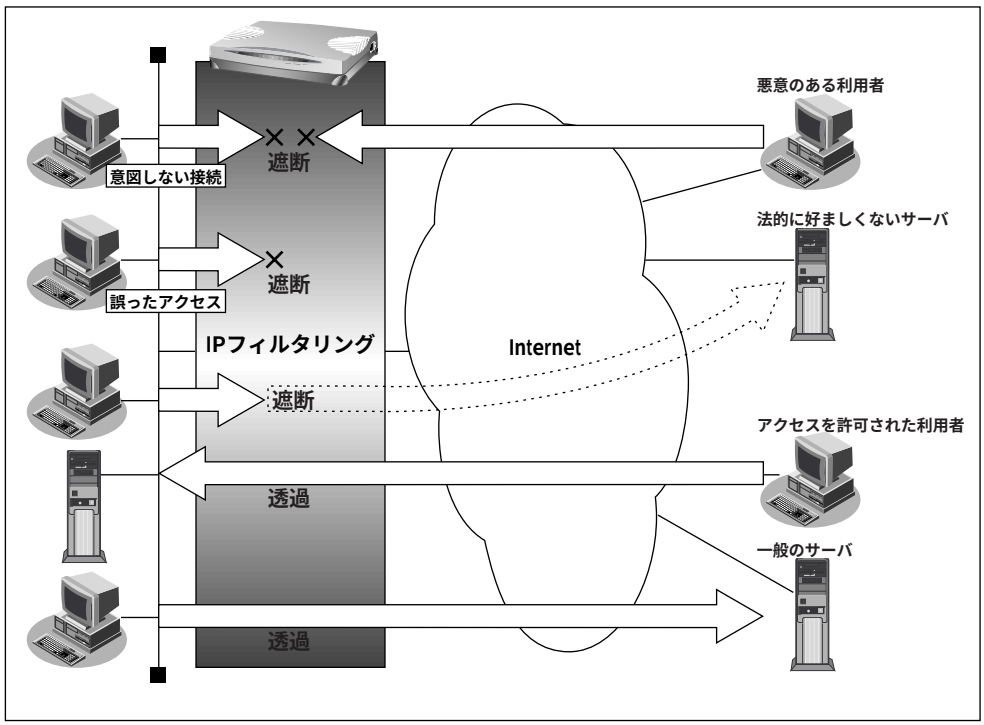
第６章　活用例（ルータ設定）

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り、ネットワークのセキュリティを向上させたり、回線への異常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、次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、パスワードを設定したり「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.356）

■ 接続形態に応じたセキュリティ方針を決める

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」流れるデータ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ておく

- 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」流れるデータ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フィルタリング機能は「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、以下のような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

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通信だけ対象**
	TCP	**TCP通信だけ対象**
	ICMP	**ICMP通信（PINGコマンド）だけ対象**
	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対象外**

ヒント

◆ 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。

フィルタリングの動作に透過、TCP接続要求に対象外を指定した場合、コネクション要求だけを禁止する設定となり、対象となるアドレスからコネクション接続を禁止できます。

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。

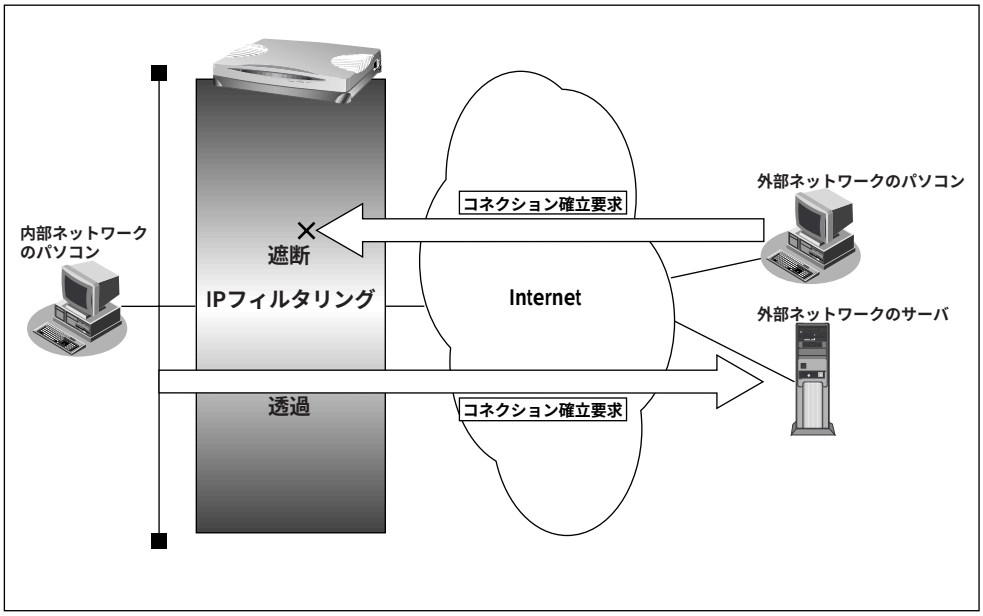
制御フラグ		TCPパケットの内容
SYN	ACK	
1	0	コネクションの確立要求
1	1	確立後の承認応答
0	1	確認応答、通常のデータ

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うことが分かります。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行えます。

以下に、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透過



◆IPアドレスとアドレスマスクの決め方

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。

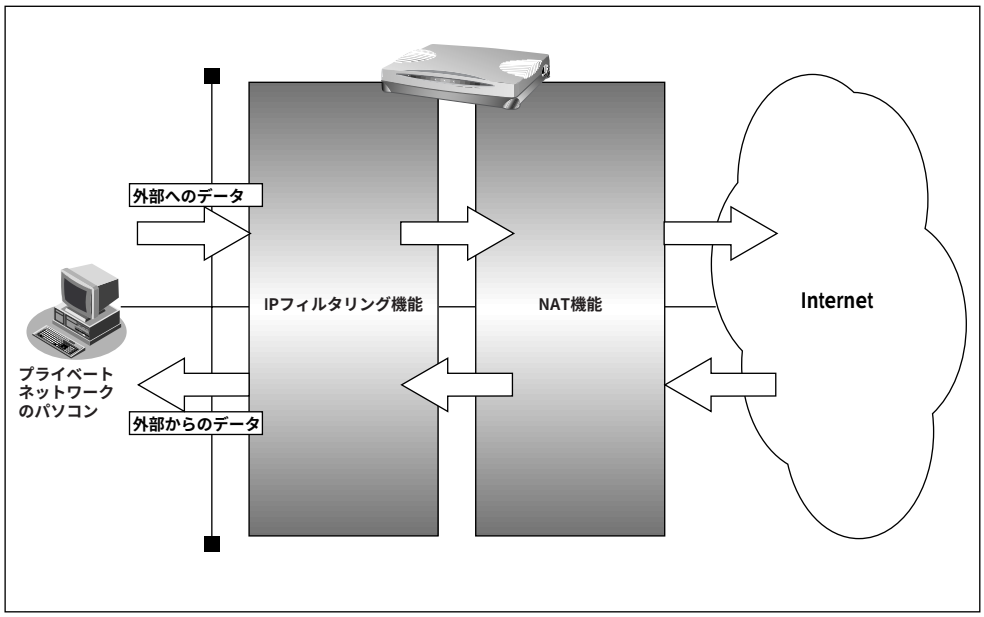
☛ 参照 「用語集」（P.601）

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後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として「TCP」または「すべて」を選択した場合だけ有効です。それ以外のプロトコルでは意味がありません。以下の設定例では、TCP 接続要求の設定項目に関しては、プロトコルが「TCP」または「すべて」の場合だけ説明を記述します。

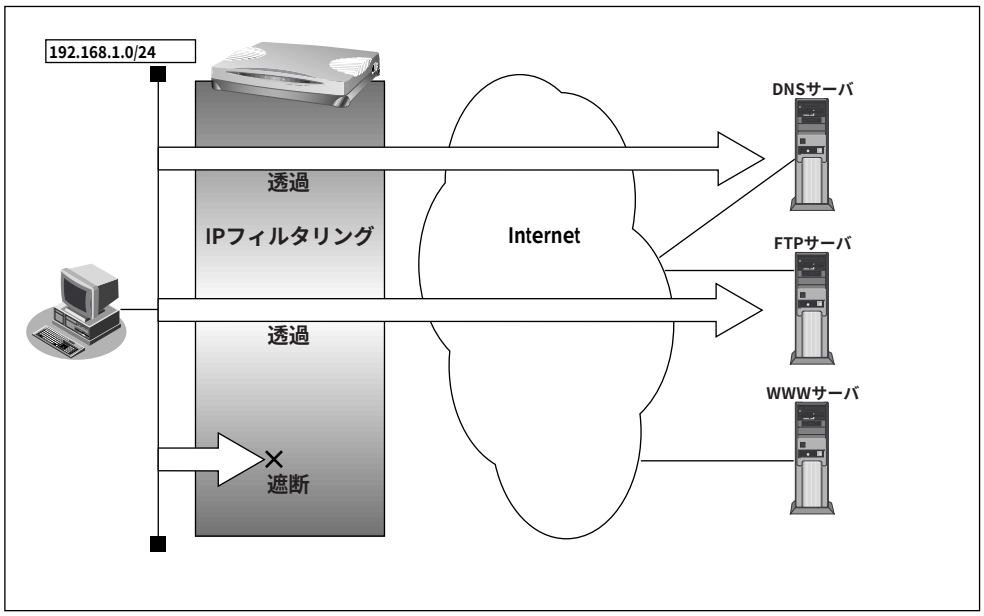
こんな事に気をつけて

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、他のサーバ（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のサーバへのアクセスを許可
- その他はすべて遮断

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

- 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

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、以下の情報を設定します。

[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

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、以下の情報を設定します。

[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

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、以下の情報を設定します。

［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

残りのパケットをすべて遮断する

9.　手順3.～5.を参考に、以下の情報を設定します。

［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

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。

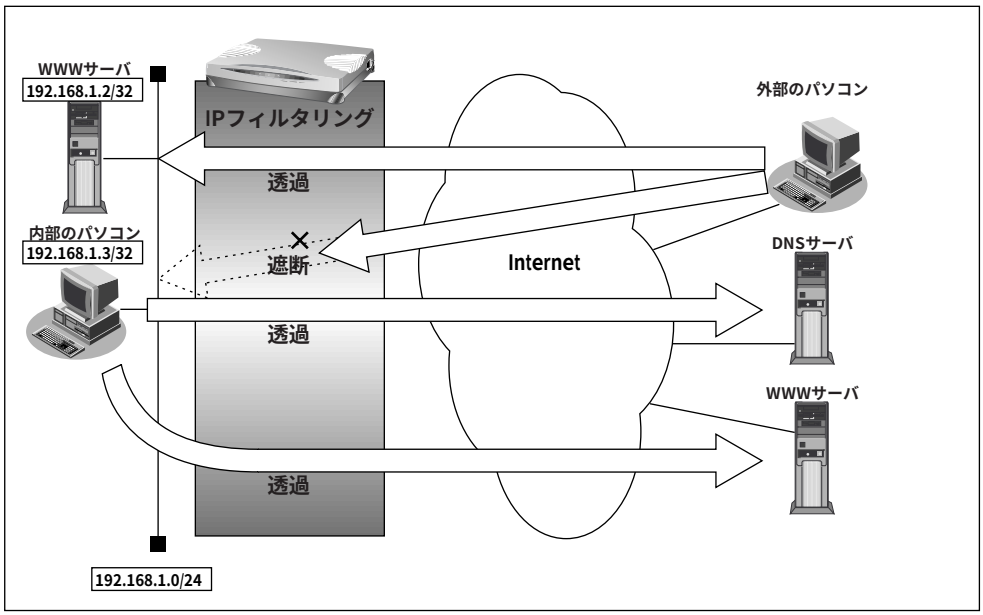
11.　［更新］ボタンをクリックします。

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。

■ 外部から特定サーバへのアクセスだけ許可する

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上の他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上の他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、そのアクセスには特に制限はつけません。



● フィルタリング設計

- LAN上のホスト（192.168.1.2/32）をWWWサーバとして利用することを許可
- 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のサーバへのアクセスは許可
- その他はすべて遮断

● 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
- 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

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側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、以下の情報を設定します。

[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

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、以下の情報を設定します。

[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

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、以下の情報を設定します。

[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

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、以下の情報を設定します。

[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

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、以下の情報を設定します。

[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

残りのパケットはすべて遮断する

11.　手順3.～5.を参考に、以下の情報を設定します。

[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

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。

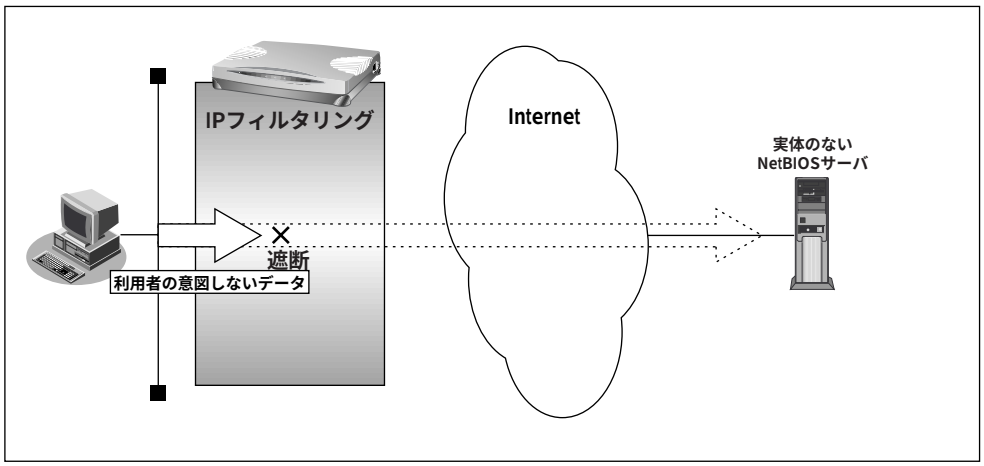
14.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

■ 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、回線に対する無駄な発信を抑止するフィルタリング設定方法について説明します。



● 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無駄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禁止する

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

5.　［更新］ボタンをクリックします。

「ネットワーク情報設定」ページへ戻ります。

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、以下の情報を設定します。

[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

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。

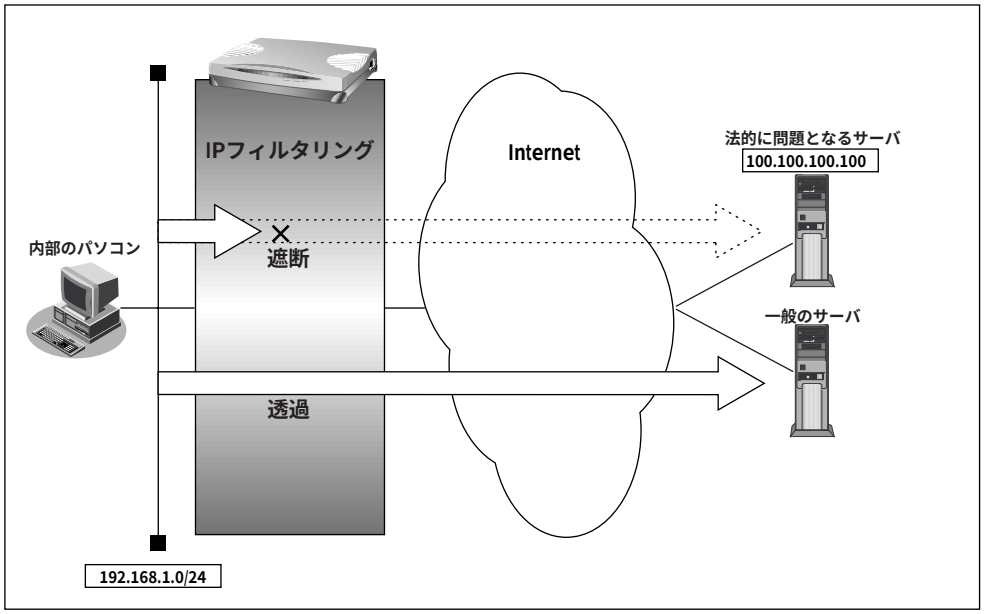
8.　［更新］ボタンをクリックします。

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について説明します。



● 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する

● 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

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。

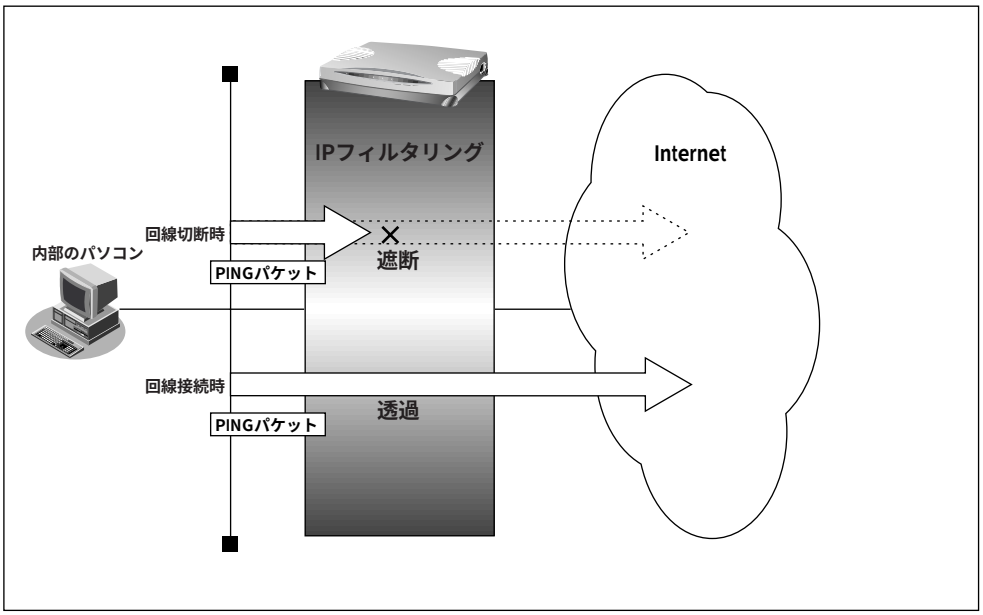
8.　［設定反映］ボタンをクリックします。

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り、意図しないPINGによる無駄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だけICMPパケットを透過させる場合の設定方法について説明します。

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だけPINGを許可には

(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。

回線接続中だけ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

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。

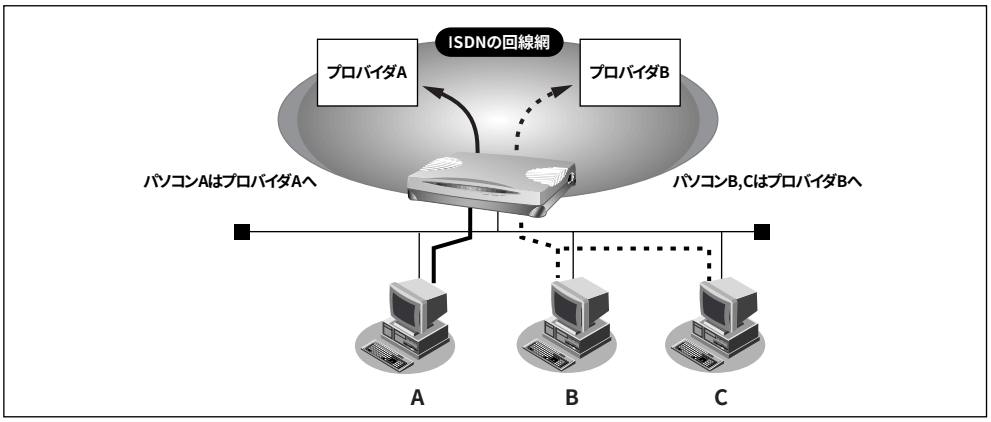
- パソコンごとに別々のプロバイダを利用する（ソースアドレスルーティング機能）
- 目的ごとに別々のプロバイダに接続する（ポートルーティング機能）
- 課金単位でプロバイダを切り替える

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。

例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。

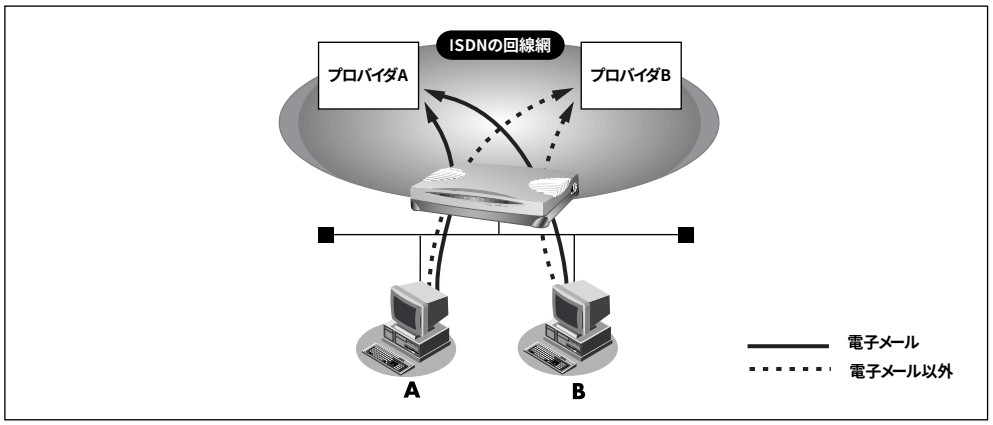


☛ 参照 「複数プロバイダと端末型接続する」（P.116）

■ 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。

例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も可能です。



● 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.344）

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。

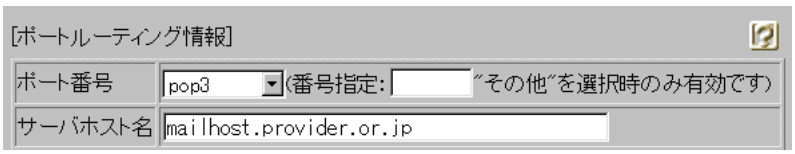
4.　［マルチルーティング］の「ポートルーティング」で［追加］ボタンをクリックします。

「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。

例えば、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だとします。

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

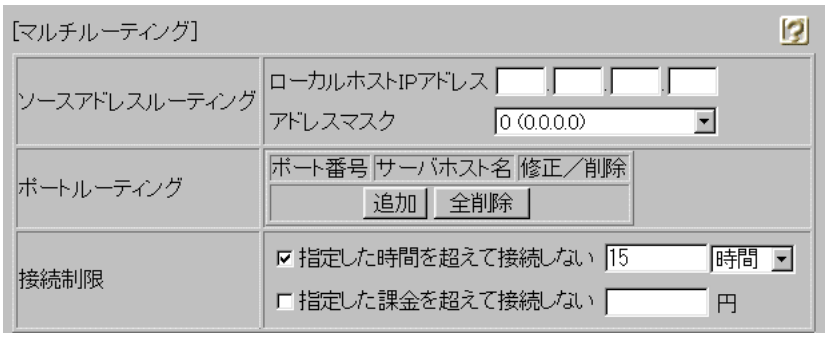
接続先には優先度があるため、マルチルーティングの設定をしない接続先の優先度を高くすると、優先度の低いマルチルーティング設定は無効となります。接続先の優先順位に気をつけてください。

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。**

DNSサーバを使いこなす（ProxyDNS）

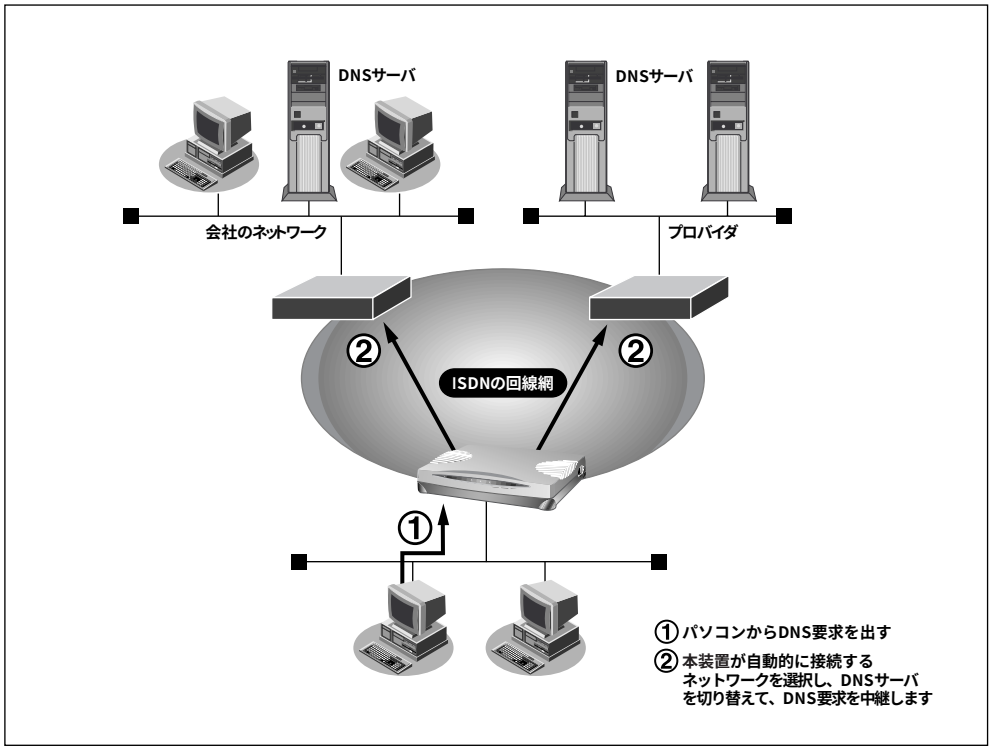
本装置のProxyDNSには、以下の機能があります。

- DNSサーバの自動切り替え機能
- 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、パソコン側で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ありません。パソコン側が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、会社のネットワークとプロバイダに接続する設定がすでに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。

- IP アドレス　→ 172.16.0.0
- アドレスマスク　→ 16（255.255.0.0）
- 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。

internet の ProxyDNS 情報を設定する

8.　手順 2. ～ 4. を参考に、以下の情報を設定します。

［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、以下の情報を設定します。

［ProxyDNS 情報設定（逆引き）］

- IP アドレス　→ なにも指定しない
- アドレスマスク　→ 0（0.0.0.0）
- 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.69）

パソコン側の設定を行う

ここではWindows® 98の場合を例に説明します。

1. **［コントロールパネル］ウィンドウで［ネットワーク］アイコンをダブルクリックします。**
2. **［ネットワーク］ダイアログボックスで［ネットワークの設定］タブをクリックします。**
3. **一覧から「TCP/IP」を選択し、［プロパティ］ボタンをクリックします。**
4. **［TCP/IPのプロパティ］画面で［DNS設定］タブをクリックします。**
5. **「DNSを使う」を選択します。**
6. **「DNSサーバーの検索順」に、本装置のIPアドレスを入力します。**

補足 必要に応じて、ホスト名にパソコンの名前（任意）を入力します。

7. **［OK］ボタンをクリックします。**
8. **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機能が有効になってます。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機能だけ利用できます。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DNSサーバのアドレスを回線の接続時に接続先より自動的に取得するため、DNSサーバのアドレスをあらかじめ設定しておく必要がなくなります。

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利用できます。

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。

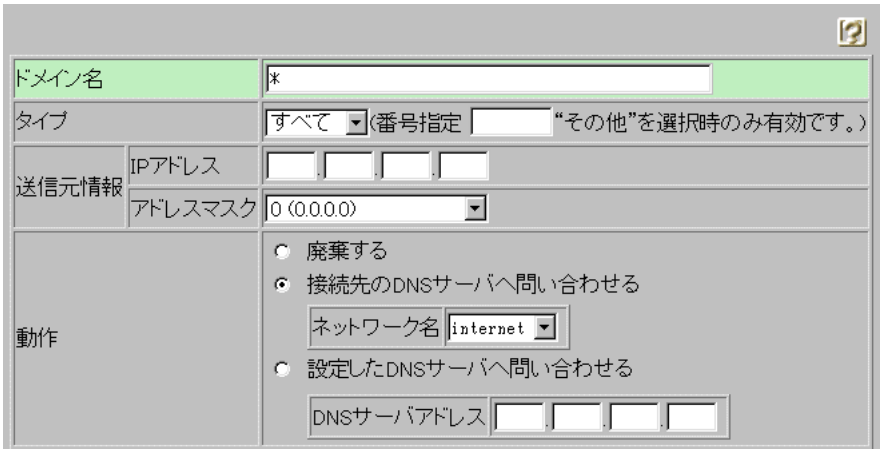
「ProxyDNS情報」ページが表示されます。

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　→ 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「パソコンの設定を行う」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。
例えば、Windows® 2000が送信する予期せぬDNSパケットにより自動発信してしまう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」に設定した場合は、問い合わせタイプがSOA（6）とSRV（33）のパケットは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.69）

こんな事に気をつけて

ProxyDNS機能を使用する場合、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にすると、正常な通信が行えない状態になります。

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示します。

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。

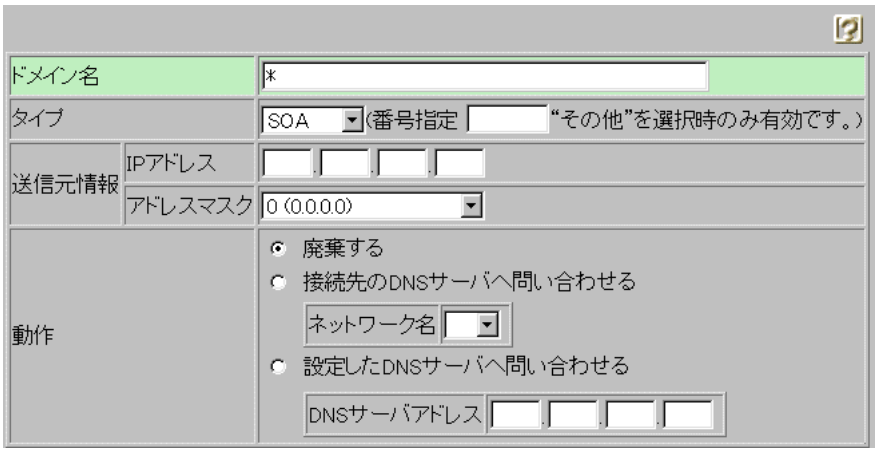
「ProxyDNS情報」ページが表示されます。

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「パソコンの設定を行う」を参照して、パソコンの設定を行います。

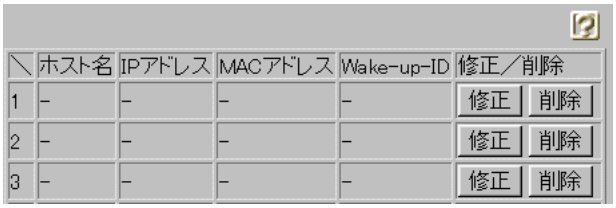
■ DNSサーバ機能

本装置のホストデータベースにホスト名とIPアドレスのペアを登録しておきます。登録されたホストに対する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	修正／削除
1	-	-	-	-	修正 削除
2	-	-	-	-	修正 削除
3	-	-	-	-	修正 削除

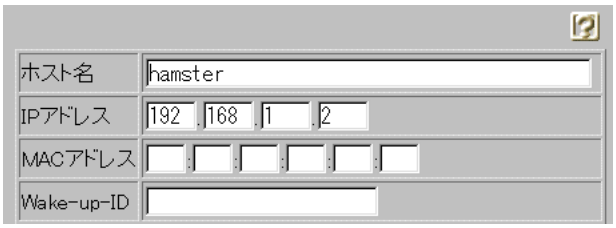
2.　未設定の欄の［修正］ボタンをクリックします。

「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　　→パソコンの名前
- IPアドレス　　→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設定します。



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

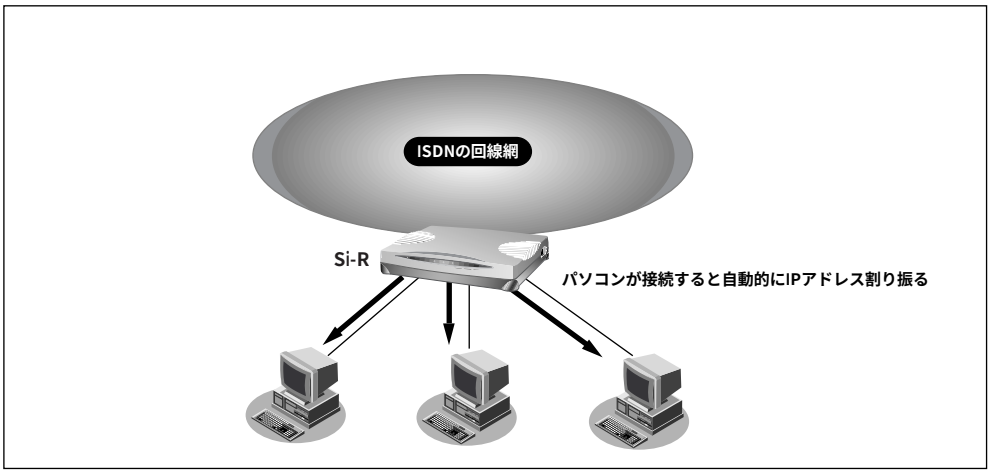
「DNSサーバの自動切り替え機能」の「パソコンの設定を行う」を参照して、パソコンの設定を行います。

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が設定する必要がありますが、この機能を利用するとDHCPクライアント機能を持つパソコンには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アドレスは自動的に再利用します。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。

本装置では、IPアドレスとMACアドレスを対応づけることによって、登録されたパソコンからDHCP要求が発行されると、常に同じIPアドレスを割り当てることができます。これを「DHCPスタティック機能」といいます。

DHCPスタティック機能を利用する場合は、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サーバ機能の併用を実現するために、「DHCPスタティック機能」をサポートしています。

■ DHCP サーバ機能を使う

DHCP サーバ機能を使う場合を例に説明します。

● 設定条件

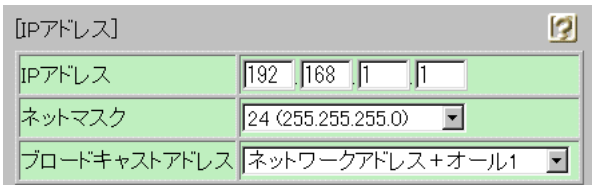
- 本装置の IP アドレス　：192.168.1.1
- DHCP サーバ機能を使用する
- パソコンに割り当てる IP アドレス　：192.168.1.2 ～ 192.168.1.33
- パソコンに割り当てる IP アドレス数　：32 個
- LAN 側のネットワークアドレス/ネットマスク　：192.168.1.0/24

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。

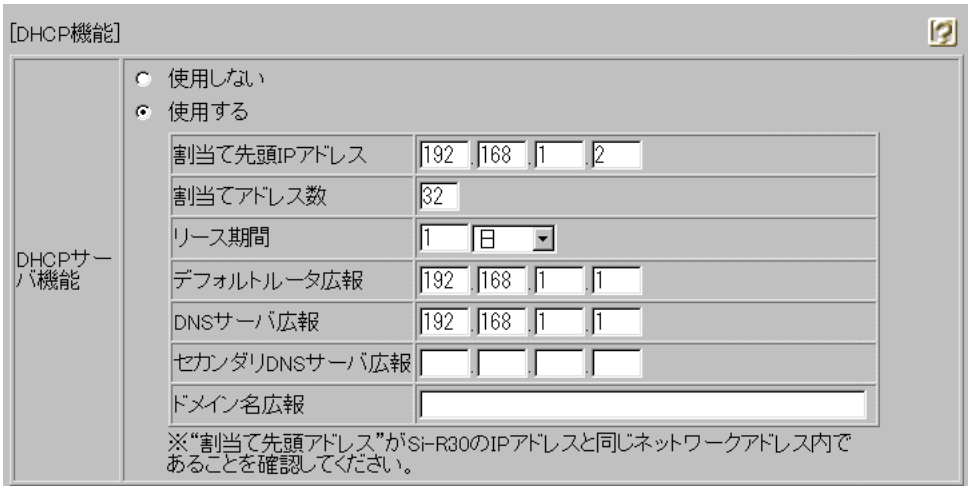
- IP アドレス　→ 192.168.1.1（本装置の LAN 側の IP アドレス）
- ネットマスク　→ 24
- ブロードキャストアドレス　→ ネットワークアドレス + オール 1



［DHCP機能］で以下の項目を指定します。

- DHCPサーバ機能　→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　→32

補足 DHCPサーバ機能で割り当てることのできる最大数は32個です。



必要に応じて上記以外の項目を設定します。

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 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。

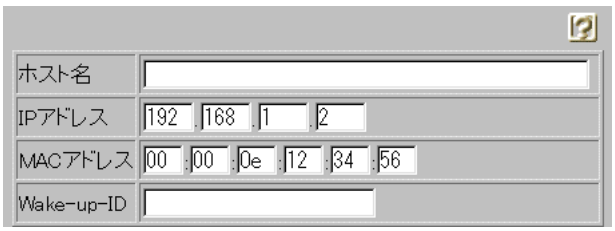
2.　未設定の欄の［修正］ボタンをクリックします。

「ホストデータベース情報設定」ページが表示されます。

3.　以下の項目を設定します。

- 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設定します。



必要に応じて上記以外の項目を設定します。

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。

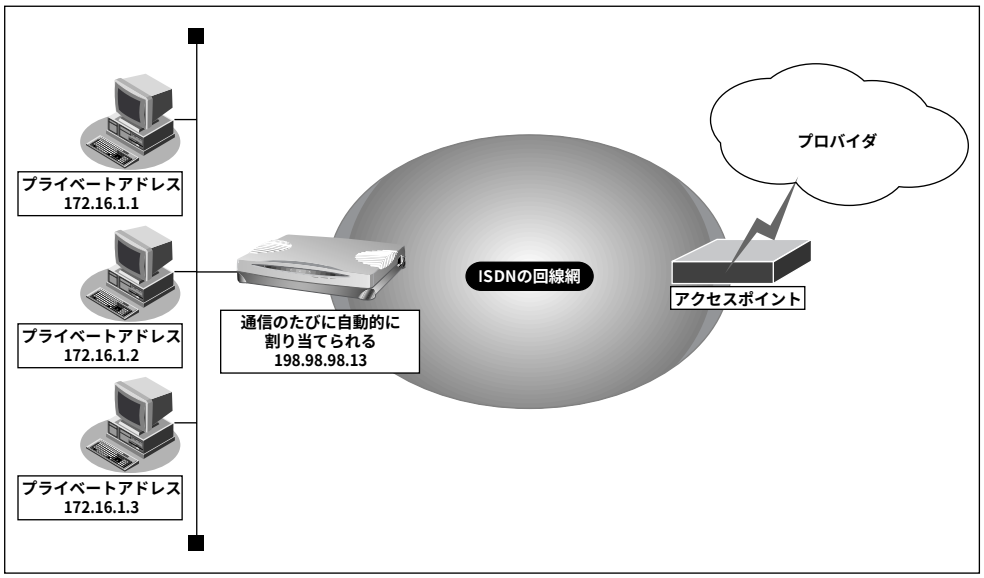
5.　［設定反映］ボタンをクリックします。

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 32 個です。

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。例えば、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、LAN内に接続されたパソコンのプライベートアドレスは外部からわからないため、外部からの不正なアクセスを遮断できます。



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いいます。
- 「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。

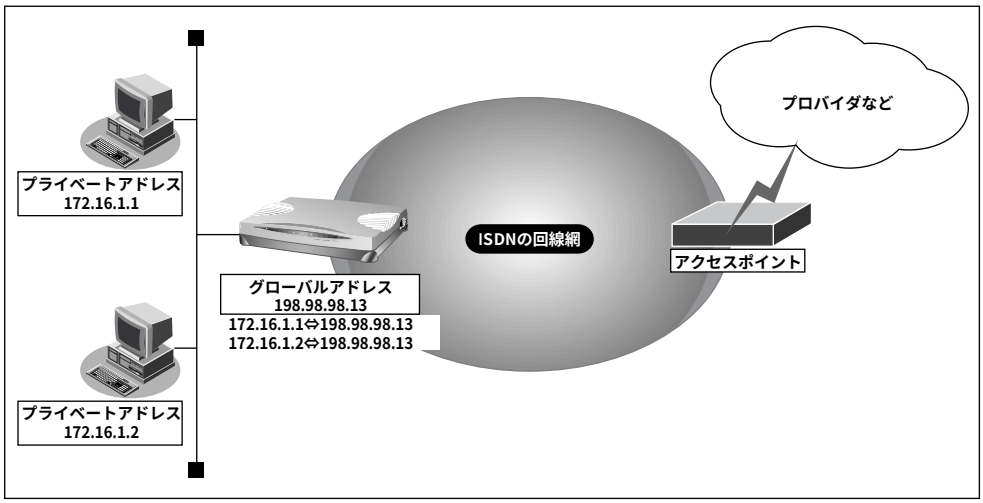
こんな事に気をつけて

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ので、ご注意ください。

ヒント

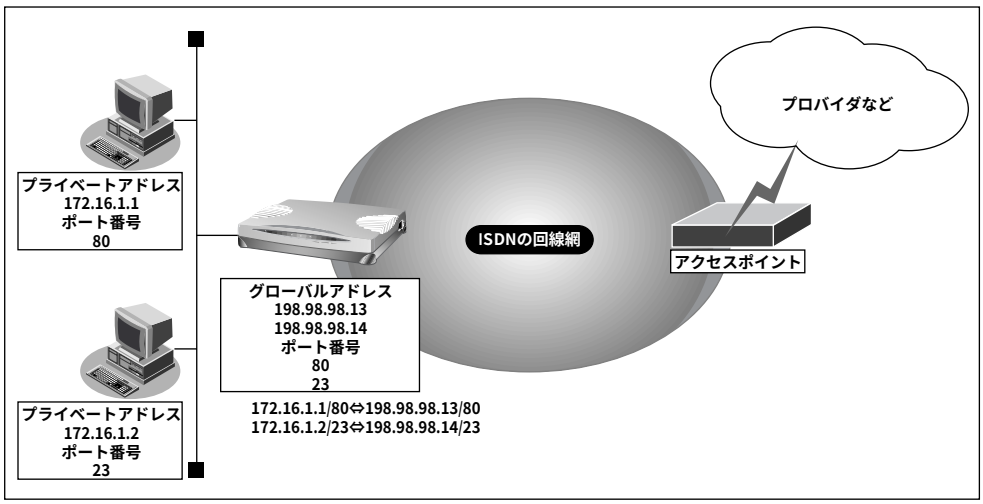
◆動的NATとは

基本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に対応づけます。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」を使えば、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機能は、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」を使えば、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、この問題が解決できます。



■ 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

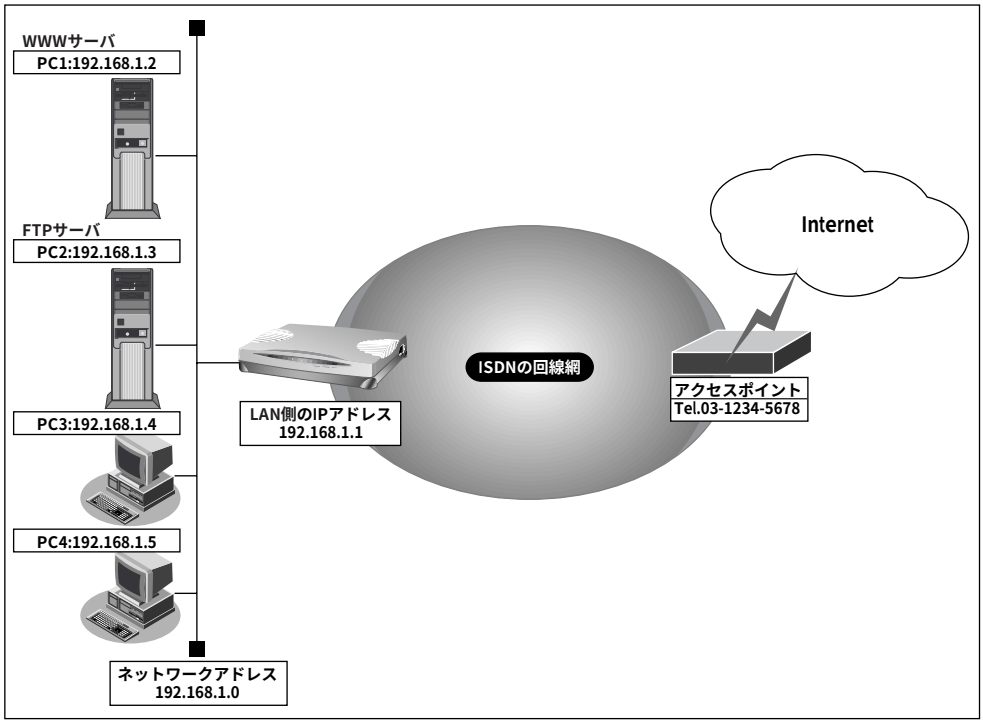
- 端末型ダイヤルアップ接続で、同時に複数のパソコンから接続する場合
- 同時に接続するパソコンの台数がグローバルアドレス数を超える場合

●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.600）」を参照してください。

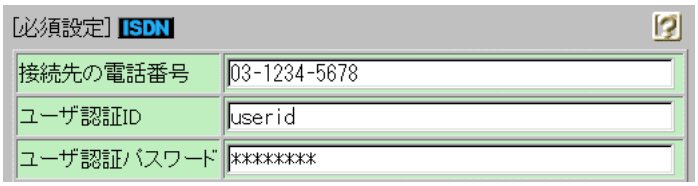
かんたん設定でダイヤルアップ接続の情報を設定する

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、通信が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］で以下の項目を設定します。

- 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 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 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。

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、以下の情報を設定します。

- 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機能	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機能	接続台数制限なし 最大256セッションまで	外部からの通信は不可能
静的NAT機能	最大32個まで割り当て可能 ＋動的NAT	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

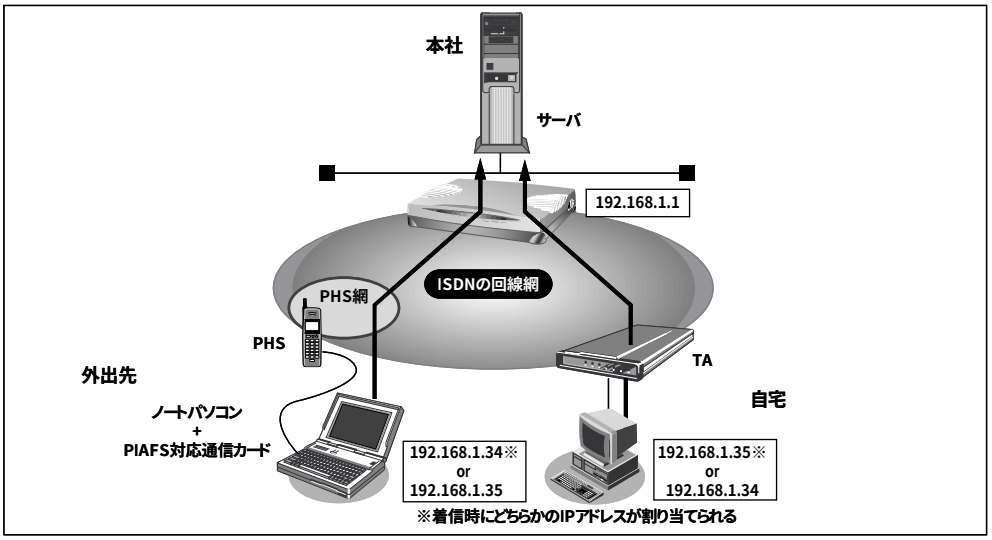
外部のパソコンから着信接続する（アクセスサーバ機能）

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.125）

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

- 認証IDと認証パスワード

  受諾認証　：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

- 認証IDと認証パスワード

  受諾認証　：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

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。

本装置を使ってセキュリティを向上させる方法としては、次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。

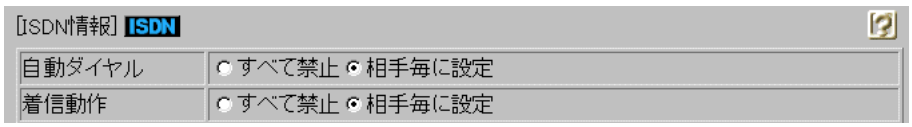
「回線情報設定」ページが表示されます。

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設定します。

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設定します。

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設定します。

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>の情報も追加してください。

- 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。

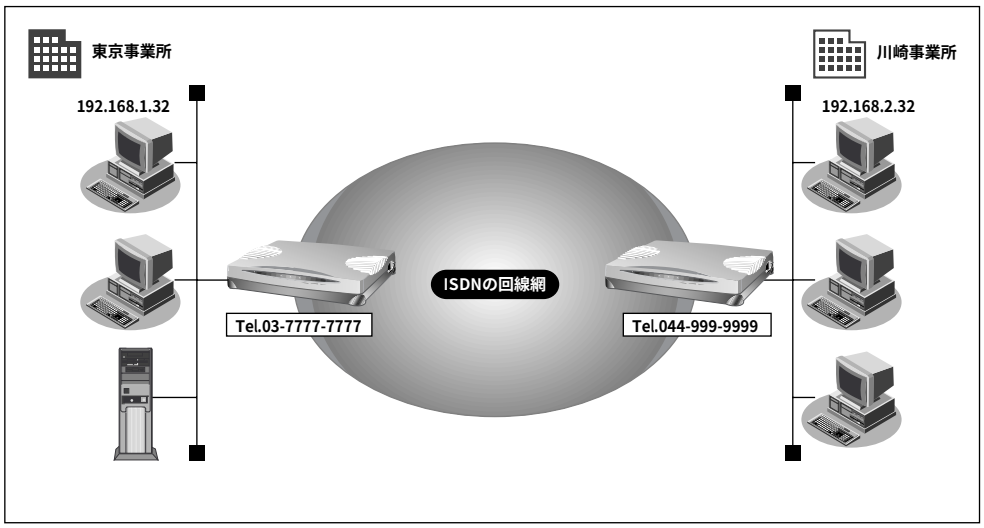
設定した内容が有効になります。

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っています。
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利用することにより、認証IDによる接続相手の識別が必要となります。
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どうしをISDNで接続する」（P.104）

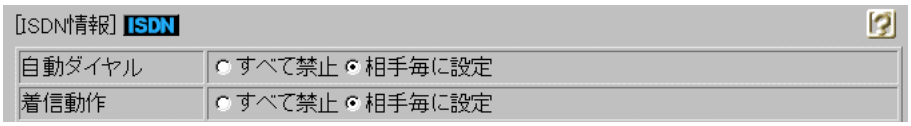
回線接続情報（東京事業所）を設定する

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設定します。

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設定します。

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。

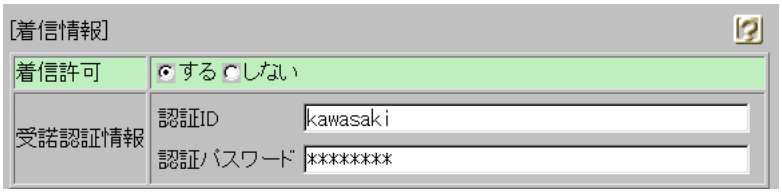
「ネットワーク情報設定」ページが表示されます。

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設定します。

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。

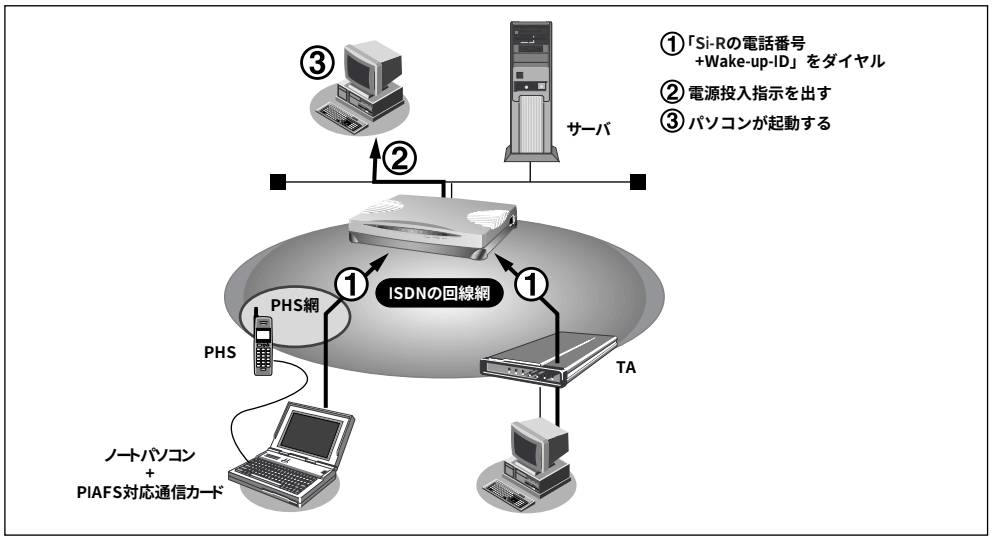
設定した内容が有効になります。

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利用できません。



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利用できます。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）で利用できます。
- 本機能を使用するだけでは、課金されません。

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。

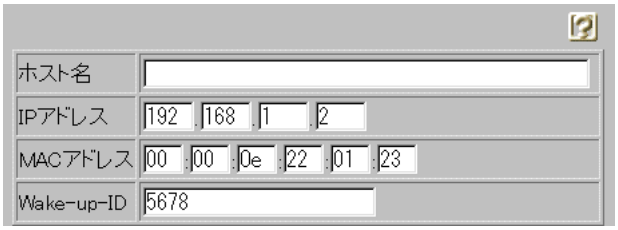
「ホストデータベース情報」ページが表示されます。

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　→起動させるパソコンの MAC アドレス
- Wake-up-ID　→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設定します。

☛ 参照　MAC アドレス→「本装置 底面」（P.31）

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。

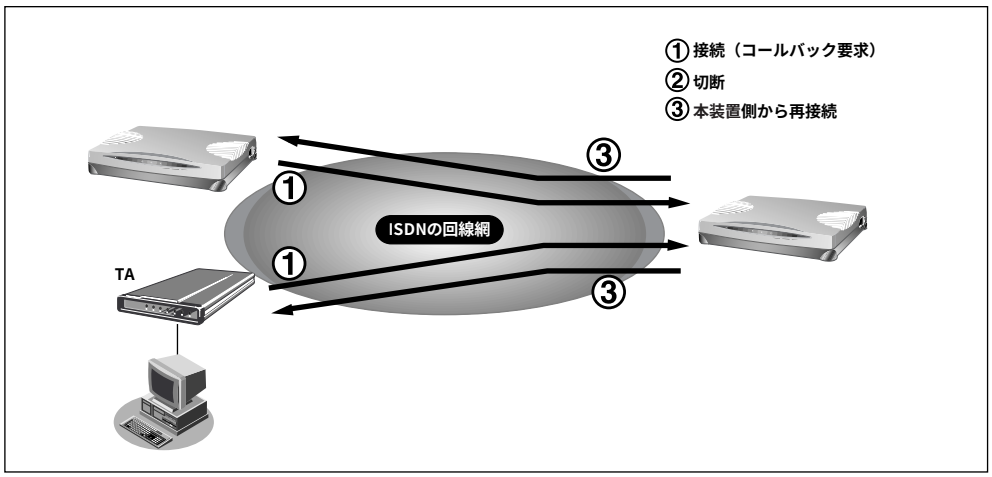
2.　相手先サブアドレスに、起動させるパソコンの「Wake-up-ID」を指定します。

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

本装置には「コールバック機能」があります。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後、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。



本装置には次の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® 3.51/4.0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、発信側にまったく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。

以下にコールバック機能を利用した設定例を記述します。

(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

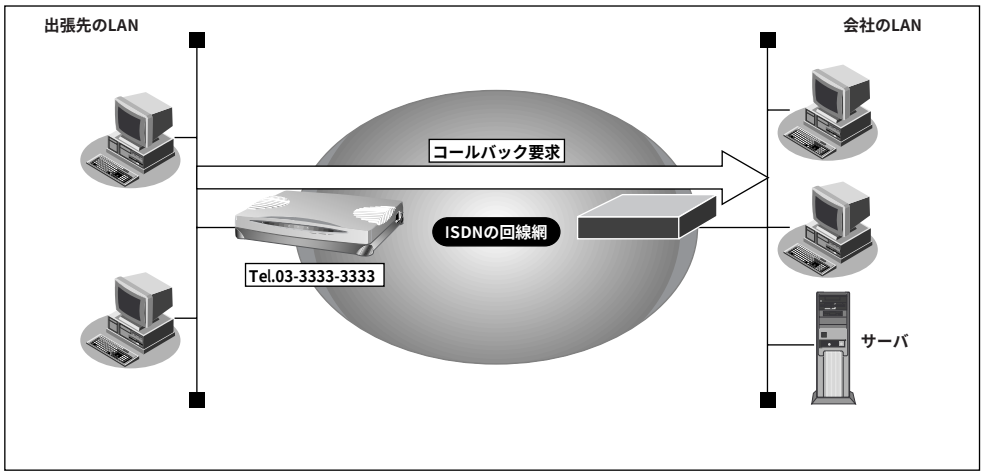
(3)無課金コールバックでコールバック要求する

(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。

■ 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例について説明します。



● 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.120)

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。

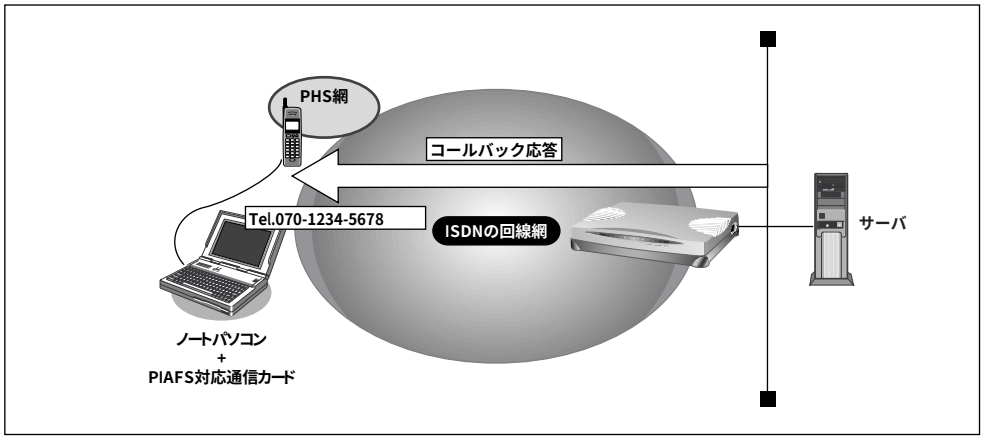
7.　［更新］ボタンをクリックします。

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

出張先から会社のサーバに＜ノートパソコン＋PHS＞からアクセスがあった場合に、コールバック応答する例について説明します。



● 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.125）

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。

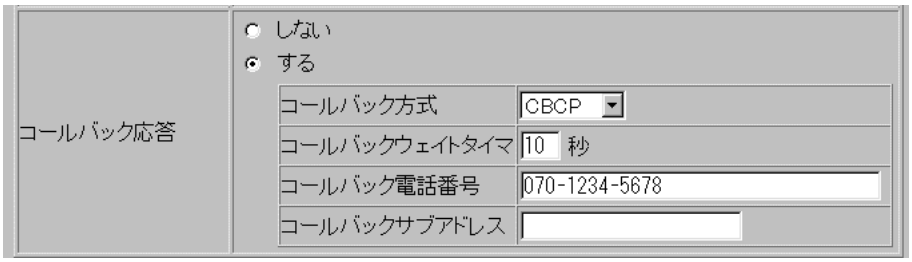
「ネットワーク情報設定」ページが表示されます。

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。

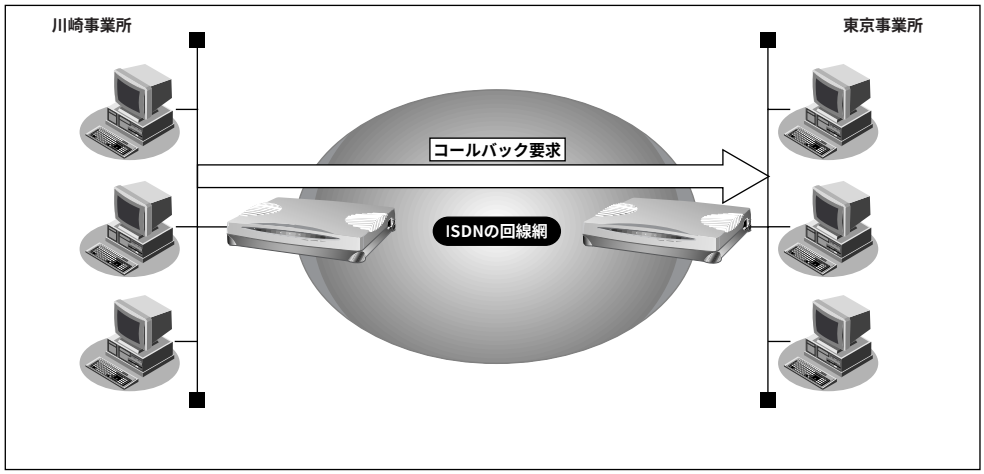
8.　［設定反映］ボタンをクリックします。

設定した内容が有効になります。

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.364）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どうしをISDNで接続する」(P.104)

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。

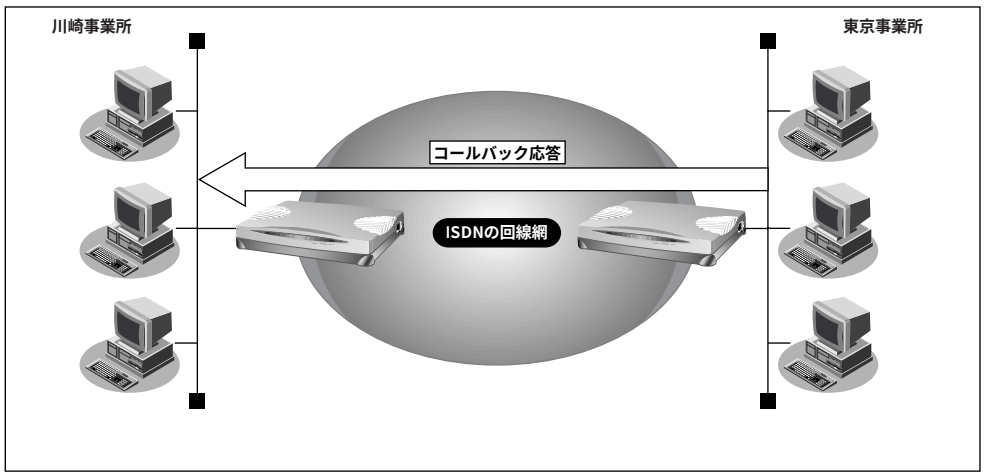
7.　［更新］ボタンをクリックします。

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どうしをISDNで接続する」（P.104）

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。

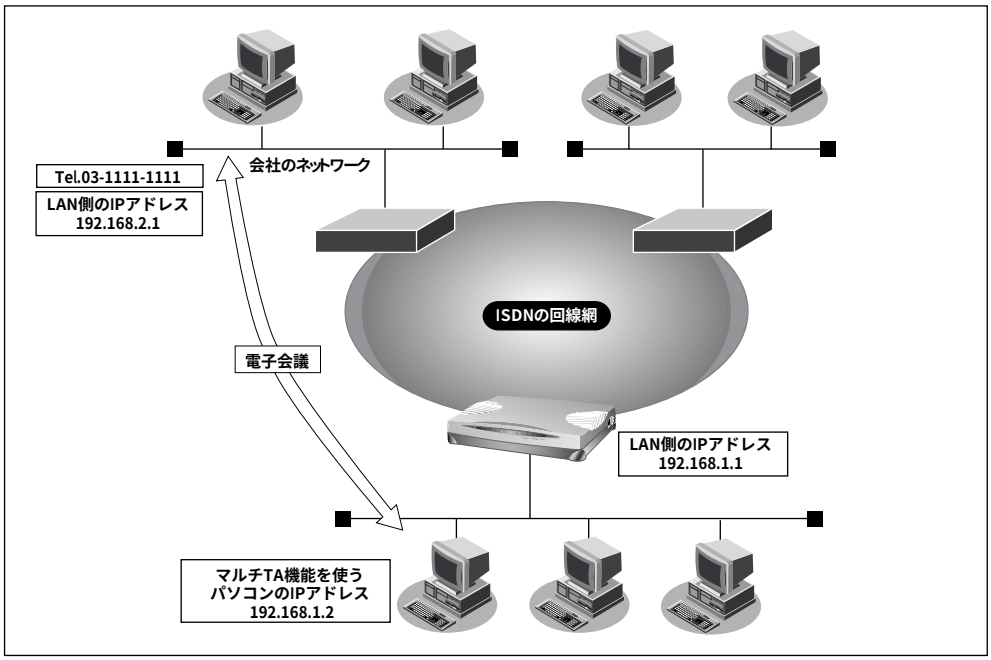
マルチTA機能を使う

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を使用せずに通信が行えるので、NATを利用すると通信できないアプリケーション（例えば、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® 95／98／2000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セッションを確立を行うことが可能です。動作確認済みのOSは、Windows® 95／98／2000です。Windows® 95の場合は、Microsoft® Windows® 95ダイヤルアップネットワーク1.3アップグレードが必要です。**
- **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おり、かつ、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）接続されるため異常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、ある特定のパソコンでマルチTA機能を利用して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

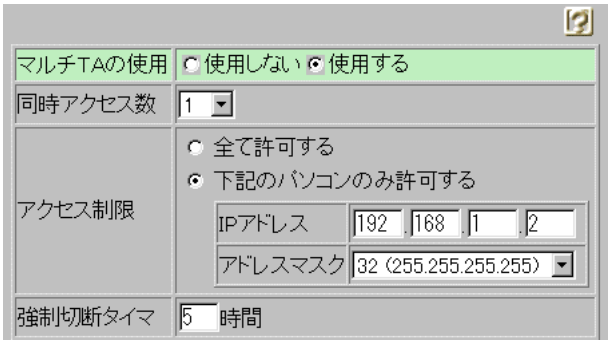
マルチTA情報を設定する

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。

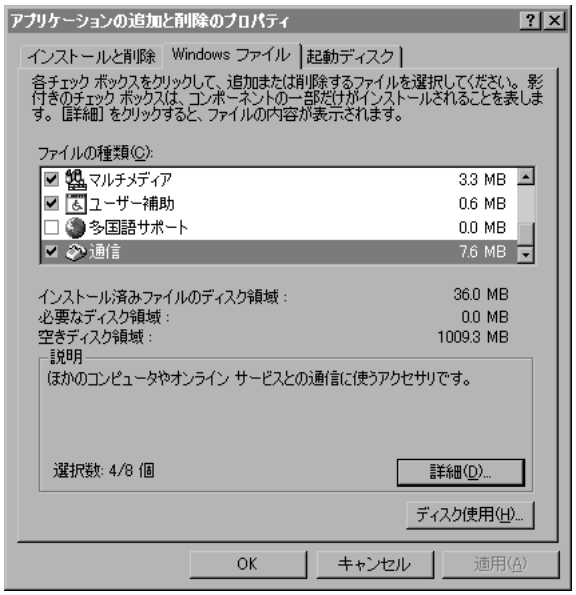
VPNアダプタを準備する（Windows® 95／98の場合）

Windows® 95をお使いの場合は、Microsoft® Windows® 95ダイヤルアップネットワーク1.3アップグレード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」で操作できます。

1.　［コントロールパネル］ウィンドウを開き、［アプリケーションの追加と削除］アイコンをダブルクリックします。

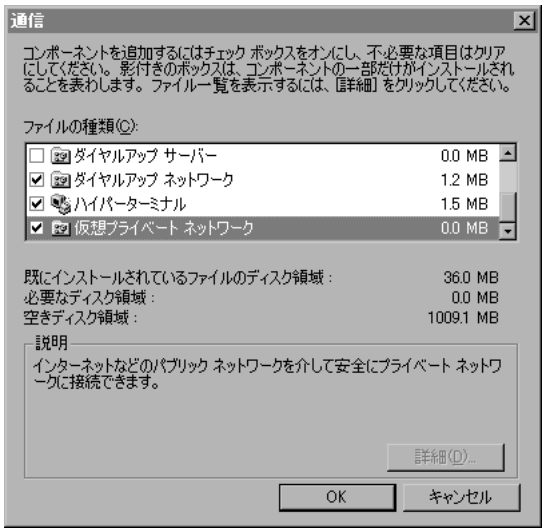
2.　［アプリケーションの追加と削除のプロパティ］ダイアログボックスで「Windowsファイル」タブをクリックして選択します。「ファイルの種類」ボックスで「通信」を選択し、［詳細］ボタンをクリックします。



［通信］ダイアログボックスが表示されます。

ここで「ファイルの種類」ボックスに「ダイヤルアップネットワーク」および「仮想プライベートネットワーク」が選択されているかを確認し、なければ次に示す手順で準備します。

3.　「ダイヤルアップネットワーク」および「仮想プライベートネットワーク」をチェックし、［OK］ボタンをクリックします。



4.　［アプリケーションの追加と削除のプロパティ］ダイアログボックスで［OK］ボタンをクリックします。

ダイヤルアップネットワークの設定をする（Windows® 95／98の場合）

1.　Windows®の画面左上の「マイコンピュータ」をダブルクリックします。

2.　「マイコンピュータ」の「ダイヤルアップネットワーク」をダブルクリックします。

3.　「ダイヤルアップネットワーク」の「新しい接続」をダブルクリックします。

4.　「新しい接続」で以下の項目を指定します。

- 接続名　→ISP仮想接続
- モデム　→Microsoft VPN Adapter

5.　［次へ］ボタンをクリックします。

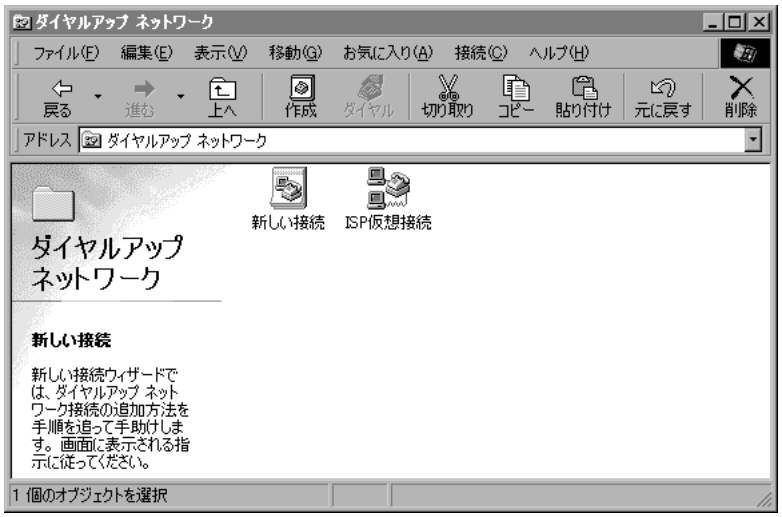
6.　以下の項目を指定します。

- 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）

7.　［次へ］ボタンをクリックします。

8.　［完了］ボタンをクリックします。

「ダイヤルアップネットワーク」に「ISP仮想接続」のアイコンが作成されます。



9.　「ISP 仮想接続」のアイコンを選択し、「ファイル」メニューから「プロパティ」を選択します。

10.　［サーバーの種類］タブをクリックします。

11.　以下の項目を指定します。

- 使用できるネットワークプロトコル　→ TCP/IP

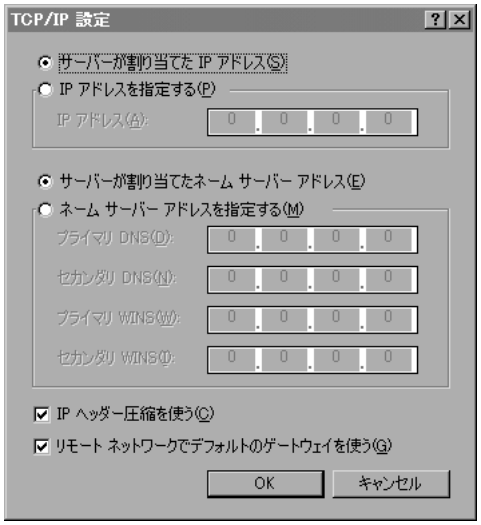
こんな事に気をつけて

［詳細オプション］の「データの暗号化を使う」は選択（使用）しないでください。

12.　[TCP/IP 設定］をクリックします。

13.　以下の項目を指定します。

- サーバーが割り当てたIPアドレス　→選択する
- サーバーが割り当てたネームサーバアドレス　→選択する
- IPヘッダー圧縮を使用　→選択する
- リモートネットワークでデフォルトのゲートウェイを使用　→選択する



14.　[OK]ボタンをクリックします。

15.　[ISP仮想接続]ダイアログボックスで[OK]ボタンをクリックします。

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® 95／98の場合）

1. Windowsの画面左上の「マイコンピュータ」の「ダイヤルアップネットワーク」アイコンをダブルクリックします。

2. 「ダイヤルアップネットワーク」の「ISP仮想接続」をダブルクリックします。

［接続］ダイアログボックスが表示されます。

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

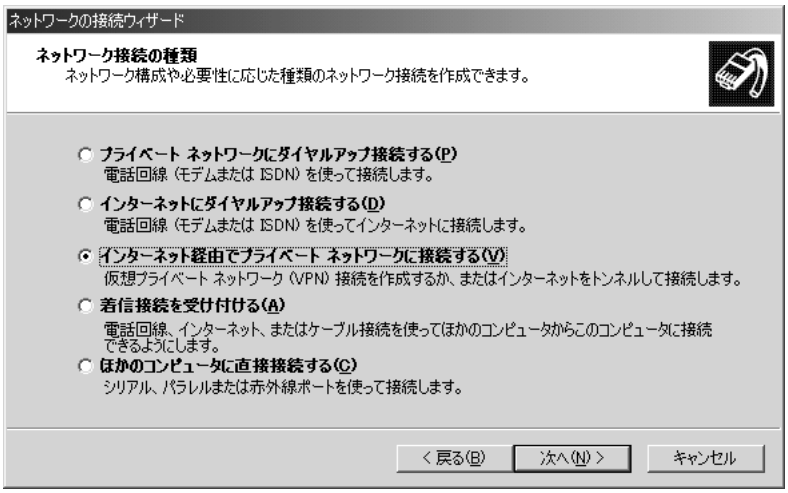
4. ［接続］ボタンをクリックします。

「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。

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。

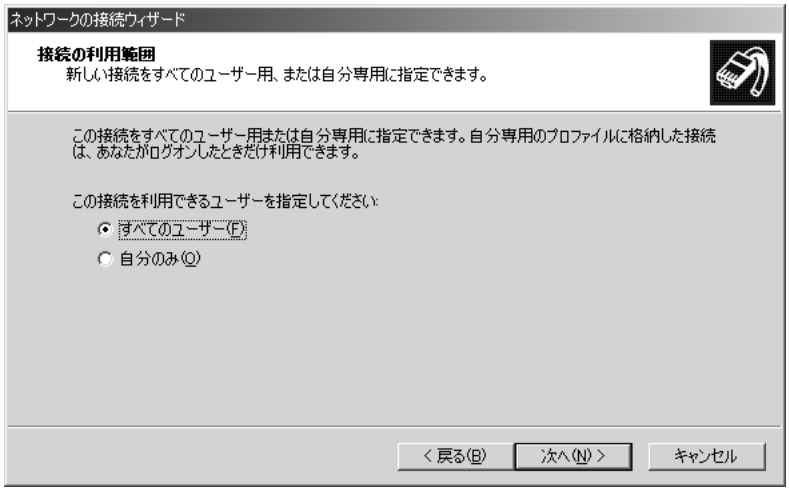
6. ［次へ］ボタンをクリックします。

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。

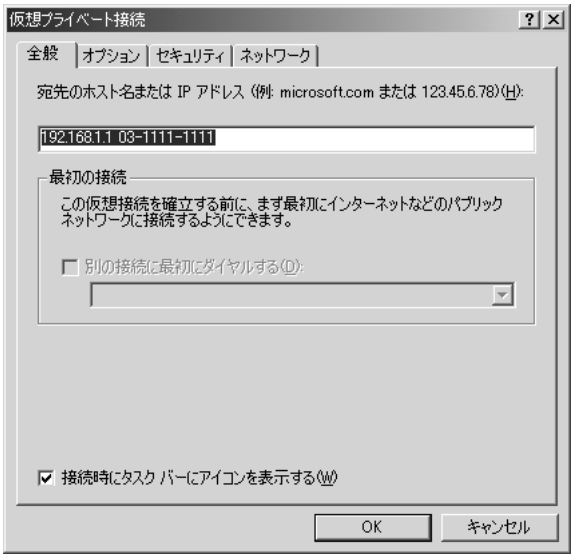
「接続の利用範囲」で「すべてのユーザ」のラジオボタンがチェックされていることを確認します。



9.　［次へ］ボタンをクリックします。

10.　［完了］ボタンをクリックします。

11.　接続画面が表示されたら、「プロパティ」を選択します。



12.　「セキュリティ」タブをクリックします。

13.　「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。

14.　[OK] ボタンをクリックします。

15.　[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。

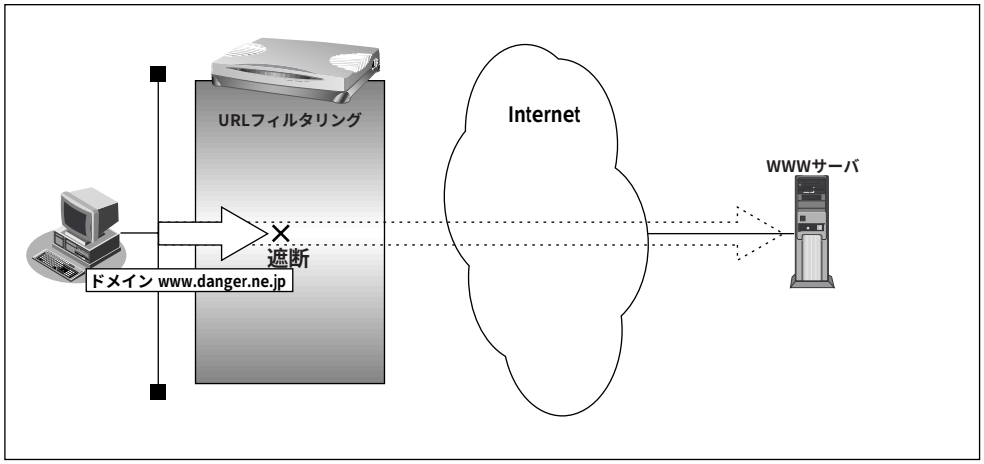
   「ユーザ名」と「パスワード」の確認処理が終わると、回線が接続されます。
   タスクバーにダイヤルアップネットワークのインジケータが表示されます。

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」を利用すると、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

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？

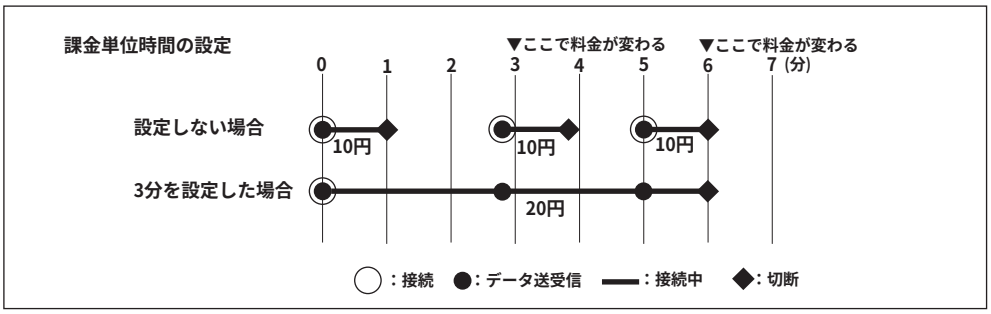
例えば「www.danger.ne.jp」と「XXX.danger.ne.jp」の両方を URL フィルタの対象とする場合は「＊ .danger.ne.jp」と指定することで両方を対象にできます。

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備えています。通信料金の無駄、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（初期値設定：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、初期設定において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、指定された料金を超えた場合に発呼を制御する機能ですが、運用中の回線を切断する機能ではありません。回線の接続中に指定され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ます。その結果、通信料金が指定された金額を超えるのでご注意ください。**

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

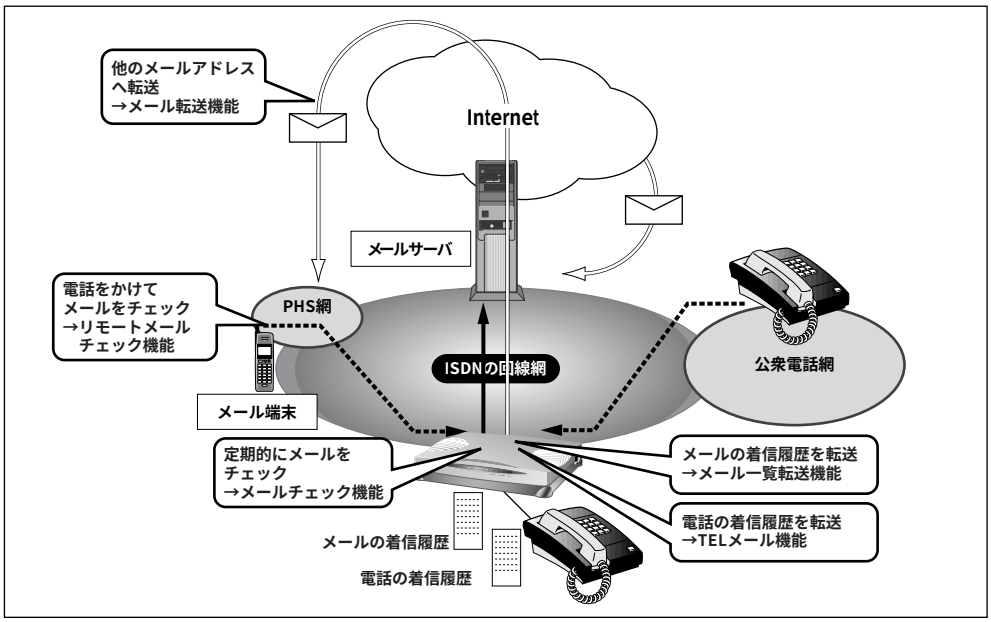
こんな事に気をつけて

- **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。**
  例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
- メール着信通知機能



こんな事に気をつけて

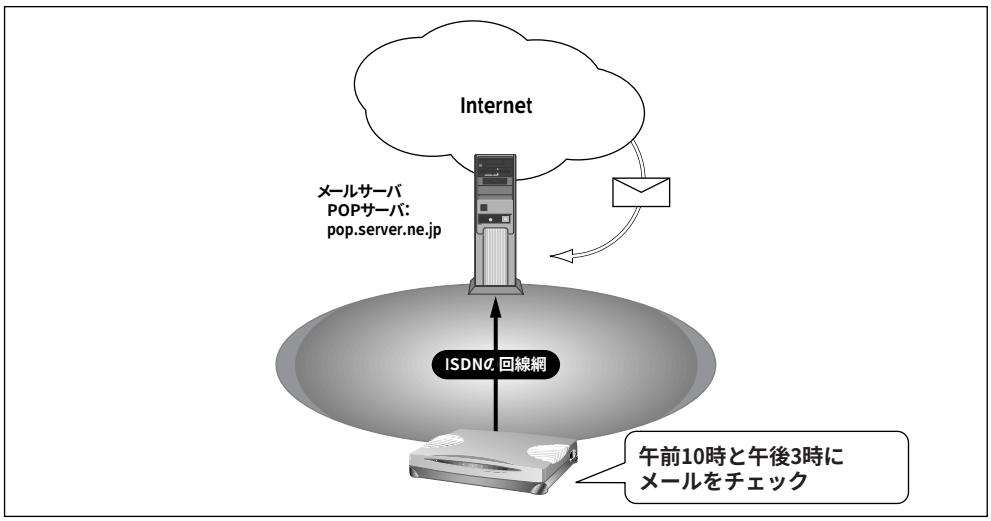
- **設定前に本装置の内部時計を正しくセットしてください。**
- **文字入力フィールドでは半角文字（0 ～9、A ～Z、a ～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。入力した場合、ブラウザでの設定が不可能となります。**
  詳細については、「付録　文字入力フィールドに入力できる文字一覧 (P.600)」を参照してください。

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 ランプが緑色に点滅します。

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。

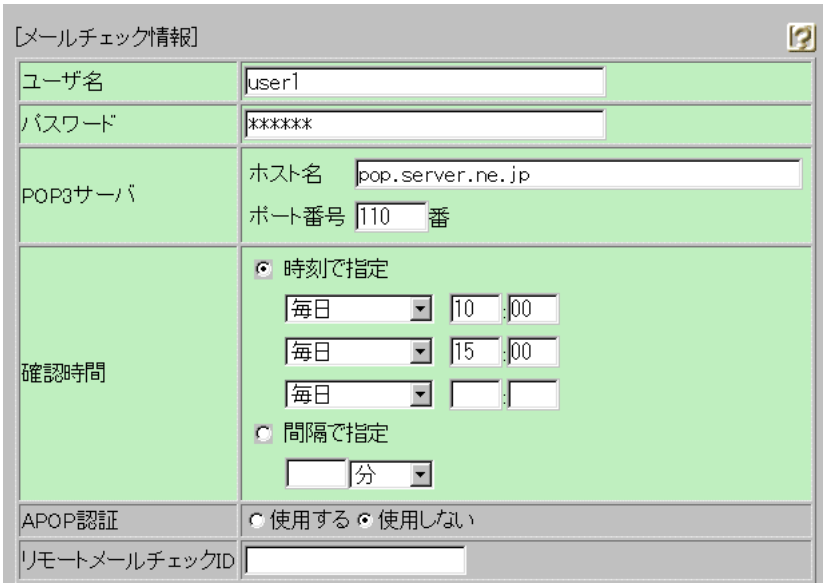
「E メールエージェント情報設定」ページが表示されます。

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。確認のしかたには以下の方法があります。

- 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.434）

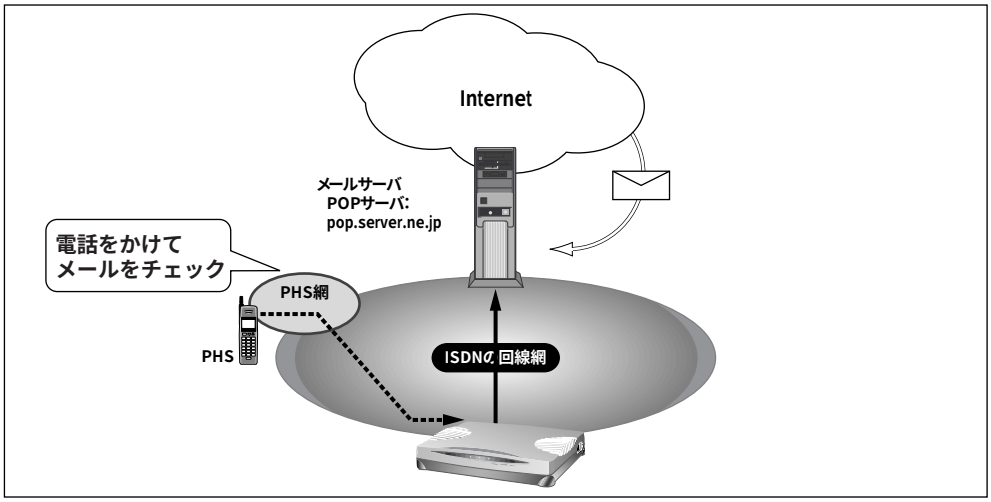
■ リモートメールチェック機能

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ランプが緑色に点滅します。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.405）、「メール一覧送信機能」（P.408）

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。

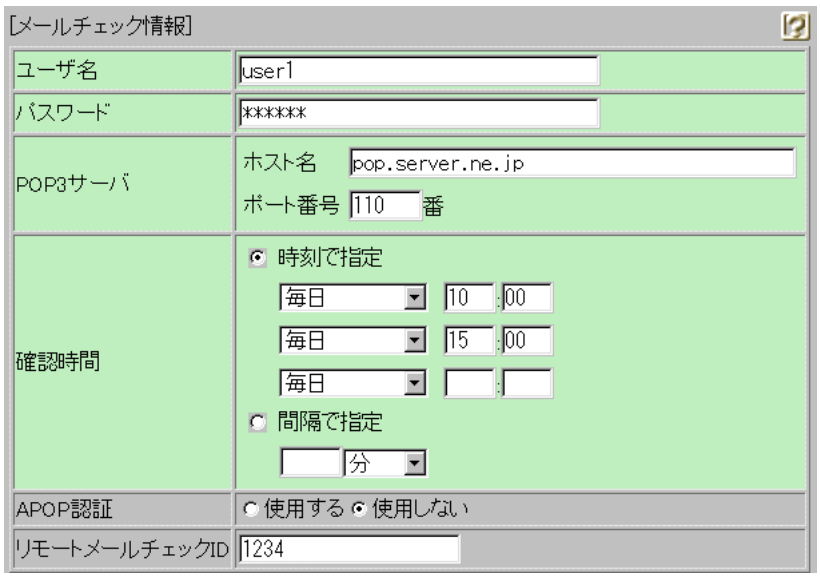
「E メールエージェント情報設定」ページが表示されます。

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。確認のしかたには以下の方法があります。

- 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.434)

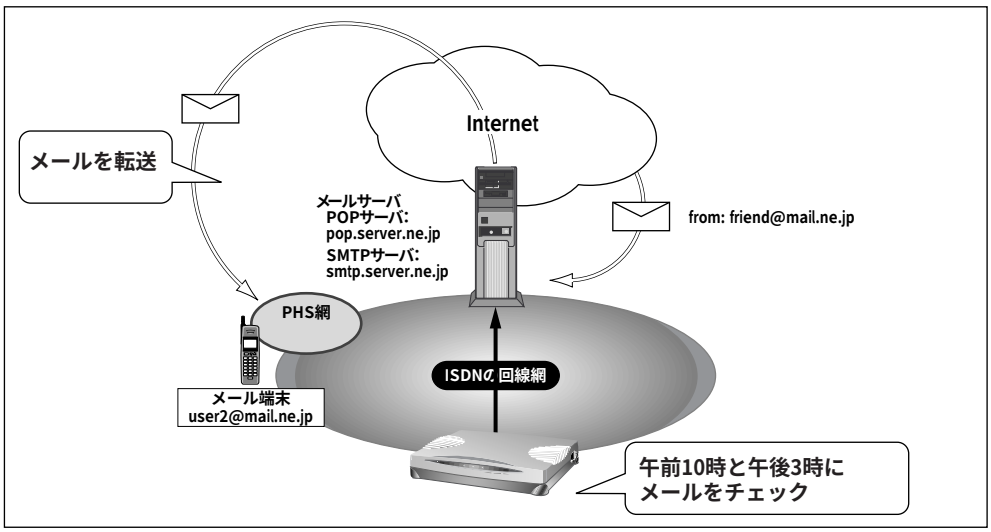
■ メール転送機能

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ものとして説明します。

☛ 参照 「メールチェック機能」（P.400）、「リモートメールチェック機能」（P.402）

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。

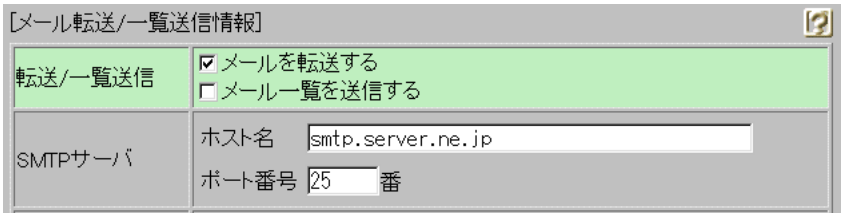
「E メールエージェント情報設定」ページが表示されます。

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。

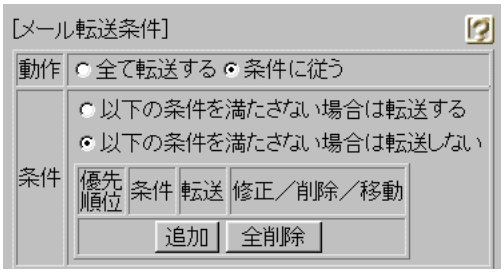
- メールアドレス　　→user2@mail.ne.jp

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



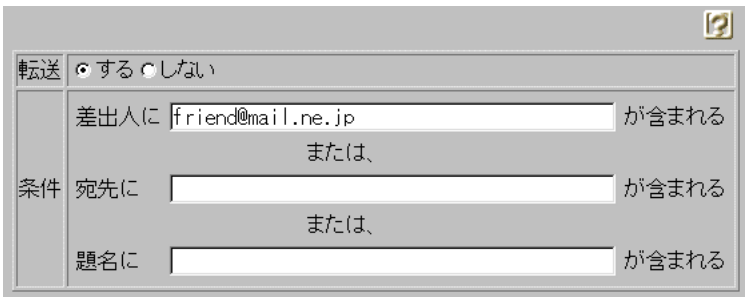
8.　条件の欄の［追加］ボタンをクリックします。

「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。

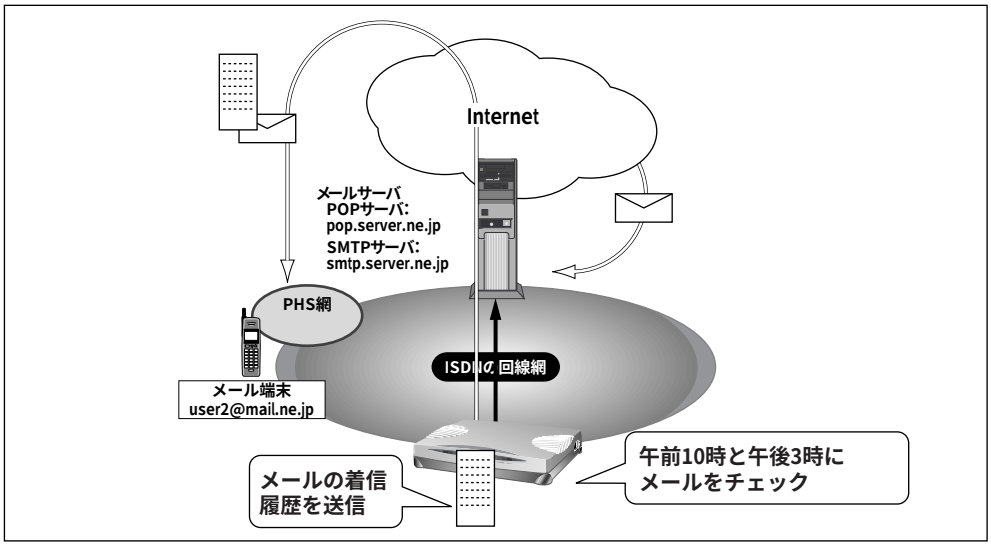
13.　［設定反映］ボタンをクリックします。

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ものとして説明します。

☛ 参照 「メールチェック機能」（P.400）、「リモートメールチェック機能」（P.402）

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。

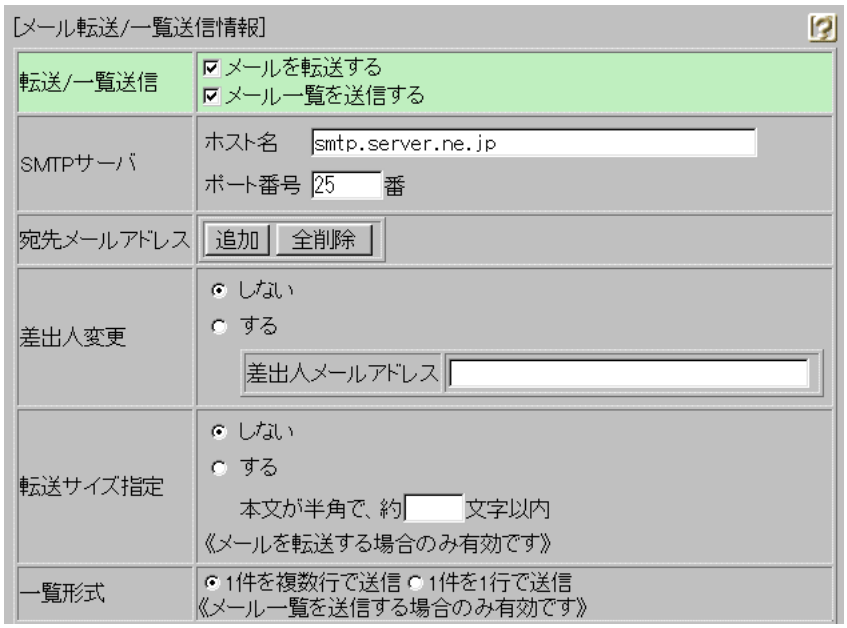
2.　［メールチェック情報一覧］で user1 の欄の［修正］ボタンをクリックします。

「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」に設定することをお勧めします。



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」に設定されている場合、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」に設定されている場合、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。

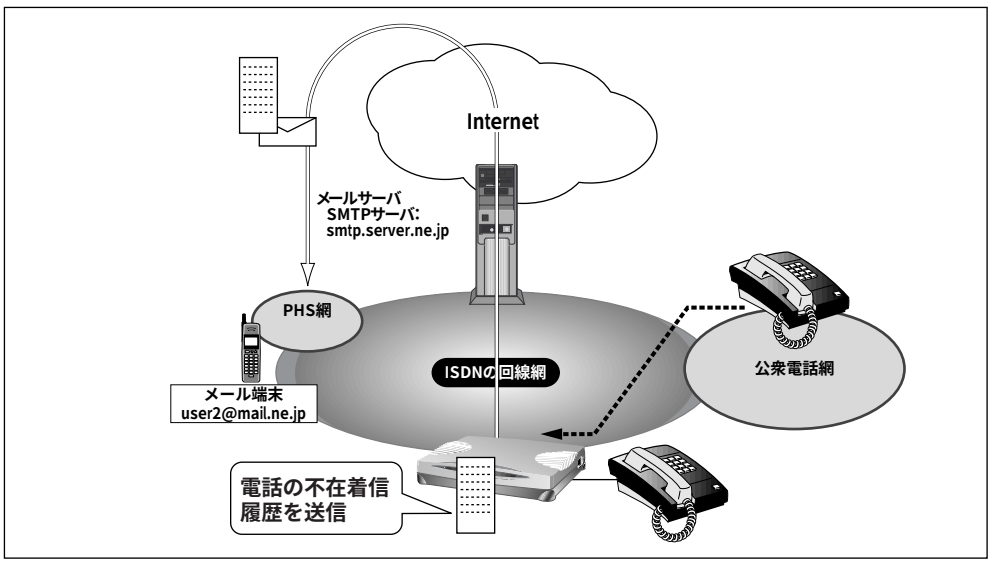
  (2)ダイヤルインサービスを利用している場合

  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

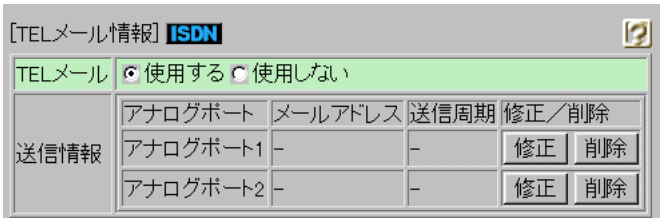
- ダイヤルインサービスを利用する
- アナログポート 1 につながっている電話への着信履歴を 1 時間ごとにメールする
- 送信先のメールアドレス　：user2@mail.ne.jp
- 差出人のメールアドレス　：tel1@si-r30
- メールサーバ名　：smtp.server.ne.jp

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



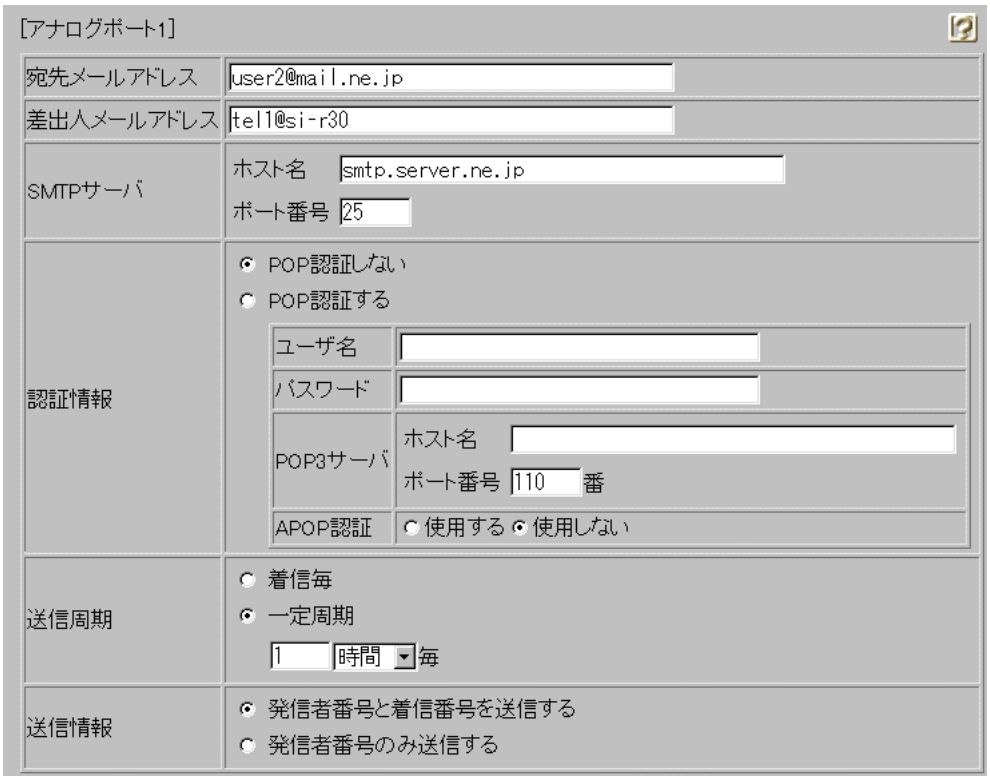
3.　送信情報（アナログポート 1）の欄の［修正］ボタンをクリックします。

「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-r30
- 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-r30>

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）

■ メール着信通知機能

メール着信通知機能を使用すると、メールが着信するとCHECKランプが緑色で点滅し、プロバイダにダイヤルアップしなくてもメール着信を知ることができます。

ここでは、プロバイダAに着信メールがあったら通知する場合を例に説明します。

補足
- プロバイダと「メール着信通知」の契約をしておく必要があります。
- NTTと「ユーザ間情報通知サービス」で「着信許可」の契約をしておく必要があります。
- ダイヤルイン番号やサブアドレスを使用して着信させる場合は、「回線情報」の「着信番号チェック」でダイヤルイン番号やサブアドレスを指定しておく必要があります。

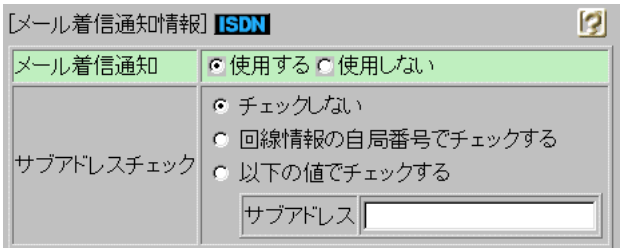
1.　詳細設定メニューのルータ設定で「Eメールエージェント情報」をクリックします。

「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.　［メール着信通知情報］で以下の項目を指定します。

- メール着信通知　　→使用する
- サブアドレスチェック　　→チェックしない

補足
ダイヤルイン番号およびサブアドレスを使用して複数のISDN機器を識別している場合にチェックする内容を指定します。



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。

ヒント

◆ターミナルアダプタ（TA）と本装置の両方を使用する場合には

TAと本装置の両方を使用し、ダイヤルイン番号およびサブアドレスで複数のISDN機器を識別している場合に、それぞれに宛てられたメールを識別するには以下の方法があります。

・電話番号（「回線情報」の自局番号チェックで指定）＋サブアドレスで識別する

・メール着信用サブアドレスで識別する

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.600）」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」、「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、2002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　→ 2002年1月1日2時00分
- 電話番号変更情報（変更前1）　→ 06-123-4567
- 電話番号変更情報（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。

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。「留守モード情報」には、以下の設定項目があります。必要に応じて留守モード中の動作を設定してください。

- 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時に、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.405）、「メール一覧送信機能」（P.408）、「TEL メール機能」（P.411）、「フレックスホンを使う」（P.266）、「留守状態を確認する（無課金）」（P.313）

- **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.428）、「留守モードの設定を行う」（P.307）、「スケジュール機能を使う」（P.415）

■ 留守モードの動作を設定する

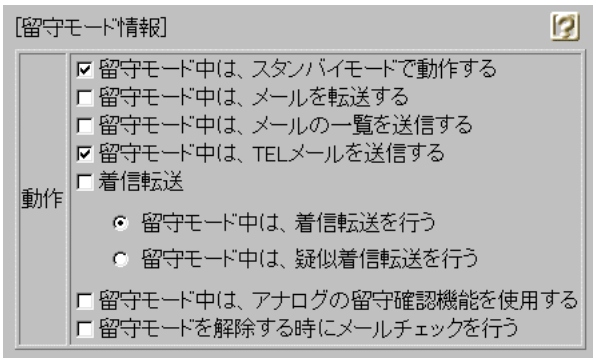
ここでは、留守モード中はスタンバイモードで動作し、かつTELメールを送信する設定を行う場合を例に説明します。

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メールで送信する。



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。