FutureNet NXRシリーズ
ユーザーズガイド GUI編

Ver.6.3.0 対応版

CENTURY SYSTEMS

目次

はじめに

◆ご注意

1 本装置の故障、誤動作、不具合、あるいは停電などの外部要因によって、通信の機会を逸したために生じた損害などの純粋経済損失につきましては、当社はいっさいその責任を負いかねますのであらかじめご了承ください。

2 通信情報が漏洩した事による経済的、精神的損害につきましては、当社はいっさいその責任を負いかねますのであらかじめご了承ください。

3 本書の内容の一部または全部を無断で転載、複写することを禁じます。

4 本書およびソフトウェア、ハードウェア、外観の内容について、将来予告なしに変更することがあります。

5 本書の内容については万全を期しておりますが、万一ご不審な点や誤り、記載漏れなどお気づきの点がありましたらご連絡ください。

◆商標の表示

□「FutureNet」はセンチュリー・システムズ株式会社の登録商標です。

□下記製品名等は米国Microsoft Corporationの登録商標です。
Microsoft、Windows、Windows Vista、Windows 7

□下記製品名等は米国Apple Inc.の登録商標です。
Macintosh、Mac OS X

その他、本書で使用する各会社名、製品名は各社の商標または登録商標です。

第1章

本装置の概要

Ⅰ．本装置の特長

FutureNet NXRシリーズの「製品概要」、「製品の特徴」、「仕様」等については、弊社のWebサイトを参照してください。

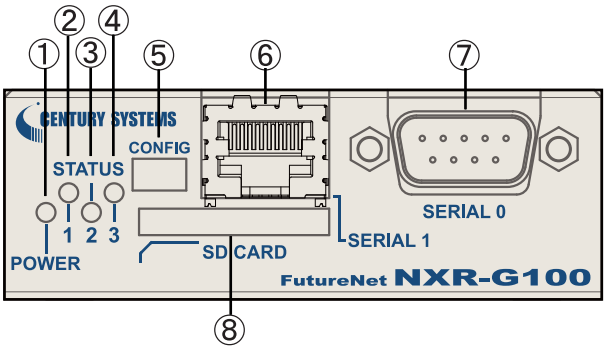
◆ FutureNet NXR-G100
http://www.centurysys.co.jp/products/router/nxrg100.html

◆ FutureNet NXR-G100/F
http://www.centurysys.co.jp/products/router/nxrg100f.html

◆ FutureNet NXR-G100/KL
http://www.centurysys.co.jp/products/router/nxrg100kl.html

II．各部の名称と機能（NXR-G100）

◆製品前面



① POWER LED
本装置の電源状態を示します。

② STATUS 1 LED
③ STATUS 2 LED
④ STATUS 3 LED
本装置のシステムおよび、サービスのステータスを示します。

システムおよびサービスのステータス	LED の表示 ①②③④
電源投入時	●●●●
システム起動中	●✳●●
システム起動後（ログイン可能状態）	●●●●
PPP/Tunnel 等の切断状態（configurable）	●●●●
PPP/Tunnel 等の接続状態（configurable）	●●●●
SD カード未装着時	●●●●
SD カード装着時	●●●●
温度異常（warning）	✳●●●
温度異常（critical）	●●●●
ファームウェア更新中	●✳●●
ファームウェア更新失敗	●●●●
システム異常	●●●●

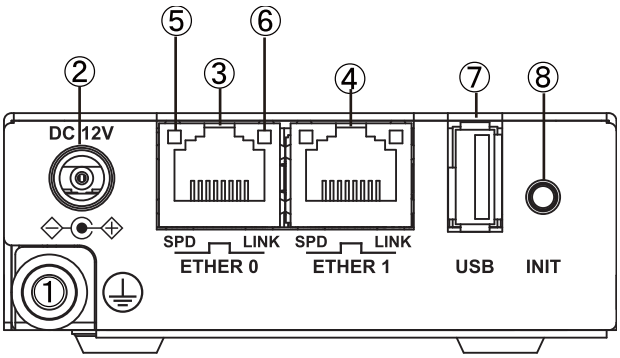
⑤ CONFIG
すべてのスイッチが上に位置している状態で使用してください。

⑥ SERIAL 1 ポート
現在のバージョンでは、使用しません。

⑦ SERIAL 0 ポート(コンソールポート)
CLI 接続の際に使用します。
RS-232C ケーブルを接続します。

⑧ SD カードスロット
SD カードを挿入します。

◆製品背面



① FG(アース)端子
保安用接続端子です。
必ずアース線を接続してください。

② DC 12V 電源コネクタ
製品付属の AC アダプタを接続します。

③ ETHER 0 ポート
10BASE-T/100BASE-TX/1000BASE-T 対応の Ethernet ポートです。主に LAN 側ポートとして使用します。

④ ETHER 1 ポート
10BASE-T/100BASE-TX/1000BASE-T 対応の Ethernet ポートです。主に WAN 側ポートとして使用します。

⑤ SPD LED(橙 / 緑)
ETHER ポートの接続速度を示します。
10BASE-T モードで接続時 : ●
100BASE-TX モードで接続時 : ●
1000BASE-T モードで接続時 : ●

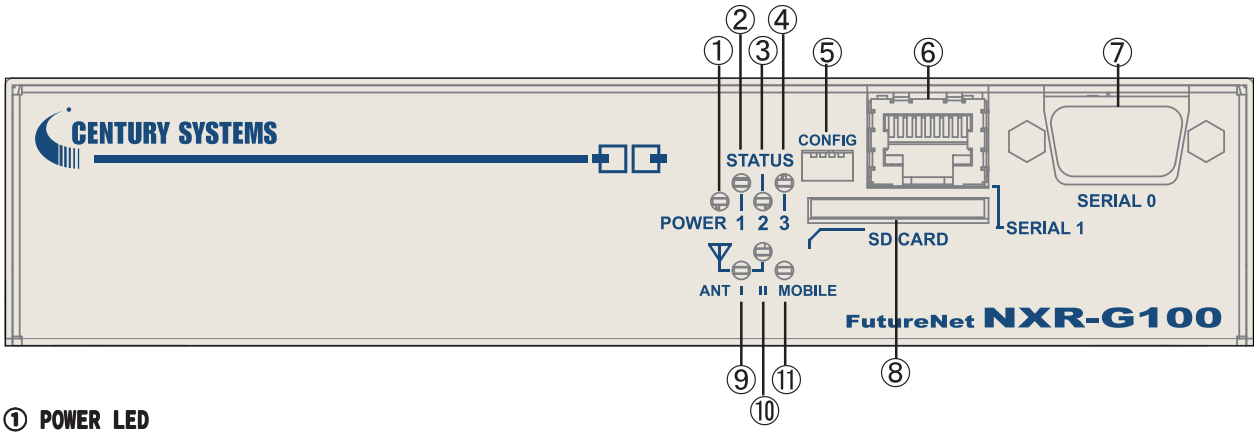
⑥ LINK LED(緑)
ETHER ポートのリンク状態を示します。
Link Down 時 : ●
Link UP 時 : ●

⑦ USB ポート
USB Flash メモリ、または USB タイプのデータ通信端末を挿入します。

⑧ INIT ボタン
本装置を工場出荷時の設定に戻して起動するときに使用します。
1. Init ボタンを押しながら電源を投入します。
2. POWER LED が、次の状態になるまで、Init ボタンを押したままにしておきます。●→●→●
3. POWER LED が点灯(●)したら、速やかに Init ボタンを放します。本装置が工場出荷設定で起動します。

III．各部の名称と機能（NXR-G100/F）

◆製品前面



① POWER LED
本装置の電源状態を示します。

② STATUS 1 LED
③ STATUS 2 LED
④ STATUS 3 LED
本装置のシステムおよび、サービスのステータスを示します。

システムおよびサービスのステータス	LED の表示 ①②③④
電源投入時	🟡🟡🟡🟡
システム起動中	🟢✳●●
システム起動後（ログイン可能状態）	🟢🟢●●
PPP/Tunnel 等の切断状態（configurable）	●●●●
PPP/Tunnel 等の接続状態（configurable）	●●🟢●
SD カード未装着時	●●●●
SD カード装着時	●●●🟢
温度異常（warning）	✳●●●
温度異常（critical）	🔴●●●
ファームウェア更新中	●✳●●
ファームウェア更新失敗	●🔴●●
システム異常	🟢🔴🔴●

⑤ CONFIG
すべてのスイッチが上に位置している状態で使用してください。

⑥ SERIAL 1ポート
現在のバージョンでは、使用しません。

⑦ SERIAL 0ポート(コンソールポート)
CLI 接続の際に使用します。
RS-232C ケーブルを接続します。

⑧ SD CARD スロット
SD カードを挿入します。

⑨ ANT I LED
⑩ ANT II LED
モバイルの電波強度を示します。

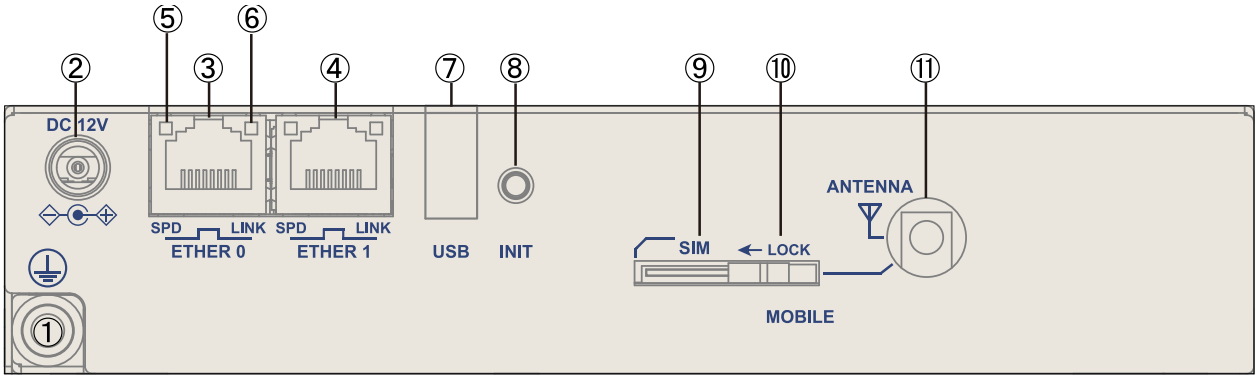
	⑨	⑩
圏外	●	●
0-1	●	🟢
2	🟢	●
3	🟢	🟢

⑪ MOBILE LED
モバイルモジュールのステータスを示します。
モジュール停止 : 🔴
モジュール起動 : ●
PPP 接続 : 🟢

NXR-G100/F は、標準 AC アダプタでは、モバイルカードの併用をサポートしていません。
モバイルカードを併用する場合は、オプション AC アダプタを、別途お求めください。

III. 各部の名称と機能（NXR-G100/F）

◆製品背面



① FG(アース)端子
保安用接続端子です。
必ずアース線を接続してください。

② DC 12V 電源コネクタ
製品付属の AC アダプタを接続します。

③ ETHER 0 ポート
10BASE-T/100BASE-TX/1000BASE-T 対応の Ethernet ポートです。主に LAN 側ポートとして使用します。

④ ETHER 1 ポート
10BASE-T/100BASE-TX/1000BASE-T 対応の Ethernet ポートです。主に WAN 側ポートとして使用します。

⑤ SPD LED(橙 / 緑)
ETHER ポートの接続速度を示します。
10BASE-T モードで接続時 : ●
100BASE-TX モードで接続時 : ●
1000BASE-T モードで接続時 : ●

⑥ LINK LED(緑)
ETHER ポートのリンク状態を示します。
Link Down 時 : ●
Link UP 時 : ●

⑦ USB ポート
USB Flash メモリ、または USB タイプのデータ通信端末を挿入します。

⑧ INIT ボタン
本装置を工場出荷時の設定に戻して起動するときに使用します。
1. Init ボタンを押しながら電源を投入します。
2. POWER LED が、次の状態になるまで、Init ボタンを押したままにしておきます。●→●→●
3. POWER LED が点灯(●)したら、速やかに Init ボタンを放します。本装置が工場出荷設定で起動します。

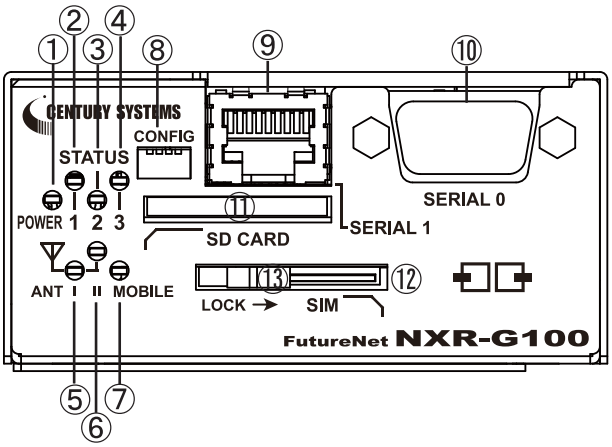
⑨ SIM カードスロット
SIM カードを挿入します。

⑩ LOCK
スライドすることによって、SIM カードをロックします。

⑪ ANTENNA
対応するアンテナ(オプション)を装着します。

Ⅳ．各部の名称と機能（NXR-G100/KL）

◆製品前面



① POWER LED
本装置の電源状態を示します。

② STATUS 1 LED
③ STATUS 2 LED
④ STATUS 3 LED
本装置のシステムおよび、サービスのステータスを示します。

システムおよびサービスのステータス	LED の表示 ①②③④
電源投入時	：●●●●
システム起動中	：●✳●●
システム起動後（ログイン可能状態）	：●●●●
PPP/Tunnel 等の切断状態（configurable）	：●●●●
PPP/Tunnel 等の接続状態（configurable）	：●●●●
SD カード未装着時	：●●●●
SD カード装着時	：●●●●
温度異常（warning）	：✳●●●
温度異常（critical）	：●●●●
ファームウェア更新中	：●✳●●
ファームウェア更新失敗	：●●●●
システム異常	：●●●●

⑤ ANT I LED
⑥ ANT II LED
モバイルの電波強度を示します。

	⑤	⑥
圏外	●	●
0-1	●	●
2	●	●
3	●	●

⑦ MOBILE LED
モバイルモジュールのステータスを示します。
モジュール停止 ： ●
モジュール起動 ： ●
PPP 接続 ： ●

⑧ CONFIG
すべてのスイッチが上に位置している状態で使用してください。

⑨ SERIAL 1ポート
現在のバージョンでは、使用しません。

⑩ SERIAL 0ポート(コンソールポート)
CLI 接続の際に使用します。
RS-232C ケーブルを接続します。

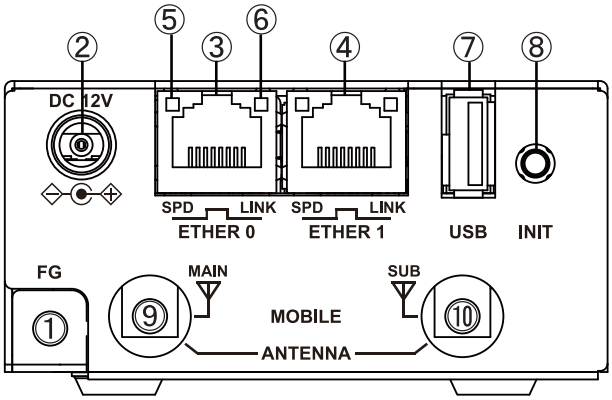
⑪ SD カードスロット
SD カードを挿入します。

⑫ SIM カードスロット
SIM カードを挿入します。

⑬ LOCK
スライドすることによって、SIM カードをロックします。

Ⅳ．各部の名称と機能（NXR-G100/KL）

◆製品背面



① FG(アース)端子
保安用接続端子です。
必ずアース線を接続してください。

② DC 12V 電源コネクタ
製品付属の AC アダプタを接続します。

③ ETHER 0ポート
10BASE-T/100BASE-TX/1000BASE-T 対応の Ethernet ポートです。主に LAN 側ポートとして使用します。

④ ETHER 1ポート
10BASE-T/100BASE-TX/1000BASE-T 対応の Ethernet ポートです。主に WAN 側ポートとして使用します。

⑤ SPD LED(橙 / 緑)
ETHER ポートの接続速度を示します。
10BASE-T モードで接続時 : ●
100BASE-TX モードで接続時 : ●
1000BASE-T モードで接続時 : ●

⑥ LINK LED(緑)
ETHER ポートのリンク状態を示します。
Link Down 時 : ●
Link UP 時 : ●

⑦ USBポート
USB Flash メモリ、または USB タイプのデータ通信端末を挿入します。

⑧ INIT ボタン
本装置を工場出荷時の設定に戻して起動するときに使用します。
1.Init ボタンを押しながら電源を投入します。
2.POWER LED が、次の状態になるまで、Init ボタンを押したままにしておきます。●→●→●
3.POWER LED が点灯(●)したら、速やかに Init ボタンを放します。本装置が工場出荷設定で起動します。

⑨ ANTENNA（MAIN）
対応するアンテナ(オプション)を装着します。

⑩ ANTENNA（SUB）
対応するアンテナ(オプション)を装着します。

Ｖ．動作環境

本製品をお使いいただくには、以下の環境を満たしている必要があります。

◆ハードウェア環境

・本製品に接続するコンピュータの全てに、LAN インタフェースがインストールされていること。

・ADSL モデム /CATV モデム /ONU に、10BASE-T、100BASE-TX または 1000BASE-T のインターフェースが搭載されていること。

・本製品と全てのコンピュータを接続するためのハブやスイッチングハブが用意されていること。

・本製品と全てのコンピュータを接続するために必要な種類のネットワークケーブルが用意されていること。

◆ソフトウェア環境

・TCP/IP を利用できる OS がインストールされていること。

・GUI で本装置にログインする場合は、接続されている全てのコンピュータの中で少なくとも 1 台に、ブラウザがインストールされていること。弊社では Internet Explorer 9 で動作確認を行っています。

なおサポートにつきましては、本製品固有の設定項目と本製品の設定に関係する OS 上の設定に限らせていただきます。
OS 上の一般的な設定やパソコンにインストールされた LAN ボード / カードの設定、各種アプリケーションの固有の設定等のお問い合わせについてはサポート対象外とさせていただきますので、あらかじめご了承ください。

第2章

装置の設置

Ⅰ．装置の設置に関する注意点

本装置の各設置方法について説明します。
下記は設置に関する注意点です。よくご確認いただいてから設置してください。

注意！

本装置は直射日光が当たるところや、温度の高いところには設置しないようにしてください。
内部温度が上がり、動作が不安定になる場合があります。

注意！

ACアダプタのプラグを本体に差し込んだ後にACアダプタのケーブルを左右および上下に引っ張らず、緩みがある状態にしてください。
抜き差しもケーブルを引っ張らず、コネクタを持って行ってください。
また、ACアダプタのケーブルを足などで引っ掛けてプラグ部に異常な力が掛からないように配線にご注意ください。

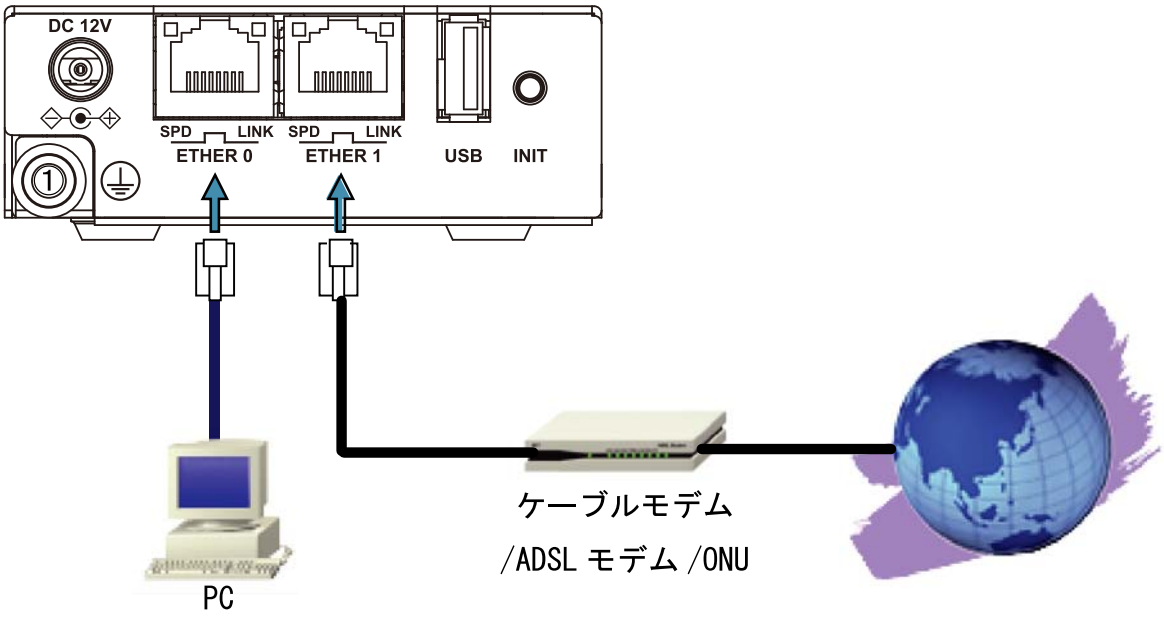
注意！

本装置側でも各ポートでARP tableを管理しているため、PCを接続しているポートを変更するとそのPCから通信ができなくなる場合があります。このような場合は、本装置側のARP tableが更新されるまで(数秒～数十秒)通信できなくなりますが、故障ではありません。

II．装置の設置（NXR-G100）

NXR-G100 と、PC や ADSL モデム / ケーブルモデム /ONU は、以下の手順で接続してください。

接続図＜例＞



1 本装置と ADSL モデム / ケーブルモデム /ONU や PC・HUB など、接続する全ての機器の電源が“ OFF ”になっていることを確認してください。

2 本装置の前面にある Ether 1 ポートと、ADSL モデム / ケーブルモデム /ONU を、LAN ケーブルで接続してください。

3 本装置の前面にある Ether 0 ポートと、HUB や PC を LAN ケーブルで接続してください。

※ 工場出荷設定状態の場合、本装置へのログインは、Ether 0 ポートに接続した PC からおこないます。

本装置の全 Ethernet ポートは Gigabit Ethernet、AutoMDI/MDI-X に対応しています。

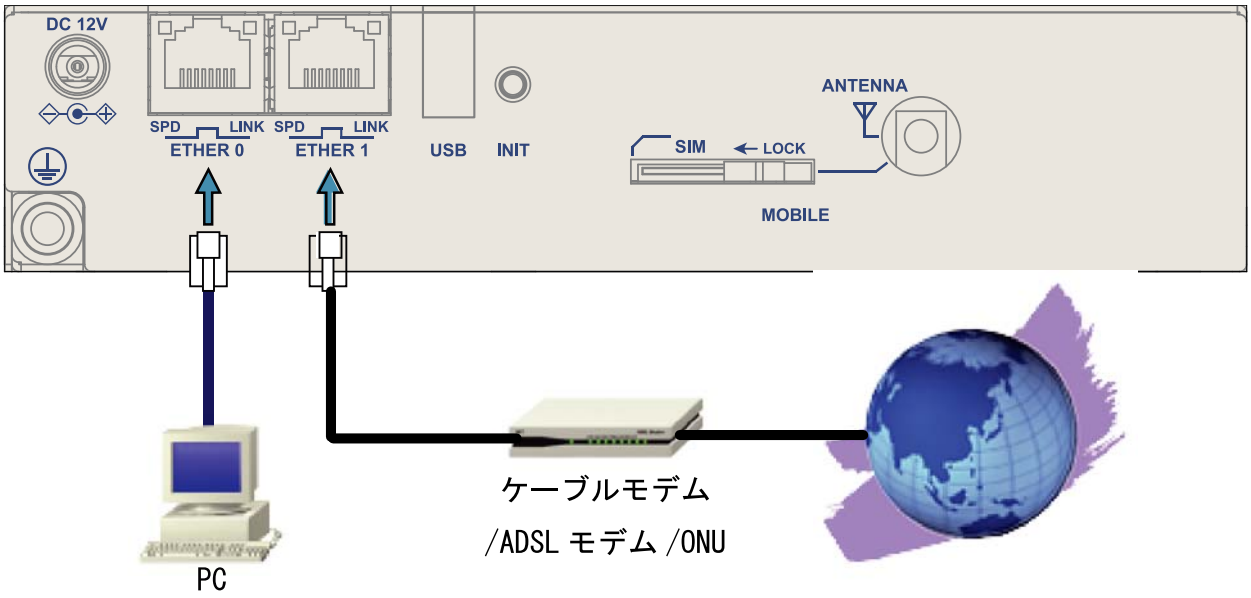
4 本装置と電源コード、電源コードとコンセントを接続してください。

5 全ての接続が完了しましたら、各機器の電源を投入してください。

III．装置の設置（NXR-G100/F）

NXR-G100/F と、PC や ADSL モデム / ケーブルモデム /ONU は、以下の手順で接続してください。

接続図＜例＞



1 本装置と ADSL モデム / ケーブルモデム /ONU や PC・HUB など、接続する全ての機器の電源が“ OFF ”になっていることを確認してください。

2 本装置の前面にある Ether 1 ポートと、ADSL モデム / ケーブルモデム /ONU を、LAN ケーブルで接続してください。

3 本装置の前面にある Ether 0 ポートと、HUB や PC を LAN ケーブルで接続してください。

※ 工場出荷設定状態の場合、本装置へのログインは、Ether 0 ポートに接続した PC からおこないます。

本装置の全 Ethernet ポートは Gigabit Ethernet、AutoMDI/MDI-X に対応しています。

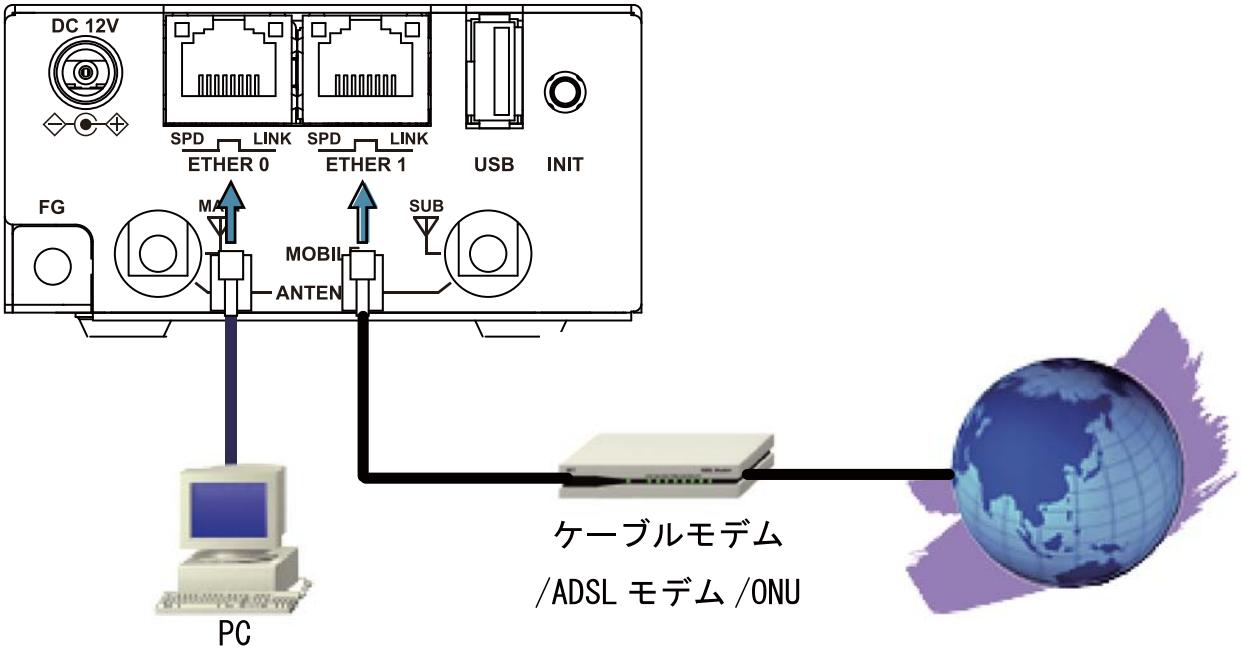
4 本装置と電源コード、電源コードとコンセントを接続してください。

5 全ての接続が完了しましたら、各機器の電源を投入してください。

Ⅳ．装置の設置（NXR-G100/KL）

NXR-G100/KL と、PC や ADSL モデム / ケーブルモデム /ONU は、以下の手順で接続してください。

接続図＜例＞



1 本装置と ADSL モデム / ケーブルモデム /ONU や PC・HUB など、接続する全ての機器の電源が“ OFF ”になっていることを確認してください。

2 本装置の前面にある Ether 1 ポートと、ADSL モデム / ケーブルモデム /ONU を、LAN ケーブルで接続してください。

3 本装置の前面にある Ether 0 ポートと、HUB や PC を LAN ケーブルで接続してください。

※ 工場出荷設定状態の場合、本装置へのログインは、Ether 0 ポートに接続した PC からおこないます。

本装置の全 Ethernet ポートは Gigabit Ethernet、AutoMDI/MDI-X に対応しています。

4 本装置と電源コード、電源コードとコンセントを接続してください。

5 全ての接続が完了しましたら、各機器の電源を投入してください。

この装置は、クラス A 情報技術装置です。
この装置を家庭環境で使用すると、電波妨害を引き起こすことがあります。
この場合には、使用者が適切な対策を講ずるよう要求されることがあります。

第3章

コンピュータのネットワーク設定

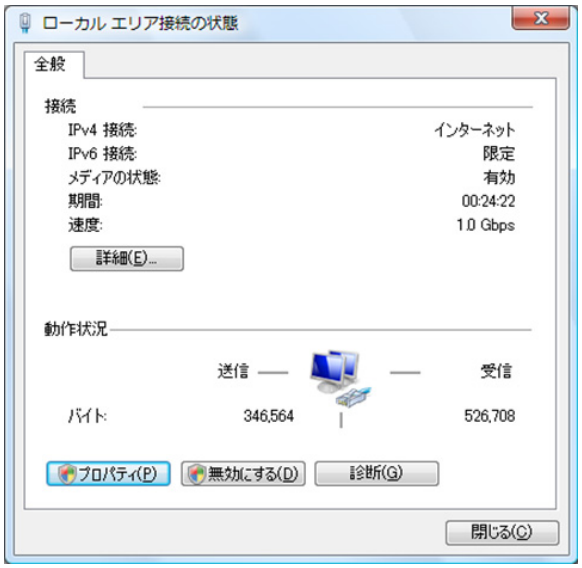
第３章　コンピュータのネットワーク設定

Ⅰ．Windows Vista のネットワーク設定

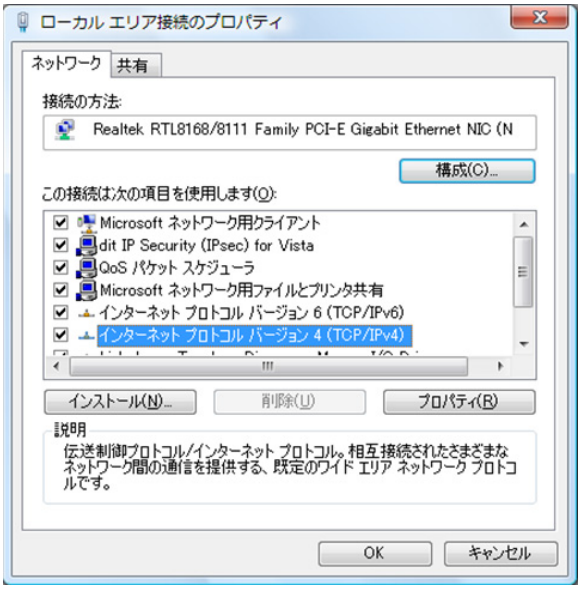
ここではWindows Vistaが搭載されたコンピュータのネットワーク設定について説明します。

1　「コントロールパネル」→「ネットワークとインターネット」→「ネットワークと共有センター」→「ネットワーク接続の管理」から、「ローカル エリア接続」を開きます。

2　「ローカル エリア接続の状態」画面が開いたらプロパティをクリックします。

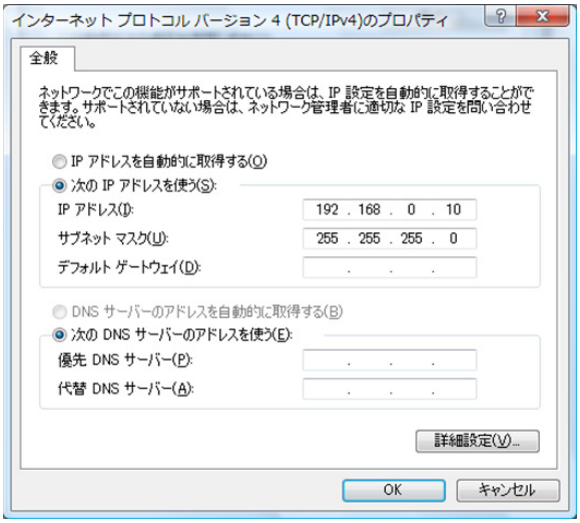


3　「ローカルエリア接続のプロパティ」画面が開いたら、「インターネットプロトコルバージョン4(TCP/IPv4)」を選択して「プロパティ」ボタンをクリックします。



4　「インターネットプロトコルバージョン4(TCP/IPv4)」の画面では、「次のIPアドレスを使う」にチェックを入れて以下のように入力します。

IPアドレス「192.168.0.10」
サブネットマスク「255.255.255.0」
デフォルトゲートウェイ「空欄」



5　最後にOKボタンをクリックして設定完了です。これで本装置へのログインの準備が整いました。

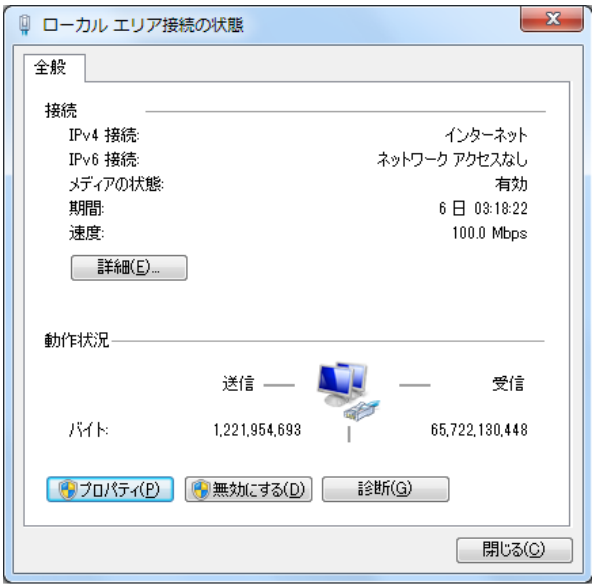
第３章　コンピュータのネットワーク設定

Ⅱ．Windows 7 のネットワーク設定

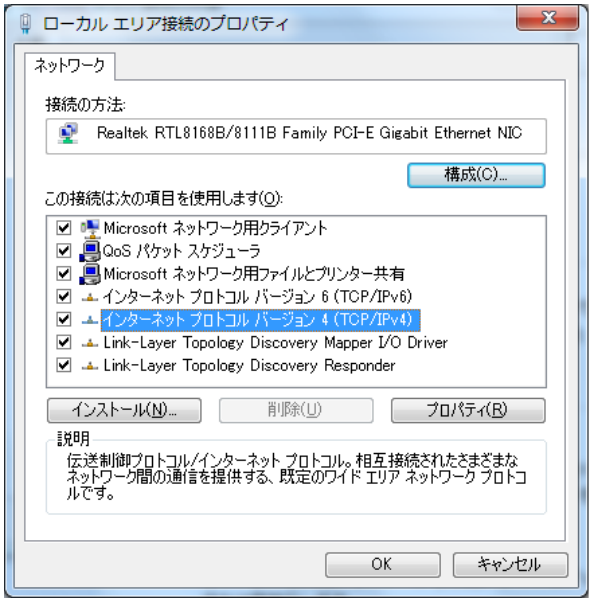
ここではWindows 7が搭載されたコンピュータのネットワーク設定について説明します。

1　「コントロールパネル」→「ネットワークとインターネット」→「ネットワークと共有センター」から、「ローカル エリア接続」を開きます。

2　「ローカル エリア接続の状態」画面が開いたらプロパティをクリックします。

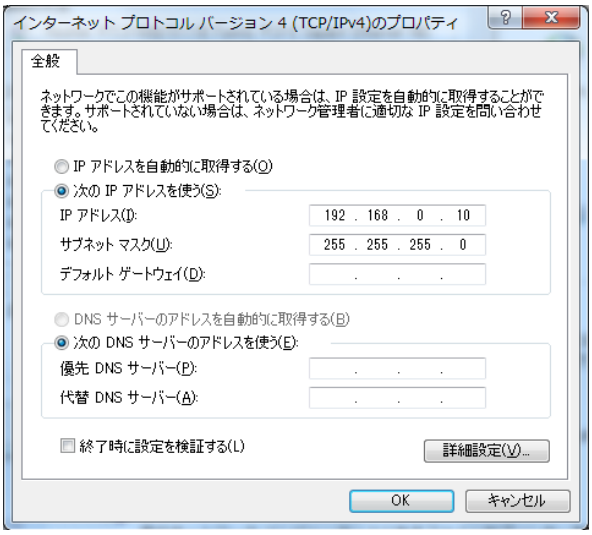


3　「ローカルエリア接続のプロパティ」画面が開いたら、「インターネットプロトコルバージョン４(TCP/IPv4)」を選択して「プロパティ」ボタンをクリックします。



4　「インターネットプロトコルバージョン４(TCP/IPv4)」の画面では、「次のIPアドレスを使う」にチェックを入れて以下のように入力します。

IPアドレス「192.168.0.10」
サブネットマスク「255.255.255.0」
デフォルトゲートウェイ「空欄」



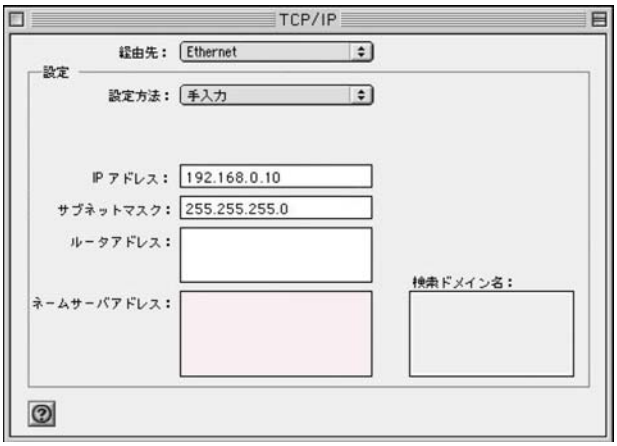
5　最後にOKボタンをクリックして設定完了です。これで本装置へのログインの準備が整いました。

III. Macintosh のネットワーク設定

ここではMacintoshのネットワーク設定について説明します。

1 「アップルメニュー」から「コントロールパネル」→「TCP/IP」を開きます。

2 経由先を「Ethernet」、設定方法を「手入力」にして、以下のように入力してください。
IPアドレス「192.168.0.10」
サブネットマスク「255.255.255.0」
ルータアドレス「空欄」

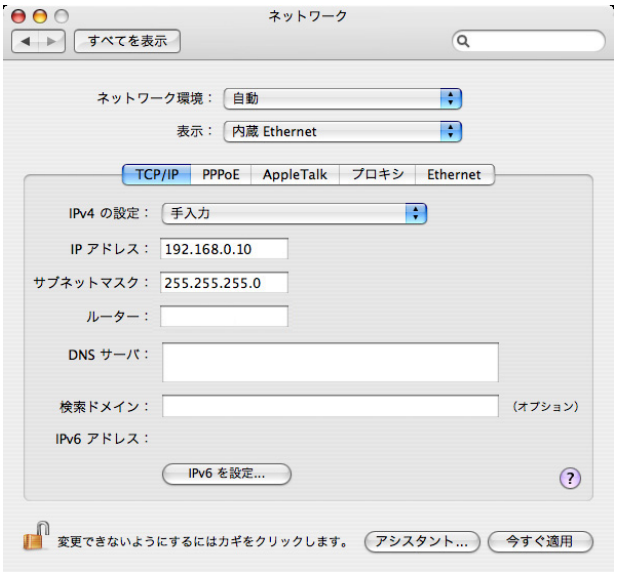


3 ウィンドウを閉じて設定を保存します。その後Macintosh本体を再起動してください。これで本装置へログインする準備が整いました。

ここでは、Mac OS Xのネットワーク設定について説明します。

1 「システム環境設定」から「ネットワーク」を開きます。

2 ネットワーク環境を「自動」、表示を「内蔵Ethernet」、IPv4の設定を「手入力」にして、以下のように入力してください。
IPアドレス「192.168.0.10」
サブネットマスク「255.255.255.0」
ルーター「空欄」



3 ウィンドウを閉じて設定の変更を適用します。これで、本装置へログインする準備が整いました。

第4章

本装置へのログイン

第４章　本装置へのログイン

Ⅰ．本装置の GUI へのログイン

■ 本装置の GUI へのログイン

1. 本装置の ETHER 0 ポートと PC を LAN ケーブルで接続します。

2. PC で Web ブラウザを起動します。

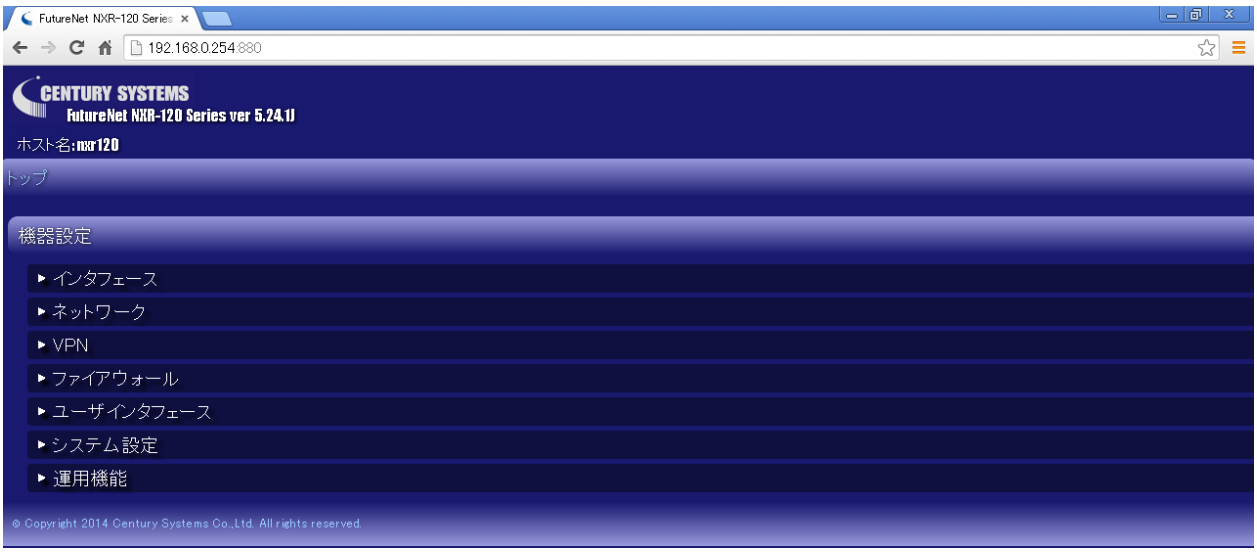
   ブラウザのアドレス欄に、以下の IP アドレスとポート番号を入力してください。

   http://192.168.0.254:880/

   ※ 192.168.0.254 は、ETHER 0 ポートの工場出荷時の IP アドレスです。アドレスを変更した場合は、そのアドレスを指定してください。**設定画面のポート番号 880 は変更することができません。**

3. 認証ダイアログ画面が表示されます。ユーザ名、パスワード共に「admin」（工場出荷設定）を入力してログインします。

4. 下記のような画面が表示されます。以上で、本装置の GUI へのログインは完了です。



Ⅱ．本装置の CLI へのログイン

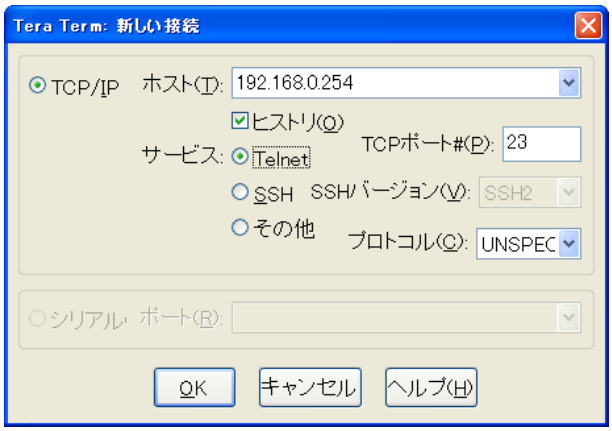
■ 本装置の CLI へのログイン(TELNET)

1．本装置の ETHER 0 ポートと PC を LAN ケーブルで接続します。

2．PC から TELNET 接続を開始すると、ログイン画面が表示されます。

3. ユーザ名、パスワード共に「admin」（工場出荷設定）を入力してログインします。

＜画面は TeraTerm による Telnet のログイン画面です＞



以上で、本装置の CLI へのログインは完了です。

Ⅱ．本装置の CLI へのログイン

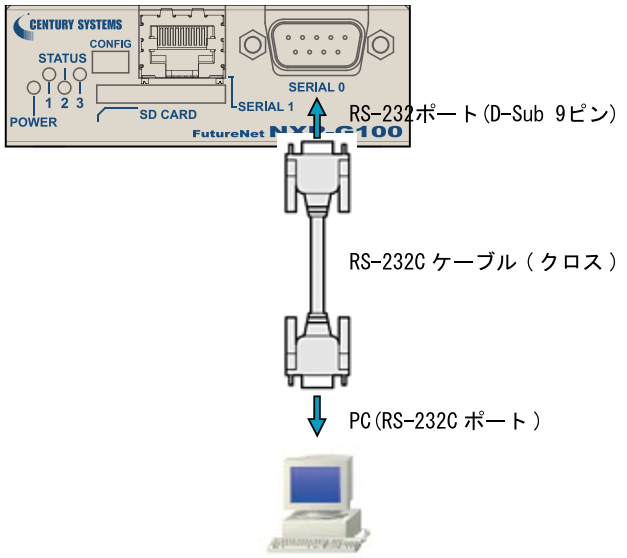
■ 本装置の CLI へのログイン(CONSOLE)

1．本装置前面の CONSOLE ポートと変換アダプタを、LAN ケーブルで接続します。接続に使用する以下の部品は、製品に付属されています。

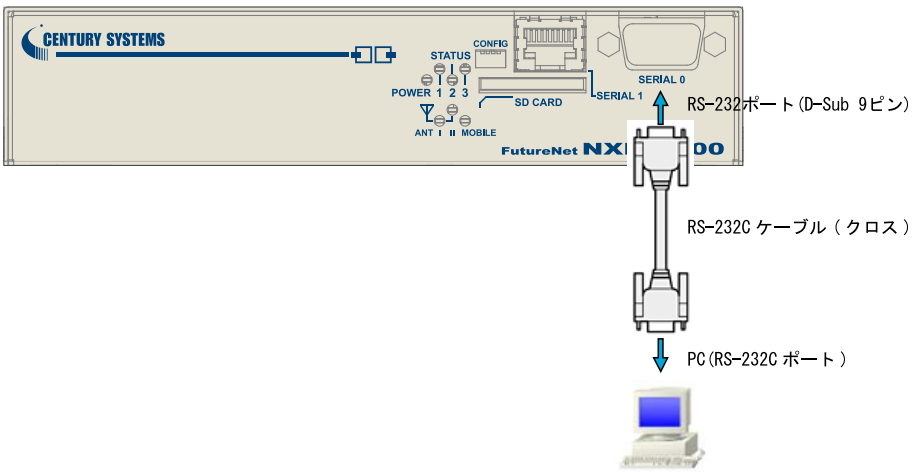
・LAN ケーブル(ストレート、１m)
・RJ-45/D-sub9 ピン変換アダプタ(クロス)

2．変換アダプタのコネクタを、PC の RS-232C ポートに接続してください。

＜NXR-G100＞



＜NXR-G100/F＞

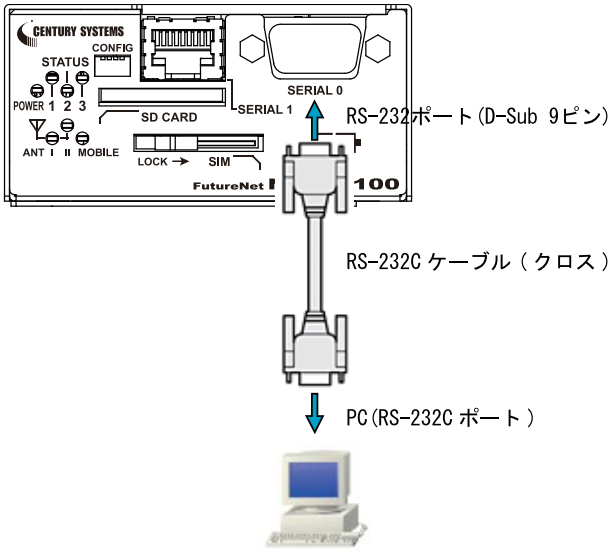


＜次ページに続く＞

Ⅱ．本装置の CLI へのログイン

■ 本装置の CLI へのログイン(CONSOLE)＜続き＞

＜ NXR-G100/KL ＞

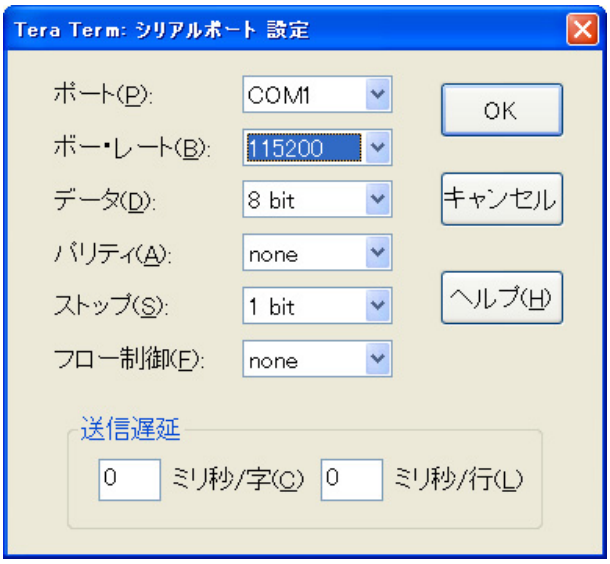


■ 本装置の CLI へのログイン(CONSOLE)＜続き＞

3．本装置を接続した PC で、設定用のターミナルソフト(TeraTerm 等)を起動します。

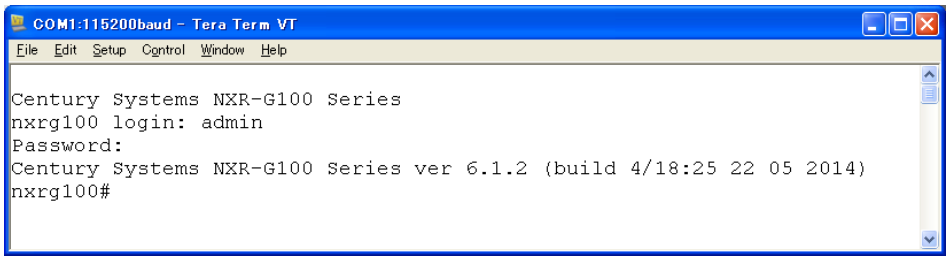
4．接続条件設定は以下のように設定します。< 設定例(TeraTerm での接続設定画面)>

※ 設定方法については、ご使用の各ターミナルソフトの説明書をご覧ください。



5．「Return」キーまたは「Enter」キーを押すと、ログイン画面が表示されます。

6．ユーザ名、パスワード共に「admin」（工場出荷設定）を入力してログインします。



以上で、本装置の CLI へのログインは完了です。

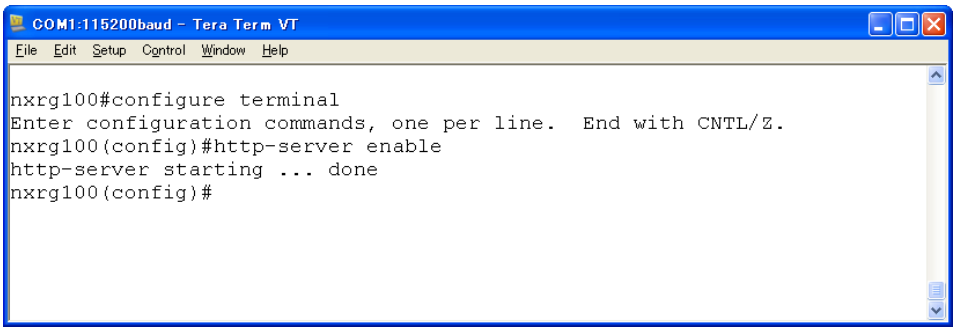
Ⅲ．HTTPサーバの起動

■ HTTP サーバの起動

本装置の工場出荷設定状態で電源を投入するとHTTPサーバが起動しますが、設定変更等によりHTTPサーバが起動しない場合は、下記の手順で HTTP サーバを起動してください。

1．CLI にログインした後、「configure terminal」コマンドで、CONFIGURATION モードに移行します。

2. 「http-server enable」コマンドを実行して、HTTP サーバを起動します。



以上で、HTTP サーバの起動は完了です。

Ⅳ．GUIで設定可能な項目

本装置のGUIで設定可能な項目の一覧です。

[インタフェース]

Ethernet I/F
- Ethernet

PPP I/F
- PPP/モバイルアカウント
- PPPoE
- モバイル設定

[ネットワーク]

IPv4
- スタティックルート
- 固定ARP
- NAT

DHCP
- DHCPネットワーク
- DHCPホスト
- DHCPリレー

- DNS
- WarpLink
- NTP

[VPN]

IPsec
- IPsecトンネル
- IPsec全体設定
- IPsec認証設定

L2TPv3
- L2TPv3接続設定
- L2TPv3全体設定

[ファイアウォール]

アクセスリスト
- IPv4アクセスリスト

[ユーザインタフェース]

SSH
- SSHサービス
- SSH鍵（netconf）

NETCONF
- NETCONF

CRP
- CRPグローバル
- CRPクライアント

[システム設定]

システム設定
- 本装置のパスワード
- ホスト名
- 内蔵時計
- セッション数

ログ
- システムログ
- ログメール

設定情報
- 設定の保存
- 設定の復帰
- 設定のリセット

ファームウェア
- ファームウェアアップデート

- スケジュール
- 省電力設定
- M2Mモード

[運用機能]

ネットワーク診断
- Ping
- Traceroute

パケットダンプ
- パケットダンプ
- パケットダンプ結果表示

ログ情報
- システムログ
- ブートログ

システム情報
- システム情報
- テクニカルサポート
- システムモニター

- 再起動
- ディスク管理
- サポート情報

第5章

インタフェース設定

第５章　インタフェース設定

Ⅰ．Ethernet I/F

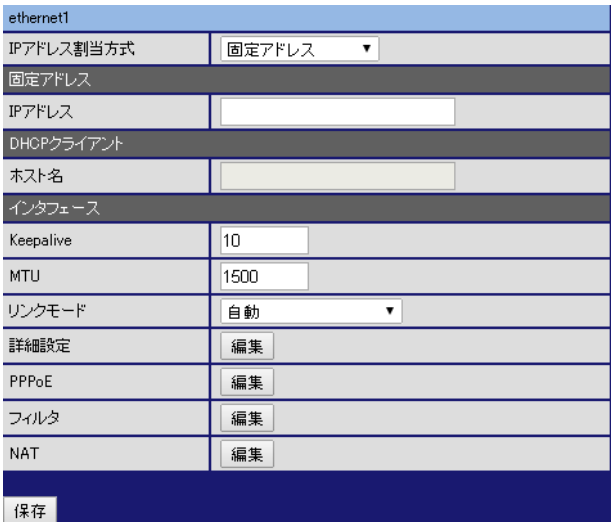
1．Ethernet

GUI画面のメニューを下記の順にクリックします。
インタフェース
　Ethernet I/F
　　・Ethernet

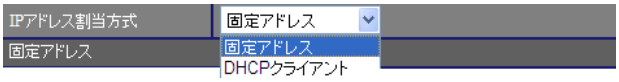
■ Ethernet

インタフェース	IPアドレス	MTU	リンクモード	編集
ethernet0	192.168.0.254/24	1500	auto	編集
ethernet1		1500	auto	編集

設定するインタフェースを選択して「編集」をクリックします。



○ IP アドレス割当方式
「固定アドレス」/「DHCP クライアント」をプルダウンから選択してください。



[固定アドレス]
○ IP アドレス
「固定アドレス」を選択した場合に入力してください。IP アドレス / マスクビット値の形式で入力してください。
[入力例]　192.168.1.254/24

[DHCP クライアント]
○ホスト名
「DHCP クライアント」を選択した場合に入力してください。必要がなければ、空欄でも構いません。

[インタフェース]
○ Keepalive
Ethernetポートのリンク状態を定期的に監視します。OSPF の使用時にリンクダウンを検知した場合、そのインタフェースに関連付けられたルーティング情報の配信を停止します。再度リンク状態がアップした場合には、そのインタフェースに関連付けられたルーティング情報の配信を再開します。監視間隔は、1-60[秒]の間で設定できます。また、0 を設定すると、リンク監視を行いません。デフォルト値は、10[秒]です。

○ MTU
「Path-MTU-Black-HOLE」現象が発生した場合等は、ここの値を変更することで回避できます。通常は初期設定の1500[バイト]のままで構いません。

○リンクモード
リンクモードをプルダウンから選択してください。工場出荷設定は「自動」です。

設定を保存するには、「保存」をクリックします。

●詳細設定

「編集」をクリックすると、下記の画面が表示されます。

○ TCP MSS
「使用しない」/「使用する」/「自動」をプルダウンから選択します。
・「使用する」場合、MSS 値（500 ～ 1460[bytes]）を設定します。
・IPv4 パケット内のプロトコルが、TCP の場合に有効な機能です。
・UDP、ICMP やその他のプロトコルでは、送信するアプリケーション側で、DF ビットを「0」にしたり、パケットサイズを小さくして送信することで対処するようにしてください。

TCP MSS
Path MTU Discovery（PMTUD）機能によって、フラグメントなしでパケットの送信を行うことが可能になります。しかし、通信の経路上に、ブラックホールルータが存在する場合や、PMTUD 機能をサポートしない機器が存在する場合は、PMTUD 機能が適切に動作しなくなるため、MTU 超えが発生したルータ上でパケットがドロップされて、End-to-end での通信に支障をきたすことになります。このような場合、TCP では、MSS フィールド値を調整することによって、サイズの大きいパケットでも、フラグメントなしで転送することが可能になるため、スループットの低下を抑制することが出来ます。

○ PROXY ARP
「使用しない」/「使用する」をプルダウンから選択します。

○ Directed Broadcast
「使用しない」/「使用する」をプルダウンから選択します。

・「使用する」を選択すると、該当するインタフェースにおいて、Directed Broadcast の転送を許可します。

Directed Broadcast
IP アドレスのホスト部がすべて「1」の IP アドレスのことです。
(例) 192.168.0.0/24 の Directed Broadcast は、192.168.0.255 です。

○ ICMP Redirects
「使用しない」/「使用する」をプルダウンから選択します。

・「使用する」を選択すると、該当するインタフェースにおいて、ICMP Redirects を送出します。

ICMP Redirects
他に適切な経路があることを通知する ICMP パケットのことです。

○ ICMP Mask Reply
「使用しない」/「使用する」をプルダウンから選択します。

・ネットワーク監視装置によっては、LAN 内装置の監視を ICMP Address Mask の送受信によって行う場合があります。
・「使用する」を選択すると、該当するインタフェースにて受信した ICMP Address Mask Request (type=17)に対して、Reply(type=18)を返送し、インタフェースのサブネットマスク値を通知します。
・「使用しない」を選択すると、Request に対して応答しません。

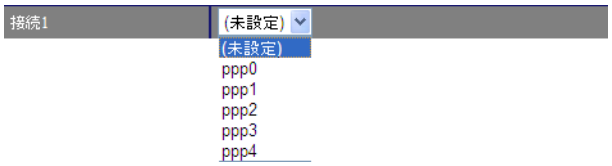
設定を保存するには、「保存」をクリックします。

Ⅰ．Ethernet I/F

● PPPoE

「編集」をクリックすると、下記の画面が表示されます。

接続番号を選択し、プルダウンからインタフェースを選択します。



設定を保存するには、「保存」をクリックします。

PPPoE 接続の設定については、
「第５章 インタフェース設定 のⅡ .PPP/ モバイル」
を参照してください。

Ｉ．Ethernet I/F

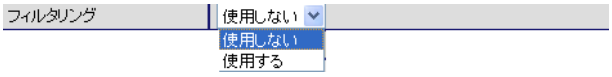
●フィルタ

「編集」をクリックします。

[ステートフルパケットインスペクション(SPI)]

○フィルタリング

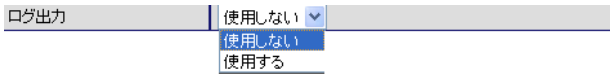
プルダウンから、「使用する」/「使用しない」を選択します。



・簡易ファイヤウォールの一つとして、SPI 機能をサポートしています。
・パケットに関連するコネクションの状態を見て、当該パケットをドロップ（または許可）します。

○ログ出力

プルダウンから、「使用する」/「使用しない」を選択します。



・パケットが SPI フィルタにマッチした場合、システムログに出力することが出来ます。
・フィルタリングを「使用する」場合に、選択することが出来ます。

○出力制限(パケット数)

1 秒当たりのログ出力数（0～100[パケット / 秒]）を指定することが出来ます。
・初期値は、10[パケット / 秒]です。

・WAN 側からの意図しないパケットが、SPI フィルタに大量にマッチする可能性があるため、ログ数を増やす場合は、十分に注意してください。
・ログ出力を「使用する」場合に、設定することが出来ます。

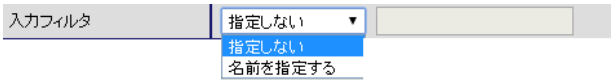
設定を保存するには、「保存」をクリックします。

Ｉ．Ethernet I/F

[IPv4フィルタ]

○入力フィルタ

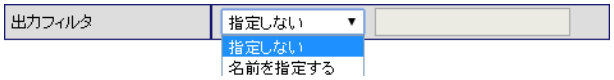
プルダウンから、「指定しない」/「名前を指定する」を選択します。



・「名前を指定する」場合は、入力フィルタの名前を指定します。

○出力フィルタ

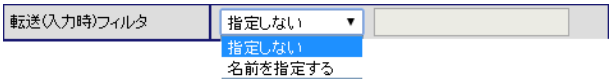
プルダウンから、「指定しない」/「名前を指定する」を選択します。



・「名前を指定する」場合は、入力フィルタの名前を指定します。

○転送（入力時）フィルタ

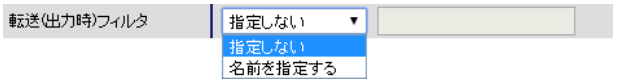
プルダウンから、「指定しない」/「名前を指定する」を選択します。



・「名前を指定する」場合は、入力フィルタの名前を指定します。

○転送（出力時）フィルタ

プルダウンから、「指定しない」/「名前を指定する」を選択します。



・「名前を指定する」場合は、入力フィルタの名前を指定します。

設定を保存するには、「保存」をクリックします。

フィルタの設定については、「第８章　ファイアウォール」を参照してください。

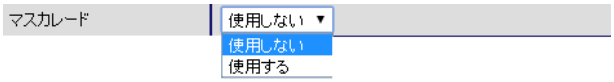
● NAT

「編集」をクリックすると、下記の画面が表示されます。

[IPv4 NAT]

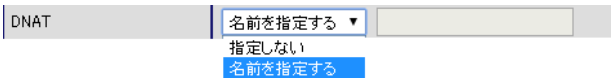
○マスカレード

プルダウンから、マスカレードの設定（「使用しない」/「使用する」）を選択します。



○ DNAT

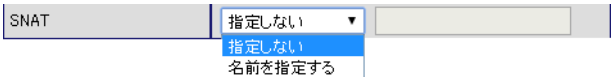
プルダウンから、DNATの設定（「指定しない」/「名前を指定する」）を選択します。



・「名前を指定する」場合は、適用するDNATの名前を入力します。

○ SNAT

プルダウンから、SNATの設定（「指定しない」/「名前を指定する」）を選択します。



・「名前を指定する」場合は、適用するSNATの名前を入力します。

設定を保存するには、「保存」をクリックします。

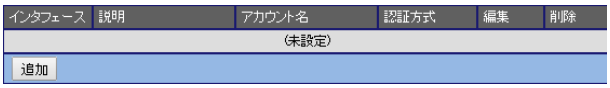
NATの設定については、「第６章　ネットワークのⅠ.IPv4、3.NAT」を参照してください。

Ⅱ．PPP/モバイル

1．PPP / モバイルアカウント

GUI画面のメニューを下記の順にクリックします。
インタフェース
　PPP/ モバイル
　　・PPP/ モバイルアカウント

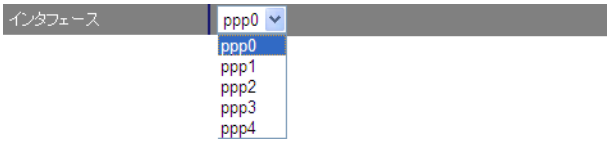
■PPP/ モバイルアカウント



PPP/ モバイルアカウントの追加

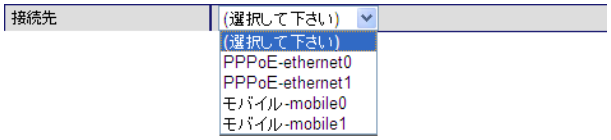
「追加」をクリックします。

○インタフェース
使用するインタフェースをプルダウンから選択します。

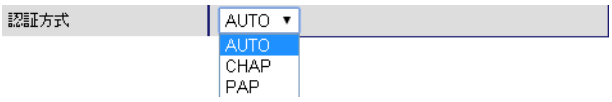


○説明
PPP/ モバイルアカウントの説明を記載します。

○接続先
プルダウンから、接続先を選択します。



○認証方式
認証方式をプルダウンから選択します。



○アカウント名
プロバイダから指定されたアカウントを入力してください。

○パスワード
プロバイダから指定された接続パスワードを入力してください。

設定を保存するには、「保存」をクリックします。

[モバイルカード設定]

接続先として「モバイル -mobile0」/「モバイル -mobile1」を選択した場合に、設定します。

○電話番号

接続先電話番号を設定します。

○ APN

APN(Access Point Name）を設定します。

・モバイルネットワークのデータ通信で必要になる接続先を指定する文字列の事です。プロバイダー毎に固有の名前を設定します。

○ CID

CID（Context Identifier）を設定します。

○ PDP タイプ

プルダウンから、PDP タイプ（「IP」/「PPP」）を選択します。

○ CRG ドメイン（※ NXR-G100/KL のみ）

KDDI の閉域型リモートアクセスサービス「(クローズド リモート ゲートウェイ（CRG)」を利用する場合に、CRG ドメインを設定します。

・接続先として、「モバイル -mobile1」を指定した場合に、設定することが出来ます。

○接続時間制限

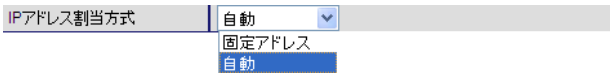
プルダウンから、接続時間制限（「使用する」/「使用しない」）を選択します。

・使用するを選択した場合は、接続時間制限（30～21474836[sec]）を指定します。初期値は、600[sec]です。

● TCP/IP

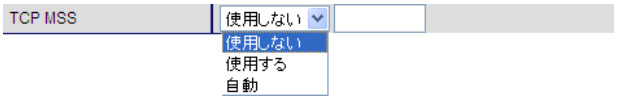
「編集」をクリックします。

○ IP アドレス割当方式
「自動」/「固定アドレス」をプルダウンから選択します。



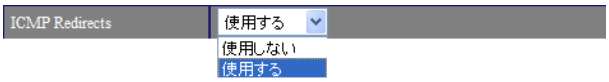
○ IP アドレス
「固定アドレス」を選択した場合に、入力します。

○ TCP MSS
「使用する」/「使用しない」/「自動」をプルダウンから選択します。



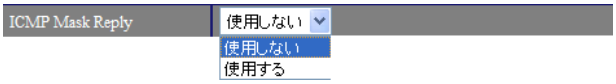
「使用する」を選択した場合、TCP MSS の値（500～1460[bytes]）を設定します。

○ ICMP Redirects
「使用する」を選択すると、該当するインタフェースにおいて、ICMP Redirects を送出します。
「使用する」/「使用しない」をプルダウンから選択します。



・ICMP Redirects とは、他に適切な経路があることを通知する ICMP パケットのことです。

○ ICMP Mask Reply
「使用する」/「使用しない」をプルダウンから選択します。



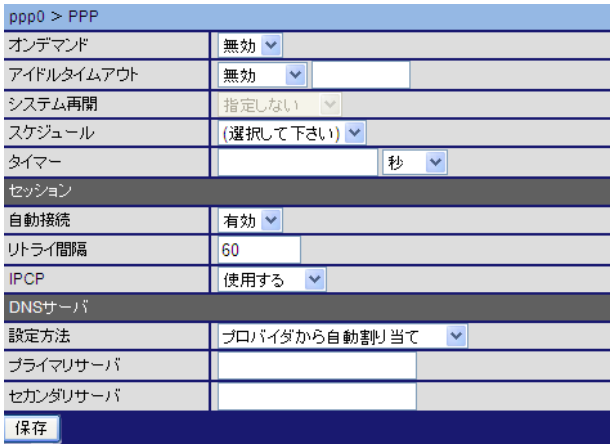
・ネットワーク監視装置によっては、LAN 内装置の監視を ICMP Address Mask の送受信によって行う場合があります。
・「使用する」を選択すると、該当するインタフェースにて受信した ICMP Address Mask Request (type=17)に対して、Reply(type=18)を返送し、インタフェースのサブネットマスク値を通知します。
・「使用しない」を選択すると、Request に対して応答しません。

設定を保存するには、「保存」をクリックします。

Ⅱ．PPP/モバイル

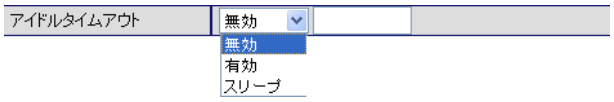
● PPP

「編集」をクリックします。



○オンデマンド
プルダウンから、「有効」/「無効」を選択します。

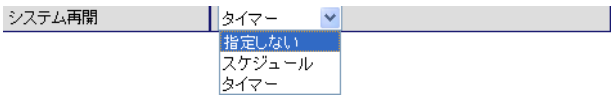
○アイドルタイムアウト
プルダウンから、「無効」/「有効」/「スリープ」を選択します。



「有効」/「スリープ」を選択した場合は、アイドルタイムアウト（30-86400[sec]）を設定します。

「有効」の場合、アイドルタイムアウトで設定した時間内に、IP パケットの送受信が無ければ、PPP を切断します（あるいはオンデマンド状態へと遷移します）。
「スリープ」の場合、アイドルタイムアウトによる PPP 切断時、システムスリープ状態に移行します。

○システム再開（システムスリープからの復帰）
「スリープ」を指定した場合、プルダウンからシステム再開の方法（「指定しない」/「スケジュール」/「タイマー」）を選択します。



○スケジュール
「スケジュール」を選択した場合、システム再開のためのスケジュール番号を指定します。
（スケジュール設定は、別途行う必要があります。）

○タイマー
「タイマー」を選択した場合、システム再開までのタイマーを設定します。
「秒」の場合、1～31536000 の値を指定します。
「分」の場合、1～525600 の値を指定します。
「時間」の場合、1～8760 の値を指定します。
「日」の場合、1～365 の値を指定します。

設定を保存するには、「保存」をクリックします。

[セッション]

○自動接続

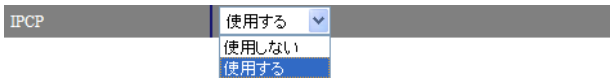
「有効」/「無効」をプルダウンから選択します。

○リトライ間隔

30-600[秒]の間で設定します。デフォルト値は60[秒]です。

○IPCP（Internet Protocol Control Protocol）

「使用する」/「使用しない」をプルダウンから選択します。



設定を保存するには、「保存」をクリックします。

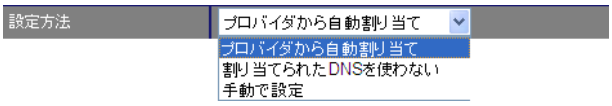
[DNSサーバ]

○設定方法

特に指定のない場合は、「プロバイダから自動割り当て」を選択します。

指定されている場合は「手動で設定」を選択して、DNSサーバのIPアドレスを入力します。

プロバイダからDNSアドレスを自動割り当てされても、そのアドレスを使用しない場合は「割り当てられたDNSを使わない」を選択します。この場合は、LAN側の各ホストにDNSサーバのアドレスをそれぞれ設定しておく必要があります。



○プライマリサーバ

○セカンダリサーバ

「手動で設定」を選択した場合に、DNSサーバのIPアドレスを入力します。

設定を保存するには、「保存」をクリックします。

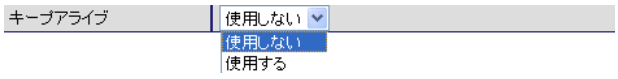
●インタフェース

「編集」をクリックします。

○MTU
MTUの値（128～1500[バイト]）を設定します。
初期値は、1454[バイト]です。

○MRU
MRUの値（128～1500[バイト]）を設定します。
初期値は、1454[バイト]です。

[LCPキープアライブ]
○キープアライブ
プルダウンから、「使用する」/「使用しない」を選択します。

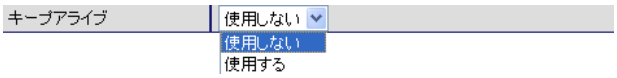


・「送信間隔」および「送信回数」は、キープアライブを「使用する」場合に、設定することが出来ます。
・LCPキープアライブが、（送信回数だけ）連続で失敗した場合に、PPPを切断します。

○送信間隔
LCPキープアライブの送信間隔（30～600[sec]）を設定します。初期値は、30[sec]です。

○送信回数
LCPキープアライブの送信回数（1～10[回]）を設定します。初期値は、3[回]です。

[ICMPキープアライブ]
○キープアライブ
プルダウンから、「使用する」/「使用しない」を選択します。



・「送信間隔」、「送信回数」および「宛先IPアドレス」は、キープアライブを「使用する」場合に、設定することが出来ます。
・ICMPキープアライブのリトライが、（送信回数だけ）連続で失敗した場合に、PPPを切断します。

○送信間隔
ICMPキープアライブの送信間隔（30～600[sec]）を設定します。初期値は、30[sec]です。

○送信回数
ICMPキープアライブのリトライ回数（0～10[回]）を設定します。初期値は、3[回]です。

○宛先IPアドレス
ICMPキープアライブの宛先IPアドレス（A.B.C.D）を設定します。

・空欄の場合は、P-t-Pゲートウェイを宛先として使用します。

設定を保存するには、「保存」をクリックします。

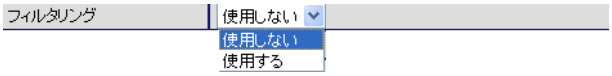
●フィルタ

「編集」をクリックします。

[ステートフルパケットインスペクション(SPI)]

○フィルタリング

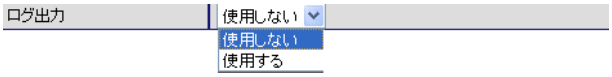
プルダウンから、「使用する」/「使用しない」を選択します。



・簡易ファイヤウォールの一つとして、SPI 機能をサポートしています。
・パケットに関連するコネクションの状態を見て、当該パケットをドロップ（または許可）します。

○ログ出力

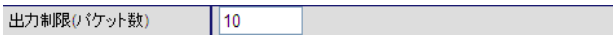
プルダウンから、「使用する」/「使用しない」を選択します。



・パケットが SPI フィルタにマッチした場合、システムログに出力することが出来ます。
・フィルタリングを「使用する」場合に、選択することが出来ます。

○出力制限(パケット数)

1 秒当たりのログ出力数（0 ～ 100[パケット / 秒]）を指定することが出来ます。初期値は、10[パケット / 秒]です。



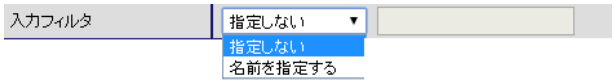
・WAN 側からの意図しないパケットが、SPI フィルタに大量にマッチする可能性があるため、ログ数を増やす場合は、十分に注意してください。
・ログ出力を「使用する」場合に、設定することが出来ます。

設定を保存するには、「保存」をクリックします。

[IPv4フィルタ]

○入力フィルタ

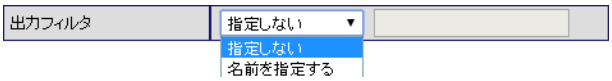
プルダウンから、「指定しない」/「名前を指定する」を選択します。



・「名前を指定する」場合は、入力フィルタの名前を指定します。

○出力フィルタ

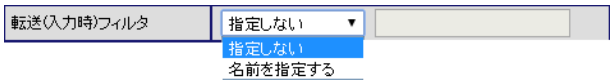
プルダウンから、「指定しない」/「名前を指定する」を選択します。



・「名前を指定する」場合は、入力フィルタの名前を指定します。

○転送（入力時）フィルタ

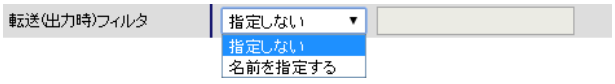
プルダウンから、「指定しない」/「名前を指定する」を選択します。



・「名前を指定する」場合は、入力フィルタの名前を指定します。

○転送（出力時）フィルタ

プルダウンから、「指定しない」/「名前を指定する」を選択します。



・「名前を指定する」場合は、入力フィルタの名前を指定します。

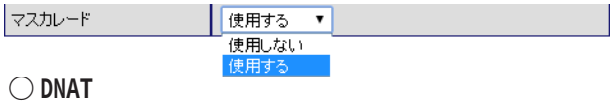
設定を保存するには、「保存」をクリックします。

● NAT

「編集」をクリックします。

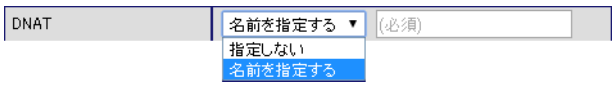
○マスカレード

プルダウンから、「使用する」「使用しない」を選択します。

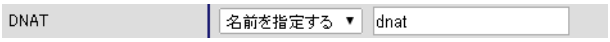


○ DNAT

プルダウンから、「名前を指定する」「指定しない」を選択します。

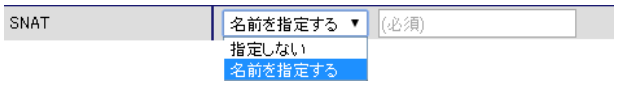


「名前を指定する」を選択した場合は、適用するDNATの名前を入力します。

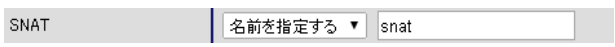


○ SNAT

プルダウンから、「名前を指定する」「指定しない」を選択します。



「名前を指定する」を選択した場合は、SNATの名前を入力します。



設定を保存するには、「保存」をクリックします。

PPP アカウントの編集

インタフェース	説明	アカウント名	認証方式	編集	削除
ppp0		aaa	auto	編集	削除

PPP アカウントを編集するには「編集」をクリックします。

ppp0	
説明	
接続先	モバイル-mobile0
認証方式	AUTO
アカウント名	aaa
パスワード	•••
モバイルカード設定	
電話番号	09012342222
APN	mobile.ne.jp
CID	1
PDPタイプ	IP
TCP/IP	編集
PPP	編集
インタフェース	編集
フィルタ	編集
NAT	編集
保存	

各項目については、**PPP アカウントの追加**を参照してください。

PPP アカウントの削除

インタフェース	サービス名	アカウント名	認証方式	編集	削除
ppp0		userid	chap	編集	削除

PPP アカウントを削除するには「削除」をクリックします。

2．PPPoE

地域 IP 網での工事や不具合、また ADSL 回線の不安定な状態によって、正常に PPPoE 接続が行えなくなることがあります。

これはユーザー側が PPPoE セッションが確立していないことを検知していても、地域 IP 網側はそれを検知していないために、ユーザー側からの新規接続要求を受け入れることができない状態になっていることが原因です。

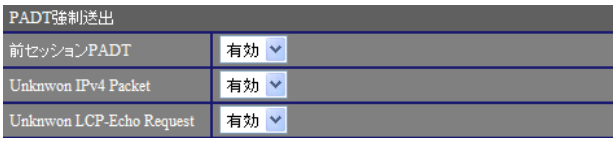
ここで PPPoE 特殊オプション機能を使うことにより、本装置が PPPoE セッションを確立していないことを検知し、強制的に PADT パケットを地域 IP 網側へ送信して、地域 IP 網側に PPPoE セッションの終了を通知します。

本装置から PADT パケットを送信することで、地域 IP 網側の PPPoE セッション情報がクリアされ、PPPoE の再接続性を高めることができます。

PADT = PPPoE Active Discovery Terminate の略。PPPoE セッションが終了したことを示すパケットです。これにより、PADT を受信した側で該当する PPPoE セッションを終了させます。

GUI 画面のメニューを下記の順にクリックします。
インタフェース
　PPP I/F
　　・PPPoE

■ PPPoE



[PADT 強制送出]

○前セッション PADT
回線接続時に前回の PPPoE セッションの PADT を強制送出します。
「有効」/「無効」をプルダウンから選択します。

○ Unknwon IPv4 Packet
非接続セッションの IPv4 パケット受信時に PADT を強制送出します。
「有効」/「無効」をプルダウンから選択します。

○ Unknwon LCP-Echo Request
非接続セッションの LCP echo request 受信時に PADT を強制送出します。
「有効」/「無効」をプルダウンから選択します。

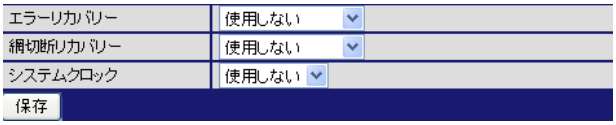
設定を保存するには、「保存」をクリックします。

地域 IP 網の工事後に PPPoE 接続が出来なくなってしまう事象を回避するためにも、PPPoE 特殊オプション機能を有効にした上で PPPoE 接続をしていただくことを推奨します。

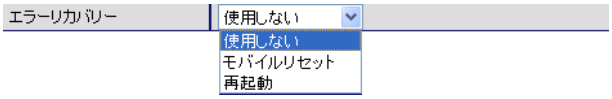
3．モバイル設定

GUI画面のメニューを下記の順にクリックします。
インタフェース
　PPP/ モバイル
　　・モバイル設定

■モバイル設定

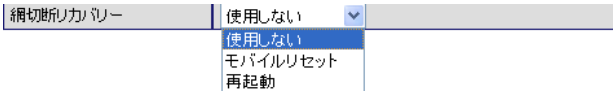


○エラーリカバリー
プルダウンから、「使用しない」/「モバイルリセット」/「再起動」を選択します。



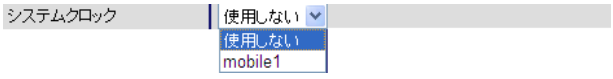
・モバイル端末との通信に重大な問題が発生する可能性が高いと判断した場合に、モバイルリセット、または再起動（システム再起動）を実行します。
・「使用しない」場合は、何も実行しません。

○網切断リカバリー
プルダウンから、「使用しない」/「モバイルリセット」/「再起動」を選択します。



・モバイルモジュールによるPPP接続時、網側から切断された場合に、モバイルリセット、または再起動（システム再起動）を実行します。
・「使用しない」場合は、何も実行しません。

○システムクロック（※NXR-G100/KLのみ）
プルダウンから、「使用しない」/「mobile 1」を選択します。



・「mobile 1」を選択した場合、LTE通信モジュールが、網側から取得した時刻情報を、NXRのシステムクロックに反映します。
・NTPサーバを設定した場合は、「mobile 1」を指定することは出来ません。

設定を保存するには、「保存」をクリックします。

第6章

ネットワーク

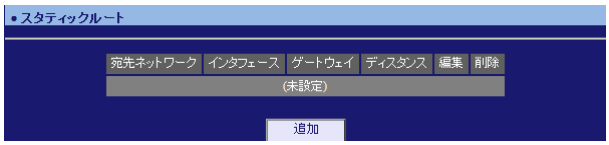
第6章　ネットワーク

Ⅰ．IPv4

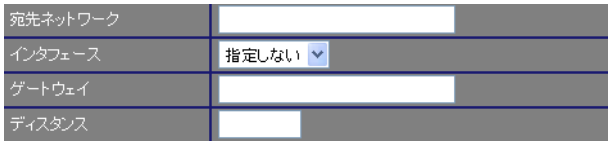
1．スタティックルート

GUI画面のメニューを下記の順にクリックします。
ネットワーク
　IPv4
　　・スタティックルート

■スタティックルート

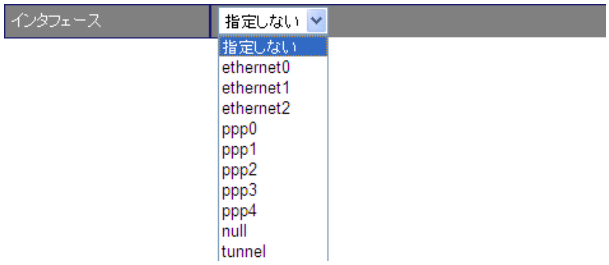


スタティックルートの追加
「追加」をクリックします。



○宛先ネットワーク
ネットワークアドレス/マスクビット値の形式で入力してください。
[入力例]　192.168.100.0/24
　　192.168.200.254/32

○インタフェース
プルダウンからインタフェースを選択します。



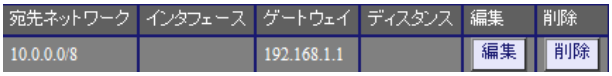
VLANインタフェースを指定する場合は、該当するethernetインタフェースを選択し、VLAN IDを入力してください。VLAN IDは、1-4094の間で設定します。

○ゲートウェイ
インタフェースを「指定しない」に選択した場合、上位ルータのIPアドレスを入力します。

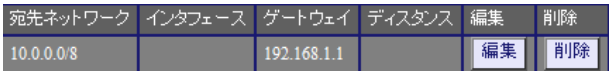
○ディスタンス
経路選択の優先順位を指定します。1-255の間で指定します。値が小さいほど優先度が高くなります。
スタティックルートのデフォルトディスタンス値は1です。

設定を保存するには、「保存」をクリックします。

スタティックルートの編集
「編集」をクリックします。



スタティックルートの削除
「削除」をクリックします。



2．固定 ARP

GUI 画面のメニューを下記の順にクリックします。
ネットワーク
　IPv4
　　・固定 ARP

■固定 ARP

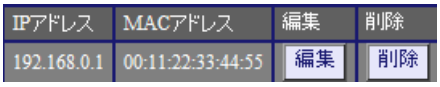
固定 ARP の追加
「追加」をクリックします。

○ IP アドレス
[入力例]　192.168.0.1

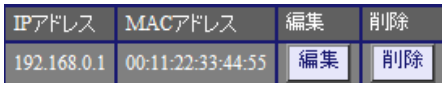
○ MAC アドレス
[入力例]　00:11:22:33:44:55

設定を保存するには、「保存」をクリックします。

固定 ARP の編集
「編集」をクリックします。



固定 ARP の削除
「削除」をクリックします。

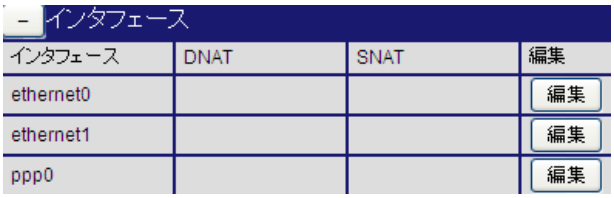


3．NAT

GUI画面のメニューを下記の順にクリックします。
ネットワーク
　IPv4
　　・NAT

■NAT

■インタフェース

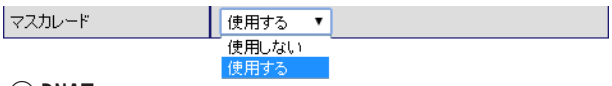


インタフェースの編集

当該インタフェースの「編集」をクリックします。

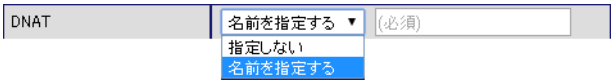
○マスカレード

プルダウンから、「使用する」「使用しない」を選択します。

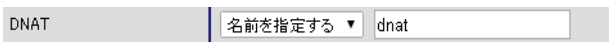


○ DNAT

プルダウンから、「名前を指定する」「指定しない」を選択します。

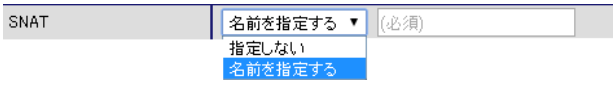


「名前を指定する」を選択した場合は、適用するDNATの名前を入力します。

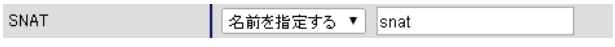


○ SNAT

プルダウンから、「名前を指定する」「指定しない」を選択します。

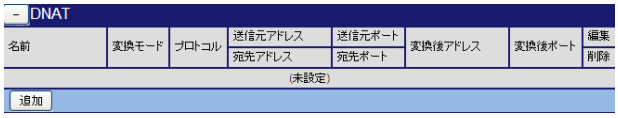


「名前を指定する」を選択した場合は、SNATの名前を入力します。



設定を保存するには、「保存」をクリックします。

■ DNAT



DNATの追加

「追加」をクリックします。

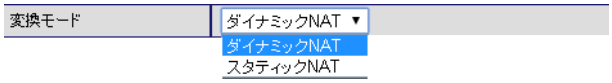
[DNAT]

○名前

DNATの名前を入力します（DNATに名前を付けます）。

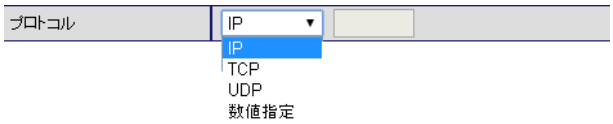
○変換モード

プルダウンから、「ダイナミックNAT」「スタティックNAT」を選択します。



○プロトコル

プルダウンから、プロトコルを選択します。
「数値指定」を選択した場合は、プロトコル番号（0-255）を指定します。



[送信元アドレス]

○送信元アドレス

以下の形式で、送信元アドレスを入力します。

A.B.C.D　：　ホストアドレス
A.B.C.D/M：　ネットワークアドレス
空欄　　：　any

○開始ポート

変換モードで「ダイナミックNAT」、プロトコルで、「TCP」/「UDP」を選択した場合に、開始ポート番号(1-65535)を指定することが出来ます。
空欄の場合、ポート番号は、「any」になります。

○終了ポート

変換モードで「ダイナミックNAT」、プロトコルで、「TCP」/「UDP」を選択した場合に、終了ポート番号(1-65535)を指定することが出来ます。
ただし、開始ポート＜終了ポートとなるように設定して下さい。

[宛先アドレス]
○宛先アドレス
以下の形式で、宛先アドレスを入力します。
A.B.C.D　：　ホストアドレス
A.B.C.D/M：　ネットワークアドレス
空欄　　：　any

○開始ポート
変換モードで「ダイナミックNAT」、プロトコルで、「TCP」/「UDP」を選択した場合に、開始ポート番号(1-65535)を指定することが出来ます。
空欄の場合、ポート番号は、「any」になります。

○終了ポート
変換モードで「ダイナミックNAT」、プロトコルで、「TCP」/「UDP」を選択した場合に、終了ポート番号(1-65535)を指定することが出来ます。
ただし、開始ポート＜終了ポートとなるように設定して下さい。

[スタティックNAT]
変換モードで、「スタティックNAT」を選択した場合に設定します。

○変換後アドレス
以下の形式で、変換後アドレスを入力します。
A.B.C.D/M

[ダイナミックNAT]
変換モードで、「ダイナミックNAT」を選択した場合に設定します。

○開始アドレス
以下の形式で、開始アドレスを入力します。
A.B.C.D

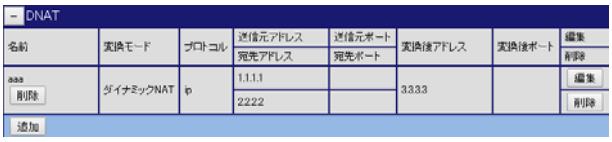
○終了アドレス
以下の形式で、開始アドレスを入力します。
A.B.C.D

○開始ポート
変換モードで「ダイナミックNAT」、プロトコルで、「TCP」/「UDP」を選択した場合に、開始ポート番号(1-65535)を指定することが出来ます。

○終了ポート
変換モードで「ダイナミックNAT」、プロトコルで、「TCP」/「UDP」を選択した場合に、終了ポート番号(1-65535)を指定することが出来ます。
ただし、開始ポート＜終了ポートとなるように設定して下さい。

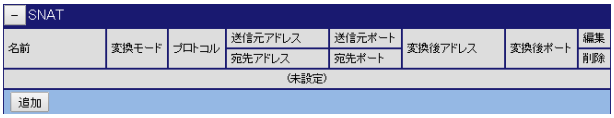
設定を保存するには、「保存」をクリックします

DNATの編集
当該項目の「編集」をクリックします。



DNATの削除
当該項目の「削除」をクリックします。

■ SNAT



SNAT の追加

「追加」をクリックします。

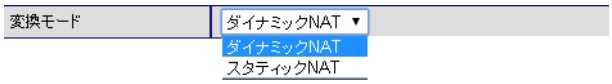
[SNAT]

○名前

SNAT の名前を入力します（SNAT に名前を付けます）。

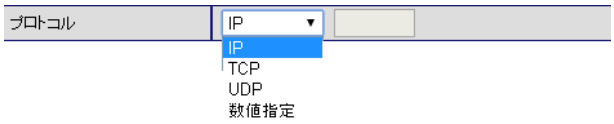
○変換モード

プルダウンから、「ダイナミック NAT」「スタティック NAT」を選択します。



○プロトコル

プルダウンから、プロトコルを選択します。
「数値指定」を選択した場合は、プロトコル番号（0-255）を指定します。



[送信元アドレス]

○送信元アドレス

以下の形式で、送信元アドレスを入力します。

A.B.C.D　：　ホストアドレス
A.B.C.D/M：　ネットワークアドレス
空欄　　：　any

○開始ポート

変換モードで「ダイナミック NAT」、プロトコルで、「TCP」/「UDP」を選択した場合に、開始ポート番号(1-65535)を指定することが出来ます。
空欄の場合、ポート番号は、「any」になります。

○終了ポート

変換モードで「ダイナミック NAT」、プロトコルで、「TCP」/「UDP」を選択した場合に、終了ポート番号(1-65535)を指定することが出来ます。
ただし、開始ポート＜終了ポートとなるように設定して下さい。

[宛先アドレス]
○宛先アドレス
以下の形式で、宛先アドレスを入力します。
A.B.C.D　：　ホストアドレス
A.B.C.D/M：　ネットワークアドレス
空欄　　：　any

○開始ポート
変換モードで「ダイナミックNAT」、プロトコルで、「TCP」/「UDP」を選択した場合に、開始ポート番号(1-65535)を指定することが出来ます。
空欄の場合、ポート番号は、「any」になります。

○終了ポート
変換モードで「ダイナミックNAT」、プロトコルで、「TCP」/「UDP」を選択した場合に、終了ポート番号(1-65535)を指定することが出来ます。
ただし、開始ポート＜終了ポートとなるように設定して下さい。

[スタティックNAT]
変換モードで、「スタティックNAT」を選択した場合に設定します。

○変換後アドレス
以下の形式で、変換後アドレスを入力します。
A.B.C.D/M

[ダイナミックNAT]
変換モードで、「ダイナミックNAT」を選択した場合に設定します。

○開始アドレス
以下の形式で、開始アドレスを入力します。
A.B.C.D

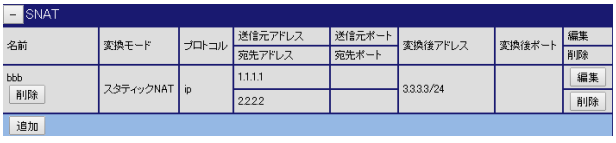
○終了アドレス
以下の形式で、開始アドレスを入力します。
A.B.C.D

○開始ポート
変換モードで「ダイナミックNAT」、プロトコルで、「TCP」/「UDP」を選択した場合に、開始ポート番号(1-65535)を指定することが出来ます。

○終了ポート
変換モードで「ダイナミックNAT」、プロトコルで、「TCP」/「UDP」を選択した場合に、終了ポート番号(1-65535)を指定することが出来ます。
ただし、開始ポート＜終了ポートとなるように設定して下さい。

設定を保存するには、「保存」をクリックします

SNATの編集
当該項目の「編集」をクリックします。



SNATの削除
当該項目の「削除」をクリックします。

第6章　ネットワーク

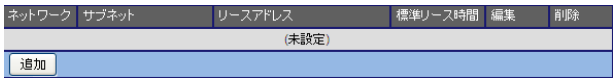
II．DHCP

1．DHCP ネットワーク

DHCP サーバ機能の設定をおこないます。

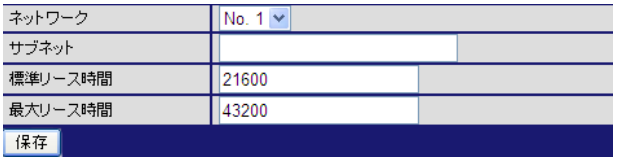
GUI 画面のメニューを下記の順にクリックします。
ネットワーク
　DHCP
　　・DHCP ネットワーク

■ DHCP ネットワーク

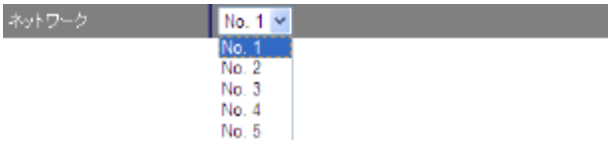


DHCP ネットワークの追加

「追加」をクリックすると、下記の画面が表示されます。



○ネットワーク
ネットワーク番号をプルダウンから選択します。



○サブネット
DHCP サーバを動作させるネットワーク空間のアドレスを設定します。
[入力例]　　172.16.0.0/16

○標準リース時間
DHCP クライアントに IP アドレスを割り当てる時間を指定します。
60-15552000[秒]の間で指定します。デフォルト値は 21600[秒]です。

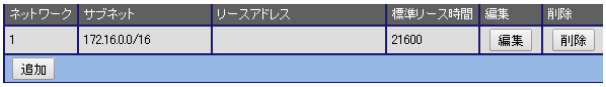
○最大リース時間
DHCP クライアントが割り当て時間を要求した時の最大割り当て時間を指定します。指定した値以上のリース時間を要求された場合、リース時間は指定値で設定されます。
60-15552000[秒]の間で指定します。デフォルト値は 43200[秒]です。

設定を保存するには、「保存」をクリックします。

II．DHCP

リースアドレスの追加

リースアドレスを追加するには、DHCPネットワークの画面で、「編集」をクリックします。

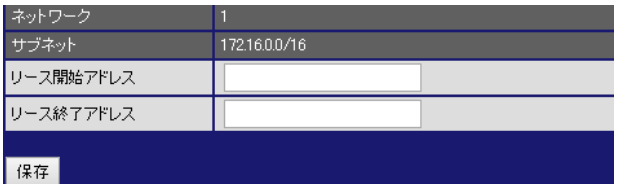


下記の画面が表示されます。

●リースアドレス

「追加」をクリックします。

下記の画面が表示されます。



○リース開始アドレス
リース開始アドレスを指定します。
[入力例] 172.16.0.1

○リース終了アドレス
リース終了アドレスを指定します。
[入力例] 172.16.10.254

・DHCPクライアントに割り当てる最初と最後のIPアドレスを指定します。両項目で設定した範囲のIPアドレスが、DHCPクライアントに割り当てられます。

設定を保存するには、「保存」をクリックします。

リースアドレスの編集

リースアドレスを編集するには、下記の画面で「編集」をクリックします。

リースアドレスの削除

リースアドレスを削除するには、「削除」をクリックします。

リースアドレスの追加

DHCPネットワークの一つのサブネット内に、複数のリースアドレスを設定することができます。
リースアドレスは、最大で16個設定することができます。
リースアドレスを追加するには、「追加」をクリックします。

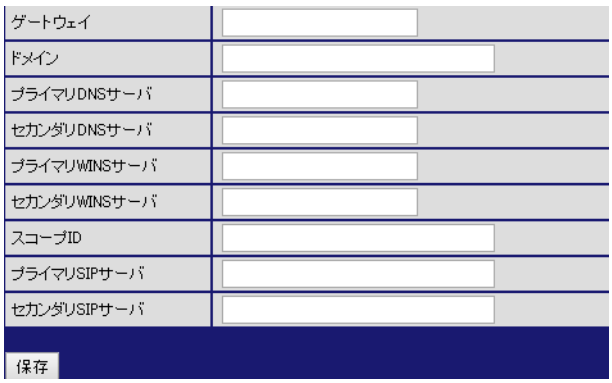
○標準リース時間
IPアドレスの標準リース時間を設定します。

○最大リース時間
IPアドレスの最大リース時間を設定します。

オプションの編集

オプションの設定 / 編集をするには、オプションの「編集」をクリックします。

下記の画面が表示されます。



●オプション

○ゲートウェイ

DHCPクライアントのデフォルトゲートウェイとなるアドレスを入力してください。通常は、本装置のインタフェースのIP アドレスを指定します。

○ドメイン

DHCPクライアントに割り当てるドメイン名を指定します（任意で指定）。

○プライマリDNS サーバ

○セカンダリDNSサーバ

DHCP クライアントに割り当てるDNS サーバアドレスを指定します（任意で指定）。

○プライマリWINS サーバ

○セカンダリWINSサーバ

DHCP クライアントに割り当てるWINS サーバのIPアドレスを指定します。

○スコープID

NetBIOS スコープID を配布できます。TCP/IP を介してNetBIOS を実行しているコンピュータでは、同じNetBIOS スコープID を使用するほかのコンピュータとのみNetBIOS 情報を交換することができます。

○プライマリSIPサーバ / セカンダリSIPサーバ

DHCPクライアントからのSIPサーバ要求に対して、SIP サーバアドレスを割り当てます。指定可能なアドレスは、IPv4アドレスまたはFQDNで、最大2つまで設定することができます。

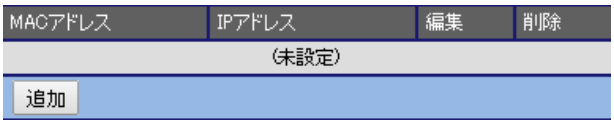
設定を保存するには、「保存」をクリックします。

2．DHCP ホスト

DHCP サーバ機能で、固定 IP アドレスを割り当てる場合の設定をおこないます。

GUI 画面のメニューを下記の順にクリックします。
ネットワーク
　DHCP
　　・DHCP ホスト

■ DHCP ホスト



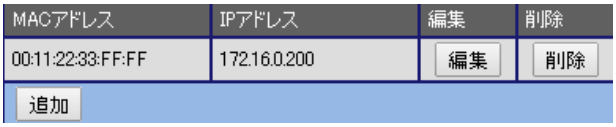
DHCP ホストの追加
「追加」をクリックします。

○ MAC アドレス
PC に装着されている LAN ボードなどの MAC アドレスを入力します。
[入力例]　00:11:22:33:ff:ff

○ IP アドレス
割り当てる IP アドレスを指定します。
[入力例]　172.16.0.200

設定を保存するには、「保存」をクリックします。

DHCP ホストの編集
「編集」をクリックします。



DHCP ホストの削除
「削除」をクリックします。

DHCP サーバ機能で、固定 IP アドレスを割り当てる場合でも、DHCP ネットワーク設定は必要です。その場合は、「DHCP サーバ設定」画面の「リース開始アドレス」「リース終了アドレス」に、「DHCP ホスト」で指定したアドレス範囲の先頭と末尾の IP アドレスを指定してください。

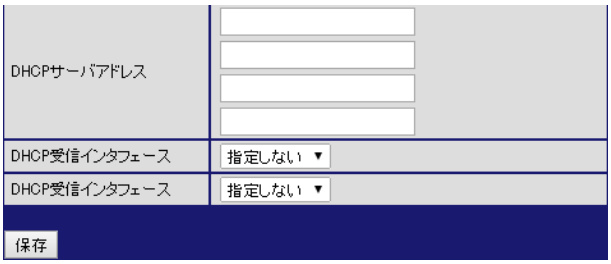
3．DHCP リレー

DHCP サーバと DHCP クライアントは、通常同じネットワークにないと通信できません。しかし、DHCP リレー機能を使うことで、異なるネットワークにある DHCP サーバを利用できるようになります。（本装置が、DHCP クライアントからの要求と DHCP サーバからの応答を中継します。）

NAT 機能を使用している場合は、DHCP リレー機能は使用できません。

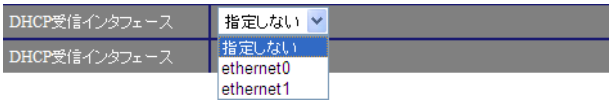
GUI 画面のメニューを下記の順にクリックします。
ネットワーク
　DHCP
　　・DHCP リレー

■ DHCP リレー



○ DHCP サーバアドレス
上位の DHCP サーバの IP アドレスを指定します。

○ DHCP 受信インタフェース
DHCP サーバ機能と同時に運用する場合を考慮して、クライアントからの BOOTP Request パケットを受信するインタフェースを指定することができます。



プルダウンから、該当するインタフェース（または「指定しない」）を選択します。
指定したインタフェース以外で受信した BOOTP Request はドロップされます。
指定しない場合は、どのインタフェースで BOOTP Request パケットを受信してもリレーされます。

設定を保存するには、「保存」をクリックします。

III．DNS

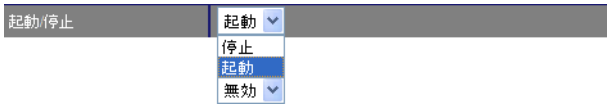
◆DNS

LAN 内の各ホストの DNS サーバ設定に本装置の IP アドレスを指定することによって、ISP から指定された DNS サーバや任意の DNS サーバへリレーすることができます。

GUI 画面のメニューを下記の順にクリックします。
ネットワーク
　・DNS

■ DNS

○起動 / 停止
サービスの「起動」/「停止」をプルダウンから選択します。



○タイムアウト
DNS サーバへの問い合わせが無応答の場合のタイムアウトを設定します。
5-30[秒]で設定できます。初期設定は 30 秒です。
使用環境によっては、DNS キャッシュのタイムアウトよりもブラウザなどのアプリケーションのタイムアウトが早く発生する場合があります。
この場合は、DNS キャッシュのタイムアウトを調整してください。

○ルート DNS 転送
設定した DNS サーバへの問い合わせに失敗した場合や、DNS サーバの指定が無い場合に、ルートサーバへ問い合わせをするかどうかを設定します。
プルダウンから「有効」/「無効」を選択します。

[DNS サーバ]
○サーバアドレス
任意の DNS サーバの IP アドレス（A.B.C.D）を入力してください。
PPPoE 接続時、ISP から指定された DNS サーバへリレーする場合は本設定の必要はありません。

[プライオリティ]
○ユーザ
○ ppp0/ppp1/ppp2/ppp3/ppp4
○ DHCP クライアント
○ DHCPv6 クライアント
DNS サーバのプライオリティ（1～20）を設定します。デフォルト値は 20 です。
同一プライオリティの場合の優先順位は、下記のとおりです。
ユーザ > ppp4 > ppp3 > ppp2 > ppp1 > ppp0 > DHCP > DHCPv6

設定を保存するには、「保存」をクリックします。

◆WarpLink

WarpLinkサービスのクライアントとして動作します（WarpLink Managerに対して、本装置の機器情報をHTTPSで送信します）。

GUI画面のメニューを下記の順にクリックします。
ネットワーク
　・WarpLink

■ WarpLink

○起動 / 停止
サービスの「起動」/「停止」をプルダウンから選択します。デフォルトは「停止」です。

・「起動」を選択すると、ダイナミックDNSが有効になり、本装置のWAN側IPアドレスを定期的（5分間隔）に送信します。

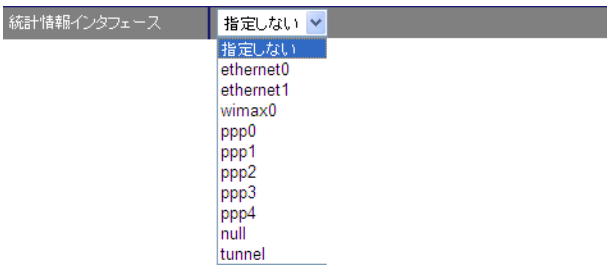
○ユーザ名
WarpLinkサービスのユーザIDを入力します。

○パスワード
WarpLinkサービスのパスワードを入力します。

○ Syslog情報送信
Syslog情報送信の「有効」/「無効」をプルダウンから選択します。デフォルトは「無効」です。

・「有効」を選択すると、本装置のsyslog情報を定期的（5分間隔）に送信します。
・サービスが停止（ダイナミックDNSが無効）の場合は、syslog情報は送信されません。
・syslog 情報は、前回からの差分を最大100キロバイト まで送信します。

○統計情報インタフェース
統計情報インタフェースをプルダウンで指定します。デフォルトは「指定しない」です。



・インタフェースを指定すると、本装置のCPU使用率、メモリ使用率および当該インタフェースのトラフィック量を定期的（5分間隔）に送信します。
・サービスが停止（ダイナミックDNSが無効）の場合は、統計情報は送信されません。
・統計情報は、30 秒間隔で取得したデータの3分間の平均を3 日分保持します。
・インタフェースは、2つまで指定することが出来ます。未指定の場合、統計情報は送信されません。

設定を保存するには、「保存」をクリックします。

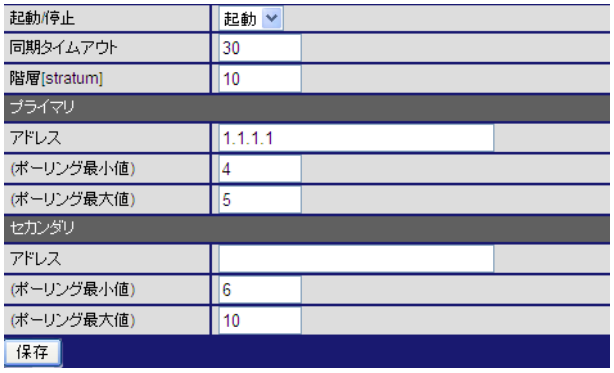
Ⅴ．NTP

◆NTP

本装置は、NTPサーバ/クライアント機能を持っています。インターネットを使った時刻同期手法の一つであるNTP(Network Time Protocol)を用いてNTPサーバと通信を行い、時刻を同期させることができます。

GUI画面のメニューを下記の順にクリックします。
ネットワーク
・NTP

■NTP



○起動/停止
サービスの「起動」/「停止」をプルダウンから選択します。

○同期タイムアウト
サーバ応答の最大待ち時間を1-30[秒]の間で設定できます。

○階層[stratum]
本装置をローカルサーバとして設定した場合のstratum level（1～15）を指定します。初期値は、「10」です。

[プライマリ]
○アドレス
NTP サーバのIP アドレスを入力します。
NTP サーバのIP アドレスを入力しない場合は、本装置はNTP サーバとしてのみ動作します。

○（ポーリング最小値）
4-16の間で指定します。デフォルト値は6です。

○（ポーリング最大値）
5-17の間で指定します。デフォルト値は10です。

「(ポーリング最小値)」「(ポーリング最大値)」によって、NTPサーバと通信をおこなう間隔を設定します。
サーバとの接続状態により、指定した最小値と最大値の範囲でポーリングの間隔を調整します。

Polling 間隔X(sec)を指定した場合、秒単位での間隔は2 のX 乗(秒)となります。
< 例 4：16 秒、 6：64 秒、... 10：1024 秒>

[セカンダリ]
○アドレス
○（ポーリング最小値）
○（ポーリング最大値）
必要に応じて、プライマリと同様に設定します。

設定を保存するには、「保存」をクリックします。

第7章

VPN

第 7 章　VPN

Ⅰ．IPsec

1．IPsec トンネル

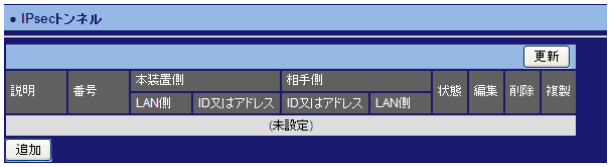
GUI 画面のメニューを下記の順にクリックします。

VPN

　IPsec

　　・IPsec トンネル

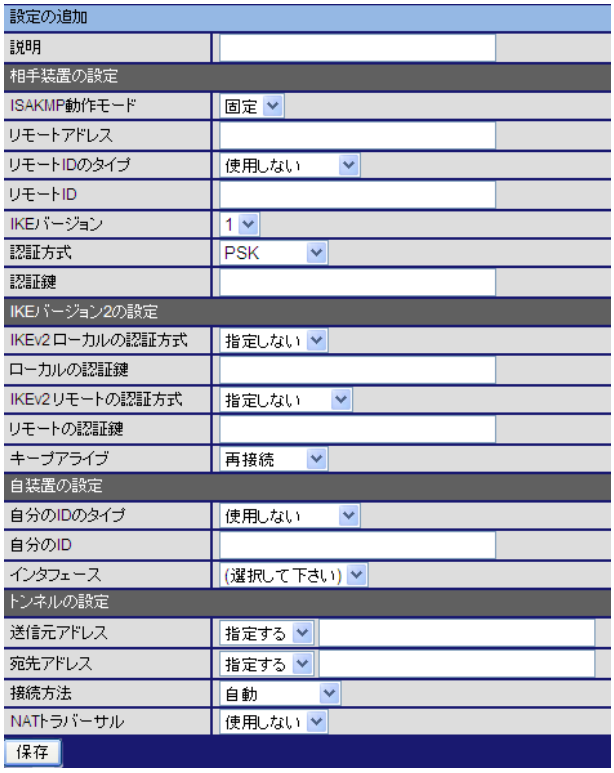
■ IPsec トンネル



IPsec トンネルの追加

IPsec トンネルを追加するには、「追加」をクリックします。

「追加」をクリックすると、下記の画面が表示されます。



○説明

IPsec トンネルの説明を記述します。

・1 ～ 64 文字の半角英数字 / 記号を使用することが出来ます。

Ⅰ．IPsec

[相手装置の設定]

○ ISAKMP 動作モード

ISAKMP 動作モード（「固定」/「動的」）を、プルダウンから選択します。

・本装置とリモート（対向装置）が、どちらも固定 IP アドレスの場合は、「固定」を選択します。
・本装置またはリモート（対向装置）のどちらか一方が、動的 IP アドレスの場合は、「動的」を選択します。

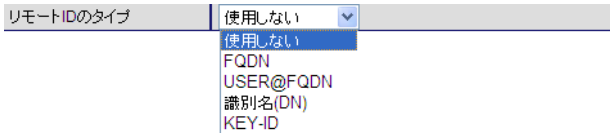
○リモートアドレス

リモートアドレス（対向装置の IPv4 アドレス）を A.B.C.D のフォーマットで入力します。

・リモートアドレスが、動的 IP アドレスの場合は、空欄にします。

○リモート ID のタイプ

プルダウンから、リモート ID のタイプを選択します。



○リモート ID

選択したリモート ID のタイプに従って、ID を入力します。

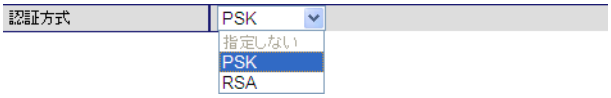
・「FQDN」の例： centurysys.co.jp
・「USER@FQDN」の例： user@centurysys.co.jp
・「識別名（DN)」の例：
C=JP, ST=Tokyo,O=century, OU=dev,
N=nxr1.centurysys.co.jp,
E=admin@centurysys.co.jp
・「KEY-ID」の例： keyid

○ IKE バージョン

プルダウンから、IKE のバージョン（「1」/「2」）を選択します。

○認証方式

プルダウンから、認証方式（「PSK」/「RSA」）を選択します。



○認証鍵

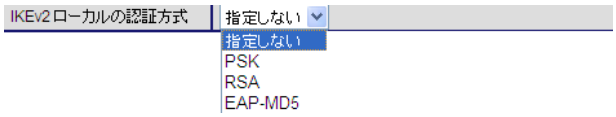
認証方式の設定に従って、認証鍵を入力します。
・「PSK」を選択した場合は、事前共有鍵を入力します。
・「RSA」を選択した場合は、RSA 公開鍵を入力します。

Ｉ．IPsec

[IKE バージョン２の設定]

○ IKEv2 ローカルの認証方式

IKEv2 で、本装置が使用する認証方式を、プルダウンから選択します。

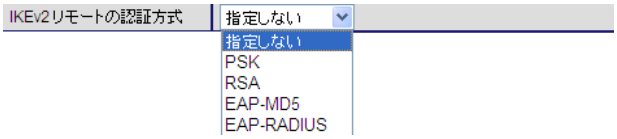


○ローカルの認証鍵

IKEv2 で、本装置が使用する認証鍵を入力します。

○ IKEv2 リモートの認証方式

IKEv2 で、対向装置が使用する認証方式を、プルダウンから選択します。

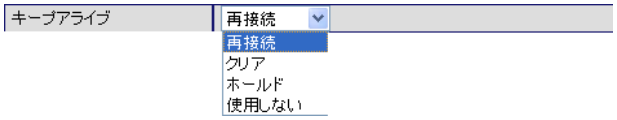


○リモートの認証鍵

IKEv2 で、対向装置が使用する認証鍵を入力します。

○キープアライブ

キープアライブでエラーを検出した場合、IKE/IPsec SA および IPsec policy を削除します。プルダウンから、その後の動作を選択します。



「再接続」

SA および policy の削除後に、IKE ネゴシエーションを開始します。
ただし、接続方法として「レスポンダー」を選択した場合は、IKE ネゴシエーションしません。

「クリア」

SA および policy の削除後は、ユーザの指示を待ちます。

「ホールド」

SA の削除後は、policy のみが有効になります。
policy にマッチするパケットを受信すると IKE ネゴシエーションを開始します。
ただし、接続方法として「レスポンダー」を選択した場合は、IKE ネゴシエーションしません。

「使用しない」

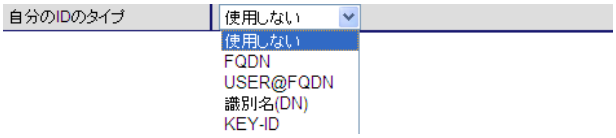
キープアライブを送信しません。ただし、対向装置からのキープアライブには応答します。

Ⅰ．IPsec

[自装置の設定]

○自分の ID タイプ

プルダウンから、リモート ID のタイプを選択します。



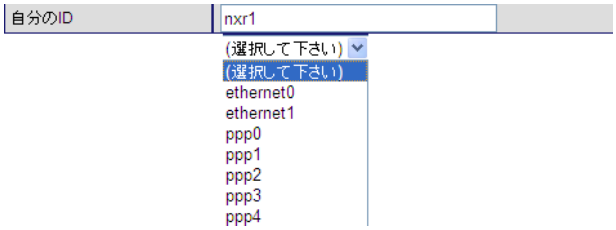
○自分の ID

選択したリモート ID のタイプに従って、ID を入力します。

- **「FQDN」の例： centurysys.co.jp**
- **「USER@FQDN」の例： user@centurysys.co.jp**
- **「識別名（DN)」の例：**
  C=JP, ST=Tokyo,O=century, OU=dev,
  N=nxr1.centurysys.co.jp,
  E=admin@centurysys.co.jp
- **「KEY-ID」の例： keyid**

○インタフェース

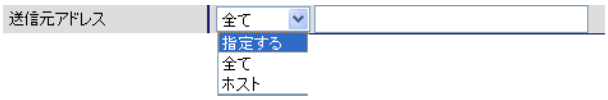
IPsec で使用するインタフェースを、プルダウンから選択します。



[トンネルの設定]

○送信元アドレス

IPsec トンネルの送信元アドレスを、プルダウンから選択します。



「指定する」

本装置側の（LAN 側の）ネットワークアドレス（A.B.C.D/M）を指定します。

「全て」

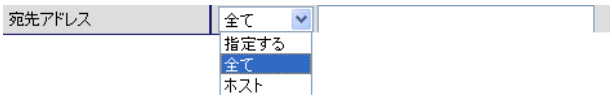
すべての送信元アドレスが、暗号化の対象となります。

「ホスト」

本装置が送信元となるパケットを暗号化します。

○宛先アドレス

IPsec トンネルの宛先アドレスを、プルダウンから選択します。



「指定する」

対向装置側の（LAN 側の）ネットワークアドレス（A.B.C.D/M）を指定します。

「全て」

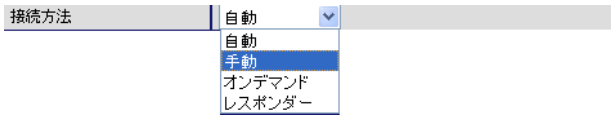
すべての宛先アドレスが、暗号化の対象となります。

「ホスト」

対向装置が宛先となるパケットを暗号化します。

Ⅰ．IPsec

○接続方法
プルダウンから、接続方法を選択します。



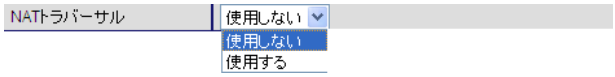
「自動」
IPsec サービス起動時に、ネゴシエーションを開始します。

「手動」
IPsec サービス起動時に、（tunnel を追加するだけで）ネゴシエーションを開始しません。Backup policy などで使用します。

「オンデマンド」
IPsec サービス起動時に、ルートのみを設定します。

「レスポンダー」
IPsec サービス起動時の動作は、「手動」と同様です。
ただし、いかなる場合（rekey を含む）においても、こちらから開始することはありません。

○NAT トラバーサル
プルダウンから、「使用する」/「使用しない」を選択します。

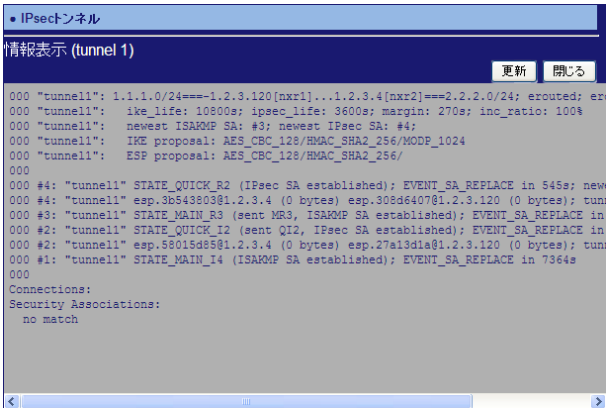


・本装置が、NAT ボックスの配下に位置する場合は、「使用する」を選択します。

１．IPsec

IPsec トンネルの状態

「表示」をクリックすると、IPsec トンネルの状態を表示します。



- 「更新」をクリックすると、最新の状態を取得することが出来ます。
- 「閉じる」をクリックすると、画面を閉じます。

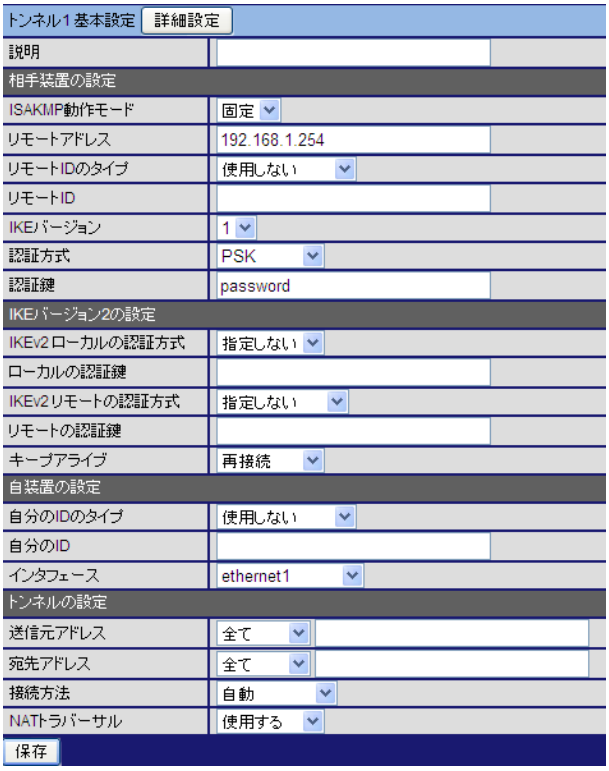
第７章　VPN

Ｉ．IPsec

IPsec トンネルの編集（基本設定）

「編集」をクリックすると、IPsec トンネルの基本設定を編集することが出来ます。

下記画面にて、各項目の編集を行います。



設定を保存するには、「保存」をクリックします。

IPsec トンネルの編集（詳細設定）

「詳細設定」をクリックすると、IPsec トンネルの詳細設定を編集することが出来ます。

[相手装置の設定]

基本設定を参照してください。

[IKE バージョン２の設定]

○ IKEv2 ローカルの認証方式

基本設定を参照してください。

○ローカルの認証鍵

基本設定を参照してください。

○ IKEv2 リモートの認証方式

基本設定を参照してください。

○リモートの認証鍵

基本設定を参照してください。

○ EAP の指定

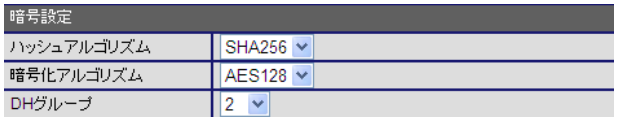
プルダウンから、EAP の指定（「使用しない」/「指定しない」/「指定する」）を選択します。

○ EAP ユーザ名

「指定する」を選択した場合、EAP 認証で使用する ID を設定します。

Ⅰ．IPsec

[暗号設定]

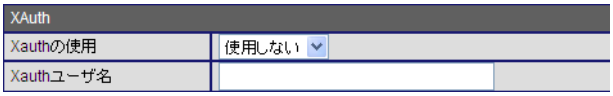


○ハッシュアルゴリズム
プルダウンから、ハッシュアルゴリズムを選択します。
・初期値は、「SHA256」です。

○暗号化アルゴリズム
プルダウンから、暗号化アルゴリズムを選択します。
・初期値は、「AES128」です。

○ DH グループ
プルダウンから、DH グループを選択します。
・初期値は、DH グループ「2」です。

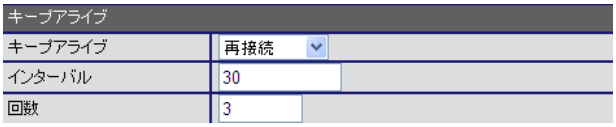
[XAuth]



○ Xauth の使用
Xauth の使用（「使用しない」/「サーバ」/「クライアント」）を、プルダウンから選択します。

○ Xauth ユーザ名
「クライアント」を選択した場合、ユーザ ID を設定します。

[キープアライブ]



○キープアライブ
基本設定を参照してください。

○インターバル
キープアライブのインターバル（10～3600 [sec]）を設定します。初期値は、「30」です。

○回数
キープアライブのリトライ回数（0～60[回]）を設定します。初期値は、「3」です。

・インターバル「30」、回数「3」の場合、30 秒間隔で、合計 4 回のキープアライブを実行し、すべて失敗した場合にエラーと判定します。

Ⅰ．IPsec

[ライフタイム]

○ライフタイム
ライフタイム（121-86400[sec]）を設定します。
・初期値は、「10800」です。

○再認証
プルダウンから、「使用する」/「使用しない 」を選択します。

・IKEv2 では、リキーのタイミングで、「再認証」または「リキー」を選択することが出来ます。
・セキュリティを考慮する場合は、「使用する」を選択します。
・再認証を行うと、負荷がかかるため、負荷に配慮する場合は、「使用しない」を選択します。

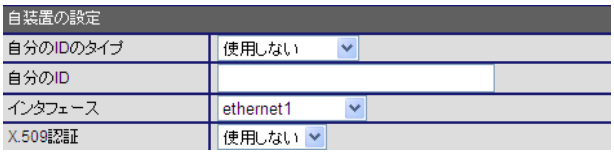
○リキーのマージン(時間)
リキーのマージン（30～360[sec]）を設定します。初期値は、「270」です。

・リキーを開始するタイミングを指定します。マージンが「270」の場合、ライフタイムが終了する 270[sec]前からリキーを開始します。

○マージン比率[%]
マージン比率（「0-100[%]」）を設定します。初期値は、「100」です。

・マージン比率によって、リキーのマージンを大きくすることが出来ます。
・マージン「270」、マージン比率「100」の場合、ライフタイム終了前の 270～540 秒の間に、ランダムなタイミングで、リキーを開始します。
・マージン比率を「0」に設定すると、毎回同じタイミングでリキーを行います。負荷やセキュリティ的に、問題があるため、設定しないことを推奨します。
・接続方法が、「レスポンダー」の場合、当該機器からはリキーを行いません。

[自装置の設定]



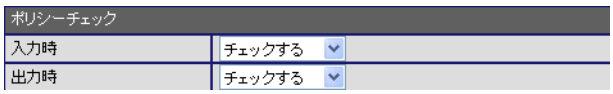
○自分の ID タイプ
基本設定を参照してください。

○自分の ID
基本設定を参照してください。

○インタフェース
基本設定を参照してください。

○ X.509 認証
・認証方式として「RSA」を指定した場合に、選択することが出来ます。
・IKEv2 ローカルの認証方式、IKEv2 リモートの認証方式として、「RSA」を指定した場合に、選択することが出来ます。

[ポリシーチェック]



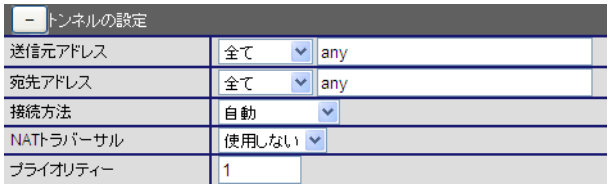
○入力時
プルダウンから、「チェックする」/「チェックしない」を選択します。

○出力時
プルダウンから、「チェックする」/「チェックしない」を選択します。

・IPsec policy のチェックを行わないように指定する機能です。特定の通信のみ IPsec 化しないような場合に、本機能を使用します。
・入力時「チェックしない」場合、inbound policy check を実行しないため、平文のパケットが、IPsec policy にマッチしても、当該パケットをドロップしません。
・出力時「チェックしない」場合、当該インタフェースから出力するパケットは、IPsec policy をチェックしないため、平文で送信します。

Ⅰ．IPsec

[トンネルの設定]



○送信元アドレス
基本設定を参照してください。

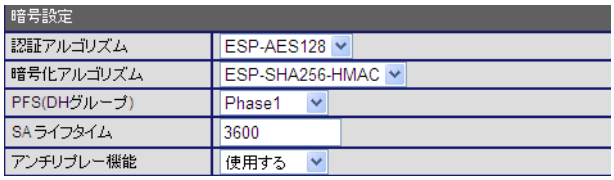
○宛先アドレス
基本設定を参照してください。

○接続方法
基本設定を参照してください。

○ NAT トラバーサル
基本設定を参照してください。

○プライオリティ
ポリシーのプライオリティ（1～255）を設定します。初期値は、「1」です。

[暗号設定]



○認証アルゴリズム
プルダウンから、認証アルゴリズムを選択します。
・初期値は、「ESP-AES128」です。

○暗号化アルゴリズム
プルダウンから、暗号化アルゴリズムを選択します。
・初期値は、「ESP-SHA256-HMAC」です。

○ PFS(DH グループ)
プルダウンから、PFS(DH グループ)を選択します。
・初期値は、「Phase1」です。

○ SA ライフタイム
IPsec SA のライフタイム（1081-86400[sec]）を設定します。
・初期値は、「3600」です。

○アンチリプレー機能
アンチリプレー機能の設定（「使用する」/「使用しない」）を、プルダウンから選択します。
・初期値は、「使用する」です。

１．IPsec

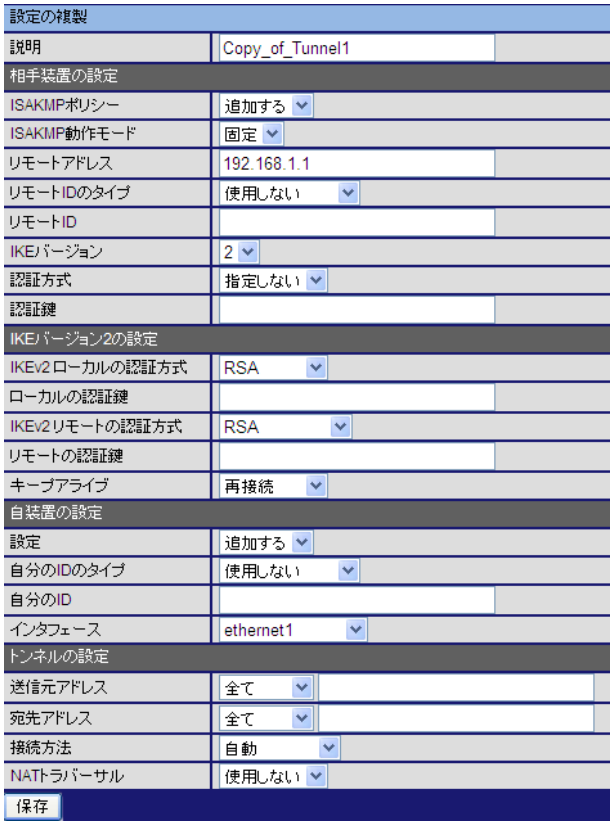
IPsec トンネルの削除

「削除」をクリックすると、トンネルを削除することが出来ます。

IPsec トンネルの複製

「設定の複製」をクリックすると、既存設定の複製を作成することが出来ます。

下記画面にて、項目の編集を行います。

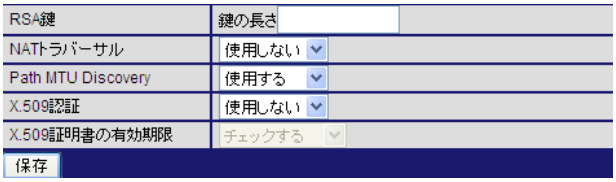


「保存」をクリックすると、設定の複製が作成されます。

2．IPsec 全体設定

GUI 画面のメニューを下記の順にクリックします。
VPN
　IPsec
　　・IPsec 全体設定

■ IPsec 全体設定



○ RSA 鍵
生成する RSA 鍵の長さ（512 ～ 1024）を指定します。

○ NAT トラバーサル
「使用する」/「使用しない」をプルダウンから選択します。

・NAT 装置の配下に、本装置が設置されている状況で、IPsec 接続を行う場合は、「使用する」を選択します。
・IKEv1 では、「使用する」/「使用しない」を選択することが出来ます。
・IKEv2 では、自動的に NAT トラバーサルが有効になります（無効にすることは、出来ません）。

○ Path MTU Discovery
「使用する」/「使用しない」をプルダウンから選択します。

・IPsec において、Path MTU Discovery を「使用しない」場合、DF ビットが「1」で、かつトンネル MTU を超えてしまう時でも、強制的にトンネリングして転送します。この場合、outer の IP ヘッダの DF ビットは、必ず「0」が設定されます。
・IPsec において、Path MTU Discovery を「使用する」場合、DF ビットが「1」で、かつトンネル MTU を超えてしまう時、fragment needed を送信元に返信し、パケットをドロップします。この場合、outer の IP ヘッダの DF ビットは、トンネリングパケットの値が設定されます。

○ X.509 認証
「使用する」/「使用しない」を、プルダウンから選択します。

・X.509 証明書を使用した認証を有効にする場合は、「使用する」を選択します。

○ X.509 証明書の有効期限
「チェックする」/「チェックしない」を、プルダウンから選択します。

・X.509 証明書の有効期間をチェックする機能です。
・「チェックする」場合、現在時刻が証明書の有効期間外であれば、当該証明書を使用することは出来ません。
・「チェックしない」場合、常に証明書の利用が可能となります。また、CRL による証明書の無効化も行いません。

設定を保存するには、「保存」をクリックします。

3．IPsec 認証設定

GUI 画面のメニューを下記の順にクリックします。

VPN

IPsec

・IPsec 認証設定

■証明書

CA 証明書の追加

「参照」をクリックして、CA 証明書を指定します。
「追加」をクリックします。

※ DER(*.der, *.cer)または PEM(*.pem)フォーマットの証明書をインポートすることができます。
・ファイルの拡張子は変更しないでください。なお、シングル DES で暗号化された鍵ファイルを使用することは出来ません。

CA 失効リストの追加

「参照」をクリックして、CA 失効リストを指定します。
「追加」をクリックします。

X.509 証明書の追加

X.509 証明書の「追加」をクリックすると、下記の画面が表示されます。

○証明書
「参照」をクリックして、証明書を指定します。

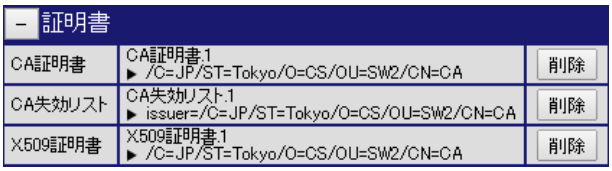
○プライベートキー
「参照」をクリックして、プライベートキーを指定します。

○パスワード
パスワードを入力します。

設定を保存するには、「保存」をクリックします。

Ⅰ．IPsec

CA 証明書の削除
「削除」をクリックします。

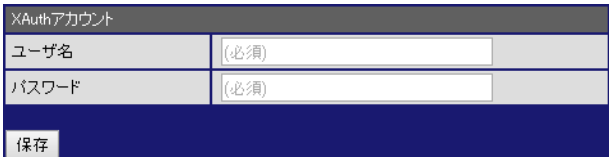


CA 失効リストの削除
「削除」をクリックします。

X.509 証明書の削除
「削除」をクリックします。

■ XAuth アカウント

XAuth アカウントの追加
XAuth アカウントの「追加」をクリックすると、
下記の画面が表示されます。



○ユーザ名
ユーザ名を入力します（必須）。

○パスワード
パスワードを入力します（必須）。

設定を保存するには、「保存」をクリックします。

XAuth アカウントの編集
「編集」をクリックします。

XAuth アカウントの削除
「削除」をクリックします。

第７章　VPN

１．IPsec

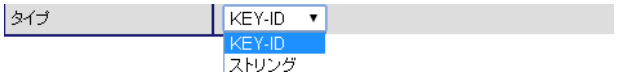
■ PSK アカウント

PSK アカウントの追加

PSK アカウントの「追加」をクリックすると、下記の画面が表示されます。

○タイプ

プルダウンから、タイプ（「FQDN」/「USER@FQDN」/「KEY-ID」）を選択します。



○ユーザ名

ユーザ名を入力します（必須）。

○パスワード

パスワードを入力します（必須）。

設定を保存するには、「保存」をクリックします。

PSK アカウントの編集

「編集」をクリックします。

PSK アカウントの削除

「削除」をクリックします。

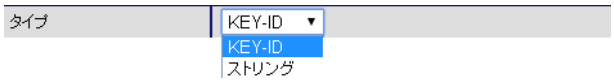
■ EAP アカウント

EAP アカウントの追加

EAP アカウントの「追加」をクリックすると、下記の画面が表示されます。

○タイプ

プルダウンから、タイプ（「KEY-ID」/「ストリング」）を選択します。



○ユーザ名

ユーザ名を入力します（必須）。

○パスワード

パスワードを入力します（必須）。

設定を保存するには、「保存」をクリックします。

EAP アカウントの編集

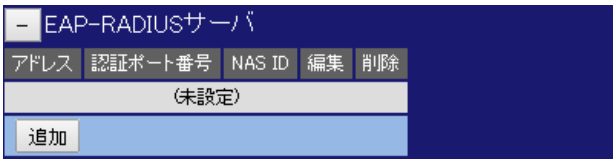
「編集」をクリックします。

EAP アカウントの削除

「削除」をクリックします。

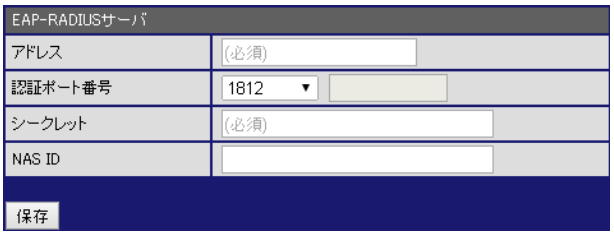
Ⅰ．IPsec

■ EAP-RADIUS サーバ



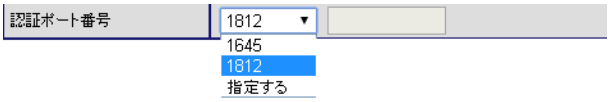
EAP-RADIUS サーバの追加

EAP-RADIUS サーバの「追加」をクリックすると、下記の画面が表示されます。



○アドレス
アカウント認証を行う RADIUS サーバのアドレス（A.B.C.D）を入力します（必須）。

○認証ポート番号
プルダウンから、認証ポート番号（「1645」/「1812」/「指定する」）を選択します。



「指定する」を選択した場合は、ポート番号（1024-65535）を指定します。

○シークレット
シークレット（秘密鍵）を入力します（必須）。

○ NAS ID
任意の文字(32文字以内)を指定することが可能です。
Default は、機種名 -IPsec(ex.NXR120-IPsec)です。

設定を保存するには、「保存」をクリックします。

EAP-RADIUS サーバの編集

「編集」をクリックします。

EAP-RADIUS サーバの削除

「削除」をクリックします。

Ⅱ．L2TPv3

1．L2TPv3 接続設定

GUI 画面のメニューを下記の順にクリックします。

VPN

L2TPv3

・L2TPv3 接続設定

■ L2TPv3 接続設定

L2TPv3 接続設定の追加

「追加」をクリックすると、下記の画面が表示されます。

○説明

当該 L2TPv3 トンネル接続設定の説明を記入します。

[トンネルの設定]

○リモート Router ID

リモート LCCE の Router ID（A.B.C.D）を入力します（必須）。

○リモートホスト名

リモート LCCE のホスト名を入力します（必須）。

○リモートアドレス

リモート LCCE のトンネルアドレス（A.B.C.D）を入力します。

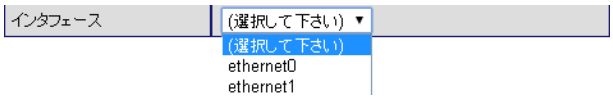
○ Hello インターバル

Hello パケットの送信間隔を設定します。

[Xconnect の設定]

○インタフェース

プルダウンから、Xconnect インタフェースを選択します。



○ Remote END ID

リモート LCCE の END ID(1-4294967295)を設定します（必須）。

○ VLAN ID

VLAN tag を使用する場合に、VLAN ID(1-4094)を設定します。

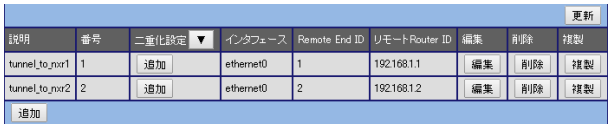
○リトライ間隔

トンネル / セッションが切断したときに、自動再接続を開始するまでの間隔（0-1000[秒]）を設定します。

「0」を設定した場合は、自動再接続を開始しません。

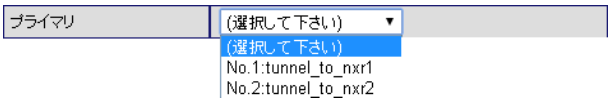
設定を保存するには、「保存」をクリックします。

L2TPv3接続設定の二重化設定

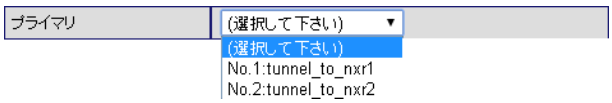


「追加」をクリックすると、以下の画面が表示されます。

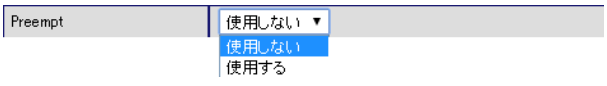
○プライマリ
プルダウンから、プライマリを選択します。



○セカンダリ
プルダウンから、セカンダリを選択します（プライマリとセカンダリは、異なるように選択します）。

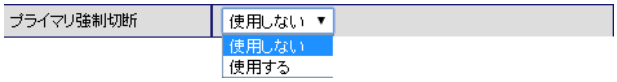


○ Preempt
プルダウンから、Preempt の設定（「使用する」/「使用しない」）を選択します。



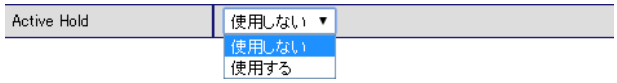
※セカンダリセッションが active の状態で、プライマリセッションが確立した時の動作を設定します。
・Preempt を「使用する」場合は、プライマリセッションが active、セカンダリセッションは standby になります。
・Preempt を「使用しない」場合は、セカンダリセッションが active のままです。

○プライマリ強制切断
プルダウンから、プライマリ強制切断の設定（「使用する」/「使用しない」）を選択します。



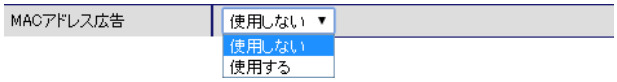
・「使用する」場合、プライマリセッションが active に移行した際に、セカンダリセッションを強制的に切断します。
・本機能を有効にする場合は、Preempt を「使用する」に設定します。

○ Active Hold
プルダウンから、Active Hold の設定（「使用する」/「使用しない」）を選択します。



・対向の LCCE からリンクダウンを受信した際に、セカンダリセッションへの切り替えを行わずに、プライマリセッションを active のまま維持する機能です。
・1 対 1 の二重化構成において、対向 LCCE でリンクダウンが発生した際に、プライマリからセカンダリへ active セッションを切り替えたとしても、通信できない状態は変わりません。このような構成では、不要なセッションの切り替えを抑止するために、本機能を「使用する」に設定することを推奨します。

○ MAC アドレス広告
プルダウンから、MAC アドレス広告の設定（「使用する」/「使用しない」）を選択します。



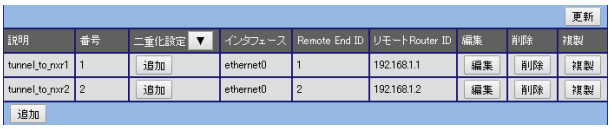
・グループ機能を使用している構成で、センター側の配下にあるスイッチの MAC テーブルを更新するために、ローカルテーブルに登録されている MAC アドレス情報を元に、疑似フレームを送信することによって、センターにある端末を発信源とする通信が可能となります。

設定を保存するには、「保存」をクリックします。

II．L2TPv3

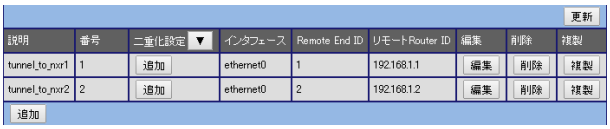
L2TPv3 接続設定二重化設定の編集

「編集」をクリックします。



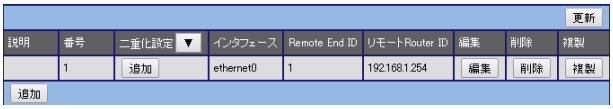
L2TPv3 接続設定二重化設定の削除

「削除」をクリックします。



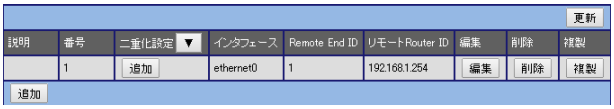
L2TPv3 接続設定の編集

「編集」をクリックします。

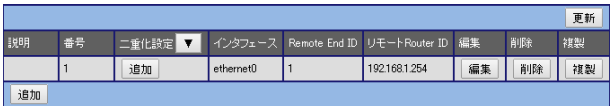


L2TPv3 接続設定の削除

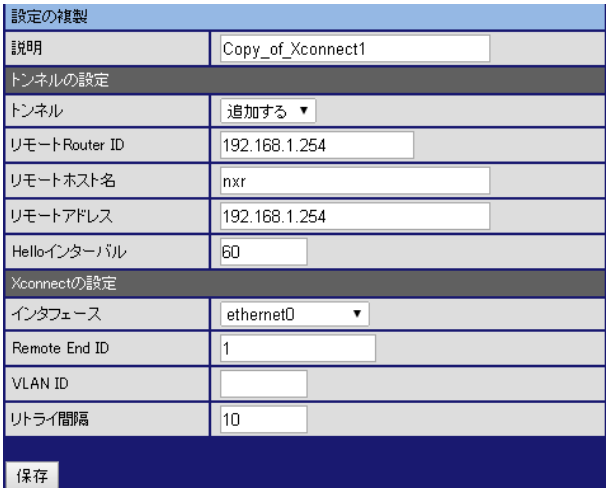
「削除」をクリックします。



L2TPv3 接続設定の複製



「複製」をクリックすると、以下の画面が表示されます。

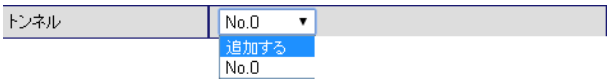


[トンネルの設定]

○トンネル

トンネルを追加する場合は、「追加する」を選択します。

トンネルを共有する場合は、既存のトンネルを選択します。



その他の項目については、**L2TPv3 接続設定の追加**を参照してください。

2．L2TPv3 全体設定

GUI 画面のメニューを下記の順にクリックします。

VPN
　L2TPv3
　　・L2TPv3 全体設定

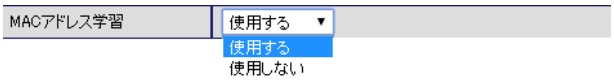
■ L2TPv3 全体設定

○ローカル Router ID
ローカル LCCE の Router ID（A.B.C.D）を入力します。

○ローカルホスト名
ローカル LCCE のホスト名を設定します。

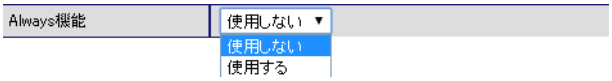
[MAC アドレス学習]

○ MAC アドレス学習
プルダウンから、MAC アドレス学習の設定（「使用する」/「使用しない」）を選択します。



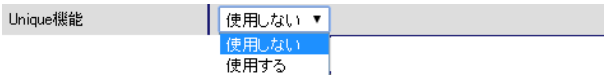
・本装置が受信したフレームの MAC アドレスを学習し、不要なトラフィックの転送を抑制する機能です。
・ブロードキャスト、マルチキャストについては、本設定に関係なく、すべて転送します。

○ Always 機能
プルダウンから、Always 機能の設定（「使用する」/「使用しない」）を選択します。



・MAC アドレス広告を「使用する」にした場合、アクティブセッションが作成されたときに、MAC アドレス広告を行いますが、Xconnect に関連するセッションが1 つも確立されていない場合は、ローカルテーブルにて MAC アドレスが学習されない為、ローカルテーブルに MAC アドレス情報が存在しません。
・Always 機能を「使用する」に設定すると、セッションが 1 つも確立されていない場合でも、ローカルテーブルに MAC アドレス学習を行います。

○ Unique 機能
プルダウンから、Unique 機能の設定（「使用する」/「使用しない」）を選択します。



・ネットワーク構成によっては、ある一つの Xconnect の Local Table、FDB に、同じ MAC アドレスが登録されることがあります。本機能を有効にすると、新しく学習した MAC アドレスが、ocal Table、FDB のどちらか一方に登録されるため、上記のような状態を回避することが出来ます。
・ある一つの Xconnect で、Loop Detect 機能と共存した場合、Loop Detect のフレームドロップ処理を優先します。つまり、この場合は、MAC アドレス学習 Unique 機能は、動作しないことになります。

○ MAC アドレスエージングタイム
本装置が学習した MAC アドレスの保持時間(30-1000[秒])を設定します。
・初期値は、300[秒]です。

II．L2TPv3

[L2TPv3 over UDP]

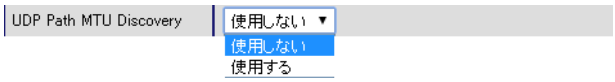
○ UDP 送信元ポート番号

L2TPv3 over UDP 使用時の送信元ポート番号（1024-65535）を指定することができます。

・初期値は、1701 です。

○ UDP Path MTU Discovery

プルダウンから、UDP Path MTU Discovery の設定（「使用する」/「使用しない」）を選択します。



L2TPv3 over UDP 使用時に、Path MTU Discovery の設定（「使用する」/「使用しない」）を行います。

・本機能を有効にした場合、送信する L2TPv3 パケットの DF(Don't Fragment)ビットを 1 にします。

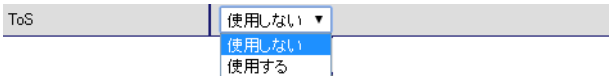
・無効にした場合は、DF ビットを常に 0 にします。

・ただし、カプセル化したフレーム長が送信インタフェースの MTU 値を超過する場合は、本設定に関係なく、フラグメントの上、DF ビットを 0 にして送信します。

[L2TPv3 over UDP]

○ ToS

プルダウンから、ToS 設定（「使用する」/「使用しない」）を選択します。



・L2TPv3 にてトンネリングされるフレームの L3 プロトコルが IP/IPv6 の場合に、IP/IPv6 ヘッダの ToS 値やユーザが指定した ToS 値を、L2TPv3 セッションパケットの IP ヘッダの IPv4 ToS field に設定する機能です。

・Control message は、0xd0 で送信します。

○トンネル ToS 値

L2TPv3 ToS 設定を「使用する」場合に、

・Control message の ToS 値（0-252[0x00-0xfc]）を指定することが出来ます。

・初期値は、208（0xd0）です。

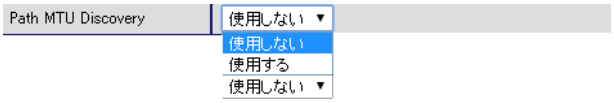
L2TPv3 ToS 設定を「使用しない」場合、

・Control message の ToS 値は、固定（0xd0）です。

[その他機能]

◯ Path MTU Discovery

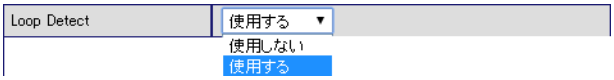
プルダウンから、Path MTU Discovery の設定（「使用する」/「使用しない」）を選択します。



・L2TPv3 over IP 使用時に、Path MTU Discovery の設定（「使用する」/「使用しない」）を行います。

◯ Loop Detect

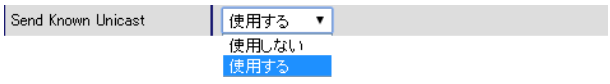
プルダウンから、Loop Detect の設定（「使用する」/「使用しない」）を選択します。



・フレームの転送がループしてしまうことを防ぐ機能です。この機能が有効になっているときは、以下の 2 つの場合にフレームの転送を行いません。
  ・Xconnect インタフェースより受信したフレームの送信元 MAC アドレスが、FDB に存在するとき。
  ・L2TPv3 セッションより受信したフレームの送信元 MAC アドレスが、ローカル MAC テーブルに存在するとき。

◯ Send Known Unicast

プルダウンから、Send Known Unicast の設定（「使用する」/「使用しない」）を選択します。



・Known unicast フレームとは、MAC アドレス学習済みの unicast フレームのことです。この機能を「使用しない」に設定すると、以下の場合に unicast フレームの転送を行いません。
  ・Xconnect インタフェースより受信した unicast フレームの送信先 MAC アドレスが Local MAC テーブルに存在する場合。

設定を保存するには、「保存」をクリックします。

第8章

ファイアウォール

第 8 章　ファイアウォール

アクセスリスト

1. IPv4 アクセスリスト

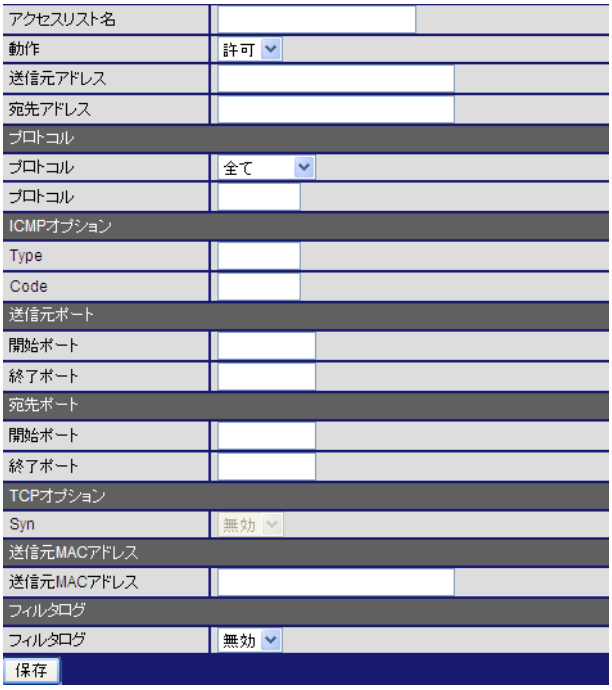
IPv4 アクセスリストの設定をおこないます。

GUI 画面のメニューを下記の順にクリックします。
ファイアウォール
　アクセスリスト
　　・IPv4 アクセスリスト

■ IPv4 アクセスリスト

IPv4 アクセスリストの追加

「追加」をクリックします。



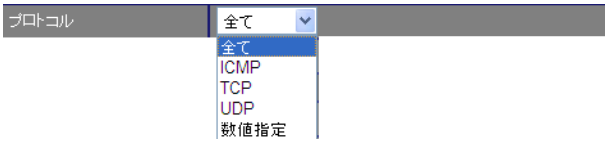
○アクセスリスト名
アクセスリスト名を指定します。

○動作
アクセスリストにマッチングするパケットの「許可」/「破棄」をプルダウンから選択します。

○送信元アドレス
送信元 IP アドレスを入力します。ホストアドレスのほか、ネットワークアドレスでの指定が可能です。
[入力例]
ホストアドレス　　192.168.253.10
ネットワークアドレス　192.168.253.0/24
any の場合は、空欄のままにします。

○宛先アドレス
宛先 IP アドレスを入力します。ホストアドレスのほか、ネットワークアドレスでの指定が可能です。
入力方法は、「送信元アドレス」と同様です。

[プロトコル]
○プロトコル
プロトコルをプルダウンから選択します。



○プロトコル
上記で「数値指定」を選択した場合に、プロトコル番号 <0-255> を入力します。

[ICMP オプション]
○ ICMP Type
0-255 の範囲で ICMP Type を指定します。
「プロトコル」で「ICMP」を選択した場合に、入力可能です。

○ ICMP Code
0-255 の範囲で ICMP Code を指定します。
「プロトコル」で「ICMP」を選択した場合に、入力可能です。

[送信元ポート]
○開始ポート / 終了ポート
1-65535 の範囲で指定します。
「プロトコル」で「TCP」/「UDP」を選択した場合に、入力可能です。

[宛先ポート]
○開始ポート / 終了ポート
1-65535 の範囲で指定します。
「プロトコル」で「TCP」/「UDP」を選択した場合に、入力可能です。

[TCP オプション]
○ TCP Syn
Syn フラグをチェックする場合は「SYN」を選択してください。
「プロトコル」で「TCP」を選択した場合に、選択可能です。

[送信元 MAC アドレス]
○送信元 MAC アドレス
送信元 MAC アドレスをチェックする場合は、対象 MAC アドレスを HH:HH:HH:HH:HH:HH のフォーマットで入力します。

[フィルタログ]
○フィルタログ
プルダウンから、「無効」/「取得」を選択します。

- 「取得」を選択すると、パケットが、当該アクセスリストにマッチした場合、システムログに出力します。
- 1 秒間に出力可能なログ数の最大値は、「10」です。
- すべてのアクセスリストにログを設定すると、システムが高負荷状態になる可能性があるため、ログ出力は、最小限にとどめるようにしてください。

設定を保存するには、「保存」をクリックします。

IPv4 アクセスリストの編集
「編集」をクリックします。

アクセスリスト名	動作	送信元アドレス / 宛先アドレス	プロトコル	ICMP Type	ICMP Code	送信元ポート / 宛先ポート	TCP Syn	送信元MACアドレス	編集 / 削除
test1 削除	許可	192.168.0.0/24 / 192.168.100.0/24	tcp			1025-65535		00:11:22:33:44:55	編集 / 削除

IPv4 アクセスリストの削除
「削除」をクリックします。

アクセスリスト名	動作	送信元アドレス / 宛先アドレス	プロトコル	ICMP Type	ICMP Code	送信元ポート / 宛先ポート	TCP Syn	送信元MACアドレス	編集 / 削除
test1 削除	許可	192.168.0.0/24 / 192.168.100.0/24	tcp			1025-65535		00:11:22:33:44:55	編集 / 削除

第9章

ユーザインタフェース

第9章　ユーザインタフェース

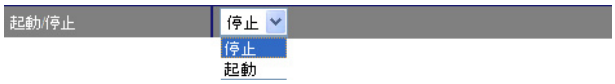
Ⅰ．SSH

1．SSHサービス

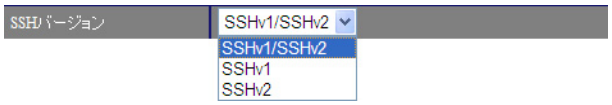
GUI画面のメニューを下記の順にクリックします。
ユーザインタフェース
　SSH
　　・SSHサービス

■ SSHサービス

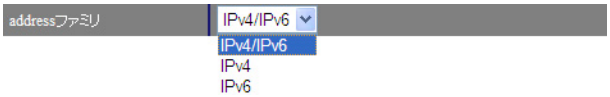
○ 起動 / 停止
「起動」/「停止」をプルダウンから選択します。



○ SSHバージョン
「SSHv1/SSHv2」/「SSHv1」/「SSHv2」をプルダウンから選択します。



○ アドレスファミリ
「IPv4/IPv6」/「IPv4」/「IPv6」をプルダウンから選択します。



[ポート番号]
○ ポート番号
SSHサーバのポート番号を指定します。デフォルト値は22です。

○ ポート番号
SSHサーバのセカンダリポート番号を指定します。

2．SSH鍵(netconf)

GUI画面のメニューを下記の順にクリックします。
ユーザインタフェース
　SSH
　　・SSH鍵(netconf)

■ SSH鍵（netconf）

SSH鍵の追加
「参照」をクリックして、ファイル(SSH公開鍵)を指定します。「保存」をクリックすると、SSH鍵が設定されます。

SSH鍵の削除
「削除」をクリックします。

第9章　ユーザインタフェース

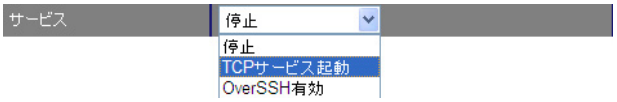
II．NETCONF

1．NETCONF

GUI画面のメニューを下記の順にクリックします。
ユーザインタフェース
　NETCONF
　　・NETCONF

■ NETCONF

○ サービス
NETCONFサービスの「起動」/「停止」を設定します。
プルダウンから「停止」/「TCPサービス起動」/「OverSSH有効」を選択します。



○ ロックタイムアウト
NETCONFによる設定変更時にlockが行われます。lock状態では、他の管理サーバまたはCLI/GUIからの設定変更は出来ません。また、CLI/GUIあるいは他の管理サーバから設定変更が行われている状態では、lockを行うことは出来ません。
lock状態が解除されるまでの時間を10-3600[秒]の間で設定します。デフォルト値は60[秒]です。

○ オートコンフィグレーション
オートコンフィグレーションの「有効」/「無効」を設定します。
プルダウンから「使用しない」/「使用する」を選択します。

設定を保存するには、「保存」をクリックします。

III．CRP

1．CRP グローバル

GUI 画面のメニューを下記の順にクリックします。
ユーザインタフェース
　CRP
　　・CRP グローバル

■ CRP グローバル

○ 送信元ポート
CRP の送信元 UDP ポートを 1024-65535 の間で設定します。デフォルト値は、10625 です。

○ ホスト名
広告するホスト名を指定します。設定がない場合、
システム設定
　　・ホスト名
で指定されたホスト名を広告します。

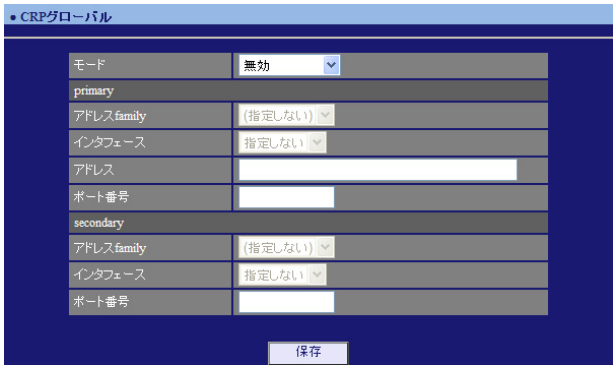
○ カスタマー ID
カスタマー ID を指定します。管理サーバ側のテナントコードと一致させてください。

○ CPE ID
CPE ID を指定します。管理サーバ側の機器コードと一致させてください。

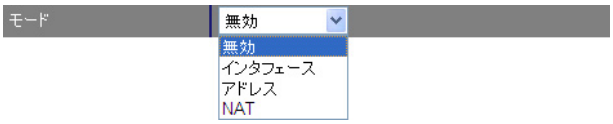
設定を保存するには、「保存」をクリックします。

● CRP Advertise

「編集」をクリックします。



○ モード
プルダウンから「無効」/「インタフェース」/「アドレス」/「NAT」を選択します。

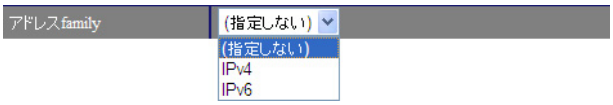


[primary]

○ アドレス family

「モード」で「インタフェース」を選択した場合に設定することができます。

プルダウンから、「IPv4」/「IPv6」を選択します。



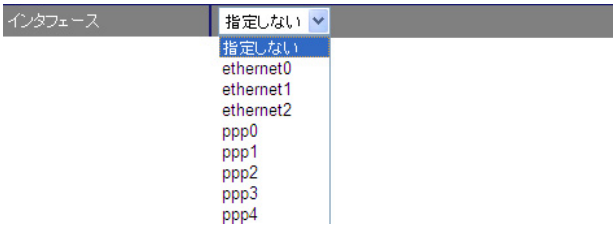
○ インタフェース

「モード」で「インタフェース」を選択した場合に設定することができます。プルダウンから、インタフェースを選択します。

選択可能なインタフェースは、下記のとおりです。

「ethernet0」/「ethernet1」/「ethernet2」

「ppp0」/「ppp1」/「ppp2」/「ppp3」



○ アドレス

「モード」で「アドレス」を選択した場合に入力することができます。

広告する本装置の IPv4 アドレス、または IPv6 アドレスを指定します。

○ ポート番号

「モード」で「インタフェース」、「アドレス」または「NAT」を選択した場合に入力することができます。

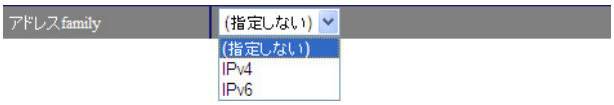
広告するポート番号を指定します。通常は 22 を指定してください。

[secondary]

「モード」で「インタフェース」を選択した場合に設定することができます。

○ アドレス family

プルダウンから、「IPv4」/「IPv6」を選択します。



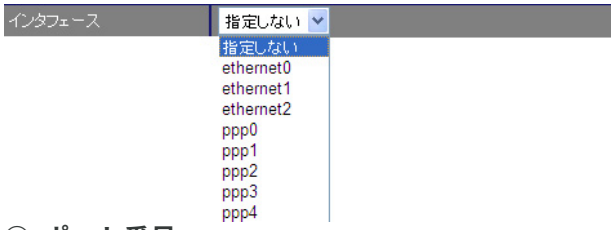
○ インタフェース

プルダウンから、インタフェースを選択します。

選択可能なインタフェースは、下記のとおりです。

「ethernet0」/「ethernet1」/「ethernet2」

「ppp0」/「ppp1」/「ppp2」/「ppp3」



○ ポート番号

広告するポート番号を指定します。通常は 22 を指定してください。

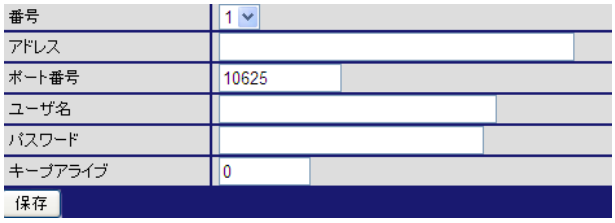
設定を保存するには、「保存」をクリックします。

2．CRP クライアント

GUI 画面のメニューを下記の順にクリックします。
ユーザインタフェース
　CRP
　　・CRP クライアント

■ CRP クライアント

「追加」をクリックします。



○ 番号
クライアントの設定番号を、プルダウンから選択します。1 または 2 を指定してください。

○ アドレス
管理サーバのアドレスを設定します。「IPv4」/「IPv6」/「FQDN」形式で入力してください。

○ ポート番号
ポート番号を設定します。1024-65535 の数値を入力してください。デフォルト値は、10625 です。

○ ユーザ名
CRP のリクエストメッセージに使用するユーザ ID を使用します。

○ パスワード
認証に使用するパスワードを設定します。

○ キープアライブ
CRP 登録に成功してから、次に CRP 登録を試行するまでの時間を指定します。デフォルト値は 0 で、CRP 登録の再試行はしません。

第 10 章

システム設定

1．システム設定

1．本装置のパスワード

本装置の設定画面にログインする際のユーザ名、パスワードを変更します。
ルータ自身のセキュリティのために、定期的なパスワード変更を推奨します。

GUI 画面のメニューを下記の順にクリックします。
システム設定
　システム設定
　　・本装置のパスワード

■本装置のパスワード

○旧パスワード
現在のパスワードを入力します。

○新パスワード
半角英数字 / 記号（5 ～ 95 文字）で、設定します。
大文字・小文字も判別しますのでご注意ください。

○新パスワード（確認用）
確認のため再度「新パスワード」を入力してください。

設定を保存するには、「保存」をクリックします。

本装置の操作を続行すると、ログイン用のダイアログ画面がポップしますので、新パスワードで再度ログインしてください。

2．ホスト名

本装置のホスト名を設定します。

GUI 画面のメニューを下記の順にクリックします。
システム設定
　システム設定
　　・ホスト名

■ホスト名

設定を保存するには、「保存」をクリックします。

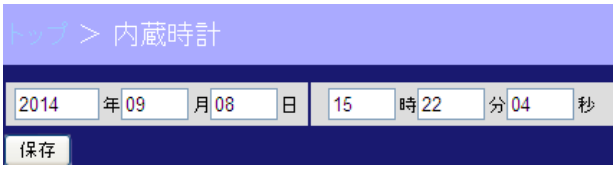
Ⅰ．システム設定

3．内蔵時計

本装置の内蔵時計を設定します。

GUI 画面のメニューを下記の順にクリックします。
システム設定
　システム設定
　　・内蔵時計

■内蔵時計



○内蔵時計
現在時刻を設定します。

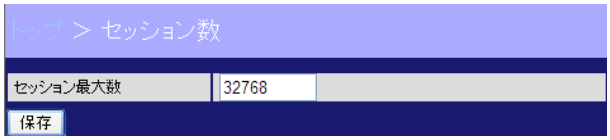
「保存」をクリックすると、時刻が設定されます。

4．セッション数

本装置のセッション最大数を設定します。

GUI 画面のメニューを下記の順にクリックします。
システム設定
　システム設定
　　・セッション数

■セッション数



○セッション数
本装置のセッション最大数（4096 ～ 65536）を指定します。
・初期値は、「32768」です。

設定を保存するには、「保存」をクリックします。

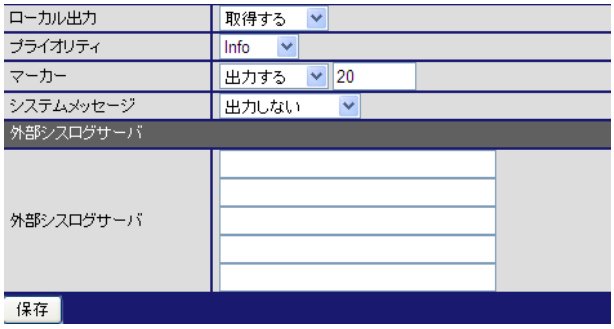
Ⅱ．ログ

1．システムログ

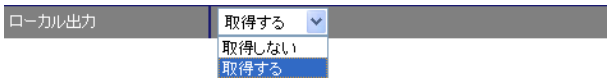
システムログの設定をおこないます。

GUI 画面のメニューを下記の順にクリックします。
システム設定
　ログ
　　・システムログ

■システムログ

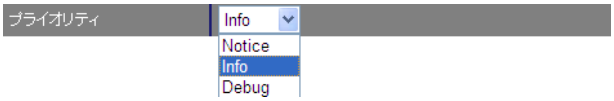


○ローカル出力
「取得する」「取得しない」をプルダウンから選択します。

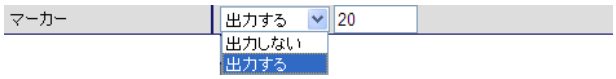


装置本体に記録しておけるログの容量には制限があります。
継続的にログを取得される場合は、外部のシスログサーバにログを送出するようにしてください。

○プライオリティ
ログ内容の出力レベルをプルダウンから選択します。
プライオリティの内容は以下のようになります。
　・Debug ：デバッグ時に有益な情報
　・Info　：システムからの情報
　・Notice：システムからの通知

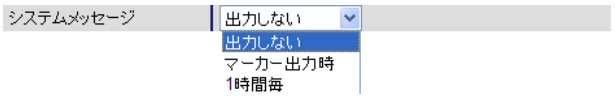


○マーカー
プルダウンから、マーカーの設定（「出力しない」/「出力する」）を選択します。



「出力する」を選択した場合、システムログが動作していることを表す「-- MARK --」ログを送出する間隔（0～99[分]）を指定します。
初期値は「20」です。

○システムメッセージ
本装置のシステム情報を定期的に出力することができます。
「出力しない」/「 マーカー出力時」/「1 時間毎」をプルダウンから選択します。



[外部シスログサーバ]
○外部シスログサーバ
シスログサーバの IP アドレス（A.B.C.D）を指定します。

設定を保存するには、「保存」をクリックします。

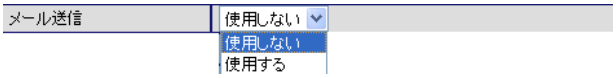
2．ログメール

ログの内容を電子メールで送信したい場合の設定です。

GUI 画面のメニューを下記の順にクリックします。
システム設定
　ログ
　　・ログメール

■ログメール

○メール送信
「使用する」/「使用しない」をプルダウンから選択します。



○宛先メールアドレス
ログメッセージの送信先メールアドレスを指定します。最大文字数は 64 文字です。

○送信元メールアドレス
送信元のメールアドレスは任意で指定できます。最大文字数は 64 文字です。

○件名
任意で指定できます。使用可能な文字は半角英数字で、最大 64 文字です。

○検出文字列
ここで指定した文字列が含まれるログをメールで送信します。文字列を指定しない場合はログメールは送信されません。

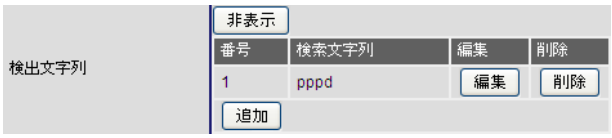
検索文字列の設定
検出文字列を設定するには、「追加」をクリックします。

○番号
1-32 の間で指定します。

○検索文字列
検出文字列には、pppd、IP、DNS などログ表示に使用される文字列を指定してください。なお、文字列の記述に正規表現は使用できません。
文字列は、半角英数字で 128 文字まで指定できます。空白・大小文字も判別します。
複数の文字(文字列)を指定すると、その文字(文字列)に完全一致したログのみ抽出して送信します。

設定を保存するには、「保存」をクリックします。

検索文字列の編集
「編集」をクリックします。



検索文字列の削除
「削除」をクリックします。

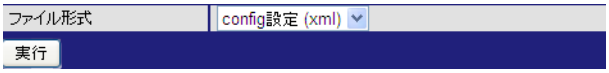
III．設定情報

1．設定の保存

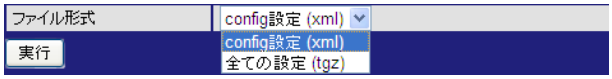
設定の保存をおこないます。

GUI 画面のメニューを下記の順にクリックします。
システム設定
　設定情報
　　・設定の保存

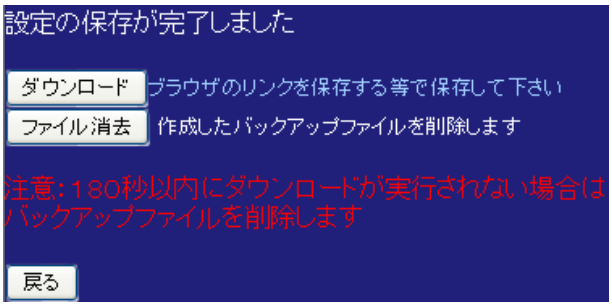
■設定の保存



○ファイル形式
プルダウンから「config 設定(xml)」/「全ての設定（tgz)」を選択します。



「実行」をクリックします。



○ダウンロード
ブラウザのリンクを保存する等で、設定ファイルを保存することが出来ます。

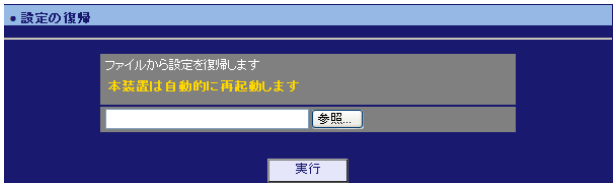
○ファイル消去
「ファイル消去」をクリックすると、作成したバックアップファイルを削除します。

2．設定の復帰

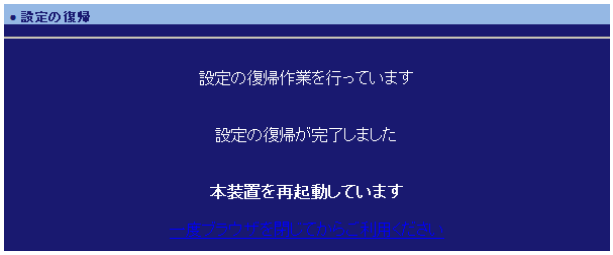
設定の復帰をおこないます。

GUI 画面のメニューを下記の順にクリックします。
システム設定
　設定情報
　　・設定の復帰

■設定の復帰



「参照」をクリックして、ファイルを指定します。
「実行」をクリックすると、設定の復帰作業がおこなわれます。



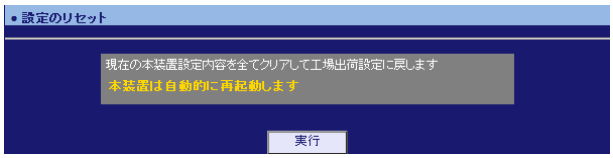
設定の復帰が完了すると、本装置が自動的に再起動します。

3．設定のリセット

設定をリセットします。

GUI 画面のメニューを下記の順にクリックします。
システム設定
　設定情報
　　・設定のリセット

■設定のリセット



「実行」をクリックすると、現在の本装置設定内容を全てクリアして工場出荷設定に戻します。本装置は自動的に再起動します。

本装置の工場出荷設定状態時では、HTTP サーバが起動していないため、GUI アクセスは出来ません。HTTP サーバの起動方法については、「第 4 章　設定画面へのログイン」を参照してください。

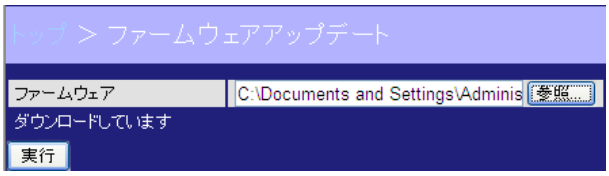
Ⅳ．ファームウェア

1．ファームウェアアップデート

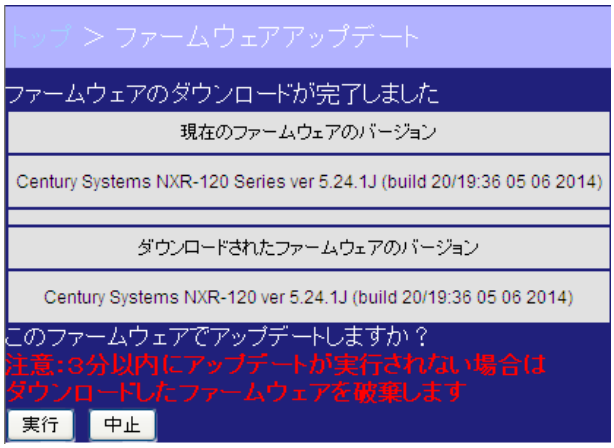
ファームウェアをアップデートします。

GUI 画面のメニューを下記の順にクリックします。
システム設定
　ファームウェア
　　・ファームウェアアップデート

■アップデート

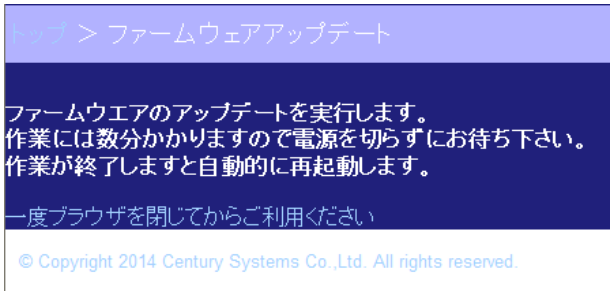


「参照」をクリックして、ファームウェアを指定します。「実行」をクリックすると、ファームウェアのアップデート画面が表示されます。



「実行」をクリックすると、ファームウェアのアップデートを開始します。すべてのサービスおよびパケット処理を停止します。

アップデートを開始すると、下記の画面が表示されます。



ファームウェアのアップデートが終了すると、本装置が自動的に再起動します。

ファームウェアアップデートの詳細については、ユーザーズガイド CLI 編を参照してください。

Ⅴ．スケジュール

◆スケジュール

設定された日付 / 曜日 / 時刻に、PPP の接続 / 切断 / 再接続などの指定された処理を実行する機能です。

GUI 画面のメニューを下記の順にクリックします。
システム設定
　・スケジュール

■スケジュール

「追加」をクリックします。

○日付
プルダウンから、日付（「日にち」/「毎日」/「毎週」）を選択します。

・「日にち」を選択した場合、「月」と「日」を指定します。
　・月　「毎月」/「1」～「12」
　・日　「毎日」/「1」～「31」

・「毎週」を選択した場合、開始曜日（と終了曜日）を指定します。
　・開始曜日　「日曜日」～「土曜日」
　・終了曜日　「日曜日」～「土曜日」
　・毎週日曜日の場合は、開始曜日に「日曜日」を指定します。

○時刻
プルダウンから、時刻を選択します。
・「毎時」/「0」～「23」時
・「0」～「59」分

○動作
指定時刻に実行する動作を、プルダウンから選択します。

・「システム再起動」を選択すると、指定時刻に、システムを再起動します。

・「スリープ」を選択すると、指定時刻に、スリープ状態へと移行します。

・「システム再開」を選択すると、指定時刻に、システムを再開（スリープ状態から復帰）します。

・「モバイルリセット」を選択すると、指定時刻に、モバイル端末のリセットを行います。
リセット対象となるモバイル番号（「mobile0」/「mobile1」）を指定します。
スケジュールによるモバイルリセットは、数時間以上の間隔を空けることを推奨します。

・「接続」/「再接続」/「切断」を選択した場合、指定時刻に、PPP の接続 / 切断 / 再接続を行います。
接続 / 切断 / 再接続を行う PPP インタフェース（「ppp0」/「ppp1」/「ppp2」/「ppp3」/「ppp4」）を指定します。
本機能によって、切断された場合、手動で切断されたものとみなし、常時接続が設定されていても、再接続は行いません。再接続する場合は、ユーザによる指示、またはスケジュールによる接続の設定が必要になります。

・「NTP 時刻修正」を選択すると、指定時刻に、NTP による時刻同期を行います。

・「ログローテート」を選択すると、指定時刻に、シスログのローテートを実行します。

Ⅴ．スケジュール

○システム再開
プルダウンから、システム再開（「指定しない」/「スケジュール」/「タイマー」）を選択します。

・動作が「スリープ」の場合に、システムの再開方法（スリープ状態からの復帰方法）を指定することが出来ます。

○スケジュール
システム再開で「スケジュール」を選択した場合に、プルダウンから、スケジュール番号を選択します。

・システム再開スケジュールは、あらかじめ設定しておきます。
・システム再開スケジュールを同時に追加するには、「(追加する)」を選択して、後述の日付と時刻を合わせて設定します。

○タイマー
システム再開が「タイマー」の場合に、システム再開までの時間（1～31,536,000[秒]）を指定します。
・「秒」/「分」/「時間」/「日」を選択して、設定します。

○日付（システム再開スケジュール）
スケジュールに「追加する」を選択した場合に、日付（システム再開スケジュール）を指定します。

○時刻（システム再開スケジュール）
スケジュールに「追加する」を選択した場合に、時刻（システム再開スケジュール）を指定します。

設定を保存するには、「保存」をクリックします。

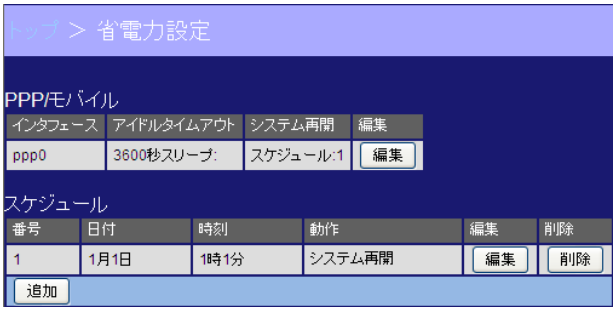
Ⅵ．省電力設定

◆省電力設定

システムをスリープ状態に移行させる機能です。
sleep 状態になると、CPU/Ethernet などへの電源供給を停止します。
工場やオフィス等の利用者がいない時間帯（休日や営業時間外）に、スリープモードを使用することで、大幅に消費電力を抑えることが可能になります。

GUI 画面のメニューを下記の順にクリックします。
システム設定
　　・省電力設定

■省電力設定



○ PPP/ モバイル
設定済 PPP インタフェースの一覧が表示されます。

「編集」を押下すると、指定した PPP インタフェースの設定画面に遷移します。

○スケジュール
設定済スケジュールの内、動作が「スリープ」/「システム再開」の一覧が表示されます。

「編集」を押下すると、指定したスケジュールの設定画面に遷移します。

「削除」を押下すると、指定したスケジュールを削除します。

「追加」を押下すると、スケジュール設定の追加画面に遷移します。

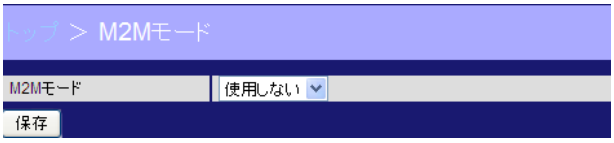
Ⅶ．M2M モード

◆M2M モード（※ NXR-G100/KL のみ）

M2M モードを設定します。

GUI 画面のメニューを下記の順にクリックします。
システム設定
　　・M2M モード

■M2M モード



○M2M モード
プルダウンから、「使用する」/「使用しない」を選択します。

・「使用する」を選択すると、消費電力を抑えるために、CPU の動作クロックを低く抑えると共に、Ethernet のリンクスピードを最大 100Mbps に抑えます。発熱量を抑えることによって、通常よりも過酷な利用環境下でも、安定した動作を提供することが可能になります。なお、M2M モードの場合、温度プロテクション機能は動作しません。

※温度プロテクション機能とは、温度状態が Warning/Critical の閾値を超えた際に、機器を守るために CPU の動作クロックを下げる機能です。CPU の動作クロックを下げることで、発熱量が低減するため、周辺温度の降下が期待出来ます。

「保存」をクリックすると、指定した値が保存されます。

第11章

運用機能

Ⅰ．ネットワーク診断

1. Ping

指定した宛先に対して、本装置から Ping を実行します。

GUI 画面のメニューを下記の順にクリックします。
運用機能
　ネットワーク診断
　　・Ping

■ Ping

○送信先
FQDN(www.xxx.co.jp などのドメイン名)、もしくは IP アドレスを入力します。

○送信回数
送信する ping パケット数を指定します。
1-10 の範囲で指定します。デフォルト値は 10 です。

「送信先」および「送信回数」を指定して、「実行」をクリックします。

2. Traceroute

指定した宛先までに経由するルータ情報を表示します。

GUI 画面のメニューを下記の順にクリックします。
運用機能
　ネットワーク診断
　　・Traceroute

■ Traceroute

○送信先
FQDN(www.xxx.co.jp などのドメイン名)、もしくは IP アドレスを入力します。

「送信先」を入力して、「実行」をクリックします。

Ⅱ．パケットダンプ

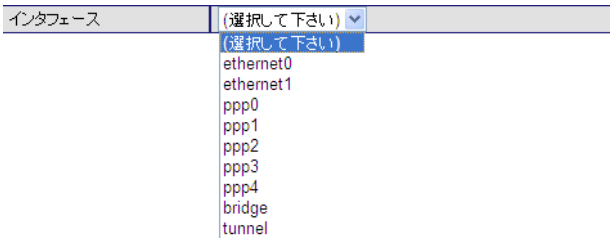
1．パケットダンプ

パケットのダンプを取得します。

GUI 画面のメニューを下記の順にクリックします。
運用機能
　パケットダンプ
　　・パケットダンプ

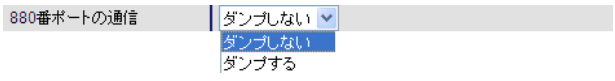
■実行

○インタフェース
ダンプを取得するインタフェースをプルダウンから選択します。



○パケット数
キャプチャするパケット数を、1-1000 の範囲で指定します。デフォルト値は 10 です。

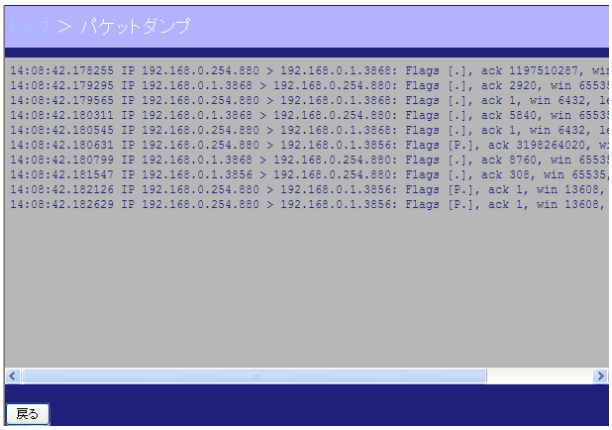
○ 880 番ポートの通信
「ダンプする」/「ダンプしない」をプルダウンから選択します。



○出力先
出力先をプルダウンから選択します。

「実行」をクリックします。

「出力先」として「画面」を選択した場合は、実行結果が画面に表示されます。



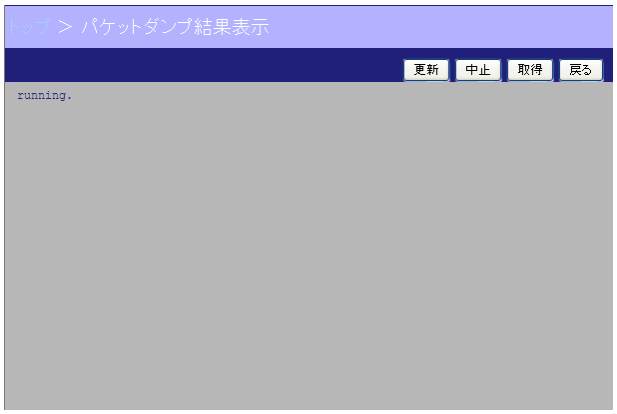
2．パケットダンプ結果表示

「出力先」として「ファイル」を選択した場合は、「結果表示」からファイルを取得します。

GUI 画面のメニューを下記の順にクリックします。
運用機能
　パケットダンプ
　　・パケットダンプ結果表示

■結果表示

[パケットダンプ取得中の表示例]

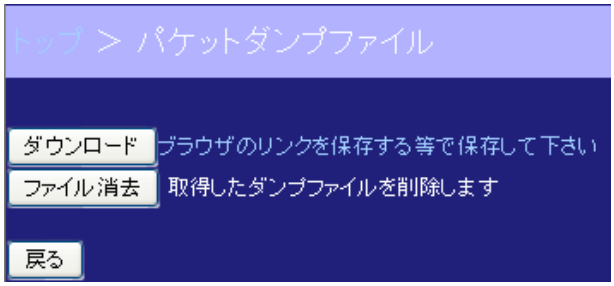


現在の状態を表示するには「更新」をクリックします。

パケットダンプを中止するには「中止」をクリックします。

[パケットダンプ取得終了の表示例]

ファイルを取得するには「取得」をクリックします。



○ダウンロード
ブラウザのリンクを保存する等で、ダンプファイルを保存することが出来ます。

○ファイル消去
「ファイル消去」をクリックすると、取得したダンプファイルを削除します。

III．ログ情報

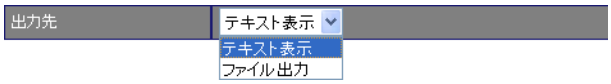
1．システムログ

システムログを表示します。

GUI 画面のメニューを下記の順にクリックします。
運用機能
　ログ情報
　　・システムログ

■システムログ

○出力先
システムログの出力先をプルダウンから選択します。



「実行」をクリックします。

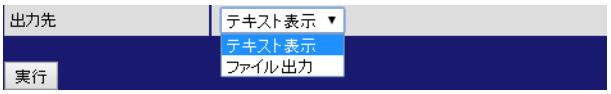
2．ブートログ

ブートログを表示します。

GUI 画面のメニューを下記の順にクリックします。
運用機能
　ログ情報
　　・ブートログ

■ブートログ

○出力先
ブートログの出力先をプルダウンから選択します。



「実行」をクリックします。

Ⅳ．システム情報

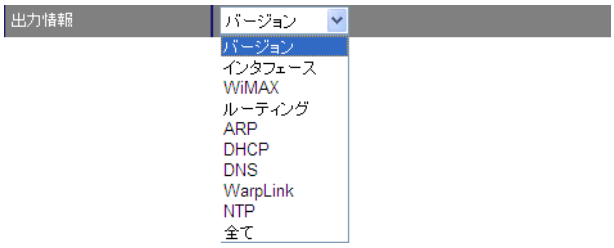
1．システム情報

システム情報を表示します。

GUI 画面のメニューを下記の順にクリックします。
運用機能
　システム情報
　　・システム情報

■システム情報

○出力情報
出力情報をプルダウンから選択します。



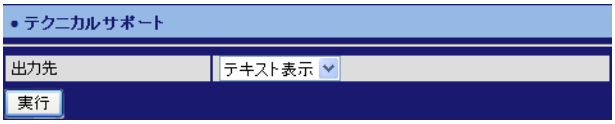
「実行」をクリックすると、選択した情報が表示されます。

2．テクニカルサポート

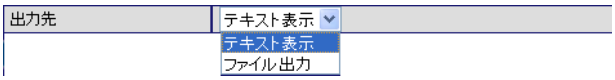
テクニカルサポート情報の表示、または取得を行います。

GUI 画面のメニューを下記の順にクリックします。
運用機能
　システム情報
　　・テクニカルサポート

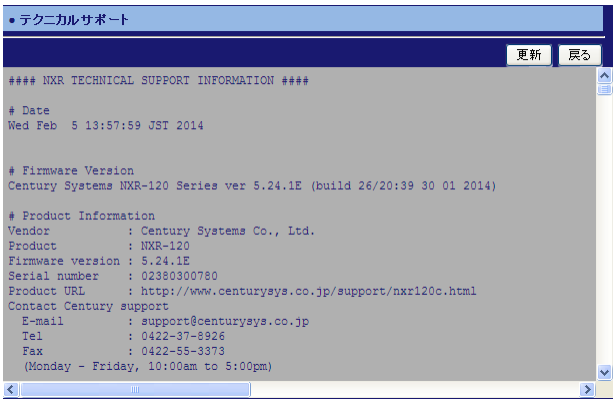
■テクニカルサポート



○出力先
出力先をプルダウンから選択して、実行をクリックします。



「テキスト表示」を選択した場合は、テクニカルサポート情報が表示されます。



「ファイル出力」を選択した場合は、下記の画面が表示されます。GUI の指示に従ってください。

Ⅳ．システム情報

3．システムモニター

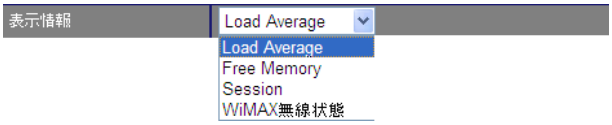
システム情報をグラフで表示します。

GUI 画面のメニューを下記の順にクリックします。
運用機能
　システム情報
　　・システムモニター

■システムモニター

○表示情報

表示情報をプルダウンから選択します。



○表示時間

表示時間（1～168[時間]）を入力します。デフォルト値は、「1」です。

○自動更新

「有効」/「無効」をプルダウンから選択します。

○更新間隔

更新間隔（1～60[分]）を入力します。デフォルト値は、「なし」です。

「実行」をクリックすると、選択した情報が表示されます。

Ⅴ．再起動

◆再起動

本装置、または各種サービスを再起動することが出来ます。

GUI 画面のメニューを下記の順にクリックします。
運用機能
　・再起動

■再起動

○再起動
プルダウンから、再起動するサービスを選択します。

・「本装置」を選択すると、システム再起動します。

Ⅵ．ディスク管理

◆ディスク管理

メディア（「USB メモリ」/「SD カード」）の取り出し、読み込み、初期化を行います。

GUI 画面のメニューを下記の順にクリックします。
運用機能
　・ディスク管理

■ディスク管理

○ USB メモリ
・「取り出し」をクリックすると、「USB メモリ」を安全に取り出すことが出来ます。
・「読み込み」をクリックすると、「USB メモリ」を読み込みます。
・「初期化」をクリックすると、「USB メモリ」を初期化します。

○ SD カード
・「取り出し」をクリックすると、「SD カード」を安全に取り出すことが出来ます。
・「読み込み」をクリックすると、「SD カード」を読み込みます。
・「SD カード」をフォーマットするには、フォーマット形式（「FAT32」/「XFS」）を選択して、「初期化」をクリックします。

Ⅶ．サポート情報

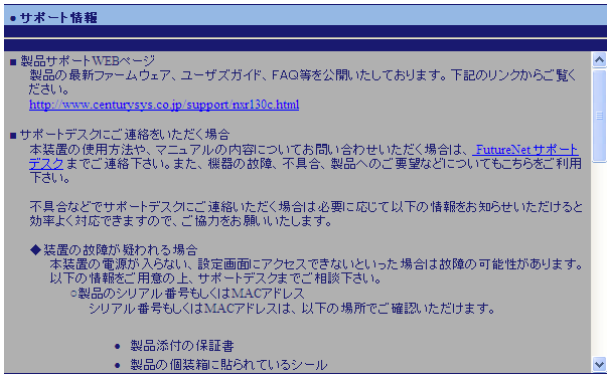
◆サポート情報

サポート情報を表示します。

GUI 画面のメニューを下記の順にクリックします。
運用機能
　・サポート情報

■サポート情報

サポート情報が表示されます。



付録

サポートについて

付録

サポートについて

◆今後のお客様サポートおよび製品開発の参考にさせていただくために、ユーザー登録にご協力をお願い致します。 弊社ホームページ内の各製品のサポートページで ”ユーザー登録 ”をクリックすると登録用の画面が開きます。

◆サポートに関する技術的なお問い合わせやご質問は、下記へご連絡ください。

・サポートデスク
e-mail ： support@centurysys.co.jp
電話 ： 0422-37-8926
FAX ： 0422-55-3373
受付時間 ： 10:00 ～ 17:00 (土日祝祭日、および弊社の定める休日を除きます)

・ホームページ http://www.centurysys.co.jp/

◆故障と思われる場合は
製品の不良や故障と思われる場合でも、必ず事前に弊社までご連絡ください。
事前のご連絡なしに弊社までご送付いただきましてもサポートをお受けすることはできません。

◆ご連絡をいただく前に
スムーズなお客様サポートをご提供するために、サポートデスクにご連絡いただく場合は以下の内容をお知らせいただきますよう、お願いいたします。

・ファームウェアのバージョンと MAC アドレス
・ネットワークの構成(図)
　どのようなネットワークで運用されているかを、差し支えのない範囲でお知らせください。
・不具合の内容または、不具合の再現手順
　何をしたときにどういう問題が発生するのか、できるだけ具体的にお知らせください。
・エラーメッセージ
　エラーメッセージが表示されている場合は、できるだけ正確にお知らせください。
・本装置の設定内容、およびコンピュータの IP 設定
・**可能であれば、「設定のバックアップファイル」をお送りください。**

◆サポート情報
弊社ホームページにて、製品の最新ファームウェア、マニュアル、製品情報を掲載しています。
また製品の FAQ も掲載しておりますので、是非ご覧ください。
下記の FutureNet サポートページから、該当する製品名をクリックしてください。
http://www.centurysys.co.jp/support/index.php

◆製品の保証について
本製品の保証期間は、ご購入から販売終了後 5 年間までです。
(但し、AC アダプタ及び添付品の保証期間はご購入から 1 年間とします。)
保証期間内でも、保証書に販売店印のないもの(弊社より直接販売したものは除く)、また保証の範囲外の故障については有償修理となりますのでご了承ください。
保証規定については、同梱の保証書をご覧ください。

FutureNet NXR シリーズ ユーザーズガイド GUI 編 Ver.6.3.0 対応版

2014 年 09 月版
発行 センチュリー・システムズ株式会社