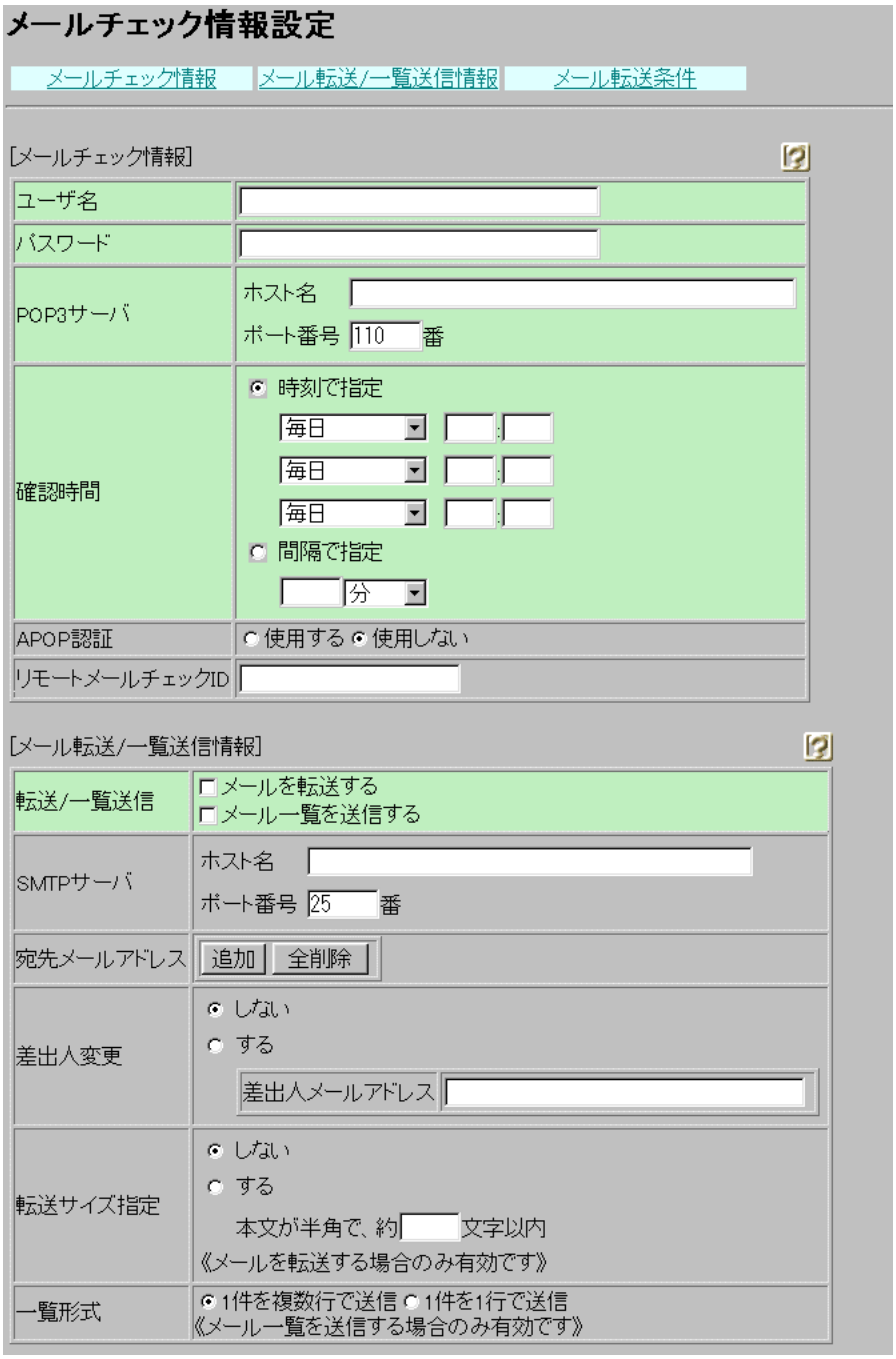
アナログポートの着信履歴を着信ごと、または一定時間ごとにメールで送信するかどうかを選択します。送信する場合は、“使用する”を選択します。

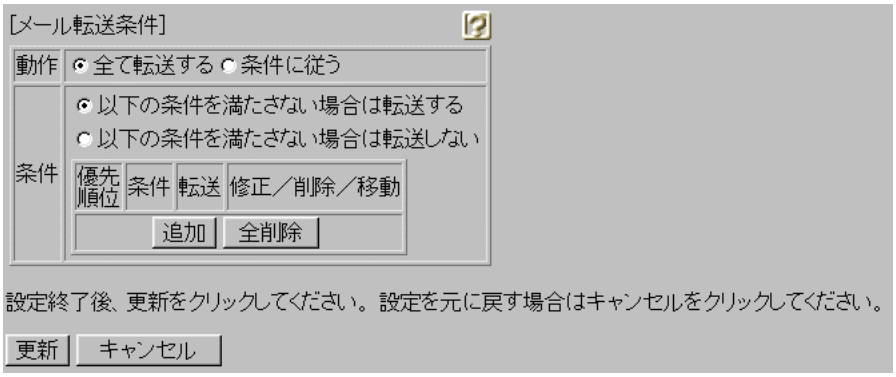
送信情報

現在、指定されているTEL メール情報の一覧です。TEL メール情報はアナログポートごとに指定できます。処理するボタンをクリックし、次のページに進みます。

メールチェック情報設定

【操作】「詳細設定メニュー」→ルータ設定「E メールエージェント情報」→［メールチェック情報一覧］





[メールチェック情報]

メールチェックとは、POP3プロトコルを使用して、指定時間になるとPOP3サーバにメールが到着しているかどうかを確認する機能です。メールが到着していれば、メールの件数、差出人、題名、送信時刻を取得します。

こんな事に気をつけて

- **指定時間になると、回線を自動接続します。あらかじめ相手情報を設定します。**
- **POP3サーバがPOP3のオプションコマンド（UIDL、TOP）を実装していない場合は、メール件数だけ取得します。**

ユーザ名

POP3サーバにアクセスするためのユーザ名を32文字以内で指定します。

パスワード

POP3サーバにアクセスするためのパスワードを32文字以内で指定します。

POP3サーバ

ホスト名にはPOP3サーバ名、またはPOP3サーバのIPアドレスを80文字以内で指定します。ポート番号は必要に応じて変更します。

確認時間

POP3サーバにメールの到着を確認する時間を、時刻、または間隔で指定します。

間隔で指定する場合は、5分～30日の範囲で指定します。

APOP認証

POP3サーバとの認証にAPOPを使用するかどうかを選択します。

こんな事に気をつけて

APOP認証を使用する場合は、POP3サーバがAPOP認証をサポートしている必要があります。

リモートメールチェックID

リモートメールチェックIDを半角英数字19文字以内で指定します。

このIDをサブアドレスとして本装置に電話をかけると、遠隔地からメールチェック、メール転送、メール一覧送信を実行できます。

[メール転送／一覧送信情報]

メール転送とは、メールチェックで取得するメールを指定する宛先メールアドレスに転送する機能です。

メール一覧送信とは、メールチェックで取得するメールの送信時刻（Date）、差出人（From）、題名（Subject）の一覧を指定の宛先メールアドレスに送信する機能です。

・1回のメールチェックで転送できるメール件数は、1ユーザにつき50件までです。

・転送できるメールの文字数は半角で約6144文字、行数は200行以内（どれも本文のみ）です。このサイズを超える部分は切り捨てられます。

・サイズを超えるメールがマルチパートで構成されている場合は、「転送できないサイズのメールが届いています。」というメールを送信します。

こんな事に気をつけて

複数の接続先を使用していると別プロバイダ経由でSMTPサーバを使用することがあり、SPAMなどの不正メール対策のためにメールの送信が行えない場合があります。
プロバイダによっては、別プロバイダ経由でもPOPの認証を行ったあとであればメールの送信を行うことができる場合があります。
詳しくはプロバイダにお問い合わせください。

転送／一覧送信

使用する機能を選択します。

SMTPサーバ

ホスト名にはSMTPサーバ名、またはSMTPサーバのIPアドレスを80文字以内で指定します。

ポート番号は必要に応じて変更します。

宛先メールアドレス

宛先メールアドレス（To）を半角80文字以内で指定します。

宛先メールアドレスは、5個まで設定できます。

差出人変更

SMTP サーバの差出人制限によりメールの転送、一覧送信が行えない場合があります。この場合は、差出人を変更することによりメールの転送、一覧送信ができるようになります。

差出人メールアドレスを変更する場合は、“する”を選択して、差出人メールアドレスを設定します。ここで指定する差出人メールアドレスを使用して、メールの転送、一覧送信を行います。

差出人メールアドレス

差出人メールアドレスを半角80文字以内で指定します。

転送サイズ指定

転送サイズ指定を行うかどうかを選択します。転送するメールのサイズを1～6144文字の範囲で指定します。

一覧形式

送信するメール一覧の形式を選択します。

[メール転送条件]

動作

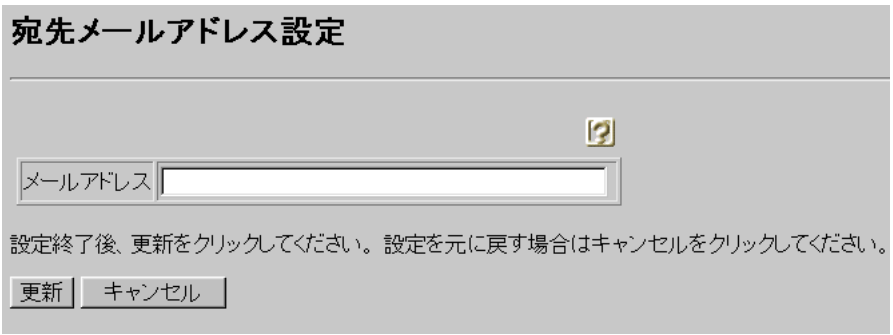
メール転送の条件を指定するかどうかを選択します。指定する場合は、“条件に従う”を選択して、条件を指定します。

条件

指定しているメール転送条件の一覧です。転送条件は装置全体で40個まで設定できます。処理するボタンをクリックし、次のページに進みます。また、条件を満たさない場合の動作はここで設定します。

宛先メールアドレス設定

【操作】「詳細設定メニュー」→ルータ設定「E メールエージェント情報」→［メールチェック情報一覧］→［メール転送／一覧送信情報］



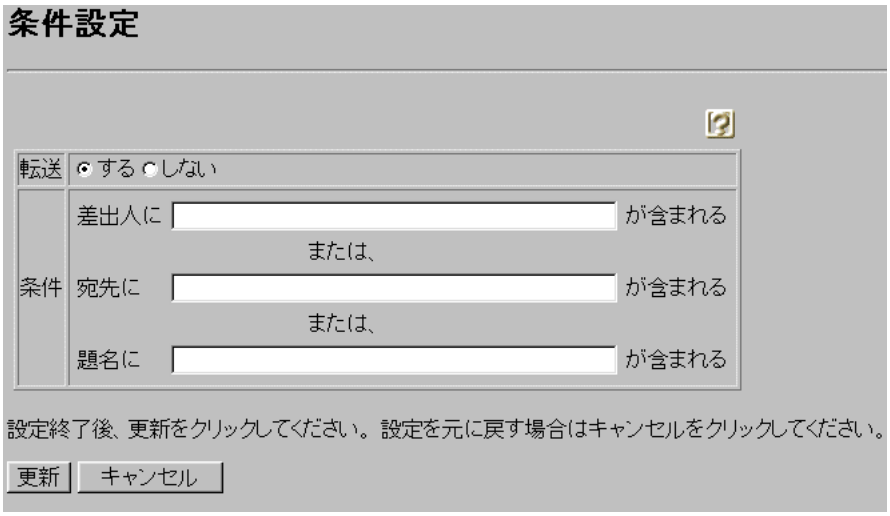
宛先メールアドレス

宛先メールアドレス（To）を半角80 文字以内で指定します。

宛先メールアドレスは、5 個まで設定できます。

条件設定

【操作】「詳細設定メニュー」→ルータ設定「E メールエージェント情報」→［メールチェック情報一覧］→［メール転送条件］



転送

条件を満たす場合にメールを転送するかどうかを選択します。

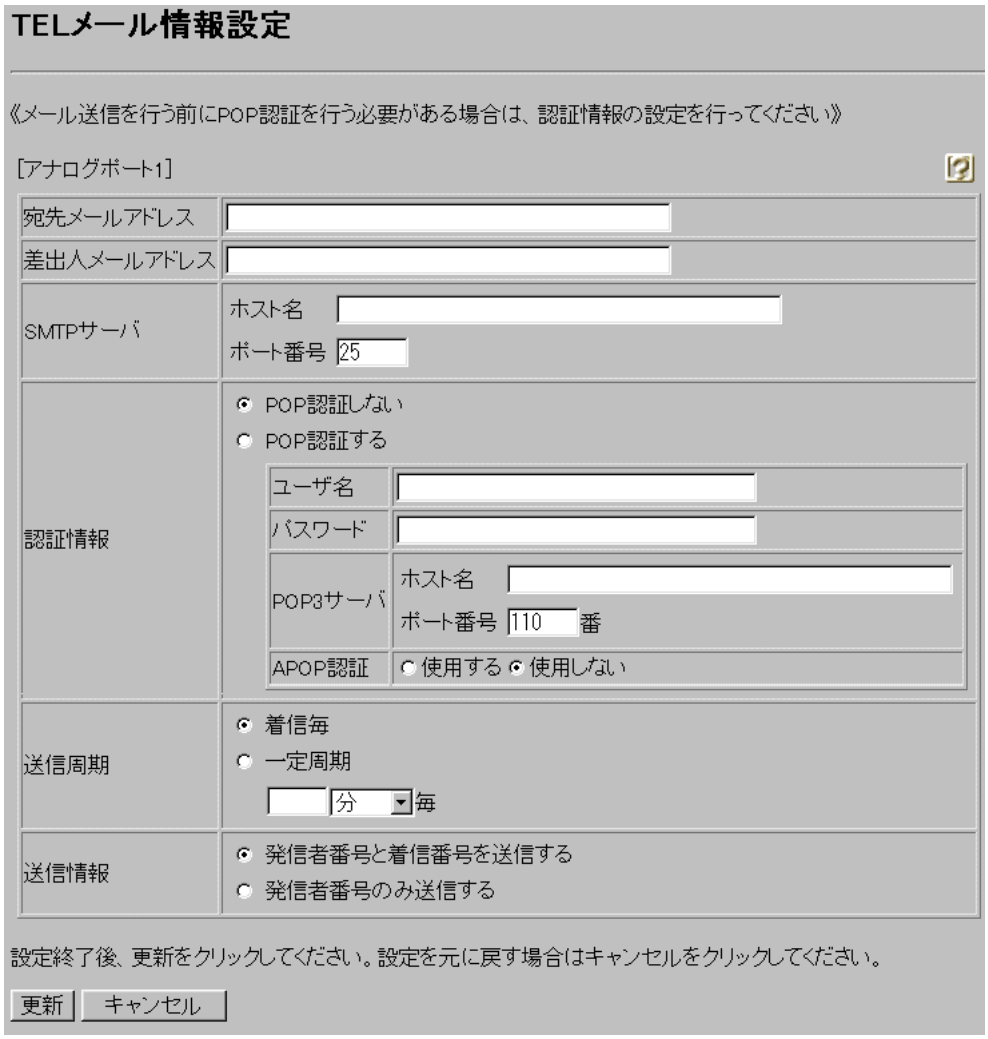
条件

差出人（From）、宛先（To）、題名（Subject）を転送条件として指定できます。

それぞれ半角40文字以内（全角20文字以内）で指定します。

TELメール情報設定

【操作】「詳細設定メニュー」→ルータ設定「Eメールエージェント情報」→［TELメール情報］



TELメールとは、アナログポートの着信履歴を着信ごと、または一定時間ごとにメールで送信する機能です。

こんな事に気をつけて

- **メール送信時には回線を自動接続します。あらかじめ相手情報を設定します。**
- **TELメールの開始がメールチェックとかさなる場合、TELメールの実行がずれる場合があります。**

[アナログポート1、2]

宛先メールアドレス

宛先メールアドレス（To）を半角80文字以内で指定します。

差出人メールアドレス

差出人メールアドレス（From）を半角80文字以内で指定します。

SMTPサーバ

ホスト名にはSMTPサーバ名、またはSMTPサーバのIPアドレスを80文字以内で指定します。

ポート番号は必要に応じて変更します。

認証情報

TELメールの送信を行う前にPOP認証をするかどうかを選択します。

こんな事に気をつけて

複数の接続先を使用していると別プロバイダ経由でSMTPサーバを使用することがあり、SPAMなどの不正メール対策のためにメールの送信が行えない場合があります。
プロバイダによっては、別プロバイダ経由でもPOPの認証を行ったあとであればメールの送信を行うことができる場合があります。
詳しくはプロバイダにお問い合わせください。

ユーザ名

POP3サーバにアクセスするためのユーザ名を32文字以内で指定します。

パスワード

POP3サーバにアクセスするためのパスワードを32文字以内で指定します。

POP3サーバ

ホスト名にはPOP3サーバ名、またはPOP3サーバのIPアドレスを80文字以内で指定します。

ポート番号は必要に応じて変更します。

APOP認証

POP3サーバとの認証にAPOPを使用するかどうかを選択します。

こんな事に気をつけて

APOP認証を使用する場合は、POP3サーバがAPOP認証をサポートしている必要があります。

送信周期

着信履歴をメールで送信するタイミングを、着信ごと、または一定周期で指定します。

一定周期で指定する場合は、5分～7日の範囲で指定します。

送信情報

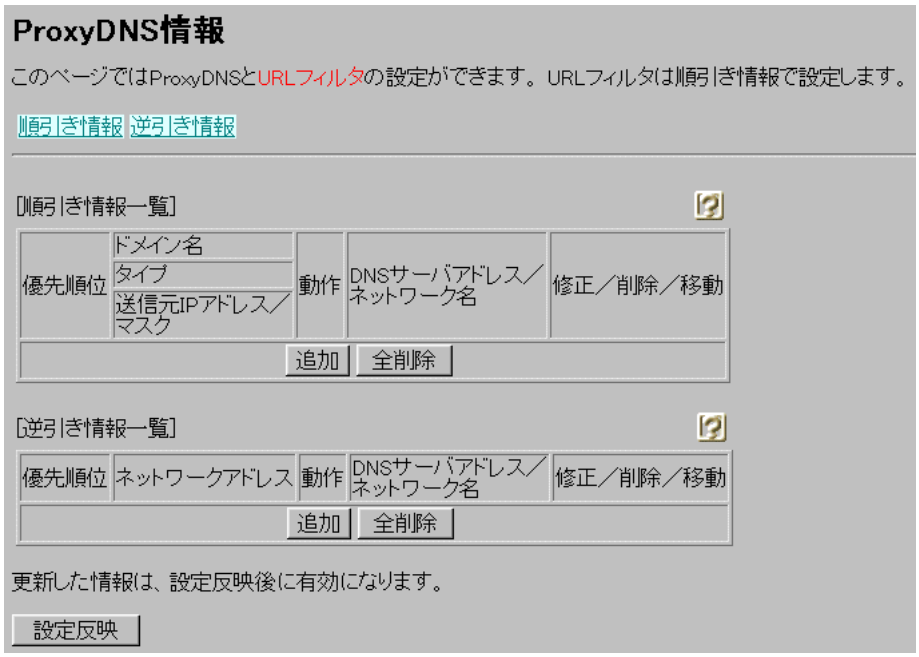
メールで送信する着信履歴の情報を選択します。

こんな事に気をつけて

- TELメールの送信情報を「発信者番号のみ送信する」に設定している場合、発信者番号が非通知になっている電話からの着信履歴は送信されません。
- TELメールの送信情報を「発信者番号と着信番号を送信する」に設定している場合、発信者番号と着信番号のどちらも有効な情報がないときは、TELメールによる着信履歴は送信されません。
- TELメール（本文）の着信番号は以下のように設定されます。
  - ダイヤルインサービスおよびｉ・ナンバーサービスを利用しない場合
    回線から着信番号が通知されないため、TELメールの情報に着信番号は含まれません。「アナログ共通情報」の「網契約に関連する設定項目」の「電話番号」に電話番号を設定していれば、この番号がTELメールの着信番号として送信されます。
  - ダイヤルインサービスを利用している場合
    回線から通知された着信番号（ダイヤルイン番号）がTELメールの着信番号として送信されます。ただし、グローバル着信を利用している場合、契約者番号にかかってくると回線から着信番号が通知されません。このとき、「アナログ共通情報」の「網契約に関連する設定項目」の「電話番号」に電話番号を設定していれば、この番号がTELメールの着信番号として送信されます。
  - ｉ・ナンバーサービスを利用している場合
    「鳴り分け1」、「鳴り分け2」、または「鳴り分け3」がTELメールの着信番号として送信されます。ただし、「アナログ共通情報」の「網契約に関連する設定項目」の「鳴り分け番号1／2／3」に電話番号を設定していれば、この番号がTELメールの着信番号として送信されます。

ProxyDNS情報

【操作】「詳細設定メニュー」→ルータ設定「ProxyDNS情報」



ヒント

◆ ProxyDNSには以下の機能があります。

・DNSサーバの自動切り替え機能

パソコンに本装置のIPアドレスをDNSサーバとして登録しておくと、接続先によって問い合わせるDNSサーバを自動的に切り替えます。

・DNSサーバ機能

ホストデータベース情報にホスト名とIPアドレスのペアを登録しておくと、ProxyDNSは該当ホスト名へのアクセスを登録されたIPアドレスへのアクセスとして切り替えます。

・URLフィルタ機能

特定のドメイン名（範囲指定も可）へのアクセスを禁止することができます。この機能は順引き情報設定で設定します。

・DNS問い合わせタイプフィルタ機能

送信元IPアドレス範囲から送信される特定の問い合わせのタイプのDNSパケットを破棄することができます。この機能は順引き情報設定で設定します。

[順引き情報一覧]

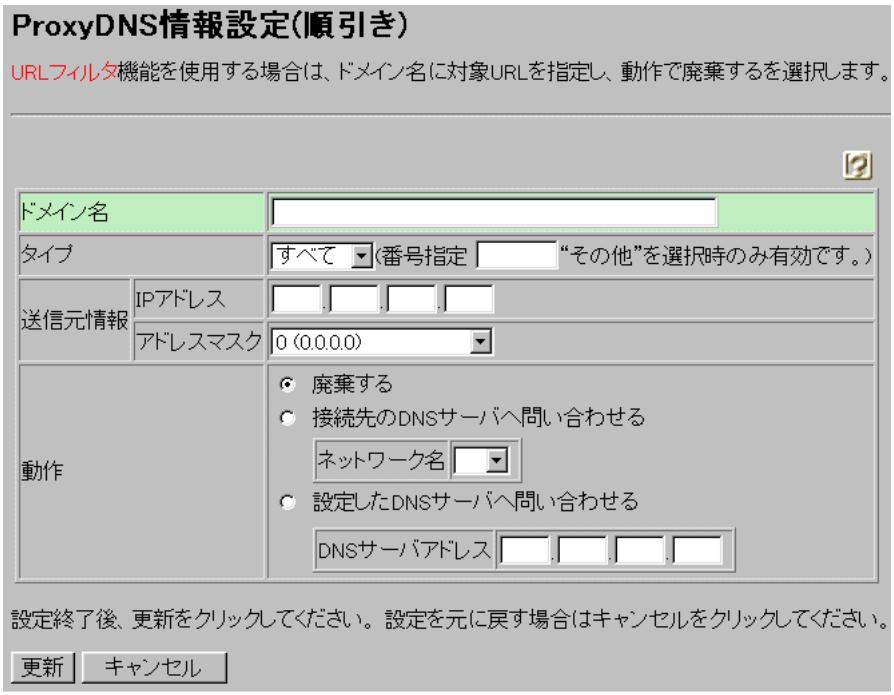
ProxyDNSの順引き情報の一覧です。順引き情報はドメイン名によりDNSサーバを切り替える範囲を指定する場合、特定ドメイン名へアクセスを禁止する場合、送信元IPアドレス範囲からの特定の問い合わせタイプのDNSパケットを破棄する場合など、ドメイン名、問い合わせタイプ・送信元IPアドレス／マスクの組み合わせによりいろいろな使い方ができます。32個まで定義できます。処理するボタンをクリックし、次のページに進みます。

[逆引き情報一覧]

ProxyDNSの逆引き情報の一覧です。逆引き情報はIPアドレスによりDNSサーバを切り替える範囲を指定する場合に使用します。32個まで定義できます。処理するボタンをクリックし、次のページに進みます。

ProxyDNS情報設定（順引き）

【操作】「詳細設定メニュー」→ルータ設定「ProxyDNS情報」→［順引き情報一覧］



ドメイン名

対象とするドメイン名の範囲を半角英数字80文字以内で指定します。範囲指定には、以下のように、'*'、または'?'が使用できます。なお、ドメイン名のチェックには大文字／小文字の区別はありません。

'*'：0文字以上の任意の文字に一致する。

'?'：1文字の任意文字に一致する。

《例》

条件：

www.*.com

一致：

www.testa.com
www.test1.test.com

条件：

test

一致：

www.test.com
test.com
test.co.jp

条件：

www.test?.com

一致：

www.test1.com
www.test2.com
www.testA.com

タイプ

対象とする問い合わせタイプを以下の5つから選択します。

・すべて （PTRを除く）

・A　　（1）

・SOA　（6）

・SRV　（33）

・その他

タイプを指定する場合は、“その他”を選択し、10進数を使用して、1～11、13～65535の範囲で指定します。

送信元IPアドレス／マスク

フィルタリング条件として送信元IPアドレスとアドレスマスクを指定します。

チェック対象となるパケットのIPアドレスと、定義するIPアドレスとアドレスマスクの論理積が等しい場合に条件に一致します。

動作

対象ドメインに対する動作を以下の3つから選択します。

廃棄する

該当ドメインの転送を無効にするフィルタを指定します。URLフィルタとして利用する場合に設定します。

接続先のDNSサーバへ問い合わせる

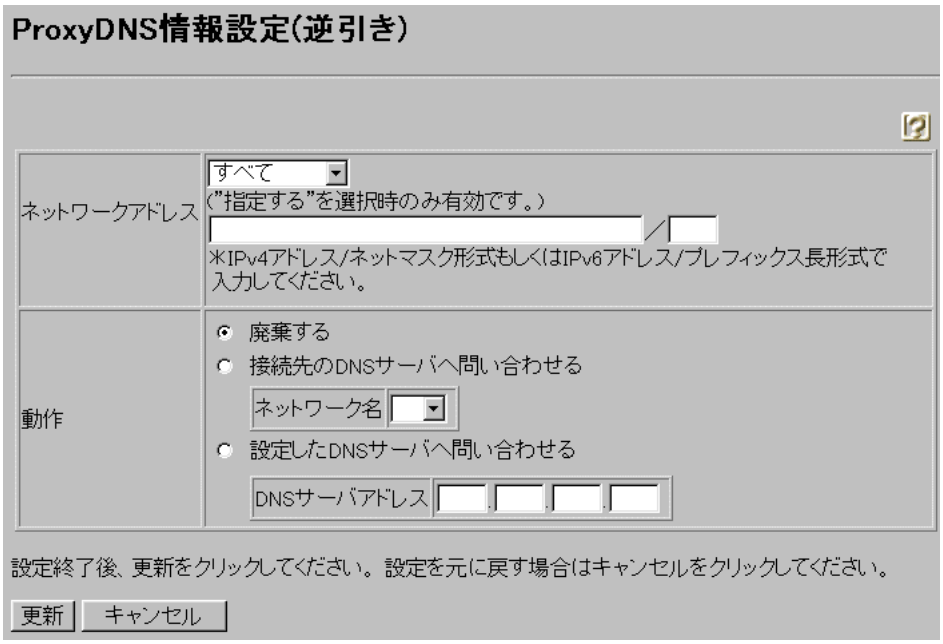
接続先情報で設定したDNSサーバへ問い合わせます。どのネットワークで使用するかを選択します。選択したネットワークに複数の接続先が登録されている場合は、マルチルーティングと優先順位に従って接続先を決定します。

設定したDNSサーバへ問い合わせる

特定のDNSサーバへ問い合わせます。問い合わせるDNSサーバのIPアドレスを指定します。

ProxyDNS情報設定（逆引き）

【操作】「詳細設定メニュー」→ルータ設定「ProxyDNS情報」→［逆引き情報一覧］



ネットワークアドレス

対象とするネットワークアドレスを以下の4つから選択します。

すべて

IPv4とIPv6両方を選択します。

IPv4すべて

IPv4アドレスをすべて選択します。

IPv6すべて

IPv6アドレスをすべて選択します。

指定する

IPv4アドレス／ネットマスク、またはIPv6アドレス／プレフィックスの形式で指定します。

動作

対象ドメインに対する動作を以下の3つから選択します。

廃棄する

該当ネットワークの転送を無効にするフィルタを指定します。

接続先のDNSサーバへ問い合わせる

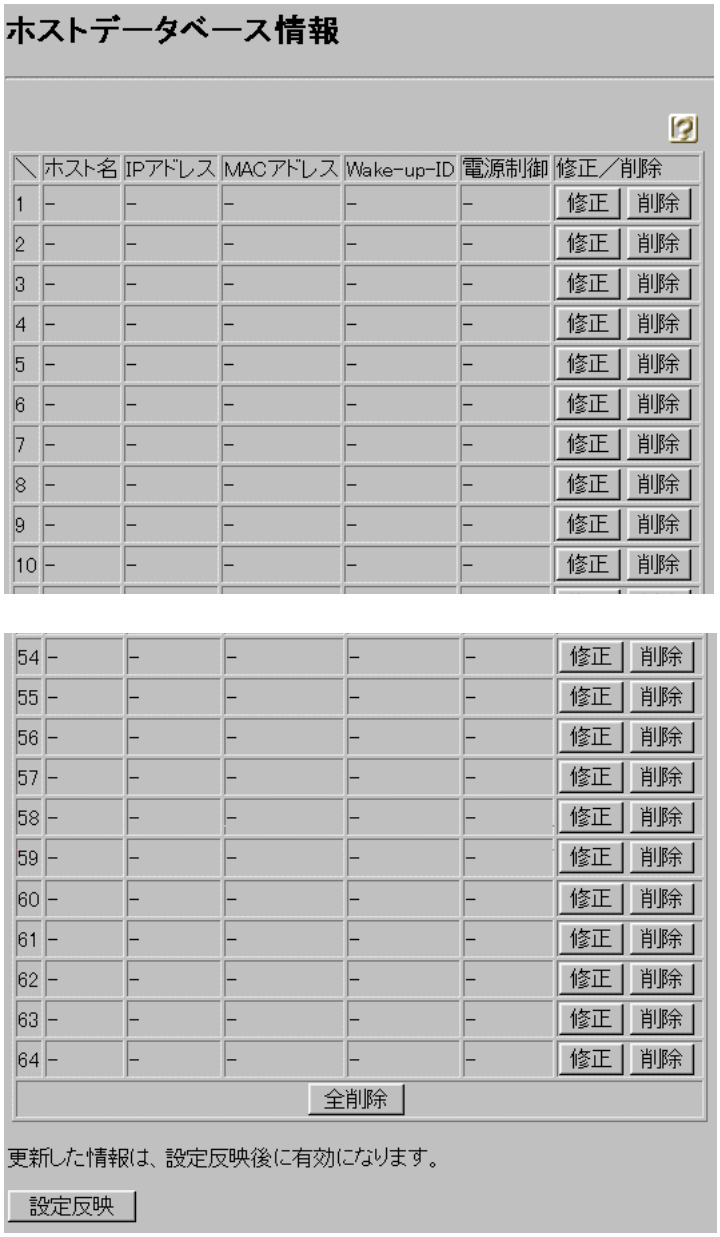
接続先情報で設定したDNSサーバへ問い合わせます。どのネットワークで使用するかを選択します。選択するネットワークに複数の接続先を登録している場合は、マルチルーティングと優先順位に従って接続先が決定されます。

設定したDNSサーバへ問い合わせる

特定のDNSサーバへ問い合わせます。問い合わせるDNSサーバのIPアドレスを指定します。

ホストデータベース情報

【操作】「詳細設定メニュー」→ルータ設定「ホストデータベース情報」



登録しているホストデータベース情報の一覧です。処理するボタンをクリックし、次のページに進みます。

ヒント

◆ ホストデータベースには以下の機能があります。

・DNS サーバ機能

「ホスト名」「IP アドレス」のペアを登録することにより、ProxyDNS の DNS サーバ機能を使用することができます。

・リモートパワーオン機能

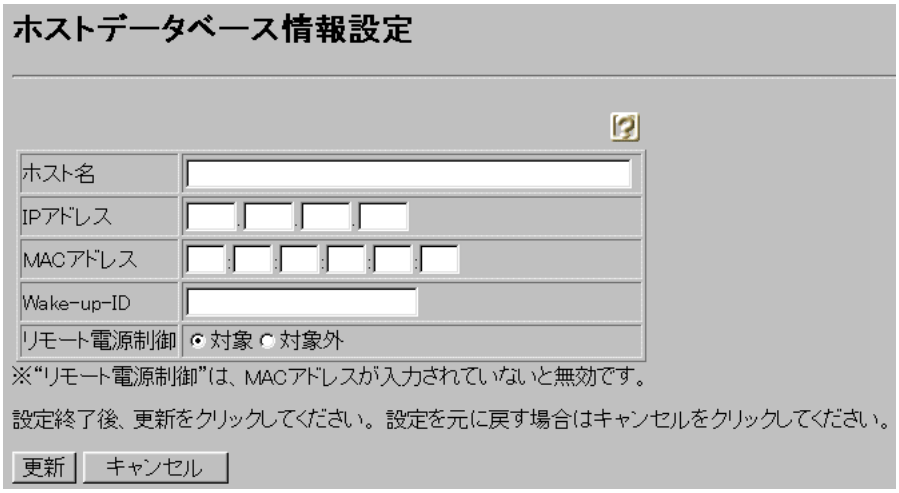
「MAC アドレス」「Wake-up-ID」のペアを登録することにより、Wakeup on LAN 機能を使用することができます。

・DHCP スタティック機能

「IP アドレス」「MAC アドレス」のペアを登録することにより、DHCP で割り当てられる IP アドレスを端末固有のものとすることができます。

ホストデータベース情報設定

【操作】「詳細設定メニュー」→ルータ設定「ホストデータベース情報」→「ホストデータベース情報」



ホスト名

DNS サーバ機能で使用されます。80 文字以内で指定します。使用する文字は半角のアルファベット・数字・ハイフン・ピリオドだけで、その他の記号は使用できません。

IPアドレス

DNS サーバ機能およびDHCPスタティック機能で使用されます。

MACアドレス

DHCP スタティック機能およびリモートパワーオン機能で使用します。MACアドレスは以下の形式で指定します。

xx:xx:xx:xx:xx:xx（xxは2桁の16進数）

Wake-up-ID

本装置は、ISDN接続を契機にして、本装置と同じセグメント上に存在するMagic Packet対応システムの電源を投入することができます。リモートパワーオン機能使用時に、Magic Packetを送出するLAN機器の識別IDを半角英数字19文字以内で指定します。

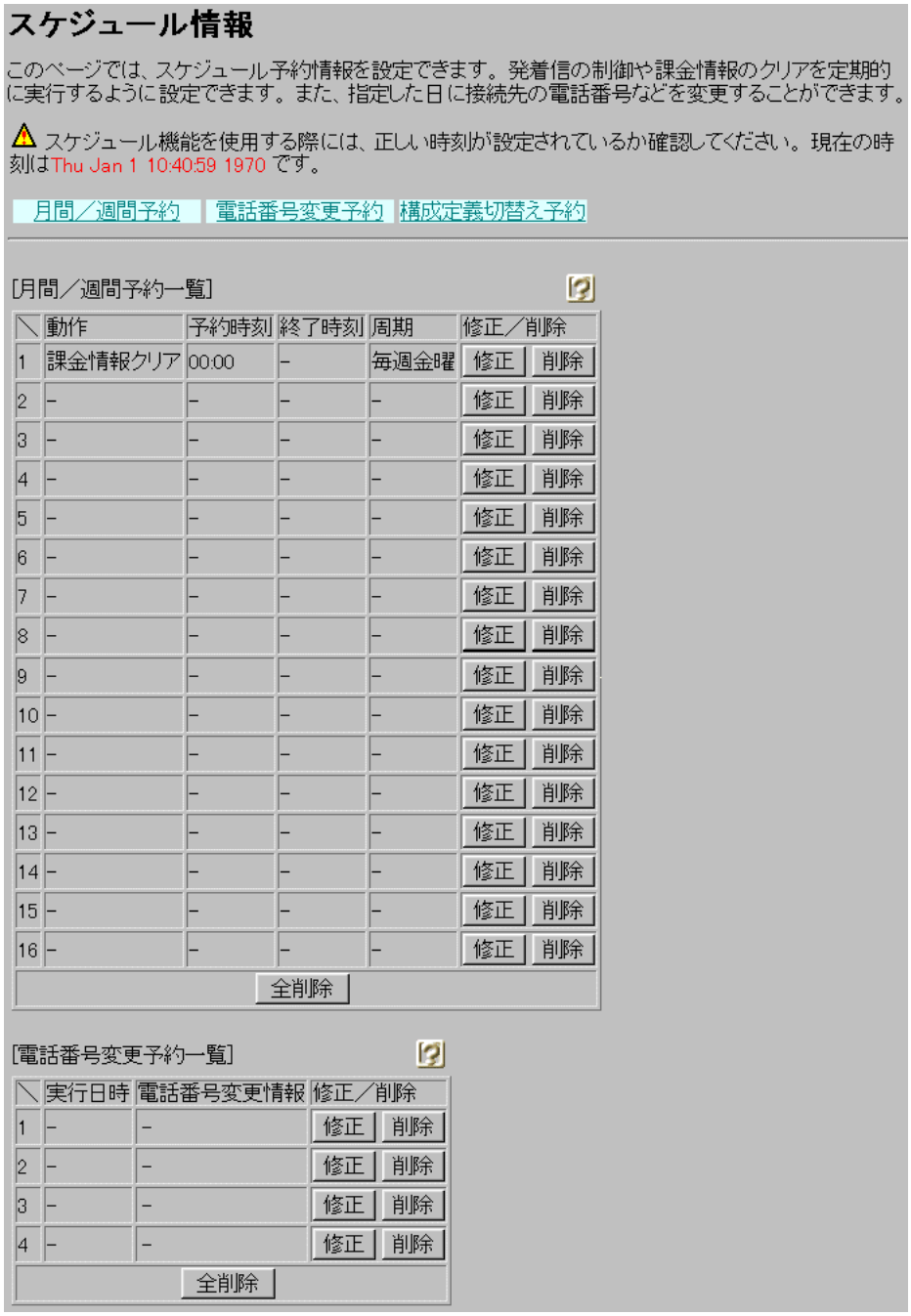
電源制御（リモート電源制御）

本装置と同じセグメントに存在するWakeup on LAN対応機器を、リモートパワーオン指示の対象とするかどうかを選択します。

この設定はスケジュール機能や手動操作でリモートパワーオンを指示する場合に使用できます。ISDN接続先からの制御対象には使用できません。

スケジュール情報

【操作】「詳細設定メニュー」→ルータ設定「スケジュール情報」



スケジュール情報

このページでは、スケジュール予約情報を設定できます。発着信の制御や課金情報のクリアを定期的に実行するように設定できます。また、指定した日に接続先の電話番号などを変更することができます。

スケジュール機能を使用する際には、正しい時刻が設定されているか確認してください。現在の時刻はThu Jan 1 10:40:59 1970 です。

月間／週間予約　電話番号変更予約　構成定義切替え予約

[月間／週間予約一覧]

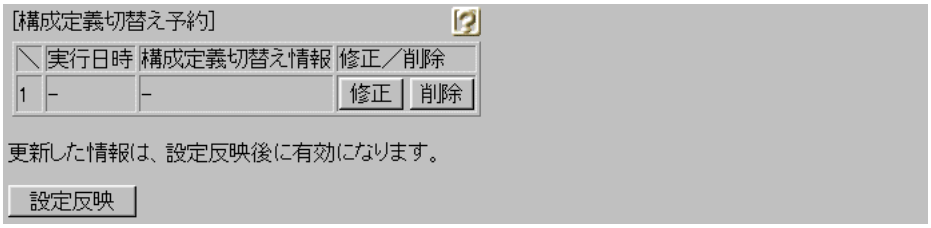
＼	動作	予約時刻	終了時刻	周期	修正／削除
1	課金情報クリア	00:00	-	毎週金曜	修正 削除
2	-	-	-	-	修正 削除
3	-	-	-	-	修正 削除
4	-	-	-	-	修正 削除
5	-	-	-	-	修正 削除
6	-	-	-	-	修正 削除
7	-	-	-	-	修正 削除
8	-	-	-	-	修正 削除
9	-	-	-	-	修正 削除
10	-	-	-	-	修正 削除
11	-	-	-	-	修正 削除
12	-	-	-	-	修正 削除
13	-	-	-	-	修正 削除
14	-	-	-	-	修正 削除
15	-	-	-	-	修正 削除
16	-	-	-	-	修正 削除

全削除

[電話番号変更予約一覧]

＼	実行日時	電話番号変更情報	修正／削除
1	-	-	修正 削除
2	-	-	修正 削除
3	-	-	修正 削除
4	-	-	修正 削除

全削除



[月間／週間予約一覧]

現在、設定されている月間、または週間の予約一覧です。処理するボタンをクリックし、次のページに進みます。

[電話番号変更予約一覧]

現在、設定されている電話番号変更の予約一覧です。処理するボタンをクリックし、次のページに進みます。

[構成定義情報切替え予約]

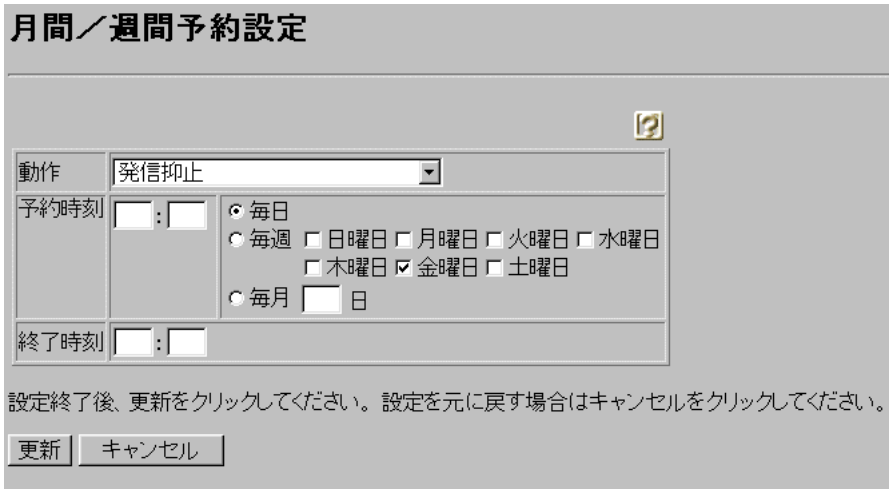
現在、設定されている構成定義情報切替えの予約一覧です。処理するボタンをクリックし、次のページに進みます。

こんな事に気をつけて

スケジュール機能を使用する前に、必ず本装置の時刻設定を操作メニューから行います。

月間／週間予約設定

【操作】「詳細設定メニュー」→ルータ設定「スケジュール情報」→［月間／週間予約一覧］



動作

以下の中から予約する処理動作を選択します。

- ・発信抑止
- ・着信抑止
- ・テレホーダイ
- ・課金情報クリア
- ・強制切断
- ・統計情報収集
- ・リモートパワーオン
- ・スタンバイモードへ移行
- ・スタンバイモードを解除
- ・留守モードへ移行
- ・留守モードを解除

予約時刻

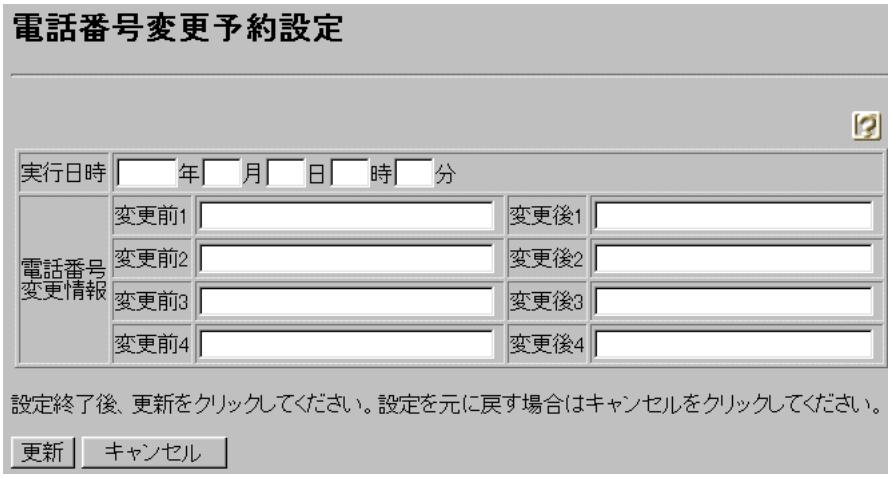
選択する動作を実行（開始）する時刻と実行周期を指定します。

終了時刻

選択する動作を終了する時刻を指定します。動作として発信抑止、着信抑止、テレホーダイを選択する場合にだけ指定できます。ここで予約時刻よりも早い時刻を指定すると、それは翌日の時刻になります。

電話番号変更予約設定

【操作】「詳細設定メニュー」→ルータ設定「スケジュール情報」→［電話番号変更予約一覧］



全構成定義情報で定義している電話番号について、指定時刻に電話番号の変更ができます。

こんな事に気をつけて

指定時刻になると自動的に再起動され、電話番号が変更されます。そのとき、データ通信／電話を使用中の場合は、回線が切断されます。

実行日時

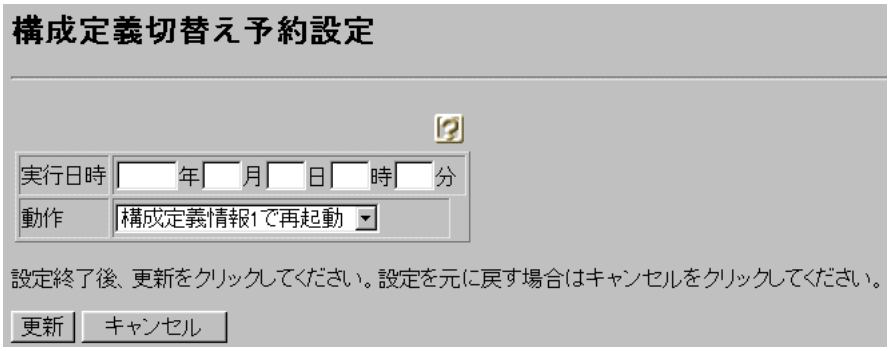
電話番号を変更する日時を西暦で指定します。

電話番号変更情報

変更前と変更後の電話番号をそれぞれ32桁以内で指定します。

構成定義切替え予約設定

【操作】「詳細設定メニュー」→ルータ設定「スケジュール情報」→［構成定義切替え予約］



本装置には構成定義情報が2つあります。指定時刻に運用する構成定義情報を切り替えることができます。指定時刻になると自動的に再起動され、構成定義情報が切り替わります。そのときに、データ通信／電話を使用中の場合は、回線が切断されますので注意してください。なお、現在運用中の構成定義情報はメンテナンスメニューの「構成定義切替え」で知ることができます。

実行日時

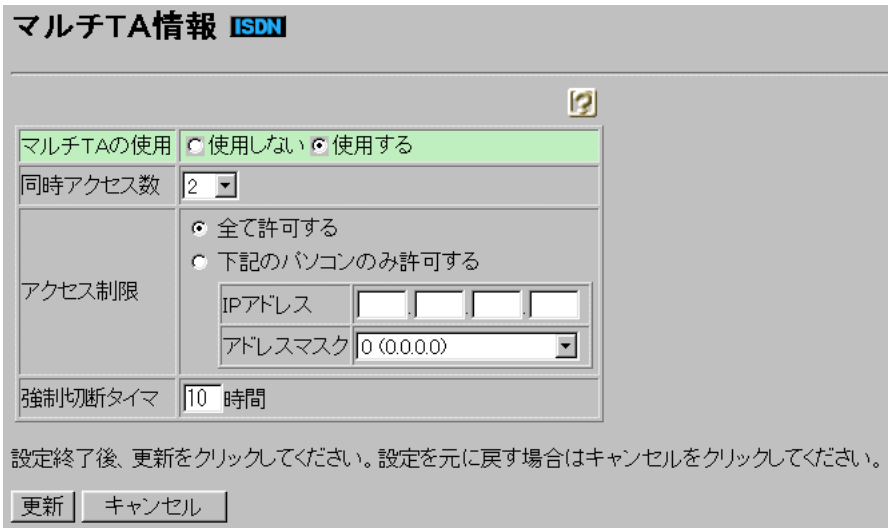
構成定義情報を切り替える日時を西暦で指定します。

動作

切り替える構成定義情報を指定します。

マルチTA情報

【操作】「詳細設定メニュー」→ルータ設定「マルチTA情報」



この機能は、LANに接続するパソコンから仮想ダイアルアップアダプタを通じてISDNのBチャネルへダイレクトに接続できるサービスです。

こんな事に気をつけて

- **パソコン側は、Microsoft® Windows®のダイヤルアップネットワークでのVPN（仮想プライベートネットワーク）機能を使用します。**
- **マルチTA機能は、Windows Vista®では使用できません。**

マルチTAの使用

マルチTAを使用するかどうかを選択します。使用する場合は、以下の項目を設定します。使用しない場合は、以下の設定は無効となります。

同時アクセス数

マルチTAとして使用するISDNのBチャネルの数を選択します。

アクセス制限

“全て許可する”を選択する場合は、すべてのパソコンが利用できます。“下記のパソコンのみ許可する”を選択した場合は、定義するIPアドレスとアドレスマスクの論理積に一致するパソコンだけ利用できます。

強制切断タイマ

データ通信時の強制切断タイマを0～24時間の範囲で指定します。

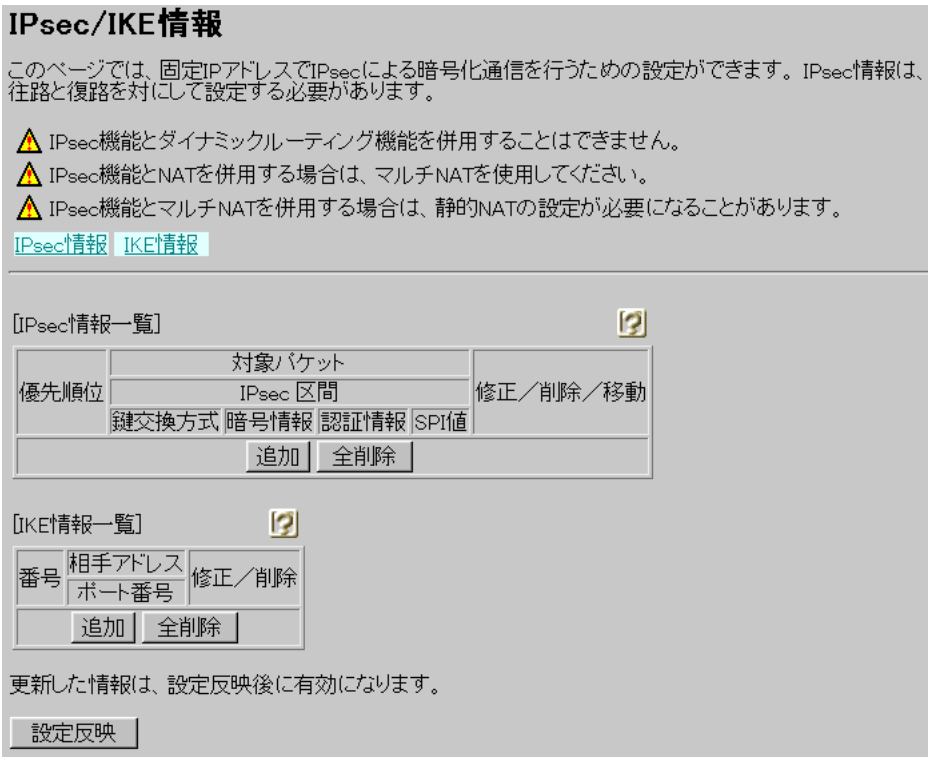
0を指定した場合には切断は行われません。

こんな事に気をつけて

- **ブラウザ画面からの強制切断操作ではマルチTA接続は切断されません。ダイヤルアップネットワークの切断操作を行います。**
- **スケジュールによる発呼抑止／強制切断はマルチTA接続では無効です。**

IPsec／IKE情報

【操作】「詳細設定メニュー」→ルータ設定「IPsec情報」



[IPsec情報一覧]

このページでは、固定IPアドレスでIPsecによる暗号化通信を行うための設定ができます。可変IPアドレスでIPsecによる暗号化通信を行う場合は、「詳細設定メニュー」→「相手情報」→「ネットワーク情報」→「接続先情報」の「IPsec情報」／「IKE情報」を設定してください。

現在、この装置に設定されているIPsec情報の一覧です。処理は優先順位1から順に行われます。IPsec情報は、手動鍵設定と自動鍵設定（交換）を合わせて、装置全体で64個（往路／復路、対の設定で32箇所）まで設定できます。

IPsec情報を1個設定することにより片方向のトンネルが1つ作成されます。トンネルは、「往路（相手装置へパケットを送信する）」と「復路（相手装置からパケットを受信する）」を対にして設定する必要があります。

本装置で設定したIPsec情報と同じ設定が、相手装置にも設定されている必要があり、本装置で往路として設定した情報を、相手装置では復路として設定します。また、本装置で復路として設定した情報は、相手装置では往路として設定します。

こんな事に気をつけて

パソコンから本装置へのパケットがトンネルに入ってしまう設定を行うと、WWW ブラウザからアクセスできなくなる場合があります。

マルチ NAT との併用

IPsec で使用する LAN の IP アドレスがマルチ NAT で使用する IP アドレスに含まれる場合は、以下の静的 NAT を指定する必要があります。

プライベート IP 情報

IP アドレス：IPsec で使用する LAN の IP アドレス

ポート番号：すべて

グローバル IP 情報

IP アドレス：IPsec で使用する LAN の IP アドレス

ポート番号：すべて

プロトコル

AH、または ESP（IPsec で使用されるプロトコルを指定）

IPsecで使用するプロトコル

IPsec で使用するプロトコルは、IPsecの設定により決定します。

暗号情報	認証情報	プロトコル
暗号化しない	認証なし	ESP（null encrypt）
暗号化しない	○	AH（認証）
○	認証なし	ESP（暗号）
○	○	ESP（認証 + 暗号）

認証情報　○：hmac-md5、または hmac-sha1

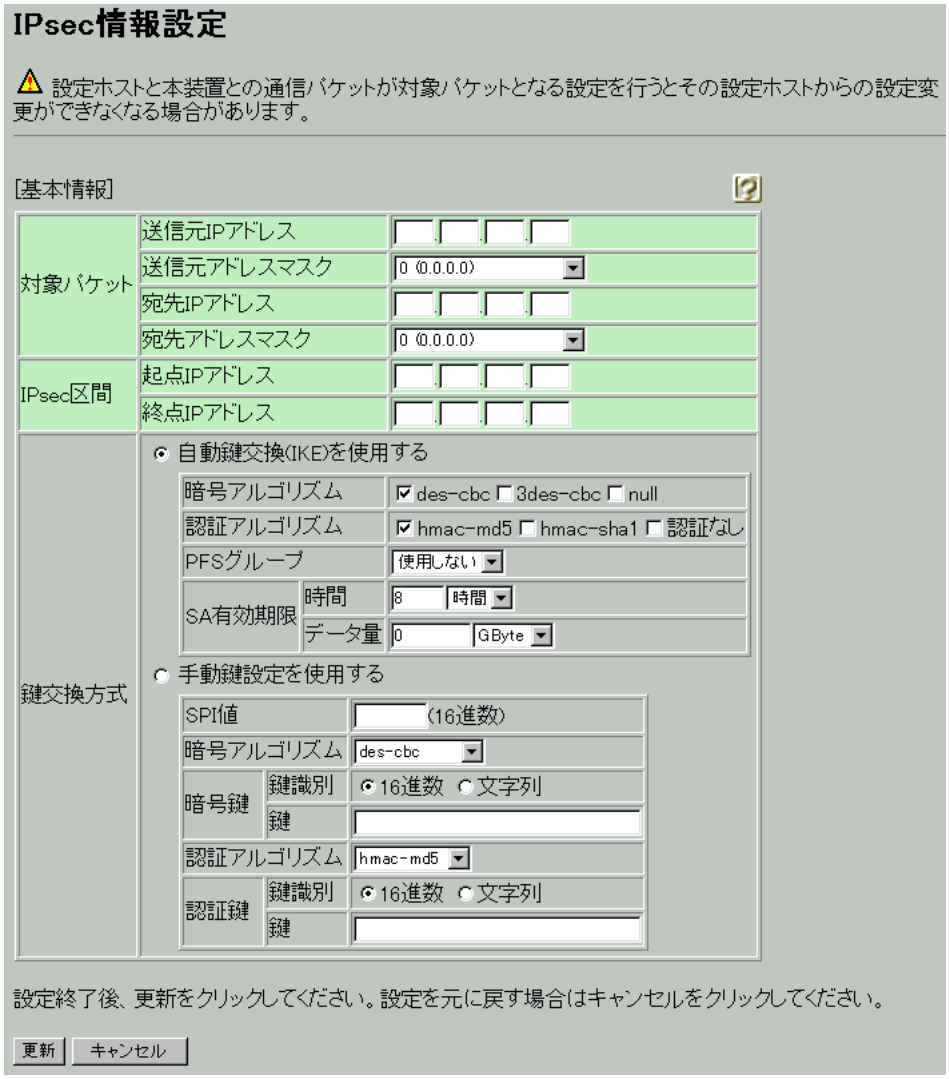
暗号情報　○：des-cbc、または 3des-cbc

[IKE 情報一覧]

現在、この装置に設定されている IKE 情報の一覧です。IKE 情報の定義は装置全体で 32 個まで設定できます。処理するボタンをクリックし、次のページに進みます。

IPsec情報設定

【操作】「詳細設定メニュー」→ルータ設定「IPsec／IKE情報」→［IPsec情報一覧］



[基本情報]

対象パケットの送信元（宛先）IPアドレス／アドレスマスク

トンネリングの対象となるIPアドレス、およびアドレスマスクを指定します。チェック対象となったパケットのIPアドレスと、指定したIPアドレスとアドレスマスクの論理積が等しい場合にトンネリングの対象となります。

IPsecを適用するセッションの送信元IPアドレスおよびアドレスマスクと、宛先IPアドレスおよびアドレスマスクを指定します。

IPsec区間の起点／終点IPアドレス

IPsecを行う区間を指定します。

往路を設定する場合

起点：IPsecで使用するLANのIPアドレス

終点：相手装置のIPアドレス

復路を設定する場合

起点：相手装置のIPアドレス

終点：IPsecで使用するLANのIPアドレス

鍵交換方式

自動鍵交換（IKE）を使用する場合

自動で鍵交換を行う場合は、“自動鍵交換（IKE）を使用する”を選択し、往路／復路で同じ暗号アルゴリズム、認証アルゴリズム、PFSグループ、SA有効期限を設定します。

暗号アルゴリズム

トンネリングするパケットの暗号アルゴリズムを使用する場合に、選択します。暗号アルゴリズムは複数定義することができます。複数定義する場合は、3DES-CBC、DES-CBC、NULLの順に比較されます。暗号アルゴリズムを選択しない場合は、パケットの暗号化を行いません。

認証アルゴリズム

トンネリングするパケットの認証アルゴリズムを選択します。認証アルゴリズムは複数定義することができます。複数定義する場合は、HMAC-MD5、HMAC-SHA1、認証なしの順に比較されます。認証アルゴリズムを選択しない場合、および“認証なし”だけを選択する場合は、パケットの認証を行いません。

PFSグループ

自動鍵交換で鍵を生成するための鍵素材です。値が大きい程セキュリティ強度は高くなりますが、その分鍵生成のための計算に時間がかかるため、装置の負荷が高くなる場合があります。PFSグループを使用しない場合は、“使用しない”を選択します。

SA有効期限

SAの有効期限を時間、およびデータ量で指定します。指定した時間が経過した時点、またはIPsec通信したデータ量が指定データ量に達した時点で、SAの有効期限が切れ、SA情報や鍵情報がIKEによって自動的に更新されます。

時間

以下の範囲で有効時間を指定します。

有効範囲）
1～24時
10～1440分
600～86400秒

データ量

以下の範囲で有効データ量を指定します。

有効範囲）
1～105 GByte（ギガバイト）
3～108000 MByte（メガバイト）
2400～110592000 KByte（キロバイト）

手動鍵設定を使用する場合

鍵設定を手動で行う場合は、“手動鍵設定を使用する”を選択し、SPI値を設定します。また、暗号アルゴリズム、認証アルゴリズムを使用する場合は、それぞれ暗号鍵、認証鍵を必ず設定します。

SPI値

SPI値は、暗号情報や認証情報を定義した、セキュリティパラメタインデックスです。相手装置の設定と同じ値を指定する必要があります。SPI値を16進数を使って、100～ffffffffの範囲で指定します。

暗号アルゴリズム

トンネリングするパケットの暗号アルゴリズムを選択します。“暗号化しない”を選択した場合は、パケットの暗号化を行いません。

暗号鍵

鍵識別

鍵の識別を選択します。

鍵

以下の範囲で16進数および文字列を使用して、暗号アルゴリズムで使用する暗号鍵を指定します。

暗号アルゴリズム	入力範囲（16進数鍵）	入力範囲（文字列鍵）
des-cbc	1～16桁	8文字
3des-cbc	1～48桁	24文字

16進数で16桁（des-cbc指定時、3des-cbc指定時は48桁）未満の鍵を指定した場合は、16（48）桁になるまで、自動的に"0"でパディングされます。

文字列で指定する場合は、8文字（des-cbc指定時、3des-cbc指定時は24文字）固定の鍵長で指定します。暗号情報のアルゴリズムに“暗号化しない”を選択した場合は、省略できます。

認証アルゴリズム

トンネリングするパケットの認証アルゴリズムを選択します。“認証なし”を選択した場合は、パケットの認証を行いません。

認証鍵

鍵識別

鍵の識別を選択します。

鍵

以下の範囲で16進数および文字列を使用して、認証アルゴリズムで使用する認証鍵を指定します。

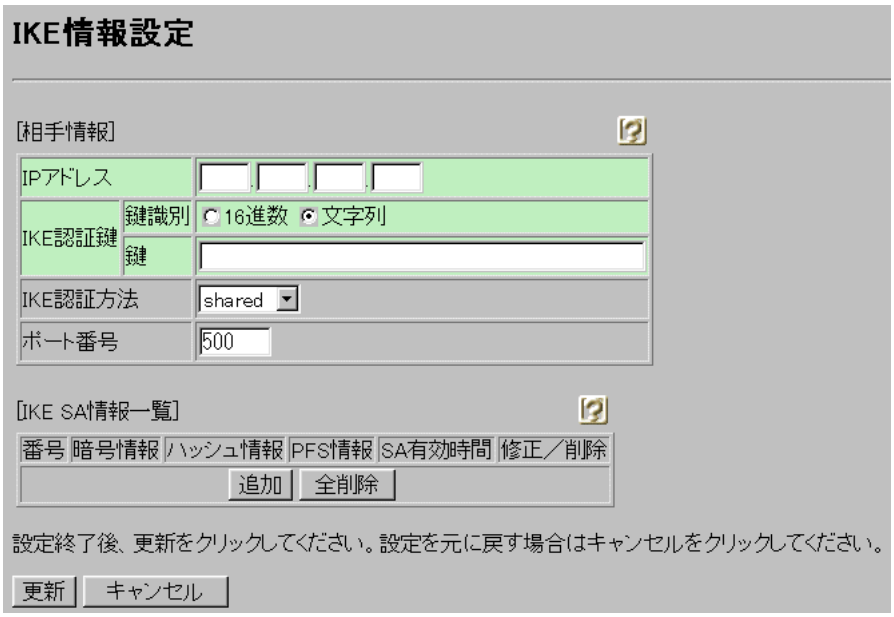
認証アルゴリズム	入力範囲（16進数鍵）	入力範囲（文字列鍵）
hmac-md5	1～32桁	16文字
hmac-sha1	1～40桁	20文字

16進数で32桁（hmac-md5指定時、hmac-sha1指定時は40桁）未満の鍵を指定した場合は、32（40）桁になるまで、自動的に"0"でパディングされます。

文字列で指定する場合は、16文字（hmac-md5指定時、hmac-sha1指定時は20文字）固定の鍵長で指定します。認証情報のアルゴリズムに“認証なし”選択した場合は、省略できます。

IKE情報設定

【操作】「詳細設定メニュー」→ルータ設定「IPsec／IKE情報」→［IKE情報一覧］



［相手情報］

自動鍵交換を使用する場合は、前述のIPsec通信に必要なSA（IPsec SA）のほかにもう1つ、安全に鍵交換を行うためのSA（ISAKMP SA）が必要です。

IPアドレス

IKEセッションを確立する、相手装置のIPアドレスを指定します。

IKE認証鍵

IKEの認証に用いる鍵を設定します。本装置のIKE認証には事前共有鍵方式を使用しているため、ここでは事前共有鍵（Pre-shared key）の設定を行います。事前共有鍵は、IKEを利用したIPsec通信を行う相手ごとに、また相手装置側でも同じ鍵を設定する必要があります。

鍵識別

鍵の識別を選択します。

鍵

以下の範囲で16進数および文字列を使用して、事前共通認証鍵を指定します。

入力範囲（16進数鍵）	入力範囲（文字列鍵）
1～256桁	1～128文字

IKE認証方法

IKEの鍵交換で、相手を認証するための認証方法を指定します。本装置では事前共有鍵方式（shared）を使用します。

ポート番号

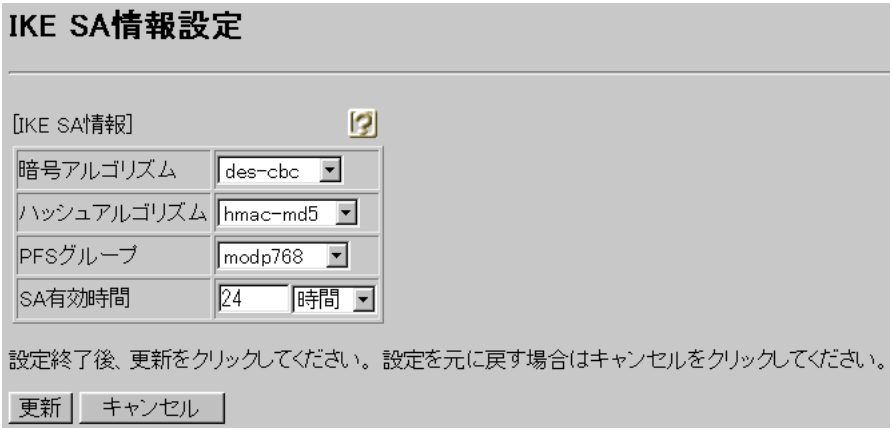
IKEプロトコルでは通常UDPのポート500番を使用します。特に問題がない限り500番を指定します。

[IKE SA情報一覧]

現在、この装置に設定されているIKE SA情報の一覧です。IKE SA情報の定義はIKE情報ごとに3個まで設定できます。処理するボタンをクリックし、次のページに進みます。

IKE SA情報設定

【操作】「詳細設定メニュー」→ルータ設定「IPsec／IKE情報」→［IKE情報一覧］→［IKE SA情報一覧］



［IKE SA情報］

IKEセッションのネゴシエーションの条件を設定します。自側の定義は相手装置の定義と一致することが条件となります。

暗号アルゴリズム

IKEセッションの送受信パケットを暗号化／復号化するための暗号アルゴリズムを選択します。IKEセッション用暗号情報設定が未定義の場合は、IKEが動作しません。

ハッシュアルゴリズム

IKEセッションのネゴシエーションパケットを認証するためのハッシュアルゴリズムを選択します。

PFSグループ

自動鍵交換で鍵を生成するための鍵素材を選択します。
値が大きい程セキュリティ強度は高くなりますが、その分鍵生成のための計算に時間がかかるため、装置の負荷が高くなる場合があります。

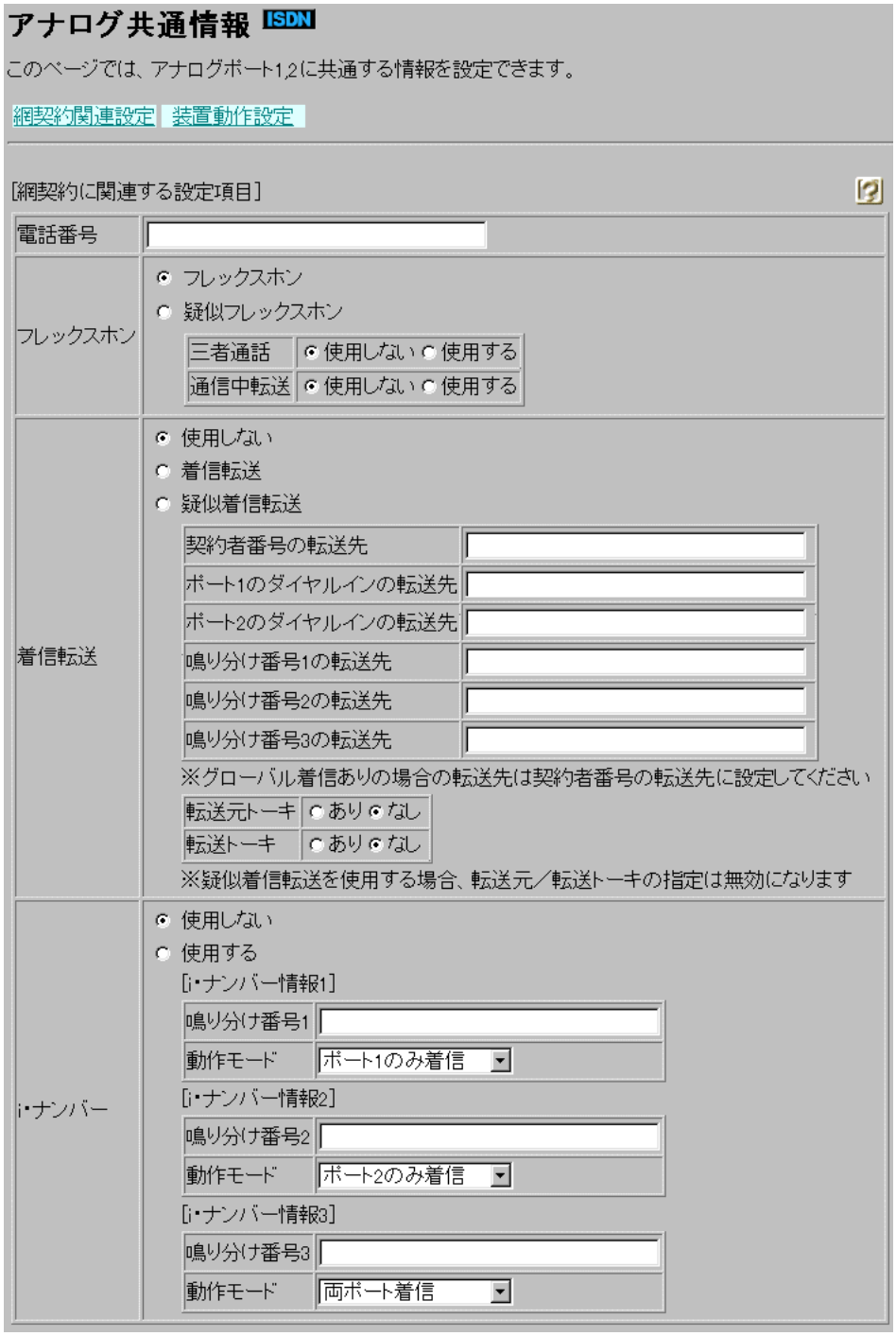
SA有効時間

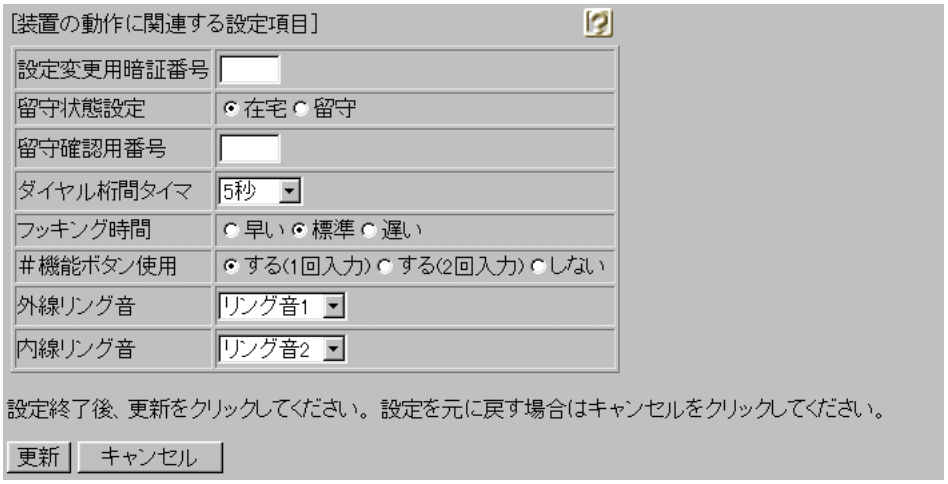
IKE SAの有効期限を時間で指定します。指定した時間が経過した時点、SAの有効期限が切れ、IKE SA情報や鍵情報がIKEによって自動的に更新されます。以下の範囲でSA有効時間を指定します。

有効範囲）
1～24時間
10～1440分
600～86400秒

アナログ共通情報

【操作】「詳細設定メニュー」→アナログ設定「アナログ共通情報」





[網契約に関連する設定項目]

ISDN回線加入契約の内容に関する情報を設定します。

電話番号

自局の電話番号を半角数字32桁以内で指定します。区切り文字として、－、(、)を使用します。この番号は、発信者番号通知機能を使用する場合、アナログ発信時に網に通知します。また、着信時に網が自局番号を通知しない場合、当番号をシステムログで表示します。

フレックスホン

NTTとの契約により、三者通話、および通信中転送機能を使用する場合は、“フレックスホン”を選択します。NTTと未契約で擬似的に使用する場合は、“疑似フレックスホン”を選択します。

三者通話

通話中にその通話を保留して、別の相手に電話をかけることができます。同時に三者で通話することもできます。

通信中転送

通話中に別の相手に電話を転送することができます。

着信転送

かかってきた電話を、契約者番号、ダイヤルイン番号、または鳴り分け番号ごとに別の電話に自動で転送することができます。転送先電話番号を32桁以内で指定します。区切り文字として、－、(、)を使用します。

使用しない

着信転送を行いません。

着信転送

着信転送を使用するにはNTTと契約する必要があります。

着信転送を使用する場合に、以下の「転送元トーキ」を流すかどうかを指定します。
「電話が転送されます。」など

着信転送を使用する場合に、以下の「転送トーキ」を流すかどうかを指定します。
「ただいま電話を転送しますので、そのままお待ちください。」など

疑似着信転送

疑似着信転送機能を使用して着信転送を行います。疑似着信転送機能を使用すると、NTTとの契約がなくても疑似的に着信転送を利用できます。

ｉ・ナンバー

本装置の背面のTEL1、TEL2に接続しているアナログ機器を鳴り分けることができます。
ｉ・ナンバーを使用するにはNTTと契約する必要があります。ｉ・ナンバーを使用するかどうかを選択します。使用する場合は、以下の項目を指定します。

鳴り分け番号

鳴り分け番号1には、契約者番号を半角数字32桁以内で指定します。鳴り分け番号2、3には、ｉ・ナンバーサービス契約時に通知する契約者番号以外の番号を半角数字32桁以内で指定します。

動作モード

ｉ・ナンバーで着信があった場合の動作を選択します。

[装置の動作に関連する設定項目]

本装置につなぐアナログ機器を利用する場合、その接続機器の動作に関する情報を設定します。

設定変更用暗証番号

外線からの設定変更時に使用する暗証番号を0～9までの数字4桁で指定します。

留守状態設定

“在宅”、または“留守”を選択します。

“留守”を選択する場合、外線からサブアドレス（留守確認用番号）つき発信することで、無課金で留守状態を確認できます。留守確認用番号の指定が必要です。

留守確認用番号

外線からの留守状態確認時に使用する確認用番号を0～9までの数字4桁で指定します。

ダイヤル桁間タイマ

アナログポートに接続する電話やFAXからダイヤルするときに、最後のダイヤル入力からINSネット64に発信するまでの時間を変更できます。

フッキング時間

電話機のキャッチボタン（フックボタン、フラッシュボタン）が正常に動作しない場合に認識時間を変更できます。

＃機能ボタン使用

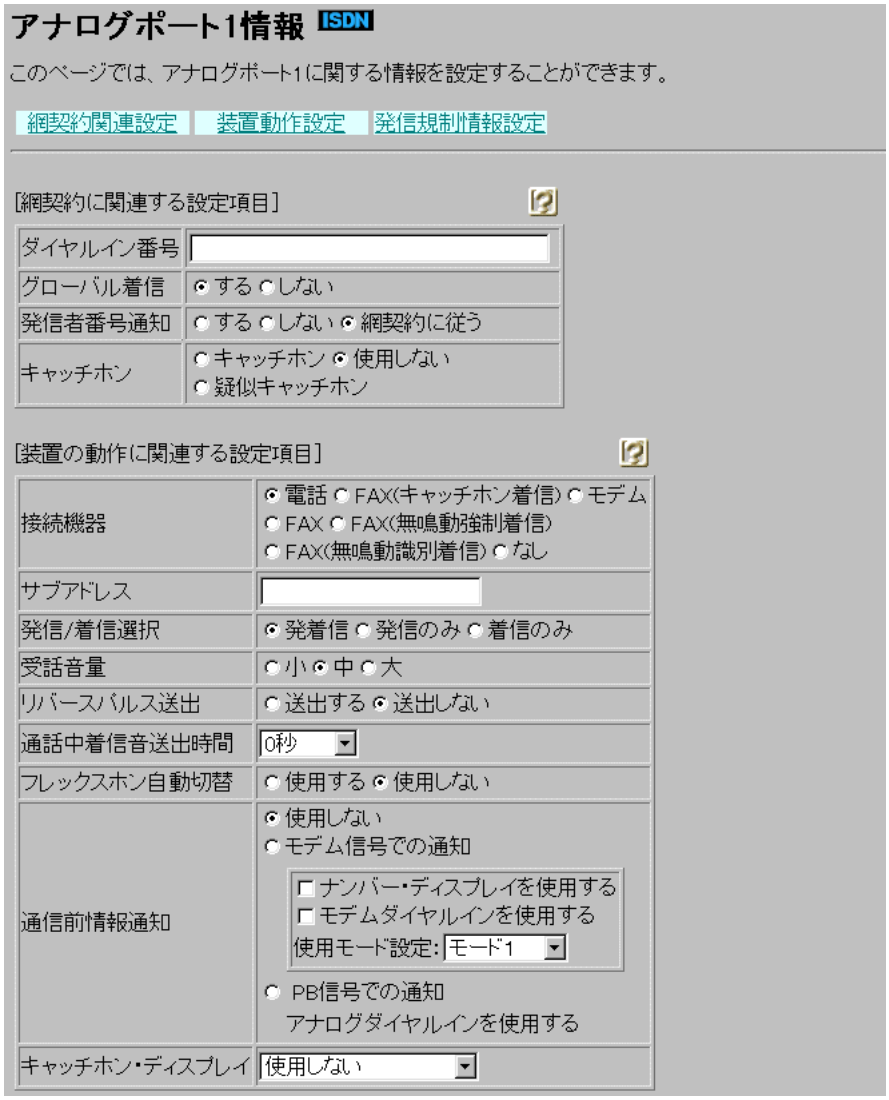
「＃」を機能ボタンとして使用するかどうかを選択します。

外線／内線リング音

外線用、内線用のリング音を選択できます。リング音1は「リーン・リーン」、リング音2は「リンリン・リンリン」、リング音3は「リンリンリン・リンリンリン」です。

アナログポート1／2情報

【操作】「詳細設定メニュー」→アナログ設定「アナログポート1／2情報」



アナログポート1情報 ISDN

このページでは、アナログポート1に関する情報を設定することができます。

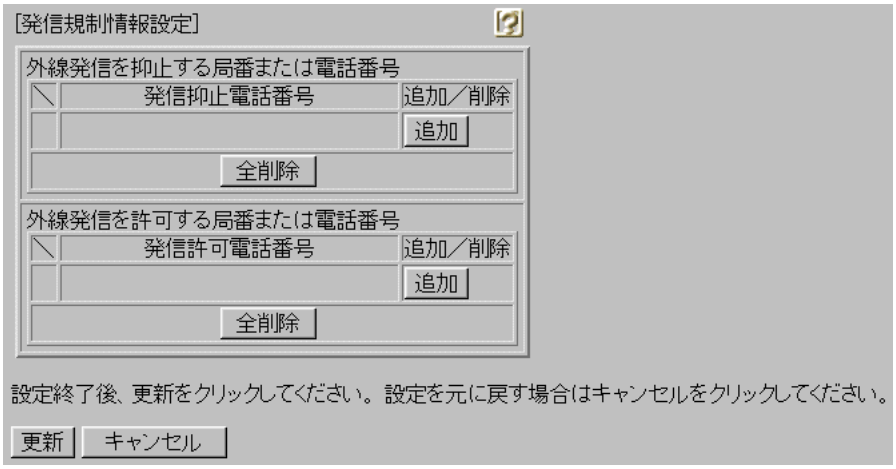
網契約関連設定　装置動作設定　発信規制情報設定

[網契約に関連する設定項目]

ダイヤルイン番号	
グローバル着信	◉する ○しない
発信者番号通知	○する ○しない ◉網契約に従う
キャッチホン	○キャッチホン ◉使用しない ○疑似キャッチホン

[装置の動作に関連する設定項目]

接続機器	◉電話 ○FAX(キャッチホン着信) ○モデム ○FAX ○FAX(無鳴動強制着信) ○FAX(無鳴動識別着信) ○なし
サブアドレス	
発信/着信選択	◉発着信 ○発信のみ ○着信のみ
受話音量	○小 ◉中 ○大
リバースパルス送出	○送出する ◉送出しない
通話中着信音送出時間	0秒
フレックスホン自動切替	○使用する ◉使用しない
通信前情報通知	◉使用しない ○モデム信号での通知 □ナンバー・ディスプレイを使用する □モデムダイヤルインを使用する 使用モード設定: モード1 ○PB信号での通知 アナログダイヤルインを使用する
キャッチホン・ディスプレイ	使用しない



[網契約に関連する設定項目]

ISDN回線加入契約の内容に関する情報を設定します。

ダイヤルイン番号

ダイヤルイン番号を32桁以内で指定します。

INSネット64の契約時にダイヤルインサービスを契約している場合は、ダイヤルイン番号を指定することにより、本装置背面のTEL1、TEL2に接続しているアナログ機器を呼び分けることができます。

ダイヤルイン番号をどれかのポートに割り振り、割り振った側の設定を行います。

ダイヤルインサービスの契約で、「グローバル着信利用を選択しない」場合は、契約者回線番号もダイヤルイン番号として利用できます。

INSネット64の契約内容（ダイヤルインサービス、グローバル着信利用）、本装置の設定内容（ダイヤルイン番号、グローバル着信）、および相手がダイヤルする番号によって着信条件が変わります。

グローバル着信

INSネット64契約の内容が以下のどちらかに該当し、相手が契約者回線番号をダイヤルする場合、この指定により、本装置背面のTEL1、TEL2に接続しているアナログ機器の呼び出しを指定できます。

・ダイヤルインサービスを契約していない

・ダイヤルインで「グローバル着信利用」で契約している

グローバル着信するかどうかを選択します。呼び出しをするポートには、“する”を選択します。

INSネット64の契約内容（ダイヤルインサービス、グローバル着信利用）、本装置の設定内容（ダイヤルイン番号、グローバル着信）、および相手がダイヤルする番号によって着信条件が変わります。

こんな事に気をつけて

ダイヤルインサービスを契約していない場合は、グローバル着信を“する”にしてください。

発信者番号通知

発信者番号（契約者回線番号、ダイヤルイン番号、または鳴り分け番号）を着信者側に通知するサービスです。

発信者はポートごとに発信者番号を通知するかどうか、または網契約内容に従うかを選択できます。網契約に従う場合は、INSネット64申込時の契約内容に従います。

ダイヤルイン番号、または鳴り分け番号を通知する場合は、「ダイヤルイン番号」に通知する電話番号を指定します。

キャッチホン

通話中に別の相手からの着信があると、その通話を保留して新しい相手と通話することができます。キャッチホンを使用するにはNTTと契約する必要があります。

フレックスホン未契約の場合は、“疑似キャッチホン”を選択すると疑似的にキャッチホンが使用できます。

接続機器でモデム／FAXを指定するポートには、通信を妨げないためにコールウェイティング動作は行いません。

[装置の動作に関連する設定項目]

本装置のアナログポート1（TEL1）につないだアナログ機器を利用する場合、その接続機器の動作に関する情報を設定します。

接続機器

アナログポート1に接続する機器を以下の中から選択します。

電話

電話を接続する場合に指定します。

FAX（キャッチホン着信）

電話つきFAXを接続し、発信時はFAXの動作、着信時は電話として動作する場合に指定します。

モデム

モデムを接続する場合に指定します。

FAX

FAXを接続する場合に指定します。

FAX（無鳴動強制着信）

無鳴動着信機能（FAXを受信するときに、着信音を鳴らさずに応答する機能）を備えたFAXを接続する場合に指定します。

FAX（無鳴動識別着信）

無鳴動着信機能を備えたFAXを接続する場合に指定します。相手がG3FAXの場合だけ無鳴動着信を行います。

なし

アナログポート1は使用できません。

サブアドレス

サブアドレスを半角英数字19文字以内で指定します。

サブアドレス番号を指定し、相手が発信するときに、そのサブアドレスを指定することで、本装置背面のTEL1、TEL2に接続しているアナログ機器を呼び分けることができます。

なお、相手がアナログ電話網から発信する場合は、サブアドレスが使用できないので、この指定による呼び分けは利用できません。

本装置のサブアドレス設定、および相手側のサブアドレスの利用状況によって着信条件が変わります。

発信／着信選択

該当するポートが発信専用／着信専用、または発着信可能かどうかを選択します。

受話音量

該当するアナログポートの受話音量を選択します。

リバースパルス送出

該当するアナログポートでリバースパルス信号を送出するかどうかを選択します。

リバースパルスは、外から電話がかかってきて通話中に相手から電話を切った場合に、通話が終了したことを通知する信号です。たとえば、留守番電話で相手が切断すると同時にメッセージの録音を終了する機能を備えているときに有効です。

通話中着信音送出時間

外線通話中に第三者から着信があると通話中に着信音が聞こえます。この通話中に着信音を送出し続ける時間を0～30秒の範囲で指定します。0を指定すると第三者が切断するまで送出し続けます。

なお、指定時間が経過し、通話中に着信音が聞こえなくなっても第三者が切断しなければ、フレッキングにより第三者と通話ができます。

フレックスホン自動切替

フレックスホン自動切り替えを使用するかどうかを選択します。

この機能は、フレックスホンを利用して通話中に、話している相手が電話を切断した場合、自動的に保留になっている相手と通話できる機能です。

通信前情報通知

アナログポートでの通信（通話）を開始する前にアナログ通信機器に対して情報を通知する機能です。以下の項目から選択します。

使用しない

通信前情報通知機能を使用しません。

モデム信号での通知

ナンバー・ディスプレイ対応アナログ機器を使用している場合、“ナンバー・ディスプレイを使用する”をチェックすると、アナログ機器に相手番号を表示できます。
NTTのナンバー・ディスプレイサービスを契約していない場合、アナログ電話網からの電話に関しては、相手番号が表示されません。また、相手側の契約内容により相手番号が表示されない場合もあります。
使用モード設定を“モード1”にして正常に動作しない場合は、“モード2”にします。

モデムダイヤルイン対応アナログ機器を使用しているの場合、“モデムダイヤルインを使用する”をチェックすると、電話やFAXなど機能ごとに個別の番号を持つことができます。着信したときに、モデム信号で相手電話番号を電話機に通知します。
使用モード設定を“モード1”にして正常に動作しない場合は、“モード2”にします。

PB信号での通知

アナログダイヤルイン対応アナログ機器を使用しているの場合、電話やFAXなど機能ごとに個別の番号を持つことができます。着信するときに、PB信号で相手電話番号を電話機に通知します。

キャッチホン・ディスプレイ

キャッチホン・ディスプレイ対応アナログ通信機器を使用している場合、「キャッチホン・ディスプレイ」の設定を「使用する（モード1）」にすることにより、アナログ通信機器に話中着信相手番号を表示することができます。

キャッチホン・ディスプレイ機能を使用している場合は、キャッチホンの設定を行う必要があります。

NTTのナンバー・ディスプレイサービスを契約していない場合、アナログ電話網からの電話に関しては、相手電話番号が表示されません。また、相手側の契約内容により相手電話番号が表示されない場合もあります。

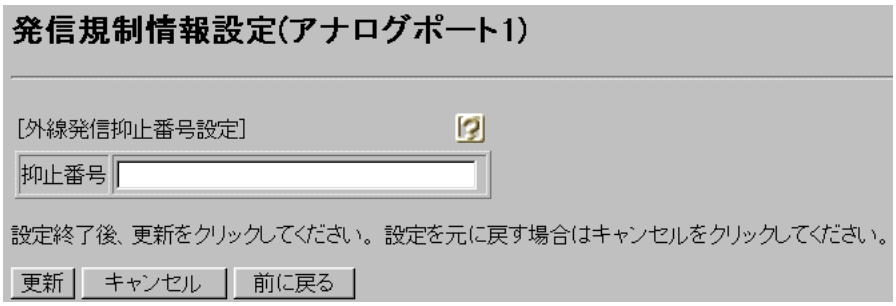
「使用する（モード1）」で正常に動作しない場合は、「使用する（モード2）」、「使用する（モード3）」、または「使用する（モード4）」にします。

[発信規制情報設定]

事前に登録した電話番号への外線発信が抑止できます。また、抑止した局番内の特定相手だけ外線発信を許可することもできます。現在、設定されている発信規制情報の一覧です。処理するボタンをクリックし、次のページに進みます。

発信規制情報設定（発信抑止）

【操作】「詳細設定メニュー」→アナログ設定「アナログポート1／2情報」→［発信規制情報設定］



［外線発信抑止番号設定］

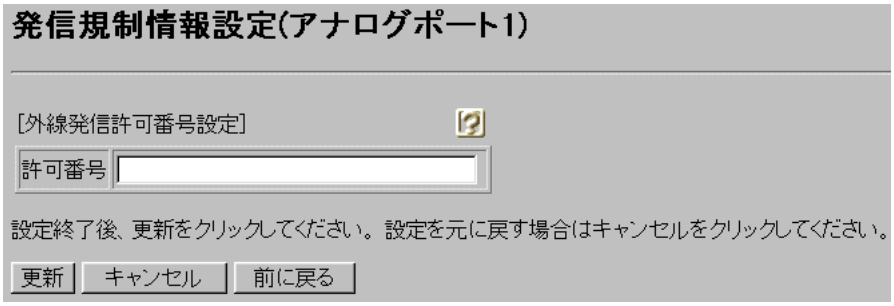
あらかじめ外線発信を抑止する局番や電話番号を登録しておきます。ポートごとに発信を抑止する番号を指定できます。

抑止番号

外線発信を抑止する番号を半角数字32桁以内で指定します。

発信規制情報設定（発信許可）

【操作】「詳細設定メニュー」→アナログ設定「アナログポート1／2情報」→［発信規制情報設定］



［外線発信許可番号設定］

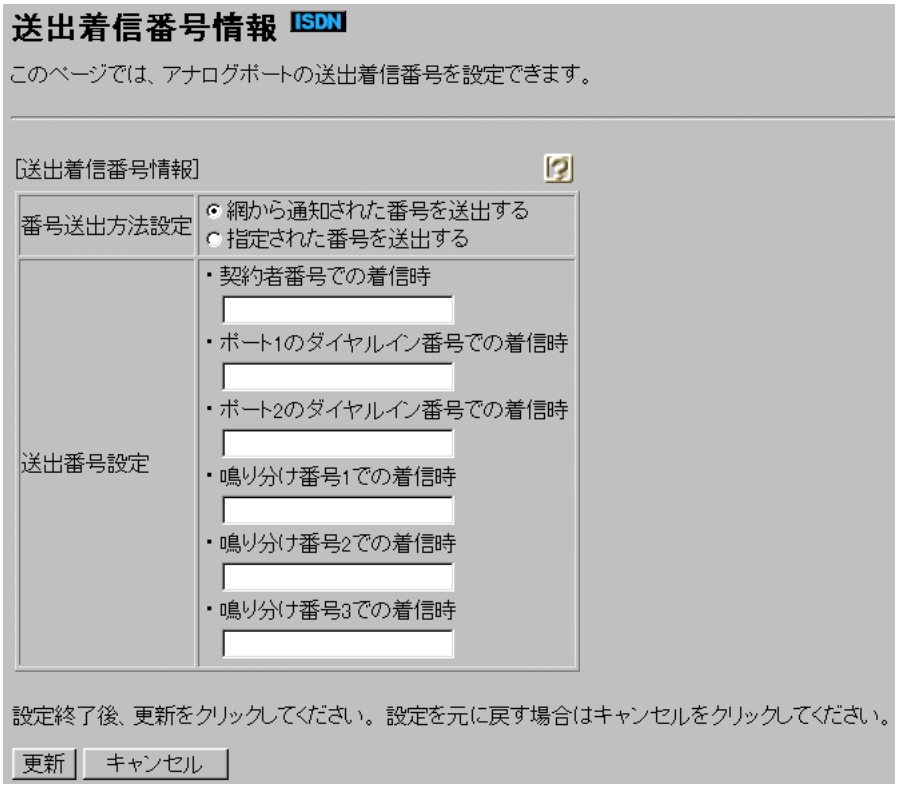
あらかじめ外線発信を規制する局番や電話番号を登録しておきます。ポートごとに発信を許可する番号を指定できます。

許可番号

外線発信を許可する番号を半角数字32桁以内で指定します。

送出着信番号情報

【操作】「詳細設定メニュー」→アナログ設定「送出着信番号情報」



[送出着信番号情報]

モデムダイヤルイン、アナログダイヤルイン時に、接続機器に送出する着信番号について設定できます。

番号送出方法設定

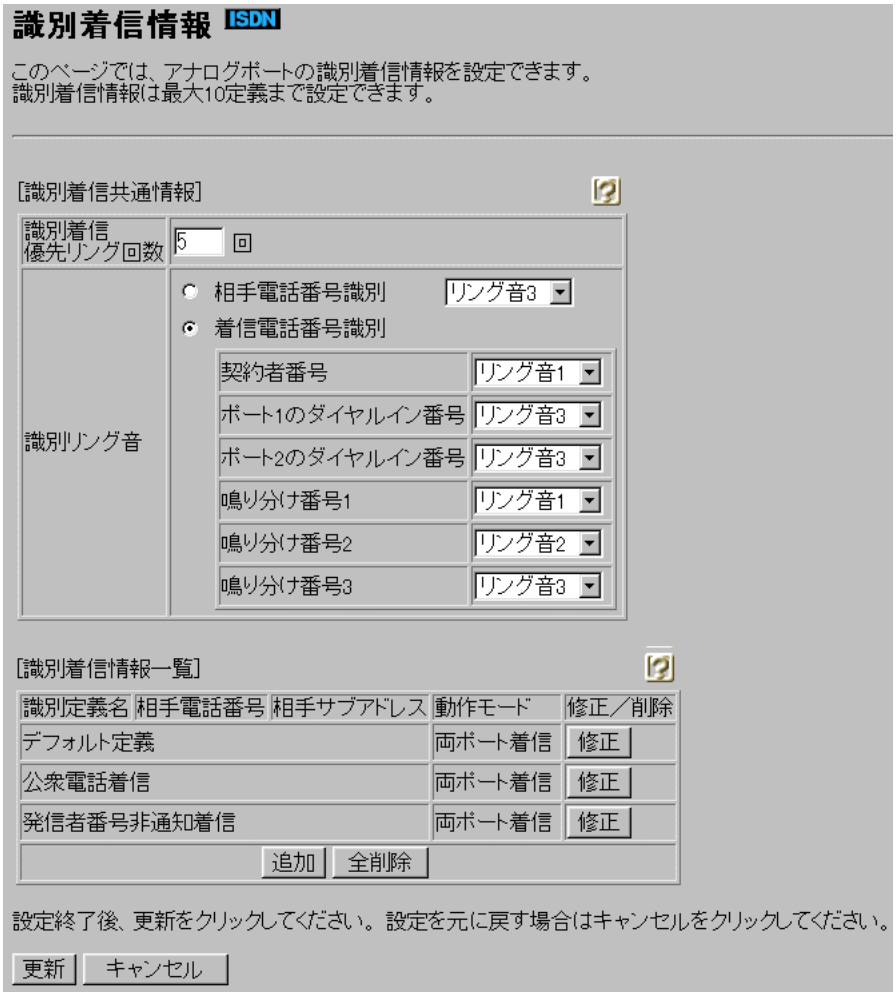
接続機器に着信番号の送出する方法を選択できます。

送出番号設定

それぞれの着信番号ごとに、機器に送出する番号を20桁以内で指定できます。なお、アナログダイヤルイン時には、指定した番号の下4桁を送出します。

識別着信情報

【操作】「詳細設定メニュー」→アナログ設定「識別着信情報」



[識別着信共通情報]

着信時に相手の発信者番号によって異なる着信時の呼び出し動作を指定できます。ここでは、識別着信情報の一覧にある相手先すべてに共通する動作を指定します。

識別着信優先リング回数

優先ポートとして指定したポートだけ呼び出すリングの回数を指定します。指定回数呼び出しても受話器を取らない場合は、両ポートの呼び出しを行います。1～10の範囲で指定できます。

識別リング音

識別着信用のリング音を選択できます。リング音1は「リーン・リーン」、リング音2は「リンリン・リンリン」、リング音3は「リンリンリン・リンリンリン」です。

“相手電話番号識別”を選択する場合は、「識別着信情報一覧」で定義した相手から着信かどうかを識別し、選択したリング音で鳴動します。“着信電話番号識別”を選択する場合は、着信する番号を識別し、選択するリング音で鳴動します。

[識別着信情報一覧]

現在、設定されている識別着信情報の一覧です。定義はデフォルト定義、公衆電話着信、発信者番号非通知着信と、それ以外に10個まで設定できます。処理するボタンをクリックし、次のページに進みます。

デフォルト定義

識別着信情報で、相手先に設定されていない相手からかかってきた電話の着信時の動作を指定します。

公衆電話着信

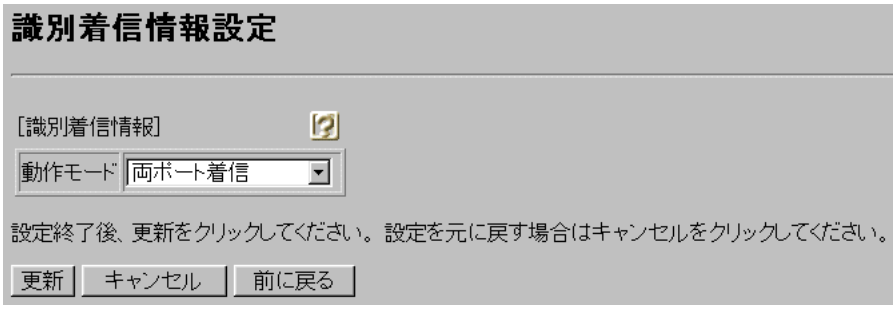
公衆電話からかかってきた電話の着信時の動作を指定します。

発信者番号非通知着信

発信者番号を通知してこない電話の着信時の動作を指定します。

識別着信情報設定（デフォルト定義）

【操作】「詳細設定メニュー」→アナログ設定「識別着信情報」→［識別着信情報一覧］



［識別着信情報］

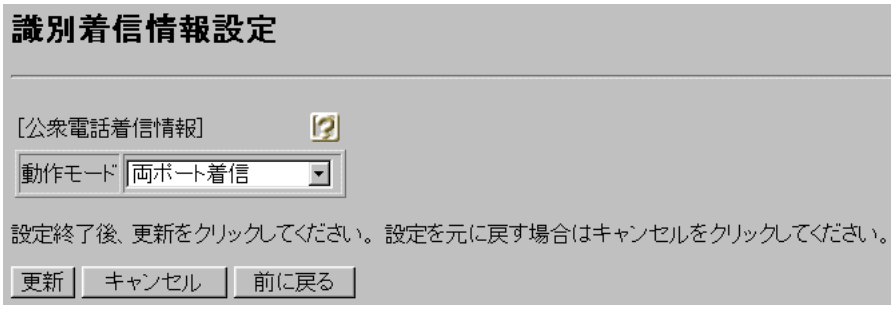
デフォルト定義には、相手先に設定していない相手からの着信の場合の動作を指定します。

動作モード

相手先に設定していない相手からの着信があるときの動作を指定します。

識別着信情報設定（公衆電話着信）

【操作】「詳細設定メニュー」→アナログ設定「識別着信情報」→［識別着信情報一覧］



［識別着信情報］

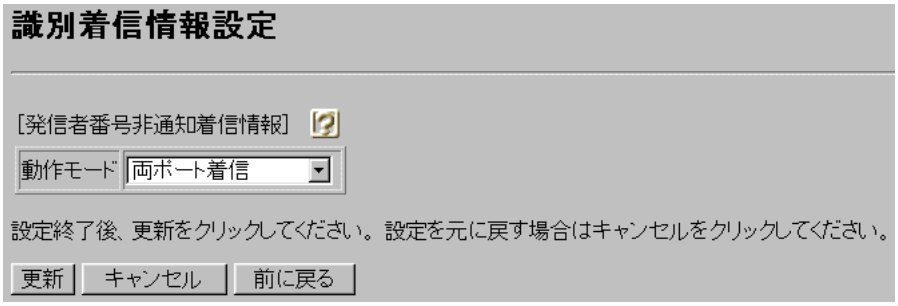
公衆電話着信には、公衆電話からの着信の場合の動作を指定します。

動作モード

公衆電話からの着信があるときの動作を指定します。

識別着信情報設定（発信者番号非通知着信）

【操作】「詳細設定メニュー」→アナログ設定「識別着信情報」→［識別着信情報一覧］



［識別着信情報］

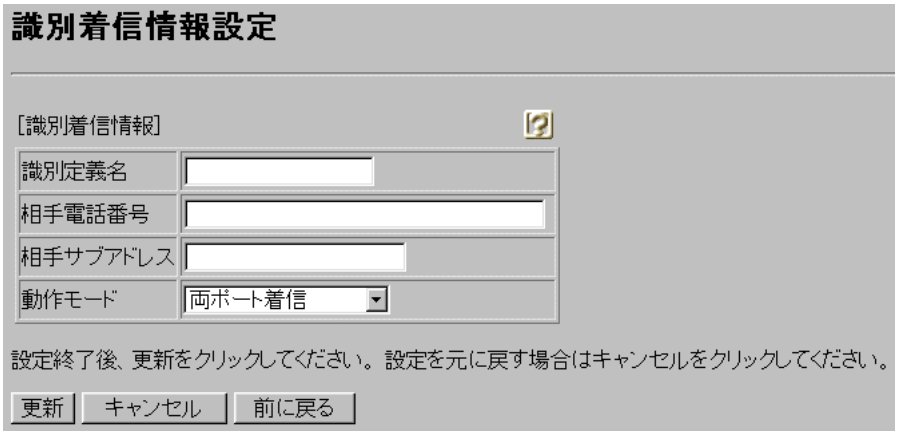
発信者番号非通知には、相手から発信者番号が通知されない場合の動作を指定します。公衆電話からの着信は、発信者番号非通知着信に含まれません。

動作モード

発信者番号非通知の着信があるときの動作を指定します。

識別着信情報設定

【操作】「詳細設定メニュー」→アナログ設定「識別着信情報」→［識別着信情報一覧］



［識別着信情報］

相手電話番号および相手サブアドレスをキーとして相手を特定し、着信時の呼び出し動作を変えることができます。

相手先の定義は10個まで指定します。（識別着信用リング音で呼び出します）

識別定義名

登録する識別着信情報の名称を半角英数字16文字以内で指定します。

相手電話番号

登録する相手の電話番号を市外局番から半角数字32桁以内で指定します。

相手サブアドレス

必要に応じて、着信相手を識別するためのサブアドレスを半角英数字19文字以内で指定します。

動作モード

該当相手からの着信があった時の動作を指定します。

こんな事に気をつけて

利用する際には、NTTのナンバー・ディスプレイサービスの契約が必要です。ただし、相手の方がINSネット64から発信者番号を通知して電話をかけて来た場合は、未契約の場合でも利用できます。

第５章　活用例（アナログ設定）

5

この章では、
本装置につないだアナログ機器を利用する方法を説明します。

スタンバイモードで使用する

データ通信を行わない場合などは、必要最小限の部分だけを動作させ、本装置の消費電力を抑えることができます。「スタンバイモード」では、アナログ機器だけが使用できます。

こんな事に気をつけて

「スタンバイモード」にすると、10BASE-T ポートにつないだ機器どうしで通信ができなくなります。

スタンバイモードにする

「通常モード」と「スタンバイモード」の切り替えは、アナログポートにつないだアナログ機器で行います。

1. **受話器を上げ、ツーという音が聞こえることを確認します。**

こんな事に気をつけて

利用する回線に「専用線」を設定している場合は、「通常モード」と「スタンバイモード」の切り替えはできません。

2. **[*] [5] をダイヤルします。**
3. **ビジートーン（プープープーという話中の音）が聞こえます。**
4. **受話器を置きます。**

スタンバイモードで動作中は、本装置の POWER ランプが緑色で点滅（点灯約2.5秒、消灯約0.5秒）します。POWER ランプ以外は消灯します。

通常モードにする

1. **受話器を上げ、ツーという音が聞こえることを確認します。**
2. **[*] [6] をダイヤルします。**
3. **ビジートーン（プープープーという話中の音）が聞こえます。**
4. **受話器を置きます。**

ヒント

◆ すぐにモードを変更するには

本装置出荷時には番号をダイヤルして [#] を1回押すと、すぐにモードを変更するようになっています。「＃機能ボタン使用」の設定はアナログ設定の「アナログ共通情報」で設定します。

アナログ機器を利用するにあたって

アナログ機器は、本装置で設定を行うとさらに便利な使い方ができます。電話機をつなぐ場合は、アナログポートにモジュラを差し込むだけで使用できます。

こんな事に気をつけて

- **電話機を1台だけつなぐ場合は、TEL1ポートにつないでください。また、TEL2ポートを使用しないように設定を変更してください（アナログ設定の「アナログポート2情報」で「接続機器」を「なし」に設定してください）。**
- **本装置を専用線で利用している場合は、アナログ機器は使うことができません（電話機を使用してIPアドレスの設定はできます）。**
- **ナンバー・ディスプレイ対応アナログ機器の機種によっては、発信者番号が正常に表示されない場合があります。**

電話の受話音量を調節する

ここでは、アナログポートのTELポート1につないだ電話機の受話音量を設定する場合を例に説明します。

1.　詳細設定メニューのアナログ設定で「アナログポート1情報」をクリックします。

「アナログポート1情報」ページが表示されます。

2.　［装置の動作に関連する設定項目］で以下の項目を指定します。

- 受話音量　→「小」、「中」、または「大」を選択する

3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

ヒント

◆ すぐに発信するには

本装置出荷時には、番号をダイヤルして [#] を1回押すと、すぐに発信するようになっています。「＃機能ボタン使用」の設定は、アナログ設定の「アナログ共通情報」ページで設定します。

◆ LCR機能などの付いた電話機を使うときには

LCR機能を備えた電話機で相手先とうまくつながらない場合は、アナログ設定の「アナログ共通情報」の順に選択し、「ダイヤル桁間タイマ」の時間を長め（10秒程度）に設定してください。

電話機のダイヤルで操作する手順の一覧を付録に載せています。

☛ 参照 「ダイヤル操作早見表」（P.674）

内線通話・内線転送機能を使う

■ 内線通話をする

1. 受話器を上げ、ツーという音が聞こえることを確認します。
2. ✱ 0 と押すと、呼び出し音が鳴ります。
3. 受話器を置いて、通話を終了します。

■ 外からかかってきた電話をもう一方のアナログポートに転送する

内線転送には、転送する側の電話に相手が出たあとに転送する場合と相手が応答する前にそのまま転送する場合の2種類があります。

ほかのアナログポートが応答したあとに転送する

1. 通話中に受話器のフックを押し（以降フッキングと呼びます）、電話を保留にします。

   第2ダイヤルトーン（プップップッという音）が聞こえてきます。

2. ✱ 0 と押して、もう一方のアナログポートにつないだ電話機を呼び出します。

補足 フッキングを行うと、保留中の相手と再度通話できます。

ヒント

◆ フッキングとは

受話器のフックを押してすぐに離すと、通話を保留できます。これを「フッキング」と言います（フックを長く押しつづけると通話が切れてしまいます）。アナログ設定の「アナログ共通情報」の「フッキング時間」で、フックを押してから通話が切れるまでの時間を変えられます。

電話機にフックボタン、キャッチボタン、またはフラッシュボタンがある場合は、このボタンを使って通話を保留にします。

3. 相手が出たら、転送することを伝えます。
4. 受話器を置いて、通話を転送します。

   もう一方のアナログポートで、保留されていた相手と通話できるようになります。

こんな事に気をつけて

もう一方のアナログポートが通話中の場合は、この機能を使うことができません。

ほかのアナログポートが応答する前に転送する

1.　通話中に受話器のフックを押し、電話を保留にします。

第2ダイヤルトーン（プップップッという音）が聞こえてきます。

2.　✱ 0と押して、もう一方のアナログポートにつないだ電話機を呼び出します。

補足 フッキングを行うと、保留中の相手と再度通話できます。

3.　受話器を置くと、通話が転送されます。

もう一方のアナログポートで受話器を取ると、保留されていた相手と通話できるようになります。

こんな事に気をつけて

- **もう一方のアナログポートが通話中の場合は、この機能を使うことができません。**
- **受話器を置いたあとは、外線電話に戻ることができません。**

登録した番号への発信を規制する

あらかじめ登録しておいた局番や電話番号への外線発信を規制します。規制した局番の電話番号でも、特定相手だけを外線発信を許可することもできます。また、ポートごとに発信を抑止する番号、発信を許可する番号を設定できます。

外線発信規制番号を設定する

ここでは、アナログポート1から局番「06」への発信を抑止するが、「06-2222-4444」への発信だけを許可する場合を例に説明します。

1.　詳細設定メニューのアナログ設定で「アナログポート1情報」をクリックします。

「アナログポート1情報」ページが表示されます。

2.　［発信規制情報設定］で「外線発信を抑止する局番または電話番号」の欄の［追加］ボタンをクリックします。

「発信規制情報（アナログポート1）」ページが表示されます。

3.　［外線発信抑止番号設定］で以下の項目を指定します。

- 抑止番号　→06

4.　［更新］ボタンをクリックします。

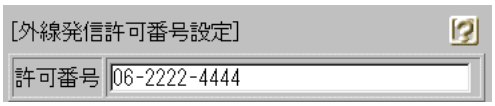
「アナログポート1情報」ページに戻ります。

5.　［発信規制情報設定］で「外線発信を許可する局番または電話番号」の欄の［追加］ボタンをクリックします。

「発信規制情報（アナログポート1）」ページが表示されます。

6.　［外線発信許可番号設定］で以下の項目を指定します。

- 許可番号　→06-2222-4444



7.　［更新］ボタンをクリックします。

「アナログポート1情報」ページに戻ります。

8.　［更新］ボタンをクリックします。

9.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

識別着信機能を使う

本装置には、以下のような識別着信機能があります。

- 相手電話番号識別：相手先電話番号（10件まで）を登録しておけば、登録した番号からの電話がかかってきたときに、呼び出し音を変えたり、指定のアナログポートだけを呼び出すことができます。また、相手ごとに着信条件を設定したり、着信拒否を設定できます。公衆電話からかけてきた電話や、発信者番号を通知してこない電話に対しても着信拒否などの動作を設定できます。

動作モード	説明
両ポート着信	着信時、両方のポートに接続された電話機の着信音が鳴ります。
ポート1のみ着信 ポート2のみ着信	着信時、指定したポートに接続された電話機だけ、着信音が鳴ります。
ポート1優先 ポート2優先	着信時、指定したポートに接続された電話機を優先して着信音が鳴ります。
着信拒否	着信しません。

- 着信電話番号識別：着信電話番号に応じて、呼び出し音を変えることができます。

こんな事に気をつけて

相手電話番号識別機能を利用する際は、NTTとの「INSナンバー・ディスプレイ」契約が必要です。ただし、相手の方がINSネット64から発信者番号を通知して電話をかけてきた場合は、未契約でも利用できます。

ヒント

◆リング音（呼び出し音）で区別する

本装置では、アナログ機器への着信音（外線リング音、内線リング音、識別リング音）を3種類のリング音（リング音1～3）で区別することができます。

リング音は、お好みに合わせて選択できます。ご購入時は以下のように設定されています。

・外線リング音　　リーン・リーン（リング音1）

・内線リング音　　リンリン・リンリン（リング音2）

・識別リング音　　リンリンリン・リンリンリン（リング音3）

■ 相手電話番号識別機能を使う（優先着信機能）

ここでは、以下のような場合を例に説明します。

- 「03-5555-5555」からの電話
  ポート1だけを識別リング音（リング音3）で呼び出す。このときポート1を5回以上呼び出しても受話器を取らない場合は、ポート2も識別リング音（リング音3）で呼び出す。
- 「03-5555-5555」以外からかかってきた電話
  ポート2だけを外線リング音（リング音1）で呼び出す。

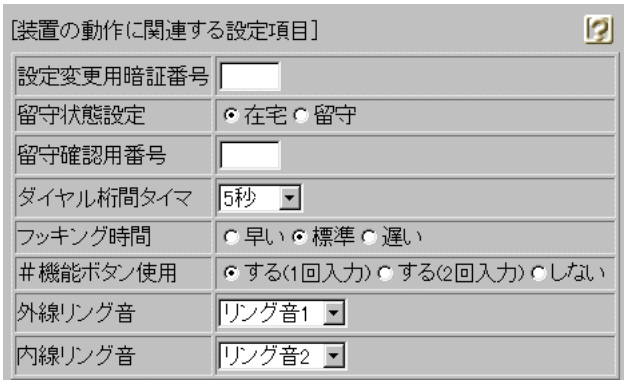
外線リング音を設定する

1.　詳細設定メニューのアナログ設定で「アナログ共通情報」をクリックします。

「アナログ共通情報」ページが表示されます。

2.　［装置の動作に関連する設定項目］で以下の項目を指定します。

- 外線リング音　　→リング音1



3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

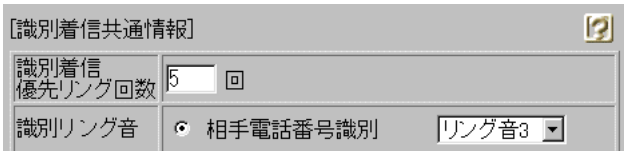
識別情報を設定する

1.　詳細設定メニューのアナログ設定で「識別着信情報」をクリックします。

「識別着信情報」ページが表示されます。

2.　［識別着信共通情報］で以下の項目を指定します。

- 識別着信優先リング回数　→5
- 識別リング音　→相手電話番号識別
→リング音3

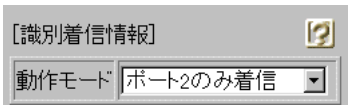


3.　［識別着信情報一覧］でデフォルト定義のテーブルの欄の［修正］ボタンをクリックします。

「識別着信情報設定」ページが表示されます。

4.　［識別着信情報］で以下の項目を指定します。

- 動作モード　→ポート2のみ着信



5.　［更新］ボタンをクリックします。

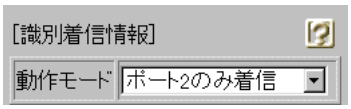
「識別着信情報」ページに戻ります。

6.　［識別着信情報一覧］で公衆電話着信のテーブルの欄の［修正］ボタンをクリックします。

「識別着信情報設定」ページが表示されます。

7.　［識別着信情報］で以下の項目を指定します。

- 動作モード　→ポート2のみ着信



8.　［更新］ボタンをクリックします。

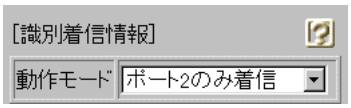
「識別着信情報」ページに戻ります。

9.　［識別着信情報一覧］で発信者番号非通知着信のテーブルの欄の［修正］ボタンをクリックします。

「識別着信情報設定」ページが表示されます。

10.　［識別着信情報］で以下の項目を指定します。

- 動作モード　→ポート2のみ着信



11.　［更新］ボタンをクリックします。

「識別着信情報」ページに戻ります。

12.　［識別着信情報一覧］で［追加］ボタンをクリックします。

「識別着信情報設定」ページが表示されます。

13.　［識別着信情報］で以下の項目を指定します。

- 識別定義名　→sikibetu1（ほかの識別定義名と重複しない任意の定義名を指定します。）
- 相手電話番号　→03-5555-5555
- 動作モード　→ポート1優先

14.　［更新］ボタンをクリックします。

「識別着信情報」ページに戻ります。

15.　［更新］ボタンをクリックします。

16.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

■ 着信電話番号識別機能を使う

ここでは、以下のような場合を例に説明します。

- 契約者回線番号（鳴り分け番号1）で着信したときは両ポートに着信し、リング音1で呼び出す。
- 追加番号（鳴り分け番号2）で着信したときはアナログポート1だけに着信し、リング音2で呼び出す。
- 追加番号（鳴り分け番号3）で着信したときはアナログポート2だけに着信し、リング音3で呼び出す。

こんな事に気をつけて

利用する際は、NTTとの「ｉ・ナンバーサービス」の契約が必要です。

ｉ・ナンバーを設定する

1.　詳細設定メニューのアナログ設定で「アナログ共通情報」をクリックします。

「アナログ共通情報」ページが表示されます。

2.　［網契約に関連する設定項目］で以下の項目を指定します。

- ｉ・ナンバー　→使用する
  ［ｉ・ナンバー情報1］
  動作モード　→両ポート着信
  ［ｉ・ナンバー情報2］
  動作モード　→ポート1のみ着信
  ［ｉ・ナンバー情報3］
  動作モード　→ポート2のみ着信

3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

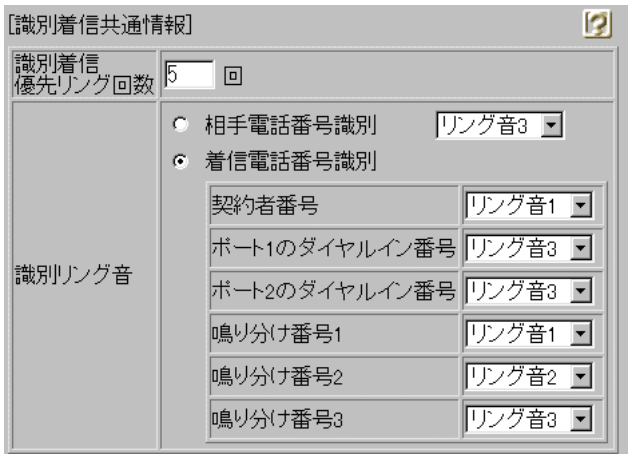
識別情報を設定する

1.　詳細設定メニューのアナログ設定で「識別着信情報」をクリックします。

「識別着信情報」ページが表示されます。

2.　［識別着信共通情報］で以下の項目を指定します。

- 識別リング音　→着信電話番号識別
  鳴り分け電話番号1　→リング音1
  鳴り分け電話番号2　→リング音2
  鳴り分け電話番号3　→リング音3



3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

疑似迷惑電話お断りを使う

迷惑電話をかからないように設定することができます。かけてほしくない相手の電話番号を登録しておき、その相手電話番号から電話がかかってきたときに、着信しないようにします。また、かかってきた電話が迷惑電話だった場合などに、通話中にダイヤル操作で相手の電話番号を登録し、以降、その電話番号からの電話は着信しないように設定できます。

こんな事に気をつけて

利用する際は、NTTとの「INSナンバー・ディスプレイ」契約が必要です。ただし、相手の方がINSネット64から発信者番号を通知して電話をかけてきた場合は、未契約でも利用できます。

疑似迷惑電話お断りを設定する

ここでは、以下のような場合を例に説明します。

- 「03-9999-9999」からの電話を着信拒否する

1.　詳細設定メニューのアナログ設定で「識別着信情報」をクリックします。

「識別着信情報」ページが表示されます。

2.　［識別着信情報一覧］で［追加］ボタンをクリックします。

「識別着信情報設定」ページが表示されます。

3.　［識別着信情報］で以下の項目を指定します。

- 識別定義名　→meiwaku（ほかの識別定義名と重複しない任意の定義名を指定します。）
- 相手電話番号　→03-9999-9999
- 動作モード　→着信拒否

4.　［更新］ボタンをクリックします。

「識別着信情報」ページに戻ります。

5.　［更新］ボタンをクリックします。

6.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

疑似迷惑電話お断りに登録する

通話中の相手電話番号を疑似迷惑電話お断りの対象として登録します。

こんな事に気をつけて

- **外線着信で通話中の相手だけ登録可能です。外線発信して通話した相手を登録することはできません。また、通話中に相手から切断され、ビジートーン送出中の状態では登録できません。**
- **識別着信情報にすでに 10 個の相手を設定してある場合は、この機能は利用できません。**
- **相手の方が発信者番号を通知しない契約を結んでいる、または通知しない設定をしている場合は、登録することはできません。**

1. 迷惑電話との通話中に、[*] [9] [#] と押します。

補足 ダイヤル時、識別着信情報には、以下の内容が登録されます。

- 識別定義名　　：meiwaku0 ～meiwaku9（登録済みの定義名は使用しません）
- 相手電話番号　　：通話相手の電話番号
- 相手サブアドレス：通話相手のサブアドレス
- 動作モード　　：着信拒否

2. 受話器を置きます。

以降、その相手からの電話は着信しません。

疑似キャッチホンを使う

外線で話をしているときに別の人から電話がかかってきた場合、通話中の方を保留にして、かけてきた方とお話しすることができます。フレックスホンサービスに含まれる「INSキャッチホン」と同様の機能ですが、疑似キャッチホンではNTTとの契約は必要ありません。

こんな事に気をつけて

- **データ通信中およびもう一方のアナログポート使用中は電話をかけてきた側で話し中になるので、この機能を利用できません。**
- **この機能を使用中は、もう一方のアナログポートは使用できません。また、データ通信も利用できません。**

補足 「接続機器」で「電話」および「FAX（キャッチホン着信）」以外を指定した場合は、通信を妨げないようにするため、疑似キャッチホンは利用できません。

疑似キャッチホン機能を設定する

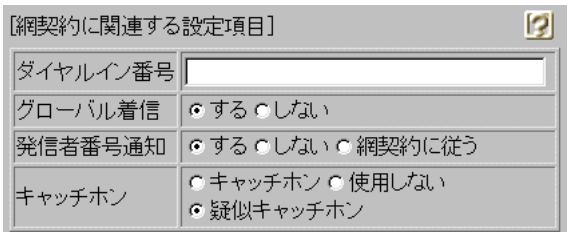
ここでは、電話機をアナログポート1につないだ場合を例に説明します。

1.　詳細設定メニューのアナログ設定で「アナログポート1情報」をクリックします。

「アナログポート1情報」ページが表示されます。

2.　［網契約に関連する設定項目］で以下の項目を指定します。

- キャッチホン　→疑似キャッチホン

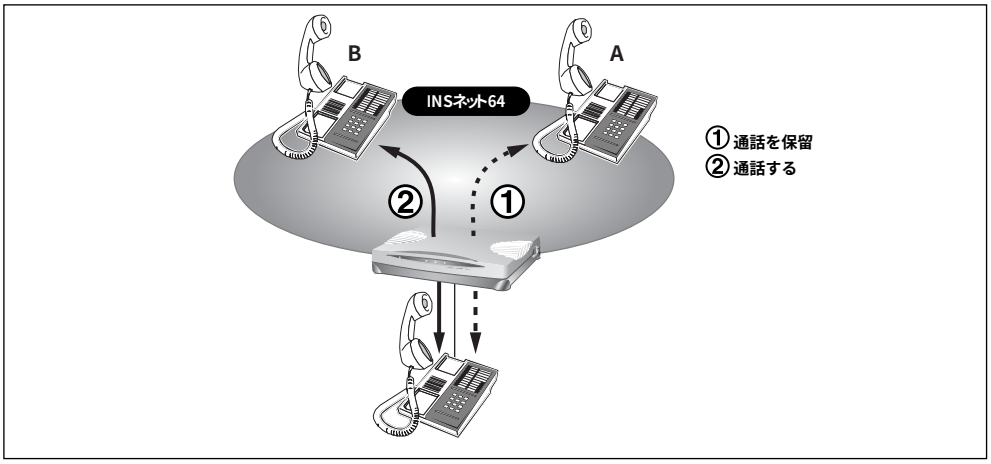


3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

疑似キャッチホンを使う



1.　相手Aとの通話中に相手Bから電話がかかってくると、受話器から通話中着信音が流れてきます。

補足
- 通話中着信音を送出する時間を指定しておくことができます。「アナログポート1／2情報」（P.337）を参照してください。
- 通話中着信音は、識別着信機能で相手に登録してあるリング音に対応して以下の表のようになります。
- 通話中着信音は、「識別着信共通情報」の「識別リング音」の設定により異なります。
「識別リング音」を「相手電話番号識別」に設定した場合、識別着信情報一覧で追加定義した相手からの着信は「プププッ」、それ以外の着信は「ププッ」となります。
「識別リング音」を「着信電話番号識別」に設定した場合、着信電話番号ごとに設定したリング音に対応して以下の表のようになります。

リング音設定	通話中着信
リング音1	ププッ
リング音2	プッ
リング音3	プププッ

2.　フッキングをします。

相手Bと通話できます。相手Aとの通話は保留になります。

3.　相手Aと通話するときは、もう一度フッキングをします。

相手Bとの通話が保留になり、相手Aと通話ができます。

4.　通話中の相手との通話を終了するときは、受話器を置きます。

リング音が鳴ります。

5.　受話器を取ります。

保留にしていた相手と通話できます。

疑似着信転送を使う

かかってきた電話が、あらかじめ設定しておいた着信転送の条件に一致すると、本装置は電話を転送します。フレックスホンサービスに含まれる「着信転送」と同様の機能ですが、疑似着信転送ではNTTとの契約は必要ありません。

こんな事に気をつけて

データ通信中およびアナログポート使用中は、電話をかけてきた側で話し中になるので、この機能を利用できません。

疑似着信転送機能を設定する

ここでは、以下のような場合を例に説明します。

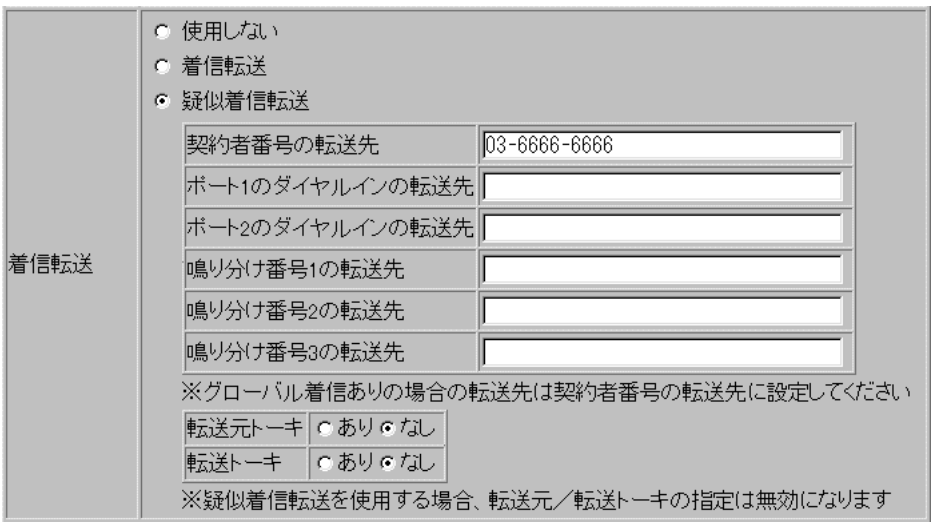
- 契約者番号にかかってきた電話を「03-6666-6666」に転送する

1.　詳細設定メニューのアナログ設定で「アナログ共通情報」をクリックします。

「アナログ共通情報」ページが表示されます。

2.　［網契約に関連する設定項目］で以下の項目を指定します。

- 着信転送　→疑似着信転送
  契約者番号の転送先　→03-6666-6666

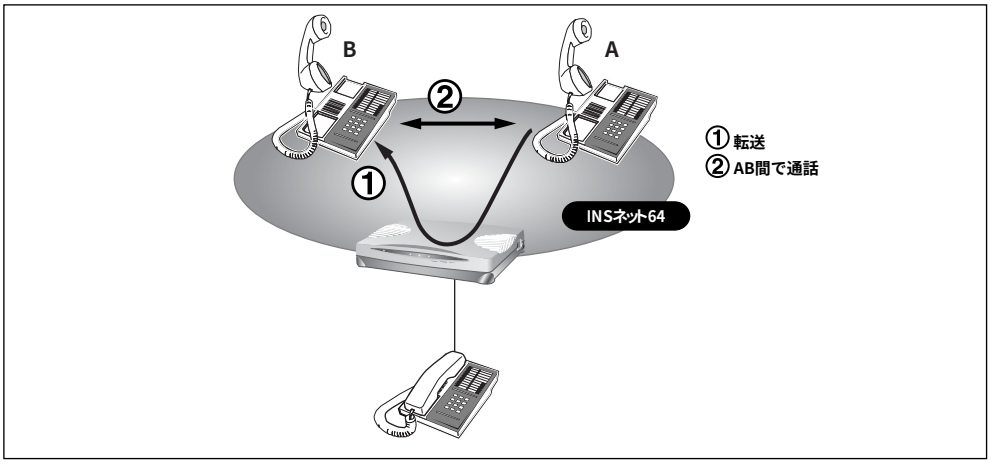


3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

疑似着信転送を使う



補足
- 本装置に電話機をつないでいなくても、疑似着信転送を利用できます。
- 着信相手から本装置までの電話料金は着信相手に課金され、本装置から転送先までの電話料金は、本装置側に課金されます。

疑似三者通話を使う

外線で話をしているときに、通話中の方を保留にして、別の人に電話をかけて通話することができます。また、3人で同時に通話することもできます。

こんな事に気をつけて

- **データ通信中およびもう一方のアナログポート使用中は電話をかけてきた側で話し中になるので、この機能を利用できません。**
- **この機能を使用中は、もう一方のアナログポートは使用できません。また、データ通信も利用できません。**

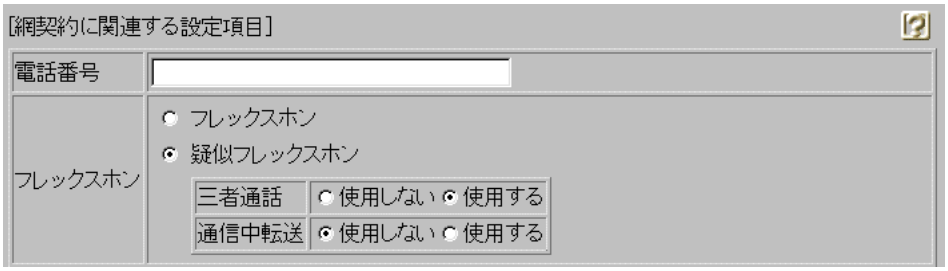
疑似三者通話機能を設定する

1.　詳細設定メニューのアナログ設定で「アナログ共通情報」をクリックします。

「アナログ共通情報」ページが表示されます。

2.　［網契約に関連する設定項目］で以下の項目を指定します。

- フレックスホン　→疑似フレックスホン
  三者通話　→使用する

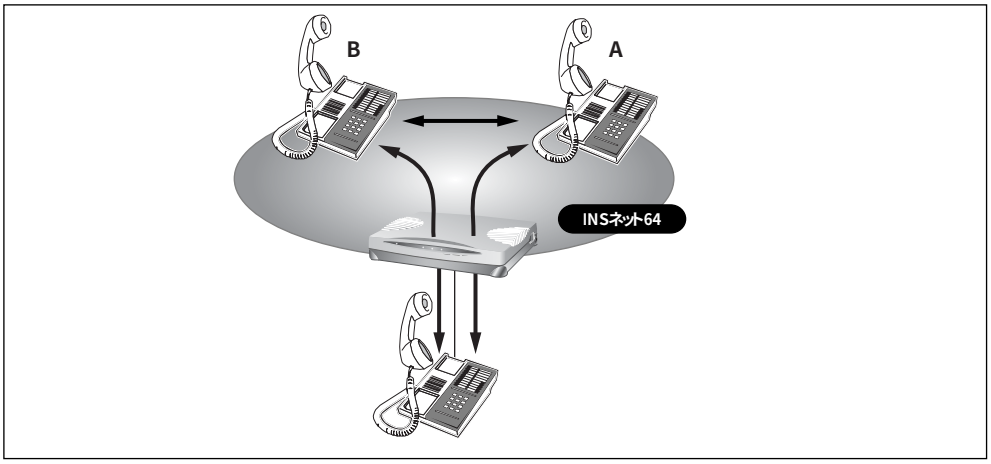


3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

疑似三者通話を使う



1.　相手Aとの通話中にフッキングをします。

通話が保留になり、第2ダイヤルトーン（プップップッという音）が聞こえてきます。

2.　相手Bへダイヤルします。

呼び出し音（プルルルという音）が聞こえます。相手Aには保留音が聞こえています。

3.　相手Bがでたら、通話を始めます。

この間、相手Aには保留音が聞こえています。

4.　ダブルフックをします。

「自分＋相手A＋相手B」の三者で同時通話ができます（ミキシングモード）。

5.　もう一度、ダブルフックをします。

相手Aとの通話は保留され、相手Bとの通話状態になります（切り替えモード）。

6.　通話中の相手との通話を終了するときは、受話器を置きます。

リング音が鳴ります。

7.　受話器を取ります。

保留中の相手と通話できます。

疑似通信中転送を使う

外線通話中の電話を、別の相手に転送することができます。

こんな事に気をつけて

- **データ通信中およびもう一方のアナログポート使用中は電話をかけてきた側で話し中になるので、この機能を利用できません。**
- **この機能を使用中は、アナログポートは使用できません。また、データ通信も利用できません。**

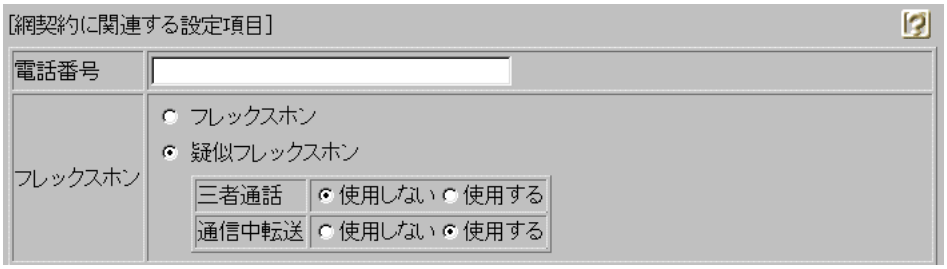
疑似通信中転送を設定する

1.　詳細設定メニューのアナログ設定で「アナログ共通情報」をクリックします。

「アナログ共通情報」ページが表示されます。

2.　［網契約に関連する設定項目］で以下の項目を指定します。

- フレックスホン　→疑似フレックスホン
  通信中転送　→使用する



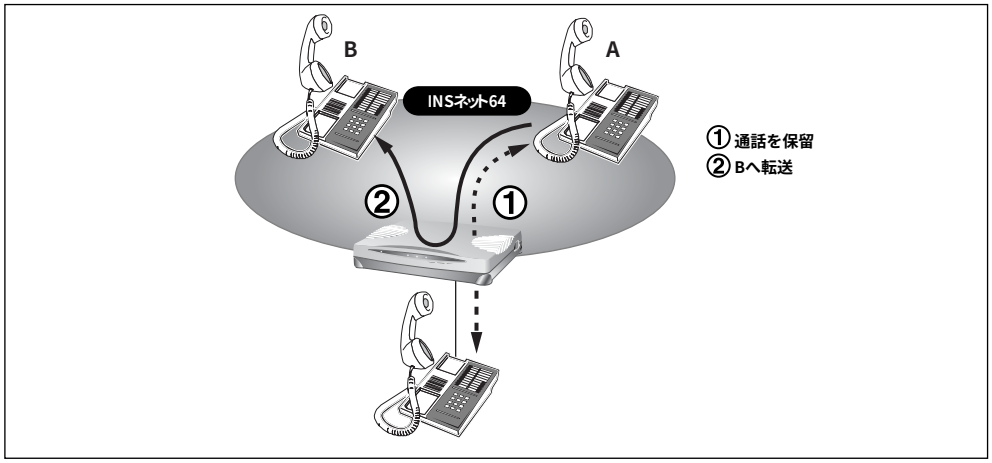
3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

疑似通信中転送を使う

「疑似通信中転送」機能を使って、通話中の電話を別の相手に転送できます。



1.　相手Aからの通話中にフッキングをします。

通話が保留になり、第2ダイヤルトーン（プップップッという音）が聞こえてきます。

2.　相手Bへダイヤルします。

呼び出し音（プルルルという音）が聞こえます。相手Aには、保留音が聞こえています。

3.　相手Bがでたら、転送中の電話があることを伝えます。

この間、相手Aには保留音が聞こえています。

4.　いったんフッキングをして、すぐに受話器を置きます。

相手Aと相手Bとで通話ができるようになります。

ヒント

◆疑似通信中転送したときの通話料はどうなるの？

疑似キャッチホンおよび疑似三者通話から、疑似通信中転送を行った場合、以下のようにそれぞれ発信者に課金されます。

	最初の通話（相手A）	2番目の通話（相手B）	疑似通信中転送	課金対象
疑似キャッチホンの場合	Aから 自分から	Bから Bから	できる できる	A、B 自分、B
疑似三者通話の場合	Aから 自分から	自分から 自分から	できる できる	A、自分 自分、自分

フレックスホンを使う

フレックスホンはNTTが提供するサービスで、「キャッチホン」「三者通話」「通信中転送」「着信転送」の4つがあります。必要な機能だけを選んで契約できます。

着信転送の設定を行う

ここでは、「着信転送」について以下の場合を例に説明します。

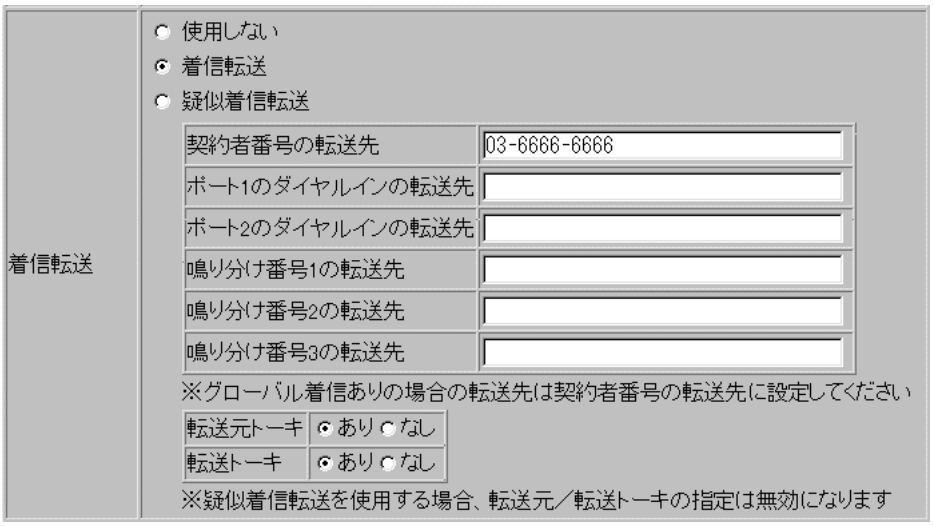
- 「着信転送」を使う
- 「転送元トーキ」「転送トーキ」ともに「あり」を選択する
- 契約者番号にかかってきた電話を「03-6666-6666」に転送する

1. 詳細設定メニューのアナログ設定で「アナログ共通情報」をクリックします。

「アナログ共通情報」ページが表示されます。

2. ［網契約に関連する設定項目］で以下の項目を指定します。

- 着信転送　→着信転送
  契約者番号の転送先　→03-6666-6666
  転送元トーキ　→あり
  転送トーキ　→あり



3. ［更新］ボタンをクリックします。

4. ［設定反映］ボタンをクリックします。

設定した内容が有効になります。

ヒント

◆転送元トーキ／転送トーキ

かかってきた電話をほかの番号に転送する際に流れるメッセージです。

・転送元トーキ：「電話が転送されます。」など

・転送トーキ　：「ただいま電話を転送しますので、しばらくお待ちください。」など

■ フレックスホンのいろいろな機能を使う

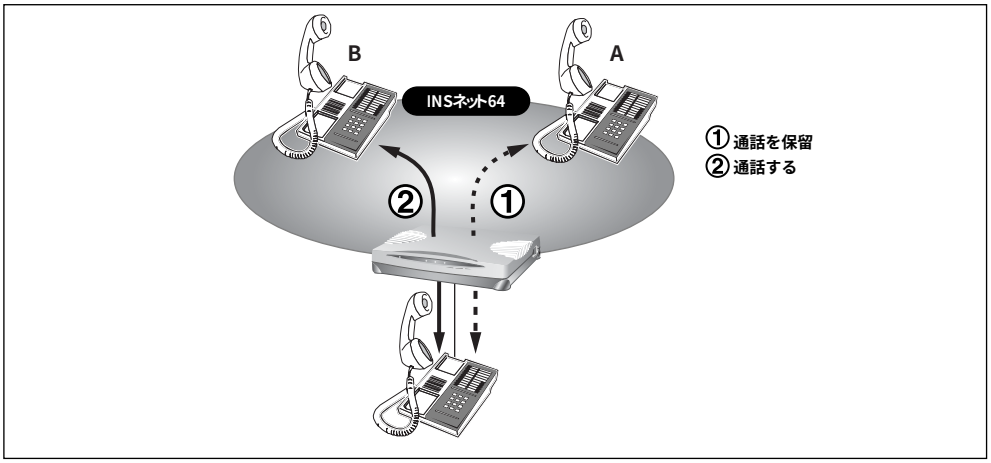
ここでは、フレックスホンの使い方を説明します。

INS キャッチホン

「INS キャッチホン」はNTT が提供するサービスです。利用の際はNTT との契約が必要です。

通話中に電話を着信した場合、いったん通話を保留にしてあとからかけてきた相手と話すことができます。

補足 「接続機器」で「電話」および「FAX（キャッチホン着信）」以外を指定した場合は、通信を妨げないようにするため、INS キャッチホンは利用できません。



1.　相手Aとの通話中に相手Bから電話がかかってくると、受話器から通話中着信音が流れてきます。

補足
- 通話中着信音を送出する時間を指定しておくことができます。「アナログ共通情報」（P.333）を参照してください。
- 通話中着信音は、識別着信機能で相手に登録してあるリング音に対応して以下の表のようになります。
- 通話中着信音は、「識別着信共通情報」の「識別リング音」の設定により異なります。
「識別リング音」を「相手電話番号識別」に設定した場合、識別着信情報一覧で追加定義した相手からの着信は「プププッ」、それ以外の着信は「ププッ」となります。
「識別リング音」を「着信電話番号識別」に設定した場合、着信電話番号ごとに設定したリング音に対応して以下の表のようになります。

リング音設定	通話中着信
リング音1	ププッ
リング音2	プッ
リング音3	プププッ

2.　フッキングをします。

相手Bと通話できます。相手Aとの通話は保留になります。

3.　相手Aと通話するときは、もう一度フッキングをします。

相手Bとの通話が保留になり、相手Aと通話ができます。

補足 NTTと三者通話または通信中転送の契約をしている場合は、この状態から以下の動作が可能です。
- 2回フッキングをする（以降、ダブルフックとよびます）と、「自分＋相手A＋相手B」の三者で同時通話ができます（三者通話）。
- いったんフッキングして、すぐに受話器を置くと、通信中転送ができます（通信中転送）。

4.　通話中の相手との通話を終了するときは、受話器を置きます。

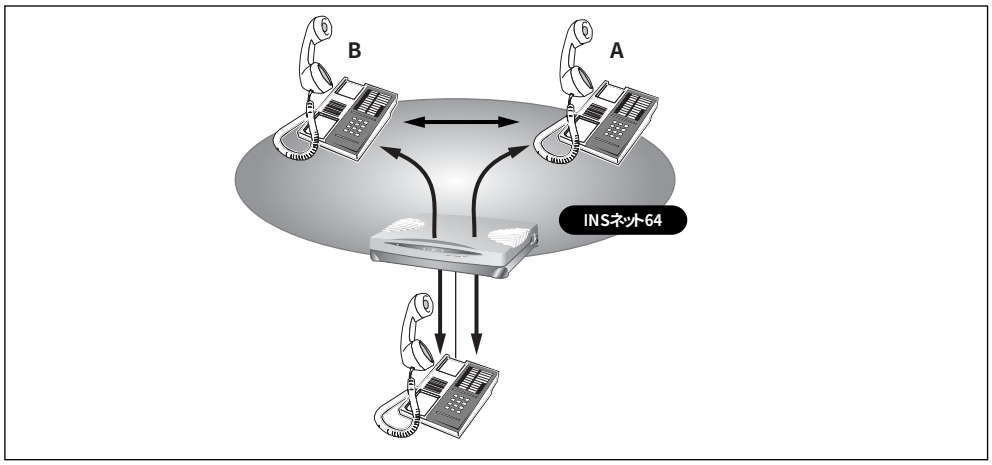
リング音が鳴ります。

5.　受話器を取ります。

保留にしていた相手と通話できます。

三者通話

「三者通話」はNTTが提供するサービスです。利用の際はNTTとの契約が必要です。



1.　相手Aとの通話中にフッキングをします。

通話が保留になり、第2ダイヤルトーン（プップップッという音）が聞こえてきます。

2.　相手Bへダイヤルします。

呼び出し音（プルルルという音）が聞こえます。相手Aには保留音が聞こえています。

3.　相手Bがでたら、通話を始めます。

この間、相手Aには保留音が聞こえています。

4.　ダブルフックをします。

「自分＋相手A＋相手B」の三者で同時通話ができます（ミキシングモード）。

5.　もう一度、ダブルフックをします。

相手Aとの通話は保留され、相手Bとの通話状態になります（切り替えモード）。

6.　通話中の相手との通話を終了するときは、受話器を置きます。

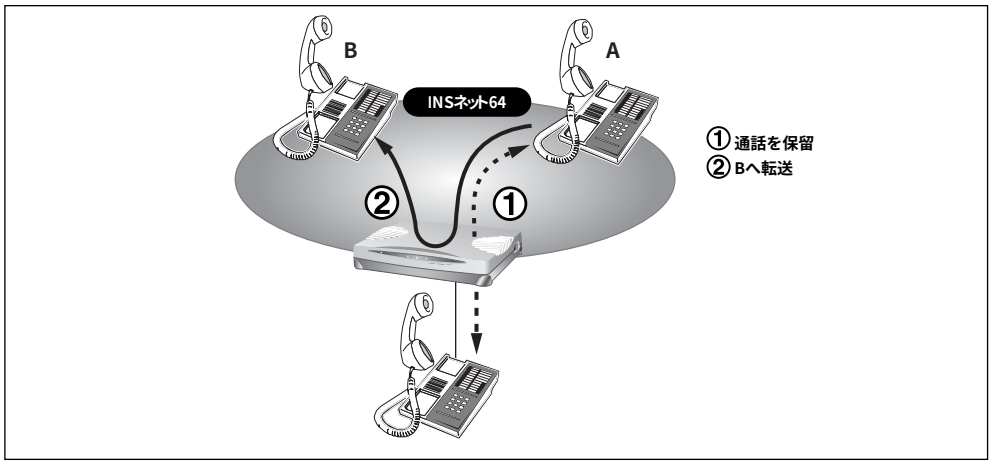
リング音が鳴ります。

7.　受話器を取ります。

保留中の相手と通話できます。

通信中転送

「通信中転送」はNTTが提供するサービスです。利用の際はNTTとの契約が必要です。
「通信中転送」機能を使って、通話中の電話を別の相手に転送できます。



1.　相手Aからの通話中にフッキングをします。

通話が保留になり、第2ダイヤルトーン（プップップッという音）が聞こえてきます。

2.　相手Bへダイヤルします。

呼び出し音（プルルルという音）が聞こえます。相手Aには、保留音が聞こえています。

3.　相手Bがでたら、転送中の電話があることを伝えます。

この間、相手Aには保留音が聞こえています。

4.　いったんフッキングをして、すぐに受話器を置きます。

相手Aと相手Bとで通話ができるようになります。

ヒント

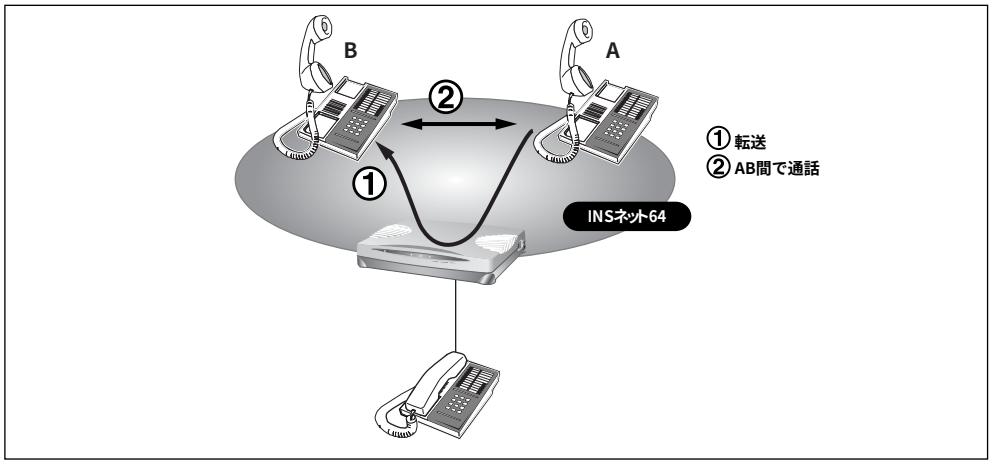
◆通信中転送したときの通話料はどうなるの？

INSキャッチホンおよび三者通話から、通信中転送を行った場合、以下のようにそれぞれ発信者に課金されます。

	最初の通話（相手A）	2番目の通話（相手B）	通信中転送	課金対象
INSキャッチホンの場合	Aから 自分から	Bから Bから	できる できる	A、B 自分、B
三者通話の場合	Aから 自分から	自分から 自分から	できる できない	A、自分 –

着信転送

「着信転送」は、NTTが提供するサービスです。利用の際はNTTとの契約が必要です。
かかってきた電話が、あらかじめ設定しておいた着信転送の条件に一致すると、本装置は電話を転送します。



補足
- 本装置に電話機をつないでいなくても、着信転送を利用できます。
- 着信相手から本装置までの電話料金は着信相手に課金され、本装置から転送先までの電話料金は、本装置側に課金されます。

フレックスホン自動切り替え機能を使う

フレックスホンを利用して通話している場合、話している相手から電話を切断したときに、保留になっていた相手と自動的に（フッキング操作をしないで）通話できるようにする機能です。この機能は疑似キャッチホン、疑似三者通話、疑似通話中転送を使用している場合でも利用できます。

フレックスホン自動切り替え機能を設定する

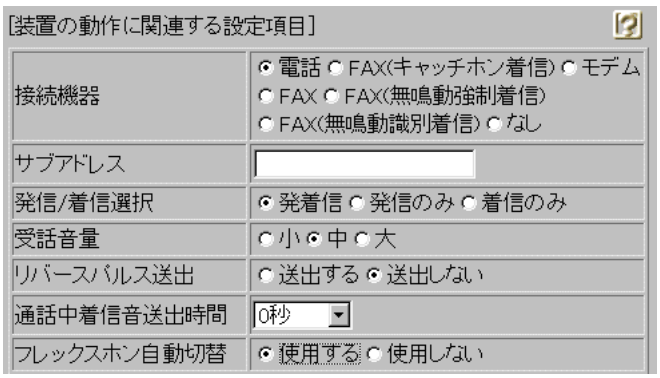
ここでは、電話機をアナログポート1につないだ場合を例に説明します。

1.　詳細設定メニューのアナログ設定で「アナログポート1情報」をクリックします。

「アナログポート1情報」ページが表示されます。

2.　［網契約に関連する設定項目］で以下の項目を指定します。

- フレックスホン自動切替　　→使用する



3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

INSボイスワープを利用する

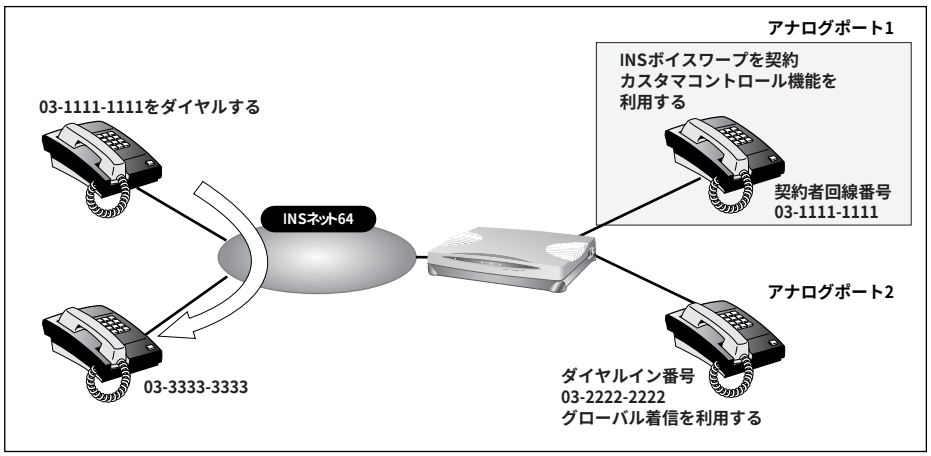
INSボイスワープはNTTが提供する高機能な着信転送サービスです。利用の際はNTTとの契約が必要です。INSボイスワープのカスタマコントロール機能（INSボイスワープを制御する手順）の詳細については、NTT支店または営業所にお問い合わせください。
ダイヤルインサービスを契約されている場合は、発信者番号通知の設定を通知するにしてください。

☛ 参照 「発信者番号通知の設定を変更する」（P.391）

また、INSボイスワープを契約した番号（契約者番号またはダイヤルイン番号）によって以下の設定が必要です。ダイヤルインサービスを契約していない場合は、設定の必要はありません。

INSボイスワープを契約者番号（アナログポート1）で契約した場合の設定

ここでは、以下の場合を例に説明します。



1.　詳細設定メニューのアナログ設定で「アナログ共通情報」をクリックします。

「アナログ共通情報」ページが表示されます。

2.　［網契約に関連する設定項目］で以下の項目を指定します。

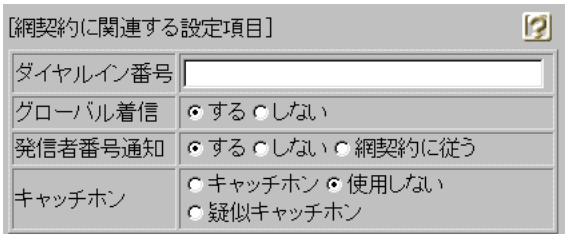
- 電話番号　→03-1111-1111（契約者回線番号）

3.　［更新］ボタンをクリックします。

4.　［アナログポート1情報へ>］ボタンをクリックします。

5.　［網契約に関連する設定項目］で以下の項目を指定します。

- 発信者番号通知　　→する



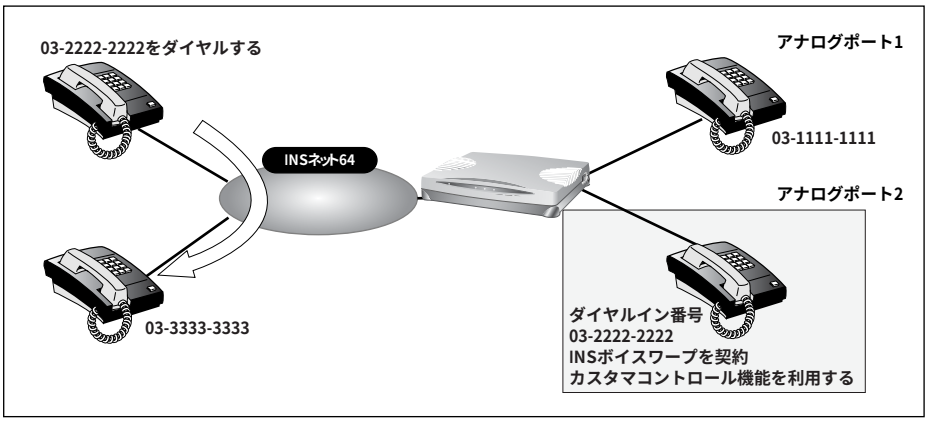
6.　［更新］ボタンをクリックします。

7.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

INSボイスワープをダイヤルイン番号（アナログポート2）で契約した場合の設定

ここでは、以下の場合を例に説明します。

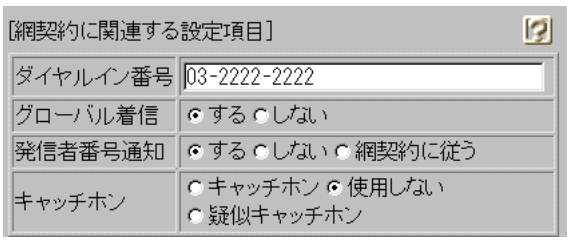


1.　詳細設定メニューのアナログ設定で「アナログポート2情報」をクリックします。

「アナログポート2情報」ページが表示されます。

2.　［網契約に関連する設定項目］で以下の項目を指定します。

- ダイヤルイン番号　→03-2222-2222（ダイヤルイン番号）
- 発信者番号通知　→する



3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

発信者番号表示（ナンバー・ディスプレイ）を使う

電話をかけてきた相手の方の電話番号（発信者番号）または発信者番号が通知されない理由を、アナログポートに接続したアナログ機器に表示することができます。

こんな事に気をつけて

- **「INS ナンバー・ディスプレイ」はNTT が提供するサービスです。利用の際はNTT との契約が必要です。ただし、相手の方がINS ネット64から発信者番号を通知して電話をかけてきた場合は、未契約でも発信者番号をアナログ機器に表示することができます。**
- **ナンバー・ディスプレイに対応していないアナログ機器をご使用の場合、発信者番号は表示されません。**

補足
- 相手の方がアナログ回線からかけてくる場合、発信者番号を通知させるにはNTTとの利用契約が必要です。
- 相手の方が電話番号を通知しない契約を結んでいる、または電話番号を通知しない操作をした場合などは、本装置に接続したアナログ機器に発信者番号は表示されません。
  発信者番号が通知されない主な理由は以下のとおりです。
  - 公衆電話からの電話のとき
  - かけてきた相手の方が電話番号を通知しない操作をしたとき、または通知しない契約になっているとき

ナンバー・ディスプレイ機能を設定する

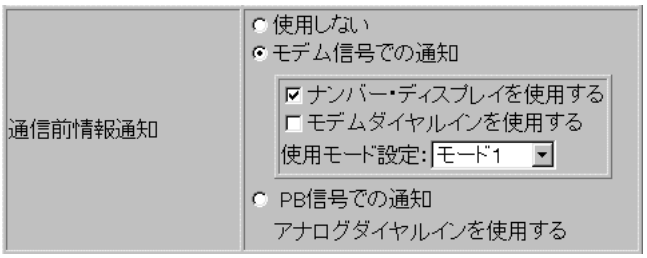
ここでは、電話機をアナログポート1につないだ場合を例に説明します。

1. 詳細設定メニューのアナログ設定で「アナログポート1情報」をクリックします。

「アナログポート1情報」ページが表示されます。

2. [装置の動作に関連する設定項目]で以下の項目を指定します。

- 通信前情報通知　→モデム信号での通知
  →ナンバー・ディスプレイを使用する
  使用モード設定　→モード1



補足「使用モード設定」で「モード1」を指定して正常に動作しない場合は、「モード2」を指定してください。

3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

- **アナログポートに接続したアナログ機器に発信者番号を表示させるためには、以下の条件を満たす必要があります。**
  - **本装置のアナログポートにナンバー・ディスプレイ対応のアナログ機器を接続し、アナログ機器のナンバー・ディスプレイ機能を「使用する」に設定する**
  - **アナログ機器を接続したアナログポートの「アナログポート情報」で「ナンバー・ディスプレイを使用する」に設定する**
- **お使いになるアナログ機器がナンバー・ディスプレイに対応していない場合や、ナンバー・ディスプレイを利用しない設定になっている場合は、誤鳴音や雑音（モデム信号）が聞こえるなど、正常に動作しない場合があります。**
- **「アナログポート情報」で「通信前情報通知」を「ナンバー・ディスプレイを使用する」設定にした場合は、「アナログ共通情報」で「外線リング音」、「内線リング音」の設定を、「識別着信情報」で「識別リング音」の設定を「リング音 1」に設定することをお勧めします。それ以外の設定（「リング音 2」「リング音 3」）を行った場合には、外線着信、内線着信および識別着信が正常に動作しないことがあります。**
- **相手の方がサブアドレス番号を通知してきてもサブアドレス番号は表示されません。**
- **ナンバー・ディスプレイ対応アナログ機器の機種によっては、発信者番号が正常に表示されない場合があります。**
- **無鳴動 FAX受信機能を使用する場合、ナンバー・ディスプレイ機能は利用できません。**

補足

- 内線通話で着信した場合、呼び出し操作を行ったアナログポート番号「01」または「02」が表示されます。
- 内線転送操作からの着信時は、転送される相手の番号が表示されます。
- ナンバー・ディスプレイに対応していないアナログ機器を利用していても本装置のシステムログ情報には発信者番号が表示されます。
- ナンバー・ディスプレイ対応確認機種については、本装置のサポートページを参照してください。

発信者番号表示（キャッチホン・ディスプレイ）を使う

通話中に電話をかけてきた相手の方の電話番号（発信者番号）または発信者番号が通知されない理由を、アナログポートに接続したアナログ機器に表示することができます。

こんな事に気をつけて

- **利用の際はNTTが提供する「INSナンバー・ディスプレイ」の契約が必要です。ただし、相手の方がINSネット64から発信者番号を通知して電話をかけてきた場合は、未契約でも発信者番号をアナログ機器に表示することができます。**
- **キャッチホン・ディスプレイに対応していないアナログ機器をご使用の場合、発信者番号は表示されません。**

補足

- 相手の方がアナログ回線からかけてくる場合、発信者番号を通知させるにはNTTとの利用契約が必要です。
- 相手の方が電話番号を通知しない契約を結んでいる、または電話番号を通知しない操作をした場合などは、本装置に接続したアナログ機器に発信者番号は表示されません。
  発信者番号が通知されない主な理由は以下のとおりです。
  - 公衆電話からの電話のとき
  - かけてきた相手の方が電話番号を通知しない操作をしたとき、または通知しない契約になっているとき

キャッチホン・ディスプレイ機能を設定する

ここでは、電話機をアナログポート1につないだ場合を例に説明します。

補足 キャッチホン・ディスプレイ機能を使用するには、「キャッチホン」の設定も必要です。

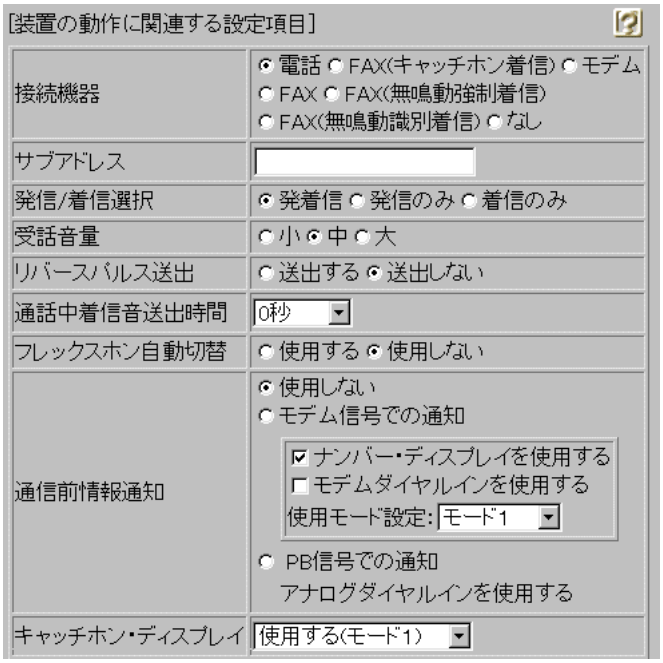
☛ 参照 「疑似キャッチホンを使う」（P.368）
「発信者番号表示（ナンバー・ディスプレイ）を使う」（P.386）

1.　詳細設定メニューのアナログ設定で「アナログポート1情報」をクリックします。

「アナログポート1情報」ページが表示されます。

2.　[装置の動作に関連する設定項目] で以下の項目を指定します。

- キャッチホン・ディスプレイ　　→使用する（モード1）



補足 使用する（モード1）を指定して正常に動作しない場合は、「使用する（モード2）」、「使用する（モード3）」、または「使用する（モード4）」を指定してください。

3.　[更新] ボタンをクリックします。

4.　[設定反映] ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

- **アナログポートに接続したアナログ機器に発信者番号を表示させるためには、以下の条件を満たす必要があります。**
  - **本装置のアナログポートにキャッチホン・ディスプレイ対応のアナログ機器を接続し、アナログ機器のキャッチホン・ディスプレイ機能を「使用する」に設定する**
  - **アナログ機器を接続したアナログポートの「アナログポート情報」で「キャッチホン・ディスプレイを使用する」に設定する**
- **お使いになるアナログ機器がキャッチホン・ディスプレイに対応していない場合や、キャッチホン・ディスプレイを利用しない設定になっている場合は、誤鳴音や雑音（モデム信号）が聞こえるなど、正常に動作しない場合があります。**
- **相手の方がサブアドレス番号を通知してきてもサブアドレス番号は表示されません。**
- **キャッチホン・ディスプレイ対応アナログ機器の機種によっては、発信者番号が正常に表示されない場合があります。**

補足

- キャッチホン・ディスプレイに対応していないアナログ機器を利用していても本装置のシステムログ情報には発信者番号が表示されます。
- キャッチホン・ディスプレイ対応確認機種については、本装置のサポートページを参照してください。

発信者番号通知の設定を変更する

「発信者番号通知」はNTTが提供する基本サービスです。
発信するときに、発信者番号（契約者回線番号、ダイヤルイン番号、または鳴り分け番号）を通知するかどうかをNTTの契約と本装置の設定との組み合わせにより選ぶことができます。発信者番号を通知する契約をしている場合でも、アナログポート1と2をそれぞれ通知しないように設定できます。

網契約	本装置の設定（発信者番号通知）			相手ダイヤル番号前に付加	
	網契約に従う	する	しない	184を付加	186を付加
通常通知	通知する	通知する	通知しない	通知しない	通知する
通常非通知	通知しない				

発信者番号通知を設定する

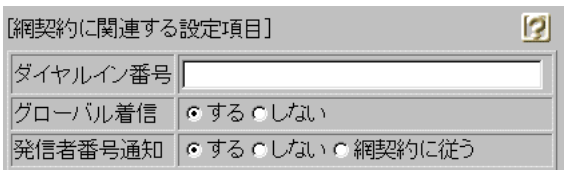
ここでは、電話機をアナログポート1につないだ場合を例に説明します。

1.　詳細設定メニューのアナログ設定で「アナログポート1情報」をクリックします。

「アナログポート1情報」ページが表示されます。

2.　［網契約に関連する設定項目］で以下の項目を指定します。

- 発信者番号通知　→「する」、「しない」、または「網契約に従う」を選択する



3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

補足　「アナログポート情報」でダイヤルイン番号に電話番号を設定し、発信者番号通知を行う設定をした場合、相手先にはダイヤルイン番号に設定した電話番号を通知します。
鳴り分け番号を通知する場合、「アナログポート情報」のダイヤルイン番号に鳴り分け番号を設定してください。

発信者電話番号を選択する

外線発信時に、ダイヤルする相手電話番号の前にプレフィックス番号を付加することによって、相手に通知する発信者番号を選択することができます。

こんな事に気をつけて

- **利用する際は、NTTとの「ダイヤルインサービス」または「ｉ・ナンバーサービス」の契約が必要です。**
- **この機能を利用する場合、アナログポート情報の「発信者番号通知」の設定は無効となり、必ず相手に発信者番号を通知します。**

1.　受話器を上げ、ツーという音が聞こえることを確認します。

2.　プレフィックス番号に続けて相手電話番号をダイヤルします。

通知する発信者番号に対応するプレフィックス番号を付加します。

［ダイヤルインサービス契約（グローバル着信する）の場合］

通知する電話番号の種別	付加するプレフィックス番号
契約者回線番号	✱70
アナログポート1情報に設定したダイヤルイン番号	✱71
アナログポート2情報に設定したダイヤルイン番号	✱72

［ｉ・ナンバー契約の場合］

通知する電話番号の種別	付加するプレフィックス番号
鳴り分け番号1（契約回線番号）	✱73
鳴り分け番号2（追加番号）	✱74
鳴り分け番号3（追加番号）	✱75

3.　呼び出し音が聞こえます。

無鳴動FAX受信機能を使う

無鳴動着信機能（FAXを受信したときに、着信音を鳴らさずに応答する機能）を持つFAXをアナログポートに接続した場合、着信音（リング音）を鳴らさずにFAXに着信させることができます。

こんな事に気をつけて

無鳴動FAX受信機能を使用する場合、ナンバー・ディスプレイ機能は利用できません。

無鳴動FAX受信機能を設定する

ここでは、FAXをアナログポート1につないだ場合を例に説明します。

1.　詳細設定メニューのアナログ設定で「アナログポート1情報」をクリックします。

「アナログポート1情報」ページが表示されます。

2.　［装置の動作に関連する設定項目］で以下の項目を指定します。

- 接続機器　→「FAX（無鳴動強制着信）」または「FAX（無鳴動識別着信）」を選択する

補足
- 「FAX（無鳴動強制着信）」を指定すると、FAX受信時に無鳴動着信処理を行います。
- 「FAX（無鳴動識別着信）」を指定すると、相手からFAX通信を行うという情報（高位レイヤ整合性：G3FAX）が着信時に通知された場合だけ無鳴動着信処理を行います。それ以外の着信は、鳴動着信処理を行います。

3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

ｉ・ナンバー着信機能を使う

ｉ・ナンバーはNTTが提供するサービスで、ご使用になる場合は、契約が必要です。着信するアナログポートを特定できます。

ヒント

◆ ｉ・ナンバー

NTTの「ｉ・ナンバー」を契約すると、1つのINSネット64に通常の電話番号に加えて、別の追加電話番号を2つまで割り当てることができます。それぞれの電話番号を使い分けることで、INSネット64につないでいる機器を呼び分けることができます。

ｉ・ナンバー着信機能を設定する

ここでは、以下のような場合を例に説明します。

- 契約者回線番号（鳴り分け番号1）で着信したときは両ポートに着信
- 追加番号（鳴り分け番号2）で着信したときはアナログポート1だけに着信
- 追加番号（鳴り分け番号3）で着信したときはアナログポート2だけに着信

1.　詳細設定メニューのアナログ設定で「アナログ共通情報」をクリックします。

「アナログ共通情報」ページが表示されます。

2.　［網契約に関連する設定項目］で以下の項目を指定します。

- ｉ・ナンバー　→使用する
  ［ｉ・ナンバー情報1］
  動作モード　→両ポート着信
  ［ｉ・ナンバー情報2］
  動作モード　→ポート1のみ着信
  ［ｉ・ナンバー情報3］
  動作モード　→ポート2のみ着信

3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

サブアドレスを設定する

サブアドレスを設定すると、着信するアナログポート（ポート1またはポート2）を特定できます。
サブアドレスは、発信側がINSネット64に加入している場合だけ利用できます。
外から電話をかけるとき、電話番号に続いて［＊］とサブアドレスをダイヤルすれば、そのサブアドレスを設定した方のアナログポートに着信させることができます。ただし、サブアドレスの番号は完全に一致しないと着信できません。

補足　相手電話番号［＊］サブアドレス

例）03-1111-1111［＊］123

こんな事に気をつけて

サブアドレスで着信ポートを特定する場合は、発信する相手側はサブアドレスを指定できるISDN機器（電話、PHSなど）の必要があります。

サブアドレスを設定する

ここでは、電話機をアナログポート1につないだ場合を例に説明します。

1.　詳細設定メニューのアナログ設定で「アナログポート1情報」をクリックします。

「アナログポート1情報」ページが表示されます。

2.　［装置の動作に関連する設定項目］でサブアドレスを指定します（19桁以内）。

- サブアドレス　→123

3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

ダイヤルイン／グローバル着信機能を使う

ダイヤルインはNTTが提供するサービスで、ご使用になる場合は、契約が必要です。着信するアナログポート（ポート1またはポート2）を特定できます。

ヒント

◆ダイヤルインサービスとグローバル着信

NTTの「ダイヤルインサービス」とは、1つのINSネット64に通常の電話番号（以降、契約者回線番号と呼びます）に加えて、「ダイヤルイン番号」と呼ばれる番号を割り当てるサービスです。契約者回線番号とダイヤルイン番号を使い分けることで、INSネット64につないでいる機器を呼び分けられるようになります。

一方「グローバル着信」とは、契約者回線番号で電話がかかってきたとき、どの電話番号で着信したかをINSネット64につないでいる機器に通知しないようにするオプションです。つまり、呼び分けしないですべての電話機を鳴らすわけです。ちなみに「ダイヤルインサービス」を契約する際、「グローバル着信利用しない」という契約にすると、相手先がダイヤルした番号に対応する電話機だけを鳴らします。

ダイヤルイン番号を1つ追加して「グローバル着信利用しない」という契約にすると、ダイヤルイン番号を2つ追加した場合と同じ料金がかかります。かかってきた電話すべてについて呼び分けをするためです。ただし、本装置ではアナログポートごとに「グローバル着信を行う／行わない」の設定ができるので、「グローバル着信利用」と契約しておけば、ダイヤルイン番号1つ分の使用料で済みます。

INSネット64の基本機能であるサブアドレスでも同じように呼び分けができます。ただし、相手がアナログ回線である場合は、サブアドレス情報のやり取りができないため、呼び分けができません。

■ ダイヤルイン／グローバル着信機能を設定する

ここでは、契約者番号で着信したときは、アナログポート1だけに着信し、ダイヤルイン番号（03-2222-2222）で着信したときは、アナログポート2だけに着信する場合を例に説明します。

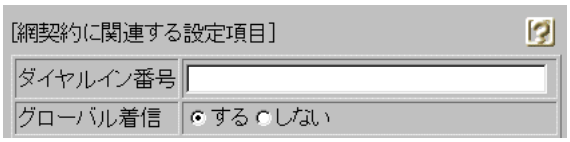
アナログポート情報1の設定

1.　詳細設定メニューのアナログ設定で「アナログポート1情報」をクリックします。

「アナログポート1情報」ページが表示されます。

2.　［網契約に関連する設定項目］で以下の項目を指定します。

- ダイヤルイン番号　→なにも設定しない
- グローバル着信　→する



3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

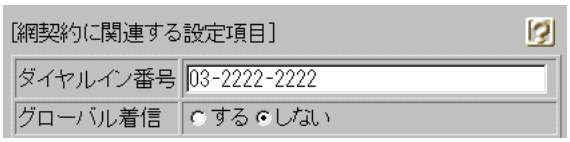
アナログポート情報2の設定

1.　詳細設定メニューのアナログ設定で「アナログポート2情報」をクリックします。

「アナログポート2情報」ページが表示されます。

2.　［網契約に関連する設定項目］で以下の項目を指定します。

- ダイヤルイン番号　→03-2222-2222
- グローバル着信　→しない



3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

モデムダイヤルイン機能を使う

モデムダイヤルインは、電話とFAXなど機能ごとに個別の番号を持つことができます。着信したときに、モデム信号で自局電話番号または送出着信情報で設定した番号を電話機に通知します。
自局電話番号を送出する場合の設定例は（その1）で、送出着信情報で設定する任意の番号を送出する場合の設定例は（その2）で説明します。

こんな事に気をつけて

- **利用する際は、NTTとの「ダイヤルインサービス」または「i・ナンバーサービス」の契約が必要です。**
- **この機能を使用する場合、アナログダイヤルイン機能は利用できません。また、ご使用になる電話機がモデムダイヤルイン機能に対応している必要があります。（電話機の設定も必要です。電話機の取扱説明書をご覧ください。）**

■ モデムダイヤルイン機能を設定する（その1：自局電話番号を送出する）

ここでは、以下の場合を例に説明します。

- アナログポート1にFAX機能付き電話をつなぐ
- ｉ・ナンバー契約を行う
- 契約者番号（鳴り分け番号1：03-2222-2222）で着信した場合は、電話に着信する
  （送出番号：03-2222-2222）
- 追加番号（鳴り分け番号2：03-3333-3333）で着信した場合は、FAXに着信する
  （送出番号：03-3333-3333）

ここでは「ｉ・ナンバー」契約をしている場合の設定例を説明していますが、「ダイヤルインサービス」を契約している場合は、「アナログダイヤルイン機能を使う」で説明している設定例を参考にして設定してください。

☛ 参照 「アナログダイヤルイン機能を使う」（P.405）

アナログ共通情報の設定

1.　詳細設定メニューのアナログ設定で「アナログ共通情報」をクリックします。

「アナログ共通情報」ページが表示されます。

2.　［網契約に関連する設定項目］で以下の項目を指定します。

- ｉ・ナンバー　→使用する
  ［ｉ・ナンバー情報1］
  鳴り分け番号1　→03-2222-2222
  動作モード　→ポート1のみ着信
  ［ｉ・ナンバー情報2］
  鳴り分け番号2　→03-3333-3333
  動作モード　→ポート1のみ着信

3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

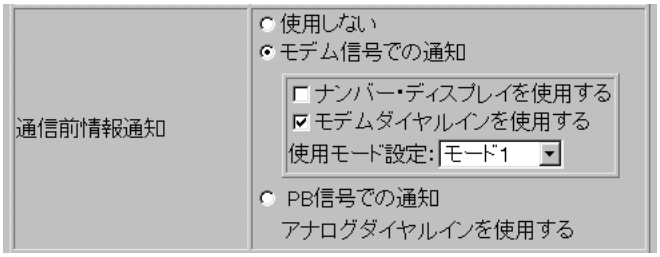
アナログポート1情報の設定

1.　詳細設定メニューのアナログ設定で「アナログポート1情報」をクリックします。

「アナログポート1情報」ページが表示されます。

2.　［網契約に関連する設定項目］で以下の項目を指定します。

- 通信前情報通知　→モデム信号での通知
  →モデムダイヤルインを使用する
  使用モード設定　→モード1



3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

■ モデムダイヤルイン機能を設定する（その2：任意の番号を送出する）

ここでは、以下のような場合を例に説明します。

- アナログポート1にFAX機能および子機付き電話をつなぐ
- ｉ・ナンバー契約を行う
- 契約者番号（鳴り分け番号1）で着信した場合は、電話に着信する（送出番号：1111）
- 追加番号（鳴り分け番号2）で着信した場合は、FAXに着信する（送出番号：2222）
- 追加番号（鳴り分け番号3）で着信した場合は、子機に着信する（送出番号：3333）

ここでは「ｉ・ナンバー」契約をしている場合の設定例を説明していますが、「ダイヤルインサービス」を契約している場合は、「アナログダイヤルイン機能を使う」で説明している設定例を参考にして設定してください。

☛ 参照 「アナログダイヤルイン機能を使う」（P.405）

アナログ共通情報の設定

1.　詳細設定メニューのアナログ設定で「アナログ共通情報」をクリックします。

「アナログ共通情報」ページが表示されます。

2.　［網契約に関連する設定項目］で以下の項目を指定します。

- ｉ・ナンバー　→使用する
  ［ｉ・ナンバー情報1］
  動作モード　→ポート1のみ着信
  ［ｉ・ナンバー情報2］
  動作モード　→ポート1のみ着信
  ［ｉ・ナンバー情報3］
  動作モード　→ポート1のみ着信

3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

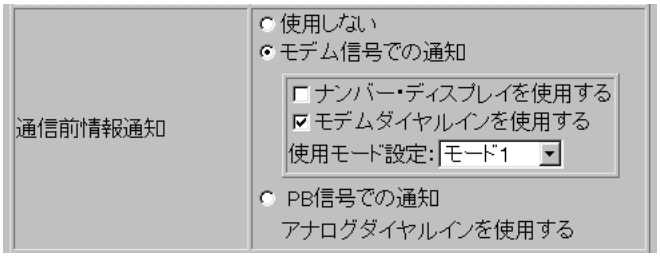
アナログポート1情報の設定

1.　詳細設定メニューのアナログ設定で「アナログポート1情報」をクリックします。

「アナログポート1情報」ページが表示されます。

2.　［網契約に関連する設定項目］で以下の項目を指定します。

- 通信前情報通知　→モデム信号での通知
  →モデムダイヤルインを使用する
  使用モード設定　→モード1



3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

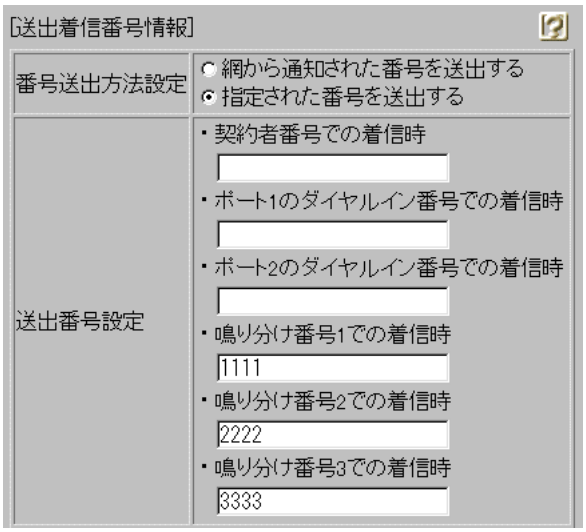
送出着信番号情報の設定

1.　詳細設定メニューのアナログ設定で「送出着信番号情報」をクリックします。

「送出着信番号情報」ページが表示されます。

2.　[送出着信番号情報] で以下の項目を指定します。

- 番号送出方法設定　→指定された番号を送出する
- 送出番号設定
  鳴り分け番号１での着信時　→1111
  鳴り分け番号２での着信時　→2222
  鳴り分け番号３での着信時　→3333



3.　[更新] ボタンをクリックします。

4.　[設定反映] ボタンをクリックします。

設定反映した内容が有効になります。

アナログダイヤルイン機能を使う

アナログダイヤルインは、電話とFAXなど機能ごとに個別の番号を持つことができます。着信したときに、PB信号で自局電話番号または送出着信情報で設定した番号を電話機に通知します。
自局電話番号を送出する場合の設定例は（その1）で、送出着信情報で設定する任意の番号を送出する場合の設定例は（その2）で説明します。

こんな事に気をつけて

- **利用する際は、NTTとの「ダイヤルインサービス」または「i・ナンバーサービス」の契約が必要です。**
- **この機能を使用する場合、ナンバー・ディスプレイおよびモデムダイヤルイン機能は利用できません。また、ご使用になる電話機がアナログダイヤルイン機能に対応している必要があります（電話機の設定も必要です。電話機の取扱説明書をご覧ください。）。**

■ アナログダイヤルイン機能を設定する（その1：自局電話番号を送出する）

ここでは、以下の場合を例に説明します。

- アナログポート1にFAX機能付き電話をつなぐ
- ダイヤルイン契約を「グローバル着信を利用する」で契約
- 契約者番号（03-2222-2222）で着信した場合は、電話に着信する（送出番号：2222）
- ダイヤルイン番号（03-2222-3333）で着信した場合は、FAXに着信する（送出番号：3333）

ここでは「ダイヤルインサービス」契約をしている場合の設定例を説明していますが、「i・ナンバー」を契約している場合は、「モデムダイヤルイン機能を使う」で説明している設定例を参考にして設定を行ってください。

☛ 参照 「モデムダイヤルイン機能を使う」（P.399）

アナログ共通情報の設定

1.　詳細設定メニューのアナログ設定で「アナログ共通情報」をクリックします。

「アナログ共通情報」ページが表示されます。

2.　［網契約に関連する設定項目］で以下の項目を指定します。

- 電話番号　→03-2222-2222

3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

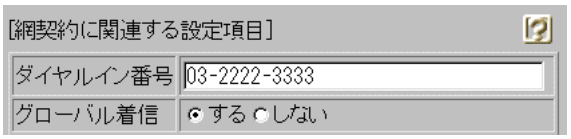
アナログポート1情報の設定

1.　詳細設定メニューのアナログ設定で「アナログポート1情報」をクリックします。

「アナログポート1情報」ページが表示されます。

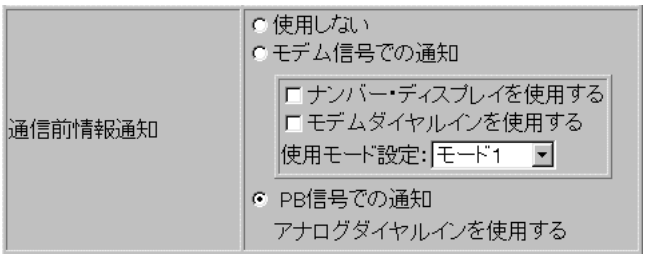
2.　［網契約に関連する設定項目］で以下の項目を指定します。

- ダイヤルイン番号　→03-2222-3333



［装置の動作に関連する設定項目］で以下の項目を指定します。

- 通信前情報通知　→PB 信号での通知



3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

■ アナログダイヤルイン機能を設定する（その2：任意の番号を送出する）

ここでは、以下の場合を例に説明します。

- アナログポート1にFAX機能付き電話をつなぐ
- ダイヤルイン契約を「グローバル着信を利用する」で契約
- 契約者番号で着信した場合は、電話に着信する（送出番号：1111）
- ダイヤルイン番号（03-2222-3333）で着信した場合は、FAXに着信する（送出番号：2222）

ここでは「ダイヤルインサービス」契約をしている場合の設定例を説明していますが、「ｉ・ナンバー」を契約している場合は、「モデムダイヤルイン機能を使う」で説明している設定例を参考に、設定してください。

☛ 参照 「モデムダイヤルイン機能を使う」（P.399）

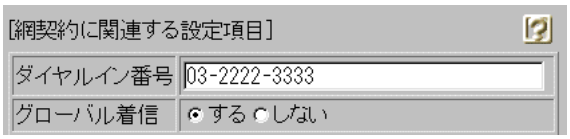
アナログポート1情報の設定

1.　詳細設定メニューのアナログ設定で「アナログポート1情報」をクリックします。

「アナログ共通情報」ページが表示されます。

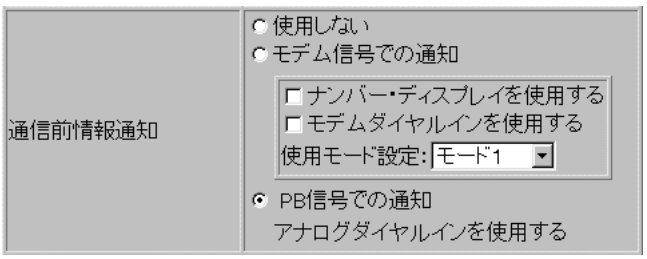
2.　［網契約に関連する設定項目］で以下の項目を指定します。

- ダイヤルイン番号　→03-2222-3333



［装置の動作に関連する設定項目］で以下の項目を指定します。

- 通信前情報通知　→PB信号での通知



3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

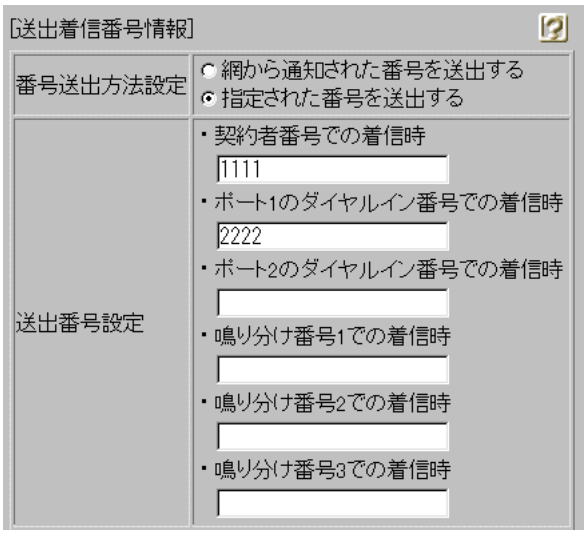
送出着信番号情報の設定

1.　詳細設定メニューのアナログ設定で「送出着信番号情報」をクリックします。

「送出着信番号情報」ページが表示されます。

2.　［送出着信番号情報］で以下の項目を指定します。

- 番号送出方法設定　→指定された番号を送出する
- 送出番号設定
  契約者回線番号での着信時　→1111
  ポート1ダイヤルインサービス番号での着信時　→2222



3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

リバースパルス送出機能を使う

リバースパルスは、外から電話がかかってきて、通話中に相手から電話を切った場合に、本装置がアナログポートに接続された機器に対して通話が終了したことを知らせるために送出する信号です。たとえば、留守番電話で相手が切断したら同時にメッセージの録音を終了する機能を備えているときに有効です。

こんな事に気をつけて

接続したアナログ機器がリバースパルスを認識する機能を備えていない場合は、リバースパルスを送出する設定を行わないでください。誤動作する場合があります。

リバースパルス送出を設定する

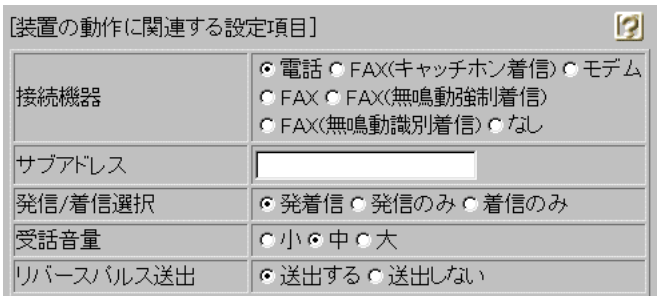
ここでは、電話機をアナログポート1につないだ場合を例に説明します。

1.　詳細設定メニューのアナログ設定で「アナログポート1情報」をクリックします。

「アナログポート1情報」ページが表示されます。

2.　［装置の動作に関連する設定項目］で以下の項目を指定します。

- リバースパルス送出　　→送出する



3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

電話機を利用して設定を変更する

本装置のアナログポート（ポート1、ポート2）に接続したアナログ機器から設定できる項目を以下に示します。

- 時計の設定
- IPアドレスの設定
- アナログ機能の設定
  - スタンバイモードの設定
  - 着信転送の設定
  - アナログポートの接続機器の設定
  - ナンバー・ディスプレイの設定
  - ｉ・ナンバーの設定
  - 鳴り分け番号の動作モードの設定
- 着信転送先の変更
- TEL メールの設定
- メールチェックの実行
- 留守状態の設定
- 留守モードの設定

補足 スタンバイモードの設定は「スタンバイモードで使用する」（P.355）で説明していますが、ここで説明する方法でも設定が可能です。また、外線からも設定が可能です。

☛ 参照 「外線から設定を変更する（無課金）」（P.419）

こんな事に気をつけて

データ通信中に電話機を利用して設定を変更するとデータ通信が切断されます。
ただし、「時計の設定」、「メールチェックの実行」の場合は、切断されません。

■ 時計を設定する

1.　受話器を上げ、ツーという音が聞こえることを確認します。

2.　✱0✱820 ＋ ✱日付＋時刻（yymmddHHMMSS）をダイヤルします。

- yy　→西暦の下2桁を指定します。00～36の場合は、西暦2000年以降とみなします。
- mm　→月を01～12までの数字で指定します。
- dd　→日付を01～31までの数字で指定します。
- HH　→時間を00～23までの数字で指定します。
- MM　→分を00～59までの数字で指定します。
- SS　→秒を00～59までの数字で指定します。

例）時刻を2008年1月1日午後2時30分00秒に設定する場合

✱0✱820✱0801011430000をダイヤルします。

3.　ピピッという音が2回とビジートーン（プープープーという話中の音）が聞こえます。

補足　正常に設定できなかった場合は、ビジートーン（プープープーという話中の音）だけが聞こえます。

4.　受話器を置きます。

5

■ IPアドレスを設定する

本装置のアナログポート（ポート1、ポート2）に接続したアナログ機器からIPアドレスの設定を行います。専用線を使用する場合でも、この機能を利用することができます。

こんな事に気をつけて

- **本装置のIPアドレスの変更を行うとLAN間通信やISDNでのデータ通信ができなくなる場合があります。**
- **DHCPサーバ機能を利用する場合には、WWWブラウザから設定を変更してください。**
- **DHCPサーバ機能を利用している場合は、本装置のIPアドレスの変更は行わないようにしてください。IPアドレスを変更すると、DHCPサーバ機能は利用できません。**

1.　受話器を上げ、ツーという音が聞こえることを確認します。

2.　✱0✱810＋✱ IPアドレス＋ネットマスク＋ブロードキャストアドレスをダイヤルします。

IPアドレス、ネットマスク、ブロードキャストアドレスの数字の区切りに✱を使います。ブロードキャストアドレスは、指定するブロードキャストアドレスに対応する数値を以下の表から選択します。

選択値	ブロードキャストアドレスの設定
0	0.0.0.0
1	255.255.255.255
2	IPアドレス／ネットマスクから求められるネットワークアドレス＋オール0
3	IPアドレス／ネットマスクから求められるネットワークアドレス＋オール1

例）IPアドレスを「192.168.2.1」、ネットマスクを「24」、ブロードキャストアドレスを「3（ネットワークアドレス＋オール1）」に設定する場合

✱0✱810✱192✱168✱2✱1✱24✱3 をダイヤルします。

3.　ピピッという音が2回とビジートーン（プープープーという話中の音）が聞こえます。

補足　正常に設定できなかった場合は、ビジートーン（プープープーという話中の音）だけが聞こえます。

4.　受話器を置きます。

■ アナログ機能を設定する

アナログポートに接続したアナログ機器から、以下のアナログ機能を設定できます。

- スタンバイモードの設定（通常モード／スタンバイモード）
- 着信転送の設定（しない／する／疑似着信転送）
- 接続機器の設定（なし／電話／モデム／ FAX／ FAX（無鳴動強制着信／無鳴動識別着信／キャッチホン着信））
- ナンバー・ディスプレイの設定（使用しない／使用する（モード1）／使用する（モード2））
- ｉ・ナンバーの設定（使用する／使用しない）
- 鳴り分け番号の動作モードの設定（ポート1のみ着信／ポート2のみ着信／両ポート着信／着信拒否）

1.　受話器を上げ、ツーという音が聞こえることを確認します。

2.　ダイヤル操作で設定を変更します。

✱0✱ に続けて以下の操作番号をダイヤルします。

機能		操作番号
スタンバイモード	通常モード	8001
	スタンバイモード	8002
着信転送	しない	6001
	する	6002
	疑似着信転送	6003
接続機器の設定	なし	40P1
	電話	40P2
	モデム	40P3
	FAX	40P4
	FAX（無鳴動強制着信）	40P5
	FAX（無鳴動識別着信）	40P6
	FAX（キャッチホン着信）	40P7
ナンバー・ディスプレイ	使用しない	41P1
	使用する（モード1）	41P2
	使用する（モード2）	41P3
ｉ・ナンバーの設定	使用しない	2201
	使用する	2202

鳴り分け番号の動作モード	**ポート1のみ着信**	22i1
	ポート2のみ着信	22i2
	両ポート着信	22i3
	着信拒否	22i4

Pには、設定を変更するアナログポートのポート番号（1または2）を入れます。

ｉには、鳴り分け番号1～3の番号（1、2、または3）を入れます。

例）ポート2の接続機器を「なし」にする場合

✱0✱4021 をダイヤルします。

3.　ピピッという音とビジートーン（プープープーという話中の音）が聞こえます。

補足　ピピッという音の鳴る回数は設定した機能によって異なります（操作で入力した最後の数字の回数です）。

例）「接続機器」の設定を「なし」に設定した場合、ピピッ（1回）プープープー
正常に設定できなかった場合は、ビジートーン（プープープーという話中の音）だけが聞こえます。

4.　受話器を置きます。

■ 着信転送先を設定する

アナログポートに接続したアナログ機器から、着信転送、および疑似着信転送の転送先を設定できます。

☛ 参照 「着信転送の設定を行う」（P.376）、「疑似着信転送を使う」（P.371）

1.　受話器を上げ、ツーという音が聞こえることを確認します。

2.　ダイヤル操作で設定を変更します。

✱0✱に続けて操作番号＋転送先電話番号をダイヤルします。

機能	操作番号
契約者回線番号の転送先	610
ポート1のダイヤルインの転送先	611
ポート2のダイヤルインの転送先	612
鳴り分け番号1の転送先	613
鳴り分け番号2の転送先	614
鳴り分け番号3の転送先	615

例）契約者回線番号を「03-1111-2222」に着信転送する設定を行う場合

✱0✱6103111122222 をダイヤルします。

3.　ピピッという音とビジートーン（プープープーという話中の音）が聞こえます。

補足 ピピッという音の鳴る回数は設定した機能によって異なります。

- 契約者回線番号の転送先を設定した場合　：1回
- ポート1のダイヤルイン番号の転送先を設定した場合　：2回
- ポート2のダイヤルイン番号の転送先を設定した場合　：3回
- 鳴り分け番号1の転送先を設定した場合　：4回
- 鳴り分け番号2の転送先を設定した場合　：5回
- 鳴り分け番号3の転送先を設定した場合　：6回

正常に設定できなかった場合は、ビジートーン（プープープーという話中の音）だけが聞こえます。

4.　受話器を置きます。

■ TELメールを設定する

アナログポートに接続したアナログ機器から、TELメールを設定できます。

☛ 参照 「TELメール機能」（P.547）

1.　受話器を上げ、ツーという音が聞こえることを確認します。

2.　ダイヤル操作で設定を変更します。

✱0✱に続けて操作番号をダイヤルします。

機能		操作番号
TELメール機能の設定	使用しない	2101
	使用する	2102

3.　ピピッという音とビジートーン（プープープーという話中の音）が聞こえます。

補足 ピピッという音の鳴る回数は設定した機能によって異なります（操作で入力した最後の数字の回数です）。
正常に設定できなかった場合は、ビジートーン（プープープーという話中の音）だけが聞こえます。

4.　受話器を置きます。

■ メールチェックを実行する

アナログポートに接続したアナログ機器から、メールチェックを実行できます。

☛ 参照 「メールチェック機能」（P.536）

1.　受話器を上げ、ツーという音が聞こえることを確認します。

2.　✱0✱8300をダイヤルします。

3.　ピピッという音が2回とビジートーン（プープープーという話中の音）が聞こえます。

補足 正常に設定できなかった場合は、ビジートーン（プープープーという話中の音）だけが聞こえます。

4.　受話器を置きます。

■ 留守状態を設定する

アナログポートに接続したアナログ機器から、留守確認機能の留守状態を設定できます。

☛ 参照 「留守状態を確認する（無課金）」（P.425）

1.　受話器を上げ、ツーという音が聞こえることを確認します。

2.　ダイヤル操作で設定を変更します。

✱0✱に続けて操作番号をダイヤルします。

機能		操作番号
留守状態の設定	在宅	2001
	留守	2002

3.　ピピッという音とビジートーン（プープープーという話中の音）が聞こえます。

補足 ピピッという音の鳴る回数は設定した機能によって異なります。（操作で入力した最後の数字の回数です）。
正常に設定できなかった場合は、ビジートーン（プープープーという話中の音）だけが聞こえます。

4.　受話器を置きます。

■ 留守モードを設定する

アナログポートに接続したアナログ機器から、留守モードを設定できます。

☛ 参照 「留守モードの動作を設定する」（P.586）

1.　受話器を上げ、ツーという音が聞こえることを確認します。

2.　ダイヤル操作で設定を変更します。

✱0✱に続けて操作番号をダイヤルします。

機能		操作番号
留守モードの設定	解除	8401
	実行	8402

3.　ピピッという音とビジートーン（プープープーという話中の音）が聞こえます。

補足 ピピッという音の鳴る回数は設定した機能によって異なります（操作で入力した最後の数字の回数です）。
正常に設定できなかった場合は、ビジートーン（プープープーという話中の音）だけが聞こえます。

4.　受話器を置きます。

外線から設定を変更する（無課金）

外線から設定できる項目を以下に示します。

- スタンバイモードの設定
- 着信転送の設定
- アナログポートの接続機器の設定
- ナンバー・ディスプレイの設定
- 着信転送先の設定
- TEL メールの設定
- 留守状態の設定

こんな事に気をつけて

サブアドレスを使用するので、発信側はサブアドレスを指定できるISDN機器（電話、PHSなど）の必要があります。

アナログポート（内線）からも設定を変更できます。

☛ 参照　内線から設定を変更する→「電話機を利用して設定を変更する」（P.410）

■ 設定変更用暗証番号を設定する

外線から設定を変更するには暗証番号が必要です（数字4桁）。

ここでは、設定変更用暗証番号を「5678」に設定する場合を例に説明します。

こんな事に気をつけて

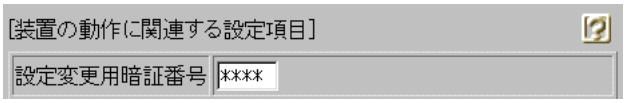
設定変更用暗証番号は「アナログポート情報」の「サブアドレス」の設定と別のものを設定してください。

1.　詳細設定メニューのアナログ設定で「アナログ共通情報」をクリックします。

「アナログ共通情報」ページが表示されます。

2.　［装置の動作に関する設定項目］で以下の項目を指定します。

- 設定変更用暗証番号　→5678（任意の数字4桁を指定します）



3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

補足　外線からの設定変更をやめる場合は、設定変更用暗証番号を削除してください。

■ 外線からアナログ機能の設定を変更する

外線の電話機から、以下のアナログ機能を設定できます。

- スタンバイモードの設定（通常モード／スタンバイモード）
- 着信転送の設定（しない／する／疑似着信転送）
- 接続機器の設定（なし／電話／モデム／ FAX／ FAX（無鳴動強制着信／無鳴動識別着信／キャッチホン着信））
- ナンバー・ディスプレイの設定（使用しない／使用する（モード1）／使用する（モード2））

補足 すでにBチャネルを2本使用しているときに、外線から設定を変更する場合、NTTの通信中着信サービスの契約が必要です。

1. 受話器を上げ、ツーという音が聞こえることを確認します。

2. ダイヤル操作で設定を変更します。

契約者回線番号、ダイヤルイン番号、または鳴り分け番号に続けて、サブアドレスとして［設定変更用暗証番号（4桁）］＋操作番号をダイヤルします。

機能		操作番号
スタンバイモード	通常モード	8001
	スタンバイモード	8002
着信転送	しない	6001
	する	6002
	疑似着信転送	6003
接続機器の設定	なし	40P1
	電話	40P2
	モデム	40P3
	FAX	40P4
	FAX（無鳴動強制着信）	40P5
	FAX（無鳴動識別着信）	40P6
	FAX（キャッチホン着信）	40P7
ナンバー・ディスプレイ	使用しない	41P1
	使用する（モード1）	41P2
	使用する（モード2）	41P3

Pには、設定を変更するアナログポートのポート番号（1または2）を入れます。

3.　呼び出し音が聞こえます。

補足
- 設定変更用暗証番号を間違えた場合は、以下のメッセージが聞こえます。
「おかけになった電話番号にはあなたと通信できる機器が接続されていません」
- 正常に設定できなかった場合は、ビジートーン（プープープーという話中の音）が聞こえます。
- この場合、本装置側には着信音は鳴りません。

4.　受話器を置きます。

■ 外線から着信転送先を設定する

外線の電話機から、着信転送および疑似着信転送の転送先を設定できます。

1.　受話器を上げ、ツーという音が聞こえることを確認します。

2.　ダイヤル操作で設定を変更します。

契約者回線番号、ダイヤルイン番号、または鳴り分け番号に続けて、サブアドレスとして［設定変更用暗証番号（4桁）］＋操作番号＋転送先電話番号をダイヤルします。

機能	操作番号
契約者回線番号の転送先	610
ポート1のダイヤルインの転送先	611
ポート2のダイヤルインの転送先	612
鳴り分け番号1の転送先	613
鳴り分け番号2の転送先	614
鳴り分け番号3の転送先	615

3.　呼び出し音が聞こえます。

補足
- 設定変更用暗証番号を間違えた場合は、以下のメッセージが聞こえます。
「おかけになった電話番号にはあなたと通信できる機器が接続されていません」
- 正常に設定できなかった場合は、ビジートーン（プープープーという話中の音）が聞こえます。
- この場合、本装置側には着信音は鳴りません。

4.　受話器を置きます。

■ 外線から TEL メールを設定する

外線の電話機から、TELメールを設定できます。

1.　受話器を上げ、ツーという音が聞こえることを確認します。

2.　ダイヤル操作で設定を変更します。

契約者回線番号、ダイヤルイン番号、または鳴り分け番号に続けて、サブアドレスとして［設定変更用暗証番号（4桁）］＋操作番号＋転送先番号をダイヤルします。

機能		操作番号
TEL メール機能の設定	使用しない	2101
	使用する	2102

3.　呼び出し音が聞こえます。

補足
- 設定変更用暗証番号を間違えた場合は、以下のメッセージが聞こえます。
「おかけになった電話番号にはあなたと通信できる機器が接続されていません」
- 正常に設定できなかった場合は、ビジートーン（プープープーという話中の音）が聞こえます。
- この場合、本装置側には着信音は鳴りません。

4.　受話器を置きます。

■ 外線から留守状態を設定する

外線の電話機から、留守確認機能の留守状態を設定できます。

☛ 参照 「留守状態を確認する（無課金）」（P.425）

1.　受話器を上げ、ツーという音が聞こえることを確認します。

2.　ダイヤル操作で設定を変更します。

契約者回線番号、ダイヤルイン番号、または鳴り分け番号に続けて、サブアドレスとして［設定変更用暗証番号（4桁）］＋操作番号をダイヤルします。

機能		操作番号
留守状態の設定	在宅	2001
	留守	2002

3.　呼び出し音が聞こえます。

補足
- 設定変更用暗証番号を間違えた場合は、以下のメッセージが聞こえます。
「おかけになった電話番号にはあなたと通信できる機器が接続されていません」
- 正常に設定できなかった場合は、ビジートーン（プープープーという話中の音）が聞こえます。
- この場合、本装置側には着信音は鳴りません。

4.　受話器を置きます。

留守状態を確認する（無課金）

留守中に外線から着信した場合、留守番電話に切り替わることなく相手に留守中であることを知らせる機能です。留守の場合は、呼び出し音のあとにビジートーン（プープープーという話中の音）が送出され、在宅の場合は、通常の呼び出し音が鳴ります。留守番電話に切り替わらないので、電話料金がかかりません。

留守確認用番号の設定をする

留守状態を確認するには、確認用番号が必要です（数字4桁）。

こんな事に気をつけて

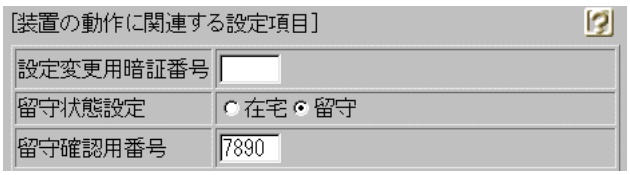
確認用番号は「アナログポート情報」の「サブアドレス」の設定と別のものを設定してください。

1.　詳細設定メニューのアナログ設定で「アナログ共通情報」をクリックします。

「アナログ共通情報」ページが表示されます。

2.　［装置の動作に関連する設定項目］で以下の項目を指定します。

- 留守確認用番号　→7890（任意の数字4桁を指定します。）



3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

「留守」または「在宅」の設定をする

外出時、帰宅時は以下のように「留守」、「在宅」を設定します。

1.　受話器を上げ、ツーという音が聞こえることを確認します。

2.　ダイヤル操作で設定を変更します。

✱0✱に続けて操作番号をダイヤルします。

機能		操作番号
留守状態の設定	在宅	2001
	留守	2002

3.　ピピッという音とビジートーン（プープープーという話中の音）が聞こえます。

補足 ピピッという音の鳴る回数は設定した機能によって異なります（操作で入力した最後の数字の回数です）。
正常に設定できなかった場合は、ビジートーン（プープープーという話中の音）だけが聞こえます。

4.　受話器を置きます。

留守状態の設定は、電話機からも設定できます。

☛ 参照 「留守状態を設定する」（P.417）、「外線から留守状態を設定する」（P.424）

外線から「留守」または「在宅」を確認する

1.　受話器を上げ、ツーという音が聞こえることを確認します。

2.　契約者回線番号、ダイヤルイン番号、または鳴り分け番号に続けて、サブアドレスとして［留守確認用番号（4桁）］をダイヤルします。

3.　呼び出し音が聞こえます。

［留守が設定されている場合］
呼び出し音の約3秒後にビジートーンが聞こえます。

［在宅が設定されている場合］
相手が受話器をあげると、通話状態になります。

4.　受話器を置きます。

第６章　活用例（ルータ設定）

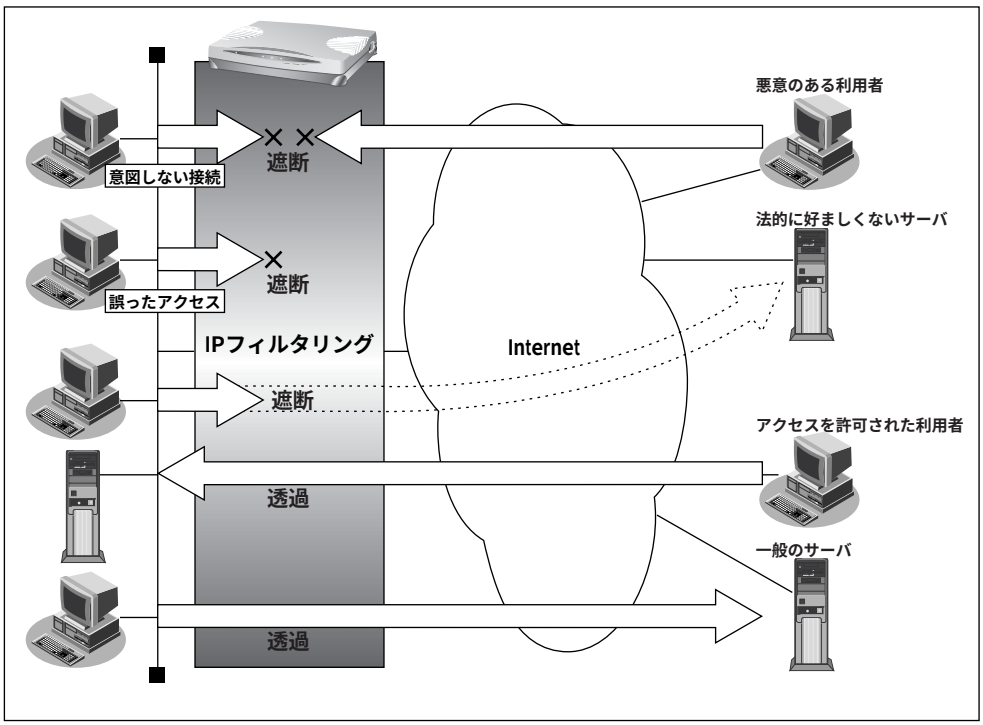
6

この章では、

本装置の便利な機能の活用方法について説明します。

IPフィルタリング機能を使う

本装置を経由してインターネットに送出される、またはインターネットから受信したパケットをIPアドレスとポート番号の組み合わせで制御することによって、ネットワークのセキュリティを向上させたり、回線への超過課金を防止することができます。



ネットワークのセキュリティを向上させるには、以下の要素について考える必要があります。

- ネットワークのセキュリティ方針
- ルータ以外の要素（ファイアウォール、ユーザ認証など）

本装置は、パスワードの設定やIPフィルタリング機能などを使ってネットワークのセキュリティを向上させることができます。

こんな事に気をつけて

- **ProxyDNSを設定している場合、ProxyDNSに対してのIPフィルタを設定しても効果はありません。**
- **本装置などのルータでは、コンピュータウィルスの感染を防ぐことはできません。パソコン側でウィルス対策ソフトを使うなど、別の手段が必要です。**

補足　NAT機能にも、セキュリティを向上させる効果があります。

☛ 参照　「マルチNAT機能（アドレス変換機能）を使う」（P.490）

■ IPフィルタリングのセキュリティ方針

インターネットに接続する場合でもLANどうしを接続する場合でも、データの流れには「外部から内部へ」「内部から外部へ」という2つの方向があります。セキュリティ方針を決める場合は、2つの方向について考慮する必要があります。

● 「外部から内部へ」のデータの流れに対するセキュリティ方針の例

- インターネット（ネットワーク型接続）の場合

  特定のパケットを受け取らないようにする

- インターネット（専用線接続）の場合

  非公開ホストへのアクセスを拒否する

- LANどうしを接続する（ISDN回線を使用）場合

  アクセスポイント電話番号が外部に知られたときの対策を立てる

- LANどうしを接続する（専用線を使用）場合

  内部ユーザによる不要なアクセスを防ぐ

● 「内部から外部へ」のデータの流れに対するセキュリティ方針の例

- インターネットの場合

  法的に問題のあるサイトなどへのアクセスを制限する

- LANどうしを接続する場合

  内部ユーザによる不要なアクセスを防ぐ

補足 IPフィルタリングは「外部から内部へ」流れるデータと「内部から外部へ」流れるデータに対し機能します。内部にあるパソコン間のデータ（LAN内のデータ）に対しては機能しません。

■ IPフィルタリングの条件

本装置では、以下の条件を指定することによって、データの流れを制限できます。

- 動作
- プロトコル
- 送信元情報（IPアドレス／アドレスマスク／ポート番号）
- 宛先情報（IPアドレス／アドレスマスク／ポート番号）
- TCP接続要求
- TOS

動作	遮断	本装置を介した通信が不可能
	透過	本装置を介した通信が可能
	透過（接続中）	本装置を介した通信が回線が接続されている時だけ可能
プロトコル	すべて	IP通信はすべて対象
	UDP	UDP通信だけを対象
	TCP	TCP通信だけを対象
	ICMP	ICMP通信（PINGコマンド）だけを対象
	IPv6 over IPv4	IPv6 over IPv4通信だけを対象
	その他	上記以外の指定
送信元情報 宛先情報 （項目共通）	IPアドレス	対象となるIPアドレス
	アドレスマスク	論理積を算出するのに利用
	ポート番号	対象となるポート番号
TCP接続要求	対象	すべて対象
	対象外	TCPコネクション確立パケットだけを対象外
TOS	TOS値	対象となるTOS値

◆ TCP接続要求とは

TCPプロトコルでのコネクション確立要求を、フィルタリングの対象にするかどうかを指定するものです。フィルタリングの動作に透過、プロトコルにTCPを指定した場合に有効です。TCPプロトコルはコネクション型であるため、コネクション確立要求を発行し、それに対する応答を受信することにより、コネクションを開設します。したがって、一方からのコネクションを禁止する場合でも、コネクション確立要求だけを遮断し、その他の応答や通常データなどを透過させるように設定しないと通信できません。

次に、TCPパケットとフラグ設定について説明します。TCPパケット内にはSYNフラグとACKフラグの2つの制御フラグがあります。このフラグの組み合わせにより、TCPパケットの内容が分かります。以下、対応表を示します。

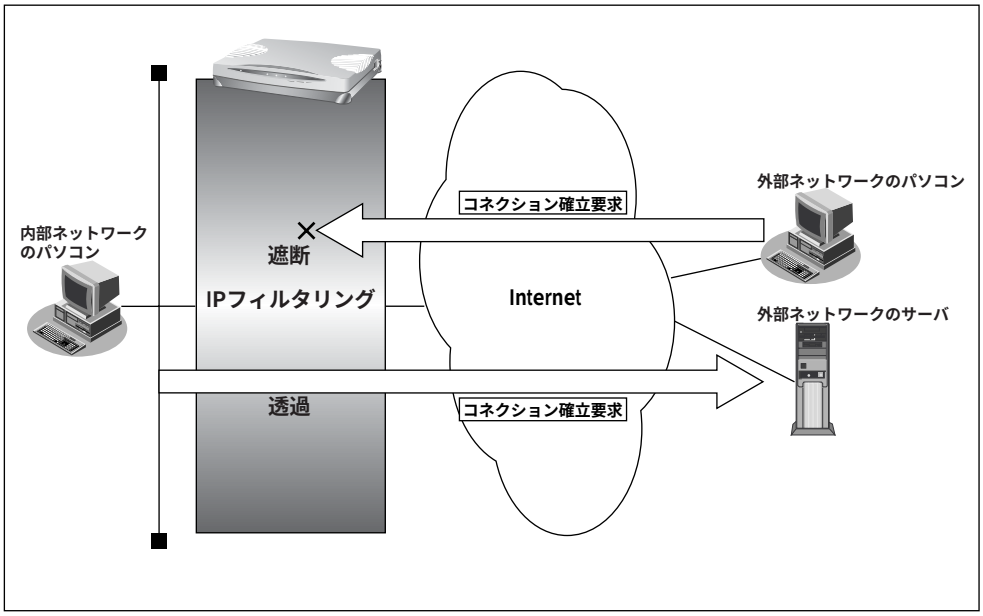
制御フラグ		TCPパケットの内容
SYN	ACK	
1	0	コネクションの確立要求
1	1	確立後の承認応答
0	1	確認応答、通常のデータ

この表から、制御フラグの組み合わせがSYN＝1、ACK＝0の場合にTCPパケットがコネクションの確立要求を行います。つまり、IPパケットが禁止されているIPアドレスからの送信を禁止すれば、TCP/IPサービスのフィルタリングができます。

telnet（ポート番号23）を例に説明します。

・外部ネットワークからのコネクション確立要求は遮断

・内部ネットワークからのコネクション確立要求は許可



◆ IPアドレスとアドレスマスクの決め方

IPフィルタリング条件の要素として「IPアドレス」と「アドレスマスク」があります。制御対象となるパケットは、本装置に届いたパケットのIPアドレスとアドレスマスクの論理積の結果が、指定したIPアドレスと一致したものに限ります。

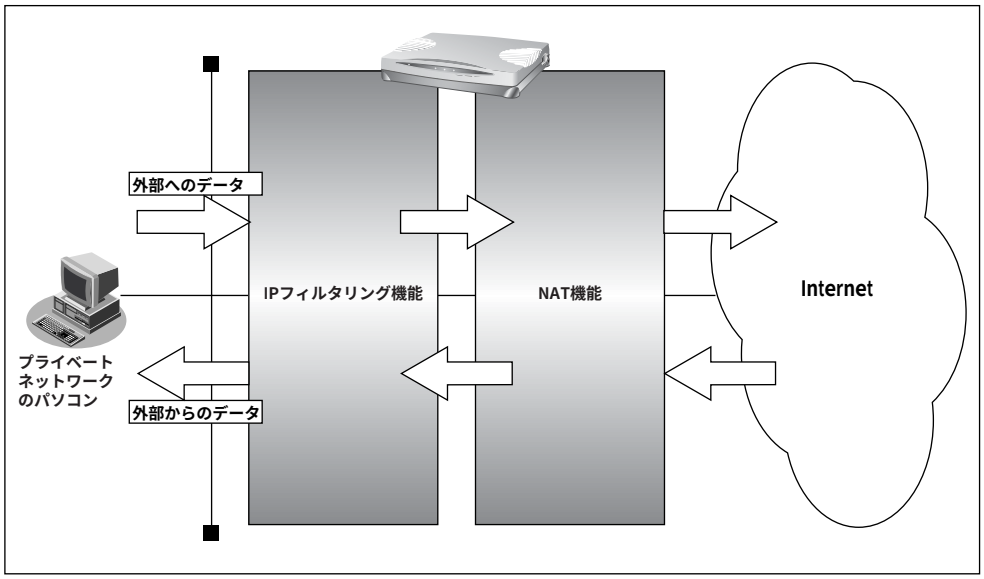
☛ 参照 「用語集」（P.755）

ヒント

◆アドレス変換（NAT）機能利用時のIPフィルタリングのかかるタイミング

プライベートネットワークからインターネット上に向かう場合は、アドレス変換でアドレスが変更される前にフィルタリング処理を通過します。また、インターネットからプライベートネットワークに向かう場合は、アドレス変換でアドレスが変更されたあとでフィルタリング処理を通過します。つまり、IPフィルタリングは「プライベートアドレス」を対象に行います。

本装置のIPフィルタリングとアドレス変換の位置付けは以下のとおりです。



補足　IPフィルタリング機能とNAT機能を同時に使用する場合、回線切断時にNAT機能の情報が消えてしまうため、回線切断後に再度接続しても、サーバからの応答が正しくアドレス変換されず、IPフィルタリング機能によってパケットは破棄されてしまいます。

フィルタリングの設計方針には大きく分類して以下の2つがあります。

A. 基本的にはパケットをすべて遮断し、特定の条件のものだけを透過させる。

B. 基本的にはパケットをすべて透過させ、特定の条件のものだけを遮断する。

設計方針Aの例として、以下の設定例について説明します。

- 外部の特定サービスへのアクセスだけを許可する
- 外部から特定サーバへのアクセスだけを許可する

設計方針Bの例として、以下の設定例について説明します。

- 利用者が意図しない発信を防ぐ
- 特定アドレスへのアクセスを禁止する
- 回線が接続しているときだけ許可する

補足 TCP 接続要求の設定は、プロトコルにTCPまたはすべてを指定した場合にだけ有効です。それ以外のプロトコルを指定した場合は無効となります。

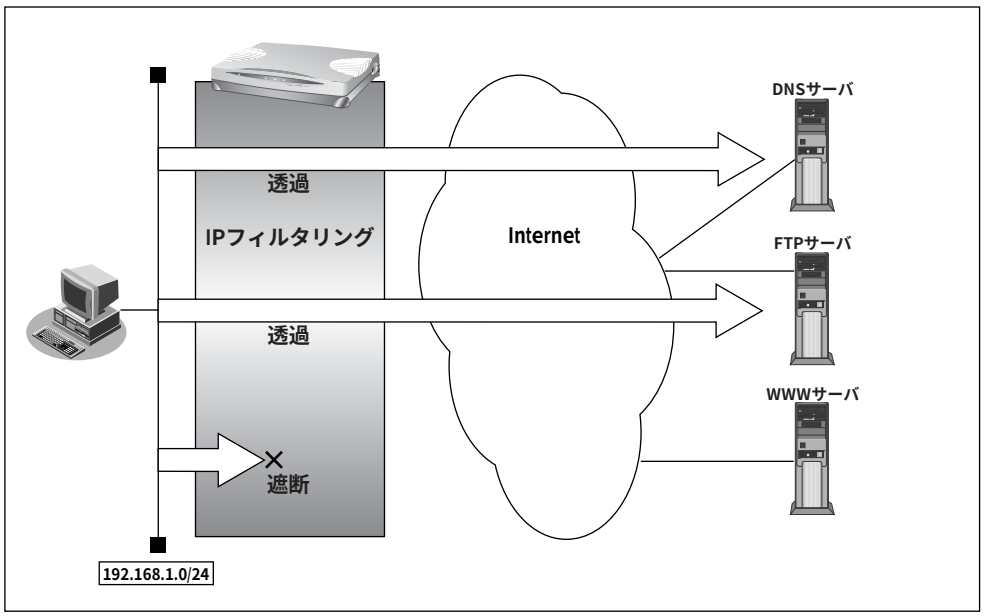
こんな事に気をつけて

フィルタリング条件が複数存在する場合、それぞれの条件に優先順位がつき、数値の小さいものから優先的に採用されます。設定内容によっては通信できなくなる場合がありますので、優先順位を意識して設定してください。

■ 外部の特定サービスへのアクセスだけを許可する

ここでは、LAN上のパソコンからインターネット上のすべてのFTPサーバに対してアクセスすることだけを許可し、ほかのサーバ（WWWサーバなど）へのアクセスを禁止する場合の設定方法を説明します。ただし、FTPサーバ名を解決するために、DNSサーバへのアクセスは許可します。

補足
- ftpでホスト名を指定する場合、DNSサーバに問い合わせが発生するため、DNSサーバへのアクセスを許可する必要があります。DNSサーバへのアクセスを許可することによって、ftpサービス以外でドメイン名を指定した場合もDNSサーバへの発信が発生します。あらかじめ接続するFTPサーバが決まっている場合は、本装置のDNSサーバ機能を利用することによって、DNSサーバへの発信を抑止することができます。
- 本装置は、ftp-dataの転送に関するフィルタリングルールを自動的に作成します。



● フィルタリング設計

- LAN 上のホスト（192.168.1.0/24）から任意のFTP サーバへのアクセスを許可
- LAN 上のホスト（192.168.1.0/24）からWAN の先のDNS サーバへのアクセスを許可
- ICMP の通信を許可
- その他はすべて遮断

こんな事に気をつけて

ICMPは、IP通信を行う際にさまざまな制御メッセージを交換します。ICMPの通信を遮断すると正常な通信ができなくなる場合がありますので、ICMP の通信を透過させる設定を行ってください。

● フィルタリングルール

- FTP サーバへのアクセスを許可するには
  （1）192.168.1.0/24 の任意のポートから、任意のFTP サーバのポート21（ftp）へのTCP パケットを透過させる
  （2）（1）の応答パケットを透過させる
- DNS サーバへのアクセスを許可するには
  （1）192.168.1.0/24 の任意のポートから、DNS サーバのポート53（domain）へのUDP パケットを透過させる
  （2）（1）の応答パケットを透過させる
- ICMP の通信を許可するためには
  （1）ICMP パケットを透過させる
- その他をすべて遮断するには
  （1）すべてのパケットを遮断する

補足 このルールでは ftp passive モードによるデータ転送はできません。

上記のフィルタリングルールの設定を行う場合を例に説明します。

任意のFTP サーバのポート21へのTCP パケットを透過させる（LAN→インターネット）

1.　詳細設定メニューのルータ設定の「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］でフィルタリングの設定を行うネットワーク情報の欄の［修正］ボタンをクリックします。

「ネットワーク情報設定」ページが表示されます。

3.　［IP フィルタリング情報一覧］で［追加］ボタンをクリックします。

「IP フィルタリング情報」ページが表示されます。

4.　［IP フィルタリング情報］で以下の項目を指定します。

- 動作　→透過
- プロトコル　→tcp
- 送信元情報
  IP アドレス　→192.168.1.0
  アドレスマスク　→24
  ポート番号　→なにも設定しない
- 宛先情報
  IP アドレス　→なにも設定しない
  アドレスマスク　→なにも設定しない
  ポート番号　→21（ftp のポート番号）
- TCP 接続要求　→対象
- TOS　→なにも設定しない

5.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

FTPサーバからの応答パケットを透過させる（インターネット→LAN）

6.　手順3.～5.を参考に、以下の情報を指定します。

［IPフィルタリング情報］

- 動作　→透過
- プロトコル　→tcp
- 送信元情報
  IPアドレス　→なにも設定しない
  アドレスマスク　→なにも設定しない
  ポート番号　→21（ftpのポート番号）
- 宛先情報
  IPアドレス　→192.168.1.0
  アドレスマスク　→24
  ポート番号　→なにも設定しない
- TCP接続要求　→対象外
- TOS　→なにも設定しない

DNSサーバのポート53へのUDPパケットを透過させる（LAN→インターネット）

7.　手順3.～5.を参考に、以下の情報を指定します。

［IPフィルタリング情報］

- 動作　→透過
- プロトコル　→udp
- 送信元情報
  IPアドレス　→192.168.1.0
  アドレスマスク　→24
  ポート番号　→なにも設定しない
- 宛先情報
  IPアドレス　→なにも設定しない
  ポート番号　→53（domainのポート番号）
- TCP接続要求　→対象
- TOS　→なにも設定しない

DNSサーバからの応答パケットを透過させる（インターネット→ LAN）

8.　手順3. ～5. を参考に、以下の情報を指定します。

［IPフィルタリング情報］

- 動作　→透過
- プロトコル　→ udp
- 送信元情報
  IPアドレス　→なにも設定しない
  アドレスマスク　→なにも設定しない
  ポート番号　→ 53（domainのポート番号）
- 宛先情報
  IPアドレス　→ 192.168.1.0
  アドレスマスク　→ 24
  ポート番号　→なにも設定しない
- TCP 接続要求　→対象
- TOS　→なにも設定しない

ICMPのパケットを透過させる

9.　手順3. ～5. を参考に、以下の情報を指定します。

［IPフィルタリング情報］

- 動作　→透過
- プロトコル　→ icmp
- 送信元情報
  IPアドレス　→なにも設定しない
  アドレスマスク　→なにも設定しない
  ポート番号　→なにも設定しない
- 宛先情報
  IPアドレス　→なにも設定しない
  アドレスマスク　→なにも設定しない
  ポート番号　→なにも設定しない
- TCP 接続要求　→対象
- TOS　→なにも設定しない

残りのパケットをすべて遮断する

10.　手順3.～5.を参考に、以下の情報を指定します。

［IPフィルタリング情報］

- 動作　→遮断
- プロトコル　→すべて
- 送信元情報
  IPアドレス　→なにも設定しない
  アドレスマスク　→なにも設定しない
  ポート番号　→なにも設定しない
- 宛先情報
  IPアドレス　→なにも設定しない
  アドレスマスク　→なにも設定しない
  ポート番号　→なにも設定しない
- TCP接続要求　→対象
- TOS　→なにも設定しない

11.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

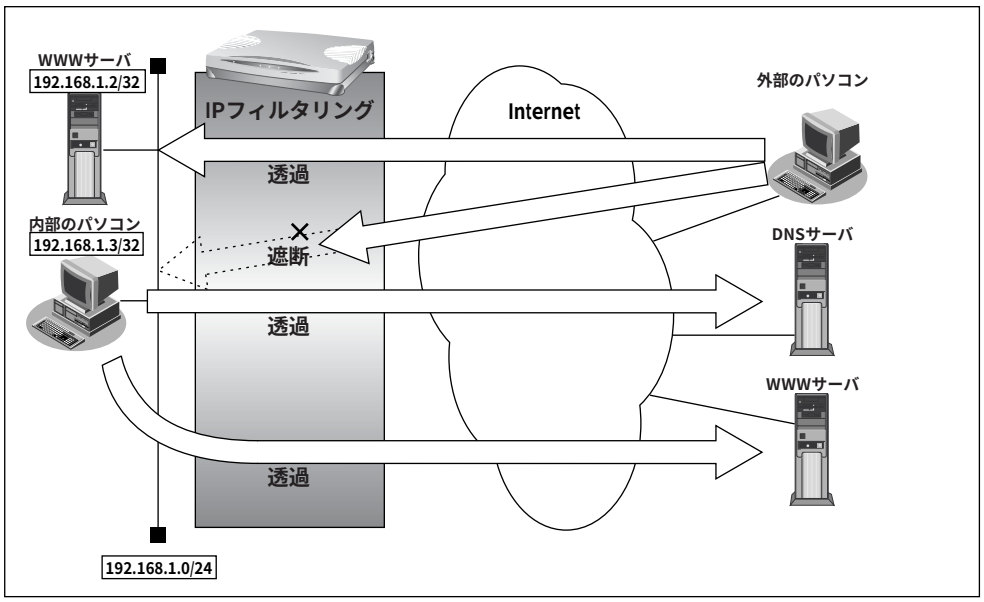
12.　［更新］ボタンをクリックします。

13.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

■ 外部から特定サーバへのアクセスだけを許可する

ここでは、LAN上のWWWサーバに対する外部のパソコンからのアクセスを許可し、LAN上のほかのパソコンへのアクセスは禁止する場合の設定方法を説明します。また、LAN上のほかのパソコンはインターネット上のWWWサーバに対してアクセスすると想定されるため、そのアクセスには制限をつけません。



● フィルタリング設計

- LAN上のホスト（192.168.1.2/32）をWWWサーバとして利用を許可
- LAN上のホスト（192.168.1.3/32）から任意のWWWサーバへのアクセスを許可
- LAN上のホスト（192.168.1.0/24）からWANの先のDNSサーバへのアクセスを許可
- ICMPの通信を許可
- その他はすべて遮断

こんな事に気をつけて

ICMPは、IP通信を行う際にさまざまな制御メッセージを交換します。ICMPの通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPの通信を透過させる設定を行ってください。

● フィルタリングルール

- LAN上のホストのWWWサーバとしての利用を許可するには

  (1)192.168.1.2/32のポート80（www-http）へのパケットを透過させる

  (2)(1）の応答パケットを透過させる

- 任意のWWWサーバへのアクセスを許可するには

  (1)192.168.1.3/32の任意のポートから任意のWWWサーバのポート80（www-http）へのパケットを透過させる

  (2)(1）の応答パケットを透過させる

- DNSサーバへのアクセスを許可するには
  (1)192.168.1.0/24の任意のポートからDNSサーバのポート53（domain）へのUDPパケットを透過させる
  (2)(1）の応答パケットを透過させる
- ICMPの通信を許可するためには
  (1)ICMPパケットを透過させる
- その他をすべて遮断するには
  (1)すべてのパケットを遮断する

上記のフィルタリングルールの設定を行う場合を例に説明します。

LAN上のホストのポート80へのパケットを透過させる（インターネット→LAN）

1.　ルータ設定の「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］でフィルタリングの設定を行うネットワーク情報の欄の［修正］ボタンをクリックします。

「ネットワーク情報設定」ページが表示されます。

3.　［IPフィルタリング情報一覧］で［追加］ボタンをクリックします。

「IPフィルタリング情報」ページが表示されます。

4.　［IPフィルタリング情報］で以下の項目を指定します。

- 動作　→透過
- プロトコル　→tcp
- 送信元情報
  IPアドレス　→なにも設定しない
  アドレスマスク　→なにも設定しない
  ポート番号　→なにも設定しない
- 宛先情報
  IPアドレス　→192.168.1.2
  アドレスマスク　→32
  ポート番号　→80（WWW-httpのポート番号）
- TCP接続要求　→対象
- TOS　→なにも設定しない

5.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

LAN上のホストからの応答パケットを透過させる（LAN→インターネット）

6.　手順3.～5.を参考に、以下の情報を指定します。

［IPフィルタリング情報］

- 動作　→透過
- プロトコル　→tcp
- 送信元情報
  IPアドレス　→192.168.1.2
  アドレスマスク　→32
  ポート番号　→80（WWW-httpのポート番号）
- 宛先情報
  IPアドレス　→なにも設定しない
  アドレスマスク　→なにも設定しない
  ポート番号　→なにも設定しない
- TCP接続要求　→対象外
- TOS　→なにも設定しない

任意のWWWサーバのポート80へのパケットを透過させる（LAN→インターネット）

7.　手順3.～5.を参考に、以下の情報を指定します。

［IPフィルタリング情報］

- 動作　→透過
- プロトコル　→tcp
- 送信元情報
  IPアドレス　→192.168.1.3
  アドレスマスク　→32
  ポート番号　→なにも設定しない
- 宛先情報
  IPアドレス　→なにも設定しない
  アドレスマスク　→なにも設定しない
  ポート番号　→80（WWW-httpのポート番号）
- TCP接続要求　→対象
- TOS　→なにも設定しない

任意のWWWサーバからの応答パケットを透過させる（インターネット→LAN）

8.　手順3.～5.を参考に、以下の情報を指定します。

［IPフィルタリング情報］

- 動作　→透過
- プロトコル　→tcp
- 送信元情報
  IPアドレス　→なにも設定しない
  アドレスマスク　→なにも設定しない
  ポート番号　→80（www-httpのポート番号）
- 宛先情報
  IPアドレス　→192.168.1.3
  アドレスマスク　→32
  ポート番号　→なにも設定しない
- TCP接続要求　→対象外
- TOS　→なにも設定しない

DNSサーバのポート53へのUDPパケットを透過させる（LAN→インターネット）

9.　手順3.～5.を参考に、以下の情報を指定します。

［IPフィルタリング情報］

- 動作　→透過
- プロトコル　→udp
- 送信元情報
  IPアドレス　→192.168.1.0
  アドレスマスク　→24
  ポート番号　→なにも設定しない
- 宛先情報
  IPアドレス　→なにも設定しない
  アドレスマスク　→なにも設定しない
  ポート番号　→53（domainのポート番号）
- TCP接続要求　→対象外
- TOS　→なにも設定しない

DNSサーバからの応答パケットを透過させる（インターネット→ LAN）

10.　手順3.～5.を参考に、以下の情報を指定します。

［IPフィルタリング情報］

- 動作　→透過
- プロトコル　→udp
- 送信元情報
  IPアドレス　→なにも設定しない
  アドレスマスク　→なにも設定しない
  ポート番号　→53（domainのポート番号）
- 宛先情報
  IPアドレス　→192.168.1.0
  アドレスマスク　→24
  ポート番号　→なにも設定しない
- TCP接続要求　→対象外
- TOS　→なにも設定しない

ICMPのパケットを透過させる

11.　手順3.～5.を参考に、以下の情報を指定します。

［IPフィルタリング情報］

- 動作　→透過
- プロトコル　→icmp
- 送信元情報
  IPアドレス　→なにも設定しない
  アドレスマスク　→なにも設定しない
  ポート番号　→なにも設定しない
- 宛先情報
  IPアドレス　→なにも設定しない
  アドレスマスク　→なにも設定しない
  ポート番号　→なにも設定しない
- TCP接続要求　→対象
- TOS　→なにも設定しない

残りのパケットをすべて遮断する

12.　手順3.～5.を参考に、以下の情報を指定します。

［IPフィルタリング情報］

- 動作　→遮断
- プロトコル　→すべて
- 送信元情報
  IPアドレス　→なにも設定しない
  アドレスマスク　→なにも設定しない
  ポート番号　→なにも設定しない
- 宛先情報
  IPアドレス　→なにも設定しない
  アドレスマスク　→なにも設定しない
  ポート番号　→なにも設定しない
- TCP接続要求　→対象
- TOS　→なにも設定しない

13.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

14.　［更新］ボタンをクリックします。

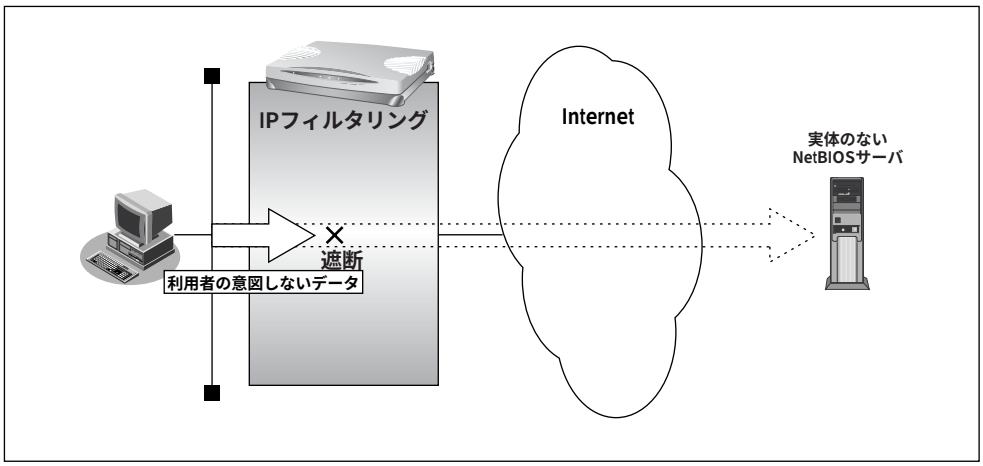
15.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

■ 利用者が意図しない発信を防ぐ

LAN上のパソコンは、利用者の意志とは無関係に、実体のないNetBIOSサーバにアクセスすることがあります。そのとき、回線が接続され、利用者が意識しないところで通信料金がかかってしまいます。

ここでは、上記のような、回線に対するむだな発信を抑止する場合のフィルタリング設定方法を説明します。



● フィルタリング設計

- ポート137～139（NetBIOSサービス）へのアクセスを禁止

● フィルタリングルール

- ポート137～139へのアクセスを禁止するには

  (1)任意のアドレスのポート137～139へのすべてのパケットを遮断する

  (2)任意のアドレスのポート137～139からのすべてのパケットを遮断する

補足 Windows®（TCP上のNetBIOS）環境のネットワークでは、セキュリティ上の問題とむだな課金を抑えるために、ポート番号137～139の外向きの転送経路をふさいでおく必要があります（「かんたん設定」の「かんたんフィルタ」では、自動的にこれらのポートをふさぐように設定されます）。

上記のフィルタリングルールの設定を行う場合を例に説明します。

ポート137～139へのすべてのパケットを遮断する

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］でフィルタリングの設定を行うネットワーク情報の欄の［修正］ボタンをクリックします。

「ネットワーク情報設定」ページが表示されます。

3.　［IPフィルタリング情報一覧］で［追加］ボタンをクリックします。

「IPフィルタリング情報」ページが表示されます。

4.　［IPフィルタリング情報］で以下の項目を指定します。

- 動作　→遮断
- プロトコル　→すべて
- 送信元情報
  - IPアドレス　→なにも設定しない
  - アドレスマスク　→なにも設定しない
  - ポート番号　→なにも設定しない
- 宛先情報
  - IPアドレス　→なにも設定しない
  - アドレスマスク　→なにも設定しない
  - ポート番号　→137-139
- TCP接続要求　→対象
- TOS　→なにも設定しない

5.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

ポート137～139からのすべてのパケットを遮断する

6.　手順3.～5.を参考に、以下の情報を指定します。

［IPフィルタリング情報］

- 動作　→遮断
- プロトコル　→すべて
- 送信元情報
  IPアドレス　→なにも設定しない
  アドレスマスク　→なにも設定しない
  ポート番号　→137-139
- 宛先情報
  IPアドレス　→なにも設定しない
  アドレスマスク　→なにも設定しない
  ポート番号　→なにも設定しない
- TCP接続要求　→対象
- TOS　→なにも設定しない

7.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

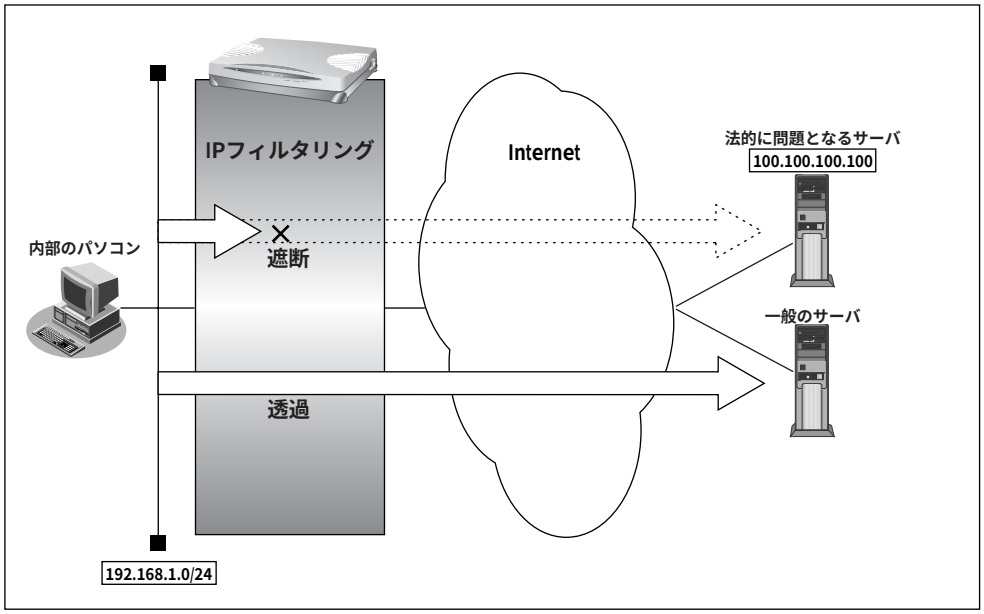
8.　［更新］ボタンをクリックします。

9.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

■ 特定アドレスへのアクセスを禁止する

ここでは、インターネット上の不当なサーバ（法的に問題となるようなサーバなど）に対するアクセスを禁止する場合の設定方法を説明します。



● フィルタリング設計

- LAN上のホスト（192.168.1.0/24）からアドレス100.100.100.100へのアクセスを禁止

● フィルタリングルール

- 特定アドレスへのアクセスを禁止するには

  (1)192.168.1.0/24から100.100.100.100の任意のポートへのすべてのパケットを遮断する

上記のフィルタリングルールの設定を行う場合を例に説明します。

アドレス（100.100.100.100）へのすべてのパケットを遮断する（LAN→インターネット）

1.　詳細設定メニューのルータ設定の「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］でフィルタリングの設定を行うネットワーク情報の欄の［修正］ボタンをクリックします。

「ネットワーク情報設定」ページが表示されます。

3.　［IP フィルタリング情報一覧］で［追加］ボタンをクリックします。

「IP フィルタリング情報」ページが表示されます。

4.　［IP フィルタリング情報］で以下の項目を指定します。

- 動作　→遮断
- プロトコル　→すべて
- 送信元情報
  IP アドレス　→ 192.168.1.0
  アドレスマスク　→ 24
  ポート番号　→なにも設定しない
- 宛先情報
  IP アドレス　→ 100.100.100.100
  アドレスマスク　→ 32
  ポート番号　→なにも設定しない
- TCP 接続要求　→対象
- TOS　→なにも設定しない

5.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

6.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

7.　［更新］ボタンをクリックします。

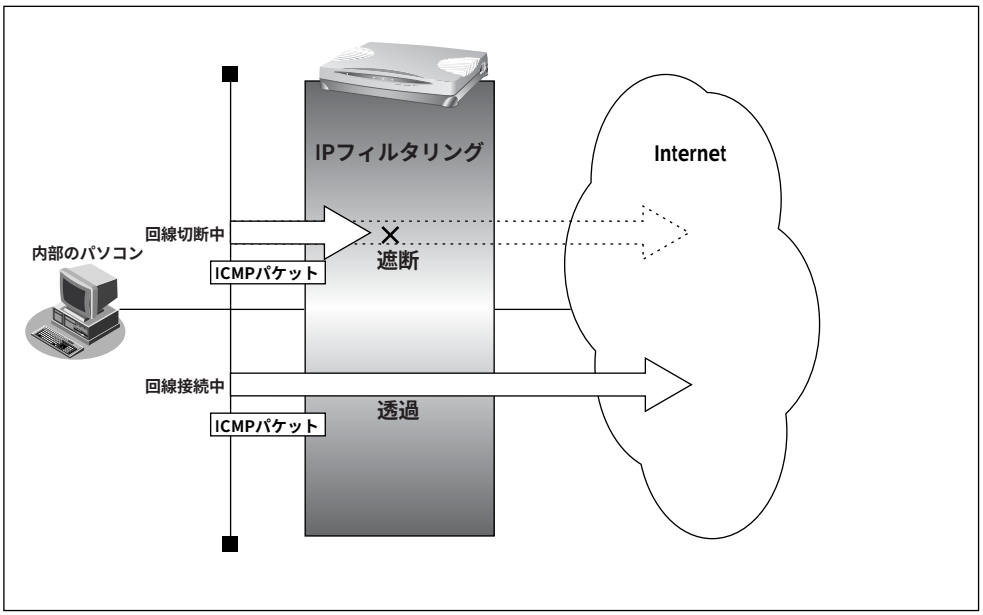
8.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

■ 回線が接続している時だけを許可する

一部のパソコンでは、ネットワークの設定によって、ログイン時に自動的にPINGを発行して回線を接続してしまうものがあります。回線接続を必要とするICMPパケットを遮断することによって、意図しないPINGによるむだな発信を抑止することができます。ここでは、回線が接続されているときにだけICMPパケットを透過させる場合の設定方法を説明します。

補足 IPアドレスを直接指定せず、DNSによる名前アドレス変換を利用した場合、発信を抑止することはできません。



● フィルタリング設計

- すでに回線が接続している場合だけPINGを許可

● フィルタリングルール

- すでに回線が接続している場合にだけPINGを許可するには

  (1)回線接続中だけICMPパケットを透過させる

上記のフィルタリングルールの設定を行う場合を例に説明します。

回線が接続しているときだけICMPパケットを透過させる

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］でフィルタリングの設定を行うネットワーク情報の欄の［修正］ボタンをクリックします。

「ネットワーク情報設定」ページが表示されます。

3.　［IPフィルタリング情報一覧］で［追加］ボタンをクリックします。

「IPフィルタリング情報」ページが表示されます。

4.　［IPフィルタリング情報］で以下の項目を指定します。

- 動作　→透過（接続中）
- プロトコル　→icmp
- 送信元情報
  IPアドレス　→なにも設定しない
  アドレスマスク　→なにも設定しない
  ポート番号　→なにも設定しない
- 宛先情報
  IPアドレス　→なにも設定しない
  アドレスマスク　→なにも設定しない
  ポート番号　→なにも設定しない
- TCP接続要求　→対象外
- TOS　→なにも設定しない

5.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

6.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

7.　［更新］ボタンをクリックします。

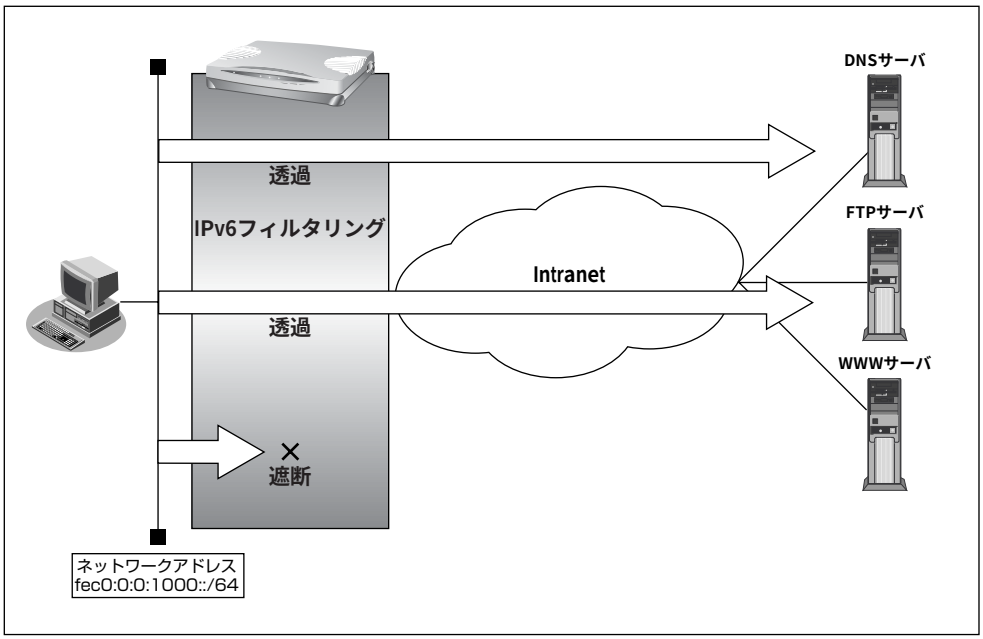
8.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

■ 外部の特定サービスへのアクセスだけを許可する（IPv6フィルタリング）

ここでは、IPv6フィルタリングを使って、LAN上のパソコンからイントラネット上のすべてのFTPサーバに対してアクセスすることだけを許可し、ほかのサーバ（WWWサーバなど）へのアクセスを禁止する場合の設定方法を説明します。ただし、FTPサーバ名を解決するためにDNSサーバへのアクセスを許可する設定にします。

補足 ftpでホスト名を指定する場合、DNSサーバに問い合わせが発生するため、DNSサーバへのアクセスを許可する必要があります。DNSサーバへのアクセスを許可することによって、ftpサービス以外でドメイン名を指定する場合もDNSサーバへの発信が発生します。



● フィルタリング設計

- LAN上のホスト（fec0:0:0:1000::/64）から任意のFTPサーバへのアクセスを許可
- LAN上のホスト（fec0:0:0:1000::/64）からWANの先のDNSサーバへのアクセスを許可
- ICMPv6の通信を許可
- その他はすべて遮断

こんな事に気をつけて

ICMPv6は、IPv6通信を行う際にさまざまな制御メッセージを交換します。ICMPv6の通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPv6の通信を透過させる設定を行ってください。

● フィルタリングルール

- FTP サーバへのアクセスを許可するには

  (1)fec0:0:0:1000::/64 の任意のポートから、任意のFTP サーバのポート 21（ftp）への TCP パケットを透過させる

  (2)(1) の応答パケットを透過させる

  (3)fec0:0:0:1000::/64 の任意のポートから、任意のFTP サーバのポート 20（ftp-data）への TCP パケットを透過させる

  (4)(3) の応答パケットを透過させる

- DNS サーバへのアクセスを許可するには

  (1)fec0:0:0:1000::/64 の任意のポートからDNS サーバのポート 53（domain）への UDP パケットを透過させる

  (2)(1) の応答パケットを透過させる

- ICMPv6 の通信を許可するためには

  (1)ICMPv6 パケットを透過させる

- その他をすべて遮断するには

  (1)すべてのパケットを遮断する

補足 このルールでは ftp passive モードによるデータ転送はできません。

上記のフィルタリングルールの設定を行う場合を例に説明します。

任意のFTP サーバのポート 21（ftp）へのTCP パケットを透過させる（LAN→イントラネット）

1.　詳細設定メニューのルータ設定の「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］でフィルタリングの設定を行うネットワーク情報の欄の［修正］ボタンをクリックします。

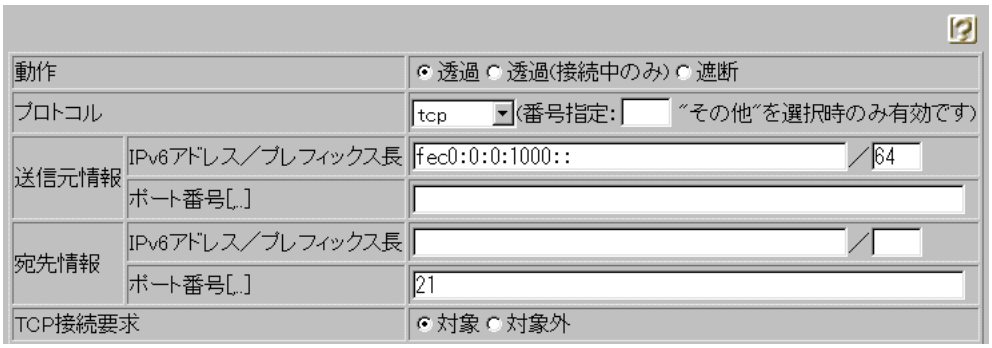
「ネットワーク情報設定」ページが表示されます。

3.　［IPv6 フィルタリング情報一覧］で［追加］ボタンをクリックします。

「IPv6 フィルタリング情報設定」ページが表示されます。

4.　［IPv6フィルタリング情報］で以下の項目を指定します。

- 動作　→透過
- プロトコル　→tcp
- 送信元情報
  IPv6アドレス／プレフィックス長　→fec0:0:0:1000::/64
  ポート番号　→なにも設定しない
- 宛先情報
  IPv6アドレス／プレフィックス長　→なにも設定しない
  ポート番号　→21（ftpのポート番号）
- TCP接続要求　→対象



5.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

FTPサーバからの応答パケットを透過させる（イントラネット→LAN）

6.　手順3.～5.を参考に、以下の情報を指定します。

［IPv6フィルタリング情報］

- 動作　→透過
- プロトコル　→tcp
- 送信元情報
  IPv6アドレス／プレフィックス長　→なにも設定しない
  ポート番号　→21
- 宛先情報
  IPv6アドレス／プレフィックス長　→fec0:0:0:1000::/64
  ポート番号　→なにも設定しない
- TCP接続要求　→対象外

任意のFTPサーバのポート20へのTCPパケットを透過させる（イントラネット→LAN）

7.　手順3.～5.を参考に、以下の情報を指定します。

［IPv6フィルタリング情報］

- 動作　→透過
- プロトコル　→tcp
- 送信元情報
  IPv6アドレス／プレフィックス長　→なにも設定しない
  ポート番号　→20
- 宛先情報
  IPv6アドレス／プレフィックス長　→fec0:0:0:1000::/64
  ポート番号　→なにも設定しない
- TCP接続要求　→対象

FTPサーバからの応答パケットを透過させる（LAN→イントラネット）

8.　手順3.～5.を参考に、以下の情報を指定します。

［IPv6フィルタリング情報］

- 動作　→透過
- プロトコル　→tcp
- 送信元情報
  IPv6アドレス／プレフィックス長　→fec0:0:0:1000::/64
  ポート番号　→なにも設定しない
- 宛先情報
  IPv6アドレス／プレフィックス長　→なにも設定しない
  ポート番号　→20
- TCP接続要求　→対象外

DNSサーバのポート53へのUDPパケットを透過させる（LAN→イントラネット）

9.　手順3.～5.を参考に、以下の情報を指定します。

［IPv6フィルタリング情報］

- 動作　→透過
- プロトコル　→udp
- 送信元情報
  IPv6アドレス／プレフィックス長　→fec0:0:0:1000::/64
  ポート番号　→なにも設定しない
- 宛先情報
  IPv6アドレス／プレフィックス長　→なにも設定しない
  ポート番号　→53
- TCP接続要求　→対象

DNSサーバからの応答パケットを透過させる（イントラネット→LAN）

10.　手順3.～5.を参考に、以下の情報を指定します。

［IPv6フィルタリング情報］

- 動作　→透過
- プロトコル　→udp
- 送信元情報
  IPv6アドレス／プレフィックス長　→なにも設定しない
  ポート番号　→53
- 宛先情報
  IPv6アドレス／プレフィックス長　→fec0:0:0:1000::/64
  ポート番号　→なにも設定しない
- TCP接続要求　→対象

ICMPv6のパケットを透過させる

11.　手順3.～5.を参考に、以下の情報を指定します。

［IPv6 フィルタリング情報］

- 動作　→透過
- プロトコル　→icmpv6
- 送信元情報
  IPv6アドレス／プレフィックス長　→なにも設定しない
  ポート番号　→なにも設定しない
- 宛先情報
  IPv6アドレス／プレフィックス長　→なにも設定しない
  ポート番号　→なにも設定しない
- TCP 接続要求　→対象

残りのパケットをすべて遮断する

12.　手順3.～5.を参考に、以下の情報を指定します。

［IPv6 フィルタリング情報］

- 動作　→遮断
- プロトコル　→すべて
- 送信元情報
  IPv6アドレス／プレフィックス長　→なにも設定しない
  ポート番号　→なにも設定しない
- 宛先情報
  IPv6アドレス／プレフィックス長　→なにも設定しない
  ポート番号　→なにも設定しない
- TCP 接続要求　→対象

13.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

14.　［更新］ボタンをクリックします。

15.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

TOS値書き換え機能を使う

本装置を経由してインターネットに送出される、またはインターネットから受信したパケットをIPアドレスとポート番号の組み合わせでTOS値を変更することにより、ポリシーベースネットワークのポリシーに合わせることができます。

■ TOS値書き換え機能の条件

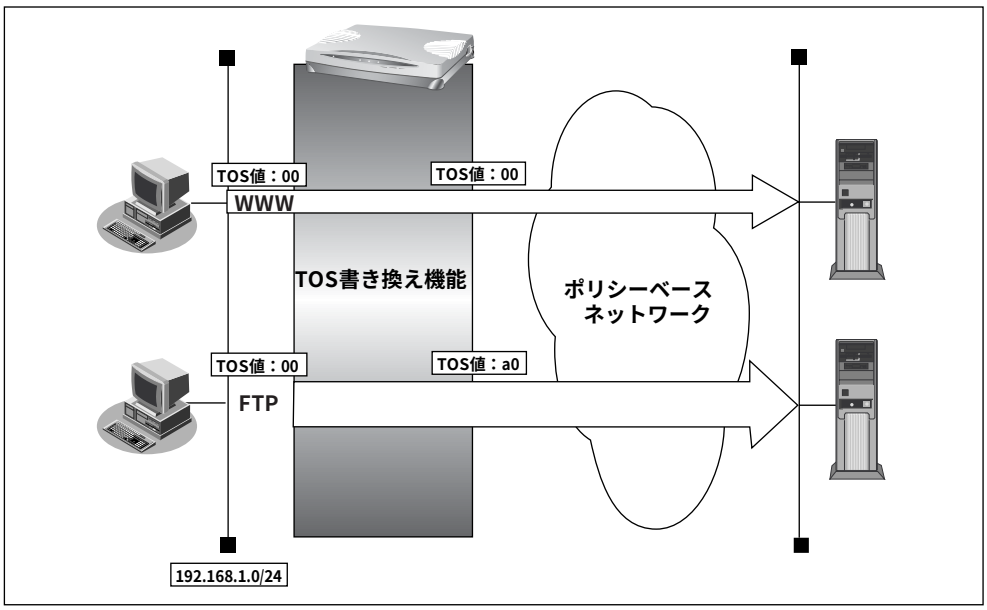
本装置では、以下の条件を指定することによって、ポリシーベースネットワークのポリシーに合ったTOS値に変更することができます。

- プロトコル
- 送信元情報（IPアドレス／アドレスマスク／ポート番号）
- 宛先情報（IPアドレス／アドレスマスク／ポート番号）
- TOS
- 新TOS

プロトコル	すべて	IP通信はすべて対象
	UDP	UDP通信だけを対象
	TCP	TCP通信だけを対象
	ICMP	ICMP通信（PINGコマンド）だけを対象
	IPv6 over IPv4	IPv6 over IPv4通信だけを対象
	その他	上記以外の指定
送信元情報 宛先情報 （項目共通）	IPアドレス	対象となるIPアドレス
	アドレスマスク	論理積を算出するのに利用
	ポート番号	対象となるポート番号
TOS	TOS値	対象となるTOS値
新TOS	TOS値	変更後のTOS値

ここでは、ネットワークが以下のポリシーを持つ場合の設定方法を説明します。

- FTP（TOS 値a0）を最優先とする
- その他はなし



FTP サーバのアクセスで TOS 値を 00 から a0 に変更する

1.　詳細設定メニューのルータ設定の「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］で TOS 値書き換えの設定を行うネットワーク情報の欄の［修正］ボタンをクリックします。

「ネットワーク情報設定」ページが表示されます。

3.　［TOS 値書き換え情報一覧］で［追加］ボタンをクリックします。

「TOS 値書き換え情報設定」ページが表示されます。

4.　［TOS値書き換え情報］で以下の項目を指定します。

- プロトコル　→tcp
- 送信元情報
  IPアドレス　→192.168.1.0
  アドレスマスク　→24
  ポート番号　→なにも設定しない
- 宛先情報
  IPアドレス　→なにも設定しない
  アドレスマスク　→なにも設定しない
  ポート番号　→20（ftp-dataのポート番号）、
  21（ftpのポート番号）
- TOS　→00
- 新TOS　→a0

5.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

6.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

7.　［更新］ボタンをクリックします。

8.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

マルチルーティングを利用する

マルチルーティング機能を使うと、設定した条件によって接続先を変更することができます。

本装置には、以下の3種類のマルチルーティング機能があります。

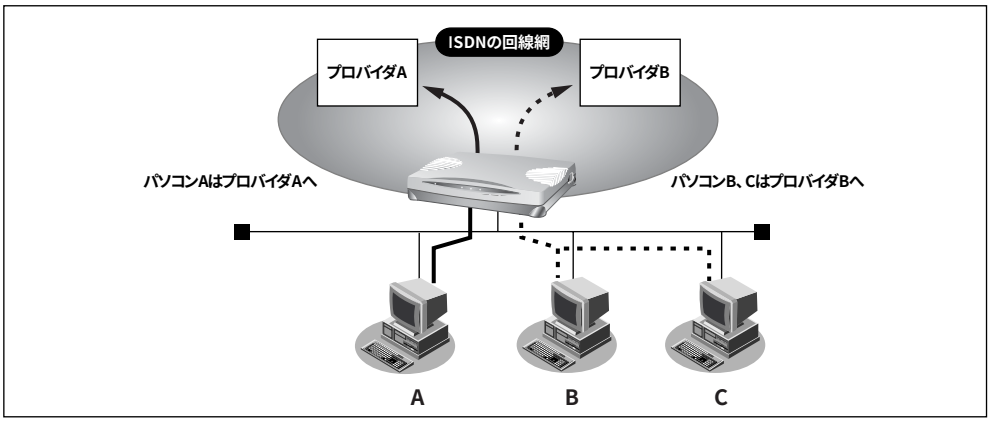
- パソコンごとに別々のプロバイダを利用する（ソースアドレスルーティング機能）
- 目的ごとに別々のプロバイダに接続する（ポートルーティング機能）
- 課金単位でプロバイダを切り替える

これらの機能は組み合わせて利用できます。

■ パソコンごとに別々のプロバイダを利用する（ソースアドレスルーティング機能）

ソースアドレスルーティング機能では、パソコンのIPアドレスごとに接続先を変えることができます。

たとえば、パソコンが複数あって、それぞれ別のプロバイダに接続する場合、本装置のソースアドレスルーティング機能を使うと便利です。

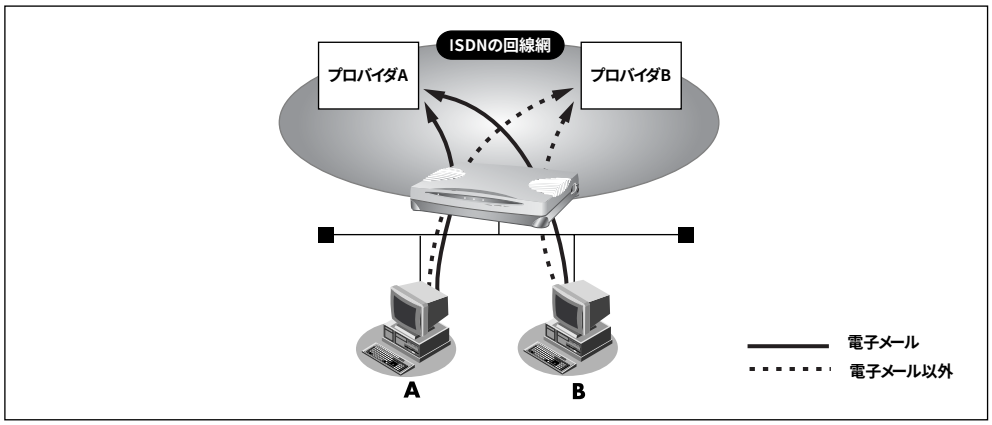


☛ 参照 「複数プロバイダと端末型接続する」（P.161）

■ 目的ごとに別々のプロバイダに接続する（ポートルーティング機能）

ポートルーティング機能では、インターネットで利用するアプリケーション（WWW、電子メールなど）ごとに接続先を変えることができます。

たとえば、電子メールはプロバイダAで、WWWブラウザはプロバイダBで利用するといったことができます。



● 設定条件

- 電子メール利用時はプロバイダAに接続
- プロバイダAのメールサーバホスト名　　：mailhost.provider.or.jp
- 電子メール以外（WWW利用など）はプロバイダBに接続

こんな事に気をつけて

ProxyDNSを使う設定にする必要があります。

☛ 参照 「DNSサーバを使いこなす（ProxyDNS）」（P.471）

マルチルーティング情報を設定する

ここでは、ネットワーク名（internet）配下の「接続先情報」としてプロバイダA（接続先名：ISP-A）、プロバイダB（接続先名：ISP-B）がすでに登録してある場合を例に説明します。

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］で「internet」欄の［修正］ボタンをクリックします。

「ネットワーク情報設定」ページが表示されます。

3.　［接続先情報一覧］で接続先「ISP-A」欄の［修正］ボタンをクリックします。

「接続先情報設定」ページが表示されます。

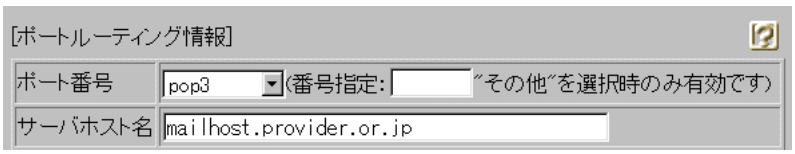
4.　［マルチルーティング］の「ポートルーティング」で［追加］ボタンをクリックします。

「ポートルーティング情報設定」ページが表示されます。

5.　電子メール利用時の設定を行います。

［ポートルーティング情報］で以下の項目を指定します。

- ポート番号　→pop3
- サーバホスト名　→mailhost.provider.or.jp（プロバイダから提示されたメールサーバホスト名）



6.　［更新］ボタンをクリックします。

「接続先情報設定」ページに戻ります。

7.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

8.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

9.　［更新］ボタンをクリックします。

10.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

補足　この例ではサーバホスト名で設定した以外のDNSへの要求は、ISP-Bに発信します。

■ 課金単位でプロバイダを切り替える

複数のプロバイダに加入していて、プロバイダのサービスによって通信料金の算定方法が違っている場合、プロバイダを有効に使い分けることができます。

たとえば、2つのプロバイダ（プロバイダA、プロバイダB）に加入していて、契約が以下に示す内容であるとします。

プロバイダ名	基本料金	追加料金
プロバイダA	2,000円 （接続時間900分まで）	10円／3分 （接続時間901分以降）
プロバイダB	970円 （接続時間600分まで）	10円／分 （接続時間601分以降）

1か月に20時間（1,200分間）インターネットを利用すると、プロバイダに支払う料金は以下のようになります。

・プロバイダAだけを利用

2,000円（プロバイダAの基本料金）＋1,000円（プロバイダAの追加料金）
＋970円（プロバイダBの基本料金）＝3,970円

・プロバイダBだけを利用

2,000円（プロバイダAの基本料金）＋970円（プロバイダBの基本料金）
＋6,000円（プロバイダBの追加料金）＝8,970円

・プロバイダAを900分利用し、プロバイダBを残り300分間利用

2,000円（プロバイダAの基本料金）＋970円（プロバイダBの基本料金）
＋0円（追加料金）＝2,970円

このような使い方をすると、プロバイダに支払う金額はそれぞれのプロバイダの基本料金2,970円だけで済みます（どちらかのプロバイダを解約するよりも安くなります）。

この場合を例に設定方法を説明します。

● 設定条件

- 接続時間900分まではプロバイダA（ISP-A）を利用する
- 接続時間901分以降はプロバイダB（ISP-B）を利用する

メインに使用するプロバイダの制限時間を指定する

ここではネットワーク名（internet）配下の「接続先情報」としてプロバイダA（接続先名：ISP-A）、プロバイダB（接続先名：ISP-B）がすでに登録してある場合を例に説明します。

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］で「internet」欄の［修正］ボタンをクリックします。

「ネットワーク情報設定」ページが表示されます。

3.　［接続先情報一覧］の接続先「ISP-A」の優先順位が「1」でない場合は、移動先の優先順位に「1」を入力し［移動］ボタンをクリックします。すでに優先順位が「1」になっている場合は、手順4.へお進みください。

こんな事に気をつけて

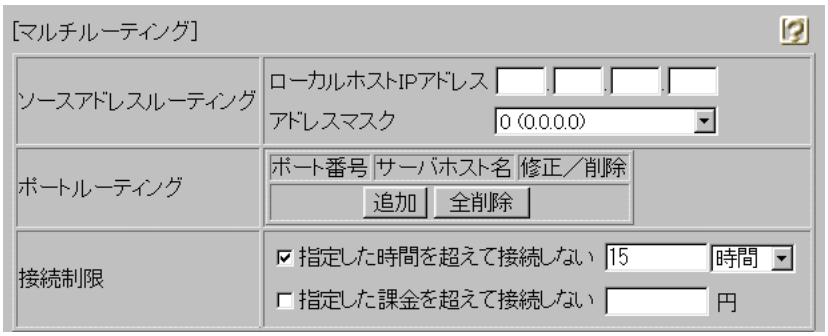
接続先には優先度があるため、マルチルーティングの設定をしない接続先の優先度を高くすると、優先度の低いマルチルーティング設定は無効となります。接続先の優先順位に気をつけてください。

4.　［接続先情報一覧］で接続先「ISP-A」欄の［修正］ボタンをクリックします。

「接続先情報設定」ページが表示されます。

5.　［マルチルーティング］で以下の項目を指定します。

- 接続制限　→指定した時間を超えて接続しない
  15時間



6.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

7.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

8.　［更新］ボタンをクリックします。

9.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

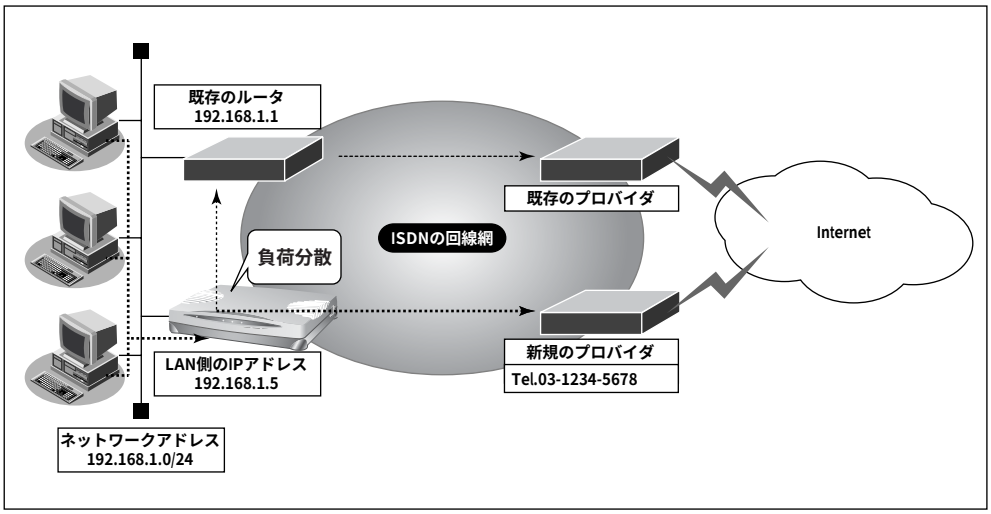
こんな事に気をつけて

- **回線切断されるまでは接続制限処理が行われないため、900分を超えて、プロバイダに接続される場合があります。**
- **本装置の電源を切ると、課金情報（通信時間累計、通信料金累計）はすべてクリアされます。**

マルチホーミング機能を使う

マルチホーミング機能を使い、別のプロバイダとの通信を並行して行うことにより、負荷分散や高信頼性化を実現できます。

ここでは、インターネットへダイヤルアップ接続する場合を例に説明します。



● 設定条件

- ISDN回線を使用する
- 接続先の電話番号　：03-1234-5678
- ユーザ認証ID　：userid
- ユーザ認証パスワード　：userpass
- 転送先ルータIPアドレス　：192.168.1.1
- 転送セッション経路監視用IPアドレス　：192.168.1.1
- ネットワークアドレス／ネットマスク　：192.168.1.0/24
- マルチホーミング機能　：順次方式（セッション数：10）
- マルチNATを使用する
- LAN上にあるパソコンのデフォルトゲートウェイを本装置に変更する

こんな事に気をつけて

- 文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。
  詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。
- マルチホーミング機能を使用する場合は、以下のようなネットワーク環境では、正しく通信できません。
  - DHCPサーバによりIPアドレスを配付している環境で、本装置でマルチホーミング機能とProxyDNS機能を併用し、DNSサーバとして本装置を使用している環境
  - マルチホーミング機能とマルチリンクPPPのBOD機能を同時に使用している環境

  また、以下のようなネットワーク環境では、転送セッション監視用IPアドレスに転送先ルータIPアドレスを指定してください。転送先ルータIPアドレス以外を指定すると正しく通信できない場合があります。
  - 転送先ルータでNAT機能を使用している環境
- WAN側セッション経路監視の宛先IPアドレスを指定した場合は、本装置から宛先IPアドレスの監視ホストに対してICMP ECHOパケットを定期的に送出します。そのため、定額制でない回線をご使用の場合には、超過課金の原因となることがあります。このような環境では、WAN側セッション経路監視の宛先IPアドレスを指定しないでください。
- WAN側セッション経路監視を行う場合は、WAN側セッション経路監視の宛先IPアドレスで指定した監視対象の装置に対して、ICMPパケットを送信（pingコマンドを実行）しないでください。
- 転送セッション経路の監視用IPアドレスとWAN側セッション経路監視の宛先IPアドレスに、誤って同じアドレスを指定した場合などには正しく動作しません。

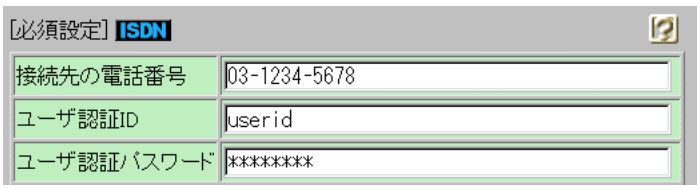
かんたん設定で新規のプロバイダとの接続情報を設定する

1. かんたん設定でインターネットへの「ISDN接続」をクリックします。

「かんたん設定（インターネットへISDN接続）」ページが表示されます。

2. ［必須設定］で以下の項目を指定します。

- 接続先の電話番号　→03-1234-5678（プロバイダから提示された内容）
- ユーザ認証ID　→userid（プロバイダから提示された内容）
- ユーザ認証パスワード　→userpass（プロバイダから提示された内容）



3. ［設定終了］ボタンをクリックします。

再起動後に、通信できる状態になります。

補足　マルチNATを使用する設定はかんたん設定で自動的に設定されます。

マルチホーミング情報を設定する

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］でマルチホーミングの設定を行うネットワーク情報の欄の［修正］ボタンをクリックします。

「ネットワーク情報設定」ページが表示されます。

3.　［マルチホーミング情報］で以下の項目を指定します。

- マルチホーミング機能　→順次方式
  切り分け閾値　→セッション数
- 最大セッション数　→10
- 転送先ルータIPアドレス　→192.168.1.1
- 転送セッション経路監視
  監視用IPアドレス　→192.168.1.1

［マルチホーミング情報］

マルチホーミング機能		○ 使用しない ◉ 順次方式 切り分け閾値：◉ セッション数 ○ 回線使用率 ○ 最大回線使用速度 ○ ラウンドロビン方式 ○ 双方方式 切り分け閾値：◉ セッション数 ○ 回線使用率 ○ 最大回線使用速度
最大セッション数		10 セッション
最大回線使用率		0 %
最大回線使用速度		0 Kbps
セッション比率(WAN側:転送側)		0 :10
転送先ルータIPアドレス		192 .168 .1 .1
セッションタイムアウト時間		5 分
転送セッション経路監視	監視用IPアドレス	192 .168 .1 .1
	ping実行間隔	10 秒
	障害認識無応答回数	3 回
	復旧判断応答回数	1 回

必要に応じて上記以外の項目を指定します。

4.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

5.　［更新］ボタンをクリックします。

6.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

パソコンのデフォルトゲートウェイの設定を変更する

パソコンのデフォルトゲートウェイのIPアドレスを192.168.1.5に指定します。

DHCPサーバを使って広報している場合は、広報するデフォルトゲートウェイのIPアドレスを192.168.1.5に指定します。

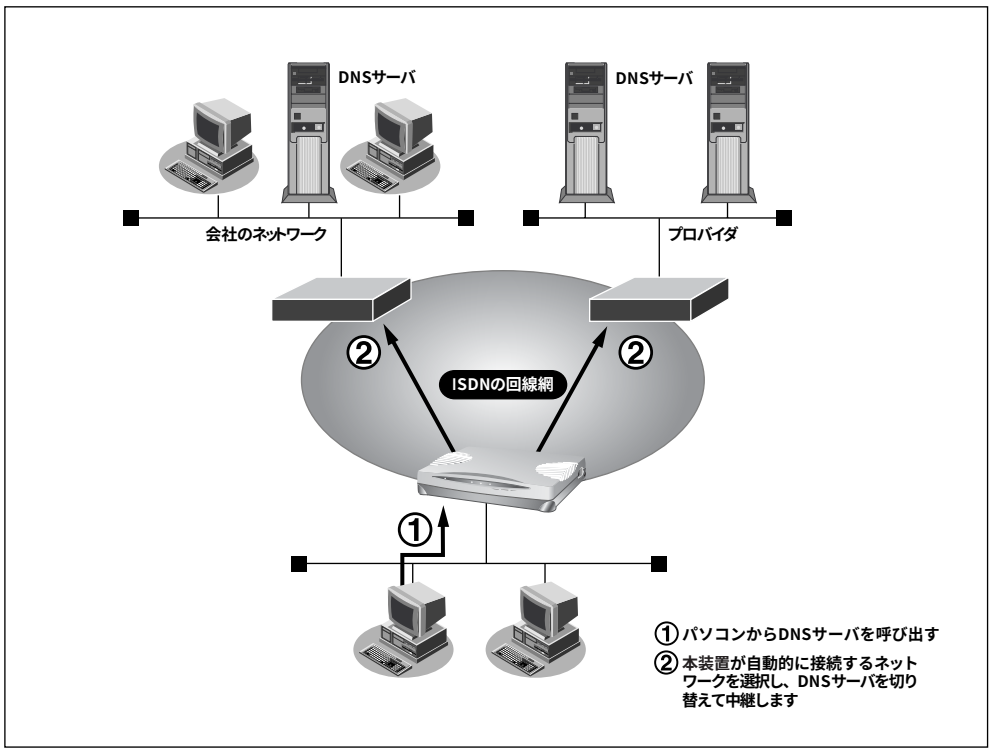
DNSサーバを使いこなす（ProxyDNS）

本装置には、以下の4種類のProxyDNSの機能があります。

- DNSサーバの自動切り替え機能
- DNSサーバアドレスの自動取得機能
- DNS問い合わせタイプフィルタ機能
- DNSサーバ機能

■ DNSサーバの自動切り替え機能

複数のプロバイダに接続するような場合、パソコンのDNSサーバのIPアドレスを変更して、再起動する必要がありました。ProxyDNSを使えば、このような手続きは必要ありません。パソコンからDNSサーバを呼び出すと、ProxyDNSが自動的に接続するネットワークを選択し、DNSサーバを切り替えて中継します。



ここでは、すでに会社のネットワークとプロバイダの接続が設定されている場合を例に説明します。また、ProxyDNS 情報は一切設定されていないものとします。

● 設定条件

[会社のネットワーク]

- ネットワークアドレス　：172.16.0.0/16
- ネットワークの名前　：kaisya
- 会社のドメイン名　：＊.kaisya.co.jp

[プロバイダ]

- ネットワークの名前　：internet

会社の ProxyDNS 情報を設定する

1.　詳細設定メニューのルータ設定で、「ProxyDNS 情報」をクリックします。

「ProxyDNS 情報」ページが表示されます。

2.　「順引き情報一覧」で［追加］ボタンをクリックします。

「ProxyDNS 情報設定（順引き）」ページが表示されます。

3.　以下の項目を指定します。

- ドメイン名　→＊.kaisya.co.jp
- 動作　→接続先の DNS サーバへ問い合わせる
  ネットワーク名　→kaisya

4.　［更新］ボタンをクリックします。

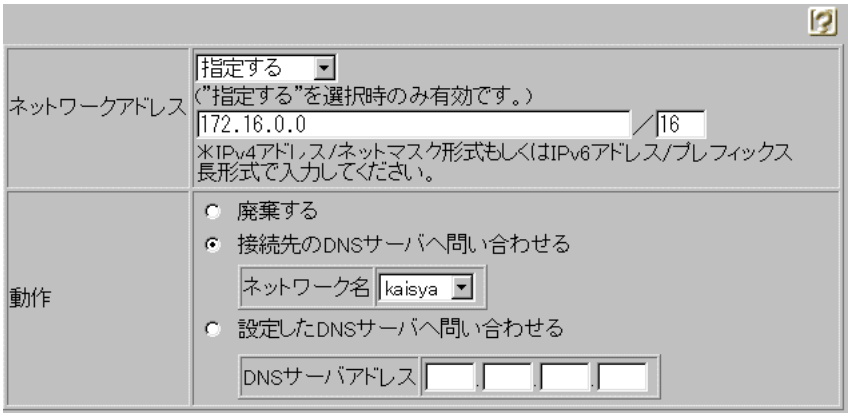
「ProxyDNS 情報」ページに戻ります。

5.　「逆引き情報一覧」で［追加］ボタンをクリックします。

「ProxyDNS 情報設定（逆引き）」ページが表示されます。

6.　以下の項目を指定します。

- ネットワークアドレス　→172.16.0.0/16
- 動作　→接続先のDNSサーバへ問い合わせる
  ネットワーク名　→kaisya



7.　[更新] ボタンをクリックします。

「ProxyDNS情報」ページに戻ります。

インターネットのProxyDNS情報を設定する

8.　手順2.～4.を参考に、以下の情報を指定します。

[ProxyDNS情報設定（順引き）]

- ドメイン名　→*
- 動作　→接続先のDNSサーバへ問い合わせる
  ネットワーク名　→internet

9.　手順5.～7.を参考に、以下の情報を指定します。

[ProxyDNS情報設定（逆引き）]

- ネットワークアドレス　→すべて
- 動作　→接続先のDNSサーバへ問い合わせる
  ネットワーク名　→internet

10.　[設定反映] ボタンをクリックします。

設定した内容が有効になります。

補足　かんたん設定のインターネットへの「ISDN接続」で、DNSサーバを「自動取得」にすると、ProxyDNS情報が自動的に設定されます。

☛参照　「かんたん設定（インターネットへISDN接続）」の省略値について（P.74）

パソコン側の設定を行う

ここではWindows® XPの場合を例に説明します。

1. **［スタート］－［コントロールパネル］をクリックします。**
2. **［ネットワーク接続とインターネット接続］をクリックします。**
3. **［ネットワーク接続］をクリックします。**
4. **［ローカルエリア接続］アイコンを右クリックし、［プロパティ］をクリックします。**
   ［ローカルエリア接続のプロパティ］ダイアログボックスが表示されます。
5. **一覧から「インターネットプロトコル（TCP/IP）」を選択し、［プロパティ］ボタンをクリックします。**
   ［インターネットプロトコル（TCP/IP）のプロパティ］ダイアログボックスが表示されます。
6. **「次のDNSサーバーのアドレスを使う」を選択します。**
7. **「優先DNSサーバー」に本装置のIPアドレスを指定します。**
8. **［OK］ボタンをクリックします。**
   ［ローカルエリア接続のプロパティ］ダイアログボックスが表示されます。
9. **［OK］ボタンをクリックします。**
   パソコンを再起動するかを確認するメッセージが表示されます。
10. **［はい］ボタンをクリックし、パソコンを再起動します。**
    再起動後に設定した内容が有効になります。

ヒント

◆本装置の「DHCPサーバ機能」を使わない場合の設定は？

かんたん設定のインターネットへの「ISDN接続」で、DNSサーバを「自動取得」にした場合、自動的にProxyDNSが有効になります。パソコン側の「DNSサーバの設定」で本装置のIPアドレスを設定すると、ProxyDNSだけ使用できます。また、本装置以外のDHCPサーバを使用している場合でも、DHCPサーバで広報するDNSサーバのIPアドレスとして本装置のIPアドレスを設定するとProxyDNSが利用できます。

■ DNSサーバアドレスの自動取得機能

ProxyDNSが、回線接続時に接続先からDNSサーバのアドレスを自動的に取得するため、DNSサーバのアドレスを設定する必要がありません。

なお、この機能は接続先がDNSサーバアドレスの配布機能（RFC1877）に対応している場合にだけ使用できます。

本装置側の設定を行う

1.　詳細設定メニューのルータ設定で「ProxyDNS情報」をクリックします。

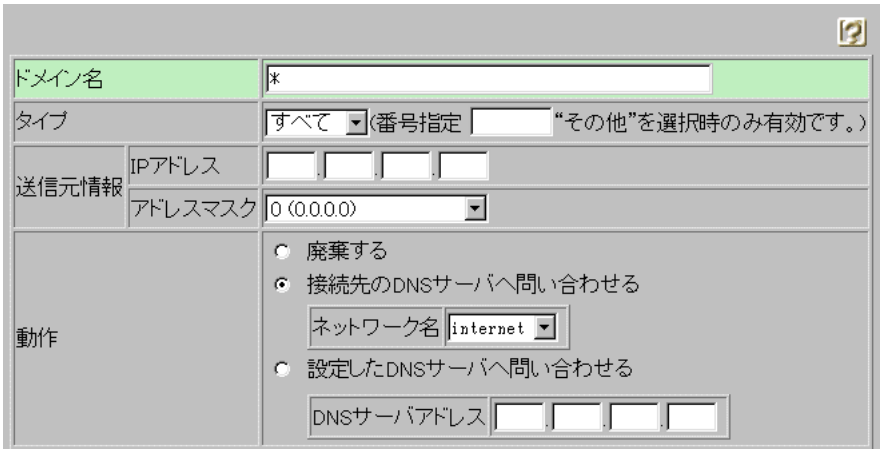
「ProxyDNS情報」ページが表示されます。

2.　［順引き情報一覧］で［追加］ボタンをクリックします。

「ProxyDNS情報設定（順引き）」ページが表示されます。

3.　以下の項目を指定します。

- ドメイン名　→＊
- 動作　→接続先のDNSサーバへ問い合わせる
  ネットワーク名　→internet（DNSサーバを使用するネットワーク名）



4.　［更新］ボタンをクリックします。

「ProxyDNS情報」ページに戻ります。

5.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

パソコン側の設定を行う

「DNSサーバの自動切り替え機能」の「パソコン側の設定を行う」（P.474）を参照して、パソコンの設定を行います。

■ DNS問い合わせタイプフィルタ機能

端末が送信するDNSパケットのうち、特定の問い合わせタイプ（QTYPE）のパケットを破棄することができます。
たとえば、Windows® 2000が送信する予期しないDNSパケットによって、自動発信する問題を回避するために、かんたん設定のかんたんフィルタを「使用する」にした場合は、問い合わせタイプがSOA（6）とSRV（33）のパケットを廃棄する設定を行います。

☛ 参照 「かんたん設定（インターネットへISDN接続）」の省略値について（P.74）

こんな事に気をつけて

ProxyDNSを使用し、問い合わせタイプがA（1）のDNS問い合わせパケットを破棄する設定を行うと、正常な通信が行えません。

問い合わせタイプがSOA (6) のDNS問い合わせパケットを破棄する設定を以下に説明します。

本装置側の設定を行う

1.　詳細設定メニューのルータ設定で「ProxyDNS情報」をクリックします。

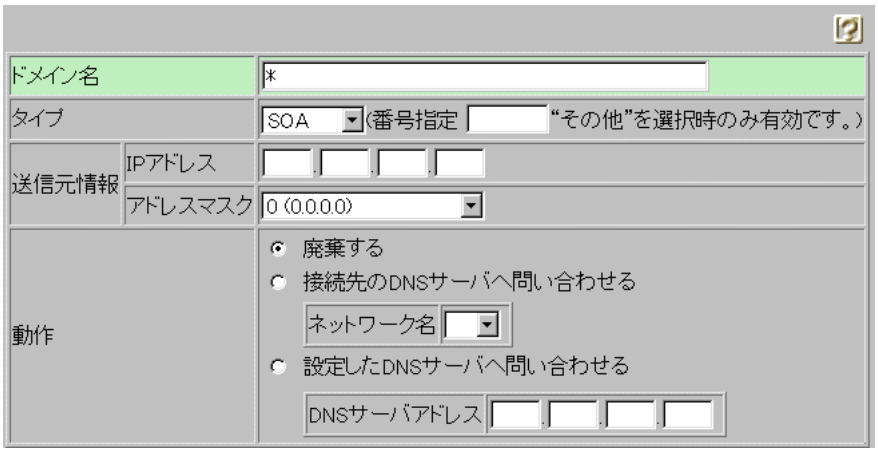
「ProxyDNS情報」ページが表示されます。

2.　［順引き情報一覧］で［追加］ボタンをクリックします。

「ProxyDNS情報設定（順引き）」ページが表示されます。

3.　以下の項目を指定します。

- ドメイン名　→＊
- タイプ　→SOA
- 動作　→廃棄する



4.　［更新］ボタンをクリックします。

「ProxyDNS情報」ページに戻ります。

5.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

パソコン側の設定を行う

「DNSサーバの自動切り替え機能」の「パソコン側の設定を行う」（P.474）を参照して、パソコンの設定を行います。

■ DNSサーバ機能

本装置のホストデータベースに、ホスト名とIPアドレスの両方を登録しておきます。登録したホストへのDNSリクエストがあった場合は、ProxyDNSがDNSサーバの代わりに応答します。LAN内の情報をあらかじめホストデータベースに登録しておくと、LAN内のホストのDNSリクエストによって回線が接続されてしまうといったトラブルを防止できます。

本装置側の設定を行う

1.　詳細設定メニューのルータ設定で「ホストデータベース情報」をクリックします。

「ホストデータベース情報」ページが表示されます。

＼	ホスト名	IPアドレス	MACアドレス	Wake-up-ID	電源制御	修正／削除
1	-	-	-	-	-	修正 削除
2	-	-	-	-	-	修正 削除
3	-	-	-	-	-	修正 削除

2.　未設定の欄の［修正］ボタンをクリックします。

「ホストデータベース情報設定」ページが表示されます。

3.　以下の項目を指定します。

- ホスト名　→host（パソコンの名前）
- IPアドレス　→192.168.1.2（パソコンのIPアドレス）

補足 ホストデータベース情報は「リモートパワーオン機能」、「DHCPスタティック機能」、「DNSサーバ機能」で使われており、それぞれ必要な項目だけを指定します。

4.　［更新］ボタンをクリックします。

「ホストデータベース情報」ページに戻ります。

5.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

パソコン側の設定を行う

「DNSサーバの自動切り替え機能」の「パソコン側の設定を行う」（P.474）を参照して、パソコンの設定を行います。

DHCP機能を使う

本装置には、以下の3種類のDHCP機能があります。

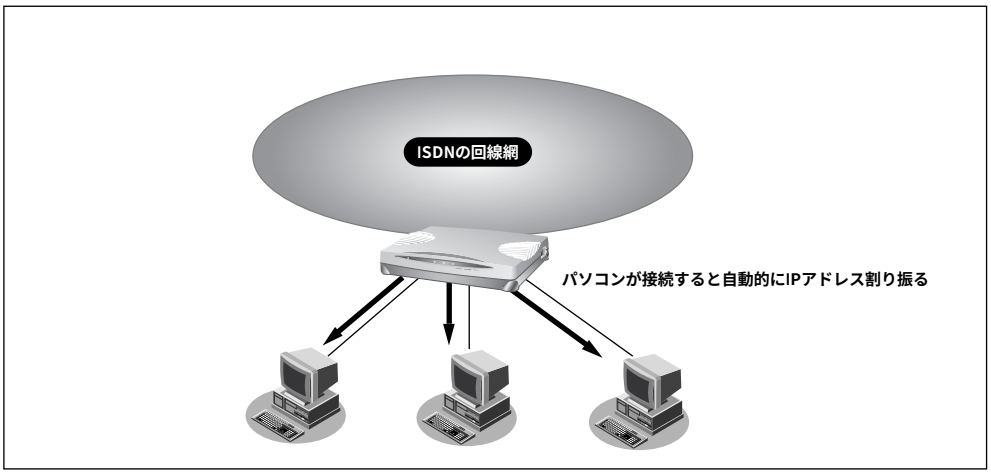
- DHCPサーバ機能
- DHCPスタティック機能
- DHCPリレーエージェント機能

■ DHCPサーバ機能を使う

DHCPサーバ機能は、ネットワークに接続されているパソコンに対して、IPアドレスの自動割り当てを行う機能です。IPアドレスは重複が許されず、また、パソコンが増えるたびに管理者はIPアドレスを設定する必要がありますが、この機能を使用するとDHCPクライアント機能を持つパソコンに対してIPアドレスの設定が不要になり、管理者の手間を大幅に省くことができます。

本装置のDHCPサーバ機能は、以下の情報を広報することができます。

- IPアドレス
- ネットマスク
- デフォルトルータのIPアドレス
- DNSサーバのIPアドレス
- ドメイン名



DHCP サーバ機能を使う場合を例に説明します。

● 設定条件

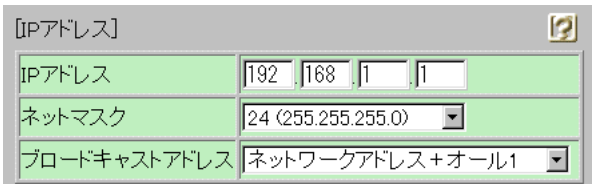
- 本装置のIPアドレス　：192.168.1.1
- DHCP サーバ機能を使用する
- パソコンに割り当てるIPアドレス　：192.168.1.2 ～192.168.1.33
- パソコンに割り当てるIPアドレス数　：64個
- LAN側のネットワークアドレス／ネットマスク　：192.168.1.0/24

1.　詳細設定メニューのルータ設定で「LAN情報」をクリックします。

「LAN情報設定」ページが表示されます。

2.　［IPアドレス］で以下の項目を指定します。

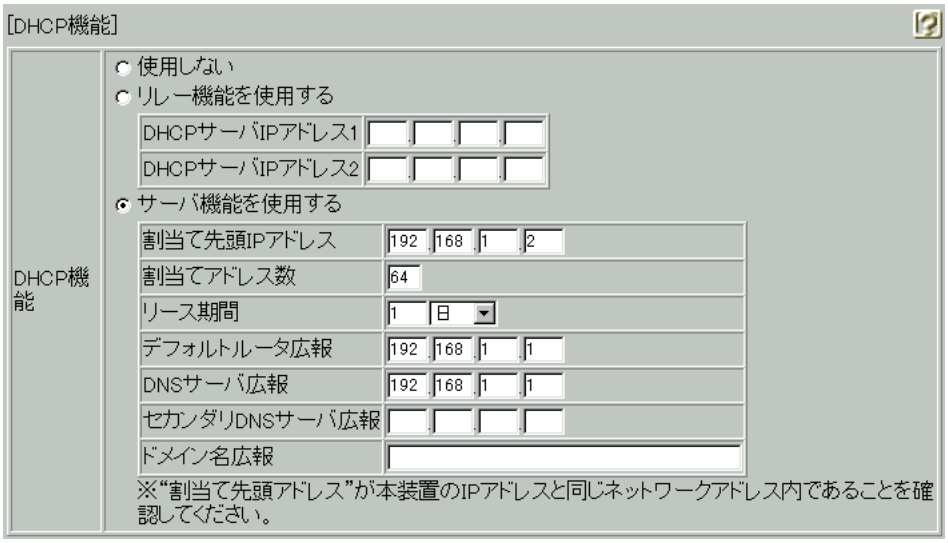
- IPアドレス　→192.168.1.1（本装置のLAN側のIPアドレス）
- ネットマスク　→24
- ブロードキャストアドレス　→ネットワークアドレス＋オール1



［DHCP機能］で以下の項目を指定します。

- DHCP機能　→サーバ機能を使用する
  割当て先頭IPアドレス　→192.168.1.2
  割当てアドレス数　→64

補足 DHCPサーバ機能で割り当てることのできる最大数は64個です。



必要に応じて上記以外の項目を指定します。

3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

■ DHCPスタティック機能を使う

DHCPサーバでは空いているIPアドレスを一定期間（またはパソコンが返却するまで）割り当て、不要になったIPアドレスを自動的に再利用します。このため、パソコンのIPアドレスは変わることがあります。
DHCPスタティック機能では、登録されたパソコンからDHCP要求が発行されると、IPアドレスとMACアドレスを対応付けることによって、常に同じIPアドレスを割り当てることができます。
DHCPスタティック機能を使用する場合は、ホストデータベース情報にIPアドレスとMACアドレスを設定します。

補足
- MACアドレスとは、LAN機器に設定されていて、世界中で重複されないように管理されている固有のアドレスです。
- 本装置がサポートしている「IPフィルタリング機能」、「静的NAT機能」、「マルチルーティング機能」などはパソコンのIPアドレスが固定されていないと使いにくい場合があります。これらの機能とDHCPサーバ機能同時に使用するために、「DHCPスタティック機能」をサポートしています。

DHCPスタティック機能を使う場合を例に説明します。

● 設定条件

- DHCPサーバ機能を使用する
- LAN側のネットワークアドレス／ネットマスク　：192.168.1.0/24
- IPアドレスを固定するパソコンのMACアドレス：00:00:0e:12:34:56
- 割当てIPアドレス　：192.168.1.2

こんな事に気をつけて

詳細設定の「LAN情報」でDHCPサーバ機能を使用する設定をしていない場合は、DHCPスタティック機能の設定は有効になりません。

1.　詳細設定メニューのルータ設定で「ホストデータベース情報」をクリックします。

「ホストデータベース情報」ページが表示されます。

2.　未設定の欄の［修正］ボタンをクリックします。

「ホストデータベース情報設定」ページが表示されます。

3.　以下の項目を指定します。

- IPアドレス　→192.168.1.2
- MACアドレス　→00:00:0e:12:34:56

補足 ホストデータベース情報は「リモートパワーオン機能」、「DHCPスタティック機能」、「DNSサーバ機能」で使われており、それぞれ必要な項目だけを指定します。

必要に応じて上記以外の項目を指定します。

4.　［更新］ボタンをクリックします。

「ホストデータベース情報」ページに戻ります。

5.　［設定反映］ボタンをクリックします。

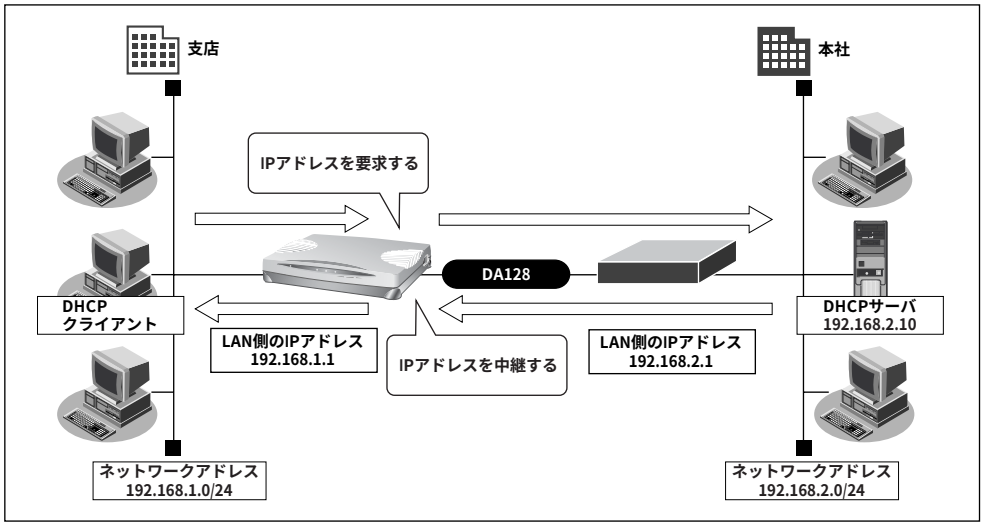
設定した内容が有効になります。

補足 DHCPスタティック機能で設定できるホストの最大数は64個です。

■ DHCP リレーエージェント機能を使う

DHCP クライアントは、同一ネットワーク上にあるサーバからIP アドレスなどの情報を獲得することができます。

DHCP リレーエージェントは、遠隔地にあるDHCP クライアントの要求やDHCP サーバが配布する情報を中継する機能です。この機能を使用すると、遠隔地の別のネットワークにDHCP サーバが存在する場合も同じように情報を獲得することができます。



● 設定条件

- 支店にDHCP クライアントが存在する
- 本社にDHCP サーバが存在する

[本社]

- ルータのIP アドレス　：192.168.2.1
- ネットワークアドレス／ネットマスク　：192.168.2.0/24
- DHCP サーバ　：192.168.2.10

[支店]

- 本装置のIP アドレス　：192.168.1.1
- ネットワークアドレス／ネットマスク　：192.168.1.0/24
- NAT を使用しない

こんな事に気をつけて

- **文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。**
  詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。
- **DHCPリレーエージェント機能を使用する場合は、NAT（アドレス変換）機能を使用できません。**

支店の本装置を設定する場合を例に説明します。

「かんたん設定（オフィスへ専用線接続）」で設定する

［必須設定］

- 本装置のIPアドレス　→192.168.1.1（本装置のLAN側のIPアドレス）
- 本装置のネットマスク　→24（支店側のLAN側のネットマスク）
- 相手ルータのIPアドレス　→192.168.2.1（接続先ルータのIPアドレス）
- 相手ルータのネットマスク　→24（接続先のネットマスク）
- 使用する回線速度　→128Kbps

［オプション設定］

- 接続ネットワーク名　→kaisya（接続するネットワークの名称）

補足 NATを使用しない設定は、かんたん設定で自動的に設定されます。

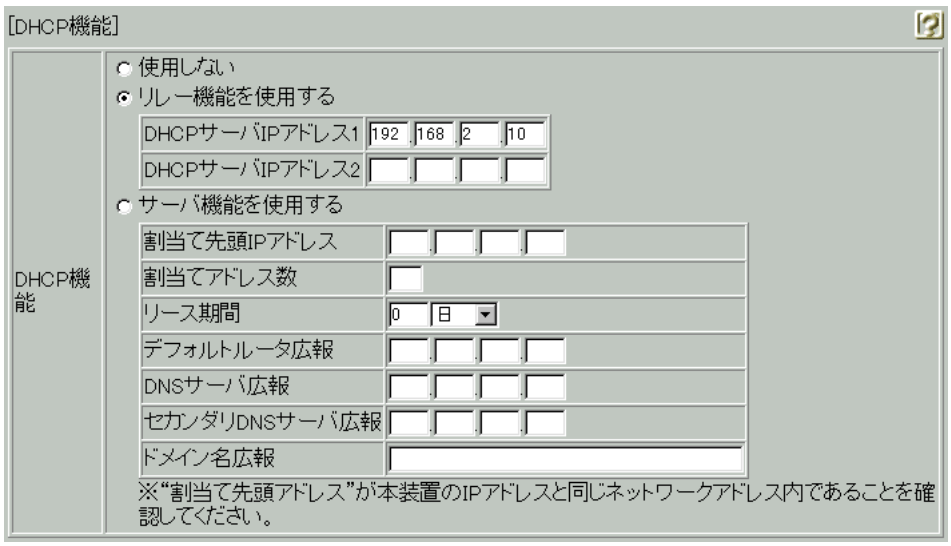
DHCP機能を設定する

1.　詳細設定メニューのルータ設定で「LAN情報」をクリックします。

「LAN情報設定」ページが表示されます。

2.　［DHCP機能］で以下の項目を指定します。

- DHCP機能　→リレー機能を使用する
  DHCPサーバIPアドレス　→192.168.2.10



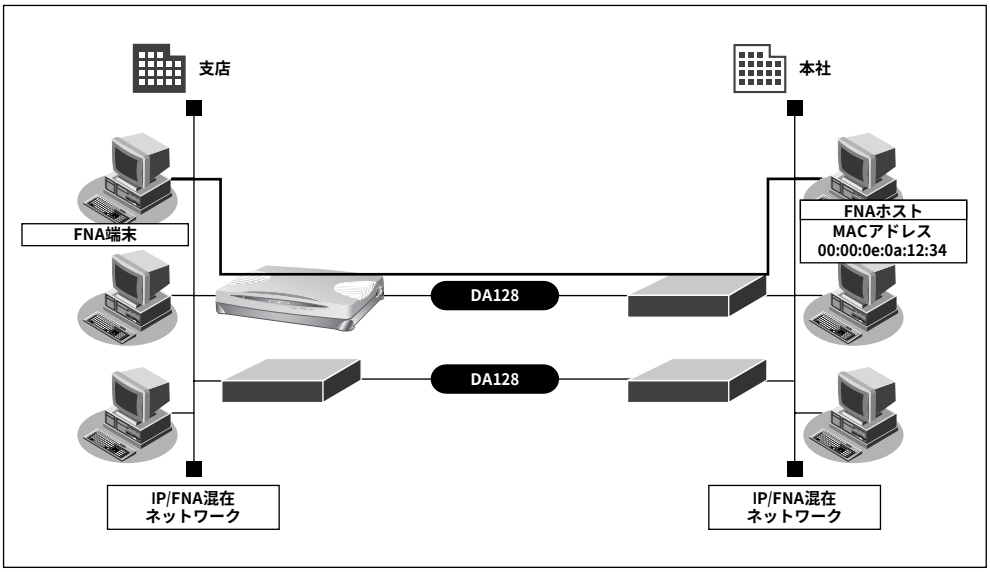
3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

ブリッジ／STP機能を使う

ブリッジ機能を使って離れたLANどうしを1つのサブネットワークとして使用できます。また、STP機能を使うと、物理的にループしているネットワークでも、論理的にループしないようにルーティングすることができます。これによりネットワーク内のデータを円滑に流すことができます。ここでは、専用線をはさんで離れたLAN（FNA）をブリッジでつなぐ場合を例に説明します。



● 設定条件

- 専用線を使用する
- 本社へFNAのデータだけをブリッジする
- STP機能を使用する

こんな事に気をつけて

- **ブリッジ機能を使うと定期的に発呼するため、超過課金が発生します。ISDN回線でSTP機能を使用しないでください。**
- **IPおよびIPv6パケットはブリッジされません。**
- **同一の相手ネットワークとIPv4通信／IPv6通信／ブリッジ通信を同時に行う場合は、それぞれの通信を別々のネットワーク情報として設定しないでください。設定すると正しく通信できません。**
- **ブリッジ機能によりネットワークを接続する場合、ブリッジで通信するパケット以外をフィルタリングする設定にしてください。フィルタリング設定を行わないと、不要なトラフィックが発生するだけでなく、IPなどのネットワークプロトコルに影響し、通信できなくなることがあります。これは、IPv6をサポートしていない相手装置が、IPv6パケットをIPパケットと認識しないため、ブリッジ対象としてブリッジングしてしまい、その結果、不整合が発生して、正しく通信ができなくなるためです。このような場合は、相手装置がブリッジングしないようにIPv6パケットのフィルタリング設定を行う必要があります。**

- **文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。**
  詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

■ 事務所 LAN どうしを専用線で接続する

この例では、すでに本社と支店が専用線接続されていることを前提として説明します。

☛ 参照 「事業所 LAN を専用線で接続する」（P.135）

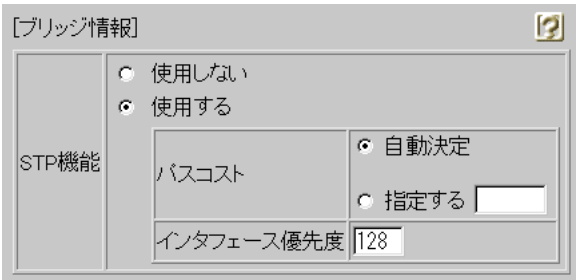
ブリッジ情報を設定する

1.　詳細設定メニューのルータ設定で「LAN 情報」をクリックします。

［LAN 情報設定］ページが表示されます。

2.　「ブリッジ情報」で以下の項目を指定します。

- STP 機能　→使用する



3.　［更新］ボタンをクリックします。

4.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

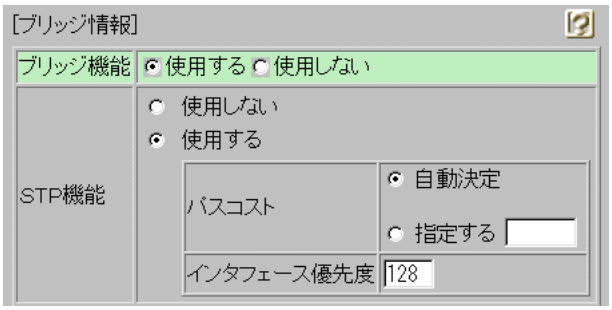
「相手情報設定」ページが表示されます。

5.　［ネットワーク情報一覧］でブリッジ設定を行うネットワーク情報の欄の［修正］ボタンをクリックします。

「ネットワーク情報設定」ページが表示されます。

6.　［ブリッジ情報］で以下の項目を指定します。

- ブリッジ機能　→使用する
- STP機能　→使用する



フィルタリング情報でFNAを透過させる（支店→本社）

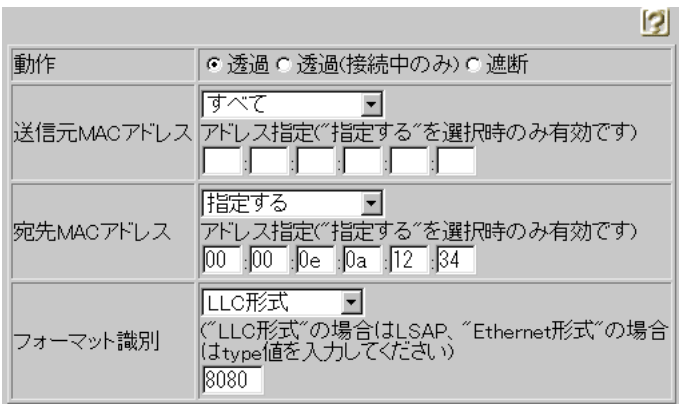
7.　［MACフィルタリング情報］で［追加］ボタンをクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

「MACフィルタリング情報設定」ページが表示されます。

8.　［MACフィルタリング情報設定］で以下の項目を指定します。

- 動作　→透過
- 送信元MACアドレス　→すべて
- 宛先MACアドレス　→指定する
  アドレス指定　→00:00:0e:0a:12:34
- フォーマット識別　→LLC形式
  LSAP　→8080



9.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

フィルタリング情報でFNAを透過させる（本社→支店）

10.　手順7.～9.を参考に、[MACフィルタリング情報設定]で以下の項目を指定します。

- 動作　→透過
- 送信元MACアドレス　→指定する
  アドレス指定　→00:00:0e:0a:12:34
- 宛先MACアドレス　→すべて
- フォーマット識別　→LLC形式
  LSAP　→8080

フィルタリング情報でSTPを透過させる

11.　手順7.～9.を参考に、[MACフィルタリング情報設定]で以下の項目を指定します。

- 動作　→透過
- 送信元MACアドレス　→すべて
- 宛先MACアドレス　→指定する
  アドレス指定　→01:80:c2:00:00:00
- フォーマット識別　→LLC形式
  LSAP　→4242

残りの通信をすべて遮断する

12.　手順7.～9.を参考に、[MACフィルタリング情報設定]で以下の項目を指定します。

- 動作　→遮断
- 送信元MACアドレス　→すべて
- 宛先MACアドレス　→すべて
- フォーマット識別　→すべて

13.　[更新]ボタンをクリックします。

「相手情報設定」ページに戻ります。

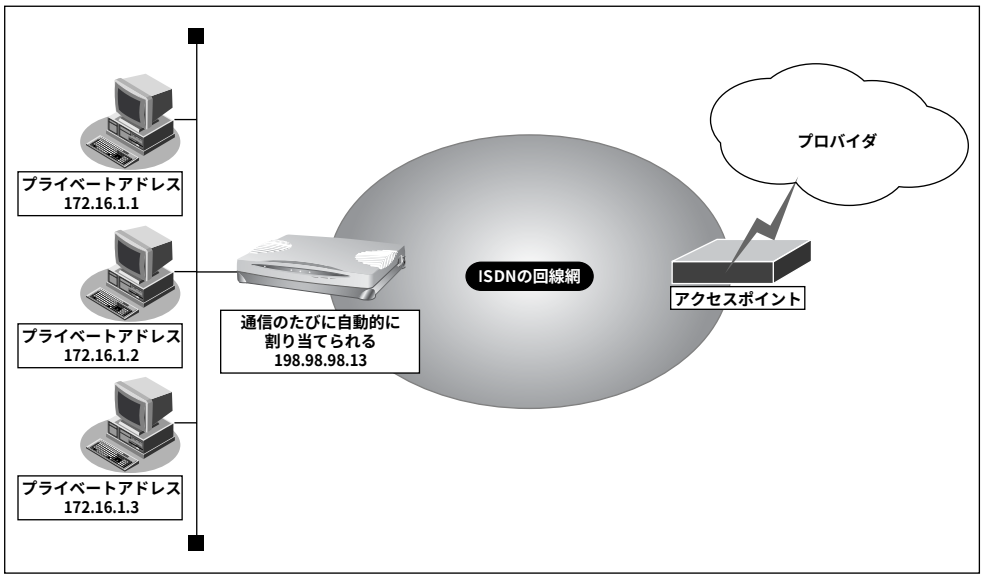
14.　[更新]ボタンをクリックします。

15.　[設定反映]ボタンをクリックします。

設定した内容が有効になります。

マルチNAT機能（アドレス変換機能）を使う

本装置はアドレス変換機能（NAT機能）をサポートしています。NAT機能は、LAN内に接続された複数台のパソコンで使用するプライベートアドレスを、本装置に割り当てたグローバルアドレスに変換する機能です。NAT機能を使用すると、限られた数のグローバルアドレスでそれ以上の数のパソコンを接続できます。たとえば、端末型接続でプロバイダからもらえる1台分のグローバルアドレスを使って、複数台のパソコンからインターネットに接続できます。また、外部からはLAN内に接続されたパソコンのプライベートアドレスがわからないため、不正なアクセスを遮断することができます。



補足
- プライベートアドレスとグローバルアドレスについて
  プライベートアドレスとは、ユーザが自由に割り当てることができるIPアドレスです。
  グローバルアドレスとは、インターネット上のホストを識別するために、InterNICなどのアドレス管理機構から割り当てられる世界で唯一のIPアドレスです。プロバイダ接続の場合はプロバイダからもらえます。
- LANどうしを接続する場合（事業所間など）、両方プライベートアドレスとなることがあります。本装置では便宜上、WAN側のアドレスをグローバルアドレス、LAN側のアドレスをプライベートアドレスと言います。
- 「端末型接続」と「ネットワーク型接続」はインターネットに接続する際のIPアドレスの割り当て方が異なります。
  端末型接続は、アクセスポイントに接続するごとにグローバルアドレスがプロバイダから動的に割り当てられます。
  ネットワーク型接続は、LANを単位として接続する形態で、あらかじめプロバイダからグローバルアドレスが割り当てられます。プロバイダ接続の場合は契約時の申し込み台数に応じてグローバルアドレスが割り当てられます。

NAT機能を使うと、すでにLANを構築している場合も、プライベートアドレスを変更することなくインターネットに接続できるようになります。しかし、同時に接続できる台数は、割り当てられたグローバルアドレスの個数に限られます。これを解決するために、マルチNAT機能があります。マルチNAT機能を使うと、ポート番号を使って、割り当てられたグローバルアドレスの個数以上のパソコンを接続できます。

マルチNAT機能とは、以下の2つの機能で構成されます。

- 動的NAT
- 静的NAT

補足 カタログなどで説明するマルチNAT機能は基本NAT、動的NAT、静的NATの総称です。

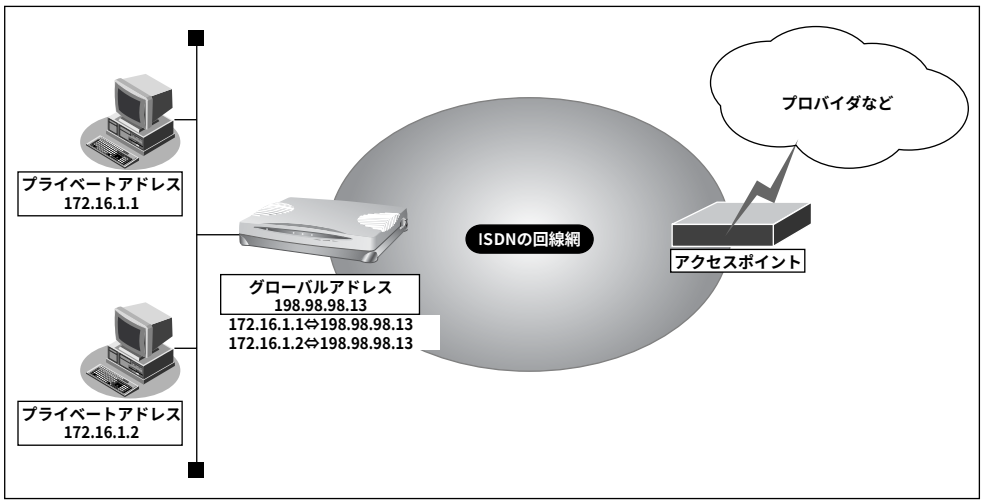
こんな事に気をつけて

IPパケットのフラグメントが発生する環境の場合は、フラグメントされた先頭パケットより前に後続パケットを受信すると、そのフラグメントパケットは破棄され、正常に通信できない場合があります。

ヒント

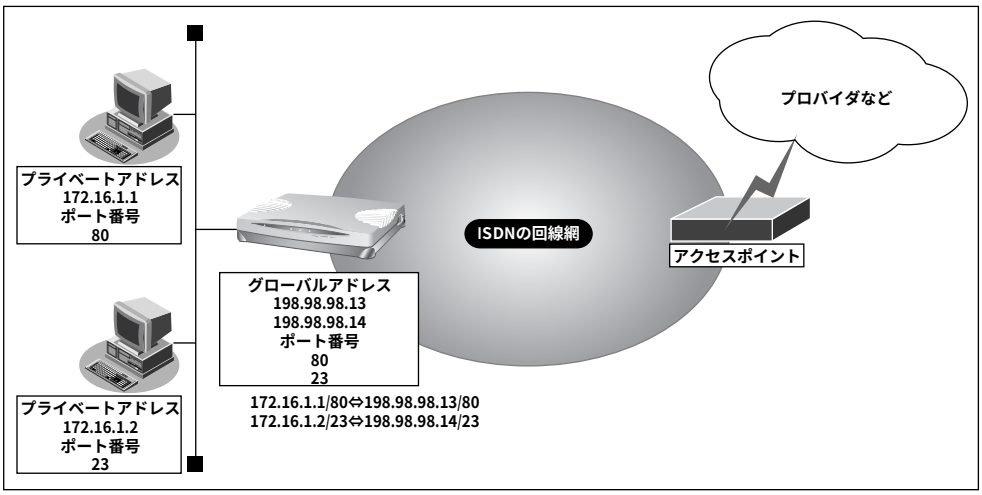
◆ 動的NATとは

基本NATは、プライベートアドレスとグローバルアドレスを1対1に対応付けます。インターネットに同時に接続できるパソコンの台数はプロバイダと契約したグローバルアドレスの個数です。「動的NAT」を使うと、使用可能なグローバルアドレスの個数以上のパソコンが同時に接続できます。



◆静的NATとは

基本NATは、通信発生のたびに空いているグローバルアドレスを割り当てます。そのため、LAN上のWebサーバを公開するような場合には適していません。「静的NAT」を使うと、特定のパソコンやアプリケーションに同じIPアドレス、ポート番号を割り当てるので、この問題を解決できます。



■ NAT機能の選択基準

ネットワーク環境および使用目的によって、適切なNAT機能を設定する必要があります。選択基準を以下に示します。

NAT機能が必要な場合

- 端末型ダイヤルアップ接続する場合
- プロバイダから割り当てられたグローバルアドレスより多くのパソコン（端末）を接続する場合（ここでいう端末には本装置も含まれます）
- 既存のネットワークのアドレスをそのまま使用する場合
- 自側のネットワークのアドレスを隠す場合

●基本NATで十分な場合

- 端末型ダイヤルアップ接続で、同時に接続するパソコン台数が1台の場合
- ネットワーク型接続で、同時に接続するパソコン台数がグローバルアドレス数以下の場合

●動的NATが必要な場合

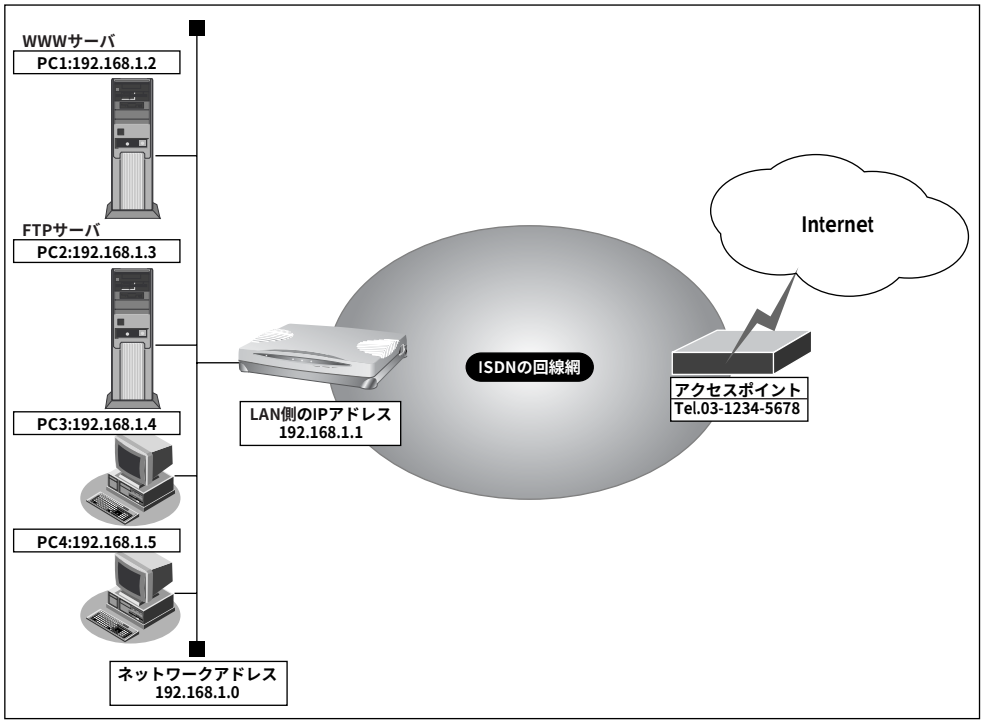
- 端末型ダイヤルアップ接続で、同時に複数のパソコンから接続する場合
- 同時に接続するパソコンの台数がグローバルアドレス数を超える場合

●静的NATが必要な場合

- 外部にサービスを公開する場合（WWWサーバ、FTPサーバなど）
- IPアドレスを意識して動作するアプリケーションを使用する場合

■ ネットワーク型接続でサーバを公開する

ここでは、静的NATを使ってサーバを公開する場合を例に説明します。



● 設定条件

- ISDNに接続する
- ネットワーク型接続を行う
- 既存のLANを使用する
- 割り当てネットワークアドレス　：10.10.10.96/29
- WWW、FTPに割り当てるIPアドレス　：10.10.10.100
- 接続先の電話番号　：03-1234-5678
- ユーザ認証ID　：userid
- ユーザ認証パスワード　：userpass
- ネットワークアドレス／ネットマスク　：192.168.1.0/24
- ブロードキャストアドレス　：192.168.1.255

こんな事に気をつけて

文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。
詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

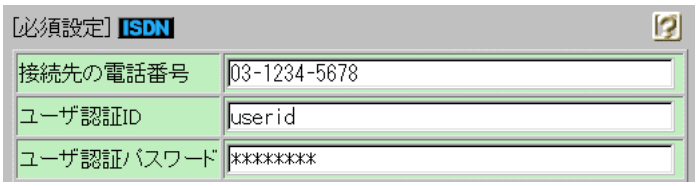
かんたん設定でダイヤルアップ接続の情報を設定する

1.　かんたん設定でインターネットへの「ISDN 接続」をクリックします。

「かんたん設定（インターネットへISDN 接続）」ページが表示されます。

2.　［必須設定］で以下の項目を指定します。

- 接続先の電話番号　→03-1234-5678（プロバイダから提示された内容）
- ユーザ認証 ID　→userid（プロバイダから提示された内容）
- ユーザ認証パスワード　→userpass（プロバイダから提示された内容）



3.　［設定終了］ボタンをクリックします。

再起動後に、通信できる状態になります。

ルータ設定でアドレス変換情報を設定する

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］でかんたん設定で登録したネットワーク情報の欄の［修正］ボタンをクリックします。

「ネットワーク情報設定」ページが表示されます。

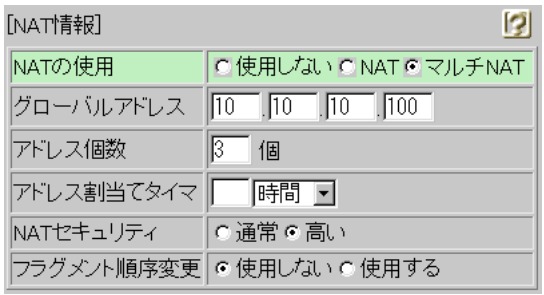
3.　［NAT 情報］で以下の項目を指定します。

- NAT の使用　→マルチ NAT
- グローバルアドレス　→10.10.10.100
- アドレス個数　→3
- NAT セキュリティ　→高い

補足　NAT セキュリティで「高い」を選択した場合、FTP やDNS が要求した相手からの応答かどうかをチェックします。相手サーバがNAT機能を使用している場合など、要求先とは別のアドレスから応答する場合には、「通常」を選択してください。

こんな事に気をつけて

ネットワーク型接続でマルチ NAT 機能を使用する場合は、グローバルアドレスの設定が必須となります。なお、端末型接続では、接続時にグローバルアドレスが割り当てられるため、設定する必要はありません。



4.　［静的 NAT 情報一覧］で［追加］ボタンをクリックします。

「このページの情報は変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

「静的NAT 情報設定」ページが表示されます。

5.　以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→192.168.1.2
  ポート番号　→www,http
- グローバル IP 情報
  IP アドレス　→10.10.10.98
  ポート番号　→www,http

こんな事に気をつけて

動的 NAT と静的 NAT が混在する場合、動的 NAT で使用する IP アドレスと静的 NAT で使用する IP アドレスは重複しないように設定してください。

6.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

7.　上記の手順4.～6.を参考に、以下の情報を指定します。

- プライベートIP情報
  IPアドレス　→192.168.1.3
  ポート番号　→ftp
- グローバルIP情報
  IPアドレス　→10.10.10.99
  ポート番号　→ftp

8.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

9.　［更新］ボタンをクリックします。

10.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

ヒント

◆ 同時に接続できる台数

機能	同時接続台数および セッション数	備考
基本NAT	グローバルIPアドレス数 セッション数制限なし	割り当て時間内は外部からの通信も可能
動的NAT	最大1024セッションまで	外部からの通信は不可能
静的NAT	最大64個まで割り当て可能	プライベートアドレスとポートをグローバルアドレスとポートに割り当てできる 割り当てたアドレスとポートに関しては外部からの通信も可能

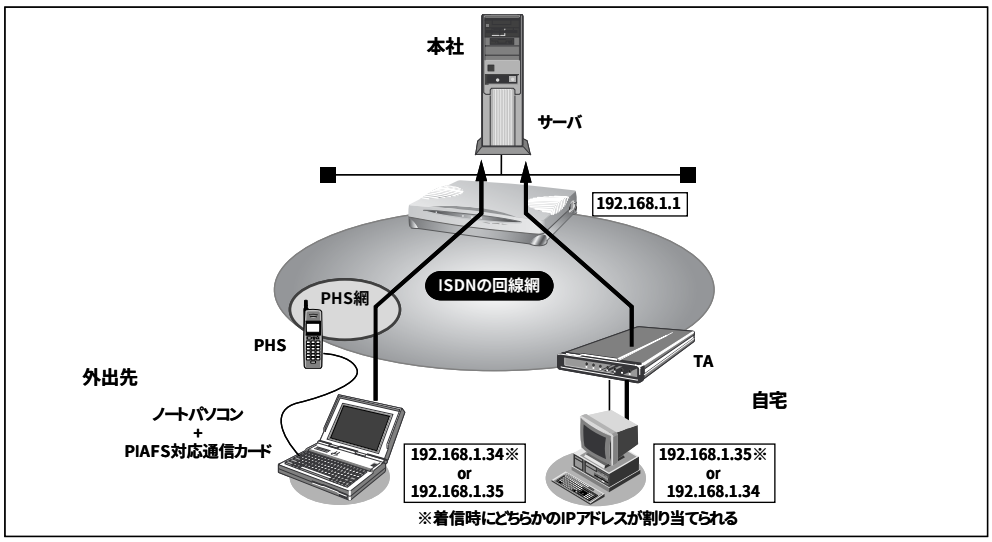
外部のパソコンから着信接続する（アクセスサーバ機能）

ISDN回線経由で外部のパソコンから本装置に着信接続する場合、本装置をリモートアクセスサーバとして使うこともできます。このようなアクセスができる環境は、以下のものが考えられます。

- デスクトップパソコン+TA　→（ISDN）　→本装置
- ノート型パソコン+ISDNカード　→（ISDN）　→本装置
- ノート型パソコン+PIAFS通信カード+PHS　→（PHS網）→（ISDN）→本装置
- 本装置　→（ISDN）　→本装置

☛参照 「外部のパソコンと接続する（TA&PHS）」（P.170）

本社の本装置を設定する場合を例に説明します。LAN情報に関する説明は省略しています。



● 設定条件

＜ノートパソコン＋PHS＞で外出先から接続

- 受諾認証ID　：mobile
- 受諾認証パスワード　：mobilepass
- PHSの電話番号は未登録

＜パソコン＋TA＞で自宅から接続

- 受諾認証ID　：soho
- 受諾認証パスワード　：sohopass
- 自宅の電話番号は未登録

- 本社のLAN側のネットワークアドレス／ネットマスク
  ：192.168.1.0/24
- 外部のパソコンに割り当てるIPアドレス　：192.168.1.34、192.168.1.35

こんな事に気をつけて

文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。
詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

ヒント

◆ 不正なアクセスを防止するには

本装置には公衆電話からもアクセスできます。ただし公衆電話では、アクセスしてきた相手の電話番号を特定できないので、本装置で使っている電話番号などの情報が外部に漏れてしまった場合はどうするのかといった問題が生じます。

その場合、本装置を使ってセキュリティを向上させる方法として、以下のようなものがあります。

・認証情報（受諾認証IDやパスワードなど）を設定する

・コールバック機能を使う

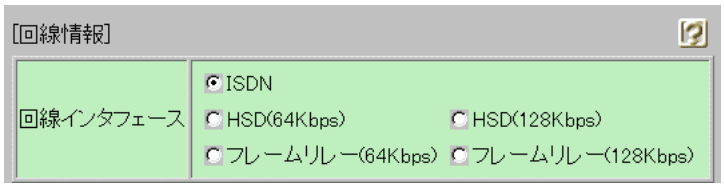
回線情報を設定する

1.　詳細設定メニューのルータ設定で「回線情報」をクリックします。

「回線情報設定」ページが表示されます。

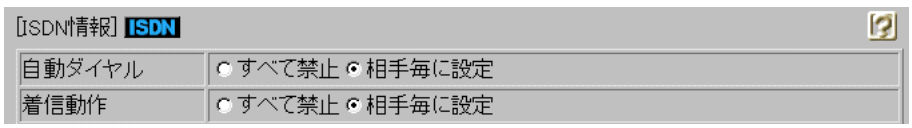
2.　［回線情報］で以下の項目を指定します。

- 回線インタフェース　→ISDN



［ISDN情報］で以下の項目を指定します。

- 着信動作　→相手毎に設定



必要に応じて上記以外の項目を指定します。

3.　［更新］ボタンをクリックします。

不特定な相手と着信接続するために必要な情報を設定する

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］の「不特定相手着信」の欄の［修正］ボタンをクリックします。

「不特定相手情報設定」ページが表示されます。

3.　［基本情報］で以下の項目を指定します。

- 割当先頭アドレス　→192.168.1.34
- 同時接続許可数　→2

必要に応じて上記以外の項目を指定します。

4.　［更新］ボタンをクリックします。

着信相手を識別するために必要な情報を設定する

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［着信相手識別情報］で以下の項目を指定します。

- 着信許可　→する
- 認証方式　→「PAP」および「CHAP」
- MP接続　→しない
- コールバック応答　→しない

必要に応じて上記以外の項目を指定します。

3.　［更新］ボタンをクリックします。

受諾認証情報を設定する

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［受諾認証ID情報一覧］で［追加］ボタンをクリックします。

「PPP受諾認証情報」ページが表示されます。

3.　［受諾認証情報］で以下の項目を指定します。

- 受諾認証ID　→mobile
- 受諾認証パスワード　→mobilepass

4.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

5.　手順2.～4.を参考に、＜パソコン＋TA＞の項目を指定します。

- 受諾認証ID　→soho
- 受諾認証パスワード　→sohopass

6.　［更新］ボタンをクリックします。

7.　［設定反映］ボタンをクリックします。

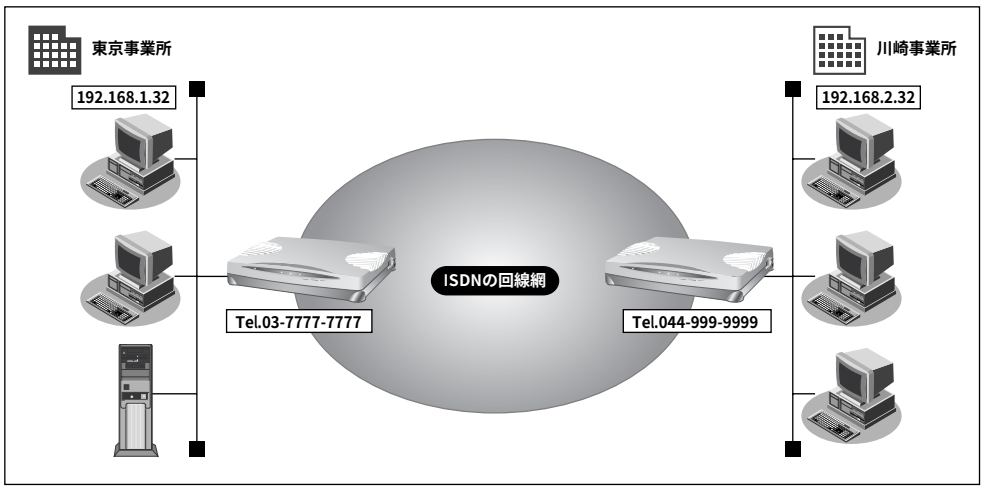
設定した内容が有効になります。

認証IDによる接続相手の識別

本装置は着信時の相手識別を発信者番号通知によって行います。
しかし、発信者番号から相手を特定できないことがあります。このような相手と通信する場合、PPPの認証プロトコルを使用して、認証IDによる接続相手の識別する必要があります。
認証IDによる相手識別は以下の場合に必要となります。

- 着信時に発信者番号が通知されない場合
- 同一相手からの着信時の発信者番号が毎回異なる場合

ここでは、東京事業所の本装置の設定で、設定済みの接続先情報（川崎事業所）に認証IDで特定するための情報を追加する場合を例に説明します。ISDN回線を介して2つの事業所（東京、川崎）のネットワークを接続します。
一方の事業所でサーバを公開していて、着信接続します。



● 設定条件

- 認証IDと認証パスワード（川崎事業所用）
  受諾認証　　：kawasaki
  受諾認証パスワード　　：kawapass
- 東京事業所でサーバを公開している
- 川崎事業所では電話番号を通知しない設定をしている

電話番号から特定できない相手との着信処理

- 認証方式PAP／CHAP
- MP接続しない
- コールバック応答しない

参照する情報

[東京事業所]

- 川崎事業所のネットワークの名前　：kaisya
- 接続先の名前　　：kawasaki

☛ 参照 「事業所LANをISDNで接続する」（P.115）

こんな事に気をつけて

文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。
詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

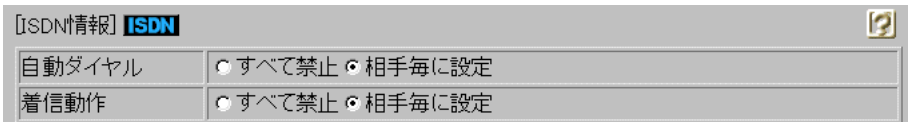
回線情報（東京事業所）を設定する

1.　詳細設定メニューのルータ設定で「回線情報」をクリックします。

「回線情報設定」ページが表示されます。

2.　[ISDN 情報] で以下の項目を指定します。

- 着信動作　→相手毎に設定



必要に応じて上記以外の項目を指定します。

3.　[更新] ボタンをクリックします。

着信相手を識別するために必要な情報を設定する

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　[着信相手識別情報] で以下の項目を指定します。

- 着信許可　→する
- 認証方式　→「PAP」および「CHAP」
- MP接続　→しない
- コールバック応答　→しない

必要に応じて上記以外の項目を指定します。

3.　［更新］ボタンをクリックします。

接続先の情報（川崎事業所）を設定する

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］で「kaisya」欄の［修正］ボタンをクリックします。

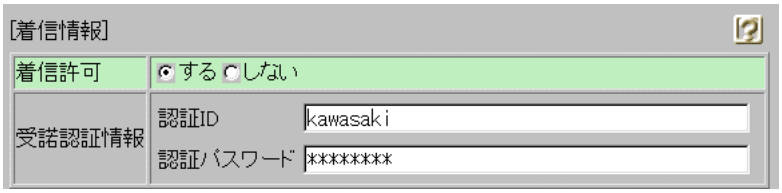
「ネットワーク情報設定」ページが表示されます。

3.　［接続先情報一覧］で「kawasaki」欄の［修正］ボタンをクリックします。

「接続先情報設定」ページが表示されます。

4.　［着信情報］で以下の項目を指定します。

- 着信許可　→する
- 受諾認証情報
  認証ID　→kawasaki
  認証パスワード　→kawapass



［発信者番号識別による着信情報］で以下の項目を指定します。

- 発信者番号による識別　→番号チェックをしない

必要に応じて上記以外の項目を指定します。

5.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

6.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

7.　［更新］ボタンをクリックします。

8.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

RADIUSクライアント機能を使う

本装置はRADIUS（Remote Authentication Dial In User Service）クライアント機能をサポートしています。

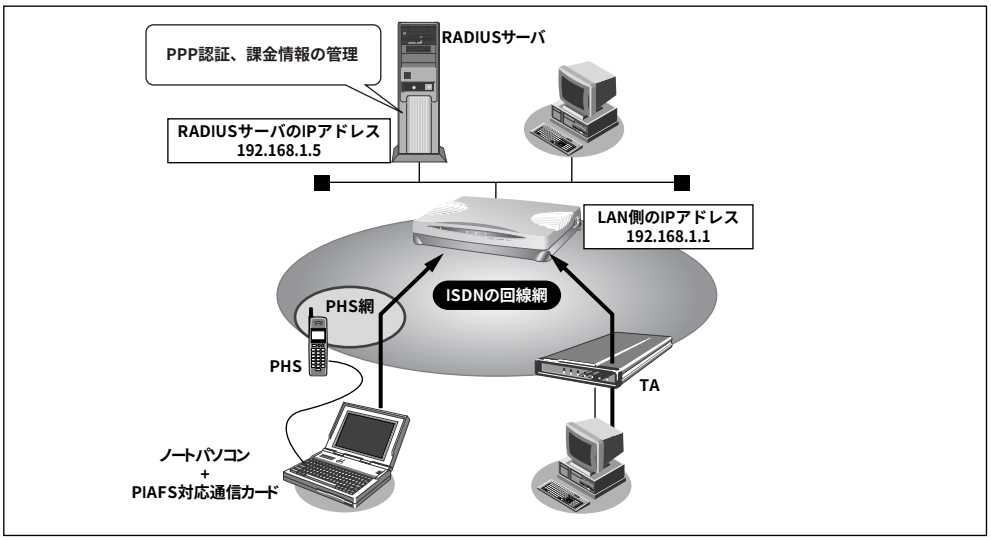
外部のパソコンからの着信要求に対して、RADIUSクライアント機能を使って、RADIUSサーバでユーザ認証を行うことができます。

RADIUSサーバを利用すると、以下のメリットがあります。

- 複数の本装置のユーザ認証や課金情報を一元管理できます。
- 本装置が持つユーザ認証の制限を超えるアクセスが可能です。

こんな事に気をつけて

RADIUS クライアント機能は、本装置を相手情報設定で設定した相手以外からの着信だけ使用できます。



● 設定条件

- 認証サービスを使用する
- 認証サーバIPアドレス　　：192.168.1.5

前述の「外部のパソコンから着信接続する（アクセスサーバ機能）」では、本装置のユーザ認証機能を使用するのに対し、ここでは、RADIUSのユーザ認証機能を使用します。どちらもセキュリティを確保することを目的とした設定例です。

この例では、「外部のパソコンから着信接続する（アクセスサーバ機能）」で説明した「回線情報を設定する」「不特定な相手と着信接続するために必要な情報を設定する」「着信相手を識別するために必要な情報を設定する」までの操作手順が同じなので、説明を省略しています。必要に応じて参照してください。

☛ 参照　設定手順→「外部のパソコンから着信接続する （アクセスサーバ機能）」（P.497）

こんな事に気をつけて

文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。
詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

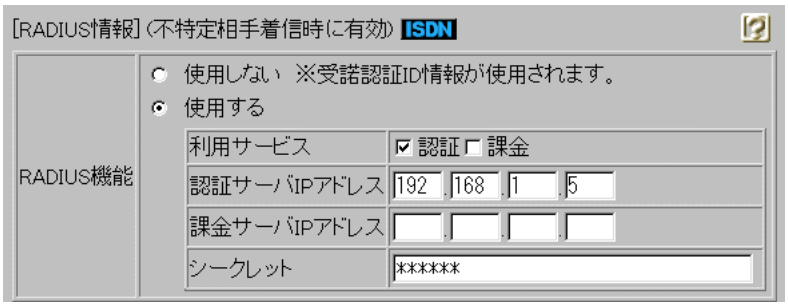
RADIUS情報を設定する

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［RADIUS情報］で以下の項目を指定します。

- RADIUS機能　→使用する
  利用サービス　→認証
  認証サーバIPアドレス　→192.168.1.5
  シークレット　→himitu



必要に応じて上記以外の項目を指定します。

3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

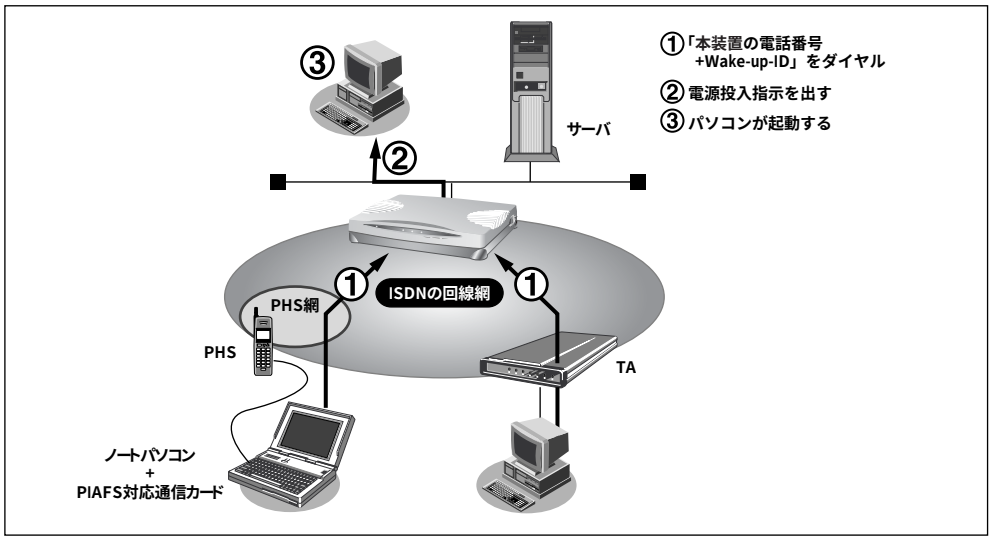
設定した内容が有効になります。

外出先や自宅から会社のパソコンを起動させる（リモートパワーオン機能）

本装置のリモートパワーオン機能は、Wakeup on LAN機能を使用して、電源OFF状態のパソコンを外出先や自宅のサブアドレスを使用できる電話機（PHSを含む）から起動させることができます。

こんな事に気をつけて

サブアドレスを指定できないアナログ電話からは、この機能を使用できません。



ヒント

◆ Wakeup on LAN機能とは？

AMD社が開発したネットワーク上の電源OFF状態のパソコンを遠隔操作で起動する機能です。起動はMagic Packetと呼ばれるパケットを送付して行います。なお、Wakeup on LAN機能はパソコンを起動するだけで電源OFFは行いません。
電源OFFする場合は、別途、電源制御用ソフトウェアが必要になります。

補足

- 本機能は、Wakeup on LANに対応したパソコンだけで使用できます。Wakeup on LAN対応機種については、パソコンのメーカーにお問い合わせください。
- 本機能は、サブアドレスを指定できるISDN機器（電話、PHSなど）で使用できます。
- 本機能を使用するだけでは、課金されません。

こんな事に気をつけて

文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。
詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

起動条件を設定する

1.　詳細設定メニューのルータ設定で「ホストデータベース情報」をクリックします。

「ホストデータベース情報」ページが表示されます。

2.　未設定の欄の［修正］ボタンをクリックします。

「ホストデータベース情報設定」ページが表示されます。

3.　以下の項目を指定します。

- MACアドレス　→00:00:0e:22:01:23（起動させるパソコンのMACアドレス）
- Wake-up-ID　→5678（起動させるためのキー番号（任意の英数字で19文字まで））

こんな事に気をつけて

「Wake-up-ID」と実際に存在するISDN機器のサブアドレスが重複しないようにしてください。

補足
- この「Wake-up-ID」による依頼を受けた本装置は、同じ「Wake-up-ID」を持つ、すべてのパソコンにMagic Packetを送信し、電源投入指示を行います。
- 複数のパソコンに同じ「Wake-up-ID」を設定すると、一回のリモートパワーオン依頼で複数のパソコンを起動することができます。
- ホストデータベース情報は「リモートパワーオン機能」、「DHCPスタティック機能」、「DNSサーバ機能」で使われており、それぞれ必要な項目だけを指定します。

☛ 参照　MACアドレス→「本装置 底面」（P.33）

4.　［更新］ボタンをクリックします。

「ホストデータベース情報」ページに戻ります。

5.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

リモートパワーオン機能を使う

1.　パソコンまたは電話機で、本装置の電話番号（ISDN 契約者番号）を入力します。

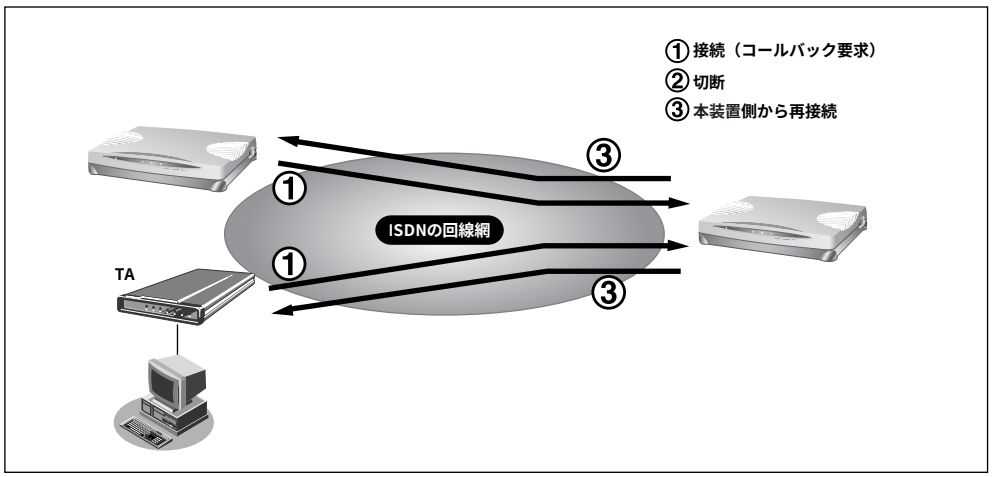
2.　相手先サブアドレスに、起動させるパソコンの「Wake-up-ID」を指定します。

本装置が該当するパソコンに対して「Magic Packet」を送信し、パソコンが起動します。

補足　パソコンが Magic Packetを受信してから起動が完了するまで、数十秒から数分かかります（お使いの機種や OSによって異なります）。

コールバック機能を利用する

本装置はコールバック機能をサポートしています。コールバック先をあらかじめ登録しておきます。登録済みの相手からアクセス要求があった場合は、まず認証を行い、いったん回線を切断したあとに、本装置から電話をかけ直します。
自宅や出張先などの遠隔地から事業所のサーバにアクセスする際、通信料金を事業所持ちにする場合にコールバック機能が便利です。また、本装置側で通信料金を一括管理できます。
コールバック機能を使うと、不特定多数の人間によるアクセスを防止することもできます。



本装置には、以下の2種類のコールバック機能があります。

- **CBCP方式を使用する**

  Windows® 95／98／2000／Me、Windows NT® 4.0のダイヤルアップ機能に対応しています。着信要求があった場合、いったんISDN回線を接続して、IDおよびパスワードの入力による認証を行います。認証が終わると本装置は回線を切断し、ダイヤル発信をやり直します。この方式では、認証が終わるまでの通信料金がかかります。

- **無課金コールバックを使用する**

  本装置どうしの場合だけ使用できます。ISDNのDチャネルを使って「発信者番号」による認証を行います。このとき回線は接続されません。認証が終わると、本装置はダイヤル発信をやり直します。ここではじめて回線が接続されます。この方式では、発信側に通信料金がかかりません。

こんな事に気をつけて

無課金コールバックは、公衆電話では利用できません。また、NTTの「発信者番号通知サービス」の契約が必要です。

補足
- Microsoft®製品やCBCP方式をサポートしている装置とコールバックを行う場合、「CBCP」を選択してください。本装置どうしでコールバックを行う場合、「無課金」も選択できます。
- コールバック応答時は、コールバック要求時に相手先より通知された通信速度で応答します。つまり、64Kbpsで要求があった場合には64Kbpsで、32Kbpsで要求があった場合には32Kbpsで応答します。

コールバック機能を使用した設定例を、以下に説明します。

(1)CBCP方式でコールバック要求する

(2)CBCP方式でコールバック応答する

(3)無課金コールバックでコールバック要求する

(4)無課金コールバックでコールバック応答する

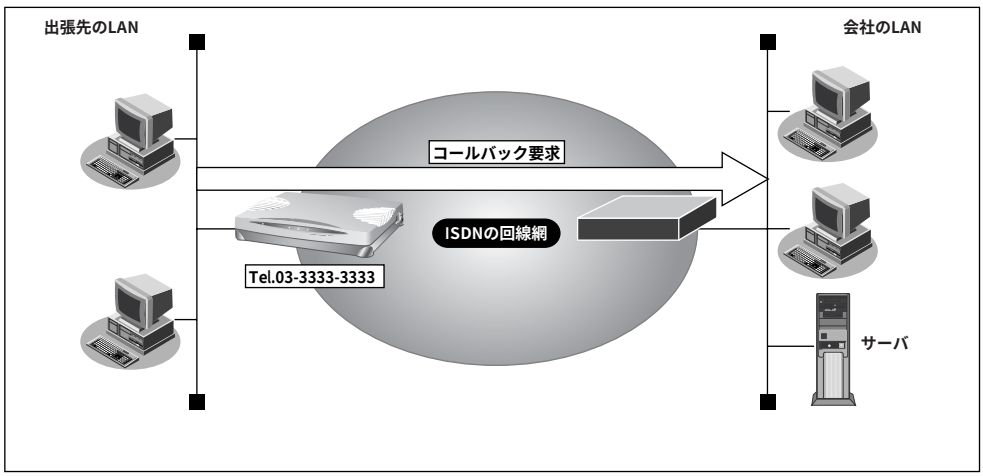
ここでは、設定済みの接続先にコールバックを追加する場合を例に説明します。

こんな事に気をつけて

文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。
詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

■ CBCP方式でコールバック要求する

出張先のパソコンから会社のサーバにアクセスする際、コールバック要求を発行する場合を例に説明します。



● 設定条件

- コールバックはCBCP方式を指定
- コールバック時の電話番号　　：03-3333-3333
- コールバックウェイトタイマ　　：60秒

参照する情報

- 会社のネットワークの名前　　：kaisya
- 接続先の名前　　：office

☛ 参照　接続先情報の設定→「インターネットとLANに同時接続する」（P.165）

コールバックを要求する接続先の情報を設定する

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］で「kaisya」欄の［修正］ボタンをクリックします。

「ネットワーク情報設定」ページが表示されます。

3.　［接続先情報一覧］で「office」欄の［修正］ボタンをクリックします。

「接続先情報設定」ページが表示されます。

4.　［発信情報］で以下の項目を指定します。

- コールバック要求　　→する
  コールバック方式　　→CBCP
  コールバックウェイトタイマ　　→60秒
  コールバック電話番号　　→03-3333-3333

補足
- 「コールバック電話番号」および「コールバックサブアドレス」で設定した番号は、コールバック元に対して通知するかけ直し電話番号およびサブアドレスを設定します。
- 「コールバックウェイトタイマ」とはコールバック要求発行後、相手からのコールバック着信までの待ち時間です。この時間内に着信が行われない場合、コールバックは失敗となります。（推奨値:60秒）
  コールバックがうまく動作しないときは、この時間を長くしてみてください。

5.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

6.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

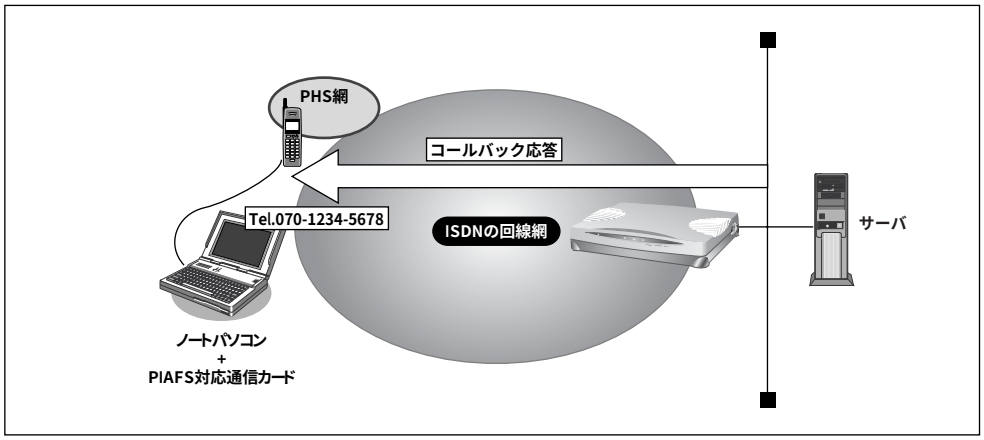
7.　［更新］ボタンをクリックします。

8.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

■ CBCP方式でコールバック応答する

＜ノートパソコン＋PHS＞で出張先から会社のサーバにアクセスする際、コールバック応答する場合の例を説明します。



● 設定条件

- ノートパソコン＋PHSで出張先からアクセスする
- コールバックはCBCP方式を指定
- コールバックウェイトタイマ　　：10秒

参照する情報

- 出張時のネットワークの名前　　：outside
- 接続先の名前　　：PHS

☛参照　接続先情報の設定→「外部のパソコンと接続する（TA&PHS）」（P.170）

コールバック応答する接続先の情報を設定する

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］でネットワーク名「outside」欄の［修正］ボタンをクリックします。

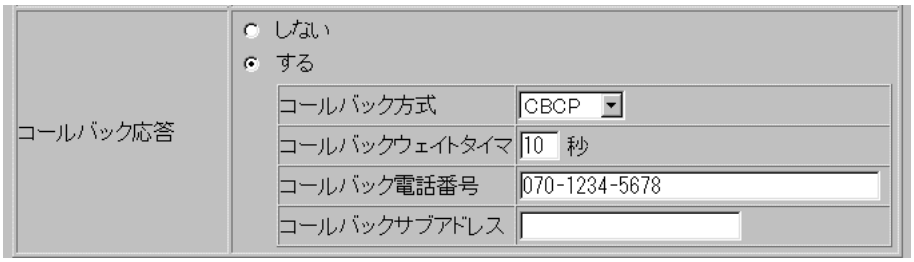
「ネットワーク情報設定」ページが表示されます。

3.　［接続先情報一覧］で「PHS」欄の［修正］ボタンをクリックします。

「接続先情報設定」ページが表示されます。

4.　［発信者番号識別による着信情報］で以下の項目を指定します。

- コールバック応答　→する
  コールバック方式　→CBCP
  コールバックウェイトタイマ　→10秒
  コールバック電話番号　→070-1234-5678



補足
- 着信情報で「コールバック電話番号」および「コールバックサブアドレス」を設定した場合、コールバック時には、着信時に相手から通知される電話番号とサブアドレスではなく、ここに設定された番号を優先して使用します。
- 「コールバックウェイトタイマ」とはコールバック要求を受け取ってからかけ直すまでの待ち時間です。回線が切断されても交換機でしばらくは回線空き状態に戻らないため、それを待ち合わせるために使用します（推奨値:10秒）。
  コールバックがうまく動作しないときは、この時間を長くしてください。

5.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

6.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

7.　［更新］ボタンをクリックします。

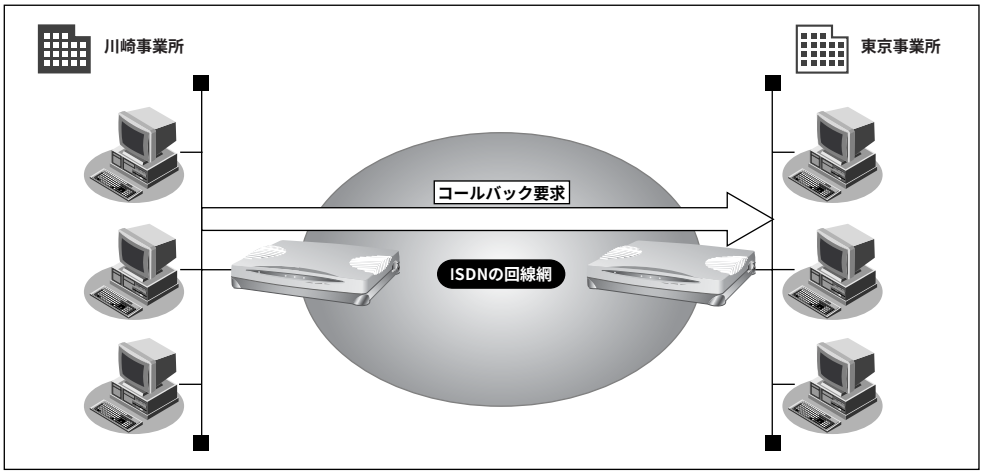
8.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

補足 上記のように出張先からの着信接続を行うための設定方法として「外部のパソコンから着信接続する （アクセスサーバ機能）」（P.497）があります。その設定方法でも、コールバック応答を指定することができます。

■ 無課金コールバックでコールバック要求する

本装置どうしを使って、ISDN回線を介して2つの事業所（東京、川崎）のネットワークを接続した場合を例に説明します。川崎事業所から東京事業所に接続する際、コールバック要求をする情報を追加します。



● 設定条件

- コールバックは無課金方式を使用
- コールバックウェイトタイマ　　：60秒

参照する情報

[川崎事業所]

- 東京事業所のネットワークの名前　：kaisya
- 接続先の名前　　：tokyo

☛ 参照　接続先情報の設定→「事業所LANをISDNで接続する」（P.115）

コールバック要求する接続先の情報を設定する（川崎事業所）

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　[ネットワーク情報一覧] でネットワーク名「kaisya」欄の [修正] ボタンをクリックします。

「ネットワーク情報設定」ページが表示されます。

3.　[接続先情報一覧] で「tokyo」欄の [修正] ボタンをクリックします。

「接続先情報設定」ページが表示されます。

4.　［発信情報］で以下の項目を指定します。

- コールバック要求　→する
  コールバック方式　→無課金
  コールバックウェイトタイマ　→60秒

補足　無課金コールバックでは［発信情報］で「コールバック電話番号」および「コールバックサブアドレス」を設定しても、これらの番号は相手に通知されません。

5.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

6.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

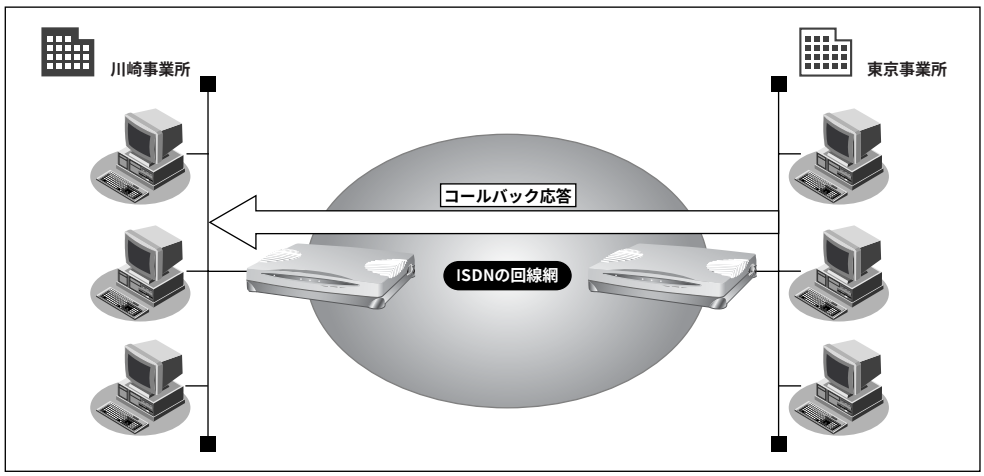
7.　［更新］ボタンをクリックします。

8.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

■ 無課金コールバックでコールバック応答する

本装置どうしを使って、ISDN回線を介して2つの事業所（東京、川崎）のネットワークを接続した場合を例に説明します。川崎事業所から東京事業所に接続する際、東京事業所からコールバック応答をする情報を追加します。



● 設定条件

- コールバックは無課金方式を使用
- コールバックウェイトタイマ　：10秒

参照する情報

[東京事業所]

- 川崎事業所のネットワークの名前　：kaisya
- 接続先の名前　：kawasaki

☛ 参照　接続先情報の設定→「事業所LANをISDNで接続する」（P.115）

コールバック応答する接続先の情報を設定する（東京事業所）

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　[ネットワーク情報一覧] で「kaisya」欄の [修正] ボタンをクリックします。

「ネットワーク情報設定」ページが表示されます。

3.　[接続先情報一覧] で「kawasaki」欄の [修正] ボタンをクリックします。

「接続先情報設定」ページが表示されます。

4.　[発信者番号識別による着信情報] で以下の項目を指定します。

- コールバック応答　→する
  コールバック方式　→無課金
  コールバックウェイトタイマ　→10秒

5.　[更新] ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

6.　[更新] ボタンをクリックします。

「相手情報設定」ページに戻ります。

7.　[更新] ボタンをクリックします。

8.　[設定反映] ボタンをクリックします。

設定した内容が有効になります。

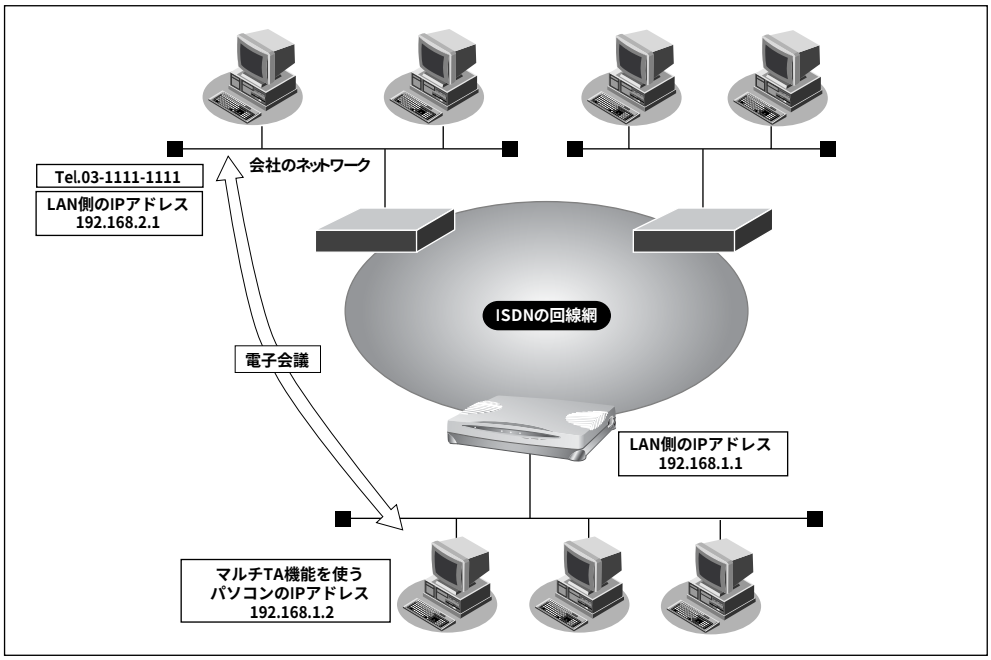
マルチTA機能を使う

本装置はマルチTA機能をサポートしています。マルチTA機能を使用すると、LAN上につながれたパソコンから本装置を擬似的なTAとして共有できます。マルチTA機能とルータ機能を同時に使用することもできます。パソコンから、NATを使用しないで通信が行えるので、NATを使用すると通信できないアプリケーション（たとえば、電子会議やインターネットゲームなど）を使用する際に便利です。

こんな事に気をつけて

- **マルチTA機能は、Windows® 95／98／Me／2000／XPのダイヤルアップネットワークに含まれるVPNの機能を利用して、装置にRS232C接続されたTAからの発信と同等のPPPセッションの確立を行うことができます。**
- **マルチTA機能は、Windows Vista®では使用できません。**
- **マルチTA機能を使用する場合、着信、コールバック、MP、課金制御機能、スケジュール機能の動作は行えません。**
- **マルチTA機能の使用中は、かんたん操作の「強制切断」は使用できません。**
- **パソコン側の設定でDNSサーバが指定されていて、ルータ設定で「相手情報」の「自動ダイヤル」に「する」が設定されている場合にマルチTA機能を使用すると、2回線（Bチャネル1本をルータ機能、もう1本をマルチTA機能）接続されるため超過課金の原因になることがあります。また、アナログ機器で先に回線を1本使用している場合、マルチTA機能を使用できない場合があります。**

ここでは、マルチTA機能を使用して、ある特定のパソコンで電子会議を行う場合を例に説明します。



● 設定条件

- ISDNに接続する
- 端末型ダイヤルアップ接続を行う
- 電子会議をするパソコンのIPアドレス　：192.168.1.2
- 会社のルータが接続されている電話番号　：03-1111-1111
- 会社のルータのIPアドレス　：192.168.2.1
- 5時間経過した場合回線を強制切断する
- ユーザ認証ID（会社）　：user1
- ユーザ認証パスワード（会社）　：userpass

こんな事に気をつけて

文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。
詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

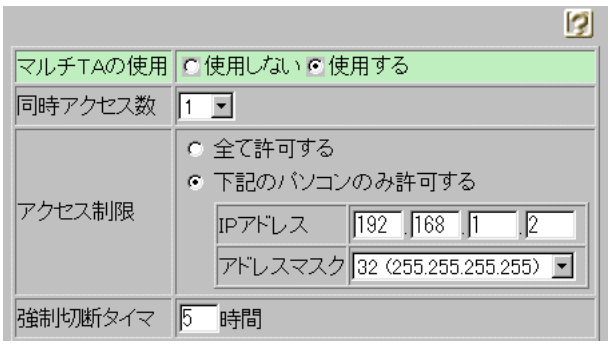
マルチTA情報を設定する

1.　詳細設定メニューのルータ設定で「マルチTA情報」をクリックします。

「マルチTA情報」ページが表示されます。

2.　以下の項目を指定します。

- マルチTAの使用　→使用する
- 同時アクセス数　→1
- アクセス制限　→下記のパソコンのみ許可する
  IPアドレス　→192.168.1.2
  アドレスマスク　→32
- 強制切断タイマ　→5



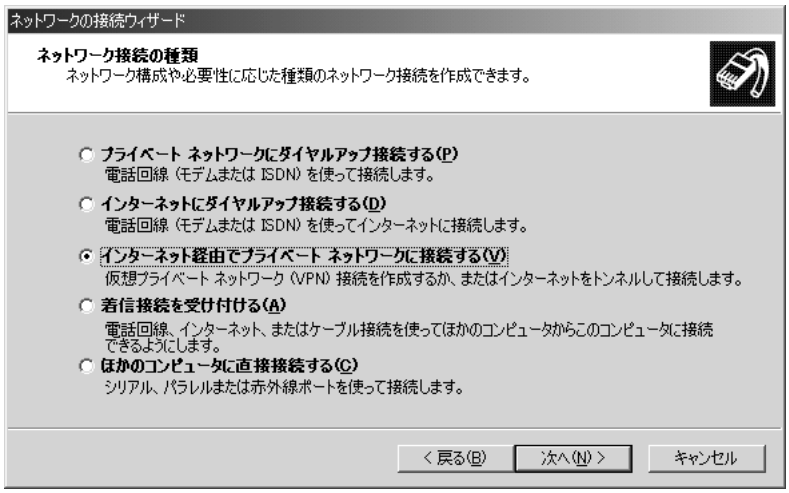
3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

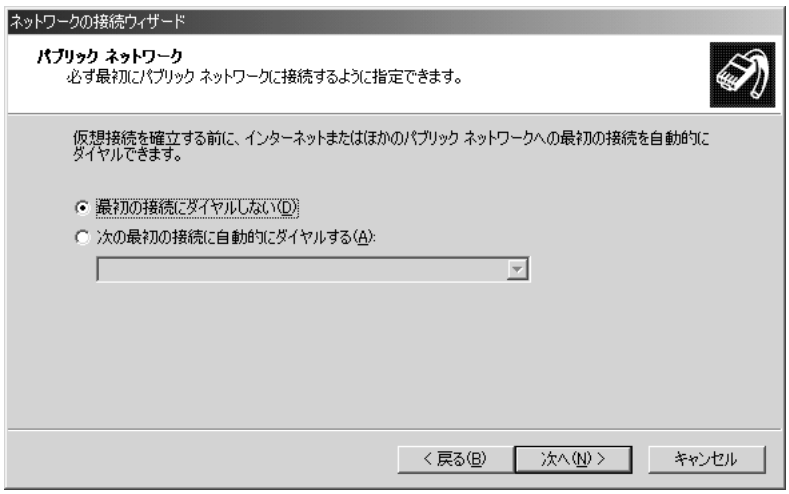
設定した内容が有効になります。

ダイヤルアップネットワークの設定をする（Windows® 2000の場合）

1. 「コントロールパネル」ウィンドウを開き、「ネットワークとダイヤルアップ」アイコンをダブルクリックします。
2. 「ネットワークとダイヤルアップ接続」の「新しい接続」をダブルクリックします。
3. ［次へ］ボタンをクリックします。
4. 「ネットワーク接続の種類」で「インターネット経由でプライベートネットワークに接続する」を選択し、［次へ］ボタンをクリックします。



5. 「パブリックネットワーク」で「最初の接続にダイヤルしない」のラジオボタンがチェックされていることを確認します。「パブリックネットワーク」設定画面が表示されない場合、手順7. に進みます。



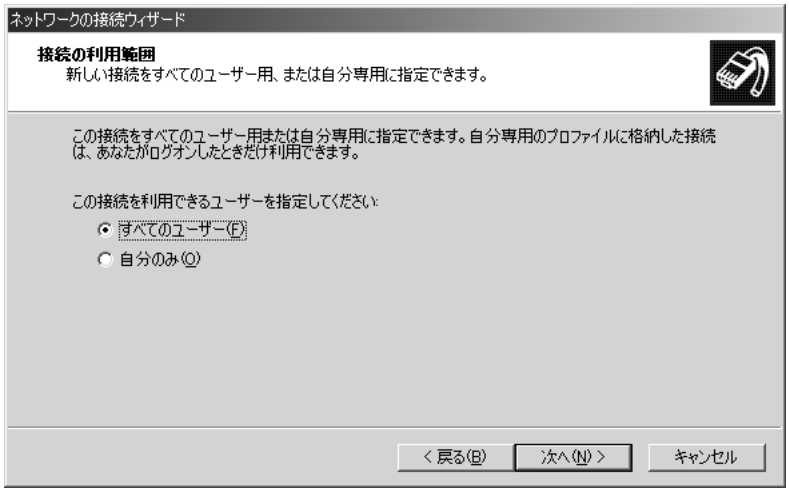
6. ［次へ］ボタンをクリックします。

7.　「接続先のアドレス」で以下の項目を指定します。

- ホスト名またはIPアドレス　→192.168.1.1 03-1111-1111（IPアドレスと電話番号の間に半角空白を入れます）

8.　[次へ] ボタンをクリックします。

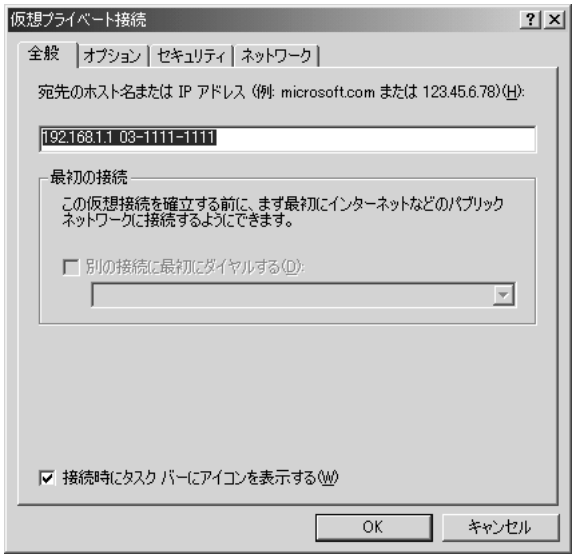
9.　「接続の利用範囲」で「すべてのユーザ」のラジオボタンがチェックされていることを確認します。



10.　[次へ] ボタンをクリックします。

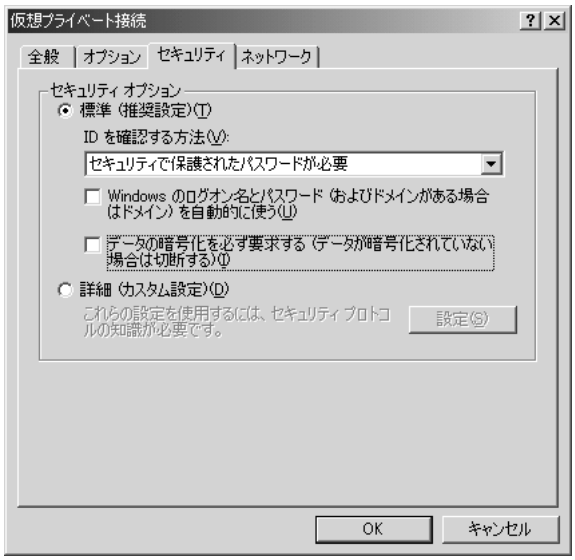
11.　[完了] ボタンをクリックします。

12. 接続画面が表示されたら、「プロパティ」を選択します。



13. 「セキュリティ」タブをクリックします。

14. 「セキュリティオプション」で「データの暗号化を必ず要求する（データが暗号化されていない場合は切断する)」のチェックボックスのチェックを外します。

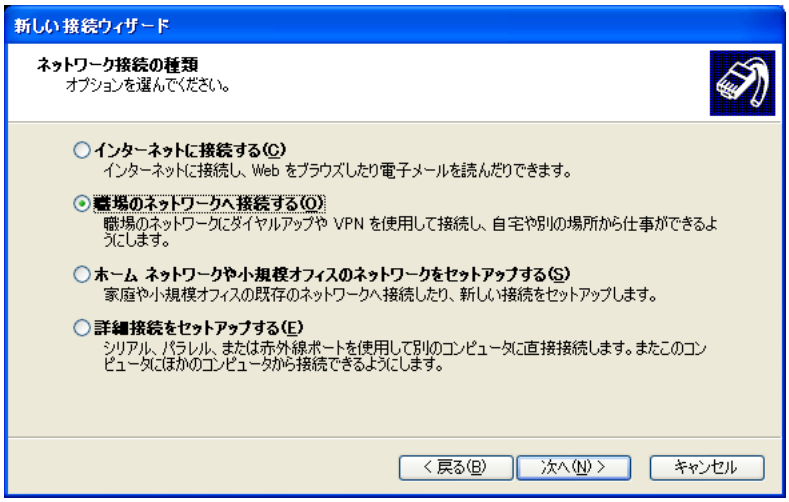


15. [OK] ボタンをクリックします。

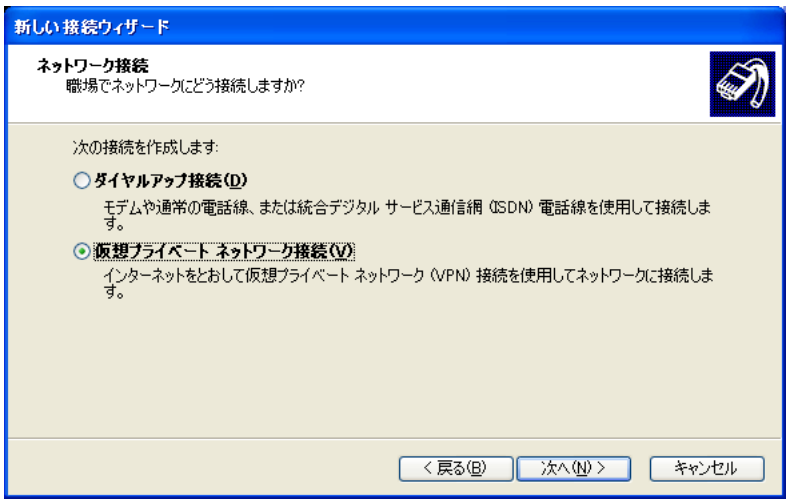
16. [キャンセル] ボタンをクリックして設定を終了します。

ダイヤルアップネットワークの設定をする（Windows® XPの場合）

1. 「コントロールパネル」ウィンドウを開き、「ネットワーク接続」アイコンをダブルクリックします。
2. 「ネットワーク タスク」の「新しい接続を作成する」をクリックします。
3. ［次へ］ボタンをクリックします。
4. 「ネットワーク接続の種類」で「職場のネットワークへ接続する」を選択し、［次へ］ボタンをクリックします。

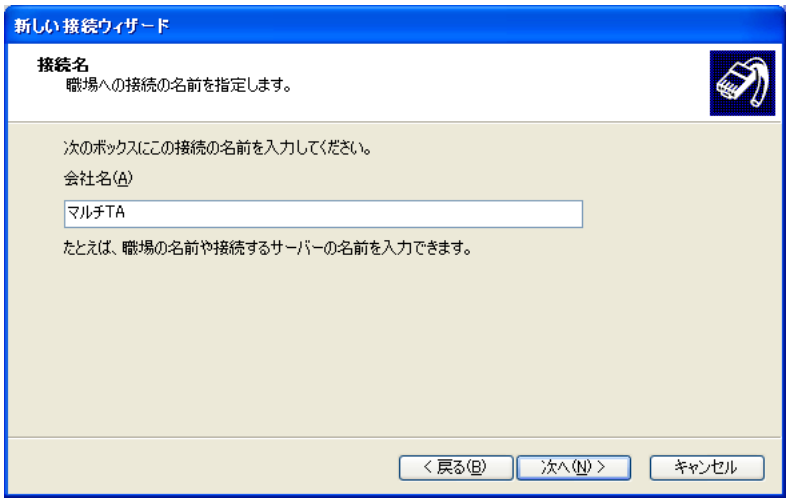


5. 「ネットワーク接続」で「仮想プライベート ネットワーク接続」を選択し、［次へ］ボタンをクリックします。



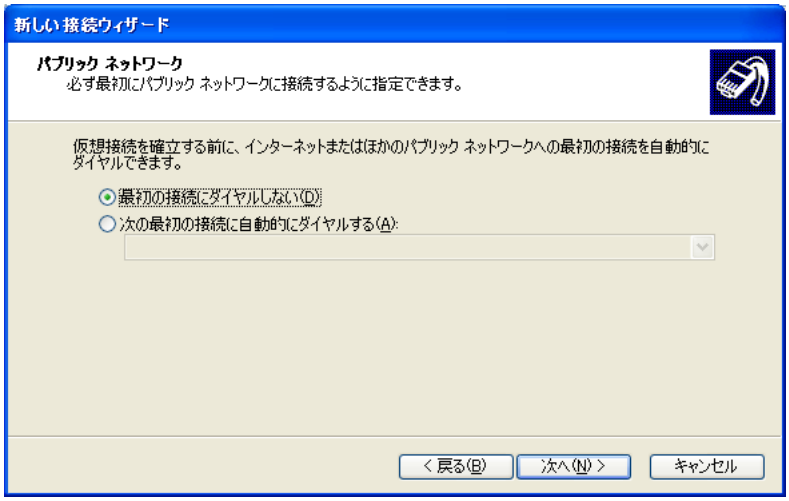
6.　「接続名」で以下の項目を指定します。

- 会社名　→この接続の名前を入力します。ここでは「マルチTA」としています。



7.　[次へ] ボタンをクリックします。

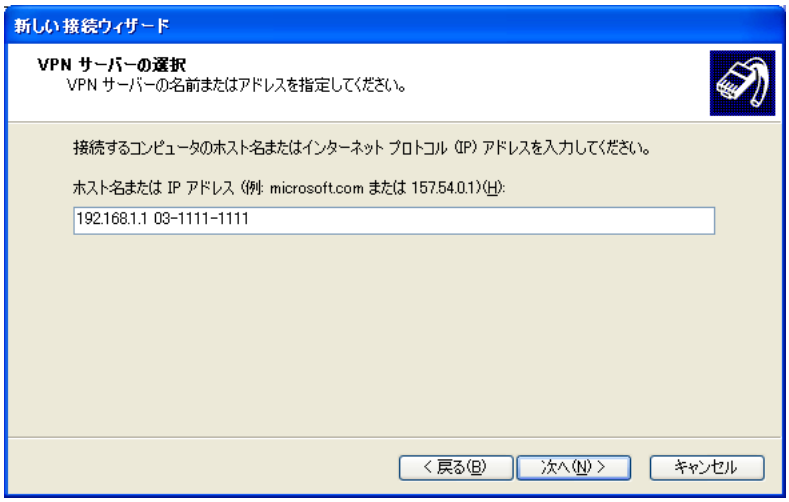
8.　「パブリック ネットワーク」で「最初の接続にダイヤルしない」のラジオボタンがチェックされていることを確認します。「パブリックネットワーク」設定画面が表示されない場合、手順 10. に進みます。



9.　[次へ] ボタンをクリックします。

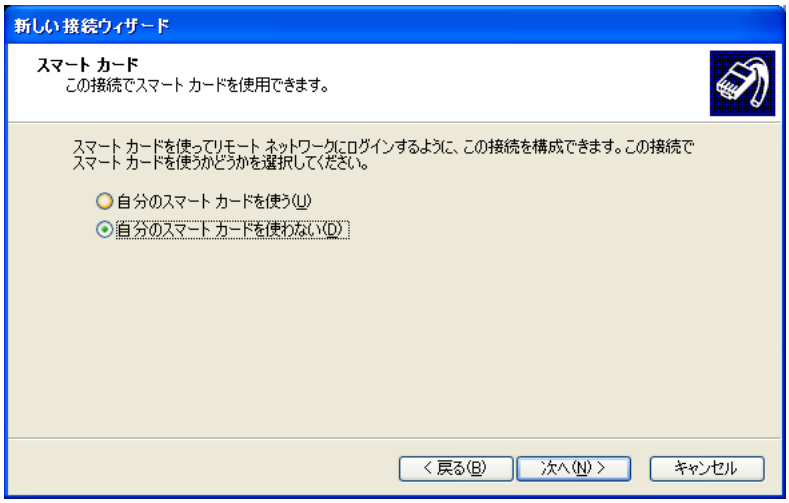
10. 「VPN サーバーの選択」で以下の項目を指定します。

- ホスト名または IP アドレス　→ 192.168.1.1 03-1111-1111（IPアドレスと電話番号の間に半角空白を入れます）



11. ［次へ］ボタンをクリックします。

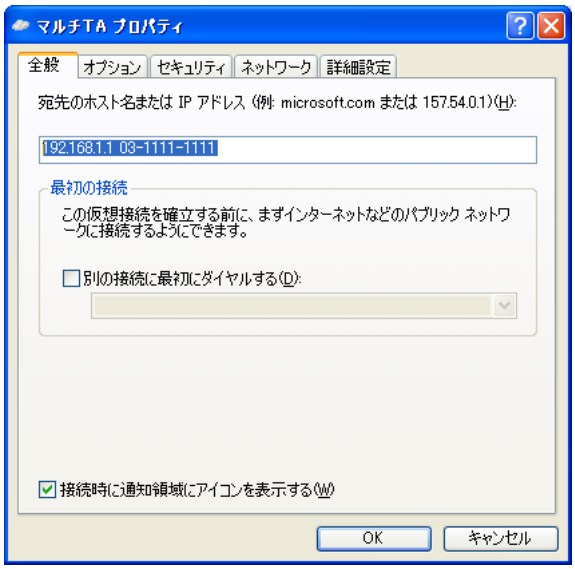
12. 「スマート カード」で「自分のスマート カードを使わない」のラジオボタンがチェックされていることを確認します。



13. ［次へ］ボタンをクリックします。

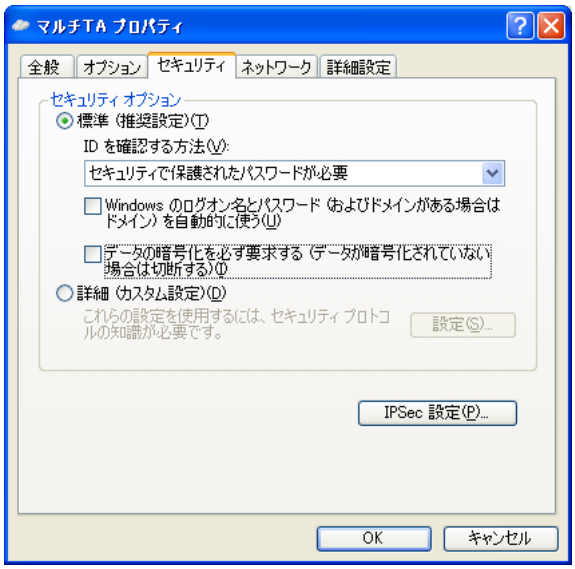
14. ［完了］ボタンをクリックします。

15. 接続画面が表示されたら、「プロパティ」を選択します。



16. 「セキュリティ」タブをクリックします。

17. 「セキュリティオプション」で「データの暗号化を必ず要求する（データが暗号化されていない場合は切断する）」のチェックボックスのチェックを外します。



18. [OK] ボタンをクリックします。

19. [キャンセル] ボタンをクリックして設定を終了します。

マルチTA機能を使って会社のネットワークに接続する（Windows® 2000の場合）

1. 「コントロールパネル」ウィンドウを開き、「ネットワークとダイヤルアップ」アイコンをダブルクリックします。

2. 「仮想プライベートネットワーク」アイコンをダブルクリックします。

3. 「ユーザー名」と「パスワード」を指定します。

   - ユーザー名　→user1
   - パスワード　→userpass

4. ［接続］ボタンをクリックします。

   「ユーザー名」と「パスワード」の確認処理が終わると、回線が接続されます。
   タスクバーにダイヤルアップネットワークのインジケータが表示されます。

5. 回線を切断するときは、ダイヤルアップネットワークのインジケータをダブルクリックして、表示されたダイアログボックスで［切断］ボタンをクリックします。

マルチTA機能を使って会社のネットワークに接続する（Windows® XPの場合）

1. 「コントロールパネル」ウィンドウを開き、「ネットワーク接続」アイコンをダブルクリックします。

2. 「マルチTA」アイコンをダブルクリックします。

3. 「ユーザー名」と「パスワード」を指定します。

   - ユーザー名　→user1
   - パスワード　→userpass

4. ［接続］ボタンをクリックします。

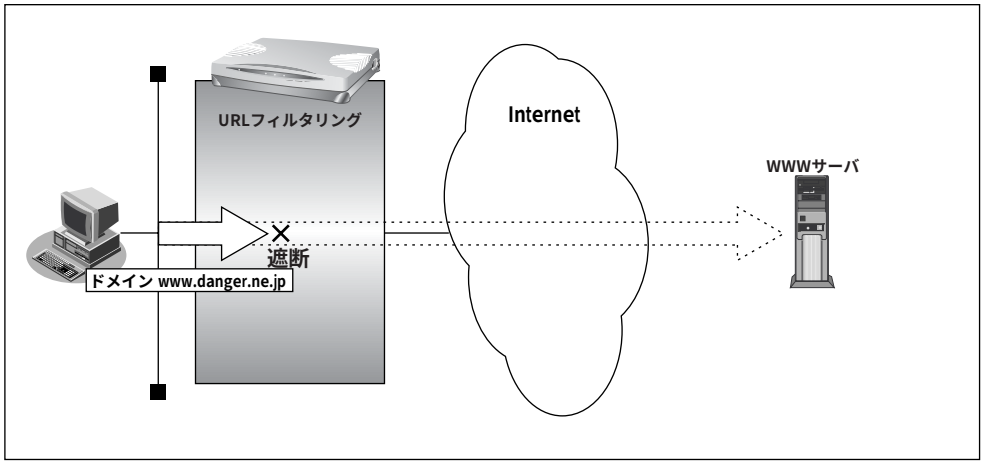
   「ユーザー名」と「パスワード」の確認処理が終わると、回線が接続されます。
   タスクバーにダイヤルアップネットワークのインジケータが表示されます。

5.　回線を切断するときは、ダイヤルアップネットワークのインジケータをダブルクリックして、表示されたダイアログボックスで［切断］ボタンをクリックします。

特定のURLへのアクセスを禁止する（URLフィルタ機能）

本装置のURLフィルタ機能を使用すると、特定のURLへのアクセスを禁止することができます。URLフィルタ機能を使用する場合は、ProxyDNS情報で設定します。

以下に設定例を説明します。



● 設定条件

- アクセスを禁止するドメイン名　：www.danger.ne.jp

こんな事に気をつけて

文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。
詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

URLの情報を設定する

1.　詳細設定メニューのルータ設定で「URLフィルタ情報」をクリックします。

「ProxyDNS情報」ページが表示されます。

2.　［順引き情報一覧］の［追加］ボタンをクリックします。

「ProxyDNS情報設定（順引き）」ページが表示されます。

3.　以下の項目を指定します。

- ドメイン名　→www.danger.ne.jp
- 動作　→廃棄する

4.　[更新] ボタンをクリックします。

「ProxyDNS情報」ページに戻ります。

5.　[設定反映] ボタンをクリックします。

設定した内容が有効になります。

ヒント

◆「＊」は使えるの？

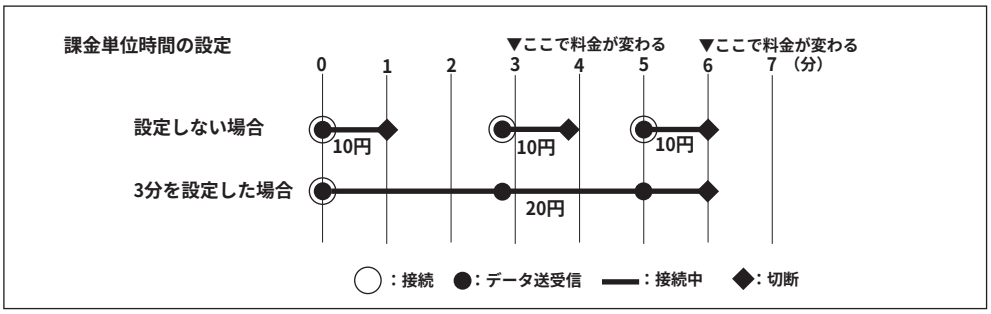
たとえば「www.danger.ne.jp」と「XXX.danger.ne.jp」の両方をURLフィルタの対象とする場合は「＊.danger.ne.jp」と指定することで両方を対象にできます。

こんな事に気をつけて

ProxyDNS（順引き）条件が複数存在する場合、それぞれの条件に優先順位がつき、数値の小さいものから優先的に採用されます。設定内容によっては通信できなくなる場合がありますので、優先順位を意識して設定してください。

通信料金を節約する（課金制御機能）

本装置は通信料金を節約するための機能をサポートしています。通信料金のむだ、使い過ぎを防ぐことができます。
ISDN回線やプロバイダの多くは、一定時間を単位として料金を算定する従量課金制度を利用して料金を決めています。通信料金が3分10円で計算される場合、3分の中で何度も切断／接続を繰り返すと、料金額はその回数×10円になります。
そこで課金単位時間（通信料金が計算されるときの単位時間）を設定し、無通信監視タイマ（初期設定値：60秒）と連動することで、単位時間内は回線を切断させないようにします。
無通信監視タイマとは、アクセスがなければ自動的に切断するときの単位時間です。
課金単位時間に3分間を指定した場合、以下のようになります。



また、データ通信に費やした通信時間や通信料金が一定の値を超えた場合、接続を禁止したり、ログにアラームを出したりする機能もあります（課金制御機能）。無意識のうちに通信料金を使いすぎてしまうのを防げます。

補足
- 超過課金対策のため、初期設定では、1週間（毎週金曜日に課金情報をクリアする）で通信料金の累計が3,000円を超えると発信抑止されるように設定されています。
- 通信時間や通信料金が設定した値を超え、接続できなくなった場合でもアナログ機器の動作には影響しません。

こんな事に気をつけて
- **設定前に本装置の内部時計を正しくセットしてください。**
- **課金制御機能は、指定した料金を超えた場合に発呼を制御しますが、運用中の回線は切断されません。指定した料金を超えても、回線が接続中のままだと料金がかかり続け、通信料金が指定された金額を超える場合があります。**

課金単位時間を設定する

ここでは、ネットワーク名（internet）配下の「接続先情報」としてプロバイダA（ISP-A）がすでに登録してある場合を例に説明します。

● 設定条件

- 無通信監視タイマ　：60秒
- 課金単位時間
  昼間（08:00～19:00）　：180秒
  夜間（19:00～23:00）　：180秒
  深夜・早朝（23:00～08:00）　：240秒

1.　詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］で「internet」欄の［修正］ボタンをクリックします。

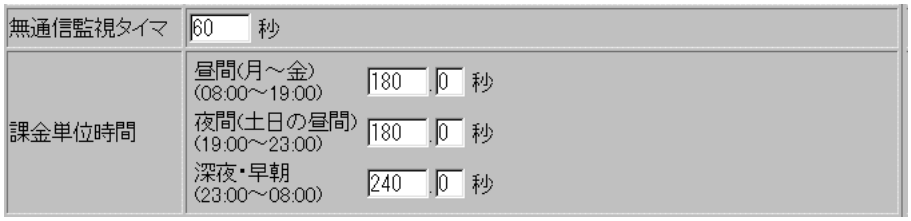
「ネットワーク情報設定」ページが表示されます。

3.　［接続先情報一覧］で［修正］ボタンをクリックします。

「接続先情報設定」ページが表示されます。

4.　［基本情報］で以下の項目を指定します。

- 無通信監視タイマ　→60秒
- 課金単位時間
  昼間　→180秒
  夜間　→180秒
  深夜・早朝　→240秒



5.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

6.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

7.　［更新］ボタンをクリックします。

8.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

■ 課金制御機能を設定する

ここでは、接続累計時間が50時間、または通信料金の合計が10,000円になったら接続要求の抑止を設定する場合を例に説明します。

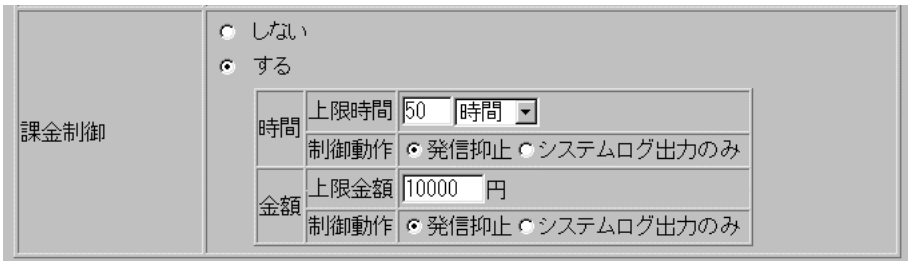
1. 詳細設定メニューのルータ設定で「回線情報」をクリックします。

「回線情報設定」ページが表示されます。

2. [ISDN 情報] で以下の項目を指定します。

- 課金制御　→する
  時間
  上限時間　→50時間
  制御動作　→発信抑止（通信時間累計が上限値になった場合の動作）
  金額
  上限金額　→10,000円
  制御動作　→発信抑止（通信料金累計が上限値になった場合の動作）

補足 「システムログ出力のみ」を選択した場合は、通信時間が「上限時間」で設定した値を超えた、または通信料金が「上限金額」で設定した値を超えたときに、システムログ情報に警告通知を記録します。



3. [更新] ボタンをクリックします。

4. [設定反映] ボタンをクリックします。

設定した内容が有効になります。

補足
- 現在の課金情報は、表示メニューで「課金情報」をクリックすると表示されます。
- 課金情報をクリアすることで、再度、発信ができるようになります。課金情報をクリアするには、表示メニューの「課金情報」から行います。

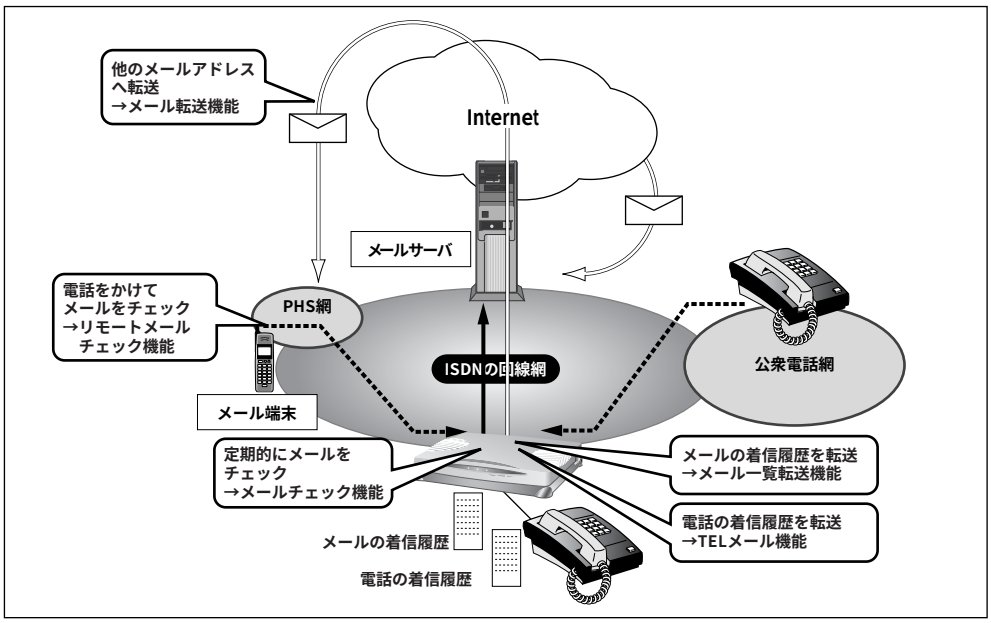
こんな事に気をつけて

- 本書の表記で使われる通信料金とは、INS ネット64基本サービスの「料金情報通知」をもとに、本装置のソフトウェアが算出した値です。算出される値は、お客様の契約や回線利用状況により異なりますので、請求金額とは必ずしも一致しません。
  たとえば以下のような場合があります。
  - INS テレホーダイサービス利用時
  - NTT DoCoMo以外の自動車電話・携帯電話と通話した場合
  - PHS と通話した場合（PIAFSによるデータ通信も含む）
- 本装置の電源を切ると、課金情報（通信時間累計、通信料金累計など）はすべてクリアされます。

Eメールエージェント機能を使う

本装置のEメールエージェント機能には、以下の機能があります。

- メールチェック機能
- リモートメールチェック機能
- メール転送機能
- メール一覧送信機能
- TEL メール機能



こんな事に気をつけて

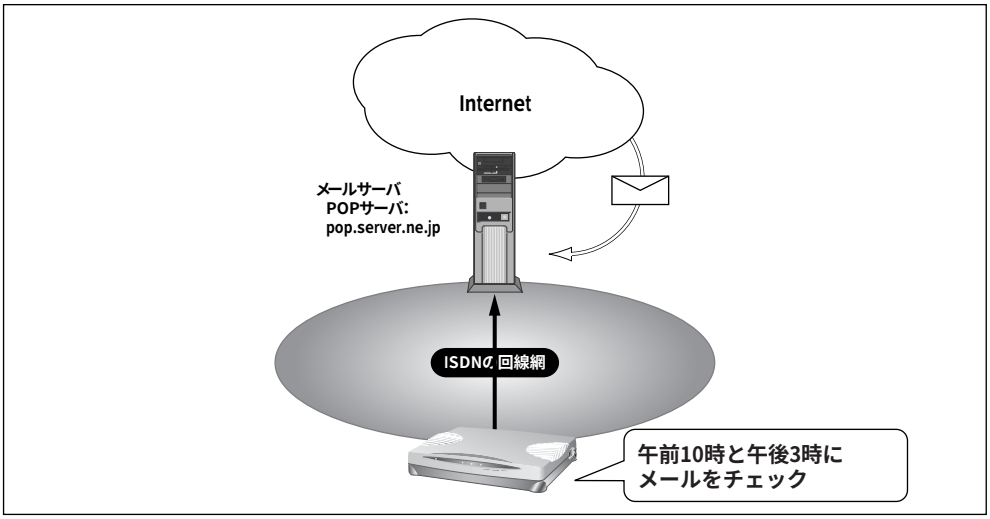
- **設定前に本装置の内部時計を正しくセットしてください。**
- **文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。**
  詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

補足 Eメールエージェント機能は、スタンバイモードでも動作します。本装置は、指定時刻になると動作し、終了するとスタンバイモードに戻ります。

■ メールチェック機能

本装置のメールチェック機能は、本装置が定期的にダイヤルアップし、メールサーバにメールが着信しているかどうか確認する機能です。メールが届いていた場合、CHECKランプが緑色で点滅します。

ここでは、本装置から定期的にメールサーバに接続し、メールの着信を確認する場合を例に説明します。



● 設定条件

- メールの着信を1日2回（午前10時と午後3時）確認する
- メールサーバ名（POPサーバ）　：pop.server.ne.jp
- メールのユーザ名　：user1
- メールのパスワード　：himitu

1.　詳細設定メニューのルータ設定で「Eメールエージェント情報」をクリックします。

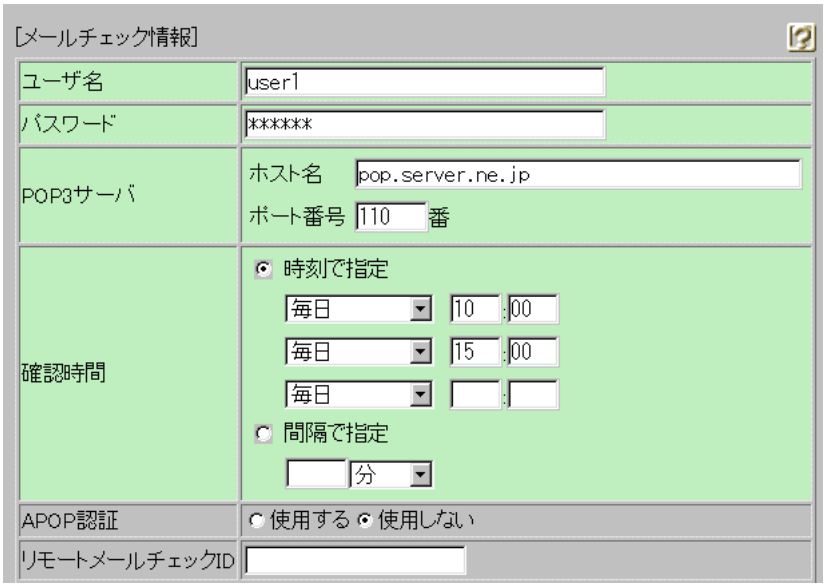
「Eメールエージェント情報設定」ページが表示されます。

2.　［メールチェック情報一覧］で［追加］ボタンをクリックします。

「メールチェック情報設定」ページが表示されます。

3.　［メールチェック情報］で以下の項目を指定します。

- ユーザ名　→user1
- パスワード　→himitu
- POP3サーバ（ホスト名）　→pop.server.ne.jp
- 確認時間　→時刻で指定
  毎日 10:00
  毎日 15:00



4.　［更新］ボタンをクリックします。

「E メールエージェント情報設定」ページに戻ります。

5.　［更新］ボタンをクリックします。

6.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

メールチェックの確認方法

本装置は、指定した時刻になるとメールチェックを行います。以下の方法で確認できます。

- 表示メニューで件数と差出人／題名／時刻を確認できます。

☛ 参照 「電子メール着信通知を見る」（P.618）

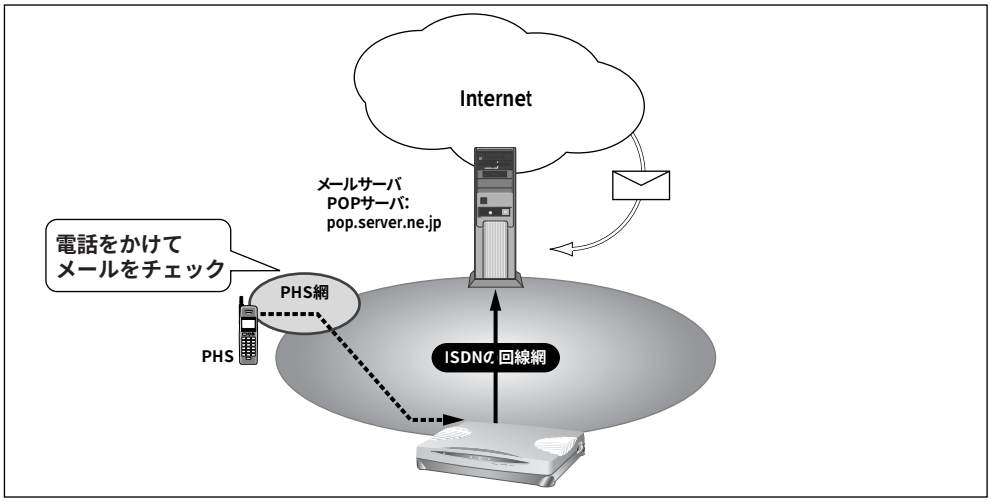
■ リモートメールチェック機能

本装置のリモートメールチェック機能は、PHSから本装置に電話をかけて、本装置にメールチェックさせる機能です。リモートメールチェック機能とメール転送機能、またはメール一覧送信機能を使って、離れた所から必要なときにメールを受け取ったり、メールの一覧を確認したりできます。

こんな事に気をつけて

サブアドレスを指定できない携帯電話などのアナログ機器からは、この機能を利用できません。

ここでは、PHSから本装置に電話をかけて、メールの着信を確認する場合を例に説明します。



● 設定条件

- PHSを使って本装置にメールチェックさせる
- リモートチェックID（サブアドレス）　：1234
- メールサーバ名　：pop.server.ne.jp
- メールのユーザ名　：user1
- メールのパスワード　：himitu

補足 この例では、メールが届いていた場合、表示メニューに表示、または本装置のCHECKランプが緑色で点滅します。離れた場所からメール端末などでメールを受け取ったり、メールの一覧を確認するには、メール転送機能、またはメール一覧送信機能を使う必要があります。

☛ 参照 「メール転送機能」（P.541）、「メール一覧送信機能」（P.544）

1.　詳細設定メニューのルータ設定で「E メールエージェント情報」をクリックします。

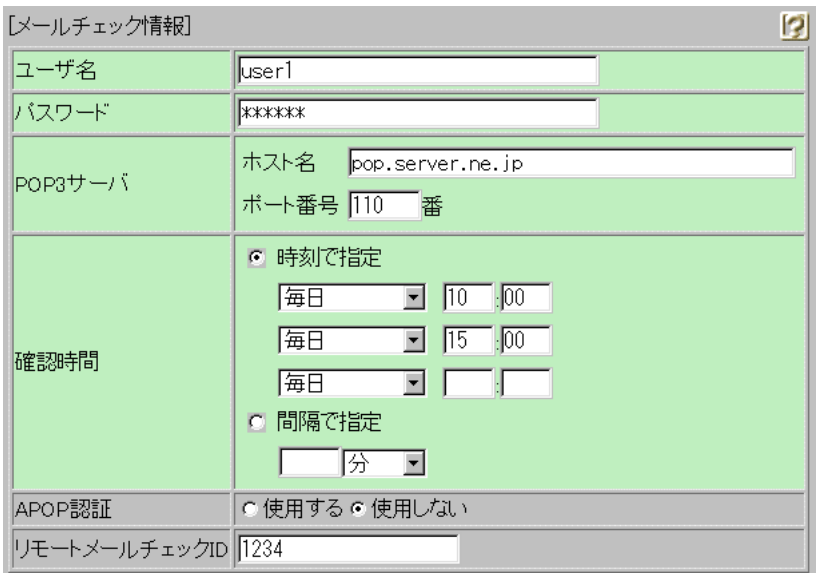
「E メールエージェント情報設定」ページが表示されます。

2.　［メールチェック情報一覧］で［追加］ボタンをクリックします。

「メールチェック情報設定」ページが表示されます。

3.　［メールチェック情報］で以下の項目を指定します。

- ユーザ名　→user1
- パスワード　→himitu
- POP3サーバ
  ホスト名　→pop.server.ne.jp
- リモートメールチェックID　→1234



こんな事に気をつけて

リモートメールチェックIDは、アナログ設定の「アナログポート情報」の「サブアドレス」、および「アナログ共通情報」の「設定変更用暗証番号」と別の番号を設定してください。

4.　［更新］ボタンをクリックします。

「E メールエージェント情報設定」ページに戻ります。

5.　［更新］ボタンをクリックします。

6.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

メールチェックの操作方法

外からPHSなどのISDN機器を使って、本装置に電話をかけます。

正常に受け付けられた場合は、ビジートーン（プープープーという話中の音）が聞こえます。

- 相手電話番号 ✱ サブアドレス（リモートメールチェックID）

  例）03-1111-1111 ✱ 1234

メールチェックの確認方法

本装置に電話をかけるとメールチェックを行います。以下の方法で確認できます。

- 表示メニューで確認する

☛ 参照 「電子メール着信通知を見る」（P.618）

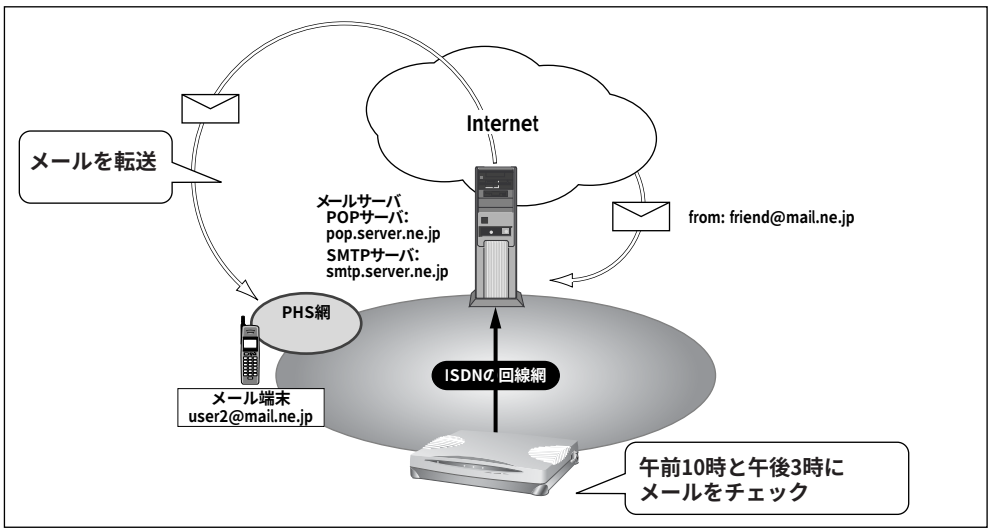
■ メール転送機能

本装置のメール転送機能は、メールサーバに着信しているメールを指定した別のメールアドレスに転送する機能です。

こんな事に気をつけて

メール転送機能を使って転送できるメールは、メールチェックで取得した新着メールだけです。

ここでは、着信しているメールをメール端末へ転送する場合を例に説明します。



● 設定条件

- 特定の人からのメールを1日2回（午前10時と午後3時）別のメールアドレスへ転送する
- 特定の人のメールアドレス　：friend@mail.ne.jp
- 転送先のメールアドレス　：user2@mail.ne.jp
- メールサーバ名（POPサーバ）　：pop.server.ne.jp
- メールサーバ名（SMTPサーバ）　：smtp.server.ne.jp
- メールのユーザ名　：user1
- メールのパスワード　：himitu

メールチェック情報を設定する

メール転送機能を使用するには、メールチェック機能、またはリモートメールチェック機能の設定が必要です。この例では、user1 に対してメールチェックの設定を行っていることを前提に説明します。

☛ 参照 「メールチェック機能」（P.536）、「リモートメールチェック機能」（P.538）

メール転送情報を設定する

1.　詳細設定メニューのルータ設定で「E メールエージェント情報」をクリックします。

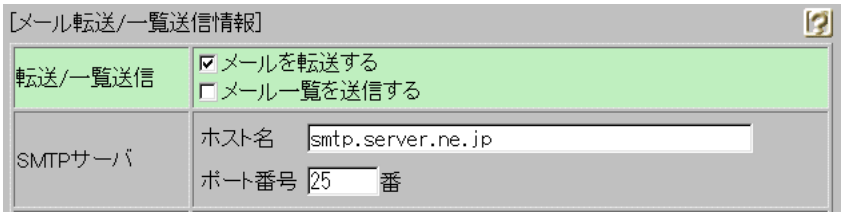
「E メールエージェント情報設定」ページが表示されます。

2.　［メールチェック情報一覧］で user1 の欄の［修正］ボタンをクリックします。

「メールチェック情報設定」ページが表示されます。

3.　［メール転送／一覧送信情報］で以下の項目を指定します。

- 転送／一覧送信　→メールを転送する
- SMTP サーバ
  ホスト名　→ smtp.server.ne.jp



4.　宛先メールアドレスの欄の［追加］ボタンをクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

「宛先メールアドレス設定」ページが表示されます。

5.　以下の項目を指定します。

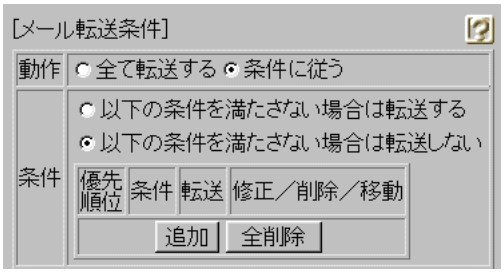
- メールアドレス　→ user2@mail.ne.jp

6.　［更新］ボタンをクリックします。

「メールチェック情報設定」ページに戻ります。

7.　［メール転送条件］で以下の項目を指定します。

- 動作　→条件に従う
- 条件　→以下の条件を満たさない場合は転送しない



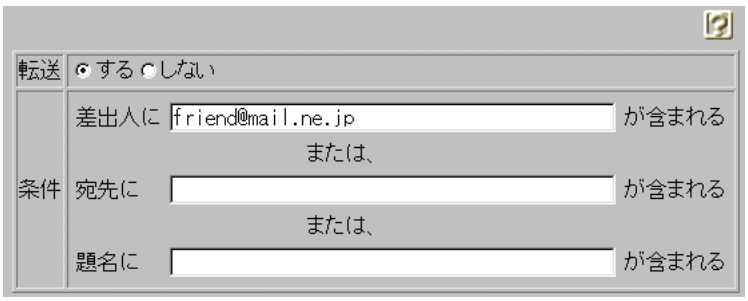
8.　条件の欄の［追加］ボタンをクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

「条件設定」ページが表示されます。

9.　以下の項目を指定します。

- 転送　→する
- 条件　→差出人に friend@mail.ne.jp が含まれる



10.　［更新］ボタンをクリックします。

「メールチェック情報設定」ページに戻ります。

11.　［更新］ボタンをクリックします。

「E メールエージェント情報設定」ページに戻ります。

12.　［更新］ボタンをクリックします。

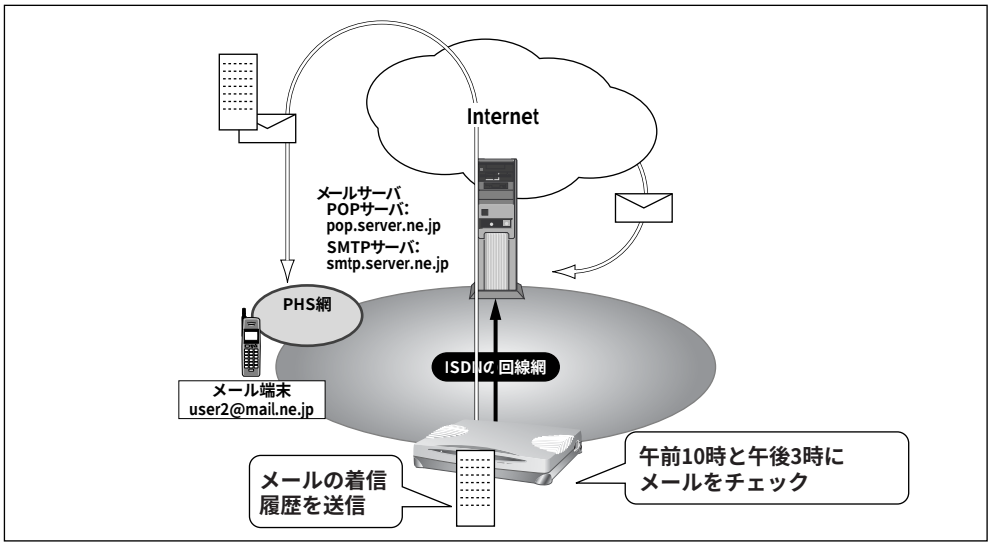
13.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

■ メール一覧送信機能

本装置のメール一覧送信機能は、メールサーバに着信しているメールの一覧情報をメールで送信する機能です。

ここでは、着信しているメールの一覧情報をメール端末へ転送する場合を例に説明します。



● 設定条件

- メールの着信履歴を1日2回（午前10時と午後3時）送信する
- メールサーバ名（POPサーバ）　：pop.server.ne.jp
- メールサーバ名（SMTPサーバ）　：smtp.server.ne.jp
- メールのユーザ名　：user1
- メールのパスワード　：himitu
- 送信先のメールアドレス　：user2@mail.ne.jp

メールチェック情報を設定する

メール転送機能を使用するには、メールチェック機能またはリモートメールチェック機能の設定が必要です。この例では、user1 に対してメールチェックの設定を行っていることを前提に説明します。

☛ 参照 「メールチェック機能」（P.536）、「リモートメールチェック機能」（P.538）

メール転送情報を設定する

1.　詳細設定メニューのルータ設定で「E メールエージェント情報」をクリックします。

「E メールエージェント情報設定」ページが表示されます。

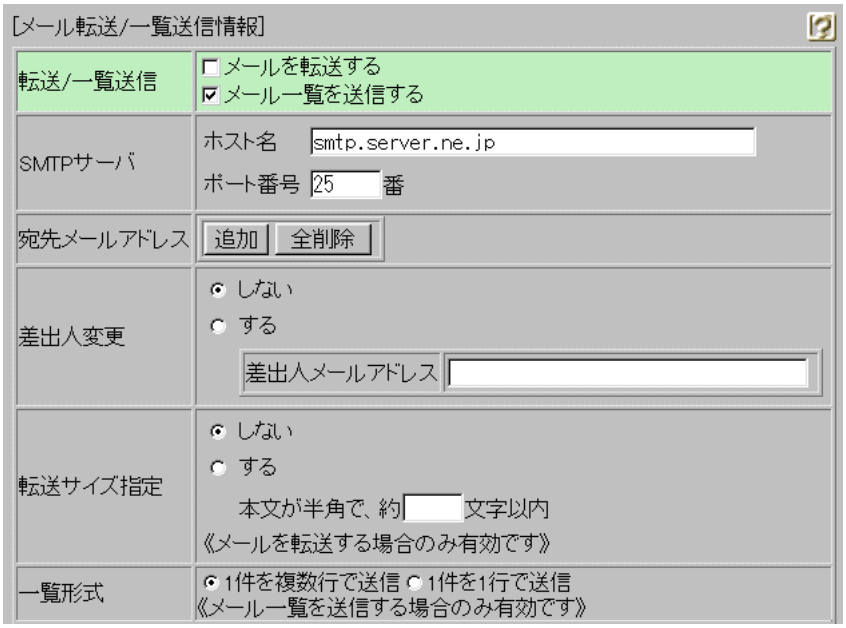
2.　［メールチェック情報一覧］で user1 の欄の［修正］ボタンをクリックします。

「メールチェック情報設定」ページが表示されます。

3.　［メール転送／一覧送信情報］で以下の項目を指定します。

- 転送／一覧送信　→メール一覧を送信する
- SMTP サーバ
  ホスト名　→ smtp.server.ne.jp
- 一覧形式　→ 1 件を複数行で送信する

補足　PHS など表示できる一行の文字数が少ないメール端末では、一覧形式を「1 件を複数行で送信する」をお勧めします。



4.　宛先メールアドレスの欄の［追加］ボタンをクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

「宛先メールアドレス設定」ページが表示されます。

5.　以下の項目を指定します。

- メールアドレス　→user2@mail.ne.jp

6.　[更新] ボタンをクリックします。

「メールチェック情報設定」ページに戻ります。

7.　[更新] ボタンをクリックします。

「E メールエージェント情報設定」ページに戻ります。

8.　[更新] ボタンをクリックします。

9.　[設定反映] ボタンをクリックします。

設定した内容が有効になります。

メール一覧の受信例

この例では、以下のような一覧内容が届きます。

From: Si-R <user1@smtp.server.ne.jp> ※1

Subject: Mail list （user1）

01. 02/29 10:00 （送信時刻が表示されます）

差出人 :

girl@mail.ne.jp ※2

題名 :

Hello　　（メールの題名が表示されます）

※1: < > 内は差出人のメールアドレスが記入されます。差出人変更の欄の差出人メールアドレスを指定した場合、指定したメールアドレスが記入されます。

※2: 差出人名が書かれているメールの場合は、差出人名が表示されます。書かれていない場合は、差出人メールアドレスが表示されます。

■ TELメール機能

本装置のTELメール機能は、かかってきた電話（アナログ）の着信履歴をメールで送信する機能です。

こんな事に気をつけて

- TELメールの送信情報が「発信者番号のみ送信する」に設定している場合、発信者番号通知が非通知になっている電話からの着信履歴は送信されません。
- TELメールの送信情報が「発信者番号と着信番号を送信する」に設定している場合、発信者番号と着信番号のどちらも有効な情報がない時は、TELメールによる着信履歴は送信されません。
- TELメールの着信番号は以下のように設定されます。

(1)ダイヤルインサービスおよびi・ナンバーサービスを利用しない場合

回線から通知されないため、TELメール情報に着信番号は含まれません。「アナログ共通情報」の「網契約に関する設定項目」の「電話番号」に電話番号が設定されていれば、その番号がTELメールの着信番号として送信されます。

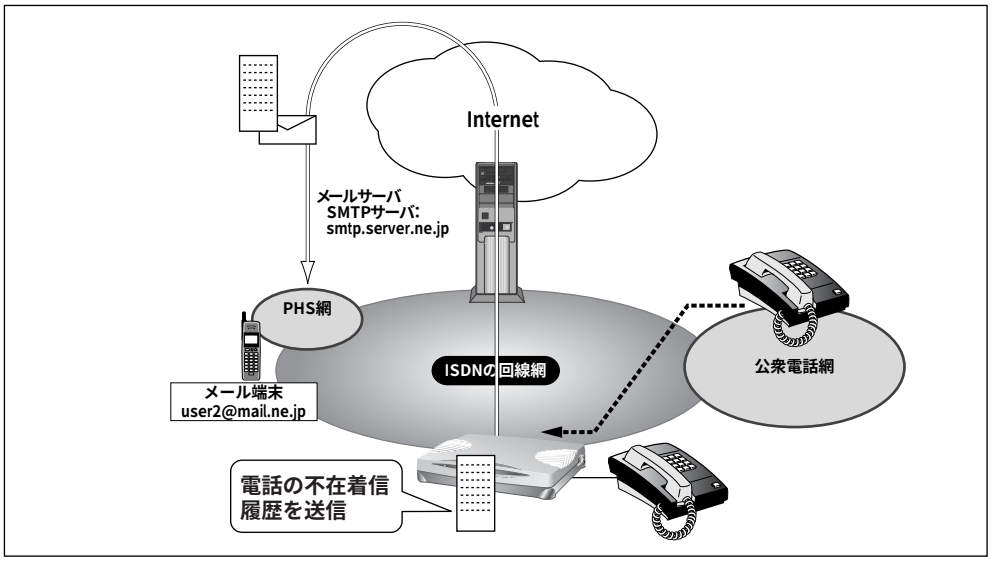
(2)ダイヤルインサービスを利用している場合

回線から通知された着信番号（ダイヤルイン番号）がTELメールの着信番号として送信されます。ただし、グローバル着信を利用している場合、契約者番号にかかってくると回線から着信番号が通知されません。この場合は、「アナログ共通情報」の「網契約に関する設定項目」の「電話番号」に電話番号が設定されていれば、その番号がTELメールの着信番号として送信されます。

(3)i・ナンバーサービスを利用している場合

「鳴り分け1」、「鳴り分け2」、または「鳴り分け3」がTELメールの着信番号として送信されます。ただし、「アナログ共通情報」の「網契約に関する設定項目」の「鳴り分け番号1／2／3」に電話番号が設定されていれば、その番号がTELメールの着信番号として送信されます。

ここでは、定期的に電話の着信履歴をメールで送信する場合を例に説明します。



● 設定条件

- ダイヤルインサービスを利用する
- アナログポート1につながっている電話への着信履歴を1時間ごとにメールする
- 送信先のメールアドレス　：user2@mail.ne.jp
- 差出人のメールアドレス　：tel1@si-r130b
- メールサーバ名　：smtp.server.ne.jp

1.　詳細設定メニューのルータ設定で「Eメールエージェント情報」をクリックします。

「Eメールエージェント情報設定」ページが表示されます。

2.　［TELメール情報］で以下の項目を指定します。

- TELメール　→使用する

［TELメール情報］ ISDN

TELメール	◉使用する ○使用しない			
送信情報	アナログポート	メールアドレス	送信周期	修正／削除
	アナログポート1	-	-	修正 削除
	アナログポート2	-	-	修正 削除

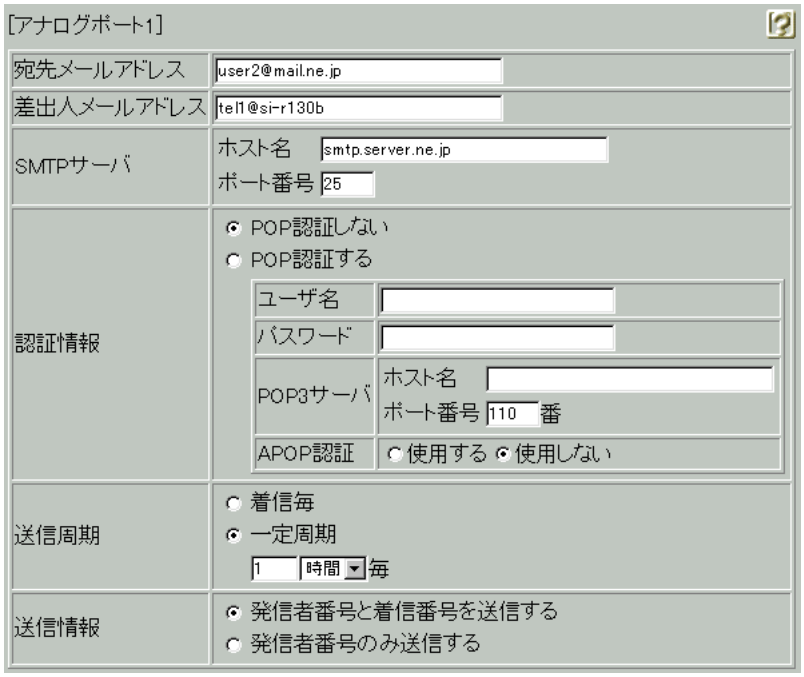
3.　送信情報（アナログポート1）の欄の［修正］ボタンをクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

［TELメール情報設定］ページが表示されます。

4.　［アナログポート 1］で以下の項目を指定します。

- 宛先メールアドレス　→user2@mail.ne.jp
- 差出人メールアドレス　→tel1@si-r130b
- SMTP サーバ（ホスト名）　→smtp.server.ne.jp
- 認証情報　→POP 認証しない
- 送信同期　→一定周期
→1 時間毎
- 送信情報　→発信者番号と着信番号を送信する



5.　［更新］ボタンをクリックします。

「E メールエージェント情報設定」ページに戻ります。

6.　［更新］ボタンをクリックします。

7.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

TEL メールの受信例

この例では、以下のような一覧内容が届きます。

From: Si-R <tel1@si-r130b>

Subject: TEL1 Mail

01．02/29 10:00　　（着信した時刻が表示されます）

発：0311112222　　（発信者番号が表示されます）

著：0312345678　　（ダイヤルイン番号にかかってきた場合、着信番号が表示されます）

スケジュール機能を使う

本装置のスケジュール機能では、特定の動作とそれを行う時間を登録できます。スケジュール予約情報を登録しておくと、特定の時間帯にデータの発着信を制限する、定期的に課金情報をクリアするといった作業を本装置が自動的に行います。スケジュール予約情報は、最大16件まで登録できます。

補足
- テレホーダイ時間以外の動作を発信抑止することで、テレホーダイ時間だけ発信可能な設定をすることができます。
- 初期設定では、毎週金曜日に課金情報がクリアされるように設定されています。

こんな事に気をつけて

設定前に本装置の内部時計を正しくセットしてください。

スケジュールを予約する

ここでは、毎日午後11時以降テレホーダイを利用する場合を例に説明します。

こんな事に気をつけて

- **「INSテレホーダイ」はNTTが提供するサービスです。利用の際は、NTTとの契約が必要です。**
- **文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。**
  詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

1. 詳細設定メニューのルータ設定で「スケジュール情報」をクリックします。

「スケジュール情報」ページが表示されます。


[月間／週間予約一覧]

＼	動作	予約時刻	終了時刻	周期	修正／削除
1	課金情報クリア	00:00	-	毎週金曜	修正 削除
2	-	-	-	-	修正 削除
3	-	-	-	-	修正 削除

2. ［月間／週間予約一覧］で未設定の欄の［修正］ボタンをクリックします。

「月間／週間予約情報設定」ページが表示されます。

3.　以下の項目を指定します。

- 動作　→テレホーダイ（動作は「発信抑止」、「着信抑止」、「テレホーダイ」、「課金情報クリア」、「強制切断」、「統計情報収集」、「リモートパワーオン」、「スタンバイモードへ移行」、「スタンバイモードを解除」、「留守モードへ移行」、「留守モードを解除」から選択できます。）
- 予約時刻　→23：00
  →毎日
- 終了時刻　→08:00

こんな事に気をつけて

- **回線接続中に、発信抑止、着信抑止が実行されても回線は切断されません。**
- **回線接続中に、スタンバイモードに移行した場合はデータ通信が切断されます。**

4.　［更新］ボタンをクリックします。

「スケジュール情報」ページに戻ります。

5.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

電話番号変更を予約する

ここでは、2008年1月1日に電話番号を「06-123-4567」から「06-6123-4567」に変更する場合を例に説明します。

1.　詳細設定メニューのルータ設定で「スケジュール情報」をクリックします。

「スケジュール情報」ページが表示されます。

2.　［電話番号変更予約一覧］で未設定の欄の［修正］ボタンをクリックします。

「電話番号変更予約設定」ページが表示されます。

3.　以下の項目を指定します。

- 実行日時　→2008年1月1日2時00分
- 電話番号変更情報
  変更前1　→06-123-4567
  変更後1　→06-6123-4567

4.　［更新］ボタンをクリックします。

「スケジュール情報」ページに戻ります。

5.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

指定時刻になると自動的に再起動され、電話番号が更新されます。その際、データ通信／電話を使用中の場合は回線が切断されます。

SNMPエージェント機能を使う

本装置は、SNMP（Simple Network Management Protocol）エージェント機能をサポートしています。

ここでは、本装置がSNMPマネージャに対してMIB情報を通知する場合を例に説明します。

ヒント

◆ SNMPとは？

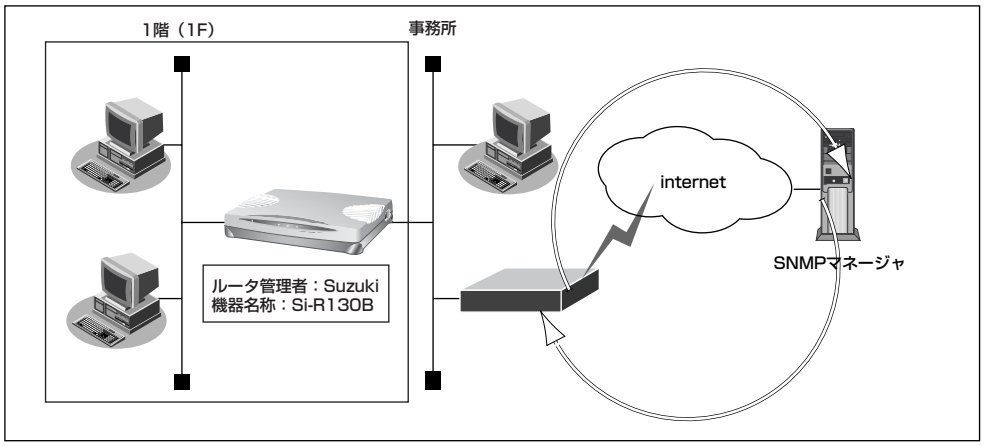
SNMP（Simple Network Management Protocol）は、ネットワーク管理用のプロトコルです。SNMPマネージャは、ネットワーク上の端末の稼動状態や障害状況を一元管理します。SNMPエージェントは、マネージャの要求に対してMIB（Management Information Base）という管理情報を返します。

また、特定の情報についてはtrapという機能を用いて、エージェントからマネージャに対して非同期通知を行うことができます。エージェントは、エージェントが起動したときにTrapを送信します。

サポートしているtrapは以下のとおりです。

- Coldstart
- LinkUp
- LinkDown
- AuthenticationFailure
- NewRoot
- TopologyChange

☛ 参照 「標準MIB定義」（P.781）、「富士通拡張MIB」（P.793）、「Trap一覧」（P.796）



● 設定条件

- ルータ管理者　　：suzuki
- 機器名称　　：Si-R130B
- 機器設置場所　　：1階（1F）

こんな事に気をつけて

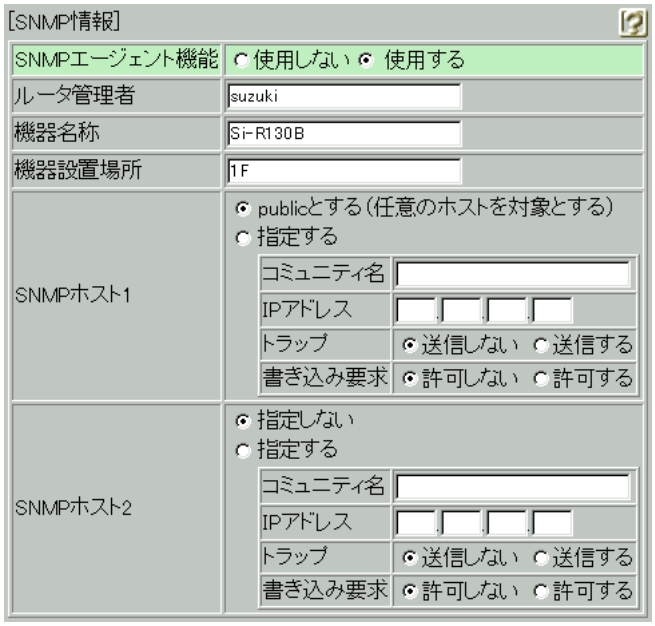
文字入力フィールドでは半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。
詳細については、「付録　文字入力フィールドに入力できる文字一覧（P.754）」を参照してください。

1.　詳細設定メニューのルータ設定で「装置情報」をクリックします。

「装置情報設定」ページが表示されます。

2.　［SNMP 情報］で以下の項目を指定します。

- SNMPエージェント機能　　→使用する
- ルータ管理者　　→suzuki
- 機器名称　　→Si-R130B
- 機器設置場所　　→1F
- SNMPホスト1　　→publicとする
- SNMPホスト2　　→指定しない



3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

VPN機能を利用する

VPN（Virtual Private Network）機能は、インターネットを利用して遠隔地のLANをつなぐと、遠隔地のLAN上のアプリケーションやデータが、同じオフィスのLANのように利用できる機能です。また、認証情報や暗号情報を設定することにより、インターネット上を流れるデータのセキュリティを確保することができます。

本装置には以下のVPN機能があります。

- 固定IPアドレスでのVPN（手動鍵交換）
  固定IPアドレスで送信元、送信先のIPアドレス範囲を指定してVPN通信を行います。認証情報、暗号情報の鍵は手動で交換します。
- 固定IPアドレスでのVPN（自動鍵交換）
  固定IPアドレスで送信元、送信先のIPアドレス範囲を指定してVPN通信を行います。認証情報、暗号情報の鍵は自動で交換します。
- 可変IPアドレスでのVPN
  自側のIPアドレスが動的に割り当てられる環境で、経路情報（送信先のIPアドレス）に従ってVPN通信を行います。認証情報、暗号情報の鍵は自動で交換します。
- NAT変換後にVPN
  可変IPアドレスでのVPNに加えて、VPNのトンネルに入る前に送信元のIPアドレスをNATによって変換することができます。

こんな事に気をつけて

- **VPN機能はIPv4だけで使用できます。IPv6では使用できません。**
- **固定IPアドレスでVPN機能を使う場合は、詳細設定の「IPsec情報」で設定します。動的に割り当てられる環境でVPN機能を使う場合には、「相手情報」→「ネットワーク情報」からIPsec情報を設定します。**
- **固定IPアドレスでVPN機能を使用し、自動鍵交換を行う場合、自動鍵交換の自側IPアドレスにはIKEの通信を行うインタフェースのIPアドレスが使用されます。相手側で宛先IPアドレスを定義をする際に、IKEの通信を行うインタフェースのIPアドレスを指定するよう注意してください。IKEの通信を行うインタフェース以外のIPアドレスを指定した場合、自動鍵交換がうまくいきません。**
- **NAT変換には、IPsecの前の変換とIPsecの後の変換があります。IPsec前に変換する場合はIPsec用の「ネットワーク情報」で設定します。IPsec後に変換する場合は、プロバイダ接続用の「ネットワーク情報」で設定します。**
- **インターネットVPNでは、VPN装置どうしがインターネットを介して通信する必要があるため、VPN装置にはインターネット上で使用可能なグローバルなIPアドレスを使用してください（NATを使用している場合は、マルチNAT（静的NAT）でIPアドレスを割り当てます。）**
- **VPN相互接続するアドレスがプライベートアドレスの場合、重複しないように設計してください。**
- **VPN機能では、IPv4パケット通信だけをサポートしています。したがって、IPv4パケット以外はVPNの対象とならないため中継されません。**
- **暗号パケットが多重に暗号される形態で使用しないでください。暗号パケットが二重に暗号化され、復号処理が正常に行えないため通信異常となります。**
- **固定IPアドレスでのVPN機能と可変IPアドレスでのVPN機能は同時に使用できません。**
- **IPsec機能とダイナミックルーティング機能を同時に使用することはできません。**

- IPsec機能とNATを同時に使用する場合は、マルチNATを使用してください。
- IPsec機能とマルチNATを同時に使用する場合は、静的NATの設定が必要となることがあります。

ヒント

◆ VPNとは？

暗号化技術や認証技術を使って、インターネットを仮想的な専用線として利用する技術です。また、VPNを使ってつないだルータ間の通信経路のことをトンネルと言います。

◆ 自動鍵交換とは？

IPsecの通信に使用される暗号化・認証用の鍵素材を、自動で作成・更新します。鍵素材を定期的に自動更新させることにより、セキュリティの強度を高めることができます。自動鍵交換を使用しない場合には、手動で鍵を設定する必要があります。

■ 固定IPアドレスでのVPN（手動鍵交換）

IPsec機能を使って手動鍵交換でVPNを構築する場合を例に説明します。

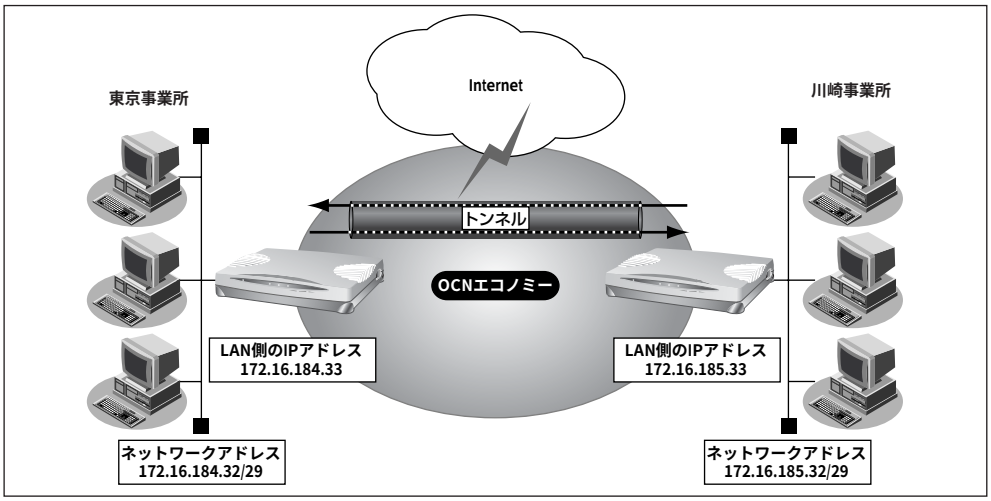
ここでは、「「かんたん設定」で設定する （インターネットへ専用線接続のとき）」（P.85）の設定を参考に東京事業所と川崎事業所の設定が以下のとおり設定されていることを前提とします。

[東京事業所]

- 本装置のIPアドレス　：172.16.184.33
- LAN側のネットワークアドレス／ネットマスク　：172.16.184.32/29

[川崎事業所]

- 本装置のIPアドレス　：172.16.185.33
- LAN側のネットワークアドレス／ネットマスク　：172.16.185.32/29



● 設定条件

- 東京事業所から川崎事業所へのVPN情報

  SPI　：100
  認証アルゴリズムと認証秘密鍵　：hmac-md5、0123456789（16進数）
  暗号アルゴリズムと暗号秘密鍵　：des-cbc、123456789a（16進数）
  対象パケット　：東京事業所LANのすべてのパケット

- 川崎事業所から東京事業所へのVPN情報

  SPI　：101
  認証アルゴリズムと認証秘密鍵　：hmac-md5、23456789ab（16進数）
  暗号アルゴリズムと暗号秘密鍵　：des-cbc、3456789abc（16進数）
  対象パケット　：川崎事業所LANのすべてのパケット

ヒント

◆ SPIとは？

トンネルの識別子です。SPIはトンネルの往路と復路でそれぞれ異なる値を設定します。トンネルをつなぐ本装置を設定するときには、同じ方向のトンネルには同じSPIを定義します。

こんな事に気をつけて

- **暗号アルゴリズムにdes-cbcを選択する場合、鍵に単純な文字列（同一文字だけ、文字列の繰り返しなど）を指定すると、暗号強度が低下するおそれがありますので指定しないでください。**
  暗号アルゴリズムに3des-cbcを選択する場合は、鍵を16桁ごとに3つに分割した、それぞれ3つの暗号強度が低下する鍵（弱い鍵）にならないようにしてください。
  des-cbcで弱い鍵として具体的に知られているものには以下のようなものがあり、本装置は、これらの文字列で始まる鍵で通信できないようにしています。
  0101 0101 0101 0101、1F1F 1F1F E0E0 E0E0、E0E0 E0E0 1F1F 1F1F、
  FEFE FEFE FEFE FEFE
  01FE 01FE 01FE 01FE、1FE0 1FE0 0EF1 0EF1、01E0 01E0 01F1 01F1、
  FE01 FE01 FE01 FE01、E01F E01F F10E F10E、E001 E001 F101 F101
  1FFE 1FFE 0EFE 0EFE、011F 011F 010E 010E、E0FE E0FE F1FE F1FE、
  FE1F FE1F FE0E FE0E、1F01 1F01 0E01 0E01、FEE0 FEE0 FEF1 FEF1
- **暗号アルゴリズムに3desを選択する場合は、以下のように鍵を16桁ごとに3つに分割し、それぞれ3つが鍵1≠鍵2≠鍵3となるように鍵を設定してください。**

  鍵：1122334455667788　9900aabbccddeeff　1122334455667788
  鍵1（16桁）　鍵2（16桁）　鍵3（16桁）

  鍵1＝鍵3のように鍵を設定すると、16バイトの鍵で暗号化するのと同じ結果になります。また、鍵1＝鍵2、鍵2＝鍵3のように鍵を設定すると、それぞれ鍵3、鍵1のdes-cbc暗号と同じ結果になります（鍵1＝鍵2＝鍵3の場合も同様です）。

東京事業所の設定をする

1.　詳細設定メニューのルータ設定で、「IPsec 情報」をクリックします。

「IPsec ／IKE 情報」ページが表示されます。

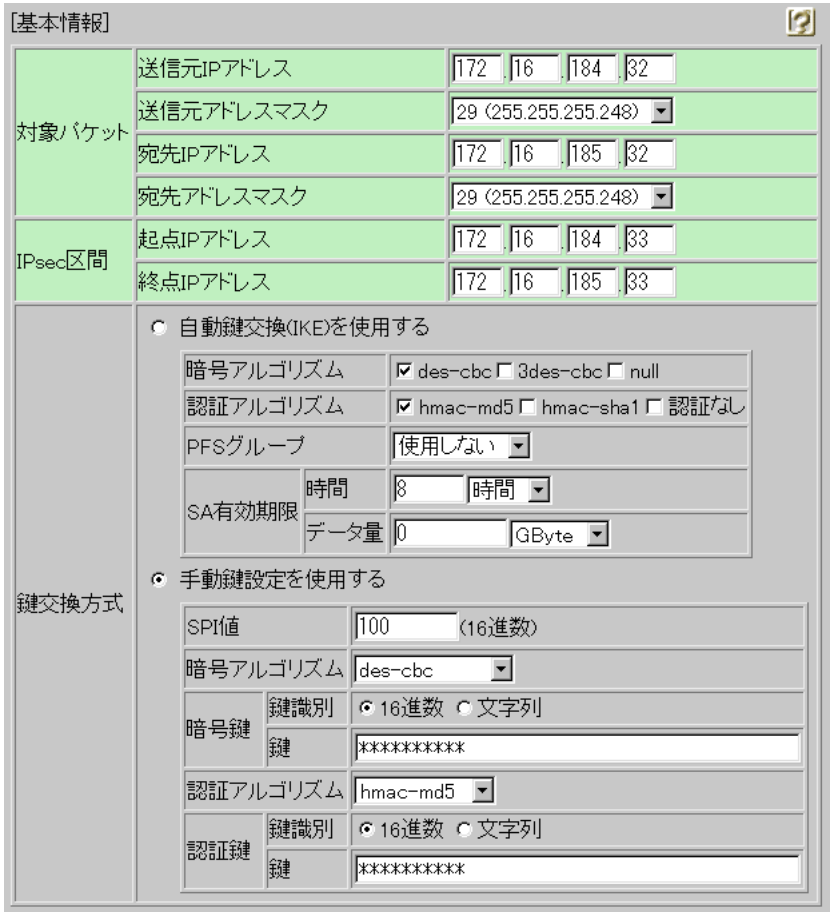
往路（東京事業所→川崎事業所）のVPN 情報を設定する

2.　「IPsec 情報一覧」の［追加］ボタンをクリックします。

「IPsec 情報設定」ページが表示されます。

3.　「基本情報」で以下の項目を指定します。

- 対象パケット
  - 送信元IPアドレス　→172.16.184.32
  - 送信元アドレスマスク　→29（255.255.255.248）
  - 宛先IPアドレス　→172.16.185.32
  - 宛先アドレスマスク　→29（255.255.255.248）
- IPsec区間
  - 起点IPアドレス　→172.16.184.33
  - 終点IPアドレス　→172.16.185.33
- 鍵交換方法　→手動鍵設定を使用する
  - SPI 値　→100
  - 暗号アルゴリズム　→des-cbc
  - 暗号鍵
  - 鍵識別　→16進数
  - 鍵　→123456789a
  - 認証アルゴリズム　→hmac-md5
  - 認証鍵
  - 鍵識別　→16進数
  - 鍵　→0123456789



こんな事に気をつけて

認証や暗号用の鍵には、文字列か数値（16進数）を使用することができます。鍵として数値を入力したつもりでも、鍵識別で文字列を指定していると、文字列として認識されてしまうために、鍵が一致しない原因になります。

4.　［更新］ボタンをクリックします。

「IPsec／IKE情報」ページに戻ります。

復路（川崎事業所→東京事業所）のVPN情報を設定する

5.　手順2.～4.を参考に、以下の項目を指定します。

- 対象パケット
  送信元IPアドレス　→172.16.185.32
  送信元アドレスマスク　→29（255.255.255.248）
  宛先IPアドレス　→172.16.184.32
  宛先アドレスマスク　→29（255.255.255.248）
- IPsec区間
  起点IPアドレス　→172.16.185.33
  終点IPアドレス　→172.16.184.33
- 鍵交換方法　→手動鍵設定を使用する
  SPI値　→101
  暗号アルゴリズム　→des-cbc
- 暗号鍵
  鍵識別　→16進数
  鍵　→3456789abc
  認証アルゴリズム　→hmac-md5
  認証鍵
  鍵識別　→16進数
  鍵　→23456789ab

6.　「設定反映」をクリックします。

設定した内容が有効になります。

川崎事業所の設定をする

「東京事業所の設定をする」を参考に、以下の川崎事業所の設定をします。

往路（川崎事業所→東京事業所）のVPN情報を設定する

- 対象パケット
  送信元IPアドレス　→172.16.185.32
  送信元アドレスマスク　→29（255.255.255.248）
  宛先IPアドレス　→172.16.184.32
  宛先アドレスマスク　→29（255.255.255.248）
- IPsec区間
  起点IPアドレス　→172.16.185.33
  終点IPアドレス　→172.16.184.33
- 鍵交換方法　→手動鍵設定を使用する
  SPI値　→101
  暗号アルゴリズム　→des-cbc
  暗号鍵
  鍵識別　→16進数
  鍵　→3456789abc
  認証アルゴリズム　→hmac-md5
  認証鍵
  鍵識別　→16進数
  鍵　→23456789ab

復路（東京事業所→川崎事業所）のVPN情報を設定する

- 対象パケット
  送信元IPアドレス　→172.16.184.32
  送信元アドレスマスク　→29（255.255.255.248）
  宛先IPアドレス　→172.16.185.32
  宛先アドレスマスク　→29（255.255.255.248）
- IPsec区間
  起点IPアドレス　→172.16.184.33
  終点IPアドレス　→172.16.185.33
- 鍵交換方法　→手動鍵設定を使用する
  SPI値　→100
  暗号アルゴリズム　→des-cbc
  暗号鍵
  鍵識別　→16進数
  鍵　→123456789a
  認証アルゴリズム　→hmac-md5
  認証鍵
  鍵識別　→16進数
  鍵　→0123456789

7.　「設定反映」をクリックします。

設定した内容が有効になります。

■ 固定IPアドレスでのVPN（自動鍵交換）

IPsec機能を使って自動鍵交換でVPNを構築する場合を例に説明します。

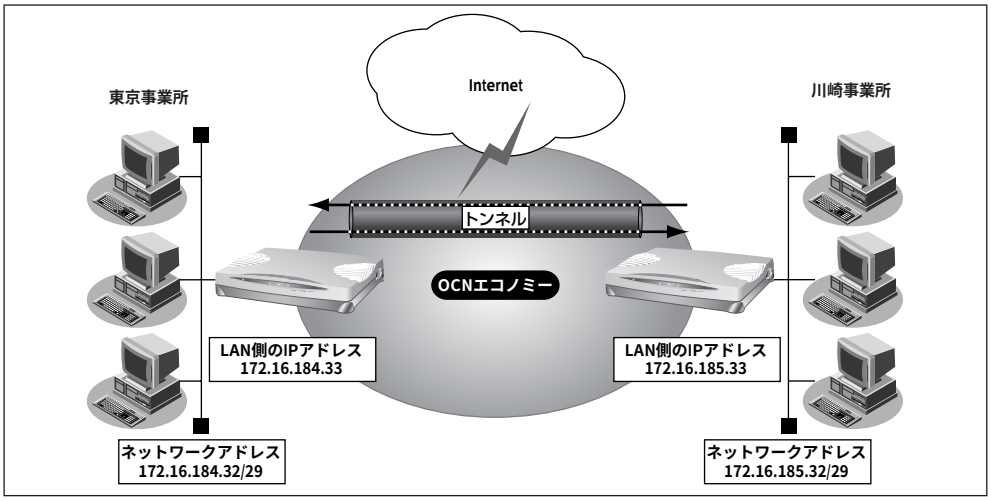
ここでは、「「かんたん設定」で設定する （インターネットへ専用線接続のとき）」（P.85）の設定を参考に東京事業所と川崎事業所の設定が以下のとおり設定されていることを前提とします。

[東京事業所]

- 本装置のIPアドレス　：172.16.184.33
- LAN側のネットワークアドレス／ネットマスク　：172.16.184.32/29

[川崎事業所]

- 本装置のIPアドレス　：172.16.185.33
- LAN側のネットワークアドレス／ネットマスク　：172.16.185.32/29



● 設定条件

- 東京事業所から川崎事業所へのVPN情報
  - 認証アルゴリズム　：hmac-md5
  - 暗号アルゴリズム　：des-cbc
  - PFSグループ　：使用しない
- 川崎事業所から東京事業所へのVPN情報
  - 認証アルゴリズム　：hmac-md5
  - 暗号アルゴリズム　：des-cbc
  - PFSグループ　：使用しない
- IKE情報
  - IKE認証鍵　：12345678901234567890（16進数）
  - IKE認証方法　：shared
  - 暗号アルゴリズム　：des-cbc
  - ハッシュアルゴリズム　：hmac-md5
  - PFSグループ　：modp768

ヒント

◆ PFS グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固することができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

東京事業所の設定をする

1.　詳細設定メニューのルータ設定で、「IPsec 情報」をクリックします。

「IPsec ／ IKE 情報」ページが表示されます。

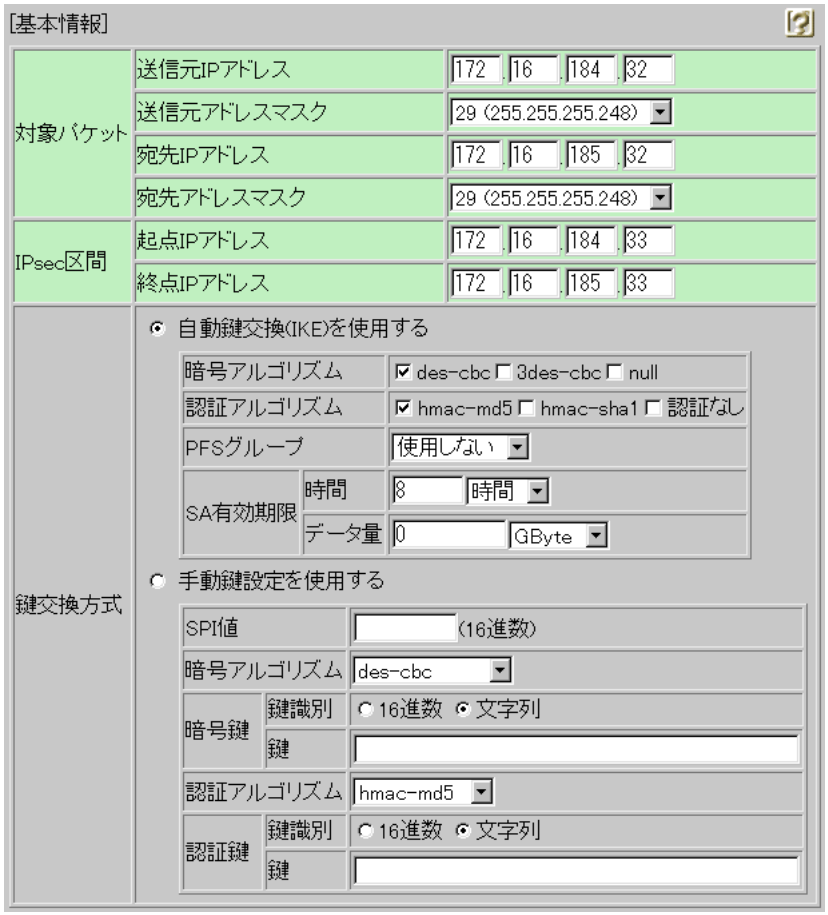
往路（東京事業所→川崎事業所）の VPN 情報を設定する

2.　「IPsec 情報一覧」の［追加］ボタンをクリックします。

「IPsec 情報設定」ページが表示されます。

3.　「基本情報」で以下の項目を指定します。

- 対象パケット
  送信元 IP アドレス　→ 172.16.184.32
  送信元アドレスマスク　→ 29（255.255.255.248）
  宛先 IP アドレス　→ 172.16.185.32
  宛先アドレスマスク　→ 29（255.255.255.248）
- IPsec 区間
  起点 IP アドレス　→ 172.16.184.33
  終点 IP アドレス　→ 172.16.185.33
- 鍵交換方法　→自動鍵交換（IKE）を使用する
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5
  PFS グループ　→使用しない
  SA 有効期限
  時間　→ 8 時間
  データ量　→ 0 GByte



4.　［更新］ボタンをクリックします。

「IPsec／IKE情報」ページに戻ります。

こんな事に気をつけて

- **SA有効期限は時間とデータ量の両方で指定することができますが、両方で指定した場合に、不整合が起きる可能性があるので、時間だけで指定することをお勧めします。また、時間とデータ量の両方で指定する場合には、時間を極端に大きくして、データ量を極端に小さくするような設定を行うと、不整合が起きる可能性があります。**
- **往路／復路のVPN情報の暗号アルゴリズム、認証アルゴリズム、PFSグループ、SA有効期限は同じものを指定する必要があります。**

復路（川崎事業所→東京事業所）のVPN情報を設定する

5.　手順2.～4.を参考に、以下の項目を指定します。

- 対象パケット
  送信元IPアドレス　→172.16.185.32
  送信元アドレスマスク　→29（255.255.255.248）
  宛先IPアドレス　→172.16.184.32
  宛先アドレスマスク　→29（255.255.255.248）
- IPsec区間
  起点IPアドレス　→172.16.185.33
  終点IPアドレス　→172.16.184.33
- 鍵交換方法　→自動鍵交換（IKE）を使用する
  暗号アルゴリズム　→des-cbc
  認証アルゴリズム　→hmac-md5
  PFSグループ　→使用しない
  SA有効期限
  時間　→8時間
  データ量　→0 GByte

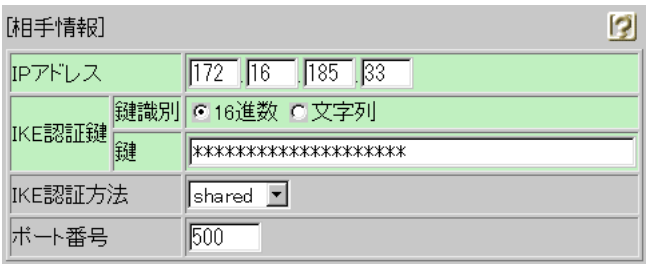
IKE情報を設定する

6.　「IKE情報一覧」の［追加］ボタンをクリックします。

「IKE情報設定」ページが表示されます。

7.　「相手情報」で以下の項目を指定します。

- IPアドレス　→172.16.185.33
- IKE認証鍵
  鍵識別　→16進数
  鍵　→12345678901234567890
- IKE認証方法　→shared
- ポート番号　→500



こんな事に気をつけて

「IKE 情報設定」の「相手情報」で指定する IP アドレスは、「IPsec 情報設定」の「基本情報」で指定する IPsec 区間の相手ゲートウェイの IP アドレスに一致させる必要があります。

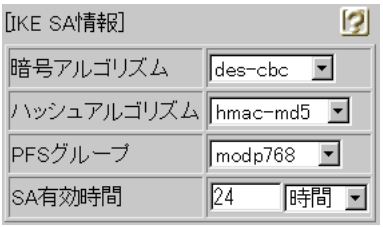
8. 「IKE SA 情報一覧」の［追加］をクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

「IKE SA 情報設定」ページが表示されます。

9. 「IKE SA 情報」で以下の項目を指定します。

- 暗号アルゴリズム　→ des-cbc
- ハッシュアルゴリズム　→ hmac-md5
- PFS グループ　→ modp768
- SA 有効時間　→ 24 時間



10. ［更新］ボタンをクリックします。

「IKE 情報設定」ページに戻ります。

11. ［更新］ボタンをクリックします。

「IPsec ／ IKE 情報」ページに戻ります。

12. ［設定反映］ボタンをクリックします。

設定した内容が有効になります。

川崎事業所の設定をする

「東京事業所の設定をする」を参考に、以下の川崎事業所の設定をします。

往路（川崎事業所→東京事業所）のVPN情報を設定する

- 対象パケット
  送信元IPアドレス　→172.16.185.32
  送信元アドレスマスク　→29（255.255.255.248）
  宛先IPアドレス　→172.16.184.32
  宛先アドレスマスク　→29（255.255.255.248）
- IPsec区間
  起点IPアドレス　→172.16.185.33
  終点IPアドレス　→172.16.184.33
- 鍵交換方法　→自動鍵交換（IKE）を使用する
  暗号アルゴリズム　→des-cbc
  認証アルゴリズム　→hmac-md5
  PFSグループ　→使用しない
  SA有効期限
  時間　→8時間
  データ量　→0 GByte

復路（東京事業所→川崎事業所）のVPN情報を設定する

- 対象パケット
  送信元IPアドレス　→172.16.184.32
  送信元アドレスマスク　→29（255.255.255.248）
  宛先IPアドレス　→172.16.185.32
  宛先アドレスマスク　→29（255.255.255.248）
- IPsec区間
  起点IPアドレス　→172.16.184.33
  終点IPアドレス　→172.16.185.33
- 鍵交換方法　→自動鍵交換（IKE）を使用する
  暗号アルゴリズム　→des-cbc
  認証アルゴリズム　→hmac-md5
  PFSグループ　→使用しない
  SA有効期限
  時間　→8時間
  データ量　→0 GByte

IKE情報を設定する

- IPアドレス　→172.16.184.33
- IKE認証鍵
  鍵識別　→16進数
  鍵　→12345678901234567890
- IKE認証方法　→shared
- ポート番号　→500

IKE SA情報を設定する

- 暗号アルゴリズム　→des-cbc
- ハッシュアルゴリズム　→hmac-md5
- PFSグループ　→modp768
- SA有効時間　→24時間

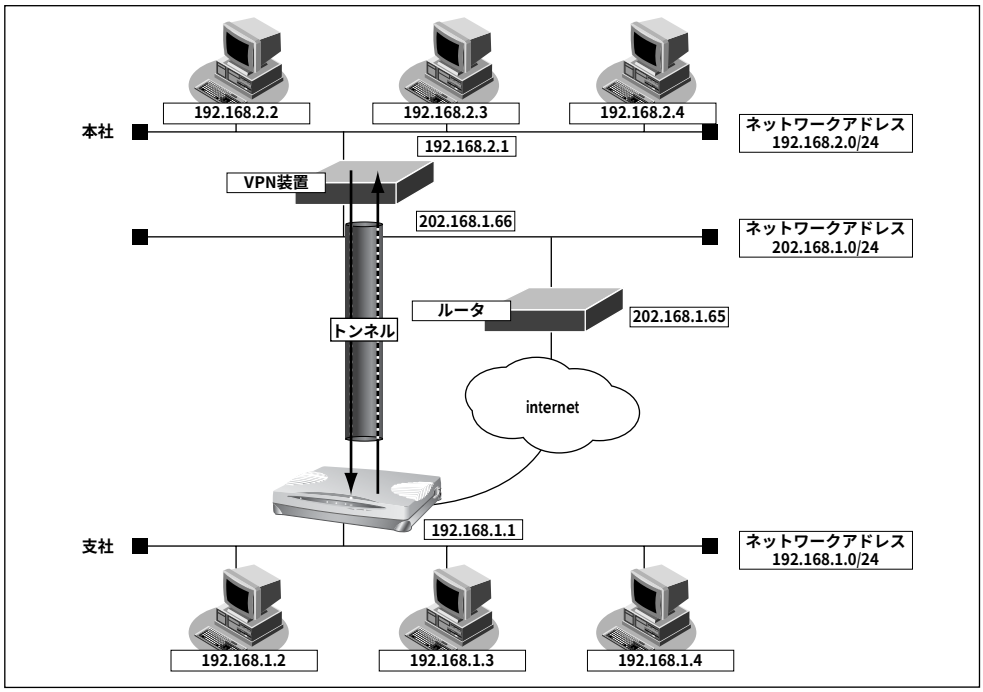
13.　［設定反映］をクリックします。

設定した内容が有効になります。

■ 可変IPアドレスでのVPN

接続するたびにIPアドレスが変わる環境でVPNを構築する場合を例に説明します。

ここでは、回線接続を契機としたIKEネゴシエーション開始動作およびIKEセッション監視機能を使用する構成になっています。



● 設定条件

- ISDN回線を使用する
- 接続先の電話番号　：03-1234-5678
- ユーザ認証ID　：userid（プロバイダから提示された内容）
- ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- 本装置のIPアドレス　：192.168.1.1
- ネットワークアドレス／ネットマスク
  ：192.168.1.0/24
- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IKE（UDP:500番ポート）のプライベートIPアドレス
  ：192.168.1.1
- ESPのプライベートIPアドレス　：192.168.1.1
- 利用方法　：IPsec／IKE（Aggressive Mode）
- 自装置名　：shiten
- IDタイプ　：FQDN

- 本社側エンドポイントアドレス　：202.168.1.66
- 本社のネットワークアドレス／ネットマスク
  ：192.168.2.0/24
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec PFS グループ　：modp768
- IKE 認証鍵　鍵　：123456789a
- IKE 暗号アルゴリズム　：des-cbc
- IKE ハッシュアルゴリズム　：hmac-md5
- IKE PFS グループ　：modp768
- IKE ネゴシエーション開始動作　：対象回線接続契機
- IKE セッション監視
  宛先 IP アドレス　：192.168.2.1
  正常送信間隔　：10秒
  異常送信間隔　：3分

ヒント

◆ PFS グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固することができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは？

ネゴシエーションで使用する自装置を識別する ID の種別です。相手 VPN 装置の設定に合わせます。

かんたん設定で新規のプロバイダとの接続情報を設定する

1.　かんたん設定でインターネットへの「ISDN 接続」をクリックします。

「かんたん設定（インターネットへのISDN 接続）」ページが表示されます。

2.　［必須設定］で以下の項目を指定します。

- 接続先の電話番号　→03-1234-5678
- ユーザ認証 ID　→userid（プロバイダから提示された内容）
- ユーザ認証パスワード　→userpass（プロバイダから提示された内容）

3.　［設定終了］ボタンをクリックします。

再起動後に、通信できる状態になります。

インターネットからIPsec／IKEパケットを受信する設定をする

1.　詳細メニューで、「相手情報」をクリックします。

2.　［ネットワーク情報一覧］でプロバイダとの接続を行うネットワーク情報欄の［修正］をクリックします。

「ネットワーク情報設定」ページが表示されます。

3.　［接続先情報一覧］でプロバイダとの接続を行う接続先情報欄の［修正］をクリックします。

「接続先情報設定」ページが表示されます。

4.　［ダイヤル基本情報］で以下の項目を指定します。

- 接続保持機能　→常時

5.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

6.　［静的NAT情報一覧］で［追加］をクリックします。

「静的NAT情報設定」ページが表示されます。

7.　以下の項目を指定します。

- プライベートIP情報
  IPアドレス　→192.168.1.1
  ポート番号　→その他
  番号指定　→500
- グローバルIP情報
  IPアドレス　→何も設定しない
  ポート番号　→その他
  番号指定　→500
- プロトコル　→udp

8.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

9.　上記の手順の6.～8.を参考に、以下の項目を指定します。

- プライベートIP情報
  IPアドレス　→192.168.1.1
  ポート番号　→すべて
- グローバルIP情報
  IPアドレス　→何も設定しない
  ポート番号　→すべて
- プロトコル　→esp

10.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

VPNの設定をする

1.　詳細メニューで、「相手情報」をクリックします。

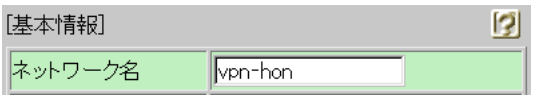
「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］で［追加］をクリックします。

「ネットワーク情報設定」ページが表示されます。

3.　［基本情報］で以下の項目を指定します。

- ネットワーク名　→vpn-hon



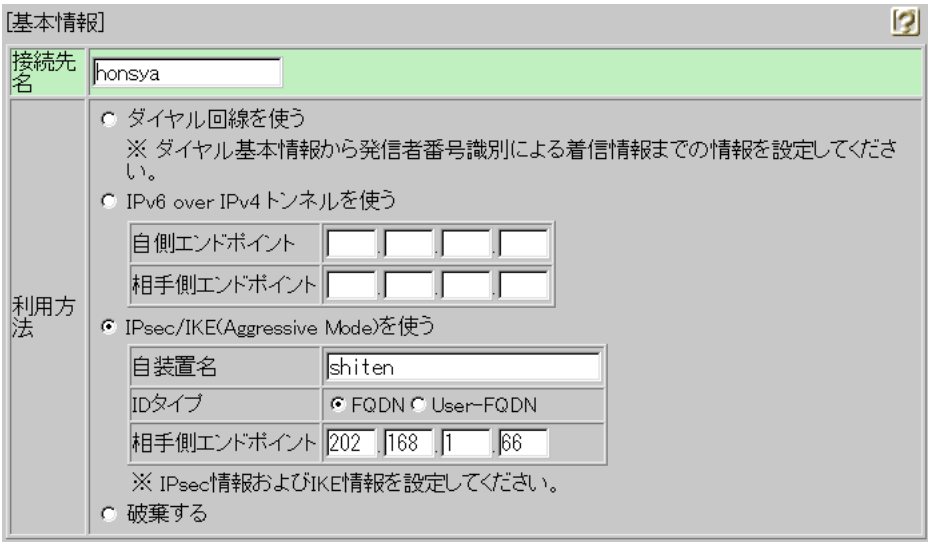
4.　［接続先情報一覧］で［追加］ボタンをクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

「接続先情報設定」ページが表示されます。

5.　［基本情報］で以下の項目を指定します。

- 接続先名　→honsya
- 利用方法　→IPsec／IKE（Aggressive Mode）を使う
  自装置名　→shiten
  IDタイプ　→FQDN
  相手側エンドポイント　→202.168.1.66

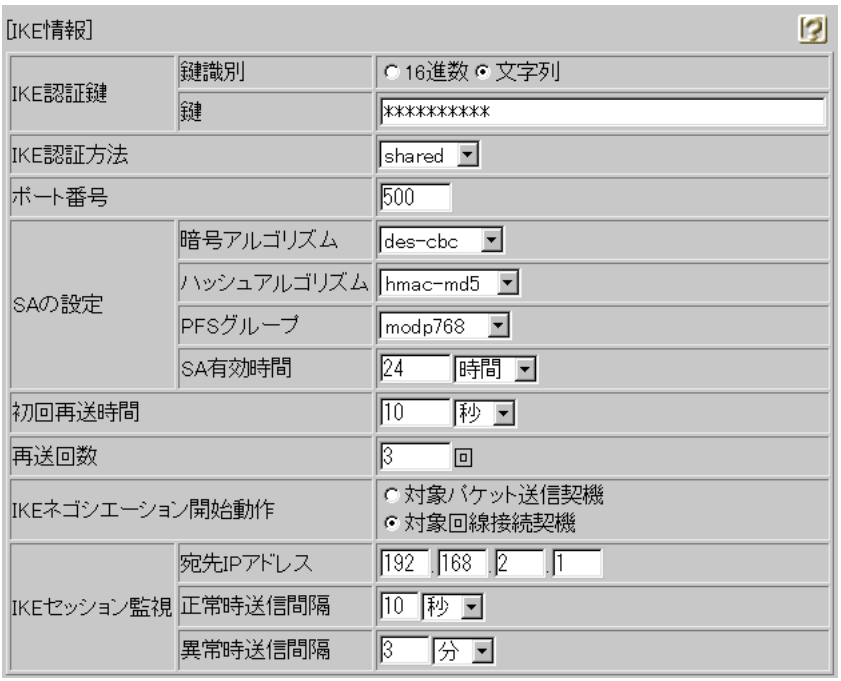


6.　［IPsec 情報］で以下の項目を指定します。

- 対象パケット
  送信元 IP アドレス　→ 192.168.1.0
  送信元アドレスマスク　→ 24（255.255.255.0）
  宛先 IP アドレス　→何も指定しない
  宛先アドレスマスク　→ 0（0.0.0.0）
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5
  PFS グループ　→ modp768

7.　［IKE 情報］で以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→123456789a
- SAの設定
  暗号アルゴリズム　→des-cbc
  ハッシュアルゴリズム　→hmac-md5
  PFS グループ　→modp768
- IKE ネゴシエーション開始動作　→対象回線接続契機
- IKE セッション監視
  宛先 IP アドレス　→192.168.2.1
  正常送信間隔　→10 秒
  異常時送信間隔　→3 分



こんな事に気をつけて

- **認証や暗号用の鍵には、文字列か数値（16 進数）を使用することができます。鍵として数値を入力したつもりでも、鍵識別で文字列を指定していると、文字列として認識されてしまうために、鍵が一致しない原因になります。**
- **IKE セッション監視の宛先 IP アドレスは、［IPsec 情報］の“対象パケット”に含まれる IP アドレスを指定してください。また、指定先の IP アドレスは、相手 IPsec ゲートウェイの IPsec 対象パケット範囲を指定することをお勧めします。**
- **IKE セッション監視の宛先 IP アドレスは常時運転している IPsec 対象の装置を指定してください。宛先 IP アドレスに相手 IKE サーバとは異なる装置を指定した場合、宛先 IP アドレスからの応答が受信できなくなると相手 IKE サーバが生存していても IPsec/IKE SA は解放されます。このため通信が不安定になることがあります。**

- **IKEセッション監視機能を使用すると、本装置から宛先IPアドレスのホストに対してICMP ECHOパケットを定期的に送出します。そのため、定額制でない回線を使用している場合は、超過課金の原因となることがあります。このような環境では、IKEセッション監視機能を使用しないでください。**

8.　［更新］ボタンをクリックします。

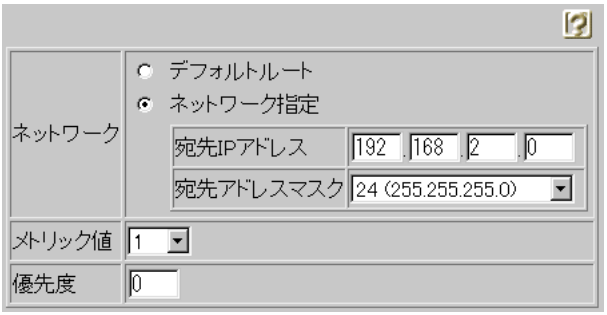
「ネットワーク情報設定」ページに戻ります。

9.　［スタティックルーティング情報一覧］で［追加］ボタンをクリックします。

「ルーティング情報設定」ページが表示されます。

10.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  宛先IPアドレス　→192.168.2.0
  宛先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1



11.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

12.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

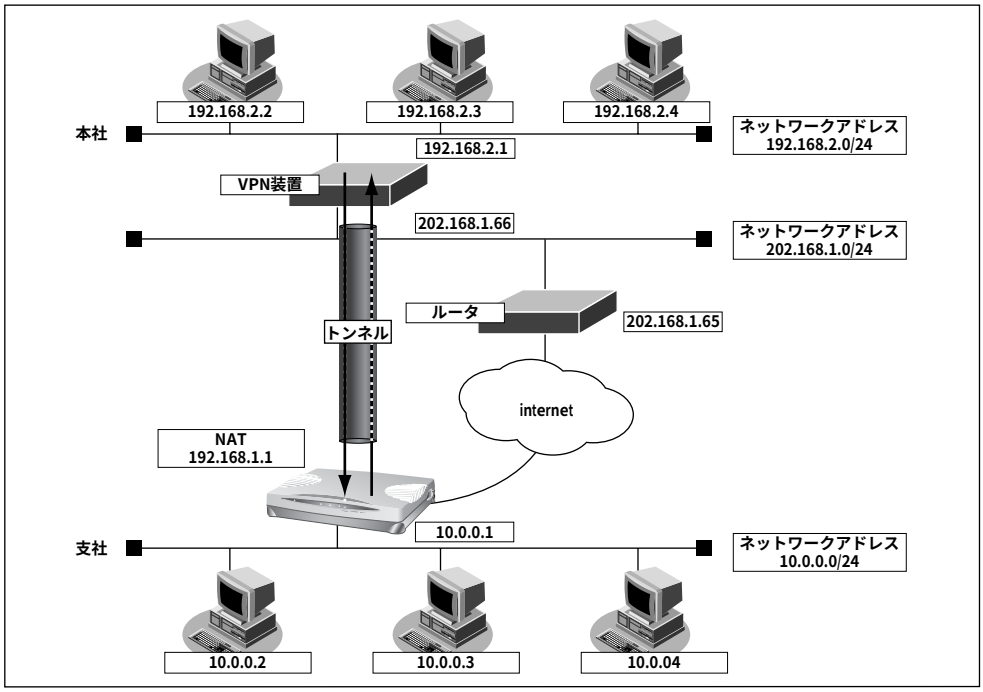
13.　［更新］ボタンをクリックします。

14.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

■ NAT変換後にVPN

可変IPアドレスのVPNから回線接続を契機としたIKEネゴシエーション開始動作およびIKEセッション監視機能を除いた環境です。ただし、支店内はローカルなIPネットワークを組んでいるために、本社と通信する場合はNAT変換を必要とする場合の例を説明します。



● 設定条件

- ISDN回線を使用する
- 接続先電話番号　：03-1234-5678
- ユーザ認証ID　：userid（プロバイダから提示された内容）
- ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- 本装置のIPアドレス　：10.0.0.1
- ネットワークアドレス／ネットマスク
  ：10.0.0.0/24
- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec前に割り当てるIPアドレス　：192.168.1.1
- IKE（UDP:500番ポート）のプライベートIPアドレス
  ：10.0.0.1
- ESPのプライベートIPアドレス　：10.0.0.1
- 利用方法　：IPsec／IKE（Aggressive Mode）
- 自装置名　：shiten

- IDタイプ　：FQDN
- 本社側エンドポイントアドレス　：202.168.1.66
- 本社のネットワークアドレス／ネットマスク　：192.168.2.0/24
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec PFSグループ　：modp768
- IKE 認証鍵　鍵　：123456789a
- IKE 暗号アルゴリズム　：des-cbc
- IKE ハッシュアルゴリズム　：hmac-md5
- IKE PFS グループ　：modp768

ヒント

◆ PFSグループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固することができます。

◆ IKEとは？

自動鍵交換を行うためのプロトコルです。

◆ IDタイプとは？

ネゴシエーションで使用する自装置を識別するIDの種別です。相手VPN装置の設定に合わせます。

かんたん設定で新規のプロバイダとの接続情報を設定する

1.　かんたん設定でインターネットへの「ISDN接続」をクリックします。

「かんたん設定（インターネットへのISDN接続）」ページが表示されます。

2.　［必須設定］で以下の項目を指定します。

- 接続先の電話番号　→03-1234-5678
- ユーザ認証ID　→userid（プロバイダから提示された内容）
- ユーザ認証パスワード　→userpass（プロバイダから提示された内容）

3.　［設定終了］ボタンをクリックします。

再起動後に、通信できる状態になります。

インターネットからIPsec／IKEパケットを受信する設定をする

1.　詳細メニューで、「相手情報」をクリックします。

「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］でプロバイダとの接続を行うネットワーク情報欄の［修正］をクリックします。

「ネットワーク情報設定」ページが表示されます。

3.　［静的NAT情報一覧］で［追加］をクリックします。

「静的NAT情報設定」ページが表示されます。

4.　以下の項目を指定します。

- プライベートIP情報
  IPアドレス　→10.0.0.1
  ポート番号　→その他
  番号指定　→500
- グローバルIP情報
  IPアドレス　→何も設定しない
  ポート番号　→その他
  番号指定　→500
- プロトコル　→udp

5.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

6.　上記の手順の3.～5.を参考に、以下の項目を指定します。

- プライベートIP情報
  IPアドレス　→10.0.0.1
  ポート番号　→すべて
- グローバルIP情報
  IPアドレス　→何も設定しない
  ポート番号　→すべて
- プロトコル　→esp

7.　［更新］ボタンをクリックします。

「相手情報設定」ページに戻ります。

VPNの設定をする

1.　詳細メニューで、「相手情報」をクリックします。

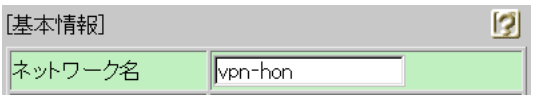
「相手情報設定」ページが表示されます。

2.　［ネットワーク情報一覧］で［追加］をクリックします。

「ネットワーク情報設定」ページが表示されます。

3.　［基本情報］で以下の項目を指定します。

- ネットワーク名　→vpn-hon



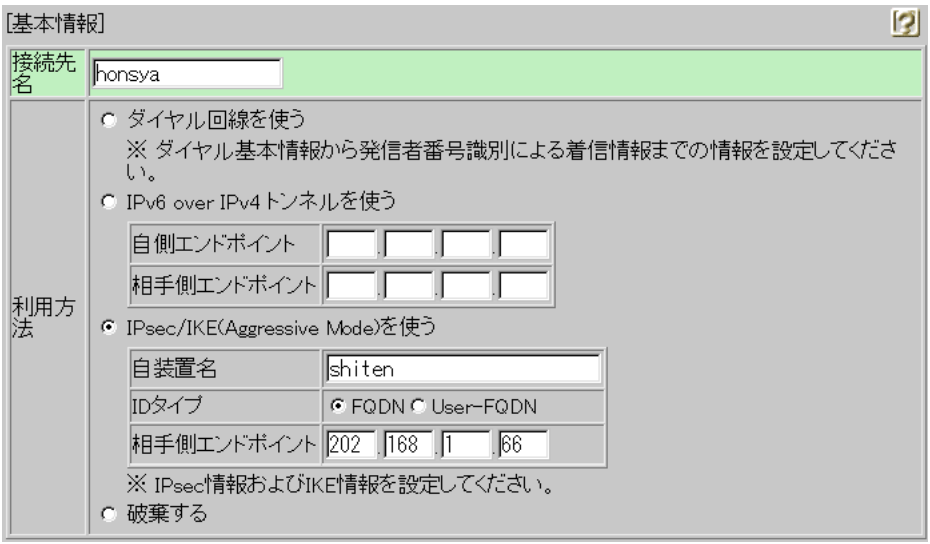
4.　［接続先情報一覧］で［追加］ボタンをクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

「接続先情報設定」ページが表示されます。

5.　［基本情報］で以下の項目を指定します。

- 接続先名　→honsya
- 利用方法　→IPsec／IKE（Aggressive Mode）を使う
  自装置名　→shiten
  IDタイプ　→FQDN
  相手側エンドポイント　→202.168.1.66



6.　［IPsec 情報］で以下の項目を指定します。

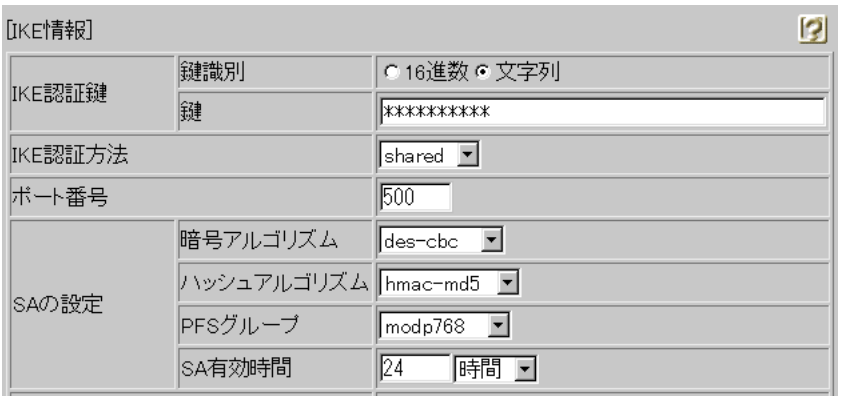
- 対象パケット
  送信元 IP アドレス　→ 192.168.1.0
  送信元アドレスマスク　→ 24（255.255.255.0）
  宛先 IP アドレス　→何も指定しない
  宛先アドレスマスク　→ 0（0.0.0.0）
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5
  PFS グループ　→ modp768

こんな事に気をつけて

NAT を使用した場合は、送信元 IP アドレスに NAT 変換後のアドレスを設定します。

7.　［IKE 情報］で以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ 123456789a
- SAの設定
  暗号アルゴリズム　→ des-cbc
  ハッシュアルゴリズム　→ hmac-md5
  PFS グループ　→ modp768



こんな事に気をつけて

認証や暗号用の鍵には、文字列か数値（16進数）を使用することができます。鍵として数値を入力したつもりでも、鍵識別で文字列を指定していると、文字列として認識されてしまうために、鍵が一致しない原因になります。

8.　［更新］ボタンをクリックします。

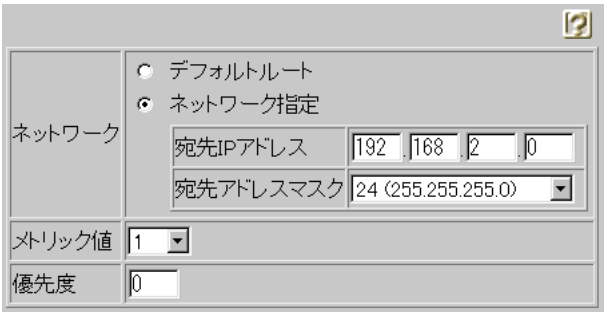
「ネットワーク情報設定」ページに戻ります。

9.　［スタティックルーティング情報一覧］で［追加］ボタンをクリックします。

「ルーティング情報設定」ページが表示されます。

10.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  宛先IPアドレス　→192.168.2.0
  宛先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1



11.　[更新] ボタンをクリックします。

「ネットワーク情報設定」ページに戻ります。

12.　[NAT 情報] で以下の項目を指定します。

- NATの使用　→マルチNAT
- グローバルアドレス　→192.168.1.1
- アドレス個数　→1個

こんな事に気をつけて

NAT 変換には、IPsec の前の変換と IPsec の後の変換があります。IPsec 前に変換する場合は、IPsec 用の「ネットワーク情報」で設定します。IPsec 後に変換する場合は、プロバイダ接続用の「ネットワーク情報」で設定します。

13.　[更新] ボタンをクリックします。

「相手情報設定」ページに戻ります。

14.　[更新] ボタンをクリックします。

15.　[設定反映] ボタンをクリックします。

設定した内容が有効になります。

セキュリティログを採取する

本装置のセキュリティログは、表示メニューで確認することができます。そのためには、あらかじめ採取するログを設定しておく必要があります。

ここではセキュリティログを採取するための設定方法について説明します。

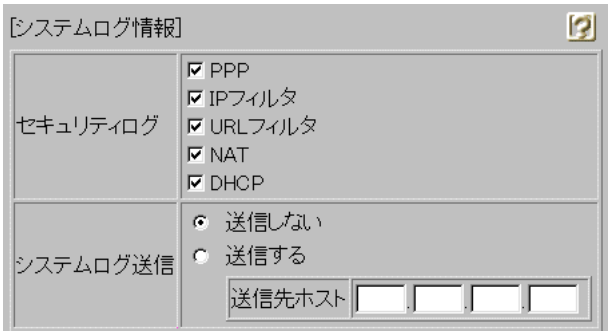
☛ 参照　ログの種類と詳細→「表示メニューを使う」（P.611）

1.　詳細設定メニューのルータ設定で「装置情報」をクリックします。

「装置情報設定」ページが表示されます。

2.　［システムログ情報］で以下の項目の中から採取するセキュリティログをチェックします。

- セキュリティログ　→PPP、IPフィルタ、URLフィルタ、NAT、DHCP



3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

留守モードの動作を設定する

本装置では、あらかじめ「留守モード情報」に留守（外出）中の動作を設定しておくことにより、在宅時の設定（留守モードOFF）と留守中の設定（留守モードON）をかんたんに切り替えることができます。留守モード中の動作は以下の項目から指定します。

- 留守中は、スタンバイモードで動作する
- 留守中は、メールチェックで取得したメールを転送する
- 留守中は、メールチェックで取得したメールの一覧をメールで送信する
- 留守中は、アナログポートごとの着信履歴をメールで送信する
- 留守中は、アナログの着信転送または疑似着信転送を行う
- 留守中は、アナログの留守確認機能を使用する
- 留守モードを解除するときに、メールチェックを行う（メール転送およびメール一覧送信は行いません）

こんな事に気をつけて

- **スタンバイモードの設定以外は、「留守モード情報」とは別にそれぞれの機能を使用するための設定が必要です。**

☛ 参照 「メール転送機能」（P.541）、「メール一覧送信機能」（P.544）、「TEL メール機能」（P.547）、「フレックスホンを使う」（P.376）、「留守状態を確認する（無課金）」（P.425）

- **なお、留守モードON／OFFの切り替えを行うには、以下の方法があります。**
  - **本装置の「操作メニュー」の「留守モード切替え」から切り替える。**
  - **アナログポートに接続された電話機から切り替える。**
  - **スケジュール機能を使用して切り替える。**

☛ 参照 「留守モードのON／OFF を設定する」（P.609）、「留守モードを設定する」（P.418）、「スケジュール機能を使う」（P.551）

■ 留守モードの動作を設定する

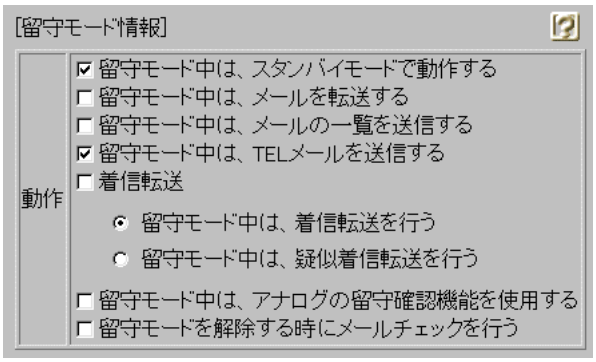
ここでは、留守モード中はスタンバイモードで動作し、かつTELメールを送信する設定を行う場合を例に説明します。

1.　詳細設定メニューのルータ設定で「装置情報」をクリックします。

「装置情報設定」ページが表示されます。

2.　［留守モード情報］で以下の項目を指定します。

- 動作　→留守モード中は、スタンバイモードで動作する、留守モード中は、TELメールを送信する



3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

VRRP機能を使う

VRRP機能は2つ以上のルータがグループを形成し、1台のルータ（仮想ルータ）のように動作します。グループ内の各ルータには優先度が設定されており、その優先度に従ってマスタルータ（実際にルーティングを行う装置）とバックアップルータ（マスタルータで異常を検出した時にルーティング処理を引き継ぐ装置）を決定します。

本装置には、以下のVRRP機能があります。

- 簡易ホットスタンバイ機能
  動的に経路制御（RIPなど）できない端末から、別のネットワークへの通信に使用しているルータがなんらかの理由で中継できなくなった場合、自動でほかのルータが通信をバックアップします。
- クラスタリング機能
  VRRPのグループを複数設定することで、通信の負荷分散と冗長構成を実現します。

こんな事に気をつけて

- VRRP機能はIPv4だけサポートしています。
- 同一のインタフェースに定義可能なVRRPグループは最大2つまでです。
- VRRPグループのグループIDは、同一装置内で重複しないように設定してください。
- VRRPグループに割り当てる仮想IPアドレスと実IPアドレスは、必ず同じサブネットになるよう設定することをお勧めします。
- 同一グループには最大2台まで属することができます。
- 同一グループとして使用できるルータはVRRPをサポートするSi-Rシリーズだけです。
- 優先度に“マスタ”を定義した場合は、バックアップルータの仮想ルータのIPアドレスにマスタルータの実IPアドレスを設定してください。
- 簡易ホットスタンバイ機能を使用する場合、ブリッジ機能と併用することはできません。また、ルータと接続するHUBは、STP機能を無効にしてください。STP機能を有効にすると、簡易ホットスタンバイで連携している装置と無関係なケーブルの抜き差しによって、故障を検出することがあります。
- VRRP機能により切り替えが発生したあと、通信が可能となるまでの時間は使用している経路制御プロトコルに依存します。
- 本装置の電源の投入、マスタルータでの動的定義変更、または装置リセットを実行した場合、バックアップルータがマスタルータとなることがあります。プリエンプトモードがonの場合は自動で切り戻りますが、プリエンプトモードがoffの場合は、操作メニューの「VRRP手動切り戻し」で切り戻しを行う必要があります。
- 優先度の値が大きい方が優先的にマスタルータとなります。
- LANに接続される装置はデフォルトルートとして仮想IPアドレスを設定してください。
- ルータに設定されるIPアドレスと仮想IPアドレスを同一にした場合、そのIPアドレスで装置にアクセスすることはできなくなることがありますので、異なるIPアドレスを設定することをお勧めします。なお、ルータに設定されるIPアドレスと仮想IPアドレスを同一にする場合は、必ず、そのルータの優先度をマスタに設定してください（優先度としてマスタを設定した場合、仮想IPアドレスは設定できません）。
- VRRP機能とIPsec/IKE機能を同時に使用する場合、マスタルータとバックアップルータは同じIPsecトンネル（対象パケットとトンネル出口のIPアドレスが同じ）を設定することができません。同じIPsecトンネルを設定した場合、相手装置からの送信パケットを正しいルータで受信できません。また、自動鍵交換については、仮想IPアドレスを使用することはできません。

- VRRP機能では、VRRP-ADメッセージに以下のパケットを使用します。IPフィルタ設定時には、このパケットを遮断しないように設定する必要があります。
  宛先IPアドレス　　：224.0.0.18
  プロトコル番号　　：112
- マルチホーミング機能と併用することはできません。
- トリガ機能を使用する場合はVRRPグループの優先度に"マスタ"を指定しないでください。
- 特定ノードダウントリガ機能を使用する場合は、本装置から宛先IPアドレスに対してICMP ECHOパケットを定期的に送出します。そのため、定額制でない回線を使用している場合は超過課金の原因となることがあります。このような環境では、特定ノードダウントリガ機能を使用しないでください。
- インタフェースダウントリガ機能を使用する場合、HUBであるLANインタフェースではダウンを検出しないため、インタフェーストリガイベントは無効となります。
- VRRP機能を使用している場合、マスタルータは、VRRP-ADメッセージ（VRRP Advertisement message：VRRP広報メッセージ）をバックアップルータに定期的に送信します。バックアップルータは、マスタルータからのVRRP-ADメッセージを受信することで、マスタルータが正常に動作していると判断します。バックアップルータは、VRRP-ADメッセージを最後に受信してから一定時間内に次のVRRP-ADメッセージが受信できなかった場合、マスタルータがダウンしたと判断し、新たなマスタルータとして動作します。
- ルートダウントリガで指定した宛先経路に対してスタティックルートが存在する場合は、ルートダウントリガは発生しません。なお、ルートダウントリガで指定した宛先経路とまったく同じ経路情報でなくても、デフォルトルート、または、よりネットワークマスクの小さい同一ネットワークの経路情報が存在した場合は、ルートダウントリガは発生しません。

■ 簡易ホットスタンバイ機能

本装置では、2台のルータを組み合わせることで簡易ホットスタンバイによる信頼性の高い通信を実現できます。

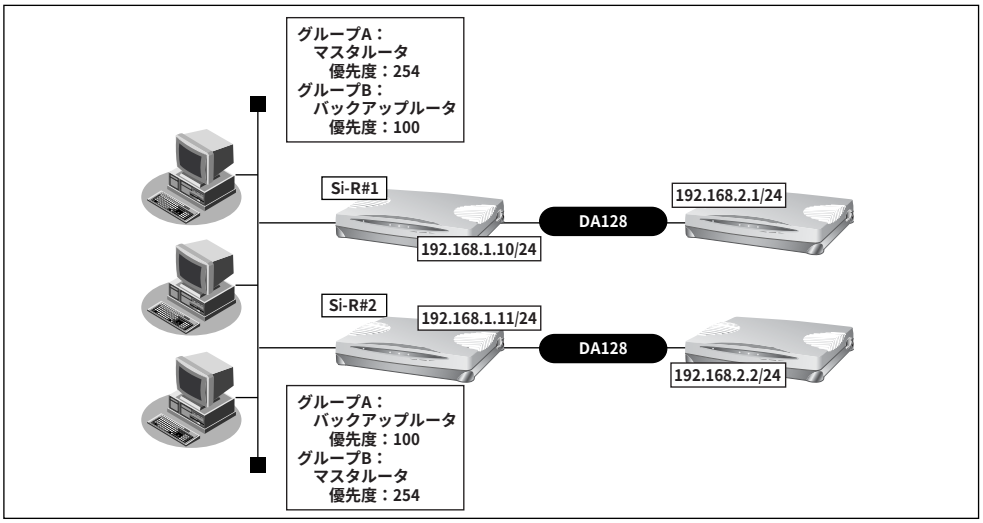
事業所LANを専用線で接続して、ホットスタンバイを構成する場合を例に説明します。

ここでは、「「かんたん設定」で設定する （オフィスへ専用線接続のとき)」（P.95）の設定を参考にWANとの接続が設定されていることを前提とします。

こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。

☛ 参照 「ご購入時の状態に戻すには」（P.665）



● 設定条件

- 専用線（128kbps）を使用する
- 故障発生後の切り戻しを手動で行う
- マスタルータはWAN側のルータを特定ノードダウントリガにより監視する

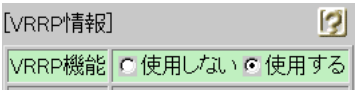
マスタルータの設定

1.　詳細設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報設定」ページが表示されます。

2.　［VRRP 情報］で以下の項目を指定します。

- VRRP情報　→使用する



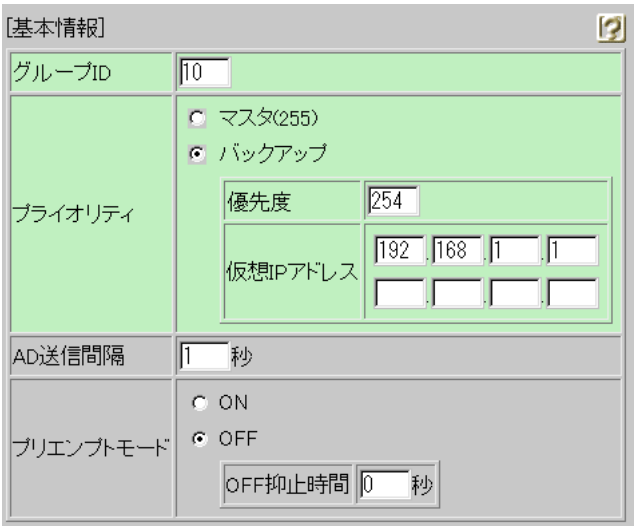
3.　［VRRP グループ情報一覧］の［修正］ボタンをクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

「VRRP グループ情報設定」ページが表示されます。

4.　［基本情報］で以下の項目を指定します。

- グループ ID　→10
- プライオリティ　→バックアップ
- 優先度　→254
- 仮想 IP アドレス　→（上段に）192.168.1.1
- プリエンプトモード　→off



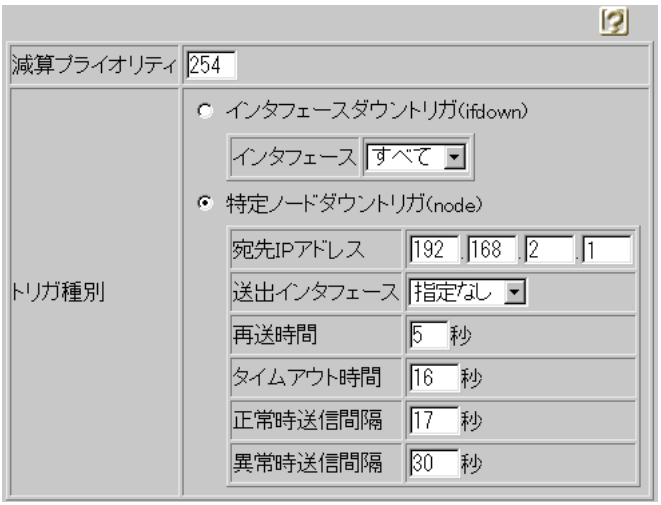
5.　［トリガ情報一覧］の［追加］をクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

「VRRP トリガ情報設定」ページが表示されます。

6.　以下の項目を指定します。

- 減算プライオリティ　→254
- トリガ種別　→特定ノードダウントリガ
- 宛先IPアドレス　→192.168.2.1
- 送出インタフェース　→指定なし
- 再送間隔　→5秒
- タイムアウト時間　→16秒
- 正常時送信間隔　→17秒
- 異常時送信間隔　→30秒



7.　[更新] ボタンをクリックします。

「VRRP グループ情報設定」ページに戻ります。

8.　[更新] ボタンをクリックします。

「LAN 情報設定」ページに戻ります。

9.　[更新] ボタンをクリックします。

10.　[設定反映] ボタンをクリックします。

設定した内容が有効になります。

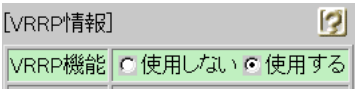
バックアップルータの設定

1.　詳細設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報設定」ページが表示されます。

2.　［VRRP 情報］で以下の項目を指定します。

- VRRP情報　→使用する

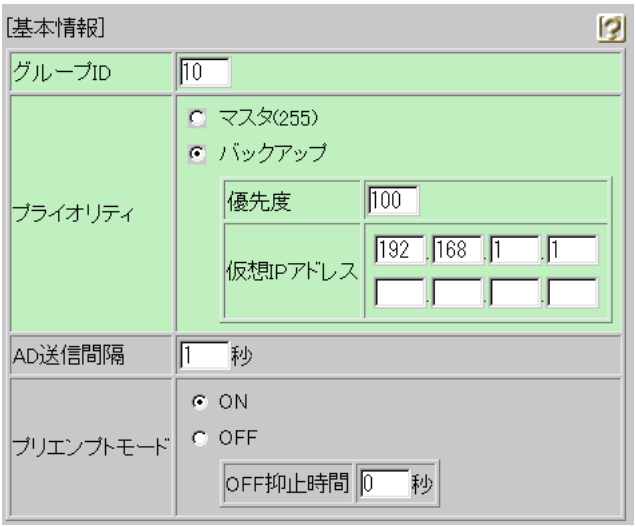


3.　［VRRP グループ情報一覧］の［修正］ボタンをクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。
「VRRP グループ情報設定」ページが表示されます。

4.　［基本情報］で以下の項目を指定します。

- グループ ID　→10
- プライオリティ　→バックアップ
- 優先度　→100
- 仮想 IP アドレス　→（上段に）192.168.1.1
- プリエンプトモード　→on



5.　［更新］ボタンをクリックします。

「LAN 情報設定」ページに戻ります。

6.　［更新］ボタンをクリックします。

7.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

■ クラスタリング機能

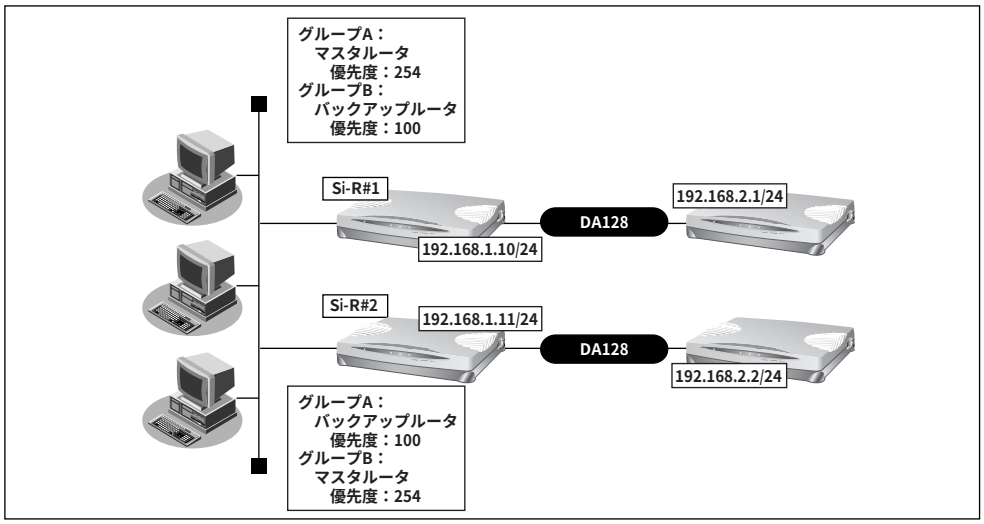
本装置では、2台のルータに複数のグループIDを設定することで、信頼性を高めると同時に通信の負荷分散を実現できます。

事務所LANを専用線で接続する場合を例に説明します。ここでは、「「かんたん設定」で設定する （オフィスへ専用線接続のとき)」（P.95）の設定を参考にWANとの接続が設定されていることを前提とします。

こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。

☛ 参照 「ご購入時の状態に戻すには」（P.665）



[グループA]

- グループID　：10
- 仮想IPアドレス　：192.168.1.1

[グループB]

- グループID　：11
- 仮想IPアドレス　：192.168.1.2

● 設定条件

- 専用線（128kbos）を使用する
- 故障発生後の切り戻しを手動で行う
- マスタルータはWAN側のルータを特定ノードダウントリガにより監視する

こんな事に気をつけて

クラスタ機能を有効に利用するには、PC からのトラフィック量に応じて、PC 側で設定するデフォルトルートの定義を適切に分散する必要があります。

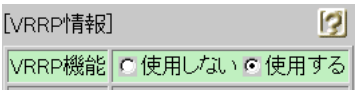
マスタルータの設定

1.　詳細設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報設定」ページが表示されます。

2.　［VRRP 情報］で以下の項目を指定します。

- VRRP 情報　→使用する



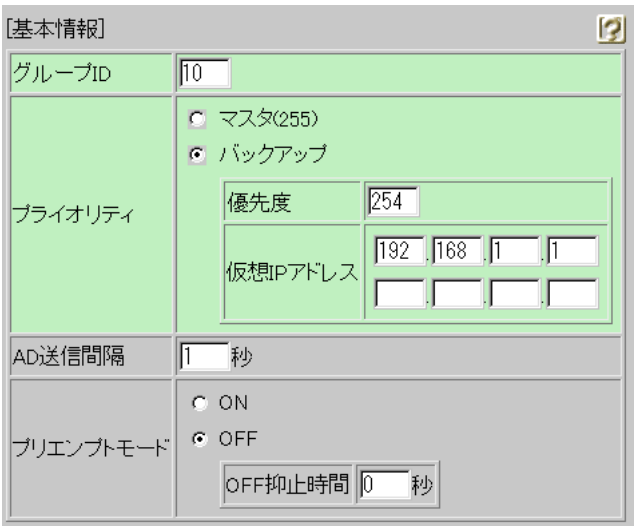
3.　［VRRP グループ情報一覧］の［修正］ボタンをクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

「VRRP グループ情報設定」ページが表示されます。

4.　［基本情報］で以下の項目を指定します。

- グループ ID　→10
- プライオリティ　→バックアップ
- 優先度　→254
- 仮想 IP アドレス　→（上段に）192.168.1.1
- プリエンプトモード　→off



5.　［トリガ情報一覧］の［追加］をクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

「VRRP トリガ情報設定」ページが表示されます。

6.　以下の項目を指定します。

- 減算プライオリティ　→254
- トリガ種別　→特定ノードダウントリガ
- 宛先 IP アドレス　→192.168.2.1
- 送出インタフェース　→指定なし
- 再送間隔　→5 秒
- タイムアウト時間　→16 秒
- 正常時送信間隔　→17 秒
- 異常時送信間隔　→30 秒

7.　［更新］ボタンをクリックします。

「VRRP グループ情報設定」ページに戻ります。

8.　［更新］ボタンをクリックします。

「LAN 情報設定」ページに戻ります。

9.　手順 3.～4. を参考に、以下の項目を設定します。

- グループ ID　→11
- プライオリティ　→バックアップ
- 優先度　→100
- 仮想 IP アドレス　→（上段に）192.168.1.2
- プリエンプトモード　→on

10.　［更新］ボタンをクリックします。

「LAN情報設定」ページに戻ります。

11.　［更新］ボタンをクリックします。

12.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

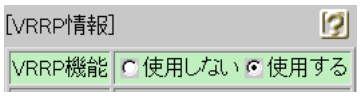
バックアップルータの設定

1.　詳細設定メニューのルータ設定で「LAN情報」をクリックします。

「LAN情報設定」ページが表示されます。

2.　［VRRP情報］で以下の項目を指定します。

- VRRP情報　→使用する



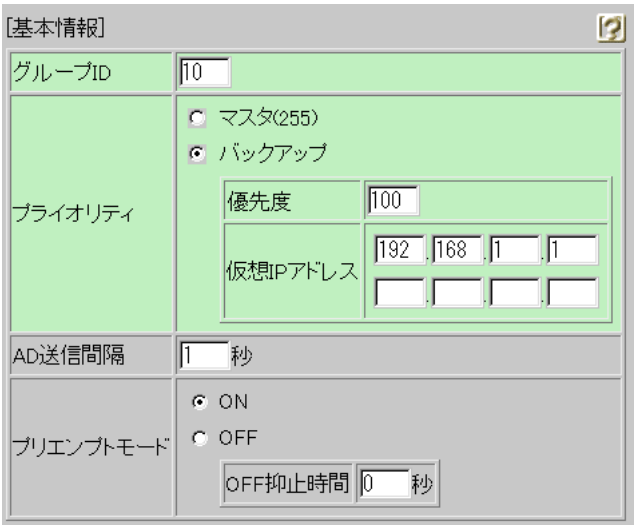
3.　［VRRPグループ情報一覧］の［修正］ボタンをクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

「VRRPグループ情報設定」ページが表示されます。

4.　［基本情報］で以下の項目を指定します。

- グループID　→10
- プライオリティ　→バックアップ
- 優先度　→100
- 仮想IPアドレス　→（上段に）192.168.1.1
- プリエンプトモード　→on



5.　［更新］ボタンをクリックします。

「LAN情報設定」ページに戻ります。

6.　手順3.～4.を参考に、以下の項目を設定します。

- グループID　→11
- プライオリティ　→バックアップ
- 優先度　→254
- 仮想IPアドレス　→（上段に）192.168.1.2
- プリエンプトモード　→off

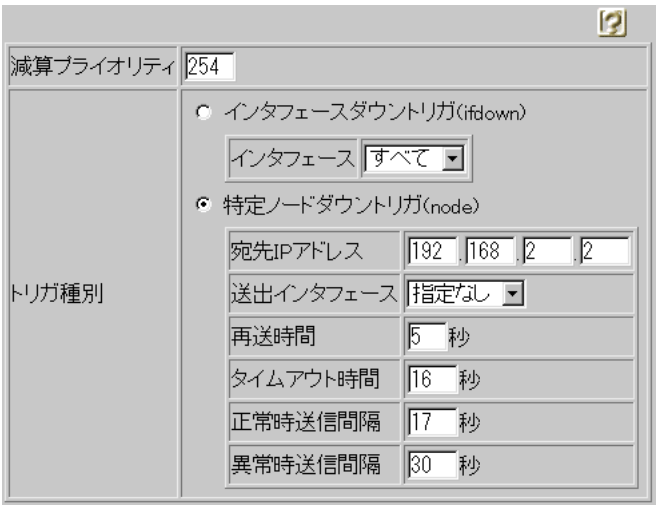
7.　［トリガ情報一覧］の［追加］をクリックします。

「このページの情報が変更されています。更新しますか？」というメッセージが表示されたら［OK］ボタンをクリックします。

「VRRPトリガ情報設定」ページが表示されます。

8.　以下の項目を指定します。

- 減算プライオリティ　→254
- トリガ種別　→特定ノードダウントリガ
- 宛先IPアドレス　→192.168.2.2
- 送出インタフェース　→指定なし
- 再送間隔　→5秒
- タイムアウト時間　→16秒
- 正常時送信間隔　→17秒
- 異常時送信間隔　→30秒



9.　[更新] ボタンをクリックします。

「VRRP グループ情報設定」ページに戻ります。

10.　[更新] ボタンをクリックします。

「LAN 情報設定」ページに戻ります。

11.　[更新] ボタンをクリックします。

12.　[設定反映] ボタンをクリックします。

設定した内容が有効になります。

第7章　運用管理とメンテナンス

7

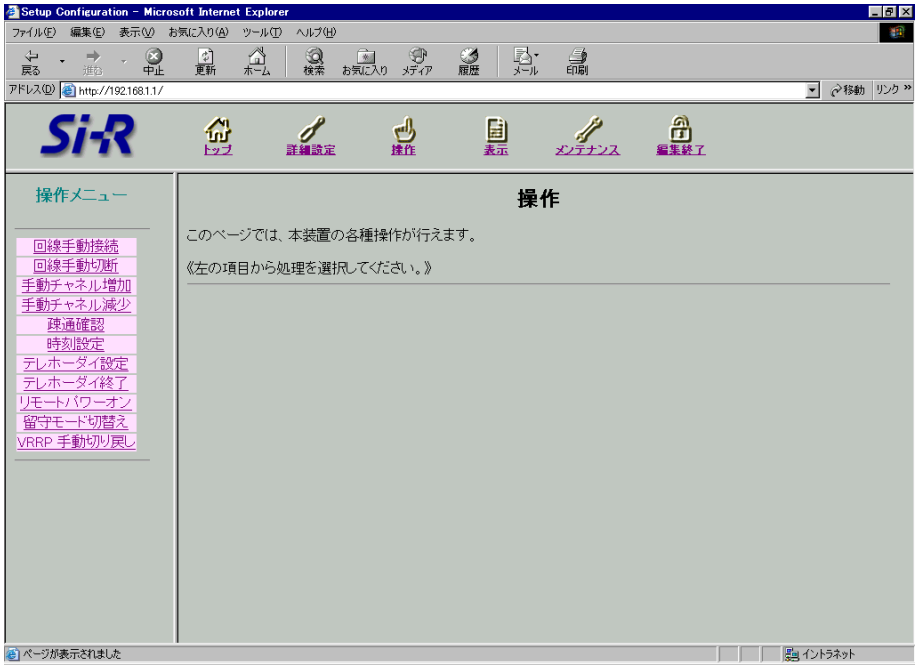
この章では、
本装置で、ISDN 回線の運用状況などの管理や確認を行う方法を説明します。

操作メニューを使う

操作メニューでは、回線の手動接続／切断、チャネル数の増加／減少、疎通確認、時刻設定、テレホーダイ設定／テレホーダイ終了、リモートパワーオン、留守モード切替え、VRRP手動切り戻しができます。

■ 操作メニューを表示する

本装置のトップページで、画面上部の［操作］アイコンをクリックすると、操作メニューが表示されます。



■ 手動で回線を接続する／切断する

接続先を指定して、手動で回線の接続／切断ができます。

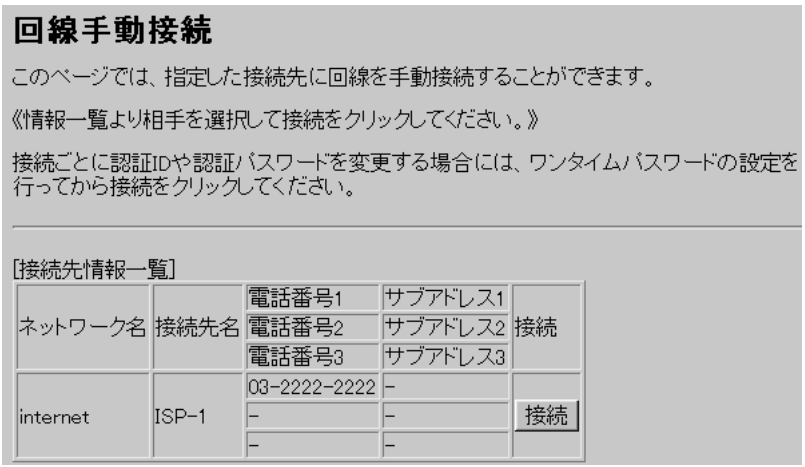
こんな事に気をつけて

回線手動接続／切断ページでは実行結果を確認できません。「表示メニュー」の「回線接続状況」で確認してください。回線手動接続の接続先情報一覧には、接続先の相手やトンネルのエンドポイントの相手など、すべての接続先情報が表示されますが、未接続状態の相手以外に対する要求は接続動作を行いません。

回線を接続する

1.　操作メニューで「回線手動接続」をクリックします。

「回線手動接続」ページが表示されます。



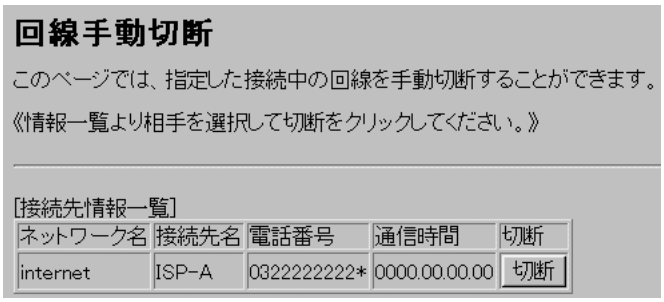
2.　［接続先情報一覧］で接続先の欄の［接続］ボタンをクリックします。

回線接続のメッセージが表示されます。

回線を切断する

1.　操作メニューで「回線手動切断」をクリックします。

「回線手動切断」ページが表示されます。



2.　［接続先情報一覧］で回線を切断する接続先の欄の［切断］ボタンをクリックします。

回線切断のメッセージが表示されます。

■ 手動でチャネルを増やす／減らす

回線接続中に、通信に使用するBチャネルの数を手動で増減できます。

こんな事に気をつけて

プロバイダがMPに対応している場合だけ、この機能を利用できます。

1.　チャネルの数を増加する場合は、操作メニューで「手動チャネル増加」をクリックします。

「チャネル数の増加要求を発行しました。」というメッセージが表示されます。

チャネルの数を減らす場合は、操作メニューで「手動チャネル減少」をクリックします。

「チャネル数の減少要求を発行しました。」というメッセージが表示されます。

■ ネットワークの接続を確認する

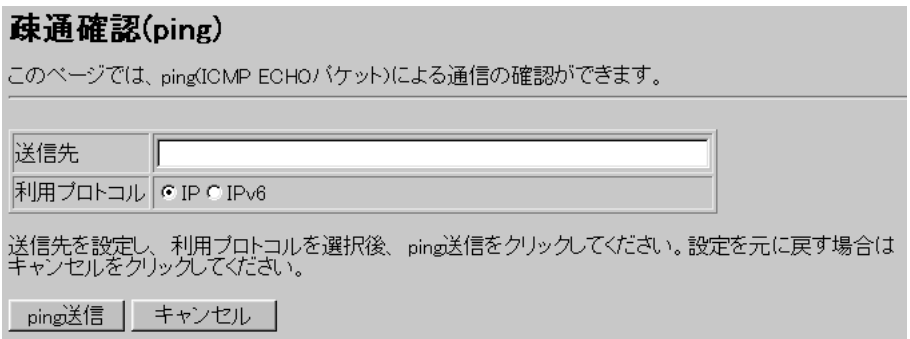
pingコマンドを使って、IP接続が成立しているかどうか確認できます。

こんな事に気をつけて

- **ping実行中は、通話料金がかかります。**
- **かんたんフィルタがかかっているときは、pingを送信できないので応答はありません。**
- **かんたんフィルタを使用している場合、ISDN回線は接続されません。**

1.　操作メニューで「疎通確認」をクリックします。

「疎通確認（ping）」ページが表示されます。



2.　「ping送信先」に送信先のIPアドレスを入力し、利用プロトコルを設定します。

3.　［Ping送信］ボタンをクリックします。

「ping実行中」というメッセージが表示されたあと、ブラウザ画面にping送信結果が表示されます。

■ 時計を設定する

本装置の内部時計の時刻を設定できます。時刻設定する方法は以下の3つがあります。

- ブラウザを利用しているパソコンの時刻を取得する方法
- ネットワーク上のTIMEサーバ、またはNTPサーバから時刻を取得する方法
- 任意の時刻を設定する方法

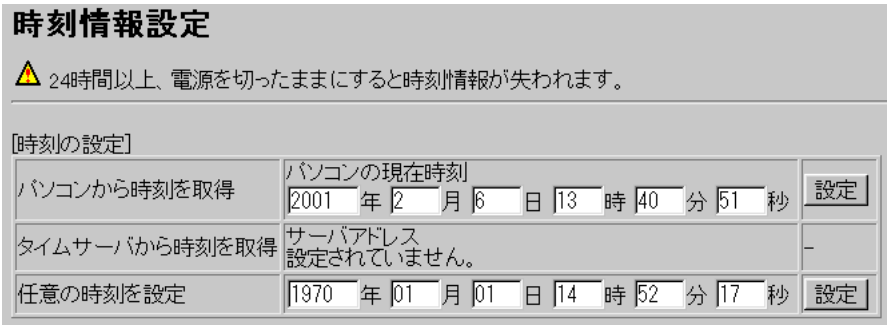
こんな事に気をつけて

24時間以上、電源を切ったままにすると時刻情報が失われます。

ここでは任意の時刻を設定する場合の例を以下に示します。

1.　操作メニューで「時刻設定」をクリックします。

「時刻情報設定」ページが表示されます。



2.　「任意の時刻を設定」を指定する場合は現在の日時を入力します。
指定する時刻の設定方法の［設定］ボタンをクリックします。

「時刻を○○○○に設定しました。」というメッセージが表示されます。

■ テレホーダイ機能を使う

INSテレホーダイは、NTTが提供するサービスです。午後11時から午前8時の深夜・早朝時間帯に、あらかじめ指定した2つの電話番号に対してかけ放題になります。
テレホーダイ機能利用時は、指定された時間だけ無通信監視機能を停止して自動切断させないようにします。

こんな事に気をつけて

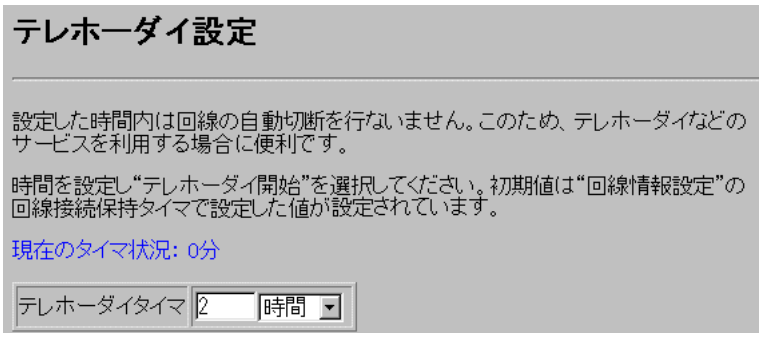
INSテレホーダイサービスを利用する場合はNTTとの契約が必要です。

補足 ルータ設定の「相手情報」で、接続先ごとにテレホーダイの使用有無を設定できます。

テレホーダイの時間帯を設定する

1.　操作メニューで「テレホーダイ設定」をクリックします。

「テレホーダイ設定」ページが表示されます。



2.　「テレホーダイタイマ」で、回線を接続したままにしておく時間を入力します。

3.　［テレホーダイ開始］ボタンをクリックします。

設定した時間、回線が接続されたままになります。

テレホーダイを開始する／停止する

1.　テレホーダイを開始するときは、操作メニューの「テレホーダイ設定」ページで［テレホーダイ開始］ボタンをクリックします。
テレホーダイを停止するときは［テレホーダイ終了］ボタンをクリックします。

［テレホーダイ終了］ボタンをクリックすると、「テレホーダイタイマをキャンセルしました」というメッセージが表示されます。

こんな事に気をつけて

［テレホーダイ開始］ボタンをクリックすると、テレホーダイ時間帯以外でも、ずっとつながった状態となります。

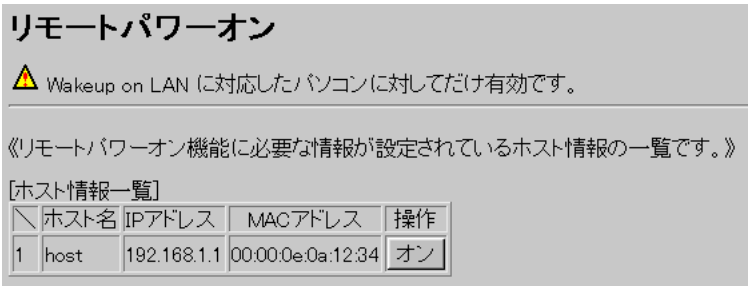
■ リモートパワーオン機能を使う

遠隔地にあるパソコンの電源投入を行う機能です。電源を投入するパソコンは、あらかじめ「ホストデータベース情報」ー「リモート電源制御」で「対象」として登録しておく必要があります。

☛ 参照 「起動条件を設定する」（P.507）

1. 操作メニューで「リモートパワーオン」をクリックします。

「リモートパワーオン」ページが表示されます。



2. 起動させるパソコンの［オン］ボタンをクリックします。

本装置が該当するパソコンに対して「Magic Packet」を送信し、パソコンが起動します。

補足 パソコンが Magic Packet を受信してから起動が完了するまで、数十秒から数分かかります（お使いの機種や OS によって異なります）。

こんな事に気をつけて

本機能は、Waleup in LAN に対応したパソコンだけ利用できます。Waleup on LAN 対応機種については、パソコンのメーカーにお問い合わせください。

■ 留守モードのON／OFFを設定する

本装置では、あらかじめ「装置情報設定」の「留守モード情報」に留守（外出）中の動作を設定しておくことにより、在宅時の設定（留守モードOFF）を留守中の設定（留守モードON）にかんたんに切り替えることができます。

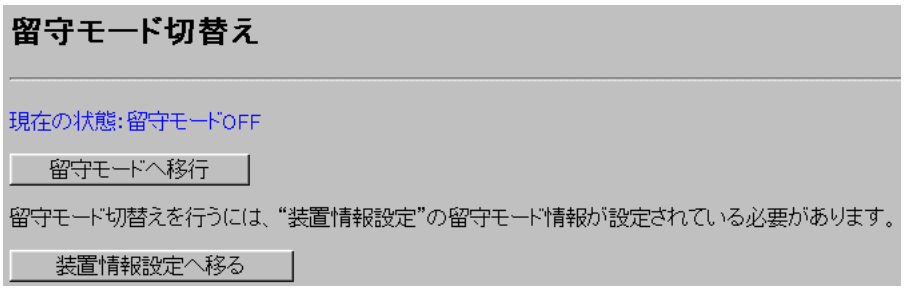
こんな事に気をつけて

「留守モード中は、スタンバイモードで動作する」設定にしている場合は、留守モードへ移行するとスタンバイモードが動作するため、操作メニューから留守モード解除ができなくなります。留守モードを解除する場合は、アナログポートに接続されている電話機で解除してください。

留守モードをONに設定する

1.　操作メニューで「留守モード切替え」をクリックします。

「留守モード切替え」ページが表示されます。



2.　留守モードをONにするときは、［留守モードへ移行］ボタンをクリックします。

「留守モードへ移行しました」というメッセージが表示されます。

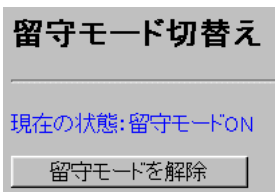
留守モード情報の設定を変更する場合は、［装置情報設定へ移る］ボタンをクリックします。

「装置情報設定」の「留守モード情報」が表示されます。

留守モードをOFFに設定する

1.　操作メニューで「留守モード切替え」をクリックします。

「留守モード切替え」ページが表示されます。



2.　留守モードをOFFにするときは、［留守モードを解除］ボタンをクリックします。

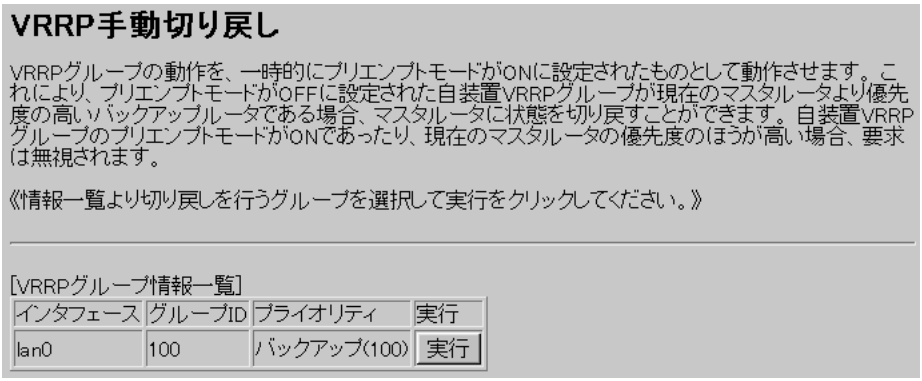
「留守モードを解除しました」というメッセージが表示されます。

■ VRRP手動切り戻し機能を使う

VRRPグループの動作を、一時的にプリエンプトモードがONに設定されたものとして動作させます。これにより、プリエンプトモードがOFFに設定された自装置VRRPグループが、現在のマスタルータより優先度の高いバックアップルータである場合、マスタルータに状態を切り戻すことができます。自装置VRRPグループのプリエンプトモードがONに設定されていたり、現在のマスタルータの優先度のほうが高い場合、要求は無視されます。

1.　操作メニューで「VRRP手動切り戻し」をクリックします。

「VRRP手動切り戻し」ページが表示されます。



2.　切り戻しを行うグループの［実行］ボタンをクリックします。

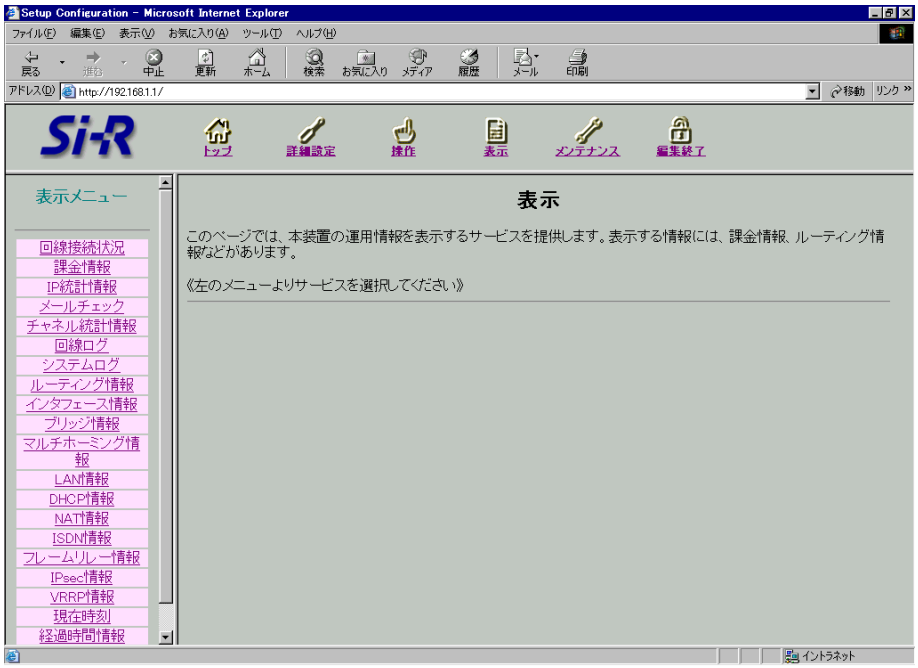
切り戻しが行われます。

表示メニューを使う

表示メニューでは、回線接続状況、回線への課金情報、IP統計情報、メールチェック、チャネル統計情報、回線ログ情報、システムログ情報、ルーティング情報、インタフェース情報、ブリッジ情報、マルチホーミング情報、LAN情報、DHCP情報、NAT情報、ISDN情報、フレームリレー情報、IPsec情報、現在時刻、経過時間情報を確認できます。

■ 表示メニューを表示する

本装置のトップページで、画面上部の［表示］アイコンをクリックすると、表示メニューが表示されます。



■ 回線接続状況を確認する

ISDN回線への接続状況を確認することができます。

1.　表示メニューで「回線接続状況」をクリックします。

「回線接続状況」ページが表示されます。

【回線接続状況】

チャネル番号	回線状態	接続形態	ネットワーク名 接続先名	電話番号	送信回線使用率	受信回線使用率	通信時間	IPアドレス	IPV6 CP	BCP
B1	接続中	発信	internet ISP-A	0322222222*	1%	100%	0000.00:00:00	172.16.32.45	-	-
B2	未使用	-	- -	-	-	-	0000.00:00:00	-	-	-

■ 課金情報で運用状況を確認する

本装置の電源を入れてから現在までの、ISDN回線に対する課金情報を確認することができます。

1.　表示メニューで「課金情報」をクリックします。

［データ通信課金情報］、［接続先別データ通信課金情報］、［マルチTA課金情報］、［アナログポート課金情報］が表示されます。

2.　以下の項目を確認します。

【データ通信課金情報】

- 通信総時間　→ データ通信の通信時間の累計です。
- 課金合計金額　→ データ通信の通信料金の累計です。
- 最長通信　→ データ通信の過去の記録で、1回の通信での最長の時間、通信料金、接続先相手です。
- 最高課金　→ データ通信の過去の記録で、1回の通信での最高金額、通信時間、接続先相手です。
- 最終接続　→ データ通信の最新の通信での、通信時間、通信料金、接続先相手です。

【接続先別データ通信課金情報】

接続先ごとの通信時間の累計および通信料金の累計が表示されます。

【マルチTA課金情報】

- 通信総時間　→ マルチTA通信の通信時間の累計です。
- 課金合計金額　→ マルチTA通信の通信料金の累計です。

■データ通信課金情報クリア

→［データ通信課金情報クリア］ボタンをクリックすると、現在保持している上記3つの情報をすべてクリアします。

【アナログポート課金情報】

- 最長通信　→ アナログ通信の過去の記録で、1回の通信での最長の時間、通信料金、接続先相手電話番号です。
- 最高課金　→ アナログ通信の過去の記録で、1回の通信での最高金額、通信時間、接続先相手電話番号です。
- 最終接続　→ アナログ通信で最新の通信での、通信時間、通信料金、接続先相手電話番号です。
- 合計　→アナログ通信の通信時間と通信料金の累計です。

■アナログポート課金情報クリア

→［アナログポート課金情報クリア］ボタンをクリックすると、現在保持しているアナログポート課金情報をすべてクリアします。

■全ての課金情報クリア→［全ての課金情報クリア］ボタンをクリックすると、現在保持している課金情報をすべてクリアします。

【データ通信課金情報】

通信総時間		0000.00:00:00
課金合計金額		0 円
最長通信	ネットワーク名	-
	接続先名	-
	時間	0000.00:00:00
	金額	0 円
最高課金	ネットワーク名	-
	接続先名	-
	時間	0000.00:00:00
	金額	0 円
最終接続	ネットワーク名	-
	接続先名	-
	時間	0000.00:00:00
	金額	0 円

接続先別データ通信課金情報			
ネットワーク名	接続先名	時間	金額

マルチTA課金情報	
通信総時間	0000.00:00:00
課金合計金額	0 円

データ通信課金情報クリア

【アナログポート課金情報】

		電話番号	時間	金額
ポート1	最長通信	-	0000.00:00:00	0円
	最高課金	-	0000.00:00:00	0円
	最終接続	-	0000.00:00:00	0円
	合計		0000.00:00:00	0円
ポート2	最長通信	-	0000.00:00:00	0円
	最高課金	-	0000.00:00:00	0円
	最終接続	-	0000.00:00:00	0円
	合計		0000.00:00:00	0円
トータル	最長通信	-	0000.00:00:00	0円
	最高課金	-	0000.00:00:00	0円
	最終接続	-	0000.00:00:00	0円
	合計		0000.00:00:00	0円

アナログポート課金情報クリア

全ての課金情報クリア

通信課金情報は、他通信事業者との網間接続使用ユーザにとっては正しい課金値とはなりません。
また通信時間は、網からトーン/アナウンスしている時間を含みます。
アナログポート課金情報のトータルはポート1とポート2の合計とは異なる場合があります。
(例:疑似着信転送時の課金情報はポートを特定できないため、トータルのみ課金情報が反映されます。)

こんな事に気をつけて

- 本書の表記で使われる通信料金とは、INS ネット64基本サービスの「料金情報通知」をもとに、本装置のソフトウェアが算出した値です。算出される値は、お客様の契約や回線利用状況により異なりますので、請求金額とは必ずしも一致しません。
  たとえば、以下のような場合があります。
  - INS テレホーダイ利用時
  - NTT DoCoMo 以外の自動車電話・携帯電話と通話した場合
  - PHS と通話した場合（PIAFS によるデータ通信も含む）
- 本装置の電源を切ると、課金情報はすべてクリアされます。

■ IP 統計情報を見る

回線を介した通信のプロトコルごとの内訳を確認できます。

1. 表示メニューで「IP 統計情報」をクリックします。

「IP 統計情報」ページが表示されます。

【IP統計情報】

```
tcp:
        95 packets sent
                90 data packets (16322 bytes)
                0 data packets (0 bytes) retransmitted
                0 resends initiated by MTU discovery
                4 ack-only packets (1 delayed)
                0 URG only packets
                0 window probe packets
                0 window update packets
                1 control packet
        156 packets received
                87 acks (for 16322 bytes)
                1 duplicate ack
                0 acks for unsent data
                72 packets (103 bytes) received in-sequence
                0 completely duplicate packets (0 bytes)
                0 old duplicate packets
                0 packets with some dup. data (0 bytes duped)
                1 out-of-order packet (0 bytes)
                0 packets (0 bytes) of data after window
                0 window probes
                0 window update packets
                0 packets received after close
                0 discarded for bad checksums
                0 discarded for bad header offset fields
                0 discarded because packet too short
        0 connection requests
        2 connection accepts
        0 bad connection attempts
        0 listen queue overflows
        2 connections established (including accepts)
        1 connection closed (including 0 drops)
                1 connection updated cached RTT on close
                1 connection updated cached RTT variance on close
                0 connections updated cached ssthresh on close
        0 embryonic connections dropped
        87 segments updated rtt (of 88 attempts)
        0 retransmit timeouts
                0 connections dropped by rexmit timeout
        0 persist timeouts
                0 connections dropped by persist timeout
        0 keepalive timeouts
                0 keepalive probes sent
                0 connections dropped by keepalive
```

```
        76 correct ACK header predictions
        66 correct data packet header predictions
udp:
        151 datagrams received
        0 with incomplete header
        0 with bad data length field
        0 with bad checksum
        0 dropped due to no socket
        74 broadcast/multicast datagrams dropped due to no socket
        0 dropped due to full socket buffers
        0 not for hashed pcb
        77 delivered
        0 datagrams output
ip:
        307 total packets received
        0 bad header checksums
        0 with size smaller than minimum
        0 with data size < data length
        0 with ip length > max ip packet size
        0 with header length < data size
        0 with data length < header length
        0 with bad options
        0 with incorrect version number
        0 fragments received
        0 fragments dropped (dup or out of space)
        0 fragments dropped after timeout
        0 packets reassembled ok
        307 packets for this host
        0 packets for unknown/unsupported protocol
        0 packets forwarded
        0 packets not forwardable
        0 redirects sent
        95 packets sent from this host
        0 packets sent with fabricated ip header
        0 output packets dropped due to no bufs, etc.
        0 output packets discarded due to no route
        0 output datagrams fragmented
        0 fragments created
        0 datagrams that can't be fragmented
        0 tunneling packets that can't find gif
icmp:
        0 calls to icmp_error
        0 errors not generated 'cuz old message was icmp
        0 messages with bad code fields
        0 messages < minimum length
        0 bad checksums
        0 messages with bad length
        0 message responses generated
ipsec:
        0 inbound packets processed successfully
        0 inbound packets violated process security policy
        0 inbound packets with no SA available
        0 invalid inbound packets
        0 inbound packets failed due to insufficient memory
        0 inbound packets failed getting SPI
        0 inbound packets failed on AH replay check
        0 inbound packets failed on ESP replay check
        0 inbound packets considered authentic
        0 inbound packets failed on authentication
        0 inbound packets considered authentic(ESPinAuth)
        0 inbound packets failed on authentication(ESPinAuth)
        0 outbound packets processed successfully
        0 outbound packets violated process security policy
        0 outbound packets with no SA available
        0 invalid outbound packets
        0 outbound packets failed due to insufficient memory
        0 outbound packets with no route
ip6:
        0 total packets received
        0 with size smaller than minimum
        0 with data size < data length
        0 with bad options
        0 with incorrect version number
        0 fragments received
        0 fragments dropped (dup or out of space)
        0 fragments dropped after timeout
```

```
        0 fragments that exceeded limit
        0 packets reassembled ok
        0 packets for this host
        0 packets forwarded
        0 packets not forwardable
        0 redirects sent
        6 packets sent from this host
        0 packets sent with fabricated ip header
        0 output packets dropped due to no bufs, etc.
        0 output packets discarded due to no route
        0 output datagrams fragmented
        0 fragments created
        0 datagrams that can't be fragmented
        0 packets that violated scope rules
        0 multicast packets which we don't join
        Mbuf statistics:
                0 one mbuf
                0 one ext mbuf
                0 two or more ext mbuf
        0 packets whose headers are not continuous
        0 tunneling packets that can't find gif
        0 packets discarded due to too many headers
        0 failures of source address selection
        0 forward cache hit
        0 forward cache miss
icmp6:
        0 calls to icmp6_error
        0 errors not generated because old message was icmp6 error or so
        0 errors not generated because rate limitation
        Output histogram:
                multicast listener report: 5
                neighbor solicitation: 1
        0 messages with bad code fields
        0 messages < minimum length
        0 bad checksums
        0 messages with bad length
        Histogram of error messages to be generated:
                0 no route
                0 administratively prohibited
                0 beyond scope
                0 address unreachable
                0 port unreachable
                0 packet too big
                0 time exceed transit
                0 time exceed reassembly
                0 erroneous header field
                0 unrecognized next header
                0 unrecognized option
                0 redirect
                0 unknown
        0 message responses generated
        0 messages with too many ND options
tcp6:
        0 packets sent
                0 data packets (0 bytes)
                0 data packets (0 bytes) retransmitted
                0 ack-only packets (0 delayed)
                0 URG only packets
                0 window probe packets
                0 window update packets
                0 control packets
        0 packets received
                0 acks (for 0 bytes)
                0 duplicate acks
                0 acks for unsent data
                0 packets (0 bytes) received in-sequence
                0 completely duplicate packets (0 bytes)
                0 old duplicate packets
                0 packets with some dup. data (0 bytes duped)
                0 out-of-order packets (0 bytes)
                0 packets (0 bytes) of data after window
                0 window probes
                0 window update packets
                0 packets received after close
                0 discarded for bad checksums
                0 discarded for bad header offset fields
                0 discarded because packet too short
```

```
        0 connection requests
        0 connection accepts
        0 bad connection attempts
        0 connections established (including accepts)
        0 connections closed (including 0 drops)
        0 embryonic connections dropped
        0 segments updated rtt (of 0 attempts)
        0 retransmit timeouts
                0 connections dropped by rexmit timeout
        0 persist timeouts
        0 connections timed out in persist
        0 keepalive timeouts
                0 keepalive probes sent
                0 connections dropped by keepalive
        0 correct ACK header predictions
        0 correct data packet header predictions
        0 PCB cache misses
udp6:
        0 datagrams received
        0 with incomplete header
        0 with bad data length field
        0 with bad checksum
        0 with no checksum
        0 dropped due to no socket
        0 multicast datagrams dropped due to no socket
        0 dropped due to full socket buffers
        0 delivered
        0 datagrams output
```

IP 統計情報の見方は「Si-R130B コマンドリファレンス」の netstat -s コマンドを参照してください。

■ 電子メール着信通知を見る

到着しているメールの確認ができます。
メールの着信を確認する場合は、「詳細設定」の「E メールエージェント情報」で情報を指定します。

メールチェック

到着しているメールがある場合は、CHECK ランプが緑色で点滅します。POP3 プロトコルを使用してメールサーバにアクセスしてメールの着信を確認します。

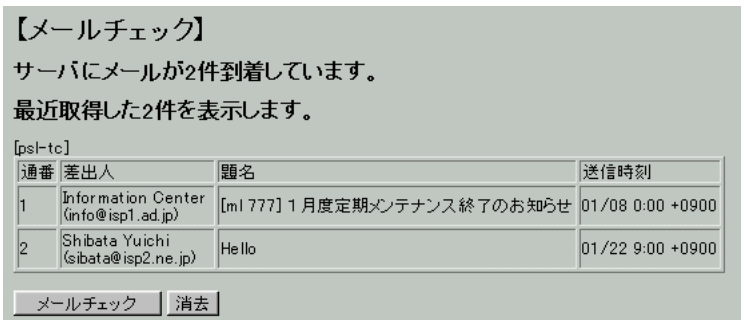
1.　表示メニューで「メールチェック」をクリックします。

「メールチェック」ページが表示されます。

2.　チェックするメールのユーザ名の欄の［表示］ボタンをクリックします。

3.　メールパスワードを入力し、［実行］ボタンをクリックします。

到着しているメールが表示されます。

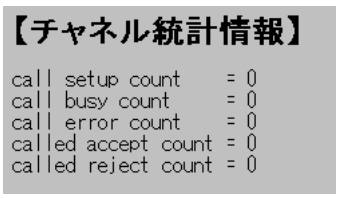


■ チャネル統計情報を見る

回線接続の情報を確認できます。

1.　表示メニューで「チャネル統計情報」をクリックします。

「チャネル統計情報」ページが表示されます。



チャネル統計情報の見方は「Si-R130B コマンドリファレンス」のisdnstat -D コマンドを参照してください。

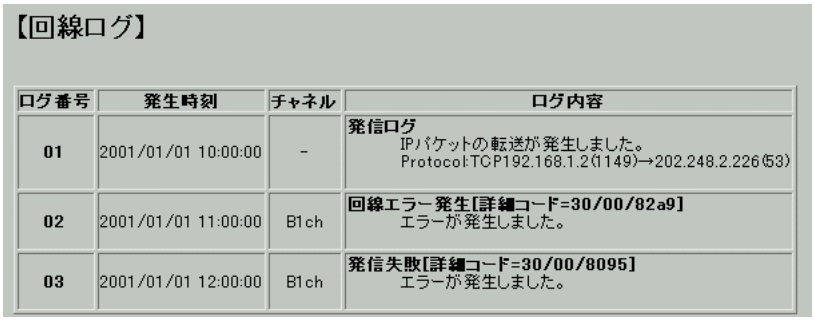
■ 回線ログ情報で運用状況を確認する

ISDN回線への接続、切断に関する情報を確認できます。通信エラーが発生した状況や、通信エラーの原因を示した「ログ内容」が表示されます。

1.　表示メニューで「回線ログ」をクリックします。

「回線ログ」ページが表示されます。

- ログ番号　→ログの番号です。
- 発生時刻　→ログが記録された時刻です。
- チャネル　→ログが記録された事象が発生したチャネルです。
- ログ内容　→ログの内容です。
  ［詳細コード=XX/XX/XXYY］の「YY」は理由コードを示します。理由コードは「ISDN理由表示番号一覧」（P.687）を参照してください。



【回線ログ】

ログ番号	発生時刻	チャネル	ログ内容
01	2001/01/01 10:00:00	-	発信ログ IPパケットの転送が発生しました。 Protocol:TCP192.168.1.2(1149)→202.248.2.226(53)
02	2001/01/01 11:00:00	B1ch	回線エラー発生[詳細コード=30/00/82a9] エラーが発生しました。
03	2001/01/01 12:00:00	B1ch	発信失敗[詳細コード=30/00/8095] エラーが発生しました。

［表示例］

> 発信ログ
> IPパケットの転送が発生しました。
> Protocol：TCP192.168.1.2（1149）→202.248.2.226（53）

［説明］

- 発信元が192.168.1.2でポート1149を使用して202.248.2.226へポート53でアクセスしたことを示します。
- ポート1149は送信元が内部で使用しているポート番号です。

■ システムログを見る

接続先や接続時間の情報などを確認できます。通信エラーや超過課金の原因を知る手がかりになります。

1.　表示メニューで「システムログ」をクリックします。

「システムログ」ページが表示されます。

【システムログ】

```
Jan 02 09:19:09 init: system startup now.
Jan 02 10:40:27 enabled: system configuration restarted
```

■ ルーティング情報を見る

ルーティングテーブルを確認できます。

1.　表示メニューで「ルーティング情報」をクリックします。

「ルーティング情報」ページが表示されます。

【ルーティング情報】

```
Routing tables

Internet:
Destination                 Gateway                 Flags      Netif Expire
default                     10.232.78.1             UGSc        lan0
1.0.0.97                    rmt44                   UHS        rmt44
1.1.1.1                     rmt0                    UHS         rmt0
10.232.78/24                link#1                  UC          lan0
10.232.78.1                 0:0:e:6f:2:14           UHLW        lan0   1138
10.232.78.61                127.0.0.1               UH           lo0
127.0.0.1                   127.0.0.1               UH           lo0
192.168.1.1                 127.0.0.1               UH           lo0
192.168.1.2                 192.168.1.1             UH          rmt0
192.168.1.10                10.232.78.61            UH          ans0
192.168.2                   192.168.1.2             UGSc        rmt0
224/4                       127.0.0.1               UGS          lo0
Total Routing Tables  4
Total ARP Tables  1

Internet6:
Destination                 Gateway                 Flags      Netif Expire
::1                         ::1                     UH           lo0
fe80::%lan0/64              link#1                  UC          lan0
fe80::%rmt0/64              link#2                  UC          rmt0
fe80::%rmt1/64              link#3                  UC          rmt1
fe80::%rmt2/64              link#4                  UC          rmt2
fe80::%rmt3/64              link#5                  UC          rmt3
fe80::%lo0/64               fe80::1%lo0             Uc           lo0
fec0:0:0:1000::/64          link#2                  UC          rmt0
ff01::/32                   ::1                     U            lo0
ff02::%lan0/32              link#1                  UC          lan0
ff02::%rmt0/32              link#2                  UC          rmt0
ff02::%rmt1/32              link#3                  UC          rmt1
ff02::%rmt2/32              link#4                  UC          rmt2
ff02::%rmt3/32              link#5                  UC          rmt3
ff02::%lo0/32               fe80::1%lo0             UC           lo0
Total Routing Tables  0
Total NDP Tables  0
```

ルーティング情報の見方は「Si-R130B コマンドリファレンス」のnetstat -rn コマンドを参照してください。

■ インタフェース情報を見る

インタフェース情報を確認できます。

1.　表示メニューで「インタフェース情報」をクリックします。

「インタフェース情報」ページが表示されます。

【インタフェース情報】

Name	Mtu	Network	Address	Ipkts	Ierrs	Opkts	Oerrs
lan0	1500	<Link#1>	00:00:0e:7f:91:31	144	0	144	0
lan0	1500	192.168.1	192.168.1.130	144	0	144	0
lan0	1500	fe80::/64	fe80::200:eff:fe7f:9131	144	0	144	0
lan0	1500	fec0:0:0:1::/64	fec0:0:0:1::1	144	0	144	0
rmt0	1500	<Link#2>		0	0	0	10
rmt0	1500	192.168.1	192.168.1.130	0	0	0	10
rmt0	1500	fe80::/64	fe80::200:eff:fe7f:9131	0	0	0	10
rmt0	1500	fec0:0:0:8000::/64	fec0:0:0:8000::1	0	0	0	10
lo0	16384	<Link#52>		71	0	71	0
lo0	16384	fe80::/64	fe80::1	71	0	71	0
lo0	16384	::1/128	::1	71	0	71	0
lo0	16384	127	127.0.0.1	71	0	71	0

インタフェース情報の見方は「Si-R130B コマンドリファレンス」のnetstat -iコマンドを参照してください。

■ ブリッジ情報を見る

ブリッジ情報を確認できます。

1.　表示メニューで「ブリッジ情報」をクリックします。

「ブリッジ情報」ページが表示されます。

【ブリッジ情報】

```
[Bridge Statistics Information]

Name    Status  STP             In      Out
lan0    invalid not use          0        0


[Learning Table Information]

HashNo.  MAC address        Name    PortNo.  Status   Age


[STP Information]

[lan0]
status             : not use
```

ブリッジ情報の見方は「Si-R130B コマンドリファレンス」のbridgestat コマンドを参照してください。

■ マルチホーミング情報を見る

マルチホーミング情報を確認できます。

1. 表示メニューで「マルチホーミング情報」をクリックします。

「マルチホーミング情報」ページが表示されます。

【マルチホーミング情報】

```
WAN route
index  SrcAddr         DstAddr         type      remain(min)

multihoming forwarding (LAN) route
index  SrcAddr         DstAddr         type      remain(min)

multihoming information
  WAN route error                       0
  multihoming forwarding route error    0
  dynamic multihoming table full        0
```

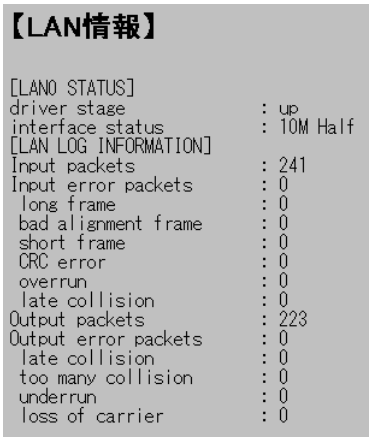
マルチホーミング情報の見方は「Si-R130B コマンドリファレンス」のmhstatコマンドを参照してください。

■ LAN情報を見る

LANの統計情報を確認できます。

1. 表示メニューで「LAN情報」をクリックします。

「LAN情報」ページが表示されます。



【LAN情報】

```
[LAN0 STATUS]
driver stage            : up
interface status        : 10M Half
[LAN LOG INFORMATION]
Input packets           : 241
Input error packets     : 0
 long frame             : 0
 bad alignment frame    : 0
 short frame            : 0
 CRC error              : 0
 overrun                : 0
 late collision         : 0
Output packets          : 223
Output error packets    : 0
 late collision         : 0
 too many collision     : 0
 underrun               : 0
 loss of carrier        : 0
```

LAN情報の見方は「Si-R130B コマンドリファレンス」のstlanコマンドを参照してください。

■ DHCP情報を見る

DHCPサーバやDHCPリレーエージェントの運用状況を確認できます。

1. 表示メニューで「DHCP情報」をクリックします。

「DHCP情報」ページが表示されます。

【DHCP情報】

```
[LAN0] DHCP Server Informations

Lease IP Address          : 192.168.1.2  [Range: 32]
Subnet Mask               : 255.255.255.0
Default Router Address    : 192.168.1.1
DNS Server Address        : 192.168.1.1
Domain Name               :
Lease Time                : 0001.00:00:00

Active Client List:
No. IP address          MAC address       Lease remain
```

DHCP情報の見方は「Si-R130Bコマンドリファレンス」のdhcpstatコマンドを参照してください。

■ NAT情報を見る

NATの統計情報を確認できます。

1. 表示メニューで「NAT情報」をクリックします。

「NAT情報」ページが表示されます。

【NAT情報】

```
*** NAT stat information ***
           to Global   to Private
translate         109          111
error               0            0

             fragment
translate           0
error               0

              current         peak
nat table           0            0

                           current
nat fragment table                 0

error accounting
  lack of memory                   0
  table not found                  0
  too small packet                 0
  other reason                     0
```

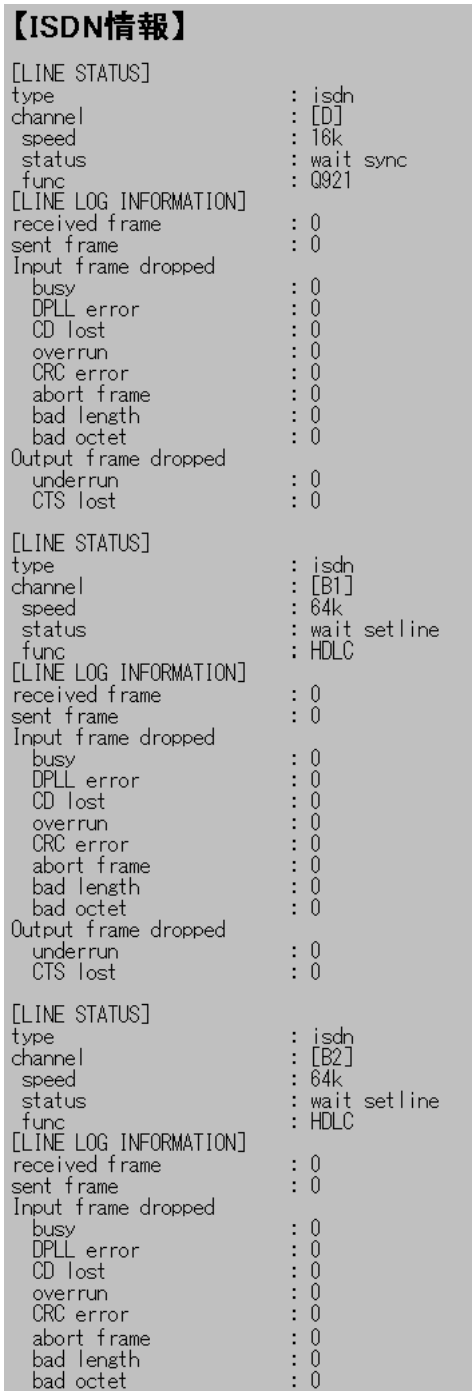
NAT情報の見方は「Si-R130Bコマンドリファレンス」のnatstatコマンドを参照してください。

■ ISDN情報を見る

ISDN関連の統計情報を確認できます。

1. 表示メニューで「ISDN情報」をクリックします。

「ISDN情報」ページが表示されます。



【ISDN情報】

```
[LINE STATUS]
type                    : isdn
channel                 : [D]
 speed                  : 16k
 status                 : wait sync
 func                   : Q921
[LINE LOG INFORMATION]
received frame          : 0
sent frame              : 0
Input frame dropped
  busy                  : 0
  DPLL error            : 0
  CD lost               : 0
  overrun               : 0
  CRC error             : 0
  abort frame           : 0
  bad length            : 0
  bad octet             : 0
Output frame dropped
  underrun              : 0
  CTS lost              : 0

[LINE STATUS]
type                    : isdn
channel                 : [B1]
 speed                  : 64k
 status                 : wait setline
 func                   : HDLC
[LINE LOG INFORMATION]
received frame          : 0
sent frame              : 0
Input frame dropped
  busy                  : 0
  DPLL error            : 0
  CD lost               : 0
  overrun               : 0
  CRC error             : 0
  abort frame           : 0
  bad length            : 0
  bad octet             : 0
Output frame dropped
  underrun              : 0
  CTS lost              : 0

[LINE STATUS]
type                    : isdn
channel                 : [B2]
 speed                  : 64k
 status                 : wait setline
 func                   : HDLC
[LINE LOG INFORMATION]
received frame          : 0
sent frame              : 0
Input frame dropped
  busy                  : 0
  DPLL error            : 0
  CD lost               : 0
  overrun               : 0
  CRC error             : 0
  abort frame           : 0
  bad length            : 0
  bad octet             : 0
```

```
Output frame dropped
  underrun                : 0
  CTS lost                : 0
```

ISDN 情報の見方は「Si-R130B コマンドリファレンス」の stins コマンドを参照してください。

■ フレームリレー情報を見る

フレームリレー関連の統計情報を確認できます。

1.　表示メニューで「フレームリレー情報」をクリックします。

「フレームリレー情報」ページが表示されます。

【フレームリレー情報】

```
[DLCI: 17]
  CIR                     : 32
  trans state             : disable
  load state              : stop
  possible send bytes     : 0
  max send bytes          : 0
  max send bytes(lower)   : 102
  max send bytes(upper)   : 1638
  max send bytes(CIR)     : 409
  sending bytes           : 0
  send throuput           : 0 bytes/s
  waiting send packets    : 0
  fecn received           : 0
  becn received           : 0
  send errors             : 0
  receive errors          : 0
  send bytes              : 0
  receive bytes           : 0
```

フレームリレー情報の見方は「Si-R130B コマンドリファレンス」の frstat コマンドを参照してください。

■ IPsec 情報を見る

IPsec 情報を確認できます。

1.　表示メニューで「IPsec 情報」をクリックします。

「IPsec 情報」ページが表示されます。

【IPsec情報】

```
[IPsec SA Information]
[1]     Remote Name(ISP-0), rmt0
        Side(Initiator), Gateway(192.168.2.1, 192.168.1.1), OUT
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=171237444(0x0a34e044)
        Created(Sep 29 17:59:03 2001), NewSA(23040secs, 3276Kbyte)
        Lifetime(28800secs), Current(332secs), Remain(28468secs)
        Lifebyte(4096Kbyte), Current(2528Kbytes), Remain(1568Kbyte)

[2]     Remote Name(ISP-0), rmt0
        Side(Initiator), Gateway(192.168.1.1, 192.168.2.1), IN
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=181913669(0x0ad7c845)
        Created(Sep 29 17:59:03 2001), NewSA(23040secs, 3276Kbyte)
        Lifetime(28800secs), Current(332secs), Remain(28468secs)
        Lifebyte(4096Kbyte), Current(2528Kbytes), Remain(1568Kbyte)
```

```
[3]     Destination(192.168.2.20/24), Source(192.168.1.10/24), rmt1
        Side(Initiator), Gateway(192.168.2.1, 192.168.1.1), OUT
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=171237444(0x0a34e044)
        Created(Sep 29 17:59:03 2001), NewSA(23040secs, 3276Kbyte)
        Lifetime(28800secs), Current(332secs), Remain(28468secs)
        Lifebyte(4096Kbyte), Current(2528Kbytes), Remain(1568Kbyte)

[4]     Destination(192.168.1.10/24), Source(192.168.2.20/24), rmt1
        Side(Initiator), Gateway(192.168.1.1, 192.168.2.1), IN
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=181913669(0x0ad7c845)
        Created(Sep 29 17:59:03 2001), NewSA(23040secs, 3276Kbyte)
        Lifetime(28800secs), Current(332secs), Remain(28468secs)
        Lifebyte(4096Kbyte), Current(2528Kbytes), Remain(1568Kbyte)

[5]     Destination(192.168.3.30/24), Source(192.168.2.20/24), rmt2
        Side(Manual), Gateway(192.168.3.1, 192.168.2.1), IN
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(---)
        Side(Manual), Status(mature), Spi=4096(0x1000)
        Created(Sep 29 17:59:03 2001), NewSA(--- secs, --- Kbyte)
        Lifetime(--- secs), Current(332secs), Remain(--- secs)
        Lifebyte(--- Kbyte), Current(2528Kbytes), Remain(--- Kbyte)

[IKE SA Information]
[1]     Destination(192.168.1.1.500), Source(192.168.2.1.500)
        Cookies(2ee33635dcc2a837:ece2a45bc12889ef)
        Side(Initiator), Status(ESTABLISHED), Exchangetype(AGGRESSIVE)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        Created(Sep 29 17:59:03 2001)
        Lifetime(86400secs), Current(10secs), Remain(86390secs)
```

IPsec情報の見方は「Si-R130B コマンドリファレンス」のipsecstatコマンドを参照してください。

■ VRRP情報を確認する

VRRPに関する情報を確認することができます。

1.　表示メニューで「VRRP情報」をクリックします。

「VRRP情報」ページが表示されます。

【VRRP情報】

```
[LAN 0]
  State              : OK
  Authentication Type: Text
  Authentication Pass: "fujitu"
  Interface statistics information:
      0          Bad checksum packets
      0          VRRP Version illegal packets
      0          VRID illegal packets

  VRID 10
    Master(PRI 255 now 255/PREEMPT ON)
    Now Master : Me
    Virtual MAC Address : 00:00:5E:00:01:0A
    Virtual Router IP Address:
        10.124.2.126
        10.124.2.224
    VRRP advertisement interval 1
    Shutdown interface trigger:
        rmt11 reduce 100  OFF
    Shutdown node trigger:
        10.232.79.193    rmt1  reduce 100  OFF
    Group statistics information:
        1          become master-router
        0          received VRRP advertisement packets
```

```
        0          VRRP advertisement interval configuration mismatched packets
        0          Authentication failed packets
        0          TTL illegal packets
        0          received priority 0 advertisement packets
        0          sent priority 0 advertisement packets
        0          VRRP type illegal packets
        0          Virtual router IP address configuration mismatched packets
        0          Authentication type illegal packets
        0          Authentication type mismatch packets
        0          Length illegal packets

 VRID 20
   Backup(PRI 100 now 50/PREEMPT OFF)
   Now Master : 10.124.2.100 Priority 255
   Virtual MAC Address : 00:00:5E:00:01:14
   Virtual Router IP Address:
       10.124.2.138
       10.124.2.139
   VRRP advertisement interval 1
   Shutdown interface trigger:
       rmt1  reduce 100  OFF
   Group statistics information:
        0          become master-router
        0          received VRRP advertisement packets
        0          VRRP advertisement interval configuration mismatched packets
        0          Authentication failed packets
        0          TTL illegal packets
        0          received priority 0 advertisement packets
        0          sent priority 0 advertisement packets
        0          VRRP type illegal packets
        0          Virtual router IP address configuration mismatched packets
        0          Authentication type illegal packets
        0          Authentication type mismatch packets
        0          Length illegal packets
```

VRRP情報の見方は「Si-R130B コマンドリファレンス」のvrrpstat コマンドを参照してください。

■ 現在時刻を見る

現在時刻を確認できます。

1.　表示メニューで「現在時刻」をクリックします。

「現在時刻」ページが表示されます。

【現在時刻】

```
Mon Jan  1 00:00:00 2001
```

■ 経過時間情報を見る

電源投入後、経過した時間を確認できます。

1.　表示メニューで「経過時間情報」をクリックします。

「経過時間情報」ページが表示されます。

【経過時間情報】

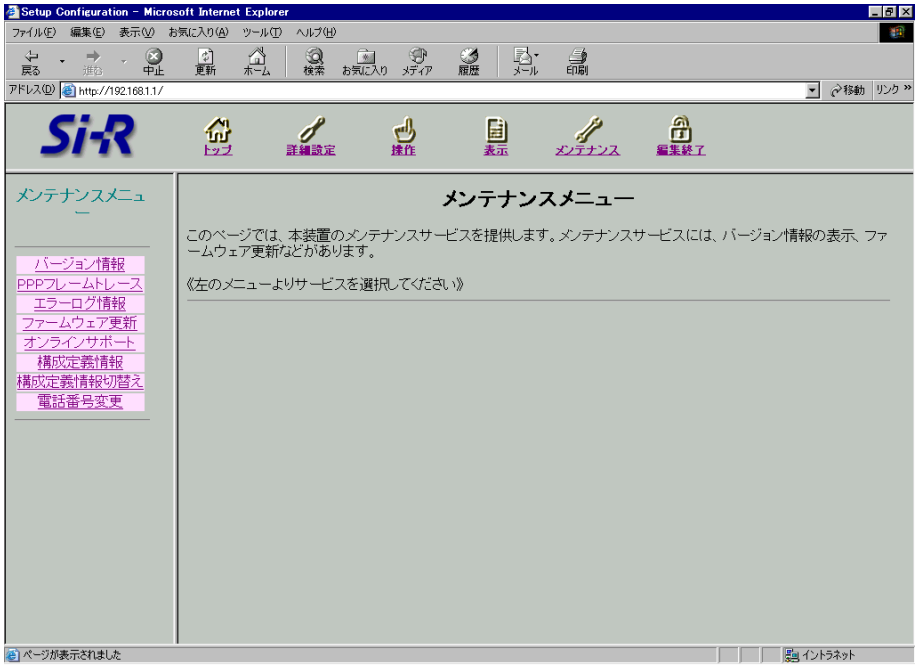
```
0001.01:48:23
```

メンテナンスメニューを使う

メンテナンスメニューでは、バージョン情報、PPPフレームトレース、エラーログ情報の確認、および本装置のファームウェアの更新、オンラインサポート、構成定義の退避／復元、電話番号の変更ができます。

■ メンテナンスメニューを表示する

本装置のトップページで、画面上部の［メンテナンス］アイコンをクリックすると、メンテナンスメニューが表示されます。



■ バージョン情報を見る

本装置内蔵ファームウェアのバージョンを確認できます。

1.　メンテナンスメニューで「バージョン情報」をクリックします。

「バージョン情報」ページが表示されます。

- 製品名　→Si-R130B：基本ソフトウェア
- バージョン情報（版数）　→FIRM：V04.07

■ PPP フレームトレース情報を見る

PPPのプロトコル情報を表示します。回線がつながりにくい場合は、ここに表示される情報を確認します。

1.　メンテナンスメニューで「PPP フレームトレース」をクリックします。

「PPP フレームトレース情報」ページが表示されます。

フレームトレース情報の見方

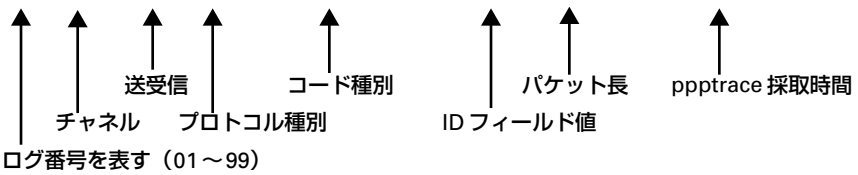
PPPフレームトレース情報は、以下のように表示されます。

表示例）

[02] B1ch : Recv LCP　Configure-Request id=00 len=19　97.09.01 09:19:54.225
　　data=c021 0100 0013 0305 c223 0505 06f0 1e4a
　　5007 0208 02

表示されている情報は、以下に示すような要素に分けられます。

[02] B1ch : Recv LCP Configure-Request id=00 len=19　97.09.01 09:19:54.225



☛ 参照 「PPP フレームトレース情報詳細」（P.689）

■ エラーログ情報を見る

本装置の異常に関する情報が記録されている場合は、ここで確認できます。
富士通の技術員へ連絡してください。その際、エラーログ情報の内容をお知らせください。

1.　メンテナンスメニューで「エラーログ情報」をクリックします。

「エラーログ情報」ページが表示されます。

■ 本装置のファームウェアを更新する

ファームウェアを更新すると、本装置に新しい機能を追加できます。

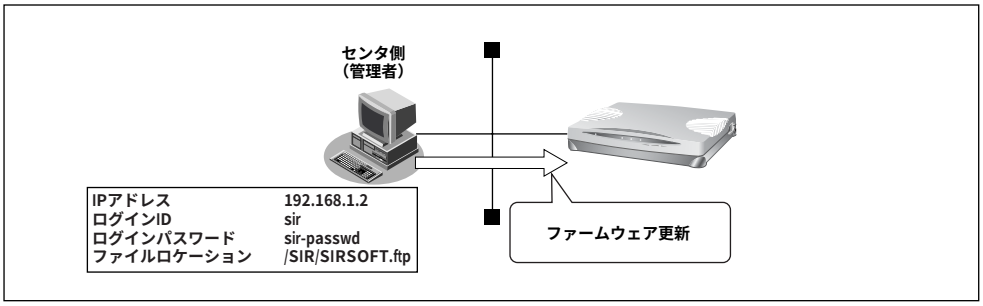
FTPサーバ（FTPサーバ機能を持つパソコンやUNIX®システム）にファームウェアファイルを配置し、WWWブラウザ（本装置の設定メニュー）を使ってネットワークに接続した本装置のファームウェアを更新できます。

ただし、初期状態ではファームウェア更新情報が設定されていないため、設定が必要です。

こんな事に気をつけて

- **ファームウェア更新中は、本装置の電源を切らないでください。**
- **ファームウェアを更新する前に、構成定義情報を退避しておいてください。**

ここでは、ファームウェア更新情報の設定方法について例をあげて説明します。

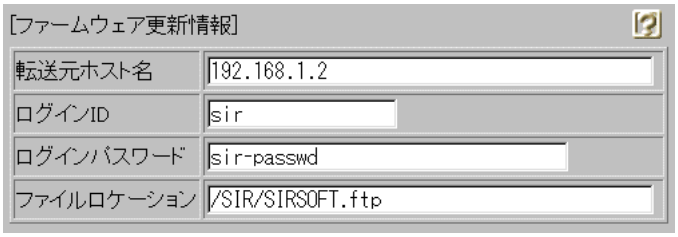


1.　詳細設定メニューのルータ設定で「装置情報」をクリックします。

「装置情報設定」ページが表示されます。

2.　［ファームウェア更新情報］で以下の項目を指定します。

- 転送元ホスト名　→192.168.1.2
- ログインID　→sir
- ログインパスワード　→sir-passwd
- ファイルロケーション　→/SIR/SIRSOFT.ftp



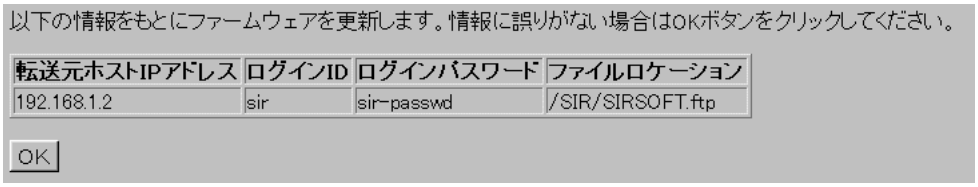
3.　［更新］ボタンをクリックします。

4.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

5.　メンテナンスメニューで「ファームウェア更新」をクリックします。

「FTPダウンロードによるファームウェア更新」ページが表示されます。



6.　表示されている内容を確認し、正しければ［OK］ボタンをクリックします。

ファームウェアの更新を開始します。

7.　「正常終了」のメッセージが表示されたら、［OK］ボタンをクリックします。

8.　［トップページに戻る］ボタンをクリックします。

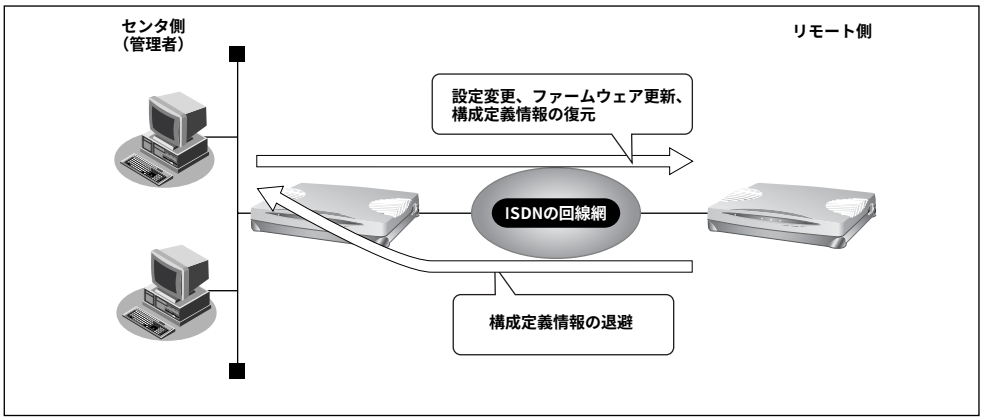
トップページに戻ります。

■ オンラインサポート機能

ISDN回線に接続された遠隔地（リモート側）の本装置に対して、管理者側（センタ側）の本装置をWWWブラウザで操作することによりメンテナンスができます。
本機能では、IP接続を必要としないため、ご購入時の状態の本装置に対しても行えます。
ただし、以下の条件を満たす必要があります。

- 対象の本装置がISDN回線に接続されていること
- 対象と同一機種の本装置がISDN回線に接続されていること
- 対象の本装置のISDN回線の「ユーザ間情報通知サービス」の契約が「着信許可」であること

以下に、それぞれの概要を示します。



(1)設定を変更する

センタ側の本装置から、リモート側の本装置の設定を行うことができます。センタ側の本装置のメンテナンスメニューからオンラインサポートを開始すると、それ以降は、通常と同様の手順でリモート側の設定を行うことができます。

(2)ファームウェア更新

センタ側の本装置から、リモート側の本装置のファームウェアを更新することができます。センタ側の本装置のメンテナンスメニューからオンラインサポートを開始すると、それ以降は、通常と同様の手順でリモート側のファームウェアを更新することができます。また、センタ側の本装置のファームウェアをリモート側に書き込むことができます。

(3)構成定義情報の退避／復元

センタ側の本装置から、リモート側の本装置の構成定義情報の退避／復元を行うことができます。センタ側の本装置のメンテナンスメニューからオンラインサポートを開始すると、それ以降は、通常と同様の手順でリモート側の構成定義情報の退避／復元を行うことができます。

メンテナンス手順

以下にオンラインサポート機能によるメンテナンス手順を説明します。

1.　センタ側の本装置のメンテナンスメニューで「オンラインサポート」をクリックします。

「オンラインサポート」ページが表示されます。

2.　リモート側の電話番号と暗証番号を指定し、［オンラインサポート開始］ボタンをクリックします。

補足　ご購入時の状態では暗証番号が設定されていないので、リモート側本装置のLANポート用MACアドレスを暗証番号として指定します。

☛ 参照　MACアドレス→「本装置 底面」（P.33）

3.　正常に接続されたあとは、センタ側の本装置を設定するのと同様の手順でリモート側の設定を行うことができます。

4.　［オンラインサポート終了］ボタンをクリックして、オンラインサポートを終了します。

B1、またはB2ランプが消灯し、回線が切断されます。

☛ 参照　表示ランプの意味→「本装置 前面」（P.30）

こんな事に気をつけて

- **本機能を使用して発信するにはINSネット64の「ユーザ間情報通知サービス」を使用するため、1回の発信につき1メッセージ分の料金が通信料金とは別にかかります。また、ISDN回線を契約するときは、ユーザ間情報通知サービスを「着信許可」にしてください。**
- **オンラインサポート中は、ISDN回線は接続されたままとなります。無通信監視タイマによる自動切断は行われません。設定終了後は、必ずオンラインサポートを終了し、回線が切断されたことを確認してください。**
- **暗証番号にはリモート側の本装置に設定された暗証番号を指定してください。一致しない場合は接続できません。なお、リモート側の本装置がご購入時の状態、またはオンラインサポート情報未設定の場合は、暗証番号としてMACアドレスを指定することにより接続できます。**
- **LANポート用MACアドレスは装置底面に表記されているとおり半角小文字の英数字で指定してください。**
- **オンラインサポートで設定できる項目はセンタ側の本装置にある項目だけに限定されます。センタ側とリモート側で機種が異なる場合、およびファームウェアの版数が異なる場合は、設定できない項目があります。**
- **センタ側の電話番号および暗証番号はセキュリティ確保のために設定しておく必要があります。ルータ設定の「装置情報」で指定してください。**

■ 構成定義情報を退避する／復元する

現在の本装置の構成定義情報をファイルに保存し、退避しておきます。必要になったときに保存しておいた構成定義情報を復元できます。

- 構成定義情報の退避：　メンテナンスメニューの「構成定義情報」ページを、WWW ブラウザ機能を使ってファイルに保存します。
- 構成定義情報の復元：　WWW ブラウザで保存しておいた「構成定義情報」ページのファイルを開き、［復元］をクリックします。

こんな事に気をつけて

現在の本装置のIP アドレスと保存時のIPアドレスが異なると復元できません。

■ 構成定義情報を切り替える

本装置は構成定義情報を内部に2つ持つことができます。「スケジュール機能」、または手動で切り替えることができます。

1.　メンテナンスメニューで「構成定義切替え」をクリックします。

「構成定義切替え」ページが表示されます。

補足　ページが表示されたときに、選択されている方が現在の構成定義情報です。

2.　再立ち上げ時に使用する構成定義情報をチェックし、［再起動］ボタンをクリックします。

再起動が行われ、選択した構成定義情報での立ち上げが行われます。

こんな事に気をつけて

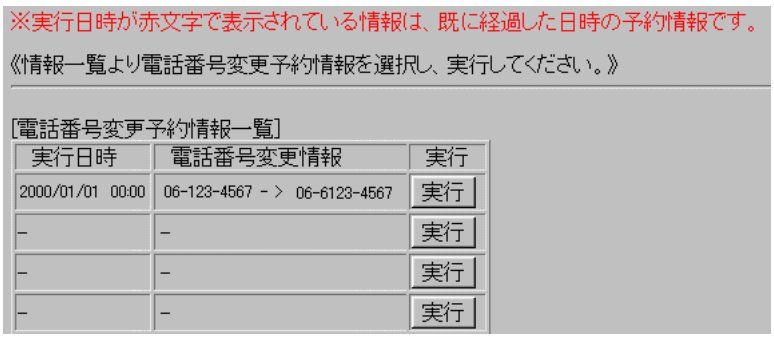
- **電源投入時は、直前に動作していた側の構成定義情報で立ち上がります。**
- **再起動すると、通話中やデータ通信の場合、切断されます。**
- **本装置のIPアドレスが変更となった場合、再起動後に本装置にアクセスするためには、パソコンの再起動およびURLを変更する必要があります。**

■ 電話番号を変更する

スケジュール情報の電話番号変更予約情報で設定した電話番号の変更を手動で行うことができます。

1.　メンテナンスメニューで「電話番号変更」をクリックします。

「電話番号変更」ページが表示されます。



2.　変更する電話番号変更予約情報の［実行］ボタンをクリックします。

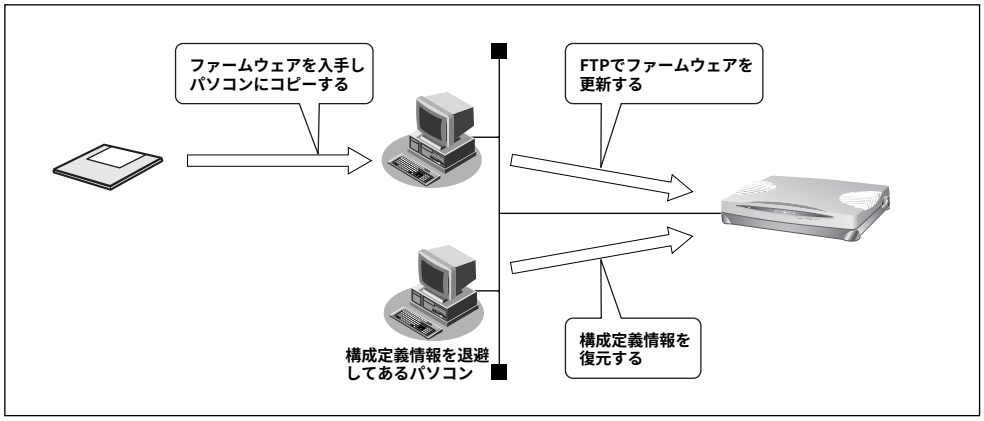
電話番号が変更されます。

3.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

FTPサーバ機能を使ってメンテナンスする

本装置はFTPサーバ機能を持っており、パソコンやUNIX®システムのftpコマンドを使って構成定義情報の退避／復元およびファームウェア更新ができます。



FTPサーバ機能を利用するときのユーザ名、パスワードは以下のとおりです。

- ユーザ名　　：ftp-admin
- パスワード　　：詳細設定で設定した管理者パスワードを指定します。

補足　管理者パスワードを設定していない場合は、FTPサーバ機能もパスワードがないものとして動作します。

●メンテナンス対象のファイル

FTPサーバ機能でメンテナンス対象となるファイル名は以下のとおりです。

- 構成定義情報1　　：config1
- 構成定義情報2　　：config2
- ファームウェア　　：firmware

●再起動方法

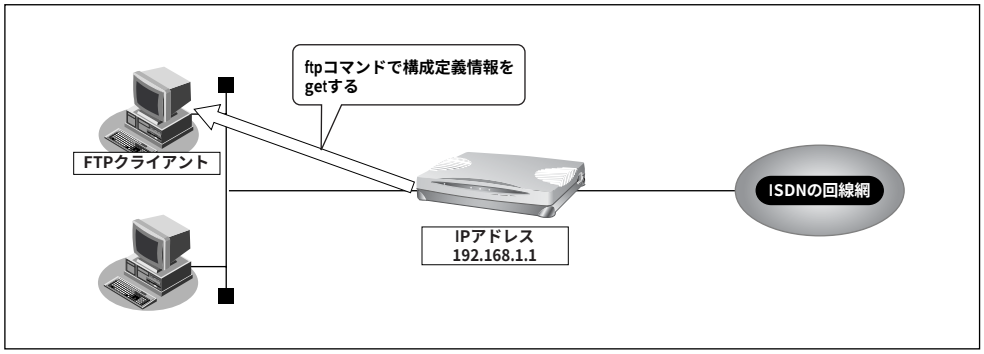
ftpコマンドのサブコマンドとして「get reset」を入力すると本装置が再起動します。

こんな事に気をつけて

セキュリティ確保のため管理者パスワードを設定することを強くお勧めします。
設定しない場合、ネットワーク上のだれからでもアクセスできるため非常に危険です。

■ FTP サーバ機能による構成定義情報の退避

パソコン上の ftp コマンドを使って、構成定義情報を退避する場合を説明します。



こんな事に気をつけて

メンテナンス作業時は、以下のことを必ず守ってください。

- **本装置の電源を切らないでください。**
- **本装置上でデータ通信していないことを確認してください。**
- **WWW ブラウザ、コンソールによる設定作業を一切していない状態で行ってください。**

● ftp コマンドの使用例

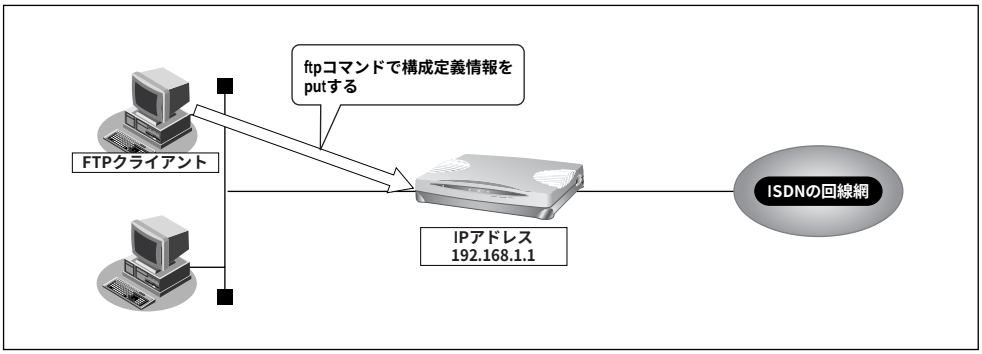
構成定義情報（config1）をパソコン上のconfig1-1 ファイルに退避する場合の例を示します。

```
# cd 構成定義情報格納ディレクトリ
# ftp 192.168.1.1                              ：本装置に接続する

Connected to 192.168.1.1.
220 Si-R130B FTP server(Ver1.0) ready.
Name(192.168.1.1:root); ftp-admin             ：ユーザ名を入力する

331 Password required for ftp-admin.
Password:                                     ：パスワードを入力する

230 User ftp-admin logged in.
ftp>bin                                       ：バイナリモードにする

200 Type set to I.
ftp>get config1 config 1-1          ：構成定義情報（config1）をconfig1-1ファイルに格納する

local: config1 remote: config1-1
200 PORT command successful.
150 Opening BINARY mode data connection for 'config1'(2753 bytes).
226 Transfer complete.
2857 bytes received in 1.10 seconds (2.44 Kbytes/s)
ftp>bye                                       ：処理を終了する

221 Goodbye.
#
```

補足 パスワードは、詳細設定の「パスワード情報」で設定した管理者パスワードを指定してください。

■ FTPサーバ機能による構成定義情報の復元

パソコン上のftpコマンドを使って構成定義情報を復元する場合を説明します。



こんな事に気をつけて

メンテナンス作業時は、以下のことを必ず守ってください。

- **本装置の電源を切らないでください。**
- **本装置上でデータ通信していないことを確認してください。**
- **WWWブラウザ、コンソールによる設定作業を一切していない状態で行ってください。**

● ftp コマンドの使用例

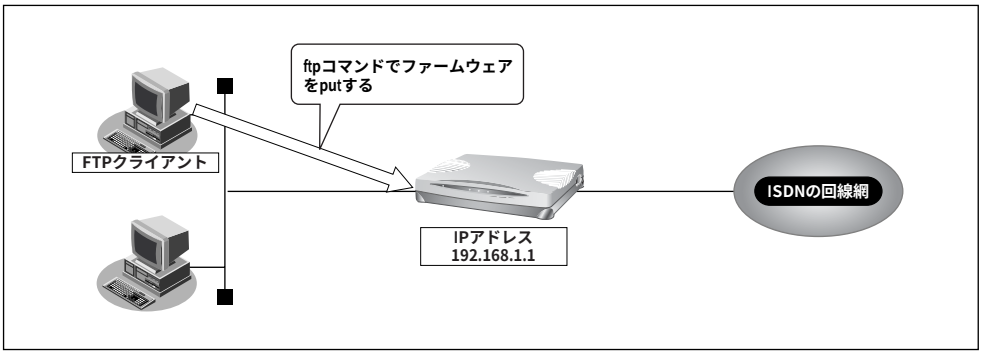
構成定義情報（config1）をパソコン上のconfig1-1 ファイルから復元する場合の例を示します。

```
# cd 構成定義情報格納ディレクトリ
# ftp 192.168.1.1                          ：本装置に接続する
Connected to 192.168.1.1.
220 Si-R130B FTP server(Ver1.0) ready.
Name(192.168.1.1:root); ftp-admin          ：ユーザ名を入力する
331 Password required for ftp-admin.
Password:                                  ：パスワードを入力する
230 User ftp-admin logged in.
ftp>bin                                    ：バイナリモードにする
200 Type set to I.
ftp>put config1-1 config1        ：config1-1 ファイルを構成定義情報（config1）として書き込む
local: config1-1 remote: config1
200 PORT command successful.
150 Opening BINARY mode data connection for 'config1'.
226- Transfer complete.
update : File information check now!
update : File information check ok.
                  ・
                  ・
226 Write complete.
2856 bytes sent in 1.10 seconds (2.44 Kbytes/s)
ftp>get reset
local: reset remote: reset
200 PORT command successful.
421 reset Request OK.bye.
ftp>bye                                    ：処理を終了する
#
```

補足
- パスワードは、詳細設定の「パスワード情報」で設定した管理者パスワードを指定してください。
- ftp コマンドのサブコマンドとして「get reset」を入力すると本装置が再起動します。

■ FTP サーバ機能によるファームウェアの更新

パソコン上の ftp コマンドを使ってファームウェアを更新する場合の例を示します。



こんな事に気をつけて

メンテナンス作業時は、以下のことを必ず守ってください。

- **本装置の電源を切らないでください。**
- **本装置上でデータ通信していないことを確認してください。**
- WWW ブラウザ、コンソールによる設定作業を一切していない状態で行ってください。
- **ファームウェアを更新する前に、構成定義情報を退避しておいてください。**

● ftp コマンドの使用例

ファームウェアをパソコン上から更新する場合について説明します。

```
# cd 構成定義情報格納ディレクトリ
# ftp 192.168.1.1                          ：本装置に接続する
Connected to 192.168.1.1.
220 Si-R130B FTP server(Ver1.0) ready.
Name(192.168.1.1:root); ftp-admin          ：ユーザ名を入力する
331 Password required for ftp-admin.
Password:                                  ：パスワードを入力する
230 User ftp-admin logged in.
ftp>bin                                    ：バイナリモードにする
200 Type set to I.
ftp>put Si-R130BSOFT.ftp firmware          ：ファームウェアを書き込む
local: Si-R130BSOFT.ftp remote: firmware
200 PORT command successful.
150 Opening BINARY mode data connection for 'firmware'.
226 Transfer complete.
update : Transfer file check now!
update : Transfer file check ok.
                  ・
                  ・
226 Write complete.
631 1966 bytes sent in 97.80 seconds (6.31 Kbytes/s)
ftp>get reset                              ：本装置を再起動する
local: reset remote: reset
200 PORT command successful.
421 reset Request OK.bye.
ftp>bye                                    ：処理を終了する
#
```

補足
- パスワードは、詳細設定の「パスワード情報」で設定した管理者パスワードを指定してください。
- ftp コマンドのサブコマンドとして「get reset」を入力すると本装置が再起動します。

第8章　トラブルシューティング

8

この章では、

本装置をご使用になっている際、トラブルがあった場合の原因の調査方法と対処方法について説明します。

回線料金がおかしいと思ったら

■ 超過課金の見分け方

超過課金とは、利用者が意図しない回線接続や回線使用が長期的に続き、その結果として必要以上の回線料金が課金されることを言います。または、異常課金と言います。

超過課金が発生する原因は2つあります。

(1)回線未接続状態でLANに接続したパソコンなどから利用者の意図しないデータが回線に流れ、その結果、回線が接続することが頻発する場合。

(2)回線を接続したあとに、LANに接続されたパソコンなどから利用者の意図しないデータが定期的に発信され、回線が長時間接続されたままの状態になる場合。

これらは課金情報を確認し、利用状況と照らし合わせることで超過課金が発生していることがわかります。課金情報で表示されている回線接続していた時間が利用時間よりも極端に長い場合には、超過課金が発生している可能性があります。

☛ 参照 「課金情報を確認する」（P.650）

■ 超過課金が発生した原因を調べる

ここでは、超過課金が発生する代表的な事例をあげ、それぞれの調査方法と対処方法について説明します。

WAN側にRIPパケットが流れている場合

【現象】

LAN側のパソコンの通信が終了したにもかかわらず、長時間回線が自動切断されない。

【原因】

WAN側接続相手（たとえばプロバイダのルータ）がダイナミックルーティングを使用し、本装置に経路情報（RIPパケット）を送信してくる場合に、通信がないにもかかわらず回線が接続されたままになることがあります。

【調査方法】

- まずLAN側端末が回線を使用した通信を行っていないことを確認します。
- もし、パソコンが通信をしているかが判断できない場合には、それらのパソコンを電源OFFします。
- この状態で本装置の表示ランプを監視します。ここでB1またはB2ランプが一定間隔（15～45秒間隔）で点滅していた場合には、経路情報などのなんらかのデータが接続相手から送られてきていることになります。
- さらに上記ランプが点滅するたびにIP統計情報を確認します。表示されたIP統計情報の中のudp XXX datagrams receivedの部分の数字が確認するたびに増加していれば、原因は経路情報（RIP）受信によるものです。

【対処方法】

IP フィルタリング機能を使って経路情報（RIP）を破棄するように以下の項目を設定してください。

- 動作　→ 遮断
- プロトコル　→ udp
- 送信元情報（IP アドレス）　→ なにも設定しない
- 送信元情報（アドレスマスク）→ なにも設定しない
- 送信元情報（ポート番号）　→ なにも設定しない
- 宛先情報（IP アドレス）　→ なにも設定しない
- 宛先情報（アドレスマスク）　→ なにも設定しない
- 宛先情報（ポート番号）　→ 520
- TCP 接続要求　→ 対象外
- TOS　→ なにも設定しない

これにより、接続相手から経路情報（RIP）が送出されてきても無通信監視時間（初期設定値は 60 秒）を経過すると回線は自動的に切断されるようになります。

補足 上記以外にも本装置の設定でWAN側にダイナミックルーティング機能を使用する設定になっていることが原因の場合もあります。この場合は、「ルータ設定」－「相手情報」－「ネットワーク情報」－「ダイナミックルーティング」の設定で、RIP 送信の項目が「送信しない」であることを確認してください。

☛ 参照 「IP フィルタリング機能を使う」（P.429）、「IP 統計情報を見る」（P.614）

パソコンからの自動送信パケット

【現象】

LAN側のパソコンなどからの通信がないにもかかわらず、いつのまにか本装置からの発信により回線接続してしまう。

【原因】

Windows® 95 ／ 98 ／ Me ／ 2000、Windows NT® のパソコンは、利用者の意図とは無関係に（利用者が通信している意識がないにもかかわらず）自動的にパケットを回線側に送出してしまう場合があります。

【調査方法】

- 利用者が通信していないこと（WWW ブラウザや電子メールなど使用していないこと）を確認してください。
- この状態で回線の発信が起きている場合には、表示メニューの回線ログを参照して発信の契機となった事象を確認してください。
- 「発信ログ　IP パケットの転送が発生しました。」の場合には、パソコンが回線側にパケットを送信しています。→【対処方法 1】
- 「発信ログ　DNS 要求が発生しました。」の場合には、パソコンが本装置の ProxyDNS 機能を利用しようとして DNS 要求を送信しています。→【対処方法 2】

【対処方法1】

IPフィルタリング機能を使ってNetBIOS over TCPの情報を回線側に流さないように設定してください。

☛ 参照 「IPフィルタリング機能を使う」（P.429）

【対処方法2】

URLフィルタ機能を使ってWindows®のワークグループ名のアクセスを禁止してください。この場合にはアクセスを禁止するドメイン名に「<ワークグループ名>＊」を指定してください。

☛ 参照 「特定のURLへのアクセスを禁止する （URLフィルタ機能）」（P.529）

【対処方法3】

パソコンが送信するDNSパケットの問い合わせタイプ（QTYPE）がA（1）、PTR（12）以外の場合、DNS問い合わせタイプフィルタ機能を使って、特定の問い合わせタイプのパケットを破棄することができます。DNSパケットの問い合わせタイプ（QTYPE）は、本装置のシステムログ情報に以下の情報が記録されていることから確認できます。
「proxydns:[<QTYPE>:<QNAME>]from<IPアドレス>to<ネットワーク名>」

☛ 参照 「DNS問い合わせタイプフィルタ機能」（P.476）

デフォルトルートどうしで接続している場合

【現象】

パソコン上のアプリケーション（WWWブラウザや電子メールなど）が異常終了し、数分から数十分間回線が接続されたままになる。

【原因】

自側および相手側本装置の両方でデフォルトルートの設定がされていることが原因です。

【調査方法】

両者のデフォルトルートの設定内容を確認してください。

【対処方法】

どちらかの本装置の設定からデフォルトルートの設定を外してください。

☛ 参照 「事業所LANをISDNで接続する」（P.115）

テレホーダイ機能の設定を誤った場合

【現象】

パソコンなどLAN側端末の通信が終了したにもかかわらず、長時間回線が自動切断されない。

【原因】

テレホーダイ機能の設定ミスによるものです。

【調査方法】

- 表示ランプのB1またはB2ランプを監視してください。このランプが点滅しないで、緑色の点灯状態が続いていることを確認してください。これはデータの送受信がなく、また電話などアナログ機器による通信もないのに回線が接続され続けている状態であることを意味します。
- 無通信監視タイマの設定に誤りがないかを確認してください。これは、「かんたん設定」－「オプション設定」－「無通信監視タイマ」で確認できます。この無通信監視タイマが0や極端に大きな値になっていないことを確認してください。

【対処方法】

テレホーダイの時間帯を正しく設定し直してください。

☛ 参照 「テレホーダイ機能を使う」（P.607）

スケジュール機能の設定を誤った場合

【現象】

スケジュール機能でテレホーダイ時間帯以外は発信抑止しているにもかかわらず、発信してしまう。

【原因】

スケジュール機能の設定誤りが原因です。

【調査方法】

- スケジュール機能の設定を確認してください。ここで予約時刻、終了時刻が正しく設定されているかを確認してください。
- さらに内部時計の時刻設定も確認してください。

【対処方法】

上記スケジュール機能および内部時計の時刻設定をそれぞれ正しく設定し直してください。

☛ 参照 「スケジュール機能を使う」（P.551）、「時計を設定する」（P.71、P.104）

接続保持機能の設定を誤った場合

【現象】

LAN側端末の通信の有無にかかわらず回線が常に接続されたままになる。

【原因】

フレッツ・ISDNなどの通信料金が定額な回線以外で接続保持の設定を「常時」にしている。

通信料金が定額な回線であっても、常時接続に設定した接続先がMP接続の可能な設定になっているため2ch同時に接続されている。

通信料金が定額な回線であっても、複数の接続先に常時接続を設定しているため2ch同時に接続されている。

【調査方法】

- まずLAN側端末が回線を使用した通信を行っていないことを確認します。
- パソコンが通信をしているかが判断できない場合は、それらのパソコンを電源OFFします。
- この状態で本装置の電源を入れて起動し、起動終了後から表示ランプを監視します。ここでB1またはB2ランプが点灯し、その状態が続く場合は、常時接続機能による接続が行われた可能性があります。
- さらに上記接続が行われたあと、シスログを確認します。表示されたシスログにby keep connectionの文字があれば常時接続機能が働いていることが確認できます。

【対処方法】

「ルータ設定」－「相手情報」－「ネットワーク情報」－「接続先情報」の接続保持の設定を確認してください。従量課金の回線には常時接続を設定しないでください。

フレッツ・ISDNの場合、通信料金が定額になるのは1ch分の通信だけであり、ほかの1chを通信に使ってしまうと課金が発生するので、MP接続を行う接続先や複数の接続先に常時接続を設定しないでください。

LAN側のパソコンを移設した場合

【現象】

ほかのLANに接続してあったパソコンなどを本装置のLANに移設したら、頻繁に回線発信が行われるようになった。または回線が切断されなくなってしまった。

【原因】

そのパソコンが以前接続されていたLAN環境で運用されていたサービスやアプリケーションがWAN環境にはふさわしくないものであることが原因です。

【調査方法】

問題のパソコンが立ち上がっているときと電源がOFFされているときとで、上記現象の発生の有無が変わることを確認してください。

【対処方法】

詳細な原因は、問題となるサービスやアプリケーションに依存するため対応方法はさまざまです。特定のサーバや特定のサービスへのアクセスが原因の場合、IPフィルタリング機能を使用して無意味な発信を抑止します。またスケジューリング機能を使用することで防止できる場合もあります。どの場合にも回線ログ情報を確認して発信の契機となったサービスやアプリケーションを特定するか、またはそのパソコンの以前の利用者にサービス内容やアプリケーションの設定内容を確認するなどして解決してください。

☛ 参照 「回線ログ情報で運用状況を確認する」（P.619）

本装置を移設した場合

【現象】

ほかの環境に接続していた本装置を移設した、または本装置が関係するネットワークの一部または全部が変更になったところ、回線発信が頻発するようになった。または回線が切断されなくなった。

【原因】

本装置の設定が新しい環境にふさわしくないものであることが原因です。

【調査方法】

特に必要ありません。

【対処方法】

本装置の設定を一度ご購入時の状態に戻したあと、最初から設定し直してください。

☛ 参照 「ご購入時の状態に戻すには」（P.665）

課金情報を確認する

本装置の電源を入れてから現在までの、ISDN回線に対する課金情報を確認することができます。

1.　本装置のトップページで、画面上部の［表示］アイコンをクリックします。

表示メニューが表示されます。

2.　表示メニューで「課金情報」をクリックします。

データ通信課金情報、接続先別データ通信課金情報、アナログポート課金情報、マルチTA課金情報が表示されます。

3.　以下の項目を確認します。

【データ通信課金情報】

- 通信総時間　→ データ通信の通信時間の累計です。
- 課金合計金額　→ データ通信の通信料金の累計です。
- 最長通信　→ データ通信の過去の記録で、1回の通信での最長の時間、通信料金、接続相手先です。
- 最高課金　→ データ通信の過去の記録で、1回の通信での最高金額、通信時間、接続相手先です。
- 最終接続　→ データ通信の最新の通信での、通信時間、通信料金、接続相手先です。

【接続先別データ通信課金情報】

接続先ごとの通信時間の累計および通信料金の累計が表示されます。

【マルチTA課金情報】

- 通信総時間　→ マルチTA通信の通信時間の累計です。
- 課金合計金額　→ マルチTA通信の通信料金の累計です。

■データ通信課金情報クリア

→［データ通信課金情報クリア］ボタンをクリックすると、現在保持している上記3つの情報をすべてクリアします。

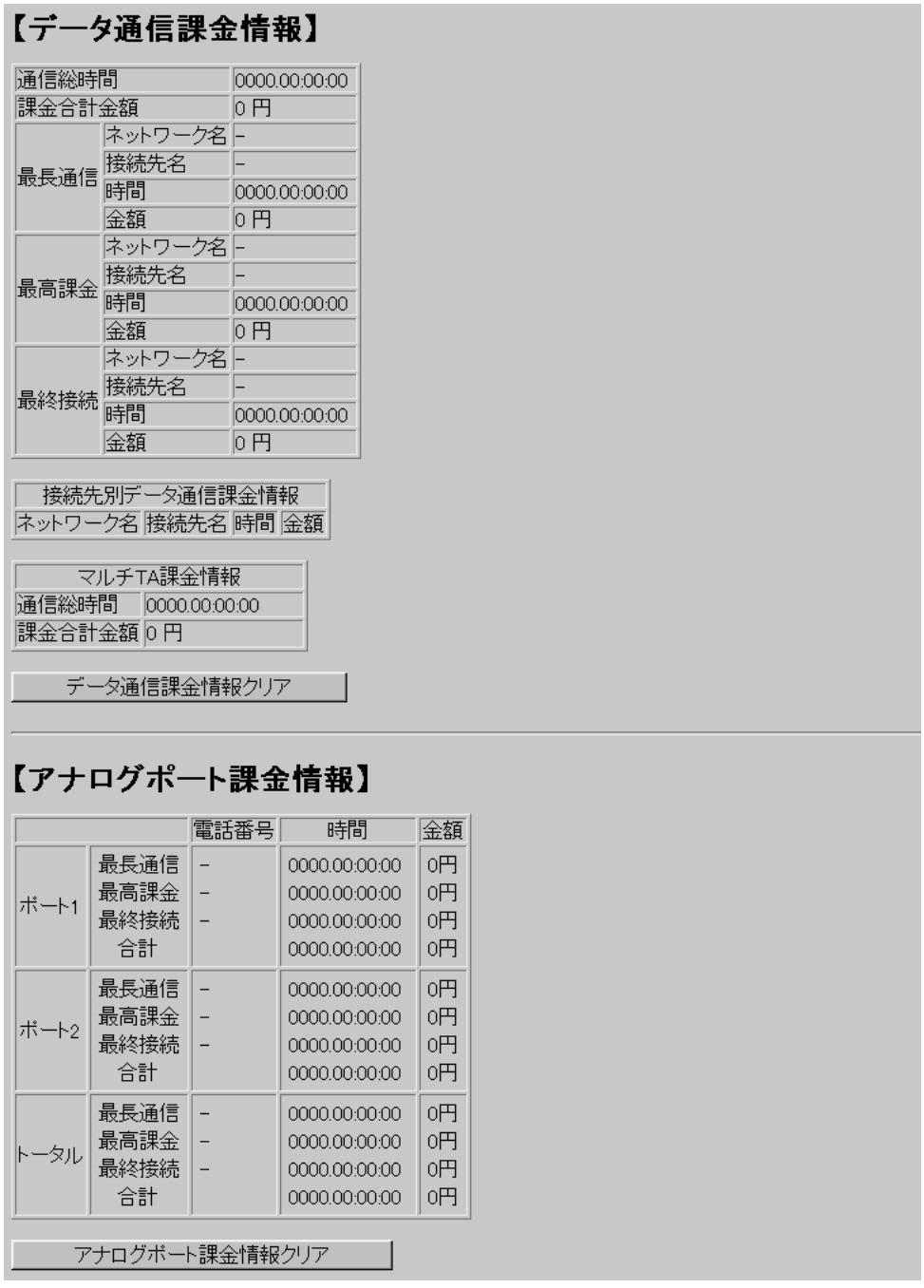
【アナログポート課金情報】

- 最長通信　→ アナログ通信の過去の記録で、1回の通信での最長の時間、通信料金、接続相手先です。
- 最高課金　→ アナログ通信の過去の記録で、1回の通信での最高金額、通信時間、接続相手先です。
- 最終接続　→ アナログ通信の最新の通信での、通信時間、通信料金、相手先電話番号です。
- 合計　→アナログ通信の通信時間と通信料金の累計です。

■アナログポート課金情報クリア

→［アナログポート課金情報クリア］ボタンをクリックすると、現在保持しているアナログポート課金情報をすべてクリアします。

■全ての課金情報クリア→［全ての課金情報クリア］ボタンをクリックすると、現在保持している課金情報をすべてクリアします。



【データ通信課金情報】

通信総時間		0000.00:00:00
課金合計金額		0 円
最長通信	ネットワーク名	-
	接続先名	-
	時間	0000.00:00:00
	金額	0 円
最高課金	ネットワーク名	-
	接続先名	-
	時間	0000.00:00:00
	金額	0 円
最終接続	ネットワーク名	-
	接続先名	-
	時間	0000.00:00:00
	金額	0 円

接続先別データ通信課金情報			
ネットワーク名	接続先名	時間	金額

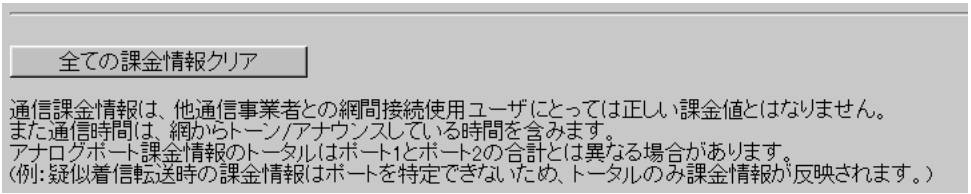
マルチTA課金情報	
通信総時間	0000.00:00:00
課金合計金額	0 円

データ通信課金情報クリア

【アナログポート課金情報】

		電話番号	時間	金額
ポート1	最長通信	-	0000.00:00:00	0円
	最高課金	-	0000.00:00:00	0円
	最終接続	-	0000.00:00:00	0円
	合計		0000.00:00:00	0円
ポート2	最長通信	-	0000.00:00:00	0円
	最高課金	-	0000.00:00:00	0円
	最終接続	-	0000.00:00:00	0円
	合計		0000.00:00:00	0円
トータル	最長通信	-	0000.00:00:00	0円
	最高課金	-	0000.00:00:00	0円
	最終接続	-	0000.00:00:00	0円
	合計		0000.00:00:00	0円

アナログポート課金情報クリア



こんな事に気をつけて

- **本書の表記で使われる通信料金とは、INS ネット64基本サービスの「料金情報通知」をもとに、本装置のソフトウェアが算出した値です。算出される値は、お客様の契約や回線利用状況により異なりますので、請求金額とは必ずしも一致しません。**
  たとえば以下のような場合があります。
  - **INS テレホーダイ利用時**
  - **NTT DoCoMo 以外の自動車電話・携帯電話と通話した場合**
  - **PHS と通話した場合（PIAFS によるデータ通信も含む）**
- **本装置の電源を切断すると、課金情報はすべてクリアされます。**

通信ができない場合には

通信ができない場合、さまざまな原因があります。まず、以下を参考に本装置の動作状況を確認してください。

ヒント

◆ 回線ログやエラー番号からトラブルの原因を探る

表示メニューの「回線ログ」ページに表示された内容やメンテナンスメニューの「エラーログ情報」ページに表示されたエラー番号から、エラーの原因をある程度特定できます。

回線ログ情報やエラーログ情報ページのプリントアウトを保管しておくことをお勧めします。

⚠警告

- **決してご自身では修理を行わないでください。**
- **本装置が故障した場合は、富士通の技術者または富士通が認定した技術員によるメンテナンスを受けてください。**

■ 起動時の動作に関するトラブル

本装置起動時のトラブルには、以下のようなものがあります。

● **POWERランプがつかない**

【原因】 電源ケーブルがコンセントに正しく接続されていない。

【対処】 電源ケーブルをコンセントに正しく接続してください。

【原因】 本装置の電源スイッチが入っていない。

【対処】 本装置の電源スイッチが「｜」側へ押されているか確認してください。

● **電源を入れてしばらくしてもCHECKランプが消灯しない**

【原因】 本体に異常が発生しました。

【対処】 富士通の技術員へ連絡してください。

● **ISDN回線につないで電源を投入したら、B1／B2ランプが橙色で点滅している**

【原因】 ISDN回線ケーブルがきちんと差し込まれていない。

【対処】 ISDN回線ケーブルをきちんと差し込んでください。

【原因】 ISDN回線の極性が反転している。

【対処】 本装置の電源を切断し、回線極性スイッチの設定で極性を変更して、再度電源を投入してください。

【原因】 ISDN回線で同期はずれが発生している。

【対処】 NTTに調査を依頼してください。

【原因】 回線契約（専用線）と本装置の設定が間違っている。

【対処】 本装置の設定を回線契約に合わせて正しく設定し直してください。

■ 本装置設定時のトラブル

● ブラウザでマニュアルどおりのURLを指定したが本装置のトップページが表示されない

【原因】 接続に誤りがある。または、10BASE-Tケーブルが断線している。

【対処】 接続したHUBポートに該当するHUB LEDが点灯しているかを確認してください。点灯していない場合には正しく接続されていないか、ケーブルが断線している可能性があります。パソコンと本装置に10BASE-Tケーブルがきちんと差し込んであることを確認し、それでもHUB LEDが点灯しない場合には別の10BASE-Tケーブルに交換してください。

【原因】 パソコンのIPアドレスやネットマスクが間違っている。

【対処】
- パソコンの設定でIPアドレスやネットマスクを設定している場合には、本装置と通信できるIPアドレスが設定されているかどうかを確認してください。
  本装置のIPアドレスやネットマスクを変更していない場合は、パソコンを以下の範囲で設定する必要があります。

  IPアドレス　　：192.168.1.2～192.168.1.254

  ネットマスク　　：255.255.255.0
- 本装置のDHCPサーバ機能を利用している場合には、パソコンを再起動してください。
- Windows® 98の場合は、「プライベートIPアドレス自動割り当て」機構により、DHCPサーバから自動取得する設定にしていても、169.254.XX.XXというIPアドレスが設定される場合があります。この場合はIPアドレスを固定で割り当てても通信できないことが多いため、ネットワークドライバとTCP/IPを設定し直してください。

補足 パソコン側のIP設定は、winipcfgコマンド（Windows® 95/98/Meの場合）やipconfigコマンド（Windows NT®、Windows® 2000/XP、Windows Vista®の場合）で確認できます。

【原因】 パソコンとTAでインターネットに接続したときの設定が残っている。

【対処】 LANインタフェースのIPアドレスを再割り当てするため、パソコンを再起動してください。

【原因】 WWWブラウザの設定が間違っている。

【対処】 ・ WWWブラウザ（Microsoft® Internet Explorer Version 6.0/7.0）の場合、［ツール］－［インターネットオプション］－［接続］のインターネットオプション画面のダイヤルアップの設定で「ダイヤルしない」が選択されていることを確認してください。「通常の接続でダイヤルする」が選択されているとWWWブラウザを起動するたびにモデムやTAからインターネットへ接続しようとして本装置と通信できない可能性があります。

・ WWWブラウザの設定でProxyサーバの設定が有効になっている可能性があります。［ツール］－［インターネットオプション］－［接続］－［LANの設定］のプロキシサーバの欄で「プロキシサーバを使用する」のチェックを外し、Proxyサーバを使用しない状態にしてください。また、Proxyサーバを使用する場合は、「プロキシの設定」の例外の欄に本装置のIPアドレス（本装置のIPアドレスを変更していない場合は192.168.1.1）を追加してください。

【原因】 パソコンのARPエントリの値がおかしくなっている。

【対処】 本装置と同じIPアドレスを持つ機器と通信した直後に、パソコンの電源を落とさないまま本装置へ接続変更を行った場合には通信できません。しばらく待つか、パソコンを再起動してください。

【原因】 本装置と同じIPアドレスを持つ機器が接続されている。

【対処】 IPアドレスが重複している機器がLAN上に存在すると、正しく通信できません。本装置から設定するパソコン以外を接続している10BASE-Tケーブルを外し、パソコンを再起動してください。

【原因】 本装置のIPアドレスが変更されている。

【対処】 変更後の本装置のIPアドレスを指定してください。

【原因】 パソコンのIPアドレスを変更していない。

【対処】 本装置のIPアドレスを変更した場合、必ずパソコン側のIPアドレスもそれに合わせて変更します。

1. 本装置のDHCPサーバ機能を利用している場合：

   パソコンを再起動してください。

2. 本装置のDHCPサーバ機能を利用していない場合：

   パソコンのIPアドレスを本装置と直接通信可能なアドレスに変更してください。また、ネットマスクを本装置に設定した値と同じ値に設定してください。このとき、DNSサーバのIPアドレスも忘れずに入力してください。

● WWWブラウザの［戻る］ボタン、またはエラー画面の［1つ前に戻る］ボタンで戻ったあと、［更新］ボタンをクリックすると入力したパスワードが削除された

【原因】 WWWブラウザの仕様です。

【対処】 ご使用のWWWブラウザによっては、画面を移動するとパスワード情報（入力データが「*」で表示されるテキストボックス）が削除されます。この場合は、パスワード情報を再入力してください。

● 変更した本装置のIPアドレスがわからなくなった
本装置に設定した管理者パスワードがわからなくなった

【対処】 本装置をご購入時の状態に戻してください。初期値にすることで管理者パスワードを削除し、IPアドレスを「192.168.1.1」に戻すことができます。それまでに設定した内容はすべて消えてしまいますので、最初から設定し直してください。

☛ 参照 「ご購入時の状態に戻すには」（P.665）

■ 回線への接続に関するトラブル

本装置で回線に接続する際のトラブルには、以下のようなものがあります。

補足
- 回線に接続できないときには、まず表示メニューで「回線ログ情報」を選択して、エラーの原因を確認してください。
- 「回線ログ情報」では原因が判別できなかった場合は、以下のチェック項目を確認してください。

● ISDNで相手先につながらない（B1／B2ランプがまったく点灯しない）

このような場合は、まず表示メニューで「回線ログ情報」をクリックして、エラーの原因を確認してください。ログの内容およびISDN理由表示番号から原因を特定することができます。

【原因】 接続先が話し中である。

【対処】 時間をおいてから接続し直してください。

【原因】 接続先の電話番号、サブアドレスの設定に誤りがある。

【対処】 接続先の電話番号、サブアドレスを正しく設定し直してください。

補足 詳細設定で設定してある場合は、「接続先情報設定」で設定を変更します。

【原因】 接続先から拒否されている。

【対処】 接続先の管理者に問い合わせてください。

【原因】 モジュラジャックの極性が反転している。

【対処】 モジュラジャックの極性が逆転している可能性があります。回線極性スイッチの設定を切り替えてください。

【原因】 課金制限値、または接続時間制限値を超えている。

【対処】 課金情報を確認し、設定した制限値を超えていないかどうかを確認してください。初期値として「金額：3000円」が設定されています。設定を変更するか、課金情報をクリアしてください。課金情報のクリアは、初期値として「毎週金曜日の0:00」が設定されています。

【原因】 スケジュール情報の月間／週間予約の動作に発信抑止を設定している場合、予約時間／終了時間、または本装置の時刻が正しく設定されていない。

【対処】 発信抑止の予約時間／終了時間、または本装置の時刻を正しく設定し直してください。

【原因】 発信が連続して失敗した場合、3分間に2回を超える再発信を行おうとすると、本装置が自動発信を抑止する。

【対処】 回線ログの情報から発信失敗の原因を確認してください。また、接続先情報の設定内容を確認し、誤りがあった場合は正しく設定し直してください。

【原因】 認証エラーなどの発信失敗が30回連続して発生したため、本装置が自動発信を抑止している。

【対処】 回線ログの情報から発信失敗の原因を確認してください。また、接続先情報の設定内容を確認し、誤りがあった場合は正しく設定し直してください。接続先情報の設定内容を変更して設定反映するか、または装置を再起動すると自動発信の抑止状態は解除されます。

● ISDNで相手先につながらない（B1／B2ランプは一時は点灯するが、すぐ消灯する）

PPPネゴシエーションで切断されている可能性があります。表示メニューの「回線ログ」およびメンテナンスメニューの「PPPフレームトレース」で原因を特定することができます。

【原因】 認証に失敗した。

【対処】 送信する認証ID、認証パスワードを正しく設定してください。

【原因】 PPPネゴシエーションに失敗した。

【対処】 接続先に適合するように設定を変更してください。

補足 PPPネゴシエーションの結果は「回線ログ情報」に、動作に関する情報は「PPPフレームトレース情報」に記載されます。

● ISDNで相手先につながらない（B1／B2ランプは点灯しているが、通信ができない）

【原因】 パソコンのルーティング情報の設定に誤りがある。

【対処】 パソコンのルーティング情報を正しく設定し直してください。

【原因】 パソコンのDNSサーバアドレスの設定に誤りがある。

【対処】 DHCPを利用していない場合には、以下のとおり設定してください。

1. 本装置のProxyDNSを利用する場合：

   DNSサーバIPアドレスに本装置のIPアドレスを設定してください。

2. 本装置のProxyDNSを利用しない場合：

   正しいDNSサーバIPアドレスを設定してください。

【原因】 本装置のルーティング情報の設定に誤りがある。

【対処】 本装置の「ダイナミックルーティング情報」、「スタティックルーティング情報」を正しく設定し直してください。

【原因】 接続先がDNSサーバアドレスの通知機能を持っていない。

【対処】 かんたん設定（インターネットへ）の場合は、プロバイダから通知されたDNSサーバアドレスを指定してください。

詳細設定の場合は、接続先情報設定にDNSサーバアドレスを指定してください。

【原因】 IP フィルタによって遮断されている。

【対処】 IP フィルタの設定を見直してください。

● HSDで相手先につながらない

【原因】 本装置の設定に誤りがある。

【対処】 ・「回線情報設定」で、正しい回線を選択しているかどうかを確認してください。
・「LAN情報設定」および「ネットワーク情報設定」で、正しいIPアドレス、ルーティング情報を設定しているかどうかを確認してください。
・「接続先情報設定」で、正しいDNS サーバを設定しているかどうかを確認してください。

【原因】 パソコンの設定に誤りがある。

【対処】「ISDNで相手先につながらない（B1／B2ランプは点灯しているが、通信ができない)」場合を参考にして、正しく設定し直してください。

【原因】 HSDの回線自体に異常がある。

【対処】 NTTに調査を依頼してください。

● 回線がつながりっぱなしになっている

【原因】 接続先から定期的にデータを受信している。

【対処】 接続先の装置側でRIP、ICMP、Keep Aliveなどのパケットを送信する設定になっていないか確認してください。

【原因】「LAN情報設定」、または「ネットワーク情報設定」の設定に誤りがある。

【対処】 ・「LAN情報設定」および「ネットワーク情報設定」で、RIP送信しない／RIP受信しない、に設定を変更してください。
・「LAN情報設定」および「ネットワーク情報設定」で、IPアドレス、ルーティング情報設定に誤りがないかを確認してください。

【原因】 ネットワーク上のコンピュータが通信を行っている。

【対処】 コンピュータが通信していないかどうか、またアプリケーションが定期的に通信を行う設定になっていないかどうかを確認してください。

【原因】 テレホーダイ機能を使用している。

【対処】 テレホーダイ機能を停止してください。

【原因】 回線接続中にパソコンやワークステーションが誤動作した。

【対処】 本装置の電源を切断してください。

● Windows® のアクティブデスクトップを使用すると、時々回線が自動的につながってしまう

アクティブデスクトップのMicrosoft® Internet Explorerチャンネルバーの中のサイトを「購読」する設定になっているなどの原因があります。この場合は、以下の手順で設定を変更してください。

1. Microsoft® Internet Explorerのメニューから［お気に入り］をクリックする。
2. ［購読の管理］をクリックする。
3. 選択されているチャンネルを削除する。

■ データ通信に関するトラブル

本装置でデータ通信を行う際のトラブルには、以下のようなものがあります。

● 回線はつながるが、データ通信ができない

【原因】 IP フィルタリング、ルーティング情報（本装置／相手）、またはNATの設定が間違っている。

【対処】 ・ IP フィルタリングの設定やNATの設定をご利用のネットワーク環境や目的に合わせて、設定し直してください。
・ 設定し直しても、通信できない場合は、富士通の技術員へ連絡してください。

● 回線は接続されてPingの応答は正常だが、WWWブラウザや電子メールは通信できない

【原因】 DNSの設定が間違っている。

【対処】 本装置のDHCP サーバおよびProxyDNS を使用するか、パソコン側でDNS サーバアドレスを正しく設定し直してください。

● 回線は接続されるが「このサーバに対するDNS項目がありません」などメッセージが表示されてブラウザの表示が止まってしまう

【原因】 DHCP サーバ機能を利用している場合、本装置の設定終了直後はパソコン側にDNSアドレス情報が含まれていないため、WWW ブラウザでURL「http://www.fujitsu.com」を入力したときに「www.fujitsu.com」のIPアドレスを取り出せず、このようなメッセージが表示されます。

【対処】 パソコンを再起動して、DHCP（DNS サーバのIP アドレス）の最新情報をパソコン側に確実に反映させてください。

【原因】 DHCP サーバ機能を利用していない場合、DNS サーバのIP アドレスを手入力する必要があります。

【対処】 マニュアルに記載されている情報（IP アドレス／ネットマスク／ゲートウェイ）に加え、DNSサーバのIPアドレスを設定してください。

● **詳細設定でIPアドレスを変更し再起動したらまったくつながらなくなった**

【原因】 DHCPの設定が古い。

【対処】 かんたん設定の場合、IPアドレス変更と連動してDHCPの割り当て先頭IPアドレスが書き変わりますが、詳細設定の場合は連動しないため、個別に設定を変更する必要があります。書き変えない場合、以下の状態になります。

例）本装置のIPアドレスを「192.168.1.1」から「172.32.100.1」に変更した場合

	［変更前］		［変更後］	
	IPアドレス	DHCP先頭IPアドレス	IPアドレス	DHCP先頭IPアドレス
かんたん設定	192.168.1.1	192.168.1.2	172.32.100.1	172.32.100.2
詳細設定	192.168.1.1	192.168.1.2	172.32.100.1	192.168.1.2

● **ブラウザを立ち上げると勝手に回線が接続されてしまう**

【原因】 ブラウザ起動時にインターネット上のページを表示するよう指定している。

【対処】 ブラウザ起動時に表示されるページに何も指定しないか、ローカルディスク上のファイルを指定してください。

● **「かんたん設定」のあと、疎通確認のためにpingを実行したが相手からの応答がない（発信もされない）**

【原因】「かんたん設定」で設定した際、「かんたんフィルタ」がかけられたためです。「かんたんフィルタ」では、「回線が切断されている時はICMP（ping）を通さない」設定になっています。

【対処】 pingを利用する場合は、IPフィルタリングの設定で、ICMPをフィルタリング対象から外してください。

● **本装置のDHCPサーバ機能を使用している環境で、「詳細設定」のLAN情報設定などの設定を変更し、“設定反映”したあと、通信できなくなった**

【原因】 パソコンに変更前のIPアドレスの経路情報が残っている。

【対処】 一部のUNIX®系OSでDHCPクライアントとして動作している場合、パソコンのIPアドレスを変更しても古い経路情報が残っており、正しく通信できない場合があります。この場合、パソコンを再起動して最新の情報をパソコンへ確実に反映させるか、またはIPアドレスを固定設定で使用してください。

● **フレッツ・ISDNを使用している環境で、回線はつながるが、一部のホームページが表示できない**

【原因】 フレッツ・ISDNを使用している場合、接続地域やプロバイダによってはフレッツ・ADSLと同じ設備を経由している可能性があります。その場合、フラグメントを禁止してICMPを遮断している一部のWebサイトを表示できないことがあります。

【対処】 本装置のMSS書き換え機能を使用してWebサーバとの間でパケット分割が起きないようにすることで解決する場合があります。書き換えサイズを1414バイトに設定してください。

■ アナログ機器に関するトラブル

本装置につないだアナログ機器を利用する際に発生する主なトラブルとその対処方法としては、以下のようなものがあります。

● アナログ機器で発信・着信できない

【原因】 本装置の電源が入っていない。

【対処】 電源スイッチが「｜」側へ押されていることを確認してください。

【原因】 停電中である。

【対処】 停電が復旧するまでお待ちください。

【原因】 LANに高い負荷がかかっており、装置内部でアナログポートの制御ができなくなっている。

【対処】 装置前面にあるLANランプが消灯に近い状態のときはLANに対して高い負荷がかかっている状態です。この場合、LAN上での通信をいったん停止し、アナログ機器が使用できることを確認してください。

【原因】 接続に誤りがある。

【対処】 本装置のアナログポートとアナログ機器のモジュラケーブルの接続を確認してください。

【原因】 アナログポートの設定に誤りがある。

【対処】「アナログポート情報」で、着信条件を確認してください。

【原因】 1つのアナログポートに2台以上のアナログ機器を接続している。

【対処】 1つのアナログポートにはアナログ機器を1台だけ接続してください。

【原因】 本装置が対応していない電話機を使用している。

【対処】 ・ トーン式（プッシュ式）の電話機を使用していることを確認してください。
・ 電話機のトーン／パルス切り替えスイッチが、「トーン」、または「PB」に設定されていることを確認してください。

● 本装置に接続された電話機に電話しても呼び出し音は聞こえるが、だれも電話に出ない

【原因】 電話機をつないでいない方のアナログポートに着信している。

【対処】 空いているアナログポートの設定を「使用しない」に変更してください。「アナログポート情報」（空いているアナログポートを選択）で「接続機器」を「なし」に選択したあとに、［設定反映］をクリックしてください。

【原因】 グローバル着信しないに設定されている。

【対処】「アナログポート情報」で「グローバル着信」を「する」に変更してください。変更後、［設定反映］ボタンをクリックしてください。

● アナログポートにモデム経由でつないでいる電話が使えない

【対処】 1つのアナログポートにはアナログ機器を1台だけ接続してください。

■ その他のトラブル

その他、以下のようなトラブルがあります。

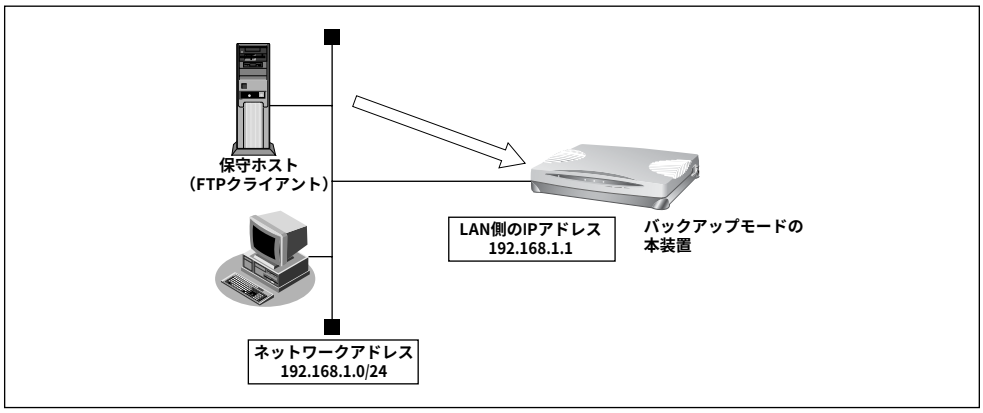
● データ通信はほとんどしていないのに、通信料金が高い

【対処】 ・「回線ログ情報」と「システムログ情報」を確認してください。

・ Windows®（TCP上のNetBIOS）環境のネットワークでは、セキュリティ上の問題と、超過課金を抑えるために、ポート番号137～139の外向きの転送経路をふさいでおく必要があります。必要に応じて「IPフィルタリング」を設定し直してください。

ファームウェア更新に失敗したときには（バックアップファーム機能）

停電などでファームウェアの更新に失敗し、本装置を起動できなくなった場合、バックアップ用のファームを起動し、ネットワーク上のFTPクライアントからファームウェアを転送することにより、正常な状態に復旧することができます。



補足
- リセットスイッチを押下しながら電源を入れるとバックアップファームが起動されます。
- バックアップモードとは、バックアップ用のファームウェア（バックアップファーム）で起動している状態のことです。

■ FTPクライアントの準備をする

1.　更新するためのファームウェアをFTPクライアントに保存します。

■ 本装置の準備をする

こんな事に気をつけて

本装置がバックアップモードで起動された場合、LAN側のIPアドレスは192.168.1.1になっています。運用中のLANでこのアドレスに問題がある場合は、FTPクライアントと2台だけの接続にしてください。

1.　本装置と保守ホスト（FTPクライアント）をLAN接続します。

本装置の10BASE-Tポートにケーブルを接続します。

2.　本装置のリセットスイッチを押しながら電源を入れます。

3.　CHECK／B1／B2／LANランプが緑色で点滅するのを確認し、リセットスイッチをはなします。

バックアップモードで起動します。

補足　バックアップモードで動作しているときは、CHECKランプが緑色で点灯します。

■ ファームウェアを更新する

1.　FTPクライアントから本装置にファームウェアを書き込みます。

☛ 参照　操作手順→「FTPサーバ機能によるファームウェアの更新」（P.641）

こんな事に気をつけて

- **ファームウェアの転送（put）中は、本装置の電源を切断しないでください。**
- **転送中に電源を切断すると、本装置が使用できなくなる場合があります。**

2.　ファームウェアの更新が正常に行われたことをランプで確認し、電源を切断します。

補足　正常に更新が行われた場合、CHECK／B1／B2／LANランプが緑色と橙色で交互に点滅します。

3.　電源を入れると、更新したファームウェアで本装置が起動します。

ご購入時の状態に戻すには

本装置を誤って設定した場合やトラブルが発生した場合には、本装置をご購入時の状態に戻すことができます。

こんな事に気をつけて

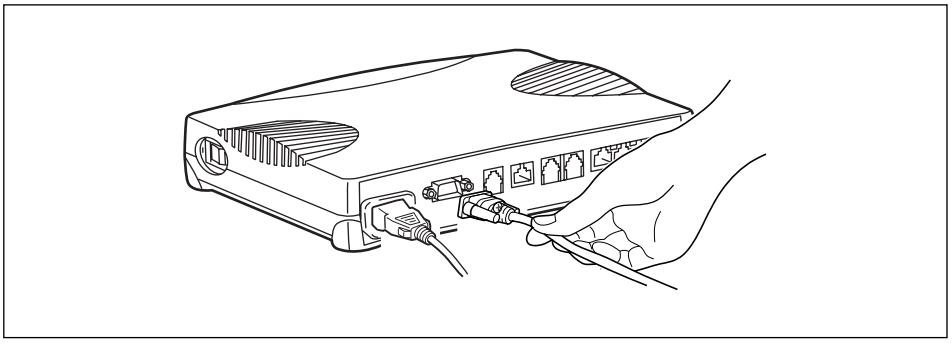
ご購入時の状態に戻すと、それまでの設定内容がすべて失われます。構成定義情報の退避、または設定内容をメモしておきましょう。

用意するもの

- RS232Cケーブル（クロス、本装置に接続する側がメス型9ピンのD-SUBコネクタ）
- ターミナルソフト（HyperTerminalなど）

本装置とパソコンをRS232Cケーブルで接続する

本装置とパソコンを接続します。



本装置をご購入時の状態に戻す

1.　パソコンでターミナルソフトを起動します。

2.　設定条件を以下のように設定します。

スタートBit	データBit	パリティBit	ストップBit	同期方式	通信速度	フロー制御
1	8	なし	1	非同期	9600	Xon／Xoff

補足　設定条件の設定方法については、ターミナルソフトのマニュアルを参照してください。

3.　[Return]キー、または［Enter］キーを押します。

8

4.　画面に「>」と表示されたことを確認します。

補足　画面に「>」が表示されない場合は、設定条件の「フロー制御」を「なし」、または「Xon／Xoff」にしてください。

5.　キーボードからlogonと入力して、[Return]キー、または[Enter]キーを押します。

6.　画面に「#」と表示されたことを確認します。

7.　キーボードからreset clearと入力して、[Return]キー、または[Enter]キーを押します。

本装置がご購入時の状態で起動します。

```
>logon
#reset clear（下線部入力）
```

付　録

バックアップ用電池について

本装置には、バックアップ用の電池をセットできます。

停電などで本装置への電源供給が止まると、バックアップ用電池を使った動作に切り替わります。

■ 電池をセットする

バックアップ用電池は、単3アルカリ乾電池を8本使用します。市販のものを別途ご購入ください。

1. 本装置の電源を切断します。

2. 本装置につないでいるケーブルをすべて取り外します。

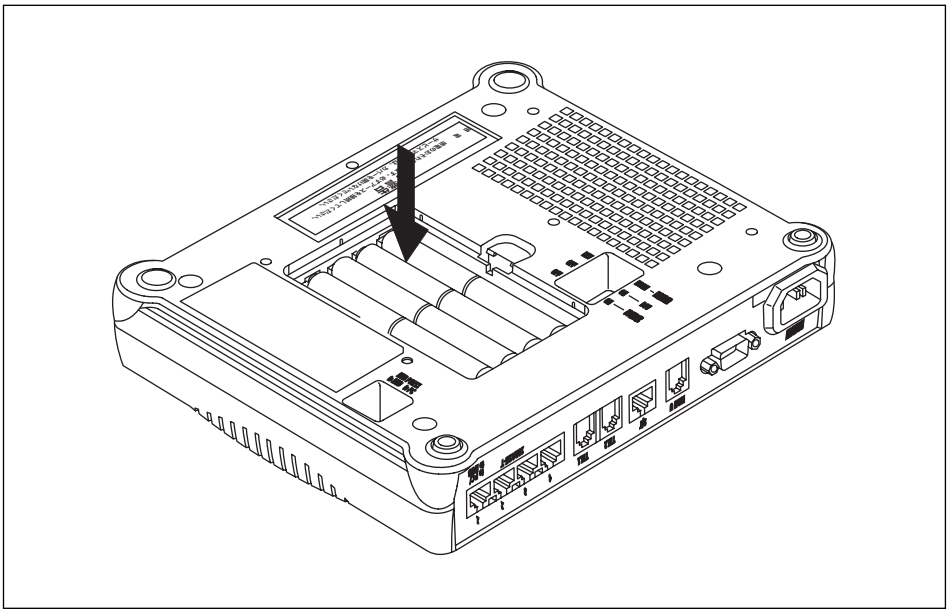
3. 本装置の底面を上にして、机の上などの安定した場所に置きます。

こんな事に気をつけて

本装置を持ち上げたままで作業しないでください。

4. 電池ボックスのフタを取り外します。

5. 表示に従って、⊕と⊖を間違えないように電池を入れます。



⚠警告

⊕マーク ⊖マークは正しく装着してください。⊕マーク ⊖マークを間違えると電池の破損や破壊を招き、本装置の破損やけがの原因になります。

6. 電池ボックスのフタを閉めます。

ヒント

◆ 電池を長持ちさせるには

停電時以外は、電池を取り外しておくことをお勧めします。入れたままにしている状態よりも、電池が長持ちします。

■ 停電時の動作について

バックアップ電池を利用すると、停電時にアナログポート（TEL1）につないだ電話機がご使用になれます。

バックアップ用電池で動作中は、本装置のPOWERランプが緑色で点滅（点灯約0.5秒、消灯約2.5秒）します。POWERランプ以外は消灯します。

こんな事に気をつけて

- **バックアップ用電池で動作中は、アナログポート（TEL2）、10BASE-Tポートにつないだ機器は使用できません。**
- **アナログポート（TEL2）で通話中に停電しても、その通話が終了するまでは使用できます。**

スイッチ設定例

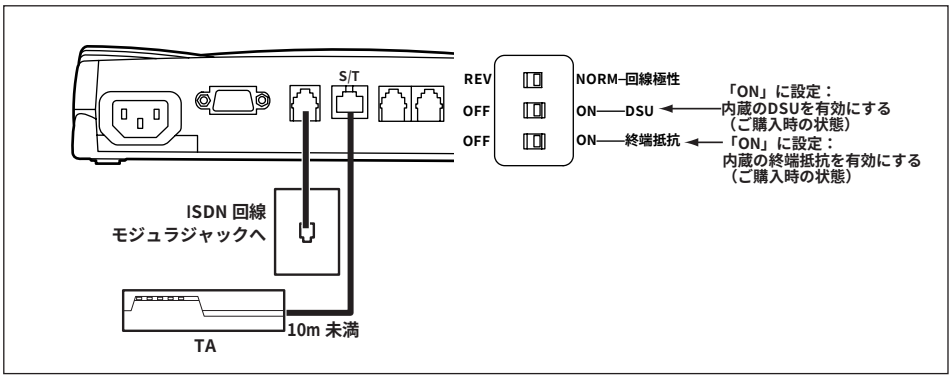
ディジタル電話機やG4FAXなど、ほかのISDN機器を本装置のDSUにつないだり、既設のDSUに本装置をつなぐときは、本装置底面のスイッチの設定を変更する必要があります。

■ 本装置のDSUを使用してほかのISDN機器をつなぐ

本装置のISDN S／Tポートから ISDN機器までのケーブルの長さによって、スイッチの設定が異なります。使用する環境を確認したうえで、必要な設定を行ってください。

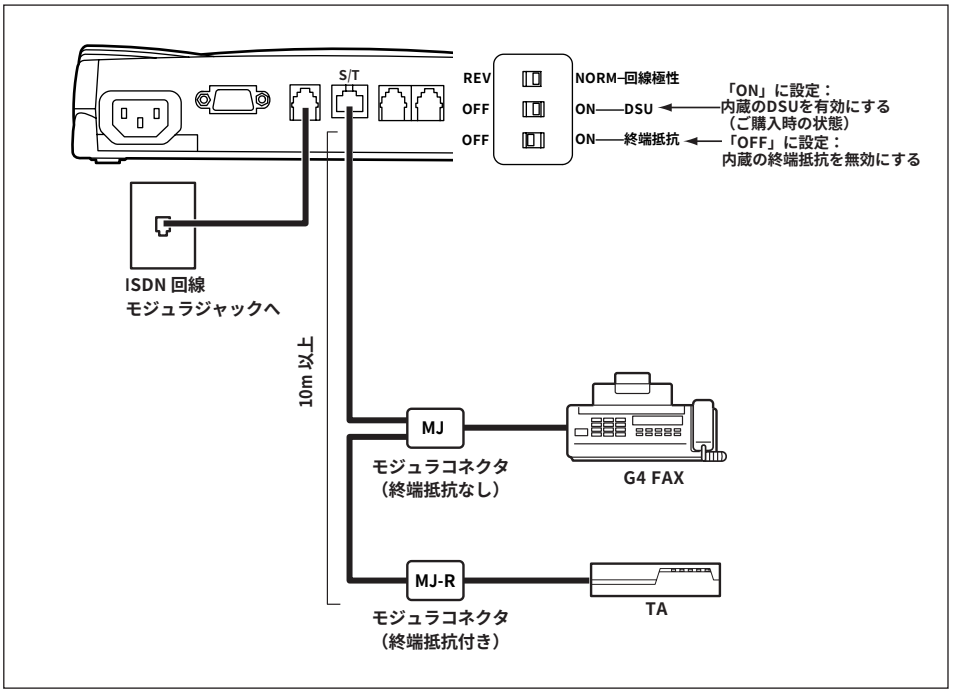
ISDN機器を 10m 未満の長さのケーブルでつなぐ場合

スイッチの設定は、ご購入時の設定のまま変更する必要はありません。



ほかのISDN機器をバス接続する場合

下図のようにバス配線し、最後尾の機器までのケーブル長が10mを超えるときは本装置の終端抵抗を無効とし、バス配線上の最後尾に位置するモジュラコネクタに終端抵抗を備えてください。スイッチの設定を、以下のように変更してください。



こんな事に気をつけて

バス配線上の最後尾に位置するモジュラコネクタに有効となる終端抵抗を備えてください。

■ 本装置を既設のDSUに接続する

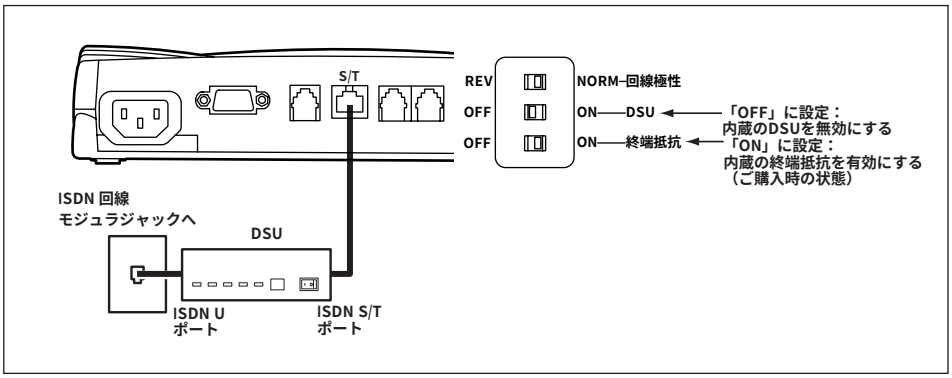
ほかのISDN機器をどのようにつなぐかによって、スイッチの設定が異なります。使用する環境を確認したうえで、必要な設定を行ってください。

こんな事に気をつけて

終端抵抗を備えたターミナルアダプタ（TA）の内蔵DSUを使う場合、終端抵抗の設定はターミナルアダプタ（TA）の説明書の指示に従ってください。

本装置だけを既設のDSUにつなぐ場合

本装置内蔵のDSUを無効に、終端抵抗を有効にし、本装置のISDN S／Tポートと既設DSUのISDN S／Tポートをつなぎます。スイッチの設定を、以下のように変更してください。



ダイヤル操作早見表

よく使うアナログ機能のダイヤルで行う操作の一覧です。

項　目		操　　作
かけ方・受け方	外線電話をかける	受話器を上げる ▶ 相手電話番号 ▶ 話をする
	リダイヤルする	受話器を上げる ▶ ✱8 ▶ 話をする
	サブアドレスを使う	受話器を上げる ▶ 相手電話番号 ✱ サブアドレス ▶ 話をする
	電話を受ける	リング音が鳴る ▶ 受話器を上げる ▶ 話をする
内線通話・内線転送	内線相手と話す	受話器を上げる ▶ ✱0 01 または 02 ▶ 話をする
	内線転送する	外線通話中 ▶ フッキング ▶ ✱0 01 または 02 ▶ 話をする ▶ 受話器を置く
フレックスホン	キャッチホン	Aと外線通話中 ▶ フッキング ▶ Bと話をする
	三者通話	Aと外線通話中 ▶ フッキング ▶ Bの電話番号 ▶ Bと話をする フッキング2回 ▶ 3人で話をする
	通信中転送	Aと外線通話中 ▶ フッキング ▶ Bの電話番号 ▶ Bと話をする フッキング ▶ 受話器を置く ▶ AとBで話をする
電話お断り疑似迷惑	通話中の相手を登録する	外線通話中 ▶ ✱9# ▶ 受話器を置く
発信者番号通知の選択	契約者回線番号	受話器を上げる ▶ ✱70 相手電話番号 ▶ 話をする
	ポート1ダイヤルイン番号	受話器を上げる ▶ ✱71 相手電話番号 ▶ 話をする
	ポート2ダイヤルイン番号	受話器を上げる ▶ ✱72 相手電話番号 ▶ 話をする
	鳴り分け番号1	受話器を上げる ▶ ✱73 相手電話番号 ▶ 話をする
	鳴り分け番号2	受話器を上げる ▶ ✱74 相手電話番号 ▶ 話をする
	鳴り分け番号3	受話器を上げる ▶ ✱75 相手電話番号 ▶ 話をする
アナログ機能の設定	i・ナンバーの設定	受話器を上げる ▶ ✱0✱220N ▶ 受話器を置く N 使用しない：1、使用する：2
	鳴り分け番号の動作モード	受話器を上げる ▶ ✱0✱22iN ▶ 受話器を置く i 鳴り分け番号1〜3の数字 N ポート1のみ着信：1、ポート2のみ着信：2、両ポート着信：3、着信拒否：4

項 目		操 作
アナログ機能の設定	ポート接続機器の設定	受話器を上げる ▶ ✱0✱40PN ▶ 受話器を置く P ポート番号1または2 N ない：1、電話：2、モデム：3、FAX：4、FAX無鳴動強制着信：5、FAX無鳴動識別着信：6、FAXキャッチホン着信：7
	ナンバー・ディスプレイ機能の設定	受話器を上げる ▶ ✱0✱41PN ▶ 受話器を置く P ポート番号1または2 N 使用しない：1、使用する（モード１）：2、使用する（モード２）：3
	着信転送機能の設定	受話器を上げる ▶ ✱0✱6000N ▶ 受話器を置く N 使用しない：1、着信転送：2、疑似着信転送：3
	スタンバイモードの設定	受話器を上げる ▶ ✱0✱8000N ▶ 受話器を置く N 通常モードにする：1、スタンバイモードにする：2
		スタンバイモードにする 受話器を上げる ▶ ✱5 ▶ 受話器を置く
		通常モードにする 受話器を上げる ▶ ✱6 ▶ 受話器を置く
着信転送先の設定	契約者回線番号の転送	受話器を上げる ▶ ✱0✱610 転送先電話番号 ▶ 受話器を置く
	ポート1ダイヤルインの転送	受話器を上げる ▶ ✱0✱611 転送先電話番号 ▶ 受話器を置く
	ポート2ダイヤルインの転送	受話器を上げる ▶ ✱0✱612 転送先電話番号 ▶ 受話器を置く
	鳴り分け番号1の転送	受話器を上げる ▶ ✱0✱613 転送先電話番号 ▶ 受話器を置く
	鳴り分け番号2の転送	受話器を上げる ▶ ✱0✱614 転送先電話番号 ▶ 受話器を置く
	鳴り分け番号3の転送	受話器を上げる ▶ ✱0✱615 転送先電話番号 ▶ 受話器を置く
メールの設定	TELメールを使用する	受話器を上げる ▶ ✱0✱2101 ▶ 受話器を置く
	TELメールを使用しない	受話器を上げる ▶ ✱0✱2102 ▶ 受話器を置く
	メールチェックの実行	受話器を上げる ▶ ✱0✱8300 ▶ 受話器を置く
留守状態の設定	在宅	受話器を上げる ▶ ✱0✱2001 ▶ 受話器を置く
	留守	受話器を上げる ▶ ✱0✱2002 ▶ 受話器を置く
留守モードの設定	解除	受話器を上げる ▶ ✱0✱8401 ▶ 受話器を置く
	実行	受話器を上げる ▶ ✱0✱8402 ▶ 受話器を置く

NTTとの契約が必要な機能

本装置の機能を利用するために必要なNTTとの契約の一覧です。

本装置の機能	ISDN契約内容および付加サービス	サービス内容
発信者番号通知 ボイスワープ 本装置どうしのコールバック	発信者番号通知（通常通知）	発信者の電話番号を相手に通知します。
オンラインサポート	ユーザ間情報通知	通信開始時と通信終了時にメッセージを送受信できます。
BOD キャッチホン 三者通話 通信中転送 着信転送	通信中着信通知	Bチャネルが2つとも使用中の場合に、3つめの着信を知らせます。
識別着信 疑似迷惑電話お断り 発信者番号表示 （ナンバー・ディスプレイ、 キャッチホン・ディスプレイ）	INSナンバー・ディスプレイ	発信者の電話番号を表示します。
キャッチホン	INSキャッチホン	通話中に着信があったときに、通話中の相手を保留にできます。
三者通話	三者通話	通話中に第三者に電話をかけて、三者間で通話できます。
通信中転送	通信中転送	通話中の電話を第三者に転送できます。
着信転送	着信転送	着信した電話を応答する前に第三者へ転送できます。
ボイスワープ	INSボイスワープまたは INSボイスワープ・セレクト	高機能な着信転送サービスです。
ダイヤルイン／グローバル着信	ダイヤルイン	電話番号を追加し、電話機ごとに鳴り分けができます。
ｉ・ナンバー着信	ｉ・ナンバー	電話番号を追加し、電話機ごとに鳴り分けができます。
モデムダイヤルイン アナログダイヤルイン	ダイヤルインまたは ｉ・ナンバー	電話番号を追加し、電話機ごとに鳴り分けができます。

仕　様

■ ハードウェア仕様

装置型名		SIR130BV4	
インタフェース	ISDN (U)	規格	JT-G.961（U 点インタフェース）
		ポート数	1 ポート
		コネクタ	6 ピン・モジュラジャック（RJ11）
		DSU	内蔵
		その他	極性反転可能、DSU 切り離し可能
	ISDN (S／T)	規格	ITU-TI.430（S／T 点インタフェース）
		ポート数	1 ポート
		回線速度	B チャネル：64K ビット／秒および 128K ビット／秒、32K ビット／秒（PIAFS 通信） D チャネル：16K ビット／秒
		適用回線	INS ネット 64 およびディジタル専用線
		コネクタ	8 ピン・モジュラジャック（RJ45）
	LAN	規格	IEEE 802.3（10BASE-T インタフェース）
		ポート数	4 ポート
		通信速度	10M ビット／秒
		コネクタ	8 ピン・モジュラジャック（RJ45）
	アナログ	2 線式アナログインタフェース	
		ポート数	2 ポート
		コネクタ	8 ピン・モジュラジャック（RJ11）
		給電電圧	-48V
	コンソール	RS232C インタフェース	
		ポート数	1 ポート
		通信速度	9600 ビット／秒
		コネクタ	9 ピン・DSUB
電源／周波数		AC100V〔50／60Hz〕	
最大消費電力		11W	
外形寸法		241mm（W）× 202mm（D）× 48mm（H）（突起部を除く）	
重量		1kg（乾電池を除く）	
温度／湿度		温度 ：0 ～ 40℃ 湿度 ：15 ～ 85%RH	
適応規格		VCCI Class-B	
停電対応		TEL1 ポートにつないだ電話で通話可能	

■ ソフトウェア仕様

データ通信に関する仕様

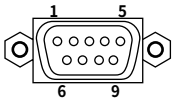
機能／分類	詳　細
ルーティング対象プロトコル	IPv4、IPv6
ブリッジ	IEEE802.10準拠
ルーティングプロトコル	スタティック、RIPv1、RIPv2、RIPng、BGP4
WANプロトコル	PPP、MP（BAP、BACP）
ヘッダ圧縮	VJ TCPヘッダ圧縮、IPヘッダ圧縮
データ圧縮	LZS
セキュリティ	PAP／CHAP（最大64件） 管理パスワード IPv4フィルタ：アドレス／ポート／IN／OUT／発信（最大64） IPv6フィルタ：アドレス／ポート／IN／OUT／発信（最大64）
VPN	IPsec/IKE（Main Mode および Aggressive Mode の発側）
設定手段	WWWブラウザ：かんたん設定／詳細設定
ロギング	回線ログ、課金情報、PPPフレームトレース、システムログ
回線接続先	登録可能数：最大48箇所 同時接続　：2箇所
回線接続／切断契機	自動、または手動
アドレス変換機能	マルチNAT
コールバック	CBCP方式、無課金方式
PIAFS対応	発信／着信可能
接続相手識別	発信者番号通知による識別、認証IDによる識別、 RADIUSクライアントによる識別
不特定相手着信	あり
フレームリレー	DLCI数：32 輻輳制御：CLLM、FECN、BECN PVC状態確認手順：JTQ.933 AnnexA
簡単／便利機能	テレホーダイ対応 マルチダイヤル機能（3箇所） DHCPサーバ機能（最大64台） 　- DHCPスタティック機能（IPアドレス固定） DHCPリレーエージェント機能 ProxyDNS機能 　- DNSサーバ自動切り替え機能 　- DNSサーバアドレスの自動取得機能（RFC1877対応） 　- DNSサーバ機能 URLフィルタ機能 Proxy ARP 時刻機能：手動設定、またはTIMEプロトコル／SNTPによる取得

機能／分類	詳　細
簡単／便利機能	マルチルーティング機能： ソースアドレス単位、ポート単位、課金単位の混在設定可能 最適切断タイマ 課金制御機能： 接続禁止時間設定 超過課金アラーム（システムログ出力） かんたんフィルタ リモートパワーオン機能（Wakeup on LAN 対応機器の遠隔起動） E メールエージェント機能：メールチェック、リモートメールチェック、メール転送、TEL メール転送 留守モード機能 スケジュール機能 オンラインサポート機能 SNMP エージェント機能 ワンタイムパスワード対応：回線手動接続による マルチホーミング機能 VRRP機能
レベルアップ	FTPクライアント機能／ FTP サーバ機能による

アナログ機能に関する仕様

機能／分類	詳　細	備　考
発着信	ナンバー・ディスプレイ	
	キャッチホン・ディスプレイ	
	ダイヤルイン	
	ｉ・ナンバー	3番号対応
	グローバル着信	
	サブアドレス	
	FAX無鳴動着信	識別・強制を選択可能
	識別着信（相手番号）	相手ごとにポート優先、ポート指定、拒否を設定可能
	識別着信（着信番号）	
	発信規制	10件まで登録可能
	リング音選択可	3種類から選択可能
	発信者番号通知	
	発信者番号選択	
	優先ポート着信	
	発着信専用選択可	
	ダイヤル桁間タイマ	
	リバースパルス送出	
	留守状態確認（無課金）	
	疑似迷惑電話おことわり	
	モデムダイヤルイン	
	アナログダイヤルイン	
フレックスホン対応	キャッチホン／三者通話／通信中転送／着信転送	自動切り替え可能
疑似フレックスホン	キャッチホン／三者通話／通信中転送／着信転送	保留音あり、自動切り替え可能
INSボイスワープ対応		
内線機能	内線通話	
	内線転送	
補助機能	発着信記録	不在時にも相手電話番号記録
	受話音量調整	3段階に設定可能
	フッキング時間選択可	3段階に設定可能
	話中着信音キャンセル	
	迷惑電話登録	

コンソールポート仕様



コネクタ形状はD-SUB 9ピンーオス
ケーブルはクロス

ピン番号	信号名	方向	内容
1	CD	入力	キャリア検出
2	RD	入力	受信データ
3	TD	出力	送信データ
4	ER	出力	データ端末レディ
5	GND	ー	グランド
6	DR	入力	データセットレディ
7	RS	出力	送信要求
8	CS	入力	送信可
9	CI	入力	呼び出し通知

設定項目の初期値一覧

各設定項目の初期値の一覧を示します。ご購入時の状態では、以下のような設定になっています。

データ通信に関する初期値

項 目				設定値
回線情報	回線情報			ISDN
	ISDN 情報	自動ダイヤル		相手毎に設定
		着信動作		相手毎に設定
		自局番号チェック		しない
		発信者番号通知		網契約に従う
		回線保持タイマ		2 時間
		課金制御	上限	3000 円
			制御動作	発信抑止
	フレームリレー情報	PVC 状態確認手順		使用する
		CLLM メッセージ		使用する
		網輻輳通知ビット		FECN、BECN
LAN 情報	IPv4	IP アドレス	アドレス	192.168.1.1
			ネットマスク	255.255.255.0
			ブロードキャスト	192.168.1.255
		セカンダリ IP アドレス		なし
		DHCP 機能（サーバ機能）	割り当て先頭アドレス	192.168.1.2
			割り当て個数	32
			リース期間	1 日
			ネットマスク広報	なし
			デフォルトルータ広報	192.168.1.1
			DNS サーバ広報	192.168.1.1
			セカンダリ DNS サーバ広報	なし
			ドメイン名広報	なし
		ダイナミックルーティング	RIP 送信	使用しない
			RIP 受信	使用しない
			BGP	使用しない
		スタティックルーティング		なし
	IPv6			使用しない
	ブリッジ			使用しない
	VRRP			使用しない
相手情報				なし

項 目			設定値
ルーティングプロトコル情報			なし
装置情報	タイムサーバ情報		使用しない
	システムログ情報	システムログ送信	しない
		ファシリティ	23
		プライオリティ	error、warn、info
		セキュリティログ	なし
	ファームウェア更新情報		なし
	SNMP情報		使用しない
	ブリッジ情報		使用しない
	オンラインサポート接続		する
	留守モード情報		なし
	telnet自動ログオフ		5分
パスワード情報			なし
Eメールエージェント情報			なし
ProxyDNS情報			なし
ホストデータベース情報			なし
スケジュール情報			毎週金曜日 00:00 課金情報クリア
マルチTA情報			使用する
IPsec情報			なし
シェル関連	環境変数	漢字コード	ShiftJIS

アナログ通信に関する初期値

項　目			設定値
アナログ共通情報	網契約に関連する設定項目	フレックスホン	使用しない
		着信転送	使用しない
		i・ナンバー	使用しない
	装置の動作に関連する設定項目	留守状態設定	在宅
		ダイヤル桁間タイマ	5秒
		フッキング時間	標準
		＃機能ボタン使用	する（1回入力）
		外線リング音	リング音1
		内線リング音	リング音2
アナログポート1／2情報	網契約に関連する設定項目	グローバル着信	する
		発信者番号通知	網契約に従う
		キャッチホン	使用しない
	装置の動作に関連する設定項目	接続機器	電話
		発信／着信選択	発着信
		受話音量	中
		リバースパルス送出	送出しない
		通信中着信音送出時間	0秒 （着信相手断まで送出）
		フレックスホン自動切替	使用しない
		通信前情報通知	使用しない
		キャッチホンディスプレイ	使用しない
送出着信番号情報		番号送出方法設定	網から通知された番号を送出する

システム最大値一覧

本装置で定義可能な最大個数、またはエントリの最大数の一覧表を示します。

項 目			最大値
ルーティング（IPv4）	ルーティングエントリ（※1）		128
		（スタティック）	(64)
	ARPエントリ		512
ルーティング（IPv6）	ルーティングエントリ（※1）		128
		（スタティック）	(64)
	Neighborキャッシュエントリ（※2）		512
BGP情報	E-BGP最大接続数		1
	BGP広報ネットワーク数		16
PPP認証ユーザ数			64
IPフィルタ	IPv4		64
	IPv6		64
TOS値書き換え			32
アドレス変換	NATテーブル数		1024
	静的NATテーブル数		64
	ルール定義数		32
接続先	登録可能数（※3）		48箇所
	同時接続		2（ISDN） 32（FR）
DHCPアドレス割り当て最大数			64
ホストデータベース定義数			64
ProxyDNS定義数			32
ポートルーティング定義数			32
スケジュール定義数			16
番号変更予約定義数			4
帯域制御（WFQ）定義数			64
フレームリレーのPVC数			32
マルチホーミング	動的エントリ数		256
	静的エントリ数		64
ブリッジ	学習テーブルエントリ数		1024
	MACフィルタ登録可能数		128
VPN通信	Main Mode	IPSec SA数	64
		IKE SA数	32
	Aggressive Mode	IPSec SA数	32
		IKE SA数	32

VRRP	VRRPグループ数	2
	トリガー数	50
アナログ識別着信	登録可能数	10
アナログ発信規制	抑止番号（ポート毎設定）	10
	許可番号（ポート毎設定）	10

※1）本装置で受信できる経路情報数は、ルーティングエントリの最大値までです。
ただし、以下のような冗長ネットワークを構築する場合は、同じ宛先への経路情報でもルーティングエントリ数として計算されるため注意してください。

- 複数のルーティングプロトコルで同じ経路情報を受信する場合
- スタティックルーティング定義と同じ経路情報をルーティングプロトコルで受信する場合

※2）IPv6のNeighborキャッシュエントリの最大値は512ですが、これには通信のための内部管理情報として利用されているエントリも含まれます。そのため、ルーティング情報で表示されるNeighborキャッシュエントリの個数が512より少なくなる場合があります。

※3）IPv6 over IPv4、IPsecなどのトンネル定義を含みます。

ISDN理由表示番号一覧

正常イベントクラス

理由コード	理由表示番号	理由種別
01	＃1	欠番
02	＃2	指定中継網へのルートなし
03	＃3	相手へのルートなし
04	＃6	チャネル利用不可
05	＃7	呼が設定済みのチャネルへ着呼
10	＃16	正常切断
11	＃17	着ユーザビジー
12	＃18	着ユーザレスポンスなし
13	＃19	相手ユーザ呼出中／応答なし
14	＃20	加入者不在
15	＃21	通信拒否
16	＃22	相手加入者番号変更
1A	＃26	選択されなかったユーザの切断復旧
1B	＃27	相手端末故障中
1C	＃28	無効番号フォーマット（不完全番号）
1D	＃29	ファシリティ拒否
1E	＃30	状態問い合わせへの応答
1F	＃31	その他の正常クラス

リソース不可クラス

理由コード	理由表示番号	理由種別
22	＃34	利用可回線／チャネルなし
26	＃38	網故障
29	＃41	一時的故障
2A	＃42	交換機輻輳
2B	＃43	アクセス情報廃棄
2C	＃44	要求回線／チャネル利用不可
2F	＃47	その他のリソース使用不可クラス

サービス利用不可クラス

理由コード	理由表示番号	理由種別
31	＃49	サービス品質（QOS）利用不可
32	＃50	要求ファシリティ未契約
39	＃57	伝達能力不許可
3A	＃58	現在利用不可伝達能力
3F	＃63	その他のサービスまたはオプションの利用不可クラス

サービス未提供クラス

理由コード	理由表示番号	理由種別
41	#65	未提供伝達能力指定
42	#66	未提供チャネル種別指定
45	#69	未提供ファシリティ要求
46	#70	制限ディジタル情報転送能力だけ可能
4F	#79	その他のサービスまたはオプションの未提供クラス

無効メッセージクラス

理由コード	理由表示番号	理由種別
51	#81	無効呼番号使用
52	#82	無効チャネル番号使用
53	#83	指定された中断呼識別番号未使用
54	#84	中断呼識別番号使用中
55	#85	中断呼なし
56	#86	指定中断呼切断復旧済み
57	#87	ユーザはCUGメンバでない
58	#88	端末属性不一致
5B	#91	無効中継網選択
5F	#95	その他の無効メッセージクラス

手順誤りクラス

理由コード	理由表示番号	理由種別
60	#96	必須情報要素不足
61	#97	メッセージ種別未定義、または未提供
62	#98	呼状態とメッセージ不一致、またはメッセージ別未定義または未提供
63	#99	情報要素未定義
64	#100	情報要素内容無効
65	#101	呼状態とメッセージ不一致
66	#102	タイマ満了による回復
6F	#111	その他の手順誤りクラス

インタワーキングクラス

理由コード	理由表示番号	理由種別
7F	#127	その他のインタワーキングクラス

PPPフレームトレース情報詳細

表示形式

● 表示例

```
[02] B1ch : Recv LCP  Configure-Request id=00 len=19  97.09.01 09:19:54.225
          data=c021 01 00 0013 0305 c223 0505 06f0 1e4a
               5007 0208 02
```

プロトコル種別　コード種別　ID　パケット長　データ

● 説明

```
[02] B1ch : Recv LCP  Configure-Request id=00 len=19  97.09.01 09:19:54.225
```

ログ番号（01～99）　チャネル　送受信　プロトコル種別　コード種別　IDフィールド値　パケット長　ppp trace採取時間

チャネル	B1ch、またはB2chが表示されます。
送受信	Send、またはRecvが表示されます。
プロトコル種別	PPPでのプロトコル種別が表示されます。以下のプロトコルが表示されます。プロトコル種別前にMP:が付加された場合は、そのパケットはMPによりカプセル化されていることを示します。

0xc021	LCP	: Link Control Protocol
0xc023	PAP	: Password Authentication Protocol
0xc223	CHAP	: Challenge-Handshake Authentication Protocol
0x8021	IPCP	: Internet Protocol Control Protocol
0x8031	BCP	: Bridge Control Protocol
0x8057	IPV6CP	: IPv6 Control Protocol
0x80FD	CCP	: Compression Control Protocol
0x80FB	ICCP	: Individual Compression Control Protocol
0xc02D	BAP	: Bandwidth Allocation Protocol
0xc02B	BACP	: Bandwidth Allocation Control Protocol
0xc029	CBCP	: Callback Control Protocol

コード種別　各プロトコルでのコードの内容が表示されます。以下の文字列が表示されます。

－プロトコル種別がLCP、IPCP、BCP、IPV6CP、CCP、ICCPの場合

Ox01	Configure-Request
Ox02	Configure-Ack
Ox03	Configure-Nak
Ox04	Configure-Reject
Ox05	Terminate-Request
Ox06	Terminate-Ack
Ox07	Code-Reject

－プロトコル種別がLCPの場合

Ox08	Protocol-Reject
Ox09	Echo-Request
Ox0A	Echo-Reply
Ox0B	Discard-Request

－プロトコル種別がCCP、ICCPの場合

Ox0E	Reset-Request
Ox0F	Reset-Act

－プロトコル種別がPAPの場合

Ox01	Authenticate-Request
Ox02	Authenticate-Ack
Ox03	Authenticate-Nak

－プロトコル種別がCHAPの場合

Ox01	Challenge
Ox02	Response
Ox03	Success
Ox04	Failure

－プロトコル種別がBAPの場合

Ox01	Call-Request
Ox02	Call-Response
Ox03	Callback-Request
Ox04	Callback-Response
Ox05	Link-Drop-Request
Ox06	Link-Drop-Resp
Ox07	Call-Status-Ind
Ox08	Call-Status-Rsp

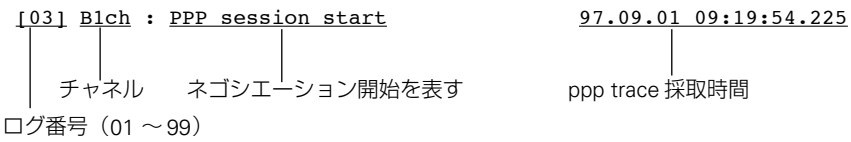
－プロトコル種別がCBCPの場合

```
Ox01      Callback-Request
Ox02      Callback-Response
Ox03      Callback-Ack
```

IDフィールド値	PPPフレーム中のIDフィールドの値が、2桁の16進数で表示されます。
パケット長	送受信したパケット長が10進数で表示されます。
data=	送受信したパケットの内容を16進数で表示します。最大108バイト分まで表示され、それよりあとは表示されません。

● 例外

ネゴシエーション開始時は、例外的に特別なトレース情報が表示されます。以下のような表示形式となります。



システムログ情報一覧

■ システムのメッセージ

(1)システム起動

```
init: system startup now.
```

【プライオリティ】　LOG_INFO

【意味】　システムが起動したことを示します。

(2)システムダウン

```
init: system down occured.  data is followings:
init:    <elog>
```

【プライオリティ】　LOG_ERROR

【意味】　システムダウンが発生したことを示します。
（注）通常は出力されません。

【パラメタの意味】　<elog>　：エラーログ情報相当を表示します。

■ ディジタル通信のメッセージ

(1)回線接続

```
protocol: connected <ch> to <target>(<dial>) by <reason>
```

【プライオリティ】　LOG_INFO

【意味】　発信により相手システムと接続したことを示します。このメッセージは ISDN 回線の場合だけ出力されます。

【パラメタの意味】

<ch>　：接続物理チャネル
B1ch または B2ch

<target>：ネットワーク名．接続先名

<dial>　：相手電話番号

<reason>：発信契機

forwarding packet	：フォワードパケット
ProxyDNS	：ProxyDNS
MP	：MP
callback	：コールバック応答発信
manual	：手動接続
keep connection	：回線接続保持機能（常時接続）による接続
bridging packet	：ブリッジパケット
STP	：STPパケット

protocol: connected <ch> from <target>(<dial>)

【プライオリティ】 LOG_INFO

【意味】 着信により相手システムと接続したことを示します。このメッセージは ISDN 回線の場合だけ出力されます。

【パラメタの意味】 <ch> : 接続物理チャネル
B1ch または B2ch
<target> : ネットワーク名．接続先名
<dial> : 相手電話番号

protocol: non-charge callback request from <target>(<dial>) is accepted

【プライオリティ】 LOG_INFO

【意味】 無課金コールバック要求を受理したことを示します。このメッセージは ISDN 回線の場合だけ出力されます。

【パラメタの意味】 <target> : ネットワーク名．接続先名
<dial> : 相手電話番号

protocol: <ch> is decided as <target>

【プライオリティ】 LOG_INFO

【意味】 <ch> で着信した相手が認証により <target> と判明したことを示します。このメッセージは ISDN 回線の場合だけ出力されます。

【パラメタの意味】 <ch> : 接続物理チャネル
B1ch または B2ch
<target> : ネットワーク名．接続先名

protocol: <ch> is MP bundled as answer<number>

【プライオリティ】 LOG_INFO

【意味】 <ch> で着信した相手が、すでに接続している不特定相手と MP として結び付けられたことを示します。

【パラメタの意味】 <ch> : 接続物理チャネル
B1ch または B2ch
<numbert>: 不特定相手番号。0 または 1 となります。

(2)回線切断

protocol: disconnected <ch> to <target> : charge=<value>yen time=<time>

【プライオリティ】 LOG_INFO

【意味】 自側より回線切断を行い、回線が切断されたことを示します。このメッセージは ISDN 回線の場合だけ出力されます。

【パラメタの意味】
<ch> : 接続物理チャネル
B1ch または B2ch
<target> : ネットワーク名．接続先名
<value> : 通話料金（円単位）
<time> : 接続時間（dddd.hh:mm:ss の形式）

protocol: disconnected <ch> from <target> : charge=<value>yen time=<time>

【プライオリティ】 LOG_INFO

【意味】 相手側、または網から回線切断が通知され、回線が切断されたことを示します。このメッセージは ISDN 回線の場合だけ出力されます。

【パラメタの意味】
<ch> : 接続物理チャネル
B1ch または B2ch
<target> : ネットワーク名．接続先名
<value> : 通話料金（円単位）
<time> : 接続時間（dddd.hh:mm:ss の形式）

protocol: <target> is disconnected, because <reason>

【プライオリティ】 LOG_INFO

【意味】 ISDN 回線のセッションが切断された理由を示します。

【パラメタの意味】
<target> : ネットワーク名．接続先名
<reason> : 切断理由
keepalive expired : 相手からの受信がまったくなくなったための切断

(3)着信拒否

protocol: rejected call from (<dial>) because <reason>

【プライオリティ】 LOG_INFO

【意味】 着信通知を拒絶したことを示します。このメッセージはISDN回線の場合だけ出力されます。

【パラメタの意味】 <dial> : 相手電話番号

<reason> : 拒否理由

permission denied : 着信が許可されていなかったための拒否

protocol: <ch> is not decided as any defined host, but anonymous login is not usable

【プライオリティ】 LOG_INFO

【意味】 認証により着信相手判断を行おうとしたが、一致する接続先情報がなく、かつ不特定相手着信ができない状態であったため、切断することを示します。このメッセージはISDN回線の場合だけ出力されます。

【パラメタの意味】 <ch> : 接続物理チャネル

B1ch または B2ch

(4)同期確立／外れ

protocol: line synchronization is established

【プライオリティ】 LOG_INFO

【意味】 回線の同期確立が完了したことを示します。このメッセージはHSD回線の場合だけ出力されます。

protocol: line synchronization is failed

【プライオリティ】 LOG_INFO

【意味】 回線の同期はずれが発生したことを示します。このメッセージはHSD回線の場合だけ出力されます。

(5)自動発信抑止

protocol: autodial locked by <name>

【プライオリティ】　LOG_INFO

【意味】　発信抑止中のため、自動ダイヤルを中止しました。

【パラメタの意味】　<name> : 抑止の原因

schedule : スケジュール機能による抑止

limiter : 課金制限による抑止

redial :3 分間に 2 回を超える再発信のため自動発呼処理を中止した。

(6)着信抑止

protocol: callin rejected by <name>

【プライオリティ】　LOG_INFO

【意味】　着信抑止中のため、着信処理を中止しました。

【パラメタの意味】　<name> : 抑止の原因

schedule : スケジュール機能による抑止

(7)課金制御条件の制限超過

protocol: ISDN connect limit over [<reason>]

【プライオリティ】　LOG_WARNING

【意味】　課金制御条件の制限を超過して発信しようとしたことを示します。

【パラメタの意味】　<reason> : 超過した内容です。以下の情報のどちらかとなります。

time=<day>:<hour>:<min>:<sec> : 時間制限を超過しました。

charge=<charge>yen : 課金制限を超過しました。

課金制限および時間制限の両方が超過している場合には、課金制限超過の内容が出力されます。

(8)連続接続失敗による発信抑止

protocol: continuous PPP negotiation error <target> : call stop

【プライオリティ】　LOG_INFO

【意味】　連続して 30 回の接続に失敗（ISDN では接続されるが IP 通信ができずに失敗の場合のみ）し、発信を禁止したことを示します。

【パラメタの意味】　<target> : ネットワーク名．接続先名

(9)PPP ネゴシエーション失敗

protocol: <protocol> is closed by <target>

【プライオリティ】 LOG_INFO

【意味】 <protocol> が相手から終了させられ、そのデータ回線上で <protocol> で示されたプロトコルでの通信が行えなくなったことを示します。

【パラメタの意味】
<protocol> : 終了させられたプロトコル
IPCP : IPv4 用のプロトコル名
IPV6CP : IPv6 用のプロトコル名
BCP : ブリッジ用のプロトコル名
<target> : ネットワーク名 . 接続先名

■ アナログ通信のメッセージ

(1)発信完了

analog: connected <port> to (<dial>)

【プライオリティ】 LOG_INFO

【意味】 アナログの発信により相手と接続したことを示します。

【パラメタの意味】
<port> : 発信アナログポート（TEL1、TEL2）
<dial> : 相手電話番号

(2)着信完了

analog: connected (<dial1>) from (<dial2>)

【プライオリティ】 LOG_INFO

【意味】 アナログの着信により相手と接続したことを示します。

【パラメタの意味】
<dial1> : 自側電話番号
<dial2> : 相手電話番号（未通知の場合、非通知理由）

【非通知理由】

"O": サービス提供不可	Out of area
"P": ユーザ拒否	Anonymous call (Blocked number)
"S": サービス競合	Interaction with Service
"C": 公衆電話からの発信	Public payphone (Public telephone)

(3)発信中止

analog: stop calling <port> to (<dial>) <reason>

【プライオリティ】 LOG_INFO

【意味】 アナログの発信を中止した、または中止されました。

【パラメタの意味】 <port> : 発信アナログポート（TEL1、TEL2）

<dial> : 相手電話番号

<reason> : "normal" 発信したが相手が応答しないため、受話器を置いて発信を中止したことを示します。

: "layer1/2 error" 発信したが同期はずれ状態のため、発呼が中止されたことを示します。

detail=xx 発信したが回線切断などが発生し発信が中止されたことを示します。

切断理由（16進数）、（切断理由不明時は "–"）

analog: abort calling <port> to (<dial>) <reason>

【プライオリティ】 LOG_INFO

【意味】 アナログで発信したが相手より着信拒否を受信したことを示します。

【パラメタの意味】 <port> : 発信アナログポート（TEL1、TEL2）

<dial> : 相手電話番号

<reason> : detail=xx 切断理由（16進数）。（切断理由不明時は "–"）

(4)着信中止

analog: abort called (<dial1>) from (<dial2>) <reason>

【プライオリティ】 LOG_INFO

【意味】 アナログで相手より着信したが、着信を中止しました。

【パラメタの意味】 <dial1> : 自側電話番号

<dial2> : 相手電話番号（未通知の場合、非通知理由）

【非通知理由】

"O": サービス提供不可	Out of area
"P": ユーザ拒否	Anonymous call (Blocked number)
"S": サービス競合	Interaction with Service
"C": 公衆電話からの発信	Public payphone (Public telephone)

<reason> : "normal" 相手より着信したが自側で応答しないため、相手が受話器を置いたことを示します。

analog: stop called (<dial1>) from (<dial2>) <reason>

【プライオリティ】　LOG_INFO

【意味】　アナログで相手より着信したが着信拒否、または、回線切断などが発生したことを示します。

【パラメタの意味】　<dial1>　: 自側電話番号

<dial2>　: 相手電話番号（未通知の場合、非通知理由）

【非通知理由】

"O": サービス提供不可	Out of area
"P": ユーザ拒否	Anonymous call (Blocked number)
"S": サービス競合	Interaction with Service
"C": 公衆電話からの発信	Public payphone (Public telephone)

<reason> : detail=xx　切断理由（16 進数）。（切断理由不明時は"–"）

(5)自分から切断

analog: disconnected to (<dial>) charge=<value>yen time=<time> <reason>

【プライオリティ】　LOG_INFO

【意味】　アナログで相手と接続後、受話器を置いて通話相手との接続を切断したことを示します。

【パラメタの意味】　<dial>　: 相手電話番号（未通知の場合、非通知理由）

【非通知理由】

"O": サービス提供不可	Out of area
"P": ユーザ拒否	Anonymous call (Blocked number)
"S": サービス競合	Interaction with Service
"C": 公衆電話からの発信	Public payphone (Public telephone)

<value>　: 通話料金（円単位）

<time>　: 接続時間（dddd.hh:mm:ss の形式）

<reason> : "normal"　自側の受話器を置いたことより切断したことを示します。

(6)相手から切断

analog: disconnected from (<dial>) charge=<value>yen time=<time> <reason>

【プライオリティ】 LOG_INFO

【意味】 アナログで相手と接続後、通話相手との接続を切断したことを示します。

【パラメタの意味】 <dial> : 相手電話番号（未通知の場合、非通知理由）

【非通知理由】

"O": サービス提供不可	Out of area
"P": ユーザ拒否	Anonymous call (Blocked number)
"S": サービス競合	Interaction with Service
"C": 公衆電話からの発信	Public payphone (Public telephone)

<value> : 通話料金（円単位）

<time> : 接続時間（dddd.hh:mm:ss の形式）

<reason> : "normal" 通話相手が受話器を置いたことにより切断したことを示します。

detail=xx 切断理由（16進数）。（切断理由不明時は "--"）

(7)着信転送

analog: call deflection from (<dial1>) to (<dial2>) <reason>

【プライオリティ】 LOG_INFO

【意味】 アナログであらかじめ設定された相手から着信したため、別の接続相手へ自動的に転送したことを示します。

【パラメタの意味】 <dial1> : （着信元）相手電話番号（未通知の場合、非通知理由）

【非通知理由】

"O": サービス提供不可	Out of area
"P": ユーザ拒否	Anonymous call (Blocked number)
"S": サービス競合	Interaction with Service
"C": 公衆電話からの発信	Public payphone (Public telephone)

<dial2> : （転送先）相手電話番号

<reason> : "normal" 正常に別の接続相手へ転送できたことを示します。

detail=xx 切断理由（16進数）。（切断理由不明時は "--"）

(8)着信あり

analog: receive call (<dial1>) from (<dial2>) <reason>

【プライオリティ】 LOG_INFO

【意味】 アナログで相手より着信しました。
以降のログで着信完了（connected）、着信中止（abort called、stop called）が表示されます。

【パラメタの意味】 <dial1> : 自側電話番号

<dial2> : 相手電話番号（未通知の場合、非通知理由）

【非通知理由】

"O": サービス提供不可	Out of area
"P": ユーザ拒否	Anonymous call (Blocked number)
"S": サービス競合	Interaction with Service
"C": 公衆電話からの発信	Public payphone (Public telephone)

<reason> : 高位レイヤ特性識別

※高位レイヤ整合性情報要素が含まれていた場合だけ表示します。
HLC=xx（16進数）

(9) i ・ナンバー着信要求

analog: receive call (<inumber>) from (<dial>) <reason>

【プライオリティ】 LOG_INFO

【意味】 アナログで i ・ナンバー着信しました。
以降のログで着呼完了（connected）、着呼中止（abort called、stop called）が表示されます。

【パラメタの意味】 <inumber> : "inumber1": 自局 i ・ナンバー情報1［サブアドレス］
"inumber2": 自局 i ・ナンバー情報2［サブアドレス］

<dial> : 相手局ダイヤル番号（未通知の場合、非通知理由）

【非通知理由】

"O": サービス提供不可	Out of area
"P": ユーザ拒否	Anonymous call (Blocked number)
"S": サービス競合	Interaction with Service
"C": 公衆電話からの発信	Public payphone (Public telephone)

<reason> : 高位レイヤ特性識別

※高位レイヤ整合性情報要素が含まれていた場合だけ表示します。
HLC=xx（16進数）

(10) i ・ナンバー着呼完了

```
analog: connected (<inumber>) from (<dial>)
```

【プライオリティ】 LOG_INFO

【意味】 アナログで i ・ナンバー着信により相手と接続しました。

【パラメタの意味】 <inumber> : "inumber1": 自局 i ・ナンバー情報1［サブアドレス］
"inumber2": 自局 i ・ナンバー情報2［サブアドレス］

<dial> : 相手局ダイヤル番号［サブアドレス］（網からND通知されてきた場合だけ。未通知の場合、非通知理由を表示）

【非通知理由】

"O": サービス提供不可	Out of area
"P": ユーザ拒否	Anonymous call (Blocked number)
"S": サービス競合	Interaction with Service
"C": 公衆電話からの発信	Public payphone (Public telephone)

(11) i ・ナンバー着呼中止

```
analog: abort called (<inumber>) from (<dial>) <reason>
```

【プライオリティ】 LOG_INFO

【意味】 アナログで i ・ナンバー着信したが、着呼を中止しました。

【パラメタの意味】 <inumber> : "inumber1": 自局 i ・ナンバー情報1［サブアドレス］
"inumber2": 自局 i ・ナンバー情報2［サブアドレス］

<dial> : 相手局ダイヤル番号（未通知の場合、非通知理由）

【非通知理由】

"O": サービス提供不可	Out of area
"P": ユーザ拒否	Anonymous call (Blocked number)
"S": サービス競合	Interaction with Service
"C": 公衆電話からの発信	Public payphone (Public telephone)

<reason> : "normal" 相手より着信したが自局側で応答しないため、相手が受話器を置きました。

(12) i ・ナンバー着信拒否

analog: stop called (<inumber>) from (<dial>) <reason>

【プライオリティ】 LOG_INFO

【意味】 アナログで i ・ナンバー着信したが、着呼を拒否しました。

【パラメタの意味】 <inumber> : "inumber1": 自局 i ・ナンバー情報1［サブアドレス］
"inumber2": 自局 i ・ナンバー情報2［サブアドレス］

<dial> : 相手局ダイヤル番号（未通知の場合、非通知理由）

【非通知理由】

"O": サービス提供不可	Out of area
"P": ユーザ拒否	Anonymous call (Blocked number)
"S": サービス競合	Interaction with Service
"C": 公衆電話からの発信	Public payphone (Public telephone)

<reason> : detail=xx

<detail=xx 表記の注意 >

切断理由（10進数）、（切断理由不明時は "–"）

切断理由（16進数）、（切断理由不明時は "–"）

(13)疑似着信転送

analog: pseudo call deflection from (<dial1>) to (<dial2>) <reason>

【プライオリティ】 LOG_INFO

【意味】 疑似着信転送が設定されているため、アナログ着信を別の相手へ自動的に転送したことを示します。

【パラメタの意味】 <dial> : （着信元）相手局ダイヤル番号（未通知の場合、非通知理由）

【非通知理由】

"O": サービス提供不可	Out of area
"P": ユーザ拒否	Anonymous call (Blocked number)
"S": サービス競合	Interaction with Service
"C": 公衆電話からの発信	Public payphone (Public telephone)

<dial2> : （転送先）相手局ダイヤル番号

<reason> : "normal" 正常に別の接続相手へ転送できました。

detail=xx

<detail=xx 表記の注意 >

切断理由（10進数）、（切断理由不明時は "–"）

切断理由（16進数）、（切断理由不明時は "–"）

1. 疑似着信転送が成功した場合（転送後の切断系は、2相手との切断ログを出力）

```
analog: pseudo call deflection from (<dial1>) to (<dial2>) normal
analog: disconnected from (<dial1or2>) charge=<value>yen time=<time> <reason>
analog: disconnected to (<dial1or2>) charge=<value>yen time=<time> <reason>
```

2. 疑似着信転送が失敗した場合（転送先話中など）

```
analog: pseudo call deflection from (<dial1>) to (<dial2>) detail=xx
```

■ オンラインサポートのメッセージ

(1)回線接続

dlinkd: connected - <mode> unknown(<dial>) by onlineSupport

【プライオリティ】 LOG_INFO

【意味】 オンラインサポート処理のために、相手システムと接続したことを示します。

【パラメタの意味】

<mode> : 発信／着信の識別

to	: 発信
from	: 着信

<dial> : 相手電話番号。サブアドレスが存在する場合は '*' に続けて表示します。

(2)回線切断

dlinkd: disconnected - <mode> unknown : charge=<value>yen time=<time>

【プライオリティ】 LOG_INFO

【意味】 自側より回線切断を行い、回線が切断されたことを示します。このメッセージは ISDN 回線の場合だけ出力されます。

【パラメタの意味】

<mode> : 切断要求を行った側

to	: 自側
from	: 相手側または網

<value> : 通話料金（円単位）

<time> : 接続時間（dddd.hh:mm:ss の形式）

(3)着信拒否

dlinkd: rejected call from unknown(<dial>) because <reason>

【プライオリティ】 LOG_INFO

【意味】 着信通知を拒絶したことを示します。

【パラメタの意味】

<dial> : 相手電話番号。サブアドレスが存在する場合は '*' に続けて表示します。

<reason> : 拒否理由

UUI error	: 接続要求に含まれる UUI が矛盾
permission denied	: オンラインサポート処理は非許可
dialno error	: 非許容の相手からのオンラインサポート要求
subaddress error	: 非許容のサブアドレス指定
Busy	: オンラインサポート中

■ ProxyDNSのメッセージ

(1)ProxyDNSの問い合わせパケット

proxydns: QNAME [<type>:<qname>] from <ipaddr> to <remote>

【プライオリティ】 LOG_INFO

【意味】 発信契機となったDNSの問い合わせパケットの内容を示します。
このメッセージはISDN回線の場合だけ出力されます。

【パラメタの意味】 <type> : 問い合わせタイプ

<type>	番号	説明
“A”	1	host address
“NS”	2	authoritative server
“CNAME”	5	canonical name
“SOA”	6	atart of authority zone
“MB”	7	mailbox domain name
“MG”	8	mail group member
“MR”	9	mail rename name
“NULL”	10	null resource record
“WKS”	11	well known service
“PTR”	12	domain name pointer
“HINFO”	13	host information
“MINFO”	14	mailbox information
“MX”	15	mail routing information
“TXT”	16	text strings
“AAAA”	28	IP6 Address
“SRV”	33	Server Selection
“ANY”	255	wildcard match
“Type[番号]”	上記以外	

<qname> : 問い合わせホスト名

<ipaddr> : 発信元ホストのIPアドレス

<remote>: 問い合わせ先ネットワーク名

(2)エラー検知によるパケット破棄

```
proxydns: ERROR: recode type <type>, class <class>, from <address>
                 QNAME [<name>]
```

【プライオリティ】　LOG_WARNING

【意味】　不正と思われるtypeやclassを持つDNS要求を破棄したことを示します。

【パラメタの意味】　<type>　: DNS要求パケットのTypeの値

<class>　: DNS要求パケットのClassの値

<address>: DNS要求発行元のIPアドレス

<name>　: DNS要求を行った名前

■ ftpdのメッセージ

(1)ログイン成功

```
ftpd: login <user> from <address>
```

【プライオリティ】　LOG_INFO

【意味】　ftpdへのログインに成功しました。

【パラメタの意味】　<user>　: ログインユーザ名

<address>: クライアントのIPアドレス

(2)ログイン失敗（認証エラー）

```
ftpd: <user> login incorrect from <address>
```

【プライオリティ】　LOG_INFO

【意味】　ftpdへのログインに失敗しました。
無効なユーザ名または間違ったパスワードです。

【パラメタの意味】　<user>　: ログインユーザ名

<address>: クライアントのIPアドレス

(3)ファイル蓄積完了

```
ftpd: <filename> Write complete
```

【プライオリティ】　LOG_INFO

【意味】　ファイル蓄積（クライアントからのput）によりROMが上書きされたことを示します。

【パラメタの意味】　<filename>: 上書きされたファイル名

■ スケジュールのメッセージ

(1)電話番号変更予約の実施

```
scheduled: action: dial number convert [<dial1>] to [<dial2>]
scheduled:   [<no>] <config>: dial number [<dial3>] convert
```

【プライオリティ】 LOG_INFO

【意味】 スケジュール機能による電話番号変更が実施されたことを示します。

【パラメタの意味】

<dial1> : 電話番号変更予約情報の変更前の電話番号

<dial2> : 電話番号変更予約情報の変更後の電話番号

<no> : 処理通番

<config> : 対象となる構成定義情報の名称

<name> は相手ネットワーク名、アクセスポイント名、または相手識別名を示します。

<n>は数字を示します。(詳細は各コマンドの説明を参照)

wan.<n>.isdn.number.<n>
wan.<n>.isdn.numbersend
remote.<name>.ap.<name>.dial.<n>.number
remote.<name>.ap.<name>.called.number
remote.<name>.ap.<name>.called.callback.number
remote.<name>.ap.<name>.callback.number
answer.callback.number
analog.isdn.number
analog.numlist.<name>
analog.flex.call.deflection.line
analog.flex.call.deflection.port1
analog.flex.call.deflection.port2
analog.flex.call.deflection.in1
analog.flex.call.deflection.in2
analog.flex.call.deflection.in3
analog.inumber.in1
analog.inumber.in2
analog.inumber.in3
tel.<n>.dialin
tel.<n>.number
tel.<n>.denylist.<n>
tel.<n>.permitlist.<n>
rcmdinfo.auth

<dial3> : 変更する電話番号

(2)電話番号変更の失敗

scheduled: config size over, convert failed.

【プライオリティ】　LOG_INFO

【意味】　スケジュール機能による電話番号変更が実施されましたが、構成定義格納サイズを超えたため、変更に失敗したことを示します。

■ メールチェックのメッセージ

(1)メールチェックの実施

emaild: <user>: mail receive check [by Remote].

【プライオリティ】　LOG_INFO

【意味】　Eメールエージェント機能によるメールチェックが実施されたことを示します。リモートメールチェックにより実施された場合は、"by Remote"が付加されます。

【パラメタの意味】　<user>　: ユーザ名

(2)メール転送の実施

emaild: <user>: mail relay to <to>

【プライオリティ】　LOG_INFO

【意味】　Eメールエージェント機能によるメール転送が実施されたことを示します。宛先メールアドレスが複数定義されている場合は、宛先メールアドレスごとに出力します。

【パラメタの意味】　<user>　: ユーザ名

<to>　: 宛先メールアドレス

(3)メール一覧送信の実施

emaild: <user>: mail list send to <to>

【プライオリティ】　LOG_INFO

【意味】　Eメールエージェント機能によるメール一覧送信が実施されたことを示します。宛先メールアドレスが複数定義されている場合は、宛先メールアドレスごとに出力します。

【パラメタの意味】　<user>　: ユーザ名

<to>　: 宛先メールアドレス

(4)TEL メールの実施

```
emaild: TEL<num>: Tel mail send to <to>
```

【プライオリティ】　LOG_INFO

【意味】　Eメールエージェント機能による TEL メールが実施されたことを示します。

【パラメタの意味】　<num>　: ポート番号

<to>　: 宛先メールアドレス

(5)サーバの検索（DNS）の失敗（サーバエラー）

```
emaild: <user>[<phase>]: <server>: Host name lookup failure.
```

【プライオリティ】　LOG_INFO

【意味】　Eメールエージェントが処理を実施したが、構成定義に指定されたメールサーバを発見できなかったことを示します。

【パラメタの意味】　<user>　: ユーザ名または、ポート番号

<phase>　: 発生契機 "POP" または、"SMTP"

<server>　: メールサーバ名

(6)サーバとの接続エラー

```
emaild: <user>[<phase>]: <server>: Unable to connect.
```

【プライオリティ】　LOG_INFO

【意味】　Eメールエージェントが処理を実施したが、構成定義に指定されたメールサーバに接続できなかったことを示します。

【パラメタの意味】　<user>　: ユーザ名または、ポート番号

<phase>　: 発生契機 "POP" または、"SMTP"

<server>　: メールサーバ名

(7)メール送受信時のエラー

```
emaild: <user>[<phase>]: <message>
```

【プライオリティ】　LOG_INFO

【意味】　Eメールエージェントが処理を実施したが、メール送受信時になんらかの理由によりメールサーバがエラー通知したことを示します。

【パラメタの意味】　<user>　: ユーザ名または、ポート番号

<phase>　: 発生契機 "POP" または、"SMTP"

<message>: メールサーバが送信するエラーメッセージメールサーバから応答がない場合は、"timeout" が設定されます。

■ RADIUS クライアントのメッセージ

(1) 応答認証情報の不一致

radiusd: Bad authenticator, Secret may be wrong. id=<id> [<ch>]

【プライオリティ】　LOG_WARNING

【意味】　受信したRADIUSパケットの認証情報が不正でした。RADIUSサーバと本装置との「Secret」（認証キー）が一致していないことが考えらます。

【パラメタの意味】
<id>　: RADIUSパケットのID（Identifier）
<ch>　: 接続物理チャネル
B1ch または B2ch

(2) 認証失敗1

radiusd: authentication failed at bad Service-Type(<code>) [<ch>]

【プライオリティ】　LOG_INFO

【意味】　受信したRADIUSパケットのService-Typeアトリビュートが不正であったため認証が失敗しました。

【パラメタの意味】
<code>　: Service-Typeの値
<ch>　: 接続物理チャネル
B1ch または B2ch

(3) 認証失敗2

radiusd: authentication failed at bad Framed-Protocol(<code>) [<ch>]

【プライオリティ】　LOG_INFO

【意味】　受信したRADIUSパケットのFramed-Protocolアトリビュートが不正であったため認証が失敗しました。

【パラメタの意味】
<code>　: Framed-Protocolの値
<ch>　: 接続物理チャネル
B1ch または B2ch

(4) 認証失敗3

```
radiusd: authentication rejected: <msg> [<ch>]
```

【プライオリティ】 LOG_INFO

【意味】 RADIUS 認証サーバから認証拒否（Access-Reject)を受け取りました。

【パラメタの意味】 <msg> : 拒否されたメッセージ（Reply-Message）を表示
Reply-Message が送られてきていない場合は <msg> には何も表示されない

<ch> : 接続物理チャネル
B1ch または B2ch

(5) 認証失敗4

```
radiusd: Access-Challenge not support [<ch>]
```

【プライオリティ】 LOG_INFO

【意味】 RADIUS 認証サーバから Access-Challenge を受け取ったため、認証が失敗しました。

【パラメタの意味】 <msg> : 拒否されたメッセージ（Reply-Message）を表示
Reply-Message が送られてきていない場合は <msg> には何も表示されない

<ch> : 接続物理チャネル
B1ch または B2ch

(6) 認証失敗5

```
radiusd: auth server[<ipaddress>] not responding
```

【プライオリティ】 LOG_INFO

【意味】 RADIUS 認証サーバが無応答だったため、認証が失敗しました。

【パラメタの意味】 <ipaddress>: RADIUS 認証サーバの IP アドレス

(7) 認証失敗6

```
radiusd: authentication retry over [<ch>]
```

【プライオリティ】 LOG_INFO

【意味】 RADIUS 認証サーバからの不正応答が原因で再試行オーバとなり、認証が失敗しました。

【パラメタの意味】 <ch> : 接続物理チャネル
B1ch または B2ch

(8) 課金開始失敗1

```
radiusd: accounting start failed. server[<ipaddress>] not responding
```

【プライオリティ】 LOG_INFO

【意味】 RADIUS アカウントサーバが無応答のため課金開始が正常に行えませんでした。

【パラメタの意味】 <ipaddress>: RADIUS アカウントサーバの IP アドレス

(9) 課金開始失敗2

```
radiusd: accounting start retry over [<ch>]
```

【プライオリティ】 LOG_INFO

【意味】 RADIUS アカウントサーバからの不正応答が原因で再試行オーバとなり、課金開始が失敗しました。

【パラメタの意味】 <ch> : 接続物理チャネル
B1ch または B2ch

(10) 課金終了失敗1

```
radiusd: accounting stop failed. server[<ipaddress>] not responding
```

【プライオリティ】 LOG_INFO

【意味】 RADIUS アカウントサーバが無応答のため課金終了が正常に行えませんでした。

【パラメタの意味】 <ipaddress>: RADIUS アカウントサーバの IP アドレス

(11) 課金終了失敗2

```
radiusd: accounting stop retry over [<ch>]
```

【プライオリティ】 LOG_INFO

【意味】 RADIUS アカウントサーバからの不正応答が原因で再試行オーバとなり、課金終了が失敗しました。

【パラメタの意味】 <ch> : 接続物理チャネル
B1ch または B2ch

(12) 課金終了再試行の中断

radiusd: abort accounting stop retry sequence [<ch>]

【プライオリティ】 LOG_INFO

【意味】 課金終了通知（Accounting-Request:Stop）の再送中に以下の認証または課金要求を受け付け、再送処理を終了しました。

【パラメタの意味】 <ch> : 接続物理チャネル
B1ch または B2ch

■ セキュリティのメッセージ

(1)ProxyDNS による DNS 要求破棄

proxydns: rejected by <no> : QNAME [<type>:<qname>] from <ipaddr>

【プライオリティ】 LOG_NOTICE

【意味】 ProxyDNS で、破棄指定により破棄されたことを示します。

【パラメタの意味】 <no> : reject を行ったproxydns 命令の定義番号
（注）画面上の番号ではなく、コマンドライン上の番号
<type> : 問い合わせタイプ
<qname> : 問い合わせホスト名
<ipaddr> : 発信元ホストの IP アドレス

(2)ProxyDNS による unicode DNS要求の破棄

proxydns: rejected by unknown character : QTYPE [<type>] from <ipaddr>

【プライオリティ】 LOG_NOTICE

【意味】 ProxyDNS で、非表示文字の破棄指定により破棄されたことを示します。

【パラメタの意味】 <type> : 問い合わせタイプ
<ipaddr> : 発信元ホストの IP アドレス

(3)IP Filter によるパケット破棄

protocol: rejected at filter(<name>.<no>) : <P> <SA>:<SP> -> <DA>:<DP>

【プライオリティ】 LOG_NOTICE

【意味】 IP Filter で、破棄指定により破棄されたことを示します。

【パラメタの意味】
<name> : ネットワーク名
<no> : reject を行ったip filter 命令の定義番号
（注）画面上の番号ではなく、コマンドライン上の番号
<P> : プロトコル種別（TCP、UDP、ICMP、IP、その他は番号）
TCP のSYN パケットの場合は、TCP（S）と出力する
<SA> : source IP address
<SP> : source port （プロトコル種別がTCP またはUDP であった場合）
<DA> : destination IP address
<DP> : destination port （プロトコル種別がTCP またはUDP であった場合）

(4)IPv6 Filter によるパケット破棄

protocol: rejected at filter(<name>.<no>) : <P> <SA>(<SP>) -> <DA>(<DP>)

【プライオリティ】 LOG_NOTICE

【意味】 IPv6 Filter で、破棄指定により破棄されたことを示します。

【パラメタの意味】
<name> : ネットワーク名
<no> : reject を行ったip6 filter 命令の定義番号
（注）画面上の番号ではなく、コマンドライン上の番号
特殊フィルタルールに適合した場合には、その内容が出力されます。
same address : source/destination ともに同じアドレスであった
tiny fragment : tiny fragment を検出した
overlap fragment : overlap fragment を検出した
unknown fragment : unknown fragment を検出した
default restrict : デフォルトフィルタに適合した
<P> : プロトコル種別（TCP、UDP、ICMPV6、その他は番号）
TCP のSYN パケットの場合は、TCP（S）と出力する
<SA> : source IPv6 address
<SP> : source port （プロトコル種別がTCP またはUDP であった場合）
<DA> : destination IPv6 address

<DP> : destination port （プロトコル種別がTCPまたはUDPであった場合）

(5)NATによるパケット破棄

```
protocol: rejected at NAT(<name>) : <P> <SA>:<SP> -> <DA>:<DP>
```

【プライオリティ】 LOG_NOTICE

【意味】 NATで、変換テーブルがなかったことにより破棄されたことを示します。

【パラメタの意味】 <name> ：ネットワーク名

<P> ：プロトコル種別（TCP、UDP、ICMP、IP、その他は番号）
TCPのSYNパケットの場合は、TCP（S）と出力する

<SA> : source IP address

<SP> : source port （プロトコル種別がTCPまたはUDPであった場合）

<DA> : destination IP address

<DP> : destination port （プロトコル種別がTCPまたはUDPであった場合）

(6)NAT変換テーブル作成

```
protocol: NAT:table: <P> <SA> -> <DA>:<DP>
```

【プライオリティ】 LOG_NOTICE

【意味】 NATで、パケット転送に伴い、変換テーブルを作成したことを示します。

【パラメタの意味】 <P> ：プロトコル種別（TCP、UDP、ICMP、IP、その他は番号）
基本NATによるテーブル作成の場合は、ALLと表示する

<SA> : source IP address

<SP> : source port （プロトコル種別がTCPまたはUDPであった場合）

<DA> : destination IP address

<DP> : destination port （プロトコル種別がTCPまたはUDPであった場合）

(7)PPP 着信拒否

protocol: rejected call from <target>(<dial>) by PPP:<reason>

【プライオリティ】 LOG_NOTICE

【意味】 PPP ネゴシエーション中に着信を拒否したことを示します。

【パラメタの意味】 <target> : ネットワーク名.接続先名

<dial> : 接続ダイアル番号

<reason> : 認証失敗理由

authentication rejected : 認証利用そのものが拒否された

callback rejected : コールバックなしで着信を要求された

wrong account(<id>) : 不正認証情報受信（<id>にID情報を出力）

(8)DHCP サーバのアドレス配布

dhcpd: Server allocation <ip_address> to <mac_address>

【プライオリティ】 LOG_NOTICE

【意味】 DHCP サーバが DHCP クライアントにアドレスを配布したことを示します。

【パラメタの意味】 <ip_address> : DHCP クライアントに配布した IP アドレス

<mac_address> : DHCP クライアントの MAC アドレス

■ マルチ TA のメッセージ

(1)回線接続

mtad: connected <ch> to (<dial>) by multiTA

【プライオリティ】　LOG_INFO

【意味】　発信により相手システムと接続したことを示します。

【パラメタの意味】　<ch>　: 接続物理チャネル
B1ch または B2ch
<dial>　: 接続ダイアル番号

(2)自側からの回線切断

mtad: disconnected <ch> to (<dial>) : charge=<value>yen time=<time>

【プライオリティ】　LOG_INFO

【意味】　自側より回線切断を行い、回線が切断されたことを示します。

【パラメタの意味】　<ch>　: 接続物理チャネル
B1ch または B2ch
<dial>　: 接続ダイアル番号
<value>　: 通話料金（円単位）
<time>　: 接続時間（dddd.hh:mm:ss の形式）

(3)相手または網からの回線切断

mtad: disconnected <ch> from (<dial>) : charge=<value>yen time=<time>

【プライオリティ】　LOG_INFO

【意味】　相手側、または網から回線切断が通知され、回線が切断されたことを示します。

【パラメタの意味】　<ch>　: 接続物理チャネル
B1ch または B2ch
<dial>　: 接続ダイアル番号
<value>　: 通話料金（円単位）
<time>　: 接続時間（dddd.hh:mm:ss の形式）

■ フレームリレーのメッセージ

(1)CLLM メッセージ受信

frctl: received CLLM(<kind>) about <remote_name>(DLCI:<dlci>)

【プライオリティ】 LOG_INFO

【意味】 CLLM メッセージを受信しました。

【パラメタの意味】

<kind> : CLLM メッセージの種類

2 ：トラフィックによる軽輻輳

3 ：トラフィックによる重輻輳

6 ：装置故障（短時間）

7 ：装置故障（長時間）

10：保守動作（短時間）

11：保守動作（長時間）

16：原因不明の軽輻輳

17：原因不明の重輻輳

輻輳通知を受けた場合はスループットを減少させます。

装置故障通知または保守動作通知を受けた PVC をインアクティブにします。

<remote_name>: 相手ネットワーク名

ネットワーク名がない場合は 「remote<remote番号 >」

<dlci> : 通知内容に該当する DLCI

(2)PVC 状態アクティブ

frctl: <remote_name>(DLCI:<dlci>) became active

【プライオリティ】 LOG_INFO

【意味】 PVC 状態確認手順のフル状態表示または単一 PVC 非同期状態表示によって PVC がアクティブになりました。

【パラメタの意味】

<remote_name>: 相手ネットワーク名

ネットワーク名がない場合は 「remote<remote番号 >」

<dlci> : アクティブとなった PVC の DLCI

(3)PVC 状態インアクティブ

frctl: <remote_name>(DLCI:<dlci>) became inactive

【プライオリティ】 LOG_INFO

【意味】 PVC 状態確認手順のフル状態表示または単一 PVC 非同期状態表示によって PVC がインアクティブになりました。

【パラメタの意味】 <remote_name>: 相手ネットワーク名
ネットワーク名がない場合は 「remote<remote番号>」
<dlci> : インアクティブとなった PVC の DLCI

(4)CLLM メッセージ軽輻輳通知による PVC アクティブ

frctl: <remote_name>(DLCI:<dlci>) became active by CLLM light

【プライオリティ】 LOG_INFO

【意味】 CLLM メッセージの軽輻輳通知によって PVC がアクティブになりました。

【パラメタの意味】 <remote_name>: 相手ネットワーク名
ネットワーク名がない場合は 「remote<remote番号>」
<dlci> : アクティブとなった PVC の DLCI

(5)CLLM メッセージ重輻輳通知による PVC アクティブ

frctl: <remote_name>(DLCI:<dlci>) became active by CLLM serious

【プライオリティ】 LOG_INFO

【意味】 CLLM メッセージの重輻輳通知によって PVC がアクティブになりました。

【パラメタの意味】 <remote_name>: 相手ネットワーク名
ネットワーク名がない場合は 「remote<remote番号>」
<dlci> : アクティブとなった PVC の DLCI

(6)CLLM メッセージ装置故障通知または保守動作通知による PVC インアクティブ

frctl: <remote_name>(DLCI:<dlci>) became inactive by CLLM stop

【プライオリティ】 LOG_INFO

【意味】 CLLM メッセージの装置故障通知または保守動作通知によって PVC がインアクティブになりました。

【パラメタの意味】 <remote_name>: 相手ネットワーク名
ネットワーク名がない場合は 「remote<remote番号>」
<dlci> : インアクティブとなった PVC の DLCI

(7)T2タイマタイムアウトによるPVCアクティブ

frctl: <remote_name>(DLCI:<dlci>) became active by T2-timer timeout

【プライオリティ】　LOG_INFO

【意味】　CLLM回復タイマ（T2）のタイムアウトによってPVCがアクティブになりました。

【パラメタの意味】　<remote_name>：相手ネットワーク名
ネットワーク名がない場合は 「remote<remote番号>」
<dlci>　：アクティブとなったPVCのDLCI

(8)PVC状態確認手順による回線故障検出

frctl: PVC link was disconnected

【プライオリティ】　LOG_INFO

【意味】　PVC状態確認手順により回線異常を検出した。
最新の4回の「状態問合」メッセージの送信に対し、「状態表示」メッセージ未受信または無効メッセージ受信のエラーを3回以上検出したことを示します。

(9)PVC状態確認手順による回線の故障状態からの回復

frctl: PVC link recover

【プライオリティ】　LOG_INFO

【意味】　PVC確認手順により検出した回線異常状態から回復した。
3回連続して正しい「状態表示」メッセージを受信したことを示します。

■ ブリッジ／STPのメッセージ

(1)構成変更を検出

protocol: Topology changed [<root>:<priority>]

【プライオリティ】　LOG_INFO

【意味】　ネットワークブリッジの構成の変化を検出したことを示します。

【パラメタの意味】　<root>　：ルートブリッジのMACアドレス
<priority>　：ルートブリッジの優先度

(2)上位ブリッジのダウンを検出

protocol: STP aging timer expired [<root>:<interface>]

【プライオリティ】 LOG_INFO

【意味】 自装置の上位のブリッジ装置から定期的に送信される構成情報BPDUが規定時間内に受信できないことにより上位ブリッジ装置のダウンを検出したことを示します。

【パラメタの意味】 <root> : ルートブリッジのMACアドレス

<interface> : ダウンを検出したブリッジ装置が接続されるインタフェース名

■ マルチホーミングのメッセージ

(1)パケット転送処理部のシステムログ

protocol:dynamic multihoming table is full [<remote>]

【プライオリティ】 LOG_INFO

【意味】 動的マルチホーミング情報テーブルの情報数が最大数に達し、これ以上の情報を記録できなくなりました。

【パラメタの意味】 <remote> : ネットワーク名

(2)マルチホーミングデーモンのシステムログ

mhomed: forwarding session route error [<remote>]

【プライオリティ】 LOG_INFO

【意味】 転送セッションの経路に障害が発生しました。

【パラメタの意味】 <remote> : ネットワーク名

mhomed: forwarding session route recovery [<remote>]

【プライオリティ】 LOG_INFO

【意味】 転送セッションの経路の障害が復旧しました。

【パラメタの意味】 <remote> : ネットワーク名

(3)WAN側セッション経路の復旧

icmpwatchd: multihoming WAN session watching host is up. [<remote>]

【プライオリティ】　LOG_INFO

【意味】　WAN側セッションの経路が復旧したことを示します。

【パラメタの意味】　<remote>　: 相手ネットワーク名

<ap>　: アクセスポイント名

(4)WAN側セッション経路の障害検出

icmpwatchd: multihoming WAN session watching host is down. [<remote>]

【プライオリティ】　LOG_INFO

【意味】　WAN側セッションの経路に障害が発生したことを示します。

【パラメタの意味】　<remote>　: 相手ネットワーク名

<ap>　: アクセスポイント名

■ IPsec／IKEのメッセージ

(1)ISAKMP SAネゴシエーション

isakmp: not acceptable <etype> mode

【プライオリティ】　LOG_INFO

【意味】　サポートされていない、または受け入れられない交換タイプを受信したことを示します。このメッセージはISAKMP SAのネゴシエーションデータ受信時に、自側の設定により決定した交換タイプとは異なるタイプを受信した時に出力されます。

【パラメタの意味】　<etype>　: 交換タイプ

サポートされていない交換タイプ

1　Base

受け入れられない交換タイプ

※自側の設定により決定した交換タイプとは異なるタイプ

2　Identity Protection

4　Aggressive

isakmp: invalid encryption algorithm <algorithm>

【プライオリティ】 LOG_INFO

【意味】 サポートされていない、または不正な暗号アルゴリズムを受信したことを示します。このメッセージはISAKMP SAのネゴシエーションのデータ属性受信時に、DES-CBC、3DES-CBC以外の暗号アルゴリズムを受信した時に出力されます。

【パラメタの意味】 <algorithm> : 暗号アルゴリズム

サポートされていない暗号アルゴリズム

2 IDEA暗号アルゴリズム

3 Blowfish暗号アルゴリズム

4 RC5-R16-B64暗号アルゴリズム

6 CAST暗号アルゴリズム

不正な暗号アルゴリズム

1～6以外の不定の値

※以下の暗号アルゴリズムはサポートされているため出力されることはありません。

1 DED CBC暗号アルゴリズム

5 3DEC CBC暗号アルゴリズム

isakmp: invalid hash algorithm <algorithm>

【プライオリティ】 LOG_INFO

【意味】 サポートされていない、または不正なハッシュアルゴリズムを受信したことを示します。このメッセージはISAKMP SAのネゴシエーションのデータ属性受信時に、MD5、SHA以外のハッシュアルゴリズムを受信した時に出力されます。

【パラメタの意味】 <algorithm> : ハッシュアルゴリズム

サポートされていないハッシュアルゴリズム

3 Tigerハッシュアルゴリズム

不正なハッシュアルゴリズム

1～3以外の不定の値

※以下のハッシュアルゴリズムはサポートされているため出力されることはありません。

1 MD5アルゴリズム

2 SHAアルゴリズム

isakmp: invalid authentication method <method>

【プライオリティ】 LOG_INFO

【意味】 サポートされていない、不正な認証方式を受信したことを示します。このメッセージはISAKMP SAのネゴシエーションのデータ属性受信時に、共通鍵（Pre-shared key）認証以外の認証方法を受信した時に出力されます。

【パラメタの意味】 <method> ：認証方法

サポートされていない認証方式

2 DSS署名認証方式

3 RSA署名認証方式

4 RSA暗号認証方式

5 改良RSA暗号認証方式

不正な認証方式

1～5以外の不定の値

※以下の認証方式はサポートされているため出力されることはありません。

1 既知共有鍵認証方式

isakmp: invalid DH group type <group>

【プライオリティ】 LOG_INFO

【意味】 サポートされていない、または不正なグループタイプを受信したことを示します。このメッセージはISAKMP SAのネゴシエーションのデータ属性受信時に、RFC2409に定義されている中でMODP以外のグループタイプを受信した時に出力されます。

【パラメタの意味】 <group> ：グループ記述子

サポートされていないグループタイプ

2 ECP楕円関数グループ

3 EC2N楕円関数グループ

不正な認証方式

1～3以外の不定の値

※以下のグループタイプはサポートされているため出力されることはありません。

1 MODP指数関数グループ

isakmp: ignore the packet, expecting the packet encrypted

【プライオリティ】 LOG_INFO

【意味】 受信パケットが暗号化されていることを期待していたが、暗号化されていないため、パケットを破棄したことを示します。このメッセージはISAKMP SAのネゴシエーションで、鍵交換後のパケットは暗号化されることを期待するが、暗号化されていないパケットを受信した時に出力されます。

isakmp: Expecting IP address type in main mode, but <type>

【プライオリティ】 LOG_INFO

【意味】 Mainモードで受信したIDペイロードのIPアドレスタイプが、期待していたタイプでなかったことを示します。このメッセージはISAKMP SAのネゴシエーションを共有鍵（Pre-shared key）認証で行う場合に、IDペイロードの交換がIPv4アドレス、IPv6アドレス以外で行われた時に出力されます。

【パラメタの意味】 <type> ：IDタイプ

サポートされていないグループタイプ

1	IPv4アドレス
2	省略なしドメイン名
3	省略なしユーザ名
4	IPv4アドレスとネットマスク
5	IPv6アドレス
6	IPv6アドレスとネットマスク
7	IPv4アドレス範囲指定
8	IPv6アドレス範囲指定
9	証明書対象者のX.501バイナリDERエンコーディング
10	証明書対象者のX.509バイナリDERエンコーディング
11	独自ID情報

不正なIDタイプ

1～11以外の不定の値

isakmp: phase1 information overflow.

【プライオリティ】　LOG_INFO

【意味】　ISAKMP SAのネゴシエーションで、Phase1情報が最大数を超えたことを示します。このメッセージは、大規模構成で同時にIPsec/IKE通信を行い、それぞれのIPsec SA更新のタイミングが同時期に行われた場合や相手装置の問題によって定義数以上のネゴシエーションが行われた場合に出力されます。

isakmp: phase2 information overflow.

【プライオリティ】　LOG_INFO

【意味】　ISAKMP SAのネゴシエーションで、Phase2情報が最大数を超えたことを示します。このメッセージは、大規模構成で同時にIPsec/IKE通信を行い、それぞれのIPsec SA更新のタイミングが同時期に行われた場合や相手装置の問題により定義数以上のネゴシエーションが行われた場合に出力されます。

(2)IKEセッションの復旧

icmpwatchd: IKE session watching host is up. [<remote>.<ap>]

【プライオリティ】　LOG_INFO

【意味】　IKEセッションの監視ホスト、または接続回線が復旧したことを示します。

【パラメタの意味】　<remote>　：相手ネットワーク名

<ap>　：アクセスポイント名

(3)IKEセッションの障害検出

icmpwatchd: IKE session watching host is down. [<remote>.<ap>]

【プライオリティ】　LOG_INFO

【意味】　IKEセッションの監視ホスト、または接続回線に障害が発生したことを示します。

【パラメタの意味】　<remote>　：相手ネットワーク名

<ap>　：アクセスポイント名

(4)IPsec SA ネゴシエーション

isakmp: invalid transform id=<id> in <protocol>

【プライオリティ】 LOG_INFO

【意味】 サポートされていない、または不正なトランスフォーム ID を受信したことを示します。このメッセージは IPsec SA のネゴシエーション開始時に、受信したトランスフォームペイロードトランスフォーム ID が未サポート、または不正な認証または暗号アルゴリズムの場合に出力されます。

【パラメタの意味】 <id> : トランスフォーム ID（認証／暗号アルゴリズム）

protocol が ISAKMP の時

不正なトランスフォーム ID

1 以外の不定の値

※以下のトランスフォーム ID はサポートされているため出力されることはありません。

1 IKE

protocol が AH の時

サポートされていないトランスフォーム ID

3 DES 認証アルゴリズム

不正なトランスフォーム ID

1～3 以外の不定の値

※以下のトランスフォーム ID はサポートされているため出力されることはありません。

2 MD5 認証アルゴリズム

3 SHA 認証アルゴリズム

protocol が ESP の時

サポートされていないトランスフォーム ID

1 DES IV64 暗号アルゴリズム

4 RC5 暗号アルゴリズム

5 IDEA 暗号アルゴリズム

6 CAST 暗号アルゴリズム

7 Blowfish 暗号アルゴリズム

8 トリプル IDEA 暗号アルゴリズム

9 DES IV32 暗号アルゴリズム

10 RC4 暗号アルゴリズム

不正なトランスフォーム ID

1～10 以外の不定の値

※以下のトランスフォームIDはサポートされているため出力されることはない。

2　DES暗号アルゴリズム

3　3DES暗号アルゴリズム

<protocol>　: プロトコル

1　ISAKMPプロトコル

2　認証プロトコル

3　暗号プロトコル

isakmp: invalid encryption mode=<mode>

【プライオリティ】　LOG_INFO

【意味】　サポートされていない、または不正なカプセルモードを受信したことを示します。このメッセージはIPsec SAのネゴシエーションのデータ属性受信時に、トンネルモード以外のカプセルモードを受信した時に出力されます。

【パラメタの意味】　<mode>　: カプセルモード

サポートされていないカプセルモード

2　トランスポートモード

不正なカプセルモード

1、2以外の不定の値

※以下のカプセルモードはサポートされているため出力されることはありません。

1　トンネルモード

isakmp: invalid authentication algorithm=<algorithm>

【プライオリティ】　LOG_INFO

【意味】　サポートされていない、または不正な認証アルゴリズムを受信したことを示します。このメッセージはIPsec SAのネゴシエーションのデータ属性受信時に、HMAC-MD5、HMAC-SHA1以外の認証アルゴリズムを受信した時に出力されます。

【パラメタの意味】　<algorithm>　: 認証アルゴリズム

サポートされていない認証アルゴリズム

3　DES MAC認証アルゴリズム

4　KPDK認証アルゴリズム

不正な認証アルゴリズム

1～4以外の不定の値

※以下の認証アルゴリズムはサポートされているため出力されることはない。

1　HMAC MD5 認証アルゴリズム

2　HMAC SHA認証アルゴリズム

(5)ISAKMP、IPsec 共通

isakmp: invalid value of DOI 0x<doi>

【プライオリティ】　LOG_INFO

【意味】　不正なDOIの値を受信したことを示します。このメッセージはISAKMP SAまたはIPsec SAのネゴシエーション開始時に、受信したSAペイロードのDOIがIPsec DOI以外の場合に出力されます。

【パラメタの意味】　<doi>　: DOI

00000001以外の不定の値

isakmp: invalid situation 0x<situation>

【プライオリティ】　LOG_INFO

【意味】　サポートされていない、または不正なSituationの値を受信したことを示します。このメッセージはISAKMP SAまたはIPsec SAのネゴシエーション開始時に、受信したSAペイロードのSituationがSIT_IDENTITY_ONLY以外の場合に出力されます。

【パラメタの意味】　<situation>　: situation

サポートされていないSituation

00000002

ネゴシエーション中のSAが、ラベル付けされたセキュリティが必要な環境にあることを示します。

00000004

ネゴシエーション中のSAが、ラベルが付いたインテグリティを必要とする環境にあることを示します。

不正なsituation

00000001、00000002、00000004以外の不定の値

※以下のSituationはサポートされているため出力されることはありません。

0000000x

発信元ID情報によってSAを確認することを指定する

isakmp: invalid protocol id <id>

【プライオリティ】　LOG_INFO

【意味】　サポートされていない、または不正なプロトコルIDの値を受信したことを示します。このメッセージはISAKMP SAまたはIPsec SAのネゴシエーション開始時に、受信したプロポーザルペイロードのプロトコルIDがISAKMP、AH、ESP以外の場合に出力されます。

【パラメタの意味】　<id>　：プロトコルID

サポートされていないプロトコルID

4　圧縮プロトコル

不正なプロトコルID

1～4以外の不定の値

※以下のプロトコルIDはサポートされているため出力されることはありません。

1　ISAKMPプロトコル

2　IPsec認証プロトコル

3　IPsec暗号プロトコル

isakmp: invalid life type <type>

【プライオリティ】　LOG_INFO

【意味】　不正な Life タイプを受信したことを示します。このメッセージはISAKMP SAまたはIPsec SAのネゴシエーションのデータ属性受信時に、RFC2409に定義されていないLifeタイプを受信した時に出力されます。

【パラメタの意味】　<type>　：Lifeタイプ

不正なプロトコルID

1、2以外の不定の値

※以下のLifeタイプはサポートされているため出力されることはありません。

1　単位秒

2　単位キロバイト

isakmp: invalid attribute type <type>

【プライオリティ】 LOG_INFO

【意味】 サポートされていない、または不正な属性タイプを受信したことを示します。このメッセージはISAKMP SAまたはIPsec SAのネゴシエーションのデータ属性受信時に、サポートされていないまたはRFC2409に定義されていない属性タイプを受信した時に出力されます。

【パラメタの意味】 <type> : 属性タイプ

ISAKMP SAネゴシエーションの時

サポートされていない属性タイプ

- 8 グループ生成2属性タイプ
- 9 グループ曲線A属性タイプ
- 10 グループ曲線B属性タイプ
- 15 フィールド長属性タイプ

不正な属性タイプ

1～15以外の不定の値

※以下の属性タイプはサポートされているため出力されることはありません。

- 1 暗号アルゴリズム
- 2 ハッシュアルゴリズム
- 3 認証方法
- 4 グループ記述子
- 5 グループタイプ
- 6 グループ素数／規約多項式
- 7 グループ生成1
- 11 Lifeタイプ
- 12 Life継続期限
- 13 prf
- 14 鍵長

IPsec SAネゴシエーションの時

サポートされていない属性タイプ

- 7 鍵ラウンド属性タイプ
- 8 圧縮辞書サイズ属性タイプ
- 9 圧縮プライベート アルゴリズム

不正な属性タイプ

1～9以外の不定の値

※以下の属性タイプはサポートされているため出力されることはありません。

1　Life タイプ
2　Life 継続期限
3　グループ記述子
4　カプセルモード
5　認証アルゴリズム
6　鍵長

isakmp: invalid group description=<group>

【プライオリティ】　LOG_INFO

【意味】　サポートされていない、または不正なグループ記述子を受信したことを示します。このメッセージは ISAKMP SA または IPsec SA のネゴシエーションのデータ属性受信時に、サポートされていないまたは RFC2409 に定義されていないグループ記述子を受信した時に出力されます。

【パラメタの意味】　<group>　: グループ記述子

サポートされていないグループ記述子

3　EC2N[2^155] 楕円関数グループ
4　EC2N[2^185] 楕円関数グループ
5　1536 ビット MODP グループ

不正なグループ記述子

1 ～ 5 以外の不定の値

※以下のグループ記述子はサポートされているため出力されることはありません。

1　768 ビット MODP グループ
2　1024 ビット MODP グループ

isakmp: ignore the packet, received unexpecting payload type <group>

【プライオリティ】　LOG_INFO

【意味】　期待していないペイロードタイプを受信したため、そのパケットを破棄したことを示します。このメッセージはISAKMP SA またはIPsec SA のネゴシエーションで、受信したパケットに期待していないペイロードが含まれていた時に出力されます。

【パラメタの意味】　<group>　: ペイロードタイプ

- 0　noneペイロード
- 1　SAペイロードタイプ
- 2　プロポーザルペイトロードタイプ
- 3　トランスフォームペイトロードタイプ
- 4　鍵交換ペイロードタイプ
- 5　ID ペイロードタイプ
- 6　証明書ペイロードタイプ
- 7　証明書要求ペイロードタイプ
- 8　ハッシュペイロードタイプ
- 9　署名ペイロードタイプ
- 10　Nonceペイロードタイプ
- 11　通知ペイロードタイプ
- 12　削除ペイロードタイプ
- 13　ベンダ ID ペイロードタイプ

不正なペイロードタイプ

0～13以外の不定の値

isakmp: received invalid next payload type <receive type>, expecting <expect type>

【プライオリティ】 LOG_INFO

【意味】 期待していたペイロードタイプとは異なるペイロードが次ペイロードに指定されていたことを示します。このメッセージはISAKMP SAまたはIPsec SAのネゴシエーションで、自身が受けるのパケット構成とは異なる構成のパケットを受信した時に出力されます。

【パラメタの意味】 <receive type>: 受信した次ペイロードタイプ

0	noneペイロード
1	SAペイロードタイプ
2	プロポーザルペイロードタイプ
3	トランスフォームペイロードタイプ
4	鍵交換ペイロードタイプ
5	IDペイロードタイプ
6	証明書ペイロードタイプ
7	証明書要求ペイロードタイプ
8	ハッシュペイロードタイプ
9	署名ペイロードタイプ
10	Nonceペイロードタイプ
11	通知ペイロードタイプ
12	削除ペイロードタイプ
13	ベンダIDペイロードタイプ

不正なペイロードタイプ

0～13以外の不定の値

<expect type>: 期待していたペイロードタイプ

1	SAペイロードタイプ
8	ハッシュペイロードタイプ

isakmp: HASH mismatched side=<side> exchange type=<type> status=<status>

【プライオリティ】 LOG_INFO

【意味】 受信したハッシュ値と受信パケットから生成したハッシュ値が一致しないことを示します。このメッセージはISAKMP SAまたはIPsec SAのネゴシエーション中に、イニシエータまたはレスポンダによって出力されます。イニシエータまたはレスポンダから受信したパケットがデータの破壊や改竄などにより、正常なパケットと判断できなかったことを示します。また、Aggressive交換では、共通鍵が一致しない場合も出力されます。

【パラメタの意味】

<side> : 自側の状態

- 0 イニシエータ側
- 1 レスポンダ側

<type> : ISAKMP交換の種類

- 2 Identity Protection交換
- 4 Aggressive交換
- 32 Quick交換

<status> : ISAKMP交換での状態

Identity Protection交換イニシエータの時

- 7 3rdメッセージ受信時

Identity Protection交換レスポンダの時

- 5 3rdメッセージ受信時

Aggressive交換イニシエータの時

- 3 1rdメッセージ受信時

Aggressive交換レスポンダの時

- 3 2stメッセージ受信時

Quick交換イニシエータの時

- 5 1stメッセージ受信時

Quick交換レスポンダの時

- 1 1stメッセージ受信時
- 5 2stメッセージ受信時

isakmp: psk mismatched.

【プライオリティ】 LOG_INFO

【意味】 ISAKMP SAのネゴシエーションで共通鍵が一致していない可能性があることを示します。共通鍵が一致していない可能性がある時にレスポンダにより出力されます。

isakmp: give up phase1 negotiation.

【プライオリティ】　LOG_INFO

【意味】　ISAKMP　SAのネゴシエーションの再送回数が終了したことを示します。このメッセージは回線異常、相手装置の問題によりネゴシエーションパケットが受信できなかった場合や設定ミスによりパケットが破棄されたことにより、ネゴシエーションが失敗した時に出力されます。

isakmp: IPsec SA protocol id mismatched.

【プライオリティ】　LOG_INFO

【意味】　IPsec SAのネゴシエーションプロトコルが、受信したIPsec SAのネゴシエーションと一致しなかったことを示します。IPsec SAのネゴシエーションに失敗した時にレスポンダによって出力されます。

isakmp: IPsec SA encryption algorithm mismatched.

【プライオリティ】　LOG_INFO

【意味】　IPsec SAの暗号アルゴリズムが、受信したIPsec SAの暗号アルゴリズムと一致しなかったことを示します。IPsec SAのネゴシエーションに失敗した時にレスポンダによって出力されます。

isakmp: IPsec SA authentication algorithm mismatched.

【プライオリティ】　LOG_INFO

【意味】　IPsec SAの認証アルゴリズムが、受信したIPsec SAの認証アルゴリズムと一致しなかったことを示します。IPsec SAのネゴシエーションに失敗した時にレスポンダによって出力されます。

isakmp: IPsec SA pfs group mismatched.

【プライオリティ】　LOG_INFO

【意味】　IPsec SAのPFSグループが、受信したIPsec SAのPFSグループと一致しなかったことを示します。IPsec SAのネゴシエーションに失敗した時にレスポンダによって出力されます。

isakmp: give up phase2 negotiation.

【プライオリティ】　LOG_INFO

【意味】　IPsec　SAのネゴシエーションの再送回数が終了したことを示します。このメッセージは回線異常、相手装置の問題によりネゴシエーションパケットが受信できなかった場合や設定ミスによりパケットが破棄されたことにより、ネゴシエーションが失敗した時に出力されます。

protocol: weak key not usable for des-cbc encryption.

【プライオリティ】　LOG_INFO

【意味】　IPsec SAのdes-cbc暗号鍵にRFC2409のAppendix Aに記述されているweak keyを設定したことを示します。des-cbc暗号鍵にRFC2409のAppendix Aに記述されている鍵が設定され、IPsec SAの作成を行わなかった時に出力されます。

protocol: weak key not usable for 3des-cbc encryption.

【プライオリティ】　LOG_INFO

【意味】　IPsec SAの3des-cbc暗号鍵にRFC2409のAppendix Aに記述されているweak keyを設定したことを示します。3des-cbc暗号鍵設定時に暗号鍵を8バイトごとの3つの鍵に分割した際、3つの鍵のどれかにRFC2409のAppendix Aに記述されている鍵が設定され、IPsec SAの作成を行わなかった時に出力されます。

■ BGP4のメッセージ

(1)マーカフィールド異常

bgpd: <address> <direct> NOTIFICATION 1/1 (Message Header Error/ Connection Not Synchronized.) <detail>

【プライオリティ】　LOG_INFO

【意味】　不当なマーカフィールドを受信しました。

【パラメタの意味】　<address>　: 相手装置のIPアドレス

<direct>　："received"は相手側で異常を検出し、自側にその異常を通知したことを示します。
"sending"は自側で異常を検出し、相手側にその異常を通知したことを示します。

<detail>　：異常となった原因の詳細情報

(2)メッセージ長異常

bgpd: <address> <direct> NOTIFICATION 1/2 (Message Header Error/Bad Message Length.)<detail>

【プライオリティ】 LOG_INFO

【意味】 規定長範囲外のメッセージ長のメッセージを受信しました。

【パラメタの意味】 <address> ：相手装置のIPアドレス

<direct> ："received"は相手側で異常を検出し、自側にその異常を通知したことを示します。
"sending"は自側で異常を検出し、相手側にその異常を通知したことを示します。

<detail> ：異常となった原因の詳細情報

(3)メッセージタイプ異常

bgpd: <address> <direct> NOTIFICATION 1/3 (Message Header Error/Bad Message Type.)<detail>

【プライオリティ】 LOG_INFO

【意味】 サポート外のメッセージタイプを受信しました。

【パラメタの意味】 <address> ：相手装置のIPアドレス

<direct> ："received"は相手側で異常を検出し、自側にその異常を通知したことを示します。
"sending"は自側で異常を検出し、相手側にその異常を通知したことを示します。

<detail> ：異常となった原因の詳細情報

(4)バージョン異常

bgpd: <address> <direct> NOTIFICATION 2/1 (OPEN Message Error/ Unsupported Version Number.)<detail>

【プライオリティ】 LOG_INFO

【意味】 サポート外のBGPバージョンのメッセージを受信しました。

【パラメタの意味】 <address> ：相手装置のIPアドレス

<direct> ："received"は相手側で異常を検出し、自側にその異常を通知したことを示します。
"sending"は自側で異常を検出し、相手側にその異常を通知したことを示します。

<detail> ：異常となった原因の詳細情報

(5)AS 番号異常

bgpd: <address> <direct> NOTIFICATION 2/2 (OPEN Message Error/Bad Peer AS.) <detail>

【プライオリティ】 LOG_INFO

【意味】 設定外のAS番号または自側と同じAS番号を受信しました。

【パラメタの意味】 <address> ：相手装置のIPアドレス

<direct> ："received"は相手側で異常を検出し、自側にその異常を通知したことを示します。
"sending"は自側で異常を検出し、相手側にその異常を通知したことを示します。

<detail> ：異常となった原因の詳細情報

(6)BGP-ID異常

bgpd: <address> <direct> NOTIFICATION 2/3 (OPEN Message Error/Bad BGP Identifier.) <detail>

【プライオリティ】 LOG_INFO

【意味】 不当なBGP-IDを受信しました。

【パラメタの意味】 <address> ：相手装置のIPアドレス

<direct> ："received"は相手側で異常を検出し、自側にその異常を通知したことを示します。
"sending"は自側で異常を検出し、相手側にその異常を通知したことを示します。

<detail> ：異常となった原因の詳細情報

(7)サポート外オプション

bgpd: <address> <direct> NOTIFICATION 2/4 (OPEN Message Error/ Unsupported Optional Parameter.)<detail>

【プライオリティ】 LOG_INFO

【意味】 サポート外のオプションを受信しました。

【パラメタの意味】 <address> ：相手装置のIPアドレス

<direct> ："received"は相手側で異常を検出し、自側にその異常を通知したことを示します。
"sending"は自側で異常を検出し、相手側にその異常を通知したことを示します。

<detail> ：異常となった原因の詳細情報

(8)認証異常

bgpd: <address> <direct> NOTIFICATION 2/5 (OPEN Message Error/ Authentication Failure.)<detail>

【プライオリティ】 LOG_INFO

【意味】 認証に失敗しました。

【パラメタの意味】 <address> ：相手装置のIPアドレス

<direct> ："received"は相手側で異常を検出し、自側にその異常を通知したことを示します。
"sending"は自側で異常を検出し、相手側にその異常を通知したことを示します。

<detail> ：異常となった原因の詳細情報

(9)HOLD時間受入れ不可

bgpd: <address> <direct> NOTIFICATION 2/6 (OPEN Message Error/ Unacceptable Hold Time.)<detail>

【プライオリティ】 LOG_INFO

【意味】 受入れ不可なHOLD時間を受信しました。

【パラメタの意味】 <address> ：相手装置のIPアドレス

<direct> ："received"は相手側で異常を検出し、自側にその異常を通知したことを示します。
"sending"は自側で異常を検出し、相手側にその異常を通知したことを示します。

<detail> ：異常となった原因の詳細情報

(10)ケイパビリティ受入れ不可

bgpd: <address> <direct> NOTIFICATION 2/7 (OPEN Message Error/ Unsupported Capability.)<detail>

【プライオリティ】 LOG_INFO

【意味】 受入れ不可なケイパビリティを受信しました。

【パラメタの意味】 <address> ：相手装置のIPアドレス

<direct> ："received"は相手側で異常を検出し、自側にその異常を通知したことを示します。
"sending"は自側で異常を検出し、相手側にその異常を通知したことを示します。

<detail> ：異常となった原因の詳細情報

(11)属性異常

bgpd: <address> <direct> NOTIFICATION 3/1 (UPDATE Message Error/ Malformed Attribute List.)<detail>

【プライオリティ】 LOG_INFO

【意味】 受信した属性の処理中に異常が発生しました。

【パラメタの意味】 <address> ：相手装置のIPアドレス

<direct> ："received"は相手側で異常を検出し、自側にその異常を通知したことを示します。
"sending"は自側で異常を検出し、相手側にその異常を通知したことを示します。

<detail> ：異常となった原因の詳細情報

(12)サポート外既知属性

bgpd: <address> <direct> NOTIFICATION 3/2 (UPDATE Message Error/ Unrecognized Well-known Attribute.)<detail>

【プライオリティ】 LOG_INFO

【意味】 サポート外の属性を既知属性として受信しました。

【パラメタの意味】 <address> ：相手装置のIPアドレス

<direct> ："received"は相手側で異常を検出し、自側にその異常を通知したことを示します。
"sending"は自側で異常を検出し、相手側にその異常を通知したことを示します。

<detail> ：異常となった原因の詳細情報

(13)既知属性の消失

bgpd: <address> <direct> NOTIFICATION 3/3 (UPDATE Message Error/Missing Well-known Attribute.)<detail>

【プライオリティ】 LOG_INFO

【意味】 UPDATEメッセージを受信しましたが、必要な属性がすべてそろいませんでした。

【パラメタの意味】 <address> ：相手装置のIPアドレス

<direct> ："received"は相手側で異常を検出し、自側にその異常を通知したことを示します。
"sending"は自側で異常を検出し、相手側にその異常を通知したことを示します。

<detail> ：異常となった原因の詳細情報

(14)属性フラグ異常

bgpd: <address> <direct> NOTIFICATION 3/4 (UPDATE Message Error/Missing Well-known Attribute.)<detail>

【プライオリティ】 LOG_INFO

【意味】 無効な属性フラグを受信しました。

【パラメタの意味】 <address> ：相手装置のIPアドレス

<direct> ："received"は相手側で異常を検出し、自側にその異常を通知したことを示します。
"sending"は自側で異常を検出し、相手側にその異常を通知したことを示します。

<detail> ：異常となった原因の詳細情報

(15)属性長異常

bgpd: <address> <direct> NOTIFICATION 3/5 (UPDATE Message Error/Attribute Length Error.)<detail>

【プライオリティ】 LOG_INFO

【意味】 不当な値の属性長を受信しました。

【パラメタの意味】 <address> ：相手装置のIPアドレス

<direct> ："received"は相手側で異常を検出し、自側にその異常を通知したことを示します。
"sending"は自側で異常を検出し、相手側にその異常を通知したことを示します。

<detail> ：異常となった原因の詳細情報

(16)ORIGIN属性異常

bgpd: <address> <direct> NOTIFICATION 3/6 (UPDATE Message Error/Invalid ORIGIN Attribute.)<detail>

【プライオリティ】 LOG_INFO

【意味】 不当な値のORIGIN属性を受信しました。

【パラメタの意味】 <address> ：相手装置のIPアドレス

<direct> ："received"は相手側で異常を検出し、自側にその異常を通知したことを示します。
"sending"は自側で異常を検出し、相手側にその異常を通知したことを示します。

<detail> ：異常となった原因の詳細情報

(17)メッセージループ

bgpd: <address> received NOTIFICATION 3/7 (UPDATE Message Error/AS Routing Loop.) <detail>

【プライオリティ】 LOG_INFO

【意味】 相手側で経路情報を通知するメッセージが AS 間でループしていることを検出し、自側にその異常を通知したことを示します。

【パラメタの意味】 <address> ：相手装置のIPアドレス

<detail> ：異常となった原因の詳細情報

(18)NEXT-HOP 属性異常

bgpd: <address> <direct> NOTIFICATION 3/8 (UPDATE Message Error/Invalid NEXT_HOP Attribute.) <detail>

【プライオリティ】 LOG_INFO

【意味】 不当な値のNEXT-HOP 属性を受信しました。

【パラメタの意味】 <address> ：相手装置のIPアドレス

<direct> ："received"は相手側で異常を検出し、自側にその異常を通知したことを示します。
"sending"は自側で異常を検出し、相手側にその異常を通知したことを示します。

<detail> ：異常となった原因の詳細情報

(19)オプション属性異常

bgpd: <address> received NOTIFICATION 3/9 (UPDATE Message Error/Optional Attribute Error.) <detail>

【プライオリティ】 LOG_INFO

【意味】 相手側で不当なオプション属性を受信し、自側にその異常を通知したことを示します。

【パラメタの意味】 <address> ：相手装置のIPアドレス

<detail> ：異常となった原因の詳細情報

(20)不当経路情報

bgpd: <address> <direct> NOTIFICATION 3/10 (UPDATE Message Error/Invalid Network Field.) <detail>

【プライオリティ】 LOG_INFO

【意味】 不当な値の経路情報を受信しました。

【パラメタの意味】 <address> ：相手装置のIPアドレス

<direct> ："received"は相手側で異常を検出し、自側にその異常を通知したことを示します。
"sending"は自側で異常を検出し、相手側にその異常を通知したことを示します。

<detail> ：異常となった原因の詳細情報

(21)不当なAS_PATH

bgpd: <address> <direct> NOTIFICATION 3/11 (UPDATE Message Error/Malformed AS_PATH.) <detail>

【プライオリティ】 LOG_INFO

【意味】 不当な値のAS_PATHを受信しました。

【パラメタの意味】 <address> ：相手装置のIPアドレス

<direct> ："received"は相手側で異常を検出し、自側にその異常を通知したことを示します。
"sending"は自側で異常を検出し、相手側にその異常を通知したことを示します。

<detail> ：異常となった原因の詳細情報

(22)HOLD時間満了

bgpd: <address> <direct> NOTIFICATION 4/0 (Hold Timer Expired) <detail>

【プライオリティ】 LOG_INFO

【意味】 相手側との無通信状態がネゴシエージョンした結果のHOLD時間を経過しました。

【パラメタの意味】 <address> ：相手装置のIPアドレス

<direct> ："received"は相手側で異常を検出し、自側にその異常を通知したことを示します。
"sending"は自側で異常を検出し、相手側にその異常を通知したことを示します。

<detail> ：異常となった原因の詳細情報

(23)内部状態矛盾

bgpd: <address> <direct> NOTIFICATION 5/0 (Finite State Machine Error) <detail>

【プライオリティ】 LOG_INFO

【意味】 bgpd内部の状態に矛盾が発生しました。

【パラメタの意味】 <address> ：相手装置のIPアドレス

<direct> ："received"は相手側で異常を検出し、自側にその異常を通知したことを示します。
"sending"は自側で異常を検出し、相手側にその異常を通知したことを示します。

<detail> ：異常となった原因の詳細情報

(24)BGPセッション終了

bgpd: <address> <direct> NOTIFICATION 6/0 (Cease) <detail>

【プライオリティ】 LOG_INFO

【意味】 BGPのセッションを終了しました。なお、自装置でenableコマンドの実行またはWWWブラウザの設定画面で［設定反映］ボタンをクリックした場合も記録されます。

【パラメタの意味】 <address> ：相手装置のIPアドレス

<direct> ："received"は相手側でBGPのセッションを終了したことを示します。
"sending"は自側でBGPのセッションを終了したことを示します。

<detail> ：異常となった原因の詳細情報

(25)設定外装置からの接続受信

bgpd: <address> BGP connection IP address is not configured

【プライオリティ】 LOG_INFO

【意味】 設定されていない装置から接続要求を受信しました。

【パラメタの意味】 <address> ：接続要求を行った装置のIPアドレス

■ VRRPのメッセージ

1）VRRPグループ開始

zebra: vrrp group is started. <interface> vrid<vrid>

【プライオリティ】　LOG_INFO

【意味】　<interface>と<vrid>が示すVRRPグループが動作を開始しました。

【パラメタの意味】　<interface>：インタフェース名

<vrid>　：自装置に設定されたVRID

2）マスタルータ／バックアップルータ／イニシャル切り替わり

zebra: vrrp state is changed into the <state> state. <interface> vrid<vrid>

【プライオリティ】　LOG_INFO

【意味】　<interface>と<vrid>が示すVRRP状態が<state>で示された状態に変更されました。

【パラメタの意味】　<interface>：インタフェース名

<vrid>　：自装置に設定されたVRID

<state>　：変更後の状態

master　：マスタルータ

backup　：バックアップルータ

Initialize　：イニシャル

3）インタフェースアップ／ダウントリガイベント発生

zebra: vrrp interface <state> trigger event occurred. <interface> vrid<vrid> No.<trigger_no> <target_if>

【プライオリティ】　LOG_INFO

【意味】　<interface>、<vrid> および <trigger_no> が示す番号で定義されたインタフェーストリガイベントが発生し、イベントの状態が<state>になりました。

【パラメタの意味】

<interface>　：インタフェース名

<vrid>　：自装置に設定されたVRID

<trigger_no>　：トリガイベント定義番号

<target_if>　：トリガイベントの対象となるインタフェース名

<state>　：変更後の状態

up　：トリガイベントに設定されたインタフェースがアップし、イベントが不適用になりました。

down　：トリガイベントに設定されたインタフェースがダウンし、イベントが適用されました。

4）ルートアップ／ダウントリガイベント発生

```
zebra: vrrp <state> trigger event occurred. <interface> vrid<vrid>
No.<trigger_no> route <target_route> <target_if>
```

【プライオリティ】　LOG_INFO

【意味】　<an_no>と<vrid>と<trigger_no>が示す番号で定義されたルートトリガイベントが発生し、イベントの状態が<state>になりました。

【パラメタの意味】

<state>　：変更後の状態

- up　：トリガイベントに設定された経路が復旧し、イベントが不適用になりました。
- down　：トリガイベントに設定された経路が損失し、イベントが適用されました。

<interface>　：インタフェース名

<vrid>　：自装置に設定されたVRID

<trigger_no>　：トリガイベント定義番号

<target_route>　：トリガイベントの対象となる経路

<target_if>　：トリガイベントの対象となる経路のパケット送出インタフェース名

5）ノードアップ／ダウントリガイベント発生

```
zebra: vrrp node <state> trigger event occurred. <interface> vrid<vrid>
No.<trigger_no> <target_node>
```

【プライオリティ】　LOG_INFO

【意味】　<interface>と<vrid>と<trigger_no>が示す番号で定義されたノードトリガイベントが発生し、イベントの状態が<state>になりました。

【パラメタの意味】

<interface>　：インタフェース名

<vrid>　：自装置に設定されたVRID

<trigger_no>　：トリガイベント定義番号

<target_node>　：トリガイベントの対象となるノードのIPv4アドレス

<state>　：変更後の状態

- up　：トリガイベントに設定されたノードがアップし、イベントが不適用になりました。
- down　：トリガイベントに設定されたノードがダウンし、イベントが適用されました。

6）マスタルータダウン検出

zebra: vrrp master router down detection. <interface> vrid<vrid> [<address>] #<code>

【プライオリティ】　LOG_INFO

【意味】　<interface> と <vrid> が示す VRRP グループのマスタルータのダウンを検出しました。

【パラメタの意味】　<interface> : インタフェース名

<vrid> : ダウンしたマスタルータの VRID

<address> : 異常を検出したマスタルータの実 IP アドレス（XXX.XXX.XXX.XXX）

<code> : 検出した異常の種類

01 : マスタルータ放棄（優先度 0 の VRRP-AD 受信）

02 : VRRP-AD 受信タイムアウト

7）受信 VRRP-AD TTL 異常

zebra: vrrp packet include invalid TTL. from <interface> [<address>]

【プライオリティ】　LOG_INFO

【意味】　<interface> が示すインタフェースに TTL が 255 でない VRRP パケットを受信しました。

【パラメタの意味】　<interface> : インタフェース名

<address> : 受信した VRRP パケットの送信元 IP アドレス（XXX.XXX.XXX.XXX）

8）受信 VRRP-AD 認証タイプ異常

zebra: vrrp packet authentication method mismatched. from <interface> [<address>]

【プライオリティ】　LOG_INFO

【意味】　<interface> が示すインタフェースに認証方法の一致しない VRRP パケットを受信しました。

【パラメタの意味】　<interface> : インタフェース名

<address> : 受信した VRRP パケットの送信元 IP アドレス（XXX.XXX.XXX.XXX）

9）受信VRRP-AD認証パスワード異常

zebra: vrrp packet authentication data check failed. from <interface> [<address>]

【プライオリティ】　LOG_INFO

【意味】　<interface>が示すインタフェースに認証パスワードの一致しないVRRPパケットを受信しました。

【パラメタの意味】　<interface>：インタフェース名

<address>：受信したVRRPパケットの送信元IPアドレス（XXX.XXX.XXX.XXX）

10）VRID重複設定

zebra: vrrp <interface> vrid<vrid> is not initialized. this vrid is already used

【プライオリティ】　LOG_INFO

【意味】　指定されたVRIDがすでに装置内で有効となっているため、このVRRPグループが利用できないことを示します。

【パラメタの意味】　<interface>：インタフェース名

<vrid>：無効となったVRID

11）仮想ルータのIPアドレスインタフェースサブネット外設定

zebra: vrrp virtual router IP address out of interface subnet. <interface> vrid<vrid> <address>

【プライオリティ】　LOG_INFO

【意味】　このVRRPグループの仮想ルータのIPアドレスが、インタフェースのサブネット外であることを示します。

【パラメタの意味】　<interface>：インタフェース名

<vrid>：無効となったVRID

<address>：サブネット外である仮想ルータのIPアドレス

12）仮想ルータのIPアドレスインタフェース同一アドレス設定

zebra: vrrp same invalid virtual router IP address as real IP address was set as backup. <interface> vrid<vrid> <address>

【プライオリティ】　LOG_INFO

【意味】　バックアップ設定であるVRRPグループの仮想ルータのIPアドレスが、インタフェースの実IPアドレスと同一であるため、このVRRPグループが利用できないことを示します。

【パラメタの意味】　<interface> :インタフェース名

<vrid> :無効となったVRID

<address> :実インタフェースと同一である仮想ルータのIPアドレス

13）VRRP使用不可インタフェース

zebra: vrrp lan<no> is not attached: cannot use vrrp on this lan

【プライオリティ】　LOG_INFO

【意味】　このLANインタフェースでは、VRRPが利用できないことを示します。

【パラメタの意味】　<no> :lan定義番号

■ SNMPのメッセージ

1）不当なSNMPエージェントアドレスの設定

snmpd: illegal SNMP agent address

【プライオリティ】　LOG_INFO

【意味】　自装置の IP アドレスとして割り当てられていない IP アドレスが、SNMPエージェントアドレスとして定義されています。そのため、SNMPエージェントおよびTRAP機能では、自装置のIPアドレスを使用します。SNMP マネージャとは正常に通信できない場合があります。

■ その他のメッセージ

(1)課金情報のクリア

<name>: ISDN(<type>) totalcharge=<value>yen totaltime=<time>

【プライオリティ】 LOG_INFO

【意味】 課金情報をクリアし、統計情報、課金情報を通知したことを示します。

【パラメタの意味】

<name> : 課金情報をクリアしたプログラム

- scheduled : スケジュール機能によるクリア
- httpd : ブラウザによるクリア
- telnetd : telnet コマンドによるクリア

<type> : データまたはアナログの種別を示します。

- data : データポート
- analog : アナログポート
- multita : マルチTA

<value> : 総通話料金（円単位）

<time> : 総接続時間（dddd.hh:mm:ss の形式）

(2)システムリセットエラー

<name>: ERROR: system reset busy.

【プライオリティ】 LOG_ERROR

【意味】 リセット処理を実施しようとしたが、ファーム更新中、構成定義の保存中、他スレッドでリセット処理中などにより、リセット処理ができなかったことを示します。

【パラメタの意味】

<name> : リセットを実施したプログラム

- scheduled : スケジュールによる電話番号変更後のリセット
- httpd : ブラウザによるリセット
- telnetd : telnetd コマンドによるリセット

(3)動的定義反映実行

enabled: system configuration restarted

【プライオリティ】 LOG_INFO

【意味】 動的定義反映が実行されたことを示します。

(4)IPアドレス重複

enabled: lan <no> has same network/address as lan <other_no>

【プライオリティ】　LOG_INFO

【意味】　LANのIPアドレス、セカンダリIPアドレスで設定したネットワークアドレスが重複していることを示します。

【パラメタの意味】　<no>　: lan定義番号

<other_no>: lan定義番号

enabled: remote <no> has same remote address as remote <other_no>

【プライオリティ】　LOG_INFO

【意味】　<no>と<other_no>の相手情報のリモートIPアドレスが重複していることを示します。

【パラメタの意味】　<no>　: 相手定義番号

<other_no>: 相手定義番号

(5)重複メッセージの省略

same message repeated <num> times

【プライオリティ】　直前のメッセージと同じ

【意味】　同じメッセージが繰り返されたので表示を省略したことを示します。

【パラメタの意味】　<num>　: 繰り返された回数

【注意事項】　このメッセージは、重複したメッセージの繰り返しが終わり、異なるメッセージが出力された時に、その異なるメッセージの直前に出されます。

文字入力フィールドに入力できる文字一覧

文字入力する場合に、使用できる文字の一覧を以下に示します。

	!		#	$			‘	(	)	*	+	,	-	.	/
0	1	2	3	4	5	6	7	8	9	:	;		=		?
@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	Q	R	S	T	U	V	W	X	Y	Z	[	¥	]	^	_
‘	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	

⚠注意

文字入力フィールドでは半角文字だけを使用してください。ただし、空白文字、「”」、「<」、「>」、「&」、「%」は入力しないでください。入力すると、ブラウザでの設定が不可能となります。ただし、一部の設定では全角文字の設定ができます。

☛ 参照 Eメールエージェントのメール転送条件の設定（P.541）

用語集

2分岐モジュラコネクタ	1本の回線を2つに分岐させるためのコネクタです。
AS（Autonomous System）	ポリシーに従って運用するネットワークのことで、自律システムとも言います。
AS番号	プロバイダに割り当てられた固有の番号です。
BGP4（Border Gateway Protocol 4）	インターネットでドメイン（プロバイダ）間の経路制御に用いられている業界標準プロトコルです。IP-VPNサービスで採用されています。
DA64、DA128	ディジタルアクセス64、ディジタルアクセス128
DHCP（Dynamic Host Configuration Protocol）	ネットワーク上のホストに対して、IPアドレスやネットマスクなどのネットワーク構成情報を動的に割り当てるための機能です。本装置は、DHCPサーバ機能をサポートしており、DHCPクライアント機能を持っているパソコンに対して、自動的にIPアドレスなどの情報を割り当てることができます。 →DHCPサーバ
DHCPサーバ	DHCPを用いて、IPアドレスなどの設定を配布・管理するシステムです。
DNS（Domain Name System）	IPアドレスとドメイン名を対応させるシステムです。 →ドメイン名、DNSサーバ
DNSサーバ	IPアドレスとドメイン名の対応を管理するコンピュータ、またはソフトです。
DSU（Digital Service Unit）	NTTの電話回線とディジタル通信機器の間につなぎます。本装置やISDN機器などのディジタル通信機器が送受信するディジタル信号と、ISDN回線で使用されているディジタル信号とを変換します。ディジタルサービス装置とも呼ばれます。
HSD線	→ハイ・スーパー・ディジタル線
i・ナンバー	INSネット64の付加サービスです。このサービスをご契約になると契約者回線番号のほかに2つの電話番号を持つことができます。動作モードを設定することによって、接続している端末を鳴り分けさせることができます。
IKE（Internet Key Exchange）	RFC2409で規定されており、IPsec通信で採用されている業界標準の鍵交換プロトコルです。以前はISAKMP（Internet Security Association and key Management protocol）／Oakleyと呼ばれていました。IPsec通信で使用される鍵情報のほかに暗号アルゴリズム、認証アルゴリズムなどSAのパラメタの交換や設定も行います。

INSネット64	NTTが提供するISDN通信網サービスです。回線1本につき2つのBチャネル（64Kbps）と、1つのDチャネル（16Kbps）を備えています。
IP（Internet Protocol）	通信プロトコルのひとつです。インターネットで標準的に使われています。
IPsec	TCP/IPによる通信のセキュリティを強化するための技術の総称であり、IETF（Internet Engineering Task Force）で標準化作業が進められているインターネット標準プロトコルです。データをカプセリングしてトンネルする方法であるESP、ユーザ認証用のデータをIPパケットに組み込むAH（Authentication Header）などがあります。本装置では、認証付きESPによるIPsec方式が利用できます。
IP-VPN	通信事業者の閉域IPネットワーク網を通信経路として用いる仮想的な私設網。IP-VPNでは、複数のプロバイダのネットワークを経由する必要があるインターネットとは異なり、専用線接続のようなセキュリティ、回線品質が確保されたデータ通信が可能。当社のFENICSビジネスIPネットワークサービスをはじめ、ULTINA IP-VPN（ソフトバンクテレコム）、Arcstar IP-VPN（NTTコミュニケーションズ）、KDDI IP-VPN（KDDI）などで提供されています。
IPv6（Internet Protocol Version 6）	通信プロトコルのひとつです。現在インターネットで主に使われているIP（IPv4）のアドレス枯渇問題を解決する次世代のインターネットプロトコルとして利用されはじめています。
IPv6アドレス	IPv6による通信を行う際、ネットワーク上の機器を識別するためのものです。通常は「fec0::1000:200:eff:feaa:50c」のように、128bitのIPv6アドレスを16bitずつにコロンで区切って16進数で表します。
IPアドレス	IPによる通信（IPネットワーク）を行う際、ネットワーク上の機器を識別するためのものです。通常は「192.168.1.1」のように、ピリオドをはさんだ4つの数字（0～255）で表します。
IPアドレスの静的割り当て	ネットワーク上のホストそれぞれに固有のIPアドレスを割り当てることを言います。
IPアドレスの動的割り当て	ネットワーク上のホストに、必要に応じてIPアドレスを割り当てることを言います。
ISDN（Integrated Services Digital Network）	ディジタル通信網の国際標準規格です。

LAN（Local Area Network）	構内回線を使用した狭い地域でのコンピュータ・ネットワークです。局部地域通信網とも呼ばれます。企業内では社内LANと呼ばれます。
LANカード	EthernetポートをもたないパソコンをLANにつなぐために使います。
MP（Multilink PPP）	INSネット64で提供しているBチャネル（64Kbps）2本を論理的に束ねることによって、最大128Kbpsでの通信を可能にします。
NAT（Network Address Translation）	アドレス変換機能とも言います。NATは、プライベートアドレスとグローバルアドレスを変換する機能です。本装置では、NAT機能を拡張したマルチNATもサポートしています。
ping	IPによる通信（IPネットワーク）で、疎通確認をするためのコマンドです。
WAN（Wide Area Network）	一般の電話回線、ISDN回線、専用線などを使い、遠隔地のLANどうしを接続するネットワークです。広域情報通信網とも呼ばれます。
WWWブラウザ	HTTP（HyperText Transfer Protocol）を用いて取得した文字、画像などを表示するためのソフトです。主なものとしてMicrosoft® Internet Explorerなどがあります。
アドレスマスク	IPアドレスを持ったパソコン、ホスト、サーバなどのネットワークに接続されている装置のグループを表現するときに使用します。アドレスマスクは、たとえば、あるネットワーク内の端末全部をまとめて表現するときなどに便利な書き方です。このアドレスマスクには、ネットワーク全体を示すためのネットマスクと、ローカルなネットワーク（サブネット）を示すサブネットマスクなどがあります。また、ネットワークの形状とは無関係にIPアドレスn番からn+m番までの端末を指す場合にも使われます（ここでnとmは2のべき乗の数になります）。 これらマスク値には“24”などと書きます。これは32bitのIPアドレスの最初の24bit分がマスク値であることを示すものです。また“255.255.255.0”などのようにドット表記で表現する場合もあります。 たとえば、192.168.2.0のネットワーク番号はClass Cですからネットマスク値は24（255.255.255.0）です。 ここでサブネットマスクとして26（255.255.255.192）を指定すれば、 （1）192.168.2.0～192.168.2.63 （2）192.168.2.64～192.168.2.127 （3）192.168.2.128～192.168.2.191

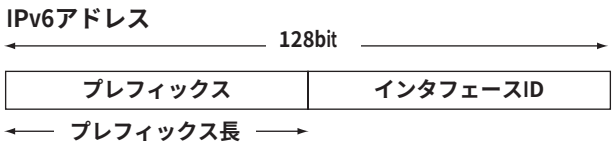
	（4）192.168.2.192 ～ 192.168.2.255 の4つサブネットワークが作られます。 さらにここで（1）のサブネット内の端末のうち、192.168.2.192 ～ 192.168.2.207 のIPアドレスを持った16台の端末グループを表現する場合には、アドレスマスク192.168.2.192/28（255.255.255.240）と指定します。 なお、ネットマスクとサブネットマスクは明確な区別なしに使われることも多いようです。本マニュアルではネットマスクとサブネットマスクの両方の意味も含めてネットマスクと呼びます。
アナログ回線	NTTの従来の回線網です。NTTでは加入者回線と呼びます。
インタフェースID	IPv6アドレスのホストを識別する部分です。128bitのIPv6アドレスのうち、プレフィックスを除いた部分がインタフェースIDとなります。 → プレフィックス
課金単位時間	無通信監視タイマと連動して単位時間内は回線を切断しないように動作させ、通信料金を節約することができます。
カスケード接続	ハブどうしをつなぐことを言います。
加入者回線	→アナログ回線
疑似キャッチホン	NTTとの契約なしで、キャッチホンと同様の使いかたができます。
グローバルアドレス	インターネット上のホストを識別するためにInterNICなどのアドレス管理機構から割り当てられる、唯一無二のIPアドレスです。
グローバル着信機能	NTTのダイヤルインサービスを利用している場合でも、ダイヤルイン番号による呼び分けを行わないようにする機能です。
サブアドレス	同一のISDN回線上につないだ複数のISDN機器を呼び分けるときに使用します。通常の電話番号の末尾に設定しておきます （例：03 － 1111 － 1111 ＊ 001）。
サブネットマスク	→ネットマスク
三者通話	通話中に電話がかかってきた場合、三者で通話できるサービスです。
終端抵抗	ISDN機器をつなぐ配線を流れるディジタル信号を安定させるためのものです。
詳細設定メニュー	［詳細設定］アイコンをクリックすると、このメニューが表示されます。 このメニューからルータ設定とアナログ設定ができます。

専用線接続	ハイ・スーパー・ディジタル線（HSD）やディジタルアクセス64／128（DA64／128）などのディジタル専用線を使ってプロバイダと常時接続します。
操作メニュー	［操作］アイコンをクリックすると、このメニューが表示されます。
ダイヤルインサービス	NTTが提供するサービスです。会社などの構内にある電話を、外部から直接呼び出せます。
ダイヤルイン番号	NTTのダイヤルインサービスで、電話機それぞれに割り当てられる番号です。
ダイヤルトーン	電話機の受話器を上げたときに聞こえる、「ツー」という音のことです。
ターミナルアダプタ	モデムやアナログ電話機、FAXなどのアナログ機器をISDN回線につなぐための装置です。
ダブルフック	通話中に電話機のフックを2回押すことです。
端末型ダイヤルアップ接続	パソコン1台だけでプロバイダに接続するためのサービスです。インターネットを利用するたびにプロバイダにダイヤルします。接続するたびにIPアドレスが1個割り当てられます。
着信転送	かかってきた電話を受けずに、ほかの番号に転送します。
通信中転送	通話中の電話を、別の番号に転送します。
ディジタル電話機	TA（ターミナルアダプタ）などを介さず、ISDN回線に直接つなぐことができる電話機です。
テレホーダイ	NTTが提供するサービスです。午後11時から午前8時までの深夜・早朝時間帯に、あらかじめ指定した2つの電話番号に対してかけ放題になります。利用にあたっては、NTTとの契約が必要です。
転送元／転送トーキ	かかってきた電話を、別の電話に転送する際、相手にメッセージを流すかどうかを指定できます。この場合、NTTとの契約が必要です。「アナログ共通情報」ページの「着信転送」で「する」を選択します。ここで転送トーキ「あり」を選択すると、“ただいま電話を転送しますので、しばらくお待ちください。”などのメッセージが流れます。転送元トーキ「あり」を選択すると、“電話が転送されます。”などのメッセージが流れます。
電池ボックス	バックアップ用の電池を収納します。
ドメイン名	インターネットに接続されているコンピュータを識別するための名前です。たとえば「xxx@ △△△.ne.jp」という電子メールアドレスを持っている場合なら、「△△△.ne.jp」がドメイン名になります。
トーン／パルス切替スイッチ	ダイヤルする際に発信する信号の種類を切り替えるためのスイッチです。通常電話機の底面や背面にあります。

鳴り分け番号	ｉ・ナンバーサービスを契約すると2つまで電話番号が追加できます。契約者回線番号が鳴り分け番号1となり、追加番号がそれぞれ鳴り分け番号2、3となります。
ナンバー・ディスプレイ	ナンバー・ディスプレイ対応電話機を使用している場合、「使用する」を選択すると、電話機に相手番号を表示させることができます。通常の電話機をご利用の場合は「使用しない」を選択してください。相手がISDN回線の場合は、NTTのINSナンバー・ディスプレイサービスを契約していなくても、相手番号が通知されます。相手がアナログ電話網の場合は、INSナンバー・ディスプレイサービスを契約しないと相手番号が通知されません。
ネットマスク	IPアドレスからネットワーク部とホスト部を分離するための区切りを表します。たとえば、IPアドレスが「192.168.1.1」、ネットマスクが「255.255.255.0」の場合、ネットワーク部は「192.168.1」、ホスト部は「1」になります。
ネットワーク型ダイヤルアップ接続	複数のパソコンからプロバイダに接続するためのサービスです。インターネットを利用するたびにプロバイダにダイヤルします。契約した台数分のIPアドレスが割り当てられます。LAN型ダイヤルアップ接続とも呼びます。
ネットワーク部	→ネットマスク
ハイ・スーパー・ディジタル線（HSD）	NTTが提供する高速ディジタル通信サービスです。特定の地点を専用線で接続します。料金は定額制です。
ハブ	3台以上のパソコンやワークステーションを10BASE-TケーブルでつないでLANを構築するときに使う装置です。
バックアップ用電池	本装置で停電時のバックアップ用に使用します。単3アルカリ乾電池8本が必要です。
発信者番号通知	電話をかけてきた相手の番号を通知する機能です。
表示メニュー	[表示] アイコンをクリックすると、このメニューが表示されます。
ファームウェア	本装置を操作するための内蔵ソフトウェアです。 →メンテナンスメニュー
フッキング	通話中に電話機のフックを1回押すことです。通話中の電話を保留にするときに使います。
フレックスホン	NTTが提供するサービスです。コールウェイティング、三者通話、通信中転送、着信転送の4種類があります。
フレッツ・ISDN	NTTが提供するダイヤルアップ接続方式のサービスです。定額料金なので常時接続に近い形でインターネットができます。

プレフィックス（prefix）

IPv6アドレスのネットワークを識別する部分です。128bitのIPv6アドレスのうち、プレフィックス長で指定される上位部分がプレフィックスとなります。



ホスト部

→ネットマスク

マルチダイヤル機能

ダイヤルしたアクセスポイントにつながらないとき、登録しておいた別のアクセスポイントに自動的にダイヤルする機能です。

→「同一プロバイダのアクセスポイントを複数指定（マルチダイヤル）」（P.74）

無通信監視タイマ

プロバイダとの通信が一定時間なかったとき、自動的に回線を切断する機能です。

メンテナンスメニュー

［メンテナンス］アイコンをクリックすると、このメニューが表示されます。

モジュラコネクタ

電話回線の屋内配線と電話機をつなぐための機具（大きさ約3×7cm）。取り付け、取り外しには電気通信工事担任者資格が必要です。現在ではモジュラジャックの使用が主流になっています。

モジュラジャック

一般家屋の電話線用などで使用する、壁面に取り付けられたモジュラケーブルの差込口です。

Q&A

DSU、アナログポート関連

Q1. U点インタフェースとは何ですか？

A. **屋内に配線されたケーブルを挿入するためのインタフェースです。**

ISDN網は、以下のような経路をたどります。この屋内配線で設置された口から伸びるケーブルをDSUが受けるインタフェースのことをU点インタフェースと言います。

NTTの交換機－電線－屋内配線－［DSU－ISDN機器］※

※［ ］内は利用者施設です。

Q2. DSUを無効にして、既設のDSUに接続することはできますか？

A. **できます。**

Q3. TAやG4FAXなど、ほかのISDN機器が接続できますか？

A. **できます。**

Q4. DSU折り返し機能はありますか？

A. **あります。**

ISDN回線を新規に申し込む場合には、『（DSU折り返し）機能あり』でお答えください。

Q5. 本装置を設定する前に、アナログポートにつないだ電話は使えますか？

A. **ご利用できます。**

ただし、設定するまでは『グローバル着信』と『電話（モデム）』しか利用できません。ダイヤルインサービスやFAXをご利用する場合は、利用形態に合わせた設定をお早めに行ってください。

Q6. アナログポートごとに電話番号を割り当てられますか？

A. **ダイヤルイン契約、または ｉ・ナンバー契約をしていただくか、サブアドレスを設定することで割り当てられます。****(P.396)**

Q7. 今まで使っていた番号をそのまま使うことはできますか？

A. **可能です。**

アナログ回線からISDN回線への『同番移行』が可能な地域であれば、今お使いの電話番号をそのまま利用できます。

Q8. アナログポートごとにダイヤルイン設定は可能ですか？

A. **設定できます。****(P.397)**

Q9. ダイヤルインサービスを使わずに、アナログポートに優先順位をつけられますか？

A. **つけられます。****(P.360)**

Q10. フレックスホンに対応していますか？

A. **対応しています。****(P.376)**

Q11. MP機能を使っているときに電話がかかってきたらどうなりますか？

A. **電話も受けることができます。**

アナログ使用時縮退機能によって、電話用に2Bのうち1Bを解放します。ただし、アナログ使用時縮退機能を使わない設定になっているか接続先が別々の場合、またはISDN回線契約上『通信中着信通知サービス』のご契約をされていない場合、回線は自動的に縮退されません。

Q12. 停電時でも電話が使えますか？

A. **以下のようになります。**

1. ISDN S／Tポートに接続されたディジタル電話機は乾電池が装着されているときだけご使用になれます。
2. TEL1 ポートに接続された電話機は、乾電池が装着されているときだけご使用になれます。

10BASE-Tハブについて

Q13. 5台以上のパソコンをハブポートにつなげられますか？

A. ハブを増設することによりつなげられます。

ネットワーク構成について

Q14.『端末型接続』と『ネットワーク型接続』にはどんな違いがありますか？

A. IPアドレスの割り当てかたに違いがあります。

［端末型接続契約］

- 「TA＋パソコン1台」、または「モデム＋パソコン1台」で接続する契約です。
- 端末型ダイヤルアップ契約という場合もあります。
- プロバイダのアクセスポイントに接続するごとにIPアドレスが動的に割り当てられるため、事前にIPアドレスをパソコンに設定する必要がありません（固定にできません）。

［ネットワーク型接続契約］

- LANを単位とした接続をする契約です。
- LAN型接続契約などという場合もあります。
- 事前にIPアドレスを各パソコンに設定しておく必要がありません。

補足 本装置を利用する場合、パソコン1台しか接続できない端末型接続契約であっても、NAT機能を用いることで複数のパソコンからインターネットに接続することができます（接続先のプロバイダがNAT機能の使用を禁止しない限り可能）。

Q15. 本装置にISDN回線を介してTA＋パソコンから接続できますか？

A. できます。（P.497）

Q16. フレッツ・ISDNでも利用できますか？

A. 利用できます。

Q17. 本装置どうしで接続できますか？

A. 本装置どうしの（ネットワーク型）接続は可能です。（P.115）

ただし、2台の本装置それぞれを「かんたん設定」で設定しただけではつながりません。受信側の本装置に、以下のどちらかを設定してください。

- 方法1. 認証プロトコルを使用しない。
- 方法2. 認証IDとパスワードを設定する。

Q18. PHSからの着信はできますか？

A. できます。（P.497）

Q19. 一方をプロバイダ、一方を会社のルータに（同時に）つなぐことはできますか？

A. できます。（P.165）

Q20. 複数のプロバイダを利用できますか？

A. マルチルーティング機能を使えばできます。（P.462）

サポート機能について

Q21. 複数台のパソコンから同時にインターネットにアクセスできますか？

A. できます。アクセス可能な台数は利用形態により異なります。

接続形態	NAT使用形態	同時接続制限
端末型接続	基本NAT	1台（早い者勝ち）
	動的NAT	最大1024セッション
	静的NAT	最大1024セッション+マッピングした情報数
ネットワーク型接続	使わない	ネットワークのすべての端末
	基本NAT	割り当てられたグローバルIPアドレスの数
	動的NAT	最大1024セッション
	静的NAT	最大1024セッション+マッピングした情報数

Q22. 本装置のLANには最大何台のパソコンが接続できますか？

A. ネットワークのルールに従えば、接続台数の制限はありません。

たとえば、192.168.1.0/255.255.255.0のネットワークであった場合、192.168.1.1～192.168.1.254の254台のうち、本装置の1台分を差し引いた253台までのパソコンが接続できます。

補足 本装置のDHCPサーバ機能を利用すると、最大64台までIPアドレスなどの情報を自動的に割り当てられます。65台以上パソコンがある場合は、65台目からIPアドレスなどの情報をそれらに個別に設定してください。

Q23. どんなプロトコルをサポートしていますか？

A. インターネットプロトコル（IPv4、IPv6）をサポートしています。

IP（Internet Protocol）は、その名のとおりインターネットで通信を行うためのプロトコルです。インターネットに接続する場合にはこのプロトコルが必要不可欠です。AppleTalk、IPX／SPX、FNA、SNAなどの通信プロトコルではブリッジでの中継でだけ利用できます。

Q24. MP とは何ですか？

A. **MP（Multilink PPP）は複数の回線を束ね、回線速度を高速化する技術です。**

MP は、回線の通信状況に合わせて空き回線を利用し、複数回線（ISDN の場合、2本）を1つの回線に見立てて回線速度を高速化し、通信状態を良くするプロトコルです。たとえば、ISDN 回線（2B=64Kbps ×2本）を束ねて128Kbps の速度を持つ1つの回線に見立てることができます。

本装置の場合は、ISDN を1本（2B）収容できますので、64Kbps の回線を2本を1本に見立てて128Kbps の回線速度を作り出します。ただし、MP 利用時の回線使用料金は2本分かかります。

Q25. DHCP とは何ですか？

A. **DHCP（Dynamic Host Configuration Protocol）は、IPアドレスなどの情報を割り当てるためのプロトコルです。**

これを利用することにより、管理元（DHCP サーバ）から各パソコン（DHCP クライアント）に対し、IP アドレスやゲートウェイアドレスなどネットワークの各種設定を自動化できます。ネットワーク環境が変化した場合でも、管理元の設定を変更することでパソコン側の設定も変更できます。本装置には DHCP サーバ機能が搭載されています。（P.479）

Q26. DNS とは何ですか？

A. **DNS（Domain Name Service）は、ホスト名（または端末名）とIP アドレスを管理するデータベースです。**

DNS にアクセスすることによって、そこに登録されている世界中のアドレス情報を取り出すことができます。たとえば、よく使われている Web や e-mail で表記されるホスト名（たとえば、www.fujitsu.com）はこのデータベースを使い、IP アドレスに変換されます。Web などのアプリケーションは検索してきた結果（IP アドレス）を利用して通信することができるようになります。

Q27. 接続する相手を認証することはできますか？

A. **PAP、または CHAP により認証できます。（P.115）**

Q28. データ圧縮機能をサポートしていますか？

A. **以下の圧縮方式をサポートしています。**

- VJ ヘッダ圧縮、IP ヘッダ圧縮、LZS によるデータ圧縮

  ただし、これらの圧縮機能は、接続開始時の交渉で、相手が同意した場合だけ有効になります。

Q29. マルチダイヤル機能とは何ですか？

A. **接続先の電話番号を3つまで登録して、1つ目の電話番号が話し中であれば、2つ目の電話番号に自動的にダイヤルする機能です。話し中でつながりにくいプロバイダに接続するときに有効です。**

Q30. テレホーダイ機能とは何ですか？

A. 自動回線切断機能（※）を簡単な操作で停止させて、指定した時間内は、回線を切断しないようにする機能です。NTTのテレホーダイサービス利用時に効果的です。

補足 ※一定時間（無通信監視タイマの設定：初期設定1分）、回線上の通信がない状態が続くと、回線使用料を余分に払わないようにするために自動的に回線を切断する機能です。

Q31. 使用状況／稼動状況などを表示できますか？

A. 表示メニュー（P.611）で表示できる情報はWWWブラウザを介して表示／出力ができます。

Q32. 発信専用にできますか？

A. できます。

詳細設定メニューのルータ設定で「回線情報」をクリックし、「回線情報設定」ページの［ISDN情報］の中の「着信動作」の設定で「すべて禁止」を選択します。

本装置の設定について

Q33. 回線（ISDN／専用線）に接続していなくても設定できますか？

A. 設定できます。

本装置が回線設置より早く手元に届いても、事前に設定できます。

回線が設置されるまでは、本装置を使ってLAN環境の構築などを行ってください。

Q34. 本装置の設定にはどんなブラウザが利用できますか？

A. Microsoft® Internet Explorer Version 6.0とMicrosoft® Internet Explorer Version 7.0です。

Q35. IPアドレスを設定する場合、使ってはいけないIPアドレスはありますか？

A. 以下の3種類のIPアドレスは使わないでください。

- すでにに利用されているIPアドレス
  IPネットワークでは、IPアドレスが世界中で必ず1つであることを条件に構成されています。プライベートアドレスを使って接続する端末型接続の場合でも、NAT機能を用いて世界中で1つしかないIPアドレス（グローバルアドレス）に変換します。
- ネットワーク部を示すIPアドレス（0ブロードキャスト）
  ネットワーク部（そのまま）+ホスト部がすべて0（2進数表記）のIPアドレス
- ブロードキャストアドレスを示すIPアドレス（1ブロードキャスト）
  ネットワーク部（そのまま）+ホスト部がすべて1（2進数表記）のIPアドレス

ネットワーク部／ホスト部の求めかたは以下のとおりです。

ネットワーク部=IPアドレス&ネットマスク（論理積）

ホスト部=IPアドレス&（notネットマスク）（論理積と排他）

たとえば、本装置のデフォルトIPアドレスである、192.168.1.1／255.255.255.0（24bit）の場合、ネットワーク部／ホスト部は以下のとおりです。

ネットワーク部

```
192.168.1.1      =    11000000.10101000.00000001.00000001
&255.255.255.0   =    11111111.11111111.11111111.00000000
192.168.1.0      =    11000000.10101000.00000001.00000000
```

ホスト部

```
192.168.1.1      =    11000000.10101000.00000001.00000001
&0.0.0.255       =    00000000.00000000.00000000.11111111
0.0.0.1          =    00000000.00000000.00000000.00000001
```

この場合、以下のようになります。

本装置のIPアドレス　　=192.168.1.1（ホスト1番）
ネットワークアドレス　　=192.168.1.0（ホスト部:00000000）
ブロードキャストアドレス　=192.168.1.255（ホスト部:11111111）

Q36. 認証ID／パスワードに日本語は使えますか？

A. 使えません。

本装置で扱えるのは英数字と記号（ただし、2バイト文字は除く）だけです。プロバイダからもらったパスワードが日本語の場合、プロバイダに依頼して英数字に変更してください。

Q37. FTPだけデータを通すことはできますか？

A. IPフィルタリング機能を使えばできます。

Q38. ポート番号によるフィルタリングはできますか？

A. できます。

本装置のIPフィルタリングは、IPアドレス／ポート番号／TCP接続要求を対象にするか（TCPのみ）などの設定が可能です。フィルタリング動作としては、透過／遮断／透過（接続中のみ）があります。

Q39. WAN側IPアドレスを割り当てられますか？

A. 割り当てられます。

詳細設定メニューのルータ設定で「相手情報」をクリックし、「相手情報設定」ページの［ネットワーク情報一覧］から「ネットワーク情報設定」ページを開き、「WAN側IPアドレス」の設定で「設定する」を選択し、かつ、IPアドレスを入力してください。

Q40. WAN側IPアドレスを割り当てないunnumberedの設定はできますか？

A. できます。

unnumbered設定を行う場合、詳細設定メニューのルータ設定で「相手情報」をクリックし、「相手情報設定」ページの［ネットワーク情報一覧］から「ネットワーク情報設定」ページを開き、「WAN側IPアドレス」の設定で「設定しない」を選択してください。

Q41. 着信側になったときに、動的にIPアドレスを割り当てることができますか？

A. 割り当てられます。最大2つまで割り当てることができます。（P.497）

Q42. むだな回線接続要求を止める方法は？

A. 回線ログとIPフィルタリングを利用します。

回線ログには発信契機となったパケット情報がページに出力されます。この情報を元にIPフィルタリングを行います。

たとえば、

Protocol:ICMP192.168.1.3（xxx）→164.71.2.5（yyy）

という行が回線ログのページ上に複数個表示されたとします。この場合、このパケットを遮断することで、回線のむだな発信が止められます。

以下にIPフィルタリングの設定ページ（詳細設定）を表示します。設定画面の各項目を入力します。

動作	遮断
プロトコル	ICMP
［送信元情報］	
IPアドレス	192.168.1.3
アドレスマスク	32
ポート番号	なにも指定しない
［宛先情報］	
IPアドレス	164.71.2.5
アドレスマスク	32
ポート番号	なにも指定しない
TCP接続要求	どちらでも可

再起動後（できれば電源を切断してから）、一定時間放置したあとに、再度回線ログを確認してください。上記の情報が表示されていないことが確認できると思います。

Q43. 時刻を設定することはできますか？

A. 端末から時刻を取得、タイムサーバから時刻を取得、または任意の時刻を設定の3通りの方法で設定できます。

- 操作メニューの「時刻設定」でパソコンから時刻を取得、または任意の時刻を設定することができます。
- 詳細設定メニューでルータ設定の「装置情報」をクリックし、「装置情報設定」ページの［タイムサーバ情報］の設定で、「使用する」を選択し、かつ、「プロトコル」「タイムサーバIPアドレス」「自動時刻設定間隔」を設定すると、本装置からの時刻問い合わせにより自動的に時刻を合わせます。
  また、［タイムサーバ情報］が設定されている場合、操作メニューの「時刻設定」で、タイムサーバからの時刻を取得の［設定］ボタンをクリックすることによって、即時に取得することもできます。

セキュリティについて

Q44. セキュリティはどのように確保しますか？

A. 発信者番号チェック、CHAP／PAP、IPフィルタリング、NATなどの機能で確保できます。（P.429）

- 発信者番号チェック　：接続先の電話番号が登録されているかどうかを確認します。もし、登録されていなければ回線は接続されません。
- CHAP／PAP　：回線接続のプロトコル（PPP）で、接続を制御するための認証方式です。
- IPフィルタリング　：特定のIPアドレスだけ透過（逆に遮断）し、不要な通信を遮断できます。
- NAT　：本装置を介してLAN側とインターネット側のIPアドレスを変換して、LAN側のアドレスをインターネット側から見えなくします。

Q45. 発信元の電話番号を区別して着信許可／拒否することができますか？

A. できます。（P.252）

なお、初期設定の状態では、事前に登録していない接続先からの着信要求は拒否するようになっています。

Q46. CHAPやPAPを使用していますか？

A. 使用しています。

本装置は2点間で回線を接続するためPPPというプロトコル（手順）で行われますが、この処理の途中でCHAP／PAPといった認証プロトコルを使用します。本装置では認証処理は以下のようになっています。

［発信時］

相手を認証しません。

相手が認証を要求してきた場合は、手順に従い自側の認証ID／パスワードを送出します。

［着信時］

相手を認証します（認証をしない設定にすることも可能）。

相手が認証を要求してきた場合は、手順に従い自側の認証ID／パスワードを送出します。

Q47. 特定のパソコンからインターネット接続を禁止することはできますか？

A.『IPフィルタリング（詳細設定）』を行うことで実現可能です。

たとえば、192.168.1.3から本装置を介してインターネット接続できなくする場合の設定内容は以下のようになります。

動作	遮断
プロトコル	すべて
IPアドレス	192.168.1.3
アドレスマスク	255.255.255.255

Q48. 特定のパソコンだけをインターネットからアクセスできるようにする。

A. 『IP フィルタリング（詳細設定）』を行うことで実現可能です。

たとえば、192.168.1.0/24のネットワークの192.168.1.3へのアクセスを許す場合の設定内容は以下のようになります。

［優先順位1］

動作	透過
プロトコル	すべて
IPアドレス	192.168.1.3
アドレスマスク	255.255.255.255

［優先順位2］

動作	遮断
プロトコル	すべて
IPアドレス	192.168.1.0
アドレスマスク	255.255.255.0

Q49. インターネットからLAN上のサーバへのアクセスを禁止する。

A. NAT 機能を利用することで、実現可能です。

NAT機能は本装置を介してインターネットにアクセスする段階で、元のIPアドレスを別のIPアドレスに振り替えてインターネット上のサーバと通信するための機能です。

パソコンのIPアドレス（プライベートアドレス）を、違うIPアドレス（グローバルアドレス）に変換して通信するため、LANからインターネットに向かってアクセスできても、インターネットからLANに向かってアクセスできません（IPアドレスの変換テーブルに変換情報がないため）。

IPフィルタリング機能を使って細かい設定をすることなく、インターネットからのアクセスを止められます。

運用について

Q50. 本装置で利用できるのはどんな端末ですか？

A. 以下の条件がそろっていれば、パソコン、ワークステーションはほとんどご利用いただけます。

- Ethernetポート、またはEthernetアダプタを備えている。
- IPプロトコルをサポートしている。

Q51. 回線をつなぐにはどうしたら良いのですか？

A. アプリケーションを起動して、そのままインターネットにアクセスしていただければ回線はつながります。

たとえば、ブラウザを例にしますと、以下の手順で回線が接続されます。

1 www.fujitsu.com を指定します。

2 端末は www.fujitsu.com の IP アドレスがわからないので、DNS サーバに対して www.fujitsu.com の IP アドレスが何であるかを問い合わせます。DNS サーバに対して要求を送る時には、ルーティングテーブルを見て本装置にデータを転送すれば良いことを判断します。

3 データを受け取った本装置は、ルーティングテーブルを見て回線の向こう側に DNS サーバがいることを判断した結果、回線を接続する必要があると理解し、回線を接続します。

Q52. ブラウザを終了すると回線は切れますか？

A. ブラウザを終了させただけでは切れません。

自動回線切断機能は、ある一定の時間 ISDN 回線上にデータが 1 つも流れなかったとき、はじめて回線切断処理を行います。このため、ブラウザをはじめとするアプリケーション終了時には回線は切断されません。

ただし、本装置の操作メニューで「手動切断」処理を行うことで、任意のタイミングで回線を切断できます。

なお、前記「一定時間」は設定できます。設定項目の名前は『無通信監視タイマ』です。

Q53. ブラウザ以外から手動切断する方法はありますか？

A. ありません。

緊急時は、回線側のケーブルを抜けば接続状態にある回線を切断できます。

Q54. 複数の人が同時にメールを読むことは可能ですか？

A. プロバイダのサービスに依存します。

たとえば、プロバイダで、接続用の ID1 つに対して最大 5 個のメールアカウントを利用できるサービスがあるとします。このサービスを利用すれば、本装置経由で複数の人が同時にメールを読めます。

Q55. プロキシサーバは利用できますか？

A. ご利用いただけます。

プロキシサーバを使用する場合は、以下を参考にして本装置だけをプロキシの対象外にしてください。

1 Microsoft® Internet Explorer を起動します。

2 「インターネットオプション」をクリックします。

- Microsoft® Internet Explorer 6.0 の場合
  メニューバーの［ツール］をクリックします。
- Microsoft® Internet Explorer 7.0 の場合
  ツールバーまたはメニューバーの［ツール］をクリックします。

3 インターネットオプション画面の「接続」タブで、［LANの設定］ボタンをクリックします。

4 プロキシサーバーの「LAN にプロキシサーバーを使用する」が選択されていることを確認し、［詳細設定］ボタンをクリックします。

5 「HTTP」にプロバイダの Proxy サーバを指定します。

6 例外の「次で始まるアドレスにはプロキシを使用しない」に本装置の IP アドレス（192.168.1.1）を指定します。

Q56. Windows® のネットワークコンピュータでWANの先の相手のコンピュータを見ることはできますか？

A. ISDN 回線を介した場合、見られません。

lmhosts ファイルに、接続先のコンピュータの IP アドレスとホスト名を登録し、「検索」機能でホストを検索してください。

lmhosts ファイルを使用する代わりに、本装置の ProxyDNS 機能で接続先のコンピュータの IP アドレスを登録しておくこともできます。（P.471）

Q57. ほかの機種で DHCP サーバを動かしていますが問題ないですか？

A. 本装置の DHCP サーバ機能は止めてください。

本装置の DHCP サーバ機能より、UNIX® サーバや Windows NT® サーバなどほかの機種の方が、より細かい情報をパソコンに割り当てることができます。本装置の DHCP サーバ機能は停止して、既存の DHCP サーバをそのまま使用されることをお勧めします。

Q58. 電源はどうやって切断したら良いのですか？

A. 通常運用では電源スイッチをそのまま切断していただいても、本装置本体には影響を与えません。

⚠注意

ファームウェアのバージョンアップ作業を行っている場合は、絶対に電源を切断しないでください。

パソコンについて

Q59. IPアドレスを設定する場合、使ってはいけないIPアドレスはありますか？

A. 以下の3種類のIPアドレスを使ってはいけません。（P.757）

- すでに利用されているIPアドレス
  IPネットワークでは、IPアドレスが世界中で必ず1つであることを条件に構成されています。プライベートアドレスを使って接続する端末型接続の場合でも、NAT機能を用いて世界中で1つしかないIPアドレスに変換します。
- ネットワークアドレスを示すIPアドレス（0ブロードキャスト）
  ネットワーク部（そのまま）+ホスト部がすべて0（2進数表記）のIPアドレス
- ブロードキャストアドレスを示すIPアドレス（1ブロードキャスト）
  ネットワーク部（そのまま）+ホスト部がすべて1（2進数表記）のIPアドレス

NAT（マルチNAT）について

Q60. NATとは何ですか？

A. Network Address Translationの略です。

簡単に言えば、本装置と同じLANにつながっているパソコンのIPアドレスが、本装置を通ってインターネットに出て行く時に、違うIPアドレスになって出て行く機能です。

本装置ではNAT機能を拡張したマルチNATをサポートしています。

Q61. NATの設定方法は？

A. 詳細設定の相手情報から行います。

かんたん設定で端末型接続を選んだ場合、動的NATが動作するように設定されますが、それ以外のNAT機能を利用する場合は、必ず詳細設定で動作を設定する必要があります。

Q62.（基本／静的／動的）NATの違いは何ですか？

A. 同時接続できる台数、機能制限に以下のような違いがあります。

NATの種類	同時接続制限（セッション数）	備考
基本NAT	割り当てIPアドレス数	割り当て時間内は外部を起点とした通信も可能
動的NAT	1024セッション	外部を起点とした通信は不可能
静的NAT	1024セッションとマッピングした情報	プライベートアドレス（とポート）をグローバルアドレス（とポート）にマッピングできる／マッピングしたアドレス（とポート）に関しては、外部を起点とした通信も可能

Q63. NAT機能を利用した場合、FTPが使えなくなるのですか？

A. **本装置のNAT機能ならば大丈夫です。**

本来のNAT機能の場合、IP通信の要となるIPヘッダ（葉書などの住所／郵便番号）部分に書き込まれているプライベートアドレスをグローバルアドレス（またはその逆）に変換する機能です。

しかしFTPの場合、パソコンがIPヘッダの上位層（葉書でいうと文章）でローカルIPアドレス（住所）を伝え、サーバは教えられた"ローカルIPアドレス（プライベートアドレス）"にデータを送信しますが、存在しない（または存在してもサービスを望んでいない）ため、通信は失敗に終わります。

そこで本装置のNAT機能は、FTP通信を見つけると上位層のローカルIPアドレス（プライベートアドレス）をグローバルアドレスに書き換えて正しく通信できるようにしています。

Q64. NATを使っている場合、IPフィルタリングはどのタイミングで実行されますか？

A. **プライベートアドレスを使って行われます。**

つまり、LANからインターネット上に向かう場合は、NAT機能でアドレスが変更される前にフィルタリング対象であるかどうかをチェックします。また、インターネットからLANに向かう場合は、NAT機能でアドレス変換されたあとでフィルタリング対象であるかどうかをチェックします。

どちらの場合でも、遮断処理の対象になったパケットは通信対象から外れますから、不要なパケットが流れて発信契機、または無通信監視タイマの対象から外れます。

ログ関連について

Q65. どんなログを表示できますか？

A. **以下のログが見られます。**

[表示メニューで確認できる内容]

- 回線接続状況：　現在の接続先情報が表示されます（回線状態（1B通信／MP通信）、接続形態（発信／着信）、接続先（名前／ダイヤル番号）、回線使用率（送信／受信）、通信時間（接続時間）、IPアドレス）。
- 課金情報：　電源投入（または再起動）後の回線使用料金が表示されます。
- IP統計情報：　回線を介した通信のプロトコルごとの内訳が表示されます。
- メールチェック：　POP3プロトコルを使用してメールの着信を確認した情報が表示されます。
- チャネル統計情報：　回線接続の情報が表示されます（発信回数、発信（接続）失敗回数、接続先話中回数）。
- 回線ログ：　回線接続に関する情報が表示されます（接続処理時間、接続契機パケット、回線接続失敗理由）。
- システムログ：　電源投入後のログが表示されます。
- ルーティング情報：　ルーティングテーブルが表示されます。

- インタフェース情報： インタフェースの使用状況を確認できます。
- ブリッジ情報： ブリッジの使用状況およびSTP情報を確認できます。
- マルチホーミング情報： マルチホーミング使用時の経路情報を確認できます。
- LAN情報： LANの統計情報を確認できます。
- DHCP情報： DHCPサーバやDHCPリレーエージェントの運用状況を確認できます。
- NAT情報： NATの統計情報を確認できます。
- ISDN情報： ISDN関連の統計情報を確認できます。
- フレームリレー情報： フレームリレー関連の統計情報を確認できます。
- IPsec情報： IPsec情報を確認できます。
- VRRP情報： VRRP情報を確認できます。
- 現在時刻： 現在の時刻（設定時刻）が表示されます。TIMEサーバと連動させたり、手動で入力できます（24時間以上、電源を切断したままにすると初期化されます。初期日時は1970/01/01/00:00:00）。
- 経過時間情報： 電源投入後の時間が表示されます。

[メンテナンスメニューで確認できること]

- バージョン情報： ファームウェアバージョンを表示します。
- PPPフレームトレース： 回線接続ネゴシエーションを表示します。
- エラーログ情報： エラーログが表示されます。
- 構成定義情報： 設定情報が表示されます。

Q66. syslogは使えますか？

A. **使えます。システムログを設定できます。**

Q67. syslogのファシリティのコードは何ですか？

A. **23（個人が割り当てできる数）が設定されます。**

Q68. syslogでどんな情報（プライオリティ）が入手できますか？

A. **以下の情報が入手できます。**

- LOG_ERR エラーメッセージ
- LOG_WARN 警告メッセージ
- LOG_NOTICE エラー以外のシステムメッセージ
- LOG_INFO 回線情報など

マルチTAについて

Q69. マルチTA機能ってなに？

A. 本装置でTAと同じように通信する機能です。Windows® 95／98／2000のダイヤルアップネットワークの仮想プライベートネットワークの機能を使って、TAを使ったPPP接続と同等の通信を行う機能です。

Q70. TAとはなにが違うの？

A. いろいろ違います。

まず、接続方法が違います。

TAの場合には、一般的にはパソコンのシリアルポートとTAのシリアルポートをシリアルケーブルを使って接続します。マルチTA機能は、パソコンのLANポートと本装置のHUBポートをLANケーブルを使って接続します。

このため、TAはシリアルケーブルで接続した1台のパソコンからしか使えませんが、マルチTAはLANに接続されていますので、LAN上のどのパソコンからでも使うことができます。

また、TAを利用する場合にはシリアルポートの速度によってはISDNの性能を生かしきれない場合がありますが、マルチTAの場合にはパソコンと本装置の間を10MbpsのLANで接続しますから、ISDNの性能を生かしきることができます。

いくつか、TAなら可能なことでもマルチTAで不可能なことがありますので注意してください。

- パケット通信はできません。
- 着信やコールバックはできません。
- MP通信はできません。
- 専用線では使えません。
- 非同期通信はできません。
- RVS-COMは使えません。
- ATコマンド操作はできません。

Q71. どうやって使うの？

A. TAやモデムでの接続と同じように使います。

接続をする場合には、ダイヤルアップネットワークから接続アイコンを選んで接続します。

切断をする場合には、接続ウィンドウから「切断」を選んで切断します。

TAやモデムでの接続と同じです。

Q72. どういうときに使うの？

A. **NATを利用すると不都合がある場合や、IP以外のプロトコルを利用する場合にお使いください。**

プロバイダとの端末型ダイヤルアップ契約では、本装置でNATを使わないと通信できませんが、NATを使ってしまうと通信できないアプリケーションもいくつか存在します。

また、本装置はIPルータです。IP以外のプロトコル（AppleTalk、IPX／SPX、FNA、SNAなど）は、ブリッジでの中継でだけご利用いただけます。

マルチTAは通常のTAと同等の通信を提供しますから、NATは使われませんし、Windows®がサポートしているプロトコルであればどのプロトコルでも通信が可能です。

Q73. 無通信監視機能はありますか？

A. **本装置は無通信監視は行いません。**

標準MIB定義

■ systemグループ

名称	オブジェクト識別子	SYNTAX	ACCESS
sysDescr	system.1	DisplayString	RO
sysObjectID	system.2	ObjectID	RO
sysUpTime	system.3	TimeTicks	RO
sysContact	system.4	DisplayString	RW ※
sysName	system.5	DisplayString	RW ※
sysLocation	system.6	DisplayString	RW ※
sysServices	system.7	INTEGER	RO

※次回リセット時まで有効

■ interfaceグループ

名称	オブジェクト識別子	SYNTAX	ACCESS
ifNumber	interfaces.1	INTEGER	RO
ifTable	interfaces.2	Aggregate	NA
ifEntry	ifTable.1	Aggregate	NA
ifIndex	ifEntry.1	INTEGER	RO
ifDescr	ifEntry.2	DisplayString	RO
ifType	ifEntry.3	INTEGER	RO
ifMtu	ifEntry.4	INTEGER	RO
ifSpeed	ifEntry.5	Gauge	RO
ifPhysAddress	ifEntry.6	PhysAddress	RO
ifAdminStatus	ifEntry.7	INTEGER	RO
ifOperStatus	ifEntry.8	INTEGER	RO
ifLastChange	ifEntry.9	TimeTicks	RO
ifInOctets	ifEntry.10	Counter	RO
ifInUcastPkts	ifEntry.11	Counter	RO
ifInNUcastPkts	ifEntry.12	Counter	RO
ifInDiscards	ifEntry.13	Counter	RO
ifInErrors	ifEntry.14	Counter	RO
ifInUnknownProtos	ifEntry.15	Counter	RO
ifOutOctets	ifEntry.16	Counter	RO
ifOutUcastPkts	ifEntry.17	Counter	RO
ifOutNUcastPkts	ifEntry.18	Counter	RO
ifOutDiscards	ifEntry.19	Counter	RO
ifOutErrors	ifEntry.20	Counter	RO
ifOutQLen	ifEntry.21	Gauge	RO
ifSpecific	ifEntry.22	ObjectID	RO

■ address translationグループ

名称	オブジェクト識別子	SYNTAX	ACCESS
atTable	at.1	Aggregate	NA
atEntry	atTable.1	Aggregate	NA
atIfIndex	atEntry.1	INTEGER	RO
atPhysAddress	atEntry.2	PhysAddress	RO
atNetAddress	atEntry.3	NetworkAddress	RO

■ ipグループ

ipグループ

名称	オブジェクト識別子	SYNTAX	ACCESS
ipForwarding	ip.1	INTEGER	RO
ipDefaultTTL	ip.2	INTEGER	RO
ipInReceives	ip.3	Counter	RO
ipInHdrErrors	ip.4	Counter	RO
ipInAddrErrors	ip.5	Counter	RO
ipForwDatagrams	ip.6	Counter	RO
ipInUnknownProtos	ip.7	Counter	RO
ipInDiscards	ip.8	Counter	RO
ipInDelivers	ip.9	Counter	RO
ipOutRequests	ip.10	Counter	RO
ipOutDiscards	ip.11	Counter	RO
ipOutNoRoutes	ip.12	Counter	RO
ipReasmTimeout	ip.13	INTEGER	RO
ipReasmReqds	ip.14	Counter	RO
ipReasmOKs	ip.15	Counter	RO
ipReasmFails	ip.16	Counter	RO
ipFragOKs	ip.17	Counter	RO
ipFragFails	ip.18	Counter	RO
ipFragCreates	ip.19	Counter	RO

ipAddrTableグループ

名称	オブジェクト識別子	SYNTAX	ACCESS
ipAddrTable	ip.20	Aggregate	NA
ipAddrEntry	ipAddrTable.1	Aggregate	NA
ipAdEntAddr	ipAddrEntry.1	IpAddress	RO
ipAdEntIfIndex	ipAddrEntry.2	INTEGER	RO
ipAdEntNetMask	ipAddrEntry.3	IpAddress	RO
ipAdEntBcastAddr	ipAddrEntry.4	INTEGER	RO
ipAdEntReasmMaxSize	ipAddrEntry.5	INTEGER	RO

ipRouteグループ

名称	オブジェクト識別子	SYNTAX	ACCESS
ipRouteTable	ip.21	Aggregate	NA
ipRouteEntry	ipRouteTable.1	Aggregate	NA
ipRouteDest	ipRouteEntry.1	IpAddress	RO
ipRouteIfIndex	ipRouteEntry.2	INTEGER	RO
ipRouteMetric1	ipRouteEntry.3	INTEGER	RO
ipRouteMetric2	ipRouteEntry.4	INTEGER	RO
ipRouteMetric3	ipRouteEntry.5	INTEGER	RO
ipRouteMetric4	ipRouteEntry.6	INTEGER	RO
ipRouteNextHop	ipRouteEntry.7	IpAddress	RO
ipRouteType	ipRouteEntry.8	INTEGER	RO
ipRouteProto	ipRouteEntry.9	INTEGER	RO
ipRouteAge	ipRouteEntry.10	INTEGER	RO
ipRouteMask	ipRouteEntry.11	IpAddress	RO
ipRouteMetric5	ipRouteEntry.12	INTEGER	RO
ipRouteInfo	ipRouteEntry.13	ObjectID	RO

ipNetToMedia グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
ipNetToMediaTable	ip.22	Aggregate	NA
ipNetToMediaEntry	ipNetToMediaTable.1	Aggregate	NA
ipNetToMediaIfIndex	ipNetToMediaEntry.1	INTEGER	RO
ipNetToMediaPhysAddress	ipNetToMediaEntry.2	PhysAddress	RO
ipNetToMediaNetAddress	ipNetToMediaEntry.3	IpAddress	RO
ipNetToMediaType	ipNetToMediaEntry.4	INTEGER	RO

その他の ip グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
ipRoutingDiscards	ip.23	Counter	RO

ipForward グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
ipForward	ip.24	Aggregate	NA
ipForwardNumber	ipForward.1	Gauge	RO
ipForwardTable	ipForward.2	Aggregate	NA
ipForwardEntry	ipForwardTable.1	Aggregate	NA
ipForwardDest	ipForwardEntry.1	IpAddress	RO
ipForwardMask	ipForwardEntry.2	IpAddress	RO
ipForwardPolicy	ipForwardEntry.3	INTEGER	RO
ipForwardNextHop	ipForwardEntry.4	IpAddress	RO
ipForwardIfIndex	ipForwardEntry.5	INTEGER	RO
ipForwardType	ipForwardEntry.6	INTEGER	RO
ipForwardProto	ipForwardEntry.7	INTEGER	RO
ipForwardAge	ipForwardEntry.8	INTEGER	RO
ipForwardInfo	ipForwardEntry.9	ObjectID	RO
ipForwardNextHopAS	ipForwardEntry.10	INTEGER	RO
ipForwardMetric1	ipForwardEntry.11	INTEGER	RO
ipForwardMetric2	ipForwardEntry.12	INTEGER	RO
ipForwardMetric3	ipForwardEntry.13	INTEGER	RO
ipForwardMetric4	ipForwardEntry.14	INTEGER	RO
ipForwardMetric5	ipForwardEntry.15	INTEGER	RO

■ icmp グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
icmpInMsgs	icmp.1	Counter	RO
icmpInErrors	icmp.2	Counter	RO
icmpInDestUnreachs	icmp.3	Counter	RO
icmpInTimeExcds	icmp.4	Counter	RO
icmpInParmProbs	icmp.5	Counter	RO
icmpInSrcQuenchs	icmp.6	Counter	RO
icmpInRedirects	icmp.7	Counter	RO
icmpInEchos	icmp.8	Counter	RO
icmpInEchoReps	icmp.9	Counter	RO
icmpInTimestamps	icmp.10	Counter	RO
icmpInTimestampReps	icmp.11	Counter	RO
icmpInAddrMasks	icmp.12	Counter	RO
icmpInAddrMaskReps	icmp.13	Counter	RO
icmpOutMsgs	icmp.14	Counter	RO
icmpOutErrors	icmp.15	Counter	RO
icmpOutDestUnreachs	icmp.16	Counter	RO
icmpOutTimeExcds	icmp.17	Counter	RO
icmpOutParmProbs	icmp.18	Counter	RO
icmpOutSrcQuenchs	icmp.19	Counter	RO
icmpOutRedirects	icmp.20	Counter	RO
icmpOutEchos	icmp.21	Counter	RO
icmpOutEchoReps	icmp.22	Counter	RO
icmpOutTimestamps	icmp.23	Counter	RO
icmpOutTimestampReps	icmp.24	Counter	RO
icmpOutAddrMasks	icmp.25	Counter	RO
icmpOutAddrMaskReps	icmp.26	Counter	RO

■ tcp グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
tcpRtoAlgorithm	tcp.1	INTEGER	RO
tcpRtoMin	tcp.2	INTEGER	RO
tcpRtoMax	tcp.3	INTEGER	RO
tcpMaxConn	tcp.4	INTERGER	RO
tcpActiveOpens	tcp.5	Counter	RO
tcpPassiveOpens	tcp.6	Counter	RO
tcpAttemptFails	tcp.7	Counter	RO
tcpEstabResets	tcp.8	Counter	RO
tcpCurrEstab	tcp.9	Gauge	RO
tcpInSegs	tcp.10	Counter	RO
tcpOutSegs	tcp.11	Counter	RO
tcpRetransSegs	tcp.12	Counter	RO
tcpConnTable	tcp.13	Aggregate	NA
tcpConnEntry	tcpConnTable.1	Aggregate	NA
tcpConnState	tcpConnEntry.1	INTEGER	RO
tcpConnLocalAddress	tcpConnEntry.2	IpAddress	RO
tcpConnLocalPort	tcpConnEntry.3	INTEGER	RO
tcpConnRemAddress	tcpConnEntry.4	IpAddress	RO
tcpConnRemPort	tcpConnEntry.5	INTEGER	RO
tcpInErrs	tcp.14	Counter	RO
tcpOutRsts	tcp.15	Counter	RO

■ udp グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
udpInDatagrams	udp.1	Counter	RO
udpNoPorts	udp.2	Counter	RO
udpInErrors	udp.3	Counter	RO
udpOutDatagrams	udp.4	Counter	RO
udpTable	udp.5	Aggregate	NA
udpEntry	udpTable.1	Aggregate	NA
udpLocalAddress	udpEntry.1	IpAddress	RO
udpLocalPort	udpEntry.2	INTEGER	RO

■ snmp グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
snmpInPkts	snmp.1	Counter	RO
snmpOutPkt	snmp.2	Counter	RO
snmpInBadVersions	snmp.3	Counter	RO
snmpInBadCommunityNames	snmp.4	Counter	RO
snmpInBadCommunityUses	snmp.5	Counter	RO
snmpInASNParseErrs	snmp.6	Counter	RO
snmpInTooBigs	snmp.8	Counter	RO
snmpInNoSuchNames	snmp.9	Counter	RO
snmpInBadValues	snmp.10	Counter	RO
snmpInReadOnlys	snmp.11	Counter	RO
snmpInGenErrs	snmp.12	Counter	RO
snmpInTotalReqVars	snmp.13	Counter	RO
snmpInTotalSetVars	snmp.14	Counter	RO
snmpInGetRequests	snmp.15	Counter	RO
snmpInGetNexts	snmp.16	Counter	RO
snmpInSetRequests	snmp.17	Counter	RO
snmpInGetResponses	snmp.18	Counter	RO
snmpInTraps	snmp.19	Counter	RO
snmpOutTooBigs	snmp.20	Counter	RO
snmpOutNoSuchNames	snmp.21	Counter	RO
snmpOutBadValues	snmp.22	Counter	RO
snmpOutGenErrs	snmp.24	Counter	RO
snmpOutGetRequests	snmp.25	Counter	RO
snmpOutGetNexts	snmp.26	Counter	RO
snmpOutSetRequests	snmp.27	Counter	RO
snmpOutGetResponses	snmp.28	Counter	RO
snmpOutTraps	snmp.29	Counter	RO
snmpEnableAuthenTraps	snmp.30	INTEGER	RO

■ ppp グループ

pppLcp グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
pppLinkStatusTable	pppLink.1	Aggregate	NA
pppLinkStatusEntry	pppLinkStatusTable.1	Aggregate	NA
pppLinkStatusPhysicalIndex	pppLinkStatusEntry.1	INTEGER	RO
pppLinkStatusBadAddresses	pppLinkStatusEntry.2	Counter	RO
pppLinkStatusBadControls	pppLinkStatusEntry.3	Counter	RO
pppLinkStatusPacketTooLongs	pppLinkStatusEntry.4	Counter	RO
pppLinkStatusBadFCSs	pppLinkStatusEntry.5	Counter	RO
pppLinkStatusLocalMRU	pppLinkStatusEntry.6	INTEGER	RO
pppLinkStatusRemoteMRU	pppLinkStatusEntry.7	INTEGER	RO
pppLinkStatusLocalToPeer ACCMap	pppLinkStatusEntry.8	OctetString	RO
pppLinkStatusPeerToLocal ACCMap	pppLinkStatusEntry.9	OctetString	RO
pppLinkStatusLocalToRemote ProtocolCompression	pppLinkStatusEntry.10	INTEGER	RO
pppLinkStatusRemoteToLocal ProtocolCompression	pppLinkStatusEntry.11	INTEGER	RO
pppLinkStatusLocalToRemote ACCompression	pppLinkStatusEntry.12	INTEGER	RO
pppLinkStatusRemoteToLocal ACCompression	pppLinkStatusEntry.13	INTEGER	RO
pppLinkStatusTransmitFcsSize	pppLinkStatusEntry.14	INTEGER	RO
pppLinkStatusReceiveFcsSize	pppLinkStatusEntry.15	INTEGER	RO
pppLinkConfigTable	pppLink.2	Aggregate	NA
pppLinkConfigEntry	pppLinkConfigTable.1	Aggregate	NA
pppLinkConfigInitialMRU	pppLinkConfigEntry.1	INTEGER	RO
pppLinkConfigReceiveACCMap	pppLinkConfigEntry.2	OctetString	RO
pppLinkConfigTransmitACCMap	pppLinkConfigEntry.3	OctetString	RO
pppLinkConfigMagicNumber	pppLinkConfigEntry.4	INTEGER	RO
pppLinkConfigFcsSize	pppLinkConfigEntry.5	INTEGER	RO

ppplp グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
ppplpTable	ppplp.1	Aggregate	NA
ppplpEntry	ppplpTable.1	Aggregate	NA
ppplpOperStatus	ppplpEntry.1	INTEGER	RO
ppplpLocalToRemote CompressionProtocol	ppplpEntry.2	INTEGER	RO
ppplpRemoteToLocal CompressionProtocol	ppplpEntry.3	INTEGER	RO
ppplpRemoteMaxSlotId	ppplpEntry.4	INTEGER	RO
ppplpLocalMaxSlotId	ppplpEntry.5	INTEGER	RO
ppplpConfigTable	ppplp.2	Aggregate	NA
ppplpConfigEntry	ppplpConfigTable.1	Aggregate	NA
ppplpConfigAdminStatus	ppplpConfigEntry.1	INTEGER	RO
ppplpConfigCompression	ppplpConfigEntry.2	INTEGER	RO

pppBridgeグループ

名称	オブジェクト識別子	SYNTAX	ACCESS
pppBridgeTable	pppBridge.1	Aggregate	NA
pppBridgeEntry	pppBridgeTable.1	Aggregate	NA
pppBridgeOperStatus	pppBridgeEntry.1	INTEGER	RO
pppBridgeLocalToRemote TinygramCompression	pppBridgeEntry.2	INTEGER	RO
pppBridgeRemoteToLocal TinygramCompression	pppBridgeEntry.3	INTEGER	RO
pppBridgeLocalToRemoteLanId	pppBridgeEntry.4	INTEGER	RO
pppBridgeRemoteToLocalLanId	pppBridgeEntry.5	INTEGER	RO
pppBridgeConfigTable	pppBridge.2	Aggregate	NA
pppBridgeConfigEntry	pppBridgeConfigTable.1	Aggregate	NA
pppBridgeConfigAdminStatus	pppBridgeConfigEntry.1	INTEGER	RO
pppBridgeConfigTinygram	pppBridgeConfigEntry.2	INTEGER	RO
pppBridgeConfigRingId	pppBridgeConfigEntry.3	INTEGER	RO
pppBridgeConfigLineId	pppBridgeConfigEntry.4	INTEGER	RO
pppBridgeConfigLanId	pppBridgeConfigEntry.5	INTEGER	RO
pppBridgeMediaTable	pppBridge.3	Aggregate	NA
pppBridgeMediaEntry	pppBridgeMediaTable.1	Aggregate	NA
pppBridgeMediaMacType	pppBridgeMediaEntry.1	INTEGER	RO
pppBridgeMediaLocalStatus	pppBridgeMediaEntry.2	INTEGER	RO
pppBridgeMediaRemoteStatus	pppBridgeMediaEntry.3	INTEGER	RO
pppBridgeMediaConfigTable	pppBridge.4	Aggregate	NA
pppBridgeMediaConfigEntry	pppBridgeMedia ConfigTable.1	Aggregate	NA
pppBridgeMediaConfigMacType	pppBridgeMedia ConfigEntry.1	INTEGER	RO
pppBridgeMediaConfigLocal Status	pppBridgeMedia ConfigEntry.2	INTEGER	RO

■ dot1dBridgeグループ

dot1dBaseグループ

名称	オブジェクト識別子	SYNTAX	ACCESS
dot1dBaseBridgeAddress	dot1dBase.1	OctetString	RO
dot1dBaseNumPorts	dot1dBase.2	INTEGER	RO
dot1dBaseType	dot1dBase.3	INTEGER	RO
dot1dBasePortTable	dot1dBase.4	Aggregate	NA
dot1dBasePortEntry	dot1dBasePortTable.1	Aggregate	NA
dot1dBasePort	dot1dBasePortEntry.1	INTEGER	RO
dot1dBasePortIfIndex	dot1dBasePortEntry.2	INTEGER	RO
dot1dBasePortCircuit	dot1dBasePortEntry.3	ObjectID	RO
dot1dBasePortDelayExceeded Discards	dot1dBasePortEntry.4	Counter	RO
dot1dBasePortMtuExceeded Discards	dot1dBasePortEntry.5	Counter	RO

dot1dStp グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
dot1dStpProtocolSpecification	dot1dStp.1	INTEGER	RO
dot1dStpPriority	dot1dStp.2	INTEGER	RO
dot1dStpTimeSinceTopology Change	dot1dStp.3	TimeTicks	RO
dot1dStpTopChanges	dot1dStp.4	Counter	RO
dot1dStpDesignatedRoot	dot1dStp.5	OctetString	RO
dot1dStpRootCost	dot1dStp.6	INTEGER	RO
dot1dStpRootPort	dot1dStp.7	INTEGER	RO
dot1dStpMaxAge	dot1dStp.8	TimeOut	RO
dot1dStpHelloTime	dot1dStp.9	TimeOut	RO
dot1dStpHoldTime	dot1dStp.10	INTEGER	RO
dot1dStpForwardDelay	dot1dStp.11	TimeOut	RO
dot1dStpBridgeMaxAge	dot1dStp.12	TimeOut	RO
dot1dStpBridgeHelloTime	dot1dStp.13	TimeOut	RO
dot1dStpBridgeForwardDelay	dot1dStp.14	TimeOut	RO
dot1dStpPortTable	dot1dStp.15	Aggregate	NA
dot1dStpPortEntry	dot1dStpPortTable.1	Aggregate	NA
dot1dStpPort	dot1dStpPortEntry.1	INTEGER	RO
dot1dStpPortPriority	dot1dStpPortEntry.2	INTEGER	RO
dot1dStpPortState	dot1dStpPortEntry.3	INTEGER	RO
dot1dStpPortEnable	dot1dStpPortEntry.4	INTEGER	RO
dot1dStpPortPathCost	dot1dStpPortEntry.5	INTEGER	RO
dot1dStpPortDesignatedRoot	dot1dStpPortEntry.6	OctetString	RO
dot1dStpPortDesignatedCost	dot1dStpPortEntry.7	INTEGER	RO
dot1dStpPortDesignatedBridge	dot1dStpPortEntry.8	OctetString	RO
dot1dStpPortDesignatedPort	dot1dStpPortEntry.9	OctetString	RO
dot1dStpPortForwardTransitions	dot1dStpPortEntry.10	Counter	RO

dot1dTp グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
dot1dTpLearnedEntryDiscards	dot1dTp.1	Counter	RO
dot1dTpAgingTime	dot1dTp.2	INTEGER	RO

dot1dTpFdb グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
dot1dTpFdbTable	dot1dTp.3	Aggregate	NA
dot1dTpFdbEntry	dot1dTpFdbTable.1	Aggregate	NA
dot1dTpFdbAddress	dot1dTpFdbEntry.1	OctetString	RO
dot1dTpFdbPort	dot1dTpFdbEntry.2	INTEGER	RO
dot1dTpFdbStatus	dot1dTpFdbEntry.3	INTEGER	RO

dot1dTpPort グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
dot1dTpPortTable	dot1dTp.4	Aggregate	NA
dot1dTpPortEntry	dot1dTpPortTable.1	Aggregate	NA
dot1dTpPort	dot1dTpPortEntry.1	INTEGER	RO
dot1dTpPortMaxInfo	dot1dTpPortEntry.2	INTEGER	RO
dot1dTpPortInFrames	dot1dTpPortEntry.3	Counter	RO
dot1dTpPortOutFrames	dot1dTpPortEntry.4	Counter	RO
dot1dTpPortInDiscards	dot1dTpPortEntry.5	Counter	RO

dot1dStaticグループ

名称	オブジェクト識別子	SYNTAX	ACCESS
dot1dStaticTable	dot1dStatic.1	Aggregate	NA
dot1dStaticEntry	dot1dStaticTable.1	Aggregate	NA
dot1dStaticAddress	dot1dStaticEntry.1	OctetString	RO
dot1dStaticReceivePort	dot1dStaticEntry.2	INTEGER	RO
dot1dStaticAllowedToGoTo	dot1dStaticEntry.3	OctetString	RO
dot1dStaticStatus	dot1dStaticEntry.4	INTEGER	RO

■ frame-relayグループ

frDlcmiグループ

名称	オブジェクト識別子	SYNTAX	ACCESS
frDlcmiTable	frame-relay.1	Aggregate	NA
frDlcmiEntry	frDlcmiTable.1	Aggregate	NA
frDlcmiIfIndex	frDlcmiEntry.1	INTEGER	RO
frDlcmiState	frDlcmiEntry.2	INTEGER	RO
frDlcmiAddress	frDlcmiEntry.3	INTEGER	RO
frDlcmiAddressLen	frDlcmiEntry.4	INTEGER	RO
frDlcmiPollingInterval	frDlcmiEntry.5	INTEGER	RO
frDlcmiFullEnquiryInterval	frDlcmiEntry.6	INTEGER	RO
frDlcmiErrorThreshold	frDlcmiEntry.7	INTEGER	RO
frDlcmiMonitoredEvents	frDlcmiEntry.8	INTEGER	RO
frDlcmiMaxSupportedVCs	frDlcmiEntry.9	INTEGER	RO
frDlcmiMulticast	frDlcmiEntry.10	INTEGER	RO

frCircuitグループ

名称	オブジェクト識別子	SYNTAX	ACCESS
frCircuitTable	frame-relay.2	Aggregate	NA
frCircuitEntry	frCircuitTable.1	Aggregate	NA
frCircuitIfIndex	frCircuitEntry.1	INTEGER	RO
frCircuitDlci	frCircuitEntry.2	INTEGER	RO
frCircuitState	frCircuitEntry.3	INTEGER	RO
frCircuitReceivedFECNs	frCircuitEntry.4	INTEGER	RO
frCircuitReceivedBECNs	frCircuitEntry.5	INTEGER	RO
frCircuitSentFrames	frCircuitEntry.6	INTEGER	RO
frCircuitSentOctets	frCircuitEntry.7	INTEGER	RO
frCircuitReceivedFrames	frCircuitEntry.8	INTEGER	RO
frCircuitReceivedOctet	frCircuitEntry.9	INTEGER	RO
frCircuitCreationTime	frCircuitEntry.10	TimeTicks	RO
frCircuitLastTimeChange	frCircuitEntry.11	TimeTicks	RO
frCircuitCommittedBurst	frCircuitEntry.12	INTEGER	RO
frCircuitExcessBurst	frCircuitEntry.13	INTEGER	RO
frCircuitThroughput	frCircuitEntry.14	INTEGER	RO

frErrグループ

名称	オブジェクト識別子	SYNTAX	ACCESS
frErrTable	frame-relay.3	Aggregate	NA
frErrEntry	frErrTable.1	Aggregate	NA
frErrIfIndex	frErrEntry.1	INTEGER	RO
frErrType	frErrEntry.2	INTEGER	RO
frErrData	frErrEntry.3	OctetString	RO
frErrTime	frErrEntry.4	TimeTicks	RO

frame-relay-globals グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
frTrapState	frame-relay-globals.1	INTEGER	RO

■ dot3 グループ

dot3Stats グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
dot3StatsTable	dot3.	Aggregate	NA
dot3StatsEntry	dot3StatsTable.1	Aggregate	NA
dot3StatsIndex	dot3StatsEntry.1	INTEGER	RO
dot3StatsAlignmentErrors	dot3StatsEntry.2	Counter	RO
dot3StatsFCSErrors	dot3StatsEntry.3	Counter	RO
dot3StatsSingleCollisionFrames	dot3StatsEntry.4	Counter	RO
dot3StatsMultipleCollisionFrames	dot3StatsEntry.5	Counter	RO
dot3StatsSQETestErrors	dot3StatsEntry.6	Counter	RO
dot3StatsDeferredTransmissions	dot3StatsEntry.7	Counter	RO
dot3StatsLateCollisions	dot3StatsEntry.8	Counter	RO
dot3StatsExcessiveCollisions	dot3StatsEntry.9	Counter	RO
dot3StatsInternalMacTransmit Errors	dot3StatsEntry.10	Counter	RO
dot3StatsCarrierSenseErrors	dot3StatsEntry.11	Counter	RO
dot3StatsExcessiveDeferrals	dot3StatsEntry.12	Counter	NA
dot3StatsFrameTooLongs	dot3StatsEntry.13	Counter	RO
dot3StatsInRangeLengthErrors	dot3StatsEntry.14	Counter	NA
dot3StatsOutOfRangeLengthFields	dot3StatsEntry.15	Counter	NA
dot3StatsInternalMacReceiveErrors	dot3StatsEntry.16	Counter	RO
dot3StatsEtherChipSe	dot3StatsEntry.17	ObjectID	NA

dot3Coll グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
dot3CollTable	dot3.5	Aggregate	NA
dot3CollEntry	dot3CollTable.1	Aggregate	NA
dot3CollIndex	dot3CollEntry.1	INTEGER	RO
dot3CollCount	dot3CollEntry.2	INTEGER	RO
dot3CollFrequencies	dot3CollEntry.3	Counter	RO

■ snmpDot3RptrMgt グループ

rptr グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
rptrGroupCapacity	rptrRptrInfo.1	INTEGER	RO
rptrOperStatus	rptrRptrInfo.2	INTEGER	RO
rptrHealthText	rptrRptrInfo.3	DisplayString	RO
rptrReset	rptrRptrInfo.4	INTEGER	RO
rptrNonDisruptTest	rptrRptrInfo.5	INTEGER	RO
rptrTotalPartitionedPorts	rptrRptrInfo.6	Gauge	RO

rptrGroup グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
rptrGroupTable	rptrGroupInfo.1	Aggregate	NA
rptrGroupEntry	rptrGroupTable.1	Aggregate	NA
rptrGroupIndex	rptrGroupEntry.1	INTEGER	RO
rptrGroupDescr	rptrGroupEntry.2	DisplayString	RO
rptrGroupObjectID	rptrGroupEntry.3	ObjectID	RO
rptrGroupOperStatus	rptrGroupEntry.4	INTEGER	RO
rptrGroupLastOperStatusChange	rptrGroupEntry.5	TimeTicks	RO
rptrGroupPortCapacity	rptrGroupEntry.6	INTEGER	RO

rptrPort グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
rptrPortTable	rptrPortInfo.1	Aggregate	NA
rptrPortEntry	rptrPortTable.1	Aggregate	NA
rptrPortGroupIndex	rptrPortEntry.1	INTEGER	RO
rptrPortIndex	rptrPortEntry.2	INTEGER	RO
rptrPortAdminStatus	rptrPortEntry.3	INTEGER	RO
rptrPortAutoPartitionState	rptrPortEntry.4	INTEGER	RO
rptrPortOperStatus	rptrPortEntry.5	INTEGER	RO

rptrMonitor グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
rptrMonitorTransmitCollisions	rptrMonitorRptrInfo.1	Counter	RO

rptrMonitorGroup グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
rptrMonitorGroupTable	rptrMonitorGroupInfo.1	Aggregate	NA
rptrMonitorGroupEntry	rptrMonitorGroupTable.1	Aggregate	NA
rptrMonitorGroupIndex	rptrMonitorGroupEntry.1	INTEGER	RO
rptrMonitorGroupTotalFrames	rptrMonitorGroupEntry.2	Counter	RO
rptrMonitorGroupTotalOctets	rptrMonitorGroupEntry.3	Counter	RO
rptrMonitorGroupTotalErrors	rptrMonitorGroupEntry.4	Counter	RO

rptrMonitorPort グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
rptrMonitorPortTable	rptrMonitorPortInfo.1	Aggregate	NA
rptrMonitorPortEntry	rptrMonitorPortTable.1	Aggregate	NA
rptrMonitorPortGroupIndex	rptrMonitorPortEntry.1	INTEGER	RO
rptrMonitorPortIndex	rptrMonitorPortEntry.2	INTEGER	RO
rptrMonitorPortReadableFrames	rptrMonitorPortEntry.3	Counter	RO
rptrMonitorPortReadableOctets	rptrMonitorPortEntry.4	Counter	RO
rptrMonitorPortFCSErrors	rptrMonitorPortEntry.5	Counter	RO
rptrMonitorPortAlignmentErrors	rptrMonitorPortEntry.6	Counter	RO
rptrMonitorPortFrameTooLongs	rptrMonitorPortEntry.7	Counter	RO
rptrMonitorPortShortEvents	rptrMonitorPortEntry.8	Counter	RO
rptrMonitorPortRunts	rptrMonitorPortEntry.9	Counter	RO
rptrMonitorPortCollisions	rptrMonitorPortEntry.10	Counter	RO
rptrMonitorPortLateEvents	rptrMonitorPortEntry.11	Counter	RO
rptrMonitorPortVeryLongEvents	rptrMonitorPortEntry.12	Counter	RO
rptrMonitorPortDataRate Mismatches	rptrMonitorPortEntry.13	Counter	RO
rptrMonitorPortAutoPartitions	rptrMonitorPortEntry.14	Counter	RO
rptrMonitorPortTotalErrors	rptrMonitorPortEntry.15	Counter	RO

rptrAddrTrack グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
rptrAddrTrackTable	rptrAddrTrackPortInfo.1	Aggregate	NA
rptrAddrTrackEntry	rptrAddrTrackTable.1	Aggregate	NA
rptrAddrTrackGroupIndex	rptrAddrTrackEntry.1	INTEGER	RO
rptrAddrTrackPortIndex	rptrAddrTrackEntry.2	INTEGER	RO
rptrAddrTrackLastSourceAddress	rptrAddrTrackEntry.3	OctetString	RO
rptrAddrTrackSourceAddrChanges	rptrAddrTrackEntry.4	Counter	RO
rptrAddrTrackNewLastSrcAddress	rptrAddrTrackEntry.5	OctetString	RO

富士通拡張MIB

■ nosChannelグループ

名称	オブジェクト識別子	SYNTAX	ACCESS
nosChTable	nosChannel.1	Aggregate	NA
nosChEntry	nosChTable.1	Aggregate	NA
nosChIndex	nosChEntry.1	INTEGER	RO
nosChTypeExtension	nosChEntry.2	OCTET STRING	NA
nosChLine	nosChEntry.3	INTEGER	NA
nosChUsage	nosChEntry.10	OCTET STRING	NA
nosChErrorTime	nosChEntry.11	INTEGER	NA
nosChBackupCounters	nosChEntry.12	Counter	NA
nosChBackupFailureCounters	nosChEntry.13	Counter	NA
nosChCongestionTime	nosChEntry.14	INTEGER	NA
nosChCongestionCounters	nosChEntry.15	Counter	NA
nosChLoadsplitCounters	nosChEntry.16	Counter	NA
nosChLoadsplitFailureCounters	nosChEntry.17	Counter	NA
nosChErrorText1	nosChEntry.18	DisplayString	NA
nosChErrorText2	nosChEntry.19	DisplayString	NA
nosChErrorText3	nosChEntry.20	DisplayString	NA
nosChErrorText4	nosChEntry.21	DisplayString	NA
nosChErrorText5	nosChEntry.22	DisplayString	NA
nosChErrorText6	nosChEntry.23	DisplayString	NA
nosChErrorText7	nosChEntry.24	DisplayString	NA
nosChErrorText8	nosChEntry.25	DisplayString	NA
nosChErrorText9	nosChEntry.26	DisplayString	NA
nosChErrorText10	nosChEntry.27	DisplayString	NA
nosChErrorText11	nosChEntry.28	DisplayString	NA
nosChErrorText12	nosChEntry.29	DisplayString	NA
nosChErrorText13	nosChEntry.30	DisplayString	NA
nosChErrorText14	nosChEntry.31	DisplayString	NA
nosChErrorText15	nosChEntry.32	DisplayString	NA
nosChErrorText16	nosChEntry.33	DisplayString	NA
nosChErrorText17	nosChEntry.34	DisplayString	NA
nosChErrorText18	nosChEntry.35	DisplayString	NA
nosChErrorText19	nosChEntry.36	DisplayString	NA
nosChErrorText20	nosChEntry.37	DisplayString	NA
nosChReceivedFrames	nosChEntry.39	Counter	NA
nosChReceivedFcsErrorFrames	nosChEntry.40	Counter	NA
nosChReceivedOtherErrorFrames	nosChEntry.41	Counter	NA
nosChSentFrames	nosChEntry.42	Counter	NA
nosChReceivedOctets	nosChEntry.43	Counter	NA
nosChSentOctets	nosChEntry.44	Counter	NA
nosChReceivedAbortedFrames	nosChEntry.45	Counter	NA
nosChTransmitUnderrunErrs	nosChEntry.46	Counter	NA
nosChReceivedOverrunErrs	nosChEntry.47	Counter	NA
nosChUnderrunAndOverrunErrs	nosChEntry.48	Counter	NA
nosChReceivedBufferErrs	nosChEntry.49	Counter	NA
nosChTransmitBufferErrs	nosChEntry.50	Counter	NA
nosChReceivedBufferOverFlows	nosChEntry.51	Counter	NA
nosChTransmitBufferOverFlows	nosChEntry.52	Counter	NA
nosChType	nosChEntry.53	INTEGER	RO
nosChSpeed	nosChEntry.54	INTEGER	RO
nosChStatus	nosChEntry.55	INTEGER	RO
nosChSlotid	nosChEntry.56	INTEGER	NA

■ nosPortExt1 グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
nosPortExt1Table	nosPortExt1.1	Aggregate	NA
nosPortExt1Entry	nosPortExt1Table.1	Aggregate	NA
nosPortExt1Index	nosPortExt1Entry.1	INTEGER	RO
nosPortExt1UsualTarget	nosPortExt1Entry.2	OCTET STRING	RO
nosPortExt1BackupTarget	nosPortExt1Entry.3	OCTET STRING	RO
nosPortExt1LoadsplitTarget	nosPortExt1Entry.4	OCTET STRING	RO
nosPortExt1CurrentTarget	nosPortExt1Entry.5	OCTET STRING	RO
nosPortExt1UsualChannel	nosPortExt1Entry.6	OCTET STRING	RO
nosPortExt1BackupChannel	nosPortExt1Entry.7	OCTET STRING	RO
nosPortExt1LoadsplitChannel	nosPortExt1Entry.8	OCTET STRING	RO
nosPortExt1CurrentChannel	nosPortExt1Entry.9	OCTET STRING	RO
nosPortExt1CallOperStatus	nosPortExt1Entry.10	INTEGER	RO
nosPortExt1CallAdminStatus	nosPortExt1Entry.11	INTEGER	RW

■ nosTarget グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
nosTargetTable	nosTarget.1	Aggregate	NA
nosTargetEntry	nosTargetTable.1	Aggregate	NA
nosTargetIndex	nosTargetEntry.1	INTEGER	RO
nosTargetRemoteSnpaAddress	nosTargetEntry.2	OCTET STRING	RO
nosTargetReservedRemote SnpaAddress	nosTargetEntry.3	OCTET STRING	NA
nosTargetRemoteSubAddress	nosTargetEntry.4	OCTET STRING	RO
nosTargetReservedRemote SubAddress	nosTargetEntry.5	OCTET STRING	NA
nosTargetMaxRetryCalling	nosTargetEntry.6	INTEGER	RO
nosTargetCallingPriority	nosTargetEntry.7	INTEGER	RO
nosTargetIdleStatusTime	nosTargetEntry.8	INTEGER	RO
nosTargetCallSetupTime	nosTargetEntry.9	DisplayString	RO
nosTargetCallClearTime	nosTargetEntry.10	DisplayString	RO
nosTargetTotalTime	nosTargetEntry.11	INTEGER	RO
nosTargetTotalCharge	nosTargetEntry.12	INTEGER	RO
nosTargetCallSetupCounters	nosTargetEntry.13	Counter	RO
nosTargetCallErrorCounters	nosTargetEntry.14	Counter	RO
nosTargetCallBusyCounters	nosTargetEntry.15	Counter	RO
nosTargetJoinedChannel	nosTargetEntry.16	OCTET STRING	RO

■ nosCallLimiter グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
nosCallLimiterTable	nosCallLimiter.1	Aggregate	NA
nosCallLimiterEntry	nosCallLimiterTable.1	Aggregate	NA
nosCallLimiterIndex	nosCallLimiterEntry.1	INTEGER	RO
nosCallLimiterRemoteSnpa Address	nosCallLimiterEntry.2	OCTET STRING	RO
nosCallLimiterRemoteSnpa SubAddress	nosCallLimiterEntry.3	OCTET STRING	RO
nosCallLimiterMaxPeriod	nosCallLimiterEntry.4	INTEGER	RO
nosCallLimiterCurrentPeriod	nosCallLimiterEntry.5	INTEGER	RO
nosCallLimiterLastPeriod	nosCallLimiterEntry.6	INTEGER	RO
nosCallLimiterStatus	nosCallLimiterEntry.7	INTEGER	RO

■ nonosSystem グループ

名称	オブジェクト識別子	SYNTAX	ACCESS
nosResetSystem	nonosSystem.1	INTEGER	RW

Trap一覧

特定の情報については、trapという機能を用いてエージェントからマネージャに対して非同期通知を行うことができます。エージェントは、事象が発生したときにtrapを送信します。

以下に、サポートしているtrapを説明します。

- Coldstart
  本装置の起動時および再起動時に1回だけ通知します。
- LinkUp
  本装置の通信リンクの中のどれかがUP状態になったときに、SNMPマネージャに対してに通知します。
- LinkDown
  本装置の通信リンクに障害があったときに、SNMPマネージャに対してに通知します。
  また、装置の起動時、再起動時、構成定義反映時にも送信される場合があります。
- AuthenticationFailure
  SNMPのコミュニティの認証に失敗したときに、SNMPマネージャに対して通知します。
- NewRoot
  本装置がルートブリッジになるときに、SNMPマネージャに対して通知します。
- TopologyChange
  本装置がLearning状態からForwarding 状態に、またはForwarding状態からBlocking状態に変更するときに、SNMPマネージャに対して通知します。

索引

記号

B

C

D

E

F

G

H

I

L

M

N

P

R

S

T

U

V

W

あ

い

え

お

そ

た

ち

つ

て

と

な

に

ね

は

ひ

ふ

へ

Si-R130B 取扱説明書

P3NK-3262-01Z0

発行日　　2008年10月

発行責任　　富士通株式会社

Printed in Japan

■ 警告表示について

危害や損害の内容を示すために、以下の記号を使用しています。

記号	記号の意味
	△ で表示された記号は、警告や注意事項を示しています。記号の中やその脇には、具体的な内容が記載されています。
	○ で表示された記号は、してはいけない禁止行為を示しています。記号の中やその脇には、具体的な内容が記載されています。
	● で表示された記号は、必ず従っていただく行為の強制、指示を示しています。記号の中やその脇には、具体的な内容が記載されています。

⚠注意　正しく使用しない場合、軽傷または中程度の傷害を負うおそれがあることを示します。
また、本装置や本装置に接続している機器に損害を与えるおそれがあることを示します。

注意事項			
 禁止	本装置を薬品の噴霧気中や薬品の触れる場所など腐食性ガス発生環境下では使用しないでください。破損・故障の原因となります。	 注意	装置への結露は破損・故障の原因となりますので結露を防止してください。
 禁止	外気が直接流入する場所に装置を設置すると粉塵等の影響により破損/ 故障の原因となります。	 禁止	噴霧式加湿器が噴霧する水滴中の不純物が乾燥すると白粉となって、機器内部に付着するため、不純物の含まれない水を使用してください。 破損・故障の原因となります。
 禁止	潮風に含まれる塩分は絶縁不良や部材の腐食劣化の原因となるため、製品は海岸から離れた場所に設置を行ってください。 破損・故障の原因となります。	 注意	浸水、雨漏り、給水配管の漏れ等がない場所に設置してください。
 注意	粉末消火剤や泡消火材は、機器や媒体を汚損するリスクがあるため、使用する消火剤は、機器影響の少ない消火剤等の使用を推奨いたします。	 注意	鼠の侵入による信号ケーブルや電源ケーブルのかじりによる誤動作、断線、漏電、絶縁不良を防止するため、侵入するような隙間や穴を塞いでください。

■ セキュリティの確保について

パスワードを設定しない場合、ネットワーク上のだれからでも本装置の設定を行うことができます。セキュリティの面からは非常に危険なため、パスワードは必ず設定してください。また、設定したパスワードは定期的に変更するようにしてください。

コマンドラインインタフェースまたはWebブラウザを操作して、本装置の設定・運用を行う設定用パソコンは、本装置にアクセスができるネットワーク上のどこに配置してもご利用いただけますが、セキュリティの面から外部からのアクセスができない運用管理専用に敷設されたネットワーク上に配置してください。

このような運用管理専用ネットワークがない場合は、本装置にアクセスできるパソコンを制限するなどのセキュリティ対策を行ってください。

☛ 参照 「装置を保護する」

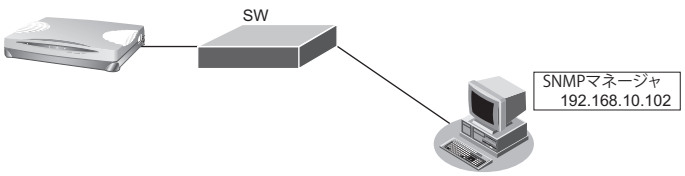
装置を保護する

本装置に対するセキュリティ対策として、以下の設定を行います。

- 管理者(admin)用パスワードの設定
- オートログアウトの設定
- SNMP接続に対するアクセス制限

設定例

以下にそれぞれの設定を行う場合の例を示します。



● 設定条件

- 管理者(admin) パスワード　：sir_admin-2022
- IPアドレス　：192.168.10.100/24
- オートログアウトの設定（ログインしたままの状態で指定時間無操作だった際に自動切断を行う）
  コンソールのオートログアウト時間　：5分
  Telnetのオートログアウト時間　：5分
- SNMP設定
  アクセス許可するSNMPマネージャ　：192.168.10.102
  コミュニティ名　：private
  マネージャからの書き込み　：許可しない

```
adminパスワードをsir_admin-2022に設定
# password set sir_admin-2022

コンソール接続のオートログアウト時間を5分に設定
# consoleinfo autologout 5m

Telnetのオートログアウト時間を5分に設定
# telnetinfo autologout 5m

自装置IPアドレスの設定
# lan 0 ip address 192.168.10.100/24 3

SNMPを有効、コミュニティ名をprivate、書き込み許可しない
# snmp service on
# snmp manager 0 192.168.10.102 private on disable

設定終了
# save
# enable
```