FutureNet MA-E200 Series

ウェブユーザインターフェース操作マニュアル

Version 1.2.1

CENTURY SYSTEMS

はじめに

このたびは本装置をご購入いただきまして、誠にありがとうございます。
本書には、本装置を安全に使用していただくための重要な情報が記載されています。ご使用の前に本書をよくお読みになり、正しくお使いいただけますようお願い致します。
特に、本書に記載されている「安全にお使いいただくために」をよく読み、理解されたうえで本装置をご使用ください。
また、本書は本装置の使用中、いつでも参照できるように大切に保管してください。

■ご注意

(1) 本書の内容の一部または全部を無断で転用、転載しないようお願いいたします。

(2) 本書の内容および製品仕様、外観は、改良のため予告なく変更することがあります。

(3) 本装置の仕様は日本国内向けとなっておりますので、海外ではご利用できません。
This equipment is designed for use in Japan only and cannot be used in any other country.

(4) 本書の作成にあたっては万全を期しておりますが、本書の内容の誤りや省略に対して、また本書の適用の結果生じた間接損害を含め、いかなる損害についても責任を負いかねますのでご了承ください。

(5) 製品の保証に関する規定については製品添付の製品保証書をご覧下さい。

(6) 本製品にて提供されるファームウェアおよび本製品用として弊社より提供される更新用ファームウェアを、本製品に組み込んで使用する以外の方法で使用することは一切許可しておりません。

■セキュリティの確保について

パスワードを設定しない、もしくはデフォルトパスワードを使用する場合、ネットワーク上のだれからでも本装置の設定を行うことができます。
セキュリティの面からは非常に危険な為、ユニークなパスワードを設定することを強く推奨します。

■最新情報の入手について

当社では、製品に関する最新の情報（最新のファームウェア、マニュアルなど）を下記ホームページでご案内しています。
ぜひご活用下さい。

センチュリー・システムズ（株）
FutureNet サポートデスク
http://www.centurysys.co.jp/support/

また、本書について万一ご不審な点や誤り、記載漏れなど、お気付きの点がございましたら、下記までご連絡ください。

センチュリー・システムズ（株）
FutureNet サポートデスク
support@centurysys.co.jp

■商標について

目次

1. はじめに

この文書は、**MA-E200** Series(以下、**MA-E2xx**)のウェブユーザインターフェース(以下、WebUI)の操作仕様について記載します。

2. 概要

MA-E2xx WebUI は、**MA-E2xx** で稼働する Web サーバを介して、**MA-E2xx** システム設定機能を提供します。

2.1. 基本画面構成

画面は、メニュー部と設定画面部に分かれます。

2.2. 機能

MA-E2xx WebUI は、次の機能を持ちます。

基本設定機能

Ethernet、PPP(発信/着信)、DHCP、静的ルーティング、ファイアウォール、日付・時刻設定を行うことができます。

サービス設定機能

MA-E2xx 本体の NTP による時刻同期設定を行うことができます。

アプリケーション設定機能

死活監視設定を行うことができます。

シリアル監視設定機能

ser2net 設定を行うことができます。

保守・運用機能

WebUI パスワード設定、Syslog メッセージ、ping テスト、設定データ管理、ファームウェア更新、システム再起動を行うことができます。

2.3. 動作環境

本 WebUI は、JavaScript を使用しています。ご利用のウェブブラウザにおいて、JavaScript 機能を有効にして下さい。

動作確認に使用した OS とウェブブラウザは以下の通りです。
Windows XP SP2: Internet Explorer 8
Windows Vista(32bit): Internet Explorer 8

2.4. ウェブユーザインターフェースへのアクセス

PC 上からのウェブブラウザから、

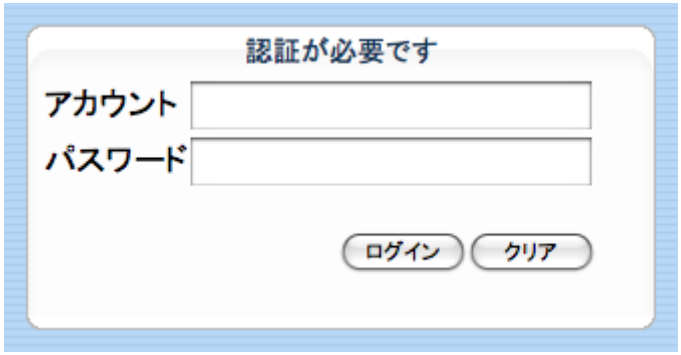
http://(MA-E2xx　IP アドレス)

へアクセスして下さい。

工場出荷時の IP アドレスは、は下記の通りです。

Ether　0	192.168.253.253

アクセスすると下記のログイン画面が現れます。



初期アカウントは、

アカウント	admin
パスワード	admin

となっております。

3. 画面別説明

3.1. 基本設定

3.1.1. インターフェース設定

「インターフェース設定」画面では、次の項目の設定を行います。

- インターフェース
- IP アドレス
- ネットマスク
- デフォルトゲートウェイ
- DHCP オプション
- DNS サーバ

3.1.1.1. Ethernet I/F 設定

「インターフェース」は **MA-E2xx** に実装されている Ethernet ポート(10/100Base-TX)に対応し、Linux システム上における eth0 デバイスに対応しています。

「IP アドレス」、「ネットマスク」は、固定 IP アドレスとしてのパラメータです。DHCP を使用する場合でも、DHCP リクエストが失敗した場合、ここに指定した IP アドレス固定値、ネットマスクが設定されます。

「デフォルトゲートウェイ」は、指定したインターフェースの先にデフォルトゲートウェイがある場合に入力して下さい。

「DHCP オプション」の“DHCP を使用する”をチェックした場合は表示が下記の通り変更になります。

「DHCP オプション」では更に次のオプションが指定可能です。

- **「再利用できるように IP アドレスを解放する」**

DHCP サーバの接続毎に異なる IP アドレスを使用しても構わない場合にチェックします。

- **「/etc/resov.conf を書き換えない」**

DHCP から取得した情報より、DNS サーバのアドレスを書き変えたくない場合にチェックします。

- **「/etc/ntp.conf を書き換えない」**

DHCP から取得した情報より、NTP サーバのアドレスを書き変えたくない場合にチェックします。

- **「デフォルトゲートウェイを設定しない」**

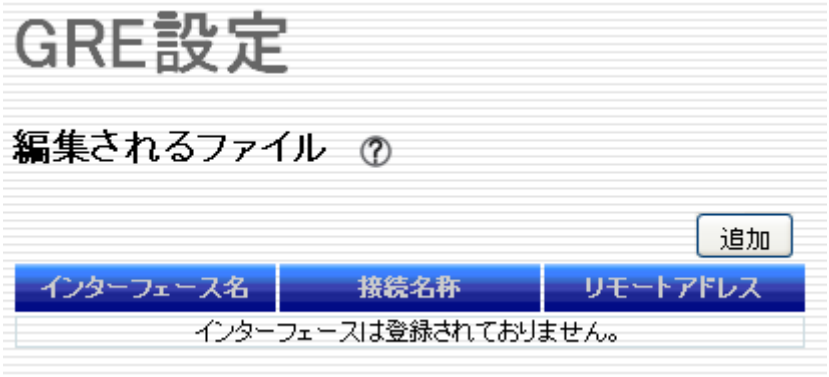
DHCP から取得した IP アドレスの情報より、デフォルトゲートウェイ情報を使用しない場合はチェックします。

3.1.1.2. DNS サーバ設定

「DNS サーバ」に指定されたアドレスにより名前の解決を行います。DNS のアドレスは2つまで登録できます。
必要項目の入力が完了した後、「設定」ボタンを押下して変更内容を **MA-E2xx** に反映させます。

3.1.2. GRE 設定

GRE(Generic Routing Encapsulation)によるトンネル設定を行います。メニューより「GRE 設定」をクリックすると、設定済み GRE トンネルインターフェースの一覧が表示されます。



3.1.2.1. GRE インターフェース編集ダイアログ

GRE のインターフェース設定を新規に追加する場合は「追加」ボタンを押すと「GRE インターフェース編集」ダイアログを表示します。

- インターフェース名
  作成するインターフェース名を表示します。アプリケーションにより自動的に割り当てられます。

- 接続名称
  このインターフェースについて名称を指定できます。この接続を識別できる任意の文字列を入力してください。

- リモートアドレス
  トンネル終端の相手側の IP アドレスを入力してください。この項目は必ず入力してください。

- ローカルアドレス
  トンネル終端の自分側の IP アドレスを入力してください。省略可能です。

- インターフェースアドレス
  このトンネルインターフェースに対して設定する IP アドレスを入力してください。省略した場合は、アドレスを設定せずにインターフェースを UP します。

- TTL
  GRE パケットの TTL 値を入力してください。設定できる値は 1 から 255 までです。

- MTU
  このインターフェースに設定する MTU 値を入力してください。設定できる値は 1500 までです。

3.1.2.2. インターフェース一覧

編集ダイアログで作成したインターフェース設定は、一覧に追加されます。

一覧の各行がひとつのインターフェースに対応します。行右端の「編集」ボタンを押すと当該インターフェースの編集ダイアログを開きます。「削除」を押すと当該インターフェースを削除します。

3.1.3. PPP(発信)設定

PPP(Point-to-Point Protocol)の発信の設定を行います。

3.1.3.1. 利用可能デバイス一覧

「利用可能デバイス一覧」では、PPP 設定が可能なデバイスの一覧が表示されます。

以下のデバイスは **MA-E2xx** が標準実装している固定インターフェースで PPP 設定が可能なものです。「着信可否」が“可”になっているデバイスは、「PPP(着信)設定」の対象となります。

名称	デバイス	種別	着信可否	備考
PPPoE (eth0)	eth0	PPPoE	不可	ether0 ポート
Modem (PORT0)	/dev/ttymxc0	モデム	可	RS-232 ポート
Modem (PORT1)	/dev/ttymxc1	モデム	可	RS-232 ポート

CF カードスロットや USB ポートに着装する利用可能デバイスは、デバイスを接続する事で自動的に追加されます。

※注意事項

Modem(PORT0)または、Modem(PORT1)を使用する場合は、/etc/inittab のシリアル設定を以下のように変更してください。

SERIAL CONSOLES

#mxc0:12345:respawn:/sbin/agetty 115200 ttymxc0 vt100

↑PORT0 をモデムとして使用する場合、先頭に#を付けてコメントアウト

#mxc1:12345:respawn:/sbin/agetty 115200 ttymxc1 vt100

↑PORT1 をモデムとして使用する場合、先頭に#を付けてコメントアウト

3.1.3.2. PPP 設定

PPP の発信設定を新規に追加する場合は「追加」ボタンを押すと「PPP(発信)設定編集」ダイアログを表示します。

■ **PPP 設定**

- PPP No.
  PPP 設定時に自動的に割り振られる連番です。

- デバイス
  プルダウンメニューにある追加可能なデバイス一覧から対象となるデバイスを指定します。

- 接続名称
  PPP 接続に任意に接続名称を付加することが可能です。

■ **モデム設定（PPPoE では設定できません）**

- 接続方式

  次の3種類の中から接続方式を設定可能です。

  - ✓ 「通常」

    手動で PPP 接続・切断操作を行います。切断された場合、自動的に再接続は行いません。

  - ✓ 「PERSIST」

    PPP 接続を常に行う設定です。設定直後のみ、手動で接続操作が必要になりますが、**MA-E2xx** を再起動すると自動的に接続を開始します。相手から切断されても自動的に再接続処理を開始し、常時接続を行います。

  - ✓ 「DEMAND」

    リモートへの IP 通信が発生した場合にのみ接続処理を開始します。

- ダイアルタイプ

  モデム接続(PORT0, PORT1)時のダイアルタイプを選択します。「トーン」または「パルス」が選択できます。
  電話回線の契約形態に合わせてプッシュ回線(トーン)またはダイアル回線(パルス)を選択して下さい。

- アイドル検知時間(秒)

  「接続方式」で「DEMAND」を設定した際にのみ適用されるパラメータです。
  「アイドル検知時間」で指定した期間、IP 通信の無通信状態が持続すると切断処理を行います。
  「DEMAND」を選択した場合は「アイドル検知時間」は“0”以外の値を指定しなければなりません。
  「通常」、「PERSIST」を選択した場合は「アイドル検知時間」の値は無効となります。

- モデム初期化コマンド

  モデム接続時に AT コマンドでモデムを初期化するコマンドを指定します。

- 電話番号

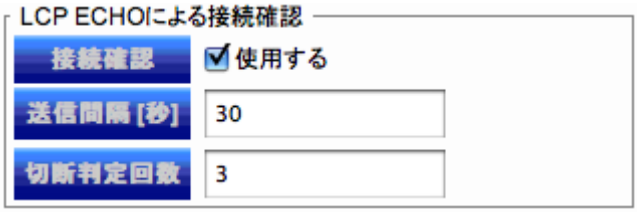
  モデム接続時の接続先の電話番号を指定します。

- Deflate 圧縮

  データ圧縮方式で Deflate 圧縮(RFC1951)を使用する場合はチェックします。

- VJ 圧縮
  データ圧縮方式で VJ 圧縮(RFC1144)を使用する場合はチェックします。

■ **LCP ECHO による接続確認**



- 接続確認
  PPP 接続で LCP ECHO による接続監視を行う場合はチェックします。

- 送信間隔(秒)
  LCP ECHO Request パケットを送信する間隔を指定します。

- 切断判定数
  MA-E2xx から送信される LCP ECHO Request に対して連続無応答の回数を閾値として指定します。
  指定した回数、連続無応答状態が継続すると PPP セッションの切断を実行します。

■ **一般設定**

- DNS サーバ
  PPP 接続時に通知される DNS サーバを取得する場合はチェックします。

- デフォルトルート
  PPP リンクをデフォルトルートとして設定する場合はチェックします。

- ローカル IP

  PPP 接続リンクのローカル(**MA-E2xx**)側の IP アドレスを手動で設定する場合は IP アドレスを入力します。相手の設定に従う場合は“0.0.0.0”を指定して下さい。

- リモート IP

  PPP 接続リンクのリモート(相手)側の IP アドレスを手動で設定する場合は IP アドレスを入力します。相手の設定に従う場合は“0.0.0.0”を指定して下さい。

- サブネットマスク

  サブネットマスクを設定します。この設定したネットマスクと次のネットマスクの論理和が値となります。

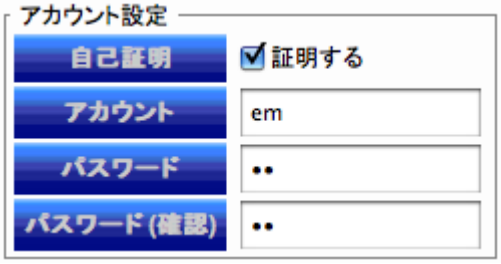
  - ネゴシエートされるリモート側の IP アドレス・クラスに適切なネットマスク
  - リモート側と同一ネットワーク上システムの非 point-to-point ネットワークインターフェースのネットマスク

- MTU

  PPP リンクの MTU を設定します。(バイト)

  NTT フレッツ・サービスにて接続する場合は”1454”に設定します。

■ **アカウント設定**



- 自己証明

  PPP 接続に自己証明を行うか設定します。

- アカウント

  自己証明に使用されるアカウント(ID)を設定します。

- パスワード

  上記アカウントに対応したパスワードを設定します。

- パスワード(確認)

  上記パスワードと同じものを確認用に再度入力します。

3.1.3.3. PPP 設定/状態

「PPP 設定」の各項目を指定して「OK」ボタンを押下すると、その設定が追加されます。「Cancel」を押すと、追加／編集を取りやめます。設定が完了すると以下の通り、「PPP 設定/状態」設定が表示されます。

各行右端の「編集」ボタンを押下すると、パラメータの編集が行えます。「削除」ボタンを押下すると、当該行の設定が削除されます。

各カラムについて説明します。

■ No.

接続設定に対して一意に振られた番号です。対応する ppp インターフェースのユニット番号となります。No.0 に対応するネットワークインターフェース名は"ppp0"です。

■ 接続名称

「PPP(発信)設定編集」ダイアログで設定した名称です。

■ デバイス

使用するデバイス名です。

■ 接続状態

PPP 接続の状態を示します。

表示	説明
未接続	ppp インターフェースが停止している状態。
接続処理中	発信を開始し、ダイアルや PPP 接続処理を行っている状態。
接続中	PPP が接続完了し、IP 通信ができる状態。
休止	DEMAND 接続において、peer へのトラフィック発生時に自動発信できる状態。
回線断	発信時のエラーや、相手側から切断された後の状態。要因については、Syslog(ppp)を参照して確認します。
デバイス無し	使用するデバイスが、USB モデムなどの取り外し可能デバイスの場合に、当該デバイスが検出できない状態。

■ Local IP / Remote IP

PPP 接続の自分側と相手側の IP アドレスです。接続状態が「接続中」の場合は、IPCP によりネゴシエートされたアドレスが表示されます。

■ **制御**

接続制御ボタンを配置します。接続状態によって配置されるボタンが異なります。接続制御については、次節(3.1.3.4)に示します。

3.1.3.4. 接続制御

制御カラムにある「接続」「停止」「切断」ボタンは、基本的には PPP デーモン(pppd)の起動(「接続」)と終了(「停止」,「切断」)を行います。「接続方式」で「通常」, 「PERSIST」, 「DEMAND」の指定により PPP 接続の挙動が異なります。挙動については、下記にて説明します。

■ **「接続方式」=「通常」**

No.	接続名称	デバイス	接続状態	Local IP	Remote IP	制御
0	e-mobile	emobile(USB)	未接続	---	---	接続

① “通常”の選択の場合、PPP 接続/切断は全て手動にて行います。「接続」ボタンを押すと、以下のダイアログが表示されます。

② その後、「PPP 設定/状態」で接続状態は以下の通り推移します。

No.	接続名称	デバイス	接続状態	Local IP	Remote IP	制御
0	e-mobile	emobile(USB)	接続処理中	---	---	停止

↓ しばらくして「更新」ボタンを押す

No.	接続名称	デバイス	接続状態	Local IP	Remote IP	制御
0	e-mobile	emobile(USB)	接続中	114.48.1.100	10.64.64.64	切断

③ PPP 接続が正常に確立すると「接続状態」は、「接続処理中」から「接続中」に推移し、「Local IP」, 「Remote IP」欄に IP アドレスが表示されます。PPP 接続を終了させる場合は「切断」ボタンを押下すると以下のポップアップメニューが表示されセッションを終了します。

■ 「接続方式」=「PERSIST」

「PERSIST」の PPP 接続設定を新規に追加した直後は、PPP デーモンは起動していません。「通常」の場合と同じく手動により PPP 接続/切断を行います。

MA-E2xx を再起動した場合は PPP デーモンが起動し、PPP 接続は自動的に行われます。相手先から切断されても自動的に再接続処理を行い、常時接続を行います。

「PPP 設定/状態」にて「接続」、「切断」操作を行った場合は強制的に PPP デーモンを起動、終了させることになります。

■ 「接続方式」=「DEMAND」

① 「DEMAND」の PPP 接続設定を新規に追加した直後は、最初の「接続」ボタンで PPP デーモンを起動します。この時点では PPP 接続は行われません。(接続状態=「休止」)

No.	接続名称	デバイス	接続状態	Local IP	Remote IP	制御
0	e-mobile	emobile(USB)	休止	10.64.64.64	10.112.112.112	接続 切断

② 休止状態のとき、**MA-E2xx** からリモートへの IP 通信がある場合に自動的に PPP 接続を開始します。WebUI から強制的にリモートへの PPP 接続を開始する場合は「接続」ボタンを再度押下することでリモートへ対し ping を送信し、以下のダイアログを表示します。

③ PPP 接続が正常に確立すると「接続状態」は、「休止」から「接続中」に変わります。

No.	接続名称	デバイス	接続状態	Local IP	Remote IP	制御
0	e-mobile	emobile(USB)	接続中	114.48.35.69	10.112.112.112	切断

接続確立後、無通信状態のまま接続設定の「アイドル検知時間」で指定した時間が経過すると、回線を自動的に切断し「休止」状態に戻ります。

④ 「切断」ボタンを押すと、以下のダイアログを表示し PPP インターフェースを停止します。

接続状態は「未接続」となり、PPP デーモンは終了し、以降の DEMAND 接続が出来なくなります。

No.	接続名称	デバイス	接続状態	Local IP	Remote IP	制御
0	e-mobile	emobile(USB)	未接続	---	---	接続

再び DEMAND 接続を行えるようにするには、①の操作を行い接続状態を「休止」状態にして下さい。

3.1.4. PPP(着信)設定

PPP(Point-to-Point Protocol)の着信設定を行います。

3.1.4.1. 接続設定

■ **PPP 着信機能**

➢ PPP 着信

着信機能を使用する場合は、「使用する」をチェックして「設定」ボタンを押下して下さい。

着信機能を使用しない場合は、チェックを外して「設定」ボタンを押下して下さい。

■ **モデム設定**

- デバイス
  プルダウンメニューにあるデバイス一覧から、対象となるデバイスを指定します。PPP(発信)設定の、「利用可能デバイス一覧」表中の「着信可否」項目が"可"と表示されているデバイスが、プルダウンメニューに表示されます。

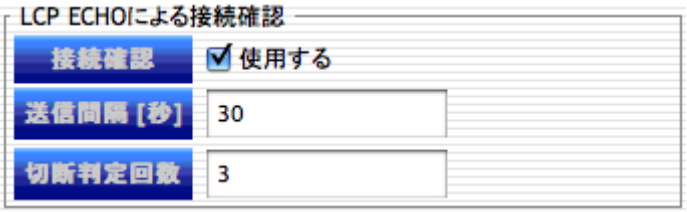
- アイドル検知時間(秒)
  「アイドル検知時間」で指定した期間、IP 通信の無通信状態が持続すると切断処理を行います。
  「アイドル検知時間」=“0”は、自動で切断処理を行わない場合に指定します。(=常に手動で切断処理を行う)

- モデム初期化コマンド
  モデム接続時に AT コマンドでモデムを初期化するコマンドを指定します。

- Deflate 圧縮
  データ圧縮方式で Deflate 圧縮(RFC1951)を使用する場合はチェックします。

- VJ 圧縮
  データ圧縮方式で VJ 圧縮(RFC1144)を使用する場合はチェックします。

■ **LCP ECHO による接続確認**

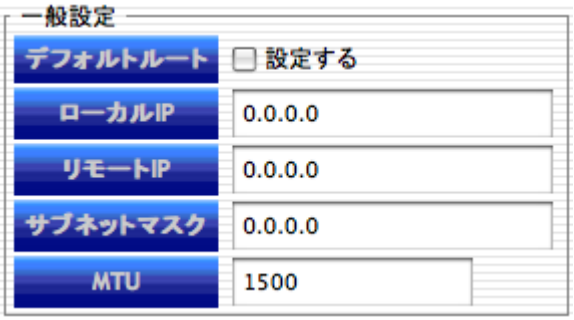


- 接続確認
  LCP ECHO による接続監視を行う場合はチェックします。

- 送信間隔(秒)
  LCP ECHO Request パケットを送信する間隔を指定します。

- 切断判定回数
  MA-E2xx から送信される LCP ECHO Request に対して連続無応答の回数を閾値として指定します。
  「切断判定回数」の回数、連続無応答状態が継続すると PPP セッションの切断を実行します。

■ **一般設定**



➢ デフォルトルート

PPP リンクをデフォルトルートとして設定する場合はチェックします。

➢ ローカル IP

PPP リンクのローカル(**MA-E2xx**)側の IP アドレスを手動で設定する場合は IP アドレスを入力します。相手の設定に従う場合は“0.0.0.0”を指定して下さい。

➢ リモート IP

PPP 接続リンクのリモート(相手)側の IP アドレスを手動で設定する場合は IP アドレスを入力して下さい。相手の設定に従う場合は“0.0.0.0”を指定して下さい。

➢ サブネットマスク

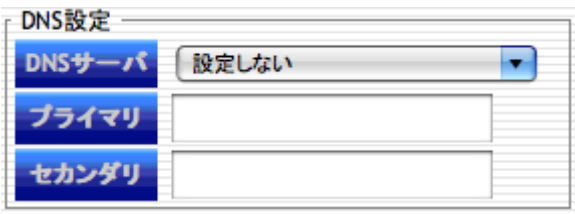
サブネットマスクを設定します。この設定したネットマスクと次のネットマスクの論理和が値となります。

- ネゴシエートするリモート側の IP アドレス・クラスに適切なネットマスク
- リモート側と同一ネットワーク上システムの非 point-to-point ネットワークインターフェースのネットマスク

➢ MTU

PPP リンクの MTU を設定します。(バイト)

■ **DNS 設定**



➢ DNS サーバ

PPP 着信時に通知する、DNS サーバのアドレスを指定します。

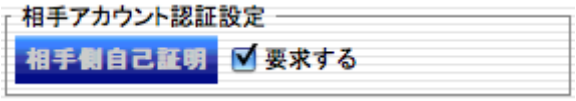
✓ 設定しない

PPP 着信時に DNS サーバのアドレスを通知しません。

✓ 指定アドレスを設定
以下の「プライマリサーバ」と「セカンダリサーバ」に設定したアドレスを、DNS サーバの
アドレスとして通知します。

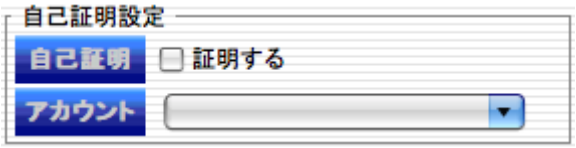
✓ 本機器のローカル IP を設定
以上の「一般設定」の「ローカル IP」に設定したアドレスを、DNS サーバのアドレスとして通知します。
「ローカル IP」に“0.0.0.0”と設定した場合は LAN 側の IP アドレスを DNS サーバのアドレスとして
通知します。

■ **相手アカウント認証設定**



➢ 相手アカウント認証設定
着信時に、アカウント認証を行う場合は「要求する」にチェックします。このアカウント認証は「PPP(着信)アカウント編集」に設定されているアカウントが対象となります。

■ **自己証明設定**



➢ 自己証明
着信時に自己証明を行う場合はチェックします。

➢ アカウント
自己証明のアカウントを指定して下さい。このアカウントは「PPP(着信)アカウント編集」タブに設定されているアカウントから選択します。

3.1.4.2. PPP(着信)アカウント編集

「PPP の着信用アカウント設定」を新規に追加する場合は「着信用アカウント設定」のタブから「追加」ボタンを押してください。次の編集ダイアログが表示されます。

■ **アカウント**

着信時の認証（相手アカウント認証・自己証明）に使用されるアカウント（ID）を設定します。

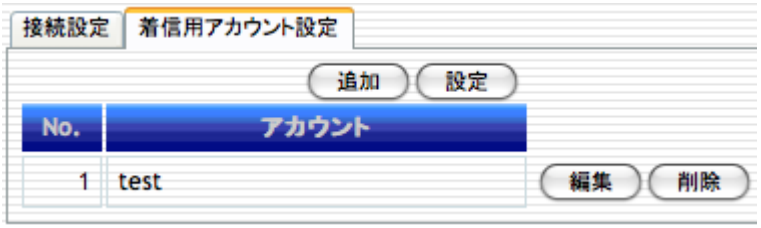
■ **パスワード**

上記アカウントに対応したパスワードを設定します。

■ **パスワード(確認)**

上記パスワードと同じものを確認用に再度入力して下さい。

「PPP(着信)アカウント編集」の各項目を指定して「OK」ボタンを押すと、「Cancel」を押すと、追加／編集を取りやめます。設定が完了すると以下の通り、「着信用アカウント設定」が表示されます。



各行右端の「編集」ボタンを押下すると、パラメータの編集が行えます。「削除」ボタンを押下すると、当該行の設定が削除されます。「設定」ボタンを押下する事で変更内容が **MA-E2xx** に反映されます。

3.1.5. DHCP サーバ設定

「DHCP サーバ設定」画面では DHCP クライアント機能の状態確認と、DHCP サーバ機能の設定を行います。

3.1.5.1. 現在の eth0 の設定

DHCP サーバは、eth0 で稼動させることができます。「インターフェース設定」において、eth0 へ固定 IP アドレスを設定する必要があります。

「現在の eth0 の設定」では eth0 の状態を確認できます。

「インターフェース設定」で eth0 の DHCP を有効にしていると上記のような表示になります。DHCP を無効にしていると、以下の表示になります。

3.1.5.2. DHCP サーバ設定

「DHCP サーバ設定」では、以下の項目の入力が完了した後、「設定」ボタンを押下して変更内容を **MA-E2xx** に反映させます。

- **DHCP サーバ機能**

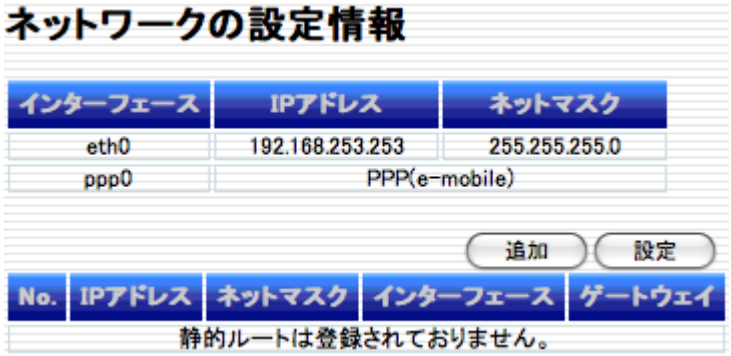
  DHCP サーバを利用する場合チェックします。

- **リース範囲設定**

  DCHP クライアントに割り当てる IP アドレスの範囲を指定します。

3.1.6. 静的ルーティング設定

静的ルーティング設定を行います。



新規にルーティング設定を追加したい場合は「追加」ボタンを押すと、次の設定画面が表示されます。

アドレス、ネットマスク、インターフェース、ゲートウェイの項目を指定して「適用」ボタンを押下すると、その設定が一覧に追加されます。追加を取り止めたい場合は「中止」ボタンを押して下さい。設定が完了すると以下の通り、ルーティング設定が表示されます。この時点ではまだ、**MA-E2xx** へ対してルーティングの設定は行われていません。

各行右端の「編集」ボタンを押すと、パラメータの編集が行えます。「削除」ボタンを押すと、当該行の設定が削除されます。

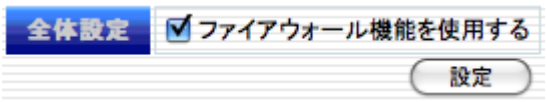
必要項目の入力が完了した後、「設定」ボタンを押して変更内容を **MA-E2xx** に反映させます。

3.1.7. ファイアウォール設定

ファイアウォール設定は、次の設定を行います。

項目	説明
ゾーン設定	インターフェースごとにファイアウォールの内側か外側かを決めます。
NAPT 設定	NAPT を行うインターフェースの設定を行います。
ルール設定	パケットフィルタリングルールおよび、ポートフォワーディングルールを設定します。
1 対 1NAT 設定	仮想 IP アドレスを定義し、実アドレスとの NAT を設定します。

3.1.7.1. 全体設定



「ファイアウォール」のデフォルトポリシーは、ローカル側インターフェースからの接続を許可し、インターネット側インターフェースからの接続を遮断します。

「ファイアウォール機能を使用する」をチェックし、「設定」ボタンを押すことでファイアウォール機能が有効になります。このボタンは、以降説明する全てのパラメータを入力後、最後に実行して下さい。

3.1.7.2. ゾーン設定

MA-E2xx で定義されているインターフェースの一覧が表示されます。インターフェース毎にゾーン定義(「ローカル側」,「インターネット側」)を行います。インターネット側とは、ファイアウォールの外側を意味します。ローカル側とはファイアウォールの内側です。

上記の例では、eth0 と ppp50 がローカル側、ppp0 がインターネット側です。

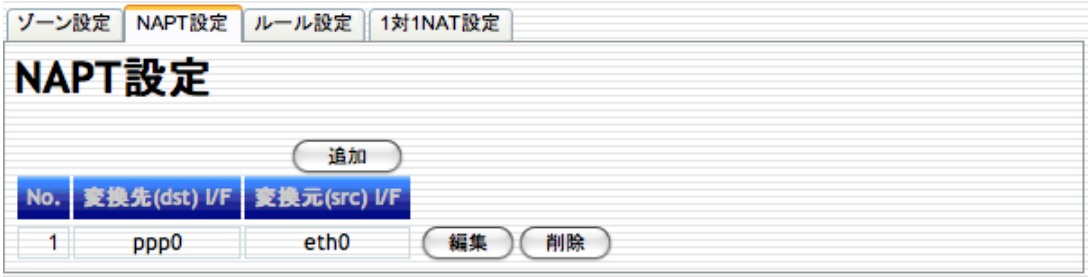
3.1.7.3. NAPT 設定

NAPT の変換先インターフェース・変換元インターフェースを定義します。変換元から変換先へフォワードするパケットのソースアドレスを、**MA-E2xx** のアドレス(変換先インターフェースに設定されているアドレス)に変換します。

「NAPT 設定」のタブから「追加」ボタンを押下すると次の設定画面が表示されます。

通常、「変換先(dst) I/F」にインターネット側(WAN)を指定し、「変換元(src) I/F」にローカル側の I/F を指定します。

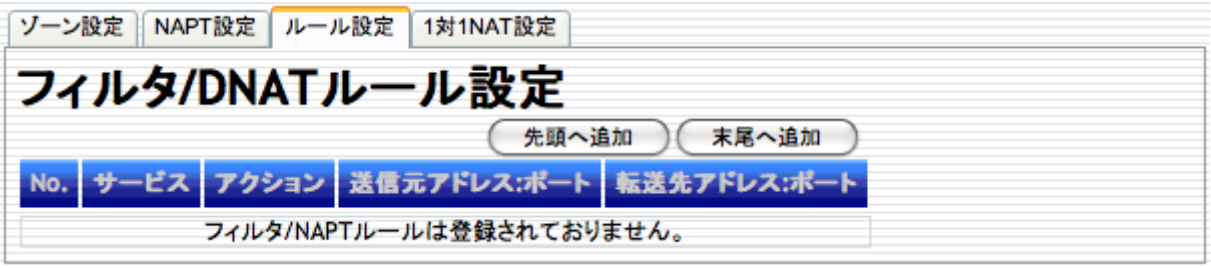
各項目を指定して「OK」ボタンを押下すると、その設定が追加されます。途中で操作を取り止めたい場合は「Cancel」ボタンを押下して下さい。設定が完了すると以下の様な表示になります。



各行右端の「編集」ボタンを押すと、パラメータの編集が行えます。「削除」ボタンを押すと、当該行の設定が削除されます。

3.1.7.4. ルール設定

インターネット側からローカル側方向のフィルタリング設定および、ポートフォワーディング設定を行います。ファイアウォールのデフォルトポリシーは、ローカル側からの接続を許可し、インターネット側からの接続を遮断します。ここで設定するルールとは、このポリシーに対する例外です。



新規にルールを追加する場合は「先頭へ追加」または「末尾へ追加」ボタンを押します。ボタンを押した後、「フィルタ/NAPT ルール設定画面」が表示されます。

■ **サービス**

プルダウンメニューにてフィルタの対象となるサービスを選択します。「Port/Protocol」を選択時は、ポート番号及びプロトコルの指定が必要になります。それ以外のサービスの種類ではポート番号、プロトコルの入力は必要ありません。現在指定可能なサービスの品目は次の通りです。

“Port/Protocol”, “Amanda”, “Auth”, “Bit Torrent”, “CVS”, “DNS”, “Distcc”, “Edonkey”, “FTP”, “Finger”, “GRE”, “Gnutella”, “HTTP”, “HTTPS”, “ICQ”, “IMAP”, “IMAPS”, “IPIP”, “IPP”, “IPPserver”, “IPsec”, “IPsecah”, “IPsecnat”, “Jetdirect”, “L2TP”, “LDAP”, “LDAPS”, “MySQL”, “NNTP”, “NNTPS”, “NTP”, “NTPbrd”, “PCA”, “POP3”, “POP3S”, “Ping”, “PostgreSQL”, “Printer”, “RDP”, “Rdate”, “Rsync”, “SMB”, “SMBBI”, “SMBswat”, “SMTP”, “SMTPS”, “SNMP”, “SPAMD”, “SSH”, “SVN”, “SixXS”, “Submission”, “Syslog”, “TFTP”, “Telnet”, “Telnets”, “Time”, “VNC”, “VNCL”, “Web”, “Webmin”, “Whois”

■ **ポート番号**

対象パケットのポート番号を指定します。

「サービス」にて「Port/Protocol」を選択した場合にのみ指定できます。

■ **プロトコル**

対象パケットのプロトコルを指定します。プロトコルで指定できる項目は、「TCP」, 「UDP」, 「ICMP」の 3 種類です。「サービス」にて「Port/Protocol」を選択した場合にのみ指定できます。

■ **アクション**

対象パケットに対する動作を選択します。

許可(ACCEPT)	指定したサービスまたはプロトコルの、インターネット側からの通信を許可します。
拒否(REJECT)	指定したサービスまたはプロトコルの、インターネット側からの通信を拒否します。
ポート転送(DNAT)	指定したサービスまたはプロトコルを、ローカル側の IP アドレス、ポートに対して転送します。

■ **送信元アドレス/ポート番号**

対象パケットの送信元アドレスまたはネットワークを指定します。IP アドレス(x.x.x.x)か、CIDR 形式(x.x.x.x/x)を入力して下さい。空欄の場合、送信元アドレスの限定をしません。

送信元ポート番号は 0 から 65535 までの数値で指定して下さい。空欄の場合、送信元ポート番号を限定しません。

■ **転送先アドレス/ポート番号**

対象パケットの転送先アドレスを指定します。ローカル側の IP アドレス(x.x.x.x)を入力して下さい。転送先ポート番号は 0 から 65535 までの数値で指定して下さい。

宛先が **MA-E2xx** 自身の場合は、空にしてください。

■ **変換前アドレス**

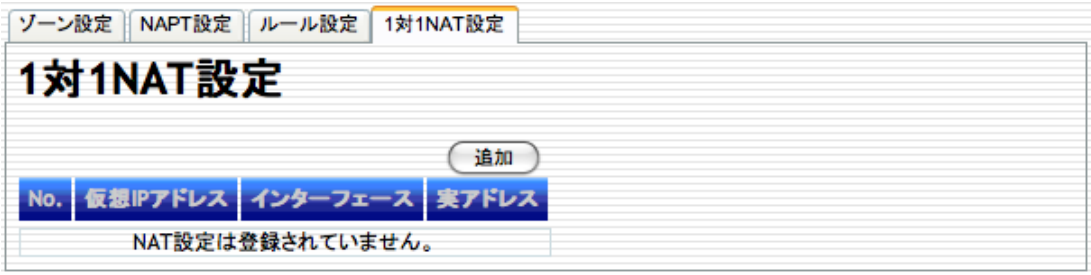
対象パケットの NAT 変換前の転送先アドレスを指定する場合は、IP アドレス(x.x.x.x)を入力して下さい。

「フィルタ/NAPT ルール編集」の項目を指定して「OK」ボタンを押下すると、その設定が追加されます。追加を取り止めたい場合は「Cancel」ボタンを押下して下さい。設定が完了すると以下の通り、「フィルタ/NAPT ルール」設定が表示されます。

各行右端の「編集」ボタンを押下すると、パラメータの編集が行えます。「削除」ボタンを押すと、当該行の設定が削除されます。また「No.」欄の各行のフィルタをドラッグすることで、ルールの並べ替えを行えます。

3.1.7.5. 1 対 1NAT 設定

仮想 IP アドレスと、実アドレスの NAT を設定します。仮想 IP アドレスは、指定したインターフェースに追加される IP エイリアスです。



「追加」を押すと、「1 対 1NAT 編集」ダイアログを表示します。

■ **仮想 IP アドレス**

作成する仮想 IP アドレス(x.x.x.x)を入力して下さい。

■ **インターフェース**

仮想 IP アドレスを追加するインターフェースを選択してください。

■ **実アドレス**

存在する IP アドレス(x.x.x.x)を入力して下さい。

「1 対 1NAT 編集」の項目を指定して「OK」ボタンを押下すると、その設定が追加されます。追加を取り止めたい場合は「Cancel」ボタンを押下して下さい。設定が完了すると以下の通り、「1 対 1NAT 設定」が表示されます。

各行右端の「編集」ボタンを押下すると、パラメータの編集が行えます。「削除」ボタンを押すと、当該行の設定が削除されます

ファイアウォールの内外で 1 対 1NAT を行う場合は、「ルール設定」で実アドレスへの許可ルールを設定してください。

3.1.8. 日付・時刻設定

「日付・時刻設定」画面では、システム時刻の変更を行うことができます。

「日付」欄をクリックすると、カレンダーが表示されますので、現在の日付をカレンダーにて指定して下さい。各項目を入力し、「設定」ボタンを押すとシステム時刻が更新されます。「更新」ボタンは最新のシステム時刻を表示させる際に使用します。

3.2. サービス設定

3.2.1. NTP 設定

NTP 設定は、指定された外部 NTP サーバとシステムクロックを同期させます。

■ **全体設定**

NTP デーモンを稼動させる場合チェックします。

■ **サーバ動作**

MA-E2xx を eth0 ネットワークの DHCP サーバとして稼動させる場合に、DHCP クライアントからの NTP サーバオプションに対して **MA-E2xx** のアドレスを返すかどうかを指定します。

■ **NTP サーバ設定**

上位 NTP サーバの IP アドレスもしくは FQDN を指定します。FQDN を指定する場合は名前解決が行えるよう「インターフェース設定」画面で DNS の設定をして下さい。

それぞれの項目を指定し入力が完了した後、「設定」ボタンを押下して変更内容を **MA-E2xx** に反映させます。

3.3. アプリケーション設定

3.3.1. 死活監視設定

MA-E2xx の Ether0 ポートに接続された機器を定期的な ping コマンドにより診断し、死活監視を行う機能です。
ポーリング条件内での応答がない場合は E-mail にて通知することが可能です。

3.3.1.1. 監視設定

■ **<u>「ポーリング条件設定」</u>**

✧ ポーリング間隔

Ping コマンドのポーリング間隔を指定します。間隔時間は 30, 60, 90, 120 秒で指定可能です。

✧ リトライ回数

「リトライ回数」で定義した回数を超えて Ping コマンドに対して連続して無応答だった場合異常と判定します。
回数は 10 回まで指定可能です。

■ **<u>監視対象ホスト設定</u>**

「監視対象ホスト設定」で新規に監視対象ホストを追加したい場合は「追加」ボタンを押下します。ボタンを押下した後、「監視対象の編集」が表示されます。監視対象ホストとして登録できる上限は最大 7 個までです。

■ **IP アドレス**

監視対象ホストの IP アドレスを指定します。

■ **備考**

監視対象ホストに関する備考を追加することが可能です。備考の情報はメール通知時の「本件」と「本文」に HostName として使用されます。また空欄の場合は「IP:***.***.***.***」が自動的に挿入されます。

■ **有効/無効**

監視対象として有効にする場合はチェックします。

必要項目の指定の後、「適用」ボタンを押下すると、その設定が追加されます。途中で操作を取り止めたい場合は「中止」ボタンを押下して下さい。設定が完了すると以下の通り、「監視対象ホスト設定」が表示されます。

各行右端の「編集」ボタンを押下するとパラメータの編集が行えます。「削除」ボタンを押下すると当該行の設定が削除されます。一覧にある監視対象を一括して有効にしたい場合は「全て有効」ボタンを無効にしたい場合は「全て無効」ボタンを押下して下さい。

3.3.1.2. 通知先設定

■ <u>E-Mail 通知</u>

✧ 送信先メールアドレス

E-mail 通知の送信先メールアドレスを指定します。最大 3 ヶ所まで登録できます。

※名前解決が行えるよう「インターフェース設定」画面で DNS の設定をして下さい。

✧ 有効

E-mail 通知を利用する場合は当該送信先メールアドレスをチェックします。

注）「通知先設定」は、下記「E-Mail 設定」を先に設定しないと入力出来ません。

3.3.1.3. E-Mail 設定

■ **必須項目**

✧ 有効/無効

E-Mail アカウントを有効にする場合はチェックします。

✧ SMTP サーバ名

SMTP サーバを IP アドレスもしくは FQDN で指定します。

✧ POP3 サーバ名

POP3 サーバを IP アドレスもしくは FQDN で指定します。

✧ ユーザ ID

POP3 のユーザ ID を入力します。

✧ パスワード

上記ユーザ ID に対応するパスワードを入力します。

✧ 名前

E-Mail の差出人の名前を設定します。

✧ メールアドレス

差出人の E-Mail のアドレスを入力します。

■ **オプション項目**

✧ SMTP ポート

SMTP ポート番号を指定可能です。デフォルトは 25 です。

✧ POP3 ポート

SMTP ポート番号を指定可能です。デフォルトは 110 です。

✧ 認証方式

「SMTP 認証」「POP Before SMTP 認証」「SMTP over TLS 認証」「認証なし」からメールサーバへの認証方式を指定することが可能です。

尚、「SMTP over TLS 認証」は“Submission over TLS” (SMTP ポート番号: 587)および“SMTP over SSL”(SMTP ポート番号: 465)の2種類を意味しますので、プロバイダやメールサーバの指定するポート番号を確認して設定して下さい。

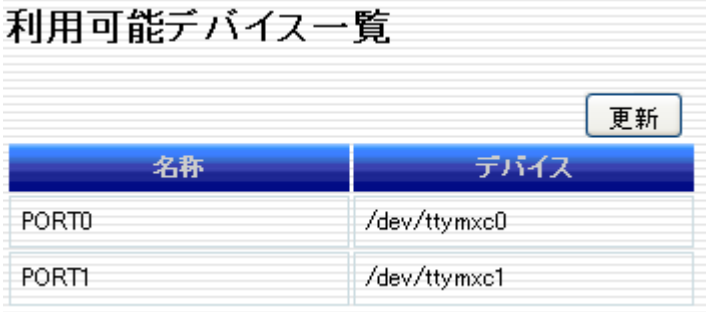
3.4. シリアル監視設定

3.4.1. ser2net 設定

ser2netはプロトコル変換を行い、シリアルで繋がれた機器をネットワーク経由で使用可能にする機能です。
ser2netは特定のTCPポートでネットワークから接続を待ち受けており、TCP接続が確立するとシリアルポートをオープンします。TCPポートから受信したPCデータをシルアルポートへ送信し、シリアルポートから受信したデータをTCPポートへ送出します。

3.4.1.1. 利用可能デバイス一覧

「利用可能デバイス一覧」では、ser2net を利用したシリアル監視・制御可能なデバイスの一覧が表示されます。



※注意事項

Modem(PORT0)または、Modem(PORT1)を使用する場合は、/etc/inittab のシリアル設定を以下のように変更してください。

SERIAL CONSOLES

#mxc0:12345:respawn:/sbin/agetty 115200 ttymxc0 vt100

↑PORT0 をモデムとして使用する場合、先頭に#を付けてコメントアウト

#mxc1:12345:respawn:/sbin/agetty 115200 ttymxc1 vt100

↑PORT1 をモデムとして使用する場合、先頭に#を付けてコメントアウト

3.4.1.2. サービス設定

■ **サービス**

ser2net サービスを使用する場合にチェックします。

■ **制御ポート**

ser2net デーモンをネットワーク側から制御する場合にチェックします。

■ **制御ポート番号**

ser2net デーモン制御用の、TCP のポート番号を設定します。

設定したTCPポートからtelnetログインする事ができ、コマンドを発行する事でシリアル制御信号の操作、ポート状態の確認、コネクションの切断ができます。

制御ポートでは次のコマンドが使用できます。

```
exit - leave the program.
help - display this help.
version - display the version of this program.
monitor <type> <tcp port> - display all the input for a given port on
       the calling control port.  Only one direction may be monitored
       at a time.  The type field may be 'tcp' or 'term' and specifies
       whether to monitor data from the TCP port or from the serial port
       Note that data monitoring is best effort, if the controller port
```

```
        cannot keep up the data will be silently dropped.  A controller
        may only monitor one thing and a port may only be monitored by
        one controller.
monitor stop - stop the current monitor.
disconnect <tcp port> - disconnect the tcp connection on the port.
showport [<tcp port>] - Show information about a port. If no port is
        given, all ports are displayed.
showshortport [<tcp port>] - Show information about a port in a one-line
        format. If no port is given, all ports are displayed.
setporttimeout <tcp port> <timeout> - Set the amount of time in seconds
        before the port connection will be shut down if no activity
        has been seen on the port.
setportconfig <tcp port> <config> - Set the port configuration as in
        the device configuration in the ser2net.conf file.  Valid options
        are: 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200,
        EVEN, ODD, NONE, 1STOPBIT, 2STOPBITS, 7DATABITS, 8DATABITS,
        LOCAL (ignore modem control), [-]RTSCTS, [-]XONXOFF.
        Note that these will not change until the port is disconnected
        and connected again.
setportcontrol <tcp port> <controls>
        Dynamically modify the characteristics of the port.  These are
        immedaite and won't live between connections.  Valid controls are
        DTRHI, DTRLO, RTSHI, and RTSLO.
setportenable <tcp port> <enable state> - Sets the port operation state.
        Valid states are:
          off - The TCP port is shut down
          raw - The TCP port is up and all I/O is transferred
          rawlp - The TCP port is up and the input is transferred to dev
          telnet - The TCP port is up and the telnet negotiation protocol
               runs on the port.
```

3.4.1.3. ポート設定

「追加」ボタンを押下すると、以下のポップアップメニューが表示されます。

■ **デバイス**

接続するデバイスを指定します。指定された TCP ポートを、このデバイスに接続されたシリアル装置へリダイレクトします。

■ **動作モード**

TCP ポートの状態制御を指定します。

✓ off

起動時に TCP ポートは無効になっていますが、制御ポートから動作モードを変更することによって接続できるようになります。

✓ raw

TCP ポートを raw モードで接続可能にします。

✓ rawlp

TCP ポートを rawlp モードで接続可能にします。

✓ telnet

TCP ポートを telnet モードで接続可能にします。

■ **ポート番号**

接続用の TCP のポート番号を設定します。

この TCP ポートを、指定したデバイスに接続されたシリアル装置へリダイレクトします。

■ **タイムアウト**

ここで指定した時間（秒）無通信の状態が続くと TCP セッションを切断します。"0"を指定した場合、本機能は無効となります。動作モードに"telnet"を選択した場合は、"0"を指定されることをお勧めします。

■ **BPS**

RS232 ポートのボーレートを指定します。

■ **パリティ**

RS232 ポートのパリティを指定します。

- ✓ なし
- ✓ 偶数
- ✓ 奇数

■ **ストップビット**

RS232 ポートのストップビットを指定します。

■ **データ長**

RS232 ポートのデータ長を指定します。

■ **フロー制御**

RS232 ポートのフロー制御を指定します。

- ✓ なし
  制御信号を無視します。
- ✓ Software Flow
  ソフトウェアフロー制御をおこないます。
- ✓ Hardware Flow
  ハードウェアフロー制御をおこないます。

■ **モデム制御ライン**

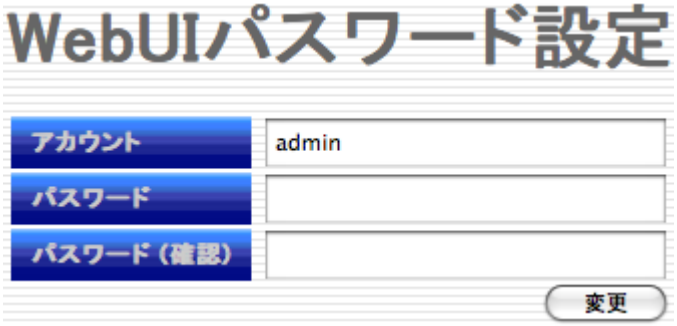
モデム制御ラインを監視するか設定します。

■ **リモートコントロール**

シリアルポートのリモートコントロール機能を設定します（RFC2217 対応）。

3.5. 保守・運用

3.5.1. WebUI パスワード設定



WebUI のログイン アカウント及びパスワードを変更したい場合に使用します。登録できるアカウントは一つだけです。アカウントの追加はできません。

3.5.2. Syslog 確認

各ログファイルの内容を表示します。
「ログファイルの選択」で「全て(everything)」、「カーネル関係(kernel)」、「PPP 関係(ppp)」、「SSH 関係(sshd)」
を選択し、指定したログファイルを確認することができます。

3.5.3. Ping 疎通テスト

指定ホストに対して ping コマンドを実行します。

■ **ホスト選択・アドレス指定**

「手入力」または後述のホスト設定に登録された備考欄のホスト名がプルダウンメニューで指定できます。「手入力」の場合は IP アドレスもしくは FQDN で指定ください。FQDN で指定をする場合は名前解決が行えるよう「インターフェース設定」画面で DNS の設定をして下さい。

■ **ホスト設定**

「ホスト設定」で新規に ping ホストを追加したい場合は「追加」ボタンを押下します。ボタンを押下した後、「ping 対象ホストの編集」が表示されます。

■ **IP アドレス**

監視対象ホストの IP アドレスを指定します。

■ **備考**

監視対象ホストに関する備考を追加することが可能です。

必要項目の指定の後、「適用」ボタンを押すと、その設定が追加されます。途中で操作を取り止めたい場合は「中止」ボタンを押して下さい。設定が完了すると、「ホスト設定」が表示されます。

各行右端の「編集」ボタンを押すと、パラメータの編集が行えます。「削除」ボタンを押すと、当該行の設定が削除されます。

3.5.4. 設定データ管理

3.5.4.1. 設定ファイルダウンロード

WebUI にて編集した各種設定をファイルとしてパソコンにダウンロードします。「ダウンロード」ボタンを押下することで実行されます。

3.5.4.2. 設定ファイルアップロード

「設定ファイルダウンロード」画面でダウンロードした設定ファイルを **MA-E2xx** に取り込み、設定を復元します。テキストボックスにファイル名を入力するか、「参照」ボタンで当該ファイルの選択し、「アップロード」ボタンを押下することで実行されます。

注1) 設定ファイルをエディタで編集する際、日本語文字は含めないで下さい。設定ファイルが読込み不能になる場合があります。

注2) 設定ファイルをアップロード後、通常再起動は不要ですが、以下の条件で設定変更を行った際は再起動が必要になります。
- 当該する設定項目: インターフェース設定
  ※前述の設定項目の初期値に対して変更を行い、設定ファイルを保存し、初期化→再起動→設定ファイルアップロードの順番で行った場合、この状態では、設定アップロードを実行しても初期化の状態が有効になり再起動をするまで反映されません。

注3) WebUI アカウント/パスワードを変更した設定ファイルを別の **MA-E2xx**(例:工場出荷時設定)にアップロードする場合、アップロード完了直後に設定ファイルのアカウント/パスワードが有効になります。そのため、WebUI で操作を行う際に、認証エラーが表示されたら、一旦ログアウトして設定ファイルのアカウントでログインし直してください。

3.5.4.3. 設定データを本体に保存

WebUI によって編集された各種設定を本体に保存します。「保存」ボタンを押下して実行されます。

3.5.4.4. 設定データ初期化

WebUI の設定データを出荷時デフォルト値に初期化する場合に、「設定初期化」ボタンを押下して実行されます。直後に「設定データを初期化しました。再起動して下さい。」のメッセージが現れ、「装置再起動/シャットダウン」のメニューに移行しますので、「シャットダウン」「再起動」のボタンを押下して下さい。

注1) WebUI アカウント/パスワードを変更した場合、初期化を実行した直後にアカウント/パスワードは工場出荷時設定(user: admin / password: admin)にリセットされます。「再起動」「シャットダウン」操作を行う際に、認証エラーが表示されたら、一旦ログアウトして工場出荷時アカウントでログインして下さい。

3.5.5. ファームウェア更新

MA-E2xx のファームウェアを更新します。パソコン上のファームウェアイメージファイルを、WebUI を経由して **MA-E2xx** に送信します。※出荷時のファームウェアは、同梱 CD の「Firmware」フォルダに格納されています。

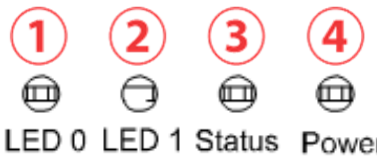
送信に成功すると、ファイルサイズと MD5 値を表示するので、正しい値かどうか確認して下さい。

「モード選択」にて設定データを保持してファームウェアをアップデートする場合は「設定データはそのまま」を指定して下さい。設定データを初期化する場合は「設定データをクリア」を選択して下さい。

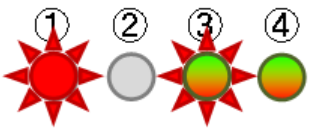
確認後、「開始」ボタンを押すと書き込みを開始します。書き込み中は、Web アクセスを含む一切のネットワークサービスを停止します。書き込みには数分を要します。尚、この操作の間は、絶対に電源を切らないでください。更新中に誤ってこれらを行うと、システムボードの交換が必要となる場合があります。この場合、弊社 FutureNet サポートデスク(support@centurysys.co.jp)にご相談下さい。

ファームウェア更新中の **MA-E2xx** 本体の LED 表示は以下の通りです。

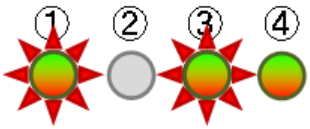
※ここでは説明のため、各 LED を次のように表現します。



① red： 点滅(200msec 毎)， ③ red/green 交互点灯(500msec 毎)，
④ green： 点灯, red：Heartbeat = kernel 更新中



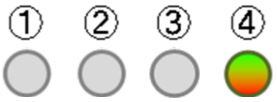
①③ red/green 交互点灯(500msec 毎)
④ green： 点灯, red：Heartbeat = rootfs アップデート時



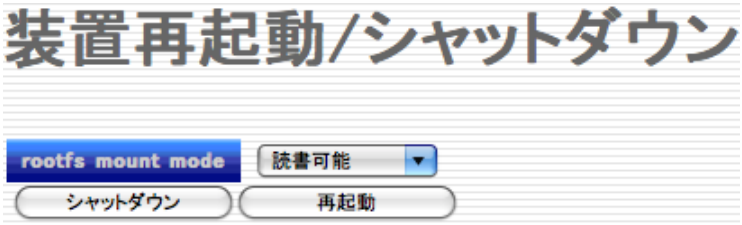
書き込みが正常終了すると、LED の赤点滅は消え、新しいファームウェアで再起動します。正常に起動した時の LED 表示は下記の通りです。

③ red：SDCard アクセス LED

④ green： 常に点灯, red：Heartbeat



3.5.6. 再起動/シャットダウン



「rootfs mount mode」は、次回起動する際に、rootfs を「読書可能」または「読込専用」モードに設定できます。どちらかを指定して、「シャットダウン」「再起動」の操作を行ってください。

「シャットダウン」ボタンを押すと **MA-E2xx** をシャットダウンします。「再起動」ボタンは、再起動を実行します。また「シャットダウン」「再起動」操作前に変更した各種設定は **MA-E2xx** 本体へ自動的に保存された後に実行されます。

3.5.7. ログアウト

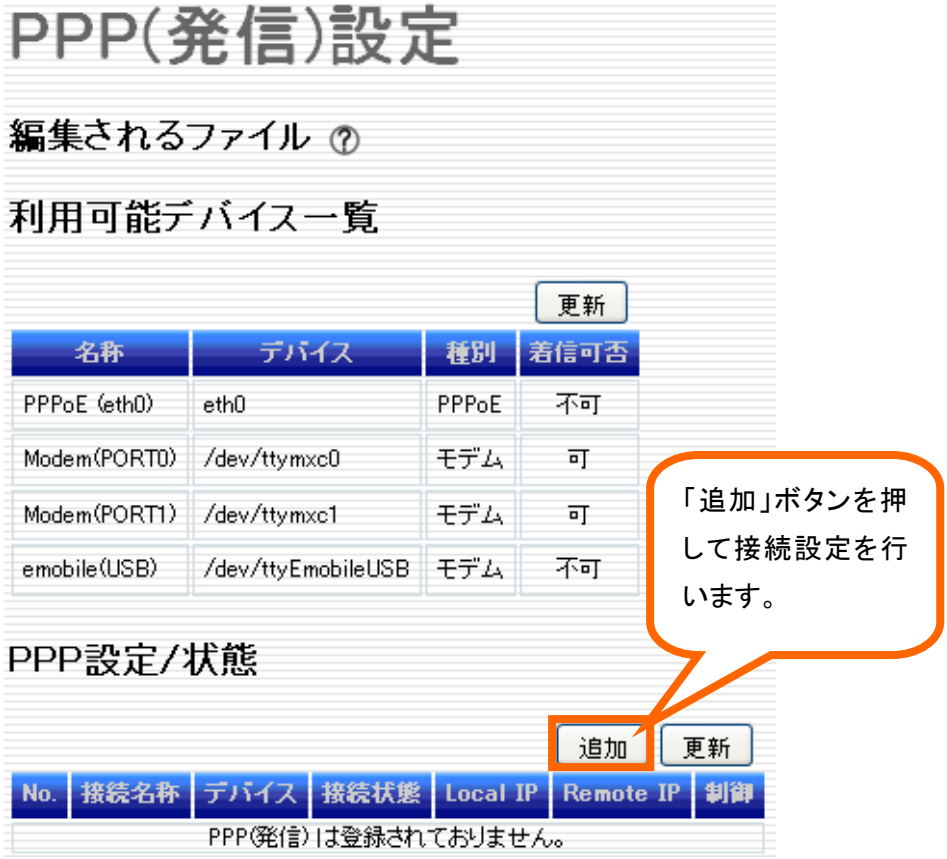
「ログアウト」ボタンを押下することで WebUI からログアウトします。

4. 設定例

4.1. e-mobile 接続の設定例

e-mobile の USB ドングルを利用して、インターネット接続サービスへ接続する設定例を示します。この例では、PPP の接続方式は「通常」を選択し、画面操作による手動での接続／切断を行います。

「PPP(発信)設定」画面で、接続設定を行います。



「追加」ボタンを押下し「PPP（発信）設定編集　PPP 設定」の画面へ移動します。

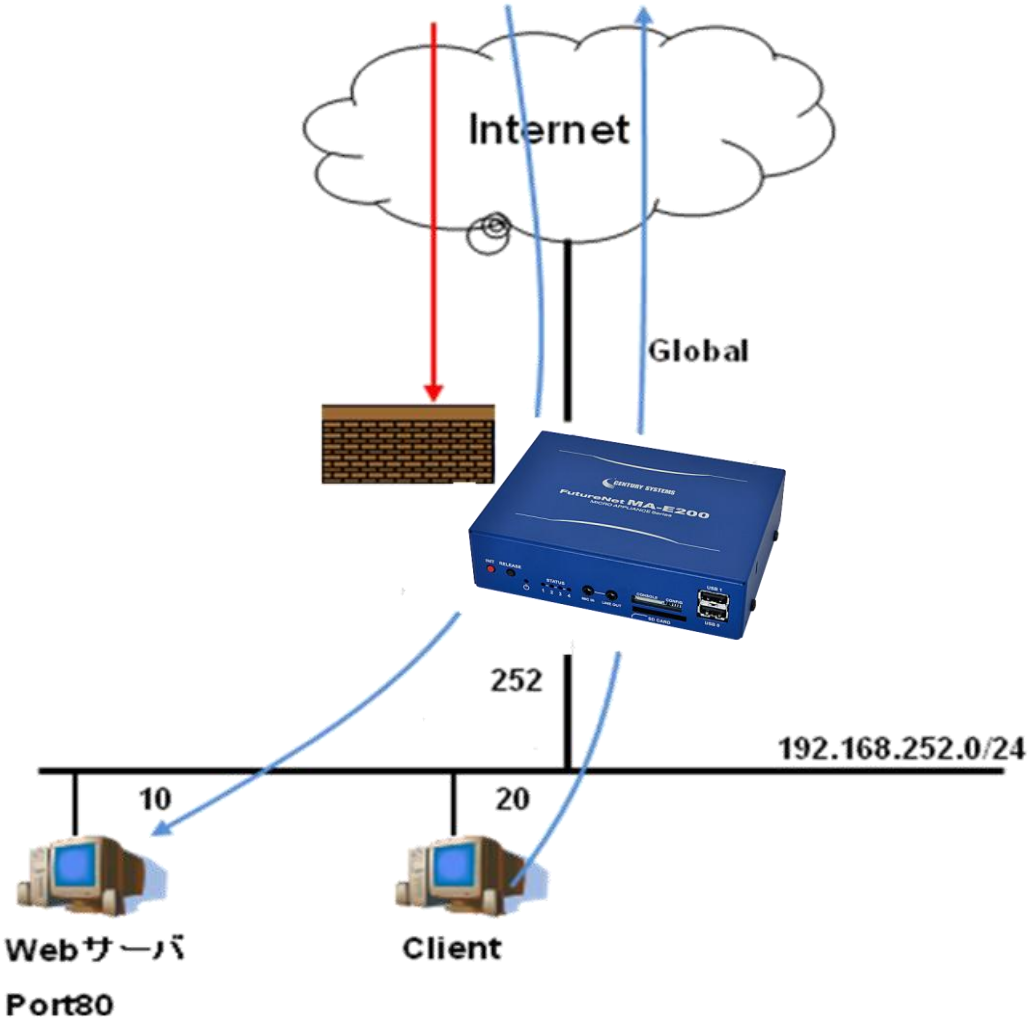
「デバイス」には「emobile(USB)」を選択します。「接続方式」を「通常」にし、PPP インターフェースをデフォルトルートとして設定します。「アカウント設定」は、自動設定されます。OK を押すと、接続設定が追加されます。

「接続」ボタンを押すと、接続を開始します。

4.2. ファイアウォール設定例

MA-E2xx でファイアウォール機能を利用する設定例を示します。ローカル側(Ether0), インターネット側(PPP)とする下図のような設定で、内部ネットワークには Web サーバ(192.168.252.10 / Port80)があり、外部へ Web サービスを提供出来るようにしてあります。内部ネットワーク上の各ホストは、**MA-E2xx** をデフォルトゲートウェイとするように設定されています。

またファイアウォールのデフォルト動作は外部から内部ネットワークへの接続を遮断します。但し、公開 Web サーバへのアクセスおよび、**MA-E2xx** 本体への Web 設定画面および SSH による外部特定ホスト(10.0.0.1*)からの接続は例外として許可するようにします。 ※10.0.0.1 は架空のグローバルアドレスです。

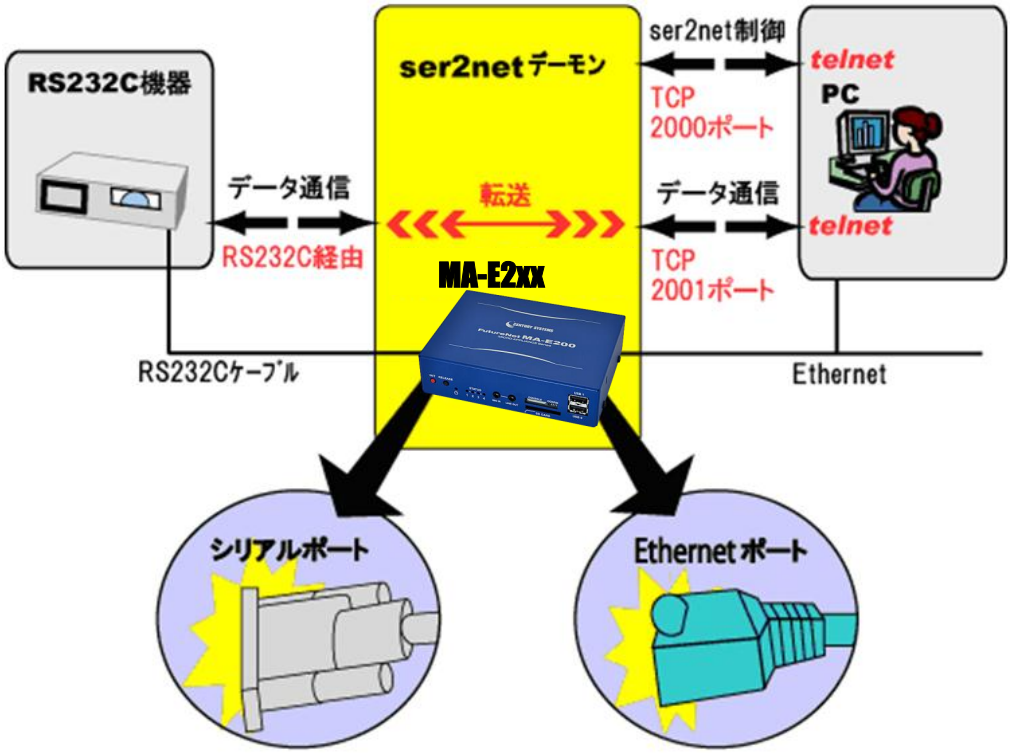


このシナリオでのファイアウォール画面の設定は、次の通りです。

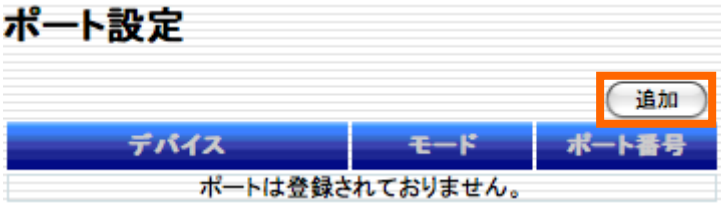
各画面を設定した後、「全体設定」の「ファイアウォール機能を使用する」にチェックし、「設定」ボタンを押します。

4.3. ser2net 設定例

ser2net サービスを利用して、telnet を使用したシリアル監視時の設定例を示します。図中の「RS232C 機器」と Ethernet 上の PC との間で通信を行います。RS232C 機器はコマンドラインインターフェースを持ちコマンドを待ち受けているものとします。PC 上のクライアントソフトは telnet を使用します。PC との TCP 接続(2001 ポート)を終端するのは本機上の ser2net デーモンであり、シリアルポートとの間でデータストリームを転送します。PC より"2000" ポートへ telnet 接続する事で ser2net デーモンを制御し、シリアル制御信号の操作、ポート状態の確認、コネクションの切断等を行います。PC および本機 Ethernet ポートは、同一 Ethernet セグメント上で IP 通信できるよう設定されているものとします。



「ser2net 設定」画面の「ポート設定」で「追加」ボタンを押下し「ser2net 設定編集」の画面へ移動します。

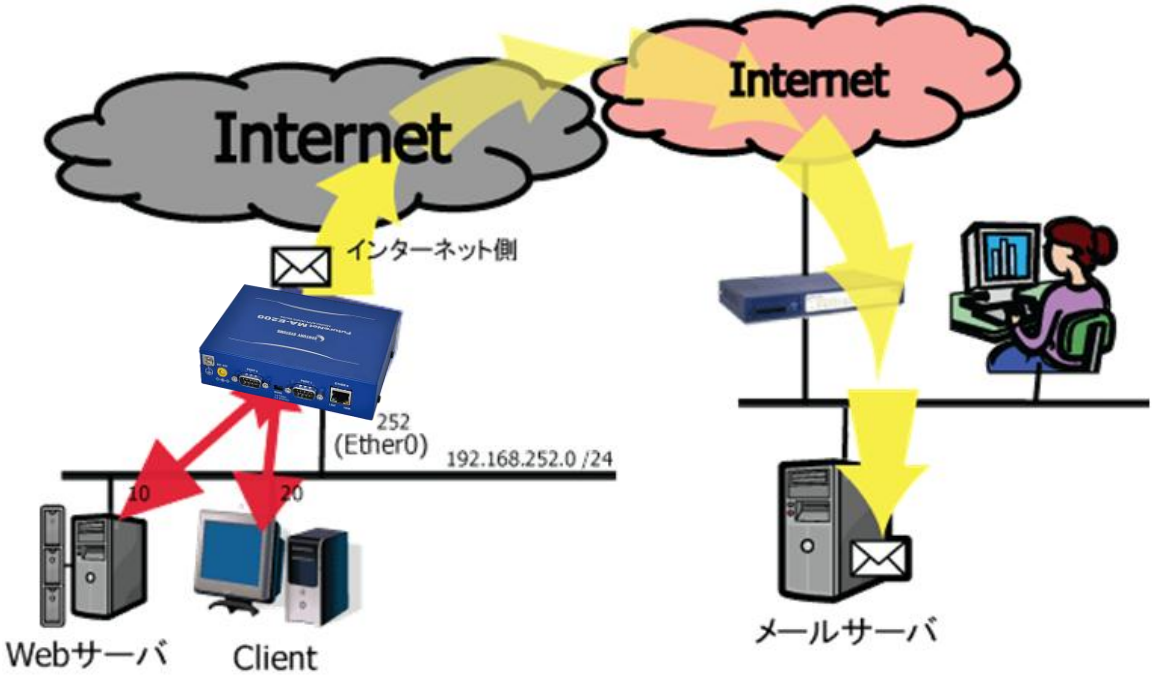


設定編集画面では、ポート設定の編集を行います。

「OK」を押すと、ポート設定を登録します。次に、「サービス設定」において、「サービス」を「使用する」にチェックし、「制御ポート」を「使用する」にチェックします。制御ポート番号に 2000 を入力します。最後に「設定」ボタンを押すと、ser2net デーモンが起動します。

4.4. 死活監視設定例

MA-E2xx で死活監視機能を利用する設定例を示します。Ethernet ポートを LAN 側(Ether0), PPP によるインターネット接続を WAN 側に接続する下図のような設定で、内部ネットワークには監視対象 Web サーバ(192.168.252.10)および Client(192.168.252.20)があり、**MA-E2xx** (192.168.252.252)から 30 秒間隔で ping によるポーリングを継続的に行い死活監視を行います。
また連続して 3 回以上 ping の応答がない場合は当該ホストを異常と判定し、E-mail による通知を実行します。E-mail の通知先アドレスは test@example.com です。



このシナリオでの死活監視画面の設定は、下記の通りです。

E-mail 通知先設定は、下記の通りです。

E-mail 設定例は、次の通りです。加入する ISP の提供するサービスを確認してメールサーバの設定を行って下さい。

5. 付録

5.1. 出荷時初期設定/設定データ初期化時設定一覧

5.1.1. 基本設定

5.1.1.1. インターフェース設定

項目	値
Ethernet I/F 設定	
Ethernet0	
IP アドレス	192.168.253.253
ネットマスク	255.255.255.0
デフォルトゲートウェイ	(空欄)
DHCP を使用する	使用しない
DNS サーバ設定	
DNS サーバ(1)	(空欄)
DNS サーバ(2)	(空欄)

5.1.1.2. GRE 設定

項目	値
GRE 設定	(空欄)

5.1.1.3. PPP(発信)設定

項目	値
PPP 設定/状態	(空欄)
PPP(発信)設定編集 PPP 設定	
デバイス	Modem
接続名称	(空欄)
モデム系設定	
接続方式	PERSIST
ダイアルタイプ	トーン
アイドル検知時間[秒]	0
モデム初期化コマンド	AT&FS0=0
電話番号	(空欄)
Default 圧縮	使用する
VJ 圧縮	使用する
LCP ECHO による接続確認	
接続確認	使用する

送信間隔[秒]	30
切断判定回数	3
一般設定	
DNS サーバ	取得する
デフォルトルート	設定しない
ローカル IP	0.0.0.0
リモート IP	0.0.0.0
サブネットマスク	0.0.0.0
MTU	1500
アカウント設定	
自己証明	証明する
アカウント	(空欄)
パスワード	(空欄)
パスワード(確認)	(空欄)

5.1.1.4. PPP(着信)設定

項目	値
PPP 着信機能	
PPP 着信	使用しない
モデム系設定	
デバイス	Modem (PORT0)
アイドル検知時間[秒]	0
モデム初期化コマンド	AT&FS0=0
Default 圧縮	使用する
VJ 圧縮	使用する
LCP ECHO による接続確認	
接続確認	使用する
送信間隔[秒]	30
切断判定回数	3
一般設定	
デフォルトルート	設定しない
ローカル IP	0.0.0.0
リモート IP	0.0.0.0
サブネットマスク	0.0.0.0
MTU	1500
DNS 設定	
DNS サーバ	設定しない

プライマリサーバ	(空欄)
セカンダリサーバ	(空欄)
相手アカウント認証設定	
相手側自己証明	要求する
自己証明設定	
自己証明	証明しない
アカウント	(空欄)
着信用アカウント設定	(空欄)

5.1.1.5. DHCP サーバ設定

項目	値
DHCP サーバ機能	利用しない
リース範囲設定	(空欄)

5.1.1.6. 静的ルーティング設定

項目	値
静的ルーティング設定	(空欄)
ルーティングテーブルの編集	
アドレス	(空欄)
ネットマスク	(空欄)
インターフェース	eth0
ゲートウェイ	(空欄)

5.1.1.7. ファイアウォール設定

項目	値
全体設定	使用しない
ゾーン設定	
ゾーン設定 1	eth0: ローカル側
ゾーン設定 2	ppp50: ローカル側
NAPT 設定	(空欄)
フィルタ/DNAT ルール	(空欄)
1 対 1NAT 設定	(空欄)

5.1.2. サービス設定

5.1.2.1. NTP 設定

項目	値
NTP 設定	

全体設定	使用しない
サーバ動作	使用しない
NTP サーバ(1)	(空欄)
NTP サーバ(2)	(空欄)

5.1.3. アプリケーション設定

5.1.3.1. 死活監視設定

項目	値
監視設定	
ポーリング間隔	30 秒
リトライ回数	1 回
監視対象ホスト	(空欄)
通知先設定	
送信先 E-mail アドレス(1)	(空欄)+無効
送信先 E-mail アドレス(2)	(空欄)+無効
送信先 E-mail アドレス(3)	(空欄)+無効
E-mail 設定	
必須項目	
有効/無効	無効
SNMP サーバ名	(空欄)
POP サーバ名	(空欄)
ユーザ	(空欄)
パスワード	(空欄)
名前	MA-E2xx Default
メールアドレス	(空欄)
オプション項目	
SMTP ポート	25
POP ポート	110
認証方式	SMTP 認証

5.1.4. シリアル監視設定

5.1.4.1. ser2net 設定

項目	値
サービス設定	
サービス	使用しない
制御ポート	使用しない
制御ポート番号	3000
ポート設定	(空欄)

5.1.5. 保守・運用

5.1.5.1. WebUI パスワード設定

項目	値
WebUI パスワード	
アカウント	admin
パスワード	admin

5.1.5.2. Syslog 確認

項目	値
ログファイル選択	全て(everything)

5.1.5.3. Ping 疎通テスト設定

項目	値
ホスト選択	手入力
アドレス指定	(空欄)
ホスト設定	(空欄)

5.1.5.4. ファームウェアアップデート

項目	値
アップロード結果	
ファイルサイズ	(空欄)
サム値	(空欄)
モード選択	設定データはそのまま

5.1.5.5. 再起動/シャットダウン

項目	値
rootfs mount mode	読書可能

6. MA-E250/F について

この項では、**MA-E250/F** とその他の **MA-E200** Series の差分のみを示します。

6.1. 画面別説明

6.1.1. PPP(発信)設定

PPP(Point-to-Point Protocol)の発信の設定を行います。

6.1.1.1. 利用可能デバイス一覧

「利用可能デバイス一覧」では、PPP 設定が可能なデバイスの一覧が表示されます。

MA-E250/F では、NTTdocomo(UM02-F)が一覧に表示されます。

名称	デバイス	種別	着信可否	備考
PPPoE (eth0)	eth0	PPPoE	不可	ether0 ポート
Modem (PORT0)	/dev/ttymxc0	モデム	可	RS-232 ポート
Modem (PORT1)	/dev/ttymxc1	モデム	可	RS-232 ポート
NTTdocomo (UM02-F)	/dev/ttyUM02F	モデム	可	FOMA UM02-F

上記以外の通信デバイスは使用できません。

※注意事項

Modem(PORT0)または、Modem(PORT1)を使用する場合は、/etc/inittab のシリアル設定を以下のように変更し

てください。

SERIAL CONSOLES

#mxc0:12345:respawn:/sbin/agetty 115200 ttymxc0 vt100

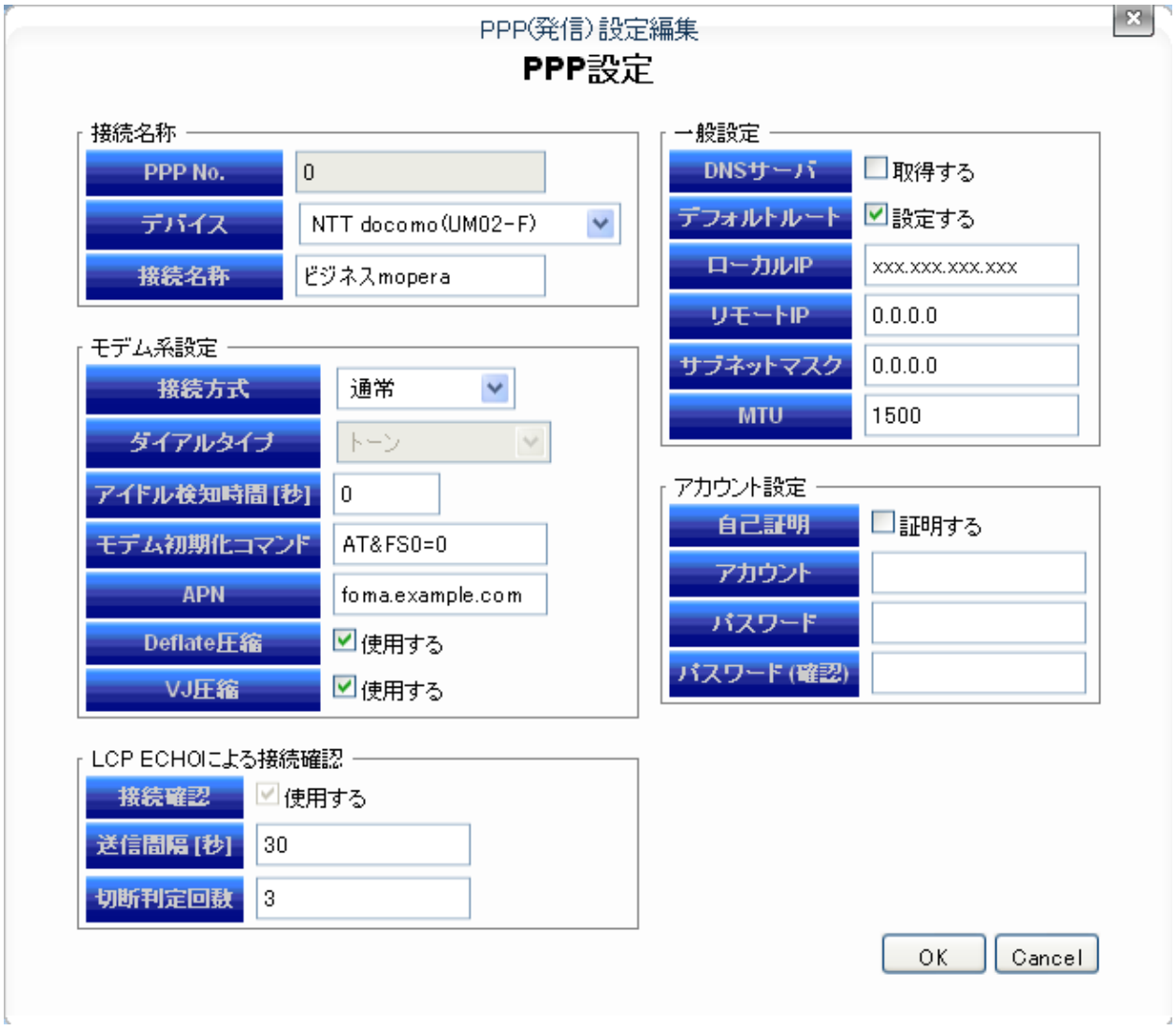
↑PORT0 をモデムとして使用する場合、先頭に#を付けてコメントアウト

#mxc1:12345:respawn:/sbin/agetty 115200 ttymxc1 vt100

↑PORT1 をモデムとして使用する場合、先頭に#を付けてコメントアウト

6.1.1.2. PPP 設定

PPP の発信設定を新規に追加する場合は「追加」ボタンを押すと「PPP(発信)設定編集」ダイアログを表示します。



■ **<u>モデム系設定</u>**

➢ APN

株式会社 NTT ドコモ様と契約したドメインを入力してください。

■ **<u>一般設定</u>**

➢ ローカル IP

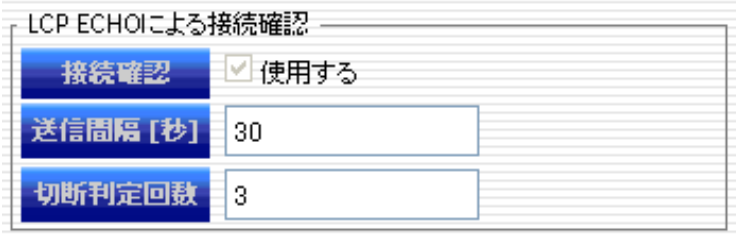
株式会社 NTT ドコモ様と契約した端末の IP アドレスを入力してください。

上記以外の PPP(発信)設定は、**MA-E200** Series と同様です。

6.1.2. PPP(着信)設定

PPP(Point-to-Point Protocol)の着信設定を行います。

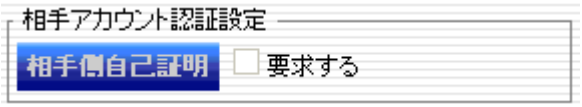
■ <u>LCP ECHO による接続確認</u>



➢ 接続確認

デバイスに NTTdocomo(UM02-F)を選択した場合、LCP ECHO による接続確認のチェックをはずすことはできません。

■ **相手アカウント認証設定**



- 相手アカウント認証設定
  デバイスに NTTdocomo(UM02-F)を選択した場合、「要求する」にチェックすることはできません。

■ **一般設定**

- ローカル IP
  株式会社 NTT ドコモ様と契約した端末の IP アドレスを入力してください。

上記以外の PPP(着信)設定は、**MA-E200** Series と同様です。

6.2. ビジネス mopera 接続の設定例

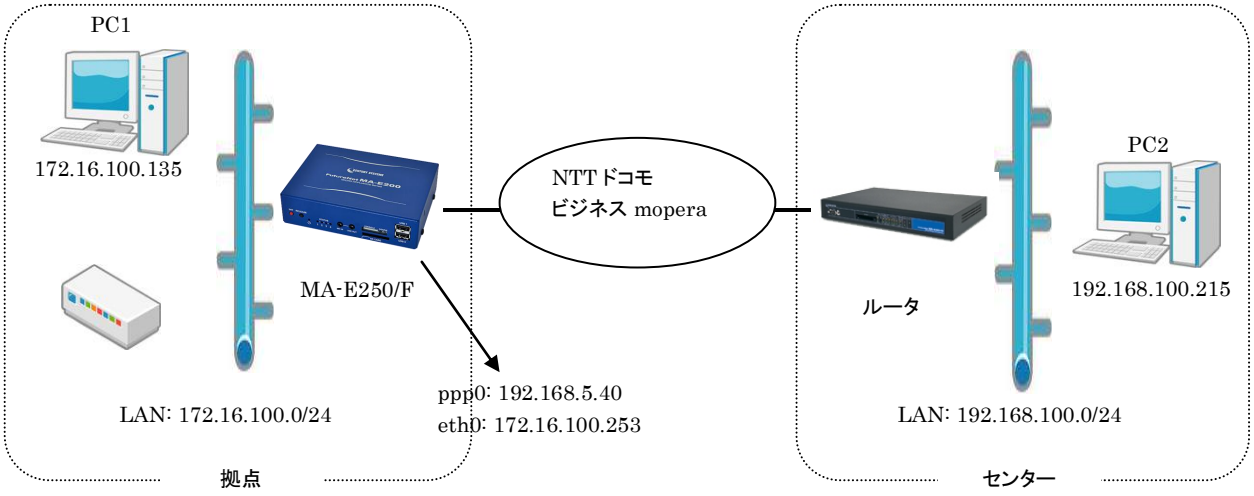
MA-E250/F 内蔵の FOMA UM02-F を使用して、ビジネス mopera 接続を行う設定例を示します。

6.2.1. 構成図

本設定例の構成図を下図に示します。

センター側ルータには、拠点とセンター間のネットワーク構成に合わせて、拠点宛てのスタティックルートを設定します。

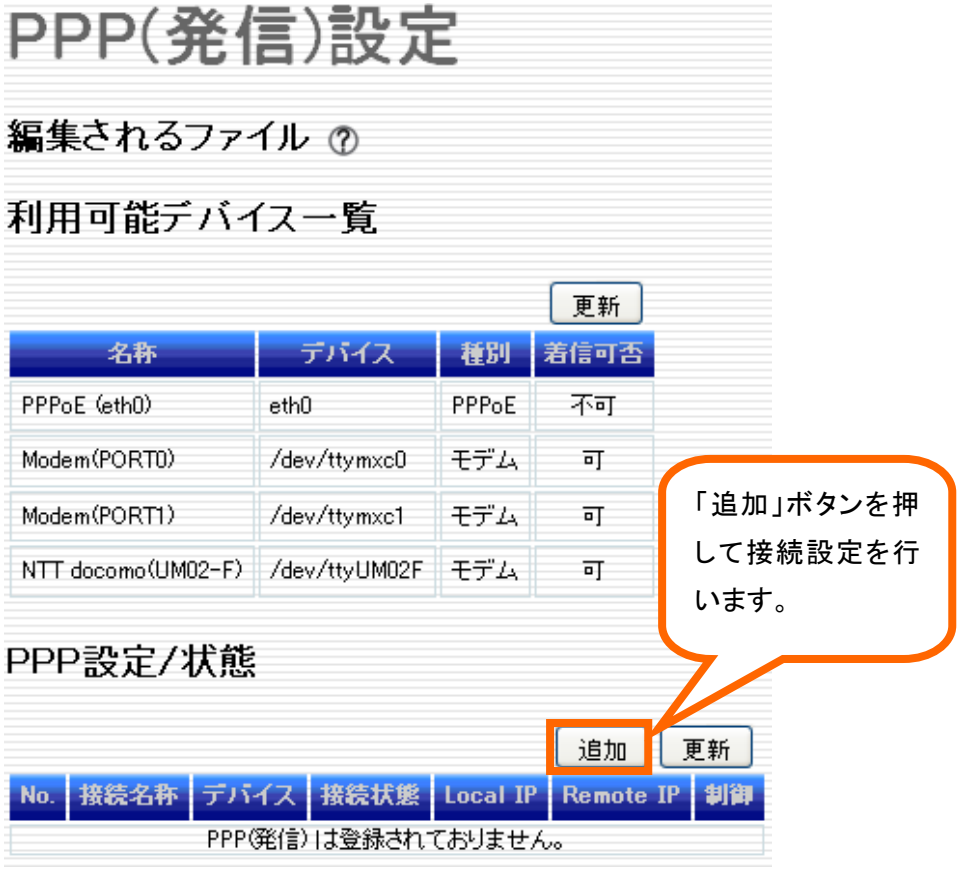
本構成図の場合は、拠点 192.168.100.0/24 宛てスタティックルートを設定します。



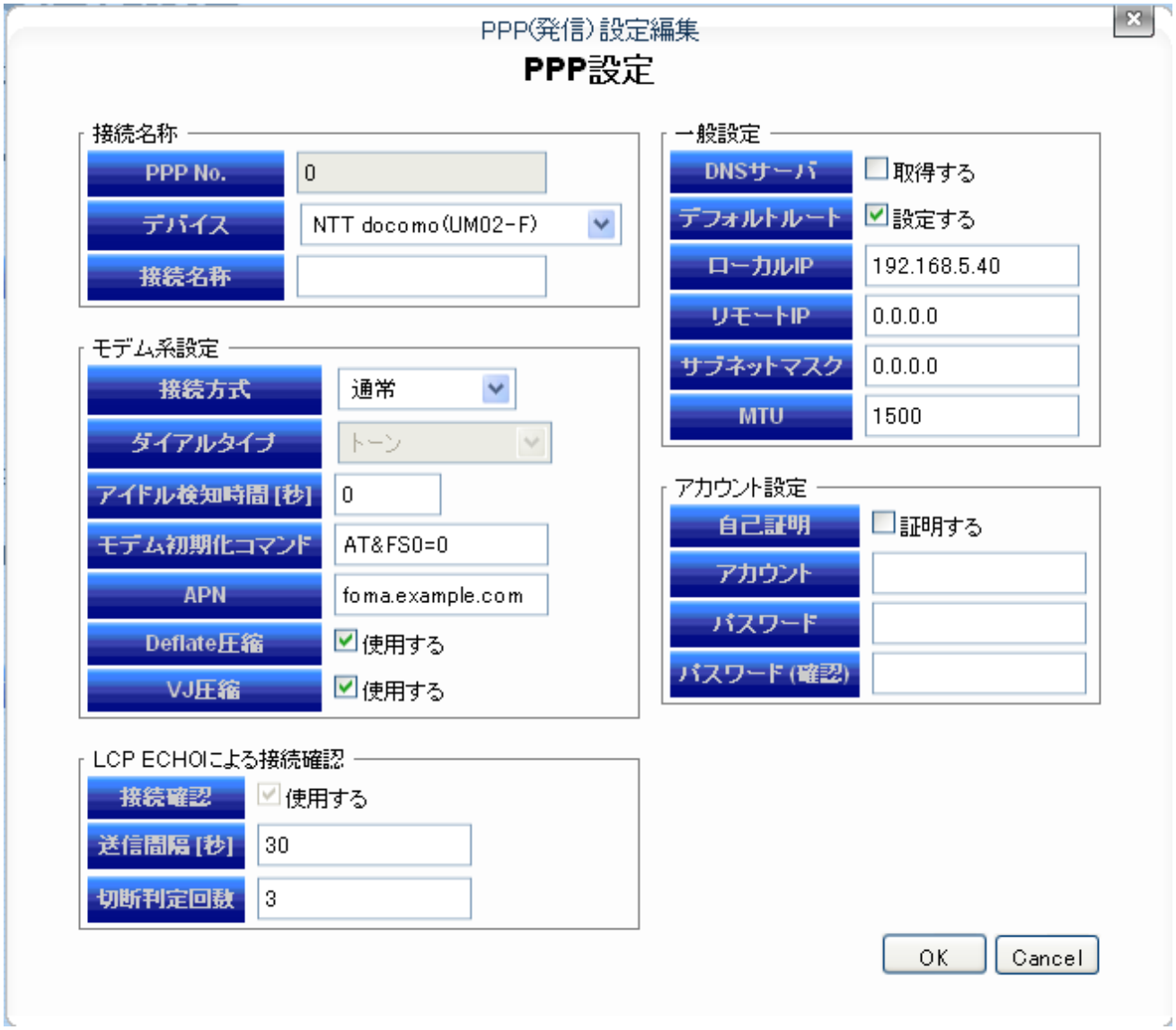
6.2.2. 発信設定

この例では、PPP の接続方式は「通常」を選択し、画面操作による手動での接続／切断を行います。

「PPP(発信)設定」画面で、接続設定を行います。



「追加」ボタンを押下し「PPP(発信)設定編集 PPP 設定」の画面へ移動します。



「デバイス」:「NTTdocomo(UM02-F)」

「接続方式」:「通常」

「デフォルトルート」:「設定する」にチェックを入れる。

「APN」:「foma.example.com」(株式会社 NTT ドコモ様と契約したドメインを入力してください。)

「ローカル IP」:192.168.5.40(株式会社 NTT ドコモ様と契約した端末の IP アドレスを入力してください。)

上記を設定し、「OK」ボタンを押すと接続設定が追加されます。

「接続」ボタンを押すと、接続を開始します。

6.2.3. 着信設定

「PPP(着信)設定」画面で、接続設定を行います。

「デバイス」:「NTTdocomo(UM02-F)」

「デフォルトルート」:「設定する」にチェックを入れる。

「ローカル IP」:192.168.5.40(株式会社 NTT ドコモ様と契約した端末の IP アドレスを入力してください。)

上記を設定し、「設定」ボタンを押すと接続設定が追加されます。

設定したローカル IP 宛にパケットを送信すると着信します。

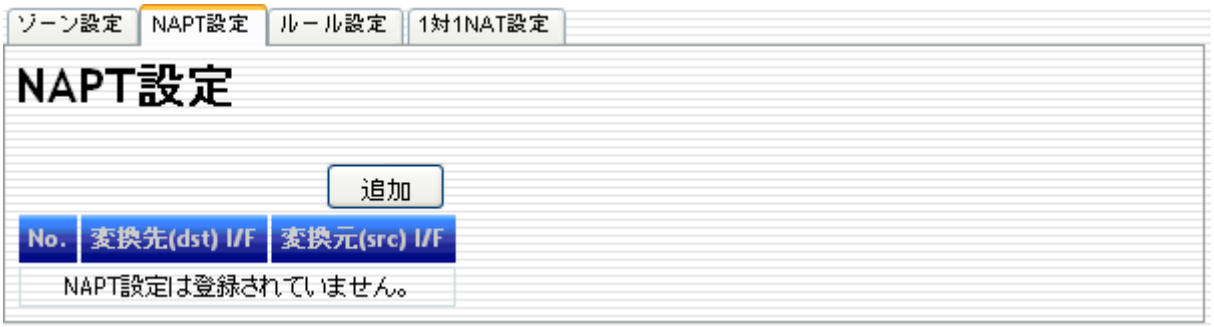
6.2.4. ファイアウォール設定

ここでは、発着信時に **MA-E250F** に到達した ping と ssh のパケットをローカル PC に転送するファイアウォール設定を紹介します。

6.2.2 と 6.2.3 の設定を行うと ppp0（発信側）と ppp50（着信側）がゾーン設定に出来ていますので、「ゾーン」の項目で「インターネット側」を選択します。

また、「全体設定」の「ファイアウォール機能を使用する」ボタンにチェックを入れます。

次に「NAPT 設定」のタブをクリックします。

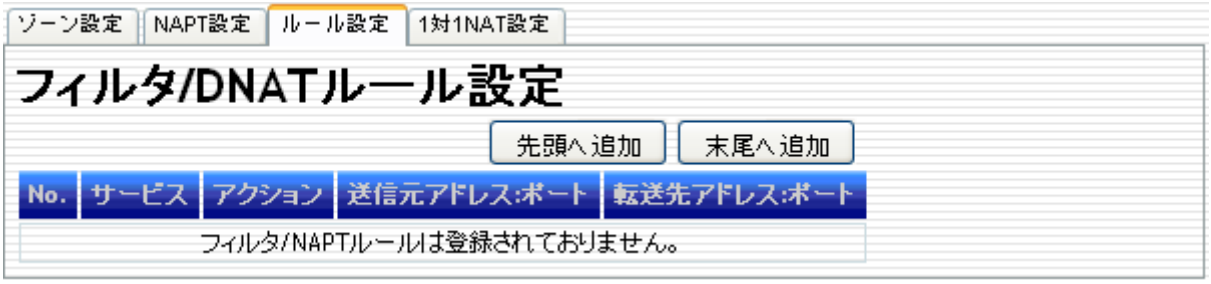


「追加」ボタンを押下して、NAPT 設定を行います。

NAPT 編集の画面が開きますので、「変換先 I/F」に「ppp0」、「変換元 I/F」に「eth0」を選択し、「OK」ボタンをクリックします。また、同様に「変換先 I/F」に「ppp50」、「変換元 I/F」に「eth0」を選択し、「OK」ボタンをクリックします。

上記2つを設定すると、下記のようになります。

次に「ルール設定」のタブをクリックします。



「末尾へ追加」ボタンを押下し、「フィルタ/NAPT ルール編集」画面を開きます。

「サービス」:「Ping」

「アクション」:「ポート転送（DNAT）」

「転送先-アドレス」:「172.16.100.135」（構成図の PC1 の IP アドレス）

「転送先-変換前アドレス」:「192.168.5.40」

（↑株式会社 NTT ドコモ様と契約した端末の IP アドレス）

上記の設定を行い、「OK」ボタンを押下します。

「サービス」:「SSH」

「アクション」:「ポート転送（DNAT）」

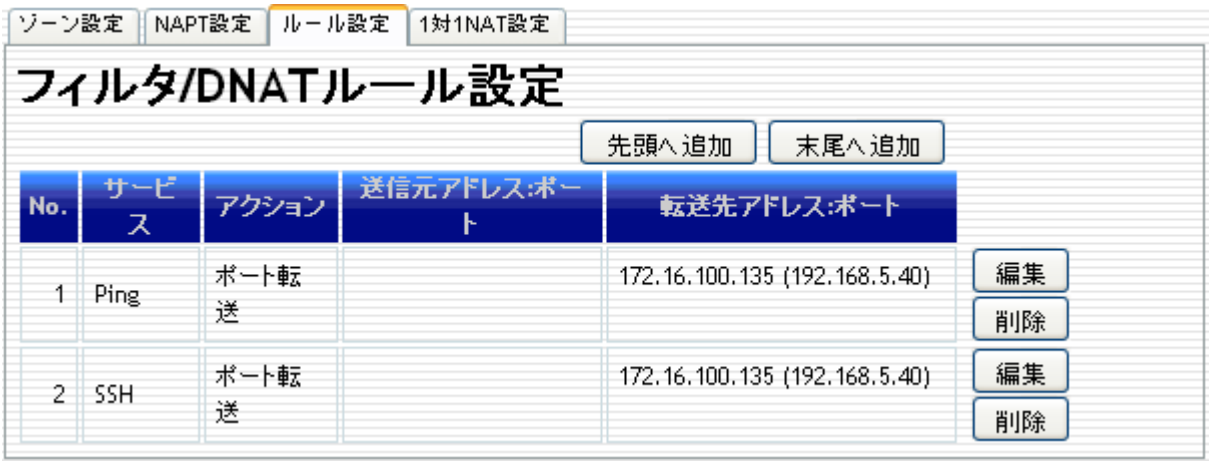
「転送先-アドレス」:「172.16.100.135」（構成図の PC1 の IP アドレス）

「転送先-変換前アドレス」:「192.168.5.40」

（↑株式会社 NTT ドコモ様と契約した端末の IP アドレス）

上記の設定を行い、「OK」ボタンを押下します。

上記2つを設定すると、下記のようになります。



全ての設定が終わったら、「設定」ボタンを押下します。

この状態でビジネス mopera に接続すると、ping や ssh のパケットが構成図の PC1 まで流れるようになります。

FutureNet MA-E200 Series ウェブユーザインターフェース操作マニュアル Ver. 1.2.1

2012 年 6 月版

発行 センチュリー・システムズ株式会社