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 601
- **操作メニューを表示する 601**
- **手動で回線を接続する／切断する 601**
- **手動でチャネルを増やす／減らす 603**
- **ネットワークの接続を確認する 603**
- **時計を設定する 604**
- **テレホーダイ機能を使う 605**
- **リモートパワーオン機能を使う 606**
- **留守モードの ON／OFF を設定する 607**
- **VRRP 手動切り戻し機能を使う 608**

表示メニューを使う 609
- **表示メニューを表示する 609**
- **回線接続状況を確認する 609**
- **課金情報で運用状況を確認する 610**
- **IP 統計情報を見る 612**
- **電子メール着信通知を見る 615**
- **チャネル統計情報を見る 616**
- **回線ログ情報で運用状況を確認する 617**
- **システムログを見る 618**
- **ルーティング情報を見る 618**
- **インタフェース情報を見る 619**
- **ブリッジ情報を見る 619**

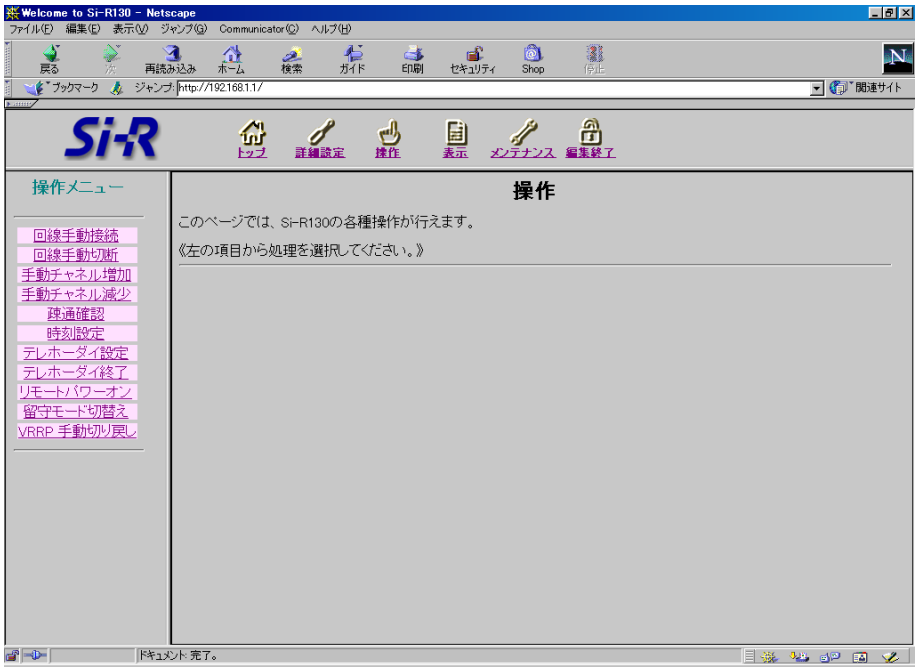
マルチホーミング情報を見る 620
LAN 情報を見る 620
DHCP 情報を見る 621
NAT 情報を見る 621
ISDN 情報を見る 622
フレームリレー情報を見る 623
IPsec 情報を見る 623
VRRP 情報を確認する 624
現在時刻を見る 625
経過時間情報を見る 625
メンテナンスメニューを使う 626
メンテナンスメニューを表示する 626
バージョン情報 627
PPP フレームトレース情報を見る 627
エラーログ情報 628
本装置のファームウェアを更新する 628
オンラインサポート機能 630
構成定義情報を退避する／復元する 632
構成定義情報を切り替える 633
電話番号を変更する 633
FTP サーバ機能を使ってメンテナンスする 634
FTP サーバ機能による構成定義情報の退避 635
FTP サーバ機能による構成定義情報の復元 637
FTP サーバ機能によるファームウェアの更新 639

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。

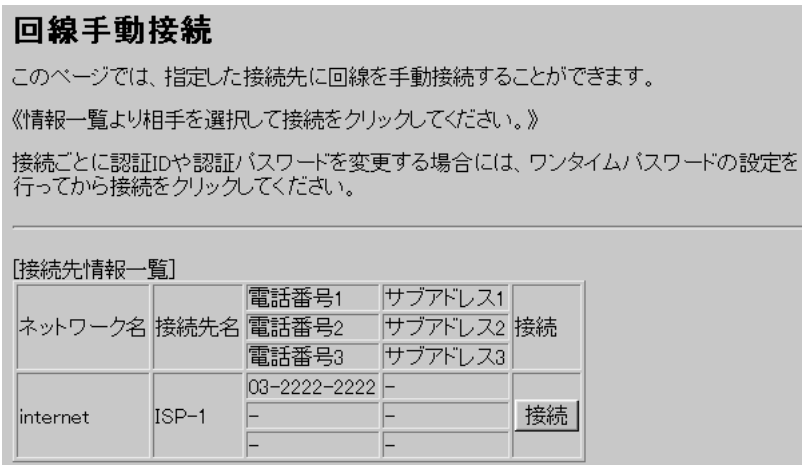
こんな事に気をつけて

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。



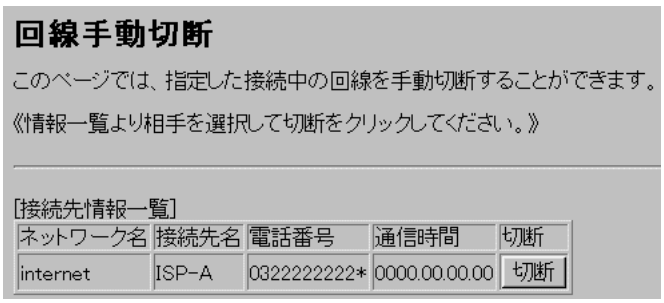
2.　［接続先情報一覧］で接続先の欄の［接続］ボタンをクリックします。

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

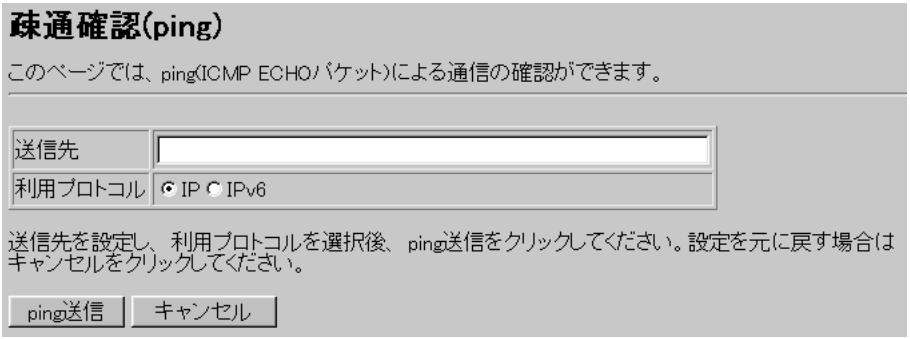
pingコマンドを使って、IP接続が成立しているかどうか確認できます。

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

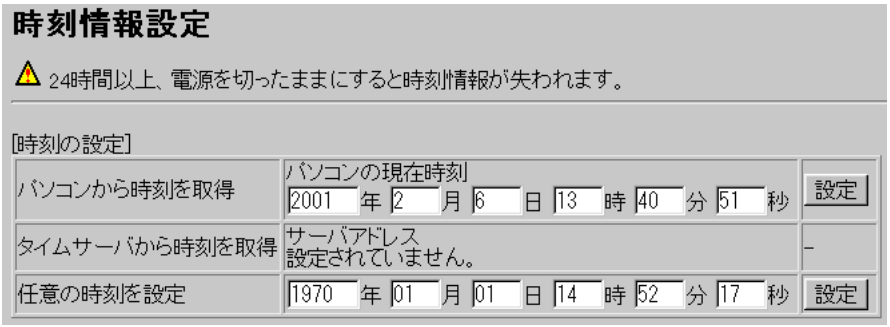
こんな事に気をつけて

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

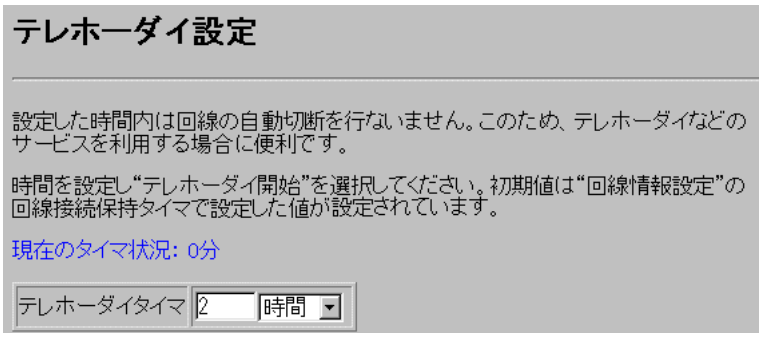
INSテレホーダイサービスを利用する場合はNTTとの契約が必要です。

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。

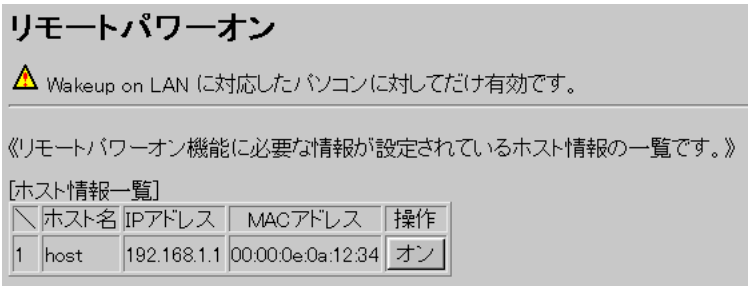
■ リモートパワーオン機能を使う

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.502)

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。

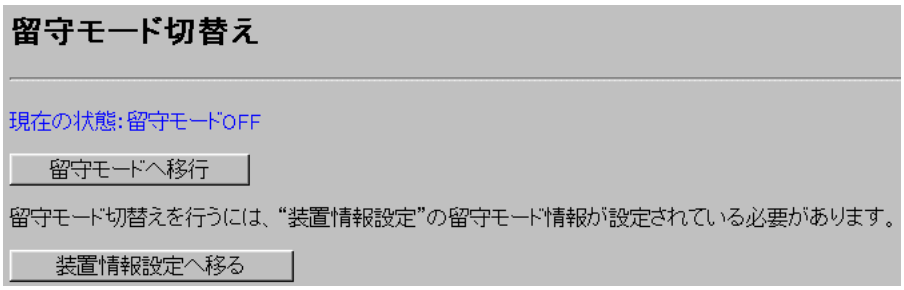
こんな事に気をつけて

「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。

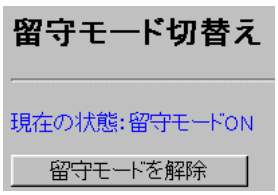
留守モード情報の設定を変更する場合は、［装置情報設定へ移る］ボタンをクリックします。

「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。

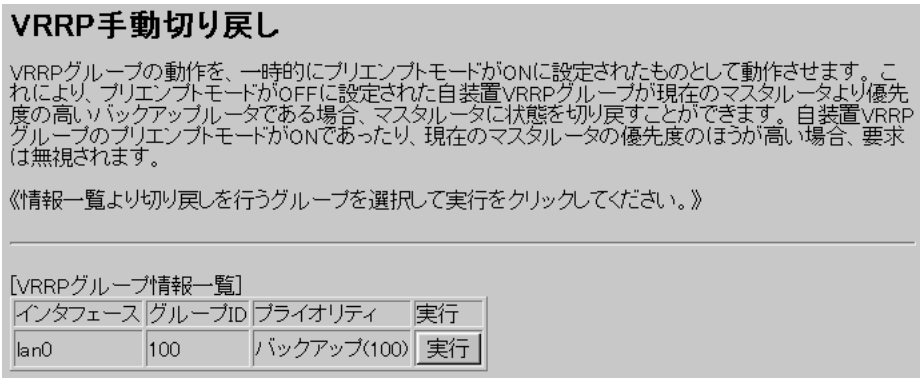
「留守モードを解除しました」というメッセージが表示されます。

■ 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。

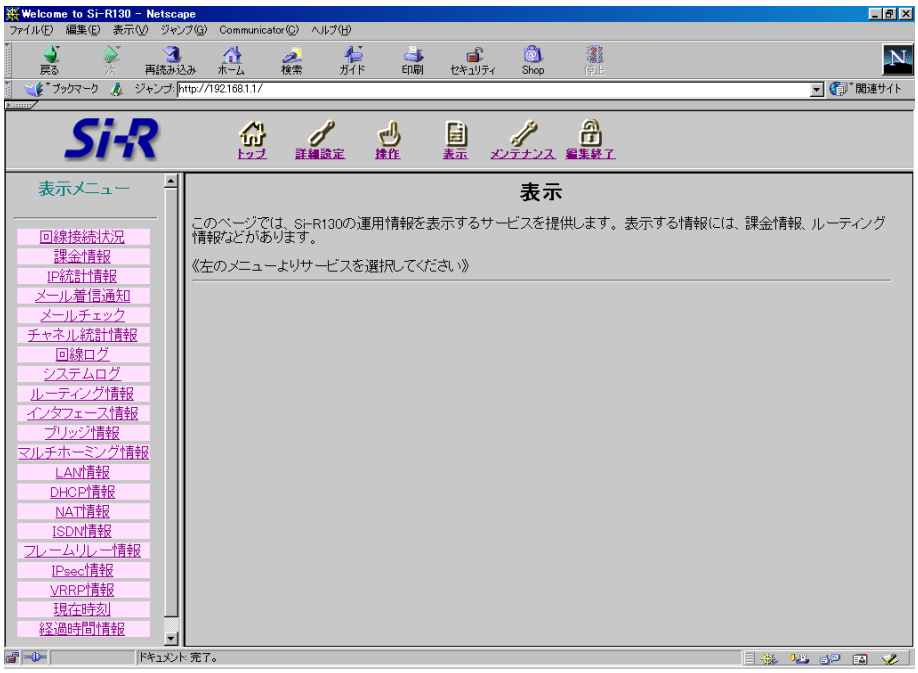
切り戻しが行われます。

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、メール着信通知、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。**
  例えば、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-R130 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。

こんな事に気をつけて

メール着信通知に表示される最大件数は 50 件です。メール着信通知の数が 50 件を超えた場合、古い通知から順に削除されます。ただし、メール着信通知の件数は最大件数を超えてもカウントされます。

メール着信通知

メール着信通知が到着すると、CHECK ランプが緑色で点滅します。

1.　表示メニューで「メール着信通知」をクリックします。

「メール着信通知」ページが表示されます。

2.　確認が終了したら、［メール着信通知消去］ボタンをクリックします。

「メール着信通知を消去しました。」というメッセージが表示され、CHECK ランプが消灯します。メール着信通知は削除されます。

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。

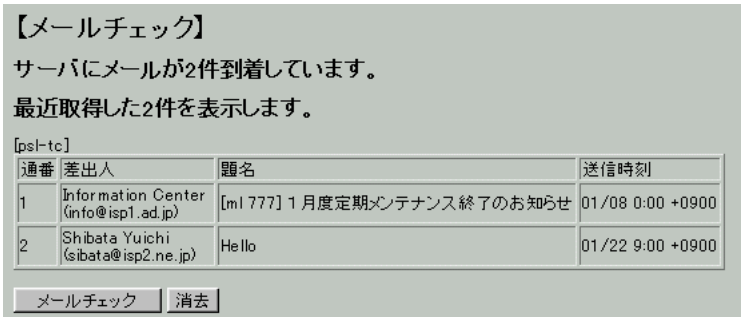
1.　表示メニューで「メールチェック」をクリックします。

「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。

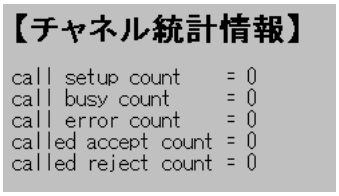


■ チャネル統計情報を見る

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-R130 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。

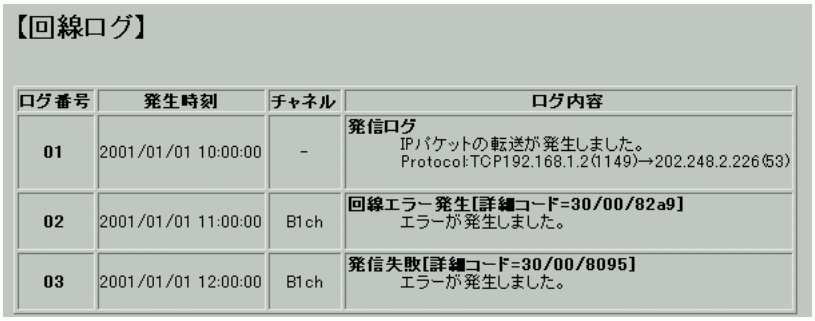
■ 回線ログ情報で運用状況を確認する

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.685）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-R130 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-R130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-R130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
```

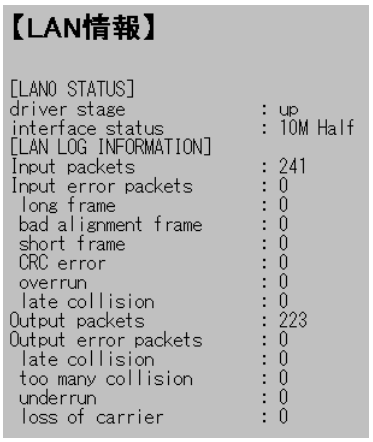
マルチホーミング情報の見方は「Si-R130コマンドリファレンス」の mhstat コマンドを参照してください。

■ 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-R130 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-R130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
```

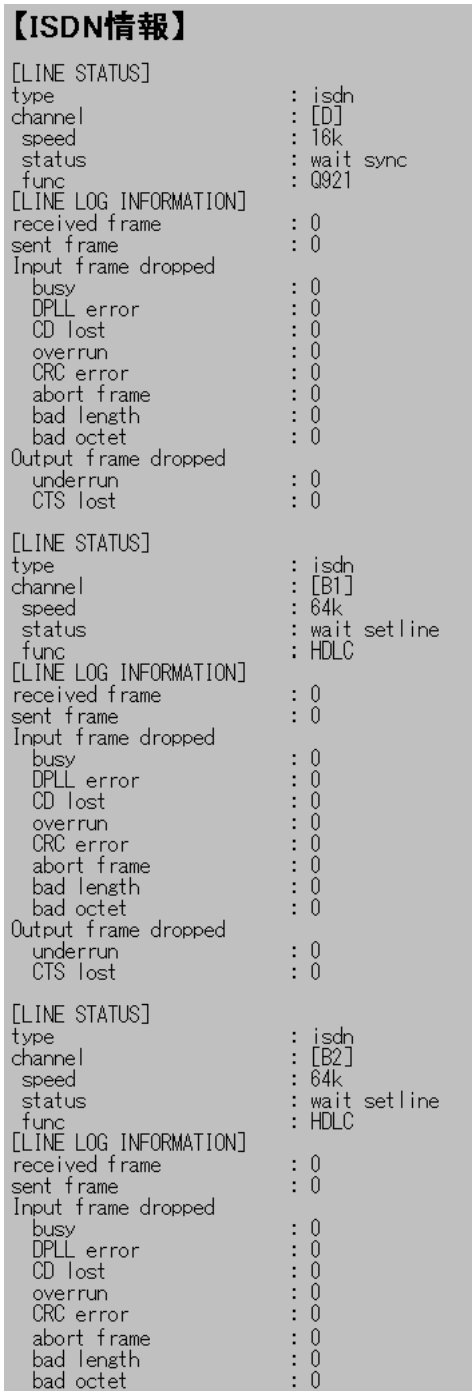
NAT情報の見方は「Si-R130コマンドリファレンス」のnatstatコマンドを参照してください。

■ 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-R130 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-R130 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-R130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-R130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】

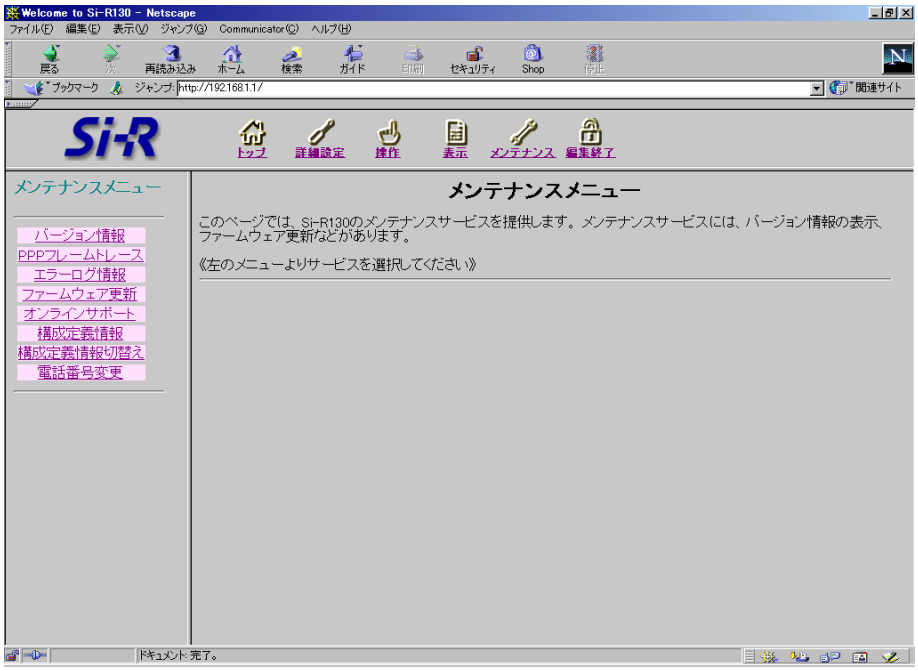
```
0001.01:48:23
```

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を更新、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。



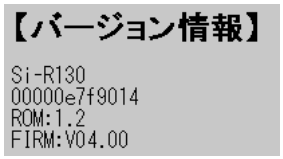
■ バージョン情報

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-R130：基本ソフトウェア
- バージョン情報（版数）　→FIRM：V04.00



■ 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

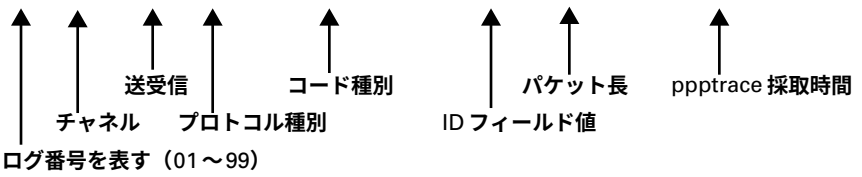
PPPフレームトレース情報は、以下のように表示されます。

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.687）

■ エラーログ情報

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。

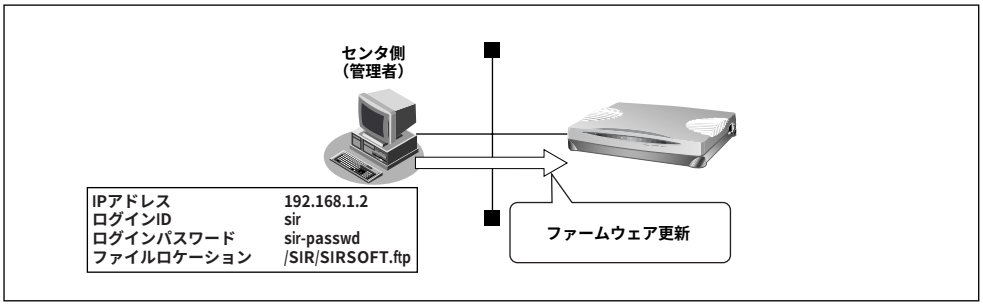
FTPサーバ（FTPサーバ機能を持つパソコンやUNIXシステム）にファームウェアファイルを配置し、WWWブラウザ（本装置の設定メニュー）を使ってネットワークに接続した本装置のファームウェアを更新できます。

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。

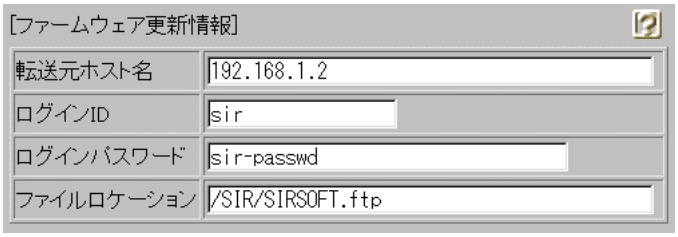


1.　詳細設定メニューのルータ設定で「装置情報」をクリックします。

「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



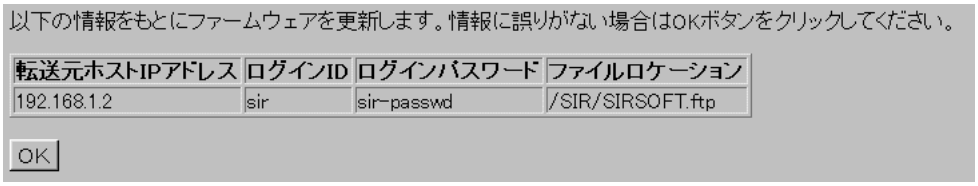
3.　［更新］ボタンをクリックします。

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。

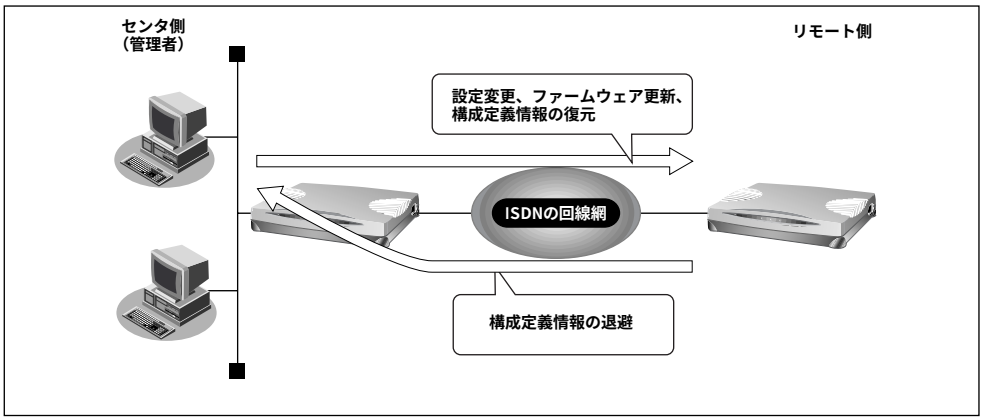
トップページに戻ります。

■ 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.31）

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.28）

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。**

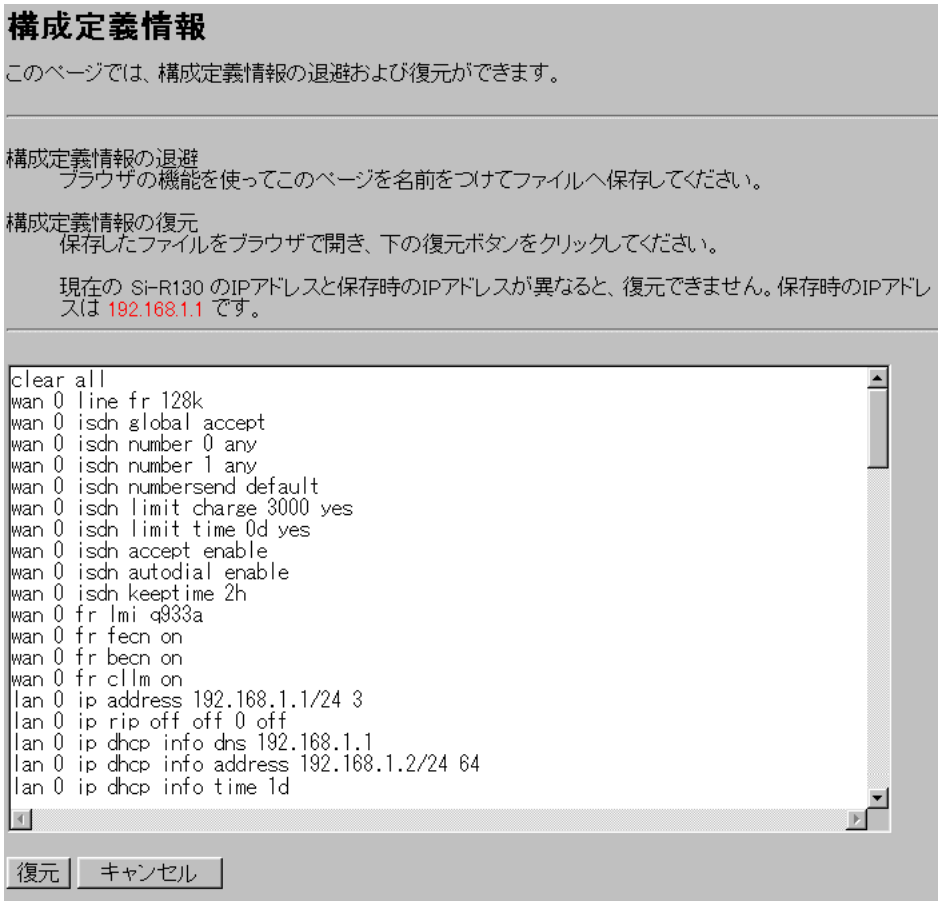
■ 構成定義情報を退避する／復元する

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

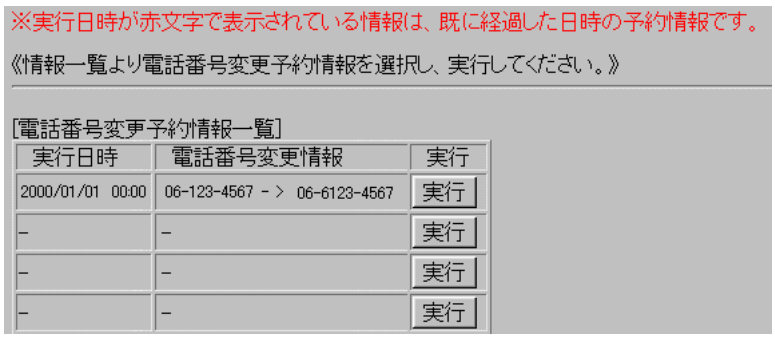
- **電源投入時は、直前に動作していた側の構成定義情報で立ち上がります。**
- **再起動すると、通話中やデータ通信の場合、切断されます。**
- **本装置の IP アドレスが変更となった場合、再起動後に本装置にアクセスするためには、パソコンの再起動および URL を変更する必要があります。**

■ 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。

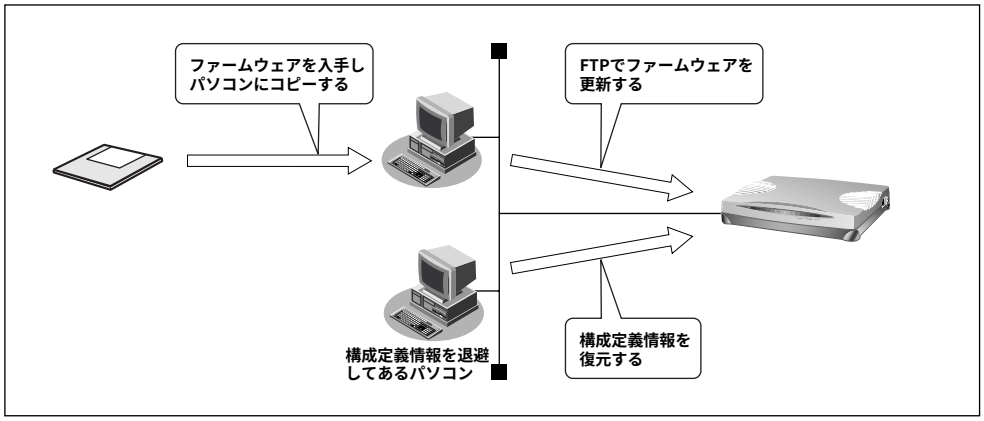
電話番号が変更されます。

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

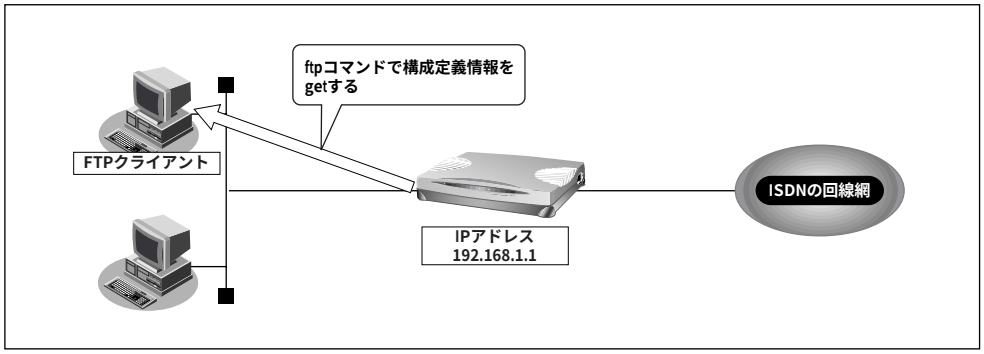
ftpコマンドのサブコマンドとして「get reset」を入力すると本装置が再起動します。

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

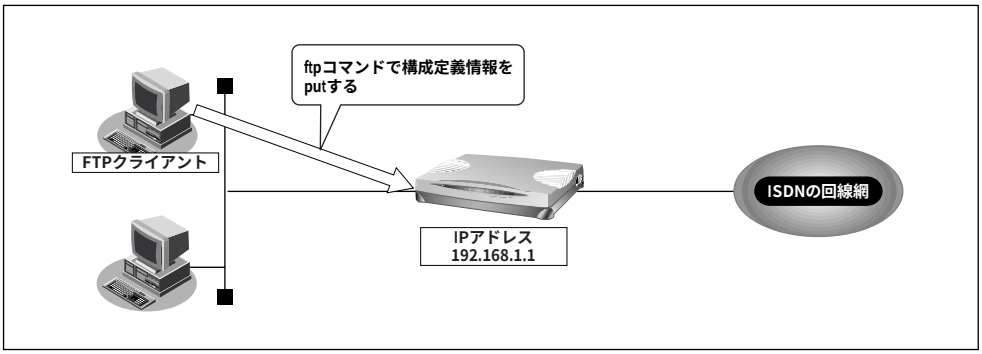
構成定義情報（config1）をパソコン上のconfig1-1 ファイルに退避する場合の例を示します。

```
# 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-R130 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

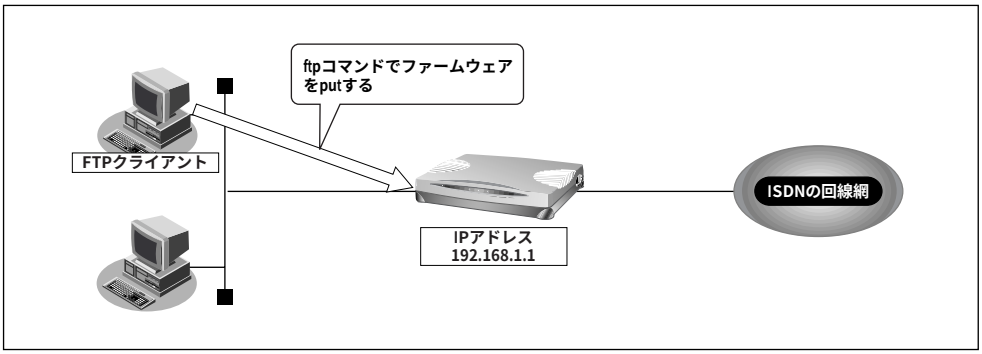
構成定義情報（config1）をパソコン上のconfig1-1 ファイルから復元する場合の例を示します。

```
# 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-R130 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-R130 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-R130SOFT.ftp firmware           ：ファームウェアを書き込む
local: Si-R130SOFT.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。