

「auひかり ビジネス」 アダプター利用マニュアル

【NT-4e】

1.3 版

2018年7月

ご使用の前に

この取扱説明書には、製品を安全に正しくお使いいただき、お使いになる方やほかの人々への危害や財産への損害を未然に防ぐために、重要な注意事項を記載しています。

注意事項は、取り扱いを誤った場合に発生が想定される危害や損害の程度を次の通り「警告」「注意」の2つに分類しています。内容をよく理解してから本文をお読みください。

■絵表示について

 警告	この表示を無視して、誤った取り扱いをすると、人が死亡または重傷を負う可能性が想定される内容を示しています。
 注意	この表示を無視して、誤った取り扱いをすると、人が傷害を負う可能性が想定される内容および物的損害のみの発生が想定される内容を示しています。

■絵表示の例

	△記号は注意(警告も含む)を促す内容であることを告げるものです。 (左図の場合は「感電注意」です。)
	○記号は禁止の行為であることを告げるものです。 (左図の場合は「分解禁止」です。)
 	●記号は行為を強制や指示する内容を告げるものです。 (左図、左は「電源プラグをコンセントから抜け」、右は「必ず実施」です。)

- この装置は、情報処理装置など電波妨害自主規制協議会(VCCI)の基準に基づくクラス 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。
- 本製品の故障、誤動作、不具合、あるいは停電などの外部要因によって生じた損害などの纯粹経済損害につきましては、当社は一切その責任をおいかねますので、あらかじめご了承ください。本製品の設置には、工事担任者資格を必要とする場合があります。無資格者の工事は違法となり、また事故のもととなりますので絶対におやめください。
- 本書を紛失または損傷したときは、販売店にてお求めください。
- 製品に関する保証範囲は故障修理に限られるものとします。
よって、故障により生じたその他の損害についての責任は負いません。

安全のために必ずお守りください

■異常時の処置について



	●万一、内部に水などが入った場合は、電源プラグをコンセントから抜いて販売店にご連絡ください。そのまま使用すると火災・感電・故障の原因となります。
	●万一、内部に異物が入った場合は、電源プラグをコンセントから抜いて販売店にご連絡ください。そのまま使用すると火災・感電・故障の原因となります。
	●万一、本装置を落としたり、ケースを破損した場合は、電源プラグをコンセントから抜いて、販売店にご連絡ください。そのまま使用すると火災・感電・故障の原因となります。
	●電源コードが傷んだら(芯線の露出、断線など)販売店に交換をご依頼ください。そのまま使用すると火災・感電の原因となります。
	●万一、煙が出ている、異臭がするなどの異常状態のまま使用すると、火災・感電・故障の原因となります。その後必ず電源プラグをコンセントから抜き、煙が出なくなるのを確認して販売店に修理をご依頼ください。お客さまによる修理は危険ですから絶対おやめください。

■取り扱いについて

警告

	●本装置に水が入ったりしないよう、また濡らさないようご注意ください。火災・感電・故障の原因となります。
	●本装置の上や近くに花びん、植木鉢、コップ、化粧品、薬品や水などの入った容器または小さな金属物を置かないでください。こぼれたり、装置内に入った場合、火災・感電・故障の原因となります。
	●すきまから内部に金属類を差し込んだり、落としたりしないでください。火災・感電・故障の原因となります。
	●本装置を分解・改造しないでください。火災・感電・故障の原因となります。
	●本装置のケースを外さないでください。電源部や内部に触れると火傷、感電の原因となります。
	●濡れた手で本装置を操作しないでください。火災・感電・故障の原因となります。

注意

	●本装置の各接続コネクタに規定以上の電圧がかからないようにしてください。火災・感電・故障の原因となります。
	●本装置の通風孔をふさがないでください。通風孔をふさぐと内部に熱がこもり火災の原因となることがあります。
	●移動する場合は、電源プラグをコンセントから外し、回線コードなど外部の接続線を外したことを確認の上、行ってください。コードが傷つき、火災・感電の原因となることがあります。
	●アース端子は必ずアースへ接続してください。感電の原因となることがあります。

■電源について

警告

	●表示された電源電圧以外の電圧で使用しないでください。火災・感電・故障の原因となります。
	●電源プラグはコンセントに確実に差し込んでください。電源プラグの刃に金属などが触れると火災・感電・故障の原因となります。
	●濡れた手で電源プラグを抜き差ししないでください。感電の原因となります。
	●タコ足配線はしないでください。火災・過熱の原因となります。
	●近くに雷が発生したときは、電源プラグや接続ケーブルなどを抜いてご使用をお控えください。雷によっては、火災・感電・故障の原因となります。
	●電源コードを傷つけたり、破損したり、加工したり、無理にまげたり、ねじったりしないでください。重いものをのせたり、加熱したり、引っぱったりすると電源コードが破損し、火災・感電・故障の原因となります。
	●電源アダプターは、必ず付属のものを使用し、それ以外のものは絶対にお使いにならないでください。火災・感電・故障の原因となります。
	●電源プラグは、ほこりが付着していないことを確認してからコンセントに差し込んでください。また、定期的に電源プラグをコンセントから抜いて点検・清掃をしてください。ほこりにより、火災・感電の原因となることがあります。

注意

	●電源プラグを抜くときは、必ずプラグを持って抜いてください。電源コードを引っ張るとコードが傷ついて火災・感電・故障の原因となることがあります。
	●電源コードを熱器具に近づけないでください。コードの被覆がとけて、火災・感電の原因となります。

■設置場所について



	●直射日光のあたるところや温度の高いところに置かないでください。内部の温度があがり、火災の原因になることがあります。
	●湿気やほこりの多い場所に置かないでください。火災・感電・故障の原因となることがあります。
	●調理台や加湿器のそばなど油煙や湯気が当たるような場所には置かないでください。火災・感電・故障の原因となることがあります。
	●ぐらついた台の上や傾いた所など不安定な場所に置かないでください。落ちたり、倒れたりして、けがの原因になることがあります。
	●振動・衝撃の多い場所には置かないでください。落ちたり、倒れたりして、けがの原因となることがあります。
	●腐食性ガス・引火性ガスが発生する場所には設置しないでください。 また、空気中塩分濃度の高い場所や塩水のかかる場所には設置しないでください。故障の原因となることがあります。
	●屋外には設置しないでください。屋外に設置した場合の動作保証はいたしません。

- テレビジョン、ラジオ、スピーカボックスなどの磁気を帯びているところや電磁波が発生しているところには置かないでください。正常に動作しないことがあります。
- 製氷庫の中など、特に温度が下がるところに置かないでください。正常に動作しないことがあります。

- 目次 -

1	はじめに.....	- 8 -
1.1	本マニュアルについて.....	- 8 -
1.2	用語の説明.....	- 8 -
1.3	製品のサポートについて.....	- 8 -
2	アダプターについて.....	- 9 -
2.1	機能概要.....	- 9 -
2.2	ネットワーク構成について.....	- 10 -
2.2.1	WAN セグメント.....	- 11 -
2.2.2	インターネットセグメント.....	- 12 -
2.2.3	LAN セグメント.....	- 13 -
2.2.4	仮想 DMZ セグメント.....	- 13 -
2.3	システム構成について.....	- 14 -
2.3.1	接続ケース 1.....	- 15 -
2.3.2	接続ケース 2.....	- 16 -
2.3.3	接続ケース 3.....	- 17 -
2.3.4	ケース毎のセグメントの状況.....	- 18 -
3	設置について.....	- 19 -
3.1	機器の説明.....	- 19 -
3.1.1	機器の外観と添付品.....	- 19 -
3.1.2	各部の名称と機能.....	- 22 -
3.1.3	ランプとボタン・スイッチの機能.....	- 25 -
3.1.4	LAN/WAN 配線用 UTP ケーブルについて.....	- 26 -
3.1.5	設置.....	- 27 -
3.2	接続について.....	- 29 -
3.2.1	WAN の接続.....	- 29 -
3.2.2	LAN の接続.....	- 30 -
3.2.3	FG の接続.....	- 31 -
3.2.4	電源の接続.....	- 32 -
3.2.5	電源の投入と電源投入後のランプ表示.....	- 33 -
4	設定編.....	- 34 -
4.1	設定概要.....	- 34 -
4.1.1	設定方法について.....	- 34 -
4.1.2	設定のための準備.....	- 35 -
4.1.3	設定画面の URL について.....	- 43 -
4.1.4	設定画面メニュー.....	- 44 -
4.2	構成情報設定.....	- 46 -
4.2.1	ネットワーク設定 - LAN 接続設定.....	- 46 -
4.2.2	ネットワーク設定 - ポート設定.....	- 48 -
4.2.3	ネットワーク設定 - SPI 設定.....	- 50 -
4.2.4	ネットワーク設定 - セキュリティ設定.....	- 51 -
4.2.5	ネットワーク設定 - パケットフィルタ設定.....	- 54 -
4.2.6	ネットワーク設定 - URL フィルタ設定.....	- 58 -
4.2.7	ネットワーク設定 - 静的 IP マスカレード設定.....	- 61 -
4.2.8	ネットワーク設定 - 静的 NAT 設定.....	- 64 -
4.2.9	ネットワーク設定 - LAN 側ルーティング設定.....	- 67 -
4.2.10	ネットワーク設定 - 高度な設定.....	- 69 -

4.3	情報表示	- 72 -
4.3.1	装置状態表示	- 72 -
4.3.2	UPnP 状態表示	- 74 -
4.3.3	LAN 側自動払い出し状況表示	- 75 -
4.3.4	ログ表示	- 76 -
4.3.5	統計情報	- 78 -
4.4	メンテナンス	- 85 -
4.4.1	疎通確認(PING)	- 85 -
4.4.2	メンテナンス - ログインパスワード変更	- 86 -
4.4.3	メンテナンス - 装置設定の保存/復元	- 87 -
4.4.4	メンテナンス - 装置再起動	- 88 -
5	機器仕様編	- 89 -
5.1	方式諸元	- 89 -
5.1.1	ハードウェア諸元	- 89 -
5.1.2	ソフトウェア諸元	- 90 -
5.2	サービス機能	- 91 -
5.2.1	サービス機能一覧	- 91 -
5.2.2	サービス機能詳細 - ネットワーク機能	- 93 -
5.3	構成情報一覧	- 116 -
5.3.1	ネットワーク設定 - LAN 接続設定	- 116 -
5.3.2	ネットワーク設定 - ポート設定	- 116 -
5.3.3	ネットワーク設定 - SPI 設定	- 116 -
5.3.4	ネットワーク設定 - セキュリティ設定	- 117 -
5.3.5	ネットワーク設定 - パケットフィルタ設定	- 117 -
5.3.6	ネットワーク設定 - URL フィルタ設定	- 118 -
5.3.7	ネットワーク設定 - 静的 IP マスカレード設定	- 118 -
5.3.8	ネットワーク設定 - 静的 NAT 設定	- 118 -
5.3.9	ネットワーク設定 - LAN 側ルーティング設定	- 119 -
5.3.10	ネットワーク設定 - 高度な設定	- 119 -
5.4	制約事項	- 119 -
6	動作切り分け	- 120 -
6.1	動作切り分けフロー	- 120 -
6.1.1	POWER ランプ消灯の場合	- 121 -
6.1.2	INIT ランプ点灯の場合	- 122 -
6.1.3	WAN ACT ランプ消灯の場合	- 122 -
6.1.4	インターネットに接続できない場合	- 123 -

1 はじめに

1.1 本マニュアルについて

本マニュアルは、「auひかり ビジネス」(KDDIが提供するインターネットアクセスサービス)に提供されるアダプター(DSUとお客さまLANを接続するためのルータ。このマニュアルでは「本装置」と記載します。)の利用マニュアルとなります。

インターネット利用時に必要となる設定項目について、このマニュアルで説明します。

※ 本装置により、電話の利用(1ch~8ch)も可能ですが、電話利用に必要な設定は KDDI にて実施致します(電話利用に関する設定は、お客さまでは変更できません)。

1.2 用語の説明

本マニュアルで使用する用語について、以下で説明します。

用語	説明
回線終端装置(ONU)	お客さま宅内に引き込んだ光ファイバーケーブルを終端する装置です。AC100Vの電源をご用意いただく必要があります。
アダプター(本装置)	「auひかり ビジネス」をお申しいただいた場合、アダプター利用有の場合にKDDIが提供する機器です(音声サービスをご利用いただく場合、本装置の利用は必須となります)。 ONUとお客さまLANを接続するためのルータとなります。 なお、本装置には、回線終端装置(以下、ONUまたはDSUと略す)などのネットワーク終端装置は内蔵されておりません。 ※アダプターを利用せず、お客さまにてルータなどの機器をご用意いただき、「auひかり ビジネス」(インターネット利用)をご利用いただくことも可能です。

1.3 製品のサポートについて

アダプターの故障発生の場合、以下の保守連絡窓口までご連絡ください。

KDDI サービスコントロールセンター (SCC)



0120-99-3751 (無料)

24時間受付／土・日・祝日も受付

故障対応時間 :9時~17時(申告の時間により翌営業日対応になる場合があります)

:オプション契約時 24時間 365日

※上記フリーコールは、携帯電話・PHSからもご利用いただけます。

2 アダプターについて

2.1 機能概要

本装置は、以下に示す機能を有しています。

機能詳細については、5 項 機器仕様を参照ください。

(1) ルータ機能

本装置は、10/100/1000Mbit/s 自動認識の LAN インターフェースを 4 ポート収容し、本装置の LAN 配下に接続した装置を WAN 側に接続するルータ機能(NAT 機能含む)を有しています。

(2) VoIP ゲートウェイ機能

本装置は、FXS または BRI ポートを PBX などに接続し、VoIP ゲートウェイ機能を実現します。
なお、BRI タイプにはクロック同期を行なうため、クロックポートを 1 ポート有しています。

2.2 ネットワーク構成について

インターネット利用時、本装置で割り当てる各セグメントについて説明します。

以下の4つのセグメントがございます。

- IP 網接続に必要な **WAN セグメント**(本セグメントの設定は KDDI が実施します)
- お客さまルータ機器などを接続するための **インターネットセグメント**(本セグメントの本装置側の設定は KDDI が実施します)
- インターネット接続を行うパソコンなどを接続する **LAN セグメント**
- 公開サーバを接続する **仮想 DMZ セグメント**

各セグメントは LAN ポートごとに IP アドレスを割り当ててのではなく、論理的に同一ポートに IP アドレスを割り当てています。そのため、本装置の WAN 側に WAN セグメント、インターネットセグメント(設定による)の IP アドレスが割り当てられます。また、LAN 側には LAN セグメント、インターネットセグメント(設定による)、仮想 DMZ セグメントの IP アドレスが割り当てられます。

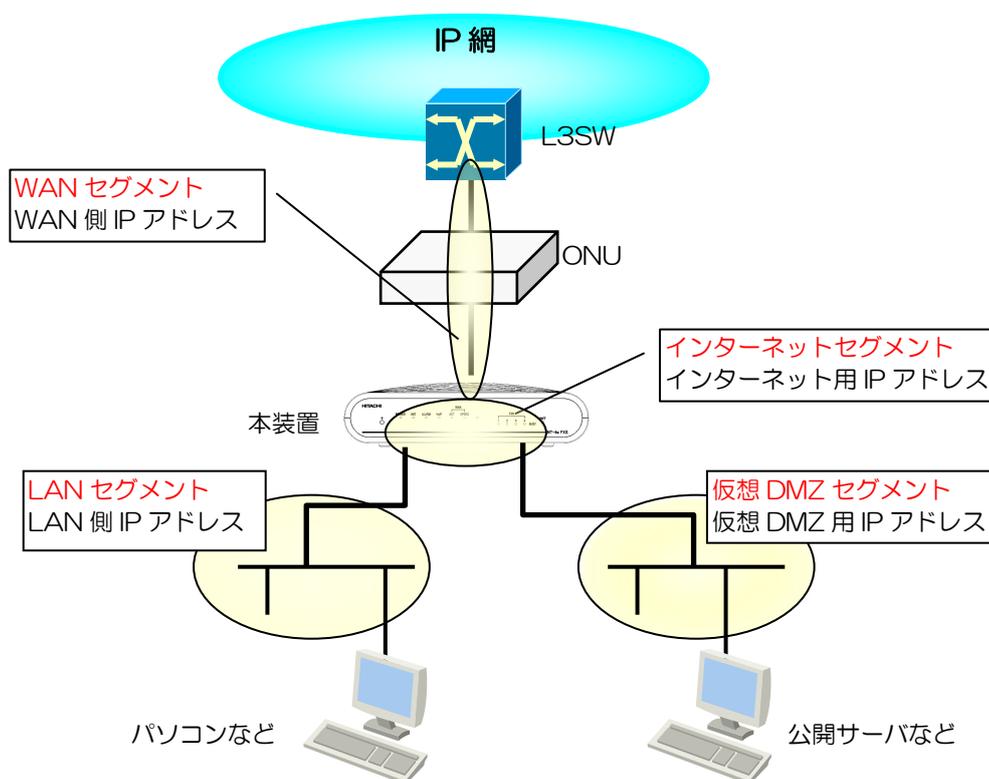


図 2.2.1-1 本装置の通信セグメント

2.2.1 WAN セグメント

本装置と IP 網とを接続するためのセグメントとなります。

WAN セグメントの WAN 側 IP アドレスは WAN ポートに割り当て、IP 網との通信経路用として使用します。

WAN セグメントで使用するアドレスはグローバル IP アドレスとなり、KDDI がアドレスの指定を行います。WAN セグメントのサブネットは基本的には /30 となります。

※ 本装置への WAN セグメントの設定は、KDDI にて実施します。

以下に設定項目を記載します。

■WAN セグメント設定項目

設定データ名称	説明	値
IP アドレス (再)	本装置 WAN ポートへの IP アドレス設定。 開通時に提示する情報「お客さま側 WAN 側 IP」となります。(「割り当て IP アドレス(WAN 側)」の老番)	KDDI 指定値
マスク長 (再)	WAN セグメントのマスク長を設定します。 通常、30 となります(/30)	30
デフォルトゲートウェイ (再)	WAN セグメントの対向機器 (IP 網側の機器) に割り当てられる IP アドレスです。 開通時に提示する情報「KDDI 側ルータ IP」となります。(「割り当て IP アドレス(WAN 側)」の老番)	KDDI 指定値

2.2.2 インターネットセグメント

お客さま機器(パソコン、ルータなど)がインターネットに接続する際、使用されるセグメントとなります。

インターネット用 IP アドレスは WAN ポートに割り当て、インターネット通信を行う場合に使用します。

インターネットセグメントで使用するアドレスはグローバル IP アドレスとなり、KDDI がアドレスの指定を行います。インターネットセグメントのサブネットは、契約するメニューにより異なります (/27、/28、/29、/30 の何れかとなります)。

LAN セグメントに接続された端末(パソコンなど)がインターネットへのアクセスを可能とするために、インターネットセグメントに割り当てる IP アドレス(インターネット用 IP アドレス)のサブネットが /30 の場合には、LAN セグメントの LAN 側 IP アドレスのパソコンなどの端末からの通信を本装置内で NAT/IP マスカレードを行い、インターネット用グローバル IP アドレスに変更して通信を行います。

サブネットが /30 以外の場合、またはサブネットが /30 であっても「NAT しない」設定の場合には、本装置は Unnumbered 接続を行い、WAN ポートにはインターネット用 IP アドレスを割り当てず、LAN ポートにインターネット用 IP アドレスの先頭を割り当てます。それ以降の IP アドレスは LAN に接続された端末が使用し、その端末がインターネット通信を行う場合は本装置では NAT/IP マスカレードを行わず、フォワーディングを行ってインターネットに送出します。この場合にも本装置でのパケットフィルタ機能は有効です。

※ 本装置へのインターネットセグメントの設定は、KDDI にて実施します。

インターネットセグメントのサブネットが /30 の場合において、LAN 側にお客さまルータがない場合、「NAT する」で設定を行います。

■インターネットセグメント設定項目

設定データ名称	説明	値
IP アドレス (再)	本装置に割り当てるインターネットセグメントの IP アドレス。開通時に提示する情報「割り当て IP アドレス(LAN 側)」の先頭ホストアドレスとなります。	KDDI 指定値
マスク長 (再)	インターネットセグメントのマスク長を設定します。お申込んだメニューごとにこととなります。 (27、28、29、30 の何れかとなる)	メニューごとに異なる
NAT 設定	NAT する/NAT しないを選択します。 本装置の利用ケースにより異なりますが、初期値は「NAT する」が設定されています。 本設定は、工事の際、確認します。	初期値は 「NAT する」 (チェックあり)
DNS サーバアドレス	参照用 DNS サーバ(DNS キャッシュ)のアドレス(プライマリとセカンダリ)を設定します。 LAN セグメントで DHCP を利用する場合、DNS サーバアドレスはこの値が払出されます。	KDDI 指定値

2.2.3 LAN セグメント

インターネットに接続するパソコンなどの端末を接続する際、使用されるセグメントです。

LAN セグメントの LAN 側 IP アドレスは本装置の LAN ポートに割り当てられます。

設定変更などによる本装置へのアクセスおよび LAN セグメントの端末がインターネットに接続する際のゲートウェイアドレスとして使用します。

また、LAN セグメントの端末へは、本装置の DHCP 機能によりパソコンなどの端末へアドレスを払い出すことも可能です。

LAN セグメントで使用するアドレスはプライベート IP アドレスとなり、お客さまにて変更が可能です。(初期状態では本装置の LAN ポートに 192.168.0.200 が割り当てられます)

※ インターネットセグメントのサブネットが/30 であり、かつ「NAT する」に設定されている場合に、インターネット接続が可能となります。

2.2.4 仮想 DMZ セグメント

仮想 DMZ セグメントは、ウェブサーバなどのインターネットに公開したい端末があり、LAN セグメントとセグメントを分ける必要がある場合に、お客さまにて設定いただく事で作成されるセグメントです。

仮想 DMZ セグメントの仮想 DMZ 用 IP アドレスは LAN ポートに割り当てられます。

仮想 DMZ セグメントで使用するアドレスはプライベート IP アドレスとなり、お客さまにて設定いただきます。(初期状態では本装置に仮想 DMZ セグメントは作成されていません)

※ 仮想 DMZ セグメント利用する場合、ポートフォワーディング機能(静的 IP マスカレード設定、静的 NAT 設定)を合わせて利用する必要があります。

2.3 システム構成について

本装置のシステム構成例を下図に示します。

本装置は、ONU を介して、KDDI の IP 網に接続され、IP 網を経由して電話網、インターネットへの接続が行われます。本装置の LAN 側に接続されたパソコンなどの端末から本装置、IP 網を経由してインターネットに接続します。

音声サービスをご利用時は、本装置の FXS または BRI インターフェースには PBX などが接続され、その配下の電話機からの通話を本装置で IP 化し、IP 網、電話網を経由して相手側電話機と接続します。

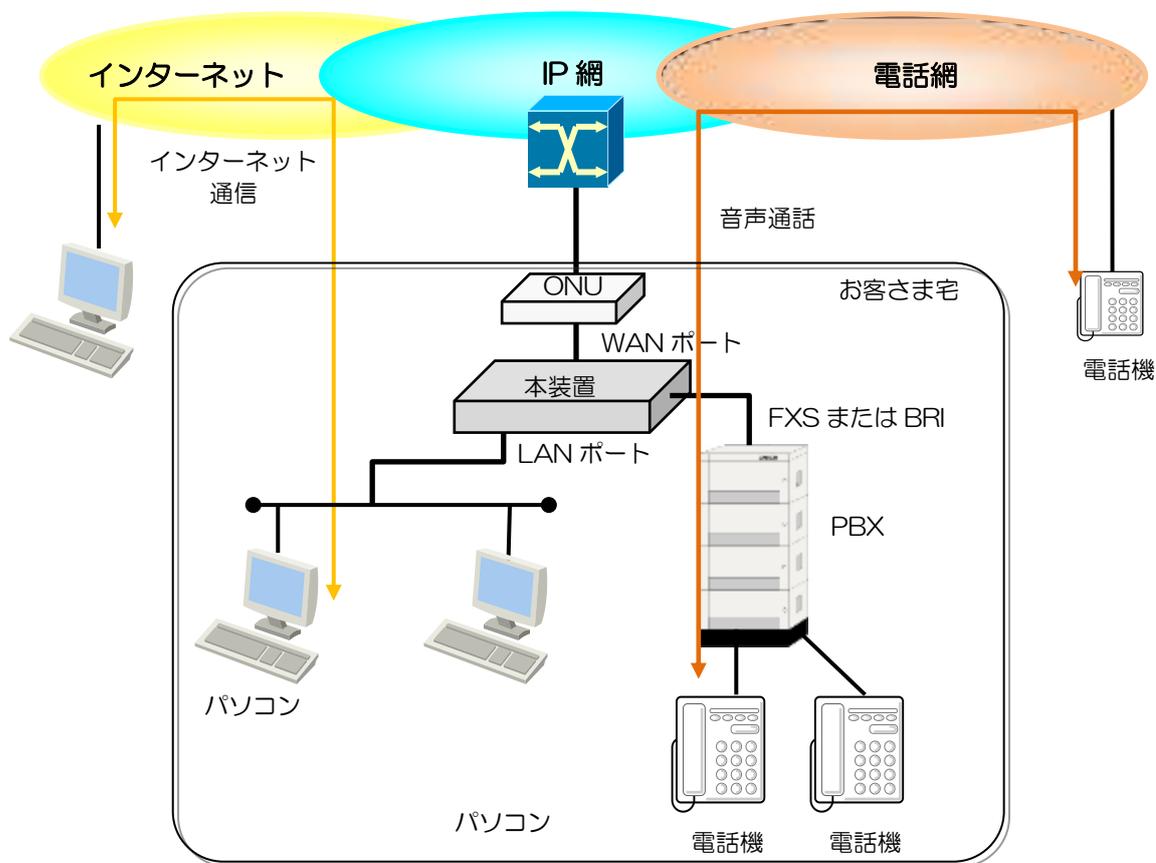


図 2.2.4-1 システム構成例

本装置を使用して、インターネット接続を利用する構成としては、以下の接続構成がございます。

- ① 接続ケース 1: 本装置にパソコンなどの端末を接続してインターネットアクセスを行う。
- ② 接続ケース 2: 本装置にパソコンなどの端末を接続してインターネットアクセスを行う。
また、本装置にサーバなどを接続して、インターネットにサーバを公開する。
- ③ 接続ケース 3: 本装置をルータとして使用する。本装置の LAN 側にお客さまのルータ機器など (ブロードバンドルータなど) を接続し、インターネットアクセスを行う。

上記の各利用のケースについて、以降で説明します。

2.3.1 接続ケース 1

本装置にパソコンなどの端末を接続してインターネットアクセスを行う。

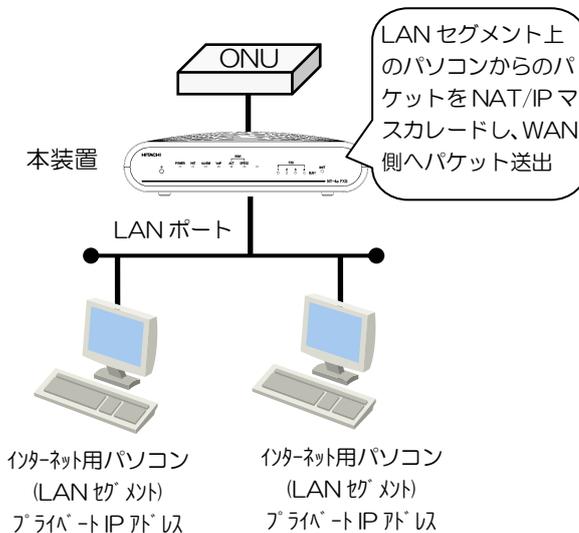


図 2.3.1-1 インターネットを行う構成
(インターネットセグメントのサブネットが /30 の場合)

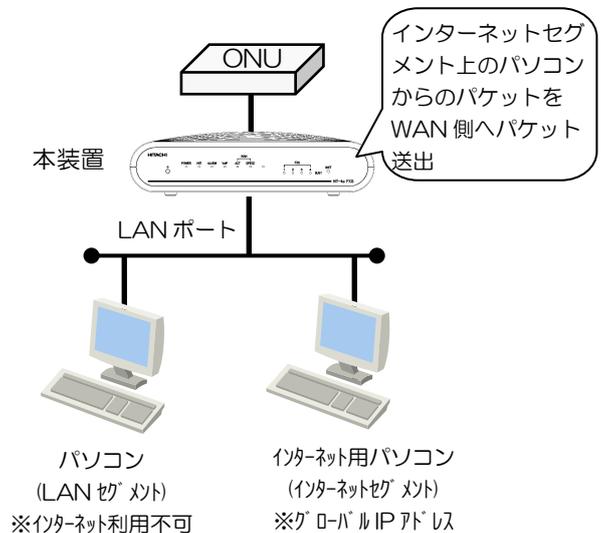


図 2.3.1-2 インターネットを行う構成
(インターネットセグメントのサブネットが /30 以外の場合)

■説明(インターネットセグメントが /30 の場合)

- 本装置の LAN ポートにパソコンなどの端末を接続してインターネット接続を行います。パソコンなどの IP アドレスは本装置から DHCP で払い出す、あるいは固定で設定することも可能です。
- パソコンなどからのインターネットアクセスは本装置で NAT/IP マスカレードされ、インターネットへ送信されます。

■説明(インターネットセグメントが /30 以外の場合)

- インターネットセグメントのサブネットが /30 以外の場合(サブネットが /30 であっても本装置の「NAT 設定」が「NAT しない」の場合も含む)、本装置での IP マスカレードは行わず、パソコンなどにインターネットセグメントのグローバルアドレスを割り当てインターネット通信を行います。
- 本装置から DHCP で IP アドレスを払い出された、あるいはインターネットセグメント以外のアドレスを設定したパソコンについては、インターネットアクセスは出来ません。

2.3.2 接続ケース 2

本装置にパソコンなどの端末を接続してインターネットアクセスを行う。

また、本装置にサーバなどの端末を接続して、インターネットにサーバを公開する。

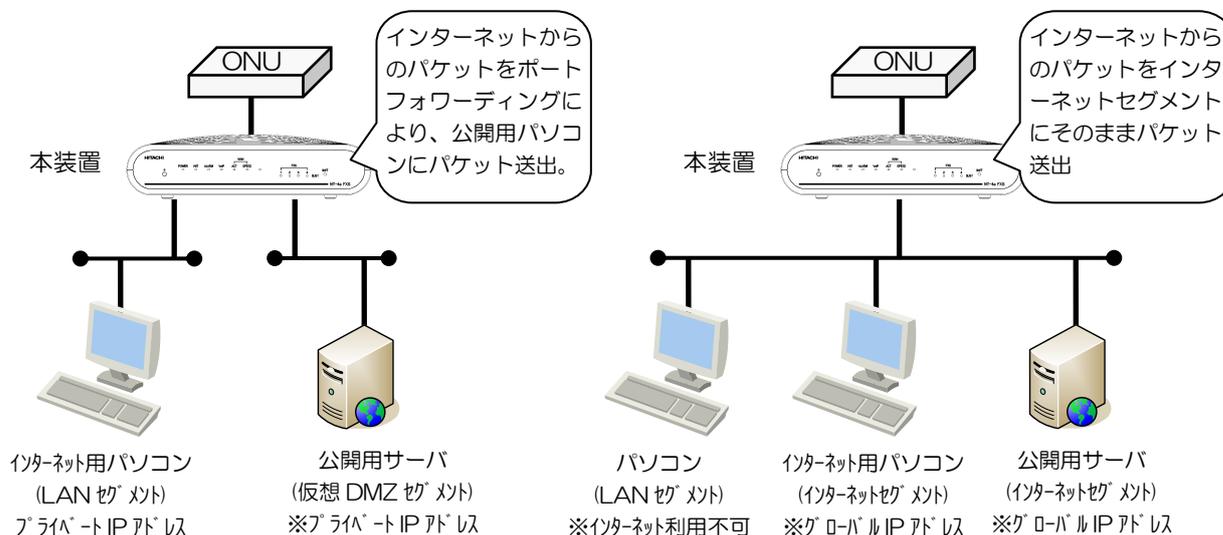


図 2.3.2-1 インターネットを行う構成
(インターネットセグメントのサブネットが
/30 の場合)

図 2.3.2-2 インターネットを行う構成
(インターネットセグメントのサブネット
が/30 以外の場合)

■説明(インターネットセグメントが/30 の場合)

- 本装置の LAN ポートにパソコンなどの端末を接続してインターネット接続を行います。パソコンなどの IP アドレスは本装置から DHCP で払い出す、あるいは固定で設定することも可能です。
- パソコンなどからのインターネットアクセスは本装置で NAT/IP マスカレードされ、インターネットへ送信されます。
- 仮想 DMZ セグメントの設定、ポートフォワーディング(静的 IP マスカレード、静的 IPNAT)機能により、インターネットからのパケットを公開用サーバに送信(アドレス変換される)します。

■説明(インターネットセグメントが/30 以外の場合)

- インターネットセグメントのサブネットが/30 以外の場合(サブネットが/30 であっても本装置の「NAT 設定」が「NAT しない」の場合も含む)、本装置での IP マスカレードは行わず、パソコンなどにインターネットセグメントのグローバル IP アドレスを割り当て、インターネット通信を行います。
- 本装置でフィルタリングを行うことで、インターネットセグメント上のグローバル IP アドレスを割り当てられた公開用サーバに対してインターネットからのパケットを送出します。
- 本装置から DHCP で IP アドレスを払い出された、あるいはインターネットセグメント以外のアドレスを設定したパソコンについては、インターネットアクセスは出来ません。

2.3.3 接続ケース3

本装置をルータとして使用する。本装置のLAN側にお客さまのルータ機器など(ブロードバンドルータなど)を接続し、インターネットアクセスを行う。

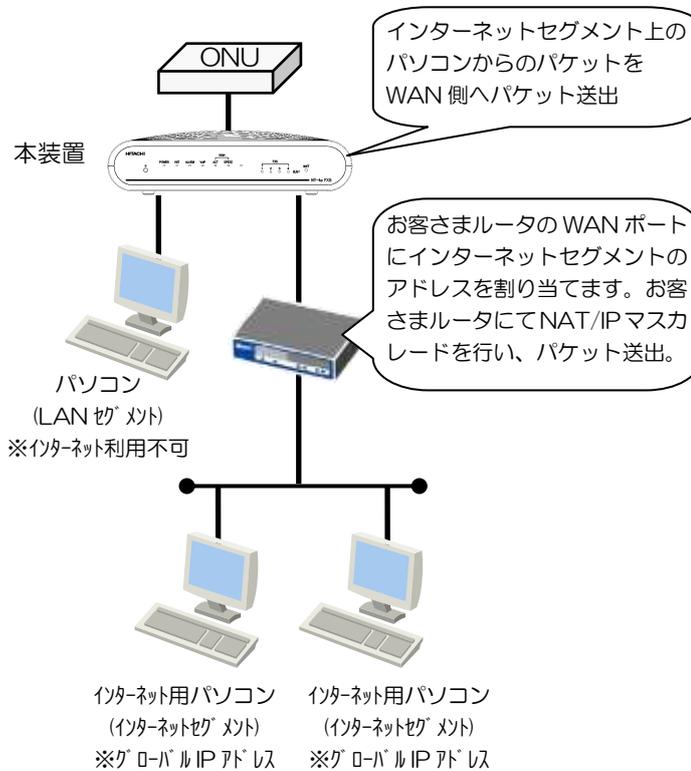


図 2.3.3-1 インターネットを行う構成

■説明

- 本装置のLANポートにお客さまご用意のルータ(NAT機能のあるブロードバンドルータなど)を接続する場合、インターネットセグメントのサブネットによらず、本装置の「NAT設定」を“NATしない”に設定して、お渡しします。
- お客さまご用意のルータのWANポートにインターネットセグメントのグローバルIPアドレスを割り当てます。
- お客さまご用意のルータLAN側にあるパソコンなどの端末から送出されたパケットをお客さまご用意のルータでNAT/IPマスカレードを行い、本装置にパケット送出を行います。本装置は、WAN側にパケット送出を行い、インターネット接続を行います。
- 本装置からDHCPでIPアドレスを払い出された、あるいはインターネットセグメント以外のアドレスを設定したパソコンについては、インターネットアクセスは出来ません。

2.3.4 ケース毎のセグメントの状況

各利用ケースでの各セグメントの状況を下表に示します。

表 2.3.4-1 各サービス選択時のセグメント使用状況

サービス選択 セグメント	セグメント			
	WAN セグメント	インターネット セグメント	LAN セグメント	仮想 DMZ セグメント
接続ケース 1 (/30)	●	● (NAT あり)	○	-
接続ケース 1 (/30 以外)	●	● (NAT なし)	×	-
接続ケース 2 (/30) ※公開サーバあり	●	● (NAT あり)	○	○
接続ケース 2 (/30 以外) ※公開サーバあり	●	● (NAT なし)	×	-
接続ケース 3	●	● (NAT なし)	×	-

●:KDDI にて設定する箇所。

○:必要に応じてお客さまにて設定が必要。

×:インターネット接続は不可。

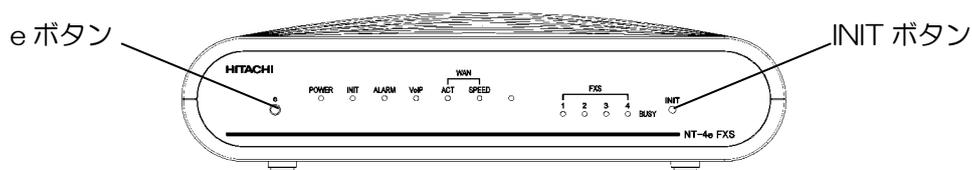
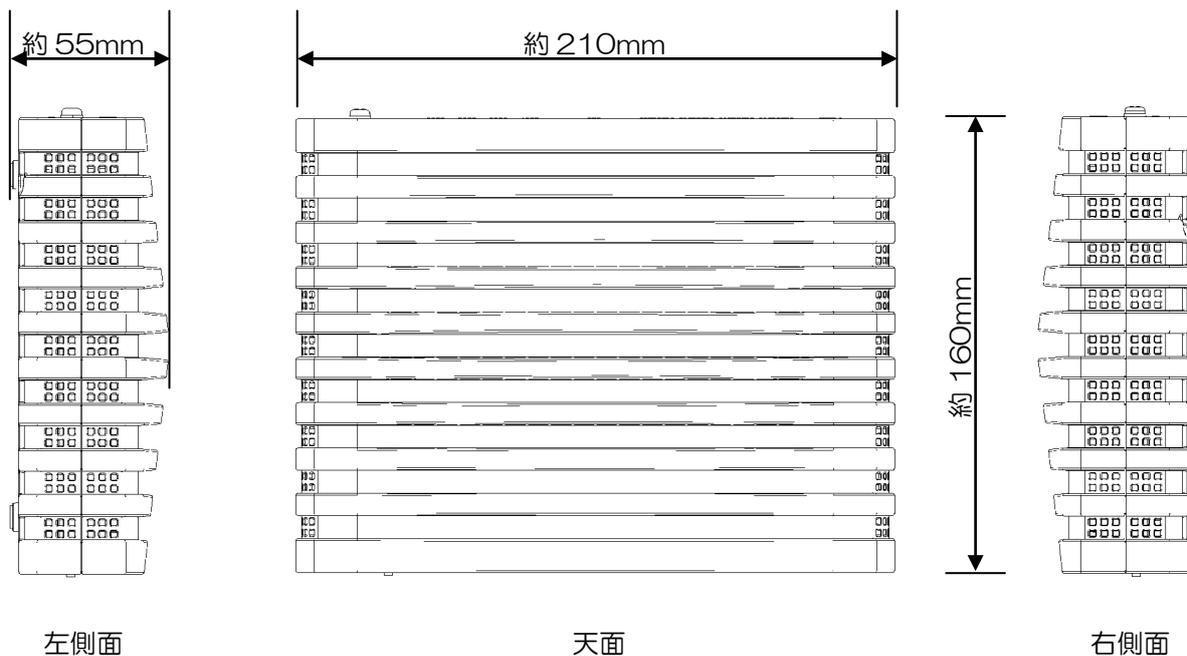
-:使用しないため設定不要。

3 設置について

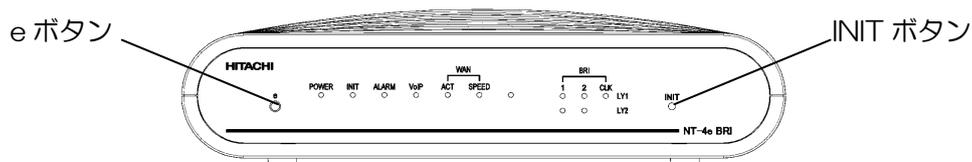
3.1 機器の説明

3.1.1 機器の外観と添付品

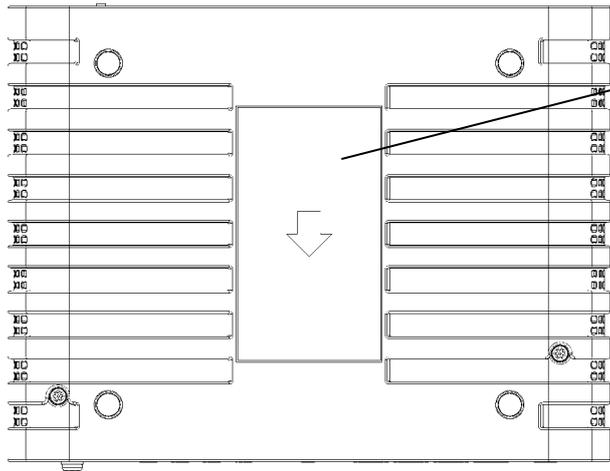
3.1.1.1 機器の外観



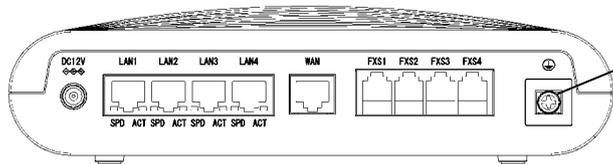
正面(FXS タイプ)



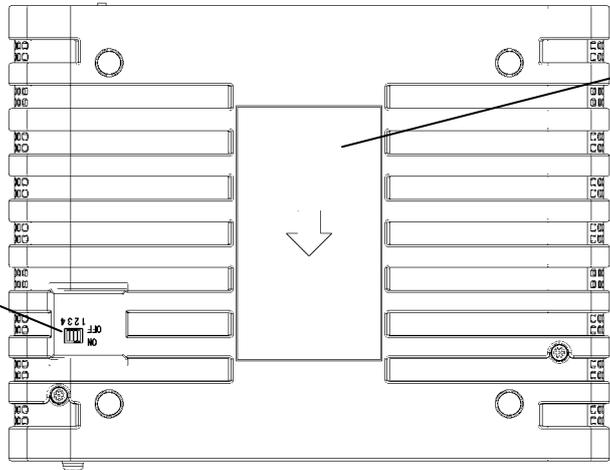
正面(BRI タイプ)



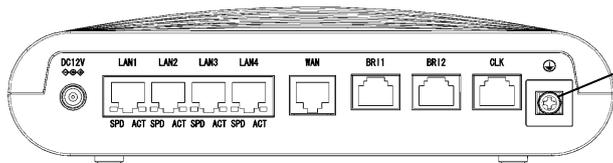
底面 (FXS)



背面 (FXS)



底面 (BRI)



背面 (BRI)

3.1.1.2 添付品

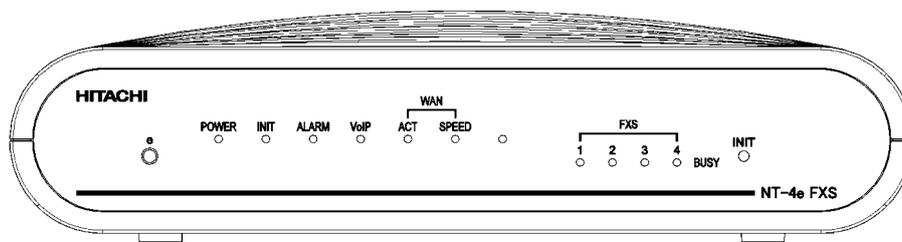
添付品として、本体以外に以下があることを確認してください。

- ・電源アダプター(1 個)
- ・ONU 接続用 カテゴリ 5e ケーブル(1 本)

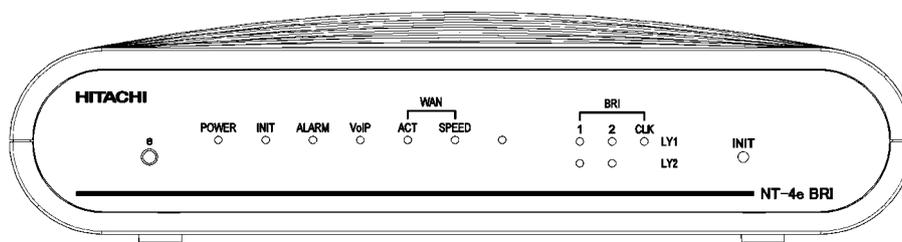
3.1.2 各部の名称と機能

各部の名称ならびに機能を示す。

3.1.2.1 各部の名称と機能(前面)



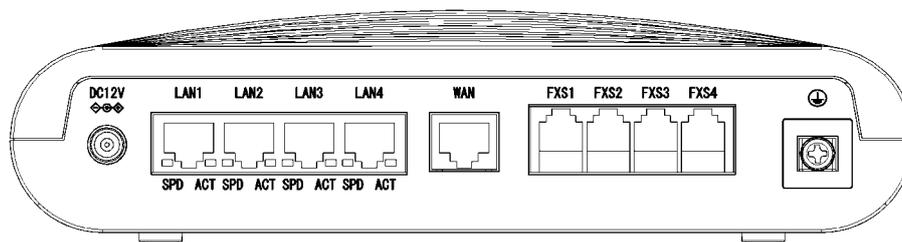
正面(FXS)



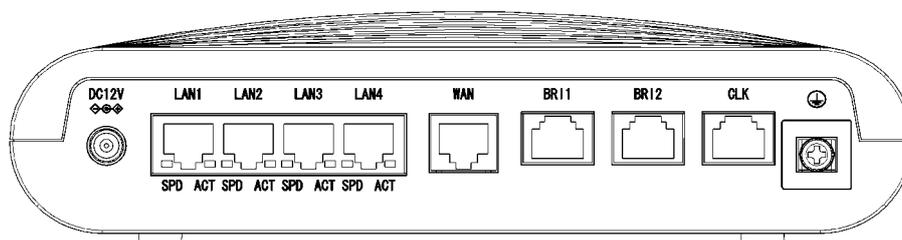
正面(BRI)

名称	説明
e ボタン	ランプ消灯モード復旧ボタン ランプ消灯モード設定時に本ボタンを押すことにより、ランプ消灯モードから復旧する。
POWER ランプ	電源状態表示
INIT ランプ	工場出荷状態表示
ALARM ランプ	障害状態表示
VoIP ランプ	音声通信状態表示
WAN ACT ランプ	WAN 回線状態表示
WAN SPEED ランプ	WAN 回線速度表示
表示なしランプ	親子設定状態表示
FXS1~4 BUSY ランプ	FXS 回線状態表示
BRI1~2・CLK LY1 ランプ	BRI 回線状態表示
BRI1~2 LY2 ランプ	BRI 回線状態表示
INIT ボタン	初期化ボタン 本装置を工場出荷状態に戻す場合に使用する。 ※初期状態に戻り、IP 網との接続が出来なくなるため、使用しないでください。

3.1.2.2 各部の名称と機能(背面)



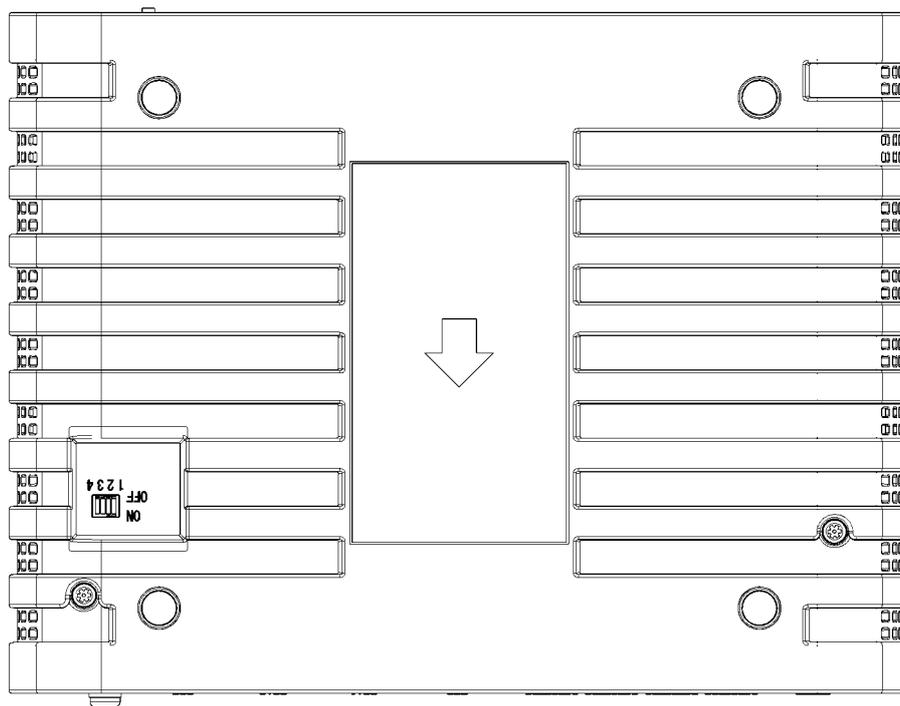
背面(FXS)



背面(BRI)

名称	説明
DC12V	付属の電源アダプターを接続する。
LAN1~4 ポート	IP 端末を接続する。
SPD ランプ	LAN ポート回線速度表示
ACT ランプ	LAN ポート回線状態表示
WAN ポート	ONU に接続する。
FXS1~4 ポート	PBX などを接続する。
BRI1~2 ポート	PBX などを接続する。
CLK ポート	ISDN 基本インターフェース(S/T 点)などを接続する クロック同期ポート。
FG 端子	アース線を接続する。

3.1.2.3 各部の名称と機能(底面)



底面 (BRI)

名称	説明
スライドスイッチ(BRIのみ)	CLK ポート終端抵抗(入・切)スイッチ CLK を供給する回線に複数の装置を接続する場合、 最遠端装置のみに終端抵抗を入れる。 装置交換時にも設定を忘れないこと。 ※KDDI で設定します。お客さまにて変更しないようお願いします。

3.1.3 ランプとボタン・スイッチの機能

ランプとボタン・スイッチの機能を示す。

3.1.3.1 ランプの機能

本装置のランプの種類および機能を下表に示す。

ランプ名称	状態	機能
POWER	消灯	電源オフ
	緑点灯	電源オン
	緑点滅	装置起動中
INIT	消灯	通常状態
	橙点灯	工場出荷状態
ALARM	消灯	通常状態
	赤点灯	ハード故障検出
VoIP	消灯	VoIP 使用不可
	緑点灯	VoIP 通信可能
	緑点滅	VoIP 発信中、着信中、通信中
WAN ACT	消灯	リンクダウン
	緑点灯	リンクアップ
	緑点滅	データ送受信中
WAN SPEED	消灯	回線速度 100M または 10M または未接続
	橙点灯	回線速度 1G
表示なしランプ	消灯	単独または親機設定
	緑点灯	子機設定
FXS1~4 BUSY	消灯	FXS ポート未使用
	緑点灯	FXS ポート使用中
	緑点滅	FXS ポート閉塞
BRI1~2・CLK LY1	消灯	レイヤ 1 未確立
	緑点灯	レイヤ 1 確立
BRI1~2 LY2	消灯	レイヤ 2 未確立
	緑点灯	レイヤ 2 確立
LAN1~4 SPD	消灯	LAN 速度 10M 時
	橙点灯	LAN 速度 1G/100M 時
LAN1~4 ACT	消灯	リンクダウン
	緑点灯	リンクアップ
	緑点滅	データ送受信中

3.1.3.2 ボタン・スイッチの機能

本装置のボタン・スイッチの種類および機能を下表に示す。

名称	機能	操作説明
e ボタン	ランプ消灯モード復旧ボタン	ランプ消灯モード時、本ボタンを押すことで本装置をランプ消灯モードから復旧する。
INIT ボタン	装置初期化	初期状態に戻り、IP 網との接続が出来なくなるため、使用しないでください。
スライドスイッチ	CLK ポート 100Ω 終端抵抗 オン・オフ	CLK ポート内蔵の終端抵抗を切り離す場合にスイッチすべて(1~4)を OFF にする。 工場出荷時は、すべて ON 側になっている。

3.1.4 LAN/WAN 配線用 UTP ケーブルについて

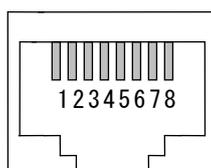
WAN および LAN インターフェースを接続するケーブルは、LAN 配線用エンハンスドカテゴリ 5UTP ケーブル(以下カテゴリ 5e ケーブル)または LAN 配線用カテゴリ 6UTP ケーブル(以下カテゴリ 6 ケーブル)を使用してください。

本装置の WAN および LAN インターフェースは、MDI/MDIX 自動切り替え機能を有しており、ストレートケーブルでもクロスケーブルでもどちらでも接続が可能です。

以下に WAN/LAN インターフェースの仕様を示します

項目		仕様		
インターフェース仕様	インターフェース	1000BASE-T	100BASE-TX	10BASE-T
	通信速度	1Gbit/s	100Mbit/s	10Mbit/s
	速度選択	オートネゴシエーション(固定も可)		
配線	推奨ケーブル	カテゴリ 5e ケーブル		
	ストレート/クロス	自動 MDI/MDIX 切り替え(固定も可)		
	インピーダンス	100Ω		
	最大セグメント長	100m		
コネクタ	RJ-45			

WAN および LAN コネクタ(RJ-45)



ピン No.	1000BASE-T		100BASE-TX/10BASE-T	
	MDI	MDIX	MDI	MDIX
1	BI_DA+	BI_DB+	TD+	RD+
2	BI_DA-	BI_DB-	TD-	RD-
3	BI_DB+	BI_DA+	RD+	TD+
4	BI_DC+	BI_DD+	未使用	未使用
5	BI_DC-	BI_DD-	未使用	未使用
6	BI_DB-	BI_DA-	RD-	TD-
7	BI_DD+	BI_DC+	未使用	未使用
8	BI_DD-	BI_DC-	未使用	未使用

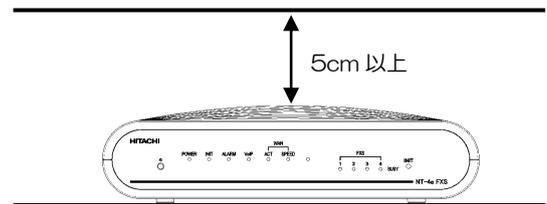
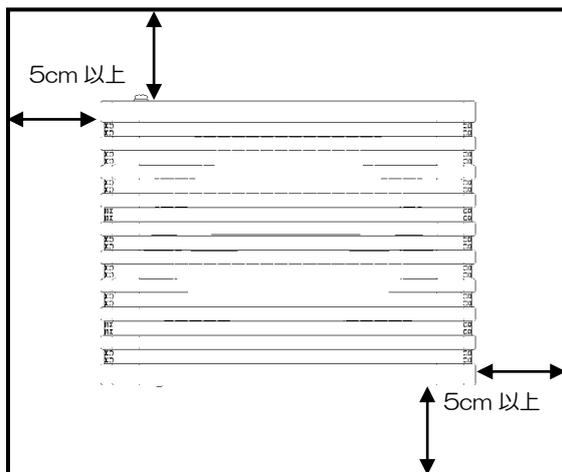
3.1.5設置

本装置は、横置き設置となります。以下に設置方法を示します。

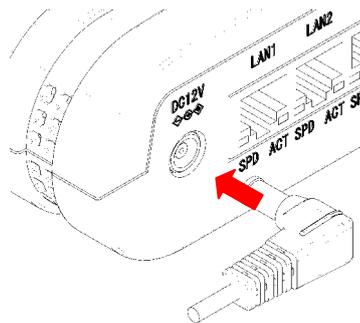
水平な場所に設置し、装置の前後左右と上面それぞれ 5cm 以上の空間を設け、通風孔を塞がないように設置してください。

耐震バンドなどで固定する場合には、通風孔を塞がないように 2 本のバンドで装置両端を固定するなどの方法を取るようになしてください。

※本装置の設定は、KDDI にて実施します。



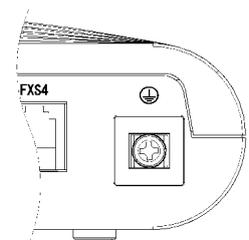
電源コードは、図のように本体側へしっかりと差し込みます。



本装置の FG 端子は、必ずアースに接続してください。

アースに接続しないと雷などにより機器が破損する恐れがございます。

また、外来ノイズによる誤動作の可能性がございます。



【注意】

本装置の設置に関して、以下の点に注意し、設置してください。

- ・装置動作環境を満足すること。
- ・直射日光の当たる場所や暖房設備・屋外など、温度の上がる場所への設置はしないこと。
- ・腐食性ガスや引火性ガスが発生する場所(温泉地など)への設置はしないこと。
- ・空气中塩分濃度の高い場所や塩水のかかる場所(海岸部)への設置はしないこと。
- ・振動、衝撃の多い場所には設置しないこと。
- ・磁気および電磁波などの影響が懸念される場所(電子レンジ、スピーカなど)には設置しないこと。

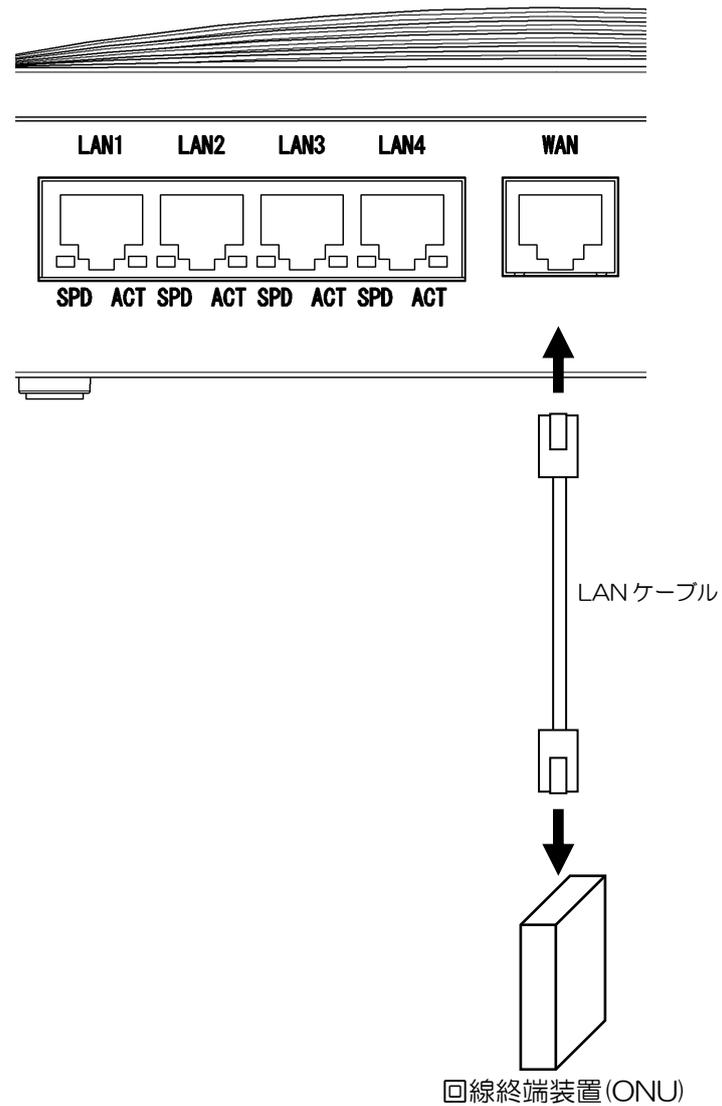
3.2 接続について

3.2.1 WANの接続

※KDDIで実施する作業です。

本装置のWANポートとONU(回線終端装置)をLANケーブルで接続します。

(ケーブルはKDDIで準備します)



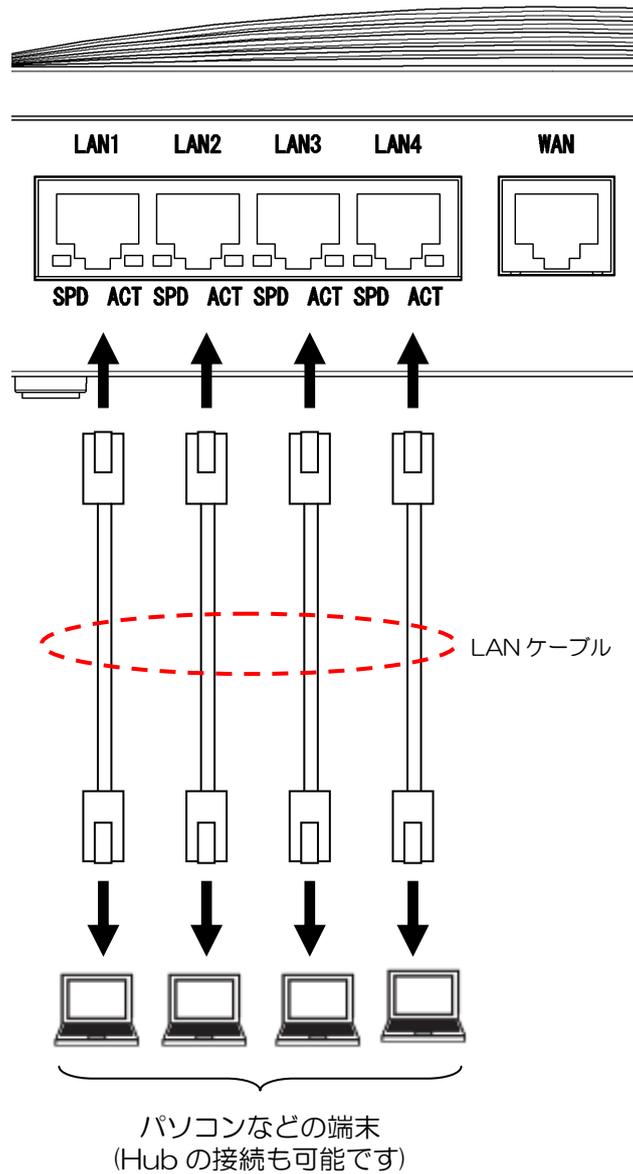
3.2.2 LAN の接続

本装置の LAN ポートに、パソコンを LAN ケーブルで接続します。

※

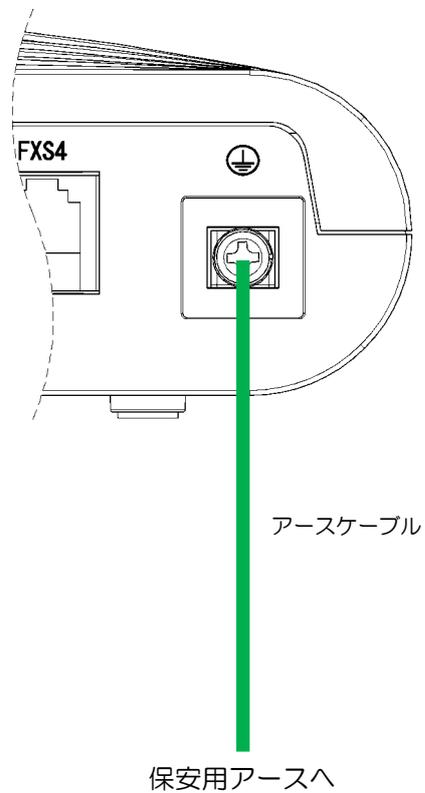
LAN ケーブル以外を LAN ポートに接続しないでください。

LAN ケーブルはカテゴリ 5e またはカテゴリ 6 を使用してください。



3.2.3 FGの接続

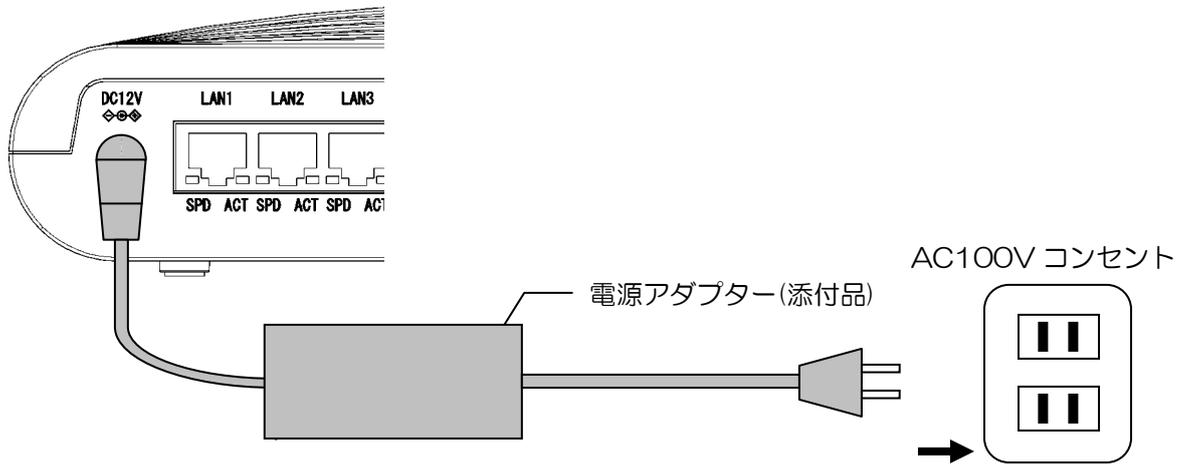
本装置のFG端子にアース線を接続します。



※本装置のFG端子は、必ずアースに接続すること。
アースに接続しないと雷などにより機器が破損する恐れがあります。
また、外来ノイズによる誤動作の可能性もあります。

3.2.4 電源の接続

本装置に添付の電源アダプターを接続し、電源アダプターの AC プラグを AC100V の商用電源に接続します。



※添付の電源アダプター以外は、絶対に接続しないでください。

※電源コードは、本体側へしっかりと差し込んでください。

3.2.5 電源の投入と電源投入後のランプ表示

本装置の電源投入後のランプ表示を以下に示します。

○:点灯 △:点滅 ×:消灯

ランプ名称	電話使用あり		電話使用なし
	親機	子機	
POWER ランプ	○緑	○緑	○緑
INIT ランプ	×	×	×
ALARM ランプ	×	×	×
VoIP ランプ	○緑	○緑	×
WAN ACT ランプ	※1	※1	※1
WAN SPEED ランプ	○橙	○橙	○橙
表示なしランプ	×	○緑	×
FXS1~4 BUSY ランプ	※2	※2	×
BRI1~2 LY1 ランプ	※3	※3	×
BRI1~2 LY2 ランプ	※3	※3	×
CLK LY1 ランプ	※3	※3	×
LAN1~4 ACT ランプ	※4	※4	※4
LAN1~4 SPD ランプ	※5	※5	※5

※1:使用状態により○緑または△緑

※2:使用(設定)状態により○緑または×、△緑は閉塞状態

※3:使用(設定)状態により○緑または×

※4:使用状態により○緑または△緑または×

※5:使用状態により○橙または×

(ランプ表示の異常状態)

- ①POWER ランプが消灯している場合は、電源が正常に供給されていない、または、本装置の故障が考えられます。電源アダプターの接続を確認してください。
- ②ALARM ランプが赤点灯した場合は、本装置の故障です。
- ③電話使用あり設定で、VoIP ランプ消灯は設定および ONU・網側の状態を確認してください。
- ④WAN ACT ランプ消灯は、ONU・網側の状態を確認してください。
- ⑤WAN SPEED ランプ消灯は、ONU・網側の状態を確認してください。
- ⑥子機設定で、表示なしランプ消灯は親機との接続を確認してください。

4 設定編

4.1 設定概要

4.1.1 設定方法について

本装置の設定は、LAN インターフェースに接続されたパソコンからウェブブラウザにより行います。設定画面は日本語により表示されるので画面にしたがって各種データ設定や状態、ログなどの表示を行います。

本装置にアクセスするときは、パスワードによる認証が要求されます。
(認証完了後、パスワードを変更することが可能です)

本装置の設定を変更する場合、下記手順にて行います。

- マウスを使用して設定画面上の項目を指定し、キーボードにて必要な変更を行います。
- その後、「設定保存」ボタンをクリックして変更内容を本装置へ設定します。
「設定保存」ボタンをクリックしないと本装置への変更内容が反映されません。
- ブラウザ上の変更内容を元に戻したい場合には「元に戻す」ボタンをクリックします。
- 必要な変更に対して、各画面で「設定保存」ボタンをクリックした後、変更した内容を有効とするためには、本装置の再起動が必要となる場合があります、変更された内容は再起動後に有効となります。

注意事項

- ※「元に戻す」ボタンをクリックすると、変更内容が元に戻るが、一旦「設定保存」ボタンで設定した内容は元に戻せません。
- ※「設定保存」ボタンをクリックする前に、ほかの設定画面などを開いた場合、設定した値は破棄されません。
- ※ 設定保存時の結果表示画面には、入力された値がそのまま表示されるが、再表示した場合は、表示を最適化します。
- ※ 稼働中の本装置の設定変更を行う場合は、変更を行う前に「装置設定の保存/復元」を参照し、現在動作中の設定内容を保存します。
- ※ 複数ブラウザによる同時設定を行わないようにしてください。
- ※ 設定画面での操作は、画面内に配置されているボタンなどで行うこと。ウェブブラウザのボタンやキーボードでのショートカットを使用すると、正常に動作しない場合がございます。
- ※ 通信の負荷が非常に高い場合、ウェブブラウザによる画面表示が遅くなる場合がございます。

4.1.2 設定のための準備

本装置へ接続し、設定する端末(保守用パソコン)の設定方法を示します。

なお、ここで示す設定例は本装置が DHCP サーバとして機能している場合の手順となります。

本装置への接続確認は、以下の組み合わせで行っています。

(異なる組み合わせで接続を行う場合、正常に表示されない場合がございます)

対応 OS	対応ウェブブラウザ
Microsoft Windows 7	Internet Explorer 9.0
Microsoft Windows 7	Internet Explorer 8.0
Microsoft Windows Vista (SP1/SP2 を含む)	Internet Explorer 7.0 以上
Microsoft Windows XP(SP3 以上)	Internet Explorer 6.0

4.1.2.1 設定の流れ

手順	作業項目	作業内容
1	準備	接続および設定に必要なものを準備する。
2	端末の接続	本装置の LAN ポートに端末(確認用のパソコン)を接続する。
3	端末の設定	確認用のパソコンの設定を行う。 ・DHCP の設定 ・ブラウザの設定
4	ウェブログイン	本装置の LAN ポートに接続したパソコンでブラウザ(インターネットエクスプローラ)を起動し、「http://192.168.0.200/」へアクセスします。 ログインする。
5	設定確認・変更	必要に応じて設定変更を行います。

4.1.2.2 準備

本装置の設定・動作確認のため、以下のものを準備してください。

- ・ 端末(接続確認用の Windows パソコン)
- ・ LAN 接続用ケーブル

4.1.2.3 Windows® 7 利用時の準備

下記の手順にしたがってパソコンを設定します

(1) インターネットプロパティの設定

- ①「コントロールパネル」を表示
Windows® 7 を起動し、「スタート」メニューから「コントロールパネル」をクリックします。
- ②「ネットワークとインターネット」を表示
コントロールパネルの「ネットワークとインターネット」をクリックします。
- ③「インターネットオプション」を表示
[インターネットオプション]をクリックします。
- ④[接続]タブで[ダイヤルしない]を選択
「インターネットのプロパティ」の「接続」タブをクリックします。
「ダイヤルアップと仮想プライベートネットワークの設定」で「ダイヤルしない」が選択されていることを確認します。
[ネットワーク接続が存在しないときには、ダイヤルする]や[通常の接続でダイヤルする]が選択されている場合は、[ダイヤルしない]をクリックします。
- ⑤「ローカルエリアネットワーク(LAN)の設定」の[LANの設定]をクリックします。
- ⑥「ローカルエリアネットワーク(LAN)の設定」を次のように設定します。
 - 「自動構成」のチェックを外す
「設定を自動的に検出する」、「自動構成スクリプトを使用する」のチェックがついていないことを確認する。チェックがついている場合は、すべてのチェックを外します。
 - 「プロキシサーバ」のチェックを外す
「LAN にプロキシサーバを使用する」のチェックが付いている場合は、チェックを外し、[OK]をクリックします。
- ⑦「インターネットのプロパティ」の[OK]をクリックします。

(2) ネットワークの設定

- ①「コントロールパネル」を表示
Windows® 7 を起動し、「スタート」メニューから「コントロールパネル」をクリックします。
- ②「ネットワークと共有センター」を表示
コントロールパネルの「ネットワークの状態とタスクの表示」をクリックします。
- ③「ネットワーク接続」を表示
「アダプターの設定の変更」をクリックします。
- ④「ローカルエリア接続の状態」を表示
「ローカルエリア接続」をダブルクリックします。

●「ネットワーク接続」の「ブロードバンド」の欄に、PPPoE設定がされていて、その設定が既定の接続に設定されている場合には、PPPoEのアイコンを右クリックして、表示されるサブメニューの「既定の接続を解除」を選択し、クリックします。

- ⑤「ローカルエリア接続のプロパティ」を表示
「ローカルエリア接続の状態」の[プロパティ]をクリックします。
「ユーザーアカウント制御」画面が表示された場合は、[続行]をクリックします。
- ⑥「インターネットプロトコルバージョン 4(TCP/IPv4)のプロパティ」を表示
「ローカルエリア接続のプロパティ」の一覧から[インターネットプロトコルバージョン (TCP/IPv4)]を選択し、[プロパティ]をクリックします。
- ⑦IP アドレスと DNS を設定
「インターネットプロトコルバージョン 4(TCP/IPv4)のプロパティ」の[IP アドレスを自動的に取得する]と、[DNS サーバのアドレスを自動的に取得する]を選択します。IP アドレスと DNS の設定を確認したら[詳細設定]をクリックします。
- ⑧DHCP 設定を確認し、[OK]をクリックします。
「TCP/IP 詳細設定」の[IP 設定]タブをクリックして、一覧に「DHCP 有効」と表示されているか確認します。
- 「DHCP有効」となっていない場合、手順7の画面で「IPアドレスを自動的に取得する」と、「DNSサーバのアドレスを自動的に取得する」を選択してあるか、再度確認します。
- ⑨「インターネットプロトコルバージョン 4(TCP/IPv4)のプロパティ」の[OK]をクリックします。
- ⑩「ローカルエリア接続のプロパティ」の[OK]をクリックします。
- ⑪「ローカルエリア接続の状態」の[閉じる]をクリックします。

(3) ネットワークの設定を確認する

- ①「ローカルエリア接続の状態」を表示
「ネットワークの設定」の手順①～③を行います。
- ② 「ローカルエリア接続の状態」で「詳細」をクリックします。
[詳細]をクリックする。
- ③ IPアドレスを確認
以下の個所に設定が反映されたことを確認する。
・IPv4 IPアドレス
・IPv4 サブネットマスク
・IPv4 デフォルトゲートウェイ
これらのアドレスはすべて自動で設定されます。

●各情報が正常に設定されていない場合は、パソコンと本装置の電源を切ってから電源やケーブルなどの接続を確認し、本装置の電源を入れてからパソコンの電源を入れ、手順①からやり直してください。

4.1.2.4 Windows Vista® 利用時の準備

下記の手順にしたがってパソコンを設定します

(1) インターネットプロパティの設定

- ①「コントロールパネル」を表示
Windows Vista®を起動し、「スタート」メニューから「コントロールパネル」をクリックします。
- ②「ネットワークとインターネット」を表示
コントロールパネルの「ネットワークとインターネット」をクリックします。
- ③「インターネットオプション」を表示
[インターネットオプション]をクリックします。
- ④[接続]タブで[ダイヤルしない]を選択
「インターネットのプロパティ」の「接続」タブをクリックします。
「ダイヤルアップと仮想プライベートネットワークの設定」で「ダイヤルしない」が選択されていることを確認します。
[ネットワーク接続が存在しないときには、ダイヤルする]や[通常の接続でダイヤルする]が選択されている場合は、[ダイヤルしない]をクリックします。
- ⑤「ローカルエリアネットワーク(LAN)の設定」の[LANの設定]をクリックします。
- ⑥「ローカルエリアネットワーク(LAN)の設定」を次のように設定します。
 - 「自動構成」のチェックを外す。
「設定を自動的に検出する」、「自動構成スクリプトを使用する」のチェックがついていないことを確認する。チェックがついている場合は、すべてのチェックを外す。
 - 「プロキシサーバ」のチェックを外す。
「LAN にプロキシサーバを使用する」のチェックが付いている場合は、チェックを外し、[OK]をクリックする。
- ⑦「インターネットのプロパティ」の[OK]をクリックする。

(2) ネットワークの設定

- ①「コントロールパネル」を表示
Windows Vista® を起動し、「スタート」メニューから「コントロールパネル」をクリックします。
- ②「ネットワークと共有センター」を表示
コントロールパネルの「ネットワークの状態とタスクの表示」をクリックします。
- ③「ネットワーク接続」を表示
「ネットワーク接続の管理」をクリックします。
- ④「ローカルエリア接続の状態」を表示
「LANまたは高速インターネット」内の「ローカルエリア接続」をダブルクリックします。

●「ネットワーク接続」の「ブロードバンド」の欄に、PPPoE設定がされていて、その設定が既定の接続に設定されている場合には、PPPoEのアイコンを右クリックして、表示されるサブメニューの「既定の接続を解除」を選択し、クリックします。

- ⑤「ローカルエリア接続のプロパティ」を表示
「ローカルエリア接続の状態」の[プロパティ]をクリックします。
「ユーザーアカウント制御」画面が表示されるので、[続行]をクリックします。
- ⑥「インターネットプロトコルバージョン4(TCP/IPv4)のプロパティ」を表示
「ローカルエリア接続のプロパティ」の一覧から[インターネットプロトコルバージョン(TCP/IPv4)]を選択し、[プロパティ]をクリックします。
- ⑦IPアドレスとDNSを設定
「インターネットプロトコルバージョン4(TCP/IPv4)のプロパティ」の[IPアドレスを自動的に取得する]と、[DNSサーバのアドレスを自動的に取得する]を選択します。
IPアドレスとDNSの設定を確認したら[詳細設定]をクリックします。
- ⑧DHCP設定を確認し、[OK]をクリック
「TCP/IP詳細設定」の[IP設定]タブをクリックして、一覧に「DHCP有効」と表示されているか確認します。
- 「DHCP有効」となっていない場合、手順7の画面で「IPアドレスを自動的に取得する」と、「DNSサーバのアドレスを自動的に取得する」を選択してあるか、再度確認します。
- ⑨「インターネットプロトコルバージョン4(TCP/IPv4)のプロパティ」の[OK]をクリックします。
- ⑩「ローカルエリア接続のプロパティ」の[OK]をクリックします。
- ⑪「ローカルエリア接続の状態」の[閉じる]をクリックします。

(3) ネットワークの設定を確認する

- ①「ローカルエリア接続の状態」を表示
「ネットワークの設定」の手順①～④を行います
- ②「ローカルエリア接続の状態」で「詳細」をクリック
[詳細]をクリックします。
- ③IPアドレスを確認
以下の個所に設定が反映されたことを確認します。
・IPv4 IPアドレス
・IPv4 サブネットマスク
・IPv4 デフォルトゲートウェイ
これらのアドレスはすべて自動で設定されます。

●各情報が正常に設定されていない場合は、パソコンと本装置の電源を切ってから電源やケーブルなどの接続を確認し、本装置の電源を入れてからパソコンの電源を入れ、手順①からやり直してください。

4.1.2.5 Windows® XP 利用時の準備

下記の手順にしたがってパソコンを設定します

(1) インターネットプロパティの設定

- ①コントロールパネルを表示
Windows® XP を起動し、「スタート」メニューから「コントロールパネル」をクリックします。
- ②「ネットワークとインターネット」を表示
コントロールパネルの「ネットワークとインターネット接続」をクリックします。
- ③「インターネットオプション」を表示
「ネットワークとインターネット接続」の「インターネットオプション」をクリックします。
- ④ [接続]タブで[ダイヤルしない]を選択
「インターネットのプロパティ」の「接続」タブをクリックします。
「ダイヤルアップと仮想プライベートネットワークの設定」で「ダイヤルしない」が選択されていることを確認します。
[ネットワーク接続が存在しないときには、ダイヤルする]や[通常の接続でダイヤルする]が選択されている場合は、[ダイヤルしない]をクリックします。
- ⑤ ローカルエリアネットワーク(LAN)の設定の[LANの設定]をクリックします。
- ⑥ ローカルエリアネットワーク(LAN)の設定を次のように設定します。
 - 「自動構成」のチェックを外す。
「設定を自動的に検出する」、「自動構成スクリプトを使用する」のチェックがついていないことを確認する。チェックがついている場合は、すべてのチェックを外す。
 - 「プロキシサーバ」のチェックを外す。
「LANにプロキシサーバを使用する」のチェックが付いている場合は、チェックを外し、[OK]をクリックする。
- ⑦「インターネットのプロパティ」の[OK]をクリックする。

(2) ネットワークの設定

- ①「コントロールパネル」を表示
Windows® XP を起動し、「スタート」メニューから「コントロールパネル」をクリックします。
- ②「ネットワークとインターネット接続」を表示
コントロールパネルの「ネットワークとインターネット接続」をクリックします。
- ③「ネットワーク接続」を表示
「ネットワークとインターネット接続」の「ネットワーク接続」をクリックします。
- ④「ローカルエリア接続の状態」を表示
「LANまたは高速インターネット」内の「ローカルエリア接続」をダブルクリックします。

●「ネットワーク接続」の「ブロードバンド」の欄に、PPPoE設定がされていて、その設定が既定の接続に設定されている場合には、PPPoEのアイコンを右クリックして、表示されるサブメニューの「既定の接続を解除」を選択し、クリックします。

- ⑤「ローカルエリア接続のプロパティ」を表示
「ローカルエリア接続の状態」の[プロパティ]をクリックします。
- ⑥「インターネットプロトコル(TCP/IP)のプロパティ」を表示
「ローカルエリア接続のプロパティ」の一覧から[インターネットプロトコル(TCP/IP)]を選択し、[プロパティ]をクリックします。
- ⑦IPアドレスとDNSを設定
「インターネットプロトコル(TCP/IP)のプロパティ」の[IPアドレスを自動的に取得する]と、「DNSサーバのアドレスを自動的に取得する」を選択します。
IPアドレスとDNSの設定を確認したら[詳細設定]をクリックします。
- ⑧DHCP設定を確認し、[OK]をクリック
「TCP/IP詳細設定」の[IP設定]タブをクリックして、一覧に「DHCP有効」と表示されているか確認します。
- 「DHCP有効」となっていない場合、手順7の画面で「IPアドレスを自動的に取得する」と、「DNSサーバのアドレスを自動的に取得する」を選択してあるか、再度確認します。
- ⑨「インターネットプロトコル(TCP/IP)のプロパティ」の[OK]をクリックします。
- ⑩「ローカルエリア接続のプロパティ」の[OK]をクリックします。
- ⑪「ローカルエリア接続の状態」の[閉じる]をクリックする。

(3) ネットワークの設定を確認する

- ①「ローカルエリア接続の状態」を表示
「ネットワークの設定」の手順①～④を行います。
- ②[サポート]タブで「接続状態」を確認
「ローカルエリア接続の状態」の[サポート]タブをクリックします。
- ③IPアドレスを確認
以下の個所に設定が反映されたことを確認します。
・IPアドレス
・サブネットマスク
・デフォルトゲートウェイ
これらのアドレスはすべて自動で設定される。

- 各情報が正常に設定されていない場合は、[修復]をクリックします。
IPアドレス、サブネットマスク、デフォルトゲートウェイの各情報が再度表示されます。

●[修復]をクリックしても各情報が正常に設定されていない場合は、パソコンと本装置の電源を切ってから電源やケーブルなどの接続を確認し、本装置の電源を入れてからパソコンの電源を入れ、手順①からやり直してください。

4.1.2.6 ウェブブラウザの準備

以下の手順に従い、パソコンのウェブブラウザの設定を行います。

(1) JavaScript の設定

- ① Internet Explorer®を起動し、ツールバーの「ツール」→「インターネットオプション」をクリックします。
- ② 「セキュリティ」タブをクリックし、[レベルのカスタマイズ]をクリックします。
- ③ スクリプト項目のアクティブスクリプトが [有効にする]に設定されていることを確認し、[OK]をクリックします。

(2) キャッシュ機能の設定

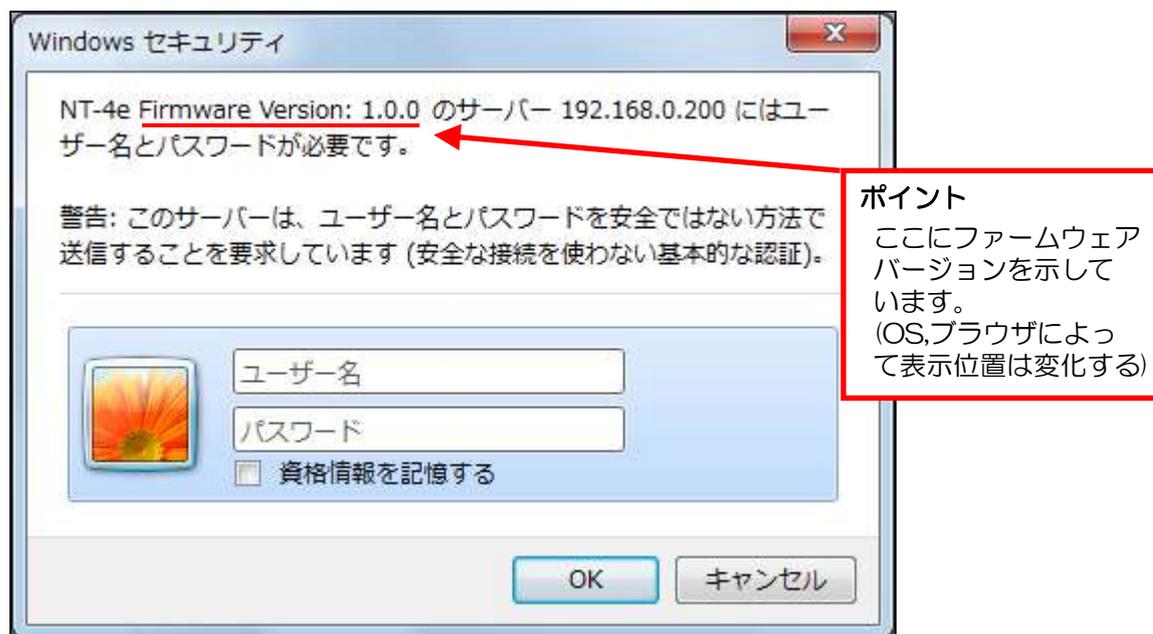
- ① Internet Explorer®を起動し、ツールバーの「ツール」→「インターネットオプション」をクリックします。
- ② 「全般」タブをクリックし、[閲覧の履歴]の [設定]をクリックします。
- ③ 「ウェブサイトを表示するたびに確認する」に設定されていることを確認し、[OK]をクリックします。

4.1.3 設定画面の URL について

本装置の設定画面にアクセスするための URL は、以下の通りです。

(本装置の LAN 側 IP アドレスを指定します)

http://192.168.0.200/



・ユーザー名とパスワード初期値は下記の通りです

ユーザー名	user
パスワード	00000000

注意事項

※本装置はログアウト操作が無いため、終了時はウェブブラウザを閉じてください。

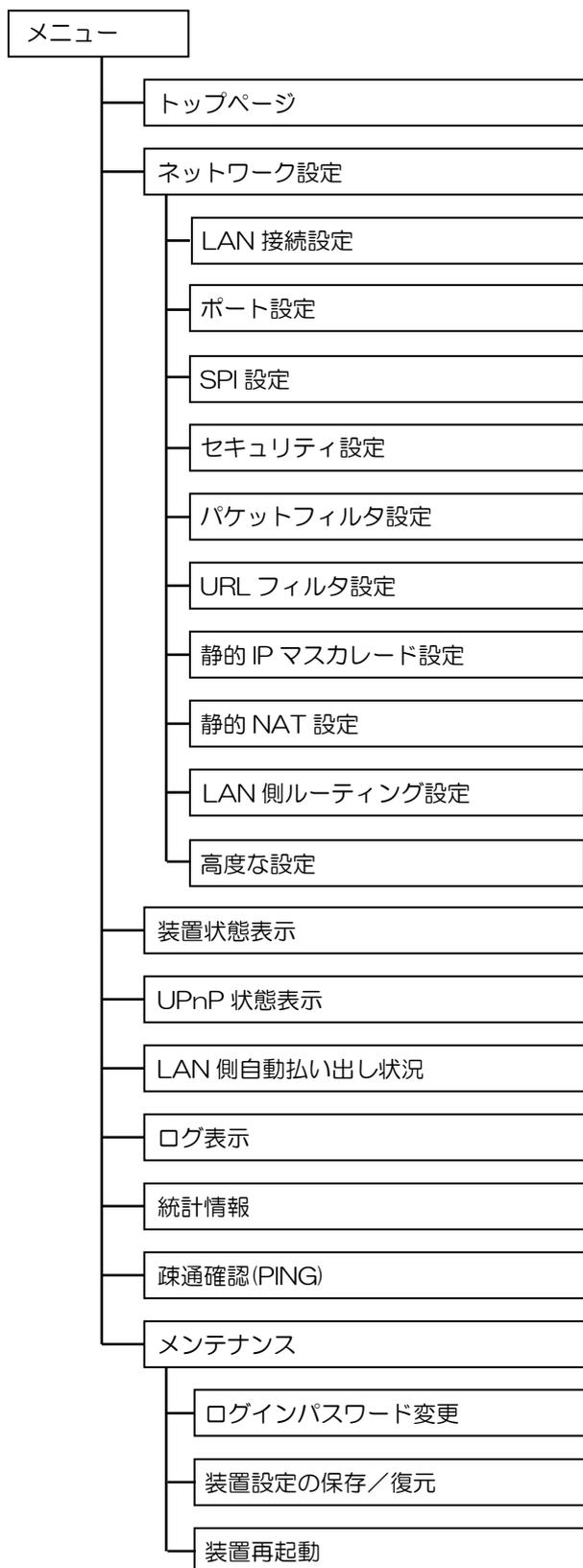
※お客さまにて LAN セグメントの設定を変更している場合、上記とは異なります。

※パスワードをお客さまにて変更されている場合、上記とは異なります。

4.1.4 設定画面メニュー

4.1.4.1 メニュー構成

お客さまにて利用可能なメニューは以下の通りです。



4.1.4.2 設定メニュー画面(最小表示)

NT-4e (BRIタイプ)

— MENU — 操作ヘルプ

- **トップページ**

構成情報設定

- + ネットワーク設定

装置情報表示

- 装置状態表示
- UPnP状態表示
- LAN側自動払い出し状況
- ログ表示
- 統計情報

メンテナンス

- 疎通確認(PING)
- + メンテナンス

Web設定画面です。
メニューを選択してください。

サービス状態

品名/型番	NT-4e(BRIタイプ)/NT4E-BRIKD
ファームウェアバージョン	1.0.0
動作モード	本装置単独
サービス選択	電話、インターネット使用

4.1.4.3 設定メニュー画面(展開表示)

NT-4e (BRIタイプ)

— MENU — 操作ヘルプ

- **トップページ**

構成情報設定

- ネットワーク設定
 - LAN接続設定
 - ポート設定
 - SPI設定
 - IPsec設定
 - セキュリティ設定
 - パケットフィルタ設定
 - URLフィルタ設定
 - 静的IPマスカレード設定
 - 静的NAT設定
 - LAN側ルーティング設定
 - 高度な設定

装置情報表示

- 装置状態表示
- UPnP状態表示
- LAN側自動払い出し状況
- ログ表示
- 統計情報

メンテナンス

- 疎通確認(PING)
- メンテナンス
 - ログインパスワード変更
 - 装置設定の保存/復元
 - 装置再起動

Web設定画面です。
メニューを選択してください。

サービス状態

品名/型番	NT-4e(BRIタイプ)/NT4E-BRIKD
ファームウェアバージョン	1.0.0
動作モード	本装置単独
サービス選択	電話、インターネット使用

4.2 構成情報設定

4.2.1 ネットワーク設定 - LAN 接続設定

LAN 側(LAN セグメント)の接続について設定します。

LAN接続設定

トップページ>ネットワーク設定>LAN接続設定

項目名の末尾に(再)の付いた項目を変更した場合、変更内容を有効にするには再起動が必要になります。

LAN側セグメント設定

IPアドレス/マスク長(再) ?	192.168.0.200 / 24
------------------	--------------------

LAN側セグメント自動払い出し設定

自動払い出し(再) ?	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
リース時間(再) ?	4 時間
払い出し開始IPアドレス(再) ?	192.168.0.201
払い出し個数(再) ?	50
WINSサーバアドレス(再) ?	

【設定手順】

- 1 ウェブブラウザを起動して、設定メニューを開く。
- 2 設定メニューから「ネットワーク設定」をクリックする。
- 3 ネットワーク設定メニューから「LAN 接続設定」をクリックする。
- 4 各項目を設定する。
- 5 「設定保存」ボタンをクリックする。
- 6 項目名に(再)の付いた項目を変更した場合、変更内容を有効にするには、装置の再起動が必要となる。

注意事項

- ※ 本設定を変更後、設定画面にアクセスできなくなる場合がある。
その場合は、ウェブブラウザを一度終了し、接続するパソコンの設定を本装置と合わせたあと、ウェブブラウザを開きなおすこと。

次ページに設定項目を示す。

・LAN 側セグメント設定

設定データ名称	説明	初期値
IP アドレス (再)	LAN 側セグメントの IP アドレスを設定する。	192.168.0.200
マスク長 (再)	LAN 側セグメントのマスク長を設定する。 設定範囲:8~30	24

※ 他セグメントのサブネットと重複はエラーとなりそれぞれ別のサブネットとする必要があります。

・LAN 側セグメント自動払い出し設定

設定データ名称	説明	初期値
自動払い出し (再)	LAN 側セグメントへの DHCP による自動払い出しの使用/未使用を選択する。	使用する
リース時間 (再)	払い出し IP アドレスの貸出時間を設定する。 設定範囲:1~72(時間)	4(時間)
払い出し開始 IP アドレス (再)	払い出し IP アドレスの開始アドレスを設定する。 動作モードをカスケード接続(子)に設定した場合、自動的に [192.168.50.201] に設定される。(設定変更は可能)	192.168.0.201
払い出し個数 (再)	払い出す IP アドレスの個数を設定する。 設定範囲:1~253(最大値は LAN 側セグメントのマスク長による)	50
WINS サーバアドレス (再)	LAN 側セグメントに WINS(Windows Internet Naming Service) サーバがある場合に、DHCP で払い出す WINS サーバのアドレスを設定する。	なし

4.2.2 ネットワーク設定 - ポート設定

WAN、LAN ポートの通信速度、MDI/MDI-X モードについて設定・変更が可能です。

ポート設定

トップページ>ネットワーク設定>ポート設定

ポート設定

ポート種別	通信速度 ?	MDI/MDI-Xモード ?
WAN	AUTO	AUTO
LAN1	AUTO	AUTO
LAN2	AUTO	AUTO
LAN3	AUTO	AUTO
LAN4	AUTO	AUTO

【設定手順】

- 1 ウェブブラウザを起動して、設定メニューを開く。
- 2 設定メニューから「ネットワーク設定」をクリックする。
- 3 ネットワーク設定メニューから「ポート設定」をクリックする。
- 4 各項目を設定する。
- 5 「設定保存」ボタンをクリックする。

注意事項

- ※ 本設定を変更後、設定画面にアクセスできなくなる場合がある。
その場合は、ウェブブラウザを一度終了し、接続するパソコンの設定を本装置と合わせたあと、ウェブブラウザを開きなおすこと。

次ページに設定項目を示す。

・ポート設定(WAN、LAN1~4)

設定データ名称	説明	初期値
通信速度	<p>各ポートの通信速度を選択する。</p> <p>[AUTO] 伝送速度の最大値を 1Gbit/s として、伝送速度/伝送モードを自動で設定する。</p> <p>[AUTO(100M MAX)] 伝送速度の最大値を 100Mbit/s として、伝送速度/伝送モードを自動で設定する。</p> <p>[100M FULL] 伝送速度を 100Mbit/s、伝送モードを全二重に設定する。</p> <p>[100M HALF] 伝送速度を 100Mbit/s、伝送モードを半二重に設定する。</p> <p>[10M FULL] 伝送速度を 10Mbit/s、伝送モードを全二重に設定する。</p> <p>[10M HALF] 伝送速度を 10Mbit/s、伝送モードを半二重に設定する。</p>	AUTO
MDI/MDI-X モード	<p>各ポートの MDI/MDI-X を固定するか、自動切り替えにするかを選択する。 WAN ポートは[AUTO]固定</p> <p>[AUTO] MDI/MDI-X を自動切り替えに設定する。</p> <p>[MDI-X] MDI-X 固定に設定する。</p>	AUTO

※ 通信速度は接続する相手端末、ネットワーク装置と設定を必ず合わせる必要があります。

4.2.3 ネットワーク設定 - SPI 設定

SPI(ステートフル・パケット・インスペクション)機能について設定します。

SPI 機能は常にオンになっており、タイム値を短くすることで、セキュリティが向上する場合がありますが、TCP タイムアウト、UDP タイムアウトの設定が短い場合、接続できなくなる場合がございます。

SPI設定

トップページ>ネットワーク設定>SPI設定

各種SPI設定

TCPタイムアウト?	3600	秒
UDPタイムアウト?	180	秒
ICMPタイムアウト?	60	秒

【設定手順】

- 1 ウェブブラウザを起動して、設定メニューを開く。
- 2 設定メニューから「ネットワーク設定」をクリックする。
- 3 ネットワーク設定メニューから「SPI 設定」をクリックする。
- 4 各項目を設定する。
- 5 「設定保存」ボタンをクリックする。

・各種 SPI 設定

設定データ名称	説明	初期値
TCP タイムアウト	TCP セッション確立後、無通信時のセッションの有効時間を入力する。 設定範囲:30~7200(秒)	3600(秒)
UDP タイムアウト	無通信時の UDP ステート管理の有効時間を入力する。 設定範囲:30~7200(秒)	180(秒)
ICMP タイムアウト	無通信時の ICMP ステートの管理時間を入力する。 設定範囲:30~7200(秒)	60(秒)

4.2.4 ネットワーク設定 - セキュリティ設定

本装置のファイアウォールについて設定します。

セキュリティ設定

トップページ>ネットワーク設定>セキュリティ設定

登録を追加または登録内容を変更するには、該当する番号の[編集]ボタンをクリックしてください。

ファイアウォール設定一覧

番号	ルールNo. (0:無効)	フィルタ種別	送信元IPアドレス			編集
		プロトコル	送信元ポート	宛先ポート	セキュリティログ保存	
		ICMPタイプ	ICMPコード			
1						編集
2						編集
3						編集
4						編集

【設定手順】

- 1 ウェブブラウザを起動して、設定メニューを開く。
- 2 設定メニューから「ネットワーク設定」をクリックする。
- 3 ネットワーク設定メニューから「セキュリティ設定」をクリックする。

次ページへ続く。

- 4 「ファイアウォール設定一覧」で該当するエントリ番号の「編集」をクリックし、エントリ編集画面を表示する。

セキュリティ設定

トップページ>ネットワーク設定>セキュリティ設定>エントリ編集

ファイアウォール設定

エントリ番号	1
ルールNo. <small>?</small>	0 (0:無効)
フィルタ種別 <small>?</small>	拒否 <small>▼</small>
送信元IPアドレス(開始IP - 終了IP) <small>?</small>	* <input type="text"/> ~ * <input type="text"/>
プロトコル <small>?</small>	* <input type="text"/>
送信元ポート(開始ポート - 終了ポート) <small>?</small>	* <input type="text"/>
宛先ポート(開始ポート - 終了ポート) <small>?</small>	* <input type="text"/>
ICMPタイプ <small>?</small>	* <input type="text"/>
ICMPコード <small>?</small>	* <input type="text"/>
セキュリティログ保存 <small>?</small>	<input checked="" type="checkbox"/> 保存する

ファイアウォール設定一覧

番号	ルールNo. (0:無効) <small>?</small>	送信元IPアドレス <small>?</small>		宛先ポート <small>?</small>	セキュリティログ保存 <small>?</small>
		フィルタ種別 <small>?</small>	送信元ポート <small>?</small>		
		プロトコル <small>?</small>	ICMPタイプ <small>?</small>	ICMPコード <small>?</small>	
1					<input type="button" value="編集"/>
2					<input type="button" value="編集"/>

- 5 各項目を設定する。
6 「設定保存」ボタンをクリックする。

次ページに設定項目を示す。

・ファイアウォール設定(エントリ番号 1~96)

設定データ名称	説明	初期値
ルール No.	ファイアウォール設定エントリの優先順位を数値で設定する。 値が小さいほど優先順位が高くなる。 [0]を入力すると、そのエントリは無効になる。 同一の数値を複数エントリに設定することはできない。([0]は除く) 設定範囲:0~999	0
フィルタ種別	ファイアウォール設定に適合したパケットの処理方法を選択する。 [許可] ファイアウォール設定に適合したパケットは中継する。 [拒否] ファイアウォール設定に適合したパケットは破棄する。	拒否
送信元 IP アドレス (開始 IP - 終了 IP)	ファイアウォール設定として、送信元 IP アドレスの範囲を入力する。 すべての送信元 IP アドレスを対象にする場合は、開始 IP/終了 IP に[*] を入力する。 単一の IP アドレスを指定する場合は開始 IP/終了 IP に同じ IP アドレスを を入力する。 設定範囲:* / IPv4 アドレス形式	*
プロトコル	ファイアウォール設定として、プロトコルの番号、または予約済の名前を を入力する。 すべてのプロトコルを対象にする場合は[*]を入力する。 予約済の名前として、[TCP][UDP][ICMP][TCP UDP]が用意されてい る。 設定範囲:* / 予約名 / 1~255	*
送信元ポート (開始ポート - 終了ポート)	ファイアウォール設定として、ポートの番号、または予約済の名前を入力 する。 すべてのポート番号を対象にする場合は[*]を入力する。 予約済の名前として、下記が用意されている。 [ftp][ftpdata][telnet][smtp][domain][www] [pop3][sunrpc][nntp][ntp][login][route][pptp] ポート番号を範囲指定する場合は、最小値と最大値を[-](半角ハイフン) でつないで入力する。 設定範囲:* / 予約名 / 1~65535	*
宛先ポート (開始ポート - 終了ポート)		
ICMP タイプ	ファイアウォール設定として、ICMP タイプを入力する。 「プロトコル」が[ICMP]のときに有効となる。 すべての ICMP タイプを対象にする場合は[*]を入力する。 設定範囲:* / 0~255	*
ICMP コード	ファイアウォール設定として、ICMP コードを入力する。 「プロトコル」が[ICMP]のときに有効となる。 すべての ICMP コードを対象にする場合は[*]を入力する。 「ICMP タイプ」が[*]の場合、[*]以外設定できない。 設定範囲:* / 0~255	*
セキュリティログ保存	ファイアウォール設定に一致し、破棄したパケットがあった場合、セキュ リティログに保存するかどうかを選択する。 「フィルタ種別」が[許可]の場合、[保存する]に設定することはできない。 [保存する](チェックあり) 破棄したパケットがあった場合、セキュリティログに保存する。 [保存しない](チェックなし) 破棄したパケットがあっても、セキュリティログに保存しない。	保存する (チェックあり)

4.2.5 ネットワーク設定 - パケットフィルタ設定

本装置のパケットフィルタについて設定・変更を行います。

パケットフィルタ設定

トップページ>ネットワーク設定>パケットフィルタ設定

登録を追加または登録内容を変更するには、該当する番号の[編集]ボタンをクリックしてください。

パケットフィルタ設定一覧

番号	ルールNo. (0:無効)	通信方向 ?	フィルタ種別 ?	TCPフラグ ?	
		送信元IPアドレス ?		宛先IPアドレス ?	
		プロトコル ?	送信元ポート ?	宛先ポート ?	
		ICMPタイプ ?	ICMPコード ?	セキュリティログ保存 ?	
1					編集
2					編集
3					編集

【設定手順】

- 1 ウェブブラウザを起動して、設定メニューを開く。
- 2 設定メニューから「ネットワーク設定」をクリックする。
- 3 ネットワーク設定メニューから「パケットフィルタ設定」をクリックする。

次ページへ続く。

- 「パケットフィルタ設定一覧」で該当するエントリ番号の「編集」をクリックし、エントリ編集画面を表示する。

パケットフィルタ設定

トップページ>ネットワーク設定>パケットフィルタ設定>エントリ編集

パケットフィルタ設定

エントリ番号	1
ルールNo. <small>?</small>	0 (0:無効)
通信方向 <small>?</small>	WAN→LAN <small>▼</small>
フィルタ種別 <small>?</small>	拒否 <small>▼</small>
TCPフラグ <small>?</small>	指定しない <small>▼</small>
送信元IPアドレス(開始IP - 終了IP) <small>?</small>	* <input type="text"/> ~ * <input type="text"/>
宛先IPアドレス(開始IP - 終了IP) <small>?</small>	* <input type="text"/> ~ * <input type="text"/>
プロトコル <small>?</small>	* <input type="text"/>
送信元ポート(開始ポート - 終了ポート) <small>?</small>	* <input type="text"/>
宛先ポート(開始ポート - 終了ポート) <small>?</small>	* <input type="text"/>
ICMPタイプ <small>?</small>	* <input type="text"/>
ICMPコード <small>?</small>	* <input type="text"/>
セキュリティログ保存 <small>?</small>	<input type="checkbox"/> 保存する

パケットフィルタ設定一覧

番号	ルールNo. <small>?</small> (0:無効)	通信方向 <small>?</small>	フィルタ種別 <small>?</small>	TCPフラグ <small>?</small>	
		送信元IPアドレス <small>?</small>	宛先IPアドレス <small>?</small>		
		プロトコル <small>?</small>	送信元ポート <small>?</small>	宛先ポート <small>?</small>	
		ICMPタイプ <small>?</small>	ICMPコード <small>?</small>	セキュリティログ保存 <small>?</small>	
1					<input type="button" value="編集"/>

- 各項目を設定する。
- 「設定保存」ボタンをクリックする。

次ページに設定項目を示す。

・パケットフィルタ設定(エントリ番号 1~128)

設定データ名称	説明	初期値
ルール No.	パケットフィルタ設定エントリの優先順位を数値で設定する。 値が小さいほど優先順位が高くなる。 [0]を入力すると、そのエントリは無効になる。 同一の数値を複数エントリに設定することはできない。([0]は除く) 設定範囲:0~999	0
通信方向	処理したいパケットの方向を選択する。 [WAN→LAN] WAN から LAN 方向のパケットを処理する。 [LAN→WAN] LAN から WAN 方向のパケットを処理する。 [両方向] 両方向のパケットを処理する。	WAN→LAN
フィルタ種別	フィルタリング条件に適合したパケットの処理方法を選択する。 [許可] フィルタリング条件に適合したパケットは中継される。 [拒否] フィルタリング条件に適合したパケットは破棄される。	拒否
TCP フラグ	フィルタリング条件として、TCP フラグの種類を選択する。 「プロトコル」で[TCP]以外を指定した場合は、「TCP フラグ」の設定は無視される。 [指定しない] フラグを指定しない。 [SYN] コネクション確立要求時のフラグを指定する。 [ESTABLISHED] コネクション確立後のフラグを指定する。	指定しない
送信元 IP アドレス (開始 IP - 終了 IP)	フィルタリング条件として、送信元 IP アドレスの範囲を入力する。 すべての送信元 IP アドレスを対象にする場合は、開始 IP/終了 IP に[*]を入力する。 単一の IP アドレスを指定する場合は開始 IP/終了 IP に同じ IP アドレスを入力する。 設定範囲:* / IPv4 アドレス形式	*
宛先 IP アドレス (開始 IP - 終了 IP)	フィルタリング条件として、宛先 IP アドレスの範囲を入力する。 すべての宛先 IP アドレスを対象にする場合は、開始 IP/終了 IP に[*]を入力する。 単一の IP アドレスを指定する場合は開始 IP/終了 IP に同じ IP アドレスを入力する。 設定範囲:* / IPv4 アドレス形式	*

次ページへ続く。

設定データ名称	説明	初期値
プロトコル	フィルタリング条件として、プロトコルの番号、または予約済の名前を入力する。 すべてのプロトコルを対象にする場合は[*]を入力する。 予約済の名前として、[TCP][UDP][ICMP][TCP UDP]が用意されている。 設定範囲*/ 予約名 / 1~255	*
送信元ポート (開始ポート - 終了ポート)	フィルタリング条件として、ポートの番号、または予約済の名前を入力する。 すべてのポート番号を対象にする場合は[*]を入力する。 予約済の名前として、下記が用意されている。 [ftp][ftpdata][telnet][smtp][domain][www] [pop3][sunrpc][nntp][ntp][login][route][ppp] ポート番号を範囲指定する場合は、最小値と最大値を[-](半角ハイフン)で つないで入力する。 設定範囲*/ 予約名 / 1~65535	*
宛先ポート (開始ポート - 終了ポート)		
ICMP タイプ	フィルタリング条件として、ICMP タイプを入力する。 「プロトコル」が[ICMP]のときに有効となる。 すべての ICMP タイプを対象にする場合は[*]を入力する。 設定範囲*/ 0~255	*
ICMP コード	フィルタリング条件として、ICMP コードを入力する。 「プロトコル」が[ICMP]のときに有効となる。 すべての ICMP コードを対象にする場合は[*]を入力する。 「ICMP タイプ」が[*]の場合、[*]以外設定できない。 設定範囲*/ 0~255	*
セキュリティログ保存	フィルタリング条件に一致し、破棄したパケットがあった場合、セキュリティログに保存するかどうかを選択する。 「フィルタ種別」が[許可]の場合、[保存する]に設定することはできない。 [保存する](チェックあり) 破棄したパケットがあった場合、セキュリティログに保存する。 [保存しない](チェックなし) 破棄したパケットがあっても、セキュリティログに保存しない。	保存しない (チェックなし)

次ページへ続く。

4.2.6 ネットワーク設定 - URL フィルタ設定

本装置の URL フィルタについて設定・変更を行います。

URLフィルタ設定

トップページ>ネットワーク設定>URLフィルタ設定

登録を追加または登録内容を変更するには、該当する番号の[編集]ボタンをクリックしてください。

URLフィルタ許可設定

URLフィルタ 使用しない

URLフィルタ設定一覧

番号	比較条件 <input type="checkbox"/>	比較文字 <input type="checkbox"/>	
1			<input type="button" value="編集"/>
2			<input type="button" value="編集"/>
3			<input type="button" value="編集"/>
4			<input type="button" value="編集"/>
5			<input type="button" value="編集"/>

【設定手順】

- 1 ウェブブラウザを起動して、設定メニューを開く。
- 2 設定メニューから「ネットワーク設定」をクリックする。
- 3 ネットワーク設定メニューから「URL フィルタ設定」をクリックする。

次ページへ続く。

4 「URL フィルタ許可設定」を設定する。

・URL フィルタ許可設定

設定データ名称	説明	初期値
URL フィルタ	URL フィルタ方式を設定する。 [使用しない] URL フィルタを使用しない。 [許可リスト設定] 設定した URL のみ DNS サーバへのアクセスを許可する。 [拒否リスト設定] 設定した URL の DNS サーバへのアクセスを拒否する。	使用しない

5 「設定保存」をクリックして、設定した内容を保存する。

6 「URL フィルタ設定一覧」で該当するエントリ番号の「編集」をクリックし、エントリ編集画面を表示する。

URLフィルタ設定

トップページ>ネットワーク設定>URLフィルタ設定>エントリ編集

URLフィルタ設定

エントリ番号	1
比較条件 ?	ドメイン ▼
比較文字(後方一致) ?	

URLフィルタ設定一覧

番号	比較条件 ?	比較文字 ?	
1			<input type="button" value="編集"/>
2			<input type="button" value="編集"/>

7 各項目を設定する。

8 「設定保存」ボタンをクリックする。

次ページに設定項目を示す。

・URL フィルタ設定(エントリ番号 1~20)

設定データ名称	説明	初期値
比較条件	<p>比較条件を設定する。</p> <p>[ドメイン] ドット区切りを明確に判定する。比較は後方一致で行う 例) URL http://www.kddi.co.jp →ドメイン www.kddi.co.jp 比較文字列 jp > 一致 比較文字列 co.jp > 一致 比較文字列 kddi.co.jp > 一致 比較文字列 ddi.co.jp > 不一致 比較文字列 kddi.co > 不一致(後方一致しない) 比較文字列 www > 不一致(後方一致しない)</p> <p>[キーワード] ドット区切りを識別せずに判定する。 例) URL http://www.kddi.co.jp →ドメイン www.kddi.co.jp 比較文字列 jp > 一致 比較文字列 co.jp > 一致 比較文字列 kddi.co.jp > 一致 比較文字列 ddi.co.jp > 一致 比較文字列 kddi.co > 一致 比較文字列 www > 一致 比較文字列 kddi.co.jp > 不一致</p>	ドメイン
比較文字	<p>比較条件に使用する文字列を設定する。 最大文字数:半角 255 文字 使用可能文字:半角英数字/一部記号(「.」「-」)</p>	なし

※URL フィルタを設定しても、その時点で既にウェブ画面が表示されている場合は表示を継続することがあります。この場合はブラウザを再起動してください。

4.2.7 ネットワーク設定 - 静的 IP マスカレード設定

本装置の静的 IP マスカレードについて設定・変更を行います。

静的IPマスカレード設定

トップページ>ネットワーク設定>静的IPマスカレード設定

NAPTテーブルの静的登録ができます。IPアドレスの変換に加えて、ポート番号を固定的に変換する場合に使用します。
登録を追加または登録内容を変更するには、該当する番号の[編集]を押してください。

静的IPマスカレード設定一覧

番号	優先順位	宛先IPアドレス	変換対象プロトコル	
		宛先ポート	変換対象ポート	
1				編集
2				編集
3				編集
4				編集
5				編集

【設定手順】

- 1 ウェブブラウザを起動して、設定メニューを開く。
- 2 設定メニューから「ネットワーク設定」をクリックする。
- 3 ネットワーク設定メニューから「静的 IP マスカレード設定」をクリックする。

次ページへ続く。

- 4 「静的 IP マスカレード設定一覧」で該当するエントリ番号の「編集」をクリックし、エントリ編集画面を表示する。

静的IPマスカレード設定

トップページ>ネットワーク設定>静的IPマスカレード設定>エントリ編集

[戻る](#)

静的IPマスカレード設定

エントリ番号	1
優先順位 ?	<input type="text"/>
宛先IPアドレス ?	<input type="text"/>
変換対象プロトコル ?	TCP ▼
宛先ポート ?	<input type="text"/>
変換対象ポート ?	<input type="text"/>

[設定保存](#) [元に戻す](#)

静的IPマスカレード設定一覧

番号	優先順位 ?	宛先IPアドレス ?	変換対象プロトコル ?	
		宛先ポート ?	変換対象ポート ?	
1				編集
2				編集
3				編集

- 5 各項目を設定する。
6 「設定保存」ボタンをクリックする。

次ページに設定項目を示す。

・静的 IP マスカレード設定(エントリ番号 1~50)

設定データ名称	説明	初期値
優先順位	<p>静的 IP マスカレード設定エントリの優先順位を数値で設定する。</p> <p>値が小さいほど優先順位が高くなり、最初に合致したエントリで動作する。</p> <p>[0]を入力すると、そのエントリは無効になる。</p> <p>同一の数値を複数エントリに設定することはできない。</p> <p>設定範囲:0~999</p>	0
宛先 IP アドレス	<p>LAN 側端末の IP アドレスを指定する。</p> <p>WAN 側に公開したいアプリケーションが実行されている端末を指定する。</p>	なし
変換対象 プロトコル	<p>WAN 側に公開したいアプリケーションが使用するプロトコルを選択する。</p> <p>[TCP] アプリケーションが使用するプロトコルとして TCP を選択する。</p> <p>[UDP] アプリケーションが使用するプロトコルとして UDP を選択する。</p> <p>[TCP と UDP 両方] アプリケーションが使用するプロトコルとして TCP と UDP の両方を選択する。</p>	TCP
宛先ポート	<p>WAN 側に公開したいアプリケーションが LAN 側端末上で使用する TCP/UDP ポート番号、または予約済の名前を入力する。</p> <p>予約済の名前としては、下記が用意されている。</p> <p>[ftp][ftpdata][telnet][smtp][domain][www] [pop3][sunrpc][nntp][ntp][login][route][pptp]</p> <p>設定範囲:予約名 / 1~65535</p>	なし
変換対象ポート	<p>WAN 側に公開したいアプリケーションが使用する TCP/UDP のポート番号、または予約済の名前を入力する。</p> <p>WAN 側からはこのポート番号を指定して、LAN 側端末上で実行中のアプリケーションにアクセスすることができる。</p> <p>予約済の名前としては、下記が用意されている。</p> <p>[ftp][ftpdata][telnet][smtp][domain][www] [pop3][sunrpc][nntp][ntp][login][route][pptp]</p> <p>設定範囲:予約名 / 1~65535</p>	なし

4.2.8 ネットワーク設定 - 静的 NAT 設定

本装置の静的 NAT について設定・変更をおこないます。

静的NAT設定

トップページ>ネットワーク設定>静的NAT設定

登録を追加または登録内容を変更するには、該当する番号の[編集]ボタンをクリックしてください。

静的NAT設定一覧

番号	優先順位 ?	宛先IPアドレス ?	変換対象プロトコル ?	変換対象ポート ?	
1					編集
2					編集
3					編集
4					編集
5					編集
6					編集

【設定手順】

- 1 ウェブブラウザを起動して、設定メニューを開く。
- 2 設定メニューから「ネットワーク設定」をクリックする。
- 3 ネットワーク設定メニューから「静的 NAT 設定」をクリックする。

次ページへ続く。

- 4 「静的 NAT 設定一覧」で該当するエントリ番号の「編集」をクリックし、エントリ編集画面を表示する。

静的NAT設定

トップページ>ネットワーク設定>静的NAT設定>エントリ編集

通話中に[設定保存]ボタン、または[削除]ボタンをクリックして設定変更を行った場合、通話が切断されることがあります。

[戻る](#)

静的NAT設定

エントリ番号	1
優先順位 <small>?</small>	<input type="text"/>
宛先IPアドレス <small>?</small>	<input type="text"/>
変換対象プロトコル <small>?</small>	TCP <small>▼</small>
変換対象ポート(開始ポート - 終了ポート) <small>?</small>	<input type="text"/>

[設定保存](#) [元に戻す](#)

静的NAT設定一覧

番号	優先順位 <small>?</small>	宛先IPアドレス <small>?</small>	変換対象プロトコル <small>?</small>	変換対象ポート <small>?</small>	
1					編集
2					編集

- 5 各項目を設定する。
- 6 「設定保存」ボタンをクリックする。

次ページに設定項目を示す。

・静的 NAT 設定(エントリ番号 1~64)

設定データ名称	説明	初期値
優先順位	<p>静的 NAT 設定エントリの優先順位を数値で設定する。</p> <p>値が小さいほど優先順位が高くなり、最初に合致したエントリで動作する。</p> <p>[0]を入力すると、そのエントリは無効になる。</p> <p>同一の数値を複数エントリに設定することはできない。</p> <p>設定範囲:0~999</p>	0
宛先 IP アドレス	<p>LAN 側端末の IP アドレスを指定する。</p> <p>WAN 側に公開したいアプリケーションが実行されている端末を指定する。</p>	なし
変換対象 プロトコル	<p>WAN 側に公開したいアプリケーションが使用するプロトコルの選択をする。</p> <p>[TCP] アプリケーションが使用するプロトコルとして TCP を選択する。</p> <p>[UDP] アプリケーションが使用するプロトコルとして UDP を選択する。</p> <p>[TCP と UDP 両方] アプリケーションが使用するプロトコルとして TCP と UDP の両方を選択する。</p> <p>[ICMP] アプリケーションが使用するプロトコルとして ICMP を選択する。</p> <p>[全プロトコル(共有)] アプリケーションが使用する全プロトコルを対象とする</p>	TCP
変換対象ポート (開始ポート - 終了ポート)	<p>WAN 側に公開したいアプリケーションが使用する TCP/UDP のポート番号、または予約済の名前を入力する。</p> <p>WAN 側からはこのポート番号を指定して、LAN 側端末上で実行中のアプリケーションにアクセスすることができる。</p> <p>予約済の名前としては、下記が用意されている。</p> <p>[ftp][ftpdata][telnet][smtp][domain][www] [pop3][sunrpc][nntp][ntp][login][route][pptp]</p> <p>ポート番号を範囲指定する場合は、最小値と最大値を[-](半角ハイフン)でつないで入力する。(範囲指定に予約済の名前は使用できない)</p> <p>設定範囲:予約名 / 1~65535</p>	なし

4.2.9 ネットワーク設定 - LAN 側ルーティング設定

本装置の LAN 側静的ルーティングについて設定・変更を行います。

LAN側ルーティング設定

トップページ>ネットワーク設定>LAN側ルーティング設定

IPルーティングテーブルの静的登録ができます。
設定を変更または削除するには、[編集]ボタンをクリックしてください。
設定を追加するには、空欄の[編集]ボタンをクリックしてください。

LAN側ルーティング設定一覧

エントリ番号	宛先IPアドレス/マスク長 ?	ゲートウェイ ?	
1			<input type="button" value="編集"/>
2			<input type="button" value="編集"/>
3			<input type="button" value="編集"/>
4			<input type="button" value="編集"/>
5			<input type="button" value="編集"/>
6			<input type="button" value="編集"/>
7			<input type="button" value="編集"/>
8			<input type="button" value="編集"/>
9			<input type="button" value="編集"/>
10			<input type="button" value="編集"/>

【設定手順】

- 1 ウェブブラウザを起動して、設定メニューを開く。
- 2 設定メニューから「ネットワーク設定」をクリックする。
- 3 ネットワーク設定メニューから「LAN 側ルーティング設定」をクリックする。
- 4 「LAN 側ルーティング設定一覧」で該当するエントリ番号の「編集」ボタンをクリックし、エントリ編集画面を表示する。

LAN側ルーティング設定

トップページ>ネットワーク設定>LAN側ルーティング設定>エントリ編集

LAN側ルーティング設定

エントリ番号	1
宛先IPアドレス/マスク長 <small>?</small>	<input type="text"/> / <input type="text"/>
ゲートウェイ <small>?</small>	<input type="text"/>

LAN側ルーティング設定一覧

エントリ番号	宛先IPアドレス/マスク長 <small>?</small>	ゲートウェイ <small>?</small>	
1			<input type="button" value="編集"/>
2			<input type="button" value="編集"/>

- 5 各項目を設定する。
- 6 「設定保存」ボタンをクリックする。

・LAN 側ルーティング設定(エントリ番号 1~20)

設定データ名称	説明	初期値
宛先 IP アドレス	宛先 IP アドレスを設定する。	なし
マスク長	マスク長を設定する。 設定範囲:8~32	なし
ゲートウェイ	宛先へのゲートウェイアドレスを設定する。	なし

4.2.10 ネットワーク設定 - 高度な設定

UPnP 機能、PING 応答機能、外部へのサーバ公開に関する設定・変更を行います。

高度な設定

トップページ>ネットワーク設定>高度な設定

UPnP設定

UPnP機能 使用する

PING応答機能

インターネット用セグメント応答 応答する

外部へのサーバ公開設定

外部へのサーバ公開 公開しない
 仮想DMZで公開する
 簡易的に公開する

公開するホストのIPアドレス

仮想DMZのIPアドレス空間/マスク長 /
DMZをポートVLANで区分けする 区分けしない

「外部へのサーバ公開」の選択で、設定項目を表示

【設定手順】

- 1 ウェブブラウザを起動して、設定メニューを開く。
- 2 設定メニューから「ネットワーク設定」をクリックする。
- 3 ネットワーク設定メニューから「高度な設定」をクリックする。
- 4 各項目を設定する。
- 5 「設定保存」ボタンをクリックする。

・UPnP 設定

設定データ名称	説明	初期値
UPnP 機能	UPnP を使用する場合は、「使用する」にチェックする。 「Windows [®] Live Messenger」など UPnP が必須のサービスやアプリケーションを利用できる。 また、UPnP で「Windows [®] Live Messenger」などを使用する場合は、パソコンの設定も必要となる。	使用する (チェックあり)

・PING 応答機能

設定データ名称	説明	初期値
インターネット用 セグメント応答	インターネット用セグメントへの PING 応答有無を設定する。	応答する (チェックあり)

次ページへ続く。

・外部へのサーバ公開設定

設定データ名称	説明	初期値
外部へのサーバ公開	外部へのサーバ公開方式を選択する。 [公開しない] 外部へサーバ公開しない。 [仮想 DMZ で公開する] 仮想 DMZ セグメントを設定し公開する。 [簡易的に公開する] LAN 側セグメント内のサーバを設定し公開する。	公開しない
仮想 DMZ の IP アドレス空間	「外部へのサーバ公開」で[仮想 DMZ で公開する]を選択時のみ項目が表示される。 仮想 DMZ の IP アドレス空間を設定する。 ※他セグメントのサブネットと重複は不可。 ※本装置は DNS サーバとして動作できない。	なし
マスク長	「外部へのサーバ公開」で[仮想 DMZ で公開する]を選択時のみ項目が表示される。 仮想 DMZ の IP アドレス空間のマスク長を設定する。 設定範囲:24~30	なし
DMZ をポート VLAN で区別する	「外部へのサーバ公開」で[仮想 DMZ で公開する]を選択時のみ項目が表示される。 DMZ をポート VLAN で区別する/しないを設定する。 [区別しない] DMZ をポート VLAN で区別しない。 [区別する(LAN1~4)] DMZ を指定した LAN ポートで区別する。	区別しない
公開するホストの IP アドレス	「外部へのサーバ公開」で[簡易的に公開する]を選択時のみ項目が表示される。 公開するサーバの IP アドレスを設定する。	なし

4.3 情報表示

本装置の現在の状態や各種ログが表示されます。

4.3.1 装置状態表示

本装置の各種情報を表示します。

装置状態表示

トップページ>装置状態表示

システム状態

ファームウェアバージョン	2.0.0	
現在時刻	2012.5.11 13:38	
ランプ消灯モード	通常動作中	<input type="button" value="ランプ消灯モード解除"/>

ネットワーク状態

インタフェース	通信速度(bit/s)	MACアドレス
WAN	-	00:1F:67:6D:69:9E
LAN1	-	00:1F:67:6D:69:5E
LAN2	1G FULL	
LAN3	-	
LAN4	-	

インターネットセグメントIPアドレス

IPアドレス	3.0.0.2
--------	---------

PPPoE接続状態

電話	-
インターネット	-

PPPoE 接続の場合

ランプ状態

POWER	●	INIT	●	ALARM	●	VoIP	●		
Port1-LY1	●	Port1-LY2	●	Port2-LY1	●	Port2-LY2	●	Clock LY1	●

機種が BRI の場合

ランプ状態

POWER	●	INIT	●	ALARM	●	VoIP	●
BUSY1	●	BUSY2	●	BUSY3	●	BUSY4	●

機種が FXS の場合

【表示手順】

- 1 ウェブブラウザを起動して、設定メニューを開く。
- 2 設定メニューから「装置状態表示」をクリックする。

・システム状態

表示項目	説明
ファームウェアバージョン	本装置で現在運用されているファームウェアバージョンが表示される。
現在時刻	装置内時計の現在時刻が表示される。(自動的には更新しない)
ランプ消灯モード	現在のランプ消灯モードが表示される。(ランプ消灯モード中/通常動作中) 「ランプ消灯モード解除」ボタンで、一時的にランプ消灯モードを解除できる。(30 分経過で、ランプ消灯モードとする。) ユーザー用アカウントでは表示されない。

・ネットワーク状態

表示項目	説明
通信速度(WAN/LAN1~4)	各ポートの通信速度が表示される。
MAC アドレス	各ポートの MAC アドレスが表示される。

・インターネットセグメント IP アドレス

表示項目	説明
IP アドレス	インターネット用セグメントの IP アドレスが表示される。

・PPPoE 接続状態

PPPoE 接続の場合

表示項目	説明
電話	電話用 PPPoE 接続の状態を表示する。(=/接続中/切断中/確立中/停止中)
インターネット	インターネット用 PPPoE 接続の状態を表示する。 (=/接続中/切断中/確立中/停止中)

・ランプ状態

表示項目	説明
各ランプ名称	各ランプの状態が表示される。 ●:点灯 ○:消灯 *:点滅

4.3.2 UPnP 状態表示

UPnP 状態を表示します。

UPnP状態表示						
トップページ>UPnP状態表示						
UPnP状態表示 						
No.	登録日時	要求元IPアドレス	サービスホスト	プロトコル	ローカルホスト	説明
1	2011/09/15 01:11:26	192.168.100.2	192.168.1.2	TCP	192.168.100.200	123

【表示手順】

- 1 ウェブブラウザを起動して、設定メニューを開く。
- 2 設定メニューから「UPnP 状態表示」をクリックする。

・UPnP 状態表示

表示項目	説明
登録日時	本装置がリクエストを受け取った時間を表示する。
要求元 IP アドレス	リクエストを送信した IP アドレスを表示する。
サービスホスト	接続先を表示する。
プロトコル	UPnP 用のアドレス変換 (ポート指定) 設定情報のプロトコルを表示する。
ローカルホスト	ローカルホストを表示する。
説明	UPnP 対応アプリケーションによって設定された説明を表示する。

4.3.3 LAN 側自動払い出し状況表示

LAN 側自動払い出し状況を表示します。

払い出し状況 		
現在の時刻	2011/09/15 10:00:00	
現在の払い出し件数	2	
IPv4アドレス(/マスク長)	MACアドレス	リース終了時間
192.168.100.2/24	00:0B:97:BB:56:E5	2011/09/15 12:00:00
192.168.100.11/24	00:0B:A2:E3:2D:5A	2011/09/15 11:00:00

【表示手順】

- 1 ウェブブラウザを起動して、設定メニューを開く。
- 2 設定メニューから「LAN 側自動払い出し状況表示」をクリックする。

・払い出し状況

表示項目	説明
現在の時刻	現在の時刻を表示する。
現在の払い出し件数	自動払い出し件数を表示する。
IPv4 アドレス(/マスク長)	IPv4 アドレスとマスク長を表示する。
MAC アドレス	MAC アドレスを表示する。
リース終了時間	リース時間を表示する。

4.3.4 ログ表示

各種ログの表示、およびログのクリアを実施します。

ログ表示

トップページ>ログ表示

ログ情報の選択 ?

ログ情報の種類

セキュリティログ ▼

ログ情報の表示

ログ情報のクリア

【表示手順】

- 1 ウェブブラウザを起動して、設定メニューを開く。
- 2 設定メニューから「ログ表示」をクリックする。

・ログ情報の選択

表示項目	説明
ログ情報の種類	ユーザー用アカウントではセキュリティログのみ表示。 [セキュリティログ] 本装置のセキュリティに関するログ。 [すべて(クリアのみ有効)] 全ログをクリアする場合に選択する。

4.3.4.1 セキュリティログ

本装置のセキュリティに関するログを表示します。

- ・ 外部から受信したパケットのうち SPI によって廃棄したパケット
- ・ 外部から受信したパケットのうちパケットフィルタによって廃棄したパケット

ログ表示

トップページ>ログ表示

ログ情報の選択

ログ情報の種類

セキュリティログ

Nb.	受信日時	送信元IPアドレス/ポート	宛先IPアドレス/ポート	プロトコル	アクション
1	2011.01.01 16:40:00	192.168.1.100/65534	192.168.1.101/65534	TCP	廃棄[パケットフィルタ]

【表示手順】

- 1 ウェブブラウザを起動して、設定メニューを開く。
- 2 設定メニューから「ログ表示」をクリックする。
- 3 ログ情報の種類から「セキュリティログ」を選択する。
- 4 [ログ情報の表示]ボタンをクリックする。

注意事項

- ※ プロトコルが TCP/UDP 以外のパケットはポート番号が「-」で表示される。
- ※ フラグメントされた 2 番目以降のパケットはポート番号が「+」で表示される。
- ※ セキュリティログは、電源を切ると登録データが消去される。
- ※ 最大 100 件までのログが表示され、100 件を超えると古いものから順に削除される。

・セキュリティログ

表示項目	説明
受信時間	廃棄したパケットを受信した日時を表示する。
送信元 IP アドレス/ポート	廃棄したパケットの送信先 IP アドレスとポートが表示される。
宛先 IP アドレス/ポート	廃棄したパケットの宛先 IP アドレスとポートが表示される。
プロトコル	廃棄したパケットのプロトコルが表示される。
アクション	パケットを廃棄した要因が表示される。 (廃棄[NAT]/廃棄[SPI]/廃棄[ファイアウォール]/廃棄[パケットフィルタ])

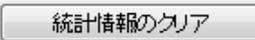
4.3.5 統計情報

各種統計情報の表示、および統計情報のクリアを実施します。

統計情報

トップページ>統計情報

統計情報の選択 

統計情報の種類 LAN   

【表示手順】

- 1 ウェブブラウザを起動して、設定メニューを開く。
- 2 設定メニューから「統計情報」をクリックする。

・統計情報の選択

表示項目	説明
統計情報の種類	表示、またはクリアする統計情報を選択し、各ボタンで実施する。 [LAN] 本装置の LAN の統計情報。 [WAN] 本装置の WAN の統計情報。 [端末ポート] 本装置の端末ポートの統計情報。 [すべて(クリアのみ有効)] 全統計情報をクリアする場合に選択する。

注意事項

- ※ 統計情報が最大値を超えた場合、0 クリアし再カウントする。

4.3.5.1 LAN 統計情報

本装置の LAN の統計情報を表示します。

統計情報

トップページ>統計情報

統計情報の選択 

統計情報の種類 LAN

LAN統計情報

項目	LAN1	LAN2	LAN3	LAN4
受信ユニキャストパケット数	0	0	0	182
受信ブロードキャストパケット数	0	0	0	67
受信マルチキャストパケット数	0	0	0	42
送信ユニキャストパケット数	0	0	0	206
送信ブロードキャストパケット数	0	0	0	2
送信マルチキャストパケット数	0	0	0	0
送信エラーパケット数	0	0	0	0
送信破棄パケット数	0	0	0	0
コリジョン発生回数	0	0	0	0
レートコリジョン発生回数	0	0	0	0
受信異常発生回数	0	0	0	0
受信アライメント異常発生回数	0	0	0	0
受信FCSエラー発生回数	0	0	0	0
受信パラメータ異常発生回数	0	0	0	0
受信フラグメント発生回数	0	0	0	0
受信破棄パケット数	0	0	0	6
不正キャリアセンス検出回数	0	0	0	0

【表示手順】

- 1 ウェブブラウザを起動して、設定メニューを開く。
- 2 設定メニューから「統計情報」をクリックする。
- 3 ログ情報の種類から「LAN」を選択する。
- 4 [統計情報の表示]ボタンをクリックする。

注意事項

※ LAN 統計情報は、電源を切ると消去される。

・LAN 統計情報(LAN1~LAN4)

表示項目	説明	最大値
受信ユニキャストパケット数	受信ユニキャストパケット数を表示する。	4294967295
受信ブロードキャストパケット数	受信ブロードキャストパケット数を表示する。	
受信マルチキャストパケット数	受信マルチキャストパケット数を表示する。	
送信ユニキャストパケット数	送信ユニキャストパケット数を表示する。	
送信ブロードキャストパケット数	送信ブロードキャストパケット数を表示する。	
送信マルチキャストパケット数	送信マルチキャストパケット数を表示する。	
送信エラーパケット数	コリジョンにより再送リミットが発生した回数を表示する。	
送信廃棄パケット数	送信エラーなどで廃棄したパケット数を表示する。	
コリジョン発生回数	コリジョンが発生した回数を表示する。	
レートコリジョン発生回数	レートコリジョンが発生した回数を表示する。	
受信異常発生回数	パケット受信時に異常となった回数を表示する。	
受信アライメント異常発生回数	パケット受信時にアライメント異常が発生した回数を表示する。	
受信 FCS エラー発生回数	受信パケットの FCS エラー発生回数を表示する。	
受信パラメータ異常発生回数	受信パケットのパラメータ異常が発生した回数を表示する。	
受信フラグメント発生回数	パケット受信時にフラグメントが発生した回数を表示する。	
受信廃棄パケット数	受信エラーなどで廃棄したパケット数を表示する。	
不正キャリアセンス検出回数	不正キャリアセンスを検出した回数を表示する。	

4.3.5.2 WAN 統計情報

本装置の WAN の統計情報を表示します。

統計情報

トップページ>統計情報

統計情報の選択 

統計情報の種類 WAN

WAN統計情報

受信ユニキャストパケット数	0
受信ブロードキャストパケット数	0
受信マルチキャストパケット数	0
送信ユニキャストパケット数	0
送信ブロードキャストパケット数	0
送信マルチキャストパケット数	0
送信エラーパケット数	0
送信破棄パケット数	0
コリジョン発生回数	0
レートコリジョン発生回数	0
受信異常発生回数	0
受信アライメント異常発生回数	0
受信FCSエラー発生回数	0
受信パラメータ異常発生回数	0
受信フラグメント発生回数	0
受信破棄パケット数	0
不正キャリアセンス検出回数	0

【表示手順】

- 1 ウェブブラウザを起動して、設定メニューを開く。
- 2 設定メニューから「統計情報」をクリックする。
- 3 ログ情報の種類から「WAN」を選択する。
- 4 [統計情報の表示]ボタンをクリックする。

注意事項

- ※ WAN 統計情報は、電源を切ると消去される。

・WAN 統計情報

表示項目	説明	最大値
受信ユニキャストパケット数	受信ユニキャストパケット数を表示する。	4294967295
受信ブロードキャストパケット数	受信ブロードキャストパケット数を表示する。	
受信マルチキャストパケット数	受信マルチキャストパケット数を表示する。	
送信ユニキャストパケット数	送信ユニキャストパケット数を表示する。	
送信ブロードキャストパケット数	送信ブロードキャストパケット数を表示する。	
送信マルチキャストパケット数	送信マルチキャストパケット数を表示する。	
送信エラーパケット数	コリジョンにより再送リミットが発生した回数を表示する。	
送信廃棄パケット数	送信エラーなどで廃棄したパケット数を表示する。	
コリジョン発生回数	コリジョンが発生した回数を表示する。	
レートコリジョン発生回数	レートコリジョンが発生した回数を表示する。	
受信異常発生回数	パケット受信時に異常となった回数を表示する。	
受信アライメント異常発生回数	パケット受信時にアライメント異常が発生した回数を表示する。	
受信 FCS エラー発生回数	受信パケットの FCS エラー発生回数を表示する。	
受信パラメータ異常発生回数	受信パケットのパラメータ異常が発生した回数を表示する。	
受信フラグメント発生回数	パケット受信時にフラグメントが発生した回数を表示する。	
受信廃棄パケット数	受信エラーなどで廃棄したパケット数を表示する。	
不正キャリアセンス検出回数	不正キャリアセンスを検出した回数を表示する。	

4.3.5.3 端末ポート統計情報

本装置の端末ポートの統計情報を表示します。

統計情報

トップページ>統計情報

統計情報の選択

統計情報の種類 端末ポート 統計情報の表示 統計情報のクリア

端末ポート統計情報 BRI 対応の場合

項目	ポート1		ポート2	
	チャンネル1	チャンネル2	チャンネル1	チャンネル2
RTP統計	RTP送信パケット数	0	0	0
	RTP受信パケット数	0	0	0
	RTP送信廃棄パケット数	0	0	0
	RTP受信廃棄パケット数	0	0	0
	RTCP送信パケット数	0	0	0
	RTCP受信パケット数	0	0	0
	RTCP送信廃棄パケット数	0	0	0
	RTCP受信廃棄パケット数	0	0	0
受信ゆらぎ	ゆらぎ最大時間(ms)	0	0	0
	ゆらぎ最小時間(ms)	0	0	0
	ゆらぎ時間[0ms]パケット数	0	0	0
	ゆらぎ時間[20ms]パケット数	0	0	0
	ゆらぎ時間[40ms]パケット数	0	0	0
	ゆらぎ時間[60ms]パケット数	0	0	0
	ゆらぎ時間[80ms]パケット数	0	0	0
	ゆらぎ時間[100ms]パケット数	0	0	0
	ゆらぎ時間[120ms]パケット数	0	0	0
	ゆらぎ時間[140ms]パケット数	0	0	0
	ゆらぎ時間[160ms]パケット数	0	0	0
	ゆらぎ時間[180ms]パケット数	0	0	0
	ゆらぎ時間[200ms]パケット数	0	0	0
	ゆらぎ時間(その他)パケット数	0	0	0

【表示手順】

- 1 ウェブブラウザを起動して、設定メニューを開く。
- 2 設定メニューから「統計情報」をクリックする。
- 3 ログ情報の種類から「端末ポート」を選択する。
- 4 [統計情報の表示]ボタンをクリックする。

注意事項

※ 端末ポート統計情報は、電源を切ると消去される。

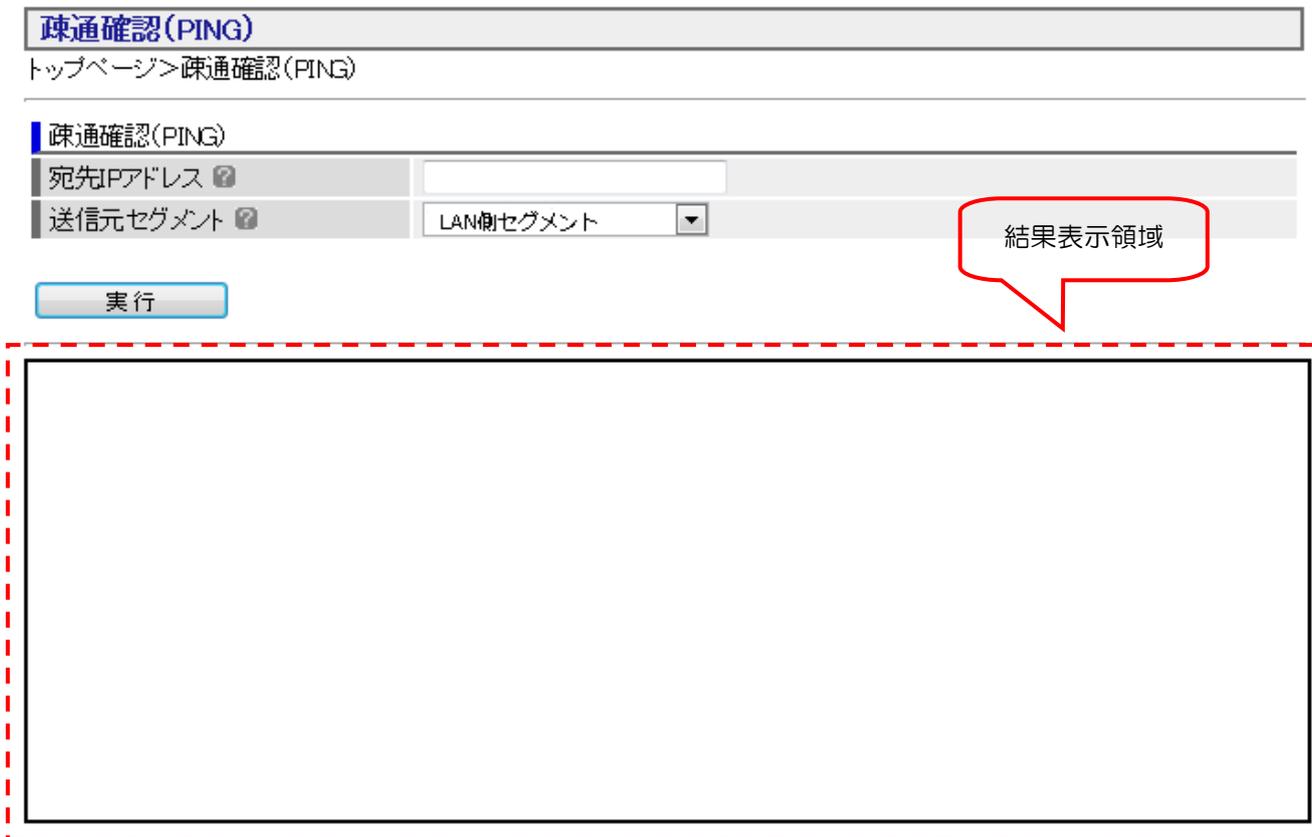
・端末ポート統計情報(FXS:ポート 1~ポート 4、BRI:ポート 1 チャンネル 1~ポート 2 チャンネル 2)

表示項目	説明	最大値
RTP 送信パケット数	RTP 送信パケット数を表示する。	999999999
RTP 受信パケット数	RTP 受信パケット数を表示する。	
RTP 送信破棄パケット数	RTP 送信破棄パケット数を表示する。	
RTP 受信破棄パケット数	RTP 受信破棄パケット数を表示する。	
RTCP 送信パケット数	RTCP 送信パケット数を表示する。	
RTCP 受信パケット数	RTCP 受信パケット数を表示する。	
RTCP 送信破棄パケット数	RTCP 送信破棄パケット数を表示する。	
RTCP 受信破棄パケット数	RTCP 受信破棄パケット数を表示する。	
ゆらぎ最大時間(ms)	RTP 受信パケットの最大ゆらぎ時間を表示する。	
ゆらぎ最小時間(ms)	RTP 受信パケットの最小ゆらぎ時間を表示する。	
ゆらぎ時間[xxms]/パケット数	当該時間を中心値として前後10ms間で受信したRTPパケット数を表示する。	
ゆらぎ時間(その他)/パケット数	ゆらぎ時間が200msを越えたパケット数を表示する。	

4.4 メンテナンス

4.4.1 疎通確認(PING)

PING テストを実施します。



疎通確認(PING)

トップページ>疎通確認(PING)

疎通確認(PING)

宛先IPアドレス ?

送信元セグメント ? LAN側セグメント

実行

結果表示領域

【疎通確認手順】

- 1 ウェブブラウザを起動して、設定メニューを開く。
- 2 設定メニューから「疎通確認(PING)」をクリックする。
- 3 「宛先 IP アドレス」を設定する。
- 4 「送信元セグメント」を選択する。
- 5 「実行」ボタンをクリックする。
- 6 数秒後に画面が切り替わり、結果表示領域に疎通確認結果が表示される。
結果に「0% packet loss」という表示があれば、疎通確認成功となる。
この表示が無い場合、疎通確認は失敗している。

・疎通確認(PING)

項目	説明
宛先 IP アドレス	疎通確認(PING)を実施する IP アドレスを入力する。
送信元セグメント	送信元となるセグメントをプルダウンにより選択する。

4.4.2 メンテナンス - ログインパスワード変更

本装置の設定画面へウェブブラウザからログインするためのパスワードを設定します。

ログインパスワード変更	
トップページ>メンテナンス>ログインパスワード変更	
ログインパスワード変更	
新しいパスワード 	<input type="text"/> [半角英数字(A~Z, a~z, 0~9, -, /, _)16文字まで]
新しいパスワード(確認用) 	<input type="text"/> [半角英数字(A~Z, a~z, 0~9, -, /, _)16文字まで]
<input type="button" value="設定保存"/>	
※ ログインのパスワード変更を行う画面です。注意して操作してください。	

【変更手順】

- 1 ウェブブラウザを起動して、設定メニューを開く。
- 2 設定メニューから「メンテナンス」をクリックする。
- 3 メンテナンスメニューから「ログインパスワード変更」をクリックする。
- 4 「新しいパスワード」と「新しいパスワード(確認用)」に変更後のパスワードを入力する。
- 5 「設定保存」ボタンをクリックして、設定した内容を保存する。

・ログインパスワード変更

項目	説明
新しいパスワード	変更後のパスワードを入力する。 最大文字数:16文字 使用可能文字:半角英数字/一部記号(「-」「/」「_」)
新しいパスワード(確認用)	変更後のパスワードの確認入力。 最大文字数:16文字 使用可能文字:半角英数字/一部記号(「-」「/」「_」)

4.4.3 メンテナンス - 装置設定の保存/復元

装置設定の保存と復元ができます。

復元を実施した場合、現在の設定は破棄されます。

装置設定の保存/復元

トップページ>メンテナンス>装置設定の保存/復元

装置設定値の保存と復元ができます。
復元を行うと現在の設定は破棄されます。
構成情報ファイルのファイル名とディレクトリ名には、全角文字及び半角カナが使用できないことがあります。

装置設定の保存

ユーザ用構成情報ファイルをPCIに保存

保存

装置設定の復元

復元する構成情報ファイルを選択

参照...

選択中の構成情報ファイルをもとに復元

復元

【装置設定の保存手順 ユーザー用】

- 1 ウェブブラウザを起動して、設定メニューを開く。
- 2 設定メニューから「メンテナンス」をクリックする。
- 3 メンテナンスメニューから「装置設定の保存/復元」をクリックする。
- 4 「ユーザー用構成情報ファイルをパソコンに保存」の「保存」ボタンをクリックする。
- 5 ダウンロードの確認ダイアログが表示されたら「保存」ボタンをクリックする。
- 6 保存するディレクトリを選択し、「保存」ボタンをクリックする。

注意事項

- ※ ユーザー用の構成情報ファイルには、ユーザ用アカウントで変更可能な構成情報だけが保存される。

【装置設定の復元手順】

- 1 ウェブブラウザを起動して、設定メニューを開く。
- 2 設定メニューから「メンテナンス」をクリックする。
- 3 メンテナンスメニューから「装置設定の保存/復元」をクリックする。
- 4 復元するファイル名をドライブ名から入力するか、「参照」ボタンをクリックして、ファイルを選択する。
- 5 「復元」ボタンをクリックする。
- 6 メッセージが表示されたら、「OK」ボタンをクリックする。
- 7 ファイルが正常な場合、自動的に再起動される。

注意事項

- ※ 通話中に装置設定の復元を実施すると、通話が切断される。(緊急通報中を除く)
- ※ パスワードは復元されない。

4.4.4 メンテナンス - 装置再起動

本装置を再起動します。

装置再起動

トップページ>メンテナンス>装置再起動

装置の再起動を行います。
現在の接続を一旦切断した後、機器を再起動します。

装置の再起動 ?

装置の再起動

【再起動手順】

- 1 ウェブブラウザを起動して、設定メニューを開く。
- 2 設定メニューから「メンテナンス」をクリックする。
- 3 メンテナンスメニューから「装置再起動」をクリックする。
- 4 「実行」ボタンをクリックする。

注意事項

- ※ 再起動が完了するまで、本装置の電源を絶対に切らないこと。
- ※ 通話中に再起動を実施すると、通話が切断される。
ただし、緊急通報中はエラーメッセージが表示され、再起動されない。
- ※ 再起動が完了するまで、約 1 分 30 秒かかる。
- ※ インターネット接続を行っている場合は、接続が切断される。
- ※ 再起動実施で LAN リンク断が 2 回発生する。(リンクアップ中に再起動で、リンクダウン⇒リンクアップ⇒リンクダウン⇒リンクアップとなる。)

5 機器仕様編

5.1 方式諸元

5.1.1 ハードウェア諸元

	項目	仕様
WAN ポート	物理インターフェース	8ピンモジュージャック(RJ-45)
	ポート数	1ポート
	規格	1000BASE-T/100BASE-TX/10BASE-T (IEEE802.3ab/IEEE802.3u/IEEE802.3) オートネゴシエーション
LAN ポート	物理インターフェース	8ピンモジュージャック(RJ-45)
	ポート数	4ポート(スイッチングハブ内蔵)
	規格	1000BASE-T/100BASE-TX/10BASE-T (IEEE802.3ab/IEEE802.3u/IEEE802.3) オートネゴシエーション
FXS ポート	物理インターフェース	6ピンモジュージャック(RJ-11)
	ポート数	4ポート
	規格	TTC 標準 JT-I431 準拠
BRI(CLK) ポート	物理インターフェース	8ピンモジュージャック(RJ-45)
	ポート数	2ポート(1ポート)
	規格	TTC 標準 JT-I430 準拠
VoIP	音声符号化則	ITU-T JT-G.711(μ Law)
	DTMF	みなし音声(透過)
	エコーキャンセラ	ITU-T JT-G.168(64ms)
	音声レベル	10 ~ 0 ~ -18dB(2dB ステップ)
ランプ表示	POWER ランプ	電源状態表示
	INIT ランプ	工場出荷状態表示
	ALARM ランプ	障害状態表示
	VoIP ランプ	音声通信状態表示
	WAN ACT ランプ	WAN 状態表示
	WAN SPEED ランプ	WAN 速度表示
	表示なしランプ	親子設定状態表示
	FXS1~4 BUSY ランプ	FXS 状態表示
	BRI1~2・CLK LY1 ランプ	BRI 状態表示
	BRI1~2 LY2 ランプ	BRI 状態表示
	LAN SPD ランプ	LAN 速度表示
	LAN ACT ランプ	LAN 状態表示
操作部	e ボタン	ランプ消灯モード復旧ボタン
	INIT ボタン	設定初期化用ボタン ※初期状態に戻り、IP 網との接続が出来なくなるため、使用しないでください。
	スライドスイッチ	CLK ポート終端抵抗オン/オフスイッチ
クロック精度	自走時:±50ppm 従属時:外部供給クロック精度による	
筐体外観	横置き型	
動作環境	温度:0~40℃ 湿度:20~80%(結露しないこと) 塵埃:5%/W 以下または、0.15mg/m ³ 以下	
外形寸法	約 210(W)×160(D)×55(H)mm(突起物を除く)	
電源	AC100V(50/60Hz)	
消費電力	最大 15W(電源アダプター含む)	
質量	約 1kg(電源アダプター含まず)	
電磁妨害波規格 VCCI	VCCI クラス A	

5.1.2 ソフトウェア諸元

項目		仕様	
VoIP 機能	対応プロトコル	SIP/2.0	
	呼制御	RFC3261/RFC3262/RFC3264/RFC2327/RFC3311 (UPDATE)/ RFC3323/ RFC3325/ RFC3455 (P-Called-Party-ID)/ RFC3966/RFC4028/RFC4566/ TS-1008 トランスポート:RFC768、ネットワーク:RFC791、RFC2460	
	同時通話数	16ch(カスケード構成時)	
	利用可能電話番号	500 番号	
ルータ機能	ルーティング方式	スタティックルーティング(LAN 側ルーティング:最大 20 件)	
	DHCP サーバ機能	あり(最大 253 アドレス割り当て)	
	DNS リレー機能	あり	
	NAT 機能	静的 IP マスカレード:最大 50 件 静的 NAT:最大 64 アドレス 動的 IP マスカレード:あり 動的 NAT:あり	
	仮想 DMZ 機能	あり	仮想 DMZ 機能と簡易 DMZ 機能は排他利用とする。
	簡易 DMZ 機能	あり	
	ポート VLAN 機能	あり(仮想 DMZ 機能時のみ有効)	
	VPN パススルー機能	あり	
	セカンダリアドレス機能	あり(インターネットアドレスのサブネットが/30 以外の場合のみ有効)	
	ユニバーサルプラグアンド プレイ (UPnP) 機能	あり	
	ファイアウォール機能	フィルタの種類(許可/拒否)、適用セグメント(音声・インターネット)、送信元 IP アドレス、プロトコル種別、送信元ポート、宛先ポート、ICMP タイプ、ICMP コード、セキュリティログ保存有無 登録数:96 件	
	SPI 機能	あり	
	パケットフィルタ機能	通信方向、フィルタ種別(拒否/許可)、TCP フラグ、送信元 IP アドレス、宛先 IP アドレス、プロトコル種別、送信元ポート、宛先ポート、ICMP タイプ、ICMP コード、セキュリティログ保存有無 登録数:最大 128 件	
	URL フィルタ機能	拒否リスト、許可リスト 登録数:最大 20 件	
PING 応答選択機能	あり(WAN、音声、インターネット)		
設定・保守機能	設定方法	ウェブブラウザによる設定・保守	
	状態表示機能	装置状態表示、UPnP 状態表示、LAN 側自動払い出し状況表示	
	ログ機能	装置ログ:最大 1000 件 通話ログ:最大 2000 件 REGISTER ログ:最大 2000 件 セキュリティログ:最大 100 件 信号系ログ:最大 500 件(BRI のみ) ジッタログ:最大 240 件	
	統計機能	LAN 統計情報、WAN 統計情報、端末ポート統計情報、	
	SIP メッセージ情報表示 機能	SIP メッセージ:最大 1024 件×2 面 (新情報、旧情報の 2 面)	

5.2 サービス機能

5.2.1 サービス機能一覧

・サービス機能一覧(1/2)

	分類	機能名称	機能概要
ネットワーク	ルーティング対象	IPv4	ルーティング対象プロトコルとして IPv4 をサポートする。
	LAN 接続	IPv4 アドレス払い出し機能	DHCPv4 により、LAN セグメント上の端末へ IP アドレスを払い出す機能。
	ポート	通信速度選択機能	WANポートおよび各LANポートの通信速度をそれぞれ設定する機能。
		MDI/MDI-X 選択機能	WAN ポートおよび各 LAN ポートそれぞれについて、自動設定か MDI-X かを選択する機能。
	セキュリティ	ファイアウォール機能	WAN 側から本装置宛の packets をフィルタリングする機能。
		SPI 機能	ステートフル・パケット・インスペクション機能。
		パケットフィルタ機能	本装置を通過するパケットについて、WAN 側または LAN 側への不要なパケットの転送を防御する機能。
		URL フィルタ機能	DNS リレー機能を使用する場合に特定のドメイン名、キーワードについて、DNS アドレス解決時に解決を拒否または許可することによりインターネットへのアクセス制限を可能とする機能。
		PING 応答選択機能	WAN 側からの PING に対して応答するか否かを選択する機能。
	ネットワーク	ルーティング	静的 IP マスカレード機能
静的 NAT 機能			あらかじめ設定した情報による NAT 機能。
動的 NAT、動的 IP マスカレード機能			LAN側のプライベートアドレスをWAN側のグローバルアドレスに変換する機能。
ポートフォワーディング			UPnP に対応しない外部からアクセスを許容する機器の接続を可能とする機能。
LAN 側ルーティング機能			本装置の LAN 側におけるルーティング機能。
仮想 DMZ 機能			インターネットへサーバを公開するため、仮想 DMZ 用サブネットを構築し、WAN 側に公開する機能。
簡易 DMZ 機能			LAN 側の端末を簡易 DMZ 端末として設定することにより、静的 NAT/静的 IP マスカレードに合致しない WAN 側からの packets を簡易 DMZ 端末に中継する機能。
ポート VLAN 機能			仮想 DMZ 機能を使用時において、仮想 DMZ 端末を使用するポートを指定し、ポート VLAN を構築し、ほかのポートとの通信と独立させる機能。
DNS リレー機能			LAN 側の端末に対して、本装置が DNS サーバとして動作し、WAN 側にはリゾルバとして動作する。端末からの DNS 解決要求を受けると、WAN 側の DNS サーバに問い合わせを行い、その結果を LAN 側端末に通知する機能。
VPN パススルー			LAN 側端末が VPN を張る場合に本装置でポート番号変換を行わないように静的 IP マスカレードの設定を行い、VPN 用の packets を通過させる機能。
UPnP		UPnP 選択機能	ネットワークサービスにおける UPnP 機能を使用するか否かを選択する機能。
Marking		TOS 値設定機能	LAN 側の端末から WAN 側のインターネットへの packets については TOS 値を強制的に 0 に設定する機能。

・サービス機能一覧(2/2)

分類	機能名称	機能概要
メンテナンス	設定端末接続	設定画面表示機能
	構成情報 ファイル操作	構成情報インポート機能
		構成情報エクスポート機能
	統計情報機能	統計情報機能
	状態表示機能	システム状態
		呼状態
		REGISTER 状態
		UPnP 状態表示
		LAN 側自動払い出し状況
	障害状態	
	ログ採取 ・表示機能	セキュリティログ
	操作	疎通確認機能
		閉塞/閉塞解除機能
		ログクリア機能
	ログインパスワード 設定	ログインパスワード設定

5.2.2 サービス機能詳細 - ネットワーク機能

ネットワーク接続に関するサービス機能の詳細を示す。

5.2.2.1 ルーティング対象 - IPv4

【機能説明】

本装置でルーティング対象とするプロトコルは、IPv4 アドレスを持つパケットとなる。
なお、本装置が生成するパケットの TTL はすべて 64 となる。

【備考・注意事項】

なし。

5.2.2.2 LAN 接続 - IPv4 アドレス払い出し機能

【機能説明】

DHCPv4 による IPv4 アドレス払い出し機能を具備する。設定端末などを LAN 側に接続する際、DHCP による IPv4 アドレス情報の払い出しを行う。設定により、最大 253 個まで払い出し可能となる。(払い出し可能数は設定により変更が可能。)

なお、WAN 側への払い出しは行えない。

払い出す情報を下記に示す。

- ・IP アドレス
- ・デフォルトゲートウェイアドレス(ルータアドレス)
- ・サブネットマスク(マスク長 8~30)
- ・DNS サーバアドレス
- ・リース時間(1 時間~72 時間)
- ・WINS サーバアドレス(本装置に WINS サーバアドレスが設定されていた場合のみ)

DHCP で払い出す IP アドレスは LAN セグメントの IP アドレスとなる。

なお、払い出した IP アドレスと MAC アドレスの関連は「LAN 側自動払い出し状況-払い出し状況-払い出しクリア」の[クリア]ボタン押下によりクリアされる。

【備考・注意事項】

設定により DHCP サーバ機能を使用しないことも可能である。(アドレス払い出しを行わない)一度払い出した情報(払い出した IP アドレスと MAC アドレスの対応)は保存しているが、電源オフでは保持しない。

WINS:Windows Internet Name Service の略称

5.2.2.5 セキュリティ - SPI 機能

【機能説明】

ステートフル・パケット・インスペクション(Stateful Packet Inspection)機能。

本装置でルーティング/NAPT する UDP、TCP、ICMP の各パケットにおいて、WAN 側からの不正パケット(状態不一致、シーケンス異常など)の検出を行い、不正パケットの廃棄を行う。

LAN 側端末からの通信開始により、WAN 側ポートを開く。設定された時間内に通信が無かった場合、または通信終了(TCP のセッション終了など)した場合には WAN 側のポートを自動的に閉じて、以後のパケットを受け付けない。

なお、設定時間はプロトコル毎(TCP、UDP、ICMP)に設定が可能。(30 秒～7200 秒)

【備考・注意事項】

SPI 機能は本装置宛のパケット、本装置の配下にある端末へフォワーディングするパケットの両方に適用される。インターネット、WAN 側のパケットが該当する。

5.2.2.6 セキュリティ - パケットフィルタ機能

【機能説明】

本装置を通過する(フォワーディングする)パケットについて、IP アドレス、プロトコル、ポート番号などの条件により通過あるいは廃棄することにより WAN 側または LAN 側への不要なパケット転送を防御する機能。ただし、LAN 側から LAN 側へのパケットには適用しない。

本機能により選択的にパケットを廃棄したり、通過させたりすることができる。

パケットフィルタリング設定として、通信方向、TCP フラグ、送信元 IP アドレス、宛先 IP アドレス、プロトコル、送信元ポート、宛先ポート、ICMP タイプ、ICMP コードの指定が可能。

フィルタ条件は複数の設定が可能であり、ルール No.により優先順位が指定できる。

本機能により廃棄したパケットについてはセキュリティログに記録することができる。また、記録しないことも設定により選択可能。

パケットフィルタ条件は 128 件が設定可能。

設定項目は以下となる。

- ・ルール番号(0~999)
- ・通信方向(WAN→LAN、LAN→WAN、両方向)
- ・フィルタの種別(許可/拒否)
- ・TCP フラグ(指定しない/SYN/ESTABLISHED)
- ・送信元 IP アドレス
- ・宛先 IP アドレス
- ・プロトコル(1~255)
- ・送信元ポート番号(1~65535)
- ・宛先ポート番号(1~65535)
- ・ICMP タイプ(1~255)
- ・ICMP コード(1~255)
- ・セキュリティログ保存(保存する/保存しない)

【備考・注意事項】

本設定はインターネット通信にのみ適用し、[ルータとして使用]設定での下部に接続した VoIP-GW での通信パケットには適用しない。

SPI機能を使用する場合、通過が許可されたパケットに対応する応答パケットは廃棄条件を無視し、通過が許可される。

ICMP タイプ、ICMP コードはプロトコルとして ICMP を設定した場合のみ有効となる。

プロトコルとして ICMP を設定し、ICMP タイプ、ICMP コードを設定しない場合は ICMP すべてに対しての設定となる。

5.2.2.7 セキュリティ - URL フィルタ機能

【機能説明】

本装置の DNS リレー/DNS プロキシ機能を使用してアドレス解決を行う場合に、特定のドメイン名、キーワードについて、DNS アドレス解決時に解決を拒否または許可することによりインターネットへのアクセス制限を行う機能。

フィルタ条件として、登録されているドメイン名、キーワードを拒否(許可設定)、ブラックリスト(拒否設定)の選択が可能である。

なお、拒否・許可選択はすべての URL フィルタのエントリに同一で適用される。(拒否、許可は個別に設定することはできない。)

ドメイン名の場合には後方一致およびドット区切りで判定する。キーワードの場合には部分一致で判断し、ドット区切りは関係しない。

フィルタ条件は最大 20 件の登録が可能。

設定項目は以下となる。

- ・URL フィルタ許可設定(使用しない/許可リスト/拒否リスト)
- ・比較条件(ドメイン/キーワード)
- ・比較文字(256 文字までの文字列)

【備考・注意事項】

本装置の DNS リレー/DNS プロキシ機能を使用してアドレス解決を行う場合に有効となる。

DNS リレー/DNS プロキシ機能を使用しない(LAN 側端末が本装置の IP アドレスを DNS サーバとして設定せず、外部 DNS サーバを直接指定していた)場合、本機能は使用できない。

5.2.2.8 セキュリティ - PING 応答選択機能

【機能説明】

WAN 側から本装置宛の PING(ICMP Echo Request)に対して応答(ICMP Echo Reply)を返すかどうかを設定する。

設定はセグメントごとに応答の可否を選択でき、WAN 側セグメント応答、電話用セグメント応答、インターネット用セグメント応答で設定可能。

PING 応答機能を使用するにした場合、該当セグメント宛の PING(ICMP Echo Request)を受信した場合、応答(ICMP Echo Reply)を返送する。使用しない場合には PING(ICMP Echo Request)を廃棄し、応答を返さない。

本設定は LAN 側からの PING に対しては意味を持たない。

【備考・注意事項】

送信元の IP アドレスについては判定しない。

インターネット用セグメントのみ応答可否を設定可能となる。

5.2.2.9 ルーティング - 静的 IP マスカレード機能

【機能説明】

WAN 側から本装置宛の packets において、設定されている IP アドレス/ポートが宛先の場合に WAN 側のグローバルアドレスをローカルアドレスに変換する。

あらかじめ固定的に使用するポート番号と LAN 側の端末を結びつけることができ、本機能を使用することによって WAN 側にサーバを公開する、あるいは WAN 側からの特定ポートの通信を指定したパソコンなどに送受信できる。

必要に応じて NAT エントリの設定をすることで、特定のサイトから特定のパソコンへ直接アクセスできる。ネットワーク対応ゲームやストリーミングなどの外部から直接アクセスが必要なアプリケーションを使用することができる。

静的 IP マスカレードは 50 個の設定が可能である。

設定項目は以下となる。

優先順位: エントリ内の優先度を示す。値が小さいほど優先度が高い(先に処理を行う)

宛先 IP アドレス: LAN 側端末の IP アドレスを示す。WAN 側に公開する端末を指定する。

変換対象プロトコル: WAN に公開するアプリケーションが使用するプロトコルを指定する。

宛先ポート: WAN 側に公開するアプリケーションが使用する LAN 側でのポート番号を指定する。

変換対象ポート: WAN 側でアプリケーションが使用するポート番号を指定する。WAN 側からのこのポート番号を指定して通信を行う。

【備考・注意事項】

異なったエントリで同一の優先順位は設定できない。

静的 IP マスカレード設定は静的 NAT 設定より優先して処理される。

5.2.2.10 ルーティング - 静的 NAT 機能

【機能説明】

WAN 側から本装置宛のパケットにおいて、WAN 側から受信した宛先が設定されている宛先 IP アドレスであった場合に WAN 側のグローバルアドレスをローカルアドレスに変換する。

あらかじめ固定的に LAN 側のプライベート IP アドレスと WAN 側のグローバル IP アドレスを結びつけることができ、WAN 側から LAN 側端末を指定したパソコンなどに送受信することができる。

静的 NAT は 64 個の設定が可能である。

設定項目は以下となる。

優先順位: エントリ内の優先度を示す。値が小さいほど優先度が高い(先に処理を行う)

宛先 IP アドレス: LAN 側端末の IP アドレスを示す。WAN 側に公開する端末を指定する。

変換対象プロトコル: WAN に公開するアプリケーションが使用するプロトコルを指定する。

変換対象ポート: WAN 側でアプリケーションが使用するポート番号を指定する。WAN 側からのこのポート番号を指定して通信を行う。範囲を指定しての設定も可能。

【備考・注意事項】

静的 IP マスカレード機能は IP アドレス、ポート番号で関連付けるが、静的 NAT 機能の場合は IP アドレスのみで関連付ける。

異なったエントリで同一の優先順位は設定できない。

静的 IP マスカレード設定は静的 NAT 設定より優先して処理される。

5.2.2.11 ルーティング - 動的 NAT、動的 IP マスカレード機能

【機能説明】

1 つの WAN 側 IP アドレスを共有し、WAN 側に送出する送信元アドレスを変換する。

これにより 1 つのグローバル IP アドレスを利用して、LAN 内のプライベート IP アドレスを持つ複数のパソコンなどをインターネットなどに接続することができる。

動的 NAT 設定により、ローカルな IP アドレスしか割り当てられていない LAN 側端末から透過的に WAN 側へのアクセスを可能とする。動的 NAT 設定は、ICMP などポート番号の概念のないプロトコルに対して適用する。

ポート番号の概念の存在するプロトコルに対しては、IP マスカレード設定を適用する。

【備考・注意事項】

本機能はインターネット用セグメントのマスク長が 30 の場合のみ有効となる。

本機能を使用するための設定(IP アドレスなど)を行う必要はない。

静的 IP マスカレード設定、静的 NAT 設定に適用されない通信が動的 IP マスカレード/動的 NAT が適用される。(静的 IP マスカレード、静的 NAT 設定の優先度が高い)

5.2.2.12 ルーティング - ポートフォワーディング

【機能説明】

WAN側から特定のポート番号宛にパケットが届いたときに、あらかじめ設定しておいた静的NAT、静的IP マスカレード設定に基づいて指定されたLAN側の端末にパケットを転送する機能。

【備考・注意事項】

なし。

5.2.2.13 ルーティング - LAN側ルーティング機能

【機能説明】

LAN-LAN間のルーティングを可能とする機能。

設定された宛先IPアドレス/マスク長宛のパケットを設定されたゲートウェイを経由して転送する。LAN側にルータを接続し、ルータのLAN側に接続された端末にパケットを転送する場合などに使用する。

LAN側ルーティング設定は20個の設定が可能。

設定項目は以下となる。

- ・エントリ番号(1~20)
- ・宛先IPアドレス/マスク長
- ・ゲートウェイ

【備考・注意事項】

LAN側ルーティング機能はインターネットを使用する場合、およびサービス選択が「ルータとして使用(電話使用)、(電話、インターネット使用)」設定の場合のみ有効となる。

5.2.2.14 ルーティング - 仮想 DMZ 機能

【機能説明】

LAN 側に通常の通信セグメントとは別に仮想 DMZ (DeMilitarized Zone) 用セグメントを構成し、WAN 側からのパケットはすべて仮想 DMZ 用セグメントに転送される。

仮想 DMZ 用セグメントはマスク長 24~30 が指定可能である。ほかのセグメントと IP アドレスの重複はできない(設定エラーとなる)。

LAN 側通信セグメントには LAN 側から開始した通信のみが転送されるため、セキュリティが確保しやすくなる。

仮想 DMZ 用セグメントに位置する端末には WAN 側からパケットが転送されてくるため、端末のセキュリティには十分注意して設定を行うこと。

また、ポート VLAN 機能を合わせて使用することで、LAN 側端末と仮想 DMZ の端末とのポート間通信を遮断することができる。

設定項目は以下となる。

- ・外部へのサーバ公開(公開しない/仮想 DMZ で公開する/簡易的に公開する)
- ・仮想 DMZ の IP アドレス空間/マスク長
- ・DMZ をポート VLAN で分けする

【備考・注意事項】

仮想 DMZ 機能と簡易 DMZ 機能はどちらか一方を選択する設定であるため、同時には使用することができない。

仮想 DMZ 機能はインターネット用セグメントのマスク長が/30 の場合のみ有効。

WAN 側にサーバ公開する、あるいは WAN 側からパケットを転送させるためには静的 IP マスカレード設定または静的 NAT 設定により公開する端末の IP アドレスを設定する必要がある。

5.2.2.15 ルーティング - 簡易 DMZ 機能

【機能説明】

簡易 DMZ (DeMilitarized Zone) を設定することで静的 IP マスカレードや静的 NAT の設定条件に合致しない外部 (WAN 側) からのパケットをすべて簡易 DMZ で設定した端末 (公開するホストの IP アドレスにより指定する) へ中継する。

簡易 DMZ は公開するサーバとして 1 つの IP アドレスのみ設定が可能であり、その IP アドレスは LAN 側セグメント内の IP アドレスとなる。

ただし、簡易 DMZ 以外の LAN 側端末から開始した通信の戻りは簡易 DMZ 端末へは転送されない。設定項目は以下となる。

- ・外部へのサーバ公開 (公開しない / 仮想 DMZ で公開する / 簡易的に公開する)
- ・公開するホストの IP アドレス

【備考・注意事項】

簡易 DMZ で設定した端末は LAN 側端末と同一のセグメントに存在する。

簡易 DMZ 機能と仮想 DMZ 機能はどちらか一方を選択する設定であるため、同時には使用することができない。

簡易 DMZ 機能はインターネット用セグメントのマスク長が /30 の場合のみ有効となる。

5.2.2.16 ルーティング - ポート VLAN 機能

【機能説明】

仮想 DMZ (DeMilitarized Zone) 機能を使用する場合において、仮想 DMZ 端末を接続するポートを指定してポート VLAN を構築することで、仮想 DMZ の端末とほかのポートでの LAN 側端末との通信を遮断することができる。

設定項目は以下となる。

- ・DMZ をポート VLAN で区分けする

【備考・注意事項】

ポート VLAN は仮想 DMZ 機能でのみ有効となり、固定的な用途にのみ使用が可能である。

5.2.2.17 ルーティング - DNS リレー機能

【機能説明】

LAN 側の端末から本装置あてに送られてきた DNS Query を各 DNS サーバへ転送し、問い合わせ結果を送信元の ALN 側端末に返信する。

LAN 側端末にはサーバとして動作し、WAN 側にはリゾルバとして動作する。取得成功した時点で LAN 端末へ応答を返す。

DNS リレー機能を使用する場合は URL フィルタ機能を使用できる。DNS リレー機能を使用しない場合には URL フィルタ機能は無効となる。

【備考・注意事項】

LAN 型接続(複数 IP アドレスの割り当てがある場合)には直接 DNS サーバへ問い合わせを行うことがある。この場合には DNS リレー機能は働かない。

DNS リレー機能は LAN 側端末が本装置を DNS サーバとして登録した場合に有効となる。

DHCP サーバ機能を使用して IP アドレスを払い出した場合は、DNS サーバとして本装置を指定して払い出している。

DNS リレー機能は DNS プロキシ機能と同等の機能である。

5.2.2.18 ルーティング - VPN パススルー機能

【機能説明】

LAN 側の端末とインターネットにある端末との端末間で仮想プライベートネットワーク (VPN:Virtual Private Network)通信が行えるように、VPN に使用するパケットを IP マスカレード機能により通過させることができる機能。

VPN パススルーで使用するプロトコルは下記となる。

- ・PPTP(Point to Point Tunneling Protocol)
- ・IPsec(IP Security)
- ・L2TP(Layer 2 Tunneling)

また、LAN 側の端末として VPN サーバを設置する場合、WAN 側からの接続を可能とするために、静的 IP マスカレードの設定が必要になる。

下記のようなアクセスが可能となる。

- ・LAN 側の PPTP クライアントから WAN 側の PPTP サーバへのアクセス
- ・WAN 側の PPTP クライアントから LAN 側の PPTP サーバへのアクセス
- ・LAN 側の IPsec クライアントから WAN 側の IPsec サーバへのアクセス
- ・WAN 側の IPsec クライアントから LAN 側の IPsec サーバへのアクセス
- ・LAN 側の L2TP クライアントから WAN 側の L2TP サーバへのアクセス
- ・WAN 側の L2TP クライアントから LAN 側の L2TP サーバへのアクセス

【備考・注意事項】 なし。

5.2.2.19 UPnP - UPnP 選択機能

【機能説明】

ネットワークサービスにおける UPnP 機能を使用するか否かを選択する機能。

UPnP とは、Universal Plug and Play の略であり、XML 技術をベースに開発されたネットワーク機器同士の相互自動認識方式。

UPnP 機能は、LAN 側に接続された端末から NAT 設定、IP マスカレード設定を行うことにより、NAT による IP アドレスやポート番号の変換を気にすることなく通信が可能となる。

UPnP 仕様は下記のものとなる。

linuxigd-1.0

libupnp-1.3.1

【備考・注意事項】

なし。

5.2.2.20 フィルタリング処理

【機能説明】

本装置でのパケット受信から送信までの処理を以下に示す。

機能、方向により適用されるフィルタ、処理が異なってくる。

色づけされた箇所は設定が可能な項目となる。

【備考・注意事項】

なし。

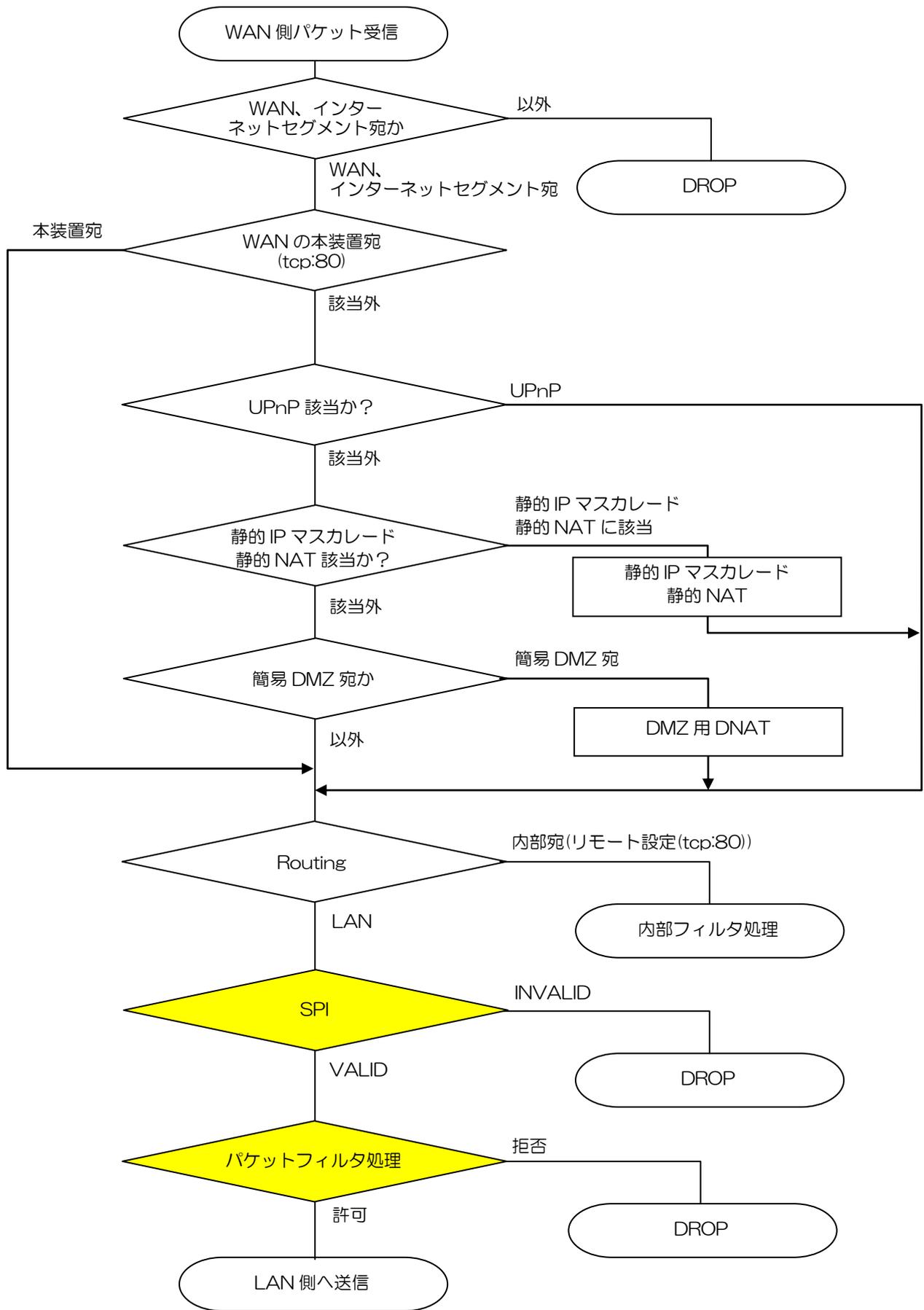


図 5.2.2-1WAN→LAN 方向のフィルタリング処理

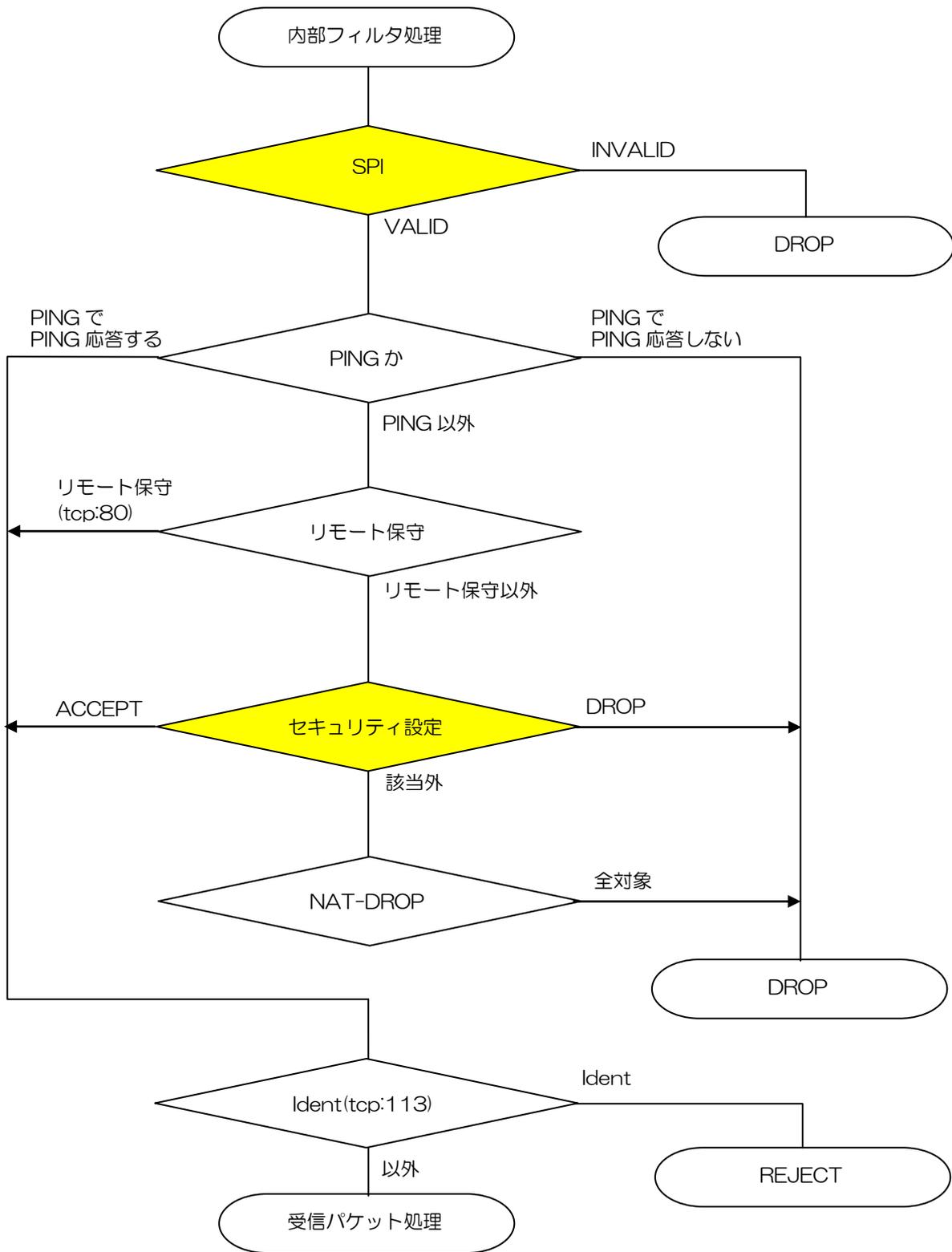


図 5.2.2-2 自装置宛のフィルタリング処理

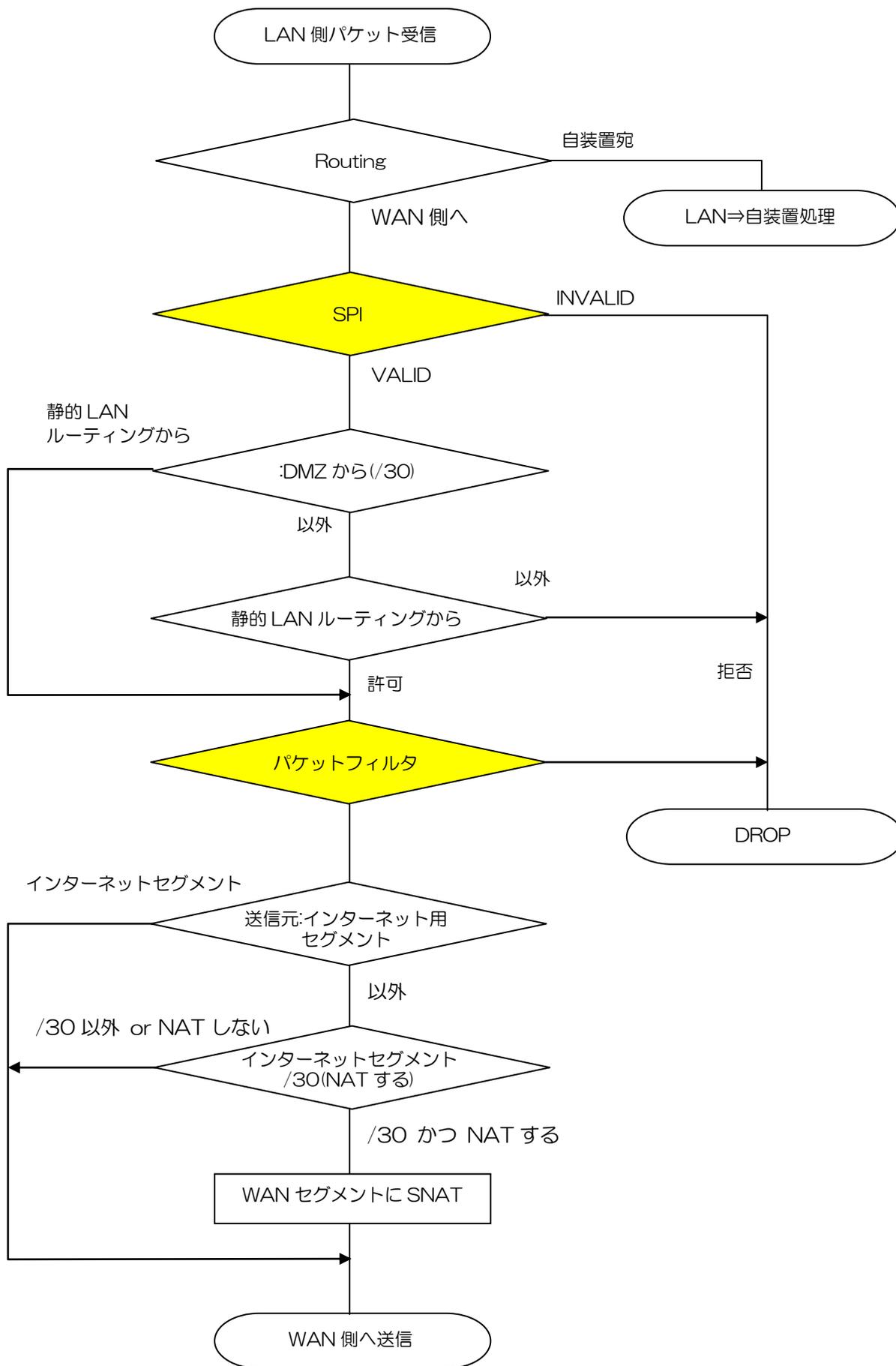


図 5.2.2-3 LAN側からの受信パケット処理

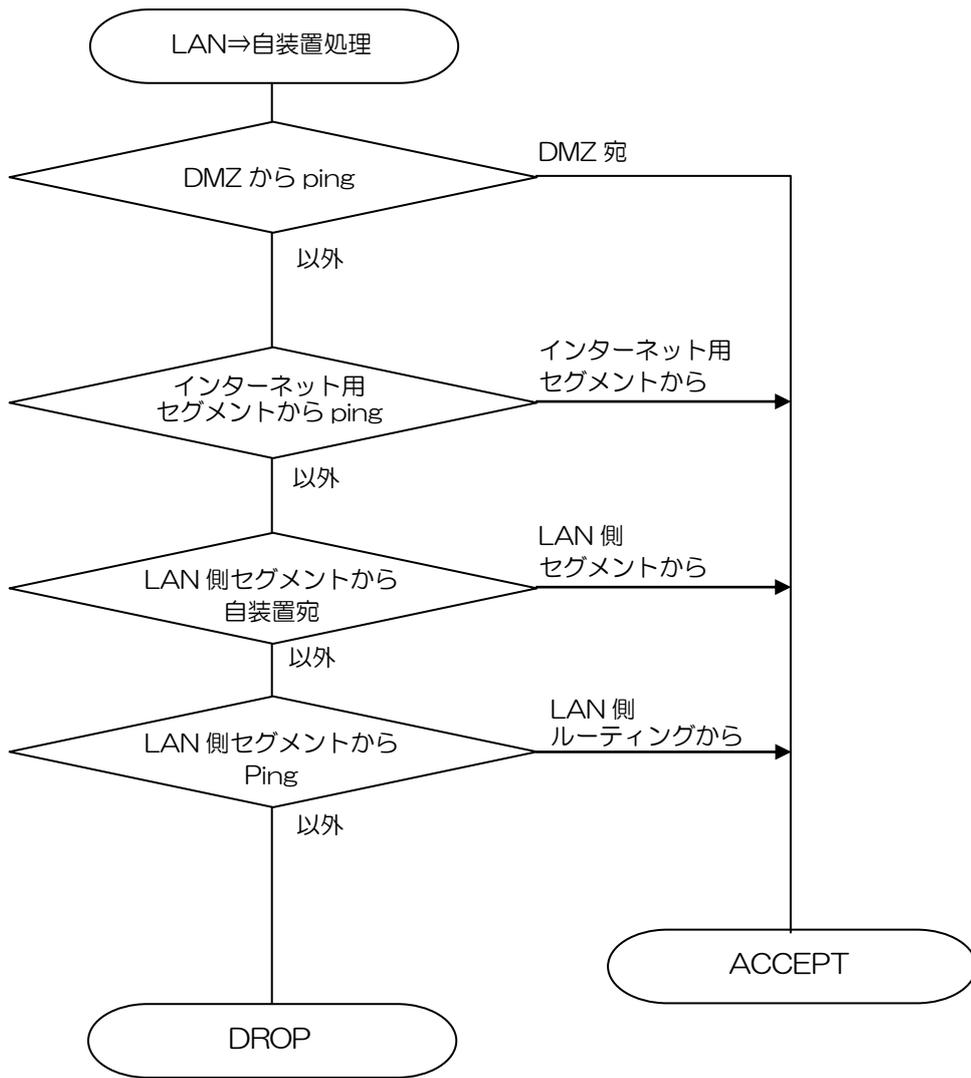


図 5.2.2-4 LAN側から自装置宛のパケット受信処理

5.2.2.21 構成情報インポート機能

【機能説明】

本装置の「メンテナンス - 装置設定の保存/復元」の操作により、エクスポートした構成情報ファイルを本装置に送信し、構成情報ファイルの内容を、本装置の構成情報として復元することが可能。構成情報ファイルはテキストで記述されている。インポートする場合、設定を変更する項目のみを記述することにより少ない容量のファイルとして書き込みができる。

ファイルをインポートする場合、装置内部で構成情報の整合性チェックを行う。整合性が取れていない場合には更新ができない。

下表に整合性でエラーが発生する内容を記す。IP アドレス系のエラーは複数の条件でエラーが発生するため、集約して記載している。

表 5.2.2.21-1 構成情報インポート時の整合性エラー内容

発生箇所	エラー内容	対処
ネットワーク設定	IP アドレスを重複して設定した。	IP アドレス設定の見直し
	ネットワークを重複して設定した。	
	使用不可アドレスを設定した。(ネットワークアドレス、ブロードキャストアドレスを使用した。)	
	IP アドレスとデフォルトゲートウェイアドレスのネットワークが異なって設定した。	
	IP アドレスの設定範囲が不正。	
	必須入力情報が入力されていない。	DNS サーバアドレス見直し
インターネット系設定	設定内容が重複した。(ルール No、優先順位、)	セキュリティ、フィルタ設定の見直し
	設定範囲が不正。(設定終了値を開始値より小さく設定した。)	
	「フィルタ種別」が[許可]の場合は「セキュリティログ保存」に[保存する]は設定できない。	
	「ICMP タイプ」が[*]の場合は「ICMP コード」に[*]以外は設定できない。	
	「変換対象プロトコル」が[TCP][UDP][TCP と UDP 両方]以外の場合、変換対象ポートは設定できない。	
	「DNS ドメイン名」が空白の場合は、「IP アドレス」は入力必須である。	SIP 共通設定の見直し
	「DNS ドメイン名」が空白以外の場合は、「IP アドレス」は設定できない。	
保守	ファームウェア更新指定日の設定値が異常。	更新時間の確認

【備考・注意事項】

パスワードは復元されない。

インポートした構成情報の値が、本装置内の値と差がなくとも復元後に再起動となる。

5.2.2.22 構成情報エクスポート機能

【機能説明】

本装置の「メンテナンス - 装置設定の保存/復元」の操作により、構成情報ファイルを保守端末にエクスポートすることが可能。

構成情報ファイルは、暗号化されていないテキストファイルで、テキストエディタにより閲覧可能。

【備考・注意事項】

なし。

5.2.2.23 統計情報機能

【機能説明】

本装置は、本装置が送受信するイーサネットフレームの統計情報を収集し、表示する機能を具備する。カウント対象は、LAN インターフェース、WAN インターフェース、端末ポート (FXS ポート 1~4、BRI ポート 1 チャンネル 1~ポート 2 チャンネル 2) であり、端末ポートでは RTP/RTCP 関連の統計情報 (呼処理でオープンした UDP ポートで送受信したフレーム) を収集する。

収集した統計情報は、「統計情報」の「統計情報の選択 - 統計情報の種類」を選択することで、表示、クリアが可能。また、すべての統計情報をクリアすることも可能 (送受信カウンタクリア)

表 5.2.2.23-1 LAN 統計情報、WAN 統計情報

表示項目	説明
受信ユニキャストパケット数	受信ユニキャストパケット数を表示する。
受信ブロードキャストパケット数	受信ブロードキャストパケット数を表示する。
受信マルチキャストパケット数	受信マルチキャストパケット数を表示する。
送信ユニキャストパケット数	送信ユニキャストパケット数を表示する。
送信ブロードキャストパケット数	送信ブロードキャストパケット数を表示する。
送信マルチキャストパケット数	送信マルチキャストパケット数を表示する。
送信エラーパケット数	コリジョンにより再送リミットが発生した回数を表示する。
送信廃棄パケット数	送信エラーなどで廃棄したパケット数を表示する。
コリジョン発生回数	コリジョンが発生した回数を表示する。
レートコリジョン発生回数	レートコリジョンが発生した回数を表示する。
受信異常発生回数	パケット受信時に異常となった回数を表示する。
受信アライメント異常発生回数	パケット受信時にアライメント異常が発生した回数を表示する。
受信 FCS エラー発生回数	受信パケットの FCS エラー発生回数を表示する。
受信パラメータ異常発生回数	受信パケットのパラメータ異常が発生した回数を表示する。
受信フラグメント発生回数	パケット受信時にフラグメントが発生した回数を表示する。
受信廃棄パケット数	受信エラーなどで廃棄したパケット数を表示する。
不正キャリアセンス検出回数	不正キャリアセンスを検出した回数を表示する。

表 5.2.2.23-2 端末ポート統計情報

表示項目	説明
RTP 送信パケット数	RTP 送信パケット数を表示する。
RTP 受信パケット数	RTP 受信パケット数を表示する。
RTP 送信破棄パケット数	RTP 送信破棄パケット数を表示する。
RTP 受信破棄パケット数	RTP 受信破棄パケット数を表示する。
RTCP 送信パケット数	RTCP 送信パケット数を表示する。
RTCP 受信パケット数	RTCP 受信パケット数を表示する。
RTCP 送信破棄パケット数	RTCP 送信破棄パケット数を表示する。
RTCP 受信破棄パケット数	RTCP 受信破棄パケット数を表示する。
ゆらぎ最大時間(ms)	RTP 受信パケットの最大ゆらぎ時間を表示する。
ゆらぎ最小時間(ms)	RTP 受信パケットの最小ゆらぎ時間を表示する。
ゆらぎ時間[xxms]パケット数	当該時間を中心値として前後 10ms 間で受信した RTP パケット数を表示する。
ゆらぎ時間(その他)パケット数	ゆらぎ時間が 200ms を越えたパケット数を表示する。

【備考・注意事項】

統計情報は、電源を切ると消去される。

5.2.2.24 状態表示機能

【機能説明】

装置の状態を表示する機能であり、保守端末を操作することで、システム状態、ネットワーク状態、インターネットセグメント IP アドレス、ランプ状態、子状態、ポート状態、サーバ通信状態、REGISTER 状態、DNS 接続状態、閉塞状態を保守画面に表示可能。

保守画面の内容は、動作モード、サービス選択、機種、アカウントによって異なり、詳細は「4.3.1 装置状態表示」参照のこと。

(1)ポート状態の詳細表示

「装置状態表示」-「ポート状態」の[詳細確認]ボタンを押下することで、その時点のポート個別の通話状態を表示する。

【備考・注意事項】

なし。

5.2.2.25 状態表示機能 - 障害状態

【機能説明】

ハード障害を検出時に、ALARM ランプを点灯させることで、本装置の正面パネルでハード故障を確認することができる。また、各ランプにより装置の状態を確認することができる。

また、障害状態は「装置状態表示」でも確認が可能。

【備考・注意事項】

WAN の SPEED ランプは 1Gbit/s でリンクした場合を示し、100Mbit/s、10Mbit/s でリンクした場合は消灯となる。

点灯表示となっていないランプも設定状態、装置状態により点灯、点滅となる場合がある。

ALARM ランプ点灯時は、ハード故障のためほかのランプの状態に意味を持たない。

5.2.2.26 UPnP 状態表示

【機能説明】

保守画面の「UPnP 状態表示」選択により、現在の UPnP 状態を表示する。
表示内容は下記。

- ・登録日時:本装置がリクエストを受信した時刻
- ・要求元 IP アドレス:リクエストを送信した端末の IP アドレス
- ・サービスホスト:接続先の IP アドレス
- ・プロトコル:UPnP 用のアドレス変換(ポート指定)設定情報のプロトコル
- ・ローカルホスト:ローカルホストの IP アドレス
- ・説明:UPnP 対応アプリケーションによって設定された説明

【備考・注意事項】

なし。

5.2.2.27 LAN 側自動払い出し状況

【機能説明】

保守画面の「LAN 側自動払い出し状況表示」選択により、LAN 側セグメントにおける DHCP サーバ機能による IP アドレス払い出し状況を表示する。

- ・現在の払い出し件数:IP アドレスを払い出した数
- ・IPv4 アドレス(/マスク長):払い出した IP アドレス、マスク長
- ・MAC アドレス:IP アドレスを払い出し端末の MAC アドレス
- ・リース終了時間:IP アドレスのリース終了となる時間

【備考・注意事項】

なし。

5.2.2.28 ログ採取・表示機能 - セキュリティログ

【機能説明】

ファイアウォールにて廃棄したパケットの情報を採取し、最新の 100 件を表示する機能。

本装置は、外部から受信したパケットの中で NAT、SPI、ファイアウォール、パケットフィルタにより廃棄したパケットの受信ログを採取する。

(ファイアウォール、パケットフィルタのフィルタ種別を許可にした場合での条件合致時の許可パケットについては、廃棄されないのでログには採取されない。)

セキュリティログは設定画面の「ログ表示 - セキュリティログ」選択により表示可能。

表 5.2.2.28-1 セキュリティログ採取内容

表示項目	説明
受信日時	廃棄したパケットを受信した時刻を表示する。
送信元 IP アドレス/ポート	廃棄したパケットの送信元 IP アドレスとポートを表示する。
宛先 IP アドレス/ポート	廃棄したパケットの宛先 IP アドレスとポートを表示する。
プロトコル	廃棄したパケットのプロトコルを表示する。
アクション	パケットを廃棄した要因を表示する。 廃棄[NAT]/廃棄[SPI]/廃棄[ファイアウォール]/廃棄[パケットフィルタ]

※プロトコルが TCP/UDP 以外のパケットはポート番号が「-」で表示される。

※フラグメントされた 2 番目以降のパケットはポート番号が「+」で表示される。

※セキュリティログは、装置内蔵のフラッシュメモリーには記録されないため、電源を切るとログ情報は保存されず、消去される。

※最大 100 件までのログが表示され、100 件を超えた場合は古いものから順に削除される。

【備考・注意事項】

なし。

5.2.2.29 疎通確認機能

【機能説明】

本装置は設定画面から指定された IP アドレス宛に Ping を発行し、応答結果を表示することでノード間の疎通確認を行うことができる。

なお、本装置は複数の IP アドレス情報(ネットワークセグメント)を保有することから、送信元 IP アドレスの指定のために送信元セグメントを指定する。

宛先 IP アドレスが属するセグメントと送信元セグメントは同じものを指定すること。セグメントが異なった場合には Ping が通らないことがある。

送信元セグメントを指定すると、本装置に設定されているセグメントの IP アドレスを I オプションに設定して ping コマンドを発行する。

【備考・注意事項】

宛先 IP アドレスと送信元セグメントの組み合わせにより Ping が破棄される場合がある。また、装置内部のネットワークセグメント間で通信制限を行っている場合は Ping 応答が返らない場合がある。

5.2.2.30 ログクリア機能

【機能説明】

設定画面の「ログ表示」において、各ログ単位、または全ログを消去することが可能。

消去した場合には、装置内蔵のフラッシュメモリーに記録されていたログも消去される。

5.2.2.31 ログインパスワード設定

【機能説明】

本装置の保守画面にて、設定画面表示時に要求される認証用のパスワードを変更することが可能。

ログイン ID は” user” 固定であり、パスワードの初期値は” 00000000” である。

パスワードは最大 16 文字まで入力可能、使用可能文字は半角英数字/一部記号(「-」「/」「_」)である。

5.3 構成情報一覧

5.3.1 ネットワーク設定 - LAN 接続設定

・LAN 側セグメント設定

設定データ名称	設定値	初期値
IP アドレス(再)	IPv4 アドレス	192.168.0.200
マスク長(再)	8~30	24

・LAN 側セグメント自動払い出し設定

設定データ名称	設定値	初期値
自動払い出し(再)	使用する/使用しない	使用する
リース時間(再)	1~72(時間)	4(時間)
払い出し開始 IP アドレス(再)	IPv4 アドレス	192.168.0.201
払い出し個数(再)	1~253	50
WINS サーバアドレス(再)	IPv4 アドレス	なし

5.3.2 ネットワーク設定 - ポート設定

・ポート設定(WAN,LAN1~4)

設定データ名称	設定値	初期値
通信速度	AUTO/ AUTO(100M MAX) /100M FULL/100M HALF /10M FULL/10M HALF	AUTO
MDI/MDI-X モード	AUTO/ MDI-X	AUTO

5.3.3 ネットワーク設定 - SPI 設定

・各種 SPI 設定

設定データ名称	設定値	初期値
TCP タイムアウト	30~7200(秒)	3600(秒)
UDP タイムアウト	30~7200(秒)	180(秒)
ICMP タイムアウト	30~7200(秒)	60(秒)

5.3.4 ネットワーク設定 - セキュリティ設定

・ファイアウォール設定(エントリ番号 1~96)

設定データ名称	設定値	初期値
ルール No.	0~999	0
フィルタ種別	許可/拒否	拒否
送信元 IP アドレス (開始 IP - 終了 IP)	* / IPv4 アドレス形式	*
プロトコル	* / 1~255 / 予約名 ([TCP][UDP][ICMP][TCP UDP])	*
送信元ポート (開始ポート - 終了ポート)	* / 1~65535 /予約名	*
宛先ポート (開始ポート - 終了ポート)	([ftp][ftpdata][telnet][smtp][domain][www][pop3][su nrpc][nntp][ntp][login][route][pptp])	
ICMP タイプ	* / 0~255	*
ICMP コード	* / 0~255	*
セキュリティログ保存	保存する/保存しない	保存する

5.3.5 ネットワーク設定 - パケットフィルタ設定

・パケットフィルタ設定(エントリ番号 1~128)

設定データ名称	設定値	初期値
ルール No.	0~999	0
通信方向	WAN→LAN/ LAN→WAN/両方向	WAN→LAN
フィルタ種別	許可/拒否	拒否
TCP フラグ	指定しない/SYN/ ESTABLISHED	指定しない
送信元 IP アドレス (開始 IP - 終了 IP)	* / IPv4 アドレス形式	*
宛先 IP アドレス (開始 IP - 終了 IP)	* / IPv4 アドレス形式	*
プロトコル	* / 1~255 / 予約名([TCP][UDP][ICMP][TCP UDP])	*
送信元ポート (開始ポート - 終了ポート)	* / 1~65535 /予約名	*
宛先ポート (開始ポート - 終了ポート)	([ftp][ftpdata][telnet][smtp][domain][www][pop3][su nrpc][nntp][ntp][login][route][pptp])	
ICMP タイプ	* / 0~255	*
ICMP コード	* / 0~255	*
セキュリティログ保存	保存する/保存しない	保存しない

5.3.6 ネットワーク設定 - URL フィルタ設定

・URL フィルタ許可設定

設定データ名称	設定値	初期値
URL フィルタ	使用しない/許可リスト設定/拒否リスト設定	使用しない

・URL フィルタ設定(エントリ番号 1~20)

設定データ名称	設定値	初期値
比較条件	ドメイン/キーワード	ドメイン
比較文字	半角英数字/一部記号(「.」「-」)(最大半角 255 文字)	なし

5.3.7 ネットワーク設定 - 静的 IP マスカレード設定

・静的 IP マスカレード設定(エントリ番号 1~50)

設定データ名称	設定値	初期値
優先順位	0~999	0
宛先 IP アドレス	IPv4 アドレス	なし
変換対象プロトコル	TCP/UDP/TCP と UDP 両方	TCP
宛先ポート	1~65535 /予約名 ([ftp][ftpdata][telnet][smtp][domain][www] [pop3][sunrpc][nntp][ntp][login][route][pptp])	なし
変換対象ポート	1~65535 /予約名 ([ftp][ftpdata][telnet][smtp][domain][www] [pop3][sunrpc][nntp][ntp][login][route][pptp])	なし

5.3.8 ネットワーク設定 - 静的 NAT 設定

・静的 NAT 設定(エントリ番号 1~64)

設定データ名称	設定値	初期値
優先順位	0~999	0
宛先 IP アドレス	IPv4 アドレス	なし
変換対象プロトコル	TCP/UDP/TCP と UDP 両方 /ICMP/全プロトコル(共有)	TCP
変換対象ポート (開始ポート - 終了ポート)	1~65535 /予約名 ([ftp][ftpdata][telnet][smtp][domain][www] [pop3][sunrpc][nntp][ntp][login][route][pptp])	なし

5.3.9 ネットワーク設定 - LAN 側ルーティング設定

・LAN 側ルーティング設定(エントリ番号 1~20)

設定データ名称	設定値	初期値
宛先 IP アドレス	IPv4 アドレス	なし
マスク長	8~32	なし
ゲートウェイ	IPv4 アドレス	なし

5.3.10 ネットワーク設定 - 高度な設定

・UPnP 設定

設定データ名称	設定値	初期値
UPnP 設定	使用する/使用しない	使用する

・PING 応答機能

設定データ名称	設定値	初期値
WAN 側セグメント 応答	応答する/応答しない	応答する
インターネット用 セグメント応答	応答する/応答しない	応答する

・外部へのサーバ公開設定

設定データ名称	設定値	初期値
外部へのサーバ公開	公開しない/仮想 DMZ で公開する /簡易的に公開する	公開しない
仮想 DMZ の IP アドレス空間	IPv4 アドレス	なし
マスク長	24~30	なし
DMZ をポート VLAN で区別する	区別しない/区別する(LAN1~4)	区別しない
公開するホストの IP アドレス	IPv4 アドレス	なし

5.4 制約事項

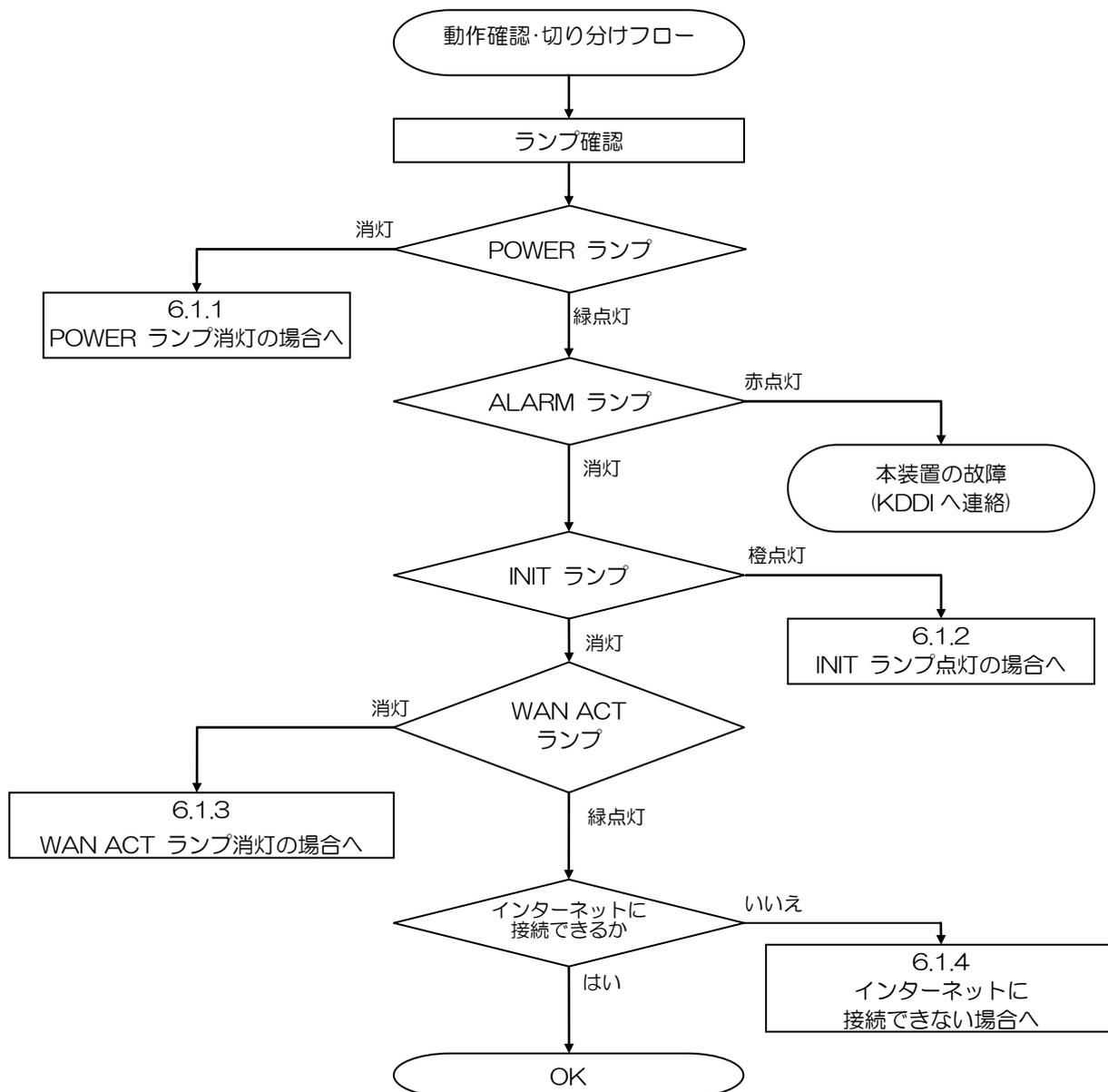
■設定データ保存

本装置は設定データのすべてを装置内蔵のフラッシュメモリーに格納します。設定データの保存中に、再起動あるいは電源断が発生した場合、最悪のケースでは装置内蔵のフラッシュメモリーが破壊され、システムを正常に運用することができなくなります。

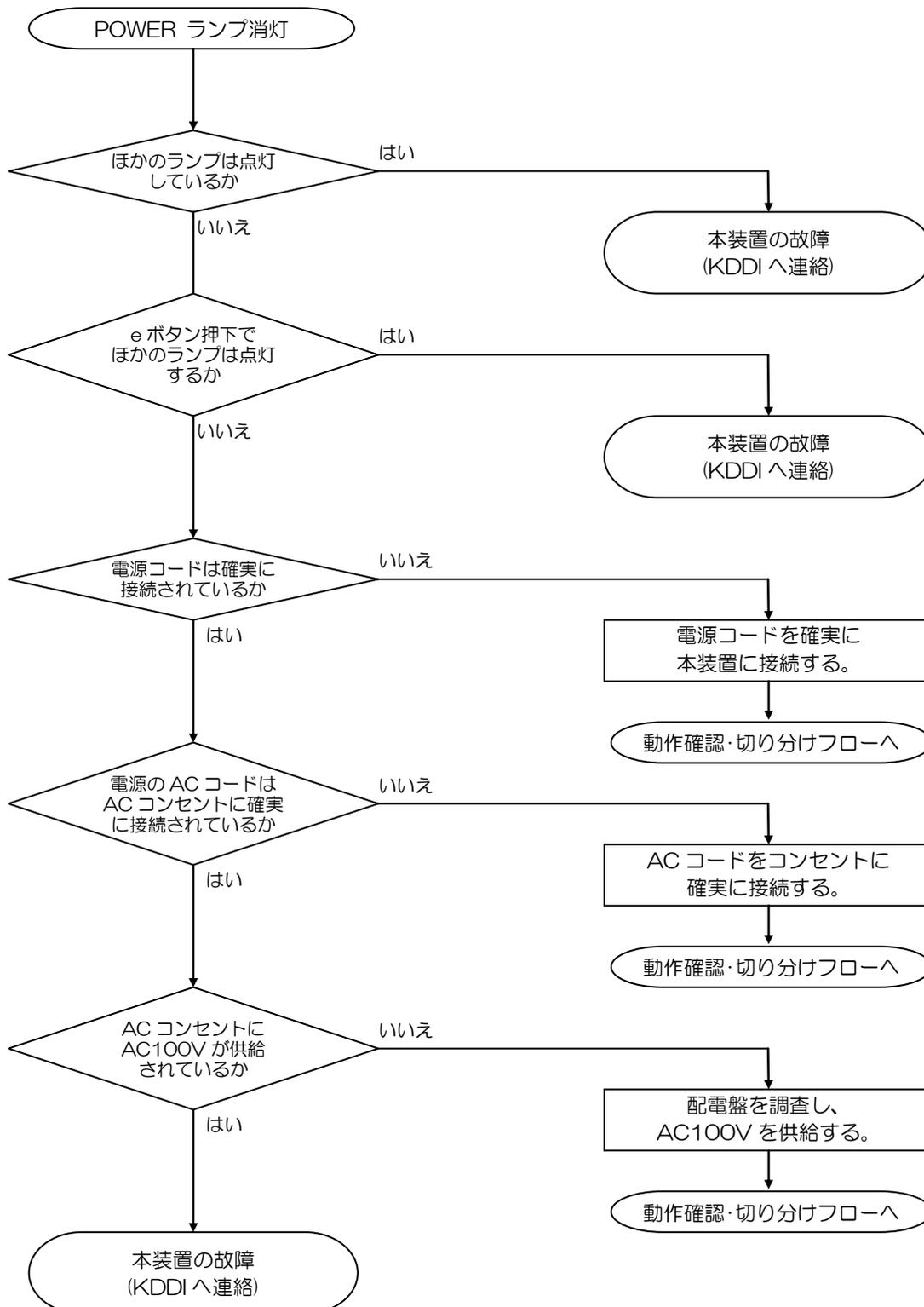
6 動作切り分け

6.1 動作切り分けフロー

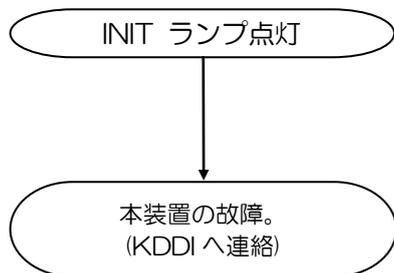
本装置の設置後の動作確認と障害切り分けフローを以下に示す。



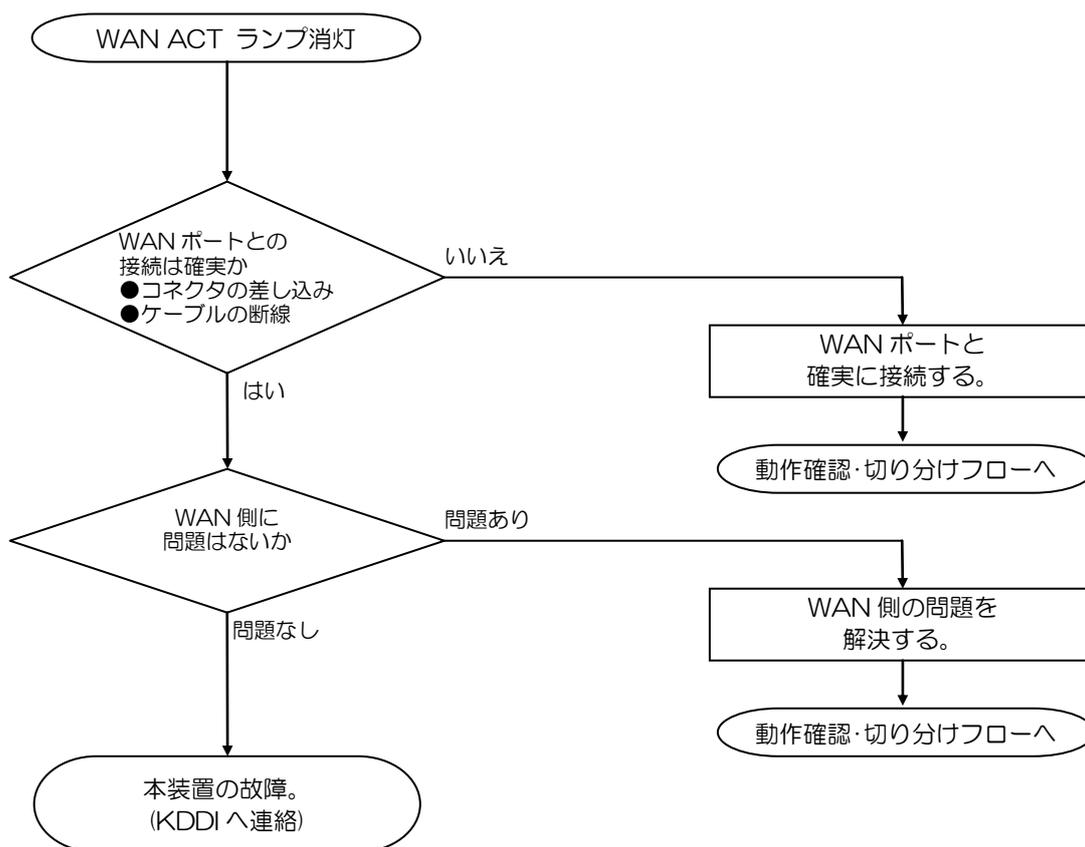
6.1.1 POWER ランプ消灯の場合



6.1.2 INIT ランプ点灯の場合

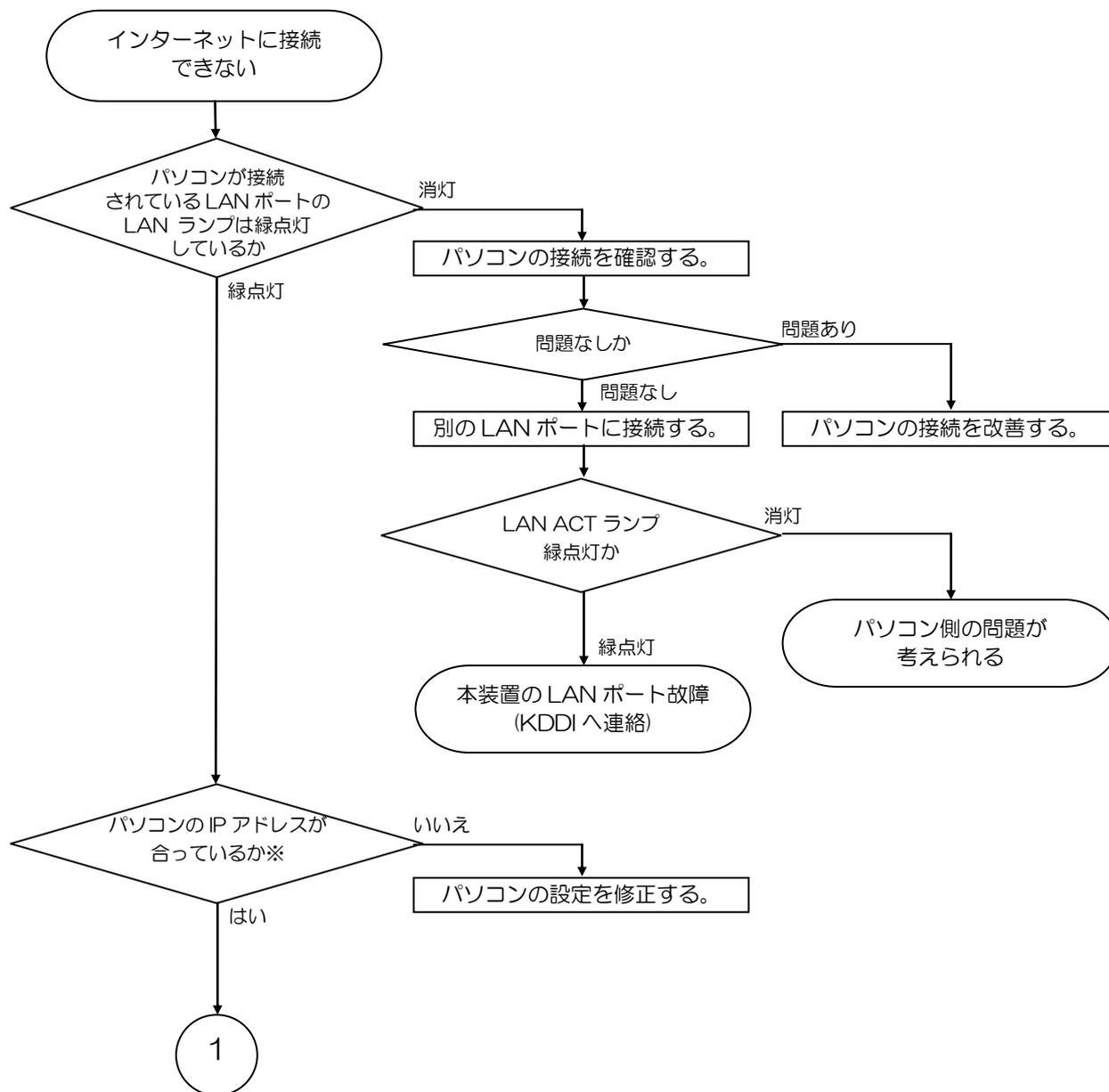


6.1.3 WAN ACT ランプ消灯の場合



※ WAN SPEED ランプは 1Gbps で点灯します。消灯している場合は、WAN 側の機器の速度を確認する。

6.1.4 インターネットに接続できない場合



※ 仮想 DMZ 設定時には、インターネットに接続するポートに制限が発生する。

