

トークネット光アダプタ取扱説明書

(タイプ a4,b4)

1.1 版



TOHKnet

ご使用前に




本書には、装置を安全に正しくお使いいただき、お使いになる方や他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とおり「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下さい。

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。）

厳守事項

パスワードの取り扱いについて

本装置の設定画面で入力していただくユーザ用パスワードはお客様の大切な個人情報です。パスワードを変更する場合、入力は必ずお客様自身で行ってください。

2018年12月1日以降にお申込みいただいたお客さまについては、本装置の設定変更をお客さまご自身で行うことが出来ませんので、パスワードの通知は行っていません。

ご使用にあたってのお願い

電波障害自主規制

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

VCCI-A

本装置の故障、誤動作、不具合、あるいは停電等の外部要因によって生じた損害等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兼ねますので、あらかじめご了承ください。本装置の設置には、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。

**装置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。**

本書および本装置のハードウェア、ソフトウェア、外観などの仕様は、お客様にお知らせすることなく変更される場合があります。

VCCIは、情報処理装置等電波障害自主規制協議会の略称です。

Windows Vista[®] は、Microsoft[®] Windows Vista[®] operating systemの略です。

Windows Vistaは、米国Microsoft Corporation の米国およびその他の国における商標です。

Windows[®] 7は、Microsoft[®] Windows[®] 7 operating systemの略です。

Windows[®] 8は、Microsoft[®] Windows[®] 8 operating systemの略です。

Windowsは米国Microsoft Corporationの米国およびその他の国における登録商標です。

Internet Explorer は、米国Microsoft Corporationの米国およびその他の国における登録商標または商標です。

JavaScript[®] は、米国およびその他の国における、Oracle の商標または登録商標です。

その他、各会社名、各製品名は各社の商標または登録商標です。

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。お客様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。
	すきま等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。
	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。

注意



	本装置に触れる場合には、予めラックの金属フレーム部を触る等、体にたまった静電気を除去してから作業を行なってください。 帯電したまま装置に触れると静電気による故障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、引っ張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、けがの原因となる場合があります。
	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。故障の原因となる場合があります。
	本装置を重ね置き設置しないでください。故障の原因となる場合があります。
	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	10
1.1.	本資料について	10
2.	本装置について	10
2.1.	機能概要	10
2.1.1.	機能概要	10
2.1.2.	システム構成について	11
2.1.3.	ネットワーク構成について	15
2.2.	機器の説明	22
2.2.1.	機器の外観	22
2.2.2.	各部の名称と機能	24
2.2.3.	ランプとボタン・スイッチの機能	27
2.2.4.	配線	29
2.3.	工事と手順	34
2.3.1.	設置工事	34
2.3.2.	接続工事	36
2.3.3.	電源の投入と電源投入後のランプ表示	46
3.	本装置の設定	47
3.1.	設定方法について	47
3.1.1.	保守端末の設定	47
3.1.2.	設定画面へのアクセス方法	58
3.1.3.	設定画面メニュー	59
3.2.	構成情報設定	61
3.2.1.	ネットワーク設定 - LAN 接続設定	61
3.2.2.	ネットワーク設定 - ポート設定	63
3.2.3.	ネットワーク設定 - SPI 設定	65
3.2.4.	ネットワーク設定 - セキュリティ設定	66
3.2.5.	ネットワーク設定 - パケットフィルタ設定	70
3.2.6.	ネットワーク設定 - URL フィルタ設定	75
3.2.7.	ネットワーク設定 - 静的 IP マスカレード設定	78
3.2.8.	ネットワーク設定 - 静的 NAT 設定	81
3.2.9.	ネットワーク設定 - LAN 側ルーティング設定	84
3.2.10.	ネットワーク設定 - 高度な設定	86
3.3.	情報表示	89
3.3.1.	装置状態表示	89
3.3.2.	UPnP 状態表示	91

3.3.3.	LAN 側自動払い出し状況	92
3.3.4.	ログ表示	93
3.3.5.	統計情報	95
3.4.	メンテナンス	102
3.4.1.	疎通確認 (PING)	102
3.4.2.	メンテナンス - ログインパスワード変更	103
3.4.3.	メンテナンス - 装置設定の保存 / 復元	104
3.4.4.	メンテナンス - 装置再起動	105
3.5.	電話の設定	106
3.5.1.	着信ポート選択	106
3.5.2.	ユーザ個別情報	108
3.5.3.	端末インタフェース設定	110
4.	機器仕様	111
4.1.	方式諸元	111
4.1.1.	ハードウェア諸元	111
4.1.2.	ソフトウェア諸元	112
4.2.	サービス機能	113
4.2.1.	ルーティング対象 - IPv4	113
4.2.2.	LAN 接続 - IPv4 アドレス払い出し機能	114
4.2.3.	ポート - 通信速度選択機能	115
4.2.4.	ポート - MDI/MDI-X 選択機能	116
4.2.5.	セキュリティ - ファイアウォール機能	117
4.2.6.	セキュリティ - SPI 機能	118
4.2.7.	セキュリティ - パケットフィルタ機能	119
4.2.8.	セキュリティ - URL フィルタ機能	120
4.2.9.	セキュリティ - PING 応答選択機能	121
4.2.10.	ルーティング - 静的 IP マスカレード機能	122
4.2.11.	ルーティング - 静的 NAT 機能	123
4.2.12.	ルーティング - 動的 NAT、動的 IP マスカレード機能	124
4.2.13.	ルーティング - ポートフォワーディング機能	125
4.2.14.	ルーティング - LAN 側ルーティング機能	126
4.2.15.	ルーティング - 仮想 DMZ 機能	127
4.2.16.	ルーティング - 簡易 DMZ 機能	128
4.2.17.	ルーティング - ポート VLAN 機能	129
4.2.18.	ルーティング - DNS リレー機能	130
4.2.19.	ルーティング - VPN パススルー機能	131
4.2.20.	UPnP - UPnP 選択機能	132
4.3.	構成情報一覧	133
4.3.1.	ネットワーク設定 - LAN 接続設定	133

4.3.2.	ネットワーク設定 - ポート設定	133
4.3.3.	ネットワーク設定 - SPI 設定	134
4.3.4.	ネットワーク設定 - セキュリティ設定	134
4.3.5.	ネットワーク設定 - パケットフィルタ設定	135
4.3.6.	ネットワーク設定 - URL フィルタ設定	136
4.3.7.	ネットワーク設定 - 静的 IP マスカレード設定	136
4.3.8.	ネットワーク設定 - 静的 NAT 設定	137
4.3.9.	ネットワーク設定 - LAN 側ルーティング設定	137
4.3.10.	ネットワーク設定 - 高度な設定	138
5.	参考	139
5.1.	互換表示設定方法	139

1. はじめに

1.1. 本資料について

本資料は、トークネット光に提供されるアダプタ（ONU とお客様 LAN を接続するためのルータ。この資料では「本装置」と記載します。）の取扱説明書となります。

2. 本装置について

2.1. 機能概要

2.1.1. 機能概要

本装置は、以下に示すインターネット接続機能（BBR 機能）と IP 電話接続機能（音声 GW 機能）を有しています。

（ 1 ）インターネット接続機能（BBR 機能）

本装置は、10M/100M/1G bit/s 自動認識の LAN インタフェースを 4 ポート収容し、本装置の LAN 配下に接続した装置を WAN 側に接続するブロードバンドルータ機能を有しています。

（ 2 ）IP 電話接続機能（音声 GW 機能）

本装置は、FXS または BRI を PBX 等に接続し、WAN 側の SIP サーバ等へ VoIP で接続する音声ゲートウェイ機能を有しています。

2.1.2. 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 IP 網に接続し、IP 網を経由してインターネットおよび電話網への接続を行いません。

インターネットには、本装置の LAN 側に接続された PC 等の端末から本装置、IP 網を経由して接続します。また、電話網には、本装置の FXS または BRI インタフェースに接続された PBX 等の配下の電話機から、本装置、IP 網を経由して接続します。

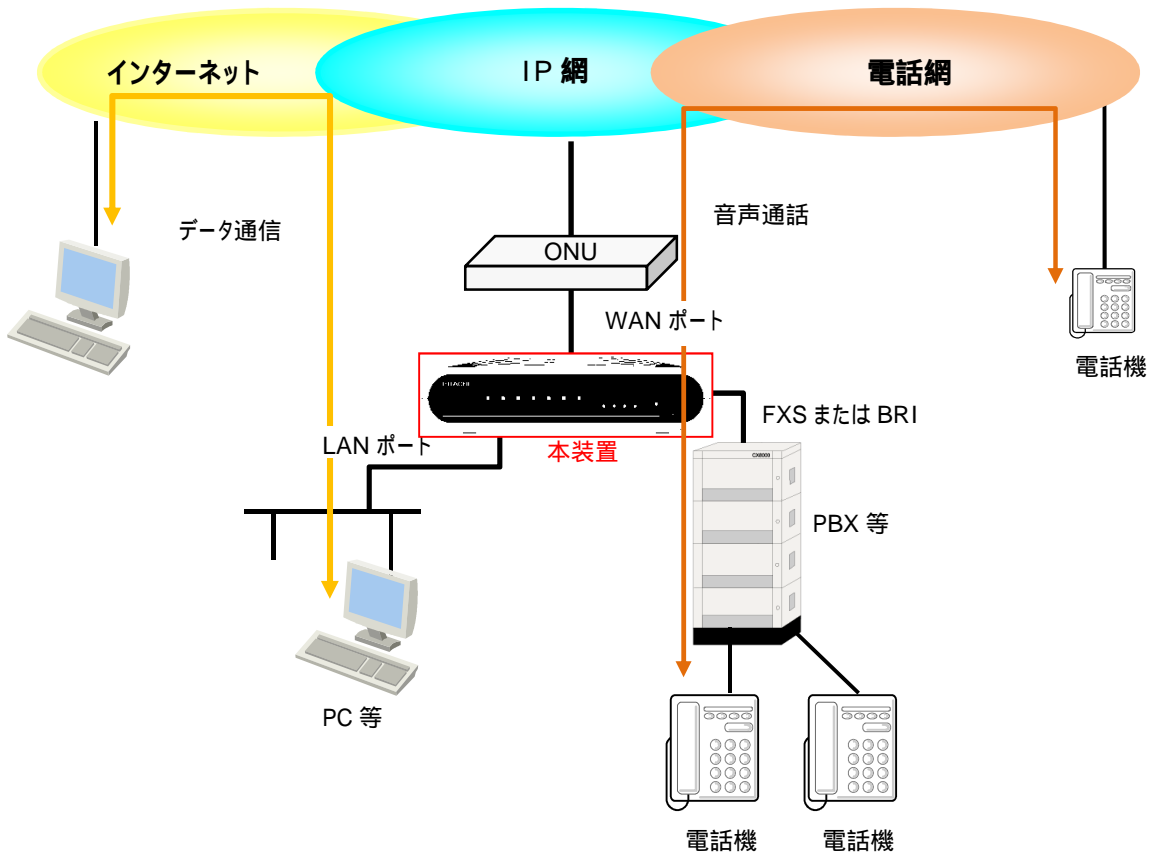


図 2.1.2-1 システム構成例

本書では WAN 側を IP 網とも示します。

本装置を利用した構成としては、以下の 3 通りがあります。

- 「電話のみ利用」 ……PBX/電話機を接続して電話機能を使用する
- 「電話 + インターネット利用」 ……PBX/電話機を接続して電話機能を使用する、また PC 等の端末を接続してインターネット通信を行う
- 「インターネットのみ利用」 ……PC 等の端末を接続してインターネット通信を行う

各構成を以下に示します。

2.1.2.1. 「電話のみ利用」の構成

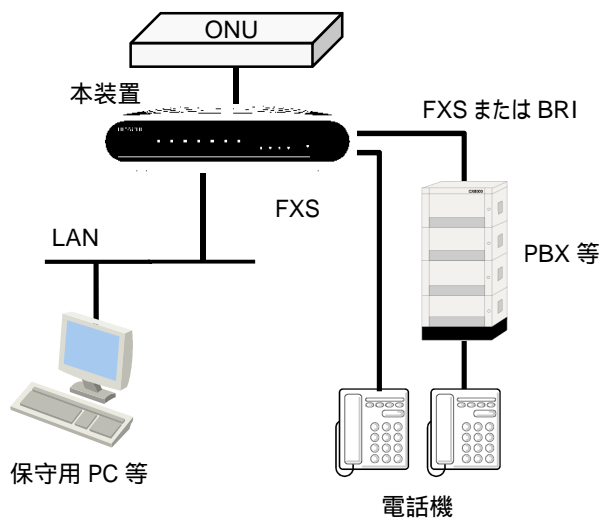


図 2.1.2.1-1 「電話のみ利用」の構成

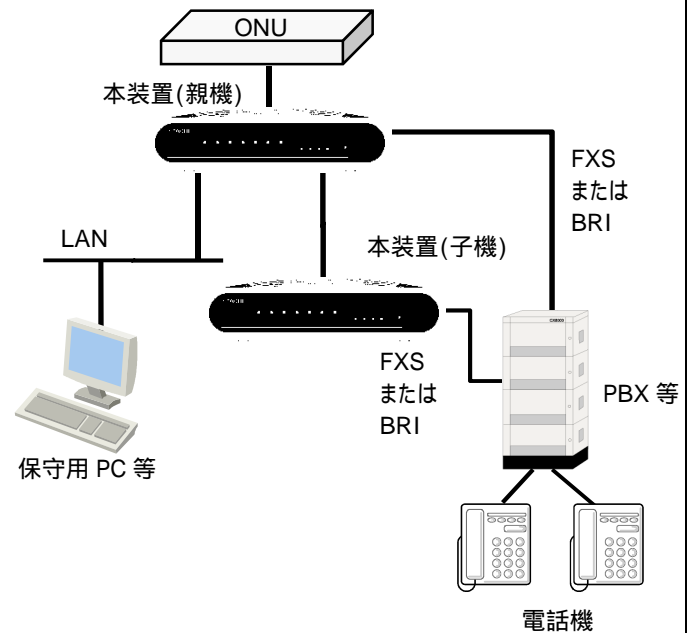


図 2.1.2.1-2 「電話のみ利用」の構成
(カスケード接続)

本装置の FXS ポートまたは BRI ポートに PBX または電話機等を接続します。接続した電話機により音声通話が行えます。

FXS タイプの場合は 4 ポートを持ち、BRI タイプの場合は 2 ポートを持っております。カスケード接続構成により、FXS は 8 ポート、BRI は 4 ポートまで拡張できます。

カスケード接続する場合は、親機、子機で同一インターフェースに統一する必要があります。(親機 FXS , 子機 BRI とはできない)

本装置の LAN ポートに PC 等を接続することもできますが、PC 等は本装置の保守用 (本装置の Web 設定用) としてのみ使用でき、インターネット接続はできません。

2.1.2.2. 「電話 + インターネット利用」の構成

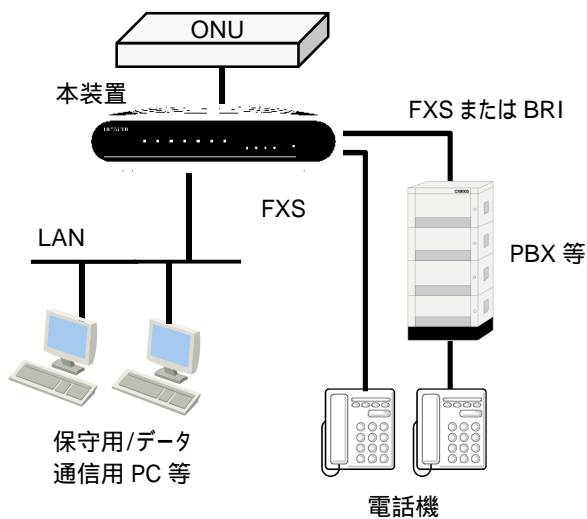


図 2.1.2.2-1 「電話 + インターネット利用」の構成

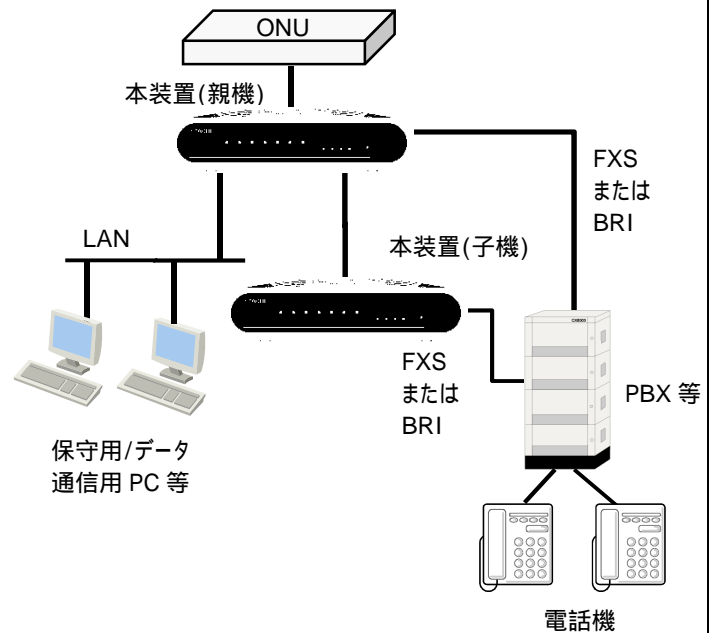


図 2.1.2.2-2 「電話 + インターネット利用」の構成
(カスケード接続)

本装置の FXS ポートまたは BRI ポートに PBX または電話機等を接続します。接続した電話機により音声通話が行えます。

FXS タイプの場合は 4 ポートを持ち、BRI タイプの場合は 2 ポートを持っております。カスケード接続構成により、FXS は 8 ポート、BRI は 4 ポートまで拡張できます。

カスケード接続する場合は、親機、子機で同一インターフェースに統一する必要があります。(親機 FXS , 子機 BRI とはできない)

また、本装置の LAN ポートに PC 等を接続し、PC 等からのデータ通信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。NAT しない設定とした場合には、PC 等からのデータ通信アクセスは本装置での NAT/IP マスカレードは行われません。

なお、本構成でカスケード接続した場合、カスケード子機ではインターネット通信はできません。

2.1.2.3. 「インターネットのみ利用」の構成

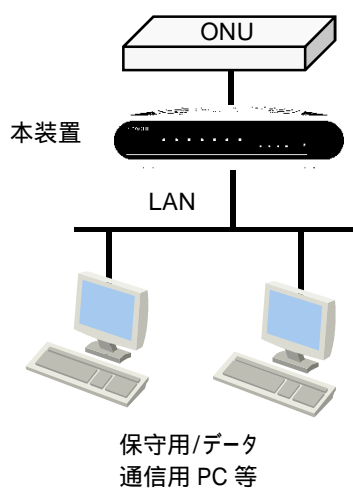


図 2.1.2.3-1 「インターネットのみ利用」の構成

本装置の LAN ポートに PC 等を接続し、PC 等からのデータ通信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。NAT しない設定とした場合には、PC 等からのデータ通信アクセスは本装置での NAT/IP マスカレードは行われません。

2.1.3. ネットワーク構成について

2.1.3.1. ネットワーク構成

本装置は、音声通信、インターネット通信（以下、データ通信）、カスケード接続を行うために複数の IP アドレスを WAN ポート、LAN ポートに割り当てを行います。

下図に本装置で割り当てを行う通信セグメント/IP アドレスを示します。

各セグメントは LAN ポート毎に 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おります。そのため、WAN 側に電話用、データ通信用セグメントの 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、カスケード用セグメント、仮想 DMZ 用セグメントの IP アドレスが割り当てられます。（設定により割り当てられる IP アドレスは変化する。）

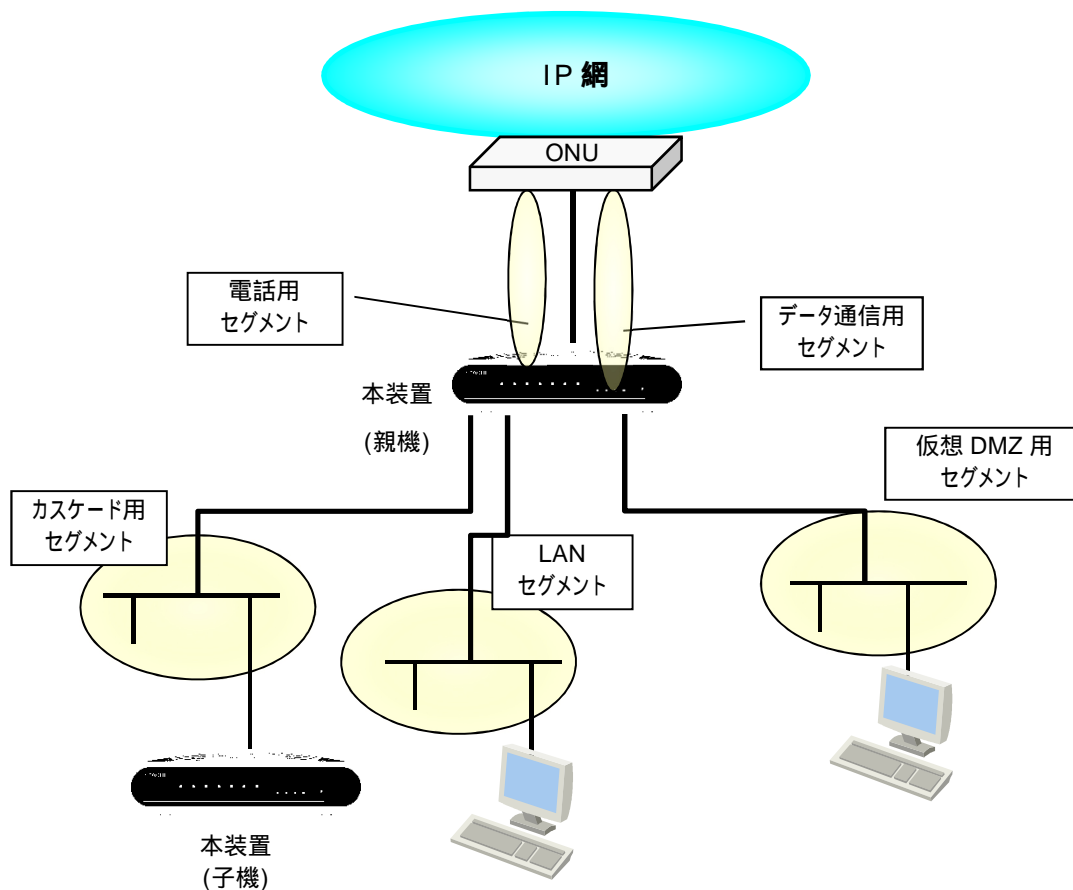


図 2.1.3.1-1 本装置の通信セグメント

本図ではセグメント、IP アドレスに絞った構成図としているため、FXS/BRI インタフェース及び PBX 等の電話機器については省略している。

(1) 電話用セグメント

電話用セグメントの IP アドレスは WAN ポートに割り当てます。電話用 IP アドレスは音声通信を行う場合に使用し、音声通話 (SIP、RTP/RTCP パケットの送受信) は電話用 IP アドレスとなります。音声用 IP アドレスは本装置内でクローズし、LAN 側からは見えません。

(2) データ通信用セグメント

データ通信用セグメントの IP アドレスは WAN ポートに割り当て、データ通信を行う場合に使用します。データ通信では LAN 側に接続された端末 (PC 等) がデータ通信アクセスを可能とするために、LAN セグメントの PC 等端末からの通信を本装置内で NAT / IP マスカレードを行い、データ通信用 IP アドレスに変換して通信を行います。

(3) LAN 用セグメント

LAN セグメントの IP アドレスは LAN ポートに割り当て、本装置の保守用として使用します。LAN 側 IP アドレスは本装置の DHCP 機能により PC 等の端末へアドレスを払い出しますが、このアドレスは LAN セグメントのアドレスとなります。

NAT しない設定とした場合には、本装置では NAT / IP マスカレードを行わず、ソースアドレスを LAN 側 IP アドレスのままフォワーディングします。

(4) 仮想 DMZ 用セグメント

仮想 DMZ 用セグメントの IP アドレスは LAN ポートに割り当て、データ通信接続を行う場合で、仮想 DMZ 機能を使用する場合に使用します。

データ通信を使用しない場合および、データ通信を使用するが、仮想 DMZ を使用しない場合には本セグメントは割り当てを行いません。(セグメント、IP アドレスを割り当てない)

(5) カスケード接続用セグメント

カスケード接続用セグメントの IP アドレスは、本装置同士をカスケード接続する場合に使用します。

カスケードの親機の場合は LAN ポートにカスケード接続 IP アドレスを割り当めます。子機の場合は WAN ポートに割り当てを行い、カスケード親機と子機間の通信 (疎通確認、音声通信) のみに使用します。(外部との接続は不可)

本セグメントのサブネットは /29 固定となります。

カスケード接続を行わない場合は本セグメントの割り当てを行いません。

以下に各構成によるセグメント使用状況を示します。

2.1.3.2. 「電話のみ利用」の場合

(1) 本装置単独の場合

「電話のみ利用」の場合は、『電話用セグメント』『LAN セグメント』を使用します。

音声通話は『電話用セグメント』を使用します。

保守接続には『LAN セグメント』を使用します。

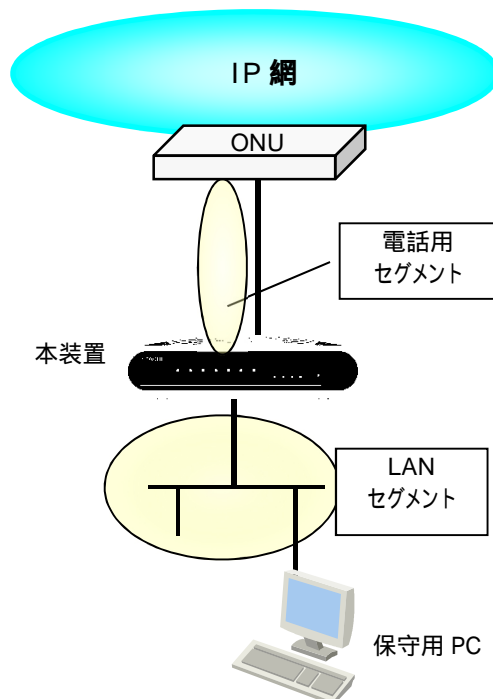


図 2.1.3.2-1 電話を使用設定時の通信セグメント

(2) カスケード接続構成の場合

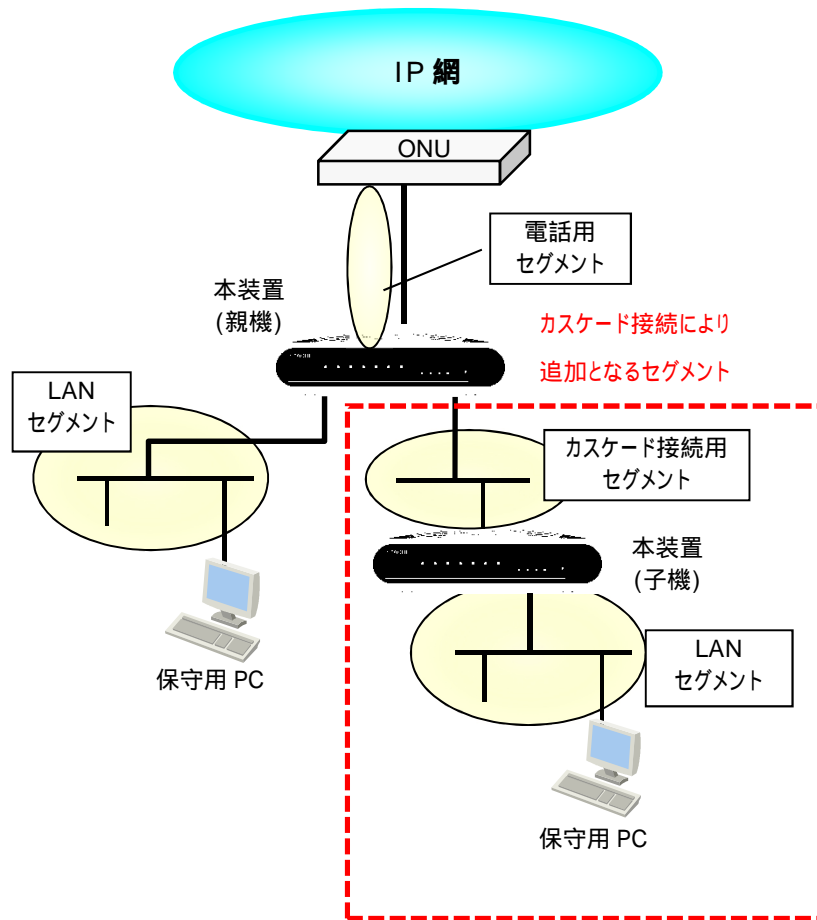


図 2.1.3.2-2 カスケード接続時の通信セグメント

カスケード接続を行った場合には、『カスケード接続用セグメント』が追加となります。
カスケード子機の場合、『カスケード接続用セグメント』と、『LAN セグメント』となります。

2.1.3.3. 「電話 + インターネット利用」の場合

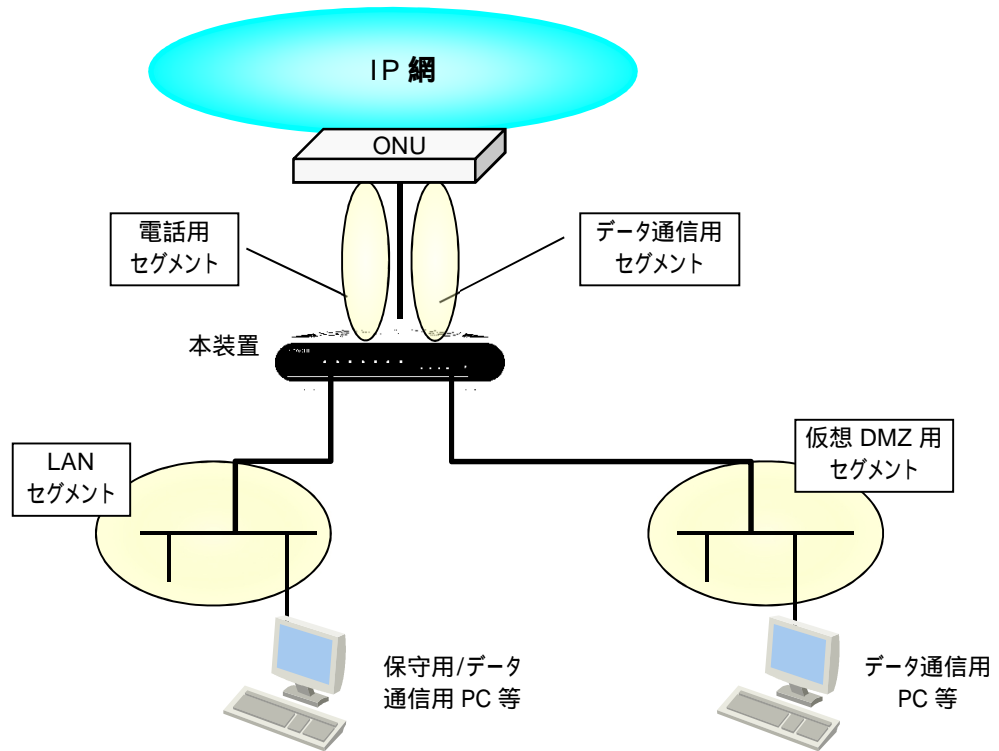


図 2.1.3.3-1 電話、データ通信を使用時の通信セグメント

「電話 + インターネット」の場合は、『電話用セグメント』『データ通信用セグメント』『LAN セグメント』を使用します。設定により『仮想 DMZ 用セグメント』を使用します。

音声通話は『電話用セグメント』を使用します。

インターネット通信は『データ通信用セグメント』を使用します。データ通信用セグメントの設定内容により、『LAN セグメント』もデータ通信で使用します。

仮想 DMZ 機能を使用する場合は『仮想 DMZ 用セグメント』を使用します。

カスケード接続を行った場合には、『カスケード接続用セグメント』が追加となります。

2.1.3.4. 「インターネットのみ利用」の場合

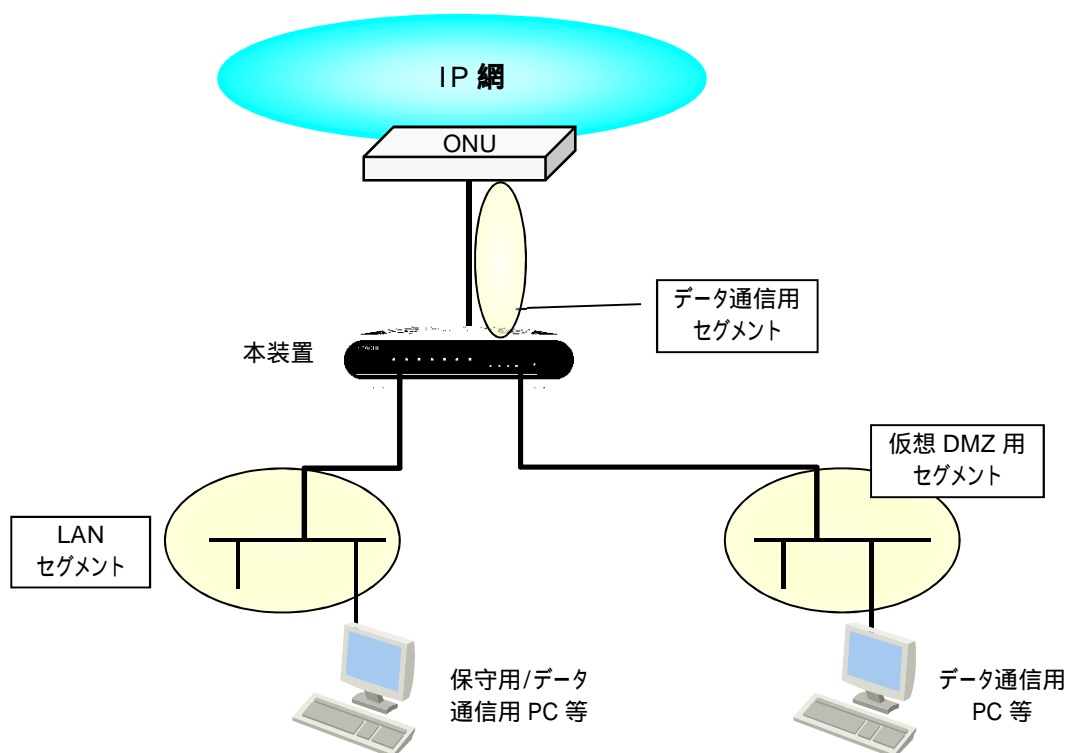


図 2.1.3.4-1 データ通信を使用時の通信セグメント

「インターネットのみ利用」の場合は、『データ通信用セグメント』を使用する。データ通信用セグメントの設定内容により、『LAN セグメント』もデータ通信で使用します。

仮想 DMZ 機能を使用する場合は『仮想 DMZ 用セグメント』を使用します。

2.1.3.5. 各構成におけるセグメント設定

サービス選択の各設定におけるセグメント使用状況を表 2.1.3.5-1 に示します。

本装置では、使用可能なセグメントが多岐にわたるため、各セグメントに設定する IP アドレス・ネットワークが重複しないように設定を行うこと。

表 2.1.3.5-1 各サービス選択時のセグメント使用状況

セグメント 構成	セグメント				
	B (電話)	C (データ通信)	D (LAN 側)	E (仮想 DMZ)	F (カスケード)
「電話のみ利用」		×		×	
「電話 + インターネット利用」					
「インターネット利用」	×				×

：セグメント、IP アドレスの設定が必要

×：セグメント、IP アドレスの設定が不要(使用しない)

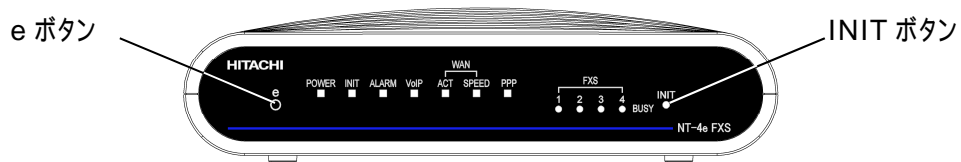
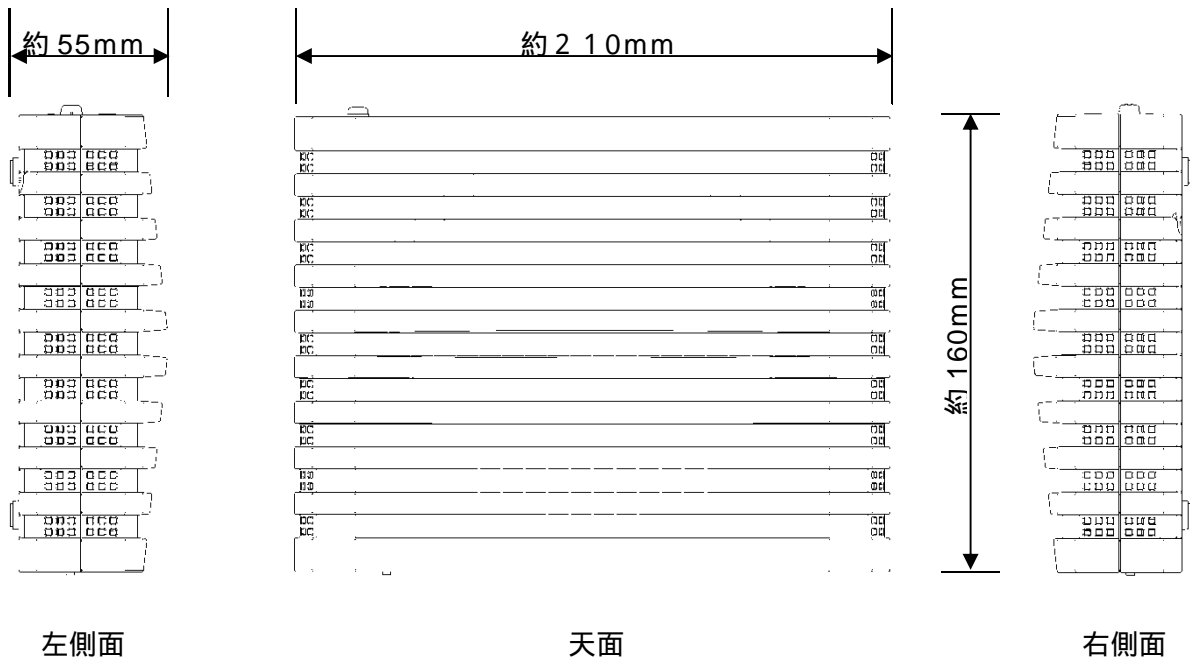
：使用する場合はサービス選択以外の箇所でセグメント、IP アドレスの設定が必要

：保守端末接続としてのみ使用

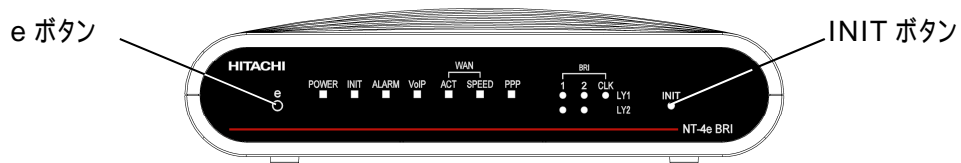
2.2. 機器の説明

本装置について、外観や各部の名称などを示します。

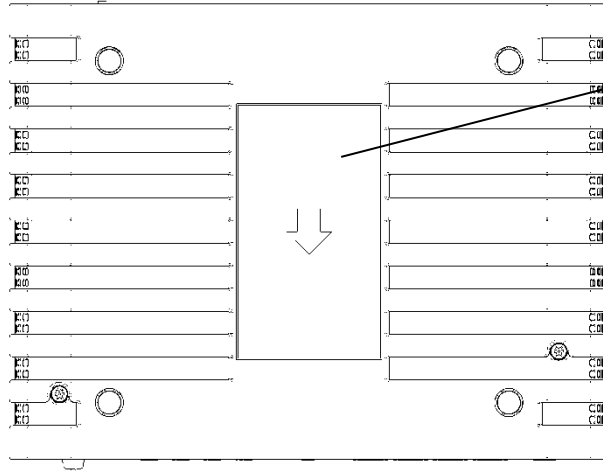
2.2.1. 機器の外観



正面 (FXS)

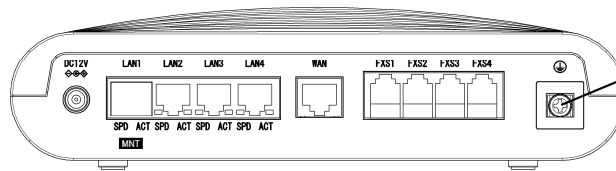


正面 (BRI)



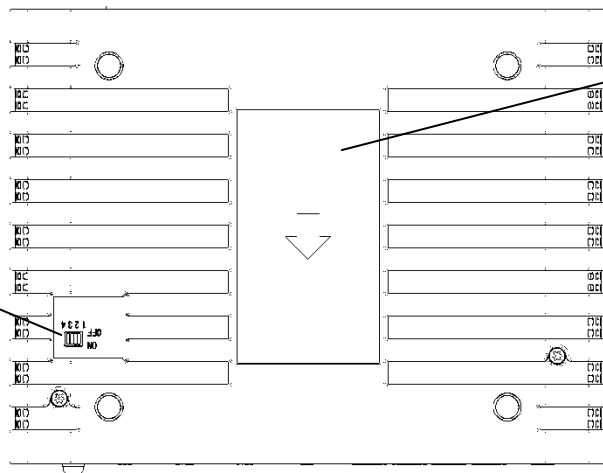
品名紙

底面 (FXS)



F G 端子

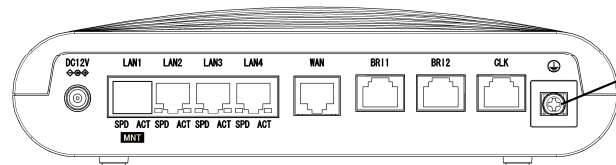
背面 (FXS)



品名紙

スライドスイッチ

底面 (BRI)



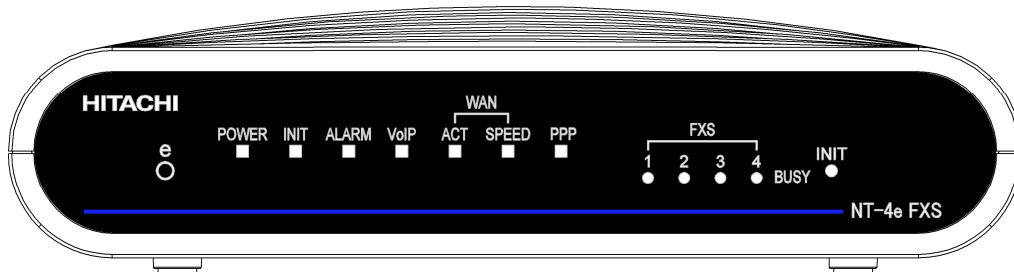
F G 端子

背面 (BRI)

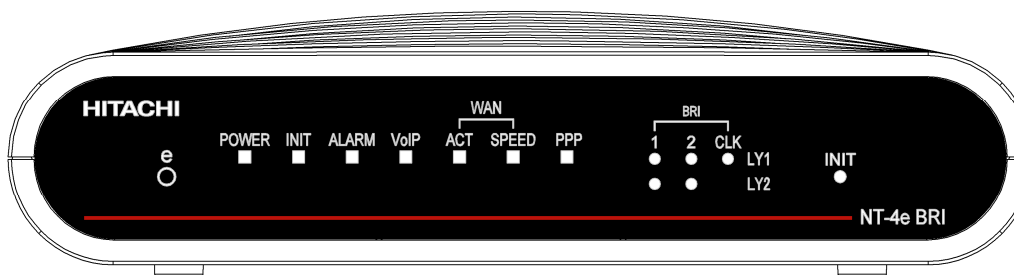
2.2.2. 各部の名称と機能

各部の名称ならびに機能を示します。

2.2.2.1. 各部の名称と機能（正面）



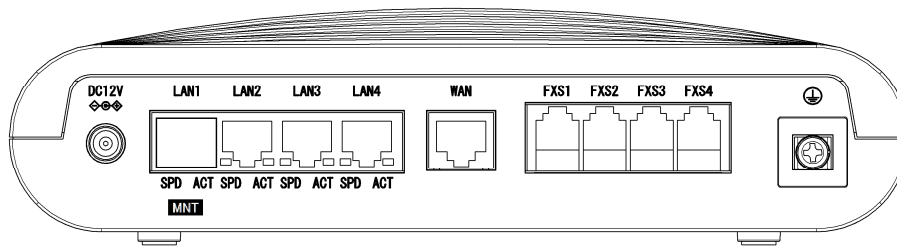
正面（FXS）



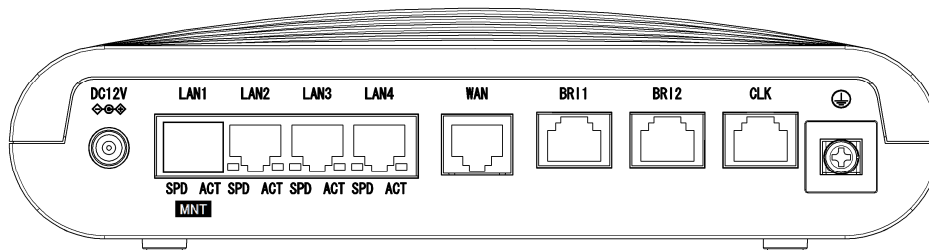
正面（BRI）

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
PPP ランプ	PPPoE 接続状態表示
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。 通信できなくなるため、使用しないでください。

2.2.2.2. 各部の名称と機能（背面）



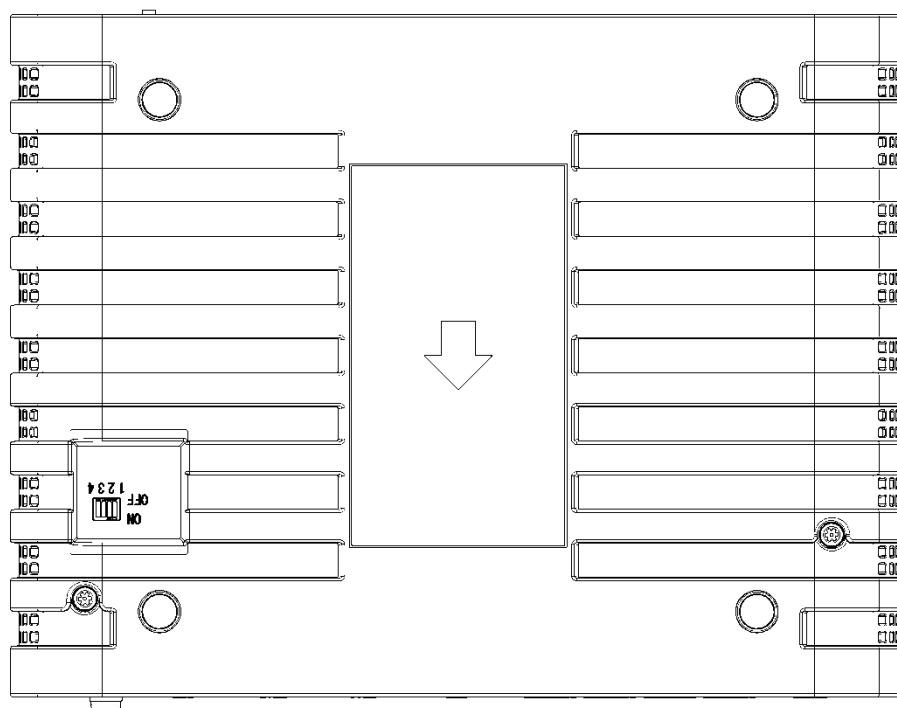
背面（FXS）



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、電話機器等を接続する。
BRI1～2ポート	PBX 等を接続する。
CLK ポート	ISDN 基本インタフェース（S/T 点）等を接続する クロック同期ポート。
FG 端子	アース線を接続する。 アース線は、1.6mm以上のものを使用のこと。

2.2.2.3. 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）	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。

2.2.3. 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します。

2.2.3.1. 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します。

ランプ名称	状態	機能
POWER	消灯	電源オフ
	緑点灯	装置動作中
	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、本装置の故障
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 10Mbit/s 時または未接続
	橙点灯	回線速度 1Gbit/s または 100Mbit/s 時
PPP	消灯	PPPoE 接続なし
	緑点灯	PPPoE 接続あり
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 10Mbit/s 時または未接続
	橙点灯	LAN 速度 1 Gbit/s / 100Mbit/s 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

2.2.3.2. 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します。

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 網と接続できなくなるため、使用しないで下さい。
スライドスイッチ	BRI CLK ポート 100 終端抵抗 入・切	CLK ポート内蔵の終端抵抗を切り離す場合にスイッチ全て（1～4）を OFF（切）にする。 工場出荷時は、全て ON（入）側になっている。

2.2.4. 配線

WAN/LAN ならびに FXS、BRI (CLK) インタフェースに対する配線を示します。

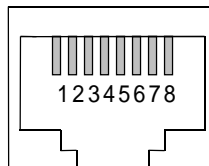
2.2.4.1. WAN/LAN 配線用 UTP ケーブルについて

WAN および LAN インタ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 5 UTP 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 6 UTP ケーブル(以下カテゴリ 6 ケーブル)を使用します。本装置の WAN および LAN インタフェースは、MDI/MDIX 自動切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。(WAN 側は MDI 固定、LAN 側は MDIX 固定の設定も可能)

以下に WAN/LAN インタフェースの仕様を示します。

項目		仕様		
インタフェース仕様	インタフェース	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 切替え (WAN 側は MDI 固定も可、LAN 側は MDIX 固定も可)		
	インピーダンス	100		
	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)



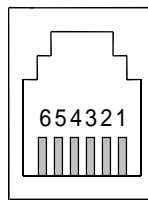
ピン No.	1000BASE-T		100BASE-TX/10BASE-T	
	MDI	MDIX	MDI	MDIX
1	BI DA+	BI DB+	TD+	RD+
2	BI DA-	BI DB-	TD-	RD-
3	BI DB+	BI DA+	RD+	TD+
4	BI DC+	BI DD+	未使用	未使用
5	BI DC-	BI DD-	未使用	未使用
6	BI DB-	BI DA-	RD-	TD-
7	BI DD+	BI DC+	未使用	未使用
8	BI DD-	BI DC-	未使用	未使用

2.2.4.2. FXS ケーブルについて

以下に FXS インタフェースの仕様を示します。

項目	仕様
配線（線路条件）	450 以下（アナログ通信端末の直流抵抗含む） ブランチ不可
コネクタ	RJ-11

FXS コネクタ（RJ-11）

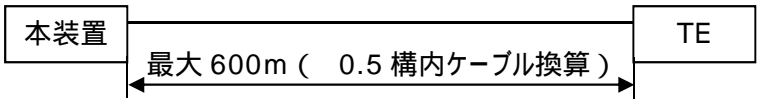
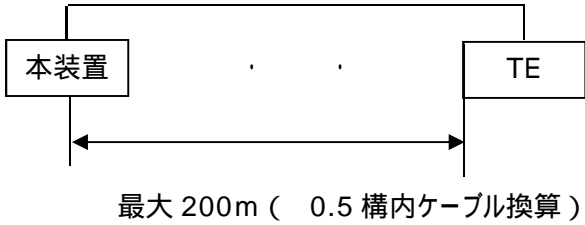


ピン No.	略 称	方 向		備 考
		本装置	PBX など	
1				
2				
3	LA	←	→	極性：+
4	LB	←	→	極性：-
5				
6				

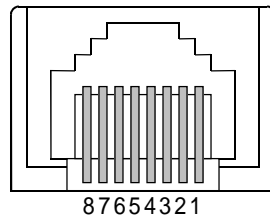
注：接続極性に注意のこと。極性を逆に接続すると、通話できない場合があります。

2.2.4.3. BRI (CLK) 配線用ケーブルについて

以下に BRI 1・2 インタフェースの仕様を示します。

項目		仕様
インタフェース仕様	インタフェース	BRI
	インタフェース規定	TTC 標準 JT-I430
配線	ポイント-ポイント接続	
	ポイント-マルチポイント接続 (短距離受動バス配線)	
最大端末接続台数		2 台 (BRI 1、BRI2 にそれぞれ 1 台ずつ接続可能)
コネクタ		RJ-45

BRI コネクタ (RJ-45)



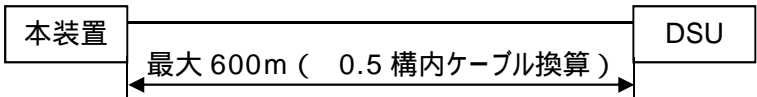
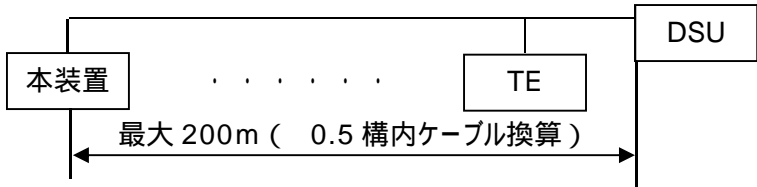
ピン No.	略称	方向	
		本装置(NT)	PBX 等(TE)
1			
2			
3	RA	←	→
4	TA	→	→
5	TB	→	→
6	RB	←	→
7			
8			

CLK ポートについて

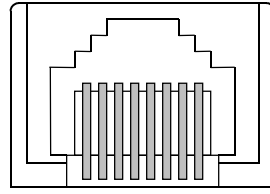
CLK ポートを ISDN 基本インタフェース回線に接続する場合、回線の契約は「ポイント-マルチポイント接続」または「ポイント-ポイント接続」の「レイヤ 1 常時起動」とすること。

なお、「ポイント-マルチポイント接続」の延長受動バス配線はできない。

以下に CLK ポートの仕様を示します。

項目		仕様
インタフェース仕様	インタフェース	BRI
	インタフェース規定	TTC 標準 JT-I430
配線	ポイント-ポイント接続	 <p>終端抵抗は配線上に 1 つとすること。本装置は終端抵抗を内蔵している。本装置以外の場所に終端抵抗を入れる場合は、本装置のスライドスイッチを OFF 側にして内蔵終端抵抗を切り離すこと。</p>
	ポイント-マルチポイント接続 (短距離受動バス配線)	 <p>バス上の最遠端の TE 部分のみに終端抵抗を入れること。本装置は終端抵抗を内蔵している。本装置が最遠端でない場合は、本装置のスライドスイッチを OFF 側にして内蔵終端抵抗を切り離すこと。</p>
コネクタ		RJ-45

CLK コネクタ (RJ-45)



87654321

ピン No.	略 称	方 向 (ストレート)	
		本装置 (TE)	DSU 等 (NT)
1			
2			
3	TA	→	→
4	RA	←	←
5	RB	←	←
6	TB	→	→
7			
8			

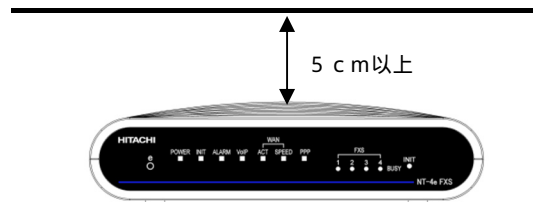
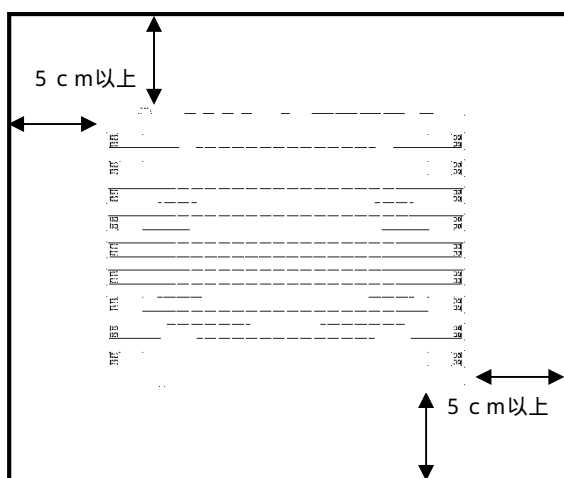
DSUに接続する場合には、アレスタ等の一次保護回路が挿入されていることを確認すること。
 なお、クロック同期方法については、2.3.2.4 BRIの接続を参照のこと。

2.3. 工事と手順

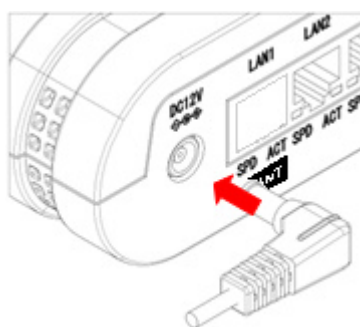
2.3.1. 設置工事

水平な場所に設置し、装置の前後左右と上面それぞれ 5 c m 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。

耐震バンド等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等の方法を取ること。



電源コードは、図のように本体側へしっかりと差し込むこと。

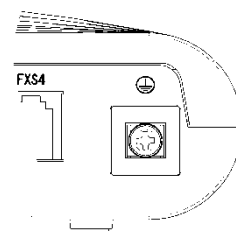


本装置の FG 端子は、必ずアースに接続（D 種接地）すること。

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る。

また、外来ノイズによる誤動作の可能性がある。

アース線は、1.6mm 以上のものを使用のこと。



【注意】

装置の設置に関して、以下の点に注意し設置すること。

- ・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・屋外等、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（温泉地等）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。
- ・空調などの風が直接当たる場所には設置しないこと。
- ・磁気および電磁波等の影響が懸念される場所（電子レンジ、スピーカ等）には設置しないこと。

2.3.2. 接続工事

2.3.2.1. 準備

本装置の接続工事に必要な以下のものを準備すること。

- ・ 接続機器（PBX 等）の取扱説明書および工事保守マニュアル
- ・ 保守端末（保守用 PC）

対応 OS	対応 Web ブラウザ
Microsoft [®] Windows [®] 8.1	Internet Explorer [®] 11
Microsoft [®] Windows [®] 8	Internet Explorer [®] 11
Microsoft [®] Windows [®] 8	Internet Explorer [®] 10
Microsoft [®] Windows [®] 7	Internet Explorer [®] 11
Microsoft [®] Windows [®] 7	Internet Explorer [®] 10
Microsoft [®] Windows [®] 7	Internet Explorer [®] 9
Microsoft [®] Windows [®] 7	Internet Explorer [®] 8
Microsoft [®] Windows Vista [®] (SP1/SP2 を含む)	Internet Explorer [®] 7 以上

Web ブラウザのバージョンにより、表示に差異が発生する場合があります。

正常に表示されない場合は、互換勢表示設定方法の操作を実施する。

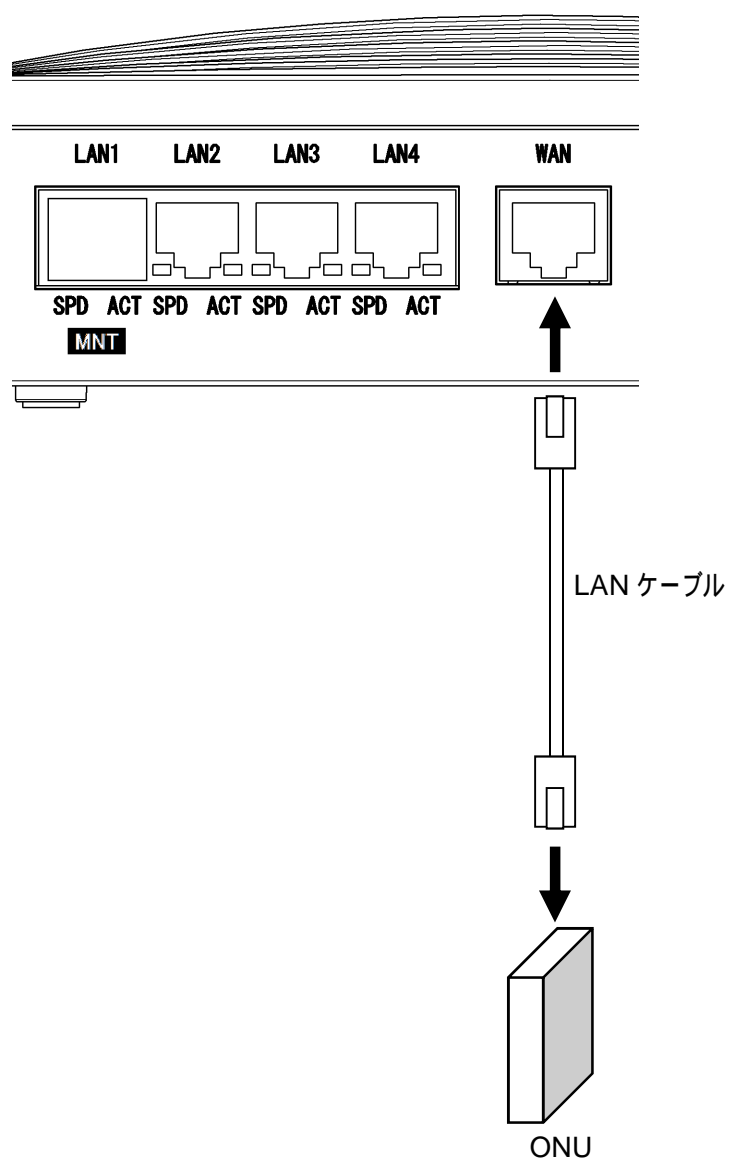
- ・ WAN 接続用ケーブル
- ・ LAN 接続用ケーブル
- ・ FXS または BRI 接続用ケーブル（必要に応じてモジュラーローゼットなど）
- ・ FG 接続用ケーブル（アース線は、1 . 6 mm 以上のものを使用のこと。）
- ・ 工具類（ドライバーなど）
- ・ テスター類（電圧チェック用など）

2.3.2.2. WAN の接続

本装置の WAN ポートと、ONU を LAN ケーブルで接続する。

カスケード接続(子)の場合は、カスケード接続(親)の LAN ポートに接続する。LAN ケーブル以外を WAN ポートに接続しないこと。

LAN ケーブルはカテゴリ 5e またはカテゴリ 6 のケーブルを使用すること。

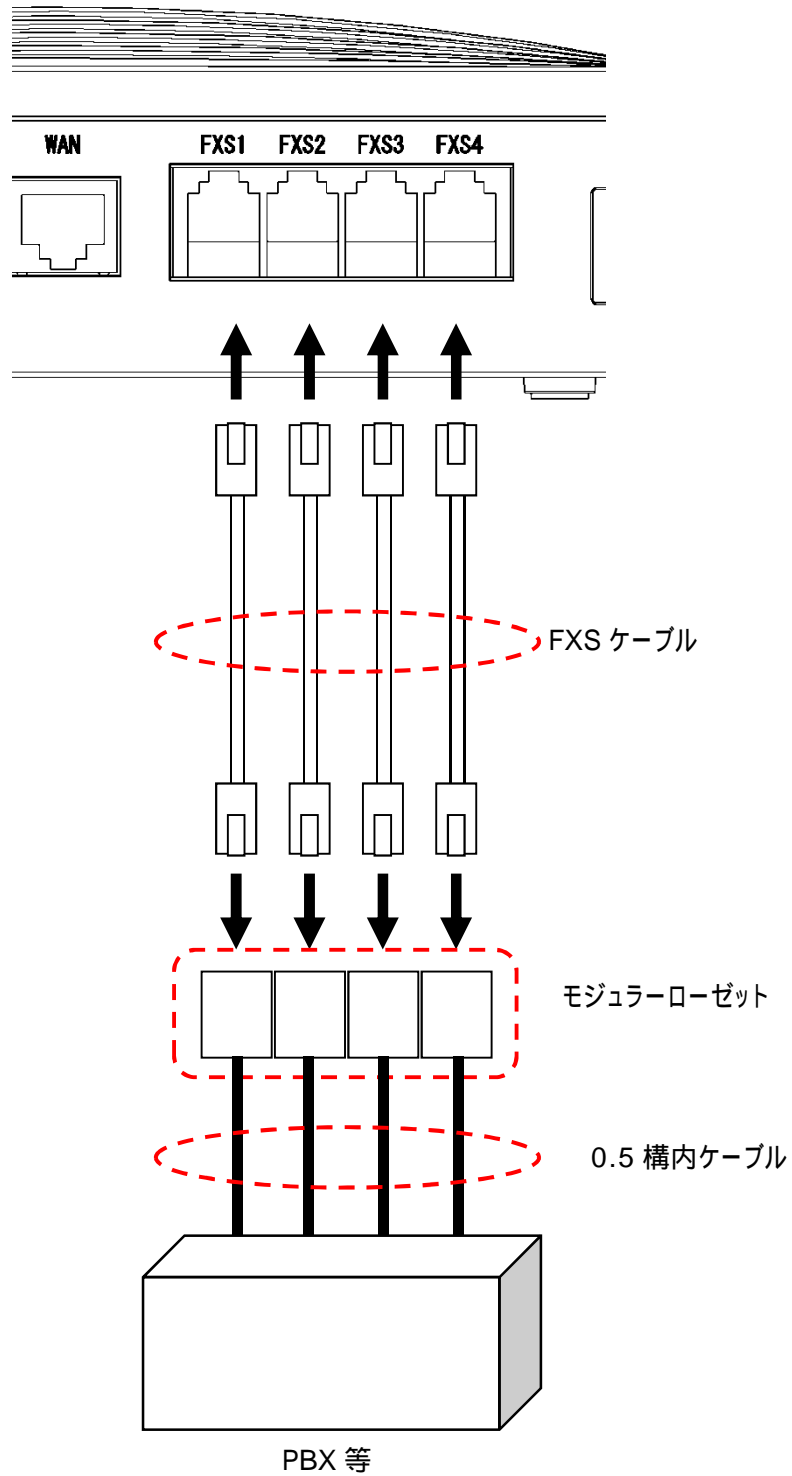


2.3.2.3. FXS の接続

FXS ポートと PBX 等を接続する。

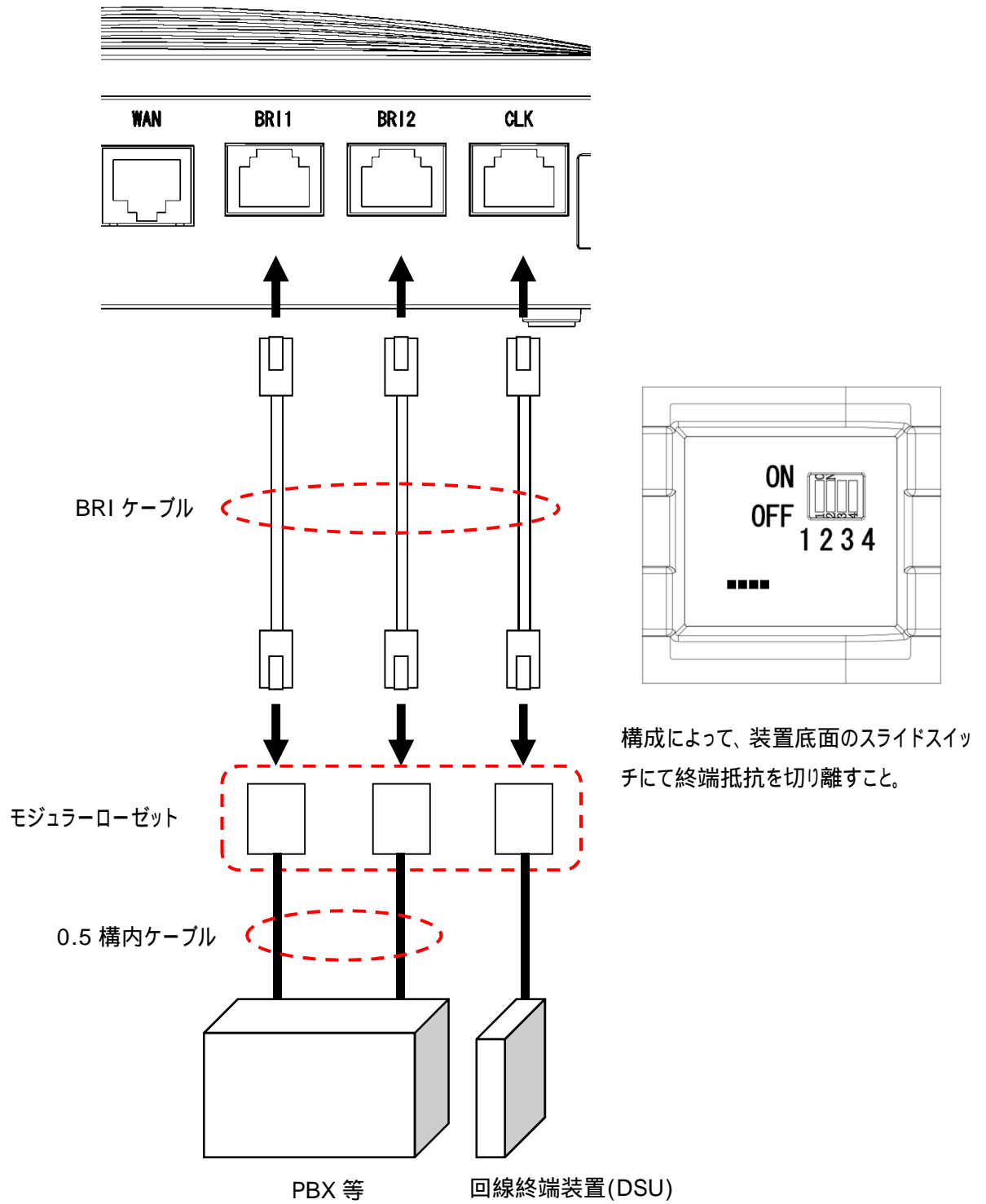
FXS ケーブル以外を FXS ポートに接続しないこと。

注：接続極性に注意のこと。極性を逆に接続すると、通話できない場合があります。



2.3.2.4. BRI の接続

BRI ポートと PBX 等を接続する。
BRI ケーブル以外を BRI ポートに接続しないこと。



【参考】

クロック同期方式について

BRIタイプにおいて、PBX等とのクロック同期を確実に行うためには、ISDN基本インタフェース回線を準備し、ISDN基本インタフェース回線からのクロックをマスターとすることを推奨する。

ISDN基本インタフェース回線がない場合は、本装置の自走クロックをマスターとしてPBX側が同期する方式が基本となる。

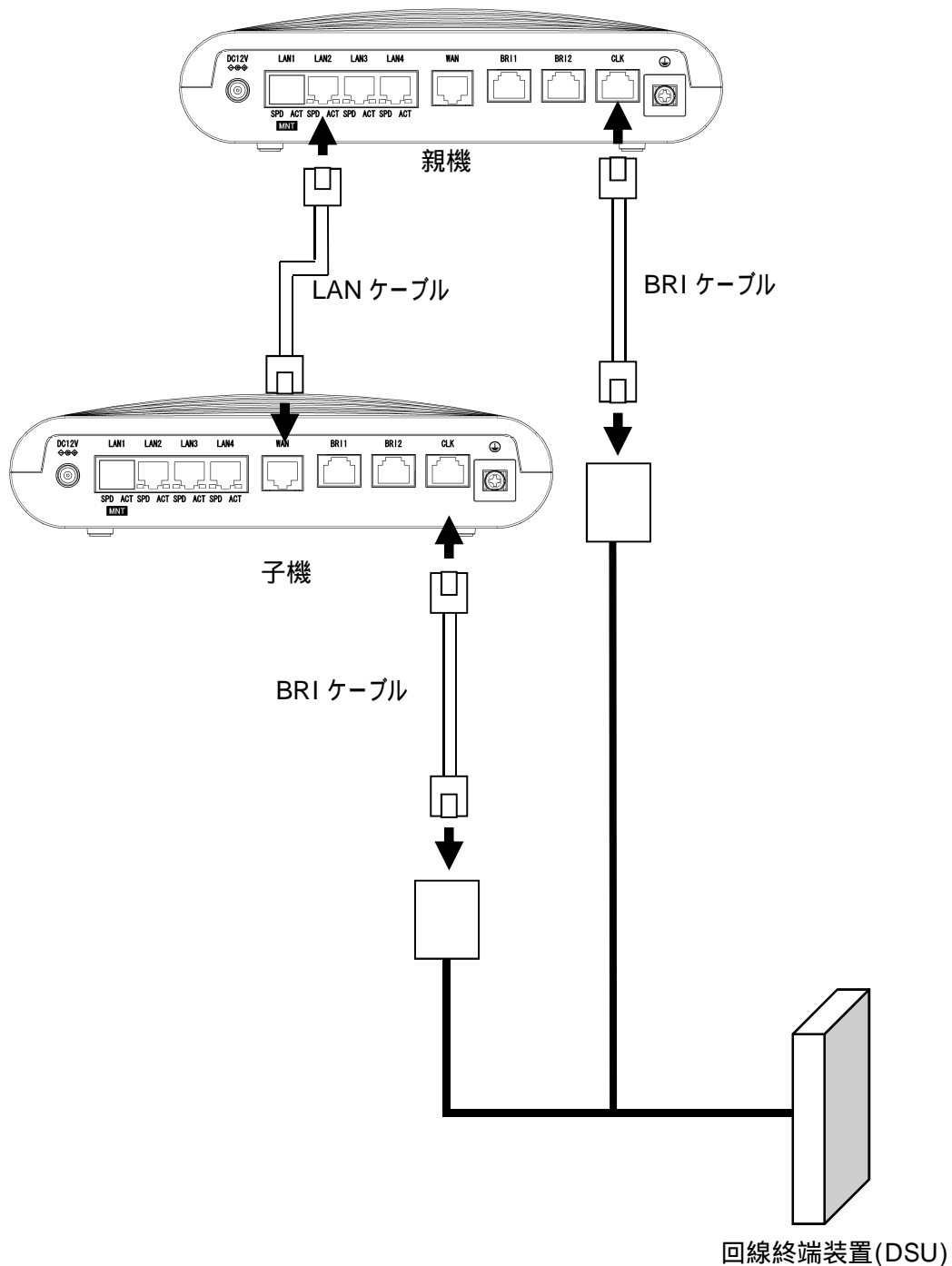
(1) ISDN 基本インタフェース回線との接続

ISDN 基本インタフェース回線と接続する場合、回線の契約は「ポイント - マルチポイント接続」の「レイヤ1 常時起動」とすること。レイヤ1 呼毎起動であっても動作はするが推奨しない。

本装置の設定は、CLK ポートを「有効」とし、本装置の設定も「P - MP（常時接続）」とすること。（子機についても同様に設定すること。）

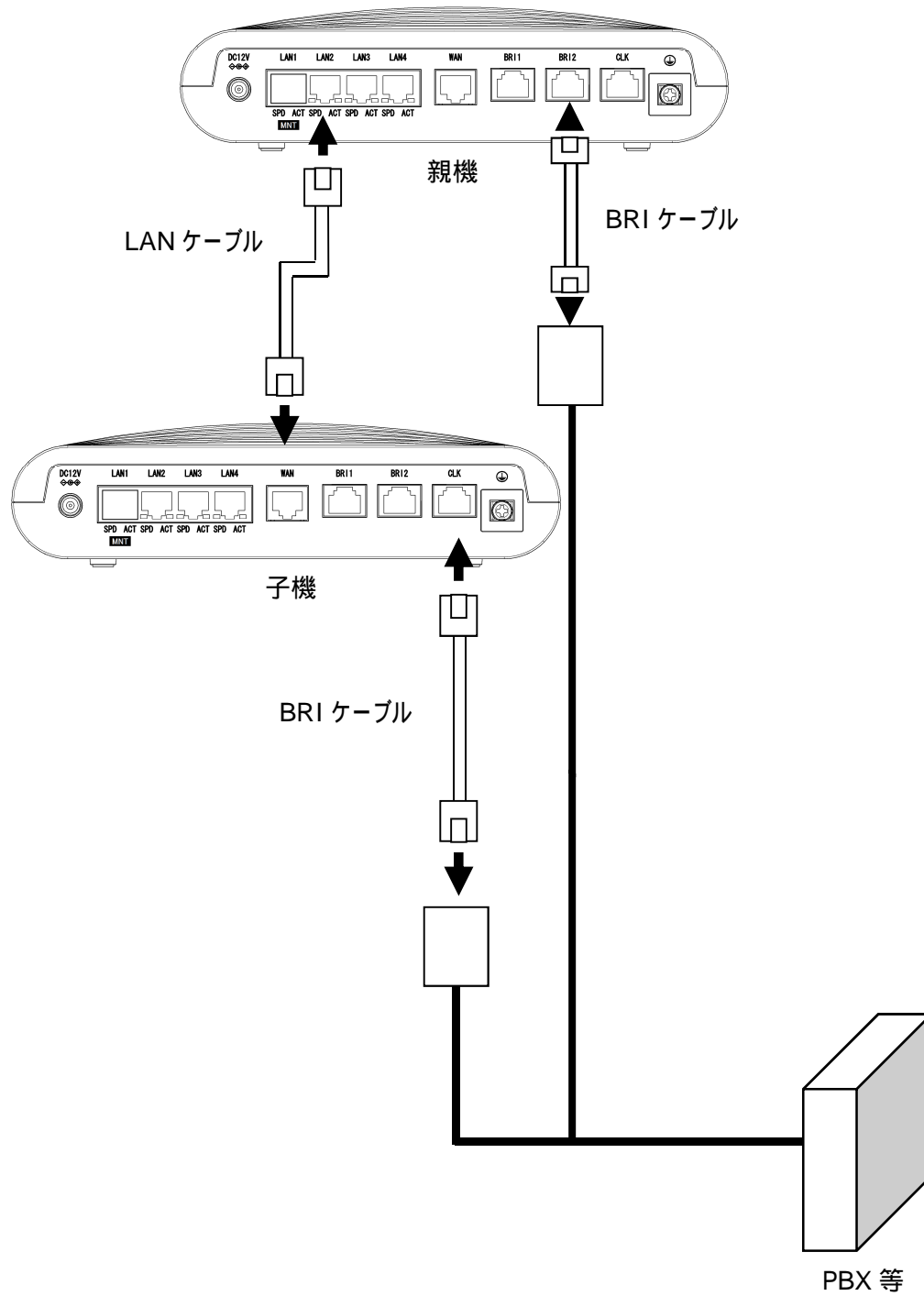
また、DSU から一番遠いところに終端抵抗を入れること。

本装置は、終端抵抗を内蔵している。本装置が最遠端でない場合は、スライドスイッチを全てOFF にすることで内蔵の終端抵抗を切り離す。



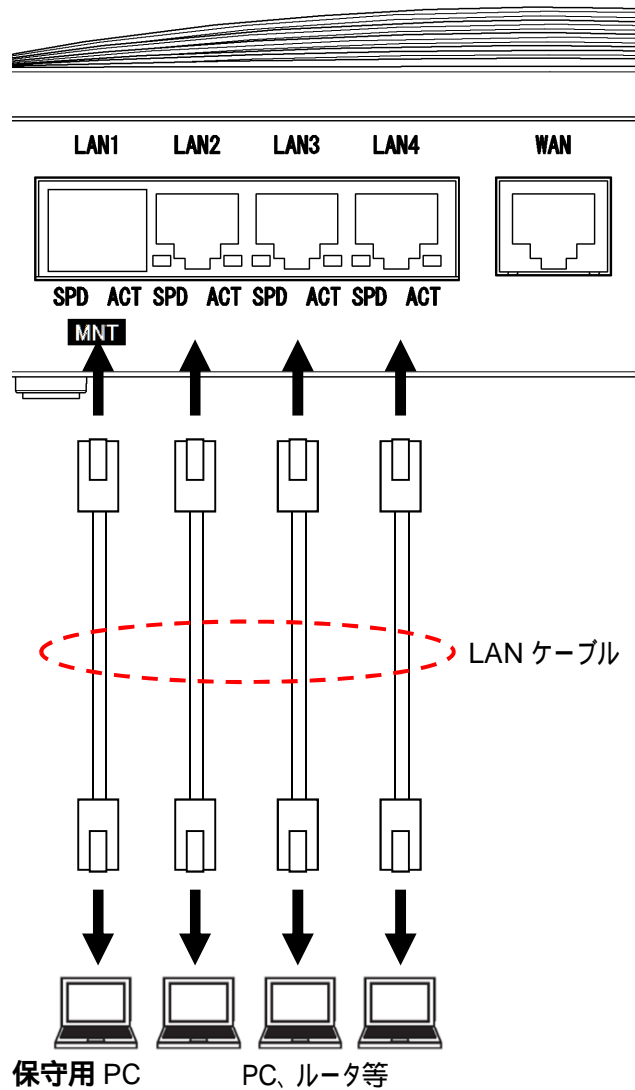
(2) ISDN 基本インタフェース回線がない場合

この場合、本装置の BRI ポートがクロック供給元となり、PBX、本装置の子機にクロックを供給する。
本装置の設定は、親機側のクロック供給元となる BRI ポートの設定を「P - MP (常時接続) 」とし、子機側の CLK ポートを「有効」とし、「P - MP (常時接続) 」とすること。



2.3.2.5. LAN の接続

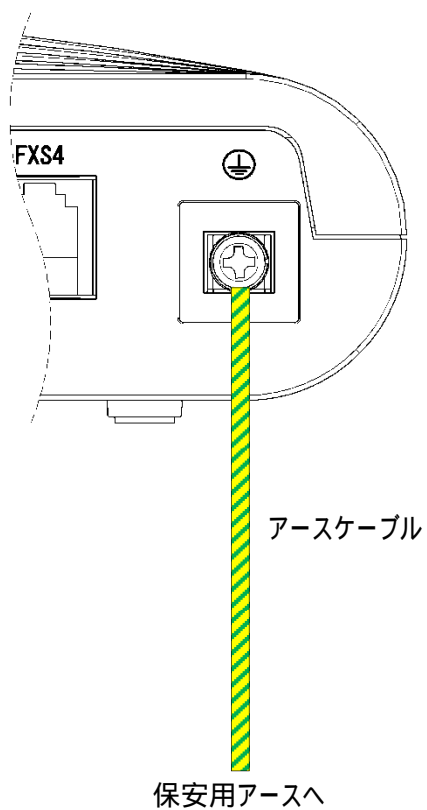
本装置の LAN ポートに、PC、ルータ等を LAN ケーブルで接続する。
LAN ケーブル以外を LAN ポートに接続しないこと。
LAN ケーブルはカテゴリ 5e またはカテゴリ 6 のケーブルを使用すること。



保守用 PC を接続するために LAN1 ポートを空けておくことを推奨する。
LAN1 ポートに保守用 PC を接続する場合は、キャップを外して接続する。

2.3.2.6. FG の接続

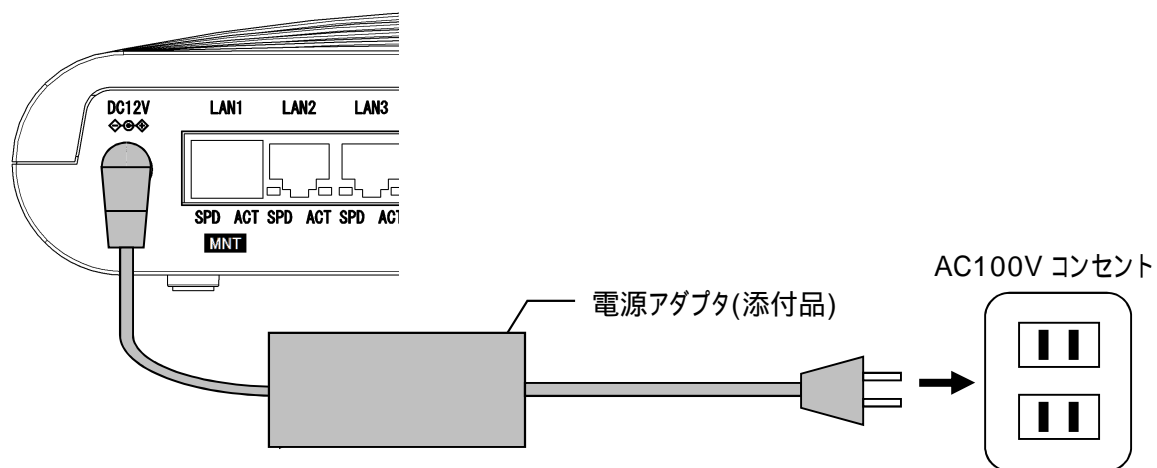
本装置の FG 端子にアース線を接続する。



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る。
また、外来ノイズによる誤動作の可能性もある。
アース線は、緑 / 黄色 AWG 14 (1.6mm) 以上のものを使用のこと。

2.3.2.7. 電源の接続

本装置に添付の電源アダプタを接続し、電源アダプタの A C プラグを AC100V の商用電源に接続する。電源スイッチはなく、接続後すぐに起動します。



添付の電源アダプタ以外は、絶対に接続しないこと。

電源コードは、図のように本体側へしっかりと差し込むこと。

2.3.3. 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。

ランプ名称	電話使用あり	電話使用なし	説明
	親機		
POWER ランプ	点灯緑	点灯緑	
ALARM ランプ	消灯	消灯	
VoIP ランプ	点灯緑	消灯	電話使用しない設定では常に消灯。
WAN ACT ランプ	点灯緑	点灯緑	
PPP ランプ	消灯	消灯	常に消灯。

(ランプ表示の異常状態)

POWER 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、本装置の故障である。電源アダプタの接続を確認すること。

ALARM ランプが赤点灯した場合は、本装置の故障、または 8 回連続で本装置のファームウェアが立ち上がらなかった (本装置の立ち上げ中に電源オフされたを含む) 場合である。

電源を再投入しても ALM ランプ点灯する場合は本装置の故障であり、機器交換となる。

電話使用あり設定で VoIP ランプ消灯時は、設定および ONU・電話網側の状態を確認すること。

WAN ACT ランプ消灯は、本装置の WAN ポートの接続状態、または ONU・電話網側の状態を確認すること。

3. 本装置の設定

3.1. 設定方法について

本装置の設定は、WEB ブラウザを使用して行ないます。保守端末を本装置の LAN ポートに接続して、本装置にアクセスします。

2018 年 12 月 1 日以降にお申込みいただいたお客さまについては、お客さまご自身での設定変更はできません。設定変更を希望される場合は、別途当社へお申込みが必要となります。

3.1.1. 保守端末の設定

本装置の保守端末（保守用 PC）の設定方法を示します。

設定例は本装置が DHCP サーバとして機能する場合の手順となります。

保守端末の対応 OS と対応 Web ブラウザを以下に示します。

対応 OS	対応 Web ブラウザ
Microsoft [®] Windows [®] 8.1	Internet Explorer [®] 11
Microsoft [®] Windows [®] 8	Internet Explorer [®] 11
Microsoft [®] Windows [®] 8	Internet Explorer [®] 10
Microsoft [®] Windows [®] 7	Internet Explorer [®] 11
Microsoft [®] Windows [®] 7	Internet Explorer [®] 10
Microsoft [®] Windows [®] 7	Internet Explorer [®] 9
Microsoft [®] Windows [®] 7	Internet Explorer [®] 8
Microsoft [®] Windows Vista [®] (SP1/SP2 を含む)	Internet Explorer [®] 7 以上

Web ブラウザのバージョンにより、表示に差異が発生する場合があります。

正常に表示されない場合は、互換性表示設定方法の操作を実施します。

3.1.1.1. Windows[®] 8 / 8.1 の設定

Windows[®] 8 / 8.1 の場合は、以下の手順に従って PC を設定します。

(1) インターネットプロパティの設定

コントロールパネルを表示します。

Windows[®] 8/8.1 を起動し、キーボードの [Windows ロゴ] キー と [X] キーを同時に押し、画面左下に表示されるショートカットメニューから、「コントロールパネル」をクリックします。

「ネットワークとインターネット」を表示します。

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。

「インターネットオプション」を表示します。

[インターネットオプション] をクリックします。

[接続] タブで [ダイアルしない] を選択します。

「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「ダイアルしない」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、[ダイアルしない] をクリックします。

「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。

「ローカルエリアネットワーク (LAN) の設定」を設定します。

次のように設定します。

「自動構成」のチェックを外します。

「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します。チェックがついている場合は、全てのチェックを外します。

「プロキシサーバー」のチェックを外します。

「LAN にプロキシサーバーを使用する」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。

「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

「コントロールパネル」を表示します。

Windows[®] 8 を起動し、キーボードの [Windows ロゴ] キー と [X] キーを同時に押し、画面左下に表示されるショートカットメニューから、「コントロールパネル」をクリックします。

「ネットワークと共有センター」を表示します。

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。

「ネットワーク接続」を表示します。

「アダプターの設定の変更」をクリックします。

「イーサネットの状態」を表示します。

「イーサネット」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。

「イーサネットのプロパティ」を表示します。

「イーサネットの状態」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。

「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」を表示します。

「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4 (TCP/IPv4)] を選択し、[プロパティ] をクリックします。

IP アドレスと DNS を設定します。

「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サーバー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。

DHCP 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サーバーのアドレスを自動的に取得する」を選択してあるか、再度確認する。

「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。

「イーサネットのプロパティ」の [OK] をクリックします。

「イーサネットの状態」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

「イーサネットの状態」を表示します。
「ネットワークの設定」の手順 ~ を行ないます。

「イーサネットの状態」で「詳細」をクリックします。
[詳細] をクリックします。

IPアドレスを確認します。
以下の箇所に設定が反映されたことを確認します。

- ・IPv4 IPアドレス (例：192.168.0.201)
- ・IPv4 サブネットマスク (例：255.255.255.0)
- ・IPv4 デフォルトゲートウェイ (例：192.168.0.200)

これらのアドレスは全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、PC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PCの電源を入れ、手順 からやり直してください。

3.1.1.2. Windows[®] 7 の設定

Windows[®] 7 の場合は、以下の手順に従って PC を設定します。

(1) インターネットプロパティの設定

「コントロールパネル」を表示します。

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。

「ネットワークとインターネット」を表示します。

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。

「インターネットオプション」を表示します。

[インターネットオプション]をクリックします。

[接続] タブで [ダイヤルしない] を選択します。

「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。

「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。

「ローカルエリアネットワーク (LAN) の設定」を設定します。

次のように設定します。

「自動構成」のチェックを外します。

「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します。チェックがついている場合は、全てのチェックを外します。

「プロキシサーバー」のチェックを外します。

「LAN にプロキシサーバーを使用する」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。

「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

「コントロールパネル」を表示します。

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。

「ネットワークと共有センター」を表示します。

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。

「ネットワーク接続」を表示します。

「アダプターの設定の変更」をクリックします。

「ローカルエリア接続の状態」を表示します。

「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。

「ローカルエリア接続のプロパティ」を表示します。

「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。

「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」を表示します。

「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 4 (TCP/IPv4)] を選択し、[プロパティ] をクリックします。

IP アドレスと DNS を設定します。

「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サーバー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。

DHCP 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サーバーのアドレスを自動的に取得する」を選択してあるか、再度確認してください。

「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。

「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。

「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

「ローカルエリア接続の状態」を表示します。
「ネットワークの設定」の手順 ~ を行ないます。

「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] をクリックします。

IPアドレスを確認します。

以下の箇所設定が反映されたことを確認します。

- ・IPv4 IPアドレス (例：192.168.0.201)
- ・IPv4 サブネットマスク (例：255.255.255.0)
- ・IPv4 デフォルトゲートウェイ (例：192.168.0.200)

これらのアドレスは全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、PC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PCの電源を入れ、手順 からやり直してください。

3.1.1.3. Windows Vista[®] の設定

Windows Vista[®] の場合は、以下の手順に従って PC を設定します。

(1) インターネットプロパティの設定

「コントロールパネル」を表示します。

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。

「ネットワークとインターネット」を表示します。

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。

「インターネットオプション」を表示します。

[インターネットオプション]をクリックします。

[接続] タブで [ダイヤルしない] を選択します。

「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。

「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。

「ローカルエリアネットワーク (LAN) の設定」を設定します。

次のように設定します。

「自動構成」のチェックを外します。

「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します。チェックがついている場合は、全てのチェックを外します。

「プロキシサーバー」のチェックを外します。

「LAN にプロキシサーバーを使用する」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。

「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

「コントロールパネル」を表示します。

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。

「ネットワークと共有センター」を表示します。

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。

「ネットワーク接続」を表示します。

「ネットワーク接続の管理」をクリックします。

「ローカルエリア接続の状態」を表示します。

「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。

「ローカルエリア接続のプロパティ」を表示します。

「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。

「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」を表示します。

「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4 (TCP/IPv4)] を選択し、[プロパティ] をクリックします。

IPアドレスとDNSを設定します。

「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サーバー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。

DHCP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サーバーのアドレスを自動的に取得する」を選択してあるか、再度確認してください。

「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。

「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。

「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

「ローカルエリア接続の状態」を表示します。
「ネットワークの設定」の手順 ~ を行ないます。

「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] をクリックします。

IPアドレスを確認します。

以下の箇所に設定が反映されたことを確認します。

・IPv4 IPアドレス (例：192.168.0.201)

・IPv4 サブネットマスク (例：255.255.255.0)

・IPv4 デフォルトゲートウェイ (例：192.168.0.200)

これらのアドレスは全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、PC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PCの電源を入れ、手順 からやり直してください。

3.1.1.4. Web ブラウザの設定

以下の手順に従い、PC の Web ブラウザの設定を行ないます。
正しく表示されない場合がありますので、必ず設定してください。

(1) JavaScript の設定

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。

「セキュリティ」タグをクリックし、[レベルのカスタマイズ]をクリックします。

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

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。

「全般」タグをクリックし、[閲覧の履歴]の [設定]をクリックします。

「Web 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。

表示倍率を100%以外に設定すると、ヘルプが表示しにくくなる場合があります。
ヘルプ等の表示がずれる、表示しにくい等の場合は表示倍率を100%としてください。

3.1.2. 設定画面へのアクセス方法

本装置の設定画面にアクセスするための URL を表 3.1.2-1 に、設定画面アクセス時の認証要求画面を図 3.1.2-1 に示します。

表 3.1.2-1 設定画面アクセス時の入力情報

項目	入力値	備考
URL	http://192.168.0.200/	本装置の LAN 側 IP アドレス初期値

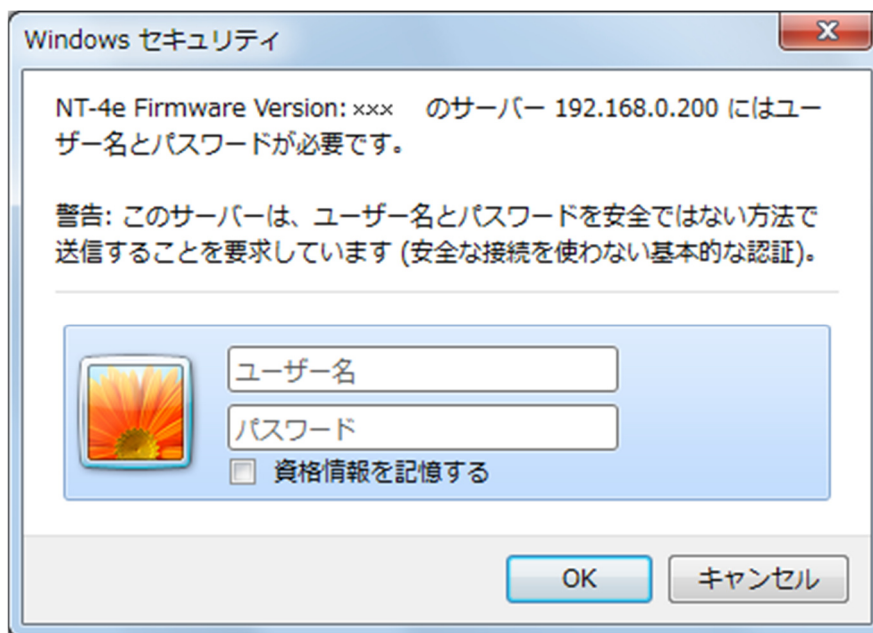


図 3.1.2-1 設定画面アクセス時の認証要求画面

注意事項

ユーザ ID / パスワードは開通時にお渡しする案内文書をご覧ください。

本装置はログアウト操作がないため、終了時は Web ブラウザを終了操作してください。

3.1.3. 設定画面メニュー

本装置の設定画面のメニュー構成を図 3.1.3-1 に、メニュー画面を図 3.1.3-2、図 3.1.3-3 に示します。



図 3.1.3-1 設定画面メニュー一覧 (一部)

ご利用機種が FXS の場合は「FXS タイプ」と表示されます。

— トップページ MENU を選択してください。

ご契約内容に応じて表示が変わります。

サービス状態	
品名	NT-4e(BRIタイプ)
ファームウェアバージョン	2.02
動作モード	カスケード接続親
サービス選択	電話、データ通信を使用(PPPoE接続)

図 3.1.3-2 設定画面のメニュー（最小表示）

ご利用機種が FXS の場合は「FXS タイプ」と表示されます。

— トップページ MENU を選択してください。

ご契約内容に応じて表示が変わります。

サービス状態	
品名	NT-4e(BRIタイプ)
ファームウェアバージョン	2.02
動作モード	カスケード接続親
サービス選択	電話、データ通信を使用(PPPoE接続)

図 3.1.3-3 設定画面のメニュー（展開表示）

実際のメニューでは、1つサブメニューを展開すると、他のサブメニューは閉じられる。
本装置の設定は、メニューから項目を選択して表示された画面上で、設定します。

3.2. 構成情報設定

ここでは主にネットワーク関連の設定方法について記載します。

3.2.1. ネットワーク設定 - LAN 接続設定

LAN 側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 Web ブラウザを起動して、保守メニューを開きます。
- 2 保守メニューから「ネットワーク設定」をクリックします。
- 3 ネットワーク設定メニューから「LAN 接続設定」をクリックします。
- 4 各項目を設定します。
- 5 「設定保存」ボタンをクリックします。
- 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。(3.4.4 装置再起動 参照)

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ります。

その場合は、Web ブラウザを一度終了し、接続する PC の設定を本装置とあわせたあと、Web ブラウザを開きなおしてください。

次ページに設定項目を示します。

・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不可。それぞれ別のサブネットとすること。

・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。	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) IP アドレスの払い出しは、「払い出し開始 IP アドレス」から LAN 側セグメントの最終 IP アドレス-1 (ブロードキャストアドレスを除く) までとなる。	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

3.2.2. ネットワーク設定 - ポート設定

LAN ポートの通信速度、MDI/MDI-X モードについて設定します。

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 ?
LAN1	AUTO	AUTO
LAN2	AUTO	AUTO
LAN3	AUTO	AUTO
LAN4	AUTO	AUTO

【設定手順】

- 1 Web ブラウザを起動して、保守メニューを開きます。
- 2 保守メニューから「ネットワーク設定」をクリックします。
- 3 ネットワーク設定メニューから「ポート設定」をクリックします。
- 4 各項目を設定します。
- 5 「設定保存」ボタンをクリックします。

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ります。

その場合は、Web ブラウザを一度終了し、接続する PC の設定を本装置とあわせたあと、Web ブラウザを開きなおしてください。

次ページに設定項目を示します。

・ポート設定 (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、自動切替えにするかを選択する。MDI-X は LAN1 ~ LAN4 のみ選択可能、MDI は WAN のみ選択可能。</p> <p>[AUTO] MDI/MDI-X を自動切替えに設定する。</p> <p>[MDI-X] MDI-X 固定に設定する。(LAN ポートのみ設定可能)</p> <p>[MDI] MDI 固定に設定する。(WAN ポートのみ設定可能)</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。

3.2.3. 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、タイマー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、接続できなくなることがあります。

SPI設定

トップページ>ネットワーク設定>SP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 Web ブラウザを起動して、保守メニューを開きます。
- 2 保守メニューから「ネットワーク設定」をクリックします。
- 3 ネットワーク設定メニューから「SPI 設定」をクリックします。
- 4 各項目を設定します。
- 5 「設定保存」ボタンをクリックします。

・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）

データ通信中に無通信となり、タイムアウトとなった後は WAN 側からの通信は閉じられる。

3.2.4. 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			
		プロトコル ICMPタイプ	送信元ポート ICMPコード	宛先ポート セキュリティログ保存		
1						編集
2						編集
3						編集
4						編集

【設定手順】

- 1 Web ブラウザを起動して、保守メニューを開きます。
- 2 保守メニューから「ネットワーク設定」をクリックします。
- 3 ネットワーク設定メニューから「セキュリティ設定」をクリックします。

次ページへ続く。

- 「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>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>	フィルタ種別 <small>?</small>		適用セグメント <small>?</small>			
		送信元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>	セキュリティログ保存 <small>?</small>	
1		<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="button" value="編集"/>
2		<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="button" value="編集"/>

- 各項目を設定します。
- 「設定保存」ボタンをクリックします。

次ページに設定項目を示します。

・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受信する。 [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。 全ての送信元 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	*
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、または予約済みの名前を入力する。 全てのプロトコルを対象にする場合は[*]を入力する。 予約済みの名前として、[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、または予約済みの名前を入力する。 全てのポート番号を対象にする場合は[*]を入力する。 予約済みの名前として、以下が用意されている。 [ftp][ftpdata][telnet][smtp][domain][www] [pop3][sunrpc][nntp][ntp][login][route][pptp]	*
宛先ポート （開始ポート - 終了ポート）	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	

設定データ名称	説明	初期値
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。 全ての 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。 全ての 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)

設定がない場合（初期状態）、全てのパケットを受信する。

（本装置のポリシーにて破棄するパケットを除く）

特定のパケットのみを受信したい場合は、以下のように設定します。

受信したいパケットを設定します。

「ルール No.」に任意の値を入力する。（0、999 以外とする）

「フィルタ種別」を [許可] とし、受信したいパケットの条件を入力（ [送信元 IP アドレス] 等を設定）する。

受信したいパケット以外を破棄する設定とする。

で設定したエントリの [ルール No.] より大きな値を設定します。

「フィルタ種別」を [拒否] とする。それ以外は [*] のままとする。

以上により、特定のパケットのみ受信、それ以外は破棄することができる。

3.2.5. 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します。

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 Web ブラウザを起動して、保守メニューを開きます。
- 2 保守メニューから「ネットワーク設定」をクリックします。
- 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」をクリックします。

次ページへ続く。

- 4 「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します。

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>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>	* ~ *		
宛先IPアドレス(開始IP - 終了IP) <small>?</small>	* ~ *		
プロトコル <small>?</small>	*		
送信元ポート(開始ポート - 終了ポート) <small>?</small>	*		
宛先ポート(開始ポート - 終了ポート) <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>	<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>	通信方向 <small>?</small>	フィルタ種別 <small>?</small>	TCPフラグ <small>?</small>	
	(0:無効)	送信元IPアドレス <small>?</small>	宛先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"/>

- 5 各項目を設定します。
 6 「設定保存」ボタンをクリックします。

次ページに設定項目を示します。

・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.	<p>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</p>	0
通信方向	<p>処理したいパケットの方向を選択する。</p> <p>[両方向] 両方向のパケットを処理する。</p> <p>[LAN WAN] LAN から WAN 方向のパケットを処理する。</p> <p>[WAN LAN] WAN から LAN 方向のパケットを処理する。</p>	WAN LAN
フィルタ種別	<p>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。</p> <p>[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。</p> <p>[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。</p>	拒否
TCP フラグ	<p>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。</p> <p>[指定しない] フラグを指定しない。</p> <p>[SYN] コネクション確立要求時のフラグを指定する。</p> <p>[ESTABLISHED] コネクション確立後のフラグを指定する。</p>	指定しない

次ページへ続く。

設定データ名称	説明	初期値
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。 全ての送信元 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。 全ての宛先 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	*
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、または予約済みの名前を入力する。 全てのプロトコルを対象にする場合は[*]を入力する。 予約済みの名前として、[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、または予約済みの名前を入力する。 全てのポート番号を対象にする場合は[*]を入力する。 予約済みの名前として、以下が用意されている。	*
宛先ポート (開始ポート - 終了ポート)	[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	

次ページへ続く。

設定データ名称	説明	初期値
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。 全ての 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。 全ての 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)

設定がない場合（初期状態）、全てのパケットを中継する。

3.2.6. 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します。

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

URLフィルタ設定一覧

番号	比較条件 <input type="text"/>	比較文字 <input type="text"/>	
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 Web ブラウザを起動して、保守メニューを開きます。
- 2 保守メニューから「ネットワーク設定」をクリックします。
- 3 ネットワーク設定メニューから「URL フィルタ設定」をクリックします。

次ページへ続く。

4 「URL フィルタ許可設定」を設定します。

・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 フィルタ方式を選択する。 [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します。

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します。

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>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 <input type="button" value="▼"/>
比較文字(後方一致)	<input type="text"/>

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"/>

7 各項目を設定します。

8 「設定保存」ボタンをクリックします。

次ページに設定項目を示します。

・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>比較条件を選択する。</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.tohknet.co.jp ドメイン www.tohknet.co.jp 比較文字列 jp > 一致 比較文字列 co.jp > 一致 比較文字列 tohknet.co.jp > 一致 比較文字列 hknet.co.jp > 不一致 比較文字列 tohknet.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.tohknet.co.jp ドメイン www.tohknet.co.jp 比較文字列 jp > 一致 比較文字列 co.jp > 一致 比較文字列 tohknet.co.jp > 一致 比較文字列 hknet.co.jp > 一致 比較文字列 tohknet.co > 一致 比較文字列 www > 一致 比較文字列 tohknetco.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。</p> <p>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 Web 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および PC の DNS キャッシュ削除 (Windows® の場合、コマンドプロンプトで「ipconfig /flushdns」を実行) を実施してください。

3.2.7. 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します。

本設定は NAT しない場合、設定内容は無効となります。

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 ? 宛先ポート ?	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

【設定手順】

- 1 Web ブラウザを起動して、保守メニューを開きます。
- 2 保守メニューから「ネットワーク設定」をクリックします。
- 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」をクリックします。

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します。

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>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 <input type="button" value="v"/>
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	宛先ポート	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

- 5 各項目を設定します。
6 「設定保存」ボタンをクリックします。

次ページに設定項目を示します。

・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	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。 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。 [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。 設定範囲：0 ~ 99	なし
宛先 IP アドレス	LAN 側端末の IP アドレスを指定する。 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。	なし
変換対象 プロトコル	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。 [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。 [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。 [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。	TCP
宛先ポート	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、または予約済みの名前を入力する。 予約済みの名前としては、以下が用意されている。 [ftp][ftpdata][telnet][smtp][domain][www] [pop3][sunrpc][nntp][ntp][login][route][pptp] 設定範囲：予約名 / 1 ~ 65535	なし
変換対象ポート	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、または予約済みの名前を入力する。 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。 予約済みの名前としては、以下が用意されている。 [ftp][ftpdata][telnet][smtp][domain][www] [pop3][sunrpc][nntp][ntp][login][route][pptp] 設定範囲：予約名 / 1 ~ 65535	なし

3.2.8. ネットワーク設定 - 静的 NAT 設定

本装置の静的 NAT について設定します。

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 Web ブラウザを起動して、保守メニューを開きます。
- 2 保守メニューから「ネットワーク設定」をクリックします。
- 3 ネットワーク設定メニューから「静的 NAT 設定」をクリックします。

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します。

静的NAT設定

トップページ>ネットワーク設定>静的NAT設定>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 <input type="button" value="v"/>
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 各項目を設定します。
- 6 「設定保存」ボタンをクリックします。

次ページに設定項目を示します。

・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	静的 NAT 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り、最初に合致したエントリで動作する。 [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。 設定範囲：0 ~ 99	なし
宛先 IP アドレス	LAN 側端末の IP アドレスを指定する。 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。	なし
変換対象 プロトコル	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。 [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。 [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。 [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。 [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。 [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	TCP
変換対象ポート (開始ポート - 終了ポート)	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、または予約済みの名前を入力する。 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。 予約済みの名前としては、以下が用意されている。 [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。(範囲指定に予約済みの名前は使用できない) 設定範囲：予約名 / 1 ~ 65535	なし

3.2.9. 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します。

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 Web ブラウザを起動して、保守メニューを開きます。
- 2 保守メニューから「ネットワーク設定」をクリックします。
- 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」をクリックします。
- 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します。

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>エントリ編集

戻る

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 ?	<input type="text"/> / <input type="text"/>
ゲートウェイ ?	<input type="text"/>

設定保存

削除

元に戻す

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"/>

5 各項目を設定します。

6 「設定保存」ボタンをクリックします。

・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

3.2.10. ネットワーク設定 - 高度な設定

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 ?	<input checked="" type="checkbox"/> 使用する
PING応答機能	
データ通信用セグメント応答 ?	<input checked="" type="radio"/> 応答する <input type="radio"/> 応答しない <input type="radio"/> 指定したIPアドレスのみ応答する
IPアドレス1 ?	<input type="text"/>
IPアドレス2 ?	<input type="text"/>
IPアドレス3 ?	<input type="text"/>
IPアドレス4 ?	<input type="text"/>
IPアドレス5 ?	<input type="text"/>
外部へのサーバ公開設定	
外部へのサーバ公開 ?	<input checked="" type="radio"/> 公開しない <input type="radio"/> 仮想DMZで公開する <input type="radio"/> 簡易的に公開する
仮想DMZのIPアドレス空間/マスク長 ?	<input type="text"/> / <input type="text"/>
DMZをポート/VLANで区分けする ?	区分けしない ▼
公開するホストのIPアドレス ?	<input type="text"/>
<input type="button" value="設定保存"/> <input type="button" value="元に戻す"/>	

【設定手順】

- 1 Web ブラウザを起動して、保守メニューを開きます。
- 2 保守メニューから「ネットワーク設定」をクリックします。
- 3 ネットワーク設定メニューから「高度な設定」をクリックします。
- 4 各項目を設定します。
- 5 「設定保存」ボタンをクリックします。

・UPnP 設定

設定データ名称	説明	初期値
UPnP 機能	<p>UPnP 機能の使用有無を選択する。 NAT しない場合、本設定の内容によらず [使用しない] として動作する。</p> <p>[使用する] (チェックあり) UPnP が必須のサービスやアプリケーションを利用できる。</p> <p>[使用しない] (チェックなし) UPnP が必須のサービスやアプリケーションを利用できない。</p>	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
データ通信用セグメント応答	<p>データ通信用セグメントへの PING 応答有無を選択する。</p> <p>[応答する] 外部からの PING 要求に対し、応答を行う。</p> <p>[応答しない] 外部からの PING 要求に対し、応答を行わない。</p> <p>[指定した IP アドレスのみ応答する] 「データ通信用セグメント応答 IP アドレス」に設定されている IP アドレスからの PING 要求に対してのみ、応答を行う。</p>	応答する
データ通信用セグメント応答 IP アドレス (1 ~ 5)	<p>PING 応答を許可する、端末の IP アドレスを設定する。</p> <p>「データ通信用セグメント応答」の設定が、[指定した IP アドレスのみ応答する] の場合のみ、入力可能となる。</p>	なし

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	<p>外部へのサーバ公開方式を選択する。</p> <p>NAT しない場合、本設定の内容によらず [公開しない] として動作する。</p> <p>[公開しない] 外部へサーバ公開しない。</p> <p>[仮想 DMZ で公開する] 仮想 DMZ セグメントを設定し公開する。</p> <p>[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。</p>	公開しない
仮想 DMZ の IP アドレス空間	<p>仮想 DMZ の IP アドレス空間を設定する。</p> <p>他セグメントのサブネットと重複は不可。</p> <p>本装置は DNS サーバとして動作できない。</p> <p>「外部へのサーバ公開」の設定が [仮想 DMZ で公開する] の場合のみ、入力可能となる。</p>	なし
マスク長	<p>仮想 DMZ の IP アドレス空間のマスク長を設定する。</p> <p>「外部へのサーバ公開」の設定が [仮想 DMZ で公開する] の場合のみ、入力可能となる。</p> <p>設定範囲：24 ~ 30</p>	なし
DMZ をポート VLAN で区別する	<p>DMZ をポート VLAN で区別する/しないを選択する。</p> <p>「外部へのサーバ公開」の設定が [仮想 DMZ で公開する] の場合のみ、入力可能となる。</p> <p>[区別しない] DMZ をポート VLAN で区別しない。</p> <p>[区別する (LAN1 ~ 4)] DMZ を指定した LAN ポートで区別する。</p>	区別しない
公開するホストの IP アドレス	<p>公開するサーバの IP アドレスを設定する。</p> <p>「外部へのサーバ公開」の設定が [簡易的に公開する] の場合のみ、入力可能となる。</p>	なし

3.3. 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。

3.3.1. 装置状態表示

本装置の各種情報を表示します。

以下に、親機での表示例を示します。

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	xxxxxx
現在時刻	2014.01.01.12:34

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	-	001F678D699E
LAN1	-	001F678D695E
LAN2	1G FULL	
LAN3	-	
LAN4	-	

データ通信用セグメントIPアドレス

IPアドレス	3.0.0.2
--------	---------

PPPoE接続状態

電話	-
データ通信	-

ランプ状態

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

通常は表示なし

機種が FXS の場合

ランプ状態

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

以下に、子機での表示例を示します。

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	XXXXXXXX
現在時刻	2014.1.1.12:34

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	-	00:11:22:33:44:55
LAN1	100M FULL	00:66:77:88:99:11
LAN2	100M FULL	
LAN3	100M FULL	
LAN4	100M FULL	

ランプ状態

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

機種が FXS の場合

ランプ状態

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

【表示手順】

- 1 Web ブラウザを起動して、保守メニューを開きます。
- 2 保守メニューから「装置状態表示」をクリックします。

・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を表示する。
現在時刻	装置内時計の現在時刻を表示する。(自動的に更新しない)

・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を表示する。
MAC アドレス	各ポートの MAC アドレスを表示する。

・データ通信用セグメント IP アドレス


表示項目	説明
IP アドレス	データ通信用セグメントの IP アドレスを表示する。

・ランプ状態

表示項目	説明
ランプ状態	各ランプの状態を表示する。 : 点灯 : 消灯 * : 点滅

3.3.2. 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 						
Nb.	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	2014/09/15 01:11:26	192.168.100.2	192.168.1.2	TCP	192.168.100.200	123

【表示手順】

- 1 Web ブラウザを起動して、保守メニューを開きます。
- 2 保守メニューから「UPnP 状態表示」をクリックします。

・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。

3.3.3. LAN 側自動払い出し状況

LAN 側自動払い出し状況を表示します。

LAN側自動払い出し状況

トップページ>LAN側自動払い出し状況

払い出し状況 ⓘ

現在の時刻	2014/09/20 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	2014/12/20 12:00:00
192.168.100.11/24	00:0B:A2:E3:2D:5A	2014/12/20 11:00:00

【表示手順】

- 1 Web ブラウザを起動して、保守メニューを開きます。
- 2 保守メニューから「LAN 側自動払い出し状況」をクリックします。

・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。

3.3.4. ログ表示

各種ログの表示、及びログのクリアを実施する。

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 Web ブラウザを起動して、保守メニューを開きます。
- 2 保守メニューから「ログ表示」をクリックします。

・ログ情報の選択

表示項目	説明
ログ情報の種類	表示、またはクリアするログを選択し、各ボタンで実施する。 [セキュリティログ] 本装置のセキュリティに関するログ。 [全て（クリアのみ有効）] 全ログをクリアする場合に選択する。

3.3.4.1. 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	2014/01/01 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 Web ブラウザを起動して、保守メニューを開きます。
- 2 保守メニューから「ログ表示」をクリックします。
- 3 ログ情報の種類から「セキュリティログ」を選択します。
- 4 [ログ情報の表示] ボタンをクリックします。

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「-」で表示されます。
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「+」で表示されます。
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ます。
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ます。

・セキュリティログ

表示項目	説明
受信日時	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。同一受信日時で大量に採取される場合は、WAN 側設備のセキュリティ状況を確認する。 (廃棄 [NAT] / 廃棄 [SPI] / 廃棄 [パケットフィルタ])

3.3.5. 統計情報

各種統計情報の表示、及び統計情報のクリアを実施します。



【表示手順】

- 1 Web ブラウザを起動して、保守メニューを開きます。
- 2 保守メニューから「統計情報」をクリックします。

・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。 (電話を使用する場合のみ表示) [全て(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、WAN、LAN の統計情報は 0 クリアし再カウントします。
端末ポートの統計情報は、最大値を保持し 0 クリアしません。

3.3.5.1. 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統計情報

項目	LAN1	LAN2	LAN3	LAN4
受信ユニキャストパケット数	4294967295	4294967295	4294967295	4294967295
受信ブロードキャストパケット数	4294967295	4294967295	4294967295	4294967295
受信マルチキャストパケット数	4294967295	4294967295	4294967295	4294967295
送信ユニキャストパケット数	4294967295	4294967295	4294967295	4294967295
送信ブロードキャストパケット数	4294967295	4294967295	4294967295	4294967295
送信マルチキャストパケット数	4294967295	4294967295	4294967295	4294967295
送信エラーパケット数	4294967295	4294967295	4294967295	4294967295
送信破棄パケット数	4294967295	4294967295	4294967295	4294967295
コリジョン発生回数	4294967295	4294967295	4294967295	4294967295
レートコリジョン発生回数	4294967295	4294967295	4294967295	4294967295
受信異常発生回数	4294967295	4294967295	4294967295	4294967295
受信アライメント異常発生回数	4294967295	4294967295	4294967295	4294967295
受信FCSエラー発生回数	4294967295	4294967295	4294967295	4294967295
受信パラメータ異常発生回数	4294967295	4294967295	4294967295	4294967295
受信フラグメント発生回数	4294967295	4294967295	4294967295	4294967295
受信破棄パケット数	4294967295	4294967295	4294967295	4294967295
不正キャリアセンス検出回数	0	0	0	0

【表示手順】

- 1 Web ブラウザを起動して、保守メニューを開きます。
- 2 保守メニューから「統計情報」をクリックします。
- 3 統計情報の種類から「LAN」を選択します。
- 4 [統計情報の表示] ボタンをクリックします。

注意事項

LAN 統計情報は、再起動や電源を切ると消去されます。

・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。	
送信破棄パケット数	送信エラー等で破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。	
受信破棄パケット数	受信エラー等で破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。	

3.3.5.2. 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統計情報

受信ユニキャストパケット数	4294967295
受信ブロードキャストパケット数	4294967295
受信マルチキャストパケット数	4294967295
送信ユニキャストパケット数	4294967295
送信ブロードキャストパケット数	4294967295
送信マルチキャストパケット数	4294967295
送信エラーパケット数	4294967295
送信破棄パケット数	4294967295
コリジョン発生回数	4294967295
レートコリジョン発生回数	4294967295
受信異常発生回数	4294967295
受信アライメント異常発生回数	4294967295
受信FCSエラー発生回数	4294967295
受信パラメータ異常発生回数	4294967295
受信フラグメント発生回数	4294967295
受信破棄パケット数	4294967295
不正キャリアセンス検出回数	0

【表示手順】

- 1 Web ブラウザを起動して、保守メニューを開きます。
- 2 保守メニューから「統計情報」をクリックします。
- 3 統計情報の種類から「WAN」を選択します。
- 4 [統計情報の表示] ボタンをクリックします。

注意事項

WAN 統計情報は、再起動や電源を切ると消去されます。

・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。	
送信破棄パケット数	送信エラー等で破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。	
受信破棄パケット数	受信エラー等で破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。	

3.3.5.3. 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

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	999999999	999999999	999999999	999999999
	RTP受信パケット数	999999999	999999999	999999999	999999999
	RTP送信廃棄パケット数	999999999	999999999	999999999	999999999
	RTP受信廃棄パケット数	999999999	999999999	999999999	999999999
	RTCP送信パケット数	999999999	999999999	999999999	999999999
	RTCP受信パケット数	999999999	999999999	999999999	999999999
	RTCP送信廃棄パケット数	999999999	999999999	999999999	999999999
	RTCP受信廃棄パケット数	999999999	999999999	999999999	999999999
受信ゆらぎ	ゆらぎ最大時間(ms)	200	200	180	160
	ゆらぎ最小時間(ms)	20	25	30	20
	ゆらぎ時間[20ms]パケット数	44	44	44	44
	ゆらぎ時間[40ms]パケット数	44	44	44	44
	ゆらぎ時間[60ms]パケット数	44	44	44	44
	ゆらぎ時間[80ms]パケット数	44	44	44	44
	ゆらぎ時間[100ms]パケット数	44	44	44	44
	ゆらぎ時間[120ms]パケット数	44	44	44	44
	ゆらぎ時間[140ms]パケット数	44	44	44	44
	ゆらぎ時間[160ms]パケット数	44	44	44	44
	ゆらぎ時間[180ms]パケット数	44	44	44	44
	ゆらぎ時間[200ms]パケット数	44	44	44	44
	ゆらぎ時間(その他)パケット数	0	1	44	44

【表示手順】

- 1 Web ブラウザを起動して、保守メニューを開きます。
- 2 保守メニューから「統計情報」をクリックします。
- 3 統計情報の種類から「端末ポート」を選択します。
- 4 [統計情報の表示] ボタンをクリックします。

注意事項

端末ポート統計情報は、電源を切ると消去されます。

・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 送信廃棄パケット数	RTP 送信廃棄パケット数を表示する。	
RTP 受信廃棄パケット数	RTP 受信廃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 送信廃棄パケット数	RTCP 送信廃棄パケット数を表示する。	
RTCP 受信廃棄パケット数	RTCP 受信廃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。	

3.4. メンテナンス

本装置の保守用機能について示します。

3.4.1. 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 Web ブラウザを起動して、保守メニューを開きます。
- 2 保守メニューから「疎通確認 (PING)」をクリックします。
- 3 「宛先 IP アドレス」を設定します。
- 4 「送信元セグメント」を選択します。
- 5 「実行」ボタンをクリックします。
- 6 数秒後に画面が切替わり、結果表示領域に疎通確認結果が表示されます。
結果に「0% packet loss」という表示があれば、疎通確認成功となります。
この表示がない場合、疎通確認は失敗しています。

・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。



3.4.2. メンテナンス - ログインパスワード変更

本装置の保守画面へ Web 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]

※ 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 Web ブラウザを起動して、保守メニューを開きます。
- 2 保守メニューから「メンテナンス」をクリックします。
- 3 メンテナンスメニューから「ログインパスワード変更」をクリックします。
- 4 変更するアカウントの「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します。
- 5 「設定保存」ボタンをクリックして、設定した内容を保存します。

・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（「-」「/」「_」）

3.4.3. 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	
構成情報ファイルをPCIに保存	<input type="button" value="保存"/>
装置設定の復元	
復元する構成情報ファイルを選択	<input type="text"/> <input data-bbox="1166 752 1251 779" type="button" value="参照..."/>
選択中の構成情報ファイルをもとに復元	<input type="button" value="復元"/>

【装置設定の保存手順】

- 1 Web ブラウザを起動して、保守メニューを開きます。
- 2 保守メニューから「メンテナンス」をクリックします。
- 3 メンテナンスメニューから「装置設定の保存 / 復元」をクリックします。
- 4 「構成情報ファイルを PC に保存」の「保存」ボタンをクリックします。
- 5 ダウンロードの確認ダイアログが表示されたら「保存」ボタンをクリックします。
- 6 保存するディレクトリを選択し、「保存」ボタンをクリックします。

【装置設定の復元手順】

- 1 Web ブラウザを起動して、保守メニューを開きます。
- 2 保守メニューから「メンテナンス」をクリックします。
- 3 メンテナンスメニューから「装置設定の保存 / 復元」をクリックします。
- 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、ファイルを選択します。
- 5 「復元」ボタンをクリックします。
- 6 メッセージが表示されたら、「OK」ボタンをクリックします。
- 7 ファイルが正常な場合、自動的に再起動されます。

注意事項

通話中に装置設定の復元を実施すると、通話が切断されます。

パスワードは復元されません。

カスケード接続（子）にて、装置設定の復元を実施した場合、カスケード接続（子）で設定可能な構成情報のみ復元されます。

3.4.4. 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、装置を再起動します。

装置の再起動 ?

装置の再起動

【再起動手順】

- 1 Web ブラウザを起動して、保守メニューを開きます。
- 2 保守メニューから「メンテナンス」をクリックします。
- 3 メンテナンスメニューから「装置再起動」をクリックします。
- 4 「実行」ボタンをクリックします。

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でください。

通話中に再起動を実施すると、通話が切断されます。

再起動が完了するまで、約 1 分 30 秒かかります。

データ通信接続を行っている場合は、接続が切断されます。

再起動実施で LAN リンク断が 2 回発生します。(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。)

3.5. 電話の設定

ここでは一部設定のみ取り扱っております。

3.5.1. 着信ポート選択

着信した電話番号毎に、接続する電話ポートを選択します。

【手順】

- 1 本装置へログイン後、以下の階層メニューを選択します。

メニュー

電話番号設定

着信ポート分け

- 2 以下のように、各設定項目に電話番号毎の着信方式および着信ポートを設定します。

(着信ポートは、FXS の場合 4 ポート、BRI の場合 2 ポートまで)

【画面イメージ図】

着信設定

番号	設定項目
1	電話番号: 022xxxyyyy
	着信方式: シーケンシャル(順次サーチ)
	着信ポート選択: <input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4
2	電話番号: 022xxzzzz
	着信方式: ラウンドロビン(巡回)
	着信ポート選択: <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4
:	親

【設定内容例】

着信電話番号	着信方式	着信ポート選択			
		ポート1	ポート2	ポート2	ポート2
022xxxyyyy	順次	レ	レ		
022xxzzzz	ラウンドロビン			レ	レ

補足事項

項目に入力する電話番号が複数存在する場合、後ろの番号を省略することも可能です。

例) 012-345-1000 ~ 012-345-1099 までを同じ着信方式および着信ポートで設定させる場合

【設定内容例】

着信電話番号	着信方式	着信ポート選択			
		ポート1	ポート2	ポート2	ポート2
0123451000	順次	レ	レ		
0123451001	順次	レ	レ		
⋮	⋮	⋮	⋮		
0123451099	順次	レ	レ		

【画面イメージ図】

着信設定 "0123451"まで共通

番号	設定項目
1	電話番号: <input type="text" value="0123451"/>
	着信方式: <input type="text" value="シーケンシャル(順次サーチ)"/>
	着信ポート選択: <input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4
2	電話番号: <input type="text"/>
	着信方式: <input type="text"/>
	着信ポート選択: <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4
⋮	⋮

3.5.2. ユーザ個別情報

電話番号を利用可能にするため、ご契約代表番号を設定します。

【手順】

- 1 本装置へログイン後、以下の階層メニューを選択します。

メニュー

電話番号設定

ユーザ個別情報

- 2 以下のように、各設定項目にご契約代表番号を設定します。

設定内容について

- ・必ずご契約代表番号を設定します。
- ・契約代表番号のルート番号は"0"にします。
- ・ルート番号"0"の「メイン情報」および「REGISTER送信」にはチェックを入れます。

【設定内容例】

ルート番号 (0-99)	電話番号
0	022xxxxxxx

契約代表番号

【画面イメージ図】

ユーザ個別情報

番号	使用する	設定項目
1	<input checked="" type="checkbox"/>	ルート <input type="text" value="0"/> メイン情報 <input checked="" type="checkbox"/> 有効 REGISTER送信 <input checked="" type="checkbox"/> 送信する <small>必ずチェックを入れること</small>
		ユーザ名 <input type="text" value="022xxxxxxx"/>
2	<input type="checkbox"/>	ルート <input type="text"/> メイン情報 <input type="checkbox"/> 有効 REGISTER送信 <input type="checkbox"/> 送信する
		ユーザ名 <input type="text"/>
:	:	:

ご利用機種が FXS タイプの場合、発信時の捕捉ポート毎に発信電話番号を設定できます。ここでは使用する発信番号の数だけ設定します。

◆設定内容について

- 発信電話番号を最大4つまで設定できます。
- 契約代表番号のルート番号は”0”にし、その他の発信電話番号のルート番号は自由に設定できます。(1~99)
- ルート番号は、「端末インタフェース設定」画面で利用します。
- 全ルート番号の「メイン情報」にチェックを入れます。
- ルート番号”0”の「REGISTER送信」にはチェックを入れます。

【設定内容例】

ルート番号 (0~99)	電話番号
0	0123451000
1	0123451010

契約代表番号
(発信電話番号①)
発信電話番号②

【画面イメージ図】

ユーザ個別情報

番号	使用する	設定項目
1	<input checked="" type="checkbox"/>	ルート <input type="text" value="0"/> メイン情報 <input checked="" type="checkbox"/> 有効 REGISTER送信 <input checked="" type="checkbox"/> 送信する <small>必ずチェックを入れること</small>
		ユーザ名 <input type="text" value="0123451000"/>
		...
2	<input checked="" type="checkbox"/>	ルート <input type="text" value="1"/> メイン情報 <input checked="" type="checkbox"/> 有効 REGISTER送信 <input type="checkbox"/> 送信する <small>必ずチェックを入れること</small>
		ユーザ名 <input type="text" value="0123451010"/>
		...

3.5.3. 端末インタフェース設定

電話インタフェースに関する設定を、ポート毎に設定します。

FXS と BRI では、項目内容が異なります。

子機のポートを設定する場合は、親機からログインして設定して下さい。

【手順】

- 1 本装置へログイン後、以下の階層メニューを選択します。

メニュー

端末インタフェース設定

FXS (or BRI)

- 2 以下のように、各設定項目にポート毎の構成情報を設定します。

- 設定内容について
- ・電話インタフェースに関する設定を、ポート毎に設定します。
 - ・ルート番号は「ユーザ個別情報」と関連します。
- (FXSの場合、対象ポートからの発信時に、ルート番号に対応する電話番号が発信電話番号として利用されます。)

【画面イメージ図】

ポート設定 (FXS)

ポート番号	ポート1	ポート2	ポート3	ポート4	
ポート	<input checked="" type="checkbox"/> 使用する	<input checked="" type="checkbox"/> 使用する	<input type="checkbox"/> 使用する	<input type="checkbox"/> 使用する	使用するポートのみにチェックを入れる
：	：	：	：	：	
ルート	<input type="text" value="0"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	「ユーザ個別情報」で設定したルート番号を設定する。
：	：	：	：	：	
ナンバーディスプレイ	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない	ポート毎にナンバーディスプレイの使用を選択する
：	：	：	：	：	
ダイヤルイン方式	<input type="radio"/> 使用しない <input type="radio"/> PB <input checked="" type="radio"/> モデム	<input checked="" type="radio"/> 使用しない <input type="radio"/> PB <input type="radio"/> モデム	<input checked="" type="radio"/> 使用しない <input type="radio"/> PB <input type="radio"/> モデム	<input checked="" type="radio"/> 使用しない <input type="radio"/> PB <input type="radio"/> モデム	ポート毎にダイヤルイン方式を選択する

【画面イメージ図】

ポート設定 (BRI)

ポート番号	ポート1	ポート2	ポート3	ポート4	
ポート	<input checked="" type="checkbox"/> 使用する	<input checked="" type="checkbox"/> 使用する	<input type="checkbox"/> 使用する	<input type="checkbox"/> 使用する	使用するポートのみにチェックを入れる
：	：	：	：	：	
レイヤ1接続状態とレイヤ2起動方式	<input type="text" value="ポイント-マルチポイント/常時接続"/>	<input type="text" value="ポイント-マルチポイント/常時接続"/>	<input type="text" value="ポイント-マルチポイント/常時接続"/>	<input type="text" value="ポイント-マルチポイント/常時接続"/>	接続形態に合わせて選択する
：	：	：	：	：	
ルート	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	「ユーザ個別情報」で設定したルート番号を設定する。
：	：	：	：	：	
ナンバーディスプレイ	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない	ポート毎にナンバーディスプレイの使用を選択する
：	：	：	：	：	

4. 機器仕様

4.1. 方式諸元

4.1.1. ハードウェア諸元

項目		仕様
WAN ポート	物理インタフェース	8 ピンモジュラージャック (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	物理インタフェース	8 ピンモジュラージャック (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	物理インタフェース	6 ピンモジュラージャック (RJ-11)
	ポート数	4 ポート
	給電電圧	約-48V (無負荷時)
BRI (CLK) ポート	物理インタフェース	8 ピンモジュラージャック (RJ-45)
	ポート数	2 ポート (1 ポート)
	規格	TTC 標準 JT-I430 準拠
	クロック精度	自走時: ±50 ppm 従属時: 外部供給クロック精度による 従属時の追従性能は自走クロック精度
VoIP	音声符号化則	ITU-T G.711 (μLaw) ITU-T G.729
	DTMF	みなし音声 (透過) / INFO メソッド
	エコーキャンセラ	ITU-T G.168 (64ms)
	音声レベル	10 ~ 0 ~ -18dB (2 dB 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 回線状態表示
	WAN SPEED ランプ	WAN 回線速度表示
	PPP ランプ	PPPoE 接続状態表示
	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
	LAN SPD ランプ	LAN ポート回線速度表示
LAN ACT ランプ	LAN ポート回線状態表示	
操作部	e ボタン	ランプ消灯モード復旧ボタン
	INIT ボタン	初期化ボタン
	スライドスイッチ	BRI : CLK ポート終端抵抗オン/オフスイッチ
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 (電源アダプタ含む)
質量	約 1kg (電源アダプタ含まず)
電磁妨害波規格 VCCI	VCCI クラス A

4.1.2. 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	
	同時通話数	8ch (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	
	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 (電話・データ通信)、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: 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 (データ通信、応答 IP アドレス指定 5 件)	
設定・保守機能	設定方法	Web ブラウザによる設定・保守 (HTTP)	
	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	セキュリティログ: 最大 100 件	
	統計機能	LAN 統計情報、WAN 統計情報、端末ポート統計情報、	

4.2. サービス機能

ネットワーク接続に関するサービス機能の詳細を示します。

4.2.1. 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。
IPv6 については未サポートのため対象外となる。
なお、本装置が生成するパケットの TTL は全て 64 となる。

【備考・注意事項】

高速フォワーディング対象は以下の条件を全てが満足した場合となる。

- ・プロトコル種別：TCP/UDP パケット
- ・フラグメントパケット

フレームサイズ：1700byte 以下

フラグメント分割数：3 分割以下

フレームサイズはフラグメントパケットの受信合計フレームサイズを示し、Ethernet ヘッダ、PPPoE ヘッダを含み、フラグメント時の IP ヘッダ等の重複分は含まない。

高速フォワーディング対象のパケットでも以下の場合、スループットが低下する。

ショートパケットのフォワーディング（512byte 以下）

フラグメントパケット受信により、リアセンブルを行う場合

フラグメントパケット受信により、リアセンブルを行わずに出力する場合

受信パケットをフラグメントして送出する場合

フラグメントパケット受信時にロス、揺らぎ、順序逆転が発生した場合

PPPoE セッション、VLAN を使用し、PPPoE ヘッダ、VLAN タグを付与する場合

、 、 は高速転送になるとスループット低下が大きくなる。順序逆転が発生した場合、順序どおりに送出するが、該当パケットは高速フォワーディングの対象外となる。

また、 でフラグメントパケットを受信し組み立てて、リアセンブルを行わない場合も高速転送でスループットが低下する。

高速フォワーディング対象外となった場合、ソフトフォワーディングとなり処理パケット量が 5000pps に制限されるため、大幅なスループット低下となる。

5000pps は音声用 RTP/RTCP パケットも含む。

WAN/LAN ポートではジャンボフレームをサポートしていない。通常のイーサネットでのフレームサイズ以上の送受信は保証しない。

同時通信数は 5 0 0 0 で制限される。（コネクション数による制限となり、カスケード子機の通話数も含まれる）

フラグメントパケットを受信した場合、高速フォワーディング対象パケットはリアセンブルを行い、送信側インタフェースの MTU にサイズを合わせて送出する。

4.2.2. 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。保守端末などを 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。

払い出す情報を以下に示す。

- ・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 側 (保守) セグメントの IP アドレスとなる。

【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

払い出す IP アドレスは設定した範囲を超えた場合、ラップして最初のアドレスに戻って払い出しは行わない。(払い出す IP アドレス : 192.168.0.201、マスク長 24 で IP アドレスを払い出す場合、192.168.0.254 まで払い出しで終了し、192.168.0.1 に戻って払い出しは行わない。)

4.2.3. ポート - 通信速度選択機能

【機能説明】

各 LAN ポートの通信速度、伝送モードを設定する機能。

オートネゴシエーション (AUTO、AUTO(100M MAX)の設定)、または通信速度、通信モードの固定設定が選択可能となっている。

設定項目は以下となる。

- ・AUTO : 通信速度、伝送モードを自動で設定する。最大速度は 1Gbit/s となる。
- ・AUTO (100M MAX)
 - : 通信速度、伝送モードを自動で設定する。最大速度は 100Mbit/s となる。
- ・100M FULL : 通信速度は 100Mbit/s、伝送モードは全二重で動作する。
- ・100M HALF : 通信速度は 100Mbit/s、伝送モードは半二重で動作する。
- ・10M FULL : 通信速度は 10Mbit/s、伝送モードは全二重で動作する。
- ・10M HALF : 通信速度は 10Mbit/s、伝送モードは半二重で動作する。

1Gbit/s で通信する場合には AUTO 設定すること。1Gbit/s の固定設定はない。

【備考・注意事項】

AUTO、AUTO (100M MAX) を選択した場合、接続する相手もオートネゴシエーションで動作させること。固定設定で動作させた場合、伝送モードが合わずに通信エラーが発生する場合がある。

また、通信速度、通信モードの固定設定で使用する場合、接続する相手も同じ通信速度、通信モードとすること。合っていない場合には通信エラーが発生する場合がある。

なお、オートネゴシエーション確定でリンクアップであるため、オートネゴシエーション中の一時的なケーブル接続はリンクアップと判断しない。

LAN リンクアップ状態で装置再起動を行った場合、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。)

4.2.4. ポート - MDI/MDI-X 選択機能

【機能説明】

各 LAN ポートの MDI/MDI-X を選択する機能。

設定項目は以下となる。

- ・AUTO : ポートの MDI/MDI-X を自動で切替える。
- ・MDI-X : ポートは MDI-X で固定して動作する。(LAN 側ポートのみ)
- ・MDI : ポートは MDI で固定して動作する。(WAN 側ポートのみ)

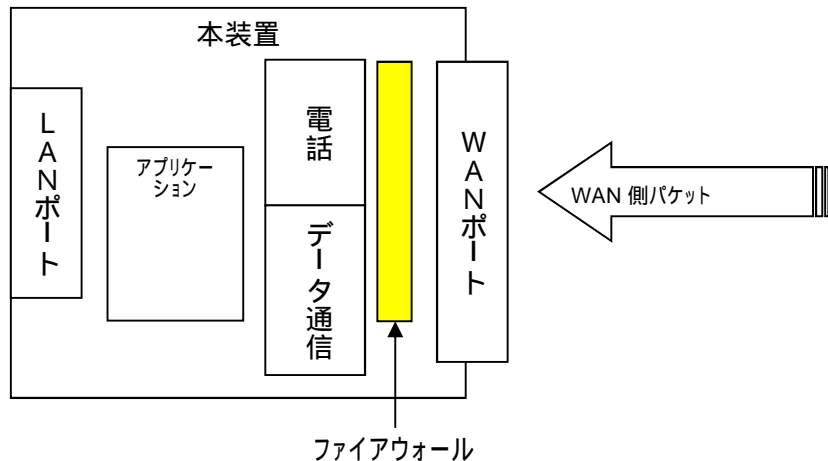
【備考・注意事項】

MDI-X 固定で動作させる場合、接続する相手も MDI-X 固定であった場合には LAN ケーブルはクロスケーブルを使用すること。また、接続する相手が MDI 固定であった場合には LAN ケーブルはストレートケーブルを使用すること。(AUTO 設定の場合、ケーブルの種類は問わない。)

4.2.5. セキュリティ - ファイアウォール機能

【機能説明】

本装置宛に受信するパケットの受信許可/拒否を設定することにより、セキュリティの向上を図る機能。装置の基本状態はパケット全てを受け入れない（拒否）動作となっているため、セキュリティを調整したい場合などに使用する。



ファイアウォール設定として、96個の設定が可能であり、設定項目として適用セグメント、送信元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。

【備考・注意事項】

本機能は本装置宛のパケットに対応する。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についてはパケットフィルタ機能によりセキュリティの向上を行う。

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全てに対しての設定となる。

4.2.6. 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、シーケンス異常等) 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なかった場合、または通信終了 (TCP のセッション終了等) 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】

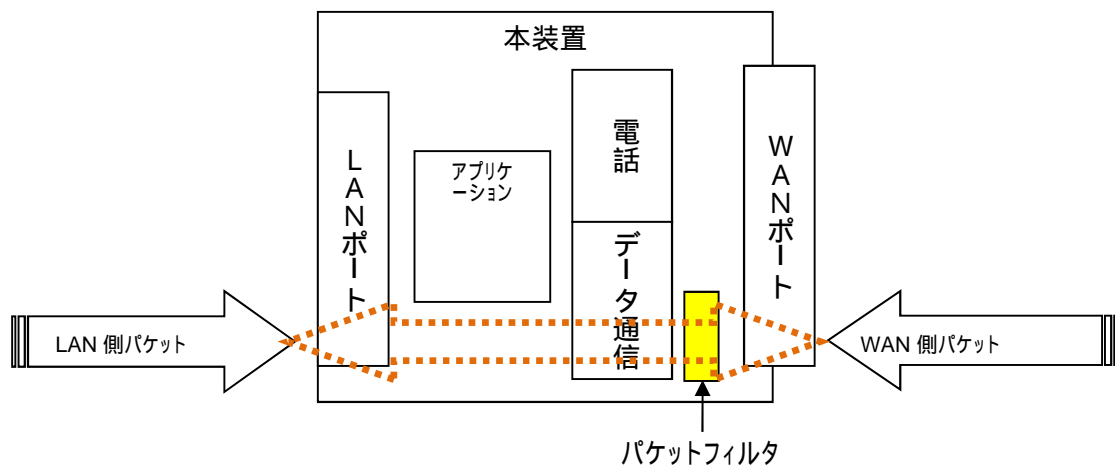
SPI 機能は本装置宛のパケット、本装置の配下にある端末へフォワーディングするパケットの両方に適用される。データ通信のパケットが該当する。

4.2.7. 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、ポート番号等の条件によりフィルタすることにより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。但し、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。

【備考・注意事項】

本設定はデータ通信にのみ適用する。

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 全てに対しての設定となる。

4.2.8. 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データ通信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・キーワードを許可する「許可リスト設定」と、逆に登録されているドメイン名・キーワードを拒否する「拒否リスト設定」の選択が可能である。

なお、拒否・許可選択は全ての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。

【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。

4.2.9. セキュリティ - PING 応答選択機能

【機能説明】

WAN側から本装置のWAN側アドレスに対する PING (ICMP Echo Request) に対して応答 (ICMP Echo Reply) を返すかどうかを設定します。LAN 側からの PING に対しては意味を持たない。

設定は、電話用セグメント、データ通信用セグメントで別々に設定が可能である。

「指定した IP アドレスのみ応答する」設定も可能であり、この場合 PING 送信元 IP アドレスに設定した IP アドレスからの PING は応答し、設定されていない IP アドレスからの PING は応答を返さない。

【備考・注意事項】

データ通信用セグメントで静的 NAT/静的 IP マスカレード設定、外部へのサーバ公開設定により ICMP を LAN 側端末に透過する設定が行われた場合、本装置での終端は行われず、LAN 側端末へ透過する。

データ通信用セグメント設定で、「NAT 設定」を [NAT しない] に設定した場合、WAN 側からの PING に対して、データ通信用セグメントの IP アドレス宛に加えて、LAN 側セグメントの本装置 IP アドレス宛にも応答する。

4.2.10. ルーティング - 静的 IP マスカレード機能

【機能説明】

WAN 側からの本装置のデータ通信用アドレス宛の packets の「プロトコル」/「宛先ポート」と、静的 IP マスカレード設定に設定されている「変換対象プロトコル」/「変換対象ポート」の情報が一致する場合に、packet の宛先を変換する。

変換する情報は、packet の宛先 IP アドレスと、宛先ポート番号であり、それぞれ静的 IP マスカレード設定に設定されている「宛先 IP アドレス」と「宛先ポート」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ことができる。もしくは WAN 側からの特定ポートの通信を指定した PC などに送受信することができる。

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 PC 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。

【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。

NAT しない場合、本機能は無効となる。

4.2.11. ルーティング - 静的 NAT 機能

【機能説明】

WAN 側からの本装置のデータ通信アドレス宛のパケットの「プロトコル」/「宛先ポート」と、静的 NAT 設定に設定されている「変換対象プロトコル」/「変換対象ポート」の情報が一致する場合に、パケットの宛先を変換する。

変換する情報は、パケットの宛先 IP アドレスであり、静的 NAT 設定に設定されている「宛先 IP 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 側の指定した PC などに送受信することができる。

静的 NAT は 6 4 個の設定が可能である。

【備考・注意事項】

静的 IP マスカレード機能は宛先 IP アドレス、宛先ポート番号の変換を行うが、静的 NAT 機能の場合は宛先 IP アドレスのみ変換を行う。

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。

NAT しない場合、本機能は無効となる。

4.2.12. 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 PC などをデータ通信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 マスカレード設定が適用する。

【備考・注意事項】

本機能を使用するための設定（IP アドレス等）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に動的 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）

NAT しない場合、本機能は無効となる。

4.2.13. ルーティング - ポートフォワーディング機能

【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】

NAT しない場合、本機能は無効となる。

4.2.14. 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等に使用する。

LAN 側ルーティング設定は 20 個の設定が可能。

【備考・注意事項】

LAN 側ルーティング機能はデータ通信を使用する場合のみ有効となる。

Redirect を受け付けない装置の通信は、ルーティングできない場合がある。

4.2.15. 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、静的 NAT を設定することで、WAN 側からのパケットを仮想 DMZ 用セグメントに転送することが可能となる。

仮想 DMZ 用セグメントはマスク長 24 ~ 30 が指定可能である。他のセグメントと 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 (静的 NAT を設定することで) 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。

【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、データ通信を使用する場合に有効となる。

WAN 側にサーバ公開するか、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。

NAT しない場合、本機能は無効となる。

4.2.16. 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) からのパケットを全て簡易 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。

但し、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。

【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、データ通信を使用する場合に有効となる。

NAT しない場合、本機能は無効となる。

4.2.17. 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 の端末と他のポートでの 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。

4.2.18. 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宛てに送られてきた DNS Query を各 DNS サーバへ転送し、問い合わせ結果を送信元の LAN 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】

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。但し、本装置ではキャッシュデータを保持しない。問い合わせがあった場合、毎回 DNS サーバへ転送し、問い合わせを行ないます。

NAT しない場合、本機能は無効となる。

4.2.19. ルーティング - VPN パススルー機能

【機能説明】

LAN 側の端末とデータ通信網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以下となる。

- ・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為に、静的 IP マスカレードの設定が必要になる。

以下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】

VPN パススルーでの IPsec 通信における ESP パケット、AH パケット、PPTP における GRE パケット等は CPU でフォワーディングされるため、伝送レートに制限がある。

（他の CPU 処理パケットを含めた転送は 5000pps で制限され、超過分は破棄される。）

4.2.20. 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 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。

【備考・注意事項】

UPnP での最大接続数は 400 件である。

NAT しない場合、本機能は無効となる。

4.3. 構成情報一覧

構成情報を一覧にて示します。設定範囲欄の は、初期値を示します。

4.3.1. 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	設定範囲	
IPアドレス(再)	XXX.XXX.XXX.XXX	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	設定範囲	
自動払い出し(再)	使用する	
	使用しない	
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)	XXX.XXX.XXX.XXX	192.168.0.201
払い出し個数(再)	1 ~ 253	50
WINS サーバアドレス(再)	XXX.XXX.XXX.XXX	

4.3.2. 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	設定範囲
通信速度	AUTO
	AUTO (100M MAX)
	100M FULL
	100M HALF
	10M FULL
	10M HALF
MDI/MDI-X モード	AUTO
	MDI-X
	MDI

4.3.3. ネットワーク設定 - SPI 設定

・各種 SPI 設定

設定データ名称	設定範囲	
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)

4.3.4. 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	設定範囲	
ルール No.	0 ~ 999	0
フィルタ種別	許可	
	拒否	
送信元 IP アドレス (開始 IP - 終了 IP)	*, XXX.XXX.XXX.XXX	*
プロトコル	*, 1 ~ 255、予約名 1	*
送信元ポート (開始ポート - 終了ポート)	*, 1 ~ 65535、予約名 2	*
宛先ポート (開始ポート - 終了ポート)	*, 1 ~ 65535、予約名 2	*
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	

1 予約名は、"TCP"、"UDP"、"ICMP"、"TCP UDP"

2 予約名は、"ftp"、"ftpdata"、"telnet"、"smtp"、"domain"、"www"、"pop3"、
"sunrpc"、"nntp"、"ntp"、"login"、"route"、"pftp"

4.3.5. 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	設定範囲	
ルール No.	0～999	0
通信方向	両方向 ----- LAN WAN ----- WAN LAN	
フィルタ種別	許可 ----- 拒否	
TCP フラグ	指定しない ----- SYN ----- ESTABLISHED	
送信元 IP アドレス（開始 IP - 終了 IP）	*、XXX.XXX.XXX.XXX	*
宛先 IP アドレス（開始 IP - 終了 IP）	*、XXX.XXX.XXX.XXX	*
プロトコル	*、1～255、予約名 1	*
送信元ポート（開始ポート - 終了ポート）	*、1～65535、予約名 2	*
宛先ポート（開始ポート - 終了ポート）	*、1～65535、予約名 2	*
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	

1 予約名は、"TCP"、"UDP"、"ICMP"、"TCP UDP"

2 予約名は、"ftp"、"ftpdata"、"telnet"、"smtp"、"domain"、"www"、"pop3"、
"sunrpc"、"nntp"、"ntp"、"login"、"route"、"pftp"

4.3.6. 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	設定範囲
URL フィルタ	使用しない
	許可リスト設定
	拒否リスト設定

・URL フィルタ設定 (エントリー番号 1 ~ 20)

設定データ名称	設定範囲
比較条件	ドメイン
	キーワード
比較文字	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 (「.」「-」)

4.3.7. 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 (エントリー番号 1 ~ 50)

設定データ名称	設定範囲
優先順位	0 ~ 99
宛先 IP アドレス	XXX.XXX.XXX.XXX
変換対象プロトコル	TCP
	UDP
	TCP と UDP 両方
宛先ポート	1 ~ 65535、予約名 1
変換対象ポート	1 ~ 65535、予約名 1

1 予約名は、"ftp"、"ftpdata"、"telnet"、"smtp"、"domain"、"www"、"pop3"、
"sunrpc"、"nntp"、"ntp"、"login"、"route"、"pftp"

4.3.8. 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	設定範囲
優先順位	0 ~ 99
宛先 IP アドレス	XXX.XXX.XXX.XXX
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)
変換対象ポート (開始ポート- 終了ポート)	1 ~ 65535、予約名 1

1 予約名は、"ftp"、"ftpdata"、"telnet"、"smtp"、"domain"、"www"、"pop3"、
"sunrpc"、"nntp"、"ntp"、"login"、"route"、"pftp"

4.3.9. 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	設定範囲
宛先 IP アドレス	XXX.XXX.XXX.XXX
マスク長	8 ~ 32
ゲートウェイ	XXX.XXX.XXX.XXX

4.3.10. ネットワーク設定 - 高度な設定

・UPnP 設定

設定データ名称	設定範囲
UPnP 設定	使用する
	使用しない

・PING 応答機能

設定データ名称	設定範囲
データ通信用セグメント応答	応答する
	応答しない
	指定した IP アドレスのみ応答する
(データ通信用セグメント応答) IP アドレス (1~5)	XXX.XXX.XXX.XXX

・外部へのサーバ公開設定

設定データ名称	設定範囲
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	XXX.XXX.XXX.XXX
マスク長	24 ~ 30
DMZ をポート VLAN で 区分けする	区分けしない
	区分けする (LAN1 ~ 4)
公開するホストの IP アドレス	XXX.XXX.XXX.XXX

5. 参考

5.1. 互換表示設定方法

以下の操作により互換表示設定を行ないます。

ブラウザのコマンドバーから[ツール]-[互換表示設定]をクリックします。

コマンドバーが表示されていない場合は、ウィンドウ上部を右クリックし、メニューの[コマンドバー]をクリックして表示します。

「互換表示設定」ウィンドウが表示されるので、[追加する Web サイト]に LAN 側セグメントの IP アドレスを入力し、[追加]をクリックします。

「互換表示に追加した Web サイト」に、 で設定した内容が表示されていることを確認し、[閉じる]をクリックします。