

# FutureNet AS-150/X

---

CDMA 1X モバイル・アクセス・ルータ

ユーザーズ・ガイド



CENTURY SYSTEMS

#### 商標について

FutureNet は、センチュリー・システムズ株式会社の商標です。

下記製品名等は米国 Microsoft Corporation の登録商標です。

Microsoft、Windows、Windows 95、Windows 98、Windows NT4.0、  
Windows 2000、Windows XP、Windows Vista、Microsoft Internet  
Explorer、Microsoft Outlook Express

その他の商品名、会社名は、各社の商標または登録商標です。

#### ご注意

- (1) お取扱いを誤った場合には責任を負いかねますので、ご使用前には必ず本マニュアルをお読み下さい。
- (2) このマニュアルの作成にあたっては万全を期しておりますが、万一不審な点、記載漏れなどお気づきのことがありましたらお問い合わせ下さい。
- (3) 本製品を使用した事によるお客様の損害、逸失利益、または第三者のいかなる請求につきましても、上記の項目(2)にかかわらず当社は一切の責任を負いかねますので、あらかじめご了承下さい。
- (4) このマニュアルの著作権および本体ハードウェア、ソフトウェアに関する知的財産権は、センチュリー・システムズ株式会社に帰属します。
- (5) このマニュアルの内容の全部または一部を無断で転用、複製することはできません。
- (6) 本マニュアルの内容および仕様、外観は、改良のため将来予告なく変更することがあります。

## — 目次 —

1 章 はじめに.....	1
1.1 AS-150/X の使い方 .....	2
1.2 梱包内容の確認.....	4
2 章 ハードウェアの名称と接続方法.....	5
2.1 AS-150/X の本体各部の名称.....	6
2.2 LED 表示.....	7
2.3 接続の方法.....	10
2.4 LAN インターフェース仕様.....	11
3 章 センターとの通信仕様.....	13
3.1 発信 着信 PPP 時間管理.....	14
3.1.1 ドメイン管理情報.....	14
3.1.2 発信、PPP 認証.....	14
3.1.3 着信、PPP 認証.....	15
3.2 NAT/PAT 変換.....	16
3.2.1 NAT コンフィグレーション・テーブルの作成方法.....	16
3.2.2 NAT コンフィグレーション・テーブルの設定例.....	18
3.2.3 セッション管理仕様.....	22
3.3 GRE トンネリング.....	23
3.4 インターネット接続と DNS リレー機能.....	25
3.5 OTA 機能.....	26
4 章 セットアップ機能.....	29
4.1 工場出荷 IP アドレスの変更.....	30
4.2 Telnet 設定の使い方.....	31
4.3 Telnet 設定内容と工場出荷値.....	34
4.4 設定値の保存と復帰.....	40
4.5 設定を工場出荷値に戻す.....	43
5 章 運用・管理に関する機能.....	45
5.1 時刻サーバ機能.....	46
5.2 パケットフィルタ機能.....	47
5.2.1 機能の概要.....	47
5.2.2 設定項目.....	48

---

5.2.3	主な設定例 .....	50
5.3	DHCP サーバ機能 .....	52
5.3.1	設定手順 .....	52
5.3.2	DHCP クライアントの設定について .....	56
5.4	通信履歴のロギング機能 .....	57
5.5	SYSLOG によるログの転送 .....	60
5.5.1	AS-150/X 側の設定 .....	60
5.5.2	ホストコンピュータ側の設定 .....	61
5.6	ステータス表示 .....	63
5.7	ファームウェアのバージョンアップ .....	68
6章	コマンド一覧 .....	71
6.1	制御コマンド .....	72
6.2	設定コマンド .....	75
7章	参考資料 .....	85
7.1	XR ルータとの GRE 拠点間通信設定例 .....	86
7.2	AS-150/X 仕様一覧 .....	91

# 第 1 章

## はじめに

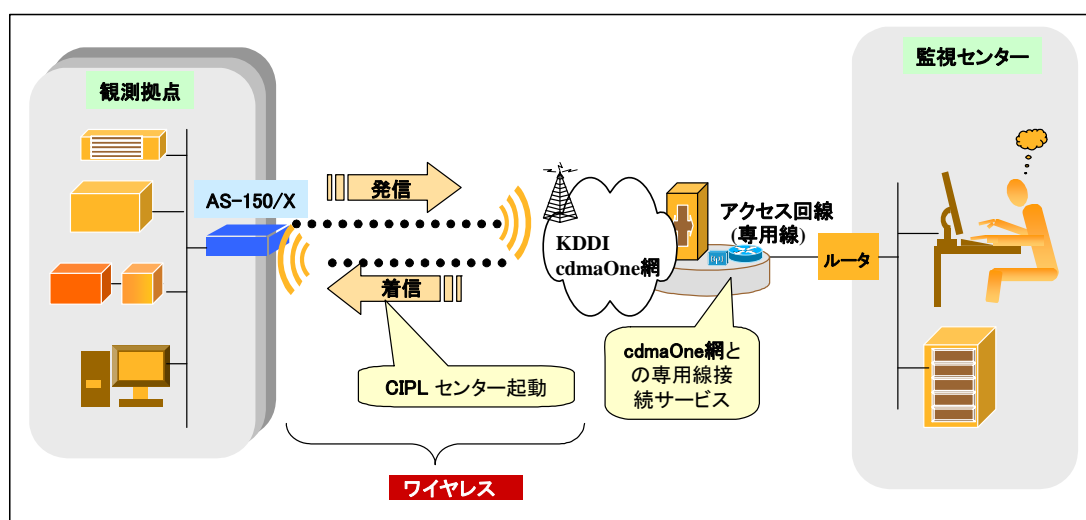
ここでは FutureNet AS-150/X の概要をご紹介します。

## 1.1 AS-150/X の使い方

FutureNet AS-150/X はKDDI株式会社が提供するCDMA 1Xサービスを使ってモバイルデータ通信を簡単に実現するための通信装置です。屋外に設置した設備・機器など、環境条件の厳しい場所でもワイヤレスの通信を実現します。

通信モジュールとしては「WM-M200」（セイコーインスツルメンツ社製）を内蔵しています。「WM-M200」は、CDMA 1Xに対応しており、下り最大 144kbps（ベストエフォート）、上り最大 64kbps（ベストエフォート）の通信性能を備えます。

下図に示す CIPL サービス環境でアクセスサーバとして使用できます。



CDMA 1Xの回線契約では拠点側ネットワークにはIPアドレスが1つだけ割り当てられます。そのため拠点側に複数のLAN装置がある場合は **NAT/PAT** (Network Address Translation/ Port Address Translation) を使うのが一般的です。AS-150/XのNAT/PATはポートフォワード(WAN側から特定のポートへのマッピング)機能を備えています。またトンネルプロトコルの1つである **GRE** (Generic Routing Encapsulation)も組み込んでいます。GREの場合はセンター側にFutureNet XRシリーズのルータを使います。AS-150/Xとセンター側ルータ間でトンネリングすると、センター側からは複数の機器間をIPアドレスで指定して通信がおこなえます。

末端機器とセンタ間のTCP/IP通信をNATまたはGREのどちらを使用するかはCIPLドメインごとに設定できます。どちらの場合も、WANインタフェースのIPアドレスはIPCP(Internet Protocol Control Protocol)はPPP上でIP通信を開始する際に、

IP アドレスの受け渡しなどに使われるプロトコルです) によって取得します。

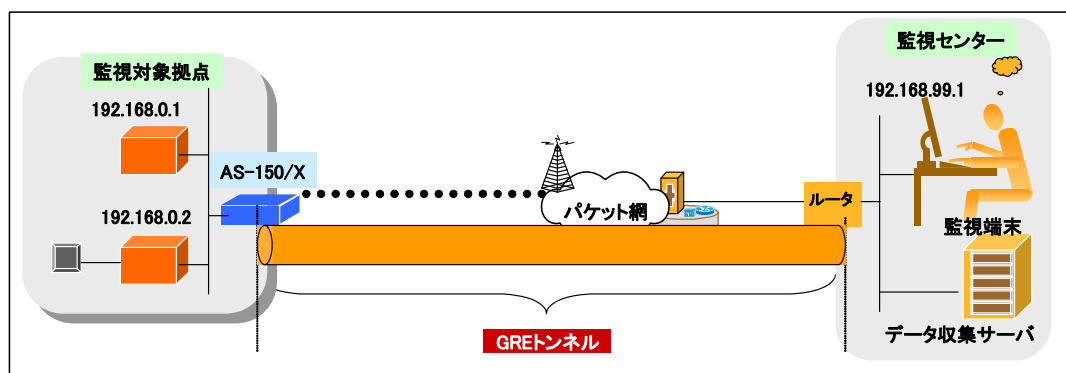
#### 1) NAT の場合

末端機器からセンターに送る IP パケットの送信元アドレスはこのアドレスに変換し (NAT)、センターから受信した IP パケットの送信先 IP アドレスは末端機器の IP アドレスに逆変換します。

#### 2) GRE の場合

末端機器からセンターに送る IP パケットは GRE カプセル化をおこないます。デリバリヘッダの送信元 IP アドレス (GRE トンネリング始点) は IPCP によって取得したアドレスとし、送信先 IP アドレス (GRE トンネリング終点) はセンターのルータ (FutureNet XR シリーズ) のアドレスとします。

センターから受信した GRE パケットはデカプセル化をおこないます。



## 1.2 梱包内容の確認

製品パッケージに含まれる内容は別紙の「パッキングリスト」に記載されています。「パッキングリスト」に含まれるものがそろっているか確認して下さい。万一、不足しているものがありましたら、お手数ですが「FutureNet サポートデスク」までご連絡下さい。

製品に同梱の CD-ROM には、本マニュアルの他にファームウェア・バージョンアップのためのユーティリティソフトが含まれています。これについても確認して下さい。



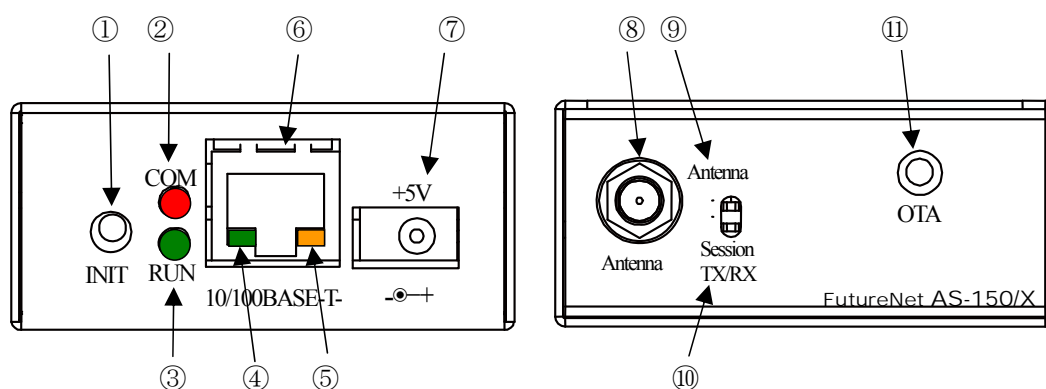
# 第2章

## ハードウェアの名称と接続方法

ここでは FutureNet AS-150/X の本体各部の名称と接続についてご説明します。

## 2.1 AS-150/X の本体各部の名称

AS-150/X の本体各部の名称と働きは以下のとおりです。



【AS-150/X 本体各部の名称と働き】

番号	名 称	働 き
①	[INIT] プッシュボタン	このボタンを押しながら本体の電源を入れると、すべての設定内容を工場出荷時の状態に初期化します。 詳細は「4.4 設定を工場出荷値に戻す」を参照してください。
②	[COM] 赤色 LED	下記「2.2 LED 表示」を参照してください。
③	[RUN] 緑色 LED	
④	イーサネットリンク LED(緑)	イーサネットリンクで点灯。データ送受信時は点滅します。
⑤	イーサネット速度 LED(橙)	100Mbps 時点灯、10Mbps 時消灯します。
⑥	[100/10BASE-T] イーサネットコネクタ	イーサネット規格の 100/10BASE-T ケーブルを接続するためのコネクタ(RJ-45)です。
⑦	[+5V] DC 電源ソケット	AC アダプタからの電源ケーブルを接続します。 必ず製品付属の AC アダプタを接続して下さい。
⑧	[Antenna] アンテナ接続端子	外部アンテナを接続する端子です。
⑨	[Antenna] 電波強度 LED	赤緑の 2 色 LED で電波強度を表示します。
⑩	[Session Tx/Rx] PPP リンク/通信 LED	PPP リンクの確立/切断 及び データ送受信状態を表示します。また OTA 実行時の状態を表示します。
⑪	[OTA] プッシュボタン	OTASP(回線開通)を行います。 詳細は「3.5 OTA 機能」を参照してください。

## 2.2 LED 表示

本装置は6個のLEDを持っています。

### (1) 動作状態の表示

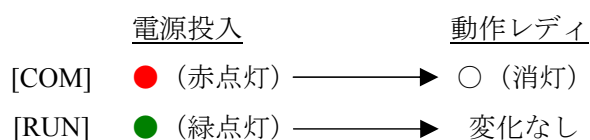
[COM]、[RUN] の2個のLEDにより、動作状態を表示します。

[COM] は本装置の運用可/不可の状態を表しています（消灯時は運用可、点灯及び点滅時は不可）。点滅は「約0.2秒点灯/0.2秒消灯」の繰り返しを意味します。

#### ●正常動作時のLED表示

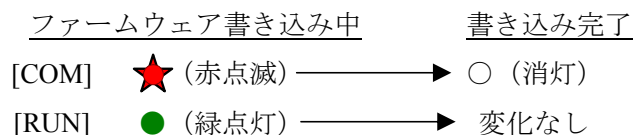
##### ①起動準備中

電源投入（または再起動）でCOM-LEDが点灯し、動作可能になると消灯します。動作可能状態になるまでに数10秒程度要します。



##### ②バージョンアップ時

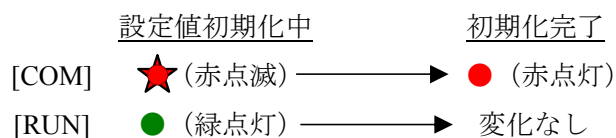
ファームウェア書き込み中はCOM-LEDが点滅し、完了で消灯します。



##### ③工場出荷値設定時

設定値初期化中はCOM-LEDが点滅し、初期化完了で点灯します(約20秒程度)。

この後停止しますので、運用する場合は電源を入れなおしてください。



## ●エラー発生時のLED表示と動作

## ①Ethernet ハードウェアエラー

COM-LED は3回点滅と1秒消灯を繰り返し、RUN-LED は連続点滅します。動作停止の状態です。

[COM] →  1秒消灯  1秒消灯  1秒消灯 ~  
 [RUN] →  ~

## ②不揮発メモリ読み書きエラー

COM-LED は4回点滅と1秒消灯を繰り返し、RUN-LED は連続点滅します。動作停止の状態です。

[COM] →  1秒消灯  1秒消灯  ~  
 [RUN] →  ~

## ③H/W システム情報読み出しエラー

COM-LED は5回点滅と1秒消灯を繰り返し、RUN-LED は連続点滅します。動作停止の状態です。

[COM] →  1秒消灯  1秒消灯  ~  
 [RUN] →  ~

## ④システムエラー

COM-LED と RUN-LED は両方とも連続点滅し、動作を停止します。ただし WatchDog 監視を行っていただければ再起動します。

[COM] →  ~  
 [RUN] →  ~

## (2) アンテナ強度の表示

電波の受信状態を1個の2色LED [Antenna] により以下のように表示します。

緑点灯：普通（3本）  
 緑点滅：やや弱い（2本）  
 赤点滅：弱い（1本）  
 赤点灯：圏外（0本）

### (3) PPP リンク/通信/OTA 状態 LED

PPP リンク及びデータ送受信の状態を 1 個の緑色 LED [Session Tx/Rx] により以下のように表示します。

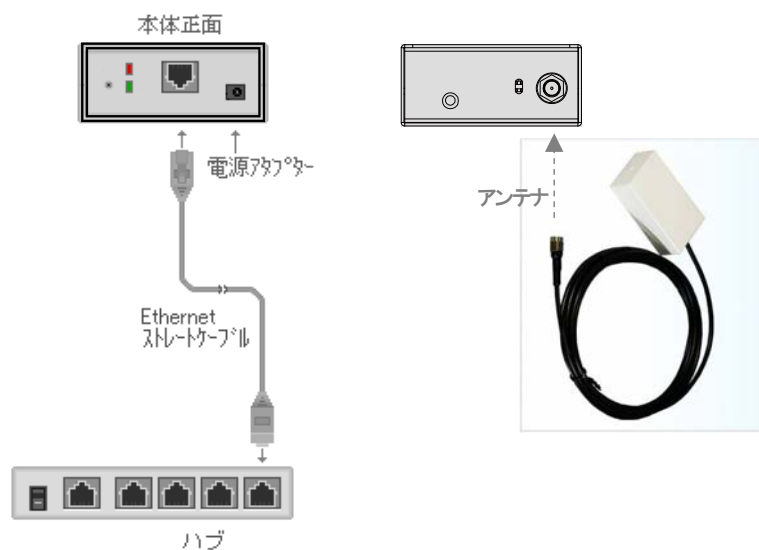
- PPP リンク確立時 点灯。PPP リンク解消時 消灯。
- PPP リンクの状態にかかわらず、データ送受信時、点滅。
- OTA 機能を実行したとき、以下の表示を行います
  - ① モジュールとのデータ送受信に伴い、点滅。
  - ② OTASP が成功した場合、約 10 秒間点灯。

### (4) イーサネットリンク/速度 LED

イーサネットコネクタの両側の 2 個の LED で、PHY リンクとデータ転送状態を表示します。「2.1 AS-150/X の本体各部の名称」を参照してください。

## 2.3 接続の方法

本体背面は次のように各機器を接続して下さい。



### 接続可能なアンテナ

AS-150/X に接続できる外部アンテナ（別売）は用途に応じて各社の製品が選択できます。使用可能な製品につきましては弊社営業部までお問い合わせください。

### LAN ケーブルの接続

本装置を LAN に接続するにはイーサネットケーブルを使って本装置の 100/10Base-T ポートをハブに接続します。イーサネットケーブルのクロス/ストレートは自動判定です。ケーブル・コネクタは、カチッと音がするまでしっかりと接続して下さい。

AC アダプタ電源には AC100V の家庭用・商用電源を使用して下さい。

## 2.4 LAN インターフェース仕様

本装置は以下のイーサネットインタフェースを備えています。

Fast Ethernet × 1 ポート  
100BASE-TX/10BASE-T (RJ-45)、Auto MDI/MDI-X

本装置の MAC アドレスの上位 3 バイトは“00806D”です。MAC アドレスは本体の裏面のシールに印刷されています。また、Telnet でログインしたときの最初の画面にも表示されます。

通信速度および通信モードについては、電源投入時、相手装置とオートネゴシエーションを行い、伝送速度と全二重/半二重を自動的に決定します。

また、接続されたイーサネット・ケーブルがストレートかクロスかを自動的に判別し、信号を切り替えます。





# 第3章

## センターとの通信仕様

ここではCIPL網を經由してセンターと通信する上で必要とする機能や設定内容についてご説明します。

## 3.1 発信 着信 PPP 時間管理

### 3.1.1 ドメイン管理情報

本装置はドメイン毎の情報として以下の内容を管理しています。

- ① ドメイン名
- ② ユーザー名
- ③ パスワード
- ④ 自動発呼先の宛先 IP アドレスとネットマスク値
- ⑤ メトリック (宛先までのホップ数)
- ⑥ 接続インターフェースとして、NAT/GRE のどちらを使用するか
- ⑦ GRE を選択した場合の GRE トンネリング終点 IP アドレス

### 3.1.2 発信、PPP 認証

センターから着信待ち受け状態時に、イーサネットインターフェースから IP パケットを受信し、その宛先 IP アドレスがドメインリストの宛先 IP グループに含まれる場合、発信し、PPP 接続を行います。WAN 側の IP アドレスは、IPCP で取得します。PPP リンク確立時、対応するドメインリストの宛先 IP ネットワークを IP ルーティングテーブルに登録します。PPP リンク確立後は、LAN 側のパソコンから受信し WAN 側にルーティングする IP パケットは、NAT 変換または GRE カプセリング後 WAN 側に送出し、WAN 側から受信した IP パケットは、NAT 逆変換または GRE デカプセリング後 LAN 側に送出します。

PPP 認証は、以下の形式で行います。

ユーザーID : ドメインに対応するユーザー名@ドメインに対応するドメイン名

パスワード : ドメインに対応するパスワード

例. 下表のように2つのドメイン登録を行っている場合の例です。

ドメイン名	domain0	domain1
ユーザー名	user0	user1

パスワード	pw0	pw1
宛先ネットワーク	192.168.201.0	192.168.202.0
マスク	255.255.255.0	255.255.255.0
メトリック	1	1
インタフェース	NAT	GRE
GRE トンネリング終点	0.0.0.0	192.168.11.126

イーサネットインターフェースから 192.168.202.1 宛での IP パケットを受信したとき発信を行います。PPP 認証は、ユーザーID が“user1@domain1”、パスワードは“pw1”となります。

この例では、192.168.202.0/24 をインターフェース GRE として、IP ルートテーブルに登録します。

### 3.1.3 着信、PPP 認証

通信モジュールからの着信通知を受けて PPP 接続を行います。WAN 側の IP アドレスは、IPCP で取得します。PPP リンク確立時、対応するドメインリストの宛先 IP ネットワークを IP ルーティングテーブルに登録します。PPP リンク確立後は、自ノードまたは LAN 側から受信し WAN 側にルーティングする IP パケットは、NAT 変換または GRE カプセリング後 WAN 側に送出し、WAN 側から受信した IP パケットは、NAT 逆変換または GRE デカプセリング後自ノードまたは LAN 側に送出します。

PPP 認証時は着信したドメイン名に従い、登録されたユーザ名、パスワードを使用します。

## 3.2 NAT/PAT 変換

AS-150/X は、PAT (Port Address Translation、別名 : IP masquerade) 機能を実装しています。PAT 機能は、複数のプライベート IP アドレスを、センター側(認証代行 RADIUS)から払い出された単一のグローバル IP アドレスに対応させる機能です。これによって LAN 上の複数の機器が AS-150/X を通して CIPL を利用できるようになります。

また、NAT コンフィグレーション・テーブルに変換データを設定することにより、次のような接続形態が実現できます。

- WAN 側にアクセスできる LAN 側の機器を限定する。
- WAN 側からアクセスできる LAN 側の機器を指定する。
- WAN 側から LAN 側にアクセスできないようにする。

### 3.2.1 NAT コンフィグレーション・テーブルの作成方法

NAT コンフィグレーション・テーブルには、最大 48 個まで変換データを登録できます。複数の変換データが登録されている場合は、エントリ番号の小さい順に比較し、マッチした変換データに従って、NAT 変換や逆変換を行います。登録できる内容は下表の項目です。

エントリ番号	NAT コンフィグレーション・テーブルのエントリ番号
プライベート IP アドレス	<p>LAN 側のプライベート IP アドレスを次のいずれかで登録します。</p> <ul style="list-style-type: none"> <li>● プライベート IP アドレスを 1 つ指定する</li> <li>● プライベート IP アドレスの始点と終点を範囲で指定する</li> <li>● すべてのアドレスを対象とする</li> </ul> <p>単一指定した場合は「NAT エントリ」となり、このプライベート IP アドレスに対して WAN 側からアクセスが可能になります。</p> <p>範囲指定、またはすべてを指定した場合は「PAT エントリ」となり、WAN 側からはアクセスできなくなります。</p> <p>NAT エントリと PAT エントリは混在可能です。</p>

プロトコル	<p>LAN 側のプロトコルを次のいずれかで指定します。</p> <ul style="list-style-type: none"><li>● 特定のプロトコルを指定する</li><li>● すべてのプロトコルを対象とする</li></ul>
ポート	<p>LAN 側の TCP/UDP ポートを指定します。指定の仕方は次のいずれかが可能です。</p> <ul style="list-style-type: none"><li>● 1つのポート番号を指定する</li><li>● 複数のポート番号を始点、終点の範囲で指定する</li><li>● すべてのポートを対象とする</li></ul> <p>ただし、この項目は NAT エントリの場合のみ有効です。 PAT エントリの場合はこの設定は無視されます（すべてのポートにマッチする）。</p>
WAN 側からのアクセスポート	<p>WAN 側から LAN 側の機器にアクセスする際のポート番号を指定します（ポートフォワード）。この項目は NAT エントリの場合のみ有効です。 WAN 側からのアクセスポートが LAN 側機器のポートと同じ場合は省略できます。</p>

## 3.2.2 NAT コンフィグレーション・テーブルの設定例

【例1】LAN側にWWWサーバー1台と、複数のクライアントがある場合の例です。

(条件)

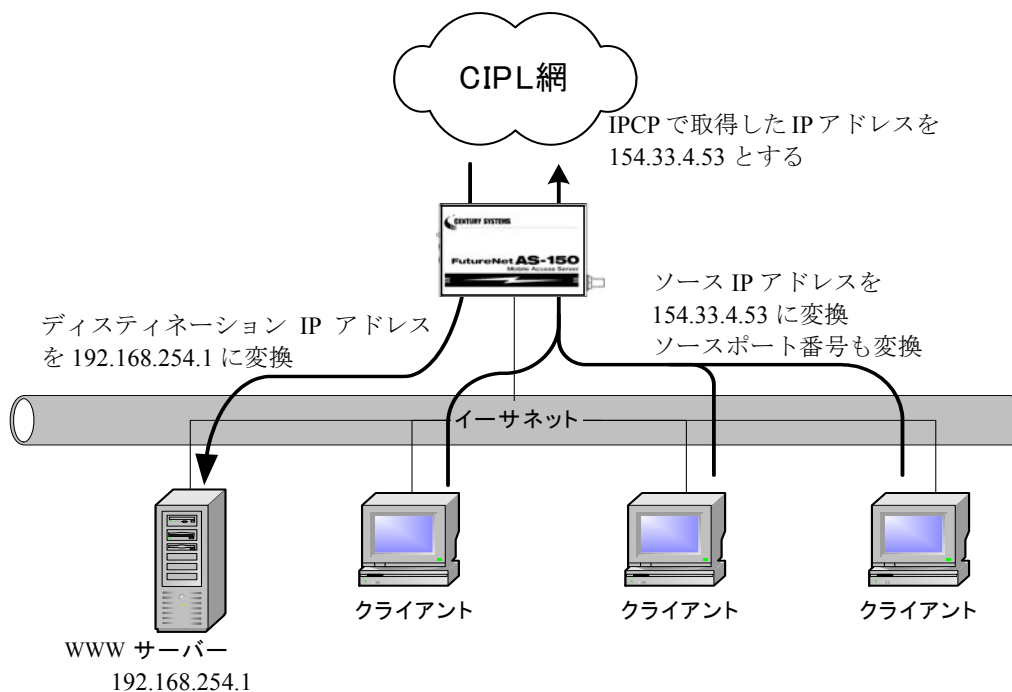
- ①WWWサーバー（プライベートIPアドレス=192.168.254.1）を、WAN側からアクセスできるようにする。
- ②その他のクライアントは全てWAN側にアクセスできるようにする（WAN側からのアクセスさせない）。

(登録)

NAT コンフィグレーション・テーブルの登録項目	①の条件	②の条件
プライベートIPアドレス	192.168.254.1	①以外すべてを対象
プロトコル	tcp	すべてを対象
ポート	www (80)	すべてを対象
WAN側からのアクセスポート	指定しない	指定しない

注) 登録時のエントリ番号は①より②を大きくします

(接続構成)



【例2】LAN側のクライアント1台に対し、WAN側からもアクセスできるようにする場合の例です。

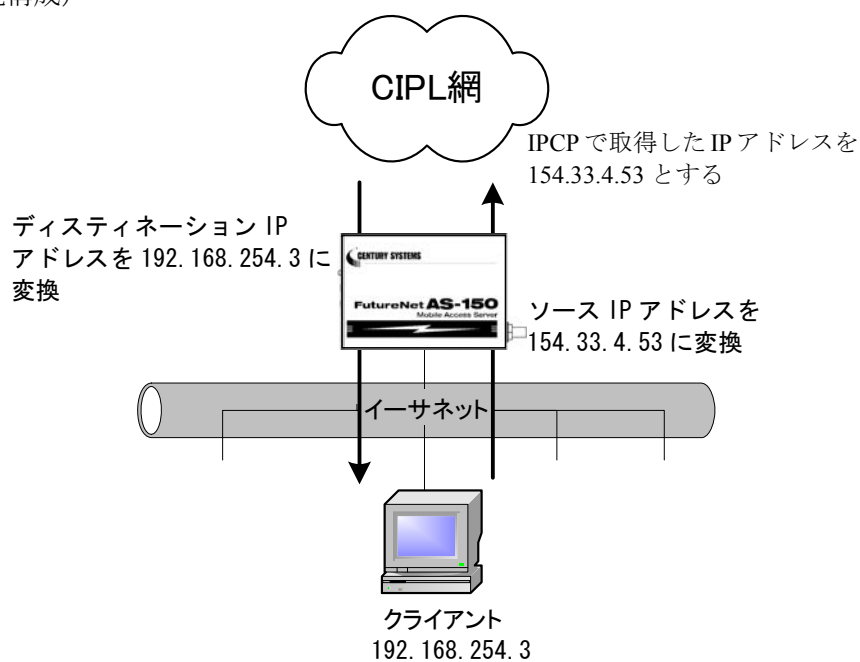
(条件)

WAN側にアクセスするクライアントを192.168.254.3のみに限定し、IPCPで取得した154.33.4.53に変換してWAN側へ送出させます。またWAN側からの154.33.4.53へのパケットも、すべて192.168.254.3に渡します。

(登録)

NAT コンフィグレーション・テーブルの登録項目	上記の条件
プライベート IP アドレス	192.168.254.3
プロトコル	すべてを対象
ポート	すべてを対象
WAN 側からのアクセスポート	指定しない

(接続構成)



【例3】WAN側にアクセスできるクライアントを限定する例です。

(条件)

WAN側にアクセスできるクライアントを、

- ① 192.168.254.2～192.168.254.4 および
- ② 192.168.254.7～192.168.254.10 に限定します。

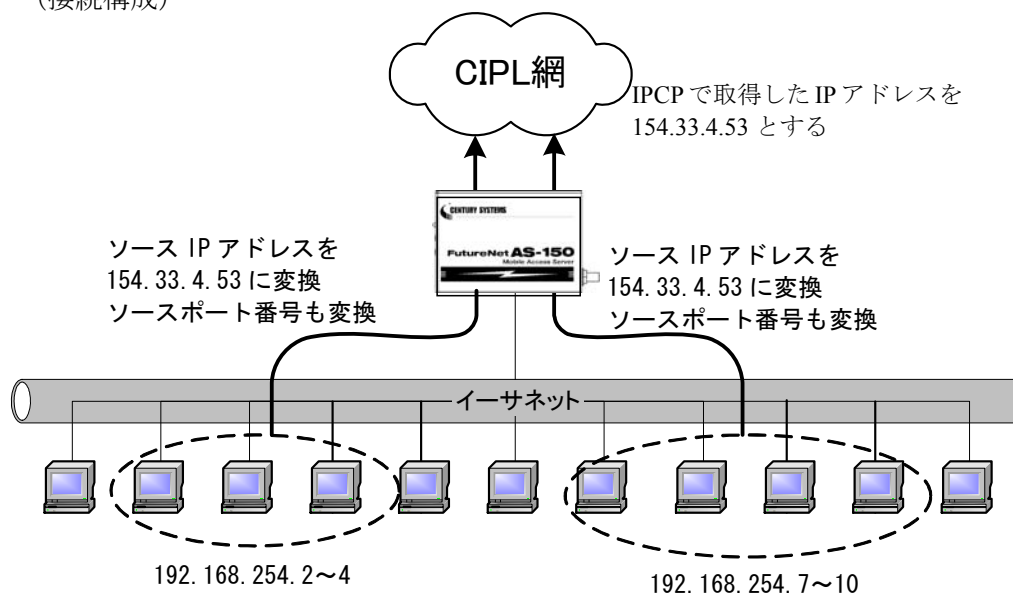
※WAN側からのアクセスは全てできません。

(登録)

NAT コンフィグレーション・テーブルの登録項目	①の条件	②の条件
プライベート IP アドレス	192.168.254.2 } 192.168.254.4	192.168.254.7 } 192.168.254.10
プロトコル	すべてを対象	すべてを対象
ポート	すべてを対象	すべてを対象
WAN側からのアクセスポート	指定しない	指定しない

注) エントリ番号の順序は無関係です

(接続構成)





【例4】ポートフォワード機能（ポート変換機能）を使う例です。

(条件)

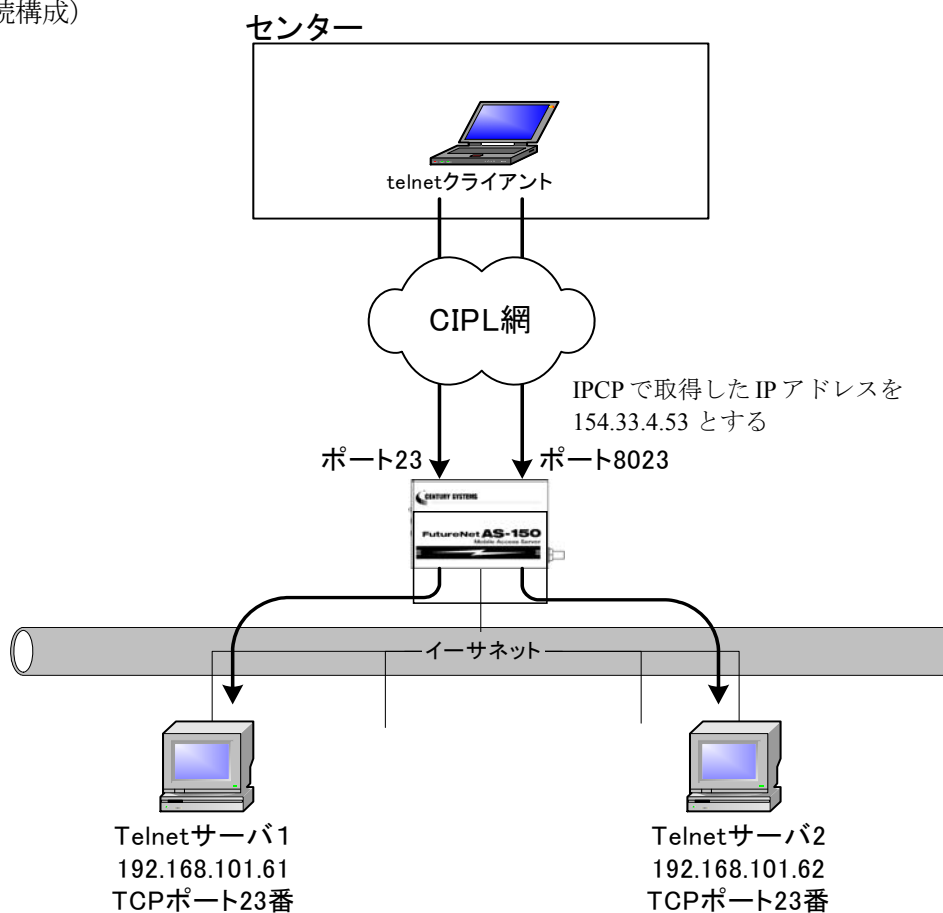
LAN側にある2つのTelnetサーバを、WAN側からアクセスできるようにします。Telnetクライアントから、①AS-150/Xの23番ポートにアクセスすると、LAN側の192.168.101.61:23につながります。②同様に8023番ポートにアクセスすると、LAN側の192.168.101.62:23につながります。

(登録)

NAT コンフィグレーション・テーブルの登録項目	①の条件	②の条件
プライベート IP アドレス	192.168.101.61	192.168.101.62
プロトコル	tcp	tcp
ポート	23	23
WAN 側からのアクセスポート	23	8023

注) エントリ番号の順序は無関係です。

(接続構成)



## 3.2.3 セッション管理仕様

AS-150/X の NAT セッション管理は、次のように行います。

## (1) PAT セッション

- 同時に存在できる PAT セッションは、最大で 1024 セッションです。（1クライアントが、1セッションしか使用しない場合は、1024 クライアントが1つの IP アドレスを共有できます）
- LAN 側から WAN 側に送信する TCP パケットや UDP パケットのソースポート番号は、0x3000～0x73FF（12288～29695）の範囲の値に変換します。
- TCP セッションは、無通信時間が 1800 秒継続した場合、あるいは、FIN/RST セグメントの送信または受信後 60 秒経過した場合にセッション管理テーブルから削除します。

UDP セッション、ICMP セッションは無通信時間が 60 秒継続した場合にセッション管理テーブルから削除します。ただし、PPP リンクが切れたときは、全セッションをテーブルから削除します。

## (2) NAT セッション

- 同時に存在できる NAT セッションは、FTP 制御コネクションを除いて、制限はありません。FTP 制御コネクションは、最大 64 セッションが同時に存在できます。
- FTP 制御コネクションは、無通信時間が 1800 秒継続した場合、あるいは、FIN/RST セグメントの送信後 60 秒経過した場合にセッション管理テーブルから削除します。

### 3.3 GRE トンネリング

AS-150/XではCIPL網を介した、IPルータ **FutureNet XR** シリーズ製品との間で、GRE トンネリング機能（RFC1701 GRE 準拠）を使うことができます。



本装置と XR 間で、GRE を設定してトンネルの用意ができると、両端の装置は次のような通信動作となります。

LAN 側インタフェースから受信したデータの宛先 IP アドレスを参照し、それが対向装置の LAN 側宛だった場合は GRE インタフェースに渡して、GRE ヘッダや WAN 側 IP アドレス等を付与し対向装置に転送します。

一方、GRE のデータを受信した対向装置では GRE ヘッダや WAN 側 IP アドレス等を取り外し、LAN 側インタフェースにデータを渡します。

この際 GRE を設定した装置配下から送信されたデータはアドレス変換等は行われません。

#### (1) GRE カプセリングとデカプセリング機能

イーサネットインタフェースからセンタに送信する（または AS-150/X 自身がセンタに送信する）IP パケットの、送信先 IP アドレスがトンネリング対象アドレス（ドメイン管理情報の宛先アドレス）であれば、カプセル化して CIPL 網に送出します。

また CIPL 網から、ディスティネーション IP アドレスが CIPL 網インタフェースの IP アドレスである GRE パケットを受信した場合、デカプセリングし、Payload パケットを取り出し、IP ルーティングを行います。

## (2) GRE ヘッダ

GRE ヘッダは4 オクテットで、値は 0x00000800 とします。

0x00000800 の意味は次の通りです。

- ① チェックサムフィールドは存在しない。
- ② ルーティングフィールドは存在しない。
- ③ キーフィールドは存在しない。
- ④ Sequence Number フィールドは存在しない。
- ⑤ Protocol Type は IP(0x0800)。

## (3) デリバリ・ヘッダ

デリバリ・ヘッダの送信元 IP アドレスは、IPCP で取得した WAN インタフェースの IP アドレスとします。

送信先 IP アドレスは、センターの XR シリーズ製品の IP アドレスとします。

TTL は、255 固定です。

## (4) GRE の MTU

GRE インタフェースの MTU は、1476 固定とします。

したがって、LAN 側から 1500 バイト、かつ Don't Fragment ビット=1 のパケットを受信した場合、ICMP Type=3(Destination Unreachable) Code=4(fragmentation needed and DF set) Next-Hop MTU=1476 を返信します。その結果として、1476 バイトのパケットを受信したら、GRE ヘッダとデリバリ・ヘッダを付加し、1500 バイトの IP パケットを PPP に渡します。

LAN 側から 1500 バイト、かつ Don't Fragment ビット=0 のパケットを受信した場合、フラグメント分割を行い、それぞれのフラグメントに GRE ヘッダとデリバリ・ヘッダを付加し、PPP に渡します。

## (5) GRE トンネリングの終点

本装置から見た GRE トンネリングの終点は XR シリーズ製品となります。

ドメイン管理テーブルにその IP アドレスを設定してください。「3.1.1 ドメイン管理情報の設定」を参照してください)

### 3.4 インターネット接続と DNS リレー機能

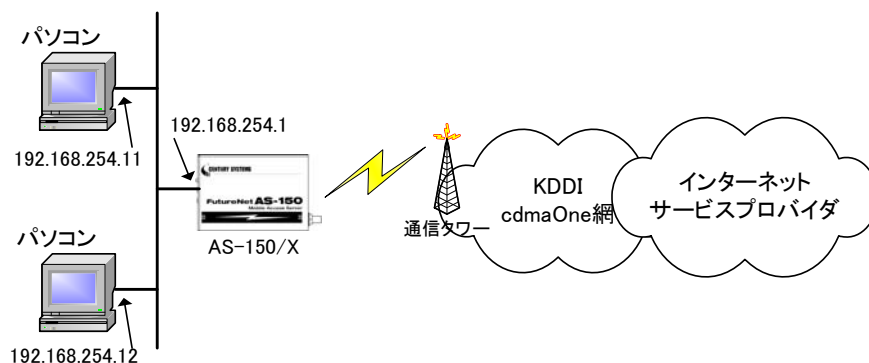
AS-150/X は、ドメインネームサーバ(DNS)の代理応答の機能を持ちます。

これは、LAN 側機器（パソコン）からのドメイン名解決要求パケットをプロバイダの DNS サーバに中継し、DNS サーバからの応答を LAN 側機器にかえす機能です。

DNS リレー機能を使用する際は以下の手順で行ってください。

- (1) ドメイン管理情報の宛先ネットワーク `0.0.0.0/0` と登録して、DNS リレー機能を有効にします。
- (2) クライアントとなる LAN 側機器（パソコン）に、デフォルトゲートウェイおよび DNS サーバとして、AS-150/X のイーサネットインタフェースの IP アドレスを設定します。（AS-150/X の DHCP サーバ機能を使えば、この設定は不要になります）
- (3) クライアントからインターネット接続を開始します。

《インターネット接続の例》



準備①：パソコンの設定は、デフォルトゲートウェイ、DNS サーバの IP アドレスを AS-150/X の IP アドレス(192.168.254.1)にします。

準備②：AS-150/X に下記を設定します (NAT の場合)。

```
domain ← 0 ← ドメイン名 ← ユーザー名 ← パスワード ← 0.0.0.0/0 ← 1
nat ← 0 ← * ← * ← * ← ipcp
dnsrelay ← activate ← on
```

注意) 上記コマンドに関しては「6.2 設定コマンド」を参照してください。

### 3.5 OTA 機能

OTA(Over The Air) は、無線を利用して通信モジュールの電話番号等 ID 情報の書込み、消し込みを可能にする機能です。電波状態が悪いと失敗しますので、電波状態が良好な状態で行うようにしてください。電波状態は LED、及び Telnet コマンドの『show antenna』（「6.1 制御コマンド」の(6)show 参照）で確認できます。

OTA には、回線を開通するとき電話番号等 ID 情報を書込む OTASP(回線利用開始)、と回線を閉塞するときの消し込み処理の OTAPA (回線の解約) があります。

本装置は、OTASP は OTA ボタンおよび Telnet コマンドの両方で、OTAPA は Telnet コマンドだけで行うことができます。

OTASP/OTAPA 実行時は、LED [Session Tx/Rx] が点滅します。OTASP に成功すると、10 秒間 [Session Tx/Rx] LED が点灯し、その後本装置は再起動します。OTASP が失敗した場合、10 秒間 LED 点灯はありません。そのまま再起動します。

#### (1) OTASP 機能

回線が開通されていない状態で、OTA ボタンが押されるか、Telnet のコマンドとして『ota sp』が入力されると、OTASP を実行します。

OTASP の実行状況、結果はログに残し、Telnet の場合は結果を表示します。回線が開通すると "OTASP is completed successfully." が表示され本装置は再起動します。

```

Ethernet address 00:80:6d:01:02:03
1) General
2) Service Type: CIPL Access Router
3) Service Settings
4) Status
5) Command Line
6) Exit
Enter number 5↵

> ota sp↵
OTASP is triggered.
AT@30
OK
OTASP1
OTASP2
OTASP3
OTASP4
OTASP5
OTASP6
OTASPQK
OTASP is completed successfully.
Rebooting...

```

OTA 向けコマンド及びリザルトコードをそのまま表示します。

OTASP 成功のメッセージ

回線の開通に失敗したり、回線がすでに開通されている状態で、Telnet のコマンドとして『ota sp』が入力された場合は、"OTASP is terminated abnormally." のエラーメッセージを表示します。また回線がすでに開通されている状態で、OTA ボタンが押下された場合は無視します。

## (2) OTAPA 機能

回線がすでに開通されている状態で、Telnet のコマンドとして『ota pa』が入力された場合、OTAPA（回線の解約）を実行します。

OTAPA の実行状況、結果はログに残し、Telnet の場合は結果を表示します。回線の解約ができると "OTAPA is completed successfully." が表示され本装置は再起動します。

```

Enter number 5↵
> ota pa↵
OTAPA is triggered.
AT@31
OK
OTAPA1
OTAPA2
OTAPA3
OTAPA4
OTAPA5
OTAPA6
OTAPAOK
OTAPA is completed successfully.
Rebooting...

```

回線の解約に失敗したり、回線が開通されていない状態で、Telnet のコマンドとして『ota pa』が入力された場合、"OTAPA is terminated abnormally." のエラーメッセージを表示します。

#### (3) モジュール製造番号表示機能

Telnet のコマンドとして『show module』が入力された場合、通信モジュールに対してその問い合わせを行い、レスポンスとして得られるモジュール製造番号、製造メーカー、型名、バージョン No を表示します。

#### (4) 電話番号表示機能

Telnet のコマンドとして『show phone』が入力された場合、通信モジュールに対してその問い合わせを行い、レスポンスとして得られる電話番号を表示します。

#### (5) ROM 書き問い合わせ番号表示要求機能

Telnet のコマンドとして『show rom』が入力された場合、通信モジュールに対してその問い合わせを行い、レスポンスとして得られる ROM 書き問合せ番号を表示します。



# 第4章

## セットアップ機能

ここでは AS-150/X の工場出荷時 IP アドレスの変更方法、及び他の設定方法についてご説明します。

## 4.1 工場出荷 IP アドレスの変更

本装置の設定は Telnet により行うことができます。

本装置の IP アドレスの工場出荷値は 192.168.254.254 に設定されてますので、お手持ちのパソコンの IP アドレスを一時的に 192.168.254.X (ただし X は 0、254 および 255 以外) に変更することにより、本装置に Telnet で接続して必要な設定をおこなうことができます。

AS-150/X を LAN に接続し、LAN 上のコンピュータから 192.168.254.254 のアドレスに Telnet コマンドを実行して下さい。Telnet 接続が成功するとパスワード確認のプロンプトが表示されます。

```
# FutureNet AS-150/X Version 1.00 #
password :
```

パスワードは“system”（工場出荷時の初期パスワード）と入力して下さい。ログインするとメニューが表示されます。

```
password :system↵
Ethernet address : 00806D123456
1) General
2) Service Type: CIPL Access Router
3) Service Settings
4) Status
5) Command Line
6) Exit
Enter number
```

このトップメニューから、1) General -> 2) TCP/IP -> 1) Ether I/F IP address を選んで、任意の IP アドレスとサブネットマスクビット値を指定して下さい。

```
IP configuration
1) Ether I/F IP address      192.168.254.254/24 ← 工場出荷値
2) Static route
3) Default route           0.0.0.0
4) IP packet filter
Enter number 1↵
Enter new IP address/mask 128.1.2.3/16 ← 設定例
```

IP アドレスとサブネットマスクビット数を指定したら Enter キーを押してトップメニューに戻り、6) Exit → 2) Save configuration & Restart を選んで下さい。

```

1) General
2) Service Type: CIPL Access Router
3) Service Settings
4) Status
5) Command Line
6) Exit
Enter number 6↵
1) Quit
2) Save configuration & Restart
Enter number 2↵ -----設定の保存と再起動を選択
Please Wait

Set up complete !

```

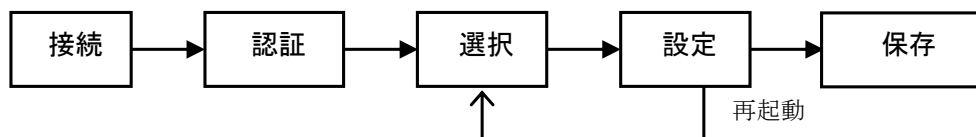
自動的に再起動がかかり、立ち上がった時点で新しいIPアドレスになります。

## 4.2 Telnet 設定の使い方

本装置の Telnet サーバは、LAN 側、PPP 側のどちらからでもログインできますが、シングルセッションですので同時に複数のユーザから接続はできません。

Telnet 接続すると、「4.1 工場出荷 IP アドレスの変更」で説明した設定メニューが表示されます。ここでは“Enter Number”のプロンプトに対してメニュー番号を指定して設定項目を選びます。設定項目を選ぶとその階層に移動し、さらにメニューの選択肢が表示されます。番号を指定しないで "↵" (Enter) キーだけを押しとひとつ上の階層に戻ります。

Telnet メニューの操作の流れは、次の通りです。



接続：Telnet コマンドで AS-150/X に接続します

認証：パスワードを入力して設定メニューを開きます

選択：設定したい内容を含むメニュー項目を選択します

設定：各メニュー項目で設定を変更します

保存：設定した内容を保存し、自動的に再起動します

設定した内容はトップメニューから 6) Exit → 2) Save configuration & Restart を選んだ時点ではじめて有効になり、AS-150/X は自動的に再起動します。また、6) Exit → 1) Quit を選ぶとそれまでの設定内容は無効となり、再起動もしません。設定内容を有効にするには、必ず 2) の Save configuration and Restart を選択して下さい。

設定値は不揮発メモリに書き込みますので、電源を落としても消えません。

トップメニューの各項目からはそれぞれ以下の項目が選択できます。

#### 1) General

AS-150/X の全体の動作や運用に関わる設定をおこないます。

IP アドレスや本体パスワードの設定などが可能です。

#### 2) Service Type:

将来機能が追加された場合の動作選択メニューです。現状は"CIPL Access Router"固定で変更できません。

#### 3) Service Settings

CIPL Access Router としての詳細動作の設定です。

#### 4) Status

通信状態の情報を表示します。「5.6 ステータス表示」を参照してください。

#### 5) Command Line

「4.2.1 コマンドラインの使い方」を参照してください。

#### 6) Exit

Telnet 設定メニューを終了します。変更した内容をキャンセルして Telnet メニューを閉じるか、設定した内容を保存して再起動するかが選べます。

#### 【Telnet 無通信切断機能について】

本装置の Telnet サーバはシングルセッションで、同時に複数のユーザからの接続は受け付けません。そのため工場出荷時は Telnet 接続したまま、何もしないで放置された場合、AS-150/X 側から約 5 分で自動的に切断するようにしています。このタイマ監視機能は、設定メニュー 1) General の 5) Start up から 1) Telnet Inactivity Timeout を選択して、時間を変更したり無効にすることができます。（「4.3.1 共通設定項目」の(7)参照）



## ■ コマンドラインの使い方

Telnet メニューの 5) Command Line を選択すると、本装置の設定値をコマンドにより変更することができます。

以下のように、コマンド入力を促すプロンプト ">" が表示されます。

```
Ethernet address 00:80:6d:01:02:03
1) General
2) Service Type: CIPL Access Router
3) Service Settings
4) Status
5) Command Line
6) Exit
Enter number 5↵
>
```

入力できるコマンドとしては、『show』、『restart』などのように入力して直ちに作用する制御コマンドと、各機能の設定を行う設定コマンドがあります。設定コマンドは『restart』の入力によって始めて本装置への書き込み保存が実行されます。

```
Enter number 5↵
> filter 0 reject in 192.168.120.100/24 * * * * ppp1↵
>syslog ipaddress 192.168.120.152↵
>syslog option system on↵
>restart↵
Please Wait...
Configuration was saved. Now restarting...
```

途中で Telnet コマンドラインを抜ける場合は『quit』コマンドを使用します。使用できるコマンドの全てを「6章 コマンド一覧」に説明しています。

### 4.3 Telnet 設定内容と工場出荷値

#### ■ General メニュー

##### (1) Password (General)

設定項目	内容	設定値	工場出荷値
Password	Telnet ログイン時のパスワード (工場出荷値は“system”)変更	半角英数記号 0～15 文字	system

##### (2) TCP/IP (General)

設定項目	内容	設定値	工場出荷値
Ether I/F IP address	本装置の IP アドレスとサブネットマスクビット数	*.*.*.* /1～30	192.168.254.254/ 24
Default route	LAN 側のデフォルトルータの IP アドレスを設定する。	*.*.*.*	0.0.0.0
Static Route	(3)参照		
IP Packet Filter	(4)参照		

##### (3) Static Route (General → TCP/IP IP)

スタティックルートは、イーサネット側に対する固定ルート設定です。LAN 上に他にルータがない場合は設定の必要はありません。複数のネットワークが相互に接続されている環境で、それぞれのネットワーク宛ての packets を、指定したルータに送信するために使用します。インターネット接続の場合は、スタティックルートを個別 LAN セグメントに対して設定してください。

設定項目は次のとおりです。

- Destination 宛先ネットワークのネットワーク番号
- Subnet Mask 宛先ネットワークのネットマスク値
- Next Router 経由するルータの IP アドレス
- Metric ホップ数

本装置では 30 までのスタティックルートを登録できます。Telnet メニューのルート 1～30 が、『route』コマンドのテーブル番号 0～29 に対応します。

設定項目	内容	設定値	工場出荷値
Destination	宛先 IP	*.*.*.*	0.0.0.0
Subnet mask	接続先 IP のサブネットマスク	*.*.*.*	0.0.0.0
Next router	最初のルータアドレス	*.*.*.*	0.0.0.0
Metric	接続先までのホップ数	0～15	0

## (4) IP Packet Filter (General → TCP/IP IP)

エントリ番号 1~32 を指定してフィルタを設定します。エントリ番号 1~32 は、『filter』コマンドのフィルタ番号 0~31 に対応します。詳細は「5.2 パケットフィルタ機能」を参照してください。

設定項目	内容	設定値	工場出荷値
type	フィルタの種類	<ul style="list-style-type: none"> <li>•pass(通過)</li> <li>•reject(破棄)</li> </ul>	無登録
dir	送受信の方向	<ul style="list-style-type: none"> <li>•in(受信フィルタ)</li> <li>•out(送信フィルタ)</li> </ul>	in
source IP address	送信元 IP アドレス	<ul style="list-style-type: none"> <li>•すべてを対象 * と書く</li> <li>•単独指定する 例) 192.10.3.5/32</li> <li>•範囲指定する 例) 192.10.3.5-92.10.3.254</li> </ul>	*
destination IP address	送信先 IP アドレス	<ul style="list-style-type: none"> <li>•すべてを対象 * と書く</li> <li>•単独指定する 例) 192.10.3.5/32</li> <li>•範囲指定する 例) 192.10.3.5-192.10.3.254</li> </ul>	*
protocol	プロトコルをニーモニック選択またはプロトコル番号で指定する	<ul style="list-style-type: none"> <li>•udp/tcp/tcpst/tcpfn/icmp</li> <li>•プロトコル番号(1~255)</li> <li>•すべては、* と書く</li> </ul>	*
source port	送信元ポート番号	<ul style="list-style-type: none"> <li>•すべてを対象 * と書く</li> <li>•単独指定する 例) 30000</li> <li>•範囲指定する 例) 30000-40000</li> </ul>	*
destination port	送信先ポート番号	<ul style="list-style-type: none"> <li>•すべてを対象 * と書く</li> <li>•単独指定する 例) 40000</li> <li>•範囲指定する 例) 40000-50000</li> </ul>	*
interface	接続インターフェース	ppp1 固定です	ppp1

## (5) DHCP server (General)

詳細は「5.3 DHCP サーバ機能」を参照してください。

設定項目	内容	設定値	工場出荷値
DHCP server	DHCP サーバの有効無効	Inactive/Active	Inactive
Subnet mask	DHCP クライアントに割り振るサブネットマスク	*.*.*.*	0.0.0.0

設定項目	内容	設定値	工場出荷値
Gateway IP address	DHCP クライアントに割り振るデフォルトゲートウェイ IP アドレス	*.*.*.*	0.0.0.0
Primary DNS server	DHCP クライアントに割り振るプライマリ DNS サーバの IP アドレス	*.*.*.*	0.0.0.0
Secondary DNS server	DHCP クライアントに割り振るセカンダリ DNS サーバの IP アドレス	*.*.*.*	0.0.0.0
WINS sever	DHCP クライアントに割り振る WINS サーバの IP アドレス	*.*.*.*	0.0.0.0
Domain name	DHCP クライアントに割り振る DNS ドメイン名	最大 31 文字	無登録
Lease time(hours)	IP アドレスの使用許可時間 (単位:時間)	0 から 9999 0 は時間無制限	24
Start address of the IP address pool	割り振る IP アドレスの開始アドレス	*.*.*.*	0.0.0.0
Number of address in the IP address pool	割り振る IP アドレスの数	0~128	0
Manually enter configuration parameters (1-128)	MAC address : IP アドレスを固定で割り振る対象を MAC アドレスで指定	16 進数 12 桁値。 バイト間を"."で区切る	00:00:00: 00:00:00
	IP address:固定で割り振る IP アドレス	*.*.*.*	0.0.0.0

(6) **SYSLOG** (General)

詳細は「5.5 SYSLOG によるログの転送」を参照してください。

設定項目	内容	設定値	工場出荷値
IP address	syslog サーバーの IP アドレス	*.*.*.*	0.0.0.0
UDP port	syslog サーバーの UDP ポート番号	1~65535	514
Log authorization messages	認証に関するログの送信	No/Yes	No
Log system messages	起動・設定変更・再起動等を記録するかどうか	No/Yes	No
Log RS232C messages	RS232C の動作ログを記録するかどうか	No/Yes	No
Log PPP messages	PPP に関するログの送信	No/Yes	No

(7) **Start up** (General)

設定項目の"Watchdog reset"は、本装置のファームウェアが正常に動作しているかどうかをハードウェアで監視し、正常に動作していないことを検出するとソフトウェアの再起動を行うものです。変更は **Save configuration & Restart** を行わなくても、**No/Yes** 選択の時点で保存されますが、動作に反映されるのは次回電源投入後です。



設定項目	内容	設定値	工場出荷値
telnet inactivity timeout	Telnetセッションを自動的に切断するタイムアウト	60～99999999(秒) 0は監視なし	300
Watchdog reset	WatchDog 監視を行うかどうかの選択	No/Yes	Yes

#### ■ Service Settings メニュー

##### (8) DOMAIN configuration table (Service Settings)

ドメインを5つまで登録できます（「3.1.1 ドメイン管理情報」参照）。Telnetメニューの入力エントリ1～5が、『domain』コマンドのドメイン番号0～4に対応しています。

設定項目	内容	設定値	工場出荷値
Domain name	ドメイン名	2～20 文字の半角数字「0～9」、半角英文字「a～z、A～Z」、ピリオド「.」、ハイフン「-」	空白
User name	ユーザー名	1～65 文字の半角数字「0～9」、半角英文字「a～z、A～Z」	空白
Password	パスワード	1～32 文字の半角数字「0～9」、半角英文字「a～z、A～Z」	空白
Destination	宛先ネットワークアドレス/マスク	0.0.0.0～254.254.254.254/0～32 0.0.0.0/0の場合は全てを対象とする	0.0.0.0/0
Metric	メトリック	1～15	1
Interface	NAT/GRE どちらを使うかの選択	•nat (Network Address Translation) •gre (General Routing Encapsulation)	nat

上表6)Interfaceで2)greを選択すると"Enter GRE tunneling target IP address"のメッセージが表示されて、GRE トンネリング終点 IP アドレスの入力を促されます。

設定項目	内容	設定値	工場出荷値
GRE tunneling target IP address	GRE トンネリング終点 IP アドレス	*.*.*.*	0.0.0.0

##### (9) NAT configuration table (Service Settings)

NAT コンフィグレーションテーブルは1～48を選んで設定できます。それぞれ『nat』コマンドのエントリ番号0～47に対応します。各エントリは以下の内容です。

設定項目	内容	設定値	工場出荷値
Private IP address	プライベート IP アドレス	•単一アドレス指定 •範囲指定(192.68.0.1～192.68.0.254) •すべてを対象”*”	設定なし
Protocol	プロトコル	•単一プロトコル番号(1～254) •プロトコル番号範囲指定 •すべてを対象”*”	設定なし

Port	LAN 側の TCP/UDP ポート	<ul style="list-style-type: none"> <li>単一ポート番号(1~65535)</li> <li>ポート番号範囲指定</li> <li>すべてを対象”*”</li> </ul>	設定なし
Access Port from WAN	WAN 側から LAN 側の器機にアクセスする際のアクセスポート番号	0~65535	設定なし

(注)「3.2 NAT/PAT 変換」参照

#### (10) Inactivity timeout (Service Settings)

AS-150/X は、上りパケット (AS-150/X→センタ) の無通信状態を監視し、無通信時間が設定値を越えた場合、PPP リンクを解消し回線を切断します。

設定項目	内容	設定値	工場出荷値
Inactivity timeout	無通信監視タイムの設定。1秒から秒単位で設定できる。0 に設定すると監視は行わない。	0-99999999 0 は監視なし	30

#### (11) PING KeepAlive (Service Settings)

CIPL 網接続を維持するため定期的に Ping (ICMP echo) を送信します。

設定項目	内容	設定値	工場出荷値
Enable/Disable	Ping キープアライブ機能を使用するか否か	Enable/Disable	Disable
Destination	Ping キープアライブパケットの宛先 IP アドレス	*.*.*.*	設定なし
Timeout	IP パケットが一定時間流れないと、Ping キープアライブパケットを投げる。その秒数を指定する。	30~4294967	50

#### (12) Auto dial options (Service Settings)

設定項目	内容	設定値	工場出荷値
Trigger packet forwarding	発信のトリガとなったパケットを送信するか (on)、破棄するか (off) の指定。on の場合、トリガとなったパケット、及び発信中に LAN から受信した最大 10 パケットをバッファリングする。発信成功後バッファリングしたパケットを送信する。“Dial retries”の回数を越えて PPP 接続に失敗した場合は廃棄する。	off(行わない) on(行う)	off
Dial retries	ダイヤル再試行回数(1分間隔)	0~99999999	0

#### (13) Packet speed (Service Settings)

設定項目	内容	設定値	工場出荷値
packet speed	契約内容に合わせて無線パケットデータ通信速度を選択する。	<ul style="list-style-type: none"> <li>low(上り 14.4kbps、下り 14.4kbps)</li> <li>high(上り 64kbps、下り 144kbps)</li> </ul>	high

(14) **VJ compression** (Service Settings)

設定項目	内容	設定値	工場出荷値
VJ compression	VJ 圧縮機能を使用するか か	•Inactivate(使用しない) •Activate(使用する)	Activate

(15) **DNS relay** (Service Settings)

設定項目	内容	設定値	工場出荷値
DNS relay	DNS リレー機能を使用するか 否か。	•Inactivate(使用しない) •Activate(使用する)	Inactivate

(注) 「3.4 インターネット接続と DNS リレー機能」 参照

## 4.4 設定値の保存と復帰

本装置に設定した値は不揮発メモリに格納します。従って本装置の電源を落としたり、ファームウェアのバージョンアップを行っても消失することはありません。

ここではコマンドラインを使って、設定値の保存と、保存した設定値を再度書き込む場合の例を記述します。

### (1) 設定値の保存

- ① Telent メニューから 5)Command Line を選択し、『show config』コマンドを使って現在の設定値（工場出荷値から変更された項目）を表示させます。

```
Ethernet address 00:80:6d:01:23:45
1) General
2) Service Type: CIPL Access Router
3) Service Settings
4) Status
5) Command Line
6) Exit
Enter number 5↓ ----- コマンドラインを選択
> show config↓
main ip 192.168.1.1
main mask 255.255.255.0
nat 0 * * * ipcp
flag menutimeout 0
>
```

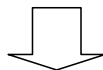
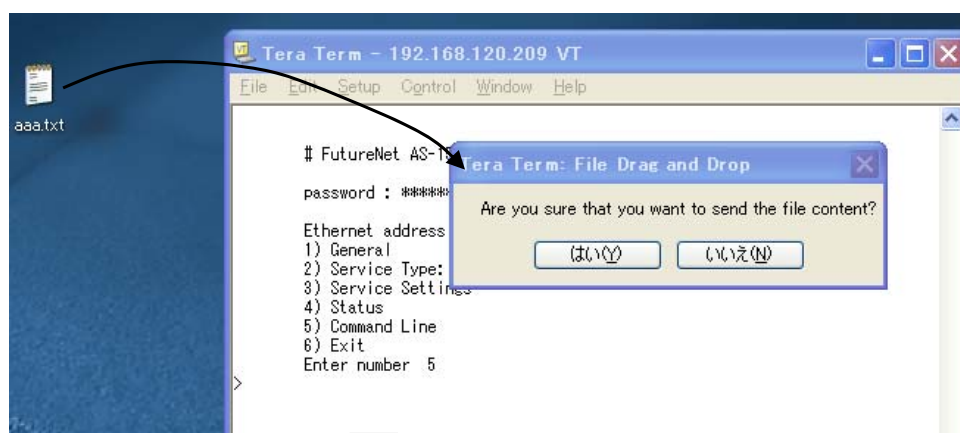
- ② 表示されたコマンド列をコピーしてメモ帳、ワードパッド、などに貼り付けて保存します。



```
aaa.txt - メモ帳
ファイル(F) 編集(E) 書式(O) 表示(V) ヘルプ(H)
main ip 192.168.1.1
main mask 255.255.255.0
nat 0 * * * ipcp
flag menutimeout 0
```

## (2) 設定値の復帰

- ① 上記で保存していた設定を AS-150/X に書き込む場合は、対象とする AS-150/X に Telnet 接続し、5)Command Line を選択してプロンプト ">" を表示させ、保存していたコマンドをコピーしてコマンドラインに貼り付けます。以下のように TeraTerm などを使用すると、保存したファイルをそのままドラッグ&ドロップして内容を貼り付けることもできます。



```

Enter number 5
> main ip 192.168.1.1
> main mask 255.255.255.0
> nat 0 * * * ipcp
> flag menutimeout 0
>

```

- ② 最後に『restart』により設定の書き込みを行います。

```

Enter number 5
> main ip 192.168.1.1
> main mask 255.255.255.0
> nat 0 * * * ipcp
> flag menutimeout 0
✕ restart!
Please Wait...
Configuration was saved. Now restarting...

```

もしくは、以下のように『quit』でコマンドラインを抜けて、トップメニューの 6) Exit から設定の書き込みを行っても同じです。

```
Enter number 5
> main ip 192.168.1.1
> main mask 255.255.255.0
> nat 0 * * * ipcp
> flag menutimeout 0
> quit↵

Ethernet address 00:80:6d:01:02:03
1) General
2) Service Type: CIPL Access Router
3) Service Settings
4) Status
5) Command Line
6) Exit
Enter number 6↵
1) Quit
2) Save configuration & Restart
Enter number 2↵
Please Wait.

Set up complete !
```

## 4.5 設定を工場出荷値に戻す

本装置のすべての設定を工場出荷時の状態に戻すことができます。これは設定がわからなくなったり、使用場所を変える場合など、現在の設定内容をすべて破棄して、最初から設定をやり直す場合におこなって下さい。

工場出荷値に戻す場合は、以下の手順で操作して下さい。

- (1) 接続している回線があれば切断します。
- (2) 電源を切ります。
- (3) 本体背面の[INIT]ボタンを押しながら電源を入れます。設定値を初期化している間 20 秒程度、赤色 LED [COM] が点滅します。点滅が点灯に変わるまで[INIT]ボタンを押しつづけてください。点灯が変わると初期化完了です。[INIT]ボタンを離して下さい。

本装置のすべての設定は工場出荷状態に戻っています。本装置は停止状態ですので、電源を入れなおして使用してください。



**注意!**

### 【工場出荷値に戻す】

本装置の設定を工場出荷値に戻すと、それまで設定した内容はすべて失われます。復帰させる必要がある場合は、Telnet コマンドの "show config" によりすべての設定値を表示させて、コピー&ペーストでファイルなどに保存してください。





# 第5章

## 運用・管理に関する機能

ここでは本装置を運用管理する上で必要な機能についてご説明します。

## 5.1 時刻サーバ機能

AS-150/X は SNTP サーバのユニキャストモードの機能を持ち、LAN 側の機器からの要求に対して現在の時刻を返したり、通信ログにタイムスタンプを付けます。

現在時刻は本装置内蔵の GPS モジュールから取得しますので、電源投入直後または圏外などでは、時刻が得られない場合もあります。この場合 AS-150/X は、RFC2030 に従い、NTP メッセージの閏秒指示子フィールド(LI)に 3 をセットし、正確な時刻が得られなかったことを SNTP 要求元に通知します。

本装置が GPS モジュールから取得した現在時刻は、以下のように Telnet のコマンドラインから『show time』により表示させることができます。

```
Ethernet address 00:80:6d:01:23:45
1) General
2) Service Type: CIPL Access Router
3) Service Settings
4) Status
5) Command Line
6) Exit
Enter number 5↵
> show time↵
2008/07/30 17:30:21
>
```

## 5.2 パケットフィルタ機能

本装置では、セキュリティの強化と異常課金防止の目的で、LAN と WAN の間を流れるパケットにフィルタを設定して、通信を制限することができます。

設定は Telnet メニューまたはそのコマンドラインから行います。

### 5.2.1 機能の概要

LAN に外部からの接続を許す際には、セキュリティに充分配慮する必要があります。パケットフィルタ機能を使うと、以下のことができます。

- ・外部から LAN に入るパケットを制限する
- ・LAN から外部に出て行くパケットを制限する
- ・自動接続に使用するパケットを制限する

本装置でこの機能が有効になっていると、IP パケットを単にルーティングするだけでなく、パケットのヘッダ情報を調べて、送信元や送信先の IP アドレス、プロトコルの種類 (TCP/UDP)、ポート番号などに基づいて、パケットを通過させたり破棄したりすることができます。

このようなパケットフィルタ機能は、コンピュータやアプリケーション側の設定を変更する必要がないために、ユーザがパケットフィルタの存在を意識することなく、簡単に利用できます。一般的には、すべてのパケットの通過を禁止しておき、ユーザに提供したいサービス (アプリケーション) のパケットだけが通過できるように、フィルタリングを設定します。

また、パケットフィルタはリモートの LAN にダイヤルアップ接続をおこなう際の、異常課金の防止にも有効です。自動接続による接続をおこなう場合、LAN 上のコンピュータやアプリケーションの設定によっては、意図しない接続がおこなわれ、膨大な通信料金が請求されることがあります。これを防ぐためにも、パケットフィルタは有効です。ユーザが意図するアプリケーションだけを通し、それ以外のものは通さないようにフィルタを設定しておけば、こういった事故を未然に防ぐことができます。

本装置に設定済みのフィルタは、Telnet の次のメニューで確認することができます。

```

General configuration
1) Password
2) TCP/IP
3) DHCP Server(option)
4) SYSLOG LOG message settings(option)
5) Start up(option)
Enter number 2↵

IP configuration
1) Ether I/F IP address 192.168.120.207/24
2) Static route
3) Default route          0.0.0.0
4) IP packet filter
Enter number 4↵
1) Entry 1 - 16
2) Entry 17 - 32
3) The list which setting finished
Enter number 3↵
filter 1 pass in ** tcp ** ppp1
filter 2 reject in * * * * * ppp1
Enter number

```

最大 32 個フィルタが設定可能

設定済みのフィルタが表示される

設定済みフィルタがなければ以下のように表示されます。

```

1) Entry 1 - 16
2) Entry 17 - 32
3) The list which setting finished
Enter number 3↵
There is not the list which setting finished.
Press return key

```

設定済みのフィルタがない場合

### 5.2.2 設定項目

本装置は IP パケットのみをフィルタリング制御の対象とします。その他のレイヤー3 プロトコルは、すべて遮断します。

ICMP、TCP、UDP 以外のレイヤー4 プロトコルはすべて通します。ICMP の制御はおこないません。TCP では、ポート番号とフラグを監視します。UDP ではポート番号を監視します。

工場出荷の状態では、フィルタは設定されていません。ユーザは 32 個までのフィルタを設定することができます。

Telnet メニューから設定する場合は、まずエントリ番号を選択し、そのエントリ番号に対してサブメニューで表示された以下の項目を設定します。エントリ 1～32 が、『filter』コマンドのフィルタ番号 0～31 に対応しています。

## (1) Type

通過フィルタ (pass) か遮断フィルタ (reject) を指定します。

- 1) pass
- 2) reject

## (2) Direction

WAN に対する受信(in)または送信(out)のフィルタ方向を指定します。

- 1) in
- 2) out

## (3) Source IP address

対象とする送信元 IP アドレスを指定します。

- 1) \* (すべての送信元を対象とする)
- 2) single address (アドレスを単独指定する)
- 3) range of address (アドレスを範囲指定する)

Enter number 2↵

Enter source IP address 192.168.101.25↵

Enter mask(1-32) 24↵

} 単独指定の場合の指定例

## (4) Destination IP address

対象とする送信先 IP アドレスを指定します。

- 1) \* (すべての送信先を対象とする)
- 2) single address (アドレスを単独指定する)
- 3) range of address (アドレスを範囲指定する)

Enter number 3↵

destination IP address

Enter beginning IP address 192.168.200.1↵

Enter end IP address 192.168.200.5↵

} 範囲指定の場合の指定例

## (5) Protocol

対象とするプロトコルを指定します。1)～6)に該当しない場合は 7) other protocol number で直接プロトコル番号を指定します。

- 1) \* (すべてのプロトコルを対象とする)
- 2) icmp
- 3) tcp
- 4) tcpfin
- 5) tpest
- 6) udp
- 7) other protocol number

## (6) Source port

- 1) \* (すべての送信元ポートを対象とする)
- 2) single port (ポートを単独指定する)
- 3) range of port (ポートを範囲指定する)

Enter number 2↵

Enter source port number (1-65535) 21↵ } 単独指定の場合の指定例

## (7) Destination port

- 1) \* (すべての送信先ポートを対象とする)
- 2) single port (ポートを単独指定する)
- 3) range of port (ポートを範囲指定する)

Enter number 3↵

destination port number

Enter beginning port number (1-65535) 100↵

Enter end port number (1-65535) 200↵ } 範囲指定の場合の指定例

## (8) Interface

現バージョンではインターフェースは ppp1 固定です。

## 5.2.3 主な設定例

以降の『filter』コマンド形式については「6.2 設定コマンド」の(5)filter を参照してください。

## ● 送信元を制限する

LAN 上のコンピュータのうち、リモート WAN にアクセスできるものを制限したり、リモート WAN 側からアクセスを許すコンピュータの、IP アドレスを指定することができます。IP アドレスだけでなく、ポート番号やパケットの種類も細かく指定できます。

例：WAN に対して、アクセスできるコンピュータを「192.168.10.10」～「192.168.10.19」に限定する。(フィルタ番号 0、1 に登録)

```
filter 0 pass out 192.168.10.10 - 192.168.10.19 * * * * ppp1
```

```
filter 1 reject out * * * * * ppp1
```

上例では、まず pass で通過させるパケットを指定し、次の reject フィルタでそれ以外のパケットを止めます。

- 送信先を制限する

LAN 上のコンピュータから、特定の接続先に向けたパケットだけを通過させる、あるいは特定の接続先に向けたパケットだけを禁止することができます。

IP アドレスだけでなく、ポート番号やパケットの種類も細かく指定できます。

例：送信先コンピュータを「192.168.30.10」～「192.168.30.19」に限定する。

```
filter 0 pass out * 192.168.10.10 - 192.168.10.19 * * * ppp1
filter 1 reject out * * * * * ppp1
```

- 接続に使用するパケットを制限する

フィルタの設定を一切おこなわないと、リモート WAN に向けたどんな種類の TCP/IP パケットも流れます。これは異常課金の原因にもなります。

例：メールによるパケットは許すが、他のアプリケーションのパケットは通さない。

```
filter 0 pass out * * * * 25 ppp1
filter 1 reject out * * * * * ppp1
```

- アプリケーションを制限する

ポート番号にフィルタをセットすることによって、本装置を通過するアプリケーションを制限することができます。たとえば、Telnet と ftp は通すが、WWW は通さないといった設定ができます。

例：IP アドレス「192.168.10.1」の機器に対して、WWW（ポート番号 80）によるアクセスを禁止するとき。

```
filter 0 reject in * 192.168.10.1/32 tcp * 80 ppp1
```

注) 単一の IP アドレスを指定する場合は、IP アドレスのマスクを 32 に設定して下さい。

### 5.3 DHCP サーバ機能

本装置は小規模（クライアント 128 台以下）の単一セグメントの LAN で用いる RFC2131 準拠の DHCP サーバに対応しています。本装置を DHCP サーバとして設定しておくこと、DHCP として設定された Windows パソコンなどのクライアントに IP アドレス、サブネットマスク、デフォルトゲートウェイなどを自動的に設定できます。これによってクライアント側の設定が不要になり、ネットワーク関連の設定の間違いも防止できます。

本装置の DHCP サーバでは以下の設定情報を提供できます。

- IP アドレス
- サブネットマスク
- デフォルトゲートウェイアドレス
- プライマリ DNS サーバ
- セカンダリ DNS サーバ
- WINS サーバ
- DNS ドメイン名

また、128 台までのクライアントに固定の IP アドレスを割り当てることもできます。

#### 5.3.1 設定手順

本装置を DHCP サーバとして設定するための手順は次のとおりです。

- (1) メインメニューから 1) General → 3) DHCP Server を選択すると、以下の DHCP 設定メニューが表示されます。

```
DHCP server configuration
1) DHCP Server - Inactive
2) Subnet Mask - 000.000.000.000
3) Gateway IP Address - 000.000.000.000
4) Primary DNS server - 000.000.000.000
5) Secondary DNS server - 000.000.000.000
6) WINS server - 000.000.000.000
7) Domain Name -
8) Lease Time (hours) - 24
9) Start Address of the IP address pool - 000.000.000.000
10) Number of Addresses in the IP address pool - 0
11) Manually enter configuration parameters
Enter number
```



(2) DHCP サーバの設定をおこないます。

設定項目の設定方法は次のとおりです。

2-1) DHCP Server

DHCP サーバ機能を有効にするか、無効にするかを指定します。このメニューを選ぶと以下の項目が表示されます。

- 1) DHCP Server - Inactivate
- 2) DHCP Server - Activate

有効にする場合は 2) DHCP Server -Activate を選択して下さい。

2-2) Subnet Mask

DHCP クライアントに割り振る IP アドレスのサブネットマスクを指定します。次のようにマスク値を設定して下さい。

例) Enter Subnet mask 255.255.255.0

この項目を使用しない場合は設定しなくてもかまいません。

2-3) Gateway IP Address

DHCP クライアントに設定するデフォルトゲートウェイの IP アドレスを指定します。次のように設定して下さい。

例) Enter Gateway IP Address 192.168.254.10

この項目を使用しない場合は設定しなくてもかまいません。

2-4) Primary DNS server

DHCP クライアントに設定するプライマリ DNS サーバの IP アドレスを指定します。次のように設定して下さい。

例) Enter Primary DNS Server Address 203.140.129.3

この項目を使用しない場合は設定しなくてもかまいません。

2-5) Secondary DNS server

DHCP クライアントに設定するセカンダリ DNS サーバの IP アドレスを指定します。次のように設定して下さい。

例) Enter Secondary DNS Server Address 203.140.129.5

この項目を使用しない場合は設定しなくてもかまいません。

2-6) WINS server

DHCP クライアントに設定する WINS サーバの IP アドレスを指定します。次のように設定して下さい。

例) Enter WINS Server Address 192.168.254.5

この項目を使用しない場合は設定しなくてもかまいません。

#### 2-7) Domain Name

DHCP クライアントに設定する DNS ドメイン名を指定します。次のように設定して下さい。

例) Enter domain name (32 chars max) centurysys.co.jp

この項目を使用しない場合は設定しなくてもかまいません。

#### 2-8) Lease Time (hours)

割り振った IP アドレスの使用を許す時間を時間(hour)単位で指定します。ここで設定された時間が経過すると、その IP アドレスは解放され、次の割り振りに使用される可能性があります (実際に解放されるか再取得されるかは使用する DHCP クライアントによります)。この値は次のように設定して下さい。なお、0 を指定すると解放しません。

例) Enter the lease time in hours 12

#### 2-9) Start Address of the IP address pool

割り振る IP アドレスの開始アドレスを指定します。このアドレスから 10)の項目で指定する数だけ IP アドレスが確保されます。次のように設定して下さい。

例) Enter the starting address of the IP pool 192.168.254.70

#### 2-10) Number of Addresses in the IP address pool

割り振る IP アドレスの数を指定します。9)の項目で指定した IP アドレスからこの数だけ IP アドレスが確保されます。次のように設定して下さい。

例) Enter the number of addresses in the IP pool 30

以上、2-1)から 2-10)までの設定ができると次のように表示されます。

```
DHCP server configuration
1) DHCP Server - Active
2) Subnet Mask - 255.255.255.000
3) Gateway IP Address - 192.168.254.010
4) Primary DNS server - 203.140.129.003
5) Secondary DNS server - 203.140.129.005
6) WINS server - 192.168.254.005
7) Domain Name - centurysys.co.jp
8) Lease Time (hours) - 12
```

```

9) Start Address of the IP address pool - 192.168.254.070
10) Number of Addresses in the IP address pool - 30
11) Manually enter configuration parameters
Enter number

```

DHCP で割り振る IP アドレスとコンピュータの組を固定したい場合は、次の設定をおこないます（オプション）。

#### 2-11) Manually enter configuration parameters

```

1) Entry      1- 16
2) Entry      17- 32
              中略)
7) Entry      97- 112
8) Entry      113- 128
Enter number  1← _____ 1~16 のグループを選択

```

ここでは 128 台分のクライアントの設定が可能です。表示のために 16 台ずつにグループ化されています。どこに設定してもかまいませんが、設定した場所を間違えないよう順番に使用することをお勧めします。

```

DHCP entry
1) 00:00:00:00:00:00 000.000.000.000
2) 00:00:00:00:00:00 000.000.000.000
3) 00:00:00:00:00:00 000.000.000.000
   中略)
12) 00:00:00:00:00:00 000.000.000.000
13) 00:00:00:00:00:00 000.000.000.000
14) 00:00:00:00:00:00 000.000.000.000
15) 00:00:00:00:00:00 000.000.000.000
16) 00:00:00:00:00:00 000.000.000.000
Enter number

```

この表示の 1 行が 1 つの DHCP エントリです。設定していないところは“0”が表示されています。登録するエントリ番号を指定して設定をおこなって下さい。各エントリには次の項目があります。

```

1) Mac Address 00:00:00:00:00:00
2) Assigned IP address - 000.000.000.000
3) Delete this entry
Enter number

```

それぞれ次の意味を持ちます。

##### 1) Mac Address

クライアントの MAC アドレス (Ethernet Address) を指定します。16 進数で 1 バイトごとにスペースで区切って指定して下さい。

## 2) Assigned IP address

指定した MAC アドレスに割り当てる IP アドレスを指定します。  
ここで割り当てるアドレスは 9) Start Address of the IP address pool と 10) Number of Addresses in the IP address pool で指定した範囲以外のアドレスを割り当ててください。

## 3) Delete this entry

このエントリを削除する際に使用します。

## (3) メインメニューに戻って設定を保存して下さい。

```

General configuration
1) Password
2) TCP/IP
3) DHCP Server(option)
4) SYSLOG LOG message settings(option)
5) Start up(option)
Enter number↓ _____ メインメニューに戻る
Ethernet address : 00806D3B0003
1) General
2) Service Type: CIPL Access Router
3) Service Settings
4) Status
5) Command Line
6) Exit
Enter number 6↓
1) Quit
2) Save configuration & Restart
Enter number 2↓ _____ 保存と再起動を選択
Please Wait

Set up complete !

```

## 5.3.2 DHCP クライアントの設定について

本装置を使用しているセグメント上の Windows95/98/XP のマシンでは、TCP/IP の設定で「IP アドレスを自動的に取得する」を、WindowsNT のマシンでは TCP/IP 設定の「IP アドレス」タブで「DHCP サーバから IP アドレスを取得する」を選択すると、DHCP クライアントになります。DHCP クライアントシステム起動時に DHCP サーバである本装置から IP アドレスなどの設定情報を受け取ります。

DHCP サーバによって割り当てられた IP アドレスは Lease Time で指定された時間の間使用されます。

## 5.4 通信履歴のロギング機能

AS-150/X は、直近の通信履歴のログデータ（日時+アンテナ強度+メッセージ）を最大で 300 件まで本装置内部メモリに格納します。ログデータは AS-150/X のパワーオフによって消滅しますが、システムの（TELNET メニューやコマンドによる）リスタートや、ファームウェアのバージョンアップを行っても消滅しません。

ログデータは Telnet の『show log』コマンドによって以下のように表示されます。

```

1) General
2) Service Type: CIPL Access Router
3) Service Settings
4) Status
5) Command Line
6) Exit
Enter number 5↵
> show log↵
1 1900/01/01 00:00:00 (3) CIPL Access Server AS-150/X system up.
2 1900/01/01 00:00:00 (3) AS-150/X is INITIAL state.
3 1900/01/01 00:00:00 (2) AS-150/X is NULL state.
>

```

↓
↓
↓  
発生日時
電波強度
メッセージ

### (1) 発生日時

事象が発生した日時です。

### (2) 電波強度

メッセージ発生時点の電波強度を以下の数値で表しています。

- (3) : 普通
- (2) : やや弱い
- (1) : 弱い
- (0) : 非常に弱い
- (-1) : 圏外

## (3) メッセージ一覧

通信履歴として格納されるログデータのメッセージとその意味は下表のとおりです。

項番	ログメッセージ	意味
1	CIPL Access Server AS-150/X system up.	AS-150/X が電源投入またはリスタートし、正常に起動した。
2	WM-M200 Power ON sequence failed.	AS-150/X が通信モジュールのパワーオンシーケンスを実行したが、パワーオンに失敗した。
3	WM-M200 Hardware Reset sequence failed.	AS-150/X が通信モジュールのハードウェアリセットシーケンスを実行したが、リセットに失敗した。
4	AS-150/X is INITIAL state.	AS-150/X が INITIAL ステートに達した。
5	WM-M200 does not respond to AT command.	AS-150/X と通信モジュールの同期がとれている状態で、通信モジュールから応答を返らなかった。この場合、AS-150/X はリスタートする。
6	INITIAL state : Timeout ( 1 minutes )	INITIAL ステートが 1 分以上継続したので、リスタートする。
7	AS-150/X is NULL state.	NULL ステート( 待ち受け状態 )に移行した。
8	About to dialout to<ドメイン名>	IP 層から発信要求が来たので発信した。
9	Dialout successfully finished.	発信に成功した。
10	Dialout Failed. : NO CARRIER	発信に失敗した。(NO CARRIER 応答)
11	Dialout Failed. : 60 sec.TIMEOUT	発信に失敗した。(60 秒間応答なし)
12	WM-M200 : DSR = high and CTS = high	通信モジュールに異常を検出したので、INITIAL ステートに戻って初期化をやり直す。
13	SMS received from <ユーザーデータ文字列>	着信を受けた。
14	About to callback to <ユーザーデータ文字列>	着信に対してコールバックを行う。
15	Callback successfully finished.	コールバックに成功した。
16	Callback failed. : NO CARRIER	コールバックに失敗した。(NO CARRIER 応答)
17	Callback failed. : 60 sec. TIMEOUT	コールバックに失敗した。(60 秒間応答なし)
18	PPP link established. IP address = <CIPL インターフェースの IP アドレス>	PPP リンクが確立した。CIPL のインターフェースの IP アドレスは、IPCP によって取得したもので、カスタマーコントロールでモジュールごとに登録したものが払い出されたもの。

19	Dormant state : RI = low	ドーマント状態で、モジュールが RI 信号 low を出力。
20	Dormant state : SMS received from <ドメイン名>	ドーマント状態で、SMS 着信。
21	Dormant state : SMS domain <ドメイン名> is not configured.	SMS データのドメイン名が AS-150/X に設定されていない。
22	Dormant state : failed to read/delete SMS.	SMS データの読み出し/削除に失敗した。
23	PPP link : Inactivity Timeout occurred.	PPP link でインアクティビティタイムアウトが発生したので、AS-150/X は PPP リンクを切断する。
24	PPP link disconnected. : CD = high (physical layer down)	PPP リンクが切断された。モジュールが出力する CD 信号は high。
25	PPP link disconnected : DTR = high	PPP リンクが切断された。AS-150/X は DTR 信号 high を出力する。
26	AS-150/X is TIME-WAIT state.	PPP リンク切断後の時間待ちに移行した。
27	TCP downloader : Firmware Downloaded.	ファームウェアがダウンロードされ、AS-150/X はリスタートする。
28	TELNET : Configuration was saved. Now restarting.....	TELNET の設定データが保存され、リスタートする。
29	Out Of Service T.O	圏外状態が設定した時間経過した。
30	WM-M200 : software reset	通信モジュールをソフトウェアリセットする。
31	Out Of Service T.O : 3 times continuation	項番 29 の圏外タイムアウトが 3 回連続で発生し、その間一度も圏内にならなかった。
32	AS-150/X AUTO REBOOT	定時リブートした。
33	WM-M200 : PS_HOLD = low	通信モジュールがパワーオフ状態になった。
34	UART1 TimeOut.	通信モジュール (UART1) から応答が得られなかった。
35	WM-M200 Software Reset failed.	WM-M200 モジュールをソフトウェアリセットしようとしたが、失敗した。
36	UART2 TimeOut.	通信モジュール (UART2) から応答が得られなかった。
37	NO CARRIER : 8 times continuation	NO CARRIER を 8 回連続で検出した。(その間一度も接続できない場合。)

## 5.5 SYSLOG によるログの転送

本装置はログ情報を外部の Syslog サーバに転送する機能を備えています。ログ転送機能では以下のカテゴリの情報を選択して転送できます。

- 認証  
本装置自身へのログインの成否、本装置を経由したリモートアクセスでのログインの成否といった認証に関するログ情報です。ログインに関するセキュリティ監視に有効です。
- システム  
本装置の設定の変更、起動／再起動、エラーメッセージなど運用に関連したログ情報です。このカテゴリのメッセージは本装置の運用の監視に有効です。
- RS-232  
通信モジュールとの送受信に関するログ情報です。通信モジュールとの動作内容の診断に有効です。
- PPP  
PPP の動作状況に関するログ情報です。PPP の動作内容の診断に有効です。

SYSLOG 転送機能は、上記のログメッセージを UNIX の syslog 形式でホストコンピュータに送信する機能です。この機能を利用するには、syslogd (SYSLOG デーモン) が動作しているホストコンピュータが必要です。

### 5.5.1 AS-150/X 側の設定

SYSLOG ログ転送機能を利用するには、Telnet による初期設定が必要です。Telnet では初期設定のメインメニューから 1) General - 6) SYSLOG LOG message settings を選択し、設定をおこなってください。

General configuration	
1) Password	
2) TCP/IP	
3) DHCP Server(option)	
4) SYSLOG LOG message settings(option)	
5) Start up(option)	
Enter number 4↵	
1) Syslog Server IP Address	000.000.000.000
2) Syslog UDP Port	514
3) Log authorisation messages	NO



4) Log system messages	NO
5) Log RS232C messages	NO
6) Log PPP messages	NO
Enter number	

各項目の内容は次の通りです。

1) Syslog Server IP Address

syslog サーバの IP アドレスを設定して下さい。

2) Syslog UDP Port

syslog サーバの UDP ポート番号を設定して下さい。

通常は工場出荷値（514）のままかまいません。

3) Log authorisation messages

認証の成功・失敗を記録するかどうかを設定して下さい。セキュリティの管理の目的で利用できます。

4) Log system messages

本装置の起動、設定変更、再起動、エラーなどを記録するかどうかを設定して下さい。本装置の運用状況の監視の目的で利用できます。

5) Log RS232 messages

通信モジュールとの通信動作のログを取るかどうかを設定して下さい。

通信状況を診断するのに有効です。

6) Log PPP messages

本装置の PPP 動作のログを取るかどうかを設定して下さい。PPP の動作状態を診断するのに有効です。

### 5.5.2 ホストコンピュータ側の設定

syslog 機能はほとんどの UNIX では標準で使用できます。Windows パソコンの場合はフリーソフトやシェアウェアで利用できるものがあります。本装置は、ホストコンピュータに対して次のような syslog メッセージを送信します。

ログメッセージの種類	facility	level
Log system messages	user	info
Log RS232C messages		
Log PPP messages		
Log authorisation	auth	info

ホストコンピュータはこれらのメッセージを受信するために、`/etc/syslog.conf`を設定し、`syslog` デーモンを起動しなければなりません。`/etc/syslog.conf` の設定例を以下に示します。

【`/etc/syslog.conf` の設定例】

User.*	root	(1)
Auth.*	/var/log/authlog	(2)
*.err;kern.debug;auth.debug;mail.crit;	/dev/console	(3)
*.notice;kern.debug;lpr.info;mail.crit;news.err	/var/log/messages	
mail.info	/var/log/maillog	
cron.*	/var/cron/log	
*.err	root	
*.emerg	*	

- (1) facility が `user` であるすべてのメッセージ（すなわち、本装置の立ち上げ時のメッセージ）を、ユーザ `root` に送るよう設定しています。ユーザ `root` がログインしていれば、メッセージが `root` の画面上に表示されます。
- (2) facility が `auth` であるすべてのメッセージ（すなわち、Telnet 初期設定ログイン成功・失敗）を、`/var/log/authlog` ファイルに記録します。
- (3) `auth.debug` を指定していますが、これは `debug` より上位の `auth` メッセージを `/dev/console` に出力せよ、という意味です。本装置の出すメッセージは `info` レベル（`debug` より上位）なので、`/dev/console` にも出力されます。

`syslog` デーモンを再起動する場合は、UNIX の場合は、`kill` コマンドを使ってデーモンプロセスに `HUP` シグナルを送ります。

`syslog` の詳しい使用方法については、UNIX のマニュアル・ページ（`man syslog.conf`）や、参考書等を参照して下さい。

## 5.6 ステータス表示

メインメニューから 4) Status を選択すると、ステータスメニューが表示されます。

```

1) General
2) Service Type: CIPL Access Router
3) Service Settings
4) Status
5) Command Line
6) Exit
Enter number 4↵

System Up Time 00 day(s) 00:27:49

1) UART1 Status
2) UART2 Status
3) PPP Status
4) Ethernet Status
5) Network Error Log
6) ICMP Log
7) NAT Error Log
8) Log Clear
9) IP Route Table
10) ARP Table
11) System Error Log
12) System Error Log Clear
Enter number

```

System Up Time は、本装置が立ち上がったからの経過時間を表します。49日まで計測できます。49日を越えると、0日に戻ります。ステータスメニューでは、次の各ステータスを見ることができます。

1) UART1 Status、2) UART2 Status の両ステータス情報は、CIPL 通信モジュールとのデータ送受信状態を表します。通常 UART1 Status の DSR は常に on です。

3) PPP Status は、PPP 通信に関する情報です。

上記 1)、2)、3)共に、障害発生時に弊社サポートで障害解析時の参考とします。

### 4) Ethernet Status

●Ethernet Status メニューの先頭には、以下のようにイーサネットリンク状態が表示されます。

Ethernet Link Status : UP (リンク確立) /DOWN (リンク切断)

- [Ethernet receive error] のステータスは、AS-150/X の Ethernet Controller チップがパケット受信時にカウントするエラー（OSI の 7 階層モデルでいうデータリンク層で検出されるエラー）です。

[Frame Length Violation] , [Nonoctet Aligned Frame] , [Short Frame] , [CRC Error] は受信した Ethernet パケットのヘッダ情報と実際のデータが異なること（=パケットが壊れていること）を示します。

[Overrun] はコントローラチップのバッファがいっぱいになり、処理される前に次のパケットが到着した回数を示します。

[Collision] はデータリンク層で検出されたパケットの衝突回数を示すもので、ネットワークが混んでいる場合にカウントアップされます。いずれのデータリンクレベルのエラーも Ethernet Controller チップ内の誤り制御機能によって処理されるため、このレベルでのエラーが直接データ抜けなどに繋がることはありません。

- [Ethernet send error] のステータスは、AS-150/X の Ethernet Controller チップがパケット送信時にカウントするデータリンク層での送信に関するエラーです。

これらのカテゴリのエラーが高い値を示すときは AS-150/X の LAN 側インタフェースの故障や、LAN 回線、ハブ、LAN ケーブルなどのネットワーク機器の不具合の可能性が考えられます。ただし、IP や TCP/UDP のレベルでエラーがカウントされていなければとくに対策を施す必要はありません。

## 5) Network Error Log

IP、TCP、UDP で発生したエラーの数を表示します。

[IP] は IP 層でカウントされるエラーです。IP 層のヘッダやパケットの組み立てに関するエラーです。

[TCP] は TCP のレベルでカウントされるエラーです。再送やチェックサムエラーの原因は過剰なトラフィックなどによって発生することがありますが、これはアプリケーション上は問題ありません。ただし、これも数が多いと TCP よりさらに上位のアプリケーションのレベルでタイムアウトが発生する可能性があります。LAN 内のトラフィックとの相関、IP 層やデータリンク層のエラー発生数との相関を見てどこに問題があるかを切り分けます。

[UDP] は UDP のレベルでカウントされるエラーです。UDP レベルでバッファオーバーフローやチェックサムエラーが起こるとそのデータグラムは捨てられることとなります。アプリケーションで再送がおこなわれれば問題は

ありませんが、そうでない場合はデータ抜けが発生します。LAN内のトラフィックとの相関、IP層やデータリンク層のエラー発生数との相関を見てどこに問題があるかを切り分けます。

#### 6) ICMP Log

ICMPパケットの送受信履歴を表示します。

[ICMP Receive] と [ICMP Send] は ICMP(Internet Control Message Protocol) を使って収集されるステータス情報です。

#### 7) NAT Error Log

IPフレーム送受信処理中にエラーを検出した場合、破棄したパケット数を表示します。

#### 8) Log Clear

ステータスログ、エラー回数をゼロに戻します。ただし、システムエラーログは消去しません。

#### 9) IP Route Table

IPルートテーブルを表示します。

【ルートテーブルの表示例】

Codes: C - connected, P - PPP, S - Static, D - Default route, I - ICMP					
Code	Destination	Metric	Next Hop	TTL	Interface
C	192.9.200.0/24	0	0.0.0.0	0	Ethernet
S	000.000.000.000/0	1	192.168.101.001	0	Ethernet
C	192.9.201.186/32	0	0.0.0.0	0	Port 1

経路の特性を表します表示の意味は次のとおりです。

#### Code

- C : Connected (直接接続)
- P : PPPによる経路
- S : スタティックルート
- I : ICMP Redirectにより更新された経路

#### Destination

経路終点のネットワークアドレス (またはホストアドレス) およびサブネットマスクのビット数を表します。  
000.000.000.000/0 はデフォルトゲートウェイです。

#### Metric

経路終点に到達するまでに経由するルータの数です。

#### Next Hop

Destination に到達するためのゲートウェイ（ルータ）のアドレスです。本機に直接つながっている場合は、“0.0.0.0”と表示されます。

#### TTL (Time To Live)

この経路の有効時間です（単位：秒）。RIP による経路情報は少なくとも 180 秒間はルートテーブルに保存されますが、それ以上経過しても更新されなかった経路は異常と判断され、ルートテーブルから削除されます。

#### Interface

この経路で使用されるインタフェース名です。

### 10) ARP Table

現在の ARP テーブルの内容を表示します。

IP address	Ethernet address
192.168.120.005	0080adba2717
192.168.120.120	000cf1c6dc7d
192.168.120.105	000d871241d1

### 11) System Error Log

本装置で万一、システムエラーが発生すると赤色 [COM] と緑色 [RUN] の両 LED が同期して点滅する状態になり、数秒後に再起動が起こります（\*）。発生したシステムエラーの内容は（タイムスタンプ付きで）装置の不揮発メモリに、上書きで 1 件記録されます。本メニューによりその記録された内容が表示されます。システムエラーが発生していない場合は、“System error message is not logged” と表示されます。また Watchdog リセットが発生した回数が “Number of watchdog resets” で示されます。

(\* ) Watchdog リセットを有効にしていない場合は再起動は起こらず、両 LED が点滅したまま停止状態です。本装置の電源を OFF/ON しない限り復旧しません。

システムエラーは AS-150/X の内部の以下のような事象で発生します。

- ・メモリーエラー
- ・メモリ領域不足
- ・スタックオーバフロー
- ・Null ポインタ参照
- ・不正なパラメータ
- ・その他の予期しないエラー

このような状態が発生する原因としては次の可能性が考えられます。

- ・1. ハードウェアの不具合

- 2. 電源の瞬断、一時的な電圧低下、ノイズなどによる外部要因による誤動作
- 3. ファームウェアの不具合

このうちどれが原因かはエラー状態の発生状況および、再現性の有無によって判断します。

システムエラーログに記録されたメッセージは本装置の電源を OFF/ON しても消去されません。別のシステムエラーが発生するとメッセージは上書きされ、また装置を工場出荷時の状態に初期化すると消去されます。

#### 12) System Error Log Clear

上記システムエラーログとして記録されたメッセージを消去します。

## 5.7 ファームウェアのバージョンアップ

本装置は書換え可能なフラッシュメモリを搭載しており、そこにファームウェア・プログラムを格納しています。ファームウェアのバージョンアップは、LAN 上または CIPL 網経由の遠隔地のどちらからでも、Windows パソコンを使って行うことができます。

バージョンアップを行う Windows パソコンには、本装置付属の Windows ユーティリティ「TCP ダウンローダ」をインストールします。

本装置にあらかじめ Telnet で設定していた内容は、バージョンアップを行っても消失しません。従ってバージョンアップを行う前に設定値を保存する必要はありません。

### ① TCP ダウンローダのインストール

バージョンアップを行う Windows パソコンには、製品に添付の CD-ROM から TCP ダウンローダをインストールして下さい。TCP ダウンローダのディレクトリにある setup.exe を実行するとインストール画面が開きます。画面の指示にしたがってインストールをおこなって下さい。

### ② TCP ダウンローダーを起動します。

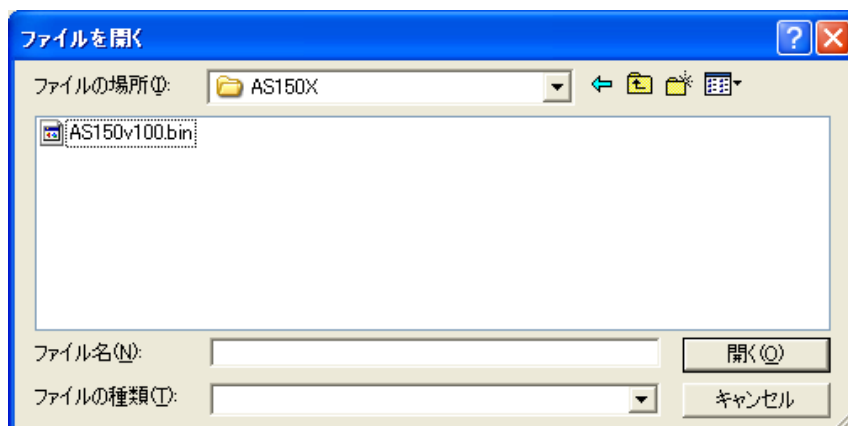
起動すると次の画面が開きます。





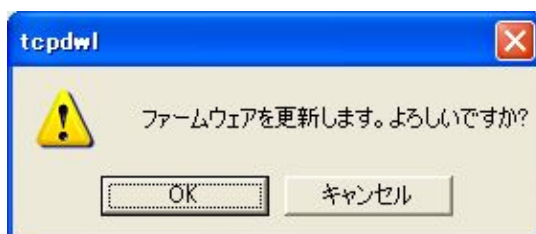
この画面の「ホスト名または IP アドレス」の欄に、本装置の IP アドレスを入力して下さい。Hosts ファイルに本装置のホスト名を登録している場合はホスト名を指定することもできます。ポート番号の値は変更しないで下さい。

- ③ IP アドレスの指定ができれば、[ダウンロード開始] ボタンをクリックします。



ここで入手した新ファームウェアファイルを指定して下さい。

- ④ ファームウェアファイルを選択し、[開く] ボタンをクリックして下さい。装置がダウンロードモードに切り替わります。



- ⑤ [OK] ボタンをクリックすると、ダウンロードを開始します。

進行状況が下のウィンドウに表示されます。



- ⑥ 上のダイアログが出ればダウンロード成功です。



# 第 6 章

## コマンド一覧

AS-150/X に Telnet で接続し、コマンドラインから設定や表示を行う場合に使用するコマンドを記述しています。

## 6.1 制御コマンド

制御コマンドは入力と同時に作用するリアルタイム・コマンドです。

### (1) connect – PPP 回線を接続する

形 式

connect ◀ [<ドメイン番号>]

説 明

PPP 回線を接続する。

<ドメイン番号>	0 ~ 4。 省略可能。省略した場合、ドメイン 0 に対して接続試行する。
----------	--

### (2) disconnect – PPP 回線を切断する

形 式

disconnect

説 明

PPP 回線を切断する。

### (3) factorydefault – 通信モジュールを工場出荷状態に戻す

形 式

factorydefault

説 明

本装置に内蔵している通信モジュールを工場出荷状態に戻す

### (4) help – 使用可能なコマンド一覧を表示する

形 式

help

説 明

コマンドラインで使用できる全コマンドの一覧、及び各コマンド形式を表示する。

### (5) ota – OTA(Over The Air)機能を実行する

形 式

ota ◀<キーワード>

説 明

OTAの起動要求を行い、結果(OTASP1/OTAPA1...OTASP OK等)を表示する。結果はsyslogにも出力する。キーワードとして下記を指定できる。

<キーワード>	意味
sp	OTASP起動要求（利用開始登録）
pa	OTAPA起動要求（解約手続き）

## (6) ping - ping パケットを送出する

形 式

ping [-t] [-n &lt;count&gt;] [-l &lt;size&gt;] [-w &lt;timeout&gt;] &lt;IP アドレス&gt;

説 明

指定されたIPアドレス宛てに1秒間隔でICMP ECHO リクエストを送信し、応答結果を表示する。

-t	ICMP ECHO リクエストをCTRL+C が押下されるまで繰り返し送出する。
-n <count>	<count> としてICMP ECHO リクエストの送出回数を指定する。(1 ~ 99999) -n オプションが指定されない場合のデフォルト値は4回。
-l <size>	<size> としてICMP ECHO のデータサイズをバイト数で指定する。(1 ~ 1448) -l オプションが指定されない場合のデフォルト値は32バイト。
-w <timeout>	<timeout> としてタイムアウト時間をミリ秒単位で指定する。(1000 ~ 99999) -w オプションが指定されない場合のデフォルト値は2秒。
<IPアドレス>	ping送出先のIPアドレスを指定する

応答が返った場合の表示例

```
> ping 192.168.6.2
```

Pinging 192.168.6.2 with 32 bytes of data:

```
Reply from 192.168.6.2: bytes=32 time=4ms seq=1
```

```
Reply from 192.168.6.2: bytes=32 time=4ms seq=1
```

```
Reply from 192.168.6.2: bytes=32 time=4ms seq=1
```

```
Reply from 192.168.6.2: bytes=32 time=4ms seq=1
```

応答がなければ Requested timed out. が表示される。

## (7) show - 各種情報を表示する

形 式

show &lt;キーワード&gt;

説 明

<キーワード>	説明
antenna	現在のアンテナ本数を表示する。 0: 圏外 1: 0本 2: 1本 3: 2本 4: 3本

config	現在設定中のすべての設定値をコマンド形式で表示する。
log [n]	通信履歴のログデータを、古いものから順に最大 n 件表示する。n を省略した場合、最大 300 件表示する。
module	通信モジュール製造番号を表示する。例：8SKKI062620 このコマンドは通信中は使えない。
phone	通信モジュールに登録されている電話番号を表示する。 例：09061925141
rom	ROM 書き問い合わせ番号を通信モジュールに要求し、結果を表示する。例：7060
time	GPS 時刻を表示する。例：2008/07/23 10:26:05

- (8) restart — 設定値の保存と再起動を行う

形 式

restart

説 明

現在の設定値を不揮発メモリに格納し、再起動する。

- (9) quit — コマンドモードを終了する

形 式

quit

説 明

コマンドモードを終了し、Telnet メニューに戻る。

## 6.2 設定コマンド

1つまたは複数の設定コマンドを入力した後、制御コマンド『restart』を入力することで、はじめて設定コマンドが有効になります。

### (1) autoreboot – 定時リブートの設定

形 式

autoreboot <キーワード> <値>

説 明

本装置を定時に定期的に再起動させる設定をする。万一本装置内部で何らかの異常が生じた場合、その内容によっては再起動により復旧される。

<キーワード>	<値>
activate	off : 定時リブート機能を off にする。(工場出荷値) on : 定時リブート機能を on にする。
time	何時にリブートさせるかを設定する (0~23 時)。 (工場出荷値 : 0 時)

### (2) clr – 設定値の初期化

形 式

clr

説 明

設定を工場出荷値に戻す。ただし、自 IP アドレス/マスク値だけは工場出荷値に戻さない。

### (3) dhcp – DHCP サーバの設定

形 式 1

dhcp <キーワード> <値>

形 式 2

dhcp client <エントリ番号> <MAC アドレス> <IP アドレス>

形 式 3

dhcp client <エントリ番号> delete

説 明

本装置を DHCP サーバとして使用する場合に設定する。

<キーワード>	<値>
activate	● off : サーバ機能を off にする。(工場出荷値) ● on : サーバ機能を on にする。
startip	割り当て開始アドレスを設定する。
noofip	割り当てアドレス個数を設定する(1~128)
mask	ネットマスクの値を設定する。

gateway	デフォルトゲートウェイの IP アドレスを設定する。
domain	DHCP で割り当てるドメイン名を設定する（半角英数字 31 文字以内）。
pridns	プライマリ DNS サーバーの IP アドレスを設定する。
secdns	セカンダリ DNS サーバーの IP アドレスを設定する。
leasetime	DHCP で割り当てる IP アドレスのリース時間を設定する（値の範囲=0~9999、単位：時間。0 を設定すると、リース時間無制限（infinite lease）となる）。
wins	DHCP で割り当てる WINS サーバアドレスを設定する。

2番目の形式：最大128台まで固定IPの割り当てが可能。

<エントリ番号>	0~127 (Telnet メニューでは 1~128)
<MAC アドレス>	対称器機の MAC アドレスを 16 進数 12 桁で指定する。
<IP アドレス>	割り振る IP アドレスを *.*.*.* の形式で指定する。

3番目の形式：割り当てを削除する。

<エントリ番号>	0~127
----------	-------

#### (4) dnsrelay – DNS リレーの設定

形 式

dnsrelay activate <値>

説 明

DNS リレー機能の有効/無効を設定する。（「3.4 インターネット接続と DNS リレー機能」参照）

<値>	off : DNS リレー機能を off にする。（工場出荷値） on : DNS リレー機能を on にする。
-----	---

#### (5) domain – ドメイン・コンフィグレーション・テーブルの設定

形 式 1

domain <ドメイン番号> <ドメイン名> <ユーザー名> <パスワード> <自動発呼先アドレス/マスク> <メトリック>

形 式 2 （テーブルを削除する場合）

domain <ドメイン番号> delete

説 明

ドメイン管理テーブルを設定する。（「3.1.1 ドメイン管理情報」参照）

<ドメイン番号>	0 ~ 4 （Telnet メニューでは 1~5）
<ドメイン名>	半角英小文字、数字、ピリオド、ハイフンのみで 2~20 文字。ただし、ピリオドおよびハイフンは先頭および末尾にあってはならない。
<ユーザー名>	半角数字「0~9」、半角英文字「a~z、A~Z」で 1~65 文字。
<パスワード>	半角数字「0~9」、半角英文字「a~z、A~Z」で 1~32 文字。



<自動発呼先アドレス/マスク>	自動発呼のトリガとする IP パケットの宛先アドレス/マスクを指定する。例：“192.168.1.0/24”。 0.0.0.0/0 の場合は全てのパケットを対象とする。
<メトリック>	1～15。

2番目の形式：

<ドメイン番号>	<ドメイン番号>で削除するテーブルを指定する。
----------	-------------------------

#### (6) filter — IP フィルタの設定

形 式 1

```
filter <number> <type> <dir> <srcaddr> <dstaddr> <protocol> <srcport> <dstport> <interface>
```

形 式 2 (テーブルを削除する場合)

```
filter <number> delete
```

説 明

パケットフィルタ機能の設定をおこなう。パラメータは省略できない。  
(「5.2 パケットフィルタ機能」参照)

<number>	フィルタ番号を 0～31 で指定する。(Telnet メニューでは 1～32)
<type>	フィルタタイプを指定する。 pass：一致すれば通す。 reject：一致すれば破棄する。
<dir>	指定した方向のパケットをフィルタリングの対象とする。 in：受信パケットをフィルタリングする。 out：送信パケットをフィルタリングする。
<srcaddr>	IP アドレス、または IP アドレスの範囲を指定する。この送信元 IP アドレスを持つパケットをフィルタの対象とする。 ● アドレスを単独で指定する場合 [IP アドレス/マスクビット数] ● アドレスの範囲を指定する場合 [アドレス始点:アドレス終点] ● すべての送信元を対象とする場合 “*” と書く。
<dstaddr>	IP アドレス、または IP アドレスの範囲を指定する。この送信先 IP アドレスを持つパケットをフィルタの対象とする。 ● アドレスを単独で指定する場合 [IP アドレス/マスクビット数] ● アドレスの範囲を指定する場合 [アドレス始点:アドレス終点] ● すべての送信先を対象とする場合 “*” と書く。
<protocol>	プロトコル番号 (1～254)、またはニーモニック 指定した種類のプロトコルをフィルタリングの対象とする。ニ

	一モニックは、次のものが指定できる。 udp, tcp, tpest, tcpfin, icmp, * (全てのプロトコル)
<srcport>	送信元ポート番号 (1~65534) を指定する。この送信元ポート番号を持つパケットをフィルタの対象とする。 ● 特定のポートを指定する場合 ポート番号、または一モニックを記述する。 ● ポートの範囲を指定する場合 [送信元ポート番号始点:送信元ポート番号終点] ● すべての送信元ポートを対象とする場合 “*”と書く。
<dstport>	送信先ポート番号 (1~65534) を指定する。この送信先ポート番号を持つパケットをフィルタの対象とする。 ● 特定のポートを指定する場合 ポート番号、または一モニックを記述する。 ● ポート範囲指定する場合 [送信先ポート番号始点:送信先ポート番号終点] ● すべての送信先ポートを対象とする場合 “*”と書く。
<interface>	接続インターフェース。ppp1 と書く。

2番目の形式：

<number>	削除するフィルタをフィルタ番号を 0~31 で指定する
----------	-----------------------------

■ 参考：一モニックとプロトコル番号／ポート番号の一覧表

一モニック	プロトコル番号
icmp	1
tcp	6
udp	17
tpest	254
tcpfin	254

一モニック	ポート番号
ftpdata	20
ftp	21
telnet	23
smtp	25
domain	53
www	80
pop3	110
sunrpc	111
nntp	119
ntp	123
login	513
route	520

(7) flag — 本装置のスタートアップに関する設定

形式

flag □<キーワード> □<値>

説明

wd の on/off 指定だけは他の設定コマンドと異なり、コマンド入力時点で設定保存される。ただし動作に反映されるのは本装置の電源入れ直し後となる。

<キーワード>	<値>
wd	on : ウォッチドッグ・リセット機能を有効にする。 off : ウォッチドッグ・リセット機能を無効にする。 この変更は直ちに不揮発メモリに保存する。
menutimeout	telnet の無通信切断タイマの秒数を記述する (0 及び 60~99999999、0 のときタイムアウトなし)

## (8) interface — ドメインのインタフェースの設定

形 式

interface ◁ドメイン番号&gt; ◁IP パケット変換方法&gt; ◁IP アドレス&gt;

説 明

AS-150/X とセンタとの IP 通信における IP パケットの変換方法をドメイン毎に設定する。

<ドメイン番号>	ドメイン番号を、0 から 4 で指定する。
<IP パケット変換方法>	nat : Network Address Translation gre : General Routing Encapsulation
<IP アドレス>	IP パケット変換方法で"gre"を指定した場合に、GRE トンネリングの終点 IP アドレスを指定する。

## (9) main — 本装置の基本情報の設定

形 式

main ◁キーワード&gt; ◁値&gt;

説 明

本装置自身の IP アドレス、ネットマスク、デフォルトルータ、パスワード、といった基本情報を設定する。

<キーワード>	<値>
ip	本装置のイーサネットインタフェースの IP アドレス。
mask	上記 IP アドレスのサブネットマスク値
gateway	LAN 側にデフォルトルータを設ける場合は、その IP アドレスを設定する。
password	Telnet ログイン時の管理者パスワードを設定する。使用可能な文字は、半角英数記号 0~15 文字 (工場出荷値 "system")
packetforwarding	発信のトリガとなったパケットを送信するか(on)、破棄するか(off)の指定。on の場合、トリガとなったパケット、及び発信中に LAN から受信した最大 10 パケットをバッファリングする。発信成功後バッファリングしたパケットを送信する。"redial"回数を越えて PPP 接続に失敗の場合は廃棄する。 off : 破棄する (工場出荷値) on : 送信する

## (10) nat - NAT コンフィグレーション・テーブルの設定

## 形式 1

```
nat <エン트리番号> <プライベート IP アドレス> <プロトコル> <ポート>
    <グローバル IP アドレス> [<WAN 側からのアクセスポート>]
```

## 形式 2 (テーブルを削除する場合)

```
nat <エン트리番号> delete
```

## 説明

NAT コンフィグレーションテーブルを設定する。

<エン트리番号>	0 ~ 47 (Telnet メニューでは 1~48)
<プライベート IP アドレス>	次の 3 つの形式が入力可能。 <ul style="list-style-type: none"> <li>● 単一アドレス指定 例：“192.168.0.1”</li> <li>● アドレス範囲指定 (始点：終点) 例：“192.168.0.1:192.168.0.254”</li> <li>● すべてのプライベート IP アドレスを対象とする “*” (PAT エン트리)</li> </ul>
<プロトコル>	プロトコル番号(1~254)、またはニーモニック。次の 3 つの形式が入力可能。 <ul style="list-style-type: none"> <li>● 単一プロトコル番号指定 例：“80”</li> <li>● ニーモニック単一指定 (icmp,tcp,tcpst,tcpfin,udp) 例：“tcp”</li> <li>● すべてのプロトコルを対象とする “*”</li> </ul>
<ポート>	TCP/UDP ポート番号(1~65535)、またはニーモニック。次の 3 つの形式が入力可能。ただし、PAT エントリの場合はこの設定は無視される。 <ul style="list-style-type: none"> <li>● 単一ポート番号指定 例：“21”</li> <li>● ニーモニック単一指定 (ftp, ftpdata, telnet, smtp,www, pop3, sunrpc, nntp, ntp, login, domain, route, pptp) 例：“ftp”</li> <li>● ポート範囲指定 (始点：終点) 例：“0:12287”</li> <li>● すべてのポートを対象とする “*”</li> </ul>
<グローバル IP アドレス>	“ipcp”を指定する。
<WAN 側からのアクセスポート>	WAN 側から LAN 側の機器にアクセスする際のポート番号を設定する。(1~65535) この項目は NAT エントリの場合のみ有効となる。 WAN 側からのアクセスポートが LAN 側機器のポートと同じ場合は省略できる。

2番目の形式：

<エン트리番号>	エン트리番号で指定されたテーブルを削除する。
----------	------------------------

## (11) oosreset - 圏外定時間リセットの設定

形 式

oosreset &lt;キーワード&gt; &lt;値&gt;

説 明

電波の受信状態が圏外のまま一定時間継続した場合に通信モジュールをソフトウェアリセットする。

<キーワード>	<値>
activate	off : 圏外定時間リセット機能を off にする。 on : 圏外定時間リセット機能を on にする。(工場出荷値)
time	圏外が何分継続でリセットさせるかを設定する (1~10 分)。 (工場出荷値 : 3 分)

## (12) packetspeed - 無線パケットデータ通信速度の設定

形 式

packetspeed ⊣ &lt;キーワード&gt;

説 明

契約のサービスに従い無線パケットデータ通信速度を設定する。キーワードとして下記を指定できる。

<キーワード>	意味
low	低速 (上り 14.4kbps、下り 14.4kbps)
high	高速 (上り 64kbps、下り 144kbps) (工場出荷値)

## (13) pingkeepalive - CIPL 回線接続維持に関する設定

形 式

pingkeepalive ⊣ &lt;enable/disable&gt; ⊣ &lt;destination&gt; ⊣ &lt;timeout&gt;

説 明

PPP 接続中、CIPL 網接続を維持するため定期的に Ping (ICMP echo) を送信する。

<enable/disable>	enable : Ping キープアライブを行う disable : Ping パケットの送出は行わない
<destination>	<IP アドレス> : Ping 送出先の IP アドレスを指定する 例 : 192.168.101.69
<timeout>	30~4294967 秒で Ping 送出の間隔を指定する

## (14) ppp\_interval - PPP 切断後の待ち時間設定

形 式

ppp\_interval ⊣ &lt;秒数&gt;

説 明

PPP 切断後、再び発信/着信できるようになるまでの秒数を設定する。

<秒数>	0~1000。工場出荷値は 10。
------	-------------------

## (15) route — スタティックルートの設定

形 式 1

route &lt;テーブル番号&gt; &lt;宛先アドレス/マスク&gt; &lt;ゲートウェイ&gt; &lt;メトリック&gt;

形 式 2 (テーブルを削除する場合)

route &lt;テーブル番号&gt; delete

説 明

本装置のスタティック・ルーティング・テーブルの設定をおこなう。LAN 側に対して有効。他のルータを経由してアクセスをおこなう場合にその経路情報を登録する。これによって異なるネットワークからでも本装置がアクセスできるようになる。ルータ越えでインターネット接続する場合は、デフォルトルートではなくこのスタティックルートを使う。

<テーブル番号>	0 から 29 を指定する。(Telnet メニューでは 1~30)
<宛先アドレス/マスク>	単一ホストの IP アドレス、または宛先ネットワークのネットワーク番号、またはサブネットワーク番号を、IP アドレスとマスクビットで指定する。例：192.168.1.0/24
<ゲートウェイ>	宛先ネットワークに到達するために経由する最初のゲートウェイの IP アドレス。0 を設定することはできない。
<メトリック>	宛先ネットワークまでのホップ数。0~15 までの数値。

2番目の形式：

<テーブル番号>	削除するルートを<テーブル番号>で指定する。
----------	------------------------

## (16) rsport — PPP インアクティビティタイマ値の設定

形 式

rsport 0 inactivitytimer &lt;値&gt;

説 明

<値>には PPP インアクティビティタイマ値を秒単位で指定する。0 秒はタイムアウト無しの設定。

## (17) syslog — SYSLOG 機能の設定

形 式 1

syslog &lt;キーワード&gt; &lt;値&gt;

形 式 2

syslog option &lt;キーワード&gt; &lt;on/off&gt;

説 明

本装置の各種ログ情報を SYSLOG サーバー (デーモン) に転送する場合に設定する。

<キーワード>	<値>
ipaddress	SYSLOG サーバーの IP アドレス。「0.0.0.0」は、SYSLOG 機能を使わないことを意味する。
port	SYSLOG サーバーの UDP ポート番号。通常は 514。

2番目の形式：

<キーワード>	< on/off >
system	off : システムログは取らない on : システムログを取る
rs232c	off : 通信モジュールに関するログは取らない on : 通信モジュールに関するログを取る
auth	off : 認証に関するログは取らない on : 認証に関するログを取る
ppp	off : PPP の動作状況に関するログは取らない on : PPP の動作状況に関するログを取る

(18) vjcompression - VJ 圧縮の設定

形 式

vjcompression □<キーワード> □<値>

説 明

VJ 圧縮機能は TCP/IP ヘッダーを圧縮して転送効率を向上させる。あらかじめ相手側が対応していないと分かっている場合は、off 設定にしてネゴシエーション・パケットを流さないこともできる。

<キーワード>	<値>
activate	off : VJ 圧縮機能を off にする。 on : VJ 圧縮機能を on にする。(工場出荷値)





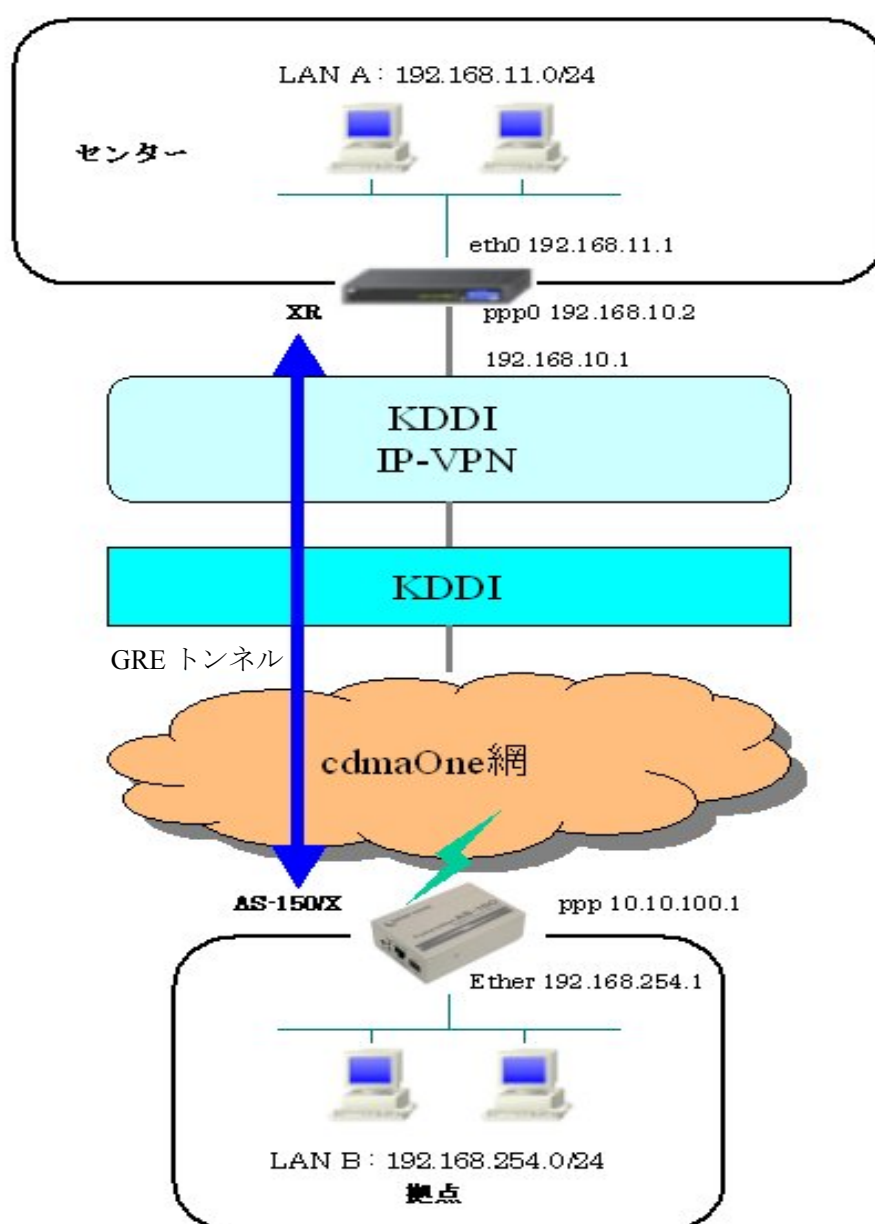
# 第7章

参考資料

## 7.1 XR ルータとの GRE 拠点間通信設定例

この例は、FutureNet AS-150/X の GRE トンネリング機能を利用し、XR <-> AS-150/X 間で通信を行う設定例です。これにより AS-150/X 側で NAT を利用せずに配下の装置へのアクセスが可能になります。

### (1) 構成例



## (2) 要件

## ➤ インタフェースおよび PPP/PPPoE

- XR では専用線接続の設定を行っています。
- AS-150/X では CIPL 網に接続するための設定を行います。

主なインタフェースおよび PPP/PPPoE のパラメータ

	XR	AS-150/X
LAN 側インタフェース	Ether0	Ether
LAN 側 IP アドレス	192.168.11.1	192.168.254.1
WAN 側インタフェース	ppp0	ppp
WAN 側 IP アドレス	192.168.10.2	ipcp で取得

## ➤ GRE

- XR のインタフェースアドレスを GRE1 は「172.16.0.1」と設定しています。

主な GRE のパラメータ

	XR	AS-150/X
対向拠点	AS-150/X	XR
インタフェースアドレス	172.16.0.1/30	-
リモート(宛先)アドレス	10.10.100.1	192.168.10.2
ローカル(送信元)アドレス	192.168.10.2	-
PEER アドレス	172.16.0.2/30	-
MTU	1476	-
MSS 設定[MSS 値]	有効[0]	-

## ➤ その他

- スタティックルート設定で AS-150/X 配下の LAN へのルートをスタティックルートでインタフェース「gre1」で設定しています。

## (3) 設定例

## ■ XR (センタルータ) 側の設定

ポイント : AS-150/X と GRE トンネリングによる接続を行います。また IP-VPN 網に接続するための専用線設定も行っています。

## &lt;&lt;インタフェース設定&gt;&gt;

## [Ethernet0 の設定]

IP アドレスに「192.168.11.1」を設定します。

※IP アドレスの設定を変更した場合、即設定が反映されます。

<input checked="" type="radio"/> 固定アドレスで使用
IP アドレス <input type="text" value="192.168.11.1"/>
ネットマスク <input type="text" value="255.255.255.0"/>
MTU <input type="text" value="1500"/>

## &lt;&lt;PPP/PPPoE 設定&gt;&gt;

## [専用線設定]

専用線を利用するため、本装置の IP アドレスおよび接続先の IP アドレスを設定します。

プロバイダ名	<input type="text" value="CIPL"/>
<b>専用線設定</b>	
本装置のIPアドレス	<input type="text" value="192.168.10.2"/>
接続先のIPアドレス	<input type="text" value="192.168.10.1"/>

## [接続設定]

接続ポートとして「Leased Line(128K)」を選択しています。

接続先の選択	<input checked="" type="radio"/> 接続先1 <input type="radio"/> 接続先2 <input type="radio"/> 接続先3 <input type="radio"/> 接続先4 <input type="radio"/> 接続先5
接続ポート	<input type="radio"/> Ether0 <input type="radio"/> Ether1 <input type="radio"/> Ether2 <input type="radio"/> BRI(64K) <input type="radio"/> BRI MP(128K) <input type="radio"/> Leased Line(64K) <input checked="" type="radio"/> Leased Line(128K) <input type="radio"/> RS232C
接続形態	<input type="radio"/> 手動接続 <input checked="" type="radio"/> 常時接続 <input type="radio"/> スケジューラ接続
RS232C/BRI接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続
IPマスカレード	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
ステータフルパケット インスペクション	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効 <input type="checkbox"/> DROPしたパケットのLOGを取得
デフォルトルートの設定	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効

## &lt;&lt;GRE 設定&gt;&gt;

## [GRE1 設定]

AS-150/X との GRE トンネルを設定します。

インタフェースアドレス	172.16.0.1/30 (例:192.168.0.1/30)
リモート(宛先)アドレス	10.10.100.1 (例:192.168.1.1)
ローカル(送信元)アドレス	192.168.10.2 (例:192.168.2.1)
PEERアドレス	172.16.0.2/30 (例:192.168.0.2/30)
TTL	255 (1-255)
MTU	1476 (最大値 1500)
Path MTU Discovery	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効

MSS 設定を「有効」にしています。

MSS設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効 MSS値 0 Byte (有効時にMSS値が0の場合は、MSS値を自動設定(Clamp MSS to MTU)します。)
-------	---

## &lt;&lt;スタティックルート設定&gt;&gt;

AS-150/X 配下の LAN への通信が GRE トンネルを通るようにインタフェース「gre1」でスタティックルートを設定しています。

アドレス	ネットマスク	インターフェース/ゲートウェイ	ディスタンス <1-255>
192.168.254.0	255.255.255.0	gre1	1

※XR ルータの設定方法の詳細は各ユーザーズガイドをご参照下さい。

## ■ AS-150/X（拠点ルータ）側の設定

ポイント：XR と GRE トンネリングによる接続を行います。

```

    }
    5) Command Line
    6) Exit
    Enter number 5↵
> show config↵      解説：現在の設定内容を表示させる
main ip 192.168.254.1
main mask 255.255.255.0
domain 0 1.example test testpass 192.168.11.0/24 1
interface 0 gre 192.168.10.2
dhcp activate off
>
  
```

<解説>

```
main↵ip↵192.168.254.1
main↵mask↵255.255.255.0
```

AS-150/X の Ethernet ポートの IP アドレス、ネットマスクを設定します。

```
domain↵0↵1.example↵test↵testpass↵192.168.11.0/24↵1
```

ドメイン管理テーブルを設定します。

ドメイン番号：0（ドメイン番号は0～4で表示されます）

ドメイン名：1.example

ユーザ名：test

パスワード：testpass

自動発呼先アドレス/ネットマスク：192.168.11.0/24

メトリック：1

```
interface↵0↵gre↵192.168.10.2
```

AS-150/X とセンタ(XR)との IP 通信における IP パケットの変換方法を設定します。

ドメイン番号：0（ドメイン番号は0～4で表示されます）

IP パケット変換方法：gre

GRE トンネルの終点 IP アドレス：192.168.10.2

```
dhcp↵activate↵off
```

DHCP サーバ機能は無効を表しています。（デフォルト）

## 7.2 AS-150/X 仕様一覧

LAN 側 インタフェース	Fast Ethernet インタフェース	10BASE-T/100BASE-TX x 1 ポート Auto MDI/MDI-X、コネクタ RJ-45
WAN 側 インタフェース	対応回線	KDDI CDMA 1X 最大通信速度 下り 144kbps/上り 64kbps ※ ベストエフォート
ネットワーク機能	搭載プロトコル	PPP、IPCP、IP、ICMP、TCP、UDP、Telnet、DHCP、SYSLOG、ARP、 GRE、SNTP
	ルーティング	スタティックルート、デフォルトルート、パケットフィルタ
	NAT/PAT	送信元 NAT 対応
	GRE カプセル化	FutureNet XR ルータ互換
	DHCP サーバ	最大 128 台
CIPL 接続	ドメイン登録数	最大 5 個
	発信	宛先 IP アドレスによりドメインを切り替え
	着信	(センター起動) 接続元 IP アドレスによりドメインを切り替え
OTA 機能	OTASP (回線契約)	本体 OTA ボタン/設定画面からの操作
	OTAPA (回線解約)	設定画面からの操作
運用管理	設定手段	telnet 接続によるコマンドラインインタフェース
	ファームウェア 更新	専用ソフトウェアからネットワーク経由で可能
	回線維持機能	ping keepalive 機能
	ログ機能	システムログ/ Syslog で送信、通信履歴をメモリに保存/遠隔から参照
	診断機能	電波強度表示 LED、PPP リンク状態表示 LED、 ping による疎通確認、ログ情報表示、ステータス表示
	その他	SNTP (Simple Network Time Protocol) サーバ
認定/準拠	VCCI	Class A 準拠
サイズ・重量	外観寸法	90mm(W) × 62mm(D) × 28mm(H) ※ 突起物を除く
	重量	本体:約 260g、AC アダプタ: 120g
環境	使用電源、 電源形状	DC5V±5% 2A AC アダプター(入力 AC 100V±10% 50~60Hz、平行 2 ピン)
	消費電力	最大 6W
	動作環境条件	-20°C~60°C(AC アダプタを除く)、25%~85%(結露なきこと)
	保存温度	-30~60°C、25~90%(結露なきこと)
添付品		CD(取扱説明書含む)、AC アダプタ、保証書、ゴム足

FutureNet AS-150/X CDMA 1X モバイルアクセスルータ  
ユーザーズマニュアル

---

2009年 1月 6日第3版

発行 センチュリー・システムズ株式会社

Copyright(c) Century Systems Co., Ltd. 2008

---

東京都 武蔵野市 境 1-15-14 宍戸ビル 〒180-0022  
Tel. 0422-37-8911 Fax. 0422-55-3373  
<http://www.centurysys.co.jp/>