



IX2000/IX3000 シリーズ

VPN 対応高速アクセスルータ

Web 設定マニュアル

ご注意

ご使用前に本書をよくお読みの上、正しくお使いください。

お読みになったあとは、いつでもご覧になれる場所に必ず保管してください。

はじめに

このたびは「UNIVERGE IX2000/IX3000 シリーズ」（以下、本装置）をお買い上げいただきありがとうございます。

本装置は、シリアル接続のローカルコンソール、または Telnet や SSH などのリモートコンソールによるコマンドライン設定、およびパソコンの Web ブラウザによる Web 設定に対応しています。

本書では、Web 設定について説明しています。

Web 設定では、ウィザードの流れにしたがってパラメータの入力、選択を行うことで、インターネット接続や VPN 接続、クラウド接続などの基本的なネットワーク構成をはじめ、フィルタや静的 NAT の設定が可能です。また、ログの収集やソフトウェアの更新などの保守管理が可能です。

メモ

- Web 設定では、簡単な操作を主な目的としているため、主要な機能のみ設定可能です。全ての機能、または詳細な設定を行うには、ローカルコンソールまたはリモートコンソールによるコマンドライン設定が必要です。コマンドライン設定については、『取扱説明書』『コマンドリファレンスマニュアル』をご覧ください。
- IX2107/IX2235 は工場出荷の時点で、Web 設定を行うための設定が投入されています。IX2215/IX2310/IX3315 で Web 設定を行う場合、Web 設定を行うための設定を別途投入する必要があります。

注意

- (1) ご使用になる前に、『取扱説明書』の「本製品について」および「安全にお使い頂くために」「故障を防ぐためにお守りいただきたいこと」をご覧ください。正しくお使いいただきますようお願い致します。
- (2) 本書の内容の一部または全部を無断で転載することは禁止しています。
- (3) 本書の内容については、将来予告なしに変更することがあります。
- (4) 本装置のソフトウェアバージョン、ご使用になっている OS や Web ブラウザによって、本書の説明と実際に表示される内容が異なることがあります。本書では、参考に Windows 10、Microsoft Edge ブラウザを利用するための設定方法を記載しています。
- (5) 本書は内容について万全を期しておりますが、万一ご不審の点や誤り、記載漏れなどお気づきのことがありましたら、ご一報くださいますようお願い致します。
- (6) 運用した結果については、(5)項にかかわらずいかなる責任も負いかねますので、あらかじめご了承ください。

注意

- IX2107/IX2235/IX2310 には装置前面に MODE スイッチがあります。Web 設定を利用する場合は、MODE スイッチを OFF に設定する必要があります。工場出荷時は ON に設定されています。MODE スイッチの設定を変更したときは、装置を再起動する必要があります。

■商標について

Microsoft および Windows は、米国 Microsoft Corporation の米国および他の国における登録商標または商標です。

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

「フレッツ光」「フレッツ・VPN ワイド」は NTT 東日本株式会社および NTT 西日本株式会社の登録商標です。

Amazon Web Services は、米国その他の諸国における、Amazon.com, Inc. またはその関連会社の商標です。

Microsoft Azure は、米国 Microsoft Corporation の米国およびその他の国における商標または登録商標です。

KDDI-IP フォン、KDDI 光ダイレクト、au ひかり ビジネスは KDDI 株式会社の登録商標です。

FT フォン、スマートひかりは株式会社フォーバルテレコムの登録商標です。

OCN.Phone Office, .Phone Direct, Arcstar IP Voice, OCN 回線は、NTT コミュニケーションズ株式会社の登録商標です。

FUSION IP-Phone は楽天コミュニケーションズ株式会社の登録商標です。

Skype Connect™ は、Skype の商標です。

ホワイトオフィスは、ソフトバンク株式会社の登録商標です。

おとく光電話は、ソフトバンク株式会社の商標です。

ひかり電話オフィス A (エース) は、NTT 東日本株式会社および NTT 西日本株式会社の商標です。

NetMeister は、NEC プラットフォームズ株式会社の登録商標です。

その他、本書に記載されている会社名・製品・サービス名は、各社の登録商標または商標です。

■本装置の最新の情報について

本装置に関する最新の情報(最新のマニュアル、設定例など)を下記ホームページでご案内しています。ぜひご利用ください。

VPN 対応高速アクセスルータ UNIVERGE IX シリーズ
<https://jpn.nec.com/univerge/ix/index.html>

Web 設定でできること

Web 設定では、以下の操作が可能です。

- **かんたん設定** ウィザードの流れにしたがってパラメータの入力、選択を行うことで、インターネット接続や VPN(仮想プライベートネットワーク)接続、クラウド接続の設定などを簡単に行うことができます。また、対応する UNIVERGE Aspire シリーズと連携した IP 電話サービス接続の設定が可能です。
- **詳細設定** かんたん設定で設定した内容を変更することや、新しく設定を追加することができます。またフィルタの設定やサーバをインターネットに公開するための静的 NAT の設定などを行うことができます。また、設定した内容を確認することができます。
- **端末管理** LAN 内に接続されている端末を管理することができます。リンクマネージャの設定、Web 認証の設定、および Wake on LAN 機能によるリモートからの端末電源オンなどができます。
- **保守管理** 装置状態の表示や装置ログの取得、設定データのダウンロード／アップロード、また、ソフトウェアの更新や設定の初期化などを行うことができます。
- **拡張ページ** HTML などをまとめた zip ファイルをアップロードすることで、Web ページの追加・置き換えが可能です。

マニュアルの構成と表記について



マニュアルの構成

本書は、以下の内容で構成されています。

各章の説明や表示イメージは主に IX2107 を使用した手順を紹介しています。

章	タイトル	内容
1	Web 設定の準備	Web 設定のトップページにアクセスするために必要なケーブルの接続やパソコンと Web ブラウザの設定などについて説明しています。
2	メニュー	トップページやログイン/ログアウトの方法などについて説明しています。
3	かんたん設定	ウィザードの流れにしたがってパラメータの入力、選択を行う「かんたん設定」について説明しています。
4	詳細設定	Web 設定で行うことのできる項目について、機能ごとに説明しています。
5	端末管理	端末管理で行うことのできる項目について、機能ごとに説明しています。
6	保守管理	装置状態の表示、装置ログの取得、設定データの管理、設定の初期化、装置の再起動、ソフトウェアの更新などについて説明しています。
7	拡張ページ	拡張ページの削除やアップロードの仕方を説明しています。
8	困ったときには	画面に表示されるメッセージ、接続状態表示と問題対処方法について説明しています。

マニュアルの表記について

記号	意味
	間違えるとエラーとなる内容や、設定の制限事項など、注意していただきたい内容について説明しています。
	本装置の内部動作や補足情報など、操作をするうえで知っておくとより理解が深まる内容を説明しています。
[]	マウスで選択する項目は[]で括って記載しています。
「 」	画面に表示されるメッセージや項目は「 」で括って記載しています。

Web 設定で利用可能な Web ブラウザについて

以下の Web ブラウザに対応しています。

- Microsoft Edge®
- Microsoft Edge® (Chromium 版)

Web 設定で利用可能な文字について

Web ブラウザでは一部の文字を除き、以下の半角文字の入力が可能です。

コード番号																
	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9	+A	+B	+C	+D	+E	+F
20	空白 (注)	!	" (注)	#	\$	%	&	'	()	*	+	,	-	.	/
30	0	1	2	3	4	5	6	7	8	9	:	:	<	=	>	? (注)
40	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
50	P	Q	R	S	T	U	V	W	X	Y	Z	[¥ (注)]	^	_
60	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
70	p	q	r	s	t	u	v	w	x	y	z	{		}	~	

注意

- 上の表に存在しない文字(漢字やひらがななどの全角文字や制御文字)は入力できません。これらの文字を入力したときは、Web ブラウザで入力エラーが表示されます。
- Web ブラウザのウィザード(かんたん設定、詳細設定、拡張ページ、保守管理)による設定時に、文字入力フォームに空白文字(スペース)、「`”`」、「`?`」、「`¥`」の文字を入力しないでください。Web ブラウザで入力エラーが表示されます。

メモ

- 一部の設定箇所では、全角文字を入力することができます。

もくじ

はじめに	1
Web 設定でできること	3
マニュアルの構成と表記について	4
Web 設定で利用可能な Web ブラウザについて	5
Web 設定で利用可能な文字について	5

1 Web 設定の準備..... 1-1

1.1 IX2107/IX2235 をお使いの方	1-2
1.1.1 ケーブル類を接続する	1-2
1.1.2 MODE スイッチを設定する (IX2107/IX2235)	1-5
1.1.3 本装置の電源を入れる	1-5
1.1.4 パソコンのネットワークを設定する	1-6
1.1.5 パソコンのブラウザを設定する	1-9
1.1.6 Web 設定のトップページを開く	1-12
1.2 IX2215/IX2310/IX3315 をお使いの方	1-15
1.2.1 ケーブル類を接続する	1-15
1.2.2 MODE スイッチを設定する (IX2310)	1-17
1.2.3 本装置の電源を入れる	1-17
1.2.4 Web 設定を行うための設定を投入する	1-18
1.2.5 パソコンのネットワークを設定する	1-22
1.2.6 パソコンのブラウザを設定する	1-26
1.2.7 Web 設定のトップページを開く	1-28

2 メニュー..... 2-1

2.1 トップページ	2-3
2.2 ログインする	2-4
2.3 ログアウトする	2-10
2.4 設定の保存	2-12

3 かんたん設定..... 3-1

3.1 インターネット接続	3-2
3.2 インターネット接続+VPN 接続	3-20
3.3 インターネット接続+フレッツ・VPN ワイド接続	3-41
3.4 フレッツ・VPN ワイド接続	3-58
3.5 NGN VPN 接続	3-70
3.5.1 NetMeister の事前登録	3-71
3.5.2 NGN VPN 接続の設定	3-72
3.5.3 センタの場合の設定	3-75
3.5.4 拠点の場合の設定	3-84
3.6 IPv6 IPoE 接続	3-92
3.7 クラウド接続	3-104
3.8 IP 電話サービス接続	3-124

4 詳細設定..... 4-1

4.1	基本設定	4-2
4.1.1	パスワードの設定	4-2
4.1.2	装置名の設定	4-6
4.1.3	時刻の設定	4-8
4.1.4	保守の設定	4-10
4.1.5	NetMeister の設定	4-14
4.1.6	ゼロタッチの設定	4-17
4.2	LAN	4-19
4.2.1	LAN アドレスの設定	4-19
4.2.2	DHCP サーバの設定	4-22
4.3	WAN	4-24
4.3.1	プロバイダの設定	4-24
4.3.2	静的 NAT の設定	4-34
4.3.3	WAN フィルタの設定 (Ver10.3 以降の機能)	4-38
4.3.4	WAN フィルタの設定 (Ver10.2 までの設定がある場合)	4-44
4.3.5	URL フィルタの設定	4-50
4.3.6	QoS の設定	4-55
4.3.7	通信セキュリティの設定	4-65
4.4	VPN・クラウド	4-68
4.4.1	VPN の設定	4-68
4.4.2	L2TP の設定	4-77
4.4.3	クラウドの設定	4-80
4.5	NGN 網 VPN の設定	4-91
4.5.1	NetMeister の事前登録	4-93
4.5.2	サービス情報サイトの事前登録	4-93
4.5.3	NGN 網 VPN 設定	4-98
4.6	デバイス	4-104
4.6.1	デバイスの設定	4-104
4.7	UTM	4-108
4.7.1	トップページ	4-108
4.7.2	基本設定	4-110
4.7.3	UTM の詳細設定	4-116
4.7.4	アンチウイルス (AV) の設定	4-120
4.7.5	不正侵入防止 (IPS) の設定	4-124
4.7.6	Web ガード (WG) の設定	4-128
4.7.7	URL フィルタリング (UF) の設定	4-132
4.7.8	グループ別ポリシー設定	4-139
4.7.9	ホワイトリスト設定	4-144
4.7.10	UTM 脅威レポート	4-148

5 端末管理.....5-1

5.1	リンクマネージャの設定	5-2
5.2	Web 認証の設定	5-15

6 保守管理.....6-1

6.1	装置状態の表示	6-2
6.2	装置ログの取得	6-6
6.3	設定データの管理	6-7
6.3.1	設定データのダウンロード (バックアップ)	6-7

6.3.2 設定データのアップロード(リストア)	6-9
6.4 設定の初期化	6-15
6.5 ソフトウェアの更新	6-18
6.6 ping の実行	6-22
6.7 任意コマンドの実行	6-23
6.8 IP 電話サービス保守	6-25
6.9 URL オフロード	6-27
6.10 リンクマネージャ	6-28
6.11 Wake on LAN	6-30
6.12 再起動	6-32
7 拡張ページ	7-1
7.1 拡張ページのアップロード	7-2
7.2 拡張ページの削除	7-5
8 困ったときには	8-1
8.1 メッセージエリアの警告メッセージ	8-1
8.2 入力エラーメッセージ	8-3

1. Web 設定の準備

1 Web 設定の準備

本章では、Web 設定のトップページにアクセスするまでの手順について説明します。

1.1 IX2107/IX2235 をお使いの方

- ケーブル類を接続する
- MODE スイッチを設定する(IX2107/IX2235)
- 本装置の電源を入れる
- パソコンのネットワークを設定する
- パソコンのブラウザを設定する
- Web 設定のトップページを開く

1.2 IX2215/IX2310/IX3315 をお使いの方

- ケーブル類を接続する
- MODE スイッチを設定する(IX2310)
- 本装置の電源を入れる
- Web 設定を行うための設定を投入する
- パソコンのネットワークを設定する
- パソコンのブラウザを設定する
- Web 設定のトップページを開く

1. Web 設定の準備

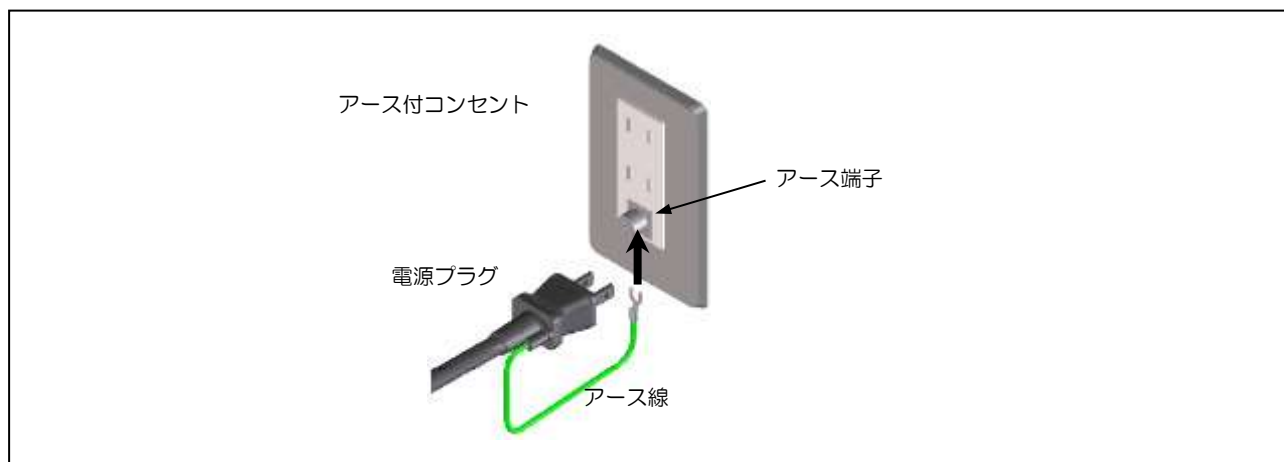
1.1 IX2107/IX2235 をお使いの方

IX2107/IX2235 は工場出荷の時点で、Web 設定を行うための設定が投入されています。

1.1.1 ケーブル類を接続する

- (1) 添付の電源ケーブルに付いているアース線をコンセントのアース端子に確実に接続します。なお、その際、アース線についている保護キャップを外してから接続してください。

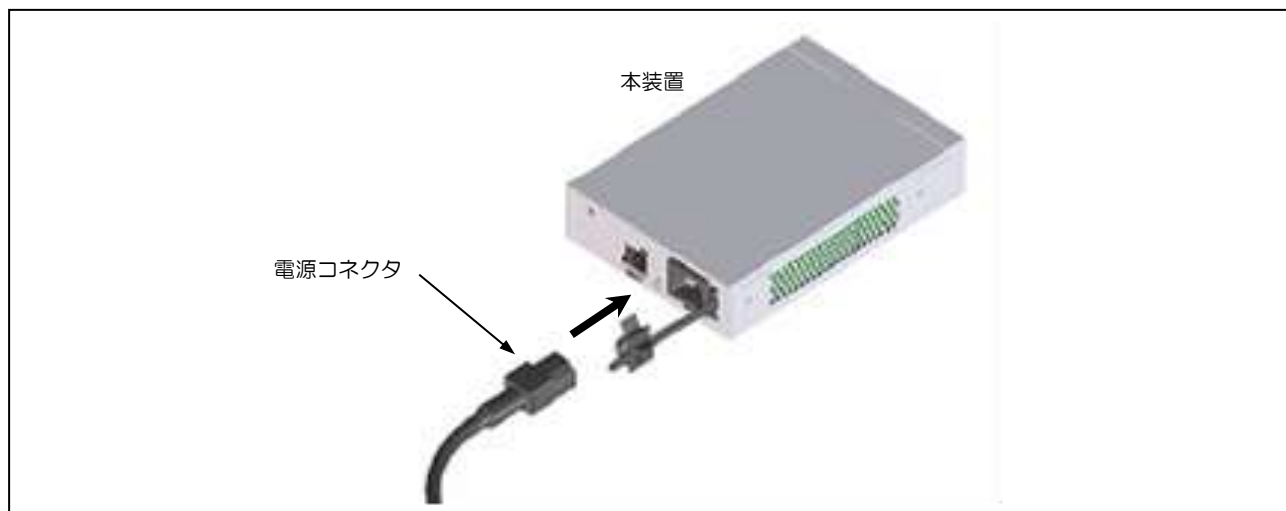
注意 接続するのはアース線のみです。(1)では電源プラグはコンセントに絶対に接続しないでください。



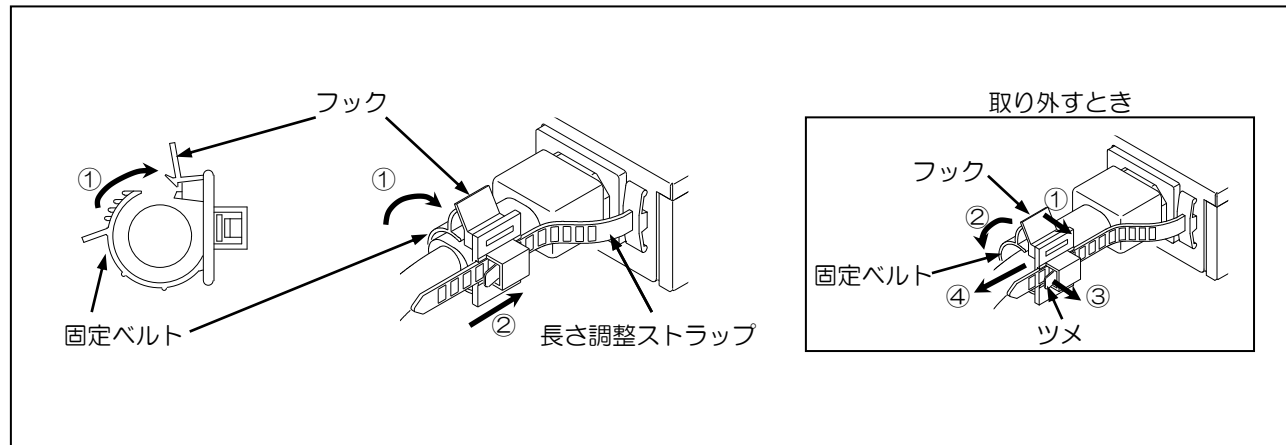
1. Web 設定の準備

(2) 電源コネクタを本装置に接続します。

注意 緩みのないように確実に挿し込みます。



(3) 電源ケーブルが製品から外れないように固定ベルトで固定します。固定ベルトは、フックに差し込んで電源ケーブルのコネクタ部分を締め付けたあと、長さ調整ストラップに沿って固定ベルトを製品側へスライドさせ、確実に固定します。



(4) 本装置の LAN 側ポートとパソコンの LAN ポートを接続します。

注意 カテゴリ 5 以上のストレート結線またはクロス結線の UTP または STP ケーブルを使用してください。

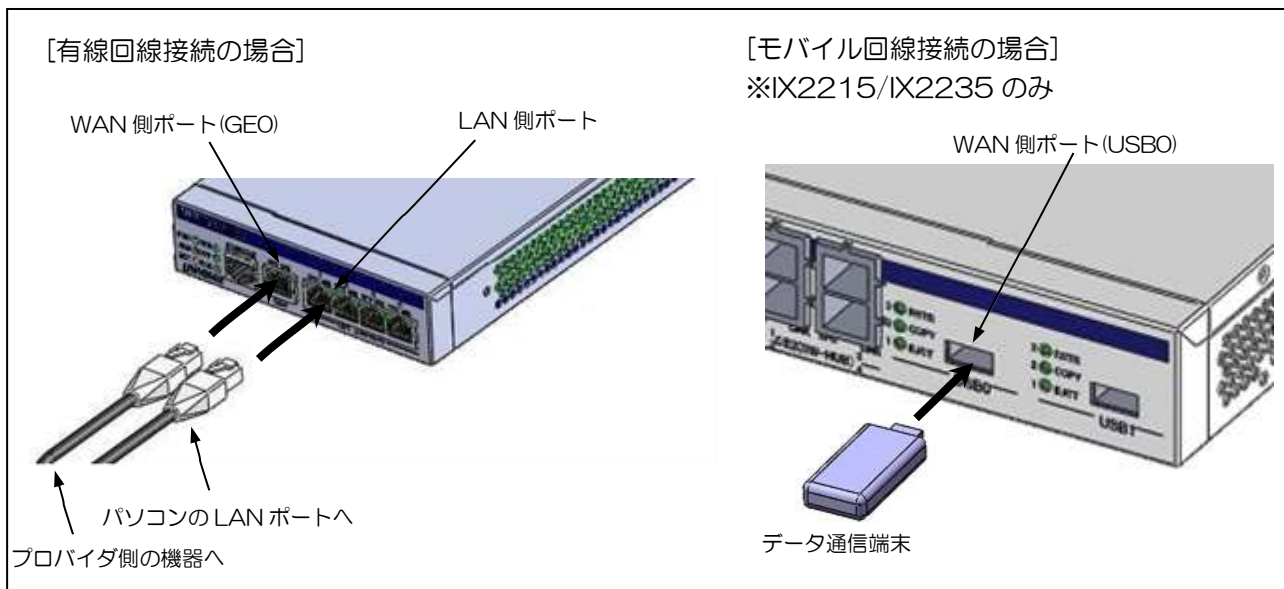
メモ LAN 側ポートは、IX2107 の場合は GE1、IX2235 の場合は GE2 を使用します。

メモ 本装置は、ストレート結線／クロス結線を自動認識します。

1. Web 設定の準備

- (5) 本装置の WAN 側ポート(GEO/USB0)とプロバイダ側の機器(ONU 等)、または、データ通信端末を接続します。

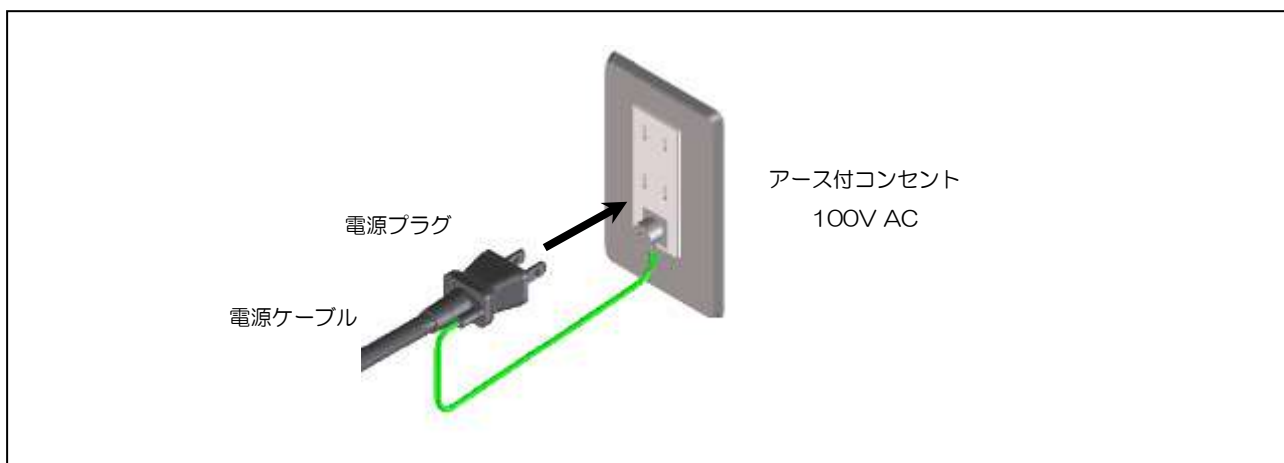
注意 ケーブルは、カテゴリ 5 以上のストレート結線またはクロス結線の UTP または STP ケーブルを使用してください。



- (6) 電源スイッチが OFF になっていることを確認し、電源ケーブルのプラグを 100V AC のコンセントに確実に差し込みます。

注意 100V AC(50Hz/60Hz)のコンセントに接続してください。

注意 プラグの緩みがないように確実に差し込みます。

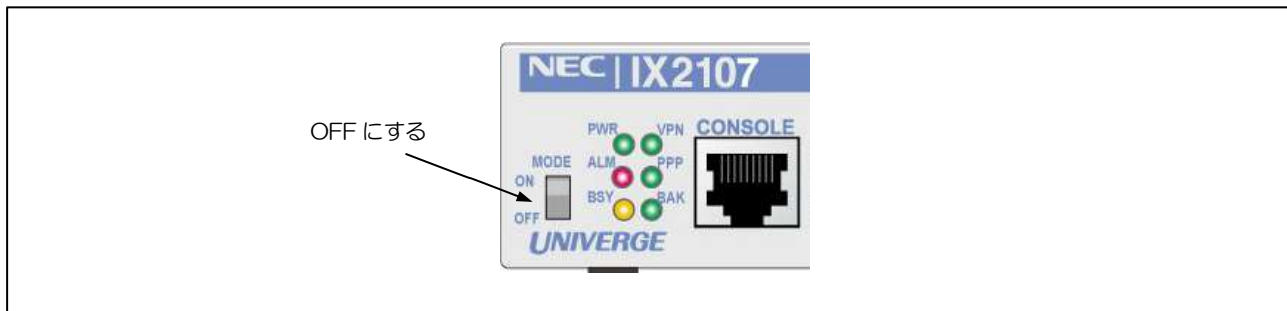


1. Web 設定の準備

1.1.2 MODE スイッチを設定する(IX2107/IX2235)

(1) MODE スイッチを OFF にします。

注意 スイッチの操作は、先の細い棒状のもの（電気を通さない材質のもの）を使用して行ってください。

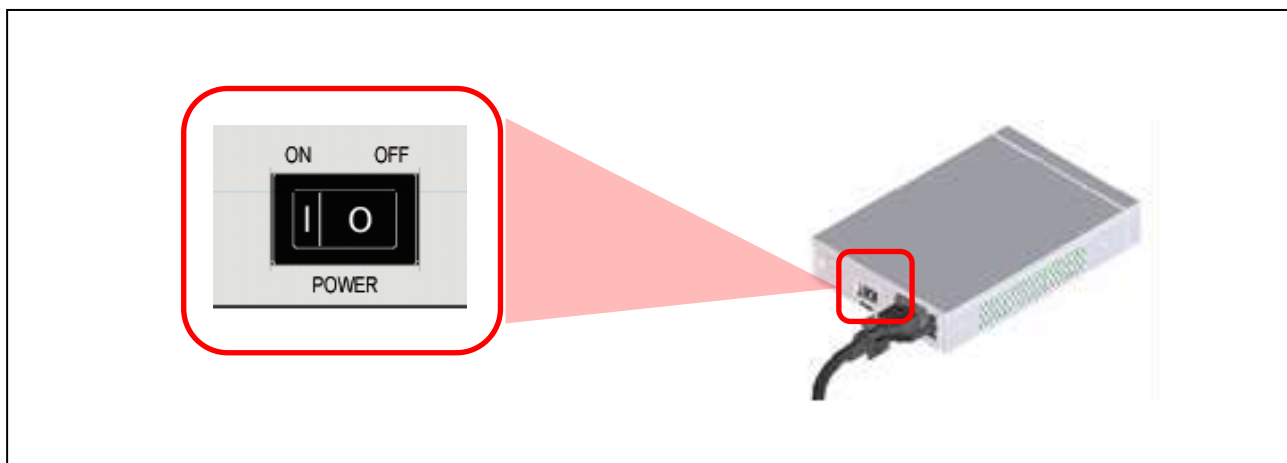


1.1.3 本装置の電源を入れる

(1) 電源スイッチの[I]を押して ON にします。起動後、前面の「POWER LED」が緑色に点灯、「ALARM LED」が消灯していることを確認します。

注意 電源を OFF にするときは、本装置前面の「BUSY LED」が点灯していないことを確認して[O]を押します。

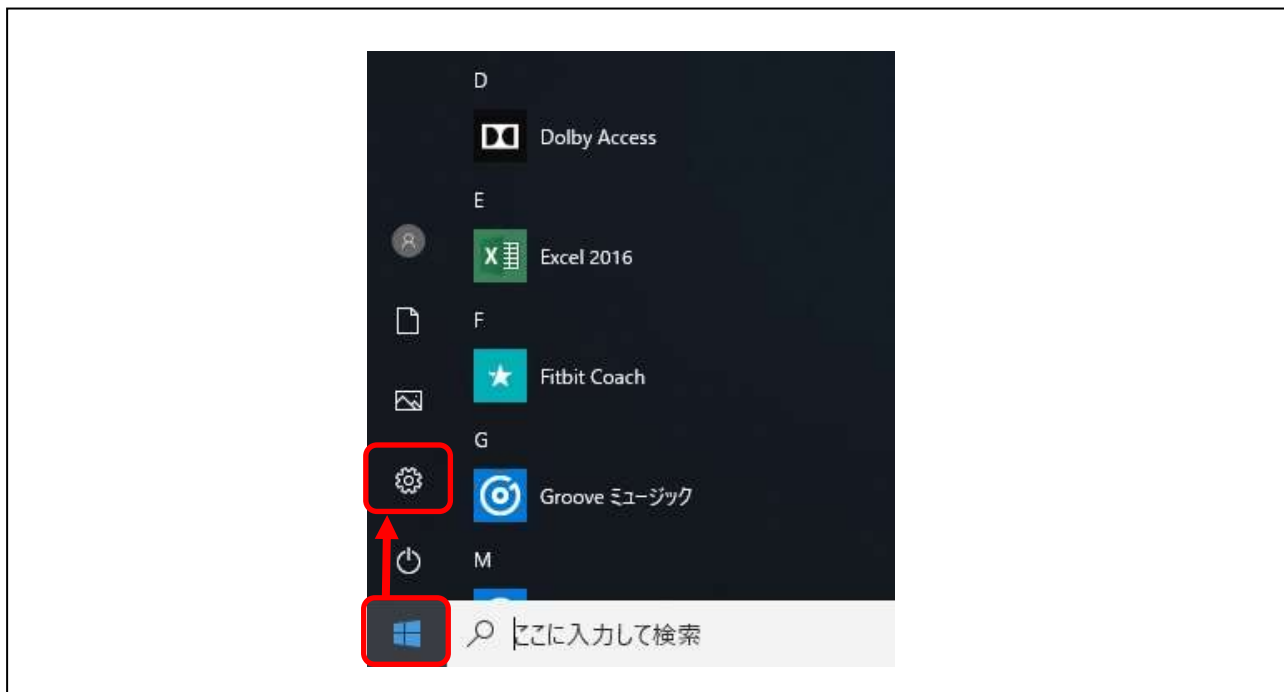
メモ 起動には 30 秒程度かかります。



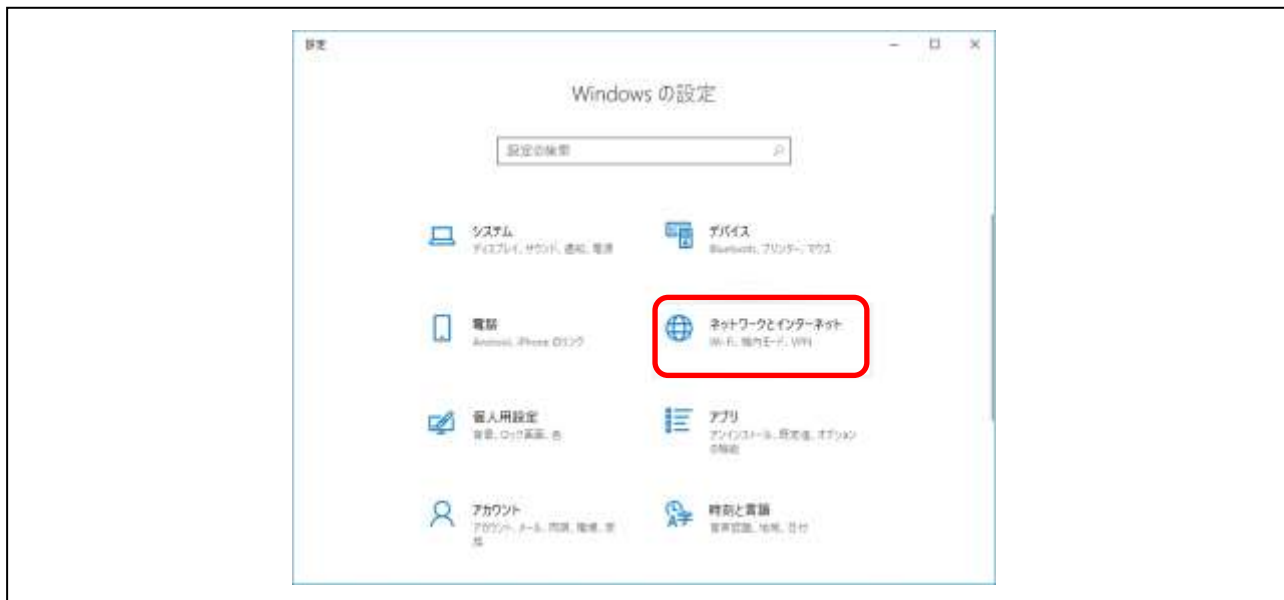
1. Web 設定の準備

1.1.4 パソコンのネットワークを設定する

- (1) 画面左下にある Windows の[スタート]メニューをクリックし、メニューの[設定]をクリックします。



- (2) [ネットワークとインターネット]をクリックします。



1. Web 設定の準備

- (3) [ネットワークの詳細設定]の[アダプターのオプションを変更する]をクリックします。



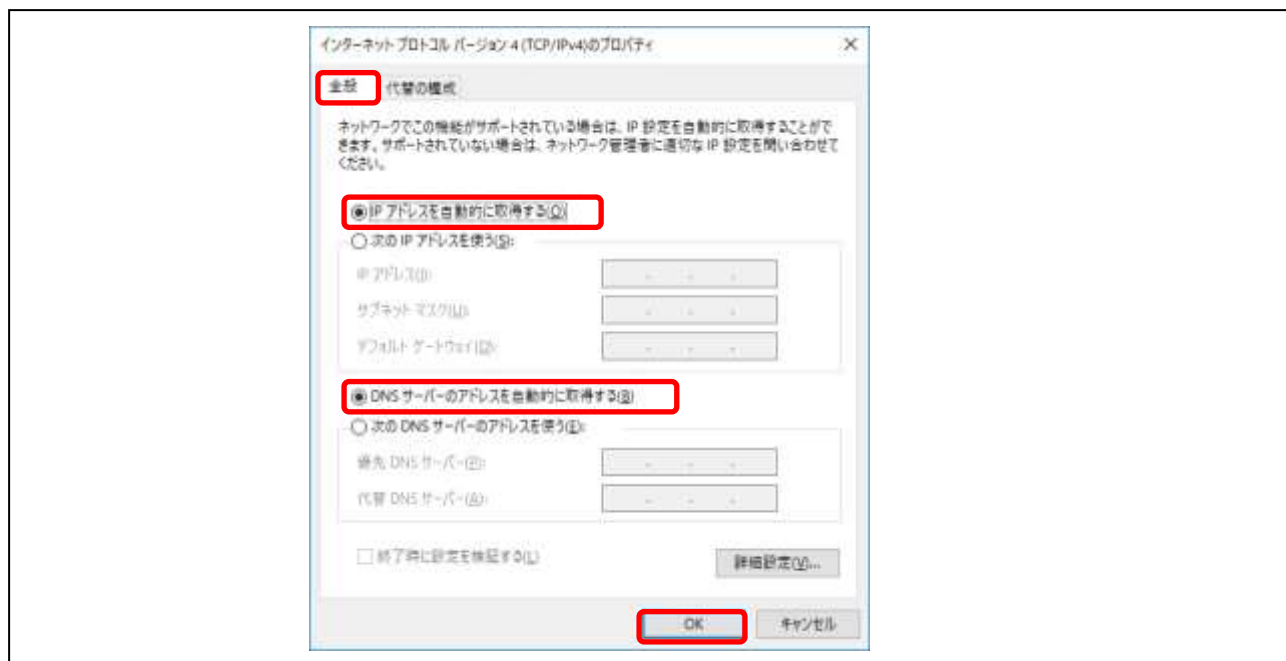
- (4) [イーサネット]を右クリックしたメニューから[プロパティ(R)]をクリックします。



パソコンにログインしている場合は、管理者アカウントのパスワード入力が必要になります。

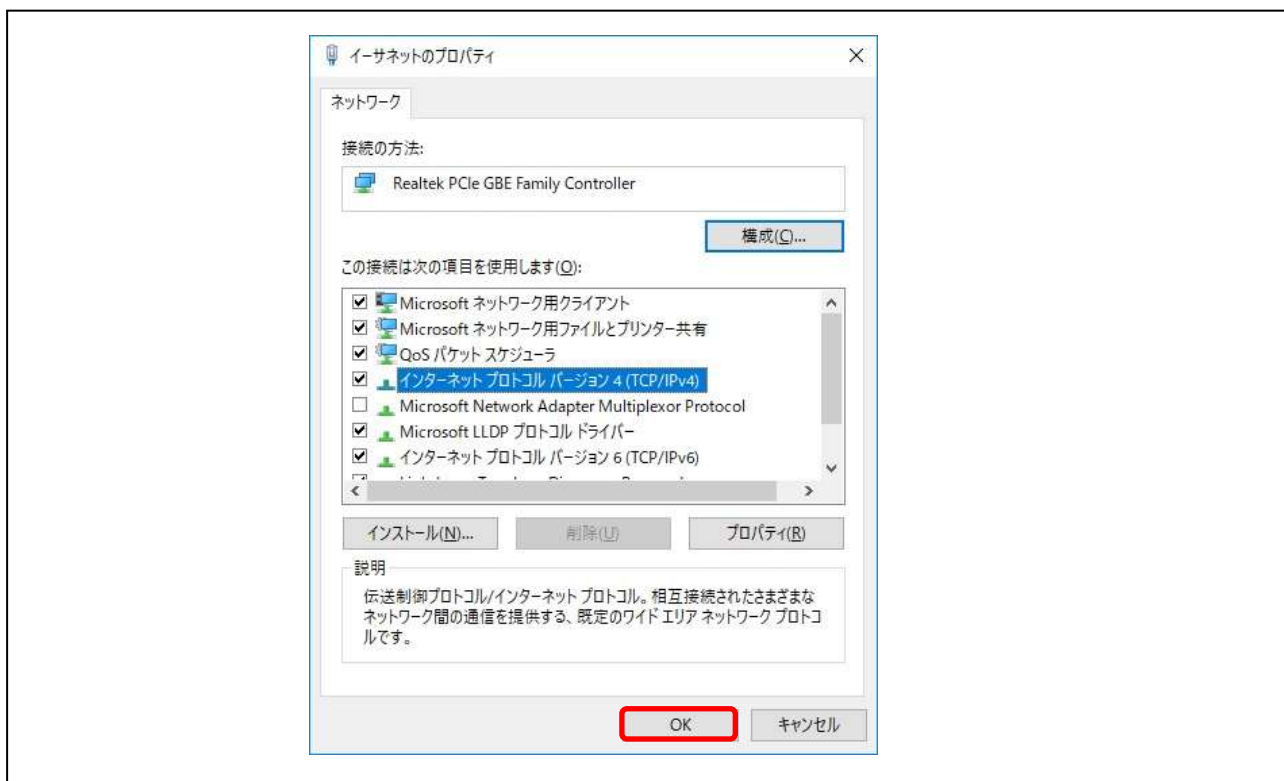
1. Web 設定の準備

- (5) 「インターネットプロトコルバージョン 4(TCP/IPv4)」を選択します。
- (6) [プロパティ(R)]をクリックします。
- (7) [全般]タブをクリックします。
- (8) [IP アドレスを自動的に取得する(O)] のラジオボタンをチェックします。
- (9) [DNS サーバーのアドレスを自動的に取得する(B)]のラジオボタンをチェックします。
- (10) [OK]をクリックして、【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】画面を閉じます。




1. Web 設定の準備

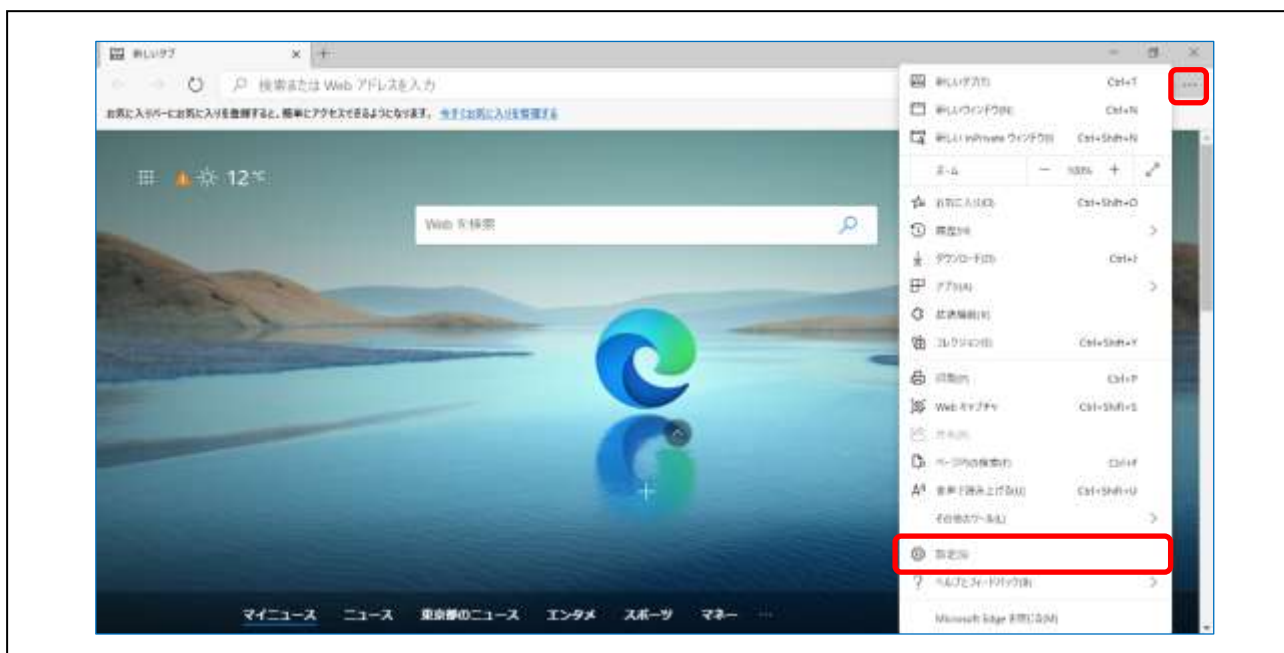
- (11) [OK]または[閉じる]をクリックして、【イーサネットのプロパティ】の画面を閉じます。



1.1.5 パソコンのブラウザを設定する

 Microsoft Edge のバージョンにより、画面の表示内容が異なる場合があります。

- (1) パソコンで、Web ブラウザ(Microsoft Edge)を起動します。
- (2) Web ブラウザのメニュー[…]をクリックし、[設定]をクリックします。



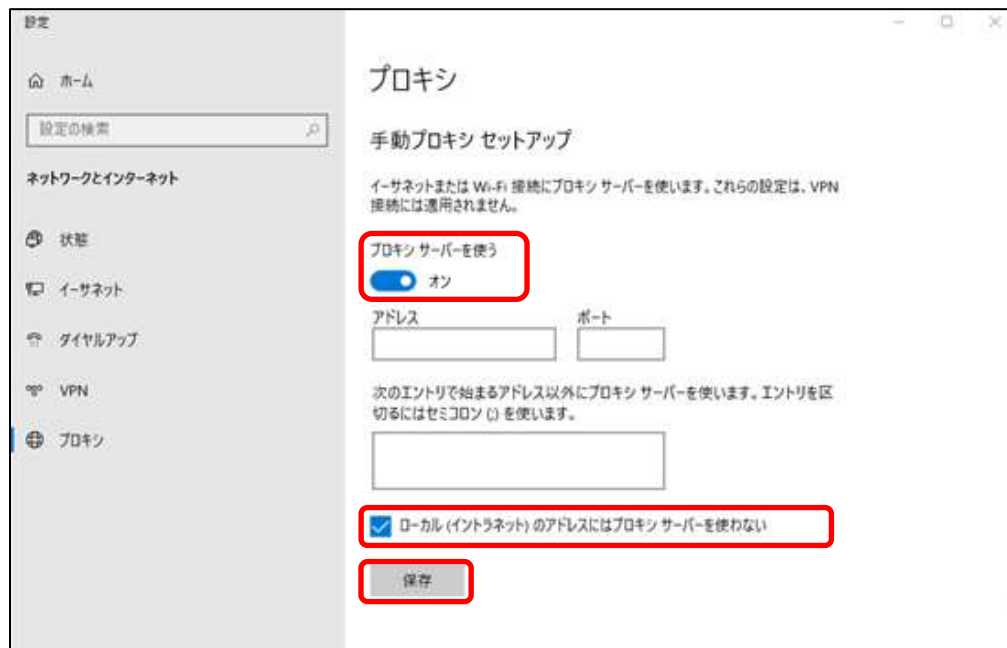
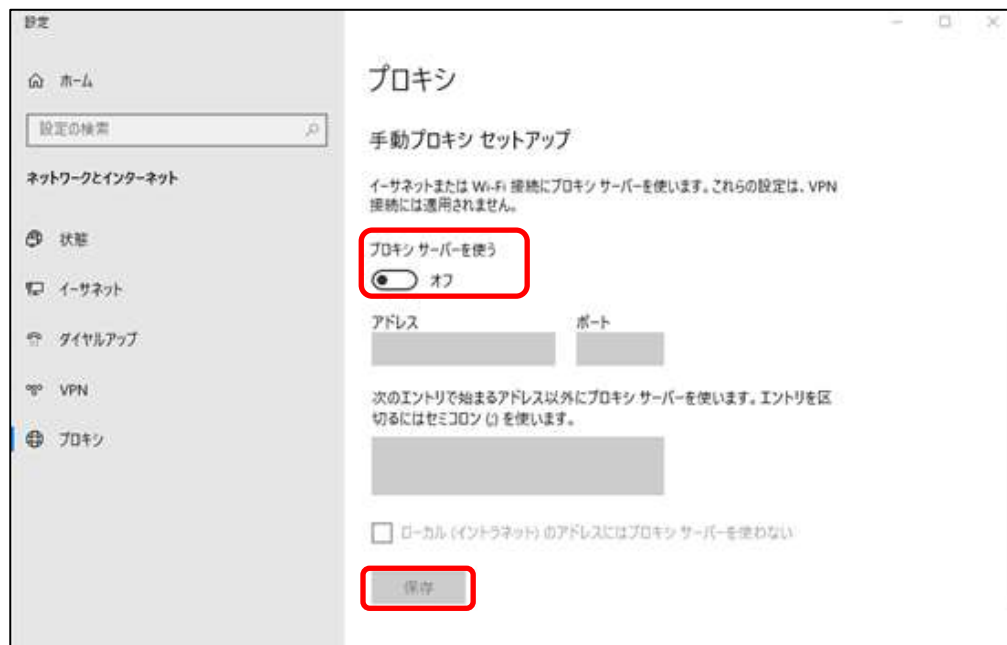
1. Web 設定の準備

- (3) 設定メニューの[システムシステムとパフォーマンス]をクリックし、[コンピューターのプロキシ設定を開く]をクリックします。



1. Web 設定の準備

- (4) [手動プロキシ セットアップ]を下方にスクロールし、[プロキシ サーバーを使う]を[オフ]にするか、[ローカル(イントラネット)のアドレスにはプロキシサーバーを使わない]にチェックして、[保存]をクリックしてください。

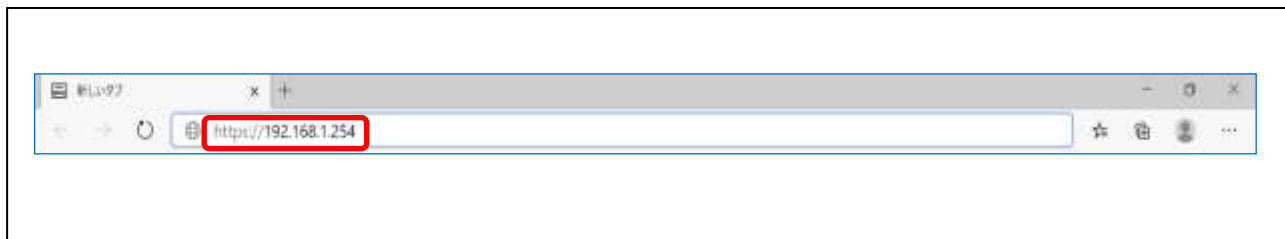


注意 本装置は Cookie を使用しています。「すべての Cookie をブロック」または「高」にすると、本装置で使用する Cookie がブロックされ、設定を行うことができません。

1. Web 設定の準備

1.1.6 Web 設定のトップページを開く

- (1) Web ブラウザのアドレスバーに半角英数字で「https://192.168.1.254/」と入力し、[Enter]キーを押します。



- ☒ 自己証明書を用いた方式のため、接続時にブラウザに「接続がプライベートではありません」、「プライバシーが保護されません」、「セキュリティ保護なし」などと表示されます。http と入力して接続することもできますが、通信内容が暗号化されないため、通信の安全性が低くなります。https での接続を推奨します。

1. Web 設定の準備

(2) Web 設定のトップページが表示されることを確認します。

■メニュー	トップページ
トップページ	
ログイン	ルータの設定を開始します。以下のリンクから選択してください。
■保守管理	パスワードを登録・変更する前にユーザ名とパスワードを入力する画面が表示された場合は、そのまま「OK」をクリックしてください。
装置状態の表示	
リンクマネージャ	
Wake on LAN	かんたん設定
■外部リンク	
製品ページ	<ul style="list-style-type: none">• インターネット接続 フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用して、インターネットに接続する設定を行います。• インターネット接続+VPN接続 フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用したインターネット接続と、インターネットVPNによる拠点間通信の設定を行います。• インターネット接続+フレッツ・VPNワイド接続 フレッツ光を使用したインターネット接続と、フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。• フレッツ・VPNワイド接続 フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。• クラウド接続 インターネットVPNや専用線を使用したクラウド接続の設定を行います。• IP電話カード接続 UNIVERGE Aspire UXと連携したIP電話ネットワークの設定を行います。
	詳細設定
	<ul style="list-style-type: none">• 詳細設定 各機能を詳細に設定します。 かんたん設定に含まれない設定を行う場合は、こちらから設定してください。
	保守管理
	<ul style="list-style-type: none">• 保守管理 装置状態の確認、ソフトウェアの更新、pingの実行など、各種保守機能の操作を行います。• Wake on LAN Wake on LAN機能を実行します。

1. Web 設定の準備

トップページを開けないときは

以下の点を確認し、対処してください。

- (1) パソコンと本装置が正しく接続されているかを確認してください。
- (2) パソコンを接続している LAN 側ポートが正しいかを確認してください。
IX2107 の場合は GE1、IX2235 の場合は GE2 を使用します。
- (3) パソコンのコマンドプロンプトから本装置の LAN 側ポートに ping を実施して、通信できるかを確認してください。通信できない場合、ローカルエリア接続を[無効]にしたあと、再度、[有効]にすることで、IP アドレスの解放／再取得を行ってください。
- (4) 本章「1.1.5 パソコンのブラウザを設定する」にしたがって、パソコンのブラウザ設定が正しいかを確認してください。
- (5) 本装置の設定を変更している場合、本装置の LAN 側ポートの IP アドレスとパソコンの IP アドレスが同じネットワークになっているか、HTTP サーバ機能が有効になっているかを確認してください。

1. Web 設定の準備

1.2 IX2215/IX2310/IX3315 をお使いの方

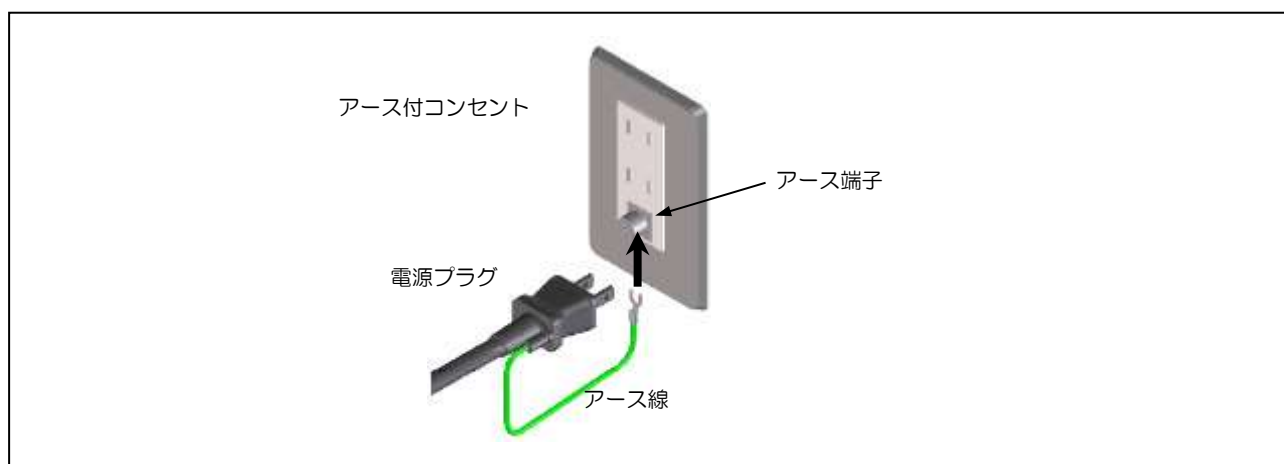
IX2215/IX2310/IX3315 で Web 設定を利用する場合、Web 設定を使用できるようにするための設定を別途投入する必要があります。

1.2.1 ケーブル類を接続する

- (1) 添付の電源ケーブルに付いているアース線をコンセントのアース端子に確実に接続します。なお、その際、アース線についている保護キャップを外してから接続してください。

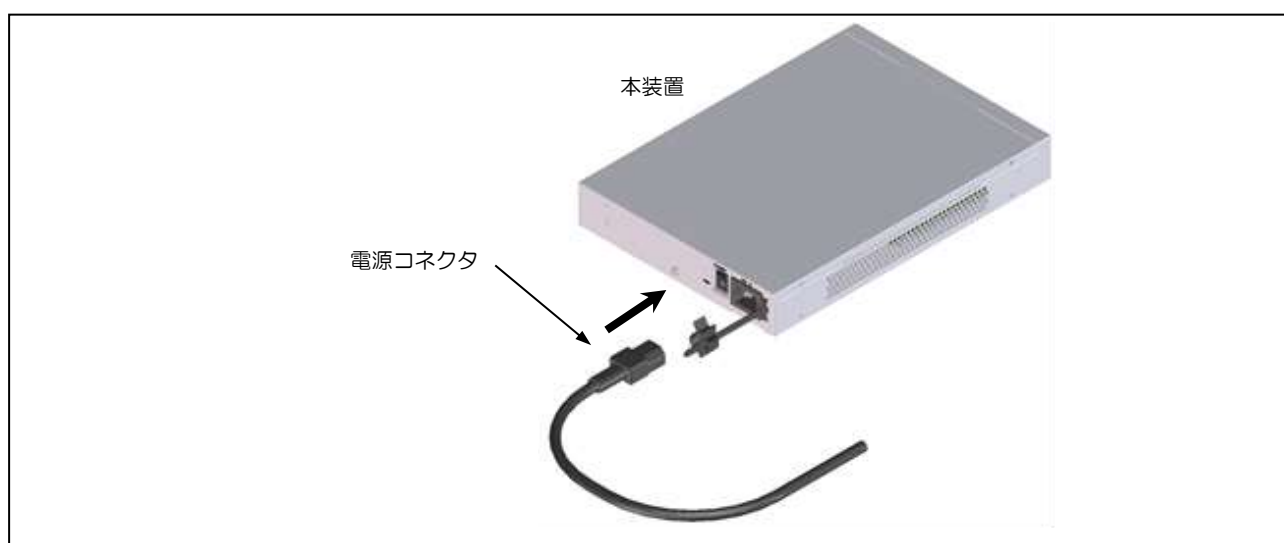
注意 接続するのはアース線のみです。(1)では電源プラグはコンセントに絶対に接続しないでください。

メモ IX3000 シリーズでは電源ケーブルにアース線が付いていないため、本作業は不要です。



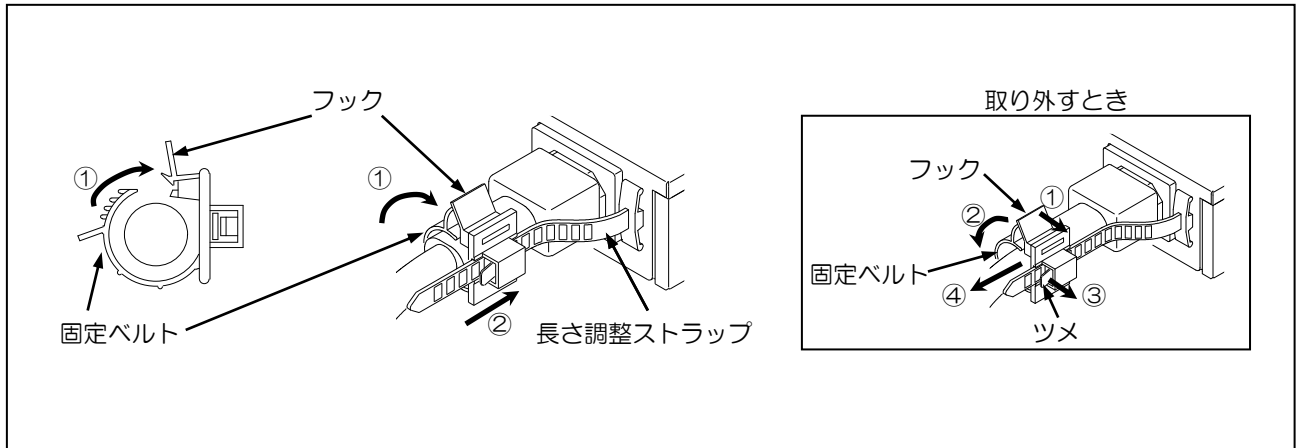
- (2) 電源コネクタを本装置に接続します。

注意 緩みのないように確実に挿し込みます。



1. Web 設定の準備

- (3) 電源ケーブルが製品から外れないように固定ベルトで固定します。固定ベルトは、フックに差し込んで電源ケーブルのコネクタ部分を締め付けたあと、長さ調整ストラップに沿って固定ベルトを製品側へスライドさせ、確実に固定します。



- (4) 本装置の LAN 側ポートとパソコンの LAN ポートを接続します。

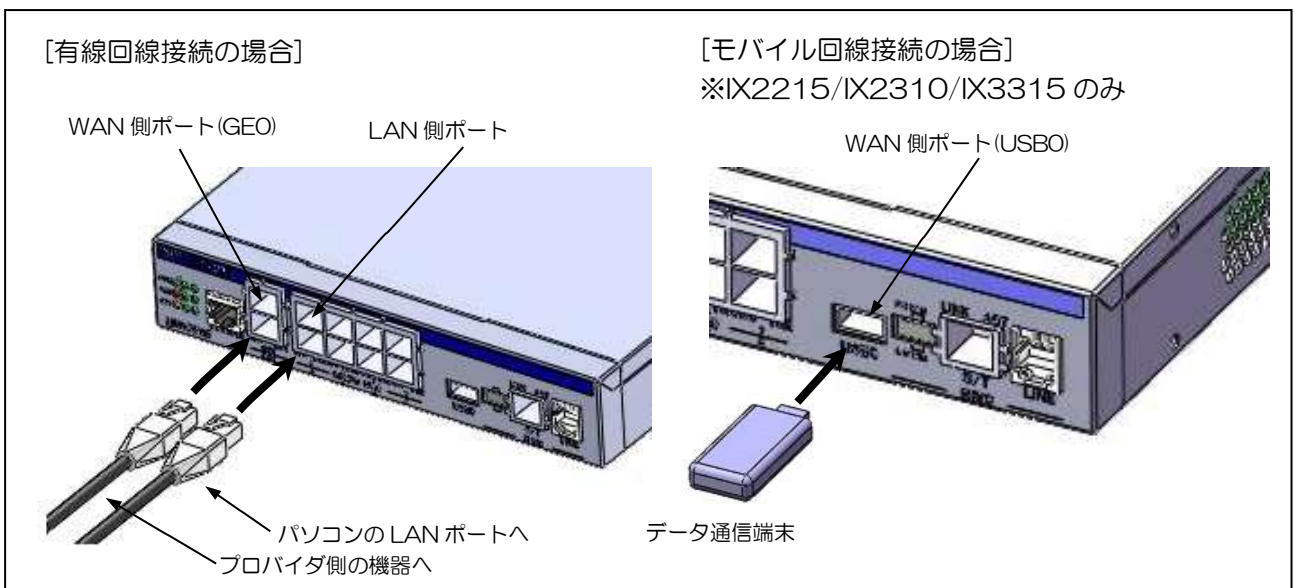
注意 カテゴリ 5 以上のストレート結線またはクロス結線の UTP または STP ケーブルを使用してください。

メモ LAN 側ポートは、IX2215 の場合は GE2、IX2310 の場合は GE3、IX3315 の場合は GE5 を使用します。

メモ 本装置は、ストレート結線/クロス結線を自動認識します。

- (5) 本装置の WAN 側ポート (GEO/USB0) とプロバイダ側の機器 (ONU 等)、または、データ通信端末を接続します。

注意 ケーブルは、カテゴリ 5 以上のストレート結線またはクロス結線の UTP または STP ケーブルを使用してください。

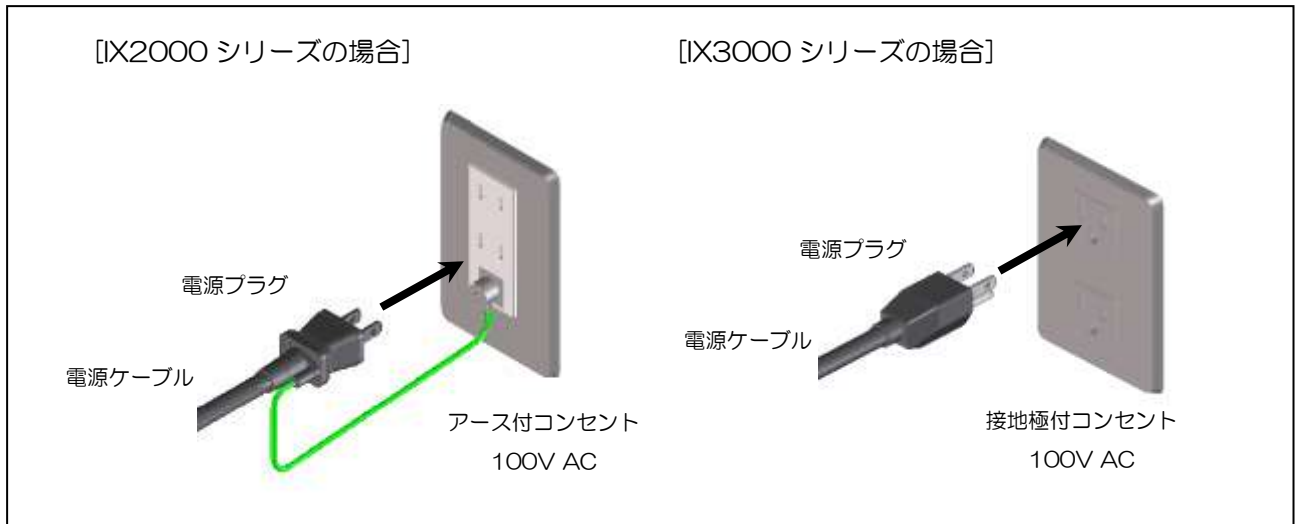


1. Web 設定の準備

- (6) 電源スイッチが OFF になっていることを確認し、電源ケーブルのプラグを 100V AC のコンセントに確実に挿し込みます。

注意 100V AC(50Hz/60Hz)のコンセントに接続してください。

注意 プラグの緩みがないように確実に挿し込みます。

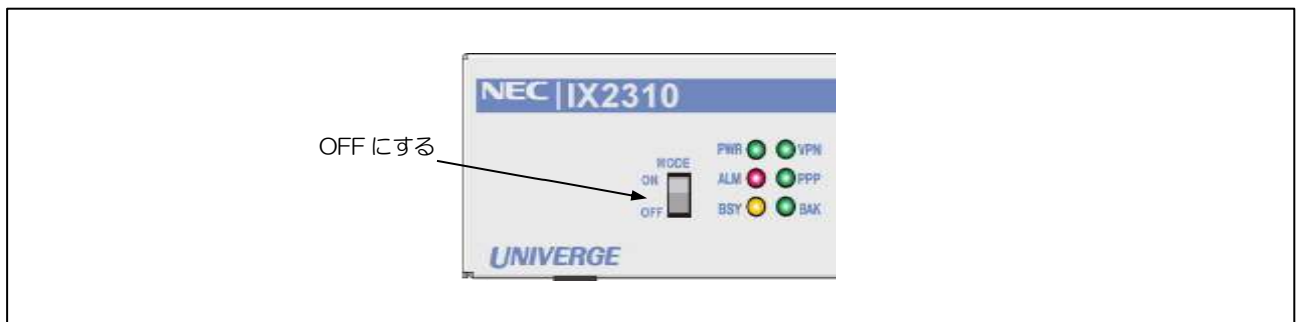


1.2.2 MODE スイッチを設定する(IX2310)

- (1) MODE スイッチを OFF にします。

注意 スイッチの操作は、先の細い棒状のもの（電気を通さない材質のもの）を使用して行ってください。

×モ MODE スイッチがない IX2215/IX3315 では本作業は不要です。



1.2.3 本装置の電源を入れる

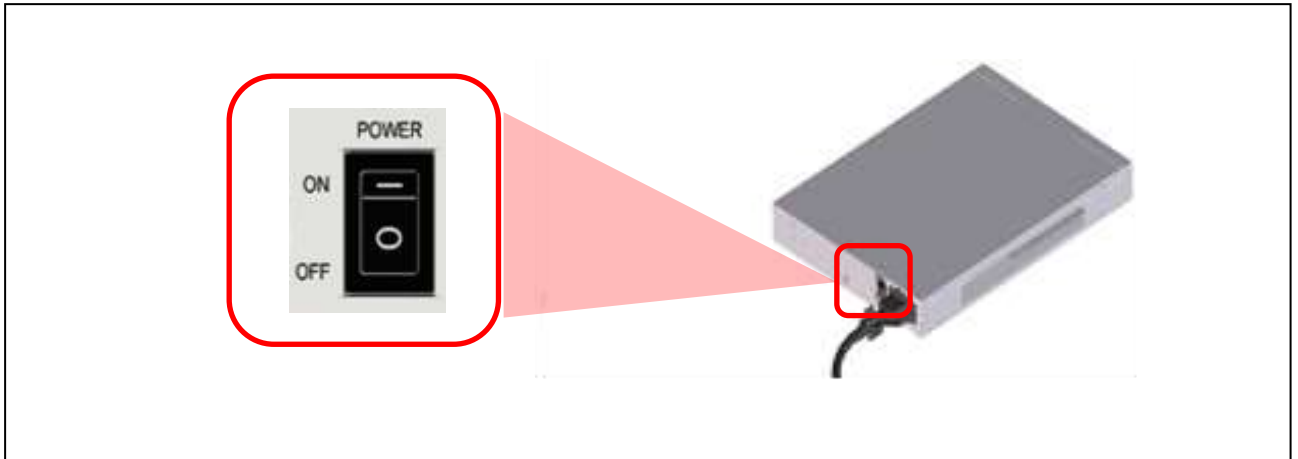
- (1) 電源スイッチの[—] を押して ON にします。起動後、前面の「POWER LED」が緑色に点灯、「ALARM LED」が消灯していることを確認します。

注意 電源を OFF にするときは、本装置前面の「BUSY LED」が点灯していないことを確認して[O]を押します。

×モ IX3000 シリーズの場合、電源スイッチの[]を押して ON にします。

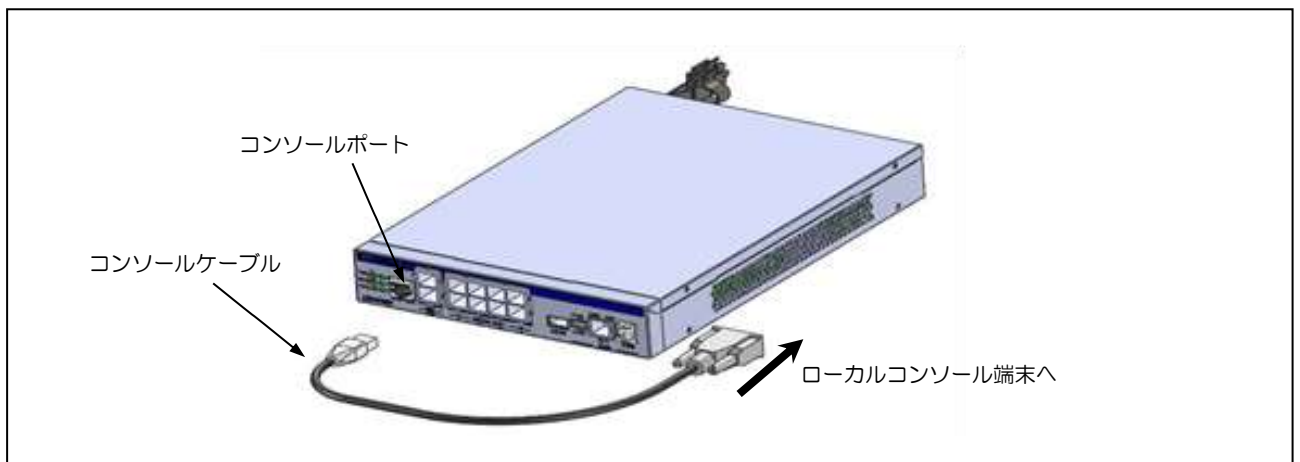
×モ 起動には 30 秒～120 秒程度かかります。

1. Web 設定の準備



1.2.4 Web 設定を行うための設定を投入する

- (1) 添付のコンソールケーブルをコンソールポートに接続します。コネクタはカチッと音がするまで確実に挿入します。コンソールケーブルの反対側をローカルコンソール端末に接続し、固定ネジを確実に締めてください。



☒ ローカルコンソール端末の接続口が USB ポートの場合は、別途シリアルコネクタ (D-SUB9 ピン(メス)) を USB に変換するためのケーブルが必要になります。

■ローカルコンソール端末の通信ソフトウェアについて

ローカルコンソールとして使用するパソコンなどの端末には、VT-100 準拠の通信ソフトウェアが必要です。通信ソフトウェアは次の設定にします。

項目	設定
通信速度	9600bps
データ長	8bit
パリティ	なし
ストップ・ビット	1bit
フロー制御	なし

1. Web 設定の準備

- (2) Web 設定を行うための設定をローカルコンソールから投入します。詳細な設定方法については、『取扱説明書』『機能説明書』をご覧ください。

【IX2215 の場合】

```
enable-config
!
logging buffered
logging subsystem all warn
logging timestamp datetime
!
ip ufs-cache enable
ip dhcp enable
ip access-list web-http-acl permit ip src any dest 192.168.1.254/32
!
http-server ip access-list web-http-acl
http-server ip enable
!
system information lan 1 GigaEthernet2.0
!
ip dhcp profile dhcp-profile
  dns-server 192.168.1.254
!
interface GigaEthernet2.0
  ip address 192.168.1.254/24
  ip dhcp binding dhcp-profile
  no shutdown
```

メモ ソフトウェアバージョンによって、上記で入力したコマンドが自動的に変換される場合があります。

1. Web 設定の準備

【IX2310 の場合】

```
default-console web
```

- メモ** コマンド入力後、Web コンソール接続するための設定が自動的に保存されます。上記コマンドを設定後は、一旦電源をオフにし、再度電源をオンにして再起動させてください。

1. Web 設定の準備

【IX3315 の場合】

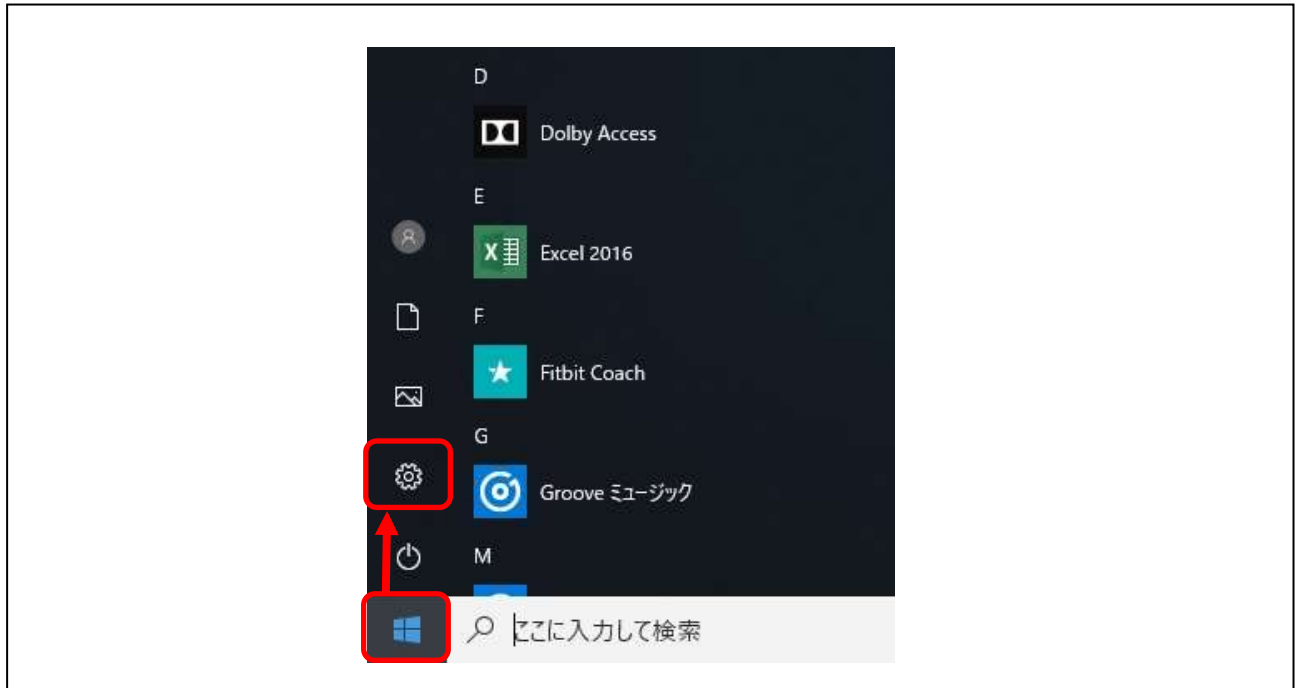
```
enable-config
!
logging buffered
logging subsystem all warn
logging timestamp datetime
!
ip ufs-cache enable
ip dhcp enable
ip access-list web-http-acl permit ip src any dest 192.168.1.254/32
!
http-server ip access-list web-http-acl
http-server ip enable
!
system-information lan 1 GigaEthernet5.0
!
ip dhcp profile dhcp-profile
  dns-server 192.168.1.254
!
interface GigaEthernet5.0
  ip address 192.168.1.254/24
  ip dhcp binding dhcp-profile
  no shutdown
```

メモ ソフトウェアバージョンによって、上記で入力したコマンドが自動的に変換される場合があります。

1. Web 設定の準備

1.2.5 パソコンのネットワークを設定する

- (1) 画面左下にある Windows の[スタート]メニューをクリックし、メニューの[設定]をクリックします。



1. Web 設定の準備

(2) [ネットワークとインターネット]をクリックします。

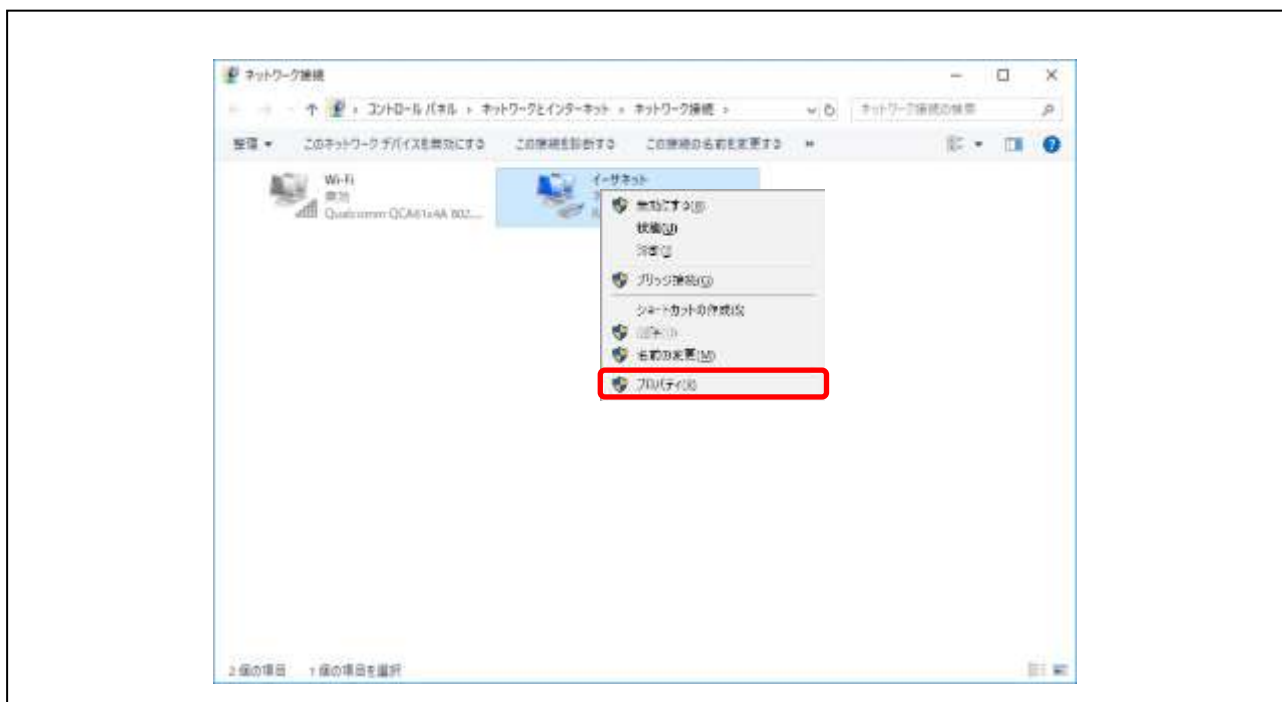


(3) [ネットワークの詳細設定]の[アダプターのオプションを変更する]をクリックします。



1. Web 設定の準備

- (4) [イーサネット]を右クリックしたメニューから[プロパティ(R)]をクリックします。

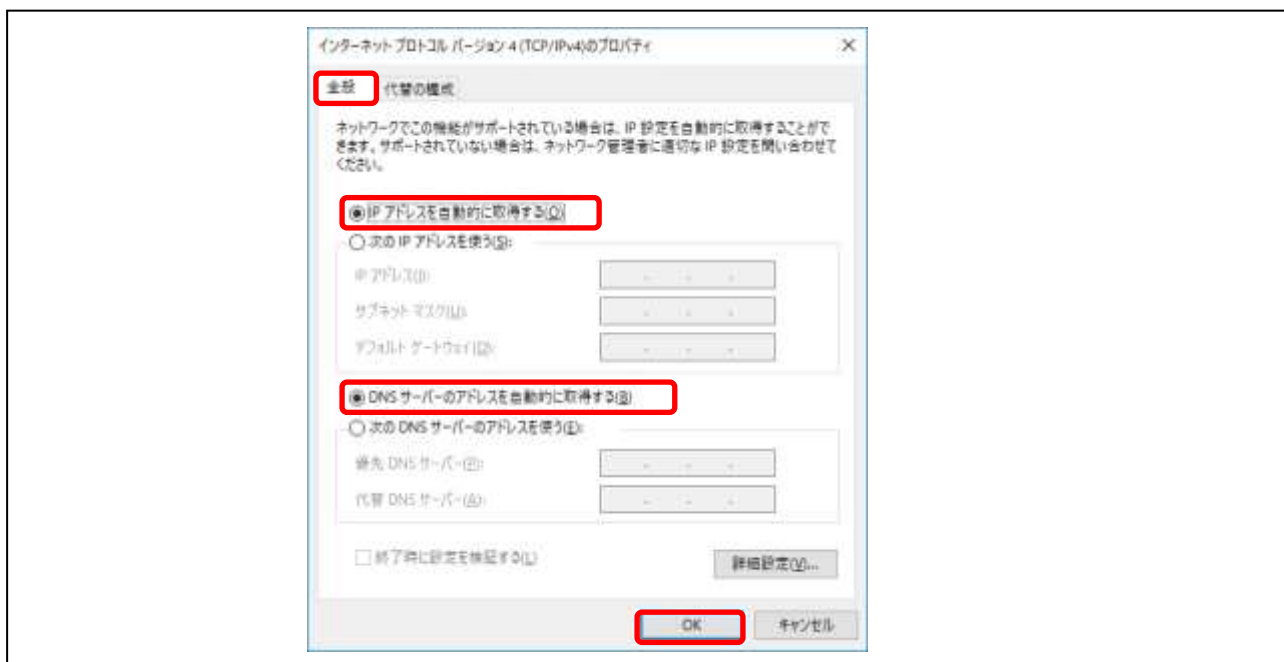


パソコンにログインしている場合は、管理者アカウントのパスワード入力が必要になります。

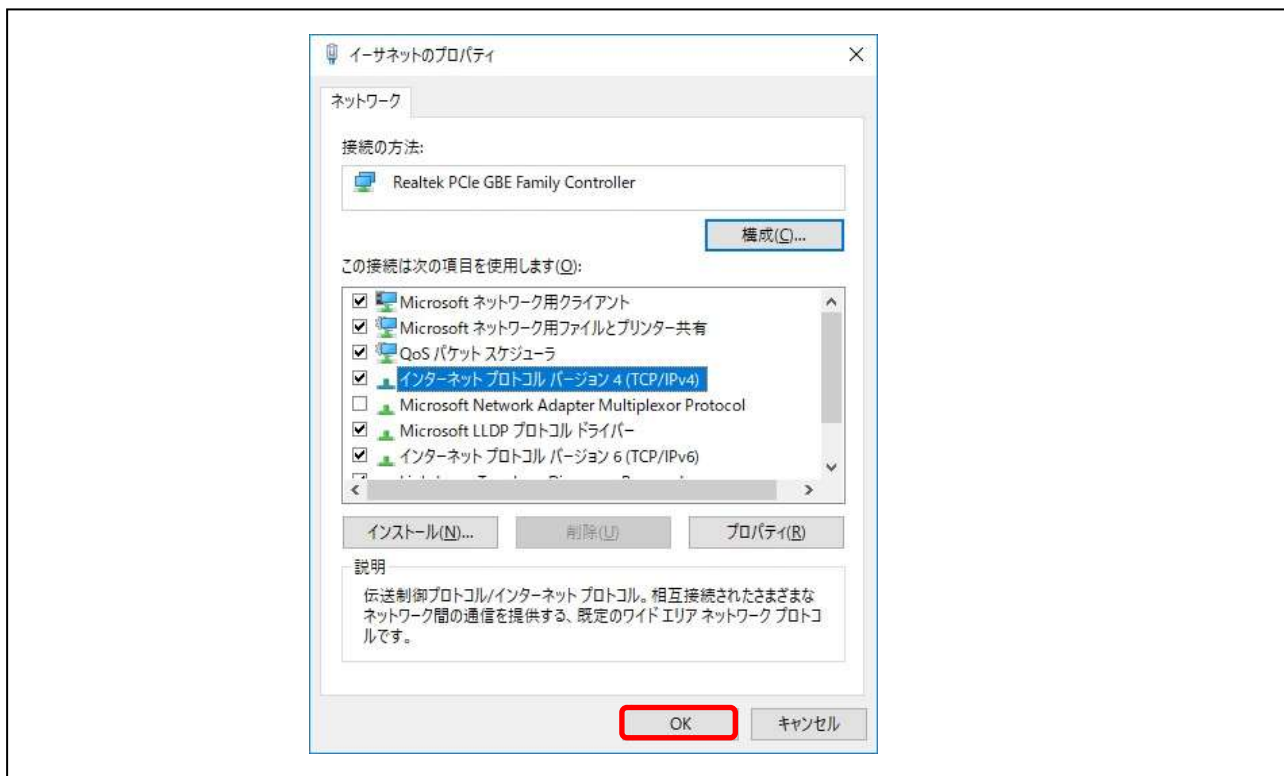
- (5) 「インターネットプロトコルバージョン 4(TCP/IPv4)」を選択します。
- (6) [プロパティ(R)]をクリックします。
- (7) [全般]タブをクリックします。
- (8) [IP アドレスを自動的に取得する(O)] のラジオボタンをチェックします。
- (9) [DNS サーバーのアドレスを自動的に取得する(B)]のラジオボタンをチェックします。

1. Web 設定の準備

- (10) [OK]をクリックして、【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】画面を閉じます。



- (11) [OK]または[閉じる]をクリックして、【イーサネットのプロパティ】の画面を閉じます。

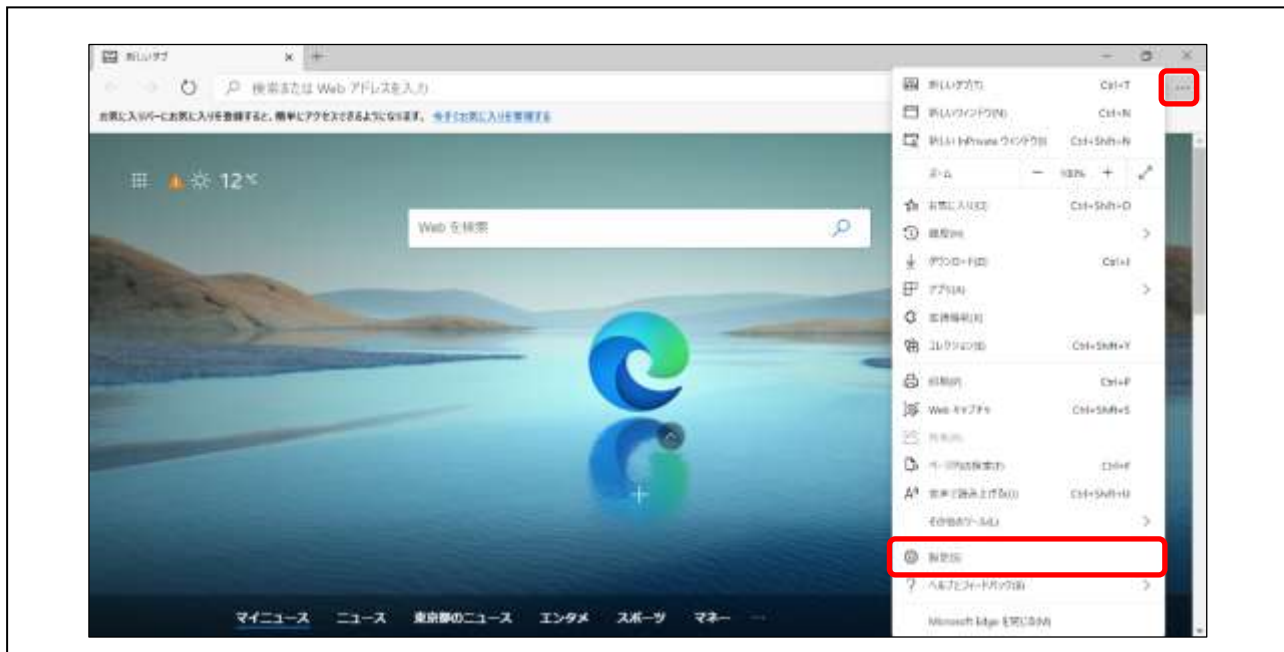


1. Web 設定の準備

1.2.6 パソコンのブラウザを設定する

☒ Microsoft Edge のバージョンにより、画面の表示内容が異なる場合があります。

- (1) パソコンで、Web ブラウザ(Microsoft Edge)を起動します。
- (2) Web ブラウザのメニュー[⋮]をクリックし、[設定]をクリックします。

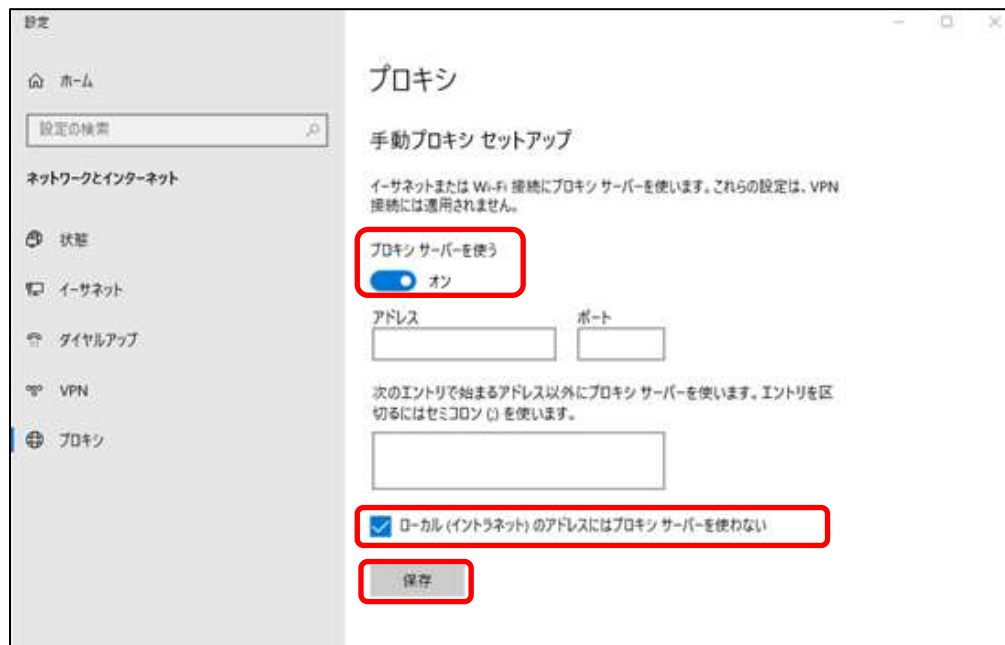
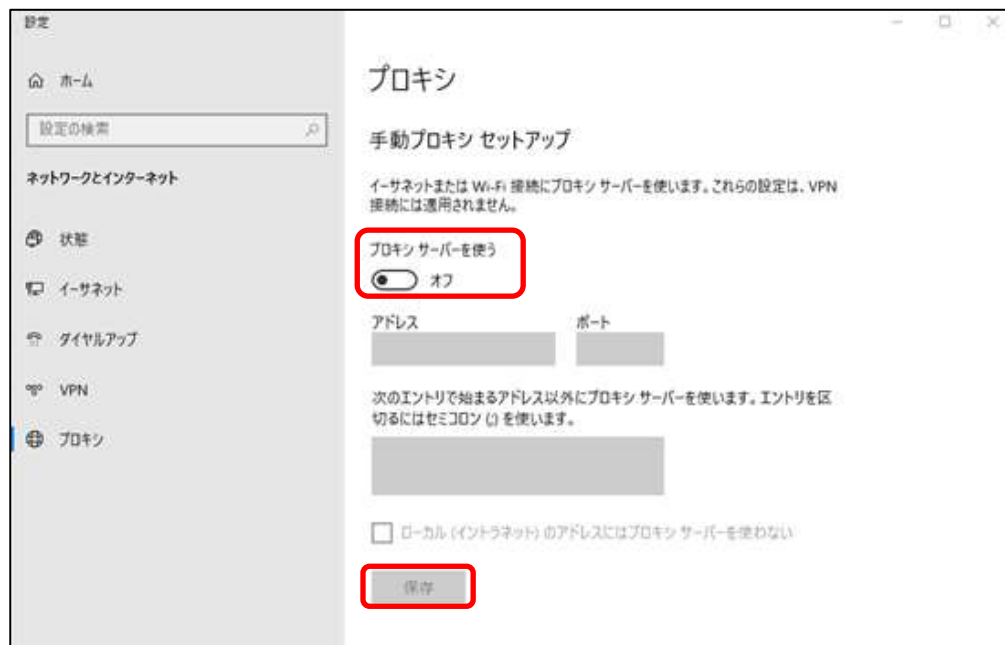


- (3) 設定メニューの[システムとパフォーマンス]をクリックし、[コンピューターのプロキシ設定を開く]をクリックします。



1. Web 設定の準備

- (4) [手動プロキシ セットアップ]を下方にスクロールし、[プロキシ サーバーを使う]を[オフ]にするか、[ローカル(イントラネット)のアドレスにはプロキシサーバーを使わない]にチェックして、[保存]をクリックしてください。

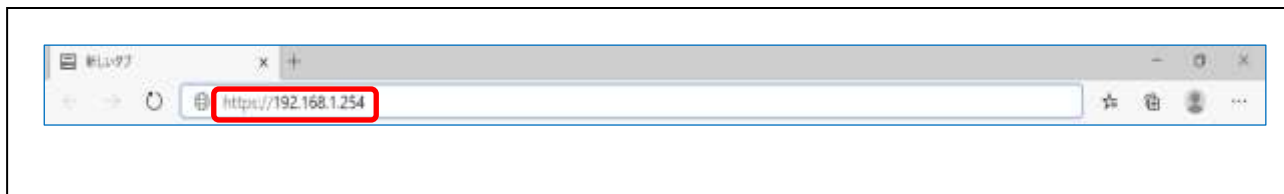


注意 本装置は Cookie を使用しています。「すべての Cookie をブロック」または「高」にすると、本装置で使用する Cookie がブロックされ、設定を行うことができません。

1. Web 設定の準備

1.2.7 Web 設定のトップページを開く

- (1) Web ブラウザのアドレスバーに半角英数字で「https://192.168.1.254/」と入力し、[Enter]キーを押します。



- ☒ 自己証明書を用いた方式のため、接続時にブラウザに「接続がプライベートではありません」、「プライバシーが保護されません」、「セキュリティ保護なし」などと表示されます。http と入力して接続することもできますが、通信内容が暗号化されないため、通信の安全性が低くなります。https での接続を推奨します。

1. Web 設定の準備

(2) Web 設定のトップページが表示されることを確認します。

■管理者メニュー	トップページ
トップページ	
ログイン	
■利用者メニュー	
装置状態の表示	
リンクマネージャ	
Wake on LAN	
■外部リンク	
製品ページ	

ルータの設定を開始します。以下のリンクから選択してください。
パスワードを登録・変更する前にユーザ名とパスワードを入力する画面が表示された場合は、そのまま「OK」をクリックしてください。

かんたん設定

- [インターネット接続](#)
フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用して、インターネットに接続する設定を行います。
- [インターネット接続+VPN接続](#)
フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用したインターネット接続と、インターネットVPNによる拠点間通信の設定を行います。
- [インターネット接続+フレッツ・VPNワイド接続](#)
フレッツ光を使用したインターネット接続と、フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
- [フレッツ・VPNワイド接続](#)
フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
- [NGN網VPN接続](#)
NGN網を用いたVPNによる拠点間の通信の設定と、NetMeisterによる装置管理の設定を行います。
- [IPv6 IPoE接続](#)
IPv6 IPoE接続の設定を行います。
プロバイダの動的IPまたは固定IPでのサービスを設定します。
- [クラウド接続](#)
インターネットVPNや専用線を使用したクラウド接続の設定を行います。
- [IP電話サービス接続](#)
対応するUNIVERGE Aspireシリーズと連携したIP電話ネットワークの設定を行います。

詳細設定

- [詳細設定](#)
各機能を詳細に設定します。
かんたん設定に含まれない設定を行う場合は、こちらから設定してください。

保守管理

- [保守管理](#)
装置状態の確認、ソフトウェアの更新、pingの実行など、各種保守機能の操作を行います。
- [Wake on LAN](#)
Wake on LAN機能を実行します。

1. Web 設定の準備

トップページを開けないときは

以下の点を確認し、対処してください。

- (1) パソコンと本装置が正しく接続されているかを確認してください。
- (2) パソコンを接続している LAN 側ポートが正しいかを確認してください。
IX2215 の場合は GE2、IX2310 の場合は GE3、IX3315 の場合は GE5 を使用します。
- (3) パソコンのコマンドプロンプトから本装置の LAN 側ポートに ping を実施して、通信できるかを確認してください。通信できない場合、ローカルエリア接続を[無効]にしたあと、再度、[有効]にすることで、IP アドレスの解放／再取得を行ってください。
- (4) 本章「1.2.6 パソコンのブラウザを設定する」にしたがって、パソコンのブラウザ設定が正しいかを確認してください。
- (5) Web 設定を行うための設定が正しく投入されているかを確認してください。

2. メニュー

2 メニュー

本章では、トップページやログイン/ログアウトの手順、設定の保存について説明します。

- 2.1 トップページ
- 2.2 ログインする
- 2.3 ログアウトする
- 2.4 設定の保存

2. メニュー

Web 設定画面の構成

Web 設定画面は、以下の4つのエリアで構成されています。

- ① 機種名エリア
- ② メニューエリア
- ③ メッセージエリア (ログイン時のみ表示)
- ④ 設定・表示エリア

メニューエリアをクリックすると、対応する画面が設定・表示エリアに表示されます。

メッセージエリアには、警告メッセージなどが表示されます(ログイン時のみ)

注意 本ページ以降に記載する画面イメージでは、①機種名エリアおよび②メニューエリアを省略している場合があります。

The screenshot shows the web management interface for a UNIVERGE IX2107 device. The interface is divided into several sections:

- 1** (Red circle): The top header area containing the device name "UNIVERGE IX2107".
- 2** (Green circle): The left sidebar menu containing various management options like "管理者メニュー", "かんたん設定", "詳細設定", etc.
- 3** (Red circle): A warning message box at the top right of the main content area, stating "!!注意!! 設定が変更されています。" (Warning: Settings have been changed).
- 4** (Green circle): The main content area displaying system and network information, including a status table for ports and WAN/VPN/UTM settings.

バージョン	稼働時間	稼働率	メモリ	内部温度	内部電圧
	1分	16%	18%	36.0℃	3.2508V

デバイス	接続状態	送信量	受信量
GE0 (GigaEthernet0)	全二重 1Gbpsで接続	0%	0%
GE1 (GigaEthernet1)	Port1: 接続されていません Port2: 接続されていません Port3: 接続されていません Port4: 全二重 1Gbpsで接続	0%	0%

接続名	接続状態	情報
WAN1: インターネット接続 (GigaEthernet0.1)	接続	IPアドレス: DNS:

接続名	接続状態	通信量[packets]
設定されていません		

ライセンス状態	ライセンス満了日時
設定されていません	

2. メニュー

2.1 トップページ

(1) メニューの[トップページ]をクリックします。

(2) トップページが表示されることを確認します。

☒ ログイン前とログイン後で、メニューエリアに表示される項目が異なります。

■ 管理者メニュー
トップページ
ログイン
■ 利用者メニュー
装置状態の表示
リンクマネージャ
Wake on LAN

■ 外部リンク
製品ページ

トップページ

ルータの設定を開始します。以下のリンクから選択してください。
パスワードを登録・変更する前にユーザ名とパスワードを入力する画面が表示された場合は、そのまま「OK」をクリックしてください。

かんたん設定

- [インターネット接続](#)
フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用して、インターネットに接続する設定を行います。
- [インターネット接続+VPN接続](#)
フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用したインターネット接続と、インターネットVPNによる拠点間通信の設定を行います。
- [インターネット接続+フレッツ・VPNワイド接続](#)
フレッツ光を使用したインターネット接続と、フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
- [フレッツ・VPNワイド接続](#)
フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
- [NGN網VPN接続](#)
NGN網を用いたVPNによる拠点間の通信の設定と、NetMeisterによる装置管理の設定を行います。
- [IPv6 IPoE接続](#)
IPv6 IPoE接続の設定を行います。
プロバイダの動的IPまたは固定IPでのサービスを設定します。
- [クラウド接続](#)
インターネットVPNや専用線を使用したクラウド接続の設定を行います。
- [IP電話サービス接続](#)
対応するUNIVERGE Aspireシリーズと連携したIP電話ネットワークの設定を行います。

詳細設定

- [詳細設定](#)
各機能を詳細に設定します。
かんたん設定に含まれない設定を行う場合は、こちらから設定してください。

保守管理

- [保守管理](#)
装置状態の確認、ソフトウェアの更新、pingの実行など、各種保守機能の操作を行います。
- [Wake on LAN](#)
Wake on LAN機能を実行します。

2. メニュー

2.2 ログインする

- (1) トップページメニューから[ログイン]、または、設定・表示エリアから設定したい項目のリンクをクリックします。

The screenshot shows the router's management interface. On the left is a navigation menu with categories: ■管理者メニュー (Administrator Menu), ■利用者メニュー (User Menu), and ■外部リンク (External Links). Under '管理者メニュー', 'ログイン' (Login) is highlighted with a red box. The main content area is titled 'トップページ' (Top Page) and contains instructions for logging in. Below this is a section titled 'かんたん設定' (Easy Setup) which is also enclosed in a red box. This section lists various connection options with brief descriptions: 'インターネット接続' (Internet Connection), 'インターネット接続+VPN接続' (Internet Connection + VPN Connection), 'インターネット接続+フレックツ・VPNワイド接続' (Internet Connection + FlexVPN Wide Connection), 'フレックツ・VPNワイド接続' (FlexVPN Wide Connection), 'NGN網VPN接続' (NGN Network VPN Connection), 'IPv6 IPoE接続' (IPv6 IPoE Connection), 'クラウド接続' (Cloud Connection), and 'IP電話サービス接続' (IP Phone Service Connection). Below the 'かんたん設定' section are two more sections: '詳細設定' (Detailed Settings) and '保守管理' (Maintenance Management), each with a list of links and brief descriptions.

■管理者メニュー	トップページ
トップページ	
ログイン	ルータの設定を開始します。以下のリンクから選択してください。 パスワードを登録・変更する前にユーザ名とパスワードを入力する画面が表示された場合は、 そのまま「OK」をクリックしてください。
■利用者メニュー	
装置状態の表示	
リンクマネージャ	
Wake on LAN	
■外部リンク	
製品ページ	

かんたん設定

- [インターネット接続](#)
フレックツ光などの有線回線やワイヤレス回線(3G・LTE)を使用して、インターネットに接続する設定を行います。
- [インターネット接続+VPN接続](#)
フレックツ光などの有線回線やワイヤレス回線(3G・LTE)を使用したインターネット接続と、インターネットVPNによる拠点間通信の設定を行います。
- [インターネット接続+フレックツ・VPNワイド接続](#)
フレックツ光を使用したインターネット接続と、フレックツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
- [フレックツ・VPNワイド接続](#)
フレックツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
- [NGN網VPN接続](#)
NGN網を用いたVPNによる拠点間の通信の設定と、NetMeisterによる装置管理の設定を行います。
- [IPv6 IPoE接続](#)
IPv6 IPoE接続の設定を行います。
プロバイダの動的IPまたは固定IPでのサービスを設定します。
- [クラウド接続](#)
インターネットVPNや専用線を使用したクラウド接続の設定を行います。
- [IP電話サービス接続](#)
対応するUNIVERGE Aspireシリーズと連携したIP電話ネットワークの設定を行います。

詳細設定

- [詳細設定](#)
各機能を詳細に設定します。
かんたん設定に含まれない設定を行う場合は、こちらから設定してください。

保守管理

- [保守管理](#)
装置状態の確認、ソフトウェアの更新、pingの実行など、各種保守機能の操作を行います。
- [Wake on LAN](#)
Wake on LAN機能を実行します。

2. メニュー

(2) ユーザ名とパスワードを入力する画面が表示されます。

“ユーザ名”と“パスワード”を入力し、[OK]ボタンをクリックします。

☒ パスワードを登録・変更する前にユーザ名とパスワードを入力する画面が表示された場合、そのまま[OK]をクリックしてください。

☒ Web 設定からパスワードを登録・変更した場合、ユーザ名の初期設定は「admin」です。

☒ パスワードは、かんたん設定、および詳細設定から変更可能です。



このサイトにアクセスするにはサインインしてください

http://host.ix-edu.nmddns.jp:11080 では認証が必要となります
このサイトへの接続は安全ではありません

ユーザ名

パスワード

2. メニュー

- (3) パスワードの設定画面が表示されますので、各項目を設定し、[反映]ボタンをクリックします。

- 管理者メニュー
 - ログアウト
- 詳細設定
 - パスワードの設定

!!注意!! パスワードが設定されていません。
『パスワードの設定』を行ってください。

パスワードの設定

管理者パスワードの設定

設定変更を行うためのパスワード設定を行います。

	現在の設定	設定の変更
ユーザ名	admin	変更できません
パスワード	パスワード設定なし	<input type="radio"/> パスワードを変更しない <input checked="" type="radio"/> パスワードを変更する <input type="text"/> 確認のためもう一度入力してください。 <input type="text"/> パスワードを入力してください。

利用者パスワードの設定

利用者メニューのためのパスワード設定を行います。
利用者ユーザを設定しない場合は、管理者ユーザでの認証となります。

	現在の設定	設定の変更
利用者ユーザ	設定なし	<input checked="" type="radio"/> 利用者ユーザを設定しない <input type="radio"/> 利用者ユーザを設定する

画面表示認証の設定

『装置状態の表示』に認証が必要かの設定を行います。

	現在の設定	設定の変更
認証の有無	不要	<input checked="" type="radio"/> 『装置状態の表示』は認証が不要 <input type="radio"/> 『装置状態の表示』に認証が必要

反映

2. メニュー

番号	項目	内容
①	ユーザ名	<p>本装置に管理者レベルの権限でログインするときのユーザを設定します。</p> <ul style="list-style-type: none"> 初期状態ではユーザ名は設定されていません。 パスワード設定後のユーザ名は「admin」です。Web 設定からは変更できません。
②	パスワード	<p>本装置にログインするときのパスワードを入力します。</p> <ul style="list-style-type: none"> 半角英数字で 1～249 文字まで入力できます。 セキュリティ性を向上させるため、パスワードの設定を強く推奨します。 <p>メモ</p> <ul style="list-style-type: none"> パスワードを変更し[反映]をクリックしたときだけ、設定したパスワードの強度評価が行われ、その結果が表示されます。 <ul style="list-style-type: none"> スコア:4 (非常に強い) スコア:3 (強い) スコア:2 (普通) スコア:1 (弱い) スコア:0 (非常に弱い) <p>注意</p> <ul style="list-style-type: none"> 大文字/小文字は区別されます。 パスワードの入力文字は表示されません。●●●のように伏せ文字で表示されます。 パスワードは、第三者に推測されにくく、忘れないような文字列を入力してください。
③	利用者ユーザ	<p>利用者メニューの「リンクマネージャ」と「Wake on LAN」機能だけを利用できるユーザを設定します。</p> <ul style="list-style-type: none"> 「利用者ユーザを設定する」が選択されている場合は、ユーザ名の表示とパスワードの設定画面が表示されます。 <p>ここで設定した利用者ユーザは、本装置にコマンドラインを使用してログインすることもできます。この場合、モニタレベル権限のユーザとなります。</p> <p>メモ</p> <ul style="list-style-type: none"> 後ほど詳細設定のパスワードの設定にて設定することができます。 利用者メニューの「リンクマネージャ」と「Wake on LAN」機能のメニューは下記をご参照ください。
④	認証の有無	<p>Web コンソール画面を起動した際に、セキュリティ性を高めるため、認証を要求できるように設定します。</p> <p>メモ</p> <ul style="list-style-type: none"> 後ほど詳細設定のパスワードの設定にて設定することができます。

参考：利用者メニューの「リンクマネージャ」と「Wake on LAN」のメニュー

<ul style="list-style-type: none"> ■ 管理者メニュー <ul style="list-style-type: none"> トップページ ログイン ■ 利用者メニュー <ul style="list-style-type: none"> 装置状態の表示 リンクマネージャ Wake on LAN ■ 外部リンク <ul style="list-style-type: none"> 製品ページ 	<p>トップページ</p> <p>ルータの設定を開始します。以下のリンクから選択してください。 パスワードを登録・変更する前にユーザ名とパスワードを入力する画面が表示された場合は、そのまま「OK」をクリックしてください。</p> <hr/> <p>かんたん設定</p> <ul style="list-style-type: none"> ● インターネット接続 フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用して、インターネットに接続する設定を行います。 ● インターネット接続+VPN接続
--	--

2. メニュー

(4) ログイン後のトップページが表示されることを確認します。

■ 管理者メニュー	
■ トップページ	!!注意!! 設定が変更されています。 再起動した場合、保存していない設定は元の状態に戻ります。 設定完了後は必ず「設定の保存」を行ってください。
■ 設定の保存	
■ ログアウト	
■ かんたん設定	トップページ
■ かんたん設定	ルータの設定を開始します。以下のリンクから選択してください。
■ 詳細設定	パスワードを登録・変更する前にユーザ名とパスワードを入力する画面が表示された場合は、そのまま「OK」をクリックしてください。
■ 詳細設定	
■ 端末管理	かんたん設定
■ 端末管理	
■ 保守管理	
■ 装置状態の表示	<ul style="list-style-type: none">● インターネット接続 フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用して、インターネットに接続する設定を行います。● インターネット接続+VPN接続 フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用したインターネット接続と、インターネットVPNによる拠点間通信の設定を行います。● インターネット接続+フレッツ・VPNワイド接続 フレッツ光を使用したインターネット接続と、フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。● フレッツ・VPNワイド接続 フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。● NGN網VPN接続 NGN網を用いたVPNによる拠点間の通信の設定と、NetMeisterによる装置管理の設定を行います。● IPv6 IPoE接続 IPv6 IPoE接続の設定を行います。 プロバイダの動的IPまたは固定IPでのサービスを設定します。● クラウド接続 インターネットVPNや専用線を使用したクラウド接続の設定を行います。● IP電話サービス接続 対応するUNIVERGE Aspireシリーズと連携したIP電話ネットワークの設定を行います。
■ 装置ログの取得	
■ 設定データの管理	
■ 設定の初期化	
■ ソフトウェアの更新	
■ pingの実行	
■ 任意コマンドの実行	
■ IP電話サービス保守	
■ URLオフロード	
■ リンクマネージャ	
■ Wake on LAN	
■ 再起動	
■ 拡張ページ	
■ 拡張ページ	
■ 外部リンク	
■ 製品ページ	
	詳細設定
	インタフェースやサーバのアドレスを指定したり、フィルタやQoS、VPN等、かんたん設定に含まれない詳細な設定を行う場合はこちらから設定してください。
	端末管理
	本装置に接続されている端末を管理します。 リンクマネージャ機能やWeb認証機能を設定します。
	保守管理
	装置状態の確認、ソフトウェアの更新、pingの実行など、各種保守機能の操作を行います。 URLオフロード機能による特定宛先のルーティング制御、 リンクマネージャ機能による端末の保守管理などが可能です。 任意のコマンドを直接実行したい場合は 任意コマンドの実行 から操作してください。

2. メニュー

強制ログイン画面について

本装置に同時にログインできるのは1ユーザまでです。

すでに本装置にログインしているユーザがいるときは、【強制ログイン】画面が表示されます。ログイン中のユーザを強制切断してログインする場合は、【強制ログイン実行】を押してください。

■ 管理者メニュー	強制ログイン
トップページ	
ログイン	既にログイン中のユーザがいます。
■ 利用者メニュー	同時にログインできるのは1ユーザまでです。
装置状態の表示	ログイン中のユーザを強制切断してログインする場合は【強制ログイン実行】を押してください。
リンクマネージャ	トップページへ 強制ログイン実行
Wake on LAN	
■ 外部リンク	
製品ページ	

ログインのロック中画面について

連続して3回ログインに失敗した場合、60秒間ロック状態となり、ログインができません。

60秒以上経過後、再度ログインを実行してください。

■ 管理者メニュー	ログインのロック中
トップページ	
ログイン	現在Webコンソールへのログインはロックされている為、ログインすることができませんでした。
■ 利用者メニュー	一定時間経過後にロックは解除されます。
装置状態の表示	[トップページへ]を押してお戻りください。
リンクマネージャ	トップページへ
Wake on LAN	
■ 外部リンク	
製品ページ	

2. メニュー

2.3 ログアウトする

(1) メニューエリアから[ログアウト]をクリックします。

■管理者メニュー	トップページ
トップページ	
設定の保存	
ログアウト	
■かんたん設定	
かんたん設定	
■詳細設定	かんたん設定
詳細設定	
■端末管理	
端末管理	
■保守管理	
装置状態の表示	
装置ログの取得	
設定データの管理	
設定の初期化	
ソフトウェアの更新	
pingの実行	
任意コマンドの実行	
IP電話サービス保守	
URLオフロード	
リンクマネージャ	
Wake on LAN	
再起動	
■拡張ページ	
拡張ページ	
■外部リンク	
製品ページ	

ルータの設定を開始します。以下のリンクから選択してください。
パスワードを登録・変更する前にユーザ名とパスワードを入力する画面が表示された場合は、そのまま「OK」をクリックしてください。

- [インターネット接続](#)
フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用して、インターネットに接続する設定を行います。
- [インターネット接続+VPN接続](#)
フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用したインターネット接続と、インターネットVPNによる拠点間通信の設定を行います。
- [インターネット接続+フレッツ・VPNワイド接続](#)
フレッツ光を使用したインターネット接続と、フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
- [フレッツ・VPNワイド接続](#)
フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
- [NGN網VPN接続](#)
NGN網を用いたVPNによる拠点間の通信の設定と、NetMeisterによる装置管理の設定を行います。
- [IPv6 IPoE接続](#)
IPv6 IPoE接続の設定を行います。
プロバイダの動的IPまたは固定IPでのサービスを設定します。
- [クラウド接続](#)
インターネットVPNや専用線を使用したクラウド接続の設定を行います。
- [IP電話サービス接続](#)
対応するUNIVERGE Aspireシリーズと連携したIP電話ネットワークの設定を行います。

詳細設定

インタフェースやサーバのアドレスを指定したり、フィルタやQoS、VPN等、かんたん設定に含まれない詳細な設定を行う場合はこちらから設定してください。

端末管理

本装置に接続されている端末を管理します。
リンクマネージャ機能やWeb認証機能を設定します。

保守管理

装置状態の確認、ソフトウェアの更新、pingの実行など、各種保守機能の操作を行います。
URLオフロード機能による特定宛先のルーティング制御、
リンクマネージャ機能による端末の保守管理などが可能です。
任意のコマンドを直接実行したい場合は[任意コマンドの実行](#)から操作してください。

2. メニュー

(2) [ログアウト実行]ボタンをクリックします。

ログアウト

ログアウトします。

よろしければ [ログアウト実行] を押してください。

ログアウト実行

(3) ログアウト後のトップページが表示されることを確認します。

■管理者メニュー	トップページ
トップページ	
ログイン	ルータの設定を開始します。以下のリンクから選択してください。
■利用者メニュー	パスワードを登録・変更する前にユーザ名とパスワードを入力する画面が表示された場合は、そのまま「OK」をクリックしてください。
装置状態の表示	
リンクマネージャ	
Wake on LAN	
■外部リンク	かんたん設定
製品ページ	

- [インターネット接続](#)
フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用して、インターネットに接続する設定を行います。
- [インターネット接続+VPN接続](#)
フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用したインターネット接続と、インターネットVPNによる拠点間通信の設定を行います。
- [インターネット接続+フレッツ・VPNワイド接続](#)
フレッツ光を使用したインターネット接続と、フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
- [フレッツ・VPNワイド接続](#)
フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
- [NGN網VPN接続](#)
NGN網を用いたVPNによる拠点間の通信の設定と、NetMeisterによる装置管理の設定を行います。
- [IPv6 IPoE接続](#)
IPv6 IPoE接続の設定を行います。
プロバイダの動的IPまたは固定IPでのサービスを設定します。
- [クラウド接続](#)
インターネットVPNや専用線を使用したクラウド接続の設定を行います。
- [IP電話サービス接続](#)
対応するUNIVERGE Aspireシリーズと連携したIP電話ネットワークの設定を行います。

詳細設定

- [詳細設定](#)
各機能を詳細に設定します。
かんたん設定に含まれない設定を行う場合は、こちらから設定してください。

保守管理

- [保守管理](#)
装置状態の確認、ソフトウェアの更新、pingの実行など、各種保守機能の操作を行います。
- [Wake on LAN](#)
Wake on LAN機能を実行します。

2. メニュー

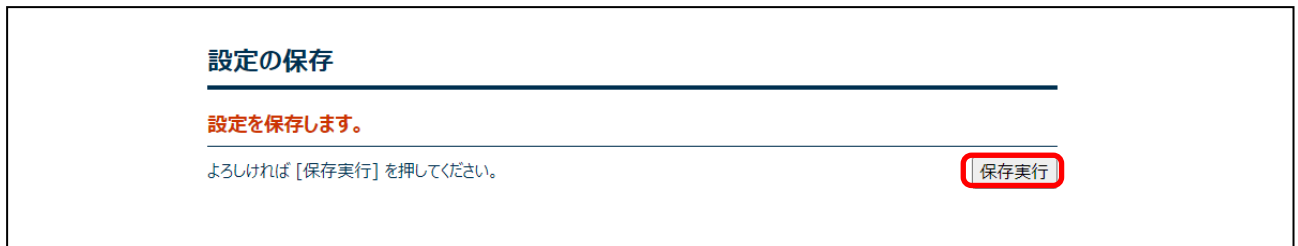
2.4 設定の保存

(1) ログイン後のメニューエリアから[設定の保存]をクリックします。

■管理者メニュー	トップページ
トップページ	
設定の保存	ルータの設定を開始します。以下のリンクから選択してください。
ログアウト	パスワードを登録・変更する前にユーザ名とパスワードを入力する画面が表示された場合は、そのまま「OK」をクリックしてください。
■かんたん設定	かんたん設定
かんたん設定	
■詳細設定	
詳細設定	
■端末管理	
端末管理	
■保守管理	
装置状態の表示	<ul style="list-style-type: none">• インターネット接続 フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用して、インターネットに接続する設定を行います。• インターネット接続+VPN接続 フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用したインターネット接続と、インターネットVPNによる拠点間通信の設定を行います。• インターネット接続+フレッツ・VPNワイド接続 フレッツ光を使用したインターネット接続と、フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。• フレッツ・VPNワイド接続 フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。• NGN網VPN接続 NGN網を用いたVPNによる拠点間の通信の設定と、NetMeisterによる装置管理の設定を行います。• IPv6 IPoE接続 IPv6 IPoE接続の設定を行います。 プロバイダの動的IPまたは固定IPでのサービスを設定します。• クラウド接続 インターネットVPNや専用線を使用したクラウド接続の設定を行います。• IP電話サービス接続 対応するUNIVERGE Aspireシリーズと連携したIP電話ネットワークの設定を行います。
装置ログの取得	
設定データの管理	
設定の初期化	
ソフトウェアの更新	
pingの実行	
任意コマンドの実行	
IP電話サービス保守	
URLオフロード	
リンクマネージャ	
Wake on LAN	
再起動	
■拡張ページ	
拡張ページ	
■外部リンク	
製品ページ	
	詳細設定
	インタフェースやサーバのアドレスを指定したり、フィルタやQoS、VPN等、かんたん設定に含まれない詳細な設定を行う場合はこちらから設定してください。
	端末管理
	本装置に接続されている端末を管理します。 リンクマネージャ機能やWeb認証機能を設定します。
	保守管理
	装置状態の確認、ソフトウェアの更新、pingの実行など、各種保守機能の操作を行います。 URLオフロード機能による特定宛先のルーティング制御、 リンクマネージャ機能による端末の保守管理などが可能です。 任意のコマンドを直接実行したい場合は 任意コマンドの実行 から操作してください。

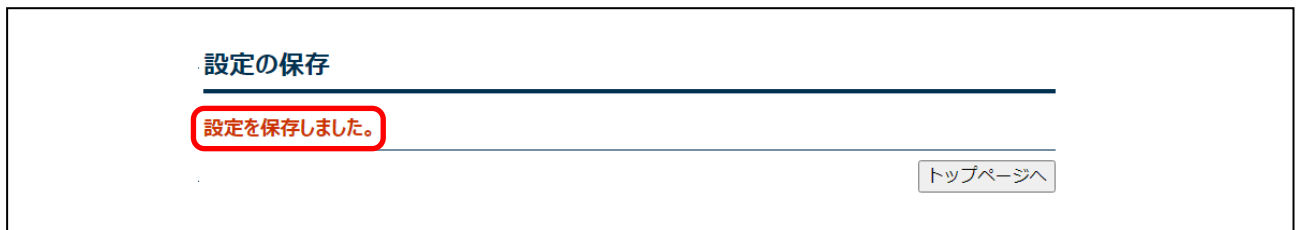
2. メニュー

(2) [保存実行]ボタンをクリックします。



The screenshot shows a page titled "設定の保存" (Save Settings). Below the title is a horizontal line. The text "設定を保存します。" (Save settings.) is displayed in red. Below this is the instruction "よろしければ [保存実行] を押してください。" (If you are satisfied, please press [Save].). On the right side of the page, there is a button labeled "保存実行" (Save), which is highlighted with a red rectangular box.

(3) 「設定を保存しました。」のメッセージを確認します。



The screenshot shows the same page as in step 2, but now the message "設定を保存しました。" (Settings saved.) is displayed in red and highlighted with a red rectangular box. The "保存実行" button is no longer visible. A new button labeled "トップページへ" (Back to top page) is located at the bottom right of the page.

3. かんたん設定

3 かんたん設定

本章では、ウィザードの流れにしたがってパラメータの入力、選択を行うことで、インターネット接続やVPN・クラウド接続などのネットワークを構築することができる『かんたん設定』について説明します。かんたん設定では、以下の設定を行うことができます。

- 3.1 インターネット接続
- 3.2 インターネット接続+VPN 接続
- 3.3 インターネット接続+フレッツ・VPN ワイド接続
- 3.4 フレッツ・VPN ワイド接続
- 3.5 NGN VPN 接続
 - NetMeister の事前登録
 - NGN VPN 接続の設定
 - センタの場合の設定
 - 拠点の場合の設定
- 3.6 IPv6 IPoE 接続
- 3.7 クラウド接続
- 3.8 IP 電話サービス接続

注意 かんたん設定を行う前に、コマンドによる設定や詳細設定が行われている場合、かんたん設定が正しく反映されないことがあります。既に設定されている場合は、あらかじめ「設定の初期化」を行ってください。

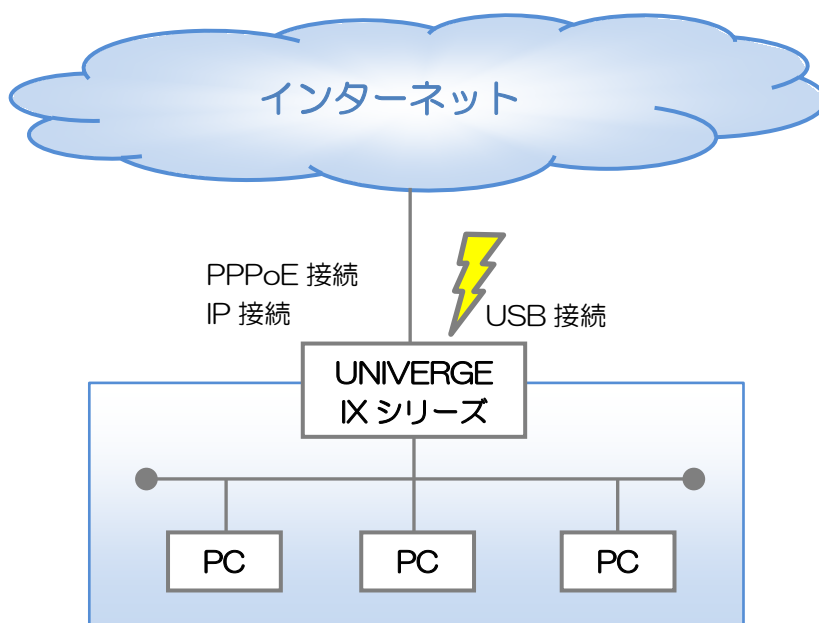
メモ IX2107/IX2235/IX2310 の場合、ゼロタッチプロビジョニングモードが ON（装置前面の MODE スイッチが ON）に設定されていると、かんたん設定を利用できません。ゼロタッチプロビジョニング機能は利用せず、かんたん設定を利用する場合は、MODE スイッチを OFF に設定してください。MODE スイッチの設定を変更したときは、装置を再起動してください。
工場出荷時は、MODE スイッチは ON に設定されています。

3. かんたん設定

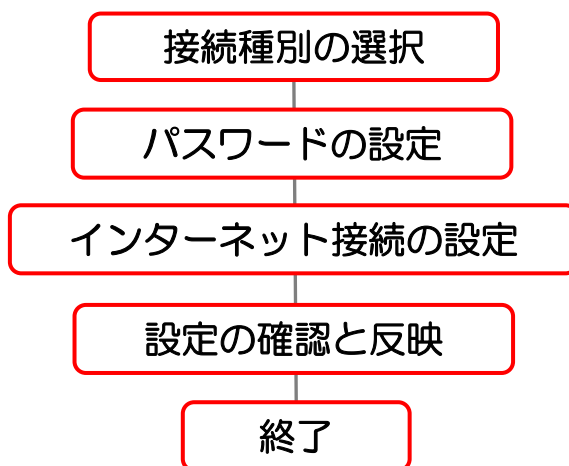
3.1 インターネット接続

フレッツ光などの有線回線やモバイル回線(3G・LTE)を使用して、インターネットに接続する設定を行います。

【構成イメージ】



【設定手順】



3. かんたん設定

(1) ログイン後のメニューエリアから[かんたん設定]をクリックします。

メモ トップページリンクをクリックすることで、接続種別の各ページに移動することも可能です。

The screenshot shows the router's management interface. On the left is a navigation menu with categories: ■管理者メニュー (Administrator Menu), ■かんたん設定 (Easy Setup), ■詳細設定 (Advanced Settings), ■端末管理 (Device Management), ■保守管理 (Maintenance Management), ■拡張ページ (Extension Pages), and ■外部リンク (External Links). The 'かんたん設定' menu item is highlighted with a red box. A red-bordered warning box at the top right contains the text: '!!注意!! 設定が変更されています。再起動した場合、保存していない設定は元の状態に戻ります。設定完了後は必ず『設定の保存』を行ってください。' (Attention!! Settings have been changed. If you restart, settings not saved will return to the original state. After completion, please always save settings.) Below the menu, the 'かんたん設定' (Easy Setup) page is displayed. It has a sub-header 'かんたん設定' and a red box around the 'インターネット接続' (Internet Connection) link. The main content lists several connection options: 'インターネット接続' (Internet Connection), 'インターネット接続+VPN接続' (Internet Connection + VPN Connection), 'インターネット接続+フレッツ・VPNワイド接続' (Internet Connection + Flets-VPN Wide Connection), 'フレッツ・VPNワイド接続' (Flets-VPN Wide Connection), 'NGN網VPN接続' (NGN Network VPN Connection), 'IPv6 IPoE接続' (IPv6 IPoE Connection), 'クラウド接続' (Cloud Connection), and 'IP電話サービス接続' (IP Phone Service Connection). Each option includes a brief description of the connection method. Below this list are sections for '詳細設定' (Advanced Settings), '端末管理' (Device Management), and '保守管理' (Maintenance Management), each with a short introductory paragraph.

3. かんたん設定

(2) 接続種別の選択で「インターネット接続」にチェックを入れ、[次へ]ボタンをクリックします。

メモ 接続種別を変更する場合には、設定の初期化が必要となります。

かんたん設定：接続種別の選択

接続種別を選択してかんたん設定を開始してください。
接続種別を変更する場合には「設定の初期化」が必要となります。

	現在の設定	設定の変更
接続種別の選択	不明なインターネット接続	<input checked="" type="radio"/> インターネット接続 フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用して、インターネットに接続する設定を行います。
		<input type="radio"/> インターネット接続 + VPN接続 フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用したインターネット接続と、インターネットVPNによる拠点間通信の設定を行います。
		<input type="radio"/> インターネット接続 + フレッツ・VPNワイド接続 フレッツ光を使用したインターネット接続と、フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
		<input type="radio"/> フレッツ・VPNワイド接続 フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
		<input type="radio"/> NGN網VPN接続 NGN網を用いたVPNによる拠点間の通信の設定とNetMeisterによる装置管理の設定を行います。
		<input type="radio"/> IPv6 IPoE接続 IPv6 IPoE接続の設定を行います。 プロバイダの動的IPまたは固定IPでのサービスを設定します。
		<input type="radio"/> クラウド接続 インターネットVPNや専用線を使用したクラウド接続の設定を行います。
		<input type="radio"/> IP電話サービス接続 対応するUNIVERGE Aspireシリーズと連携したIP電話ネットワークの設定を行います。

次へ

3. かんたん設定

(3) 管理者パスワードを変更する場合は、[パスワードを変更する]を選択し、パスワードを設定した後、[次へ]ボタンをクリックします。

メモ 管理者パスワードを変更する必要が無い場合は、そのまま[次へ]ボタンをクリックします。

メモ 接続種別の選択に戻る場合は、[戻る]ボタンをクリックしてください。

1. パスワードの設定 → 2. インターネット接続の設定 → 3. NetMeisterの設定 → 4. 設定の確認と反映
→ 5. 終了

かんたん設定：パスワードの設定

ログイン認証用のパスワードを設定します。

	現在の設定	設定の変更
ユーザ名	admin	変更できません
パスワード	パスワード設定なし	<input type="radio"/> パスワードを変更しない <input checked="" type="radio"/> パスワードを変更する <input type="text"/> 確認のためもう一度入力してください。 <input type="text"/> パスワードを入力してください。

戻る **次へ**

番号	項目	内容
①	ユーザ名	本装置にログインするときのユーザ名です。 ・初期状態ではユーザ名は設定されていません。 ・パスワード設定後のユーザ名は「admin」です。Web 設定からは変更できません。
②	パスワード	本装置にログインするときのパスワードです。 ・初期状態ではパスワードは設定されていません。 ・半角英数字で 1~249 文字まで入力できます。 注意 ・大文字/小文字は区別されます。 ・パスワードの入力文字は表示されません。●●●のように伏せ文字で表示されます。 ・パスワードは、第三者に推測されにくく、忘れないような文字列を入力してください。

3. かんたん設定

(4) [インターネット接続の設定]の各項目を設定し、[設定の確認]ボタンをクリックします。

パスワードの設定に戻る場合は、[戻る]ボタンをクリックしてください。

PPPoE 接続の場合(フレッツ光回線利用の場合)

1. パスワードの設定 → 2. インターネット接続の設定 → 3. NetMeisterの設定 → 4. 設定の確認と反映 → 5. 終了

かんたん設定：インターネット接続の設定

プロバイダと接続するWAN側インタフェースを設定します。

	現在の設定	設定の変更
接続形態		<input checked="" type="radio"/> PPPoE接続 (フレッツ光回線利用の場合) <input type="radio"/> IP接続 (ケーブルテレビ回線利用の場合)
WAN1: PPPoE接続の設定(GigaEthernet0.1)		
	現在の設定	設定の変更
ユーザ名		プロバイダから通知されているユーザ名を設定します。 (フレッツの場合、通常はユーザ名には@を含んでいます) <input type="text"/> 文字列(半角英数字)を入力してください。
パスワード		プロバイダから通知されているパスワードを設定します。 <input type="text"/> 文字列(半角英数字)を入力してください。
WAN側IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
DNSアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
通信セキュリティの設定		
	現在の設定	設定の変更
セキュリティ強度	レベル1	<input checked="" type="radio"/> レベル1 - 外部からの不要なパケットをNAPTにより廃棄します。 <input type="radio"/> レベル2 - 外部からの不要なパケットをNAPTにより廃棄します。 - 内部からの不要な通信を制限します。
LAN1: LANの設定(GigaEthernet1.0)		
LAN側IPアドレスを変更する場合は、反映後に新しいIPアドレスで接続しなおす必要があります。		
	現在の設定	設定の変更
LAN側IPアドレス	192.168.100.1/24	<input type="text" value="192.168.1.254"/> / <input type="text" value="24"/>

3. かんたん設定

番号	項目	内容
①	接続形態	「PPPoE 接続（フレッツ光回線利用の場合）」を選択します。
②	ユーザ名	プロバイダから通知されているユーザ名を設定します。 (フレッツの場合、通常はユーザ名には@を含んでいます) ・ 半角英数字で 1～59 文字まで入力できます。
③	パスワード	プロバイダから通知されているパスワードを設定します。 ・ 半角英数字で 1～79 文字まで入力できます。 注意 大文字、小文字も区別されます。
④	WAN 側 IP アドレス	PPPoE 接続の WAN 側 IP アドレスを設定します。 ・ プロバイダから WAN 側 IP アドレスが与えられていないときは「自動取得」を、固定 IP アドレスが与えられているときは「手動設定」を選択します。 ・ 「手動設定」を選択したときは、プロバイダから与えられた IP アドレスを入力し、サブネットマスクをプルダウンメニューから選択します。 注意 ・ 他のインターフェースに設定されている IP アドレスを使用することはできません。 ・ 「自動取得」を選択した場合、IP アドレスを入力することはできません。
⑤	DNS アドレス	PPPoE 接続の DNS サーバのアドレスを設定します。 ・ プロバイダから DNS サーバのアドレスが与えられていないときは「自動取得」を、与えられているとき、または独自に指定するときは「手動設定」を選択します。 ・ 「手動設定」を選択したときは、プロバイダから与えられたプライマリ DNS サーバの IP アドレスを上段に、セカンダリ DNS サーバの IP アドレスを下段に入力します。セカンダリは省略可能です。 注意 ・ 「自動取得」を選択した場合、DNS アドレスを入力することはできません。

3. かんたん設定

⑥	セキュリティ強度	<p>通信セキュリティの強度を設定します。</p> <ul style="list-style-type: none"> 外部からの不要なパケットをNAPTにより廃棄する場合は「レベル 1」を選択します。 外部からの不要なパケットをNAPTにより廃棄し、さらに内部からの不要な通信を制限する場合は、「レベル 2」を選択します。 <p>「レベル 2」を選択したときは、送信時に以下に該当する通信を廃棄します。</p> <table border="1" data-bbox="587 383 1197 947"> <tr> <td rowspan="4">宛先 IP アドレス</td> <td>0.0.0.0/8</td> </tr> <tr> <td>127.0.0.0/8</td> </tr> <tr> <td>169.254.0.0/16</td> </tr> <tr> <td>224.0.0.0/4</td> </tr> <tr> <td rowspan="5">宛先ポート番号</td> <td>135</td> </tr> <tr> <td>137</td> </tr> <tr> <td>138</td> </tr> <tr> <td>139</td> </tr> <tr> <td>445</td> </tr> <tr> <td rowspan="5">送信元ポート番号</td> <td>135</td> </tr> <tr> <td>137</td> </tr> <tr> <td>138</td> </tr> <tr> <td>139</td> </tr> <tr> <td>445</td> </tr> </table> <p>メモセキュリティ強度は、以下を参照してください。</p> <table border="1" data-bbox="587 1021 1420 1144"> <tr> <td>レベル 1 (オフ)</td> <td>NAPT により外部からのパケットを廃棄します。</td> </tr> <tr> <td>レベル 2 (標準)</td> <td>NAPT による外部からのパケット廃棄に加えて、送信フィルタにより、内部からの通信を制限します。</td> </tr> </table>	宛先 IP アドレス	0.0.0.0/8	127.0.0.0/8	169.254.0.0/16	224.0.0.0/4	宛先ポート番号	135	137	138	139	445	送信元ポート番号	135	137	138	139	445	レベル 1 (オフ)	NAPT により外部からのパケットを廃棄します。	レベル 2 (標準)	NAPT による外部からのパケット廃棄に加えて、送信フィルタにより、内部からの通信を制限します。
宛先 IP アドレス	0.0.0.0/8																						
	127.0.0.0/8																						
	169.254.0.0/16																						
	224.0.0.0/4																						
宛先ポート番号	135																						
	137																						
	138																						
	139																						
	445																						
送信元ポート番号	135																						
	137																						
	138																						
	139																						
	445																						
レベル 1 (オフ)	NAPT により外部からのパケットを廃棄します。																						
レベル 2 (標準)	NAPT による外部からのパケット廃棄に加えて、送信フィルタにより、内部からの通信を制限します。																						
⑦	LAN 側 IP アドレス	<p>LAN 側 IP アドレスを設定します。</p> <p>IP アドレスを変更する場合、現在の接続は切断されます。新しい IP アドレスに接続しなおしてください。</p>																					

3. かんたん設定

IP 接続の場合(ケーブルテレビ回線利用の場合)

1. パスワードの設定 → 2. インターネット接続の設定 → 3. NetMeisterの設定 → 4. 設定の確認と反映
→ 5. 終了

かんたん設定：インターネット接続の設定

プロバイダと接続するWAN側インタフェースを設定します。

	現在の設定	設定の変更
接続形態		<input type="radio"/> PPPoE接続 (フレッツ光回線利用の場合) <input checked="" type="radio"/> IP接続 (ケーブルテレビ回線利用の場合)
WAN1: IP接続の設定(GigaEthernet0.0)		
	現在の設定	設定の変更
WAN側IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
DNSアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
通信セキュリティの設定		
	現在の設定	設定の変更
セキュリティ強度	レベル1	<input checked="" type="radio"/> レベル1 - 外部からの不要なパケットをNAPTにより廃棄します。 <input type="radio"/> レベル2 - 外部からの不要なパケットをNAPTにより廃棄します。 - 内部からの不要な通信を制限します。
LAN1: LANの設定(GigaEthernet1.0)		
LAN側IPアドレスを変更する場合は、反映後に新しいIPアドレスで接続しなおす必要があります。		
	現在の設定	設定の変更
LAN側IPアドレス	192.168.100.1/24	192.168.1.254 / 24 ▼

3. かんたん設定

番号	項目	内容																					
①	接続形態	「IP 接続 (ケーブルテレビ回線利用の場合)」を選択します。																					
②	WAN 側 IP アドレス	<p>IP 接続の WAN 側 IP アドレスを設定します。</p> <ul style="list-style-type: none"> プロバイダから WAN 側 IP アドレスが与えられていないときは「自動取得」を、固定 IP アドレスが与えられているときは「手動設定」を選択します。 「手動設定」を選択したときは、プロバイダから与えられた IP アドレスを入力し、サブネットマスクをプルダウンメニューから選択します。 <p>注意</p> <ul style="list-style-type: none"> 他のインタフェースに設定されている IP アドレスを使用することはできません。 「自動取得」を選択した場合、IP アドレスを入力することはできません。 																					
③	DNS アドレス	<p>IP 接続の DNS サーバのアドレスを設定します。</p> <ul style="list-style-type: none"> プロバイダから DNS サーバのアドレスが与えられていないときは「自動取得」を、与えられているとき、または独自に指定するときは「手動設定」を選択します。 「手動設定」を選択したときは、プロバイダから与えられたプライマリ DNS サーバの IP アドレスを上段に、セカンダリ DNS サーバの IP アドレスを下段に入力します。セカンダリは省略可能です。 <p>注意</p> <ul style="list-style-type: none"> 「自動取得」を選択した場合、DNS アドレスを入力することはできません。 																					
④	セキュリティ強度	<p>通信セキュリティの強度を設定します。</p> <ul style="list-style-type: none"> 外部からの不要なパケットを NATP により廃棄する場合は「レベル 1」を選択します。 外部からの不要なパケットを NATP により廃棄し、さらに内部からの不要な通信を制限する場合は、「レベル 2」を選択します。 <p>「レベル 2」を選択したときは、送信時に以下に該当する通信を廃棄します。</p> <table border="1" data-bbox="588 1086 1198 1659"> <tbody> <tr> <td rowspan="4">宛先 IP アドレス</td> <td>0.0.0.0/8</td> </tr> <tr> <td>127.0.0.0/8</td> </tr> <tr> <td>169.254.0.0/16</td> </tr> <tr> <td>224.0.0.0/4</td> </tr> <tr> <td rowspan="5">宛先ポート番号</td> <td>135</td> </tr> <tr> <td>137</td> </tr> <tr> <td>138</td> </tr> <tr> <td>139</td> </tr> <tr> <td>445</td> </tr> <tr> <td rowspan="5">送信元ポート番号</td> <td>135</td> </tr> <tr> <td>137</td> </tr> <tr> <td>138</td> </tr> <tr> <td>139</td> </tr> <tr> <td>445</td> </tr> </tbody> </table> <p>メモセキュリティ強度は、以下を参照してください。</p> <table border="1" data-bbox="588 1736 1422 1856"> <tbody> <tr> <td>レベル 1 (オフ)</td> <td>NAPT により外部からのパケットを廃棄します。</td> </tr> <tr> <td>レベル 2 (標準)</td> <td>NAPT による外部からのパケット廃棄に加えて、送信フィルタにより、内部からの通信を制限します。</td> </tr> </tbody> </table>	宛先 IP アドレス	0.0.0.0/8	127.0.0.0/8	169.254.0.0/16	224.0.0.0/4	宛先ポート番号	135	137	138	139	445	送信元ポート番号	135	137	138	139	445	レベル 1 (オフ)	NAPT により外部からのパケットを廃棄します。	レベル 2 (標準)	NAPT による外部からのパケット廃棄に加えて、送信フィルタにより、内部からの通信を制限します。
宛先 IP アドレス	0.0.0.0/8																						
	127.0.0.0/8																						
	169.254.0.0/16																						
	224.0.0.0/4																						
宛先ポート番号	135																						
	137																						
	138																						
	139																						
	445																						
送信元ポート番号	135																						
	137																						
	138																						
	139																						
	445																						
レベル 1 (オフ)	NAPT により外部からのパケットを廃棄します。																						
レベル 2 (標準)	NAPT による外部からのパケット廃棄に加えて、送信フィルタにより、内部からの通信を制限します。																						
⑤	LAN 側 IP アドレス	<p>LAN 側 IP アドレスを設定します。</p> <p>IP アドレスを変更する場合、現在の接続は切断されます。新しい IP アドレスに接続しなおしてください。</p>																					

3. かんたん設定

USB 接続の場合(3G・LTE 回線利用の場合)

※IX2215/IX2235/IX2310/IX3315 のみ

1. パスワードの設定 → 2. インターネット接続の設定 → 3. NetMeisterの設定 → 4. 設定の確認と反映 → 5. 終了

かんたん設定：インターネット接続の設定

プロバイダと接続するWAN側インタフェースを設定します。

	現在の設定	設定の変更
接続形態		<input type="radio"/> PPPoE接続 (フレッツ光回線利用の場合) <input type="radio"/> IP接続 (ケーブルテレビ回線利用の場合) <input checked="" type="radio"/> USB接続 (3G・LTE回線利用の場合)
WAN1: USB接続の設定(USB-Serial0.0)		
	現在の設定	設定の変更
ユーザ名		プロバイダからユーザ名が指定されている場合に設定します。 <input type="text"/>
パスワード		プロバイダからパスワードが指定されている場合に設定します。 <input type="text"/>
PDPタイプ		プロバイダからPDPタイプが指定されている場合に設定します。 -- ▾
APN		プロバイダからAPNが指定されている場合に設定します。 <input type="text"/>
WAN側IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
DNSアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
通信セキュリティの設定		
	現在の設定	設定の変更
セキュリティ強度	レベル1	<input checked="" type="radio"/> レベル1 - 外部からの不要なパケットをNAPTにより廃棄します。 <input type="radio"/> レベル2 - 外部からの不要なパケットをNAPTにより廃棄します。 - 内部からの不要な通信を制限します。
LAN1: LANの設定(GigaEthernet2.0)		
LAN側IPアドレスを変更する場合は、反映後に新しいIPアドレスで接続しなおす必要があります。		
	現在の設定	設定の変更
LAN側IPアドレス	192.168.100.254/24	<input type="text" value="192.168.100.254"/> / <input type="text" value="24"/>

3. かんたん設定

番号	項目	内容
①	接続形態	「USB 接続 (3G・LTE 回線利用の場合)」を選択します。
②	ユーザ名	プロバイダからユーザ名が指定されている場合に設定します。 ・ 半角英数字で 1～59 文字まで入力できます。
③	パスワード	プロバイダからパスワードが指定されている場合に設定します。 ・ 半角英数字で 1～79 文字まで入力できます。 注意 ・ 大文字、小文字も区別されます。
④	PDP タイプ	プロバイダから PDP タイプが指定されている場合に設定します。
⑤	APN	プロバイダから APN が指定されている場合に設定します。 ・ 半角英数字で 1～90 文字まで入力できます。
⑥	WAN 側 IP アドレス	USB 接続の WAN 側 IP アドレスを設定します。 ・ プロバイダから WAN 側 IP アドレスが与えられていないときは「自動取得」を、固定 IP アドレスが与えられているときは「手動設定」を選択します。 ・ 「手動設定」を選択したときは、プロバイダから与えられた IP アドレスを入力し、サブネットマスクをプルダウンメニューから選択します。 注意 ・ 他のインターフェースに設定されている IP アドレスを使用することはできません。 ・ 「自動取得」を選択した場合、IP アドレスを入力することはできません。
⑦	DNS アドレス	USB 接続の DNS サーバのアドレスを設定します。 ・ プロバイダから DNS サーバのアドレスが与えられていないときは「自動取得」を、与えられているとき、または独自に指定するときは「手動設定」を選択します。 ・ 「手動設定」を選択したときは、プロバイダから与えられたプライマリ DNS サーバの IP アドレスを上段に、セカンダリ DNS サーバの IP アドレスを下段に入力します。セカンダリは省略可能です。 注意 ・ 「自動取得」を選択した場合、DNS アドレスを入力することはできません。

3. かんたん設定

⑧	セキュリティ強度	<p>通信セキュリティの強度を設定します。</p> <ul style="list-style-type: none"> 外部からの不要なパケットをNAPTにより廃棄する場合は「レベル 1」を選択します。 外部からの不要なパケットをNAPTにより廃棄し、さらに内部からの不要な通信を制限する場合は、「レベル 2」を選択します。 <p>「レベル 2」を選択したときは、送信時に以下に該当する通信を廃棄します。</p> <table border="1" data-bbox="590 383 1200 947"> <tr> <td rowspan="4">宛先 IP アドレス</td> <td>0.0.0.0/8</td> </tr> <tr> <td>127.0.0.0/8</td> </tr> <tr> <td>169.254.0.0/16</td> </tr> <tr> <td>224.0.0.0/4</td> </tr> <tr> <td rowspan="5">宛先ポート番号</td> <td>135</td> </tr> <tr> <td>137</td> </tr> <tr> <td>138</td> </tr> <tr> <td>139</td> </tr> <tr> <td>445</td> </tr> <tr> <td rowspan="5">送信元ポート番号</td> <td>135</td> </tr> <tr> <td>137</td> </tr> <tr> <td>138</td> </tr> <tr> <td>139</td> </tr> <tr> <td>445</td> </tr> </table> <p>メモセキュリティ強度は、以下を参照してください。</p> <table border="1" data-bbox="590 1021 1423 1144"> <tr> <td>レベル 1 (オフ)</td> <td>NAPT により外部からのパケットを廃棄します。</td> </tr> <tr> <td>レベル 2 (標準)</td> <td>NAPT による外部からのパケット廃棄に加えて、送信フィルタにより、内部からの通信を制限します。</td> </tr> </table>	宛先 IP アドレス	0.0.0.0/8	127.0.0.0/8	169.254.0.0/16	224.0.0.0/4	宛先ポート番号	135	137	138	139	445	送信元ポート番号	135	137	138	139	445	レベル 1 (オフ)	NAPT により外部からのパケットを廃棄します。	レベル 2 (標準)	NAPT による外部からのパケット廃棄に加えて、送信フィルタにより、内部からの通信を制限します。
宛先 IP アドレス	0.0.0.0/8																						
	127.0.0.0/8																						
	169.254.0.0/16																						
	224.0.0.0/4																						
宛先ポート番号	135																						
	137																						
	138																						
	139																						
	445																						
送信元ポート番号	135																						
	137																						
	138																						
	139																						
	445																						
レベル 1 (オフ)	NAPT により外部からのパケットを廃棄します。																						
レベル 2 (標準)	NAPT による外部からのパケット廃棄に加えて、送信フィルタにより、内部からの通信を制限します。																						
⑨	LAN 側 IP アドレス	<p>LAN 側 IP アドレスを設定します。</p> <p>IP アドレスを変更する場合、現在の接続は切断されます。新しい IP アドレスに接続しなおしてください。</p>																					

3. かんたん設定

(5) [NetMeister の設定]の項目を設定し、[設定の確認]ボタンをクリックします。

 インターネット接続の設定に戻る場合は、[戻る]ボタンをクリックしてください。

1. パスワードの設定 → 2. インターネット接続の設定 → 3. NetMeisterの設定 → 4. 設定の確認と反映 → 5. 終了

かんたん設定 : NetMeisterの設定

NetMeisterの設定を行います。
Web設定では、IPv4で動作する設定のみ対応しています。

設定の変更	
NetMeister	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効

[戻る](#) [設定の確認](#)

番号	項目	内容
①	NetMeister	NetMeister の「有効」 / 「無効」を設定します。 「有効」に設定すると、アカウント名等を設定することができます。

「有効」を選択するとアカウント名等の設定項目が表示されますので、各項目を設定し、[設定の確認]ボタンをクリックします。

1. パスワードの設定 → 2. インターネット接続の設定 → 3. NetMeisterの設定 → 4. 設定の確認と反映 → 5. 終了

かんたん設定 : NetMeisterの設定

NetMeisterの設定を行います。
Web設定では、IPv4で動作する設定のみ対応しています。

設定の変更	
NetMeister	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
アカウント名	NetMeisterの登録ページで申請した「グループID」を入力してください。 <input type="text"/> 文字列を入力してください。[2-63文字]
パスワード	NetMeisterの登録ページで申請した「グループパスワード」を入力してください。 <input type="radio"/> パスワードを変更しない <input checked="" type="radio"/> パスワードを変更する <input type="text"/> 文字列を入力してください。[8-31文字]
ホスト名 (装置名)	『装置名の設定』で設定した装置名を通知します。 <input type="text"/> 文字列を入力してください。[2-63文字]
拠点ID	省略した場合、装置名を通知します。 <input type="text"/>

[戻る](#) [設定の確認](#)

3. かんたん設定

番号	項目	内容
①	NetMeister	NetMeister の「有効」／「無効」を設定します。 「無効」に設定すると、アカウント名等の設定項目が隠れます。
②	アカウント名	NetMeister の登録ページで申請した「グループ ID」を設定します。 ・ 半角英数字または-(ハイフン)で 2～63 文字まで入力できます。
③	パスワード	NetMeister の登録ページで申請した「グループパスワード」を設定します。 ・ 半角英数字、_(アンダーバー)または-(ハイフン)で 8～31 文字まで入力できます。 注意 ・ 大文字／小文字は区別されます。 ・ パスワードの入力文字は表示されません。●●●のように伏せ文字で表示されます。 ・ パスワードは、第三者に推測されにくく、忘れないような文字列を入力してください。
④	ホスト名（装置名）	NetMeister に通知するホスト名を変更する必要がある場合は、ここで設定します。 ・ 半角英数字または-(ハイフン)で 2～63 文字まで入力できます。 メモ ・ NetMeister で受け付けられない文字を装置名に指定している場合等に利用します。 ・ 大文字は、小文字に変換して NetMeister に通知されます。 注意 ・ ホスト名の先頭と最後には-(ハイフン)を利用することができません。
⑤	サイト名（拠点名）	NetMeister に通知するサイト名を変更する必要がある場合は、ここで設定します。 ・ 半角英数字または-(ハイフン)で 2～31 文字まで入力できます。 メモ ・ NetMeister で受け付けられない文字を装置名に指定している場合等に利用します。 ・ 大文字は、小文字に変換して NetMeister に通知されます。 ・ サイト名を省略した場合は、装置名が NetMeister に通知されます。 注意 ・ サイト名の先頭と最後には-(ハイフン)を利用することができません。

3. かんたん設定

(6) 入力した項目が正しいことを確認し、[反映]ボタンをクリックします。

メモ NetMeister の設定に戻る場合は、[戻る]ボタンをクリックしてください。

1. パスワードの設定 → 2. インターネット接続の設定 → 3. NetMeisterの設定 → 4. 設定の確認と反映 → 5. 終了

かんたん設定：設定の確認と反映

設定内容を変更する場合は [反映] を押してください。
LAN側IPアドレスを変更する場合は、新しいIPアドレスで接続しなおしてください。

ログイン認証用パスワードの設定

	現在の設定	設定の変更
ユーザ名	admin	変更できません
パスワード	パスワード設定なし	<input type="radio"/> パスワードを変更しない <input checked="" type="radio"/> パスワードを変更する 確認のためもう一度入力してください。

インターネット接続の設定

	現在の設定	設定の変更
接続形態		<input checked="" type="radio"/> PPPoE接続（フレッツ光回線利用の場合） <input type="radio"/> IP接続（ケーブルテレビ回線利用の場合）

WAN1: PPPoE接続の設定(GigaEthernet0.1)

	現在の設定	設定の変更
ユーザ名		プロバイダから通知されているユーザ名を設定します。 (フレッツの場合、通常はユーザ名には@を含んでいます) user@example.com
パスワード		プロバイダから通知されているパスワードを設定します。 user-password
WAN側IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
DNSアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定

通信セキュリティの設定

	現在の設定	設定の変更
セキュリティ強度	レベル1	<input checked="" type="radio"/> レベル1 - 外部からの不要なパケットをNAPTにより廃棄します。 <input type="radio"/> レベル2 - 外部からの不要なパケットをNAPTにより廃棄します。 - 内部からの不要な通信を制限します。

LAN1: LANの設定(GigaEthernet1.0)

	現在の設定	設定の変更
LAN側IPアドレス	192.168.100.1/24	192.168.100.1 / 24

NetMeisterの設定

	設定の変更
NetMeister	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効

戻る 反映

3. かんたん設定

(7) 「設定内容を変更しました。」のメッセージが表示されることを確認し、[トップページへ]ボタンを押します。

1. パスワードの設定 → 2. インターネット接続の設定 → 3. NetMeisterの設定 → 4. 設定の確認と反映 → 5. 終了

かんたん設定：設定の確認と反映

設定内容を変更しました。

ログイン認証用パスワードの設定

	現在の設定	設定の変更
ユーザ名	admin	変更できません
パスワード	パスワード設定なし	<input type="radio"/> パスワードを変更しない <input checked="" type="radio"/> パスワードを変更する 確認のためもう一度入力してください。

インターネット接続の設定

	現在の設定	設定の変更
接続形態		<input checked="" type="radio"/> PPPoE接続 (フレッツ光回線利用の場合) <input type="radio"/> IP接続 (ケーブルテレビ回線利用の場合)

WAN1: PPPoE接続の設定(GigaEthernet0.1)

	現在の設定	設定の変更
ユーザ名		プロバイダから通知されているユーザ名を設定します。 (フレッツの場合、通常はユーザ名には@を含んでいます) user@example.com
パスワード		プロバイダから通知されているパスワードを設定します。 user-password
WAN側IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
DNSアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定

通信セキュリティの設定

	現在の設定	設定の変更
セキュリティ強度	レベル1	<input checked="" type="radio"/> レベル1 - 外部からの不要なパケットをNAPTにより廃棄します。 <input type="radio"/> レベル2 - 外部からの不要なパケットをNAPTにより廃棄します。 - 内部からの不要な通信を制限します。

LAN1: LANの設定(GigaEthernet1.0)

	現在の設定	設定の変更
LAN側IPアドレス	192.168.100.1/24	192.168.100.1 / 24


NetMeisterの設定

	設定の変更
NetMeister	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効

トップページへ

3. かんたん設定

(8) トップページでWAN情報の接続状態を確認します。

 [更新]ボタンをクリックすると、情報を更新することが可能です。

(9) メニューエリア、または、メッセージエリアから[設定の保存]をクリックします。



Web管理画面のスクリーンショット。メニュー、装置情報、ネットワーク情報、WAN情報、VPN情報が表示されています。

メニュー

- メニュー
 - トップページ
 - 設定の保存**
 - ログアウト
- かんたん設定
 - かんたん設定
- 詳細設定
 - 詳細設定
- 端末管理
 - 端末管理
- 保守管理
 - 装置状態の表示
 - 装置ログの取得
 - 設定データの管理
 - 設定の初期化
 - ソフトウェアの更新
 - pingの実行
 - 任意コマンドの実行
 - IP電話サービス保守
 - URLオフロード
 - リンクマネージャ
 - Wake on LAN
 - 再起動
- 拡張ページ
 - 拡張ページ
- 外部リンク
 - 製品ページ

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず**設定の保存**を行ってください。

トップページ [\[カテゴリー表示\]](#) 自動更新間隔: 停止

装置情報 (装置名: Router) 最新ログイン: 2023/10/27 10:00:00 (2023/10/27/10:00:00)

バージョン	稼働時間	稼働率	メモリ	内部温度	内部電圧
	0分	18%	29%	42.0℃	3.2508V

更新

ネットワーク情報

デバイス	接続状態	送信量	受信量
GE0 (GigaEthernet0)	全二重 1Gbpsで接続	0%	0%
GE1 (GigaEthernet1)	Port1: 全二重 1Gbpsで接続 Port2: 接続されていません Port3: 接続されていません Port4: 接続されていません	0%	0%

更新

WAN情報

接続名	接続状態	情報
WAN1: インターネット接続 (GigaEthernet0.1)	接続	IPアドレス: 

更新

VPN情報

接続名	接続状態	送信量[packets]
設定されていません		

[接続名編集](#) **更新**

3. かんたん設定

(10) [保存実行]ボタンをクリックします。

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず『設定の保存』を行ってください。

設定の保存

設定を保存します。

よろしければ [保存実行] を押してください。

[保存実行](#)

(11) 「設定を保存しました。」のメッセージを確認します。

設定の保存

[設定を保存しました。](#)

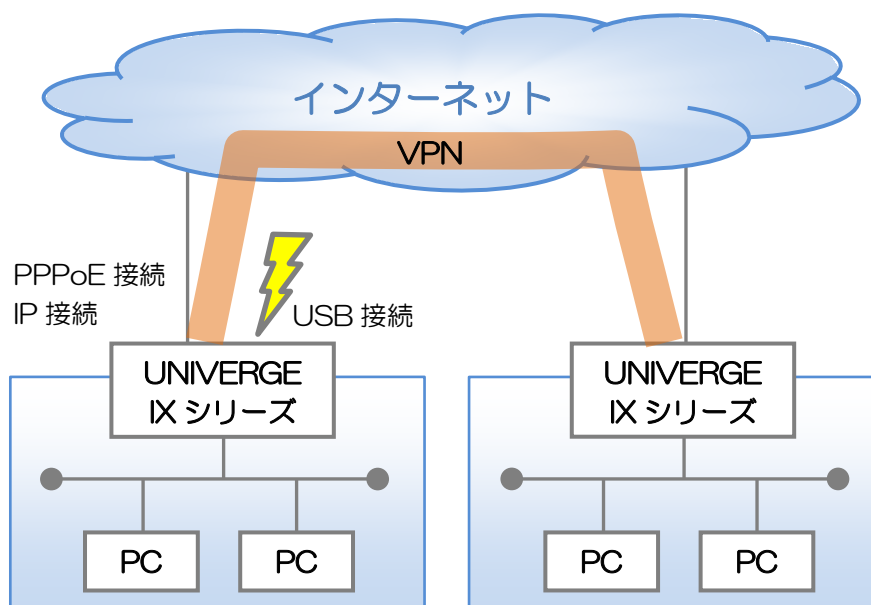
[トップページへ](#)

3. かんたん設定

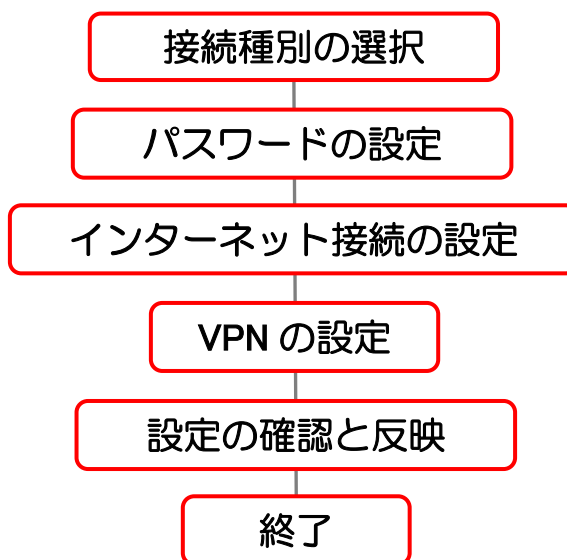
3.2 インターネット接続+VPN 接続

フレッツ光などの有線回線やモバイル回線(3G・LTE)を使用したインターネット接続と、インターネットVPNによる拠点間通信の設定を行います。

【構成イメージ】



【設定手順】



3. かんたん設定

(1) ログイン後のメニューエリアから[かんたん設定]をクリックします。

メモ トップページリンクをクリックすることで、接続種別の各ページに移動することも可能です。

■管理者メニュー

- トップページ
- 設定の保存
- ログアウト

■かんたん設定

- かんたん設定**
- 詳細設定
- 詳細設定

■端末管理

- 端末管理

■保守管理

- 装置状態の表示
- 装置ログの取得
- 設定データの管理
- 設定の初期化
- ソフトウェアの更新
- pingの実行
- 任意コマンドの実行
- IP電話サービス保守
- URLオフロード
- リンクマネージャ
- Wake on LAN
- 再起動

■拡張ページ

- 拡張ページ

■外部リンク

- 製品ページ

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず『設定の保存』を行ってください。

トップページ

ルータの設定を開始します。以下のリンクから選択してください。
パスワードを登録・変更する前にユーザ名とパスワードを入力する画面が表示された場合は、そのまま「OK」をクリックしてください。

かんたん設定

- [インターネット接続](#)
フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用して、インターネットに接続する設定を行います。
- **インターネット接続+VPN接続**
フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用したインターネット接続と、インターネットVPNによる拠点間通信の設定を行います。
- [インターネット接続+フレッツ・VPNワイド接続](#)
フレッツ光を使用したインターネット接続と、フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
- [フレッツ・VPNワイド接続](#)
フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
- [NGN網VPN接続](#)
NGN網を用いたVPNによる拠点間の通信の設定と、NetMeisterによる装置管理の設定を行います。
- [IPv6 IPoE接続](#)
IPv6 IPoE接続の設定を行います。
プロバイダの動的IPまたは固定IPでのサービスを設定します。
- [クラウド接続](#)
インターネットVPNや専用線を使用したクラウド接続の設定を行います。
- [IP電話サービス接続](#)
対応するUNIVERGE Aspireシリーズと連携したIP電話ネットワークの設定を行います。

詳細設定

インタフェースやサーバのアドレスを指定したり、フィルタやQoS、VPN等、かんたん設定に含まれない詳細な設定を行う場合はこちらから設定してください。

端末管理

本装置に接続されている端末を管理します。
リンクマネージャ機能やWeb認証機能を設定します。

保守管理

装置状態の確認、ソフトウェアの更新、pingの実行など、各種保守機能の操作を行います。
URLオフロード機能による特定宛先のレーティング制御、リンクマネージャ機能による端末の保守管理などが可能です。
任意のコマンドを直接実行したい場合は[任意コマンドの実行](#)から操作してください。

3. かんたん設定

(2) 接続種別の選択で「インターネット接続+VPN接続」にチェックを入れ、[次へ]ボタンをクリックします。

メモ 接続種別を変更する場合には、設定の初期化が必要となります。

かんたん設定：接続種別の選択

接続種別を選択してかんたん設定を開始してください。
接続種別を変更する場合には「設定の初期化」が必要となります。

	現在の設定	設定の変更
接続種別の選択	インターネット接続なし	<input type="radio"/> インターネット接続 フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用して、インターネットに接続する設定を行います。
		<input checked="" type="radio"/> インターネット接続 + VPN接続 フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用したインターネット接続と、インターネットVPNによる拠点間通信の設定を行います。
		<input type="radio"/> インターネット接続 + フレッツ・VPNワイド接続 フレッツ光を使用したインターネット接続と、フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
		<input type="radio"/> フレッツ・VPNワイド接続 フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
		<input type="radio"/> NGN網VPN接続 NGN網を用いたVPNによる拠点間の通信の設定とNetMeisterによる装置管理の設定を行います。
		<input type="radio"/> IPv6 IPoE接続 IPv6 IPoE接続の設定を行います。 プロバイダの動的IPまたは固定IPでのサービスを設定します。
		<input type="radio"/> クラウド接続 インターネットVPNや専用線を使用したクラウド接続の設定を行います。
		<input type="radio"/> IP電話サービス接続 対応するUNIVERGE Aspireシリーズと連携したIP電話ネットワークの設定を行います。

次へ

3. かんたん設定

(3) 管理者パスワードを変更する場合は、[パスワードを変更する]を選択し、パスワードを設定した後、[次へ]ボタンをクリックします。

メモ 管理者パスワードを変更する必要が無い場合は、そのまま[次へ]ボタンをクリックします。


メモ 接続種別の選択に戻る場合は、[戻る]ボタンをクリックしてください。



番号	項目	内容
①	ユーザ名	本装置にログインするときのユーザ名です。 <ul style="list-style-type: none">初期状態ではユーザ名は設定されていません。パスワード設定後のユーザ名は「admin」です。Web 設定からは変更できません。
②	パスワード	本装置にログインするときのパスワードです。 <ul style="list-style-type: none">初期状態ではパスワードは設定されていません。半角英数字で 1～249 文字まで入力できます。 注意 <ul style="list-style-type: none">大文字／小文字は区別されます。パスワードの入力文字は表示されません。●●●のように伏せ文字で表示されます。パスワードは、第三者に推測されにくく、忘れないような文字列を入力してください。

3. かんたん設定

(4) [インターネット接続の設定]の各項目を設定し、[次へ]ボタンをクリックします。

 パスワードの設定に戻る場合は、[戻る]ボタンをクリックしてください。

PPPoE 接続の場合(フレッツ光回線利用の場合)

1. パスワードの設定 → 2. **インターネット接続の設定** → 3. VPNの設定 → 4. NetMeisterの設定 →
5. 設定の確認と反映 → 6. 終了

かんたん設定：インターネット接続の設定

プロバイダと接続するWAN側インタフェースを設定します

	現在の設定	設定の変更
接続形態		<input checked="" type="radio"/> PPPoE接続 (フレッツ光回線利用の場合) <input type="radio"/> IP接続 (ケーブルテレビ回線利用の場合)

WAN1: PPPoE接続の設定(GigaEthernet0.1)

	現在の設定	設定の変更
ユーザ名		プロバイダから通知されているユーザ名を設定します。 (フレッツの場合、通常はユーザ名には@を含んでいます) <input type="text"/> 文字列(半角英数字)を入力してください。
パスワード		プロバイダから通知されているパスワードを設定します。 <input type="text"/> 文字列(半角英数字)を入力してください。
WAN側IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
DNSアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定

通信セキュリティの設定

	現在の設定	設定の変更
セキュリティ強度	レベル1	<input checked="" type="radio"/> レベル1 - 外部からの不要なパケットをNAPTにより廃棄します。 <input type="radio"/> レベル2 - 外部からの不要なパケットをNAPTにより廃棄します。 - 内部からの不要な通信を制限します。

3. かんたん設定

番号	項目	内容
①	接続形態	「PPPoE 接続 (フレッツ光回線利用の場合)」を選択します。
②	ユーザ名	プロバイダから通知されているユーザ名を設定します。 (フレッツの場合、通常はユーザ名には@を含んでいます) ・ 半角英数字で 1~59 文字まで入力できます。
③	パスワード	プロバイダから通知されているパスワードを設定します。 ・ 半角英数字で 1~79 文字まで入力できます。 注意 ・ 大文字、小文字も区別されます。
④	WAN 側 IP アドレス	PPPoE 接続の WAN 側 IP アドレスを設定します。 ・ プロバイダから WAN 側 IP アドレスが与えられていないときは「自動取得」を、固定 IP アドレスが与えられているときは「手動設定」を選択します。 ・ 「手動設定」を選択したときは、プロバイダから与えられた IP アドレスを入力し、サブネットマスクをプルダウンメニューから選択します。 注意 ・ 他のインタフェースに設定されている IP アドレスを使用することはできません。 ・ 「自動取得」を選択した場合、IP アドレスを入力することはできません。
⑤	DNS アドレス	PPPoE 接続の DNS サーバのアドレスを設定します。 ・ プロバイダから DNS サーバのアドレスが与えられていないときは「自動取得」を、与えられているとき、または独自に指定するときは「手動設定」を選択します。 ・ 「手動設定」を選択したときは、プロバイダから与えられたプライマリ DNS サーバの IP アドレスを上段に、セカンダリ DNS サーバの IP アドレスを下段に入力します。セカンダリは省略可能です。 注意 ・ 「自動取得」を選択した場合、DNS アドレスを入力することはできません。

3. かんたん設定

⑥	セキュリティ強度	<p>通信セキュリティの強度を設定します。</p> <ul style="list-style-type: none">外部からの不要なパケットをNAPTにより廃棄する場合は「レベル 1」を選択します。外部からの不要なパケットをNAPTにより廃棄し、さらに内部からの不要な通信を制限する場合は、「レベル 2」を選択します。 <p>「レベル 2」を選択したときは、送信時に以下に該当する通信を廃棄します。</p> <table border="1" data-bbox="590 385 1200 947"><tr><td rowspan="4">宛先 IP アドレス</td><td>0.0.0.0/8</td></tr><tr><td>127.0.0.0/8</td></tr><tr><td>169.254.0.0/16</td></tr><tr><td>224.0.0.0/4</td></tr><tr><td rowspan="5">宛先ポート番号</td><td>135</td></tr><tr><td>137</td></tr><tr><td>138</td></tr><tr><td>139</td></tr><tr><td>445</td></tr><tr><td rowspan="5">送信元ポート番号</td><td>135</td></tr><tr><td>137</td></tr><tr><td>138</td></tr><tr><td>139</td></tr><tr><td>445</td></tr></table> <p>メモセキュリティ強度は、以下を参照してください。</p> <table border="1" data-bbox="590 1025 1423 1144"><tr><td>レベル 1 (オフ)</td><td>NAPT により外部からのパケットを廃棄します。</td></tr><tr><td>レベル 2 (標準)</td><td>NAPT による外部からのパケット廃棄に加えて、送信フィルタにより、内部からの通信を制限します。</td></tr></table>	宛先 IP アドレス	0.0.0.0/8	127.0.0.0/8	169.254.0.0/16	224.0.0.0/4	宛先ポート番号	135	137	138	139	445	送信元ポート番号	135	137	138	139	445	レベル 1 (オフ)	NAPT により外部からのパケットを廃棄します。	レベル 2 (標準)	NAPT による外部からのパケット廃棄に加えて、送信フィルタにより、内部からの通信を制限します。
宛先 IP アドレス	0.0.0.0/8																						
	127.0.0.0/8																						
	169.254.0.0/16																						
	224.0.0.0/4																						
宛先ポート番号	135																						
	137																						
	138																						
	139																						
	445																						
送信元ポート番号	135																						
	137																						
	138																						
	139																						
	445																						
レベル 1 (オフ)	NAPT により外部からのパケットを廃棄します。																						
レベル 2 (標準)	NAPT による外部からのパケット廃棄に加えて、送信フィルタにより、内部からの通信を制限します。																						

3. かんたん設定

IP 接続の場合(ケーブルテレビ回線利用の場合)

1. パスワードの設定 → 2. インターネット接続の設定 → 3. VPNの設定 → 4. NetMeisterの設定 →
5. 設定の確認と反映 → 6. 終了

かんたん設定：インターネット接続の設定

プロバイダと接続するWAN側インタフェースを設定します。

	現在の設定	設定の変更
接続形態		<input type="radio"/> PPPoE接続 (フレッツ光回線利用の場合) <input checked="" type="radio"/> IP接続 (ケーブルテレビ回線利用の場合)
WAN1: IP接続の設定(GigaEthernet0.0)		
	現在の設定	設定の変更
WAN側IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
DNSアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
通信セキュリティの設定		
	現在の設定	設定の変更
セキュリティ強度	レベル1	<input checked="" type="radio"/> レベル1 - 外部からの不要なパケットをNAPTにより廃棄します。 <input type="radio"/> レベル2 - 外部からの不要なパケットをNAPTにより廃棄します。 - 内部からの不要な通信を制限します。

3. かんたん設定

番号	項目	内容																					
①	接続形態	「IP 接続 (ケーブルテレビ回線利用の場合)」を選択します。																					
②	WAN 側 IP アドレス	<p>IP 接続の WAN 側 IP アドレスを設定します。</p> <ul style="list-style-type: none"> プロバイダから WAN 側の IP アドレスが与えられていないときは「自動取得」を、固定 IP アドレスが与えられているときは「手動設定」を選択します。 「手動設定」を選択したときは、プロバイダから与えられた IP アドレスを入力し、サブネットマスクをプルダウンメニューから選択します。 <p>注意</p> <ul style="list-style-type: none"> 他のインタフェースに設定されている IP アドレスを使用することはできません。 「自動取得」を選択した場合、IP アドレスを入力することはできません。 																					
③	DNS アドレス	<p>IP 接続の DNS サーバのアドレスを設定します。</p> <ul style="list-style-type: none"> プロバイダから DNS サーバのアドレスが与えられていないときは「自動取得」を、与えられているとき、または独自に指定するときは「手動設定」を選択します。 「手動設定」を選択したときは、プロバイダから与えられたプライマリ DNS サーバの IP アドレスを上段に、セカンダリ DNS サーバの IP アドレスを下段に入力します。セカンダリは省略可能です。 <p>注意</p> <ul style="list-style-type: none"> 「自動取得」を選択した場合、DNS アドレスを入力することはできません。 																					
④	セキュリティ強度	<p>通信セキュリティの強度を設定します。</p> <ul style="list-style-type: none"> 外部からの不要なパケットを NATP により廃棄する場合は「レベル 1」を選択します。 外部からの不要なパケットを NATP により廃棄し、さらに内部からの不要な通信を制限する場合は、「レベル 2」を選択します。 <p>「レベル 2」を選択したときは、送信時に以下に該当する通信を廃棄します。</p> <table border="1" data-bbox="588 1086 1198 1650"> <tbody> <tr> <td rowspan="4">宛先 IP アドレス</td> <td>0.0.0.0/8</td> </tr> <tr> <td>127.0.0.0/8</td> </tr> <tr> <td>169.254.0.0/16</td> </tr> <tr> <td>224.0.0.0/4</td> </tr> <tr> <td rowspan="5">宛先ポート番号</td> <td>135</td> </tr> <tr> <td>137</td> </tr> <tr> <td>138</td> </tr> <tr> <td>139</td> </tr> <tr> <td>445</td> </tr> <tr> <td rowspan="5">送信元ポート番号</td> <td>135</td> </tr> <tr> <td>137</td> </tr> <tr> <td>138</td> </tr> <tr> <td>139</td> </tr> <tr> <td>445</td> </tr> </tbody> </table> <p>メモセキュリティ強度は、以下を参照してください。</p> <table border="1" data-bbox="588 1727 1422 1848"> <tbody> <tr> <td>レベル 1 (オフ)</td> <td>NAPT により外部からのパケットを廃棄します。</td> </tr> <tr> <td>レベル 2 (標準)</td> <td>NAPT による外部からのパケット廃棄に加えて、送信フィルタにより、内部からの通信を制限します。</td> </tr> </tbody> </table>	宛先 IP アドレス	0.0.0.0/8	127.0.0.0/8	169.254.0.0/16	224.0.0.0/4	宛先ポート番号	135	137	138	139	445	送信元ポート番号	135	137	138	139	445	レベル 1 (オフ)	NAPT により外部からのパケットを廃棄します。	レベル 2 (標準)	NAPT による外部からのパケット廃棄に加えて、送信フィルタにより、内部からの通信を制限します。
宛先 IP アドレス	0.0.0.0/8																						
	127.0.0.0/8																						
	169.254.0.0/16																						
	224.0.0.0/4																						
宛先ポート番号	135																						
	137																						
	138																						
	139																						
	445																						
送信元ポート番号	135																						
	137																						
	138																						
	139																						
	445																						
レベル 1 (オフ)	NAPT により外部からのパケットを廃棄します。																						
レベル 2 (標準)	NAPT による外部からのパケット廃棄に加えて、送信フィルタにより、内部からの通信を制限します。																						

3. かんたん設定

USB 接続の場合(3G・LTE 回線利用の場合)

※IX2215/IX2235/IX2310/IX3315のみ

1. パスワードの設定 → 2. インターネット接続の設定 → 3. VPNの設定 → 4. NetMeisterの設定 →
5. 設定の確認と反映 → 6. 終了

かんたん設定：インターネット接続の設定

プロバイダと接続するWAN側インタフェースを設定します。

	現在の設定	設定の変更
接続形態		<input type="radio"/> PPPoE接続 (フレッツ光回線利用の場合) <input type="radio"/> IP接続 (ケーブルテレビ回線利用の場合) <input checked="" type="radio"/> USB接続 (3G・LTE回線利用の場合)

WAN1: USB接続の設定(USB-Serial0.0)

	現在の設定	設定の変更
ユーザ名		プロバイダからユーザ名が指定されている場合に設定します。 <input type="text"/>
パスワード		プロバイダからパスワードが指定されている場合に設定します。 <input type="text"/>
PDPタイプ		プロバイダからPDPタイプが指定されている場合に設定します。 -- <input type="text"/>
APN		プロバイダからAPNが指定されている場合に設定します。 <input type="text"/>
WAN側IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
DNSアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定

通信セキュリティの設定

	現在の設定	設定の変更
セキュリティ強度	レベル1	<input checked="" type="radio"/> レベル1 - 外部からの不要なパケットをNAPTにより廃棄します。 <input type="radio"/> レベル2 - 外部からの不要なパケットをNAPTにより廃棄します。 - 内部からの不要な通信を制限します。

[戻る](#) [次へ](#)

3. かんたん設定

番号	項目	内容
①	接続形態	「USB 接続 (3G・LTE 回線利用の場合)」を選択します。
②	ユーザ名	プロバイダからユーザ名が指定されている場合に設定します。 ・ 半角英数字で 1～59 文字まで入力できます。
③	パスワード	プロバイダからパスワードが指定されている場合に設定します。 ・ 半角英数字で 1～79 文字まで入力できます。 注意 ・ 大文字、小文字も区別されます。
④	PDP タイプ	プロバイダから PDP タイプが指定されている場合に設定します。
⑤	APN	プロバイダから APN が指定されている場合に設定します。 ・ 半角英数字で 1～90 文字まで入力できます。
⑥	WAN 側 IP アドレス	USB 接続の WAN 側 IP アドレスを設定します。 ・ プロバイダから WAN 側 IP アドレスが与えられていないときは「自動取得」を、固定 IP アドレスが与えられているときは「手動設定」を選択します。 ・ 「手動設定」を選択したときは、プロバイダから与えられた IP アドレスを入力し、サブネットマスクをプルダウンメニューから選択します。 注意 ・ 他のインターフェースに設定されている IP アドレスを使用することはできません。 ・ 「自動取得」を選択した場合、IP アドレスを入力することはできません。
⑦	DNS アドレス	USB 接続の DNS サーバのアドレスを設定します。 ・ プロバイダから DNS サーバのアドレスが与えられていないときは「自動取得」を、与えられているとき、または独自に指定するときは「手動設定」を選択します。 ・ 「手動設定」を選択したときは、プロバイダから与えられたプライマリ DNS サーバの IP アドレスを上段に、セカンダリ DNS サーバの IP アドレスを下段に入力します。セカンダリは省略可能です。 注意 ・ 「自動取得」を選択した場合、DNS アドレスを入力することはできません。

3. かんたん設定

⑧	セキュリティ強度	<p>通信セキュリティの強度を設定します。</p> <ul style="list-style-type: none">外部からの不要なパケットをNAPTにより廃棄する場合は「レベル 1」を選択します。外部からの不要なパケットをNAPTにより廃棄し、さらに内部からの不要な通信を制限する場合は、「レベル 2」を選択します。 <p>「レベル 2」を選択したときは、送信時に以下に該当する通信を廃棄します。</p> <table border="1" data-bbox="592 383 1198 947"><tr><td rowspan="4">宛先 IP アドレス</td><td>0.0.0.0/8</td></tr><tr><td>127.0.0.0/8</td></tr><tr><td>169.254.0.0/16</td></tr><tr><td>224.0.0.0/4</td></tr><tr><td rowspan="5">宛先ポート番号</td><td>135</td></tr><tr><td>137</td></tr><tr><td>138</td></tr><tr><td>139</td></tr><tr><td>445</td></tr><tr><td rowspan="5">送信元ポート番号</td><td>135</td></tr><tr><td>137</td></tr><tr><td>138</td></tr><tr><td>139</td></tr><tr><td>445</td></tr></table> <p>メモセキュリティ強度は、以下を参照してください。</p> <table border="1" data-bbox="592 1025 1422 1144"><tr><td>レベル 1 (オフ)</td><td>NAPT により外部からのパケットを廃棄します。</td></tr><tr><td>レベル 2 (標準)</td><td>NAPT による外部からのパケット廃棄に加えて、送信フィルタにより、内部からの通信を制限します。</td></tr></table>	宛先 IP アドレス	0.0.0.0/8	127.0.0.0/8	169.254.0.0/16	224.0.0.0/4	宛先ポート番号	135	137	138	139	445	送信元ポート番号	135	137	138	139	445	レベル 1 (オフ)	NAPT により外部からのパケットを廃棄します。	レベル 2 (標準)	NAPT による外部からのパケット廃棄に加えて、送信フィルタにより、内部からの通信を制限します。
宛先 IP アドレス	0.0.0.0/8																						
	127.0.0.0/8																						
	169.254.0.0/16																						
	224.0.0.0/4																						
宛先ポート番号	135																						
	137																						
	138																						
	139																						
	445																						
送信元ポート番号	135																						
	137																						
	138																						
	139																						
	445																						
レベル 1 (オフ)	NAPT により外部からのパケットを廃棄します。																						
レベル 2 (標準)	NAPT による外部からのパケット廃棄に加えて、送信フィルタにより、内部からの通信を制限します。																						

3. かんたん設定

(5) [VPNの設定]の各項目を設定し、[次へ]ボタンをクリックします。

インターネット接続の設定に戻る場合は、[戻る]ボタンをクリックしてください。

ダイナミックVPNのタイプや拠点番号を変更すると、LAN側IPアドレスが変更されます。

拠点の場合

1. パスワードの設定 → 2. インターネット接続の設定 → 3. **VPNの設定** → 4. NetMeisterの設定 → 5. 設定の確認と反映 → 6. 終了

かんたん設定：VPNの設定

VPNを設定します。

	現在の設定	設定の変更
接続種別		<input checked="" type="radio"/> ダイナミックVPN

ダイナミックVPNの設定

2 拠点間通信でもセンタは必要です。いずれかの拠点で必ずセンタを選択してください。
タイプや拠点番号を変更すると、LAN側IPアドレスが変更されます。

	現在の設定	設定の変更
タイプ		<input checked="" type="radio"/> 拠点 <input type="radio"/> センタ
拠点番号		他の拠点と同じ番号は設定しないでください。 1 ▾
パスワード		すべての拠点で共通のパスワードを設定してください。 <input type="text"/> 文字列(半角英数字)を入力してください。
センタWAN側IPアドレス		センタ装置のWANに設定されているIPアドレスまたはドメイン名を入力してください。 <input type="text"/> 入力形式が不正です。

LAN1: LANの設定(GigaEthernet1.0)

他の拠点と重複しないように設定してください。
LAN側IPアドレスを変更する場合は、反映後に新しいIPアドレスで接続しなおす必要があります。

	現在の設定	設定の変更
LAN側IPアドレス	192.168.100.1/24	<input checked="" type="radio"/> 自動設定 <input type="radio"/> 手動設定 192.168.1.254 / 24 ▾ 自動設定で上記アドレスに設定されます。

3. かんたん設定

番号	項目	内容
①	タイプ	「拠点」を選択します。
②	拠点番号	拠点番号(1~64)を設定します。 他の拠点と同じ番号は設定しないでください。
③	パスワード	VPN 接続で使用するパスワード(事前共有鍵)です。 すべての拠点で同じ任意のパスワードを設定してください。 ・ 半角英数字で 1~128 文字まで入力できます。
④	センタ WAN 側 IP アドレス	センタ装置の WAN に設定されている IP アドレスまたはドメイン名を入力してください。
⑤	LAN 側 IP アドレス	他の拠点と重複しないように設定してください。 注意 ・ LAN 側 IP アドレスを変更する場合は、反映後に新しい IP アドレスで接続しなおす必要があります。

センタの場合

1. パスワードの設定 → 2. インターネット接続の設定 → 3. **VPNの設定** → 4. NetMeisterの設定 → 5. 設定の確認と反映 → 6. 終了

かんたん設定：VPNの設定

VPNを設定します。

	現在の設定	設定の変更
接続種別		<input checked="" type="radio"/> ダイナミックVPN

ダイナミックVPNの設定

2 拠点間通信でもセンタは必要です。いずれかの拠点で必ずセンタを選択してください。
タイプや拠点番号を変更すると、LAN側IPアドレスが変更されます。

	現在の設定	設定の変更
タイプ		<input type="radio"/> 拠点 <input checked="" type="radio"/> センタ
パスワード		すべての拠点で共通のパスワードを設定してください。 <input type="text"/> 文字列(半角英数字)を入力してください。

LAN1: LANの設定(GigaEthernet1.0)

他の拠点と重複しないように設定してください。
LAN側IPアドレスを変更する場合は、反映後に新しいIPアドレスで接続しなおす必要があります。

	現在の設定	設定の変更
LAN側IPアドレス	192.168.100.1/24	<input checked="" type="radio"/> 自動設定 <input type="radio"/> 手動設定 <input type="text" value="192.168.254.254"/> / <input type="text" value="24"/> 自動設定で上記アドレスに設定されます。

戻る

3. かんたん設定

番号	項目	内容
①	タイプ	「センタ」を選択します。
②	パスワード	VPN 接続で使用するパスワード(事前共有鍵)です。 拠点に設定したパスワードと同じパスワードを設定してください。 ・ 半角英数字で 1~128 文字まで入力できます。
③	LAN 側 IP アドレス	他の拠点と重複しないように IP アドレスを設定します。 注意 ・ LAN 側 IP アドレスを変更する場合は、反映後に新しい IP アドレスで接続しなおす必要があります。

(6) [NetMeister の設定]の項目を設定し、[設定の確認]ボタンをクリックします。

メモ VPN の設定に戻る場合は、[戻る]ボタンをクリックしてください。

1. パスワードの設定 → 2. インターネット接続の設定 → 3. VPNの設定 → 4. NetMeisterの設定 → 5. 設定の確認と反映 → 6. 終了

かんたん設定 : NetMeisterの設定

NetMeisterの設定を行います。
Web設定では、IPv4で動作する設定のみ対応しています。

設定の変更

NetMeister 無効 有効

戻る

番号	項目	内容
①	NetMeister	NetMeister の「有効」 / 「無効」を設定します。 「有効」に設定すると、アカウント名等を設定することができます。

3. かんたん設定

「有効」を選択するとアカウント名等の設定項目が表示されますので、各項目を設定し、[設定の確認]ボタンをクリックします。

1. パスワードの設定 → 2. インターネット接続の設定 → 3. VPNの設定 → 4. **NetMeisterの設定** → 5. 設定の確認と反映 → 6. 終了

かんたん設定：NetMeisterの設定

NetMeisterの設定を行います。
Web設定では、IPv4で動作する設定のみ対応しています。

設定の変更	
NetMeister	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
アカウント名	NetMeisterの登録ページで申請した「グループID」を入力してください。 <input type="text"/> 文字列を入力してください。[2-63文字]
パスワード	NetMeisterの登録ページで申請した「グループパスワード」を入力してください。 <input type="radio"/> パスワードを変更しない <input checked="" type="radio"/> パスワードを変更する <input type="text"/> 文字列を入力してください。[8-31文字]
ホスト名 (装置名)	『装置名の設定』で設定した装置名を通知します。 <input type="text" value="web-trial1"/>
拠点ID	省略した場合、装置名を通知します。 <input type="text"/>

番号	項目	内容
①	NetMeister	NetMeisterの「有効」／「無効」を設定します。 「無効」に設定すると、アカウント名等の設定項目が隠れます。
②	アカウント名	NetMeisterの登録ページで申請した「グループID」を設定します。 ・半角英数字または-(ハイフン)で2～63文字まで入力できます。
③	パスワード	NetMeisterの登録ページで申請した「グループパスワード」を設定します。 ・半角英数字、_(アンダーバー)または-(ハイフン)で8～31文字まで入力できます。 注意 ・大文字／小文字は区別されます。 ・パスワードの入力文字は表示されません。●●●のように伏せ文字で表示されます。 ・パスワードは、第三者に推測されにくく、忘れないような文字列を入力してください。
④	ホスト名 (装置名)	NetMeisterに通知するホスト名を変更する必要がある場合は、ここで設定します。 ・半角英数字または-(ハイフン)で2～63文字まで入力できます。 メモ ・NetMeisterで受け付けられない文字を装置名に指定している場合等に利用します。 ・大文字は、小文字に変換してNetMeisterに通知されます。 注意 ・ホスト名の先頭と最後には-(ハイフン)を利用することができません。
⑤	サイト名 (拠点名)	NetMeisterに通知するサイト名を変更する必要がある場合は、ここで設定します。 ・半角英数字または-(ハイフン)で2～31文字まで入力できます。 メモ ・NetMeisterで受け付けられない文字を装置名に指定している場合等に利用します。 ・大文字は、小文字に変換してNetMeisterに通知されます。 ・サイト名を省略した場合は、装置名がNetMeisterに通知されます。 注意 ・サイト名の先頭と最後には-(ハイフン)を利用することができません。

3. かんたん設定

(7) 入力した項目が正しいことを確認し、[反映]ボタンをクリックします。

メモ NetMeister の設定に戻る場合は、[戻る]ボタンをクリックしてください。

注意 本設定が反映されると、ルータの LAN 側 IP アドレスが自動的に変更されるため、Web 設定画面の接続が切れてしまいます。
Web 設定画面に再接続するには、パソコンの IP アドレスを取得し直す必要がありますので、[反映]ボタンをクリック後に、一旦パソコンのイーサネットケーブルを抜いて、あらためて挿し直してください。
また、Web 設定画面に接続するための IP アドレスは、LAN 側 IP アドレスの欄に表示されているアドレス(*)に変わります。Web ブラウザのアドレスバーに半角英数字で「https://<新しい LAN 側 IP アドレス>/」と入力し、[Enter]キーを押してください。

3. かんたん設定

1. パスワードの設定 → 2. インターネット接続の設定 → 3. VPNの設定 → 4. NetMeisterの設定 → 5. 設定の確認と反映 → 6. 終了

かんたん設定：設定の確認と反映

設定内容を変更する場合は [反映] を押してください。
LAN側IPアドレスを変更する場合は、新しいIPアドレスで接続しなおしてください。

ログイン認証用パスワードの設定

	現在の設定	設定の変更
ユーザ名	admin	変更できません
パスワード	パスワード設定なし	<input type="radio"/> パスワードを変更しない <input checked="" type="radio"/> パスワードを変更する ***** 確認のためもう一度入力してください。 *****

インターネット接続の設定

	現在の設定	設定の変更
接続形態		<input checked="" type="radio"/> PPPoE接続 (フレッツ光回線利用の場合) <input type="radio"/> IP接続 (ケーブルテレビ回線利用の場合)

WAN1: PPPoE接続の設定(GigaEthernet0.1)

	現在の設定	設定の変更
ユーザ名		プロバイダから通知されているユーザ名を設定します。 (フレッツの場合、通常はユーザ名には@を含んでいます) user@example.com
パスワード		プロバイダから通知されているパスワードを設定します。 user-password
WAN側IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
DNSアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定

通信セキュリティの設定

	現在の設定	設定の変更
セキュリティ強度	レベル1	<input checked="" type="radio"/> レベル1 - 外部からの不要なパケットをNAPTにより廃棄します。 <input type="radio"/> レベル2 - 外部からの不要なパケットをNAPTにより廃棄します。 - 内部からの不要な通信を制限します。

VPNの設定

	現在の設定	設定の変更
接続種別		<input checked="" type="radio"/> ダイナミックVPN

ダイナミックVPNの設定

	現在の設定	設定の変更
タイプ		<input checked="" type="radio"/> 拠点 <input type="radio"/> センタ
拠点番号		他の拠点と同じ番号は設定しないでください。 1
パスワード		すべての拠点で共通のパスワードを設定してください。 vpn-password
センタWAN側IPアドレス		センタ装置のWANに設定されているIPアドレスまたはドメイン名を入力してください。 192.168.1.254

LAN1: LANの設定(GigaEthernet1.0)

	現在の設定	設定の変更
LAN側IPアドレス	192.168.1.254	<input checked="" type="radio"/> 自動設定 <input type="radio"/> 手動設定 自動設定で上記IPアドレスに設定されます。

NetMeisterの設定

	設定の変更
NetMeister	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効

戻る **反映**

(8) 「設定内容を変更しました。」のメッセージが表示されることを確認し、[トップページへ]ボタンを押します。

注意 本画面が表示されない場合、Web 設定画面の接続が切れています。パソコンのIPアドレスを再取得後、新しいLAN側IPアドレスに接続しなおしてください。

3. かんたん設定

1. パスワードの設定 → 2. インターネット接続の設定 → 3. VPNの設定 → 4. NetMeisterの設定 →
5. 設定の確認と反映 → 6. 終了

かんたん設定：設定の確認と反映

設定内容を変更しました。

ログイン認証用パスワードの設定

	現在の設定	設定の変更
ユーザ名	admin	変更できません
パスワード	パスワード設定なし	<input type="radio"/> パスワードを変更しない <input checked="" type="radio"/> パスワードを変更する ***** 確認のためもう一度入力してください。 *****

インターネット接続の設定

	現在の設定	設定の変更
接続形態		<input checked="" type="radio"/> PPPoE接続（フレッツ光回線利用の場合） <input type="radio"/> IP接続（ケーブルテレビ回線利用の場合）

WAN1: PPPoE接続の設定(GigaEthernet0.1)

	現在の設定	設定の変更
ユーザ名		プロバイダから通知されているユーザ名を設定します。 (フレッツの場合、通常はユーザ名には@を含んでいます) user@example.com
パスワード		プロバイダから通知されているパスワードを設定します。 user-password
WAN側IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
DNSアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定

通信セキュリティの設定

	現在の設定	設定の変更
セキュリティ強度	レベル1	<input checked="" type="radio"/> レベル1 - 外部からの不要なパケットをNAPTにより廃棄します。 <input type="radio"/> レベル2 - 外部からの不要なパケットをNAPTにより廃棄します。 - 内部からの不要な通信を制限します。

VPNの設定

	現在の設定	設定の変更
接続種別		<input checked="" type="radio"/> ダイナミックVPN

ダイナミックVPNの設定

	現在の設定	設定の変更
タイプ		<input checked="" type="radio"/> 拠点 <input type="radio"/> センタ
拠点番号		他の拠点と同じ番号は設定しないでください。 1
パスワード		すべての拠点で共通のパスワードを設定してください。 vpn-password
センタWAN側IPアドレス		センタ装置のWANに設定されているIPアドレスまたはドメイン名を入力してください。 [IPアドレス]

LAN1: LANの設定(GigaEthernet1.0)

	現在の設定	設定の変更
LAN側IPアドレス	[IPアドレス]	<input checked="" type="radio"/> 自動設定 <input type="radio"/> 手動設定 192.168.1.254 / 24 自動設定で上記アドレスに設定されます。


NetMeisterの設定

	設定の変更
NetMeister	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効

トップページへ

3. かんたん設定

(9) トップページでWAN情報の接続状態を確認します。

 [更新]ボタンをクリックすると、情報を更新することが可能です。

(10) メニューエリア、または、メッセージエリアから[設定の保存]をクリックします。



!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず「設定の保存」を行ってください。

メニュー
トップページ
設定の保存
ログアウト

かんたん設定
かんたん設定

詳細設定
詳細設定

端末管理
端末管理

保守管理
装置状態の表示
装置ログの取得
設定データの管理
設定の初期化
ソフトウェアの更新
pingの実行
任意コマンドの実行
IP電話サービス保守
URLオフロード
リンクマネージャ
Wake on LAN
再起動

拡張ページ
拡張ページ

外部リンク
製品ページ

トップページ [\[戻る\]](#) 自動更新間隔: 停止

装置情報 (装置名: Router) 前回ログイン: ----/--/-- (-----)

バージョン	稼働時間	稼働率	メモリ	内部温度	内部電圧
5.0.4T	6分	28%	29%	43.0℃	3.2508V

ネットワーク情報

デバイス	接続状態	送信量	受信量
GE0 (GigaEthernet0)	全二重 1Gbpsで接続	0%	0%
GE1 (GigaEthernet1)	Port1: 全二重 1Gbpsで接続 Port2: 接続されていません Port3: 接続されていません Port4: 接続されていません	0%	0%

WAN情報

接続名	接続状態	情報
WAN1: インターネットVPN接続 (GigaEthernet0.1)	接続	IPアドレス: 203.0.113.1

VPN情報

接続名	接続状態	通信量[packets]
Dynamic_VPN	接続	送信: 7, 受信: 10

(11) VPN情報は、接続名にマウスカーソルを近づけることで、詳細情報を確認することができます。また、接続名をわかりやすいように変更することができます。



VPN情報

接続名	接続状態	通信量[packets]
Dynamic_VPN	接続	送信: 96, 受信: 129

ダイナミックVPN(センタ)
IPアドレス: 203.0.113.254

接続名編集 更新

3. かんたん設定

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず**設定の保存**を行ってください。

VPN情報 接続名の編集

接続名	接続状態	IPアドレス/送信量[packets]
<input type="text"/>	接続 ダイナミックVPN(センタ)	IPアドレス: 203.0.113.254 送信: 463 受信: 208

番号	項目	内容
①	接続名	接続名を設定します。 ・ 半角英数字 1~128 文字まで、または全角文字で 1~32 文字まで入力できます。

(12) [保存実行]ボタンをクリックします。

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず**設定の保存**を行ってください。

設定の保存

設定を保存します。

よろしければ [保存実行] を押してください。

(13) 「設定を保存しました。」のメッセージを確認します。

設定の保存

設定を保存しました。

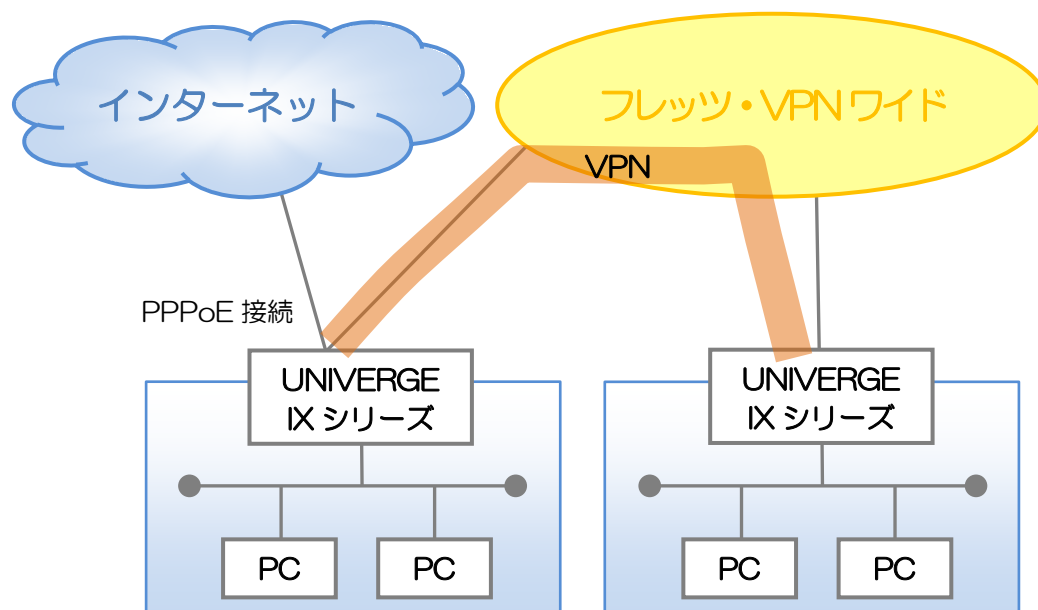
メモ 確実に VPN 接続するため、設定の保存後、再起動実行を推奨します。

3. かんたん設定

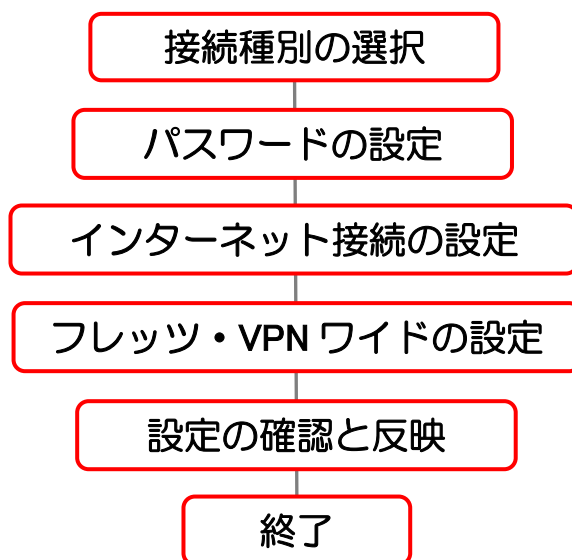
3.3 インターネット接続＋フレッツ・VPNワイド接続

フレッツ光を使用したインターネット接続と、フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。

【構成イメージ】



【設定手順】



3. かんたん設定

(1) ログイン後のメニューエリアから[かんたん設定]をクリックします。

メモ トップページリンクをクリックすることで、接続種別の各ページに移動することも可能です。

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず『設定の保存』を行ってください。

■管理者メニュー
トップページ
設定の保存
ログアウト

■かんたん設定
かんたん設定

■詳細設定
詳細設定

■端末管理
端末管理

■保守管理
装置状態の表示
装置ログの取得
設定データの管理
設定の初期化
ソフトウェアの更新
pingの実行
任意コマンドの実行
IP電話サービス保守
URLオフロード
リンクマネージャ
Wake on LAN
再起動

■拡張ページ
拡張ページ

■外部リンク
製品ページ

トップページ

ルータの設定を開始します。以下のリンクから選択してください。
パスワードを登録・変更する前にユーザ名とパスワードを入力する画面が表示された場合は、そのまま「OK」をクリックしてください。

かんたん設定

- [インターネット接続](#)
フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用して、インターネットに接続する設定を行います。
- [インターネット接続+VPN接続](#)
フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用したインターネット接続と、インターネットVPNによる拠点間通信の設定を行います。
- **[インターネット接続+フレッツ・VPNワイド接続](#)**
フレッツ光を使用したインターネット接続と、フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
- [フレッツ・VPNワイド接続](#)
フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
- [NGN網VPN接続](#)
NGN網を用いたVPNによる拠点間の通信の設定と、NetMeisterによる装置管理の設定を行います。
- [IPv6 IPoE接続](#)
IPv6 IPoE接続の設定を行います。
プロバイダの動的IPまたは固定IPでのサービスを設定します。
- [クラウド接続](#)
インターネットVPNや専用線を使用したクラウド接続の設定を行います。
- [IP電話サービス接続](#)
対応するUNIVERGE Aspireシリーズと連携したIP電話ネットワークの設定を行います。

詳細設定

インタフェースやサーバのアドレスを指定したり、フィルタやQoS、VPN等、かんたん設定に含まれない詳細な設定を行う場合はこちらから設定してください。

端末管理

本装置に接続されている端末を管理します。
リンクマネージャ機能やWeb認証機能を設定します。

保守管理

装置状態の確認、ソフトウェアの更新、pingの実行など、各種保守機能の操作を行います。
URLオフロード機能による特定宛先のルーティング制御、リンクマネージャ機能による端末の保守管理などが可能です。
任意のコマンドを直接実行したい場合は[任意コマンドの実行](#)から操作してください。

3. かんたん設定

(2) 接続種別の選択で「インターネット接続+フレッツ・VPNワイド接続」にチェックを入れ、[次へ]ボタンをクリックします。

メモ 接続種別を変更する場合には、設定の初期化が必要となります。

かんたん設定：接続種別の選択

接続種別を選択してかんたん設定を開始してください。
接続種別を変更する場合には「[設定の初期化](#)」が必要となります。

	現在の設定	設定の変更
接続種別の選択	インターネット接続なし	<input type="radio"/> インターネット接続 フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用して、インターネットに接続する設定を行います。
		<input type="radio"/> インターネット接続 + VPN接続 フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用したインターネット接続と、インターネットVPNによる拠点間通信の設定を行います。
		<input checked="" type="radio"/> インターネット接続 + フレッツ・VPNワイド接続 フレッツ光を使用したインターネット接続と、フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
		<input type="radio"/> フレッツ・VPNワイド接続 フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
		<input type="radio"/> NGN網VPN接続 NGN網を用いたVPNによる拠点間の通信の設定とNetMeisterによる装置管理の設定を行います。
		<input type="radio"/> IPv6 IPoE接続 IPv6 IPoE接続の設定を行います。 プロバイダの動的IPまたは固定IPでのサービスを設定します。
		<input type="radio"/> クラウド接続 インターネットVPNや専用線を使用したクラウド接続の設定を行います。
		<input type="radio"/> IP電話サービス接続 対応するUNIVERGE Aspireシリーズと連携したIP電話ネットワークの設定を行います。

次へ

3. かんたん設定

(3) 管理者パスワードを変更する場合は、[パスワードを変更する]を選択し、パスワードを設定した後、[次へ]ボタンをクリックします。

メモ 管理者パスワードを変更する必要が無い場合は、そのまま[次へ]ボタンをクリックします。

メモ 接続種別の選択に戻る場合は、[戻る]ボタンをクリックしてください。

1. パスワードの設定 → 2. インターネット接続の設定 → 3. フレッツ・VPNワイドの設定 →
4. NetMeisterの設定 → 5. 設定の確認と反映 → 6. 終了

かんたん設定：パスワードの設定

ログイン認証用のパスワードを設定します。

	現在の設定	設定の変更
ユーザ名	admin	変更できません
パスワード	*****	<input type="radio"/> パスワードを変更しない <input checked="" type="radio"/> パスワードを変更する 確認のためもう一度入力してください。 パスワードを入力してください。

戻る 次へ

番号	項目	内容
①	ユーザ名	本装置にログインするときのユーザ名です。 <ul style="list-style-type: none">初期状態ではユーザ名は設定されていません。パスワード設定後のユーザ名は「admin」です。Web 設定からは変更できません。
②	パスワード	本装置にログインするときのパスワードです。 <ul style="list-style-type: none">初期状態ではパスワードは設定されていません。半角英数字で 1～249 文字まで入力できます。 注意 <ul style="list-style-type: none">大文字／小文字は区別されます。パスワードの入力文字は表示されません。●●●のように伏せ文字で表示されます。パスワードは、第三者に推測されにくく、忘れないような文字列を入力してください。

3. かんたん設定

(4) [インターネット接続の設定]の各項目を設定し、[次へ]ボタンをクリックします。

メモ パスワードの設定に戻る場合は、[戻る]ボタンをクリックしてください。

1. パスワードの設定 → 2. **インターネット接続の設定** → 3. フレッツ・VPNワイドの設定 →
4. NetMeisterの設定 → 5. 設定の確認と反映 → 6. 終了

かんたん設定：インターネット接続の設定

プロバイダと接続するWAN側インタフェースを設定します。

	現在の設定	設定の変更
接続形態		<input checked="" type="radio"/> PPPoE接続（フレッツ光回線利用の場合）

WAN1: PPPoE接続の設定(GigaEthernet0.1)

	現在の設定	設定の変更
ユーザ名		プロバイダから通知されているユーザ名を設定します。 (フレッツの場合、通常はユーザ名には@を含んでいます) <input type="text"/> 文字列(半角英数字)を入力してください。
パスワード		プロバイダから通知されているパスワードを設定します。 <input type="text"/> 文字列(半角英数字)を入力してください。
WAN側IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
DNSアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定

通信セキュリティの設定

	現在の設定	設定の変更
セキュリティ強度	レベル1	<input checked="" type="radio"/> レベル1 - 外部からの不要なパケットをNAPTにより廃棄します。 <input type="radio"/> レベル2 - 外部からの不要なパケットをNAPTにより廃棄します。 - 内部からの不要な通信を制限します。

3. かんたん設定

番号	項目	内容																					
①	ユーザ名	<p>プロバイダから通知されているユーザ名を設定します。 (フレッツの場合、通常はユーザ名には@を含んでいます)</p> <ul style="list-style-type: none"> 半角英数字で1~59文字まで入力できます。 																					
②	パスワード	<p>プロバイダから通知されているパスワードを設定します。</p> <ul style="list-style-type: none"> 半角英数字で1~79文字まで入力できます。 <p>注意</p> <ul style="list-style-type: none"> 大文字、小文字も区別されます。 																					
③	WAN 側 IP アドレス	<p>PPPoE 接続の WAN 側 IP アドレスを設定します。</p> <ul style="list-style-type: none"> プロバイダから WAN 側 IP アドレスが与えられていないときは「自動取得」を、固定 IP アドレスが与えられているときは「手動設定」を選択します。 「手動設定」を選択したときは、プロバイダから与えられた IP アドレスを入力し、サブネットマスクをプルダウンメニューから選択します。 <p>注意</p> <ul style="list-style-type: none"> 他のインタフェースに設定されている IP アドレスを使用することはできません。 「自動取得」を選択した場合、IP アドレスを入力することはできません。 																					
④	DNS アドレス	<p>PPPoE 接続の DNS サーバのアドレスを設定します。</p> <ul style="list-style-type: none"> プロバイダから DNS サーバのアドレスが与えられていないときは「自動取得」を、与えられているとき、または独自に指定するときは「手動設定」を選択します。 「手動設定」を選択したときは、プロバイダから与えられたプライマリ DNS サーバの IP アドレスを上段に、セカンダリ DNS サーバの IP アドレスを下段に入力します。セカンダリは省略可能です。 <p>注意</p> <ul style="list-style-type: none"> 「自動取得」を選択した場合、DNS アドレスを入力することはできません。 																					
⑤	セキュリティ強度	<p>通信セキュリティの強度を設定します。</p> <ul style="list-style-type: none"> 外部からの不要なパケットを NATP により廃棄する場合は「レベル 1」を選択します。 外部からの不要なパケットを NATP により廃棄し、さらに内部からの不要な通信を制限する場合は、「レベル 2」を選択します。 <p>「レベル 2」を選択したときは、送信時に以下に該当する通信を廃棄します。</p> <table border="1" data-bbox="588 1319 1198 1883"> <tbody> <tr> <td rowspan="4">宛先 IP アドレス</td> <td>0.0.0.0/8</td> </tr> <tr> <td>127.0.0.0/8</td> </tr> <tr> <td>169.254.0.0/16</td> </tr> <tr> <td>224.0.0.0/4</td> </tr> <tr> <td rowspan="5">宛先ポート番号</td> <td>135</td> </tr> <tr> <td>137</td> </tr> <tr> <td>138</td> </tr> <tr> <td>139</td> </tr> <tr> <td>445</td> </tr> <tr> <td rowspan="5">送信元ポート番号</td> <td>135</td> </tr> <tr> <td>137</td> </tr> <tr> <td>138</td> </tr> <tr> <td>139</td> </tr> <tr> <td>445</td> </tr> </tbody> </table> <p>メモセキュリティ強度は、以下を参照してください。</p> <table border="1" data-bbox="588 1960 1422 2080"> <tbody> <tr> <td>レベル 1 (オフ)</td> <td>NAPT により外部からのパケットを廃棄します。</td> </tr> <tr> <td>レベル 2 (標準)</td> <td>NAPT による外部からのパケット廃棄に加えて、送信フィルタにより、内部からの通信を制限します。</td> </tr> </tbody> </table>	宛先 IP アドレス	0.0.0.0/8	127.0.0.0/8	169.254.0.0/16	224.0.0.0/4	宛先ポート番号	135	137	138	139	445	送信元ポート番号	135	137	138	139	445	レベル 1 (オフ)	NAPT により外部からのパケットを廃棄します。	レベル 2 (標準)	NAPT による外部からのパケット廃棄に加えて、送信フィルタにより、内部からの通信を制限します。
宛先 IP アドレス	0.0.0.0/8																						
	127.0.0.0/8																						
	169.254.0.0/16																						
	224.0.0.0/4																						
宛先ポート番号	135																						
	137																						
	138																						
	139																						
	445																						
送信元ポート番号	135																						
	137																						
	138																						
	139																						
	445																						
レベル 1 (オフ)	NAPT により外部からのパケットを廃棄します。																						
レベル 2 (標準)	NAPT による外部からのパケット廃棄に加えて、送信フィルタにより、内部からの通信を制限します。																						

3. かんたん設定

(5) [フレッツ・VPNワイドの設定]の各項目を設定し、[次へ]ボタンをクリックします。

メモ インターネット接続の設定に戻る場合は、[戻る]ボタンをクリックしてください。

拠点の場合

1. パスワードの設定 → 2. インターネット接続の設定 → 3. フレッツ・VPNワイドの設定 → 4. NetMeisterの設定 → 5. 設定の確認と反映 → 6. 終了

かんたん設定：フレッツ・VPNワイドの設定

VPN回線と接続するWAN側インタフェースとVPNを設定します。

	現在の設定	設定の変更
接続種別		<input checked="" type="radio"/> ダイナミックVPN

WAN2: フレッツ・VPNワイドの設定(GigaEthernet0.2)

フレッツ・VPNワイドの拠点間通信を行うためにダイナミックVPNを使用します。

	現在の設定	設定の変更
ユーザ名		フレッツ・VPNワイドを申し込んだ際のユーザ名を設定します。 (通常はユーザ名には@を含んでいます) <input type="text"/> 文字列(半角英数字)を入力してください。
パスワード		フレッツ・VPNワイドを申し込んだ際のパスワードを設定します。 <input type="text"/> 文字列(半角英数字)を入力してください。
IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定

ダイナミックVPNの設定

2 拠点間通信でもセンタは必要です。いずれかの拠点で必ずセンタを選択してください。
タイプや拠点番号を変更すると、LAN側IPアドレスが変更されます。

	現在の設定	設定の変更
タイプ		<input checked="" type="radio"/> 拠点 <input type="radio"/> センタ
拠点番号		他の拠点と同じ番号は設定しないでください。 1 ▾
パスワード		すべての拠点で共通のパスワードを設定してください。 <input type="text"/> 文字列(半角英数字)を入力してください。
センタWAN側IPアドレス		センタ装置のWANに設定されているIPアドレスまたはドメイン名を入力してください。 <input type="text"/> 入力形式が不正です。

LAN1: LANの設定(GigaEthernet1.0)

他の拠点と重複しないように設定してください。
LAN側IPアドレスを変更する場合は、反映後に新しいIPアドレスで接続しなおす必要があります。

	現在の設定	設定の変更
LAN側IPアドレス	192.168.100.1/24	<input checked="" type="radio"/> 自動設定 <input type="radio"/> 手動設定 192.168.1.254 / 24 ▾ 自動設定で上記アドレスに設定されます。

戻る 次へ

3. かんたん設定

番号	項目	内容
①	ユーザ名	フレッツ・VPN ワイドを申し込んだ際のユーザ名を設定します。 (通常はユーザ名には@を含んでいます) ・ 半角英数字で1～59文字まで入力できます。
②	パスワード	フレッツ・VPN ワイドを申し込んだ際のパスワードを設定します。 ・ 半角英数字で1～79文字まで入力できます。 注意 ・ 大文字、小文字も区別されます。
③	IPアドレス	フレッツ・VPN ワイドに接続するWAN 側 IP アドレスを設定します。 ・ 「自動取得」を選択します。特定のアドレスを固定的に設定したい場合は「手動設定」を選択してください。 ・ 「手動設定」を選択したときは、フレッツ・VPN ワイド申請時に通知された IP アドレスを入力し、サブネットマスクをプルダウンメニューから選択します。 注意 ・ 他のインタフェースに設定されている IP アドレスを使用することはできません。 ・ 「自動取得」を選択した場合、IP アドレスを入力することはできません。
④	タイプ	「拠点」を選択します。
⑤	拠点番号	拠点の識別番号です。 他の拠点と重複しない任意の番号(1～64)を設定します。 注意 ・ 本設定が反映されると、ルータの LAN 側 IP アドレスが自動的に変更されます。
⑥	パスワード	VPN 接続で使用するパスワード(事前共有鍵)です。 すべての拠点で同じ任意のパスワードを設定してください。 ・ 半角英数字で1～128文字まで入力できます。
⑦	センタ WAN 側 IP アドレス	センタ装置の WAN に設定されている IP アドレスまたはドメイン名を入力します。
⑧	LAN 側 IP アドレス	他の拠点と重複しないように IP アドレスを設定します。 注意 ・ LAN 側 IP アドレスを変更する場合は、反映後に新しい IP アドレスで接続しなおす必要があります。

3. かんたん設定

センタの場合

1. パスワードの設定 → 2. インターネット接続の設定 → 3. **フレッツ・VPNワイドの設定** →
4. NetMeisterの設定 → 5. 設定の確認と反映 → 6. 終了

かんたん設定：フレッツ・VPNワイドの設定

VPN回線と接続するWAN側インタフェースとVPNを設定します。

	現在の設定	設定の変更
接続種別		<input checked="" type="radio"/> ダイナミックVPN

WAN2: フレッツ・VPNワイドの設定(GigaEthernet0.2)

フレッツ・VPNワイドの拠点間通信を行うためにダイナミックVPNを使用します。

	現在の設定	設定の変更
ユーザ名		フレッツ・VPNワイドを申し込んだ際のユーザ名を設定します。 (通常はユーザ名には@を含んでいます) <input type="text"/> 文字列(半角英数字)を入力してください。
パスワード		フレッツ・VPNワイドを申し込んだ際のパスワードを設定します。 <input type="text"/> 文字列(半角英数字)を入力してください。
IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定

ダイナミックVPNの設定

2 拠点間通信でもセンタは必要です。いずれかの拠点で必ずセンタを選択してください。
タイプや拠点番号を変更すると、LAN側IPアドレスが変更されます。

	現在の設定	設定の変更
タイプ		<input type="radio"/> 拠点 <input checked="" type="radio"/> センタ
パスワード		すべての拠点で共通のパスワードを設定してください。 <input type="text"/> 文字列(半角英数字)を入力してください。

LAN1: LANの設定(GigaEthernet1.0)

他の拠点と重複しないように設定してください。

LAN側IPアドレスを変更する場合は、反映後に新しいIPアドレスで接続しなおす必要があります。

	現在の設定	設定の変更
LAN側IPアドレス	192.168.100.1/24	<input checked="" type="radio"/> 自動設定 <input type="radio"/> 手動設定 192.168.254.254 / 24 自動設定で上記アドレスに設定されます。

戻る 次へ

3. かんたん設定

番号	項目	内容
①	ユーザ名	フレッツ・VPN ワイドを申し込んだ際のユーザ名を設定します。 (通常はユーザ名には@を含んでいます) ・ 半角英数字で 1～59 文字まで入力できます。
②	パスワード	フレッツ・VPN ワイドを申し込んだ際のパスワードを設定します。 ・ 半角英数字で 1～79 文字まで入力できます。 注意 ・ 大文字、小文字も区別されます。
③	IP アドレス	フレッツ・VPN ワイドに接続する WAN 側 IP アドレスを設定します。 ・ 「自動取得」を選択します。特定のアドレスを固定的に設定したい場合は「手動設定」を選択してください。 ・ 「手動設定」を選択したときは、フレッツ・VPN ワイド申請時に通知された IP アドレスを入力し、サブネットマスクをプルダウンメニューから選択します。 注意 ・ 他のインタフェースに設定されている IP アドレスを使用することはできません。 ・ 「自動取得」を選択した場合、IP アドレスを入力することはできません。
④	タイプ	「センタ」を選択します。 注意 ・ 本設定が反映されると、ルータの LAN 側 IP アドレスが自動的に変更されます。
⑤	パスワード	VPN 接続で使用するパスワード(事前共有鍵)です。 拠点に設定したパスワードと同じパスワードを設定してください。 ・ 半角英数字で 1～128 文字まで入力できます。
⑥	LAN 側 IP アドレス	他の拠点と重複しないように IP アドレスを設定します。 注意 ・ LAN 側 IP アドレスを変更する場合は、反映後に新しい IP アドレスで接続しなおす必要があります。

(6) [NetMeister の設定]の項目を設定し、[設定の確認]ボタンをクリックします。

メモ フレッツ・VPN ワイドの設定に戻る場合は、[戻る]ボタンをクリックしてください。

1. パスワードの設定 → 2. インターネット接続の設定 → 3. フレッツ・VPNワイドの設定 → 4. NetMeisterの設定 → 5. 設定の確認と反映 → 6. 終了

かんたん設定 : NetMeisterの設定

NetMeisterの設定を行います。
Web設定では、IPv4で動作する設定のみ対応しています。

NetMeister 無効 有効

設定の変更

戻る **設定の確認**

番号	項目	内容
①	NetMeister	NetMeister の「有効」 / 「無効」を設定します。 「有効」に設定すると、アカウント名等を設定することができます。

3. かんたん設定

「有効」を選択するとアカウント名等の設定項目が表示されますので、各項目を設定し、[設定の確認]ボタンをクリックします。

1. パスワードの設定 → 2. インターネット接続の設定 → 3. フレッツ・VPNワイドの設定 → 4. NetMeisterの設定 → 5. 設定の確認と反映 → 6. 終了

かんたん設定：NetMeisterの設定

NetMeisterの設定を行います。
Web設定では、IPv4で動作する設定のみ対応しています。

設定の変更	
NetMeister	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
アカウント名	NetMeisterの登録ページで申請した「グループID」を入力してください。 <input type="text"/> 文字列を入力してください。[2-63文字]
パスワード	NetMeisterの登録ページで申請した「グループパスワード」を入力してください。 <input type="radio"/> パスワードを変更しない <input checked="" type="radio"/> パスワードを変更する <input type="text"/> 文字列を入力してください。[8-31文字]
ホスト名 (装置名)	『装置名の設定』で設定した装置名を通知します。 <input type="text" value="web-trial1"/>
拠点ID	省略した場合、装置名を通知します。 <input type="text"/>

番号	項目	内容
①	NetMeister	NetMeisterの「有効」／「無効」を設定します。 「無効」に設定すると、アカウント名等の設定項目が隠れます。
②	アカウント名	NetMeisterの登録ページで申請した「グループID」を設定します。 ・半角英数字または-(ハイフン)で2～63文字まで入力できます。
③	パスワード	NetMeisterの登録ページで申請した「グループパスワード」を設定します。 ・半角英数字、_(アンダーバー)または-(ハイフン)で8～31文字まで入力できます。 注意 ・大文字／小文字は区別されます。 ・パスワードの入力文字は表示されません。●●●のように伏せ文字で表示されます。 ・パスワードは、第三者に推測されにくく、忘れないような文字列を入力してください。
④	ホスト名 (装置名)	NetMeisterに通知するホスト名を変更する必要がある場合は、ここで設定します。 ・半角英数字または-(ハイフン)で2～63文字まで入力できます。 メモ ・NetMeisterで受け付けられない文字を装置名に指定している場合等に利用します。 ・大文字は、小文字に変換してNetMeisterに通知されます。 注意 ・ホスト名の先頭と最後には-(ハイフン)を利用することができません。
⑤	サイト名 (拠点名)	NetMeisterに通知するサイト名を変更する必要がある場合は、ここで設定します。 ・半角英数字または-(ハイフン)で2～31文字まで入力できます。 メモ ・NetMeisterで受け付けられない文字を装置名に指定している場合等に利用します。 ・大文字は、小文字に変換してNetMeisterに通知されます。 ・サイト名を省略した場合は、装置名がNetMeisterに通知されます。 注意 ・サイト名の先頭と最後には-(ハイフン)を利用することができません。

3. かんたん設定

(7) 入力した項目が正しいことを確認し、[反映]ボタンをクリックします。

メモ NetMeister の設定に戻る場合は、[戻る]ボタンをクリックしてください。

注意 本設定が反映されると、ルータの LAN 側 IP アドレスが自動的に変更されるため、Web 設定画面の接続が切れてしまいます。
Web 設定画面に再接続するには、パソコンの IP アドレスを取得し直す必要がありますので、[反映]ボタンをクリック後に、一旦パソコンのイーサネットケーブルを抜いて、あらためて挿し直してください。
また、Web 設定画面に接続するための IP アドレスは、LAN 側 IP アドレスの欄に表示されているアドレス(*)に変わります。Web ブラウザのアドレスバーに半角英数字で「https://<新しい LAN 側 IP アドレス>/」と入力し、[Enter]キーを押してください。

3. かんたん設定

1. パスワードの設定 → 2. インターネット接続の設定 → 3. フレッツ・VPNワイドの設定 →
 4. NetMeisterの設定 → 5. 設定の確認と反映 → 6. 終了

かんたん設定：設定の確認と反映

設定内容を変更する場合は [反映] を押してください。
 LAN側IPアドレスを変更する場合は、新しいIPアドレスで接続しなおしてください。

ログイン認証用パスワードの設定

	現在の設定	設定の変更
ユーザ名	admin	変更できません
パスワード	パスワード設定なし	<input type="radio"/> パスワードを変更しない <input checked="" type="radio"/> パスワードを変更する <input type="password" value=""/> <input type="password" value=""/> 確認のためもう一度入力してください。 <input type="password" value=""/> <input type="password" value=""/>

インターネット接続の設定

	現在の設定	設定の変更
接続形態		<input checked="" type="radio"/> PPPoE接続 (フレッツ光回線利用の場合)

WAN1: PPPoE接続の設定(GigaEthernet0.1)

	現在の設定	設定の変更
ユーザ名		プロバイダから通知されているユーザ名を設定します。 (フレッツの場合、通常はユーザ名には@を含んでいます) <input type="text" value="user@example.com"/>
パスワード		プロバイダから通知されているパスワードを設定します。 <input type="text" value="user-password"/>
WAN側IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
DNSアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定

通信セキュリティの設定

	現在の設定	設定の変更
セキュリティ強度	レベル1	<input checked="" type="radio"/> レベル1 - 外部からの不要なパケットをNAPTにより廃棄します。 <input type="radio"/> レベル2 - 外部からの不要なパケットをNAPTにより廃棄します。 - 内部からの不要な通信を制限します。

フレッツ・VPNワイドとVPNの設定

	現在の設定	設定の変更
接続種別		<input checked="" type="radio"/> ダイナミックVPN

WAN2: フレッツ・VPNワイドの設定(GigaEthernet0.2)

	現在の設定	設定の変更
ユーザ名		フレッツ・VPNワイドを申し込んだ際のユーザ名を設定します。 (通常はユーザ名には@を含んでいます) <input type="text" value="wide@example.com"/>
パスワード		フレッツ・VPNワイドを申し込んだ際のパスワードを設定します。 <input type="text" value="wide-password"/>
IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定

ダイナミックVPNの設定

	現在の設定	設定の変更
タイプ		<input checked="" type="radio"/> 拠点 <input type="radio"/> センタ
拠点番号		他の拠点と同じ番号は設定しないでください。 <input type="text" value="1"/>
パスワード		すべての拠点で共通のパスワードを設定してください。 <input type="text" value="vpn-password"/>
センタWAN側IPアドレス		センタ装置のWANに設定されているIPアドレスまたはドメイン名を入力してください。 <input type="text" value=""/>

LAN1: LANの設定(GigaEthernet1.0)

	現在の設定	設定の変更
LAN側IPアドレス		<input checked="" type="radio"/> 自動設定 <input type="radio"/> 手動設定 <input type="text" value="192.168.1.254"/> / 24 自動設定で上位アドレスに設定されます。

NetMeisterの設定

	設定の変更
NetMeister	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効

戻る **反映**

3. かんたん設定

- (8) 「設定内容を変更しました。」のメッセージが表示されることを確認し、[トップページへ]ボタンを押します。

注意 本画面が表示されない場合、Web 設定画面の接続が切れています。パソコンの IP アドレスを再取得後、新しい LAN 側 IP アドレスに接続しなおしてください。

3. かんたん設定

1. パスワードの設定 → 2. インターネット接続の設定 → 3. フレッツ・VPNワイドの設定 →
4. NetMeisterの設定 → 5. 設定の確認と反映 → 6. 終了

かんたん設定：設定の確認と反映

設定内容を変更しました。

ログイン認証用パスワードの設定

	現在の設定	設定の変更
ユーザ名	admin	変更できません
パスワード	パスワード設定なし	<input type="radio"/> パスワードを変更しない <input checked="" type="radio"/> パスワードを変更する ***** 確認のためもう一度入力してください。 *****

インターネット接続の設定

	現在の設定	設定の変更
接続形態		<input checked="" type="radio"/> PPPoE接続 (フレッツ光回線利用の場合)

WAN1: PPPoE接続の設定(GigaEthernet0.1)

	現在の設定	設定の変更
ユーザ名		プロバイダから通知されているユーザ名を設定します。 (フレッツの場合、通常はユーザ名には@を含んでいます) user@example.com
パスワード		プロバイダから通知されているパスワードを設定します。 user-password
WAN側IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
DNSアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定

通信セキュリティの設定

	現在の設定	設定の変更
セキュリティ強度	レベル1	<input checked="" type="radio"/> レベル1 - 外部からの不要なパケットをNAPTにより廃棄します。 <input type="radio"/> レベル2 - 外部からの不要なパケットをNAPTにより廃棄します。 - 内部からの不要な通信を制限します。

フレッツ・VPNワイドとVPNの設定

	現在の設定	設定の変更
接続種別		<input checked="" type="radio"/> ダイナミックVPN

WAN2: フレッツ・VPNワイドの設定(GigaEthernet0.2)

	現在の設定	設定の変更
ユーザ名		フレッツ・VPNワイドを申し込んだ際のユーザ名を設定します。 (通常はユーザ名には@を含んでいます) wide@example.com
パスワード		フレッツ・VPNワイドを申し込んだ際のパスワードを設定します。 wide-password
IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定

ダイナミックVPNの設定

	現在の設定	設定の変更
タイプ		<input checked="" type="radio"/> 拠点 <input type="radio"/> センタ
拠点番号		他の拠点と同じ番号は設定しないでください。 1
パスワード		すべての拠点で共通のパスワードを設定してください。 vpn-password
センタWAN側IPアドレス		センタ装置のWANに設定されているIPアドレスまたはドメイン名を入力してください。 []

LAN1: LANの設定(GigaEthernet1.0)

	現在の設定	設定の変更
LAN側IPアドレス		<input checked="" type="radio"/> 自動設定 <input type="radio"/> 手動設定 192.168.1.254 / 24 自動設定で上記アドレスに設定されます。


NetMeisterの設定

	設定の変更
NetMeister	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効

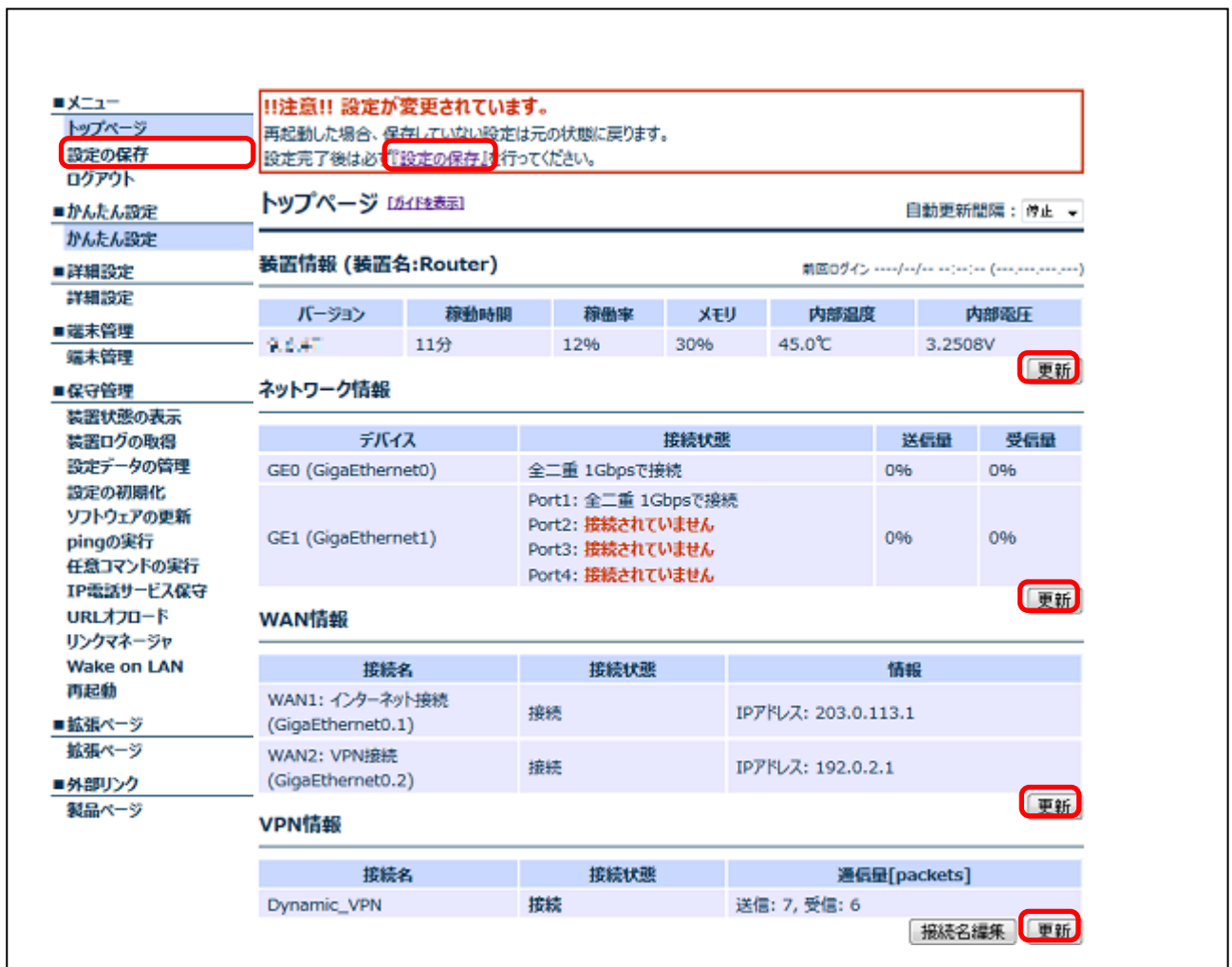
トップページへ

3. かんたん設定

(9) トップページでWAN 情報とVPN 情報の接続状態を確認します。

 [更新]ボタンをクリックすると、情報を更新することが可能です。

(10) メニューエリア、または、メッセージエリアから[設定の保存]をクリックします。



!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず「設定の保存」を行ってください。

メニュー
トップページ
設定の保存
ログアウト

かんたん設定
かんたん設定

詳細設定
詳細設定

端末管理
端末管理

保守管理
装置状態の表示
装置ログの取得
設定データの管理
設定の初期化
ソフトウェアの更新
pingの実行
任意コマンドの実行
IP電話サービス保守
URLオフロード
リンクマネージャ
Wake on LAN
再起動

拡張ページ
拡張ページ

外部リンク
製品ページ

トップページ [\[アイコン表示\]](#) 自動更新間隔: 停止

装置情報 (装置名: Router) 前回ログイン: ----/--/-- :--:--:-- (---:---:---:---)

バージョン	稼働時間	稼働率	メモリ	内部温度	内部電圧
3.1.4	11分	12%	30%	45.0℃	3.2508V

ネットワーク情報

デバイス	接続状態	送信量	受信量
GE0 (GigaEthernet0)	全二重 1Gbpsで接続	0%	0%
GE1 (GigaEthernet1)	Port1: 全二重 1Gbpsで接続 Port2: 接続されていません Port3: 接続されていません Port4: 接続されていません	0%	0%

WAN情報

接続名	接続状態	情報
WAN1: インターネット接続 (GigaEthernet0.1)	接続	IPアドレス: 203.0.113.1
WAN2: VPN接続 (GigaEthernet0.2)	接続	IPアドレス: 192.0.2.1

VPN情報

接続名	接続状態	通信量[packets]
Dynamic_VPN	接続	送信: 7, 受信: 6

接続名編集 更新

(11) VPN 情報は、接続名にマウスカーソルを近づけることで、詳細情報を確認することができます。また、接続名をわかりやすいように変更することができます。



VPN情報

接続名	接続状態	通信量[packets]
Dynamic_VPN	接続	送信: 96, 受信: 129

ダイナミックVPN(センタ)
IPアドレス: 203.0.113.254

接続名編集 更新

3. かんたん設定

	項目	内容
①	接続名	接続名を設定します。 ・ 半角英数字 1～128 文字まで、または全角文字で 1～32 文字まで入力できます。

(12) [保存実行]ボタンをクリックします。

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず「[設定の保存](#)」を行ってください。

設定の保存

設定を保存します。

よろしければ [保存実行] を押してください。

保存実行

(13) 「設定を保存しました。」のメッセージを確認します。

設定の保存

設定を保存しました。

[トップページへ](#)

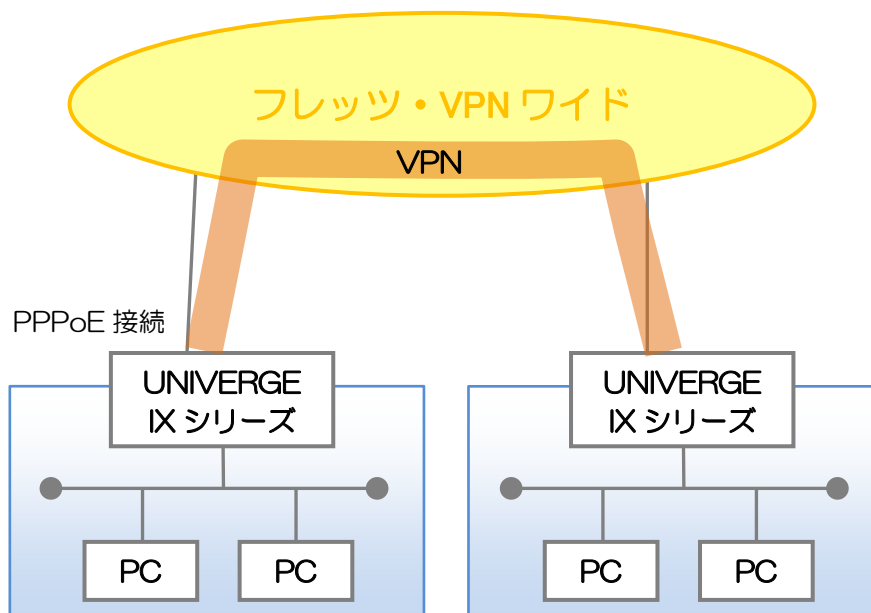
メモ 確実に VPN 接続するため、設定の保存後、再起動実行を推奨します。

3. かんたん設定

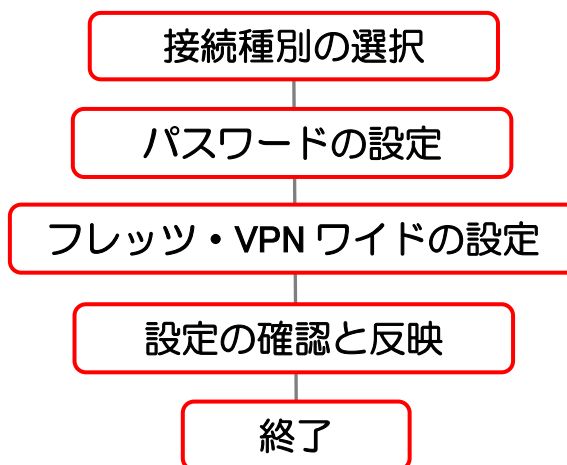
3.4 フレッツ・VPN ワイド接続

フレッツ・VPN ワイド(端末型払い出し)を使用した拠点間通信の設定を行います。

【構成イメージ】



【設定手順】



3. かんたん設定

(1) ログイン後のメニューエリアから[かんたん設定]をクリックします。

メモ トップページリンクをクリックすることで、接続種別の各ページに移動することも可能です。

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず「設定の保存」を行ってください。

管理者メニュー
トップページ
設定の保存
ログアウト

かんたん設定
かんたん設定

詳細設定
詳細設定

端末管理
端末管理

保守管理
装置状態の表示
装置ログの取得
設定データの管理
設定の初期化
ソフトウェアの更新
pingの実行
任意コマンドの実行
IP電話サービス保守
URLオフロード
リンクマネージャ
Wake on LAN
再起動

拡張ページ
拡張ページ

外部リンク
製品ページ

トップページ
ルータの設定を開始します。以下のリンクから選択してください。
パスワードを登録・変更する前にユーザ名とパスワードを入力する画面が表示された場合は、そのまま「OK」をクリックしてください。

かんたん設定

- [インターネット接続](#)
フレット光などの有線回線やワイヤレス回線(3G・LTE)を使用して、インターネットに接続する設定を行います。
- [インターネット接続+VPN接続](#)
フレット光などの有線回線やワイヤレス回線(3G・LTE)を使用したインターネット接続と、インターネットVPNによる拠点間通信の設定を行います。
- [インターネット接続+フレット・VPNワイド接続](#)
フレット光を使用したインターネット接続と、フレット・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
- **フレット・VPNワイド接続**
フレット・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
- [NGN網VPN接続](#)
NGN網を用いたVPNによる拠点間の通信の設定と、NetMeisterによる装置管理の設定を行います。
- [IPv6 IPoE接続](#)
IPv6 IPoE接続の設定を行います。
プロバイダの動的IPまたは固定IPでのサービスを設定します。
- [クラウド接続](#)
インターネットVPNや専用線を使用したクラウド接続の設定を行います。
- [IP電話サービス接続](#)
対応するUNIVERGE Aspireシリーズと連携したIP電話ネットワークの設定を行います。

詳細設定
インタフェースやサーバのアドレスを指定したり、フィルタやQoS、VPN等、かんたん設定に含まれない詳細な設定を行う場合はこちらから設定してください。

端末管理
本装置に接続されている端末を管理します。
リンクマネージャ機能やWeb認証機能を設定します。

保守管理
装置状態の確認、ソフトウェアの更新、pingの実行など、各種保守機能の操作を行います。
URLオフロード機能による特定宛先のルーティング制御、リンクマネージャ機能による端末の保守管理などが可能です。
任意のコマンドを直接実行したい場合は[任意コマンドの実行](#)から操作してください。

3. かんたん設定

(2) 接続種別の選択で「フレッツ・VPNワイド接続」にチェックを入れ、[次へ] ボタンをクリックします。

メモ 接続種別を変更する場合には、設定の初期化が必要となります。

かんたん設定：接続種別の選択

接続種別を選択してかんたん設定を開始してください。
接続種別を変更する場合には「設定の初期化」が必要となります。

	現在の設定	設定の変更
接続種別の選択	インターネット接続なし	<input type="radio"/> インターネット接続 フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用して、インターネットに接続する設定を行います。
		<input type="radio"/> インターネット接続 + VPN接続 フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用したインターネット接続と、インターネットVPNによる拠点間通信の設定を行います。
		<input type="radio"/> インターネット接続 + フレッツ・VPNワイド接続 フレッツ光を使用したインターネット接続と、フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
		<input checked="" type="radio"/> フレッツ・VPNワイド接続 フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
		<input type="radio"/> NGN網VPN接続 NGN網を用いたVPNによる拠点間の通信の設定とNetMeisterによる装置管理の設定を行います。
		<input type="radio"/> IPv6 IPoE接続 IPv6 IPoE接続の設定を行います。 プロバイダの動的IPまたは固定IPでのサービスを設定します。
		<input type="radio"/> クラウド接続 インターネットVPNや専用線を使用したクラウド接続の設定を行います。
		<input type="radio"/> IP電話サービス接続 対応するUNIVERGE Aspireシリーズと連携したIP電話ネットワークの設定を行います。

次へ

3. かんたん設定

(3) 管理者パスワードを変更する場合は、[パスワードを変更する]を選択し、パスワードを設定した後、[次へ]ボタンをクリックします。

メモ 管理者パスワードを変更する必要がある場合は、そのまま[次へ]ボタンをクリックします。

メモ 接続種別の選択に戻る場合は、[戻る]ボタンをクリックしてください。

1. パスワードの設定 → 2. フレッツ・VPNワイドの設定 → 3. 設定の確認と反映 → 4. 終了

かんたん設定：パスワードの設定

ログイン認証用のパスワードを設定します。

	現在の設定	設定の変更
ユーザ名	admin	変更できません
パスワード	パスワード設定なし	<input type="radio"/> パスワードを変更しない <input checked="" type="radio"/> パスワードを変更する <input type="text"/> 確認のためもう一度入力してください。 <input type="text"/> パスワードを入力してください。

戻る 次へ

番号	項目	内容
①	ユーザ名	本装置にログインするときのユーザ名です。 <ul style="list-style-type: none">初期状態ではユーザ名は設定されていません。パスワード設定後のユーザ名は「admin」です。Web 設定からは変更できません。
②	パスワード	本装置にログインするときのパスワードです。 <ul style="list-style-type: none">初期状態ではパスワードは設定されていません。半角英数字 1~249 文字で入力します。 注意 <ul style="list-style-type: none">大文字/小文字は区別されます。パスワードの入力文字は表示されません。●●●のように伏せ文字で表示されます。パスワードは、第三者に推測されにくく、忘れないような文字列を入力してください。

3. かんたん設定

(4) [フレッツ・VPNワイドの設定]の各項目を設定し、[設定の確認]ボタンをクリックします。

パスワードの設定に戻る場合は、[戻る]ボタンをクリックしてください。

拠点の場合

1. パスワードの設定 → 2. フレッツ・VPNワイドの設定 → 3. 設定の確認と反映 → 4. 終了

かんたん設定：フレッツ・VPNワイドの設定

VPN回線と接続するWAN側インタフェースとVPNを設定します。

	現在の設定	設定の変更
接続種別		<input checked="" type="radio"/> ダイナミックVPN

WAN1: フレッツ・VPNワイドの設定(GigaEthernet0.1)

フレッツ・VPNワイドの拠点間通信を行うためにダイナミックVPNを使用します。

	現在の設定	設定の変更
ユーザ名		フレッツ・VPNワイドを申し込んだ際のユーザ名を設定します。 (通常はユーザ名には@を含んでいます) <input type="text"/> 文字列(半角英数字)を入力してください。
パスワード		フレッツ・VPNワイドを申し込んだ際のパスワードを設定します。 <input type="text"/> 文字列(半角英数字)を入力してください。
IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
DNSアドレス		<input checked="" type="radio"/> 自動設定 <input type="radio"/> 手動設定

ダイナミックVPNの設定

2 拠点間通信でもセンタは必要です。いずれかの拠点で必ずセンタを選択してください。

タイプや拠点番号を変更すると、LAN側IPアドレスが変更されます。

	現在の設定	設定の変更
タイプ		<input checked="" type="radio"/> 拠点 <input type="radio"/> センタ
拠点番号		他の拠点と同じ番号は設定しないでください。 1 <input type="text"/>
パスワード		すべての拠点で共通のパスワードを設定してください。 <input type="text"/> 文字列(半角英数字)を入力してください。
センタWAN側IPアドレス		センタ装置のWANに設定されているIPアドレスまたはドメイン名を入力してください。 <input type="text"/> 入力形式が不正です。

LAN1: LANの設定(GigaEthernet1.0)

他の拠点と重複しないように設定してください。

LAN側IPアドレスを変更する場合は、反映後に新しいIPアドレスで接続しなおす必要があります。

	現在の設定	設定の変更
LAN側IPアドレス	192.168.100.1/24	<input checked="" type="radio"/> 自動設定 <input type="radio"/> 手動設定 192.168.1.254 / 24 <input type="text"/> 自動設定で上記アドレスに設定されます。

3. かんたん設定

番号	項目	内容
①	ユーザ名	フレッツ・VPN ワイドを申し込んだ際のユーザ名を設定します。 (通常はユーザ名には@を含んでいます) ・ 半角英数字で 1～59 文字まで入力できます。
②	パスワード	フレッツ・VPN ワイドを申し込んだ際のパスワードを設定します。 ・ 半角英数字で 1～79 文字まで入力できます。 注意 ・ 大文字、小文字も区別されます。
③	IP アドレス	フレッツ・VPN ワイドに接続する WAN 側 IP アドレスを設定します。 ・ 「自動取得」を選択します。特定のアドレスを固定的に設定したい場合は「手動設定」を選択してください。 ・ 「手動設定」を選択したときは、フレッツ・VPN ワイド申請時に通知された IP アドレスを入力し、サブネットマスクをプルダウンメニューから選択します。 注意 ・ 他のインタフェースに設定されている IP アドレスを使用することはできません。 ・ 「自動取得」を選択した場合、IP アドレスを入力することはできません。
④	DNS アドレス	PPPoE 接続の DNS サーバのアドレスを設定します。 ・ プロバイダから DNS サーバのアドレスが与えられていないときは「自動取得」を、与えられているとき、または独自に指定するときは「手動設定」を選択します。 ・ 「手動設定」を選択したときは、プロバイダから与えられたプライマリ DNS サーバの IP アドレスを上段に、セカンダリ DNS サーバの IP アドレスを下段に入力します。セカンダリは省略可能です。 注意 ・ 「自動取得」を選択した場合、DNS アドレスを入力することはできません。
⑤	タイプ	「拠点」を選択します。
⑥	拠点番号	拠点の識別番号です。 他の拠点と重複しない任意の番号(1～64)を設定します。 注意 ・ 本設定が反映されると、ルータの LAN 側 IP アドレスが自動的に変更されます。
⑦	パスワード	VPN 接続で使用するパスワード(事前共有鍵)です。 すべての拠点で同じ任意のパスワードを設定してください。 ・ 半角英数字で 1～128 文字まで入力できます。
⑧	センタ WAN 側 IP アドレス	センタ装置の WAN に設定されている IP アドレスまたはドメイン名を入力します。
⑨	LAN 側 IP アドレス	他の拠点と重複しないように IP アドレスを設定します。 注意 ・ LAN 側 IP アドレスを変更する場合は、反映後に新しい IP アドレスで接続しなおす必要があります。

3. かんたん設定

センタの場合

1. パスワードの設定 → 2. フレッツ・VPNワイドの設定 → 3. 設定の確認と反映 → 4. 終了

かんたん設定：フレッツ・VPNワイドの設定

VPN回線と接続するWAN側インタフェースとVPNを設定します。

	現在の設定	設定の変更
接続種別		<input checked="" type="radio"/> ダイナミックVPN

WAN1: フレッツ・VPNワイドの設定(GigaEthernet0.1)

フレッツ・VPNワイドの拠点間通信を行うためにダイナミックVPNを使用します。

	現在の設定	設定の変更
ユーザ名		フレッツ・VPNワイドを申し込んだ際のユーザ名を設定します。 (通常はユーザ名には@を含んでいます) <input type="text"/> 文字列(半角英数字)を入力してください。
パスワード		フレッツ・VPNワイドを申し込んだ際のパスワードを設定します。 <input type="text"/> 文字列(半角英数字)を入力してください。
IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
DNSアドレス		<input checked="" type="radio"/> 自動設定 <input type="radio"/> 手動設定

ダイナミックVPNの設定

2 拠点間通信でもセンタは必要です。いずれかの拠点で必ずセンタを選択してください。

タイプや拠点番号を変更すると、LAN側IPアドレスが変更されます。

	現在の設定	設定の変更
タイプ		<input type="radio"/> 拠点 <input checked="" type="radio"/> センタ
パスワード		すべての拠点で共通のパスワードを設定してください。 <input type="text"/> 文字列(半角英数字)を入力してください。

LAN1: LANの設定(GigaEthernet1.0)

他の拠点と重複しないように設定してください。

LAN側IPアドレスを変更する場合は、反映後に新しいIPアドレスで接続しなおす必要があります。

	現在の設定	設定の変更
LAN側IPアドレス	192.168.1.254/24	<input checked="" type="radio"/> 自動設定 <input type="radio"/> 手動設定 192.168.254.254 / 24 自動設定で上記アドレスに設定されます。

戻る

設定の確認

3. かんたん設定

番号	項目	内容
①	ユーザ名	フレッツ・VPN ワイドを申し込んだ際のユーザ名を設定します。 (通常はユーザ名には@を含んでいます) ・ 半角英数字で1～59文字まで入力できます。
②	パスワード	フレッツ・VPN ワイドを申し込んだ際のパスワードを設定します。 ・ 半角英数字で1～128文字まで入力できます。 注意 ・ 大文字、小文字も区別されます。
③	IP アドレス	フレッツ・VPN ワイドに接続する WAN 側 IP アドレスを設定します。 ・ 「自動取得」を選択します。特定のアドレスを固定的に設定したい場合は「手動設定」を選択してください。 ・ 「手動設定」を選択したときは、フレッツ・VPN ワイド申請時に通知された IP アドレスを入力し、サブネットマスクをプルダウンメニューから選択します。 注意 ・ 他のインタフェースに設定されている IP アドレスを使用することはできません。 ・ 「自動取得」を選択した場合、IP アドレスを入力することはできません。
④	DNS アドレス	PPPoE 接続の DNS サーバのアドレスを設定します。 ・ プロバイダから DNS サーバのアドレスが与えられていないときは「自動取得」を、与えられているとき、または独自に指定するときは「手動設定」を選択します。 ・ 「手動設定」を選択したときは、プロバイダから与えられたプライマリ DNS サーバの IP アドレスを上段に、セカンダリ DNS サーバの IP アドレスを下段に入力します。セカンダリは省略可能です。 注意 ・ 「自動取得」を選択した場合、DNS アドレスを入力することはできません。
⑤	タイプ	「センタ」を選択します。 注意 ・ 本設定が反映されると、ルータの LAN 側 IP アドレスが自動的に変更されます。
⑥	パスワード	VPN 接続で使用するパスワード(事前共有鍵)です。 拠点に設定したパスワードと同じパスワードを設定してください。 ・ 半角英数字で1～79文字まで入力できます。
⑦	LAN 側 IP アドレス	他の拠点と重複しないように IP アドレスを設定します。 注意 ・ LAN 側 IP アドレスを変更する場合は、反映後に新しい IP アドレスで接続しなおす必要があります。

(5) 入力した項目が正しいことを確認し、[反映]ボタンをクリックします。

メモ フレッツ・VPN ワイドの設定に戻る場合は、[戻る]ボタンをクリックしてください。

注意 本設定が反映されると、ルータの LAN 側 IP アドレスが自動的に変更されるため、Web 設定画面の接続が切れてしまいます。
Web 設定画面に再接続するには、パソコンの IP アドレスを取得し直す必要がありますので、[反映]ボタンをクリック後に、一旦パソコンのイーサネットケーブルを抜いて、あらためて挿し直してください。
また、Web 設定画面に接続するための IP アドレスは、LAN 側 IP アドレスの欄に表示されているアドレス(*)が変わります。Web ブラウザのアドレスバーに半角英数字で「https://<新しい LAN 側 IP アドレス>/」と入力し、[Enter]キーを押してください。

3. かんたん設定

1. パスワードの設定 → 2. フレッツ・VPNワイドの設定 → 3. 設定の確認と反映 → 4. 終了

かんたん設定：設定の確認と反映

設定内容を変更する場合は [反映] を押してください。
LAN側IPアドレスを変更する場合は、新しいIPアドレスで接続しなおしてください。

ログイン認証用パスワードの設定

	現在の設定	設定の変更
ユーザ名	admin	変更できません
パスワード	パスワード設定なし	<input type="radio"/> パスワードを変更しない <input checked="" type="radio"/> パスワードを変更する 確認のためもう一度入力してください。

フレッツ・VPNワイドとVPNの設定

	現在の設定	設定の変更
接続種別		<input checked="" type="radio"/> ダイナミックVPN

WAN1: フレッツ・VPNワイドの設定(GigaEthernet0.1)

	現在の設定	設定の変更
ユーザ名		フレッツ・VPNワイドを申し込んだ際のユーザ名を設定します。 (通常はユーザ名には@を含んでいます) flets@example.com
パスワード		フレッツ・VPNワイドを申し込んだ際のパスワードを設定します。 flets-password
IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
DNSアドレス		<input checked="" type="radio"/> 自動設定 <input type="radio"/> 手動設定

ダイナミックVPNの設定

	現在の設定	設定の変更
タイプ		<input checked="" type="radio"/> 拠点 <input type="radio"/> センタ
拠点番号		他の拠点と同じ番号は設定しないでください。 1
パスワード		すべての拠点で共通のパスワードを設定してください。 vpn-password
センタWAN側IPアドレス		センタ装置のWANに設定されているIPアドレスまたはドメイン名を入力してください。

LAN1: LANの設定(GigaEthernet1.0)

	現在の設定	設定の変更
LAN側IPアドレス	<input checked="" type="radio"/> 自動設定 <input type="radio"/> 手動設定 192.168.1.254 / 24 自動設定でこのIPアドレスに設定されます。 

3. かんたん設定

(6) 「設定内容を変更しました。」のメッセージが表示されることを確認し、[トップページへ]ボタンを押します。

注意 本画面が表示されない場合、Web 設定画面の接続が切れています。パソコンのIPアドレスを再取得後、新しいLAN側IPアドレスに接続しなおしてください。

1. パスワードの設定 → 2. フレッツ・VPNワイドの設定 → 3. 設定の確認と反映 → 4. 終了

かんたん設定：設定の確認と反映

設定内容を変更しました。

ログイン認証用パスワードの設定

	現在の設定	設定の変更
ユーザ名	admin	変更できません
パスワード	パスワード設定なし	<input type="radio"/> パスワードを変更しない <input checked="" type="radio"/> パスワードを変更する ***** 確認のためもう一度入力してください。 *****

フレッツ・VPNワイドとVPNの設定

	現在の設定	設定の変更
接続種別		<input checked="" type="radio"/> ダイナミックVPN

WAN1: フレッツ・VPNワイドの設定(GigaEthernet0.1)

	現在の設定	設定の変更
ユーザ名		フレッツ・VPNワイドを申し込んだ際のユーザ名を設定します。 (通常はユーザ名には@を含んでいます) flets@example.com
パスワード		フレッツ・VPNワイドを申し込んだ際のパスワードを設定します。 flets-password
IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
DNSアドレス		<input checked="" type="radio"/> 自動設定 <input type="radio"/> 手動設定

ダイナミックVPNの設定

	現在の設定	設定の変更
タイプ		<input checked="" type="radio"/> 拠点 <input type="radio"/> センタ
拠点番号		他の拠点と同じ番号は設定しないでください。 1
パスワード		すべての拠点で共通のパスワードを設定してください。 vpn-password
センタWAN側IPアドレス		センタ装置のWANに設定されているIPアドレスまたはドメイン名を入力してください。 10.10.10.1


LAN1: LANの設定(GigaEthernet1.0)

	現在の設定	設定の変更
LAN側IPアドレス	192.168.100.1/24	<input checked="" type="radio"/> 自動設定 <input type="radio"/> 手動設定 192.168.1.254 / 24 自動設定で上記アドレスに設定されます。


トップページへ

3. かんたん設定

(7) トップページでWAN 情報と VPN 情報の接続状態を確認します。

 [更新]ボタンをクリックすると、情報を更新することが可能です。

(8) メニューエリア、または、メッセージエリアから[設定の保存]をクリックします。



■管理者メニュー
トップページ
設定の保存
ログアウト

■かんたん設定
かんたん設定

■詳細設定
詳細設定

■端末管理
端末管理

■保守管理
装置状態の表示
装置ログの取得
設定データの管理
設定の初期化
ソフトウェアの更新
pingの実行
任意コマンドの実行
IP電話サービス保守
URLオフロード
リンクマネージャ
Wake on LAN
再起動

■拡張ページ
拡張ページ

■外部リンク
製品ページ

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず **設定の保存** を行ってください。

トップページ [\[アイコン表示\]](#) 自動更新間隔: 停止

装置情報 (装置名:Router) 前回ログイン: ---/---/--- (---:---:---)

バージョン	稼働時間	稼働率	メモリ	内部温度	内部電圧
5.1.11	3分	12%	29%	45.0℃	3.2508V

ネットワーク情報

デバイス	接続状態	送信量	受信量
GE0 (GigaEthernet0)	全二重 1Gbpsで接続	0%	0%
GE1 (GigaEthernet1)	Port1: 全二重 1Gbpsで接続 Port2: 接続されていません Port3: 接続されていません Port4: 接続されていません	0%	0%

WAN情報

接続名	接続状態	情報
WAN1: VPN接続 (GigaEthernet0.1)	接続	IPアドレス: 192.0.2.1

VPN情報

接続名	接続状態	通信量[packets]
Dynamic_VPN	接続	送信: 0, 受信: 0

(9) VPN 情報は、接続名にマウスカursorを近づけることで、詳細情報を確認することができます。また、接続名をわかりやすいように変更することができます。



VPN情報

接続名	接続状態	通信量[packets]
Dynamic_VPN ダイナミックVPN(センタ) IPアドレス: 203.0.113.254	接続	送信: 96, 受信: 129

3. かんたん設定

番号	項目	内容
①	接続名	接続名を設定します。 ・ 半角英数字 1～128 文字まで、または全角文字で 1～32 文字まで入力できます。

(10) [保存実行]ボタンをクリックします。

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず『**設定の保存**』を行ってください。

設定の保存

設定を保存します。

よろしければ [保存実行] を押してください。 保存実行

(11) 「設定を保存しました。」のメッセージを確認します。

設定の保存

設定を保存しました。

トップページへ

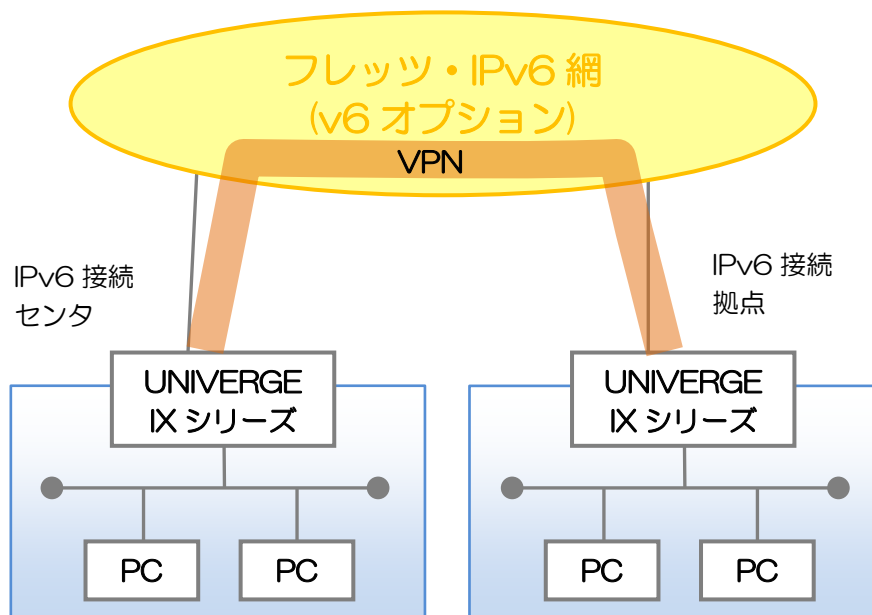
3. かんたん設定

3.5 NGN VPN 接続

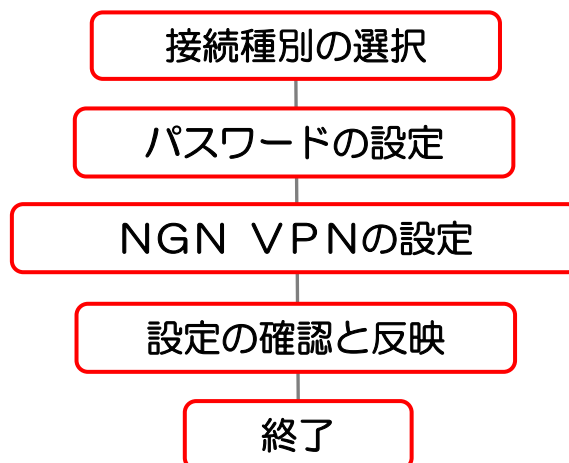
フレッツ・IPv6 網を使用した拠点間 VPN 通信の設定を行います。

メモ あらかじめ NTT 東日本または NTT 西日本のフレッツ光のサービス情報サイトにアクセスし、フレッツ・v6 オプションの申し込みが必要です。フレッツ・v6 オプションの申し込み方法は、お客様契約先の NTT 東日本または NTT 西日本のホームページを参照してください。

【構成イメージ】



【設定手順】



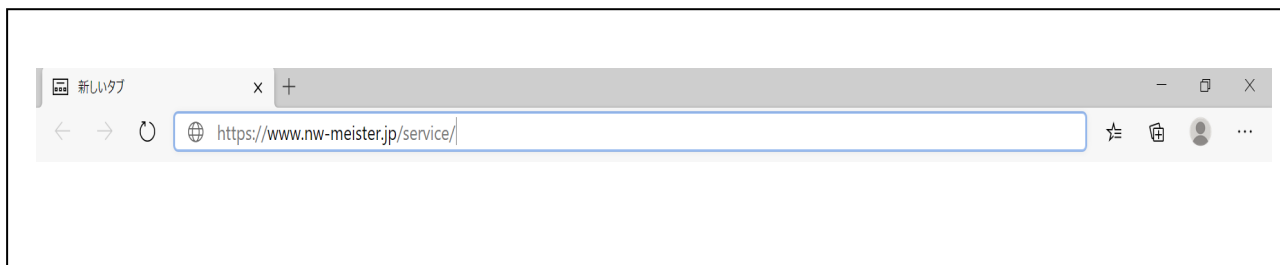
3. かんたん設定

3.5.1 NetMeister の事前登録


NetMeister に、アカウントおよびグループ ID を登録します。

 NetMeister のサイトは、<https://www.nw-meister.jp/service/> です。

(1) Web ブラウザで、NetMeister のサイトにアクセスします。



(2) NetMeister にアカウントおよびグループ ID を登録します。

 NetMeister のアカウントおよびグループ ID の登録方法は、NetMeister のサイトを参照してください。



3. かんたん設定

3.5.2 NGN VPN 接続の設定

(1) ログイン後のメニューエリアから[かんたん設定]をクリックします。

トップページのリンクをクリックすることで、接続種別の各ページに移動することも可能です。

■管理者メニュー

- トップページ
- 設定の保存
- ログアウト

■かんたん設定

- かんたん設定**
- 詳細設定
- 詳細設定

■端末管理

- 端末管理

■保守管理

- 装置状態の表示
- 装置ログの取得
- 設定データの管理
- 設定の初期化
- ソフトウェアの更新
- pingの実行
- 任意コマンドの実行
- IP電話サービス保守
- URLオフロード
- リンクマネージャ
- Wake on LAN
- 再起動

■拡張ページ

- 拡張ページ

■外部リンク

- 製品ページ

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず『設定の保存』を行ってください。

トップページ

ルータの設定を開始します。以下のリンクから選択してください。
パスワードを登録・変更する前にユーザ名とパスワードを入力する画面が表示された場合は、そのまま「OK」をクリックしてください。

かんたん設定

- インターネット接続
フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用して、インターネットに接続する設定を行います。
- インターネット接続+VPN接続
フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用したインターネット接続と、インターネットVPNによる拠点間通信の設定を行います。
- インターネット接続+フレッツ・VPNワイド接続
フレッツ光を使用したインターネット接続と、フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
- フレッツ・VPNワイド接続
フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
- NGN網VPN接続**
NGN網を用いたVPNによる拠点間の通信の設定と、NetMeisterによる装置管理の設定を行います。
- IPv6 IPoE接続
IPv6 IPoE接続の設定を行います。
プロバイダの動的IPまたは固定IPでのサービスを設定します。
- クラウド接続
インターネットVPNや専用線を使用したクラウド接続の設定を行います。
- IP電話サービス接続
対応するUNIVERGE Aspireシリーズと連携したIP電話ネットワークの設定を行います。

詳細設定

インタフェースやサーバのアドレスを指定したり、フィルタやQoS、VPN等、かんたん設定に含まれない詳細な設定を行う場合はこちらから設定してください。

端末管理


本装置に接続されている端末を管理します。
リンクマネージャ機能やWeb認証機能を設定します。

保守管理

装置状態の確認、ソフトウェアの更新、pingの実行など、各種保守機能の操作を行います。
URLオフロード機能による特定宛先のルーティング制御、
リンクマネージャ機能による端末の保守管理などが可能です。
任意のコマンドを直接実行したい場合は**任意コマンドの実行**から操作してください。

3. かんたん設定

(2) 接続種別の選択で「NGN 網 VPN 接続」にチェックを入れ、[次へ]ボタンをクリックします。

 接続種別を変更する場合には、設定の初期化が必要となります。

かんたん設定：接続種別の選択

接続種別を選択してかんたん設定を開始してください。
接続種別を変更する場合には「**設定の初期化**」が必要となります。

	現在の設定	設定の変更
接続種別の選択	インターネット接続なし	<input type="radio"/> インターネット接続 フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用して、インターネットに接続する設定を行います。
		<input type="radio"/> インターネット接続 + VPN接続 フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用したインターネット接続と、インターネットVPNによる拠点間通信の設定を行います。
		<input type="radio"/> インターネット接続 + フレッツ・VPNワイド接続 フレッツ光を使用したインターネット接続と、フレッツ・VPNワイド(端末型出し出し)を使用した拠点間通信の設定を行います。
		<input type="radio"/> フレッツ・VPNワイド接続 フレッツ・VPNワイド(端末型出し出し)を使用した拠点間通信の設定を行います。
		<input checked="" type="radio"/> NGN網VPN接続 NGN網を利用したVPNによる拠点間の通信の設定とNetMeisterによる装置管理の設定を行います。
		<input type="radio"/> IPv6 IPoE接続 IPv6 IPoE接続の設定を行います。 プロバイダの動的IPまたは固定IPでのサービスを設定します。
		<input type="radio"/> クラウド接続 インターネットVPNや専用線を使用したクラウド接続の設定を行います。
		<input type="radio"/> IP電話サービス接続 対応するUNIVERGE Aspireシリーズと連携したIP電話ネットワークの設定を行います。



3. かんたん設定

(3) 管理者パスワードを変更する場合は、[パスワードを変更する]を選択し、パスワードを設定した後、[次へ]ボタンをクリックします。

メモ 管理者パスワードを変更する必要が無い場合は、そのまま[次へ]ボタンをクリックします。

メモ 接続種別の選択に戻る場合は、[戻る]ボタンをクリックしてください。



番号	項目	内容
①	ユーザ名	<p>本装置にログインするときのユーザ名です。</p> <ul style="list-style-type: none"> 初期状態ではユーザ名は設定されていません。 パスワード設定後のユーザ名は「admin」です。Web 設定からは変更できません。
②	パスワード	<p>本装置にログインするときのパスワードです。</p> <ul style="list-style-type: none"> 初期状態ではパスワードは設定されていません。 半角英数字 1～249 文字で入力します。 <p>注意</p> <ul style="list-style-type: none"> 大文字／小文字は区別されます。 パスワードの入力文字は表示されません。●●●のように伏せ文字で表示されます。 パスワードは、第三者に推測されにくく、忘れないような文字列を入力してください。

メモ 以降の設定は、センタの設定の場合と拠点の設定の場合で異なりますので、それぞれに応じた設定の節を参照してください。

3. かんたん設定

3.5.3 センタの場合の設定

(1) [VPN の設定]の各項目を設定し、[次へ]ボタンをクリックします。

メモ パスワードの設定に戻る場合は、[戻る]ボタンをクリックしてください。

1. パスワードの設定 → 2. **VPNの設定** → 3. インターネット接続の設定 → 4. NetMeisterの設定 → 5. 設定の確認と反映 → 6. 終了

かんたん設定：VPNの設定

VPNを設定します。

ダイナミックVPNの設定

2拠点間通信でもセンタは必要です。いずれかの拠点で必ずセンタを選択してください。
タイプや拠点番号を変更すると、次ページのLAN側IPアドレスが変更されます。

	現在の設定	設定の変更
タイプ		<input type="radio"/> 拠点 <input checked="" type="radio"/> センタ
パスワード		すべての拠点で共通のパスワードを設定してください。 <input type="text"/> 文字列(半角英数字)を入力してください。

戻る 次へ

番号	項目	内容
①	タイプ	センタを選択します。
②	パスワード	VPN 接続で使用するパスワード(事前共有鍵)です。 拠点に設定したパスワードと同じパスワードを設定してください。 <ul style="list-style-type: none">半角英数字で 1~128 文字まで入力できます。

3. かんたん設定

(2) [インターネット接続の設定]の各項目を設定し、[次へ]ボタンをクリックします。

メモ VPNの設定に戻る場合は、[戻る]ボタンをクリックしてください。

1. パスワードの設定 → 2. VPNの設定 → 3. **インターネット接続の設定** → 4. NetMeisterの設定 → 5. 設定の確認と反映 → 6. 終了

◆注意事項
NTT東日本/NTT西日本が提供する「ひかり電話対応機器」(ホームゲートウェイ、ひかり電話ルータなど)の下位にIXルータを接続する場合は、ひかり電話対応機器のIPv6ファイアウォール機能を無効化してから本機能を設定してください。
ひかり電話対応機器のIPv6ファイアウォール機能が有効化されている場合、IXルータ間のVPN通信が不安定になることがあります。
具体的な設定方法については、ひかり電話対応機器のマニュアルをご参照ください。

設定を行うにはフレッツ光のサービス情報サイトにて「フレッツ・v6オプション」の申し込みが必要です。
(既にフレッツ・v6オプションの利用を申請されている場合は必要ありません。)

かんたん設定：インターネット接続の設定

インターネット接続の設定をします。

WAN1: WAN側インタフェースの設定(GigaEthernet0.0)

	現在の設定	設定の変更
WAN側アドレス	-	自動取得
デフォルトゲートウェイ	-	自動設定
DNSアドレス	-	自動取得

LAN1: LANの設定(GigaEthernet1.0)

他の拠点と重複しないように設定してください。
LAN側IPアドレスを変更する場合は、反映後に新しいIPアドレスで接続しなおす必要があります。

	現在の設定	設定の変更
LAN側IPアドレス	192.168.1.254/24	<input checked="" type="radio"/> 自動設定 <input type="radio"/> 手動設定 192.168.255.254 / 24 自動設定で上記アドレスに設定されます。

インターネット接続の設定

NetMeisterでの装置管理を行うためにはインターネットの接続をありにする必要があります。

	現在の設定	設定の変更
インターネット接続		<input checked="" type="radio"/> あり <input type="radio"/> なし

WAN2: PPPoE接続の設定(GigaEthernet0.1)

	現在の設定	設定の変更
ユーザ名		プロバイダから通知されているユーザ名を設定します。 (フレッツの場合、通常はユーザ名には@を含んでいます) [テキスト入力欄] 文字列(半角英数字)を入力してください。
パスワード		プロバイダから通知されているパスワードを設定します。 [テキスト入力欄] 文字列(半角英数字)を入力してください。

通信セキュリティの設定

	現在の設定	設定の変更
セキュリティ強度	レベル1	<input checked="" type="radio"/> レベル1 - 外部からの不要なパケットをNAPT(IPv4)、ダイナミックフィルタ(IPv6)により廃棄します。 <input type="radio"/> レベル2 - 外部からの不要なパケットをNAPT(IPv4)、ダイナミックフィルタ(IPv6)により廃棄します。 - 内部からの不要な通信を制限します。

戻る **次へ**

3. かんたん設定

番号	項目	内容																	
①	LAN 側 IP アドレス	<p>LAN 側 IP アドレスを[自動設定]/[手動設定]で選択し、設定します。 IP アドレスを変更する場合、現在の接続は切断されます。新しい IP アドレスに接続しなおしてください。</p> <p>注意</p> <ul style="list-style-type: none"> 他のセンタ・拠点と異なる IP アドレスを設定する必要があります。 																	
②	インターネット接続	<p>該当の装置をインターネット接続するか否か、[あり]/[なし]を選択します。</p> <p>メモ</p> <ul style="list-style-type: none"> インターネット接続[あり]の場合、NetMeister によるダイナミック DNS を利用可能となります。また、NetMeister による装置管理も利用可能となります。 インターネット接続[なし]の場合、NetMeister によるダイナミック DNS を利用可能となります。NetMeister による装置管理は利用できません。 																	
③	ユーザ名	<p>インターネット接続[あり]の設定の場合、プロバイダから通知されているユーザ名を設定します。 (フレッツの場合、通常はユーザ名には@を含んでいます)</p> <ul style="list-style-type: none"> 半角英数字で 1~59 文字まで入力できます。 																	
④	パスワード	<p>インターネット接続[あり]の設定の場合、プロバイダから通知されているパスワードを設定します。</p> <ul style="list-style-type: none"> 半角英数字で 1~79 文字まで入力できます。 <p>注意</p> <ul style="list-style-type: none"> 大文字/小文字は区別されます。 																	
⑤	セキュリティ強度	<p>セキュリティ強度を選択します。</p> <ul style="list-style-type: none"> 外部からの不要なパケットを NAPT (IPv4) またはダイナミックフィルタ (IPv6) により廃棄する場合は、「レベル 1」を選択します。 外部からの不要なパケットを NAPT (IPv4) またはダイナミックフィルタ (IPv6) により廃棄し、さらに内部からの不要な通信を制限する場合は、「レベル 2」を選択します。 VPN 通信以外のパケットを全て廃棄する場合は、「レベル 3」を選択します。 (VPN 以外のインターネット上の Web アクセスも禁止します) ケーブルテレビなどで、インターネットへのアクセスができない場合は、「レベル 1」を選択してください。 「レベル 2」を選択したときは、送信時に以下に該当する通信を廃棄します。 <table border="1" style="margin-left: 20px;"> <tbody> <tr> <td rowspan="4">宛先 IP アドレス</td> <td>0.0.0.0/8</td> </tr> <tr> <td>127.0.0.0/8</td> </tr> <tr> <td>169.254.0.0/16</td> </tr> <tr> <td>224.0.0.0/4</td> </tr> <tr> <td rowspan="5">宛先ポート番号</td> <td>135</td> </tr> <tr> <td>137</td> </tr> <tr> <td>138</td> </tr> <tr> <td>139</td> </tr> <tr> <td>445</td> </tr> <tr> <td rowspan="5">送信元ポート番号</td> <td>135</td> </tr> <tr> <td>137</td> </tr> <tr> <td>138</td> </tr> <tr> <td>139</td> </tr> <tr> <td>445</td> </tr> </tbody> </table>	宛先 IP アドレス	0.0.0.0/8	127.0.0.0/8	169.254.0.0/16	224.0.0.0/4	宛先ポート番号	135	137	138	139	445	送信元ポート番号	135	137	138	139	445
宛先 IP アドレス	0.0.0.0/8																		
	127.0.0.0/8																		
	169.254.0.0/16																		
	224.0.0.0/4																		
宛先ポート番号	135																		
	137																		
	138																		
	139																		
	445																		
送信元ポート番号	135																		
	137																		
	138																		
	139																		
	445																		

3. かんたん設定

(3) [NetMeister の設定]の各項目を設定し、[設定の確認]ボタンをクリックします。

メモ インターネット接続の設定に戻る場合は、[戻る]ボタンをクリックしてください。

1. パスワードの設定 → 2. VPNの設定 → 3. インターネット接続の設定 → 4. **NetMeisterの設定** → 5. 設定の確認と反映 → 6. 終了

かんたん設定 : NetMeisterの設定

NetMeisterの設定を行います。

NetMeister ダイナミックDNSの設定

設定を行うにはNetMeisterのアカウント登録が必要です。
<https://www.nw-meister.jp/service/> 事前にNetMeisterのアカウント登録を行ってください。


	現在の設定	設定の変更
ホスト名(装置名)		NetMeisterで管理する装置のホスト名を設定します。 本項目は、ダイナミックDNSサービスのドメインの一部として使用します。 <input type="text"/> 文字列を入力してください。[2-63文字]
サイト名(拠点名)		NetMeisterで管理する装置の拠点情報(拠点名)を設定します。 <input type="text"/> 文字列を入力してください。[2-31文字]
NetMeister グループID		NetMeisterに登録したグループIDを設定します。 <input type="text"/> 文字列を入力してください。[2-63文字]
NetMeister グループパスワード		NetMeisterに登録したグループパスワードを設定します。 <input type="radio"/> パスワードを変更しない <input checked="" type="radio"/> パスワードを変更する <input type="text"/> 文字列を入力してください。[8-31文字]

3. かんたん設定

番号	項目	内容
①	ホスト名(装置名)	装置のホスト名を設定します。設定したホスト名は NetMeister に通知されます。 <ul style="list-style-type: none">半角英数字または-(ハイフン)で 2~63 文字まで入力できます。 メモ <ul style="list-style-type: none">大文字は、小文字に変換して NetMeister に通知されます。 注意 <ul style="list-style-type: none">ホスト名の先頭と最後には-(ハイフン)を利用することができません。
②	サイト名(拠点名)	NetMeister に通知するサイト名を設定します。 <ul style="list-style-type: none">半角英数字または-(ハイフン)で 2~31 文字まで入力できます。 メモ <ul style="list-style-type: none">大文字は、小文字に変換して NetMeister に通知されます。 注意 <ul style="list-style-type: none">サイト名の先頭と最後には-(ハイフン)を利用することができません。
③	NetMeister グループ ID	NetMeister の登録ページで申請した「グループ ID」を設定します。 <ul style="list-style-type: none">半角英数字または-(ハイフン)で 2~63 文字まで入力できます。 注意 <ul style="list-style-type: none">NetMeister グループ ID の先頭と最後には-(ハイフン)を利用することができません。
④	NetMeister グループパスワード	NetMeister の登録ページで申請した「グループパスワード」を設定します。 <ul style="list-style-type: none">半角英数字または-(ハイフン)で 2~31 文字まで入力できます。 注意 <ul style="list-style-type: none">大文字/小文字は区別されます。パスワードの入力文字は表示されません。●●●のように伏せ文字で表示されます。

3. かんたん設定

(4) 入力した項目が正しいことを確認し、[反映]ボタンをクリックします。

 NetMeister の設定に戻る場合は、[戻る]ボタンをクリックしてください。

1. パスワードの設定 → 2. VPNの設定 → 3. インターネット接続の設定 → 4. NetMeisterの設定 → 5. 設定の確認と反映 → 6. 終了

かんたん設定：設定の確認と反映

設定内容を変更する場合は [反映] を押してください。
LAN側IPアドレスを変更する場合は、新しいIPアドレスで接続しなおしてください。

ログイン認証用パスワードの設定

	現在の設定	設定の変更
ユーザ名	admin	変更できません
パスワード	*****	<input checked="" type="radio"/> パスワードを変更しない <input type="radio"/> パスワードを変更する

ダイナミックVPNの設定

	現在の設定	設定の変更
タイプ		<input type="radio"/> 拠点 <input checked="" type="radio"/> センタ
パスワード		すべての拠点で共通のパスワードを設定してください。 <input type="text" value="vpn-password"/>

WAN1: WAN側インタフェースの設定(GigaEthernet0.0)

	現在の設定	設定の変更
WAN側アドレス	-	自動取得
デフォルトゲートウェイ	-	自動設定
DNSアドレス	-	自動取得

LAN1: LANの設定(GigaEthernet1.0)

	現在の設定	設定の変更
LAN側IPアドレス	192.168.1.254/24	<input type="radio"/> 自動設定 <input checked="" type="radio"/> 手動設定 <input type="text" value="192.168.1.254"/> / <input type="text" value="24"/>

:

NetMeister ダイナミックDNSの設定

	現在の設定	設定の変更
ホスト名(装置名)		NetMeisterで管理する装置のホスト名を設定します。 本項目は、ダイナミックDNSサービスのドメインの一部として使用します。 <input type="text"/>
サイト名(拠点名)		NetMeisterで管理する装置の拠点情報(拠点名)を設定します。 <input type="text"/>
NetMeister グループID		NetMeisterに登録したグループIDを設定します。 <input type="text"/>
NetMeister グループパスワード		NetMeisterに登録したグループパスワードを設定します。 <input type="radio"/> パスワードを変更しない <input checked="" type="radio"/> パスワードを変更する <input type="text" value="*****"/>

3. かんたん設定

- (5) 「設定内容を変更しました。」のメッセージが表示されることを確認し、[トップページへ]ボタンをクリックします。

1. パスワードの設定 → 2. VPNの設定 → 3. インターネット接続の設定 → 4. NetMeisterの設定 → 5. 設定の確認と反映 → 6. 終了

かんたん設定：終了

設定内容を変更しました。

ログイン認証用パスワードの設定

	現在の設定	設定の変更
ユーザ名	admin	変更できません
パスワード	*****	<input checked="" type="radio"/> パスワードを変更しない <input type="radio"/> パスワードを変更する

ダイナミックVPNの設定

	現在の設定	設定の変更
タイプ	センタ	<input type="radio"/> 拠点 <input checked="" type="radio"/> センタ
パスワード	vpn-password	すべての拠点で共通のパスワードを設定してください。 <input type="text" value="vpn-password"/>

WAN1: WAN側インタフェースの設定(GigaEthernet0.0)

	現在の設定	設定の変更
WAN側アドレス	-	自動取得
デフォルトゲートウェイ	-	自動設定
DNSアドレス	-	自動取得

LAN1: LANの設定(GigaEthernet1.0)

	現在の設定	設定の変更
LAN側IPアドレス	192.168.1.254/24	<input type="radio"/> 自動設定 <input checked="" type="radio"/> 手動設定 <input type="text" value="192.168.1.254"/> / <input type="text" value="24"/>

:

NetMeister ダイナミックDNSの設定

	現在の設定	設定の変更
ホスト名(装置名)	<input type="text" value=""/>	NetMeisterで管理する装置のホスト名を設定します。 本項目は、ダイナミックDNSサービスのドメインの一部として使 用します。 <input type="text" value=""/>
サイト名(拠点名)	<input type="text" value=""/>	NetMeisterで管理する装置の拠点情報(拠点名)を設定します。 <input type="text" value=""/>
NetMeister グループID	<input type="text" value=""/>	NetMeisterに登録したグループIDを設定します。 <input type="text" value=""/>
NetMeister グループパスワード	*****	NetMeisterに登録したグループパスワードを設定します。 <input checked="" type="radio"/> パスワードを変更しない <input type="radio"/> パスワードを変更する

トップページへ

3. かんたん設定

(6) トップページでWAN情報の接続状態を確認します。

メモ [更新]ボタンをクリックすると、情報を更新することが可能です。

(7) メニューエリア、または、メッセージエリアから[設定の保存]をクリックします。

The screenshot shows the 'Simple Settings' (かんたん設定) page of a router. A red box highlights the 'Save Settings' (設定の保存) button in the left sidebar. Another red box highlights a warning message at the top: '!!注意!! 設定が変更されています。再起動した場合、保存していない設定は元の状態に戻ります。設定完了後は必ず「設定の保存」を行ってください。' Below this, the 'System Information' (装置情報) section shows a table with columns for Version, Standby Time, Load Rate, Memory, Internal Temperature, and Internal Voltage. The 'Network Information' (ネットワーク情報) section contains a table for device connection status, including GE0 and GE1 ports. The 'WAN Information' (WAN情報) section shows two WAN connections (WAN1 and WAN2) with their respective connection status and IP/DNS information. The 'VPN Information' (VPN情報) section shows a dynamic VPN connection. The 'UTM Information' (UTM情報) section shows the license status. Several 'Update' (更新) buttons are visible throughout the page.

バージョン	稼働時間	稼働率	メモリ	内部温度	内部電圧
	10分	13%	19%	41.0℃	3.2508V

デバイス	接続状態	送信量	受信量
GE0 (GigaEthernet0)	全二重 1Gbpsで接続	0%	0%
GE1 (GigaEthernet1)	Port1: 全二重 1Gbpsで接続 Port2: 接続されていません Port3: 接続されていません Port4: 接続されていません	0%	0%

接続名	接続状態	情報
WAN1: WAN (GigaEthernet0.0)	接続	IPv6アドレス: DNS: DNS:
WAN2: GigaEthernet0.1	接続	IPアドレス: DNS:

接続名	接続状態	通信量[packets]
	接続 ダイナミックVPN(センタ)	送信: 306, 受信: 50

ライセンス状態	ライセンス満了日時
設定されていません	

3. かんたん設定

(8) [保存実行]ボタンをクリックします。

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず『設定の保存』を行ってください。

設定の保存

設定を保存します。

よろしければ [保存実行] を押してください。

[保存実行](#)

(9) 「設定を保存しました。」のメッセージを確認します。

設定の保存

設定を保存しました。

[トップページへ](#)

3. かんたん設定

3.5.4 拠点の場合の設定

(1) ダイナミックVPNの設定で、[VPNの設定]の各項目を設定し、[次へ]ボタンをクリックします。

メモ パスワードの設定に戻る場合は、[戻る]ボタンをクリックしてください。

番号	項目	内容
①	タイプ	拠点を選択します。
②	拠点番号	拠点の識別番号です。 他の拠点と重複しない任意の番号(1~64)を設定します。
③	パスワード	VPN 接続で使用するパスワード(事前共有鍵)です。 すべての拠点で同じ任意のパスワードを設定してください。 ・ 半角英数字で 1~128 文字まで入力できます。
④	センタの FQDN	センタ装置に設定された NetMeister の「ホスト名」と「グループ ID」を設定します。 ・ ホスト名およびグループ ID は、半角英数字で 2~63 文字まで入力できます。

3. かんたん設定

(2) [インターネット接続の設定]の各項目を設定し、[次へ]ボタンをクリックします。

メモ VPNの設定に戻る場合は、[戻る]ボタンをクリックしてください。

1. パスワードの設定 → 2. VPNの設定 → 3. **インターネット接続の設定** → 4. NetMeisterの設定 → 5. 設定の確認と反映 → 6. 終了

◆注意事項
 NTT東日本/NTT西日本が提供する「ひかり電話対応機器」(ホームゲートウェイ、ひかり電話ルータなど)の下位にIXルータを接続する場合は、ひかり電話対応機器のIPv6ファイアウォール機能を無効化してから本機能を設定してください。
 ひかり電話対応機器のIPv6ファイアウォール機能が有効化されている場合、IXルータ間のVPN通信が不安定になることがあります。
 具体的な設定方法については、ひかり電話対応機器のマニュアルをご参照ください。

設定を行うにはフレッツ光のサービス情報サイトにて“フレッツ・v6オプション”の申し込みが必要です。
 (既にフレッツ・v6オプションの利用を申請されている場合は必要ありません。)

かんたん設定：インターネット接続の設定

インターネット接続の設定をします。

WAN1: WAN側インタフェースの設定(GigaEthernet0.0)

	現在の設定	設定の変更
WAN側アドレス	-	自動取得
デフォルトゲートウェイ	-	自動設定
DNSアドレス	-	自動取得

LAN1: LANの設定(GigaEthernet1.0)

他の拠点と重複しないように設定してください。
 LAN側IPアドレスを変更する場合は、反映後に新しいIPアドレスで接続しなおす必要があります。

	現在の設定	設定の変更
LAN側IPアドレス	192.168.1.254/24	<input checked="" type="radio"/> 自動設定 <input type="radio"/> 手動設定 192.168.1.254 / 24 自動設定で上記アドレスに設定されます。

戻る 次へ

番号	項目	内容
①	LAN 側 IP アドレス	LAN 側 IP アドレスを[自動設定]/[手動設定]で選択し、設定します。 IP アドレスを変更する場合、現在の接続は切断されます。新しい IP アドレスに接続しなおしてください。 注意 ・ 他のセンタ・拠点と異なる IP アドレスを設定する必要があります。

3. かんたん設定

(3) [NetMeister の設定]の各項目を設定し、[設定の確認]ボタンをクリックします。

メモ インターネット接続の設定に戻る場合は、[戻る]ボタンをクリックしてください。

1. パスワードの設定 → 2. VPNの設定 → 3. インターネット接続の設定 → 4. **NetMeisterの設定** → 5. 設定の確認と反映 → 6. 終了

かんたん設定 : NetMeisterの設定

NetMeisterの設定を行います。

NetMeister ダイナミックDNSの設定

設定を行うにはNetMeisterのアカウント登録が必要です。
<https://www.nw-meister.jp/service/> 事前にNetMeisterのアカウント登録を行ってください。

	現在の設定	設定の変更
ホスト名(装置名)		NetMeisterで管理する装置のホスト名を設定します。 本項目は、ダイナミックDNSサービスのドメインの一部として使用します。 <input type="text"/> 文字列を入力してください。[2-63文字]
サイト名(拠点名)		NetMeisterで管理する装置の拠点情報(拠点名)を設定します。 <input type="text"/> 文字列を入力してください。[2-31文字]
NetMeister グループID		NetMeisterに登録したグループIDを設定します。 <input type="text"/> 文字列を入力してください。[2-63文字]
NetMeister グループパスワード		NetMeisterに登録したグループパスワードを設定します。 <input type="radio"/> パスワードを変更しない <input checked="" type="radio"/> パスワードを変更する <input type="text"/> 文字列を入力してください。[8-31文字]

3. かんたん設定

番号	項目	内容
①	ホスト名(装置名)	装置のホスト名を設定します。設定したホスト名は NetMeister に通知されます。 <ul style="list-style-type: none">半角英数字または-(ハイフン)で2~63 文字まで入力できます。 メモ <ul style="list-style-type: none">大文字は、小文字に変換して NetMeister に通知されます。 注意 <ul style="list-style-type: none">ホスト名の先頭と最後には-(ハイフン)を利用することができません。
②	サイト名(拠点名)	NetMeister に通知するサイト名を設定します。 <ul style="list-style-type: none">半角英数字または-(ハイフン)で2~31 文字まで入力できます。 メモ <ul style="list-style-type: none">大文字は、小文字に変換して NetMeister に通知されます。 注意 <ul style="list-style-type: none">サイト名の先頭と最後には-(ハイフン)を利用することができません。
③	NetMeister グループ ID	NetMeister の登録ページで申請した「グループ ID」を設定します。 <ul style="list-style-type: none">半角英数字または-(ハイフン)で2~63 文字まで入力できます。 注意 <ul style="list-style-type: none">NetMeister グループ ID の先頭と最後には-(ハイフン)を利用することができません。
④	NetMeister グループパスワード	NetMeister の登録ページで申請した「グループパスワード」を設定します。 <ul style="list-style-type: none">半角英数字または-(ハイフン)で2~31 文字まで入力できます。 注意 <ul style="list-style-type: none">大文字/小文字は区別されます。パスワードの入力文字は表示されません。●●●のように伏せ文字で表示されます。

3. かんたん設定

(4) 入力した項目が正しいことを確認し、[反映]ボタンをクリックします。

メモ NetMeister の設定に戻る場合は、[戻る]ボタンをクリックしてください。

1. パスワードの設定 → 2. VPNの設定 → 3. インターネット接続の設定 → 4. NetMeisterの設定 → 5. 設定の確認と反映 → 6. 終了

かんたん設定：設定の確認と反映

設定内容を変更する場合は [反映] を押してください。
LAN側IPアドレスを変更する場合は、新しいIPアドレスで接続しなおしてください。

ログイン認証用パスワードの設定

	現在の設定	設定の変更
ユーザ名	admin	変更できません
パスワード	*****	<input checked="" type="radio"/> パスワードを変更しない <input type="radio"/> パスワードを変更する

ダイナミックVPNの設定

	現在の設定	設定の変更
タイプ		<input checked="" type="radio"/> 拠点 <input type="radio"/> センタ
拠点番号		他の拠点と同じ番号は設定しないでください。 1 ↓
パスワード		すべての拠点で共通のパスワードを設定してください。 vpn-password
センタのFQDN		センタで設定したNetMeisterの「装置のホスト名」と「グループID」を入力してください。 *.v6.nmddns.jp

:

NetMeister ダイナミックDNSの設定

	現在の設定	設定の変更
ホスト名(装置名)		NetMeisterで管理する装置のホスト名を設定します。 本項目は、ダイナミックDNSサービスのドメインの一部として使 用します。 *.v6.nmddns.jp
サイト名(拠点名)		NetMeisterで管理する装置の拠点情報(拠点名)を設定します。 *.v6.nmddns.jp
NetMeister グループID		NetMeisterに登録したグループIDを設定します。 1234567890
NetMeister グループパスワード		NetMeisterに登録したグループパスワードを設定します。 <input type="radio"/> パスワードを変更しない <input checked="" type="radio"/> パスワードを変更する *****

戻る 反映

3. かんたん設定

- (5) 「設定内容を変更しました。」のメッセージが表示されることを確認し、[トップページへ]ボタンをクリックします。

1. パスワードの設定 → 2. VPNの設定 → 3. インターネット接続の設定 → 4. NetMeisterの設定 → 5. 設定の確認と反映 → 6. 終了

かんたん設定：終了

設定内容を変更しました。

ログイン認証用パスワードの設定

	現在の設定	設定の変更
ユーザ名	admin	変更できません
パスワード	*****	<input checked="" type="radio"/> パスワードを変更しない <input type="radio"/> パスワードを変更する

ダイナミックVPNの設定

	現在の設定	設定の変更
タイプ	拠点	<input checked="" type="radio"/> 拠点 <input type="radio"/> センタ
拠点番号	1	他の拠点と同じ番号は設定しないでください。 1
パスワード	vpn-password	すべての拠点で共通のパスワードを設定してください。 vpn-password
センタのFQDN		センタで設定したNetMeisterの「装置のホスト名」と「グループID」を入力してください。 .v6.nmddns.jp

:


NetMeister ダイナミックDNSの設定

	現在の設定	設定の変更
ホスト名(装置名)		NetMeisterで管理する装置のホスト名を設定します。 本項目は、ダイナミックDNSサービスのドメインの一部として使用します。 [ホスト名]
サイト名(拠点名)		NetMeisterで管理する装置の拠点情報(拠点名)を設定します。 [サイト名]
NetMeister グループID		NetMeisterに登録したグループIDを設定します。 [グループID]
NetMeister グループパスワード	*****	NetMeisterに登録したグループパスワードを設定します。 <input checked="" type="radio"/> パスワードを変更しない <input type="radio"/> パスワードを変更する

トップページへ

3. かんたん設定

(6) トップページでWAN情報の接続状態を確認します。

 [更新]ボタンをクリックすると、情報を更新することが可能です。

(7) メニューエリア、または、メッセージエリアから[設定の保存]をクリックします。



!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず **設定の保存** を行ってください。

管理者メニュー
■ トップページ
■ 設定の保存
■ ログアウト
■ かんたん設定
■ かんたん設定
■ 詳細設定
■ 詳細設定
■ 端末管理
■ 端末管理
■ 保守管理
■ 装置状態の表示
■ 装置ログの取得
■ 設定データの管理
■ 設定の初期化
■ ソフトウェアの更新
■ pingの実行
■ 任意コマンドの実行
■ IP電話サービス保守
■ URLオフロード
■ リンクマネージャ
■ Wake on LAN
■ 再起動
■ 拡張ページ
■ 拡張ページ
■ 外部リンク
■ 製品ページ

トップページ [カイトを表示] 自動更新間隔: 停止 ▼

装置情報 (装置名: Router) 前回ログイン: 2023/10/27 10:00 (---,---,---)

バージョン	稼働時間	稼働率	メモリ	内部温度	内部電圧
	5分	13%	19%	38.0℃	3.2680V

ネットワーク情報 更新

デバイス	接続状態	送信量	受信量
GE0 (GigaEthernet0)	全二重 1Gbpsで接続	0%	0%
GE1 (GigaEthernet1)	Port1: 全二重 1Gbpsで接続 Port2: 接続されていません Port3: 接続されていません Port4: 接続されていません	0%	0%

WAN情報 更新

接続名	接続状態	情報
WAN1: WAN (GigaEthernet0.0)	接続	IPv6アドレス: DNS: DNS:

VPN情報 更新

接続名	接続状態	通信量[packets]
Dynamic_VPN	接続 ダイナミックVPN(拠点)	送信: 249, 受信: 46

UTM情報 更新

ライセンス状態	ライセンス満了日時
設定されていません	

3. かんたん設定

(8) [保存実行]ボタンをクリックします。

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず『設定の保存』を行ってください。

設定の保存

設定を保存します。

よろしければ [保存実行] を押してください。

[保存実行](#)

(9) 「設定を保存しました。」のメッセージを確認します。

設定の保存

設定を保存しました。

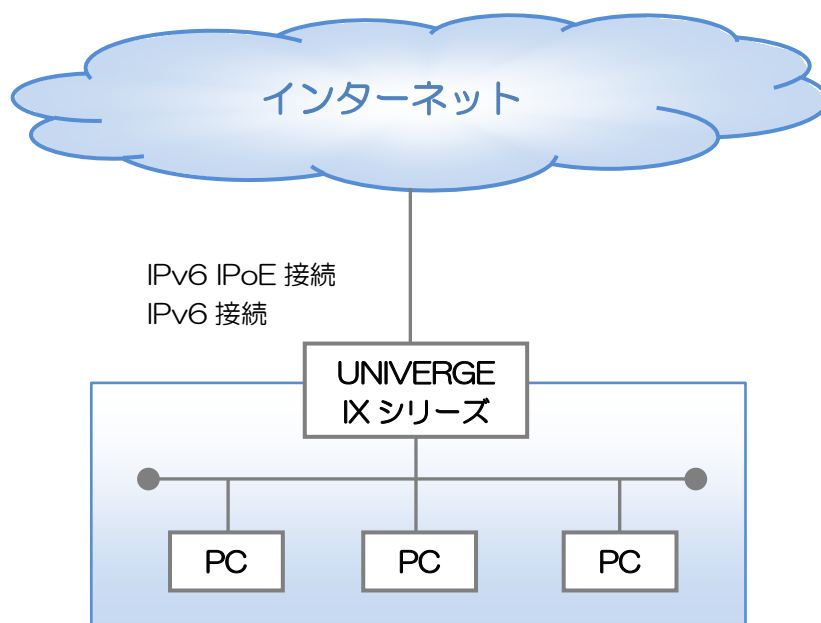
[トップページへ](#)

3. かんたん設定

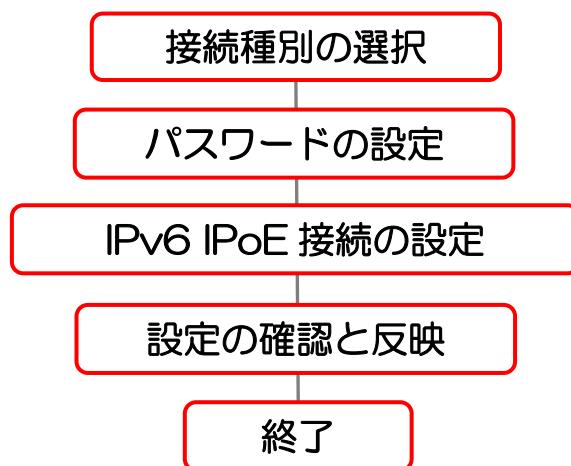
3.6 IPv6 IPoE 接続

フレッツ光などで各プロバイダが提供する IPv6 IPoE サービスを使用して、インターネットに接続する設定を行います。

【構成イメージ】



【設定手順】



3. かんたん設定


(1) ログイン後のトップページから[かんたん設定]をクリックします。

メモ かんたん設定メニューから[かんたん設定]のリンクをクリックすることで、接続種別の各ページに移動することも可能です。

■管理者メニュー	!!注意!! 設定が変更されています。 再起動した場合、保存していない設定は元の状態に戻ります。 設定完了後は必ず『設定の保存』を行ってください。
■かんたん設定	トップページ ルータの設定を開始します。以下のリンクから選択してください。 パスワードを登録・変更する前にユーザ名とパスワードを入力する画面が表示された場合は、そのまま「OK」をクリックしてください。
■詳細設定	かんたん設定 <ul style="list-style-type: none">インターネット接続 フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用して、インターネットに接続する設定を行います。インターネット接続+VPN接続 フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用したインターネット接続と、インターネットVPNによる拠点間通信の設定を行います。インターネット接続+フレッツ・VPNワイド接続 フレッツ光を使用したインターネット接続と、フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。フレッツ・VPNワイド接続 フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。NGN網VPN接続 NGN網を用いたVPNによる拠点間の通信の設定と、NetMeisterによる装置管理の設定を行います。IPv6 IPoE接続 IPv6 IPoE接続の設定を行います。 プロバイダの動的IPまたは固定IPでのサービスを設定します。クラウド接続 インターネットVPNや専用線を使用したクラウド接続の設定を行います。IP電話サービス接続 対応するUNIVERGE Aspireシリーズと連携したIP電話ネットワークの設定を行います。
■保守管理	詳細設定 インタフェースやサーバのアドレスを指定したり、フィルタやQoS、VPN等、かんたん設定に含まれない詳細な設定を行う場合はこちらから設定してください。
■拡張ページ	端末管理 本装置に接続されている端末を管理します。 リンクマネージャ機能やWeb認証機能を設定します。
■外部リンク	保守管理 装置状態の確認、ソフトウェアの更新、pingの実行など、各種保守機能の操作を行います。 URLオフロード機能による特定宛先のレーティング制御、 リンクマネージャ機能による端末の保守管理などが可能です。 任意のコマンドを直接実行したい場合は 任意コマンドの実行 から操作してください。

3. かんたん設定

(2) 接続種別の選択で「IPv6 IPoE 接続」にチェックを入れ、[次へ]ボタンをクリックします。

 接続種別を変更する場合には、設定の初期化が必要となります。

かんたん設定：接続種別の選択

接続種別を選択してかんたん設定を開始してください。
接続種別を変更する場合には「設定の初期化」が必要となります。

	現在の設定	設定の変更
接続種別の選択	インターネット接続なし	<input type="radio"/> インターネット接続 フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用して、インターネットに接続する設定を行います。
		<input type="radio"/> インターネット接続 + VPN接続 フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用したインターネット接続と、インターネットVPNによる拠点間通信の設定を行います。
		<input type="radio"/> インターネット接続 + フレッツ・VPNワイド接続 フレッツ光を使用したインターネット接続と、フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
		<input type="radio"/> フレッツ・VPNワイド接続 フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
		<input type="radio"/> NGN網VPN接続 NGN網を用いたVPNによる拠点間の通信の設定とNetMeisterによる装置管理の設定を行います。
		<input checked="" type="radio"/> IPv6 IPoE接続 IPv6 IPoE接続の設定を行います。 プロバイダの動的IPまたは固定IPでのサービスを設定します。
		<input type="radio"/> クラウド接続 インターネットVPNや専用線を使用したクラウド接続の設定を行います。
		<input type="radio"/> IP電話サービス接続 対応するUNIVERGE Aspireシリーズと連携したIP電話ネットワークの設定を行います。



3. かんたん設定

(3) 管理者パスワードを変更する場合は、[パスワードを変更する]を選択し、パスワードを設定した後、[次へ]ボタンをクリックします。

メモ 管理者パスワードを変更する必要が無い場合は、そのまま[次へ]ボタンをクリックします。

メモ 接続種別の選択に戻る場合は、[戻る]ボタンをクリックしてください。



番号	項目	内容
①	ユーザ名	本装置にログインするときのユーザ名です。 <ul style="list-style-type: none">初期状態ではユーザ名は設定されていません。パスワード設定後のユーザ名は「admin」です。Web 設定からは変更できません。
②	パスワード	本装置にログインするときのパスワードです。 <ul style="list-style-type: none">初期状態ではパスワードは設定されていません。半角英数字 1～249 文字で入力します。 注意 <ul style="list-style-type: none">大文字／小文字は区別されます。パスワードの入力文字は表示されません。●●●のように伏せ文字で表示されます。パスワードは、第三者に推測されにくく、忘れないような文字列を入力してください。

3. かんたん設定

(4) [プロバイダの設定]の各項目を設定し、[次へ]ボタンをクリックします。

メモ パスワードの設定に戻る場合は、[戻る]ボタンをクリックしてください。

1. パスワードの設定 → 2. **プロバイダの設定** → 3. インターネット接続の設定 → 4. 設定の確認と反映 → 5. 終了

かんたん設定：プロバイダの設定

プロバイダの設定をします。

	現在の設定	設定の変更
プロバイダ		<input checked="" type="radio"/> OCN(OCNバーチャルコネク)
		<input type="radio"/> JPIX(v6プラス)
		<input type="radio"/> BIGLOBE(IPv6オプション)

IPv6プレフィックス取得設定

IPv6プレフィックスの取得方法を設定します。
ひかり電話契約]があり、ひかり電話ルータのLAN側に装置を設置する場合「RA固定」を選択してください。

	現在の設定	設定の変更
プレフィックス取得方法		<input checked="" type="radio"/> PD/RA自動判別
		<input type="radio"/> RA固定

グローバルアドレスの方式設定

グローバルアドレスの割り当て方式を設定します。

	現在の設定	設定の変更
割り当て方式		<input checked="" type="radio"/> 動的
		<input type="radio"/> 固定

戻る **次へ**

番号	項目	内容
①	プロバイダ	プロバイダサービス名を選択します。
②	プレフィックス取得方法	RA 固定と PD/RA 自動判別のいずれかを選択します。
③	割り当て方式	プロバイダと契約したグローバルアドレスの割り当て方式を選択します。

3. かんたん設定

JPIX(v6 プラス)で割り当て方式が固定の場合

1. パスワードの設定 → 2. **プロバイダの設定** → 3. インターネット接続の設定 → 4. 設定の確認と反映 → 5. 終了

かんたん設定：プロバイダの設定

プロバイダの設定をします。

	現在の設定	設定の変更
プロバイダ		<input type="radio"/> OCN(OCNバーチャルコネク)
		<input checked="" type="radio"/> JPIX(v6プラス)
		<input type="radio"/> BIGLOBE(IPv6オプション)

IPv6プレフィックス取得設定

IPv6プレフィックスの取得方法を設定します。
「ひかり電話契約」があり、ひかり電話ルータのLAN側に装置を設置する場合「RA固定」を選択してください。

	現在の設定	設定の変更
プレフィックス取得方法		<input checked="" type="radio"/> PD/RA自動判別
		<input type="radio"/> RA固定

グローバルアドレスの方式設定

グローバルアドレスの割り当て方式を設定します。

	現在の設定	設定の変更
割り当て方式		<input type="radio"/> 動的
		<input checked="" type="radio"/> 固定

ダイナミックDNSサーバの設定

プロバイダから割り当てられた情報をもとに、ダイナミックDNSサーバの設定をします。

	現在の設定	設定の変更
URL		ダイナミックDNSサーバのURLを設定します。 <input type="text" value="https://www.example.com.port"/> URLを入力してください。
ユーザ名		<input type="text"/> 文字列(半角英数字)を入力してください。
パスワード		<input type="text"/> 文字列(半角英数字)を入力してください。

BRアドレスの設定

プロバイダから割り当てられたBR(Border Relay)のIPv6アドレスを設定します。

	現在の設定	設定の変更
BRアドレス		<input type="text"/> IPv6アドレスを入力してください。

IPv4グローバルアドレスの設定

プロバイダから割り当てられたIPv4グローバルアドレスを設定します。

	現在の設定	設定の変更
IPv4グローバルアドレス		<input type="text"/> IPアドレスを入力してください。

戻る 次へ

3. かんたん設定

番号	項目	内容
①	URL	プロバイダから通知されているダイナミック DNS サーバの URL を設定します。
②	ユーザ名	プロバイダから通知されているユーザ名を設定します。 ・ 半角英数字で 1～250 文字まで入力できます。
③	パスワード	プロバイダから通知されているパスワードを設定します。 ・ 半角英数字で 1～250 文字まで入力できます。 注意 大文字、小文字も区別されます。
④	BR アドレス	プロバイダから通知されている BR(Border Relay)の IPv6 アドレスを設定します。
⑤	IPv4 グローバルアドレス	プロバイダから通知されている IPv4 グローバルアドレスを設定します。

(5) [インターネット接続の設定]の項目を設定し、[設定の確認]ボタンをクリックします。

メモ プロバイダの設定に戻る場合は、[戻る]ボタンをクリックしてください。

1. パスワードの設定 → 2. プロバイダの設定 → 3. **インターネット接続の設定** → 4. 設定の確認と反映 → 5. 終了

かんたん設定：インターネット接続の設定

接続先インターネットの設定をします。

	現在の設定	設定の変更
インターネット接続		<input checked="" type="radio"/> IPv4接続 + IPv6接続 <input type="radio"/> IPv4接続

IPv6インタフェースIDの設定

ホストを識別するIDを設定します。

	現在の設定	設定の変更
インタフェースID		<input type="text" value="XX.XX.XX.XX.XX.XX.XX.XX"/> インタフェースIDを入力してください。

通信セキュリティの設定

	現在の設定	設定の変更
セキュリティ強度	レベル1	<input checked="" type="radio"/> レベル1 - 外部からの不要なパケットを NAPT(IPv4)、ダイナミックフィルタ(IPv6)により廃棄します。 <input type="radio"/> レベル2 - 外部からの不要なパケットを NAPT(IPv4)、ダイナミックフィルタ(IPv6)により廃棄します。 - 内部からの不要な通信を制限します。

LAN1: LANの設定(GigaEthernet1.0)

LAN側IPアドレスを変更する場合は、反映後に新しいIPアドレスで接続しなおす必要があります。

	現在の設定	設定の変更
LAN側IPアドレス	192.168.1.254/24	<input type="text" value="192.168.1.254"/> / <input type="text" value="24"/>

3. かんたん設定

番号	項目	内容
①	インターネット接続	「IPv4 のみの利用」または「IPv4 と IPv6 の両方を利用」を選択します。 <ul style="list-style-type: none">「IPv4 接続+IPv6 接続」の場合、IPv4 と IPv6 の両方を利用してインターネット接続します。「IPv4 接続」の場合、IPv4 のみを利用してインターネット接続します。
②	インタフェース ID	ホストを識別するための IPv6 インタフェース ID を設定します。 <ul style="list-style-type: none">割り当て方式で「動的」を選択した場合、「IPv6 インタフェース ID の設定」は表示されません。
③	セキュリティ強度	外部からの不要なパケットの廃棄と内部ネットワークからの不要な通信を制限します。 <input type="checkbox"/> メモ 外部からの不要なパケットの廃棄は停止できません。
④	LAN 側 IP アドレス	LAN 側 IP アドレスを設定します。 IP アドレスを変更する場合、現在の接続は切断されます。新しい IP アドレスに接続しなおしてください。

3. かんたん設定

(6) 入力した項目が正しいことを確認し、[反映]ボタンをクリックします。

メモ インターネット接続の設定に戻る場合は、[戻る]ボタンをクリックしてください。

1. パスワードの設定 → 2. プロバイダの設定 → 3. インターネット接続の設定 → 4. 設定の確認と反映 → 5. 終了

かんたん設定：設定の確認と反映

設定内容を変更する場合は [反映] を押してください。
LAN側IPアドレスを変更する場合は、新しいIPアドレスで接続しなおしてください。

ログイン認証用パスワードの設定

	現在の設定	設定の変更
ユーザ名	admin	変更できません
パスワード	*****	<input checked="" type="radio"/> パスワードを変更しない <input type="radio"/> パスワードを変更する

プロバイダの設定

	現在の設定	設定の変更
プロバイダ		<input checked="" type="radio"/> OCN(OCNバーチャルコネク)
		<input type="radio"/> JPIX(v6プラス)
		<input type="radio"/> BIGLOBE(IPv6オプション)

IPv6プレフィックス取得設定

	現在の設定	設定の変更
プレフィックス取得方法		<input checked="" type="radio"/> PD/RA自動判別 <input type="radio"/> RA固定

グローバルアドレスの方式設定

	現在の設定	設定の変更
割り当て方式		<input checked="" type="radio"/> 動的 <input type="radio"/> 固定

IPv6接続の設定

	現在の設定	設定の変更
接続先インターネット		<input checked="" type="radio"/> IPv4接続 + IPv6接続 <input type="radio"/> IPv4接続

通信セキュリティの設定

	現在の設定	設定の変更
セキュリティ強度	レベル1	<input checked="" type="radio"/> レベル1 - 外部からの不要なパケットをNAPT(IPv4)、ダイナミックフィルタ(IPv6)により廃棄します。 <input type="radio"/> レベル2 - 外部からの不要なパケットをNAPT(IPv4)、ダイナミックフィルタ(IPv6)により廃棄します。 - 内部からの不要な通信を制限します。

LAN1: LANの設定(GigaEthernet1.0)

	現在の設定	設定の変更
LAN側IPアドレス	192.168.100.2/24	<input type="text" value="192.168.100.2"/> / 24

戻る 反映

3. かんたん設定

(7) 「設定内容を変更しました。」のメッセージが表示されることを確認し、[トップページへ]ボタンをクリックします。

1. パスワードの設定 → 2. プロバイダの設定 → 3. インターネット接続の設定 → 4. 設定の確認と反映 → 5. 終了

かんたん設定：終了

設定内容を変更しました

ログイン認証用パスワードの設定

	現在の設定	設定の変更
ユーザ名	admin	変更できません
パスワード	*****	<input checked="" type="radio"/> パスワードを変更しない <input type="radio"/> パスワードを変更する

プロバイダの設定

	現在の設定	設定の変更
プロバイダ	JPIX (v6プラス)	<input type="radio"/> OCN(OCNバーチャルコネク) <input checked="" type="radio"/> JPIX(v6プラス) <input type="radio"/> BIGLOBE(IPv6オプション)

IPv6プレフィックス取得設定

	現在の設定	設定の変更
プレフィックス取得方法		<input checked="" type="radio"/> PD/RA自動判別 <input type="radio"/> RA固定

グローバルアドレスの方式設定

	現在の設定	設定の変更
割り当て方式	動的	<input checked="" type="radio"/> 動的 <input type="radio"/> 固定

IPv6接続の設定

	現在の設定	設定の変更
接続先インターネット	IPv4接続 + IPv6接続	<input checked="" type="radio"/> IPv4接続 + IPv6接続 <input type="radio"/> IPv4接続

通信セキュリティの設定

	現在の設定	設定の変更
セキュリティ強度	レベル1	<input checked="" type="radio"/> レベル1 - 外部からの不要なパケットをNAPT(IPv4)、ダイナミックフィルタ(IPv6)により廃棄します。 <input type="radio"/> レベル2 - 外部からの不要なパケットをNAPT(IPv4)、ダイナミックフィルタ(IPv6)により廃棄します。 - 内部からの不要な通信を制限します。


LAN1: LANの設定(GigaEthernet1.0)

	現在の設定	設定の変更
LAN側IPアドレス	192.168.1.254/24	<input type="text" value="192.168.1.254"/> / <input type="text" value="24"/>

トップページへ

3. かんたん設定

(8) トップページでWAN情報の接続状態を確認します。

 [更新]ボタンをクリックすると、情報を更新することが可能です。

(9) メニューエリア、または、メッセージエリアから[設定の保存]をクリックします。



!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず「設定の保存」を行ってください。

メニュー
トップページ
設定の保存
ログアウト

かんたん設定
かんたん設定

詳細設定
装置情報 (装置名:Router) 自動更新間隔: 停止

端末管理
端末管理

保守管理
装置状態の表示
装置ログの取得
設定データの管理
設定の初期化
ソフトウェアの更新
pingの実行
任意コマンドの実行
IP電話サービス保守
URLオフロード
リンクマネージャ
Wake on LAN
再起動

拡張ページ
拡張ページ

外部リンク
製品ページ

バージョン	稼働時間	稼働率	メモリ	内部温度	内部電圧
	8分	99%	20%	47.0℃	3.2680V

ネットワーク情報

デバイス	接続状態	送信量	受信量
GE0 (GigaEthernet0)	全二重 1Gbpsで接続	0%	0%
GE1 (GigaEthernet1)	Port1: 全二重 1Gbpsで接続 Port2: 接続されていません Port3: 接続されていません Port4: 接続されていません	0%	0%

WAN情報

接続名	接続状態	情報
WAN1: GigaEthernet0.0	接続	IPv6アドレス: なし
WAN2: Tunnel0.0	接続されていません	IPアドレス: なし

VPN情報

接続名	接続状態	通信量[packets]
Tunnel0.0	接続されていません MAP-E	送信: 0 受信: 0

UTM情報

ライセンス状態	ライセンス満了日時
設定されていません	

3. かんたん設定

(10) [保存実行]ボタンをクリックします。

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず『[設定の保存](#)』を行ってください。

設定の保存

設定を保存します。

よろしければ [保存実行] を押してください。 **保存実行**

(11) 「設定を保存しました。」のメッセージを確認します。

設定の保存

設定を保存しました。

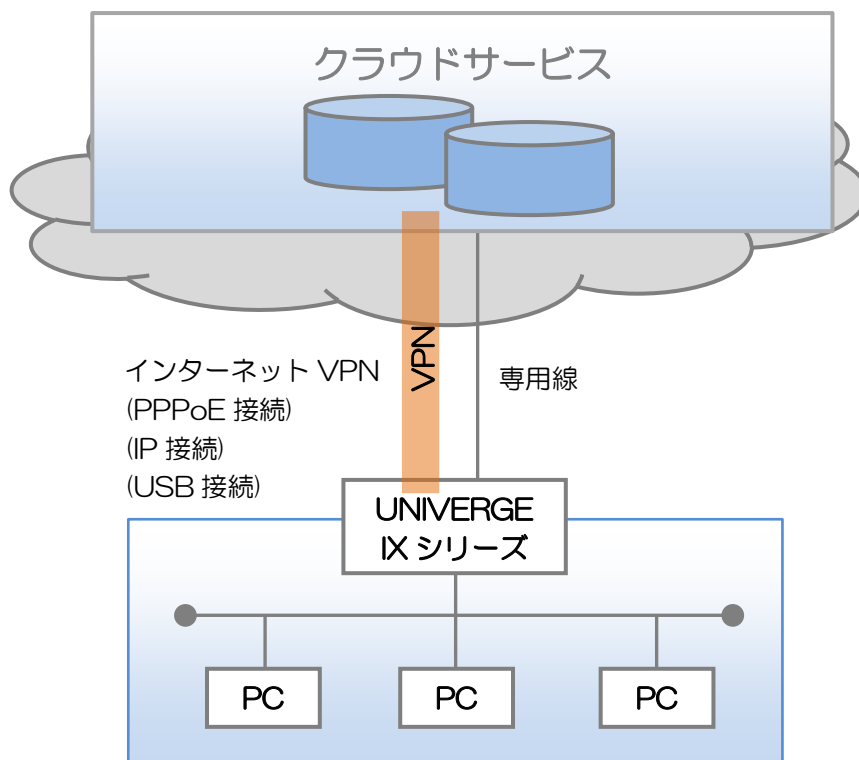
[トップページへ](#)

3. かんたん設定

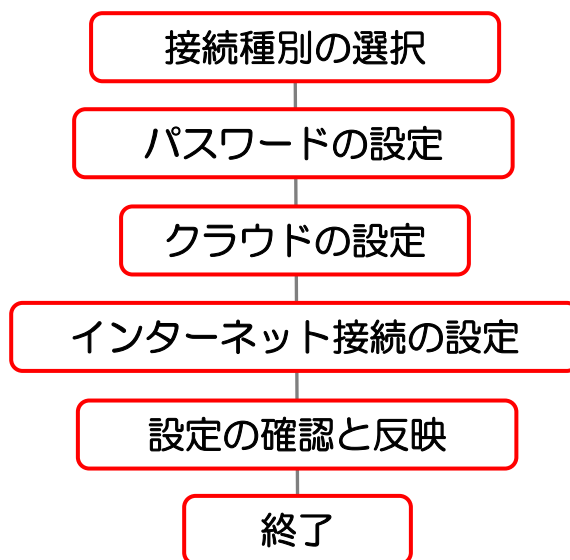
3.7 クラウド接続

インターネットVPNや専用線を使用したクラウド接続の設定を行います。

【構成イメージ】



【設定手順】



3. かんたん設定

(1) ログイン後のメニューエリアから[かんたん設定]をクリックします。

メモ トップページリンクをクリックすることで、接続種別の各ページに移動することも可能です。

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず『設定の保存』を行ってください。

かんたん設定

ルータの設定を開始します。以下のリンクから選択してください。
パスワードを登録・変更する前にユーザ名とパスワードを入力する画面が表示された場合は、そのまま「OK」をクリックしてください。

かんたん設定

- [インターネット接続](#)
フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用して、インターネットに接続する設定を行います。
- [インターネット接続+VPN接続](#)
フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用したインターネット接続と、インターネットVPNによる拠点間通信の設定を行います。
- [インターネット接続+フレッツ・VPNワイド接続](#)
フレッツ光を使用したインターネット接続と、フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
- [フレッツ・VPNワイド接続](#)
フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
- [NGN網VPN接続](#)
NGN網を用いたVPNによる拠点間の通信の設定と、NetMeisterによる装置管理の設定を行います。
- [IPv6 IPoE接続](#)
IPv6 IPoE接続の設定を行います。
プロバイダの動的IPまたは固定IPでのサービスを設定します。
- [クラウド接続](#)
インターネットVPNや専用線を使用したクラウド接続の設定を行います。
- [IP電話サービス接続](#)
対応するUNIVERGE Aspireシリーズと連携したIP電話ネットワークの設定を行います。

詳細設定

インタフェースやサーバのアドレスを指定したり、フィルタやQoS、VPN等、かんたん設定に含まれない詳細な設定を行う場合はこちらから設定してください。

端末管理

本装置に接続されている端末を管理します。
リンクマネージャ機能やWeb認証機能を設定します。

保守管理

装置状態の確認、ソフトウェアの更新、pingの実行など、各種保守機能の操作を行います。
URLオフロード機能による特定宛先のレーティング制御、リンクマネージャ機能による端末の保守管理などが可能です。
任意のコマンドを直接実行したい場合は[任意コマンドの実行](#)から操作してください。

3. かんたん設定

(2) 接続種別の選択で「クラウド接続」にチェックを入れ、[次へ]ボタンをクリックします。

メモ 接続種別を変更する場合には、設定の初期化が必要となります。

かんたん設定：接続種別の選択

接続種別を選択してかんたん設定を開始してください。
接続種別を変更する場合には、設定の初期化が必要となります。

	現在の設定	設定の変更
接続種別の選択	インターネット接続なし	<input type="radio"/> インターネット接続 フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用して、インターネットに接続する設定を行います。
		<input type="radio"/> インターネット接続 + VPN接続 フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用したインターネット接続と、インターネットVPNによる拠点間通信の設定を行います。
		<input type="radio"/> インターネット接続 + フレッツ・VPNワイド接続 フレッツ光を使用したインターネット接続と、フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
		<input type="radio"/> フレッツ・VPNワイド接続 フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
		<input type="radio"/> NGN網VPN接続 NGN網を用いたVPNによる拠点間の通信の設定とNetMeisterによる装置管理の設定を行います。
		<input type="radio"/> IPv6 IPoE接続 IPv6 IPoE接続の設定を行います。 プロバイダの動的IPまたは固定IPでのサービスを設定します。
		<input checked="" type="radio"/> クラウド接続 インターネットVPNや専用回線を使用したクラウド接続の設定を行います。
		<input type="radio"/> IP電話サービス接続 対応するUNIVERGE Aspireシリーズと連携したIP電話ネットワークの設定を行います。

次へ

3. かんたん設定

(3) 管理者パスワードを変更する場合は、[パスワードを変更する]を選択し、パスワードを設定した後、[次へ]ボタンをクリックします。

メモ 管理者パスワードを変更する必要が無い場合は、そのまま[次へ]ボタンをクリックします。

メモ 接続種別の選択に戻る場合は、[戻る]ボタンをクリックしてください。



番号	項目	内容
①	ユーザ名	本装置にログインするときのユーザ名を設定します。 <ul style="list-style-type: none">初期状態ではユーザ名は設定されていません。パスワード設定後のユーザ名は「admin」です。Web 設定からは変更できません。
②	パスワード	本装置にログインするときのパスワードを設定します。 <ul style="list-style-type: none">初期状態ではパスワードは設定されていません。半角英数字で 1～249 文字まで入力できます。 注意 <ul style="list-style-type: none">大文字／小文字は区別されます。パスワードの入力文字は表示されません。●●●のように伏せ文字で表示されます。パスワードは、第三者に推測されにくく、忘れないような文字列を入力してください。

(4) [クラウドの設定]の各項目を設定し、[次へ]ボタンをクリックします。

メモ パスワードの設定に戻る場合は、[戻る]ボタンをクリックしてください。

3. かんたん設定

AWS(Amazon Web Services)にインターネットVPNで接続する場合

注意 AWS(Amazon Web Services)とかんたん設定によるVPN接続の併用はできません。

注意 AWS(Amazon Web Services)と詳細設定によるダイナミックVPNの併用はできません。

3. かんたん設定

1. パスワードの設定 → 2. クラウドの設定 → 3. インターネット接続の設定 → 4. 設定の確認と反映 → 5. 終了

かんたん設定：クラウドの設定

クラウドのサービス種別を設定します。

	現在の設定	設定の変更
サービス種別		<input checked="" type="radio"/> AWS (Amazon Web Services) <input type="radio"/> Microsoft Azure <input type="radio"/> NEC Cloud IaaS
接続形態		<input checked="" type="radio"/> インターネットVPN <input type="radio"/> 専用線

AWS (Amazon Web Services) にインターネットVPNで接続

IPsec Tunnel #1

接続先 (クラウド)	WAN側 IPアドレス		Outside IP Addresses: の Virtual Private Gatewayを入力してください。 <input type="text"/> IPアドレスを入力してください。
	VPNアドレ ス		Inside IP Addresses: の Virtual Private Gatewayを入力してください。 <input type="text"/> IPアドレスを入力してください。
	AS番号		BGP Configuration Options: の Virtual Private Gateway ASNを入力してください。 <input type="text" value="10124"/>
接続元 (IX)	VPNアドレ ス		Inside IP Addresses: の Customer Gatewayを入力してください。 <input type="text"/> / <input type="text" value="30"/> IPアドレスを入力してください。
	AS番号		BGP Configuration Options: の Customer Gateway ASNを入力してください。 <input type="text" value="65000"/>

IPsec Tunnel #2

接続先 (クラウド)	WAN側 IPアドレス		Outside IP Addresses: の Virtual Private Gatewayを入力してください。 <input type="text"/>
	VPNアドレ ス		Inside IP Addresses: の Virtual Private Gatewayを入力してください。 <input type="text"/>
	AS番号		BGP Configuration Options: の Virtual Private Gateway ASNを入力してください。 <input type="text" value="10124"/>
接続元 (IX)	VPNアドレ ス		Inside IP Addresses: の Customer Gatewayを入力してください。 <input type="text"/> / <input type="text" value="30"/>
	AS番号		IPsec Tunnel #1 と共通です

暗号/認証の詳細設定

事前共有鍵以外の設定は、以下のセキュリティ方式が選ばれます。

IKEv1: 暗号 AES(128bit) / 認証 SHA1、Lifetime 28800 秒、DH group 2(1024bit)

IPsec: 暗号 AES(128bit) / 認証 SHA1、Lifetime 3600 秒、PFS 有効 (1024bit)

IPsec Tunnel #1

	現在の設定	設定の変更
IKE	事前共有鍵	Configure the IKE SA as follows の Pre-Shared Keyを入力してください。 <input type="text"/> 文字列(半角英数字)を入力してください。

IPsec Tunnel #2

	現在の設定	設定の変更
IKE	事前共有鍵	Configure the IKE SA as follows の Pre-Shared Keyを入力してください。 <input type="text"/>

戻る 次へ

3. かんたん設定

番号	項目	内容																		
①	サービス種別	「AWS (Amazon Web Services)」を選択します。																		
②	接続形態	「インターネット VPN」を選択します。																		
③	IPsec Tunnel#1 接続先(クラウド) WAN 側 IP アドレス	IPsec Tunnel#1 の Outside IP Addresses:の Virtual Private Gateway を入力します。																		
④	IPsec Tunnel#1 接続先(クラウド) VPN アドレス	IPsec Tunnel#1 の Inside IP Addresses:の Virtual Private Gateway を入力します。																		
⑤	IPsec Tunnel#1 接続先(クラウド) AS 番号	IPsec Tunnel#1 の BGP Configuration Options:の Virtual Private Gateway ASN(1～65535)を入力します。 ・ 初期値は「10124」です。																		
⑥	IPsec Tunnel#1 接続元 (X) VPN アドレス	IPsec Tunnel#1 の Inside IP Addresses:の Customer Gateway を入力します。																		
⑦	IPsec Tunnel#1 接続元 (X) AS 番号	IPsec Tunnel#1 の BGP Configuration Options:の Customer Gateway ASN(1～65535)を入力します。 ・ 初期値は「65000」です。																		
⑧	IPsec Tunnel#2 接続先(クラウド) WAN 側 IP アドレス	IPsec Tunnel#2 の Outside IP Addresses:の Virtual Private Gateway を入力します。 <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> ・ 複数 VPN を使用しない場合は、本設定は不要です。																		
⑨	IPsec Tunnel#2 接続先(クラウド) VPN アドレス	IPsec Tunnel#2 の Inside IP Addresses:の Virtual Private Gateway を入力します。 <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> ・ 複数 VPN を使用しない場合は、本設定は不要です。																		
⑩	IPsec Tunnel#2 接続先(クラウド) AS 番号	IPsec Tunnel#2 の BGP Configuration Options:の Virtual Private Gateway ASN(1～65535)を入力します。 ・ 初期値は「10124」です。 <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> ・ 複数 VPN を使用しない場合は、本設定は不要です。																		
⑪	IPsec Tunnel#2 接続元 (X) VPN アドレス	IPsec Tunnel#2 の Inside IP Addresses:の Customer Gateway を入力します。 <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> ・ 複数 VPN を使用しない場合は、本設定は不要です。																		
⑫	IPsec Tunnel#1 IKE 事前共有鍵	IPsec Tunnel#1 の Configure the IKE SA as follows の Pre-Shared Key を入力します。 ・ 半角英数字で 1～128 文字まで入力できます。 ・ 事前共有鍵以外の設定は、自動で以下のパラメータが選択されます。 <table border="1" style="margin-left: 20px;"> <thead> <tr> <th colspan="2">IKE (フェーズ 1)</th> </tr> </thead> <tbody> <tr> <td>バージョン</td> <td>IKEv1</td> </tr> <tr> <td>暗号化/認証方式</td> <td>AES128/SHA-1</td> </tr> <tr> <td>DH グループ</td> <td>2 (1024-bit)</td> </tr> <tr> <td>ライフタイム</td> <td>28800 秒</td> </tr> <tr> <th colspan="2">IPsec (フェーズ 2)</th> </tr> <tr> <td>暗号化/認証方式</td> <td>AES128/SHA-1</td> </tr> <tr> <td>DH グループ</td> <td>2 (1024-bit)</td> </tr> <tr> <td>ライフタイム</td> <td>3600 秒</td> </tr> </tbody> </table>	IKE (フェーズ 1)		バージョン	IKEv1	暗号化/認証方式	AES128/SHA-1	DH グループ	2 (1024-bit)	ライフタイム	28800 秒	IPsec (フェーズ 2)		暗号化/認証方式	AES128/SHA-1	DH グループ	2 (1024-bit)	ライフタイム	3600 秒
IKE (フェーズ 1)																				
バージョン	IKEv1																			
暗号化/認証方式	AES128/SHA-1																			
DH グループ	2 (1024-bit)																			
ライフタイム	28800 秒																			
IPsec (フェーズ 2)																				
暗号化/認証方式	AES128/SHA-1																			
DH グループ	2 (1024-bit)																			
ライフタイム	3600 秒																			

3. かんたん設定

⑬	IPsec Tunnel#2 IKE 事前共有鍵	<p>IPsec Tunnel#2 の Configure the IKE SA as follows の Pre-Shared Key を入力します。</p> <ul style="list-style-type: none">半角英数字で 1~128 文字まで入力できます。事前共有鍵以外の設定は、自動で以下のパラメータが選択されます。 <table border="1" data-bbox="587 347 1197 705"><tr><td colspan="2">IKE (フェーズ 1)</td></tr><tr><td>バージョン</td><td>IKEv1</td></tr><tr><td>暗号化/認証方式</td><td>AES128/SHA-1</td></tr><tr><td>DH グループ</td><td>2 (1024-bit)</td></tr><tr><td>ライフタイム</td><td>28800 秒</td></tr><tr><td colspan="2">IPsec (フェーズ 2)</td></tr><tr><td>暗号化/認証方式</td><td>AES128/SHA-1</td></tr><tr><td>DH グループ</td><td>2 (1024-bit)</td></tr><tr><td>ライフタイム</td><td>3600 秒</td></tr></table> <p>メモ</p> <ul style="list-style-type: none">複数 VPN を使用しない場合は、本設定は不要です。	IKE (フェーズ 1)		バージョン	IKEv1	暗号化/認証方式	AES128/SHA-1	DH グループ	2 (1024-bit)	ライフタイム	28800 秒	IPsec (フェーズ 2)		暗号化/認証方式	AES128/SHA-1	DH グループ	2 (1024-bit)	ライフタイム	3600 秒
IKE (フェーズ 1)																				
バージョン	IKEv1																			
暗号化/認証方式	AES128/SHA-1																			
DH グループ	2 (1024-bit)																			
ライフタイム	28800 秒																			
IPsec (フェーズ 2)																				
暗号化/認証方式	AES128/SHA-1																			
DH グループ	2 (1024-bit)																			
ライフタイム	3600 秒																			

3. かんたん設定

AWS(Amazon Web Services)に専用線で接続する場合

注意 AWS(Amazon Web Services)とかんたん設定によるVPN接続の併用はできません。

注意 AWS(Amazon Web Services)と詳細設定によるダイナミックVPNの併用はできません。

1. パスワードの設定 → 2. **クラウドの設定** → 3. インターネット接続の設定 → 4. 設定の確認と反映 → 5. 終了

かんたん設定：クラウドの設定

クラウドのサービス種別を設定します。

	現在の設定	設定の変更
サービス種別		<input checked="" type="radio"/> AWS (Amazon Web Services) <input type="radio"/> Microsoft Azure <input type="radio"/> NEC Cloud IaaS
接続形態		<input type="radio"/> インターネットVPN <input checked="" type="radio"/> 専用線

AWS (Amazon Web Services) に専用線で接続

接続先 (クラウド)	WAN側 IPアドレス	接続先のIPアドレスを入力してください。 [] IPアドレスを入力してください。
	AS番号	[10124]
	BGP パスワード	接続先と共通のパスワードを入力してください。 [] 文字列(半角英数字)を入力してください。
接続元 (IX)	WAN側 IPアドレス	接続元のIPアドレスを入力してください。 [] / [31] v IPアドレスを入力してください。
	AS番号	[65010]
	VLAN番号	接続元のVLAN番号を入力してください。 [] 数字を入力してください。

戻る **次へ**

番号	項目	内容
①	サービス種別	「AWS (Amazon Web Services)」を選択します。
②	接続形態	「専用線」を選択します。
③	接続先(クラウド) WAN側IPアドレス	接続先のIPアドレスを入力します。
④	接続先(クラウド) AS番号	接続先のBGPピアのAS番号(1~65534)を入力します。 ・初期値は「10124」です。
⑤	接続先(クラウド) BGPパスワード	接続先と共通のパスワードを設定します。 ・半角英数字で1~218文字まで入力できます。
⑥	接続元(IX) WAN側IPアドレス	接続元のIPアドレスを入力します。
⑦	接続元(IX) AS番号	接続元のBGPのAS番号(1~65534)を入力します。 ・初期値は「65010」です。
⑧	接続元(IX) VLAN番号	接続元のVLAN番号(1~4095)を入力します。

3. かんたん設定

Microsoft Azure に接続する場合

1. パスワードの設定 → 2. クラウドの設定 → 3. インターネット接続の設定 → 4. 設定の確認と反映 → 5. 終了

かんたん設定：クラウドの設定

クラウドのサービス種別を設定します。

		現在の設定	設定の変更
サービス種別			<input type="radio"/> AWS (Amazon Web Services) <input checked="" type="radio"/> Microsoft Azure <input type="radio"/> NEC Cloud IaaS
接続形態			<input checked="" type="radio"/> インターネットVPN

Microsoft Azure にインターネットVPNで接続

接続先 (クラウド)	WAN側 IPアドレス	接続先のIPアドレスを入力してください。 <input type="text"/> IPアドレスを入力してください。
	LAN側 ネットワーク	接続先の仮想ネットワークで設定しているアドレス空間のネットワークアドレスを入力してください。 <input type="text"/> / <input type="text" value="30"/> IPアドレスを入力してください。

暗号/認証の詳細設定

事前共有鍵以外の設定は、以下のセキュリティ方式が選ばれます。
 IKEv1: 暗号 AES(128bit) / 認証 SHA1、Lifetime 28800 秒、DH group 2(1024bit)
 IPsec: 暗号 AES(128bit) / 認証 SHA1、Lifetime 3600 秒、PFS 無効

		現在の設定	設定の変更
IKE	事前共有鍵		接続先と共通のパスワードを設定してください。 <input type="text"/> 文字列(半角英数字)を入力してください。

戻る

次へ

番号	項目	内容																		
①	サービス種別	「Microsoft Azure」を選択します。																		
②	接続形態	「インターネットVPN」を選択します。																		
③	接続先(クラウド) WAN 側 IP アドレス	接続先の IP アドレスを入力します。																		
④	接続先(クラウド) LAN 側ネットワーク	接続先の LAN 側のネットワークアドレスを入力します。 ・ ネットワークアドレスを入力し、サブネットマスクをプルダウンメニューから選択します。																		
⑤	IKE 事前共有鍵	接続先と共通のパスワードを設定します。 ・ 半角英数字で 1~128 文字まで入力できます。 ・ 事前共有鍵以外の設定は、自動で以下のパラメータが選択されます。 <table border="1" style="margin-top: 10px;"> <thead> <tr> <th colspan="2">IKE (フェーズ 1)</th> </tr> </thead> <tbody> <tr> <td>バージョン</td> <td>IKEv1</td> </tr> <tr> <td>暗号化/認証方式</td> <td>AES128/SHA-1</td> </tr> <tr> <td>DH グループ</td> <td>2 (1024-bit)</td> </tr> <tr> <td>ライフタイム</td> <td>28800 秒</td> </tr> <tr> <th colspan="2">IPsec (フェーズ 2)</th> </tr> <tr> <td>暗号化/認証方式</td> <td>AES128/SHA-1</td> </tr> <tr> <td>DH グループ</td> <td>無し</td> </tr> <tr> <td>ライフタイム</td> <td>3600 秒</td> </tr> </tbody> </table>	IKE (フェーズ 1)		バージョン	IKEv1	暗号化/認証方式	AES128/SHA-1	DH グループ	2 (1024-bit)	ライフタイム	28800 秒	IPsec (フェーズ 2)		暗号化/認証方式	AES128/SHA-1	DH グループ	無し	ライフタイム	3600 秒
IKE (フェーズ 1)																				
バージョン	IKEv1																			
暗号化/認証方式	AES128/SHA-1																			
DH グループ	2 (1024-bit)																			
ライフタイム	28800 秒																			
IPsec (フェーズ 2)																				
暗号化/認証方式	AES128/SHA-1																			
DH グループ	無し																			
ライフタイム	3600 秒																			

3. かんたん設定

NEC Cloud IaaS に接続する場合

1. パスワードの設定 → 2. **クラウドの設定** → 3. インターネット接続の設定 → 4. 設定の確認と反映 → 5. 終了

かんたん設定：クラウドの設定

クラウドのサービス種別を設定します。

		現在の設定	設定の変更
サービス種別			<input type="radio"/> AWS (Amazon Web Services) <input type="radio"/> Microsoft Azure <input checked="" type="radio"/> NEC Cloud IaaS
接続形態			<input checked="" type="radio"/> インターネットVPN

NEC Cloud IaaS にインターネットVPNで接続

接続先 (クラウド)	WAN側 IPアドレス		接続先のIPアドレスを入力してください。 <input type="text"/> IPアドレスを入力してください。
	LAN側 ネットワーク		接続先のLAN側のネットワークアドレスを入力してください。 <input type="text"/> / <input type="text"/> [30 ▼] IPアドレスを入力してください。

暗号/認証の詳細設定

事前共有鍵以外の設定は、以下のセキュリティ方式が選ばれます。
 IKEv1: 暗号 AES(128bit) / 認証 SHA1、Lifetime 28800 秒、DH group 2(1024bit)
 IPsec: 暗号 AES(128bit) / 認証 SHA1、Lifetime 3600 秒、PFS 有効 (1024bit)


		現在の設定	設定の変更
IKE	事前共有鍵		接続先と共通のパスワードを設定してください。 <input type="text"/> 文字列(半角英数字)を入力してください。

戻る **次へ**

番号	項目	内容																		
①	サービス種別	「NEC Cloud IaaS」を選択します。																		
②	接続形態	「インターネット VPN」を選択します。																		
③	接続先(クラウド) WAN 側 IP アドレス	接続先の IP アドレスを入力します。																		
④	接続先(クラウド) LAN 側ネットワーク	接続先の LAN 側のネットワークアドレスを入力します。 ・ ネットワークアドレスを入力し、サブネットマスクをプルダウンメニューから選択します。																		
⑤	IKE 事前共有鍵	接続先と共通のパスワードを設定します。 ・ 半角英数字で 1~128 文字まで入力できます。 ・ 事前共有鍵以外の設定は、自動で以下のパラメータが選択されます。 <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2">IKE (フェーズ 1)</th> </tr> </thead> <tbody> <tr> <td>バージョン</td> <td>IKEv1</td> </tr> <tr> <td>暗号化/認証方式</td> <td>AES128/SHA-1</td> </tr> <tr> <td>DH グループ</td> <td>2 (1024-bit)</td> </tr> <tr> <td>ライフタイム</td> <td>28800 秒</td> </tr> <tr> <th colspan="2">IPsec (フェーズ 2)</th> </tr> <tr> <td>暗号化/認証方式</td> <td>AES128/SHA-1</td> </tr> <tr> <td>DH グループ</td> <td>2 (1024-bit)</td> </tr> <tr> <td>ライフタイム</td> <td>3600 秒</td> </tr> </tbody> </table>	IKE (フェーズ 1)		バージョン	IKEv1	暗号化/認証方式	AES128/SHA-1	DH グループ	2 (1024-bit)	ライフタイム	28800 秒	IPsec (フェーズ 2)		暗号化/認証方式	AES128/SHA-1	DH グループ	2 (1024-bit)	ライフタイム	3600 秒
IKE (フェーズ 1)																				
バージョン	IKEv1																			
暗号化/認証方式	AES128/SHA-1																			
DH グループ	2 (1024-bit)																			
ライフタイム	28800 秒																			
IPsec (フェーズ 2)																				
暗号化/認証方式	AES128/SHA-1																			
DH グループ	2 (1024-bit)																			
ライフタイム	3600 秒																			

3. かんたん設定

(5) [インターネット接続の設定]の各項目を設定し、[設定の確認]ボタンをクリックします。

 クラウドの設定に戻る場合は、[戻る]ボタンをクリックしてください。

PPPoE 接続の場合(フレッツ光回線利用の場合)

1. パスワードの設定 → 2. クラウドの設定 → 3. **インターネット接続の設定** → 4. 設定の確認と反映 → 5. 終了

かんたん設定：インターネット接続の設定

プロバイダと接続するWAN側インタフェースを設定します。

	現在の設定	設定の変更
接続形態		<input checked="" type="radio"/> PPPoE接続 (フレッツ光回線利用の場合) <input type="radio"/> IP接続 (ケーブルテレビ回線利用の場合)
WAN1: PPPoE接続の設定(GigaEthernet0.1)		
	現在の設定	設定の変更
ユーザ名		プロバイダから通知されているユーザ名を設定します。 (フレッツの場合、通常はユーザ名には@を含んでいます) <input type="text"/> 文字列(半角英数字)を入力してください。
パスワード		プロバイダから通知されているパスワードを設定します。 <input type="text"/> 文字列(半角英数字)を入力してください。
WAN側IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
DNSアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定

 戻る

 設定の確認

3. かんたん設定

番号	項目	内容
①	接続形態	「PPPoE 接続(フレッツ光回線利用の場合)」を選択します。
②	ユーザ名	プロバイダから通知されているユーザ名を設定します。 (フレッツの場合、通常はユーザ名には@を含んでいます) ・ 半角英数字で 1~59 文字まで入力できます。
③	パスワード	プロバイダから通知されているパスワードを設定します。 ・ 半角英数字で 1~79 文字まで入力できます。 注意 ・ 大文字、小文字も区別されます。
④	WAN 側 IP アドレス	PPPoE 接続の WAN 側 IP アドレスを設定します。 ・ プロバイダから WAN 側 IP アドレスが与えられていないときは「自動取得」を、固定 IP アドレスが与えられているときは「手動設定」を選択します。 ・ 「手動設定」を選択したときは、プロバイダから与えられた IP アドレスを入力し、サブネットマスクをプルダウンメニューから選択します。 注意 ・ 他のインタフェースに設定されている IP アドレスを使用することはできません。 ・ 「自動取得」を選択した場合、IP アドレスを入力することはできません。
⑤	DNS アドレス	PPPoE 接続の DNS サーバのアドレスを設定します。 ・ プロバイダから DNS サーバのアドレスが与えられていないときは「自動取得」を、与えられているとき、または独自に指定するときは「手動設定」を選択します。 ・ 「手動設定」を選択したときは、プロバイダから与えられたプライマリ DNS サーバの IP アドレスを上段に、セカンダリ DNS サーバの IP アドレスを下段に入力します。セカンダリは省略可能です。 注意 ・ 「自動取得」を選択した場合、DNS アドレスを入力することはできません。

3. かんたん設定

IP 接続の場合(ケーブルテレビ回線利用の場合)

1. パスワードの設定 → 2. クラウドの設定 → 3. インターネット接続の設定 → 4. 設定の確認と反映 → 5. 終了

かんたん設定：インターネット接続の設定

プロバイダと接続するWAN側インタフェースを設定します。

	現在の設定	設定の変更
接続形態		<input type="radio"/> PPPoE接続 (フレッツ光回線利用の場合) <input checked="" type="radio"/> IP接続 (ケーブルテレビ回線利用の場合)
WAN1: IP接続の設定(GigaEthernet0.0)		
	現在の設定	設定の変更
WAN側IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
DNSアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定

番号	項目	内容
①	接続形態	「IP 接続 (ケーブルテレビ回線利用の場合)」を選択します。
②	WAN 側 IP アドレス	IP 接続の WAN 側 IP アドレスを設定します。 <ul style="list-style-type: none"> プロバイダから WAN 側 IP アドレスが与えられていないときは「自動取得」を、固定 IP アドレスが与えられているときは「手動設定」を選択します。 「手動設定」を選択したときは、プロバイダから与えられた IP アドレスを入力し、サブネットマスクをプルダウンメニューから選択します。 注意 <ul style="list-style-type: none"> 他のインタフェースに設定されている IP アドレスを使用することはできません。 「自動取得」を選択した場合、IP アドレスを入力することはできません。
③	DNS アドレス	IP 接続の DNS サーバのアドレスを設定します。 <ul style="list-style-type: none"> プロバイダから DNS サーバのアドレスが与えられていないときは「自動取得」を、与えられているとき、または独自に指定するときは「手動設定」を選択します。 「手動設定」を選択したときは、プロバイダから与えられたプライマリ DNS サーバの IP アドレスを上段に、セカンダリ DNS サーバの IP アドレスを下段に入力します。セカンダリは省略可能です。 注意 <ul style="list-style-type: none"> 「自動取得」を選択した場合、DNS アドレスを入力することはできません。

3. かんたん設定

USB 接続の場合(3G・LTE 回線利用の場合)

※IX2215/IX2235/IX2310/IX3315 のみ

1. パスワードの設定 → 2. クラウド接続の設定 → 3. **インターネット接続の設定** → 4. 設定の確認と反映 → 5. 終了

かんたん設定：インターネット接続の設定

プロバイダと接続するWAN側インタフェースを設定します。

	現在の設定	設定の変更
接続形態		<input type="radio"/> PPPoE接続（フレッツ光回線利用の場合） <input type="radio"/> IP接続（ケーブルテレビ回線利用の場合） <input checked="" type="radio"/> USB接続（3G・LTE回線利用の場合）
WAN1: USB接続の設定(USB-Serial0.0)		
	現在の設定	設定の変更
ユーザ名		プロバイダからユーザ名が指定されている場合に設定します。 <input type="text"/>
パスワード		プロバイダからパスワードが指定されている場合に設定します。 <input type="text"/>
PDPタイプ		プロバイダからPDPタイプが指定されている場合に設定します。 -- ▾
APN		プロバイダからAPNが指定されている場合に設定します。 <input type="text"/>
WAN側IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
DNSアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定

3. かんたん設定

番号	項目	内容
①	接続形態	「USB 接続 (3G・LTE 回線利用の場合)」を選択します。
②	ユーザ名	プロバイダからユーザ名が指定されている場合に設定します。 ・ 半角英数字で 1～59 文字まで入力できます。
③	パスワード	プロバイダからパスワードが指定されている場合に設定します。 ・ 半角英数字で 1～79 文字まで入力できます。 注意 ・ 大文字、小文字も区別されます。
④	PDP タイプ	プロバイダから PDP タイプが指定されている場合に設定します。
⑤	APN	プロバイダから APN が指定されている場合に設定します。 ・ 半角英数字で 1～90 文字まで入力できます。
⑥	WAN 側 IP アドレス	USB 接続の WAN 側 IP アドレスを設定します。 ・ プロバイダから WAN 側 IP アドレスが与えられていないときは「自動取得」を、固定 IP アドレスが与えられているときは「手動設定」を選択します。 ・ 「手動設定」を選択したときは、プロバイダから与えられた IP アドレスを入力し、サブネットマスクをプルダウンメニューから選択します。 注意 ・ 他のインターフェースに設定されている IP アドレスを使用することはできません。 ・ 「自動取得」を選択した場合、IP アドレスを入力することはできません。
⑦	DNS アドレス	USB 接続の DNS サーバのアドレスを設定します。 ・ プロバイダから DNS サーバのアドレスが与えられていないときは「自動取得」を、与えられているとき、または独自に指定するときは「手動設定」を選択します。 ・ 「手動設定」を選択したときは、プロバイダから与えられたプライマリ DNS サーバの IP アドレスを上段に、セカンダリ DNS サーバの IP アドレスを下段に入力します。セカンダリは省略可能です。 注意 ・ 「自動取得」を選択した場合、DNS アドレスを入力することはできません。

3. かんたん設定

(6) 入力した項目が正しいことを確認し、[反映]ボタンをクリックします。

× インターネット接続の設定に戻る場合は、[戻る]ボタンをクリックしてください。

1. パスワードの設定 → 2. クラウドの設定 → 3. インターネット接続の設定 → 4. 設定の確認と反映 → 5. 終了

かんたん設定：設定の確認と反映

設定内容を変更する場合は [反映] を押してください。

ログイン認証用パスワードの設定

	現在の設定	設定の変更
ユーザ名	admin	変更できません
パスワード	パスワード設定なし	<input type="radio"/> パスワードを変更しない <input checked="" type="radio"/> パスワードを変更する ●●●● 確認のためもう一度入力してください。 ●●●●

クラウド接続の設定

	現在の設定	設定の変更
サービス種別		<input checked="" type="radio"/> AWS (Amazon Web Services) <input type="radio"/> Microsoft Azure <input type="radio"/> NEC Cloud IaaS
接続形態		<input checked="" type="radio"/> インターネットVPN <input type="radio"/> 専用線

AWS (Amazon Web Services) にインターネットVPNで接続

接続先 (クラウド)	WAN側 IPアドレス	Outside IP Addresses:の Virtual Private Gatewayを入力してください。 203.0.113.254
	VPNアドレス	Inside IP Addresses:の Virtual Private Gatewayを入力してください。 169.254.252.25
	AS番号	BGP Configuration Options:の Virtual Private Gateway ASNを入力してください。 10124
接続元 (IX)	VPNアドレス	Inside IP Addresses:の Customer Gatewayを入力してください。 169.254.252.26 / 30
	AS番号	BGP Configuration Options:の Customer Gateway ASNを入力してください。 65000

暗号/認証の詳細設定

事前共有鍵以外の設定は、自動で適切なセキュリティ方式が選ばれます。

	現在の設定	設定の変更
IKE	事前共有鍵	Configure the IKE SA as followsの Pre-Shared Keyを入力してください。 cloud-password

インターネット接続の設定

	現在の設定	設定の変更
接続形態		<input checked="" type="radio"/> PPPoE接続 (フレッツ光回線利用の場合) <input type="radio"/> IP接続 (ケーブルテレビ回線利用の場合)

WAN1: PPPoE接続の設定(GigaEthernet0.1)

	現在の設定	設定の変更
ユーザ名		プロバイダから通知されているユーザ名を設定します。 (フレッツの場合、通常はユーザ名には@を含んでいます) user@example.com
パスワード		プロバイダから通知されているパスワードを設定します。 user-password
WAN側IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
DNSアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定

戻る 反映

3. かんたん設定

(7) 「設定内容を変更しました。」のメッセージが表示されることを確認し、[トップページへ]ボタンを押します。

1. パスワードの設定 → 2. クラウドの設定 → 3. インターネット接続の設定 → 4. 設定の確認と反映 → 5. 終了

かんたん設定：終了

設定内容を変更しました。

ログイン認証用パスワードの設定

	現在の設定	設定の変更
ユーザ名	admin	変更できません
パスワード	*****	<input type="radio"/> パスワードを変更しない <input checked="" type="radio"/> パスワードを変更する ●●●● 確認のためもう一度入力してください。 ●●●●

クラウド接続の設定

	現在の設定	設定の変更
サービス種別	AWS	<input checked="" type="radio"/> AWS (Amazon Web Services) <input type="radio"/> Microsoft Azure <input type="radio"/> NEC Cloud IaaS
接続形態	インターネットVPN	<input checked="" type="radio"/> インターネットVPN <input type="radio"/> 専用線

AWS (Amazon Web Services) にインターネットVPNで接続

接続先 (クラウド)	WAN側 IPアドレス	203.0.113.254	Outside IP Addresses:の Virtual Private Gatewayを入力してください。 203.0.113.254
	VPNアドレス	169.254.252.25	Inside IP Addresses:の Virtual Private Gatewayを入力してください。 169.254.252.25
	AS番号	10124	BGP Configuration Options:の Virtual Private Gateway ASNを入力してください。 10124
接続元 (IX)	VPNアドレス	169.254.252.26/30	Inside IP Addresses:の Customer Gatewayを入力してください。 169.254.252.26 / 30
	AS番号	65000	BGP Configuration Options:の Customer Gateway ASNを入力してください。 65000

暗号/認証の詳細設定

事前共有鍵以外の設定は、自動で適切なセキュリティ方式が選ばれます。

	現在の設定	設定の変更
IKE	事前共有鍵	cloud-password
		Configure the IKE SA as followsの Pre-Shared Keyを入力してください。 cloud-password

インターネット接続の設定

	現在の設定	設定の変更
接続形態	PPPoE接続	<input checked="" type="radio"/> PPPoE接続 (フレッツ光回線利用の場合) <input type="radio"/> IP接続 (ケーブルテレビ回線利用の場合)


WAN1: PPPoE接続の設定(GigaEthernet0.1)

	現在の設定	設定の変更
ユーザ名	user@example.com	プロバイダから通知されているユーザ名を設定します。(フレッツの場合、通常はユーザ名には@を含んでいます) user@example.com
パスワード	user-password	プロバイダから通知されているパスワードを設定します。 user-password
WAN側IPアドレス	自動取得	<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
DNSアドレス	自動取得	<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定

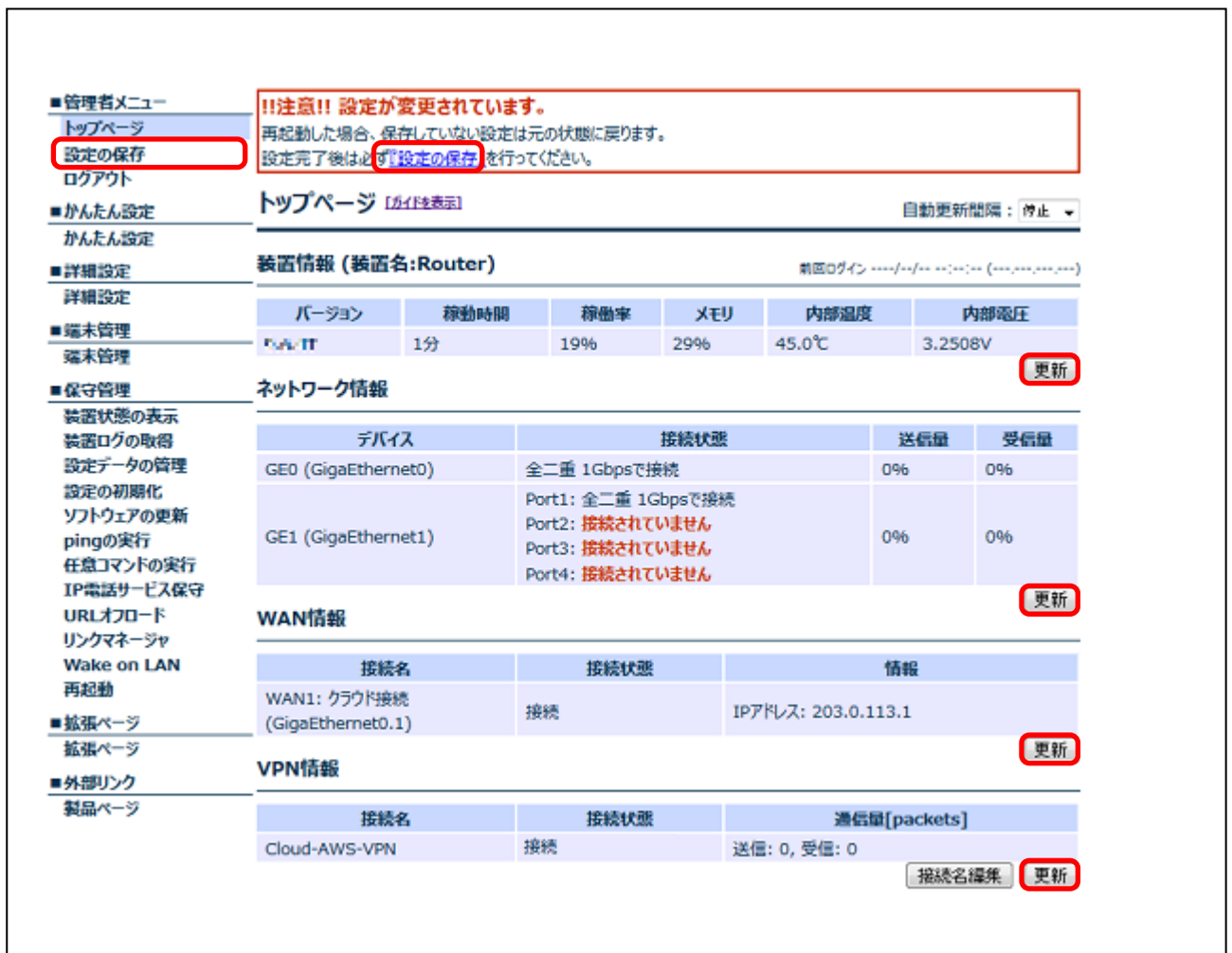
トップページへ

3. かんたん設定

(8) トップページでWAN情報の接続状態を確認します。

 [更新]ボタンをクリックすると、情報を更新することが可能です。

(9) メニューエリア、または、メッセージエリアから[設定の保存]をクリックします。



The screenshot shows the 'Easy Setup' page of a router. On the left is a navigation menu with '設定の保存' (Save Settings) highlighted. A red box highlights a warning message: '!!注意!! 設定が変更されています。再起動した場合、保存していない設定は元の状態に戻ります。設定完了後は必ず「設定の保存」を行ってください。' (Warning!! Settings have been changed. If you restart, settings not saved will return to the original state. After completion, please always click 'Save Settings').

The main content area shows system information for a 'Router' device. A table displays system metrics:

バージョン	稼働時間	稼働率	メモリ	内部温度	内部電圧
Firmware	1分	19%	29%	45.0℃	3.2508V

Below this is the 'Network Information' section with a table of network interfaces:

デバイス	接続状態	送信量	受信量
GE0 (GigaEthernet0)	全二重 1Gbpsで接続	0%	0%
GE1 (GigaEthernet1)	Port1: 全二重 1Gbpsで接続 Port2: 接続されていません Port3: 接続されていません Port4: 接続されていません	0%	0%

The 'WAN Information' section shows a table with one entry:

接続名	接続状態	情報
WAN1: クラウド接続 (GigaEthernet0.1)	接続	IPアドレス: 203.0.113.1

The 'VPN Information' section shows a table with one entry:

接続名	接続状態	通信量[packets]
Cloud-AWS-VPN	接続	送信: 0, 受信: 0

Red boxes highlight the '更新' (Refresh) buttons for the Network, WAN, and VPN information tables.

(10) VPN情報は、接続名にマウスカーソルを近づけることで、詳細情報を確認することができます。また、接続名をわかりやすいように変更することができます。



This is a close-up of the VPN information table from the previous screenshot. A red box highlights the 'Cloud-AWS-VPN' entry, which is expanded to show details:

接続名	接続状態	通信量[packets]
Cloud-AWS-VPN IPsec(IKEv1) IPアドレス: 192.0.2.1	接続	送信: 0, 受信: 0

A red box highlights the '接続名編集' (Edit Connection Name) button at the bottom right of the table.

3. かんたん設定

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず『[設定の保存](#)』を行ってください。

VPN情報 接続名の編集

接続名	接続状態	IPアドレス/送信量[packets]
接続インターフェース: Tunnel127.0 description: Cloud-AWS-VPN	接続 IPsec(IKEv1)	IPアドレス: 192.0.2.1 送信: 0 受信: 0

[反映](#) [戻る](#)

番号	項目	内容
①	接続名	接続名を設定します。 ・ 半角英数字 1~128 文字まで、または全角文字で 1~32 文字まで入力できます。

(11) [保存実行]ボタンをクリックします。

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず『[設定の保存](#)』を行ってください。

設定の保存

設定を保存します。

よろしければ [保存実行] を押してください。

[保存実行](#)

(12) 「設定を保存しました。」のメッセージを確認します。

設定の保存

設定を保存しました。

[トップページへ](#)

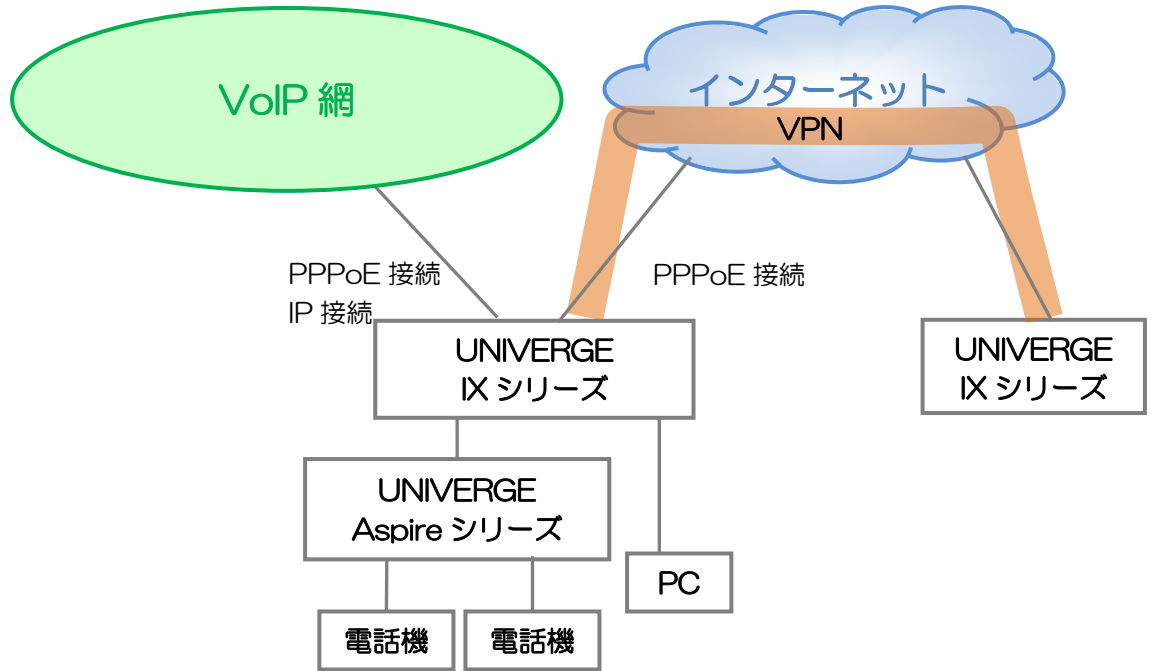
3. かんたん設定

3.8 IP 電話サービス接続

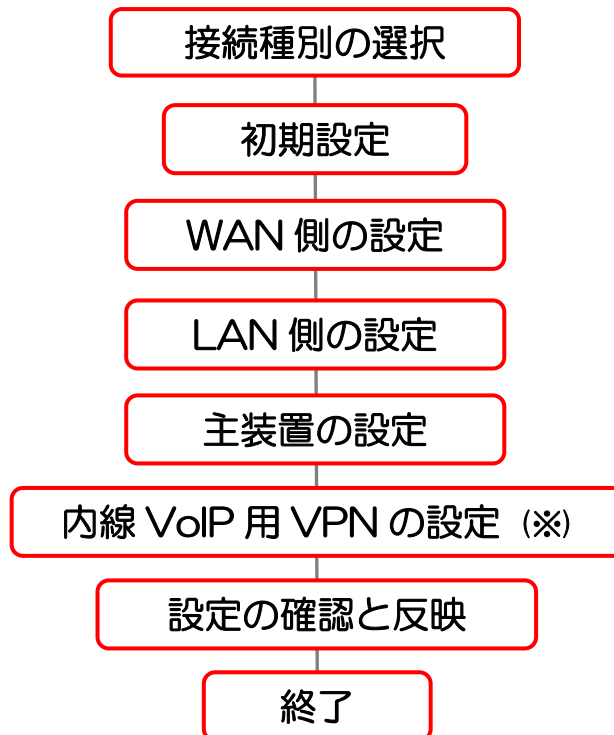
UNIVERGE Aspire シリーズと連携した IP 電話ネットワークの設定を行います。

メモ 本 Web 設定機能に対応する UNIVERGE Aspire シリーズおよび設定内容の詳細については、UNIVERGE Aspire シリーズの販売店にご相談ください。

【構成イメージ】



【設定手順】



(※) KDDI 光ダイレクト(複数固定 IP アドレス契約)、ひかり電話オフィス A(エース)のみ設定可能

3. かんたん設定

(1) ログイン後のメニューエリアから[かんたん設定]をクリックします。

メモ トップページリンクをクリックすることで、接続種別の各ページに移動することも可能です。

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず『設定の保存』を行ってください。

■メニュー
 [トップページ](#)
 [設定の保存](#)
 [ログアウト](#)
■かんたん設定
 かんたん設定
■詳細設定
 [詳細設定](#)
■端末管理
 [端末管理](#)
■保守管理
 [装置状態の表示](#)
 [装置ログの取得](#)
 [設定データの管理](#)
 [設定の初期化](#)
 [ソフトウェアの更新](#)
 [pingの実行](#)
 [任意コマンドの実行](#)
 [IP電話サービス保守](#)
 [URLオフロード](#)
 [リンクマネージャ](#)
 [Wake on LAN](#)
 [再起動](#)
■拡張ページ
 [拡張ページ](#)
■外部リンク
 [製品ページ](#)

かんたん設定
ルータの設定を開始します。以下のリンクから選択してください。

- パスワードを登録・変更する前にユーザ名とパスワードを入力する画面が表示された場合は、そのまま「OK」をクリックしてください。

かんたん設定

- [インターネット接続](#)
フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用して、インターネットに接続する設定を行います。
- [インターネット接続+VPN接続](#)
フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用したインターネット接続と、インターネットVPNによる拠点間通信の設定を行います。
- [インターネット接続+フレッツ・VPNワイド接続](#)
フレッツ光を使用したインターネット接続と、フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
- [フレッツ・VPNワイド接続](#)
フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。
- [NGN網VPN接続](#)
NGN網を用いたVPNによる拠点間の通信の設定と、NetMeisterによる装置管理の設定を行います。
- [IPv6 IPoE接続](#)
IPv6 IPoE接続の設定を行います。
プロバイダの動的IPまたは固定IPでのサービスを設定します。
- [クラウド接続](#)
インターネットVPNや専用線を使用したクラウド接続の設定を行います。
- [IP電話サービス接続](#)
対応するUNIVERGE Aspireシリーズと連携したIP電話ネットワークの設定を行います。


詳細設定
インタフェースやサーバのアドレスを指定したり、フィルタやQoS、VPN等、かんたん設定に含まれない詳細な設定を行う場合はこちらから設定してください。

端末管理
本装置に接続されている端末を管理します。
リンクマネージャ機能やWeb認証機能を設定します。

保守管理
装置状態の確認、ソフトウェアの更新、pingの実行など、各種保守機能の操作を行います。
URLオフロード機能による特定宛先のレーティング制御、リンクマネージャ機能による端末の保守管理などが可能です。
任意のコマンドを直接実行したい場合は[任意コマンドの実行](#)から操作してください。

3. かんたん設定

(2) 接続種別の選択で「IP 電話サービス接続」にチェックを入れ、[次へ]ボタンをクリックします。

 接続種別を変更する場合には、設定の初期化が必要となります。

かんたん設定：接続種別の選択

接続種別を選択してかんたん設定を開始してください。
接続種別を変更する場合には「設定の初期化」が必要となります。

	現在の設定	設定の変更
接続種別の選択	インターネット接続なし	<ul style="list-style-type: none"><input type="radio"/> インターネット接続 フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用して、インターネットに接続する設定を行います。<input type="radio"/> インターネット接続 + VPN接続 フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用したインターネット接続と、インターネットVPNによる拠点間通信の設定を行います。<input type="radio"/> インターネット接続 + フレッツ・VPNワイド接続 フレッツ光を使用したインターネット接続と、フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。<input type="radio"/> フレッツ・VPNワイド接続 フレッツ・VPNワイド(端末型払い出し)を使用した拠点間通信の設定を行います。<input type="radio"/> NGN網VPN接続 NGN網を用いたVPNによる拠点間の通信の設定とNetMeisterによる装置管理の設定を行います。<input type="radio"/> IPv6 IPoE接続 IPv6 IPoE接続の設定を行います。 プロバイダの動的IPまたは固定IPでのサービスを設定します。<input type="radio"/> クラウド接続 インターネットVPNや専用線を使用したクラウド接続の設定を行います。<input checked="" type="radio"/> IP電話サービス接続 対応するUNIVERGE Aspireシリーズと連携したIP電話ネットワークの設定を行います。



3. かんたん設定

(3) [初期設定]の各項目を設定し、[次へ]ボタンをクリックします。管理者パスワードを変更する場合は、[パスワードを変更する]を選択し、[パスワードの設定]の各項目を設定した後、[次へ]ボタンをクリックします。

管理者パスワードを変更する必要が無い場合は、そのまま[次へ]ボタンをクリックします。

接続種別の選択に戻る場合は、[戻る]ボタンをクリックしてください。

IP電話サービス接続：初期設定

IP電話サービス接続の設定を開始します。

パスワードの設定

ログイン認証用のパスワードを設定します。

	現在の設定	設定の変更
ユーザ名	admin	変更できません
パスワード	*****	<input checked="" type="radio"/> パスワードを変更しない <input type="radio"/> パスワードを変更する

回線の選択

契約内容にあわせて選択してください。
回線種別などを変更する場合には「設定の初期化」が必要となります。

	現在の設定	設定の変更
回線種別	回線設定なし	<input checked="" type="radio"/> KDDI光ダイレクト <input type="radio"/> auひかりビジネス <input type="radio"/> FTフォン（0ABJ番号） <input type="radio"/> スマートひかり <input type="radio"/> KDDI-IPフォン <input type="radio"/> OCN.Phone Office <input type="radio"/> .Phone Direct（OCN回線） <input type="radio"/> Arcstar IP Voice（OCN接続） <input type="radio"/> FTフォン（050番号） <input type="radio"/> Fusion IP-Phone <input type="radio"/> Skype Connect <input type="radio"/> ホワイトオフィス <input type="radio"/> ひかり電話オフィスA（エース） <input type="radio"/> おとく光電話
アドレス契約種別		<input checked="" type="radio"/> 固定IPアドレス契約 <input type="radio"/> 複数固定IPアドレス契約 （インターネットオプション契約含む）
インターネット通信		<input checked="" type="radio"/> 別回線でインターネットを利用しない

3. かんたん設定

番号	項目	内容
①	ユーザ名	本装置にログインするときのユーザ名を入力します。 <ul style="list-style-type: none">初期状態ではユーザ名は設定されていません。パスワード設定後のユーザ名は「admin」です。Web 設定からは変更できません。
②	パスワード	本装置にログインするときのパスワードを入力します。 <ul style="list-style-type: none">初期状態ではパスワードは設定されていません。半角英数字 1~249 文字で入力します。 注意 <ul style="list-style-type: none">大文字/小文字は区別されます。パスワードの入力文字は表示されません。●●●のように伏せ文字で表示されます。パスワードは、第三者に推測されにくく、忘れないような文字列を入力してください。
③	回線種別	契約内容にあわせて選択します。 注意 <ul style="list-style-type: none">回線種別などを変更する場合には、設定の初期化が必要となります。
④	アドレス契約種別	アドレス契約種別を選択します。
⑤	インターネット通信	別回線でインターネット通信を「利用する」/「利用しない」を選択します。 <ul style="list-style-type: none">アドレス契約種別で「複数固定 IP アドレス契約」を選択した場合、「別回線でインターネットを利用する」は表示されません。
⑥	内線 VoIP 用 VPN	内線 VoIP 用 VPN を「利用する」/「利用しない」を選択します。 <ul style="list-style-type: none">回線種別で「KDDI 光ダイレクト(複数固定 IP アドレス契約)」「ひかり電話オフィス A(エース)」以外を選択した場合、「内線 VoIP 用 VPN」は表示されません。

3. かんたん設定

(4) [WAN 側の設定]の各項目を設定し、[次へ]ボタンをクリックします。

メモ 初期設定に戻る場合は、[戻る]ボタンをクリックしてください。

KDDI 光ダイレクトの場合

1. WAN側の設定 → 2. LAN側の設定 → 3. 主装置の設定 → 4. 設定の確認と反映 → 5. 終了

IP電話サービス接続 : WAN側の設定

音声通信用のWAN側インタフェースを設定します。

WAN1: 音声通信用WAN側インタフェースの設定(GigaEthernet0.0)

	現在の設定	設定の変更
WAN側IPアドレス		WAN側インタフェースのIPアドレスを設定してください。 [] / [30] ▾ IPアドレスを入力してください。
デフォルトゲートウェイ		デフォルトゲートウェイを設定してください。局内アドレスなどで記載されている場合があります。 [] IPアドレスを入力してください。
DNSアドレス		DNSを固定設定しない場合は空欄にしてください。 [] (プライマリ) [] (セカンダリ)
回線速度	auto	契約内容により、回線速度の調整が必要になる場合があります。回線終端装置側と速度設定は合わせてください。 <input checked="" type="radio"/> auto <input type="radio"/> 1Gbps固定 <input type="radio"/> 100Mbps固定 <input type="radio"/> 10Mbps固定

戻る 次へ

番号	項目	内容
①	WAN 側 IP アドレス	WAN 側 IP アドレスを設定します。
②	デフォルトゲートウェイ	デフォルトゲートウェイを設定します。
③	DNS アドレス	DNS アドレスを設定します。 DNS を固定設定しない場合は空欄にしてください。
④	回線速度	契約内容により、回線速度の調整が必要になる場合があります。 回線終端装置側と速度設定は合わせてください。

3. かんたん設定

au ひかりビジネス、FT フォン (OABJ 番号)、スマートひかりの場合

1. WAN側の設定 → 2. LAN側の設定 → 3. 主装置の設定 → 4. 設定の確認と反映 → 5. 終了

IP電話サービス接続：WAN側の設定

音声通信用のWAN側インタフェースを設定します。

WAN1: 音声通信用WAN側インタフェースの設定(GigaEthernet0.0)

	現在の設定	設定の変更
WAN側IPアドレス		WAN側インタフェースのIPアドレスを設定してください。 <input type="text"/> / <input type="text" value="30"/> <input type="button" value="▼"/> IPアドレスを入力してください。
デフォルトゲートウェイ		デフォルトゲートウェイを設定してください。局内アドレスなどで記載されている場合があります。 <input type="text"/> IPアドレスを入力してください。
DNSアドレス		DNSを固定設定しない場合は空欄にしてください。 <input type="text"/> (プライマリ) <input type="text"/> (セカンダリ)

番号	項目	内容
①	WAN 側 IP アドレス	WAN 側 IP アドレスを設定します。
②	デフォルトゲートウェイ	デフォルトゲートウェイを設定します。
③	DNS アドレス	DNS アドレスを設定します。 DNS を固定設定しない場合は空欄にしてください。

3. かんたん設定

ひかり電話オフィス A (エース) の場合

1. WAN側の設定 → 2. LAN側の設定 → 3. 主装置の設定 → 4. 設定の確認と反映 → 5. 終了

IP電話サービス接続：WAN側の設定

音声通信用のWAN側インタフェースを設定します。

WAN1: 音声通信用WAN側インタフェースの設定(GigaEthernet0.0)

	現在の設定	設定の変更
WAN側IPアドレス		自動取得
デフォルトゲートウェイ	-	自動設定
DNSアドレス		自動取得
PPPoEブリッジ	ブリッジしない	インターネット接続用のルータがある場合はブリッジするを選択してください。 <input type="radio"/> PPPoEをブリッジする <input checked="" type="radio"/> PPPoEをブリッジしない

リモートメンテナンスの設定

	現在の設定	設定の変更
リモートメンテナンス	許可しない	<input type="radio"/> リモートメンテナンス接続を許可しない <input checked="" type="radio"/> リモートメンテナンス接続を許可する
接続元ネットワークアドレス		接続元のLAN側のネットワークアドレスを入力してください。 <input type="text"/> / 16 IPアドレスを入力してください。
VPN接続用パスワード		接続元と共通のパスワードを設定してください。 <input type="text"/>
アクセス制限		<input checked="" type="radio"/> ルータ/Aspireのみアクセス可 <input type="radio"/> 同一ネットワークのみアクセス可 <input type="radio"/> 全ネットワークにアクセス可

戻る 次へ

番号	項目	内容
①	WAN 側 IP アドレス	WAN 側 IP アドレスを自動取得します。
②	デフォルトゲートウェイ	デフォルトゲートウェイが自動設定されます。
③	DNS アドレス	DNS アドレスを自動取得します。
④	PPPoE ブリッジ	インターネット接続用のルータがある場合は「ブリッジする」を選択してください。
⑤	リモートメンテナンス	本書の「6.8 IP 電話サービス保守」にあります、リモートメンテナンス接続の受信を許可する場合はリモートメンテナンス接続を許可する選択してください。
⑥	接続元ネットワークアドレス	接続元の LAN 側のネットワークアドレスを入力します。 ・ リモートメンテナンスで「リモートメンテナンス接続を許可しない」を選択した場合は表示されません。
⑦	VPN 接続用パスワード	接続先と共通のパスワードを設定します。 ・ リモートメンテナンスで「リモートメンテナンス接続を許可しない」を選択した場合は表示されません。
⑧	アクセス制限	アクセスの許可範囲を選択します。 ・ リモートメンテナンスで「リモートメンテナンス接続を許可しない」を選択した場合は表示されません。

3. かんたん設定

KDDI-IP フォン、 OCN,Phone Office、 .Phone Direct (OCN 回線)
Arcstar IP Voice (OCN 接続)、 FT フォン (050 番号)
Fusion IP-Phone、 Skype Connect、 ホワイトオフィス の場合

1. WAN側の設定 → 2. LAN側の設定 → 3. 主装置の設定 → 4. 設定の確認と反映 → 5. 終了

IP電話サービス接続：WAN側の設定

音声通信用とデータ通信用のWAN側インタフェースを設定します。

WAN1: 音声通信用WAN側インタフェースの設定(GigaEthernet0.0)

	現在の設定	設定の変更
ユーザ名		音声通信用のPPPoE接続で使用するユーザ名を設定してください。 <input type="text"/> 文字列(半角英数字)を入力してください。
パスワード		音声通信用のPPPoE接続で使用するパスワードを設定してください。 <input type="text"/> 文字列(半角英数字)を入力してください。
WAN側IPアドレス		自動取得
デフォルトゲートウェイ	-	自動設定
DNSアドレス		DNSを手動設定しない場合は空欄にしてください。 <input type="text"/> (プライマリ) <input type="text"/> (セカンダリ)

WAN2: データ通信用WAN側インタフェースの設定()

	現在の設定	設定の変更
ユーザ名		データ通信用のPPPoE接続で使用するユーザ名を設定してください。 <input type="text"/> 文字列(半角英数字)を入力してください。
パスワード		データ通信用のPPPoE接続で使用するパスワードを設定してください。 <input type="text"/> 文字列(半角英数字)を入力してください。
WAN側IPアドレス		自動取得
デフォルトゲートウェイ	-	自動設定
DNSアドレス	-	自動取得

[戻る](#) [次へ](#)

3. かんたん設定

番号	項目	内容
①	ユーザ名	音声通信用の PPPoE 接続で使用するユーザ名を設定します。 ・ 半角英数字で 1～59 文字まで入力できます。
②	パスワード	音声通信用の PPPoE 接続で使用するパスワードを設定します。 ・ 半角英数字で 1～79 文字まで入力できます。 注意 ・ 大文字、小文字も区別されます。
③	WAN 側 IP アドレス	音声通信用の WAN 側 IP アドレスを自動取得します。
④	デフォルトゲートウェイ	音声通信用のデフォルトゲートウェイが自動設定されます。
⑤	DNS アドレス	音声通信用の DNS アドレスを設定します。 ・ アドレス契約種別で「動的 IP アドレス契約」を選択した場合、DNS アドレスを自動取得します。
⑥	ユーザ名	データ通信用の PPPoE 接続で使用するユーザ名を設定します。 ・ 半角英数字で 1～59 文字まで入力できます。 ・ インターネット通信で「別回線でインターネットを利用しない」を選択した場合、表示されません。
⑦	パスワード	データ通信用の PPPoE 接続で使用するパスワードを設定します。 ・ 半角英数字で 1～79 文字まで入力できます。 ・ インターネット通信で「別回線でインターネットを利用しない」を選択した場合、表示されません。 注意 ・ 大文字、小文字も区別されます。
⑧	WAN 側 IP アドレス	データ通信用の WAN 側 IP アドレスを自動取得します。 ・ インターネット通信で「別回線でインターネットを利用しない」を選択した場合、表示されません。
⑨	デフォルトゲートウェイ	データ通信用のデフォルトゲートウェイが自動設定されます。 ・ インターネット通信で「別回線でインターネットを利用しない」を選択した場合、表示されません。
⑩	DNS アドレス	データ通信用の DNS アドレスを自動取得します。 ・ インターネット通信で「別回線でインターネットを利用しない」を選択した場合、表示されません。

3. かんたん設定

おとく光電話の場合

1. WAN側の設定 → 2. LAN側の設定 → 3. 主装置の設定 → 4. 設定の確認と反映 → 5. 終了

IP電話サービス接続：WAN側の設定

音声通信用のWAN側インタフェースを設定します。

WAN1: 音声通信用WAN側インタフェースの設定(GigaEthernet0.0)

	現在の設定	設定の変更
WAN側IPアドレス		WAN側インタフェースのIPアドレスを設定してください。 [] / 30 IPアドレスを入力してください。
デフォルトゲートウェイ		デフォルトゲートウェイを設定してください。局内アドレスなどで記載されている場合があります。 [] IPアドレスを入力してください。
回線速度	auto	契約内容により、回線速度の調整が必要になる場合があります。 回線終端装置側と速度設定は合わせてください。 <input checked="" type="radio"/> auto <input type="radio"/> 100Mbps固定 <input type="radio"/> 10Mbps固定

[戻る](#) [次へ](#)

番号	項目	内容
①	WAN 側 IP アドレス	WAN 側 IP アドレスを設定します。
②	デフォルトゲートウェイ	デフォルトゲートウェイを設定します。
③	回線速度	契約内容により、回線速度の調整が必要になる場合があります。 回線終端装置側と速度設定は合わせてください。

3. かんたん設定

(5) [LAN 側の設定]の各項目を設定し、[次へ]ボタンをクリックします。

メモ WAN 側の設定に戻る場合は、[戻る]ボタンをクリックしてください。

別回線でインターネットを利用しない場合

1. WAN側の設定 → 2. LAN側の設定 → 3. 主装置の設定 → 4. 内線VoIP用VPNの設定 →
5. 設定の確認と反映 → 6. 終了

IP電話サービス接続：LAN側の設定

主装置を接続するLAN側インタフェースを設定します。

LAN1: LAN側インタフェースの設定(GigaEthernet1.0)

	現在の設定	設定の変更
LAN側IPアドレス	192.168.1.254/24	主装置と接続するためのLAN側IPアドレスを設定してください。 192.168.1.254 / 24

戻る 次へ

番号	項目	内容
①	LAN 側 IP アドレス	主装置と接続するための LAN 側 IP アドレスを設定します。

3. かんたん設定

別回線でインターネットを利用する場合

1. WAN側の設定 → 2. LAN側の設定 → 3. 主装置の設定 → 4. 設定の確認と反映 → 5. 終了

IP電話サービス接続：LAN側の設定

主装置やデータ通信端末を接続するLAN側インタフェースを設定します。

LAN側デバイスの設定(GigaEthernet1)

SWHUBのポート番号ごとに利用する回線を選択してください。
主装置と接続しているPortは、データ通信用に変更しないでください。

	現在の設定	設定の変更
LAN側ポートの設定		Port 1 <input checked="" type="radio"/> 音声通信 <input type="radio"/> データ通信 Port 2 <input checked="" type="radio"/> 音声通信 <input type="radio"/> データ通信 Port 3 <input checked="" type="radio"/> 音声通信 <input type="radio"/> データ通信 Port 4 <input checked="" type="radio"/> 音声通信 <input type="radio"/> データ通信
LAN1: 音声通信用LAN側インタフェースの設定(GigaEthernet1.0)		
主装置を接続するLAN側インタフェースの設定です。 LAN側IPアドレス(音声)を変更する場合は、反映後に新しいIPアドレスで接続しなおす必要があります。		
	現在の設定	設定の変更
LAN側IPアドレス (音声)	192.168.1.254/24	主装置と接続するためのLAN側IPアドレスを設定してください。 192.168.1.254 / 24
LAN2: データ通信用LAN側インタフェースの設定()		
インターネット通信を行う端末を接続するLAN側インタフェースの設定です。		
	現在の設定	設定の変更
LAN側IPアドレス (インターネット通信)		インターネット通信を行うためのLAN側IPアドレスを設定してください。 / 24 IPアドレスを入力してください。
DHCPサーバ		<input checked="" type="radio"/> 有効 <input type="radio"/> 無効

戻る 次へ

番号	項目	内容
①	LAN 側ポートの設定	SWHUB のポート番号ごとに利用する回線を選択します。
②	LAN 側 IP アドレス (音声)	主装置を接続する LAN 側インタフェースの設定をします。 主装置と接続するための LAN 側 IP アドレスを設定してください。
③	LAN 側 IP アドレス (インターネット通信)	インターネット通信を行う端末を接続する LAN 側インタフェースの設定をします。 インターネット通信を行うための LAN 側 IP アドレスを設定してください。
④	DHCP サーバ	インターネット通信を行う端末を接続する LAN 側インタフェースの設定をします。 DHCP サーバ機能の「有効」 / 「無効」を設定します。

3. かんたん設定

(6) [主装置の設定]の各項目を設定し、[設定の確認]ボタンをクリックします。

メモ LAN 側の設定に戻る場合は、[戻る]ボタンをクリックしてください。

別回線でインターネットを利用しない場合

1. WAN側の設定 → 2. LAN側の設定 → 3. **主装置の設定** → 4. 設定の確認と反映 → 5. 終了

IP電話サービス接続：主装置の設定

主装置の設定を参照して設定してください。

	現在の設定	設定の変更
VOIPDB設定		VOIPDBが利用するIPアドレス（PRG10-12-09）とポート番号（PRG84-14-06）を入力してください。 172.16.0.10 : 5060
VOIPGW設定		VOIPGWが利用するIPアドレス（PRG84-26-01）とポート番号（PRG84-26-02）を入力してください。 172.16.0.20 : 10020 ~

番号	項目	内容
①	VOIPDB 設定	VOIPDB が利用する IP アドレス (PRG10-12-09) とポート番号 (PRG84-14-06) を入力します。
②	VOIPGW 設定	VOIPGW が利用する IP アドレス (PRG84-26-01) とポート番号 (PRG84-26-02) を入力します。

3. かんたん設定

別回線でインターネットを利用する場合

1. WAN側の設定 → 2. LAN側の設定 → 3. **主装置の設定** → 4. 設定の確認と反映 → 5. 終了

IP電話サービス接続：主装置の設定

主装置の設定を参照して設定してください。

	現在の設定	設定の変更
VOIPDB設定		VOIPDBが利用するIPアドレス（PRG10-12-09）とポート番号（PRG84-14-06）を入力してください。 172.16.0.10 : 5060
VOIPGW設定		VOIPGWが利用するIPアドレス（PRG84-26-01）とポート番号（PRG84-26-02）を入力してください。 172.16.0.20 : 10020 ~
IP電話機のNAT接続設定		IP電話機（IP多機能電話機、SIP内線端末）をNAT接続する場合のみ選択して値を設定してください。 <input checked="" type="radio"/> NAT接続しない <input type="radio"/> NAT接続する

番号	項目	内容
①	VOIPDB 設定	VOIPDB が利用する IP アドレス (PRG10-12-09) とポート番号 (PRG84-14-06) を入力します。
②	VOIPGW 設定	VOIPGW が利用する IP アドレス (PRG84-26-01) とポート番号 (PRG84-26-02) を入力します。
③	IP 電話機の NAT 接続設定	IP 電話機 (IP 多機能電話機、SIP 内線端末) を NAT 接続する場合のみ選択して値を設定します。

3. かんたん設定

(7) 内線 VoIP 用 VPN を利用する場合は、[内線 VoIP 用 VPN の設定]の各項目を設定し、[設定の確認]ボタンをクリックします。

メモ 主装置の設定に戻る場合は、[戻る]ボタンをクリックしてください。

メモ 回線種別で「KDDI 光ダイレクト(複数固定 IP アドレス契約)」「ひかり電話オフィス A(エース)」以外を選択した場合、表示されません。

センタの場合

1. WAN側の設定 → 2. LAN側の設定 → 3. 主装置の設定 → 4. **内線VoIP用VPNの設定** → 5. 設定の確認と反映 → 6. 終了

IP電話サービス接続：内線VoIP用VPNの設定

内線VoIP用のWAN側インタフェースとVPNを設定します。

	現在の設定	設定の変更
接続種別		<input checked="" type="radio"/> ダイナミックVPN

WAN2: 内線VoIP用WAN側インタフェースの設定(GigaEthernet0.1)

	現在の設定	設定の変更
ユーザ名		PPPoE接続で使用するユーザ名を設定してください。 <input type="text"/> 文字列(半角英数字)を入力してください。
パスワード		PPPoE接続で使用するパスワードを設定してください。 <input type="text"/> 文字列(半角英数字)を入力してください。
内線VoIP用WAN側IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定

ダイナミックVPNの設定

	現在の設定	設定の変更
タイプ		<input type="radio"/> 拠点 <input checked="" type="radio"/> センタ
拠点間通信		<input checked="" type="radio"/> 拠点間通信を行う <input type="radio"/> 拠点間通信を行わない
パスワード		すべての拠点で共通のパスワードを設定してください。 <input type="text"/> 文字列(半角英数字)を入力してください。

番号	項目	内容
①	ユーザ名	内線 VoIP 用の PPPoE 接続で使用するユーザ名を設定します。 ・ 半角英数字で 1～59 文字まで入力できます。
②	パスワード	内線 VoIP 用の PPPoE 接続で使用するパスワードを設定します。 ・ 半角英数字で 1～79 文字まで入力できます。 注意 ・ 大文字、小文字も区別されます。
③	内線 VoIP 用 WAN 側 IP アドレス	WAN 側インタフェースの IP アドレスを設定します。
④	タイプ	「センタ」を選択します。
⑤	拠点間通信	拠点間通信を「行う」/「行わない」を選択します。
⑥	パスワード	VPN 接続で使用するパスワード(事前共有鍵)です。 拠点に設定したパスワードと同じパスワードを設定してください。 ・ 半角英数字で 1～128 文字まで入力できます。

3. かんたん設定

拠点の場合

1. WAN側の設定 → 2. LAN側の設定 → 3. 主装置の設定 → 4. 内線VoIP用VPNの設定 →
5. 設定の確認と反映 → 6. 終了

IP電話サービス接続：内線VoIP用VPNの設定

内線VoIP用のWAN側インタフェースとVPNを設定します。

	現在の設定	設定の変更
接続種別		<input checked="" type="radio"/> ダイナミックVPN

WAN2：内線VoIP用WAN側インタフェースの設定(GigaEthernet0.0)

	現在の設定	設定の変更
ユーザ名		PPPoE接続で使用するユーザ名を設定してください。 文字列(半角英数字)を入力してください。
パスワード		PPPoE接続で使用するパスワードを設定してください。 文字列(半角英数字)を入力してください。
内線VoIP用WAN側IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定

ダイナミックVPNの設定

	現在の設定	設定の変更
タイプ		<input checked="" type="radio"/> 拠点 <input type="radio"/> センタ
拠点番号		他の拠点と同じ番号は設定しないでください。 1
パスワード		すべての拠点で共通のパスワードを設定してください。 文字列(半角英数字)を入力してください。
センタWAN側IPアドレス		センタ装置のWANに設定されているIPアドレスまたはドメイン名を入力してください。 入力形式が不正です。

戻る

設定の確認

3. かんたん設定

番号	項目	内容
①	ユーザ名	内線 VoIP 用の PPPoE 接続で使用するユーザ名を設定します。 ・ 半角英数字で 1～59 文字まで入力できます。
②	パスワード	内線 VoIP 用の PPPoE 接続で使用するパスワードを設定します。 ・ 半角英数字で 1～79 文字まで入力できます。 注意 ・ 大文字、小文字も区別されます。
③	内線 VoIP 用 WAN 側 IP アドレス	WAN 側インタフェースの IP アドレスを設定します。
④	タイプ	「拠点」を選択します。
⑤	拠点番号	拠点の識別番号です。 他の拠点と重複しない任意の番号(1～64)を設定します。
⑥	パスワード	VPN 接続で使用するパスワード(事前共有鍵)です。 すべての拠点で同じ任意のパスワードを設定してください。 ・ 半角英数字で 1～128 文字まで入力できます。
⑦	センタ WAN 側 IP アドレス	センタ装置の WAN に設定されている IP アドレスまたはドメイン名を入力します。

3. かんたん設定

(8) 入力した項目が正しいことを確認し、[反映]ボタンをクリックします。

主装置の設定、あるいは内線 VoIP 用 VPN の設定に戻る場合は、[戻る]ボタンをクリックしてください。

下記は KDDI 光ダイレクトの場合の例です。

1. WAN側の設定 → 2. LAN側の設定 → 3. 主装置の設定 → 4. **設定の確認と反映** → 5. 終了

IP電話サービス接続：設定の確認と反映

設定内容を変更する場合は [反映] を押してください。
LAN側IPアドレスを変更する場合は、新しいIPアドレスで接続しなおしてください。

初期設定

	現在の設定	設定の変更
回線種別	回線設定なし	<input checked="" type="radio"/> KDDI光ダイレクト

WAN1: 音声通信用WAN側インタフェースの設定(GigaEthernet0.0)

	現在の設定	設定の変更
WAN側IPアドレス		<input type="text" value="192.0.2.1"/> / <input type="text" value="30"/> ▼
デフォルトゲートウェイ		<input type="text" value="19.0.2.2"/>
DNSアドレス		<input type="text"/> (プライマリ) <input type="text"/> (セカンダリ)
回線速度	auto	<input checked="" type="radio"/> auto

LAN1: LAN側インタフェースの設定(GigaEthernet1.0)


	現在の設定	設定の変更
LAN側IPアドレス	192.168.1.254/24	<input type="text" value="192.168.1.254"/> / <input type="text" value="24"/> ▼

主装置の設定

	現在の設定	設定の変更
VOIPDB設定		<input type="text" value="172.16.0.10"/> : <input type="text" value="5060"/>
VOIPGW設定		<input type="text" value="172.16.0.20"/> : <input type="text" value="10020"/> ~

3. かんたん設定

- (9) 「設定内容を変更しました。」のメッセージが表示されることを確認し、[トップページへ]ボタンを押します。

 下記は KDDI 光ダイレクトの場合の例です。

1. WAN側の設定 → 2. LAN側の設定 → 3. 主装置の設定 → 4. 設定の確認と反映 → 5. **終了**

IP電話サービス接続：終了

設定内容を変更しました。

初期設定

	現在の設定	設定の変更
回線種別	回線設定済み	<input checked="" type="radio"/> KDDI光ダイレクト

WAN1: 音声通信用WAN側インタフェースの設定(GigaEthernet0.0)

	現在の設定	設定の変更
WAN側IPアドレス	192.0.2.1/30	<input type="text" value="192.0.2.1"/> / <input type="text" value="30"/> ▼
デフォルトゲートウェイ	19.0.2.2	<input type="text" value="19.0.2.2"/>
DNSアドレス		<input type="text"/> (プライマリ) <input type="text"/> (セカンダリ)
回線速度	auto	<input checked="" type="radio"/> auto

LAN1: LAN側インタフェースの設定(GigaEthernet1.0)

	現在の設定	設定の変更
LAN側IPアドレス	192.168.1.254/24	<input type="text" value="192.168.1.254"/> / <input type="text" value="24"/> ▼


主装置の設定

	現在の設定	設定の変更
VOIPDB設定	172.16.0.10 5060	<input type="text" value="172.16.0.10"/> : <input type="text" value="5060"/>
VOIPGW設定	172.16.0.20 10020	<input type="text" value="172.16.0.20"/> : <input type="text" value="10020"/> ~

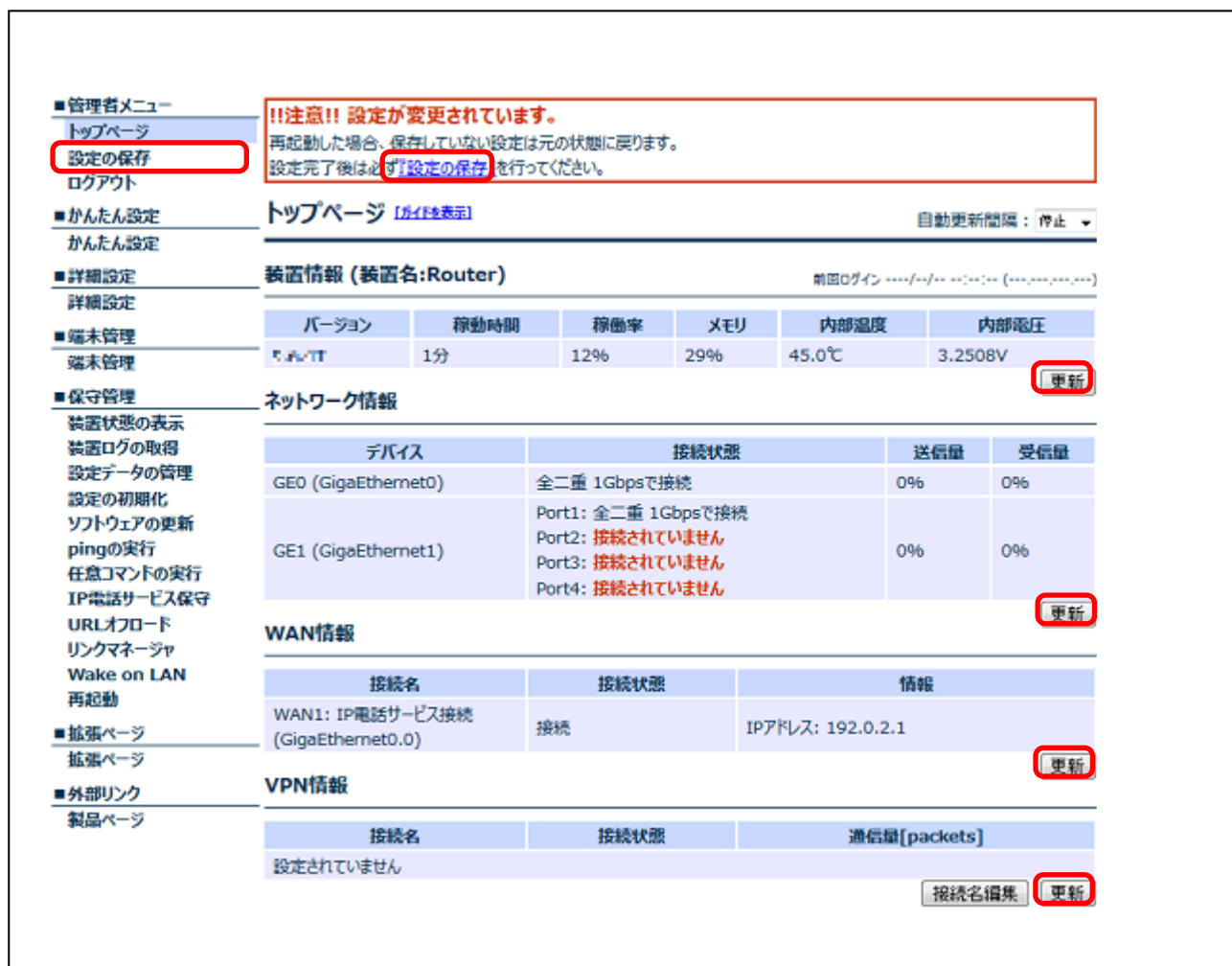
トップページへ

3. かんたん設定

(10) トップページでWAN情報の接続状態を確認します。

 [更新]ボタンをクリックすると、情報を更新することが可能です。

(11) メニューエリア、または、メッセージエリアから[設定の保存]をクリックします。



!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず**設定の保存**を行ってください。

管理メニュー
■ 管理者メニュー
 トップページ
 設定の保存
 ログアウト
■ かんたん設定
 かんたん設定
■ 詳細設定
 詳細設定
■ 端末管理
 端末管理
■ 保守管理
 装置状態の表示
 装置ログの取得
 設定データの管理
 設定の初期化
 ソフトウェアの更新
 pingの実行
 任意コマンドの実行
 IP電話サービス保守
 URLオフロード
 リンクマネージャ
 Wake on LAN
 再起動
■ 拡張ページ
 拡張ページ
■ 外部リンク
 製品ページ

トップページ [\[アイコン表示\]](#) 自動更新間隔: 停止

装置情報 (装置名:Router) 前回ログイン: ----/--/-- --:--:-- (---:---:---:---)

バージョン	稼働時間	稼働率	メモリ	内部温度	内部電圧
5.4.0.11	1分	12%	29%	45.0℃	3.2508V

更新

ネットワーク情報

デバイス	接続状態	送信量	受信量
GE0 (GigaEthernet0)	全二重 1Gbpsで接続	0%	0%
GE1 (GigaEthernet1)	Port1: 全二重 1Gbpsで接続 Port2: 接続されていません Port3: 接続されていません Port4: 接続されていません	0%	0%

更新

WAN情報

接続名	接続状態	情報
WAN1: IP電話サービス接続 (GigaEthernet0.0)	接続	IPアドレス: 192.0.2.1

更新

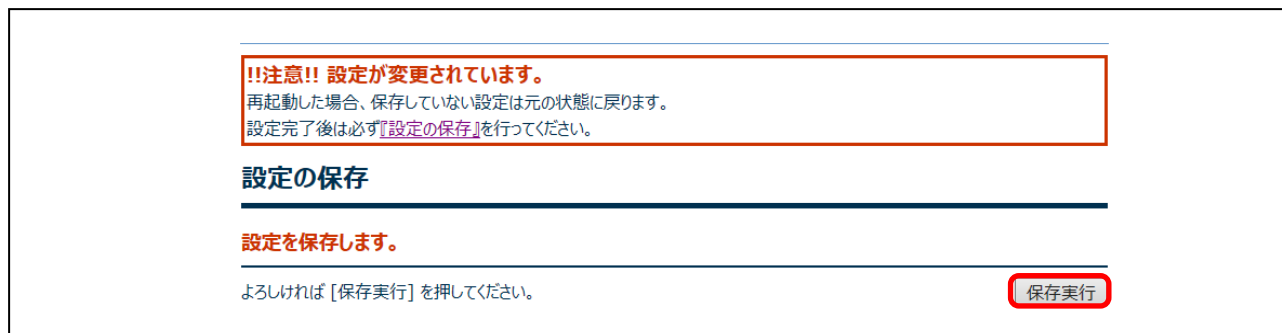
VPN情報

接続名	接続状態	通信量[packets]
設定されていません		

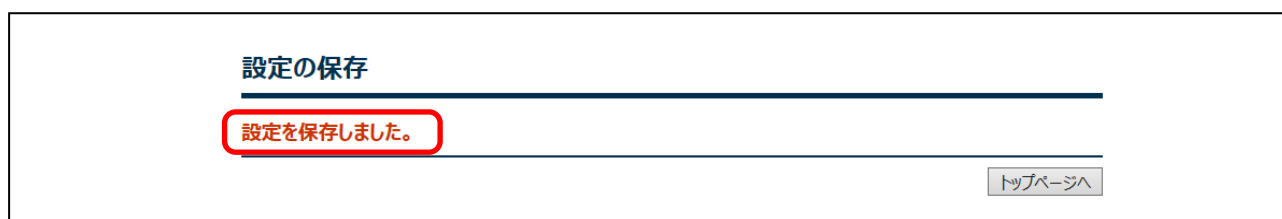
接続名編集 **更新**

3. かんたん設定

(12) [保存実行]ボタンをクリックします。



(13) 「設定を保存しました。」のメッセージを確認します。



4. 詳細設定

4 詳細設定

本章では、かんたん設定で設定した内容の変更および詳細な設定を追加できる『詳細設定』について説明します。詳細設定では、以下の操作を行うことができます。

4.1 基本設定

パスワードの設定 設定を変更したときは、設定の保存を実行してください。

- パスワードの設定
- 装置名の設定
- 時刻の設定
- 保守の設定
- NetMeister の設定
- ゼロタッチの設定

4.2 LAN

- LAN アドレスの設定
- DHCP サーバの設定

4.3 WAN

- プロバイダの設定
- 静的 NAT の設定
- WAN フィルタの設定 (Ver10.3 以降の機能)
- WAN フィルタの設定 (Ver10.2 までの設定がある場合)
- URL フィルタの設定
- QoS の設定
- 通信セキュリティの設定

4.4 VPN・クラウド

- VPN の設定
- L2TP の設定
- クラウドの設定

4.5 NGN 網 VPN の設定

- NetMeister の事前登録
- サービス情報サイトの事前登録
- NGN 網 VPN 設定

4.6 デバイス


- デバイスの設定

4.7 UTM

- トップページ
- 基本設定
- UTM の詳細設定
- アンチウイルス(AV)の設定
- 不正侵入防止(IPS)の設定
- Web ガード(WG)の設定
- URL フィルタリング(UF)の設定
- グループ別ポリシー設定
- ホワイトリスト設定
- UTM 脅威レポート

4. 詳細設定

4.1 基本設定

 設定を変更したときは、設定の保存を実行してください。

4.1.1 パスワードの設定

ログイン認証用のパスワードを設定します。

- (1) ログイン後のメニューエリアから[詳細設定]をクリックします。
- (2) 「基本設定」の項目から[パスワードの設定]をクリックします。



■ 管理者メニュー	詳細設定
トップページ	本装置の詳細な設定を行います。
設定の保存	ルータの全ての設定を利用できるわけではありません。
ログアウト	個別に設定を変更する場合は任意コマンドの実行から操作してください。
■ かんたん設定	本装置に接続された端末の制御は 端末管理 から操作してください。
かんたん設定	
■ 詳細設定	基本設定
詳細設定	本装置の基本的な設定を行います。
基本設定	保守設定ではSSH、Telnet、SNMP、Syslog等を設定します。
パスワードの設定	また、NetMeisterやゼロタッチの設定をします。
装置名の設定	
時刻の設定	
保守の設定	
NetMeisterの設定	
ゼロタッチの設定	
LAN	LAN
LANアドレスの設定	LAN側の設定を行います。
DHCPサーバの設定	IPアドレス、DHCPサーバなどを設定します。
WAN	WAN
プロバイダの設定	WAN側の設定を行います。
静的NAPTの設定	プロバイダ設定ではインターネットの接続設定を行います。
WANフィルタの設定	QoS設定ではシェーピングとPQ制御を利用できます。
・IPv4	URLフィルタの設定ではサービス事業者の提供するURLリストや
・IPv6	ユーザが指定したURLをフィルタできます。
URLフィルタリングの設定	
QoSの設定	
通信セキュリティの設定	
VPN・クラウド	VPN・クラウド
VPNの設定	IPSecやダイナミックVPN、サービス事業者ごとのクラウド設定を行います。
L2TPの設定	
クラウドの設定	
NGN網VPN	NGN網VPN
NGN網VPNの設定	NGN-IPv6網を利用したVPNの設定を行います。
デバイス	デバイス
デバイスの設定	本装置の各デバイスの設定を行います。
UTM	UTM
基本設定	本装置のUTMの設定を行います。
詳細設定	
グループ別ポリシー設定	
ホワイトリスト設定	
UTM脅威レポート	
■ 端末管理	
端末管理	
■ 保守管理	
保守管理	
■ 拡張ページ	
拡張ページ	
■ 外部リンク	
製品ページ	

- (3) 各項目を設定し、[反映]ボタンをクリックします。

4. 詳細設定

パスワードの設定

管理者パスワードの設定

設定変更を行うためのパスワード設定を行います。

	現在の設定	設定の変更
ユーザ名	admin	変更できません
パスワード	パスワード設定なし	<input type="radio"/> パスワードを変更しない <input checked="" type="radio"/> パスワードを変更する <input type="text"/> 確認のためもう一度入力してください。 <input type="text"/> パスワードを入力してください。

利用者パスワードの設定

利用者メニューのためのパスワード設定を行います。

利用者ユーザを設定しない場合は、管理者ユーザでの認証となります。

	現在の設定	設定の変更
利用者ユーザ	設定なし	<input checked="" type="radio"/> 利用者ユーザを設定しない <input type="radio"/> 利用者ユーザを設定する

画面表示認証の設定

『装置状態の表示』に認証が必要かの設定を行います。

	現在の設定	設定の変更
認証の有無	不要	<input checked="" type="radio"/> 『装置状態の表示』は認証が不要 <input type="radio"/> 『装置状態の表示』に認証が必要

保存

4. 詳細設定

番号	項目	内容
①	ユーザ名	<p>本装置に管理者レベルの権限でログインするときのユーザを設定します。</p> <ul style="list-style-type: none"> 初期状態ではユーザ名は設定されていません。 パスワード設定後のユーザ名は「admin」です。Web 設定からは変更できません。
②	パスワード	<p>本装置にログインするときのパスワードを入力します。</p> <ul style="list-style-type: none"> 半角英数字で1~249文字まで入力できます。 セキュリティ性を向上させるため、パスワードの設定を強く推奨します。 <p>メモ</p> <ul style="list-style-type: none"> パスワードを変更し[反映]をクリックしたときだけ、設定したパスワードの強度評価が行われ、その結果が表示されます。 <ul style="list-style-type: none"> スコア:4 (非常に強い) スコア:3 (強い) スコア:2 (普通) スコア:1 (弱い) スコア:0 (非常に弱い) <p>注意</p> <ul style="list-style-type: none"> 大文字/小文字は区別されます。 パスワードの入力文字は表示されません。●●●のように伏せ文字で表示されます。 パスワードは、第三者に推測されにくく、忘れないような文字列を入力してください。
③	利用者ユーザ	<p>利用者メニューの「リンクマネージャ」と「Wake on LAN」機能だけを利用できるユーザを設定します。</p> <ul style="list-style-type: none"> 「利用者ユーザを設定する」が選択されている場合は、ユーザ名の表示とパスワードの設定画面が表示されます。 <p>ここで設定した利用者ユーザは、本装置にコマンドラインを使用してログインすることもできます。この場合、モニタレベル権限のユーザとなります。</p> <p>メモ</p> <ul style="list-style-type: none"> 利用者メニューの「リンクマネージャ」と「Wake on LAN」機能のメニューは下記を参照ください。
④	認証の有無	<p>Web コンソール画面を起動した際に、セキュリティ性を高めるため、認証を要求できるように設定します。</p>

参考：利用者メニューの「リンクマネージャ」と「Wake on LAN」のメニュー

■ 管理者メニュー	トップページ
トップページ	
ログイン	ルータの設定を開始します。以下のリンクから選択してください。
■ 利用者メニュー	パスワードを登録・変更する前にユーザ名とパスワードを入力する画面が表示された場合は、そのまま「OK」をクリックしてください。
装置状態の表示	
リンクマネージャ	かんたん設定
Wake on LAN	
■ 外部リンク	<ul style="list-style-type: none"> インターネット接続
製品ページ	<ul style="list-style-type: none"> フレッツ光などの有線回線やワイヤレス回線(3G・LTE)を使用して、インターネットに接続する設定を行います。 インターネット接続+VPN接続

4. 詳細設定

(4) 「設定内容を変更しました。」のメッセージを確認します。

パスワードの設定

設定内容を変更しました。

管理者パスワードの設定

	現在の設定	設定の変更
ユーザ名	admin	変更できません
パスワード	***** スコア:4 (非常に強い)	<input checked="" type="radio"/> パスワードを変更しない <input type="radio"/> パスワードを変更する

利用者パスワードの設定

	現在の設定	設定の変更
利用者ユーザ	設定なし	<input checked="" type="radio"/> 利用者ユーザを設定しない <input type="radio"/> 利用者ユーザを設定する

画面表示認証の設定

	現在の設定	設定の変更
認証の有無	不要	<input checked="" type="radio"/> 『装置状態の表示』は認証が不要 <input type="radio"/> 『装置状態の表示』に認証が必要

[詳細設定へ](#)

4. 詳細設定

4.1.2 装置名の設定

装置名を変更します。

 設定を変更したときは、設定の保存を実行してください。

- (1) ログイン後のメニューエリアから[詳細設定]をクリックします。
- (2) 「基本設定」の項目から[装置名の設定]をクリックします。

<ul style="list-style-type: none">■管理者メニュー<ul style="list-style-type: none">トップページ設定の保存ログアウト■かんたん設定<ul style="list-style-type: none">かんたん設定■詳細設定<ul style="list-style-type: none">詳細設定基本設定パスワードの設定装置名の設定時刻の設定保守の設定NetMeisterの設定ゼロタッチの設定LAN<ul style="list-style-type: none">LANアドレスの設定DHCPサーバの設定WAN<ul style="list-style-type: none">プロバイダの設定静的NAPTの設定WANフィルタの設定<ul style="list-style-type: none">IPv4IPv6URLフィルタリングの設定QoSの設定通信セキュリティの設定VPN・クラウド<ul style="list-style-type: none">VPNの設定L2TPの設定クラウドの設定NGN網VPN<ul style="list-style-type: none">NGN網VPNの設定デバイス<ul style="list-style-type: none">デバイスの設定UTM<ul style="list-style-type: none">基本設定詳細設定グループ別ポリシー設定ホワイトリスト設定UTM脅威レポート■端末管理<ul style="list-style-type: none">端末管理■保守管理<ul style="list-style-type: none">保守管理■拡張ページ<ul style="list-style-type: none">拡張ページ■外部リンク<ul style="list-style-type: none">製品ページ	<h3>詳細設定</h3> <p>本装置の詳細な設定を行います。 ルータの全ての設定を利用できるわけではありません。 個別に設定を変更する場合は任意コマンドの実行から操作してください。 本装置に接続された端末の制御は端末管理から操作してください。</p> <hr/> <h3>基本設定</h3> <p>本装置の基本的な設定を行います。 保守設定ではSSH、Telnet、SNMP、Syslog等を設定します。 また、NetMeisterやゼロタッチの設定をします。</p> <hr/> <h3>LAN</h3> <p>LAN側の設定を行います。 IPアドレス、DHCPサーバなどを設定します。</p> <hr/> <h3>WAN</h3> <p>WAN側の設定を行います。 プロバイダ設定ではインターネットの接続設定を行います。 QoS設定ではシェーピングとPQ制御を利用できます。 URLフィルタの設定ではサービス事業者の提供するURLリストやユーザが指定したURLをフィルタできます。</p> <hr/> <h3>VPN・クラウド</h3> <p>IPSecやダイナミックVPN、サービス事業者ごとのクラウド設定を行います。</p> <hr/> <h3>NGN網VPN</h3> <p>NGN-IPv6網を利用したVPNの設定を行います。</p> <hr/> <h3>デバイス</h3> <p>本装置の各デバイスの設定を行います。</p> <hr/> <h3>UTM</h3> <p>本装置のUTMの設定を行います。</p>
---	--

4. 詳細設定

(3) 各項目を設定し、[反映]ボタンをクリックします。

装置名の設定

装置名を変更します。

装置名	現在の設定	設定の変更
Router	Router	Router

反映

番号	項目	内容
①	装置名	本装置をネットワークで識別するための名称を入力します。 <ul style="list-style-type: none">任意の装置名を付けることができます。半角英数字で1～79文字まで入力できます。初期値は「Router」です。

(4) 「設定内容を変更しました。」のメッセージと、設定が反映されたことを確認します。

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず「設定の保存」を行ってください。

装置名の設定

設定内容を変更しました。

装置名	現在の設定	設定の変更
Router#1	Router#1	Router#1

詳細設定へ

4. 詳細設定

4.1.3 時刻の設定

時刻を設定します。

- (1) ログイン後のメニューエリアから[詳細設定]をクリックします。
- (2) 「基本設定」の項目から[時刻の設定]をクリックします。

<ul style="list-style-type: none">■ 管理者メニュー<ul style="list-style-type: none">トップページ設定の保存ログアウト■ かんたん設定<ul style="list-style-type: none">かんたん設定■ 詳細設定<ul style="list-style-type: none">詳細設定基本設定<ul style="list-style-type: none">パスワードの設定装置名の設定時刻の設定保守の設定NetMeisterの設定ゼロタッチの設定LAN<ul style="list-style-type: none">LANアドレスの設定DHCPサーバの設定WAN<ul style="list-style-type: none">プロバイダの設定静約NAPTの設定WANフィルタの設定<ul style="list-style-type: none">・IPv4・IPv6URLフィルタリングの設定QoSの設定通信セキュリティの設定VPN・クラウド<ul style="list-style-type: none">VPNの設定L2TPの設定クラウドの設定NGN網VPN<ul style="list-style-type: none">NGN網VPNの設定デバイス<ul style="list-style-type: none">デバイスの設定UTM<ul style="list-style-type: none">基本設定詳細設定グループ別ポリシー設定ホワイトリスト設定UTM尚蔵レポート■ 端末管理<ul style="list-style-type: none">端末管理■ 保守管理<ul style="list-style-type: none">保守管理■ 拡張ページ<ul style="list-style-type: none">拡張ページ■ 外部リンク<ul style="list-style-type: none">製品ページ	<h3>詳細設定</h3> <p>本装置の詳細な設定を行います。 ルータの全ての設定を利用できるわけではありません。 個別に設定を変更する場合は任意コマンドの実行から操作してください。 本装置に接続された端末の制御は端末管理から操作してください。</p> <hr/> <h3>基本設定</h3> <p>本装置の基本的な設定を行います。 保守設定ではSSH、Telnet、SNMP、Syslog等を設定します。 また、NetMeisterやゼロタッチの設定をします。</p> <hr/> <h3>LAN</h3> <p>LAN側の設定を行います。 IPアドレス、DHCPサーバなどを設定します。</p> <hr/> <h3>WAN</h3> <p>WAN側の設定を行います。 プロバイダ設定ではインターネットの接続設定を行います。 QoS設定ではシェーピングとPQ制御を利用できます。 URLフィルタの設定ではサービス事業者の提供するURLリストやユーザが指定したURLをフィルタできます。</p> <hr/> <h3>VPN・クラウド</h3> <p>IPSecやダイナミックVPN、サービス事業者ごとのクラウド設定を行います。</p> <hr/> <h3>NGN網VPN</h3> <p>NGN-IPv6網を利用したVPNの設定を行います。</p> <hr/> <h3>デバイス</h3> <p>本装置の各デバイスの設定を行います。</p> <hr/> <h3>UTM</h3> <p>本装置のUTMの設定を行います。</p>
--	--

4. 詳細設定

(3) 各項目を設定し、[反映]ボタンをクリックします。

時刻の設定

時刻を設定します。

	現在の設定	設定の変更
装置時刻	2023/11/06 15:07:17 JST	<input checked="" type="radio"/> PCの現在時刻を設定する <input type="radio"/> 手動で設定する <input type="radio"/> NTPサーバと同期する

反映

番号	項目	内容
①	装置時刻	<p>本装置の時刻を設定します。</p> <ul style="list-style-type: none">PCの時刻に合わせたいときは、「PCの現在時刻を設定する」を選択します。手動で設定するときは、「手動で設定する」を選択し、時刻を入力します。 年：2001～2098、月：1～12、日：1～31、時：0～23、分：0～59、秒：0～59NTPサーバに合わせたいときは、「NTPサーバと同期する」を選択し、NTPサーバのIPアドレスを入力します。画面を表示したときには、本装置の現在時刻が表示されています。

(4) 「設定内容を変更しました。」のメッセージと、設定が反映されたことを確認します。

時刻の設定

設定内容を変更しました。

	現在の設定	設定の変更
装置時刻	2016/09/01 14:02:31 JST	<input type="radio"/> PCの現在時刻を設定する <input type="radio"/> 手動で設定する <input checked="" type="radio"/> NTPサーバと同期する
NTPサーバ	192.168.1.200	192.168.1.200

詳細設定へ

4. 詳細設定

4.1.4 保守の設定

Telnet/SSH、SNMP、ロギング機能等の保守機能を設定します。

- (1) ログイン後のメニューエリアから[詳細設定]をクリックします。
- (2) 「基本設定」の項目から[保守の設定]をクリックします。

<ul style="list-style-type: none">■ 管理者メニュー<ul style="list-style-type: none">トップページ設定の保存ログアウト■ かんたん設定<ul style="list-style-type: none">かんたん設定■ 詳細設定<ul style="list-style-type: none">詳細設定基本設定<ul style="list-style-type: none">パスワードの設定装置名の設定時刻の設定保守の設定NetMeisterの設定ゼロタッチの設定LAN<ul style="list-style-type: none">LANアドレスの設定DHCPサーバの設定WAN<ul style="list-style-type: none">プロバイダの設定静的NAPTの設定WANフィルタの設定<ul style="list-style-type: none">・IPv4・IPv6URLフィルタリングの設定QoSの設定通信セキュリティの設定VPN・クラウド<ul style="list-style-type: none">VPNの設定L2TPの設定クラウドの設定NGN網VPN<ul style="list-style-type: none">NGN網VPNの設定デバイス<ul style="list-style-type: none">デバイスの設定UTM<ul style="list-style-type: none">基本設定詳細設定グループポリシー設定ホワイトリスト設定UTM脅威レポート■ 端末管理<ul style="list-style-type: none">端末管理■ 保守管理<ul style="list-style-type: none">保守管理■ 拡張ページ<ul style="list-style-type: none">拡張ページ■ 外部リンク<ul style="list-style-type: none">製品ページ	<h3>詳細設定</h3> <p>本装置の詳細な設定を行います。 ルータの全ての設定を利用できるわけではありません。 個別に設定を変更する場合は任意コマンドの実行から操作してください。 本装置に接続された端末の制御は端末管理から操作してください。</p> <hr/> <h3>基本設定</h3> <p>本装置の基本的な設定を行います。 保守設定ではSSH、Telnet、SNMP、Syslog等を設定します。 また、NetMeisterやゼロタッチの設定をします。</p> <hr/> <h3>LAN</h3> <p>LAN側の設定を行います。 IPアドレス、DHCPサーバなどを設定します。</p> <hr/> <h3>WAN</h3> <p>WAN側の設定を行います。 プロバイダ設定ではインターネットの接続設定を行います。 QoS設定ではシェーピングとPQ制御を利用できます。 URLフィルタの設定ではサービス事業者の提供するURLリストやユーザが指定したURLをフィルタできます。</p> <hr/> <h3>VPN・クラウド</h3> <p>IPSecやダイナミックVPN、サービス事業者ごとのクラウド設定を行います。</p> <hr/> <h3>NGN網VPN</h3> <p>NGN-IPv6網を利用したVPNの設定を行います。</p> <hr/> <h3>デバイス</h3> <p>本装置の各デバイスの設定を行います。</p> <hr/> <h3>UTM</h3> <p>本装置のUTMの設定を行います。</p>
--	---

4. 詳細設定

(3) 各項目を設定し、[反映]ボタンをクリックします。

保守の設定

Telnet/SSH、SNMP、ロギング機能(logging, syslog)の設定を行います。

SSH/Telnetの設定

SSHサーバ機能とTelnetサーバ機能を設定します。

	現在の設定	設定の変更
SSH設定	無効	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
Telnet設定	有効	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効

SNMPの設定

SNMPを設定します。

	現在の設定	設定の変更
SNMP設定	無効	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効

ロギングの設定

ロギングの設定を行います。装置内への保存は常に行います。

	現在の設定	設定の変更
純正ロギング設定	有効	<input checked="" type="radio"/> 有効(無効化できません)
Syslog設定	無効	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効

ロギングを収集するレベルを機能ごとに選択します。通常は推奨設定を選択してください。

	現在の設定	設定の変更
ロギングレベル設定	推奨設定	<input checked="" type="radio"/> 変更しない <input type="radio"/> 推奨設定: 全機能 warn(2:警告レベル) <input type="radio"/> 詳細設定: 機能ごとに記録レベルを変更
全体設定	warn	warn (2:警告レベル) (warn以外へは変更できません)
イーサネット	warn	warn (2:警告レベル)
IPv4	warn	warn (2:警告レベル)
IPv6	warn	warn (2:警告レベル)
PPP/PPPoE	warn	warn (2:警告レベル)
L2TP	warn	warn (2:警告レベル)
フィルタリング	warn	warn (2:警告レベル)
NAT	warn	warn (2:警告レベル)
RIP	warn	warn (2:警告レベル)
BGP	warn	warn (2:警告レベル)
OSPF	warn	warn (2:警告レベル)
IKE	warn	warn (2:警告レベル)
IKEv2	warn	warn (2:警告レベル)
不正アクセス検知	warn	warn (2:警告レベル)
URLフィルタリング	warn	warn (2:警告レベル)
URLオフロード	warn	warn (2:警告レベル)
UTM	warn	warn (2:警告レベル)

反映

4. 詳細設定

番号	項目	内容
①	SSH 設定	SSH サーバ機能の有効化/無効化を設定します。
②	Telnet 設定	Telnet サーバ機能の有効化/無効化を設定します。
③	SNMP 設定	SNMP の有効化/無効化を設定します。 <ul style="list-style-type: none"> 有効化した場合、バージョンで v1/v2c か v3 を選択します。 v1/v2c を選択した場合、以下を設定します。 <ul style="list-style-type: none"> コミュニティ設定で、コミュニティ名を設定します。 SNMP マネージャにトラップを送信する場合は、トラップ設定で宛先の IP アドレスを設定します。 v3 を選択した場合、以下を設定します。 <ul style="list-style-type: none"> ユーザ名の設定で、ユーザ名を設定します。 認証アルゴリズムは、MD5、SHA1、SHA2-224、SHA2-256、SHA2-384、SHA2-512 から選択します。 認証パスワードで、認証のパスワードを設定します。 暗号化アルゴリズムは、DES、AES-128 から選択します。 暗号化パスワードで、暗号化のパスワードを設定します。 認証パスワードと同じ設定にすることもできます。 <ul style="list-style-type: none"> SNMP マネージャにトラップを送信する場合は、トラップ設定で宛先の IP アドレスを設定します。
④	装置ログ設定	常に有効化されます。無効化することはできません。
⑤	Syslog 設定	Syslog 送信機能の有効化/無効化を設定します。 <ul style="list-style-type: none"> 有効化する際は、Syslog サーバの IP アドレスを設定します。
⑥	ロギングレベル設定	ロギングの取得レベルを設定します。 <ul style="list-style-type: none"> 初期状態は、全機能 warn(2:警告レベル)に設定されています。 機能ごとにレベルを変更する場合は、個別に詳細設定を選択します。
⑦	全体設定	全体設定は、warn(2:警告レベル)以外への変更はできません。
⑧	個別設定	機能ごとに以下のレベルを設定することができます。 <ul style="list-style-type: none"> error(1:エラーレベル) 低 warn(2:警告レベル) ↑ notice(3:注意レベル) ↓ info(4:情報レベル) ↓ debug(5:デバッグレベル) 高 注意 高いレベルに設定すると、ルータの機能に負担がかかります。必要最小限のレベルでご利用ください。

4. 詳細設定

- (4) 「設定内容を変更しました。」のメッセージと、設定が反映されたことを確認します。

保守の設定

設定内容を変更しました。

SSH/Telnetの設定

	現在の設定	設定の変更
SSH設定	無効	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
Telnet設定	有効	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効

SNMPの設定

	現在の設定	設定の変更
SNMP設定	無効	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効

ロギングの設定

	現在の設定	設定の変更
装置ロギング設定	有効	<input checked="" type="radio"/> 有効(無効化できません)
Syslog設定	無効	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効

ロギングレベル設定

	現在の設定	設定の変更
ロギングレベル設定	推奨設定	<input type="radio"/> 変更しない <input checked="" type="radio"/> 推奨設定: 全機能 warn(2:警告レベル) <input type="radio"/> 詳細設定: 機能ごとに記録レベルを変更
全体設定	warn	warn (2:警告レベル) (warn以外へは変更できません)
イーサネット	warn	warn (2:警告レベル) ▼
IPv4	warn	warn (2:警告レベル) ▼
IPv6	warn	warn (2:警告レベル) ▼
PPP/PPPoE	warn	warn (2:警告レベル) ▼
L2TP	warn	warn (2:警告レベル) ▼
フィルタリング	warn	warn (2:警告レベル) ▼
NAT	warn	warn (2:警告レベル) ▼
RIP	warn	warn (2:警告レベル) ▼
BGP	warn	warn (2:警告レベル) ▼
OSPF	warn	warn (2:警告レベル) ▼
IKE	warn	warn (2:警告レベル) ▼
IKEv2	warn	warn (2:警告レベル) ▼
不正アクセス検知	warn	warn (2:警告レベル) ▼
URLフィルタリング	warn	warn (2:警告レベル) ▼
URLオフロード	warn	warn (2:警告レベル) ▼
UTM	warn	warn (2:警告レベル) ▼

[詳細設定へ](#)

4. 詳細設定

4.1.5 NetMeister の設定

NetMeister を設定します。

NetMeister を利用しない場合、NetMeister の設定は不要です。

NetMeister を利用する場合、あらかじめ NetMeister のサイトで「アカウント登録」と「グループ登録」が必要です。

- (1) ログイン後のメニューエリアから[詳細設定]をクリックします。
- (2) 「基本設定」の項目から[NetMeister の設定]をクリックします。



■管理者メニュー

- トップページ
- 設定の保存
- ログアウト

■かんたん設定

- かんたん設定

■詳細設定

- 詳細設定
- 基本設定
 - パスワードの設定
 - 装置名の設定
 - 時刻の設定
 - 保守の設定
 - NetMeisterの設定**
 - ゼロタッチの設定
- LAN
 - LANアドレスの設定
 - DHCPサーバの設定
- WAN
 - プロバイダの設定
 - 静的NAPTの設定
 - WANフィルタの設定
 - ・IPv4
 - ・IPv6
 - URLフィルタリングの設定
 - QoSの設定
 - 通信セキュリティの設定
- VPN・クラウド
 - VPNの設定
 - L2TPの設定
 - クラウドの設定
- NGN網VPN
 - NGN網VPNの設定
- デバイス
 - デバイスの設定
- UTM
 - 基本設定
 - 詳細設定
 - グループ別ポリシー設定
 - ホワイトリスト設定
 - UTM脅威レポート

■端末管理

- 端末管理

■保守管理

- 保守管理

■拡張ページ

- 拡張ページ

■外部リンク

- 製品ページ

NetMeisterの設定

NetMeisterの設定と動作状況です。
利用する場合は、事前に [NetMeister](#) のサイトで『アカウント登録』と『グループ登録』が必要です。

NetMeister	現在の設定
状態	無効

再認証 変更

4. 詳細設定

(3) [変更]ボタンをクリックします。

NetMeisterの設定

NetMeisterの設定と動作状況です。
利用する場合は、事前に [NetMeister](#) のサイトで『アカウント登録』と『グループ登録』が必要です。

	現在の設定
NetMeister	NetMeister (外部サイト)
状態	無効

再認証
変更

(4) 各項目を設定し、[反映]ボタンをクリックします。

NetMeisterの設定

NetMeisterの設定を行います。
Web設定では、IPv4で動作する設定のみ対応しています。

	設定の変更
NetMeister	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効 <input type="radio"/> DDNSなし有効

戻る **反映**

番号	項目	内容
①	NetMeister	NetMeister の「有効」／「無効」を設定します。 「有効」に設定すると、アカウント名等を設定することができます。

(5) 「有効」を選択するとアカウント名等の設定項目が表示されますので、各項目を設定し、[反映]ボタンをクリックします。

NetMeisterの設定

NetMeisterの設定を行います。
Web設定では、IPv4で動作する設定のみ対応しています。

	設定の変更
NetMeister	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効 <input type="radio"/> DDNSなし有効
グループID	<input type="text"/> 文字列を入力してください。[2-63文字]
グループパスワード	<input type="radio"/> パスワードを変更しない <input checked="" type="radio"/> パスワードを変更する <input type="text"/> 文字列を入力してください。[8-31文字]
拠点ID	省略可能です。 <input type="text"/>
ホスト名 (装置名)	『装置名の設定』で設定した装置名を通知します。 web-01a12 <input type="checkbox"/> DDNS ホスト名を別名で設定する

戻る **反映**

4. 詳細設定

番号	項目	内容
①	NetMeister	NetMeister の「有効」／「無効」を設定します。 「無効」に設定すると、アカウント名等の設定項目が隠れます。
②	グループ ID	NetMeister の登録ページで申請した「グループ ID」を設定します。 ・ 半角英数字または-(ハイフン)で 2~63 文字まで入力できます。
③	グループパスワード	NetMeister の登録ページで申請した「グループパスワード」を設定します。 ・ 半角英数字、_(アンダーバー)または-(ハイフン)で 8~31 文字まで入力できます。 注意 ・ 大文字／小文字は区別されます。 ・ パスワードの入力文字は表示されません。●●●のように伏せ文字で表示されます。 ・ パスワードは、第三者に推測されにくく、忘れないような文字列を入力してください。
④	ホスト名 (装置名)	NetMeister に通知するホスト名を変更する必要がある場合は、ここで設定します。 ・ 半角英数字または-(ハイフン)で 2~63 文字まで入力できます。 メモ ・ NetMeister で受け付けられない文字を装置名に指定している場合等に利用します。 ・ 大文字は、小文字に変換して NetMeister に通知されます。 注意 ・ ホスト名の先頭と最後には-(ハイフン)を利用することができません。
⑤	サイト名 (拠点名)	NetMeister に通知するサイト名を変更する必要がある場合は、ここで設定します。 ・ 半角英数字または-(ハイフン)で 2~31 文字まで入力できます。 メモ ・ NetMeister で受け付けられない文字を装置名に指定している場合等に利用します。 ・ 大文字は、小文字に変換して NetMeister に通知されます。 ・ サイト名を省略した場合は、装置名が NetMeister に通知されます。 注意 ・ サイト名の先頭と最後には-(ハイフン)を利用することができません。

4. 詳細設定

4.1.6 ゼロタッチの設定

ゼロタッチプロビジョニング機能を設定します。

ゼロタッチプロビジョニング機能を利用しない場合、ゼロタッチの設定は不要です。

ゼロタッチの設定を反映するためには、設定の保存を行ってから再起動が必要です。

(1) ログイン後のメニューエリアから[詳細設定]をクリックします。

(2) 「基本設定」の項目から[ゼロタッチの設定]をクリックします。

■ 管理者メニュー	詳細設定
トップページ	
設定の保存	本装置の詳細な設定を行います。
ログアウト	ルータの全ての設定を利用できるわけではありません。
■ かんたん設定	個別に設定を変更する場合は任意コマンドの実行から操作してください。
かんたん設定	本装置に接続された端末の制御は 端末管理 から操作してください。
■ 詳細設定	基本設定
詳細設定	
基本設定	本装置の基本的な設定を行います。
パスワードの設定	保守設定ではSSH、Telnet、SNMP、Syslog等を設定します。
装置名の設定	また、NetMeisterやゼロタッチの設定をします。
時刻の設定	
保守の設定	
NetMeisterの設定	LAN側の設定を行います。
ゼロタッチの設定	IPアドレス、DHCPサーバなどを設定します。
LAN	
LANアドレスの設定	WAN
DHCPサーバの設定	WAN側の設定を行います。
WAN	プロバイダ設定ではインターネットの接続設定を行います。
プロバイダの設定	QoS設定ではシェーピングとPQ制御を利用できます。
静的NAPTの設定	URLフィルタの設定ではサービス事業者の提供するURLリストや
WANフィルタの設定	ユーザが指定したURLをフィルタできます。
・IPv4	
・IPv6	VPN・クラウド
URLフィルタリングの設定	IPSecやダイナミックVPN、サービス事業者ごとのクラウド設定を行います。
QoSの設定	
通信セキュリティの設定	NGN網VPN
VPN・クラウド	NGN-IPv6網を利用したVPNの設定を行います。
VPNの設定	
L2TPの設定	デバイス
クラウドの設定	本装置の各デバイスの設定を行います。
NGN網VPN	
NGN網VPNの設定	
デバイス	UTM
デバイスの設定	本装置のUTMの設定を行います。
UTM	
基本設定	
詳細設定	
グループ別ポリシー設定	
ホワイトリスト設定	
UTM脅威レポート	
■ 端末管理	
端末管理	
■ 保守管理	
保守管理	
■ 拡張ページ	
拡張ページ	
■ 外部リンク	
製品ページ	

4. 詳細設定

(3) 各項目を設定し、[反映]ボタンをクリックします。

ゼロタッチの設定

ゼロタッチプロビジョニング機能の設定をします。

ゼロタッチ状態表示

装置再起動後のゼロタッチを有効にするには、[反映]を押した後、「設定の保存」を行う必要があります。

	現在の設定
装置再起動後のゼロタッチ	無効

ゼロタッチの設定

	現在の設定	設定の変更
ゼロタッチ	無効	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効

反映

番号	項目	内容
①	ゼロタッチ	ゼロタッチの「有効」／「無効」を設定します。 「有効」に設定すると、ゼロタッチプロビジョニング機能を設定することができます。

注意 ゼロタッチの設定を反映するためには、設定の保存を行ってから再起動が必要です。

※IX2107/IX2235/IX2310の場合

ゼロタッチの設定

ゼロタッチプロビジョニング機能の設定をします。

ゼロタッチ状態表示

装置再起動後のゼロタッチを有効にするには、[反映]を押した後、「設定の保存」を行う必要があります。

	現在の設定
MODEスイッチの状態	OFF
装置再起動後のゼロタッチ	無効

ゼロタッチの設定

	現在の設定	設定の変更
ゼロタッチ	無効	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効

反映

4. 詳細設定

4.2 LAN

メモ 設定を変更したときは、設定の保存を実行してください。

4.2.1 LAN アドレスの設定

LAN 側インタフェースの IP アドレスを設定します。

注意 LAN 側インタフェースの IP アドレスを変更する場合、現在の接続は切断されます。新しい IP アドレスに接続しなおしてください。

メモ LAN 側インタフェースは、それぞれ以下のインタフェースを使用します。

- IX2107 は GigaEthernet1.0
- IX2215/IX2235 は GigaEthernet2.0
- IX2310 は GigaEthernet3.0
- IX3315 は GigaEthernet5.0

- (1) ログイン後のメニューエリアから[詳細設定]をクリックします。
- (2) 「LAN」の項目から[LAN アドレスの設定]をクリックします。

4. 詳細設定

<ul style="list-style-type: none">■ 管理者メニュー<ul style="list-style-type: none">トップページ設定の保存ログアウト■ かんたん設定<ul style="list-style-type: none">かんたん設定■ 詳細設定<ul style="list-style-type: none">詳細設定基本設定<ul style="list-style-type: none">パスワードの設定装置名の設定時刻の設定保守の設定NetMeisterの設定ゼロタッチの設定LAN<ul style="list-style-type: none">LANアドレスの設定DHCPサーバの設定WAN<ul style="list-style-type: none">プロバイダの設定静的NAPTの設定WANフィルタの設定<ul style="list-style-type: none">・IPv4・IPv6URLフィルタリングの設定QoSの設定通信セキュリティの設定VPN・クラウド<ul style="list-style-type: none">VPNの設定L2TPの設定クラウドの設定NGN網VPN<ul style="list-style-type: none">NGN網VPNの設定デバイス<ul style="list-style-type: none">デバイスの設定UTM<ul style="list-style-type: none">基本設定詳細設定グループ別ポリシー設定ホワイトリスト設定UTM脅威レポート■ 端末管理<ul style="list-style-type: none">端末管理■ 保守管理<ul style="list-style-type: none">保守管理■ 拡張ページ<ul style="list-style-type: none">拡張ページ■ 外部リンク<ul style="list-style-type: none">新品ページ	<h2>詳細設定</h2> <p>本装置の詳細な設定を行います。 ルータの全ての設定を利用できるわけではありません。 個別に設定を変更する場合は任意コマンドの実行から操作してください。 本装置に接続された端末の制御は端末管理から操作してください。</p> <h2>基本設定</h2> <p>本装置の基本的な設定を行います。 保守設定ではSSH、Telnet、SNMP、Syslog等を設定します。 また、NetMeisterやゼロタッチの設定をします。</p> <h2>LAN</h2> <p>LAN側の設定を行います。 IPアドレス、DHCPサーバなどを設定します。</p> <h2>WAN</h2> <p>WAN側の設定を行います。 プロバイダ設定ではインターネットの接続設定を行います。 QoS設定ではシェーピングとPQ制御を利用できます。 URLフィルタの設定ではサービス事業者の提供するURLリストや ユーザが指定したURLをフィルタできます。</p> <h2>VPN・クラウド</h2> <p>IPSecやダイナミックVPN、サービス事業者ごとのクラウド設定を行います。</p> <h2>NGN網VPN</h2> <p>NGN-IPv6網を利用したVPNの設定を行います。</p> <h2>デバイス</h2> <p>本装置の各デバイスの設定を行います。</p> <h2>UTM</h2> <p>本装置のUTMの設定を行います。</p>
---	--

4. 詳細設定

(3) 各項目を設定し、[反映]ボタンをクリックします。

LANアドレスの設定

LAN側IPアドレスを設定します。
IPアドレスを変更する場合、現在の接続は切断されます。新しいIPアドレスに接続しなおしてください。

LAN1(GigaEthernet1.0)の設定

	現在の設定	設定の変更
IPアドレス	192.168.1.254/24	192.168.1.254 / 24

反映

番号	項目	内容
①	IPアドレス	LAN側IPアドレスを設定します。 IPアドレスを変更する場合、現在の接続は切断されます。新しいIPアドレスに接続しなおしてください。

(4) 「設定内容を変更しました。」のメッセージと、設定が反映されたことを確認します。

LANアドレスの設定

設定内容を変更しました。

LAN1(GigaEthernet1.0)の設定

	現在の設定	設定の変更
IPアドレス	192.168.1.254/24	192.168.1.254 / 24

詳細設定へ

4. 詳細設定

4.2.2 DHCP サーバの設定

LAN 側インタフェースに DHCP サーバ機能を設定します。

- (1) ログイン後のメニューエリアから[詳細設定]をクリックします。
- (2) 「LAN」の項目から[DHCPサーバの設定]をクリックします。

<ul style="list-style-type: none">■管理者メニュー<ul style="list-style-type: none">トップページ設定の保存ログアウト■かんたん設定<ul style="list-style-type: none">かんたん設定■詳細設定<ul style="list-style-type: none">詳細設定基本設定<ul style="list-style-type: none">パスワードの設定装置名の設定時刻の設定保守の設定NetMeisterの設定ゼロタッチの設定LAN<ul style="list-style-type: none">LANアドレスの設定DHCPサーバの設定WAN<ul style="list-style-type: none">プロバイダの設定静的NAPTの設定WANフィルタの設定<ul style="list-style-type: none">・IPv4・IPv6URLフィルタリングの設定QoSの設定通信セキュリティの設定VPN・クラウド<ul style="list-style-type: none">VPNの設定L2TPの設定クラウドの設定NGN網VPN<ul style="list-style-type: none">NGN網VPNの設定デバイス<ul style="list-style-type: none">デバイスの設定UTM<ul style="list-style-type: none">基本設定詳細設定グループ別ポリシー設定ホワイトリスト設定UTM脅威レポート■端末管理<ul style="list-style-type: none">端末管理■保守管理<ul style="list-style-type: none">保守管理■拡張ページ<ul style="list-style-type: none">拡張ページ■外部リンク<ul style="list-style-type: none">製品ページ	<h3>詳細設定</h3> <p>本装置の詳細な設定を行います。 ルータの全ての設定を利用できるわけではありません。 個別に設定を変更する場合は任意コマンドの実行から操作してください。 本装置に接続された端末の制御は端末管理から操作してください。</p> <hr/> <h3>基本設定</h3> <p>本装置の基本的な設定を行います。 保守設定ではSSH、Telnet、SNMP、Syslog等を設定します。 また、NetMeisterやゼロタッチの設定をします。</p> <hr/> <h3>LAN</h3> <p>LAN側の設定を行います。 IPアドレス、DHCPサーバなどを設定します。</p> <hr/> <h3>WAN</h3> <p>WAN側の設定を行います。 プロバイダ設定ではインターネットの接続設定を行います。 QoS設定ではシェーピングとPQ制御を利用できます。 URLフィルタの設定ではサービス事業者の提供するURLリストやユーザが指定したURLをフィルタできます。</p> <hr/> <h3>VPN・クラウド</h3> <p>IPSecやダイナミックVPN、サービス事業者ごとのクラウド設定を行います。</p> <hr/> <h3>NGN網VPN</h3> <p>NGN-IPv6網を利用したVPNの設定を行います。</p> <hr/> <h3>デバイス</h3> <p>本装置の各デバイスの設定を行います。</p> <hr/> <h3>UTM</h3> <p>本装置のUTMの設定を行います。</p>
---	---

4. 詳細設定

(3) 各項目を設定し、[反映]ボタンをクリックします。

DHCPサーバの設定

LAN側インタフェースにDHCPサーバ機能を設定します。
割り当て範囲を自動設定にした場合、LAN側ネットワークの全てのIPアドレスが対象になります。

LAN1(GigaEthernet1.0)の設定

	現在の設定	設定の変更
IPアドレス	192.168.1.254/24	変更できません
DHCPサーバ	有効	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
割り当て範囲	自動設定	<input checked="" type="radio"/> 自動設定 <input type="radio"/> 固定設定

反映

番号	項目	内容
①	IP アドレス	LAN 側インタフェースに設定されている IP アドレスを入力します。 ・ 変更できません。
②	DHCP サーバ	DHCP サーバ機能の「有効」／「無効」を設定します。 注意 ・ 「無効」を選択したときは、ネットワーク内のパソコン等の IP アドレスを個別に設定する必要があります。
③	割り当て範囲	DHCP サーバ機能を使用するとき、LAN 側インタフェースのネットワーク機器に割り当てる IP アドレスの範囲を指定します。 注意 ・ DHCP の割り当て範囲は、LAN 側 IP アドレスと同一のサブネットワークの範囲内である必要があります。 ・ 「DHCP サーバ」の[無効]を選択した場合、割り当て範囲を入力することはできません。

(4) 「設定内容を変更しました。」のメッセージと、設定が反映されたことを確認します。

DHCPサーバの設定

設定内容を変更しました。

LAN1(GigaEthernet1.0)の設定

	現在の設定	設定の変更
IPアドレス	192.168.1.254/24	変更できません
DHCPサーバ	有効	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
割り当て範囲	192.168.1.1 ~ 192.168.1.100	<input type="radio"/> 自動設定 <input checked="" type="radio"/> 固定設定

[192.168.1.1] ~ [192.168.1.100] [詳細設定へ](#)

4. 詳細設定

4.3 WAN

4.3.1 プロバイダの設定

プロバイダと接続するWAN側インタフェースを設定します。

- (1) ログイン後のメニューエリアから[詳細設定]をクリックします。
- (2) 「WAN」の項目から[プロバイダの設定]をクリックします。

<ul style="list-style-type: none">■ 管理者メニュー<ul style="list-style-type: none">トップページ設定の保存ログアウト■ かんたん設定<ul style="list-style-type: none">かんたん設定■ 詳細設定<ul style="list-style-type: none">詳細設定基本設定<ul style="list-style-type: none">パスワードの設定装置名の設定時刻の設定保守の設定NetMeisterの設定ゼロタッチの設定LAN<ul style="list-style-type: none">LANアドレスの設定DHCPサーバの設定WAN<ul style="list-style-type: none">プロバイダの設定静的NAPTの設定WANフィルタの設定<ul style="list-style-type: none">・IPv4・IPv6URLフィルタリングの設定QoSの設定通信セキュリティの設定VPN・クラウド<ul style="list-style-type: none">VPNの設定L2TPの設定クラウドの設定NGN網VPN<ul style="list-style-type: none">NGN網VPNの設定デバイス<ul style="list-style-type: none">デバイスの設定UTM<ul style="list-style-type: none">基本設定詳細設定グループ別ポリシー設定ホワイトリスト設定UTM脅威レポート■ 端末管理<ul style="list-style-type: none">端末管理■ 保守管理<ul style="list-style-type: none">保守管理■ 拡張ページ<ul style="list-style-type: none">拡張ページ■ 外部リンク<ul style="list-style-type: none">製品ページ	<h3>詳細設定</h3> <p>本装置の詳細な設定を行います。 ルータの全ての設定を利用できるわけではありません。 個別に設定を変更する場合は任意コマンドの実行から操作してください。 本装置に接続された端末の制御は端末管理から操作してください。</p> <hr/> <h3>基本設定</h3> <p>本装置の基本的な設定を行います。 保守設定ではSSH、Telnet、SNMP、Syslog等を設定します。 また、NetMeisterやゼロタッチの設定をします。</p> <hr/> <h3>LAN</h3> <p>LAN側の設定を行います。 IPアドレス、DHCPサーバなどを設定します。</p> <hr/> <h3>WAN</h3> <p>WAN側の設定を行います。 プロバイダ設定ではインターネットの接続設定を行います。 QoS設定ではシェーピングとPQ制御を利用できます。 URLフィルタの設定ではサービス事業者の提供するURLリストやユーザが指定したURLをフィルタできます。</p> <hr/> <h3>VPN・クラウド</h3> <p>IPSecやダイナミックVPN、サービス事業者ごとのクラウド設定を行います。</p> <hr/> <h3>NGN網VPN</h3> <p>NGN-IPv6網を利用したVPNの設定を行います。</p> <hr/> <h3>デバイス</h3> <p>本装置の各デバイスの設定を行います。</p> <hr/> <h3>UTM</h3> <p>本装置のUTMの設定を行います。</p>
--	--

4. 詳細設定

(3) 各項目を設定し、[反映]ボタンをクリックします。

IPv4、PPPoE 接続の場合(フレッツ光回線利用の場合)

プロバイダの設定

プロバイダと接続するWAN側インタフェースを設定します。

	現在の設定	設定の変更
プロトコル		<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
接続形態		<input checked="" type="radio"/> PPPoE接続 (フレッツ光回線利用の場合) <input type="radio"/> IP接続 (ケーブルテレビ回線利用の場合)

WAN1: PPPoE接続の設定(GigaEthernet0.1)

	現在の設定	設定の変更
接続名	WAN1	WAN1
ユーザ名		プロバイダから通知されているユーザ名を設定します。 (フレッツの場合、通常はユーザ名には@を含んでいます) <input type="text"/> 文字列(半角英数字)を入力してください。
パスワード		プロバイダから通知されているパスワードを設定します。 <input type="text"/> 文字列(半角英数字)を入力してください。
WAN側IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
DNSアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
NAPT		<input checked="" type="radio"/> 有効

4. 詳細設定

番号	項目	内容
①	プロトコル	「IPv4」を選択します。
②	接続形態	「PPPoE（フレッツ光回線利用の場合）」を選択します。
③	接続名	接続名を識別するための名称を入力します。 <ul style="list-style-type: none"> 任意の接続名を付けることができます。 半角英数字で1～79文字まで入力できます。 初期値は「WAN1」です。
④	ユーザ名	プロバイダから通知されているユーザ名を設定します。 (フレッツの場合、通常はユーザ名には@を含んでいます) <ul style="list-style-type: none"> 半角英数字で1～59文字まで入力できます。
⑤	パスワード	プロバイダから通知されているパスワードを設定します。 <ul style="list-style-type: none"> 半角英数字で1～79文字まで入力できます。 注意 大文字、小文字も区別されます。
⑥	WAN側IPアドレス	WAN側IPアドレスを設定します。 <ul style="list-style-type: none"> プロバイダからWAN側IPアドレスが与えられていないときは「自動取得」を、固定IPアドレスが与えられているときは「手動設定」を選択します。 「手動設定」を選択したときは、プロバイダから与えられたIPアドレスを入力し、サブネットマスクをプルダウンメニューから選択します。 注意 <ul style="list-style-type: none"> 他のインタフェースに設定されているIPアドレスを使用することはできません。 「自動取得」を選択した場合、IPアドレスを入力することはできません。
⑦	DNSアドレス	PPPoE接続のDNSサーバのアドレスを設定します。 <ul style="list-style-type: none"> プロバイダからDNSサーバのアドレスが与えられていないときは「自動取得」を、与えられているとき、または独自に指定するときは「手動設定」を選択します。 「手動設定」を選択したときは、プロバイダから与えられたプライマリDNSサーバのIPアドレスを上段に、セカンダリDNSサーバのIPアドレスを下段に入力します。セカンダリは省略可能です。 注意 <ul style="list-style-type: none"> 「自動取得」を選択した場合、DNSアドレスを入力することはできません。
⑧	NAPT	NAPTは常に有効です。設定を変更することはできません。

4. 詳細設定

IPv4、IP 接続の場合(ケーブルテレビ回線利用の場合)

プロバイダの設定

プロバイダと接続するWAN側インタフェースを設定します。

	現在の設定	設定の変更
プロトコル		<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
接続形態		<input type="radio"/> PPPoE接続 (フレッツ光回線利用の場合) <input checked="" type="radio"/> IP接続 (ケーブルテレビ回線利用の場合)

WAN1: IP接続の設定(GigaEthernet0.0)

	現在の設定	設定の変更
接続名	WAN1	<input type="text" value="WAN1"/>
WAN側IPアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
DNSアドレス		<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
NAPT		特別な理由がない限り有効にしてください <input type="radio"/> 無効 <input checked="" type="radio"/> 有効

4. 詳細設定

番号	項目	内容
①	プロトコル	「IPv4」を選択します。
②	接続形態	「IP 接続 (ケーブルテレビ回線利用の場合)」を選択します。
③	接続名	接続名を識別するための名称を入力します。 <ul style="list-style-type: none">• 任意の接続名を付けることができます。• 半角英数字で 1～79 文字まで入力できます。• 初期値は「WAN1」です。
④	WAN 側 IP アドレス	IP 接続の WAN 側 IP アドレスを設定します。 <ul style="list-style-type: none">• プロバイダから WAN 側 IP アドレスが与えられていないときは「自動取得」を、固定 IP アドレスが与えられているときは「手動設定」を選択します。• 「手動設定」を選択したときは、プロバイダから与えられた IP アドレスを入力し、サブネットマスクをプルダウンメニューから選択します。 注意 <ul style="list-style-type: none">• 他のインターフェースに設定されている IP アドレスを使用することはできません。• 「自動取得」を選択した場合、IP アドレスを入力することはできません。
⑤	DNS アドレス	IP 接続の DNS サーバのアドレスを設定します。 <ul style="list-style-type: none">• プロバイダから DNS サーバのアドレスが与えられていないときは「自動取得」を、与えられているとき、または独自に指定するときは「手動設定」を選択します。• 「手動設定」を選択したときは、プロバイダから与えられたプライマリ DNS サーバの IP アドレスを上段に、セカンダリ DNS サーバの IP アドレスを下段に入力します。セカンダリは省略可能です。 注意 <ul style="list-style-type: none">• 「自動取得」を選択した場合、DNS アドレスを入力することはできません。
⑥	NAPT	NAPT の利用を設定します。 <ul style="list-style-type: none">• 通常は「有効」を選択します。• インターネットに直接接続せず、クローズドな環境で利用する場合は、「無効」を選択することができます。 注意 <ul style="list-style-type: none">• 特殊な環境で無い限りは、「有効」に設定してください。

4. 詳細設定

IPv6、PPPoE 接続の場合(フレッツ光回線利用の場合)

プロバイダの設定

プロバイダと接続するWAN側インタフェースを設定します。

	現在の設定	設定の変更
プロトコル		<input type="radio"/> IPv4 <input checked="" type="radio"/> IPv6
接続形態		<input checked="" type="radio"/> PPPoE接続 <input type="radio"/> IPoE接続

WAN1: PPPoE接続の設定(GigaEthernet0.1)

	現在の設定	設定の変更
接続名	WAN1	WAN1
ユーザ名		プロバイダから通知されているユーザ名を設定します。 (フレッツの場合、通常はユーザ名には@を含んでいます) ***
パスワード		プロバイダから通知されているパスワードを設定します。 ***
WAN側 IPv6アドレス		<input checked="" type="radio"/> 自動取得
DNSアドレス		<input checked="" type="radio"/> 自動取得 追加でDNSアドレスを設定することができます。省略可能です。 _____

番号	項目	内容
①	プロトコル	「IPv6」を選択します。
②	接続形態	「PPPoE接続」を選択します。
③	接続名	接続名を識別するための名称を入力します。 <ul style="list-style-type: none"> ・ 任意の接続名を付けることができます。 ・ 半角英数字で1～79文字まで入力できます。 ・ 初期値は「WAN1」です。
④	ユーザ名	プロバイダから通知されているユーザ名を設定します。 (フレッツの場合、通常はユーザ名には@を含んでいます) <ul style="list-style-type: none"> ・ 半角英数字で1～59文字まで入力できます。
⑤	パスワード	プロバイダから通知されているパスワードを設定します。 <ul style="list-style-type: none"> ・ 半角英数字で1～79文字まで入力できます。 <div style="border: 1px solid black; padding: 2px; margin-top: 5px;"> 注意 大文字、小文字も区別されます。 </div>
⑥	WAN側IPv6アドレス	WAN側IPv6アドレスは常に「自動取得」です。設定を変更することはできません。
⑦	DNSアドレス	PPPoE接続のDNSサーバのアドレスを設定します。「自動選択」の他、DNSサーバを追加することができます。

4. 詳細設定

IPv6、IP 接続の場合(ケーブルテレビ回線利用の場合)

プロバイダの設定

プロバイダと接続するWAN側インタフェースを設定します。

	現在の設定	設定の変更
プロトコル		<input type="radio"/> IPv4 <input checked="" type="radio"/> IPv6
接続形態		<input type="radio"/> PPPoE接続 <input checked="" type="radio"/> IPoE接続

IPv6プレフィックス取得設定

IPv6プレフィックスの取得方法を設定します。
「ひかり電話契約」があり、ひかり電話ルータのLAN側に装置を設置する場合「RA固定」を選択してください。

	現在の設定	設定の変更
プレフィックス取得方法		<input checked="" type="radio"/> PD/RA自動判別 <input type="radio"/> RA固定

WAN1: IPoE接続の設定(GigaEthernet0.0)

	現在の設定	設定の変更
接続名	WAN1	<input type="text" value="WAN1"/>
WAN側 IPv6アドレス		<input checked="" type="radio"/> 自動取得
DNSアドレス		<input checked="" type="radio"/> 自動取得 追加でDNSアドレスを設定することができます。省略可能です。 <input type="text"/> <input type="text"/>

番号	項目	内容
①	プロトコル	「IPv6」を選択します。
②	接続形態	「IPoE 接続」を選択します。
③	プレフィックス取得方法	RA 固定とPD/RA 自動判別のいずれかを選択します。
④	接続名	接続名を識別するための名称を入力します。 ・ 任意の接続名を付けることができます。 ・ 半角英数字で 1～79 文字まで入力できます。 ・ 初期値は「WAN1」です。
⑤	WAN 側 IPv6 アドレス	WAN 側 IPv6 アドレスは常に「自動取得」です。設定を変更することはできません。
⑥	DNS アドレス	PPPoE 接続の DNS サーバのアドレスを設定します。「自動選択」の他、DNS サーバを追加することができます。

4. 詳細設定

USB 接続の場合(3G・LTE 回線利用の場合)

※IX2215/IX2235/IX2310/IX3315のみ

プロバイダの設定

プロバイダと接続するWAN側インタフェースを設定します。

	現在の設定	設定の変更
プロトコル	IPv4	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
接続形態	USB接続	<input type="radio"/> PPPoE接続 (フレッツ光回線利用の場合) <input type="radio"/> IP接続 (ケーブルテレビ回線利用の場合) <input checked="" type="radio"/> USB接続 (3G・LTE回線利用の場合)

WAN1: USB接続の設定(USB-Serial0.0)

	現在の設定	設定の変更
接続名	WAN1	<input type="text" value="WAN1"/>
ユーザ名		プロバイダからユーザ名が指定されている場合に設定します。 <input type="text"/>
パスワード		プロバイダからパスワードが指定されている場合に設定します。 <input type="text"/>
PDPタイプ		プロバイダからPDPタイプが指定されている場合に設定します。 <input type="text" value="--"/>
APN		プロバイダからAPNが指定されている場合に設定します。 <input type="text"/>
WAN側IPアドレス	自動取得	<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
DNSアドレス	自動取得	<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
NAPT	有効	<input checked="" type="radio"/> 有効

4. 詳細設定

番号	項目	内容
①	プロトコル	「IPv4」を選択します。
②	接続形態	「USB 接続 (3G・LTE 回線利用の場合)」を選択します。
③	接続名	接続名を識別するための名称を入力します。 <ul style="list-style-type: none"> 任意の接続名を付けることができます。 半角英数字で 1～79 文字まで入力できます。 初期値は「WAN1」です。
④	ユーザ名	プロバイダからユーザ名が指定されている場合に設定します。 <ul style="list-style-type: none"> 半角英数字で 1～59 文字まで入力できます。
⑤	パスワード	プロバイダからパスワードが指定されている場合に設定します。 <ul style="list-style-type: none"> 半角英数字で 1～79 文字まで入力できます。 注意 大文字、小文字も区別されます。
⑥	PDP タイプ	プロバイダから PDP タイプが指定されている場合に設定します。
⑦	APN	プロバイダから APN が指定されている場合に設定します。 <ul style="list-style-type: none"> 半角英数字で 1～90 文字まで入力できます。
⑧	WAN 側 IP アドレス	USB 接続の WAN 側 IP アドレスを設定します。 <ul style="list-style-type: none"> プロバイダから WAN 側 IP アドレスが与えられていないときは「自動取得」を、固定 IP アドレスが与えられているときは「手動設定」を選択します。 「手動設定」を選択したときは、プロバイダから与えられた IP アドレスを入力し、サブネットマスクをプルダウンメニューから選択します。 注意 <ul style="list-style-type: none"> 他のインタフェースに設定されている IP アドレスを使用することはできません。 「自動取得」を選択した場合、IP アドレスを入力することはできません。
⑨	DNS アドレス	USB 接続の DNS サーバのアドレスを設定します。 <ul style="list-style-type: none"> プロバイダから DNS サーバのアドレスが与えられていないときは「自動取得」を、与えられているとき、または独自に指定するときは「手動設定」を選択します。 「手動設定」を選択したときは、プロバイダから与えられたプライマリ DNS サーバの IP アドレスを上段に、セカンダリ DNS サーバの IP アドレスを下段に入力します。セカンダリは省略可能です。 注意 <ul style="list-style-type: none"> 「自動取得」を選択した場合、DNS アドレスを入力することはできません。
⑩	NAPT	NAPT は常に有効です。設定を変更することはできません。

4. 詳細設定

(4) 設定が反映されたことを確認します。

プロバイダの設定

プロバイダと接続するWAN側インタフェースを設定します。

	現在の設定	設定の変更
プロトコル	IPv4	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
接続形態	USB接続	<input type="radio"/> PPPoE接続 (フレッツ光回線利用の場合) <input type="radio"/> IP接続 (ケーブルテレビ回線利用の場合) <input checked="" type="radio"/> USB接続 (3G・LTE回線利用の場合)

WAN1: USB接続の設定(USB-Serial0.0)

	現在の設定	設定の変更
接続名	WAN1	<input type="text" value="WAN1"/>
ユーザ名	user@example.com	プロバイダからユーザ名が指定されている場合に設定します。 <input type="text" value="user@example.com"/>
パスワード	user-password	プロバイダからパスワードが指定されている場合に設定します。 <input type="text" value="user-password"/>
PDPタイプ	ip	プロバイダからPDPタイプが指定されている場合に設定します。 <input type="text" value="IP"/>
APN	mopera.net	プロバイダからAPNが指定されている場合に設定します。 <input type="text" value="mopera.net"/>
WAN側IPアドレス	自動取得	<input checked="" type="radio"/> 自動取得 <input type="radio"/> 手動設定
DNSアドレス	手動設定 220.159.212.200 220.159.212.201	<input type="radio"/> 自動取得 <input checked="" type="radio"/> 手動設定 セカンダリは省略可能です。 <input type="text" value="220.159.212.200"/> (プライマリ) <input type="text" value="220.159.212.201"/> (セカンダリ)
NAPT	有効	<input checked="" type="radio"/> 有効

[詳細設定へ](#)

4. 詳細設定

4.3.2 静的NAPTの設定

WAN側インタフェースに静的NAPTを設定します。

設定するには、「プロバイダの設定」が必要です。

- (1) ログイン後のメニューエリアから[詳細設定]をクリックします。
- (2) 「WAN」の項目から[静的NAPTの設定]をクリックします。

<ul style="list-style-type: none">■管理者メニュー<ul style="list-style-type: none">トップページ設定の保存ログアウト■かんたん設定<ul style="list-style-type: none">かんたん設定■詳細設定<ul style="list-style-type: none">詳細設定基本設定<ul style="list-style-type: none">パスワードの設定装置名の設定時刻の設定保守の設定NetMeisterの設定ゼロタッチの設定LAN<ul style="list-style-type: none">LANアドレスの設定DHCPサーバの設定WAN<ul style="list-style-type: none">プロバイダの設定静的NAPTの設定WANフィルタの設定<ul style="list-style-type: none">・IPv4・IPv6URLフィルタリングの設定QoSの設定通信セキュリティの設定VPN・クラウド<ul style="list-style-type: none">VPNの設定L2TPの設定クラウドの設定NGN網VPN<ul style="list-style-type: none">NGN網VPNの設定デバイス<ul style="list-style-type: none">デバイスの設定UTM<ul style="list-style-type: none">基本設定詳細設定グループ別ポリシー設定ホワイトリスト設定UTM脅威レポート■端末管理<ul style="list-style-type: none">端末管理■保守管理<ul style="list-style-type: none">保守管理■拡張ページ<ul style="list-style-type: none">拡張ページ■外部リンク<ul style="list-style-type: none">製品ページ	<h3>詳細設定</h3> <p>本装置の詳細な設定を行います。 ルータの全ての設定を利用できるわけではありません。 個別に設定を変更する場合は任意コマンドの実行から操作してください。 本装置に接続された端末の制御は端末管理から操作してください。</p> <hr/> <h3>基本設定</h3> <p>本装置の基本的な設定を行います。 保守設定ではSSH、Telnet、SNMP、Syslog等を設定します。 また、NetMeisterやゼロタッチの設定をします。</p> <hr/> <h3>LAN</h3> <p>LAN側の設定を行います。 IPアドレス、DHCPサーバなどを設定します。</p> <hr/> <h3>WAN</h3> <p>WAN側の設定を行います。 プロバイダ設定ではインターネットの接続設定を行います。 QoS設定ではシェーピングとPQ制御を利用できます。 URLフィルタの設定ではサービス事業者の提供するURLリストやユーザが指定したURLをフィルタできます。</p> <hr/> <h3>VPN・クラウド</h3> <p>IPSecやダイナミックVPN、サービス事業者ごとのクラウド設定を行います。</p> <hr/> <h3>NGN網VPN</h3> <p>NGN-IPv6網を利用したVPNの設定を行います。</p> <hr/> <h3>デバイス</h3> <p>本装置の各デバイスの設定を行います。</p> <hr/> <h3>UTM</h3> <p>本装置のUTMの設定を行います。</p>
---	--

4. 詳細設定

(3) [追加]ボタンをクリックします。

(4) 各項目を設定し、[反映]ボタンをクリックします。

機能リストにない場合、ポート番号も変換が必要な場合は、「ポート番号指定」を選択してください。

機能リスト選択の場合

番号	項目	内容
①	設定方法	「機能リスト選択」を選択します。
②	機能リスト	外部公開するプロトコル・ポート番号を選択します。
③	プライベート側 IP アドレス	プライベート側端末のIPアドレスを設定します。 空欄にした場合、ルータがWAN側アドレスで受信します。

4. 詳細設定

ポート番号指定の場合

静的NAPTの設定

機能リストにない場合、ポート番号も変換が必要な場合は、「ポート番号指定」を選択して設定してください。
設定を追加する場合は [反映] を押してください。

WAN1(GigaEthernet0.1)

	現在の設定	設定の必要
設定方法		<input type="radio"/> 機能リスト選択 <input checked="" type="radio"/> ポート番号指定
NAPT名		任意の名称を設定してください。 同一名称の設定が既にある場合は、その設定を上書きします。 <input type="text"/> 文字列(半角英数字)を入力してください。
プロトコル		<input checked="" type="radio"/> TCP <input type="radio"/> UDP
ポート番号		外部に公開するポート番号を設定してください。 <input checked="" type="radio"/> ポート指定 <input type="radio"/> ポート範囲指定 <input type="text"/> 数字を入力してください。
プライベート側 IPアドレス		プライベート側端末のIPアドレスを設定してください。 <input type="text"/> IPアドレスを入力してください。
プライベート側ポート番号		プライベート側端末が使用するポート番号を設定してください。 アドレスだけ変換する場合は「変換なし」を選択してください。 <input checked="" type="radio"/> 変換なし <input type="radio"/> 変換する

番号	項目	内容
①	設定方法	「ポート番号指定」を選択します。
②	NAPT名	任意の名称を設定してください。 同一名称の設定が既にある場合は、その設定を上書きします。 ・ 半角英数字で1~31文字まで入力できます。
③	プロトコル	TCPかUDPを選択します。
④	ポート番号	外部に公開するポート番号を設定します。
⑤	プライベート側 IP アドレス	プライベート側端末のIPアドレスを設定します。
⑥	プライベート側ポート番号	プライベート側端末のポート番号を設定します。 アドレスだけ変換する場合は「変換なし」を選択してください。

4. 詳細設定

(5) 設定が追加されたことを確認します。

静的NAPTの設定

WAN側インタフェースの静的NAPTを設定します。

WAN1(GigaEthernet0.1)

NAPT名	WAN側		プライベート側	
	プロトコル	ポート番号	IPアドレス	ポート番号
Ping	icmp	-	GigaEthernet0.1	変更なし

削除 追加

4. 詳細設定

4.3.3 WAN フィルタの設定(Ver10.3 以降の機能)

WAN 側インタフェースのフィルタを設定します。

設定するには、「プロバイダの設定」が必要です。

透過を指定したフィルタを設定した場合、それ以外の通信はすべて廃棄されます。

Ver10.2 までに Web コンソールで設定した WAN フィルタが存在する場合と、存在しない場合で表示される設定画面が異なります。

本節では、Ver10.2 までの Web コンソールで設定した WAN フィルタが存在しない場合を記載しています。Ver10.3 以降の WAN フィルタ機能を使用する場合は、Ver10.2 までの WAN フィルタ機能で設定した内容をすべて削除してください。

本 WAN フィルタの説明では、IPv4 と IPv6 を併記しています。

- (1) ログイン後のメニューエリアから[詳細設定]をクリックします。
- (2) 「WAN」[WAN フィルタの設定]の項目から「IPv4」または「IPv6」をクリックします。

4. 詳細設定

<ul style="list-style-type: none">■ 管理者メニュー<ul style="list-style-type: none">トップページ設定の保存ログアウト■ かんたん設定<ul style="list-style-type: none">かんたん設定■ 詳細設定<ul style="list-style-type: none">詳細設定基本設定パスワードの設定装置名の設定時刻の設定保守の設定NetMeisterの設定ゼロタッチの設定LAN<ul style="list-style-type: none">LANアドレスの設定DHCPサーバの設定WAN<ul style="list-style-type: none">プロバイダの設定静的NAPTの設定WANフィルタの設定<ul style="list-style-type: none">・IPv4・IPv6URLフィルタリングの設定QoSの設定通信セキュリティの設定VPN・クラウド<ul style="list-style-type: none">VPNの設定L2TPの設定クラウドの設定NGN網VPN<ul style="list-style-type: none">NGN網VPNの設定デバイス<ul style="list-style-type: none">デバイスの設定UTM<ul style="list-style-type: none">基本設定詳細設定グループポリシー設定ホワイトリスト設定UTM脅威レポート■ 端末管理<ul style="list-style-type: none">端末管理■ 保守管理<ul style="list-style-type: none">保守管理■ 拡張ページ<ul style="list-style-type: none">拡張ページ■ 外部リンク<ul style="list-style-type: none">製品ページ	<h2>詳細設定</h2> <p>本装置の詳細な設定を行います。 ルータの全ての設定を利用できるわけではありません。 個別に設定を変更する場合は任意コマンドの発行から操作してください。 本装置に接続された端末の制御は端末管理から操作してください。</p> <h2>基本設定</h2> <p>本装置の基本的な設定を行います。 保守設定ではSSH、Telnet、SNMP、Syslog等を設定します。 また、NetMeisterやゼロタッチの設定をします。</p> <h2>LAN</h2> <p>LAN側の設定を行います。 IPアドレス、DHCPサーバなどを設定します。</p> <h2>WAN</h2> <p>WAN側の設定を行います。 プロバイダ設定ではインターネットの接続設定を行います。 QoS設定ではシェーピングとPQ制御を利用できます。 URLフィルタの設定ではサービス事業者の提供するURLリストやユーザが指定したURLをフィルタできます。</p> <h2>VPN・クラウド</h2> <p>IPSecやダイナミックVPN、サービス事業者ごとのクラウド設定を行います。</p> <h2>NGN網VPN</h2> <p>NGN-IPv6網を利用したVPNの設定を行います。</p> <h2>デバイス</h2> <p>本装置の各デバイスの設定を行います。</p> <h2>UTM</h2> <p>本装置のUTMの設定を行います。</p>
--	---

4. 詳細設定

(3) WAN フィルタを適用したい方向(受信/送信)およびログの記録(する/しない)の [追加] ボタンをクリックします。

☒ 受信フィルタを設定すると、パケット受信時にフィルタの評価を行い、送信フィルタを設定すると、パケット送信時にフィルタの評価を行います。

☒ 「ログの記録」は、設定したフィルタで廃棄したパケットのログの記録を表します。フィルタで廃棄したパケットのログを取得するときは「する」の項目から、フィルタで廃棄したパケットのログを取得しないときは「しない」の項目から追加してください。

記録した廃棄ログは、「保守管理」の「装置ログの取得」で確認、保存することができます。

WANフィルタの設定 (IPv4)

WAN側インタフェースのIPv4フィルタを設定します。
フィルタを設定すると、「透過」指定したものを以外は「廃棄」されます。

WAN1(GigaEthernet0.1) : 受信フィルタ

ログの記録：しない

番号	動作	プロトコル	送信元		送信先				
			IPアドレス	ポート番号	IPアドレス	ポート番号			
									追加

ログの記録：する

番号	動作	プロトコル	送信元		送信先				
			IPアドレス	ポート番号	IPアドレス	ポート番号			
									追加

WAN1(GigaEthernet0.1) : 送信フィルタ

ログの記録：しない

番号	動作	プロトコル	送信元		送信先				
			IPアドレス	ポート番号	IPアドレス	ポート番号			
									追加

ログの記録：する

番号	動作	プロトコル	送信元		送信先				
			IPアドレス	ポート番号	IPアドレス	ポート番号			
									追加

WANフィルタの設定 (IPv6)

WAN側インタフェースのIPv6フィルタを設定します。
フィルタを設定すると、「透過」指定したものを以外は「廃棄」されます。

WAN1(GigaEthernet0.1) : 受信フィルタ

ログの記録：しない

番号	動作	プロトコル	送信元		送信先				
			IPv6アドレス	ポート番号	IPv6アドレス	ポート番号			
									追加

ログの記録：する

番号	動作	プロトコル	送信元		送信先				
			IPv6アドレス	ポート番号	IPv6アドレス	ポート番号			
									追加

WAN1(GigaEthernet0.1) : 送信フィルタ

ログの記録：しない

番号	動作	プロトコル	送信元		送信先				
			IPv6アドレス	ポート番号	IPv6アドレス	ポート番号			
									追加

ログの記録：する

番号	動作	プロトコル	送信元		送信先				
			IPv6アドレス	ポート番号	IPv6アドレス	ポート番号			
									追加

4. 詳細設定

(4) 各項目を設定し、[反映]ボタンをクリックします。

WANフィルタの設定 (IPv4)

設定を追加する場合は [反映] を押してください。

WAN1(GigaEthernet0.1) : 受信フィルタ

現在の設定		設定の変更
シーケンス番号		100
動作		<input checked="" type="radio"/> 透過 <input type="radio"/> 廃棄
プロトコル		TCP
送信元	IPアドレス	<input checked="" type="radio"/> すべて <input type="radio"/> IPアドレス指定
	ポート番号	<input checked="" type="radio"/> すべて <input type="radio"/> ポート指定 <input type="radio"/> ポート範囲指定
送信先	IPアドレス	<input checked="" type="radio"/> すべて <input type="radio"/> IPアドレス指定
	ポート番号	<input checked="" type="radio"/> すべて <input type="radio"/> ポート指定 <input type="radio"/> ポート範囲指定

戻る **反映**

WANフィルタの設定 (IPv6)

設定を追加する場合は [反映] を押してください。

WAN1(GigaEthernet0.1) : 受信フィルタ

現在の設定		設定の変更
シーケンス番号		100
動作		<input checked="" type="radio"/> 透過 <input type="radio"/> 廃棄
プロトコル		TCP
送信元	IPv6 アドレス	<input checked="" type="radio"/> すべて <input type="radio"/> IPv6アドレス指定
	ポート番号	<input checked="" type="radio"/> すべて <input type="radio"/> ポート指定 <input type="radio"/> ポート範囲指定
送信先	IPv6 アドレス	<input checked="" type="radio"/> すべて <input type="radio"/> IPv6アドレス指定
	ポート番号	<input checked="" type="radio"/> すべて <input type="radio"/> ポート指定 <input type="radio"/> ポート範囲指定

戻る **反映**

4. 詳細設定

番号	項目	内容
①	シーケンス番号	フィルタのシーケンス番号を選択します。 <ul style="list-style-type: none"> 1～4294967295のシーケンス番号を設定することができます。 複数のフィルタを設定したときは、若い番号順にパケットのフィルタリングを行います。
②	動作	パケットに対する処理動作を「透過」／「廃棄」から選択します。
③	プロトコル	フィルタリング対象とするプロトコルをプルダウンメニューから選択します。 <ul style="list-style-type: none"> プロトコルは、[TCP]、[UDP]、[ICMP]、[すべて]、[任意のプロトコル番号]から選択します。 プルダウンメニューで[任意のプロトコル番号]を選択したときは、プロトコル番号(1～255)を入力します。
④	送信元 IP アドレス	フィルタリング対象とする送信元の IP アドレスを設定します。 <ul style="list-style-type: none"> すべての IP アドレスからのパケットに対してフィルタリングを行うときは、「すべて」を選択します。 特定の IP アドレスからのパケットに対してフィルタリングを行うときは、「IP アドレス指定」を選択し、IP アドレスを入力します。
⑤	送信元ポート番号	フィルタリング対象とする送信元のポート番号を設定します。 <ul style="list-style-type: none"> すべてのポート番号のパケットに対してフィルタリングを行うときは、「すべて」を選択します。 特定のポート番号のパケットに対してフィルタリングを行うときは、「ポート指定」あるいは「ポート範囲指定」を選択し、ポート番号を入力します。 <p>注意</p> <ul style="list-style-type: none"> プロトコルで[TCP]または[UDP]を選択した場合のみ、ポート番号の設定が有効です。
⑥	送信先 IP アドレス	フィルタリング対象とする送信先の IP アドレスを設定します。 <ul style="list-style-type: none"> すべての IP アドレスへのパケットに対してフィルタリングを行うときは、「すべて」を選択します。 特定の IP アドレスへのパケットに対してフィルタリングを行うときは、「IP アドレス指定」を選択し、IP アドレスを入力します。
⑦	送信先ポート番号	フィルタリング対象とする送信先のポート番号を設定します。 <ul style="list-style-type: none"> すべてのポート番号のパケットに対してフィルタリングを行うときは、「すべて」を選択します。 特定のポート番号のパケットに対してフィルタリングを行うときは、「ポート指定」あるいは「ポート範囲指定」を選択し、ポート番号を入力します。 <p>注意</p> <ul style="list-style-type: none"> プロトコルで[TCP]または[UDP]を選択した場合のみ、ポート番号の設定が有効です。

4. 詳細設定

- (5) 設定が追加されたことを確認します。

WANフィルタの設定 (IPv4)

WAN側インタフェースのIPv4フィルタを設定します。
フィルタを設定すると、「透過」指定したものの以外は「廃棄」されます。

WAN1(GigaEthernet0.1)：受信フィルタ

ログの記録：しない

番号	振り直し	動作	プロトコル	送信元		送信先			
				IPアドレス	ポート番号	IPアドレス	ポート番号		
100		透過	TCP	すべて	すべて	すべて	すべて	変更	削除

追加

ログの記録：する

番号	動作	プロトコル	送信元		送信先			
			IPアドレス	ポート番号	IPアドレス	ポート番号		

追加

WAN1(GigaEthernet0.1)：送信フィルタ

ログの記録：しない

番号	動作	プロトコル	送信元		送信先			
			IPアドレス	ポート番号	IPアドレス	ポート番号		

追加

ログの記録：する

番号	動作	プロトコル	送信元		送信先			
			IPアドレス	ポート番号	IPアドレス	ポート番号		

追加

WANフィルタの設定 (IPv6)

WAN側インタフェースのIPv6フィルタを設定します。
フィルタを設定すると、「透過」指定したものの以外は「廃棄」されます。

WAN1(GigaEthernet0.1)：受信フィルタ

ログの記録：しない

番号	振り直し	動作	プロトコル	送信元		送信先			
				IPv6アドレス	ポート番号	IPv6アドレス	ポート番号		
100		透過	TCP	すべて	すべて	すべて	すべて	変更	削除

追加

ログの記録：する

番号	動作	プロトコル	送信元		送信先			
			IPv6アドレス	ポート番号	IPv6アドレス	ポート番号		

追加

WAN1(GigaEthernet0.1)：送信フィルタ

ログの記録：しない

番号	動作	プロトコル	送信元		送信先			
			IPv6アドレス	ポート番号	IPv6アドレス	ポート番号		

追加

ログの記録：する

番号	動作	プロトコル	送信元		送信先			
			IPv6アドレス	ポート番号	IPv6アドレス	ポート番号		

追加

4. 詳細設定

4.3.4 WAN フィルタの設定(Ver10.2 までの設定がある場合)

WAN 側インタフェースの IPv4 フィルタを設定します。

メモ Ver10.2 までに Web コンソールで設定した WAN フィルタが存在する場合と、存在しない場合で表示される設定画面が異なります。

本節では、Ver10.2 までに Web コンソールで設定した WAN フィルタが存在する場合を記載しています。Ver10.3 以降の WAN フィルタ機能を使用する場合は、Ver10.2 までに設定した WAN フィルタの内容をすべて削除し、Ver10.3 以降の WAN フィルタ機能で再設定してください。

メモ 設定するには、「プロバイダの設定」が必要です。

メモ 透過を指定したフィルタを設定した場合、それ以外の通信はすべて廃棄されます。

- (1) ログイン後のメニューエリアから[詳細設定]をクリックします。
- (2) 「WAN」 [WAN フィルタの設定]の項目から「IPv4」をクリックします。

4. 詳細設定

■ 管理者メニュー	詳細設定
トップページ	本装置の詳細な設定を行います。
設定の保存	ルータの全ての設定を利用できるわけではありません。
ログアウト	個別に設定を変更する場合は任意コマンドの実行から操作してください。
■ かんたん設定	本装置に接続された端末の制御は 端末管理 から操作してください。
かんたん設定	
■ 詳細設定	基本設定
詳細設定	本装置の基本的な設定を行います。
基本設定	保守設定ではSSH、Telnet、SNMP、Syslog等を設定します。
パスワードの設定	また、NetMeisterやゼロタッチの設定をします。
装置名の設定	
時刻の設定	LAN
保守の設定	LAN側の設定を行います。
NetMeisterの設定	IPアドレス、DHCPサーバなどを設定します。
ゼロタッチの設定	
LAN	WAN
LANアドレスの設定	WAN側の設定を行います。
DHCPサーバの設定	プロバイダ設定ではインターネットの接続設定を行います。
WAN	QoS設定ではシェーピングとPQ制御を利用できます。
プロバイダの設定	URLフィルタの設定ではサービス事業者の提供するURLリストや
静的NAPTの設定	ユーザが指定したURLをフィルタできます。
WANフィルタの設定	
IPv4	VPN・クラウド
IPv6	IPSecやダイナミックVPN、サービス事業者ごとのクラウド設定を行います。
URLフィルタリングの設定	
QoSの設定	NGN網VPN
通信セキュリティの設定	NGN-IPv6網を利用したVPNの設定を行います。
VPN・クラウド	
VPNの設定	デバイス
L2TPの設定	本装置の各デバイスの設定を行います。
クラウドの設定	
NGN網VPN	UTM
NGN網VPNの設定	本装置のUTMの設定を行います。
デバイス	
デバイスの設定	
UTM	
基本設定	
詳細設定	
グループ別ポリシー設定	
ホワイトリスト設定	
UTM脅威レポート	
■ 端末管理	
端末管理	
■ 保守管理	
保守管理	
■ 拡張ページ	
拡張ページ	
■ 外部リンク	
製品ページ	

4. 詳細設定

- (3) Ver10.2 までに作成した WAN フィルタをすべて削除したい場合は、[設定の全削除]をクリックします。

☒ 全削除を実行した場合、Ver10.3 以降の WAN フィルタの設定 (IPv4) 画面に自動的に移行し、Ver10.3 以降の WAN フィルタ機能を利用できるようになります。

WANフィルタの設定 (IPv4)

WAN側インタフェースのIPv4フィルタを設定します。
フィルタを設定すると、「透過」指定したものの以外は「廃棄」されます。

バージョン10.3で新たに実装されたWANフィルタの設定を使用するには、現在の設定を全て削除する必要があります。

設定の全削除

WAN1(GigaEthernet0.1) : 受信フィルタ

番号	動作	プロトコル	送信元		送信先		ログの記録
			IPアドレス	ポート番号	IPアドレス	ポート番号	
1	<input type="button" value="変更"/> <input type="button" value="削除"/>	透過	TCP	すべて	すべて	すべて	✓

WAN1(GigaEthernet0.1) : 送信フィルタ

番号	動作	プロトコル	送信元		送信先		ログの記録
			IPアドレス	ポート番号	IPアドレス	ポート番号	
1	<input type="button" value="変更"/> <input type="button" value="削除"/>	透過	TCP	すべて	すべて	すべて	✓

WANフィルタの設定 (IPv4)

現在の設定を全て削除する場合は [全て削除する] を押してください。

全て削除する

- (4) 既に設定済みの WAN フィルタに設定を追加する場合、WAN フィルタを適用したい方向(受信/送信)の[追加]ボタンをクリックします。

☒ 受信フィルタを設定すると、パケット受信時にフィルタの評価を行い、送信フィルタを設定すると、パケット送信時にフィルタの評価を行います。

WANフィルタの設定 (IPv4)

WAN側インタフェースのIPv4フィルタを設定します。
フィルタを設定すると、「透過」指定したものの以外は「廃棄」されます。

バージョン10.3で新たに実装されたWANフィルタの設定を使用するには、現在の設定を全て削除する必要があります。

設定の全削除

WAN1(GigaEthernet0.1) : 受信フィルタ

番号	動作	プロトコル	送信元		送信先		ログの記録
			IPアドレス	ポート番号	IPアドレス	ポート番号	
1	<input type="button" value="変更"/> <input type="button" value="削除"/>	透過	TCP	すべて	すべて	すべて	✓

追加

WAN1(GigaEthernet0.1) : 送信フィルタ

番号	動作	プロトコル	送信元		送信先		ログの記録
			IPアドレス	ポート番号	IPアドレス	ポート番号	
1	<input type="button" value="変更"/> <input type="button" value="削除"/>	透過	TCP	すべて	すべて	すべて	✓

追加

4. 詳細設定

(5) 各項目を設定し、[反映]ボタンをクリックします。

WANフィルタの設定 (IPv4)

設定を追加する場合は [反映] を押してください。

WAN1(GigaEthernet0.1) : 受信フィルタ

現在の設定		設定の変更
シーケンス番号		2
動作		<input checked="" type="radio"/> 透過 <input type="radio"/> 廃棄
プロトコル		TCP
送信元	IPアドレス	<input checked="" type="radio"/> すべて <input type="radio"/> IPアドレス指定
	ポート番号	<input checked="" type="radio"/> すべて <input type="radio"/> ポート指定 <input type="radio"/> ポート範囲指定
送信先	IPアドレス	<input checked="" type="radio"/> すべて <input type="radio"/> IPアドレス指定
	ポート番号	<input checked="" type="radio"/> すべて <input type="radio"/> ポート指定 <input type="radio"/> ポート範囲指定
ログの記録		<input checked="" type="radio"/> 記録する (✓) <input type="radio"/> 記録しない

戻る **反映**

4. 詳細設定

番号	項目	内容
①	シーケンス番号	フィルタの番号を選択します。 <ul style="list-style-type: none"> 番号 1～32 の 32 種類のフィルタを設定することができます。 複数のフィルタを設定したときは、若い番号順にパケットのフィルタリングを行います。
②	動作	パケットに対する処理動作を「透過」／「廃棄」から選択します。
③	プロトコル	フィルタリング対象とするプロトコルをプルダウンメニューから選択します。 <ul style="list-style-type: none"> プロトコルは、[TCP]、[UDP]、[ICMP]、[すべて]、[任意のプロトコル番号]から選択します。 プルダウンメニューで[任意のプロトコル番号]を選択したときは、プロトコル番号(1～255)を入力します。
④	送信元 IP アドレス	フィルタリング対象とする送信元の IP アドレスを設定します。 <ul style="list-style-type: none"> すべての IP アドレスからのパケットに対してフィルタリングを行うときは、「すべて」を選択します。 特定の IP アドレスからのパケットに対してフィルタリングを行うときは、「IP アドレス指定」を選択し、IP アドレスを入力します。
⑤	送信元ポート番号	フィルタリング対象とする送信元のポート番号を設定します。 <ul style="list-style-type: none"> すべてのポート番号のパケットに対してフィルタリングを行うときは、「すべて」を選択します。 特定のポート番号のパケットに対してフィルタリングを行うときは、「ポート指定」あるいは「ポート範囲指定」を選択し、ポート番号を入力します。 <p>注意</p> <ul style="list-style-type: none"> プロトコルで[TCP]または[UDP]を選択した場合のみ、ポート番号の設定が有効です。
⑥	送信先 IP アドレス	フィルタリング対象とする送信先の IP アドレスを設定します。 <ul style="list-style-type: none"> すべての IP アドレスへのパケットに対してフィルタリングを行うときは、「すべて」を選択します。 特定の IP アドレスへのパケットに対してフィルタリングを行うときは、「IP アドレス指定」を選択し、IP アドレスを入力します。
⑦	送信先ポート番号	フィルタリング対象とする送信先のポート番号を設定します。 <ul style="list-style-type: none"> すべてのポート番号のパケットに対してフィルタリングを行うときは、「すべて」を選択します。 特定のポート番号のパケットに対してフィルタリングを行うときは、「ポート指定」あるいは「ポート範囲指定」を選択し、ポート番号を入力します。 <p>注意</p> <ul style="list-style-type: none"> プロトコルで[TCP]または[UDP]を選択した場合のみ、ポート番号の設定が有効です。
⑧	ログの記録	設定したフィルタで廃棄したパケットのログの取得有効/無効を設定します。 <ul style="list-style-type: none"> フィルタで廃棄したパケットのログを取得するときは、「記録する」を選択します。 フィルタで廃棄したパケットのログを取得しないときは、「記録しない」を選択します。 記録した廃棄ログは、「保守管理」の「装置ログの取得」で確認、保存することができます。

4. 詳細設定

(5) 設定が追加されたことを確認します。





WANフィルタの設定 (IPv4)

WAN側インタフェースのIPv4フィルタを設定します。
フィルタを設定すると、「透過」指定したものを以外は「廃棄」されます。

バージョン10.3で新たに実装されたWANフィルタの設定を使用するには、現在の設定を全て削除する必要があります。





[設定の全削除](#)

WAN1(GigaEthernet0.1) : 受信フィルタ

番号	動作	プロトコル	送信元		送信先		ログの記録	
			IPアドレス	ポート番号	IPアドレス	ポート番号		
1	変更 削除	透過	TCP	   	すべて	すべて	すべて	✓
2	変更 削除	透過	TCP	すべて	すべて	すべて	すべて	✓

[追加](#)

WAN1(GigaEthernet0.1) : 送信フィルタ

番号	動作	プロトコル	送信元		送信先		ログの記録	
			IPアドレス	ポート番号	IPアドレス	ポート番号		
1	変更 削除	透過	TCP	すべて	すべて	   	すべて	✓

[追加](#)

4. 詳細設定

4.3.5 URL フィルタの設定

URL フィルタリング機能を実現するため、WAN 側インタフェースの URL フィルタの設定で行います。(以降、URL フィルタと記載します)

- 設定するには、「プロバイダの設定」が必要です。
- 廃棄を指定したフィルタを設定した場合、それ以外の通信はすべて透過されます。
- URL フィルタを設定すると、端末からの http、https パケット受信時に URL フィルタの評価を行います。
- 内部 URL フィルタと外部 URL フィルタを同時に利用した場合、内部 URL フィルタが優先されます。

- (1) ログイン後のメニューエリアから[詳細設定]をクリックします。
- (2) 「WAN」の項目から[URL フィルタリングの設定]をクリックします。

4. 詳細設定

■ 管理者メニュー	詳細設定
トップページ	本装置の詳細な設定を行います。
設定の保存	ルータの全ての設定を利用できるわけではありません。
ログアウト	個別に設定を変更する場合は 任意コマンドの実行 から操作してください。
■ かんたん設定	本装置に接続された端末の制御は 端末管理 から操作してください。
かんたん設定	
■ 詳細設定	基本設定
詳細設定	本装置の基本的な設定を行います。
基本設定	保守設定ではSSH、Telnet、SNMP、Syslog等を設定します。
パスワードの設定	また、NetMeisterやゼロタッチの設定をします。
装置名の設定	
時刻の設定	
保守の設定	
NetMeisterの設定	
ゼロタッチの設定	
LAN	LAN
LANアドレスの設定	LAN側の設定を行います。
DHCPサーバの設定	IPアドレス、DHCPサーバなどを設定します。
WAN	WAN
プロバイダの設定	WAN側の設定を行います。
静的NAPTの設定	プロバイダ設定ではインターネットの接続設定を行います。
WANフィルタの設定	QoS設定ではシェーピングとPQ制御を利用できます。
・IPv4	URLフィルタの設定ではサービス事業者の提供するURLリストや
・IPv6	ユーザが指定したURLをフィルタできます。
URLフィルタリングの設定	VPN・クラウド
QoSの設定	IPSecやダイナミックVPN、サービス事業者ごとのクラウド設定を行います。
通信セキュリティの設定	NGN網VPN
VPN・クラウド	NGN-IPv6網を利用したVPNの設定を行います。
VPNの設定	
L2TPの設定	デバイス
クラウドの設定	本装置の各デバイスの設定を行います。
NGN網VPN	
NGN網VPNの設定	UTM
デバイス	本装置のUTMの設定を行います。
デバイスの設定	
UTM	
基本設定	
詳細設定	
グループ別ポリシー設定	
ホワイトリスト設定	
UTM脅威レポート	
■ 端末管理	
端末管理	
■ 保守管理	
保守管理	
■ 拡張ページ	
拡張ページ	
■ 外部リンク	
製品ページ	

4. 詳細設定

- (3) 内部 URL フィルタを利用する場合は、内部 URL フィルタの[変更]ボタンをクリックします。

URLフィルタの設定

基本設定

URLフィルタの基本設定を行います。

	現在の設定
インターフェース	WAN1: GigaEthernet0.1
外部URLフィルタ	無効
MACアドレス	00:00:00:00:00:00

[変更](#)

対象範囲の設定

URLフィルタの対象外とする端末のIPアドレスを設定します。

	現在の設定
対象外端末	

[変更](#)

内部URLフィルタ

ドメイン名やIPアドレス形式で指定したURLの透過・廃棄を行います。

番号	動作	現在の設定
----	----	-------

[変更](#)

4. 詳細設定

(4) 各項目を設定し、[追加]ボタンをクリックします。

メモ 内部 URL フィルタを利用しない場合は、内部 URL フィルタの変更は不要です。

URLフィルタリングの設定

内部URLフィルタの設定

現在の設定内容を表示します。

全選択 全解除

選択	番号	動作	ドメイン名 または IPv4アドレス形式

追加

既定した位置に条件を挿入します。以下の例を参考に設定してください。
www.example.com, *example.com, *example, 192.168.1.1, 192.168.1.0/24
IPv4アドレス形式をすべてブロックする場合は 0.0.0.0/0、全通信を対象とする場合は any です。

番号	動作	ドメイン名 または IPv4アドレス形式
1	*廃棄 ○透過	

削除

選択した設定を削除します。

番号	項目	内容
①	番号	フィルタの番号を選択します。 <ul style="list-style-type: none">1 から順に割り当てられます。現在の設定内容と同じ番号を選択した場合は、新たに追加した内容をその順番に挿入します。
②	動作	該当の URL に対する処理動作を「透過」／「廃棄」から選択します。
③	ドメイン名 または IPv4 アドレス形式	フィルタリング対象とする宛先のドメイン名または IPv4 アドレスを設定します。 <ul style="list-style-type: none">カンマで区切って、複数設定することができます。その場合、[追加]ボタンをクリックすると、複数の番号で追加されます。

4. 詳細設定

- (5) メニューエリアから[詳細設定]の[URLフィルタの設定]をクリックし、設定が追加されたことを確認します。

URLフィルタの設定

基本設定

URLフィルタの基本設定を行います。

	現在の設定
インターフェース	WAN1: GigaEthernet0.1
外部URLフィルタ	無効
MACアドレス	00:11:22:33:44:55

対象範囲の設定

URLフィルタの対象外とする端末のIPアドレスを設定します。

	現在の設定
対象外端末	

内部URLフィルタ

ドメイン名やIPアドレス形式で指定したURLの透過・廃棄を行います。

番号	動作	現在の設定
1	廃棄	www.example.com

- (6) 端末から URL をアクセスしようとした際、URL フィルタで廃棄された場合は、端末側の画面に以下のようなブロック画面が表示されます。

- http によるアクセス時のみブロック画面が表示され、https によるアクセス時はブロック画面が表示されずタイムアウトになります。
- ブロック画面は、お客様の環境に合わせ、拡張ページ機能を利用してカスタマイズすることができます。

URLフィルタリング : ブロック画面

URLフィルタリング

このサイトは、フィルタリング対象のため閲覧できません。

URL: http://www.example.com

4. 詳細設定

4.3.6 QoSの設定

QoSを設定します。

設定するには、「プロバイダの設定」が必要です。

- (1) ログイン後のメニューエリアから[詳細設定]をクリックします。
- (2) 「WAN」の項目から[QoSの設定]をクリックします。

<ul style="list-style-type: none">■ 管理者メニュー<ul style="list-style-type: none">トップページ設定の保存ログアウト■ かんたん設定<ul style="list-style-type: none">かんたん設定■ 詳細設定<ul style="list-style-type: none">詳細設定基本設定<ul style="list-style-type: none">パスワードの設定装置名の設定時刻の設定保守の設定NetMeisterの設定ゼロタッチの設定LAN<ul style="list-style-type: none">LANアドレスの設定DHCPサーバの設定WAN<ul style="list-style-type: none">プロバイダの設定静的NAPTの設定WANフィルタの設定<ul style="list-style-type: none">・IPv4・IPv6URLフィルタリングの設定<ul style="list-style-type: none">QoSの設定通信セキュリティの設定VPN・クラウド<ul style="list-style-type: none">VPNの設定L2TPの設定クラウドの設定NGN網VPN<ul style="list-style-type: none">NGN網VPNの設定デバイス<ul style="list-style-type: none">デバイスの設定UTM<ul style="list-style-type: none">基本設定詳細設定グループ別ポリシー設定ホワイトリスト設定UTM脅威レポート■ 端末管理<ul style="list-style-type: none">端末管理■ 保守管理<ul style="list-style-type: none">保守管理■ 拡張ページ<ul style="list-style-type: none">拡張ページ■ 外部リンク<ul style="list-style-type: none">製品ページ	<h3>詳細設定</h3> <hr/> <p>本装置の詳細な設定を行います。 ルータの全ての設定を利用できるわけではありません。 個別に設定を変更する場合は任意コマンドの実行から操作してください。 本装置に接続された端末の制御は端末管理から操作してください。</p> <h3>基本設定</h3> <hr/> <p>本装置の基本的な設定を行います。 保守設定ではSSH、Telnet、SNMP、Syslog等を設定します。 また、NetMeisterやゼロタッチの設定をします。</p> <h3>LAN</h3> <hr/> <p>LAN側の設定を行います。 IPアドレス、DHCPサーバなどを設定します。</p> <h3>WAN</h3> <hr/> <p>WAN側の設定を行います。 プロバイダ設定ではインターネットの接続設定を行います。 QoS設定ではシェーピングとPQ制御を利用できます。 URLフィルタの設定ではサービス事業者の提供するURLリストやユーザが指定したURLをフィルタできます。</p> <h3>VPN・クラウド</h3> <hr/> <p>IPSecやダイナミックVPN、サービス事業者ごとのクラウド設定を行います。</p> <h3>NGN網VPN</h3> <hr/> <p>NGN-IPv6網を利用したVPNの設定を行います。</p> <h3>デバイス</h3> <hr/> <p>本装置の各デバイスの設定を行います。</p> <h3>UTM</h3> <hr/> <p>本装置のUTMの設定を行います。</p>
---	--

4. 詳細設定

(3) QoS 設定の「有効」 / 「無効」を設定します。

QoSの設定

QoSによる通信制御を設定します。

	現在の設定	設定の変更
QoS設定	無効	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効

番号	項目	内容
①	QoS 設定	QoS 設定の「有効」 / 「無効」を設定します。

(4) QoS 設定の「有効」を設定した場合、PQ の設定およびインターフェースシェーピングの設定が表示されます。

QoSの設定

QoSによる通信制御を設定します。

	現在の設定	設定の変更
QoS設定	無効	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効

PQの設定

優先度による通信制御の設定を表示します。
設定を変更する場合は「変更」を押してください。
「*」は、任意の値を示します。

high (qos-high)

プロトコル	送信元	送信先	その他
条件が設定されていません。			

medium (qos-medium)

プロトコル	送信元	送信先	その他
条件が設定されていません。			

normal (qos-normal)

プロトコル	送信元	送信先	その他
条件が設定されていません。			

low

プロトコル	送信元	送信先	その他
条件が設定されていません。			

インターフェースシェーピングの設定

WANインターフェースの帯域を設定します。

	現在の設定	設定の変更
シェーピング設定	無効	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効

4. 詳細設定

- (5) プライオリティキューイングによる優先制御(PQ)を設定する場合は、PQの設定の[変更]ボタンをクリックします。

PQ を利用しない場合は、PQ の設定の変更は不要です。

QoSの設定

QoSによる通信制御を設定します。

	現在の設定	設定の変更
QoS設定	無効	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効

PQの設定

優先度による通信制御の設定を表示します。
設定を変更する場合は「変更」を押してください。
「*」は、任意の値を示します。

high (qos-high)

プロトコル	送信元	送信先	その他
条件が設定されていません。			

medium (qos-medium)

プロトコル	送信元	送信先	その他
条件が設定されていません。			

normal (qos-normal)

プロトコル	送信元	送信先	その他
条件が設定されていません。			

low

プロトコル	送信元	送信先	その他
条件が設定されていません。			

インターフェースシェーピングの設定

WANインターフェースの帯域を設定します。

	現在の設定	設定の変更
シェーピング設定	無効	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効

4. 詳細設定

(6) 各項目を設定し、[追加]ボタンをクリックします。

PQ を利用しない場合は、PQ の設定の変更は不要です。

The screenshot displays the 'QoSの設定' (QoS Settings) page. It is divided into two main sections: 'PQの設定' (PQ Settings) and 'PQ設定の追加' (Add PQ Settings). The 'PQの設定' section contains four tables for different priority levels: 'high (qos-high)', 'medium (qos-medium)', 'normal (qos-normal)', and 'low'. Each table has columns for '選択' (Select), 'プロトコル' (Protocol), '送信元' (Source), '送信先' (Destination), and 'その他' (Other). The 'high' and 'low' tables show '条件が設定されています。' (Conditions are set), while the 'medium' and 'normal' tables show '条件が設定されていません。' (Conditions are not set). A '削除' (Delete) button is located to the right of the 'low' table. The 'PQ設定の追加' section has a sub-header '優先度と通信の条件を指定して「追加」をクリックしてください。' (Specify priority and communication conditions and click 'Add'). Below this is a form with fields for '優先度' (Priority) set to '高' (High), 'プロトコル' (Protocol) set to 'すべて' (All), '送信元' (Source) with an 'IPアドレス' (IP Address) field set to 'すべて' (All) and a radio button for '指定' (Specify), and '送信先' (Destination) with an 'IPアドレス' (IP Address) field set to 'すべて' (All) and a radio button for '指定' (Specify). There are also radio buttons for 'なし' (None), 'Precedence', and 'ToS'. A '変更' (Change) button and an '追加' (Add) button are at the bottom right. The '追加' button is highlighted with a red box.

4. 詳細設定

番号	項目	内容
①	優先度	<p>パケット送信の優先度をプルダウンメニューから選択します。</p> <ul style="list-style-type: none"> 優先度は、[high]、[medium]、[normal]から選択します。 <p>メモ [high]、[medium]、[normal]のいずれにも設定されていないパケットは、[low]の優先度で制御されます。</p>
②	プロトコル	<p>プロトコルをプルダウンメニューから選択します。</p> <ul style="list-style-type: none"> プロトコルは、[すべて]、[TCP]、[UDP]、[ICMP]、[指定]から選択します。 [すべて]を選択した場合、すべてのプロトコルが対象となります。 [TCP]を選択した場合、TCP が対象となり、送信元および送信先にポート番号を指定できる画面が表示されます。 [UDP]を選択した場合、UDP が対象となり、送信元および送信先にポート番号を指定できる画面が表示されます。 [ICMP]を選択した場合、ICMP が対象となります。 [指定]を選択した場合は、入力ボックスが表示され、プロトコル番号を指定することができます。
③	送信元アドレス 送信元ポート	<p>送信元の IPv4 アドレスを設定します。</p> <ul style="list-style-type: none"> IPv4 アドレスは、[すべて]、[指定]から選択します。 [すべて]を選択した場合、すべての IPv4 アドレスが対象となります。 [指定]を選択した場合、ネットワークアドレスを入力するボックスが表示されるため、XXX.XXX.XXX.XXX/XX 形式でネットワークアドレスを入力します。 <p>送信元ポートの入力ボックスは必要に応じて表示されます。</p> <ul style="list-style-type: none"> ポートは、[すべて]、[指定]、[範囲指定]から選択します。 [すべて]を選択した場合、すべてのポートが対象となります。 [指定]を選択した場合、ポート番号を入力するボックスが表示されるため、そのボックスでポート番号を指定します。 [範囲指定]を選択した場合は、ポート番号の範囲を指定するボックスが表示され、ポート番号の範囲を指定することができます。
④	送信先アドレス 送信先ポート	<p>送信先の IPv4 アドレスを設定します。</p> <ul style="list-style-type: none"> IPv4 アドレスは、[すべて]、[指定]から選択します。 [すべて]を選択した場合、すべての IPv4 アドレスが対象となります。 [指定]を選択した場合、ネットワークアドレスを入力するボックスが表示されるため、XXX.XXX.XXX.XXX/XX 形式でネットワークアドレスを入力します。 <p>送信先ポートの入力ボックスは必要に応じて表示されます。</p> <ul style="list-style-type: none"> ポートは、[すべて]、[指定]、[範囲指定]から選択します。 [すべて]を選択した場合、すべてのポートが対象となります。 [指定]を選択した場合、ポート番号を入力するボックスが表示されるため、そのボックスでポート番号を指定します。 [範囲指定]を選択した場合は、ポート番号の範囲を指定するボックスが表示され、ポート番号の範囲を指定することができます。
⑤	ToS	<p>対象となる ToS 値を設定します。</p> <ul style="list-style-type: none"> ToS 値は、[なし]、[Precedence]、[DSCP]から選択します。 [なし]を選択した場合、ToS 値を判定の対象外にします。 [Precedence]を選択した場合、Precedence 値を入力するボックスが表示されるため、数値で Precedence 値を入力します。 [DSCP]を選択した場合は、入力ボックスが表示され、数値で DSCP 値を入力することができます。

4. 詳細設定

- (7) PQ の設定の画面にもどり、設定が反映されたことを確認した後、[戻る]ボタンをクリックします。

QoSの設定

PQの設定

設定された条件に該当する通信を優先度で制御します。
条件設定を削除するにはチェックボックスを選択して [削除] を押してください。

high (qos-high)

選択	プロトコル	送信元	送信先	その他
<input type="checkbox"/>	*			*

medium (qos-medium)

選択	プロトコル	送信元	送信先	その他
<input type="checkbox"/>				
条件が設定されていません。				

normal (qos-normal)

選択	プロトコル	送信元	送信先	その他
<input type="checkbox"/>				
条件が設定されていません。				

low

選択	プロトコル	送信元	送信先	その他
<input type="checkbox"/>	*	*	*	*

PQ設定の追加

優先度と通信の条件を指定して [追加] を押してください。

優先度	プロトコル	送信元	送信先	ToS
high	すべて	IPアドレス: <input checked="" type="radio"/> すべて <input type="radio"/> 指定	IPアドレス: <input checked="" type="radio"/> すべて <input type="radio"/> 指定	<input checked="" type="radio"/> なし <input type="radio"/> Precedence <input type="radio"/> DSCP

4. 詳細設定

(8) QoS の設定の画面にもどり、設定が反映されていることを確認します。

QoSの設定

QoSによる通信制御を設定します。

	現在の設定	設定の変更
QoS設定	有効	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効

PQの設定

優先度による通信制御の設定を表示します。
設定を変更する場合は「変更」を押してください。
[*]は、任意の値を示します。

high (qos-high)

プロトコル	送信元	送信先	その他
*	192.168.0.0/24	192.168.0.0/24	*

medium (qos-medium)

プロトコル	送信元	送信先	その他
条件が設定されていません。			

normal (qos-normal)

プロトコル	送信元	送信先	その他
条件が設定されていません。			

low

プロトコル	送信元	送信先	その他
*	*	*	*

インターフェースシーピングの設定

WANインターフェースの帯域を設定します。

	現在の設定	設定の変更
シーピング設定	無効	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効

4. 詳細設定

- (9) インタフェースシェーピングを設定する場合は、シェーピング設定の「無効」／「有効」を設定し、[反映]ボタンをクリックします。

インタフェースシェーピングを利用しない場合は、インタフェースシェーピングの設定は不要です。

QoSの設定

PQの設定

設定された条件に該当する通信を優先度で制御します。
条件設定を削除するにはチェックボックスを選択して [削除] を押してください。

high (qos-high)

選択	プロトコル	送信元	送信先	その他
<input type="checkbox"/>	*	*

medium (qos-medium)

選択	プロトコル	送信元	送信先	その他
条件が設定されていません。				

normal (qos-normal)

選択	プロトコル	送信元	送信先	その他
条件が設定されていません。				

low

選択	プロトコル	送信元	送信先	その他
*	*	*	*	*

PQ設定の追加

優先度と通信の条件を指定して [追加] を押してください。

優先度	プロトコル	送信元	送信先	ToS
high	すべて	IPアドレス: * すべて ○ 指定	IPアドレス: * すべて ○ 指定	<input checked="" type="radio"/> なし <input type="radio"/> Precedence <input type="radio"/> DSCP

番号	項目	内容
①	シェーピング設定	シェーピング設定の「有効」／「無効」を設定します。

4. 詳細設定

(10) シェーピング設定の「有効」を設定した場合、シェーピングの詳細設定が表示されます。

QoSの設定

QoSによる通信制御を設定します。

	現在の設定	設定の変更
QoS設定	有効	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効

PQの設定

優先度による通信制御の設定を表示します。
設定を変更する場合は「変更」を押してください。
「*」は、任意の値を示します。

high (qos-high)

プロトコル	送信元	送信先	その他
*			*

medium (qos-medium)

プロトコル	送信元	送信先	その他
条件が設定されていません。			

normal (qos-normal)

プロトコル	送信元	送信先	その他
条件が設定されていません。			

low

プロトコル	送信元	送信先	その他
*	*	*	*

インターフェースシェーピングの設定

WANインターフェースの帯域を設定します。

	現在の設定	設定の変更
シェーピング設定	無効	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
帯域	-	<input style="width: 100px;" type="text"/> <small>数字を入力してください。</small> <input checked="" type="radio"/> Mbps <input type="radio"/> Kbps <input type="radio"/> bps

番号	項目	内容
①	シェーピング設定	シェーピング設定の「有効」 / 「無効」を設定します。
②	帯域	帯域を数値で入力します。 ・ 単位を、[Mbps]、[Kbps]、[bps]から選択します。

4. 詳細設定

- (11) 「設定内容を変更しました。」のメッセージと、設定が反映されたことを確認します。

QoSの設定

設定内容を変更しました。

	現在の設定	設定の変更
QoS設定	有効	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効

PQの設定

high (qos-high)

プロトコル	送信元	送信先	その他
条件が設定されていません。			

medium (qos-medium)

プロトコル	送信元	送信先	その他
条件が設定されていません。			

normal (qos-normal)

プロトコル	送信元	送信先	その他
条件が設定されていません。			

low

プロトコル	送信元	送信先	その他
条件が設定されていません。			

インタフェースシェーピングの設定

	現在の設定	設定の変更
シェーピング設定	有効	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
帯域	10 Mbps	<input type="text" value="10"/> <input checked="" type="radio"/> Mbps <input type="radio"/> Kbps <input type="radio"/> bps

[詳細設定へ](#)

4. 詳細設定

4.3.7 通信セキュリティの設定

通信セキュリティを設定します。

設定するには、「プロバイダの設定」が必要です。また、「プロバイダの設定」でNAPTが「有効」に設定されている必要があります。

- (1) ログイン後のメニューエリアから[詳細設定]をクリックします。
- (2) 「WAN」の項目から[通信セキュリティの設定]をクリックします。

<ul style="list-style-type: none">■ 管理者メニュー<ul style="list-style-type: none">トップページ設定の保存ログアウト■ かんたん設定<ul style="list-style-type: none">かんたん設定■ 詳細設定<ul style="list-style-type: none">詳細設定基本設定<ul style="list-style-type: none">パスワードの設定装置名の設定時刻の設定保守の設定NetMeisterの設定ゼロタッチの設定LAN<ul style="list-style-type: none">LANアドレスの設定DHCPサーバの設定WAN<ul style="list-style-type: none">プロバイダの設定静的NAPTの設定WANフィルタの設定<ul style="list-style-type: none">・IPv4・IPv6URLフィルタリングの設定QoSの設定通信セキュリティの設定VPN・クラウド<ul style="list-style-type: none">VPNの設定L2TPの設定クラウドの設定NGN網VPN<ul style="list-style-type: none">NGN網VPNの設定デバイス<ul style="list-style-type: none">デバイスの設定UTM<ul style="list-style-type: none">基本設定詳細設定グループ別ポリシー設定ホワイトリスト設定UTM尚書レポート■ 端末管理<ul style="list-style-type: none">端末管理■ 保守管理<ul style="list-style-type: none">保守管理■ 拡張ページ<ul style="list-style-type: none">拡張ページ■ 外部リンク<ul style="list-style-type: none">製品ページ	<h3>詳細設定</h3> <p>本装置の詳細な設定を行います。 ルータの全ての設定を利用できるわけではありません。 個別に設定を変更する場合は任意コマンドの実行から操作してください。 本装置に接続された端末の制御は端末管理から操作してください。</p> <hr/> <h3>基本設定</h3> <p>本装置の基本的な設定を行います。 保守設定ではSSH、Telnet、SNMP、Syslog等を設定します。 また、NetMeisterやゼロタッチの設定をします。</p> <hr/> <h3>LAN</h3> <p>LAN側の設定を行います。 IPアドレス、DHCPサーバなどを設定します。</p> <hr/> <h3>WAN</h3> <p>WAN側の設定を行います。 プロバイダ設定ではインターネットの接続設定を行います。 QoS設定ではシェーピングとPQ制御を利用できます。 URLフィルタの設定ではサービス事業者の提供するURLリストやユーザが指定したURLをフィルタできます。</p> <hr/> <h3>VPN・クラウド</h3> <p>IPSecやダイナミックVPN、サービス事業者ごとのクラウド設定を行います。</p> <hr/> <h3>NGN網VPN</h3> <p>NGN-IPv6網を利用したVPNの設定を行います。</p> <hr/> <h3>デバイス</h3> <p>本装置の各デバイスの設定を行います。</p> <hr/> <h3>UTM</h3> <p>本装置のUTMの設定を行います。</p>
--	---

4. 詳細設定

- (3) セキュリティ強度や不正アクセス検知(IDS)の「有効」／「無効」を設定し、[反映]ボタンをクリックします。

通信セキュリティの設定

通信セキュリティを設定します。

	現在の設定	設定の変更
セキュリティ強度	レベル1	<input checked="" type="radio"/> レベル1 - 外部からの不要なパケットを NAPT (IPv4)、ダイナミックフィルタ (IPv6) により廃棄します。 <input type="radio"/> レベル2 - 外部からの不要なパケットを NAPT (IPv4)、ダイナミックフィルタ (IPv6) により廃棄します。 - 内部からの不要な通信を制限します。 <input type="radio"/> レベル3 - VPN 通信以外のパケットは全て廃棄します。 (VPN 以外のインターネット上の Web アクセスも禁止します)
不正アクセス検知 (IDS)	無効	IPv4 通信にのみ有効です。 <input checked="" type="radio"/> 無効 <input type="radio"/> 有効 (不正パケットを廃棄します)

反映

番号	項目	内容																	
①	セキュリティ強度	セキュリティ強度を選択します。 <ul style="list-style-type: none"> 外部からの不要なパケットを NAPT (IPv4) またはダイナミックフィルタ (IPv6) により廃棄する場合は、「レベル 1」を選択します。 外部からの不要なパケットを NAPT (IPv4) またはダイナミックフィルタ (IPv6) により廃棄し、さらに内部からの不要な通信を制限する場合は、「レベル 2」を選択します。 VPN 通信以外のパケットを全て廃棄する場合は、「レベル 3」を選択します。 (VPN 以外のインターネット上の Web アクセスも禁止します) ケーブルテレビなどで、インターネットへのアクセスができない場合は、「レベル 1」を選択してください。 「レベル 2」を選択したときは、送信時に以下に該当する通信を廃棄します。 <table border="1" style="margin-left: 20px;"> <tbody> <tr> <td rowspan="4">宛先 IP アドレス</td> <td>0.0.0.0/8</td> </tr> <tr> <td>127.0.0.0/8</td> </tr> <tr> <td>169.254.0.0/16</td> </tr> <tr> <td>224.0.0.0/4</td> </tr> <tr> <td rowspan="5">宛先ポート番号</td> <td>135</td> </tr> <tr> <td>137</td> </tr> <tr> <td>138</td> </tr> <tr> <td>139</td> </tr> <tr> <td>445</td> </tr> <tr> <td rowspan="5">送信元ポート番号</td> <td>135</td> </tr> <tr> <td>137</td> </tr> <tr> <td>138</td> </tr> <tr> <td>139</td> </tr> <tr> <td>445</td> </tr> </tbody> </table>	宛先 IP アドレス	0.0.0.0/8	127.0.0.0/8	169.254.0.0/16	224.0.0.0/4	宛先ポート番号	135	137	138	139	445	送信元ポート番号	135	137	138	139	445
宛先 IP アドレス	0.0.0.0/8																		
	127.0.0.0/8																		
	169.254.0.0/16																		
	224.0.0.0/4																		
宛先ポート番号	135																		
	137																		
	138																		
	139																		
	445																		
送信元ポート番号	135																		
	137																		
	138																		
	139																		
	445																		
②	不正アクセス検知 (IDS)	不正アクセス検知 (IDS) 機能の「有効 (不正パケットを廃棄します)」／「無効」を設定します。IPv4 通信のみに有効で、IPv6 通信では無視されます。																	

4. 詳細設定

- (4) 「設定内容を変更しました。」のメッセージと、設定が反映されたことを確認します。

通信セキュリティの設定

設定内容を変更しました。

	現在の設定	設定の変更
セキュリティ強度	レベル1	<ul style="list-style-type: none"><input checked="" type="radio"/> レベル1<ul style="list-style-type: none">- 外部からの不要なパケットをNAPT(IPv4)、ダイナミックフィルタ(IPv6)により廃棄します。<input type="radio"/> レベル2<ul style="list-style-type: none">- 外部からの不要なパケットをNAPT(IPv4)、ダイナミックフィルタ(IPv6)により廃棄します。- 内部からの不要な通信を制限します。<input type="radio"/> レベル3<ul style="list-style-type: none">- VPN通信以外のパケットは全て廃棄します。(VPN以外のインターネット上のWebアクセスも禁止します)
不正アクセス検知 (IDS)	無効	IPv4通信にのみ有効です。 <ul style="list-style-type: none"><input checked="" type="radio"/> 無効<input type="radio"/> 有効 (不正パケットを廃棄します)

詳細設定へ

4. 詳細設定

4.4 VPN・クラウド

メモ 設定を変更したときは、設定の保存を実行してください。

4.4.1 VPN の設定

VPN による拠点間通信の設定を行います。

メモ 設定するには、「プロバイダの設定」が必要です。

メモ ダイナミック VPN と L2TP/IPsec は、それぞれ 2 つ以上設定しないでください。

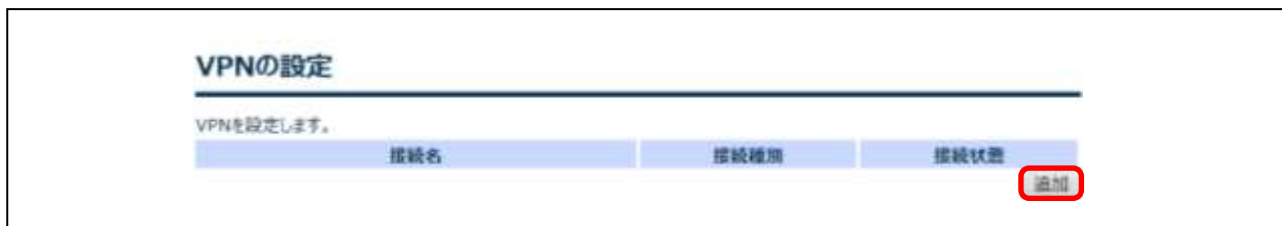
- (1) ログイン後のメニューエリアから[詳細設定]をクリックします。
- (2) 「VPN・クラウド」の項目から[VPN の設定]をクリックします。

4. 詳細設定

■ 管理者メニュー	詳細設定
トップページ	本装置の詳細な設定を行います。
設定の保存	ルータの全ての設定を利用できるわけではありません。
ログアウト	個別に設定を変更する場合は 任意コマンドの実行 から操作してください。
■ かんたん設定	本装置に接続された端末の制御は 端末管理 から操作してください。
かんたん設定	
■ 詳細設定	基本設定
詳細設定	本装置の基本的な設定を行います。
基本設定	保守設定ではSSH、Telnet、SNMP、Syslog等を設定します。
パスワードの設定	また、NetMeisterやゼロタッチの設定をします。
装置名の設定	
時刻の設定	
保守の設定	
NetMeisterの設定	
ゼロタッチの設定	
LAN	LAN
LANアドレスの設定	LAN側の設定を行います。
DHCPサーバの設定	IPアドレス、DHCPサーバなどを設定します。
WAN	WAN
プロバイダの設定	WAN側の設定を行います。
節約NAPTの設定	プロバイダ設定ではインターネットの接続設定を行います。
WANフィルタの設定	QoS設定ではシェーピングとPQ制御を利用できます。
・IPv4	URLフィルタの設定ではサービス事業者の提供するURLリストや
・IPv6	ユーザが指定したURLをフィルタできます。
URLフィルタリングの設定	
QoSの設定	
通信セキュリティの設定	
VPN・クラウド	VPN・クラウド
VPNの設定	IPSecやダイナミックVPN、サービス事業者ごとのクラウド設定を行います。
L2TPの設定	
クラウドの設定	
NGN網VPN	NGN網VPN
NGN網VPNの設定	NGN-IPv6網を利用したVPNの設定を行います。
デバイス	デバイス
デバイスの設定	本装置の各デバイスの設定を行います。
UTM	UTM
基本設定	本装置のUTMの設定を行います。
詳細設定	
グループ別ポリシー設定	
ホワイトリスト設定	
UTM脅威レポート	
■ 端末管理	
端末管理	
■ 保守管理	
保守管理	
■ 拡張ページ	
拡張ページ	
■ 外部リンク	
製品ページ	

4. 詳細設定

(3) [追加]ボタンをクリックします。



(4) 各項目を設定し、[反映]ボタンをクリックします。

ダイナミックVPN(拠点)の場合

メモ 設定の前に、LAN側のIPアドレスが他の拠点と重複していないことを必ず確認してください。

注意 クラウド接続のAWS(Amazon Web Services)と詳細設定によるダイナミックVPNの併用はできません。



4. 詳細設定

番号	項目	内容
①	接続種別	「ダイナミックVPN」を選択します。
②	タイプ	「拠点」を選択します。
③	拠点番号	拠点の識別番号です。 他の拠点と重複しない任意の番号(1~64)を設定します。
④	パスワード	VPN接続で使用するパスワード(事前共有鍵)です。 すべての拠点で同じ任意のパスワードを設定してください。 ・ 半角英数字で1~128文字まで入力できます。
⑤	センタWAN側IPアドレス	センタ装置のWANに設定されているIPアドレスまたはドメイン名を入力します。

ダイナミックVPN(センタ)の場合

メモ 設定の前に、LAN側のIPアドレスが他の拠点と重複していないことを必ず確認してください。

注意 クラウド接続のAWS(Amazon Web Services)と詳細設定によるダイナミックVPNの併用はできません。

The screenshot shows the 'VPNの設定' (VPN Settings) page. It includes a '接続種別の選択' (Connection Type Selection) section where 'ダイナミックVPN' (Dynamic VPN) is selected. Below that is the 'ダイナミックVPNの詳細設定' (Dynamic VPN Details) section, which is highlighted with a red box. This section contains a table with columns '現在の設定' (Current Setting) and '設定の変更' (Change Setting). The 'タイプ' (Type) row shows 'センタ' (Center) selected. The 'パスワード' (Password) row has a text input field. At the bottom right, there are '戻る' (Back) and '反映' (Apply) buttons.

番号	項目	内容
①	接続種別	「ダイナミックVPN」を選択します。
②	タイプ	「センタ」を選択します。
③	パスワード	VPN接続で使用するパスワード(事前共有鍵)です。 拠点に設定したパスワードと同じパスワードを設定してください。 ・ 半角英数字で1~128文字まで入力できます。

4. 詳細設定

IPsec の場合

- ☒ 接続元と接続先のアドレス契約が両方とも動的 IP アドレスの設定はできません。
- ☒ 暗号/認証の詳細設定は全て接続先の装置と一致させてください。
- ☒ 接続先の装置経由でインターネット通信を行いたい場合、接続先 LAN 側ネットワークに「0.0.0.0/0」を設定してください。

VPNの設定

設定を追加する場合は [反映] を押してください。

接続種別の選択

接続種別を選択してください。
IPsecのアドレス契約の「固定アドレス」は、ドメイン名が使用できる場合も選択可能です。
ダイナミックVPNとL2TP/IPsecは、併用できません。また、2つ以上設定しないでください。

	現在の設定	設定の変更
接続種別		<input type="radio"/> ダイナミックVPN <input checked="" type="radio"/> IPsec <input type="radio"/> IPトンネル <input type="radio"/> L2TP/IPsec
接続元アドレス契約		自装置のWAN側アドレス契約を選択してください。 <input checked="" type="radio"/> 固定IPアドレス <input type="radio"/> 動的IPアドレス
接続先アドレス契約		相手装置のWAN側アドレス契約を選択してください。 <input checked="" type="radio"/> 固定IPアドレス <input type="radio"/> 動的IPアドレス

IPsecの詳細設定 (メインモード)

	現在の設定	設定の変更
接続名		接続を識別するための任意の名称を設定してください。 <input type="text"/> 文字列(半角英数字)を入力してください。
接続先 (相手装置)	WAN側 IPアドレス	接続先のIPアドレスまたはドメイン名を入力してください。 <input type="text"/> 入力形式が不正です。
	LAN側 ネットワーク	接続先のLAN側のネットワークアドレスを入力してください。 <input type="text"/> / 24 IPアドレスを入力してください。
ルーティング		接続先のLAN側ネットワークアドレス以外にも接続するネットワーク アドレスがある場合に入力してください。 <input type="text"/> / 24 <input type="text"/> / 24 <input type="text"/> / 24 <input type="text"/> / 24

暗号/認証の詳細設定

設定は全て接続先の装置と一致させてください。

	現在の設定	設定の変更
IKE	事前共有鍵	接続先と共通のパスワードを設定してください。 <input type="text"/> 文字列(半角英数字)を入力してください。
	アルゴリズム	暗号 AES(256bit) / 認証 SHA2-256
	DHグループ	DH group 14(2048bit)
	ID	メインモードでは設定しません。
IPsec	アルゴリズム	暗号 AES(256bit) / 認証 SHA2-256

戻る

4. 詳細設定

番号	項目	内容
①	接続種別	「IPsec」を選択します。
②	接続元アドレス契約	自装置のWAN側アドレス契約を選択します。
③	接続先アドレス契約	相手装置のWAN側アドレス契約を選択します。
④	接続名	接続を識別するための任意の名称を設定します。 ・ 半角英数字で1～79文字まで入力できます。
⑤	接続先WAN側IPアドレス	接続先のIPアドレスまたはドメイン名を入力します。 注意 ・ 接続先アドレス契約で「動的IPアドレス」を選択した場合、IPアドレスおよびドメイン名のいずれも入力することはできません。接続先WAN側IPアドレスにドメイン名を入力する場合は、接続先アドレス契約を「固定IPアドレス」に設定してください。
⑥	接続先LAN側ネットワーク	接続先のLAN側のネットワークアドレスを入力します。 ・ ネットワークアドレスを入力し、サブネットマスクをプルダウンメニューから選択します。
⑦	ルーティング	接続先のLAN側ネットワークアドレス以外にも接続するネットワークアドレスがある場合に入力してください。
⑧	IKE 事前共有鍵	接続先と共通のパスワードを設定します。 ・ 半角英数字で1～128文字まで入力できます。
⑨	IKE アルゴリズム	IKEで使用する暗号と認証のアルゴリズムを選択します。 ・ 暗号アルゴリズムは、DES、3DES、AES(128 bit)、AES(192 bit)、AES(256 bit)から選択します。 ・ 認証アルゴリズムは、MD5、SHA1、SHA2-256、SHA2-384、SHA2-512から選択します。 注意 ・ 接続先(IPsec相手装置)と同じIKEアルゴリズムを選択します。
⑩	IKE DHグループ	IKEで使用する暗号と認証のDHグループを選択します。 注意 ・ 接続先(IPsec相手装置)と同じIKE DHグループを選択します。
⑪	IKE ID	接続元または接続先のアドレス契約のどちらかが動的IPアドレスの場合、接続を識別するためのIDを入力してください。 ・ 半角英数字で1～255文字まで入力できます。※ . (ドット)間の文字数は63文字まで。 注意 ・ 接続先(IPsec相手装置)と同じIKE IDを入力します。 ・ 接続元と接続先のアドレス契約が両方とも固定IPアドレスの場合、IDを入力することはできません。
⑫	IPsec アルゴリズム	IPsecで使用する暗号と認証のアルゴリズムを選択します。 ・ 暗号アルゴリズムは、DES、3DES、AES(128 bit)、AES(192 bit)、AES(256 bit)から選択します。 ・ 認証アルゴリズムは、MD5、SHA1、SHA2-256、SHA2-384、SHA2-512から選択します。 注意 ・ 接続先(IPsec相手装置)と同じIPsecアルゴリズムを選択します。

4. 詳細設定

IPトンネルの場合

VPNの設定

設定を追加する場合は [反映] を押してください。

接続種別の選択

接続種別を選択してください。
 IPsecのアドレス契約の『固定アドレス』は、ドメイン名が使用できる場合も選択可能です。
 ダイナミックVPNとL2TP/IPsecは、併用できません。また、2つ以上設定しないでください。

	現在の設定	設定の変更
接続種別		<input type="radio"/> ダイナミックVPN <input type="radio"/> IPsec <input checked="" type="radio"/> IPトンネル <input type="radio"/> L2TP/IPsec

IPトンネルの詳細設定

	現在の設定	設定の変更
接続名		接続を識別するための任意の名称を設定してください。 <input type="text"/> 文字列(半角英数字)を入力してください。
接続先 (相手装置)	WAN側 IPアドレス	接続先のIPアドレスまたはドメイン名を入力してください。 <input type="text"/> 入力形式が不正です。
	LAN側 ネットワーク	接続先のLAN側のネットワークアドレスを入力してください。 <input type="text"/> / 24 IPアドレスを入力してください。
ルーティング		接続先のLAN側ネットワークアドレス以外にも接続するネットワーク アドレスがある場合に入力してください。 <input type="text"/> / 24 <input type="text"/> / 24 <input type="text"/> / 24 <input type="text"/> / 24

戻る

番号	項目	内容
①	接続種別	「IPトンネル」を選択します。
②	接続名	接続を識別するための任意の名称を設定します。 ・ 半角英数字で1~79文字まで入力できます。
③	接続先 WAN 側 IP アドレス	接続先の IP アドレスまたはドメイン名を入力します。
④	接続先 LAN 側ネットワーク	接続先の LAN 側のネットワークアドレスを入力します。
⑤	ルーティング	接続先の LAN 側ネットワークアドレス以外にも接続するネットワークアドレスがある場合に入力してください。

4. 詳細設定

L2TP/IPsec の場合

メモ L2TP/IPsec は 2 つ以上設定しないでください。

注意 L2TP/IPsec 設定を反映するためには、設定の保存を行ってから再起動が必要です。

VPNの設定

設定を追加する場合は [反映] を押してください。

接続種別の選択

接続種別を選択してください。ダイナミックVPNとL2TP/IPsecは2つ以上設定しないでください。

	現在の設定	設定の変更
接続種別		<input type="radio"/> ダイナミックVPN <input type="radio"/> IPsec <input type="radio"/> IPトンネル <input checked="" type="radio"/> L2TP/IPsec

L2TP/IPsecの詳細設定

	現在の設定	設定の変更
同時接続数		1 (変更した場合、再起動が必要です)
アドレス割当範囲		<input type="text"/> ~ <input type="text"/> IPアドレスを入力してください。

暗号/認証の詳細設定

事前共有鍵以外の設定は、自動で適切なセキュリティ方式が選ばれます。

	現在の設定	設定の変更
IKE	事前共有鍵	接続先と共通のパスワードを設定してください。 <input type="text"/> 文字列(半角英数字)を入力してください。

接続ユーザの認証設定

リモートアクセスする端末のユーザ情報を設定してください。少なくとも 1 人分の登録が必要です。
L2TP/IPsec接続する端末側の設定は、以下のサイト(外部リンク)をご確認ください。(別のタブが開きます)
[iOS / Android / Windows](#)

	ユーザー名	パスワード	固定割当アドレス (省略可)
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>

4. 詳細設定

番号	項目	内容
①	接続種別	「L2TP/IPsec」を選択します。
②	同時接続数	L2TP/IPsecで同時に接続する端末の数(1~10)を設定します。 注意 <ul style="list-style-type: none">初期値は「0」です。変更した場合、再起動が必要です。
③	アドレス割当範囲	端末に割り当てる IP アドレスを設定します。
④	IKE 事前共有鍵	接続先と共通のパスワードを設定します。 <ul style="list-style-type: none">事前共有鍵以外の設定は、自動で適切なセキュリティ方式が選ばれます。半角英数字で 1~128 文字まで入力できます。
⑤	接続ユーザの認証設定	リモートアクセスする端末のユーザ情報を設定します。 <ul style="list-style-type: none">少なくとも 1 人分の登録が必要です。

(5) 設定が追加されたことを確認します。



注意 L2TP/IPsec 設定を反映するためには、設定の保存を行ってから再起動が必要です。

4. 詳細設定

4.4.2 L2TP の設定

L2TP/IPsec による、リモートアクセス VPN の設定を行います。

メモ L2TP/IPsec は 2 つ以上設定しないでください。

注意 L2TP/IPsec 設定を反映するためには、設定の保存を行ってから再起動が必要です。

(1) ログイン後のメニューエリアから[詳細設定]をクリックします。

(2) 「VPN・クラウド」の項目から[L2TP の設定]をクリックします。

■ 管理者メニュー トップページ 設定の保存 ログアウト	詳細設定 本装置の詳細な設定を行います。 ルータの全ての設定を利用できるわけではありません。 個別に設定を変更する場合は任意コマンドの実行から操作してください。 本装置に接続された端末の制御は 端末管理 から操作してください。
■ かんたん設定 かんたん設定	基本設定 本装置の基本的な設定を行います。 保守設定ではSSH、Telnet、SNMP、Syslog等を設定します。 また、NetMeisterやゼロタッチの設定をします。
■ 詳細設定 詳細設定 基本設定 パスワードの設定 装置名の設定 時刻の設定 保守の設定 NetMeisterの設定 ゼロタッチの設定	LAN LAN側の設定を行います。 IPアドレス、DHCPサーバなどを設定します。
LAN LANアドレスの設定 DHCPサーバの設定	WAN WAN側の設定を行います。 プロバイダ設定ではインターネットの接続設定を行います。 QoS設定ではシェーピングとPQ制御を利用できます。 URLフィルタの設定ではサービス事業者の提供するURLリストやユーザが指定したURLをフィルタできます。
WAN プロバイダの設定 静約NAPTの設定 WANフィルタの設定 ・IPv4 ・IPv6 URLフィルタリングの設定 QoSの設定 通信セキュリティの設定	VPN・クラウド IPSecやダイナミックVPN、サービス事業者ごとのクラウド設定を行います。
VPN・クラウド VPNの設定 L2TPの設定 クラウドの設定	NGN網VPN NGN-IPv6網を利用したVPNの設定を行います。
NGN網VPN NGN網VPNの設定	デバイス 本装置の名デバイスの設定を行います。
デバイス デバイスの設定	UTM 本装置のUTMの設定を行います。
UTM 基本設定 詳細設定 グループ別ポリシー設定 ホワイトリスト設定 UTM脅威レポート	
■ 端末管理 端末管理	
■ 保守管理 保守管理	
■ 拡張ページ 拡張ページ	
■ 外部リンク 製品ページ	

4. 詳細設定

(3) 各項目を設定し、[反映]ボタンをクリックします。

VPNの設定

設定を追加する場合は [反映] を押してください。

接続種別の選択

接続種別を選択してください。ダイナミックVPNとL2TP/IPsecは2つ以上設定しないでください。

	現在の設定	設定の変更
接続種別		<input type="radio"/> ダイナミックVPN <input type="radio"/> IPsec <input type="radio"/> IPトンネル <input checked="" type="radio"/> L2TP/IPsec

L2TP/IPsecの詳細設定

	現在の設定	設定の変更
同時接続数		1 (変更した場合、再起動が必要です)
アドレス割当範囲		~ IPアドレスを入力してください。

暗号/認証の詳細設定

事前共有鍵以外の設定は、自動で適切なセキュリティ方式が選ばれます。

	現在の設定	設定の変更
IKE 事前共有鍵		接続先と共通のパスワードを設定してください。 文字列(半角英数字)を入力してください。

接続ユーザの認証設定

リモートアクセスする端末のユーザ情報を設定してください。少なくとも1人分の登録が必要です。
L2TP/IPsec接続する端末側の設定は、以下のサイト(外部リンク)をご確認ください。(別のタブが開きます)
[iOS / Android / Windows](#)

	ユーザー名	パスワード	固定割当アドレス (省略可)
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

接続ユーザへのDNS通知

	現在の設定	設定の変更
DNSアドレス		接続ユーザにDNSを通知する場合に入力してください。

戻る 反映

4. 詳細設定

番号	項目	内容
①	接続種別	「L2TP/IPsec」を選択します。
②	同時接続数	L2TP/IPsecで同時に接続する端末の数(1~20)を設定します。 注意 <ul style="list-style-type: none">初期値は「0」です。変更した場合、再起動が必要です。
③	アドレス割当範囲	端末に割り当てる IP アドレスを設定します。
④	IKE 事前共有鍵	接続先と共通のパスワードを設定します。 <ul style="list-style-type: none">事前共有鍵以外の設定は、自動で適切なセキュリティ方式が選ばれます。半角英数字で 1~128 文字まで入力できます。
⑤	接続ユーザの認証設定	リモートアクセスする端末のユーザ情報を設定します。 <ul style="list-style-type: none">少なくとも 1 人分の登録が必要です。
⑥	DNS アドレス	接続ユーザに DNS を通知する場合のみ設定します。

(4) 設定が追加されたことを確認します。

The screenshot displays the VPN configuration page. At the top, there are two warning boxes in red. The first warning states: "!!注意!! 設定が変更されています。再起動した場合、保存していない設定は元の状態に戻ります。設定完了後は必ず「設定の保存」を行ってください。" The second warning states: "!!注意!! 再起動が必要な設定の変更がされています。設定を反映するためには「設定の保存」したうえで「再起動」してください。再起動を行わない場合や設定を保存せずに再起動した場合には設定が反映されません。"

Below the warnings is the section "VPNの設定". Underneath, it says "VPNを設定します." and there is a table of connections:

接続名	接続種別	接続状態
L2TP_#1	L2TP/IPsec	接続されていません

Buttons for "変更" (Change), "削除" (Delete), and "追加" (Add) are visible next to the connection entry.


注意 L2TP/IPsec 設定を反映するためには、設定の保存を行ってから再起動が必要です。

4. 詳細設定

4.4.3 クラウドの設定

クラウド接続の設定を行います。

- ※ Amazon Web Services は、米国その他の諸国における、Amazon.com, Inc.またはその関連会社の商標です。
- ※ Microsoft Azure は、米国 Microsoft Corporation の米国およびその他の国における商標または登録商標です。

 インターネット VPN での接続を行うには、「プロバイダの設定」が必要です。

- (1) ログイン後のメニューエリアから[詳細設定]をクリックします。
- (2) 「VPN・クラウド」の項目から[クラウドの設定]をクリックします。

4. 詳細設定

■ 管理者メニュー	詳細設定
トップページ	
設定の保存	
ログアウト	
■ かんたん設定	
かんたん設定	
■ 詳細設定	
詳細設定	
基本設定	
パスワードの設定	
装置名の設定	
時刻の設定	
保守の設定	
NetMeisterの設定	
ゼロタッチの設定	
LAN	
LANアドレスの設定	
DHCPサーバの設定	
WAN	
プロバイダの設定	
静的NAPTの設定	
WANフィルタの設定	
・IPv4	
・IPv6	
URLフィルタリングの設定	
QoSの設定	
通信セキュリティの設定	
VPN・クラウド	
VPNの設定	
L2TPの設定	
クラウドの設定	
NGN網VPN	
NGN網VPNの設定	
デバイス	
デバイスの設定	
UTM	
基本設定	
詳細設定	
グループ別ポリシー設定	
ホワイトリスト設定	
UTM脅威レポート	
■ 端末管理	
端末管理	
■ 保守管理	
保守管理	
■ 拡張ページ	
拡張ページ	
■ 外部リンク	
製品ページ	

詳細設定

本装置の詳細な設定を行います。
ルータの全ての設定を利用できるわけではありません。
個別に設定を変更する場合は**任意コマンドの実行**から操作してください。
本装置に接続された端末の制御は**端末管理**から操作してください。

基本設定

本装置の基本的な設定を行います。
保守設定ではSSH、Telnet、SNMP、Syslog等を設定します。
また、NetMeisterやゼロタッチの設定をします。

LAN

LAN側の設定を行います。
IPアドレス、DHCPサーバなどを設定します。

WAN

WAN側の設定を行います。
プロバイダ設定ではインターネットの接続設定を行います。
QoS設定ではシェーピングとPQ制御を利用できます。
URLフィルタの設定ではサービス事業者の提供するURLリストやユーザが指定したURLをフィルタできます。

VPN・クラウド

IPSecやダイナミックVPN、サービス事業者ごとのクラウド設定を行います。

NGN網VPN

NGN-IPv6網を利用したVPNの設定を行います。

デバイス

本装置の各デバイスの設定を行います。

UTM

本装置のUTMの設定を行います。

4. 詳細設定

(3) 各項目を設定し、[反映]ボタンをクリックします。

AWS(Amazon Web Services)に専用線で接続する場合

注意 AWS(Amazon Web Services)の専用線接続の設定を反映するためには、設定の保存を行ってから再起動が必要です。

注意 AWS(Amazon Web Services)とかんたん設定によるVPN接続の併用はできません。

注意 AWS(Amazon Web Services)と詳細設定によるダイナミックVPNの併用はできません。

【プロバイダの設定】がないため、専用線での接続のみ行えます。
インターネットVPNでの接続を行うには、【プロバイダの設定】が必要となります。

クラウドの設定

クラウドのサービス種別を設定します。

	現在の設定	設定の変更
サービス種別		<input checked="" type="radio"/> AWS (Amazon Web Services) <input type="radio"/> Microsoft Azure <input type="radio"/> NEC Cloud IaaS
接続形態		<input type="radio"/> インターネットVPN <input checked="" type="radio"/> 専用線

AWS (Amazon Web Services) に専用線で接続

接続先 (クラウド)	WAN側 IPアドレス	接続先のIPアドレスを入力してください。 <input type="text"/>
	AS番号	10124 <input type="text"/>
	BGP パスワード	接続先と共通のパスワードを入力してください。 <input type="text"/>
接続元 (IX)	WAN側 IPアドレス	接続元のIPアドレスを入力してください。 <input type="text"/> / <input type="text"/>
	AS番号	65010 <input type="text"/>
	VLAN番号	接続元のVLAN番号を入力してください。 <input type="text"/>

4. 詳細設定

番号	項目	内容
①	サービス種別	「AWS (Amazon Web Services)」を選択します。
②	接続形態	「専用線」を選択します。
③	接続先(クラウド) WAN 側 IP アドレス	接続先の IP アドレスを入力します。
④	接続先(クラウド) AS 番号	接続先の BGP ピアの AS 番号(1~65534)を入力します。 ・ 初期値は「10124」です。
⑤	接続先(クラウド) BGP パスワード	接続先と共通のパスワードを設定します。 ・ 半角英数字で 1~218 文字まで入力できます。
⑥	接続元 (IX) WAN 側 IP アドレス	接続元の IP アドレスを入力します。
⑦	接続元 (IX) AS 番号	接続元の BGP の AS 番号(1~65534)を入力します。 ・ 初期値は「65010」です。
⑧	接続元 (IX) VLAN 番号	接続元の VLAN 番号(1~4095)を入力します。

4. 詳細設定

AWS(Amazon Web Services)にインターネットVPNで接続する場合

注意 AWS(Amazon Web Services)とかんたん設定によるVPN接続の併用はできません。

注意 AWS(Amazon Web Services)と詳細設定によるダイナミックVPNの併用はできません。

4. 詳細設定

専用線での接続を行うには「設定の初期化」が必要となります。

クラウドの設定

クラウドのサービス種別を設定します。

	現在の設定	設定の変更
サービス種別		<input checked="" type="radio"/> AWS (Amazon Web Services) <input type="radio"/> Microsoft Azure <input type="radio"/> NEC Cloud IaaS
接続形態		<input checked="" type="radio"/> インターネットVPN <input type="radio"/> 専用線

AWS (Amazon Web Services) にインターネットVPNで接続

IPsec Tunnel #1

接続先 (クラウド)	WAN側 IPアドレス	Outside IP Addresses:の Virtual Private Gatewayを入力してください。 <input type="text"/> IPアドレスを入力してください。
	VPNアドレ ス	Inside IP Addresses:の Virtual Private Gatewayを入力してください。 <input type="text"/> IPアドレスを入力してください。
	AS番号	BGP Configuration Options:の Virtual Private Gateway ASNを入力してください。 <input type="text" value="10124"/>
接続元 (IX)	VPNアドレ ス	Inside IP Addresses:の Customer Gatewayを入力してください。 <input type="text"/> / <input type="text" value="30"/>
	AS番号	BGP Configuration Options:の Customer Gateway ASNを入力してください。 <input type="text" value="65000"/>

IPsec Tunnel #2

接続先 (クラウド)	WAN側 IPアドレス	Outside IP Addresses:の Virtual Private Gatewayを入力してください。 <input type="text"/>
	VPNアドレ ス	Inside IP Addresses:の Virtual Private Gatewayを入力してください。 <input type="text"/>
	AS番号	BGP Configuration Options:の Virtual Private Gateway ASNを入力してください。 <input type="text" value="10124"/>
接続元 (IX)	VPNアドレ ス	Inside IP Addresses:の Customer Gatewayを入力してください。 <input type="text"/> / <input type="text" value="30"/>
	AS番号	IPsec Tunnel #1 と共通です

暗号/認証の詳細設定

事前共有鍵以外の設定は、以下のセキュリティ方式が選ばれます。

IKEV1: 暗号 AES(128bit) / 認証 SHA1, Lifetime 28800 秒, DH group 2(1024bit)

IPsec: 暗号 AES(128bit) / 認証 SHA1, Lifetime 3600 秒, PFS 有効 (1024bit)

IPsec Tunnel #1

	現在の設定	設定の変更
IKE	事前共有鍵	Configure the IKE SA as follows of Pre-Shared Keyを入力してください。 <input type="text"/> 文字列(半角英数字)を入力してください。

IPsec Tunnel #2

	現在の設定	設定の変更
IKE	事前共有鍵	Configure the IKE SA as follows of Pre-Shared Keyを入力してください。 <input type="text"/>

初期化

4. 詳細設定

①	サービス種別	「AWS (Amazon Web Services)」を選択します。																		
②	接続形態	「インターネット VPN」を選択します。																		
③	IPsec Tunnel#1 接続先(クラウド) WAN 側 IP アドレス	IPsec Tunnel#1 の Outside IP Addresses:の Virtual Private Gateway を入力します。																		
④	IPsec Tunnel#1 接続先(クラウド) VPN アドレス	IPsec Tunnel#1 の Inside IP Addresses:の Virtual Private Gateway を入力します。																		
⑤	IPsec Tunnel#1 接続先(クラウド) AS 番号	IPsec Tunnel#1 の BGP Configuration Options:の Virtual Private Gateway ASN(1～65535)を入力します。 ・ 初期値は「10124」です。																		
⑥	IPsec Tunnel#1 接続元(X) VPN アドレス	IPsec Tunnel#1 の Inside IP Addresses:の Customer Gateway を入力します。																		
⑦	IPsec Tunnel#1 接続元(X) AS 番号	IPsec Tunnel#1 の BGP Configuration Options:の Customer Gateway ASN(1～65535)を入力します。 ・ 初期値は「65000」です。																		
⑧	IPsec Tunnel#2 接続先(クラウド) WAN 側 IP アドレス	IPsec Tunnel#2 の Outside IP Addresses:の Virtual Private Gateway を入力します。 <input type="checkbox"/> メモ ・ 複数 VPN を使用しない場合は、本設定は不要です。																		
⑨	IPsec Tunnel#2 接続先(クラウド) VPN アドレス	IPsec Tunnel#2 の Inside IP Addresses:の Virtual Private Gateway を入力します。 <input type="checkbox"/> メモ ・ 複数 VPN を使用しない場合は、本設定は不要です。																		
⑩	IPsec Tunnel#2 接続先(クラウド) AS 番号	IPsec Tunnel#2 の BGP Configuration Options:の Virtual Private Gateway ASN(1～65535)を入力します。 ・ 初期値は「10124」です。 <input type="checkbox"/> メモ ・ 複数 VPN を使用しない場合は、本設定は不要です。																		
⑪	IPsec Tunnel#2 接続元(X) VPN アドレス	IPsec Tunnel#2 の Inside IP Addresses:の Customer Gateway を入力します。 <input type="checkbox"/> メモ ・ 複数 VPN を使用しない場合は、本設定は不要です。																		
⑫	IPsec Tunnel#1 IKE 事前共有鍵	IPsec Tunnel#1 の Configure the IKE SA as follows の Pre-Shared Key を入力します。 ・ 半角英数字で 1～128 文字まで入力できます。 ・ 事前共有鍵以外の設定は、自動で以下のパラメータが選択されます。 <table border="1" style="margin-left: 20px;"> <tr> <td colspan="2">IKE (フェーズ 1)</td> </tr> <tr> <td>バージョン</td> <td>IKEv1</td> </tr> <tr> <td>暗号化/認証方式</td> <td>AES128/SHA-1</td> </tr> <tr> <td>DHグループ</td> <td>2 (1024-bit)</td> </tr> <tr> <td>ライフタイム</td> <td>28800 秒</td> </tr> <tr> <td colspan="2">IPsec (フェーズ 2)</td> </tr> <tr> <td>暗号化/認証方式</td> <td>AES128/SHA-1</td> </tr> <tr> <td>DHグループ</td> <td>2 (1024-bit)</td> </tr> <tr> <td>ライフタイム</td> <td>3600 秒</td> </tr> </table>	IKE (フェーズ 1)		バージョン	IKEv1	暗号化/認証方式	AES128/SHA-1	DHグループ	2 (1024-bit)	ライフタイム	28800 秒	IPsec (フェーズ 2)		暗号化/認証方式	AES128/SHA-1	DHグループ	2 (1024-bit)	ライフタイム	3600 秒
IKE (フェーズ 1)																				
バージョン	IKEv1																			
暗号化/認証方式	AES128/SHA-1																			
DHグループ	2 (1024-bit)																			
ライフタイム	28800 秒																			
IPsec (フェーズ 2)																				
暗号化/認証方式	AES128/SHA-1																			
DHグループ	2 (1024-bit)																			
ライフタイム	3600 秒																			

4. 詳細設定

⑬	IPsec Tunnel#2 IKE 事前共有鍵	<p>IPsec Tunnel#2 の Configure the IKE SA as follows の Pre-Shared Key を入力します。</p> <ul style="list-style-type: none">半角英数字で 1~128 文字まで入力できます。事前共有鍵以外の設定は、自動で以下のパラメータが選択されます。 <table border="1" data-bbox="590 344 1193 707"><tr><td colspan="2">IKE (フェーズ 1)</td></tr><tr><td>バージョン</td><td>IKEv1</td></tr><tr><td>暗号化/認証方式</td><td>AES128/SHA-1</td></tr><tr><td>DH グループ</td><td>2 (1024-bit)</td></tr><tr><td>ライフタイム</td><td>28800 秒</td></tr><tr><td colspan="2">IPsec (フェーズ 2)</td></tr><tr><td>暗号化/認証方式</td><td>AES128/SHA-1</td></tr><tr><td>DH グループ</td><td>2 (1024-bit)</td></tr><tr><td>ライフタイム</td><td>3600 秒</td></tr></table> <p>メモ</p> <ul style="list-style-type: none">複数 VPN を使用しない場合は、本設定は不要です。	IKE (フェーズ 1)		バージョン	IKEv1	暗号化/認証方式	AES128/SHA-1	DH グループ	2 (1024-bit)	ライフタイム	28800 秒	IPsec (フェーズ 2)		暗号化/認証方式	AES128/SHA-1	DH グループ	2 (1024-bit)	ライフタイム	3600 秒
IKE (フェーズ 1)																				
バージョン	IKEv1																			
暗号化/認証方式	AES128/SHA-1																			
DH グループ	2 (1024-bit)																			
ライフタイム	28800 秒																			
IPsec (フェーズ 2)																				
暗号化/認証方式	AES128/SHA-1																			
DH グループ	2 (1024-bit)																			
ライフタイム	3600 秒																			

4. 詳細設定

Microsoft Azure に接続する場合

専用線での接続を行うには「[設定の初期化](#)」が必要となります。

クラウドの設定

クラウドのサービス種別を設定します。

	現在の設定	設定の変更
サービス種別		<input type="radio"/> AWS (Amazon Web Services) <input checked="" type="radio"/> Microsoft Azure <input type="radio"/> NEC Cloud IaaS
接続形態		<input checked="" type="radio"/> インターネットVPN

Microsoft Azure にインターネットVPNで接続

	現在の設定	設定の変更
接続先 (クラウド)	WAN側 IPアドレス	接続先のIPアドレスを入力してください。 <input type="text"/> IPアドレスを入力してください。
	LAN側 ネットワーク	接続先の仮想ネットワークで設定しているアドレス空間のネットワーク アドレスを入力してください。 <input type="text"/> / <input type="text"/> <input type="button" value="▼"/> IPアドレスを入力してください。

暗号/認証の詳細設定

事前共有鍵以外の設定は、以下のセキュリティ方式が選ばれます。
 IKEv1: 暗号 AES(128bit) / 認証 SHA1、Lifetime 28800 秒、DH group 2(1024bit)
 IPsec: 暗号 AES(128bit) / 認証 SHA1、Lifetime 3600 秒、PFS 無効

	現在の設定	設定の変更
IKE	事前共有鍵	接続先と共通のパスワードを設定してください。 <input type="text"/> 文字列(半角英数字)を入力してください。

番号	項目	内容																		
①	サービス種別	「Microsoft Azure」を選択します。																		
②	接続形態	「インターネット VPN」を選択します。																		
③	接続先(クラウド) WAN 側 IP アドレス	接続先の IP アドレスを入力します。																		
④	接続先(クラウド) LAN 側ネットワーク	接続先の LAN 側のネットワークアドレスを入力します。 <ul style="list-style-type: none"> ネットワークアドレスを入力し、サブネットマスクをプルダウンメニューから選択します。 																		
⑤	IKE 事前共有鍵	接続先と共通のパスワードを設定します。 <ul style="list-style-type: none"> 半角英数字で 1~128 文字まで入力できます。 事前共有鍵以外の設定は、自動で以下のパラメータが選択されます。 <table border="1"> <thead> <tr> <th colspan="2">IKE (フェーズ 1)</th> </tr> </thead> <tbody> <tr> <td>バージョン</td> <td>IKEv1</td> </tr> <tr> <td>暗号化/認証方式</td> <td>AES128/SHA-1</td> </tr> <tr> <td>DH グループ</td> <td>2 (1024-bit)</td> </tr> <tr> <td>ライフタイム</td> <td>28800 秒</td> </tr> <tr> <th colspan="2">IPsec (フェーズ 2)</th> </tr> <tr> <td>暗号化/認証方式</td> <td>AES128/SHA-1</td> </tr> <tr> <td>DH グループ</td> <td>無し</td> </tr> <tr> <td>ライフタイム</td> <td>3600 秒</td> </tr> </tbody> </table>	IKE (フェーズ 1)		バージョン	IKEv1	暗号化/認証方式	AES128/SHA-1	DH グループ	2 (1024-bit)	ライフタイム	28800 秒	IPsec (フェーズ 2)		暗号化/認証方式	AES128/SHA-1	DH グループ	無し	ライフタイム	3600 秒
IKE (フェーズ 1)																				
バージョン	IKEv1																			
暗号化/認証方式	AES128/SHA-1																			
DH グループ	2 (1024-bit)																			
ライフタイム	28800 秒																			
IPsec (フェーズ 2)																				
暗号化/認証方式	AES128/SHA-1																			
DH グループ	無し																			
ライフタイム	3600 秒																			

4. 詳細設定

NEC Cloud IaaS に接続する場合

専用線での接続を行うには『設定の初期化』が必要となります。

クラウドの設定

クラウドのサービス種別を設定します。

	現在の設定	設定の変更
サービス種別		<input type="radio"/> AWS (Amazon Web Services) <input type="radio"/> Microsoft Azure <input checked="" type="radio"/> NEC Cloud IaaS
接続形態		<input checked="" type="radio"/> インターネットVPN

NEC Cloud IaaS にインターネットVPNで接続

接続先 (クラウド)	WAN側 IPアドレス	接続先のIPアドレスを入力してください。 <input type="text"/> <small>IPアドレスを入力してください。</small>
	LAN側 ネットワーク	接続先のLAN側のネットワークアドレスを入力してください。 <input type="text"/> / <input type="text"/> <input type="text"/> <small>IPアドレスを入力してください。</small>

暗号/認証の詳細設定

事前共有鍵以外の設定は、以下のセキュリティ方式が選ばれます。

IKEv1: 暗号 AES(128bit) / 認証 SHA1. Lifetime 28800 秒. DH group 2(1024bit)
 IPsec: 暗号 AES(128bit) / 認証 SHA1. Lifetime 3600 秒. PFS有効 (1024bit)

	現在の設定	設定の変更
IKE	事前共有鍵	接続先と共通のパスワードを設定してください。 <input type="text"/> <small>半角英数字を入力してください。</small>

番号	項目	内容																		
①	サービス種別	「NEC Cloud IaaS」を選択します。																		
②	接続形態	「インターネットVPN」を選択します。																		
③	接続先(クラウド) WAN側 IP アドレス	接続先のIP アドレスを入力します。																		
④	接続先(クラウド) LAN側ネットワーク	接続先のLAN側のネットワークアドレスを入力します。 ・ ネットワークアドレスを入力し、サブネットマスクをプルダウンメニューから選択します。																		
⑤	IKE 事前共有鍵	接続先と共通のパスワードを設定します。 ・ 半角英数字で 1~128 文字まで入力できます。 ・ 事前共有鍵以外の設定は、自動で以下のパラメータが選択されます。 <table border="1" style="margin-top: 10px;"> <thead> <tr> <th colspan="2">IKE (フェーズ 1)</th> </tr> </thead> <tbody> <tr> <td>バージョン</td> <td>IKEv1</td> </tr> <tr> <td>暗号化/認証方式</td> <td>AES128/SHA-1</td> </tr> <tr> <td>DHグループ</td> <td>2 (1024-bit)</td> </tr> <tr> <td>ライフタイム</td> <td>28800 秒</td> </tr> <tr> <th colspan="2">IPsec (フェーズ 2)</th> </tr> <tr> <td>暗号化/認証方式</td> <td>AES128/SHA-1</td> </tr> <tr> <td>DHグループ</td> <td>2 (1024-bit)</td> </tr> <tr> <td>ライフタイム</td> <td>3600 秒</td> </tr> </tbody> </table>	IKE (フェーズ 1)		バージョン	IKEv1	暗号化/認証方式	AES128/SHA-1	DHグループ	2 (1024-bit)	ライフタイム	28800 秒	IPsec (フェーズ 2)		暗号化/認証方式	AES128/SHA-1	DHグループ	2 (1024-bit)	ライフタイム	3600 秒
IKE (フェーズ 1)																				
バージョン	IKEv1																			
暗号化/認証方式	AES128/SHA-1																			
DHグループ	2 (1024-bit)																			
ライフタイム	28800 秒																			
IPsec (フェーズ 2)																				
暗号化/認証方式	AES128/SHA-1																			
DHグループ	2 (1024-bit)																			
ライフタイム	3600 秒																			

4. 詳細設定

- (5) 「設定内容を変更しました。」のメッセージと、設定が反映されたことを確認します。

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず『設定の保存』を行ってください。

!!注意!! 再起動が必要な設定の変更がされています。
設定を反映するためには『設定の保存』したうえで『再起動』してください。
再起動を行わない場合や設定を保存せずに再起動した場合には設定が反映されません。

インターネットVPNでの接続を行うには、『設定の初期化』が必要となります。

クラウドの設定

設定内容を変更しました。

	現在の設定	設定の変更
サービス種別	AWS	<input checked="" type="radio"/> AWS (Amazon Web Services) <input type="radio"/> Microsoft Azure <input type="radio"/> NEC Cloud IaaS
接続形態	専用線	<input type="radio"/> インターネットVPN <input checked="" type="radio"/> 専用線

AWS (Amazon Web Services) に専用線で接続

接続先 (クラウド)	WAN側 IPアドレス		接続先のIPアドレスを入力してください。 203.0.113.254
	AS番号		10124
	BGP パスワード		接続先と共通のパスワードを入力してください。 cloud-password
接続元 (IX)	WAN側 IPアドレス	203.0.113.1/31	接続元のIPアドレスを入力してください。 203.0.113.1 / 31
	AS番号	65010	65010
	VLAN番号	10	接続元のVLAN番号を入力してください。 10

[詳細設定へ](#)

4. 詳細設定

4.5 NGN 網 VPN の設定

設定を変更したときは、設定の保存を実行してください。

NGN IPv6 網を利用した VPN を設定します。また、必要に応じてインターネット接続を設定します。

初めて NGN 網 VPN の設定を行う場合、または一度設定した内容を変更する場合には、設定を初期化する必要があります。

NetMeister のダイナミック DNS サービスを利用するため、NetMeister への登録が必要となります。

- (1) ログイン後のメニューエリアから[詳細設定]をクリックします。
- (2) 「NGN 網 VPN」の項目から[NGN 網 VPN の設定]をクリックします。

4. 詳細設定

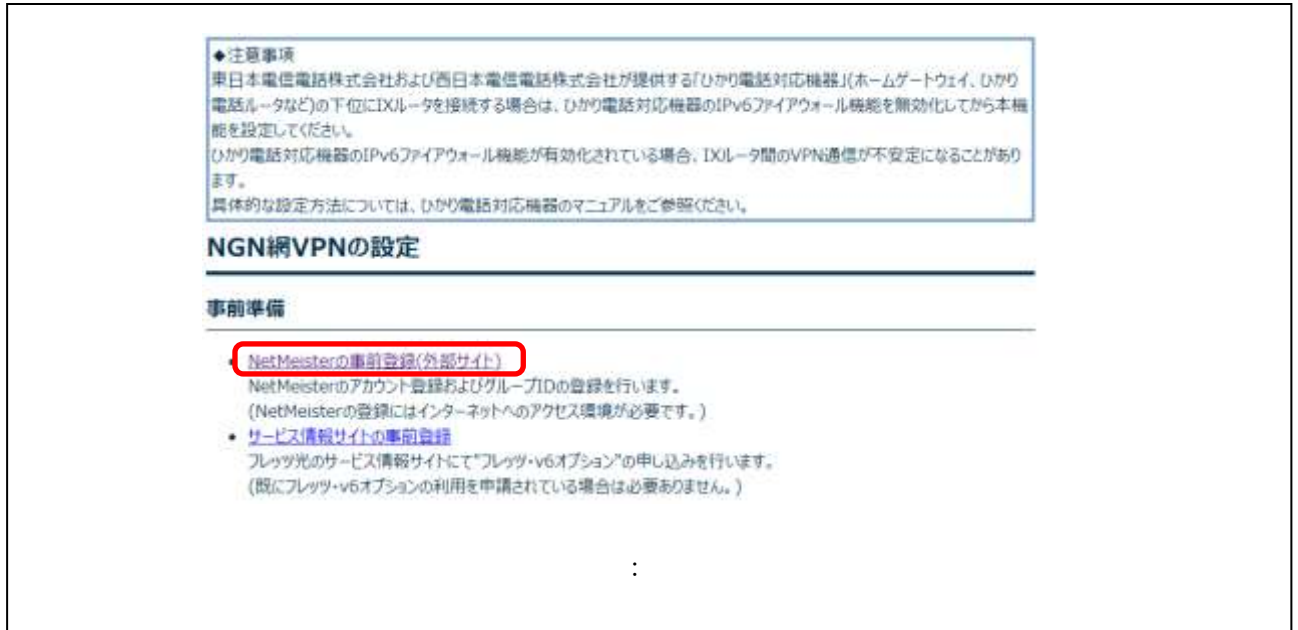
■ 管理者メニュー	詳細設定
トップページ	本装置の詳細な設定を行います。
設定の保存	ルータの全ての設定を利用できるわけではありません。
ログアウト	個別に設定を変更する場合は 任意コマンドの実行 から操作してください。
■ かんたん設定	本装置に接続された端末の制御は 端末管理 から操作してください。
かんたん設定	
■ 詳細設定	基本設定
詳細設定	本装置の基本的な設定を行います。
基本設定	保守設定ではSSH、Telnet、SNMP、Syslog等を設定します。
パスワードの設定	また、NetMeisterやゼロタッチの設定をします。
装置名の設定	
時刻の設定	LAN
保守の設定	LAN側の設定を行います。
NetMeisterの設定	IPアドレス、DHCPサーバなどを設定します。
ゼロタッチの設定	
LAN	WAN
LANアドレスの設定	WAN側の設定を行います。
DHCPサーバの設定	プロバイダ設定ではインターネットの接続設定を行います。
WAN	QoS設定ではシェーピングとPQ制御を利用できます。
プロバイダの設定	URLフィルタの設定ではサービス事業者の提供するURLリストや
静的NAPTの設定	ユーザが指定したURLをフィルタできます。
WANフィルタの設定	
・IPv4	VPN・クラウド
・IPv6	IPSecやダイナミックVPN、サービス事業者ごとのクラウド設定を行います。
URLフィルタリングの設定	
QoSの設定	NGN網VPN
通信セキュリティの設定	NGN-IPv6網を利用したVPNの設定を行います。
VPN・クラウド	
VPNの設定	デバイス
L2TPの設定	本装置の各デバイスの設定を行います。
クラウドの設定	
NGN網VPN	UTM
NGN網VPNの設定	本装置のUTMの設定を行います。
デバイス	
デバイスの設定	
UTM	
基本設定	
詳細設定	
グループ別ポリシー設定	
ホワイトリスト設定	
UTM脅威レポート	
■ 端末管理	
端末管理	
■ 保守管理	
保守管理	
■ 拡張ページ	
拡張ページ	
■ 外部リンク	
製品ページ	

4. 詳細設定

4.5.1 NetMeister の事前登録

NetMeister に、アカウントおよびグループ ID を登録します。

- (1) NGN 網 VPN の設定の事前準備の[NetMeister の事前登録(外部サイト)]をクリックします。



- (2) NetMeister にアカウントおよびグループ ID を登録します。

NetMeister のアカウントおよびグループ ID の登録方法は、NetMeister のサイトを参照してください。



4.5.2 サービス情報サイトの事前登録

NTT 東日本または NTT 西日本のフレッツ光のサービス情報サイトにアクセスし、フレッツ・v6 オプションの申し込みを行います。

4. 詳細設定

- ☒ NTT 東日本または NTT 西日本のフレッツ光のサービス情報サイトにアクセスするため、はじめて NGN 網 VPN の設定を行う場合、設定を初期化する必要があります。
- ☒ フレッツ・v6 オプションの申し込み方法は、お客様契約先の NTT 東日本または NTT 西日本のホームページを参照してください。

(1) NGN 網 VPN の設定の事前準備の[サービスサイトの事前登録]をクリックします。

◆注意事項
東日本電信電話株式会社および西日本電信電話株式会社が提供する「ひかり電話対応機器」(ホームゲートウェイ、ひかり電話ルータなど)の下位にIXルータを接続する場合は、ひかり電話対応機器のIPv6ファイアウォール機能を無効化してから本機能を設定してください。
ひかり電話対応機器のIPv6ファイアウォール機能が有効化されている場合、IXルータ間のVPN通信が不安定になることがあります。
具体的な設定方法については、ひかり電話対応機器のマニュアルをご参照ください。

NGN網VPNの設定

事前準備

- NetMeisterの事前登録(外部サイト)
NetMeisterのアカウント登録およびグループIDの登録を行います。
(NetMeisterの登録にはインターネットへのアクセス環境が必要です。)
- サービス情報サイトの事前登録
フレッツ光のサービス情報サイトで「フレッツ・v6オプション」の申し込みを行います。
(既にフレッツ・v6オプションの利用を申請されている場合は必要ありません。)

:

4. 詳細設定

- (2) サービスサイトの事前登録画面が表示されたことを確認します。

サービス情報サイトでのオプションの申込みが完了した後は、設定を[無効]にしてからVPNの設定を行ってください。
([有効]にしたままVPNの設定を行った場合には、この設定は自動的に[無効]に戻ります。再度設定を[有効]にする必要はありませんのでご注意ください。)

NGN網VPNの設定：サービス情報サイトの事前登録

サービス情報サイト接続設定

	現在の設定	設定の変更	
サービス情報サイト 接続設定	無効	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効	<input type="button" value="反映"/>

サービス情報サイトへの接続完了

※[無効]を反映後、サービス情報サイトへの接続は削除されます。
引き続き設定を行う場合は「NGN網VPNの設定」に移動してください。
[NGN網VPNの設定](#)

- (3) サービス情報サイトにアクセスできるようにするため、サービス情報サイト接続設定の有効を選択し、[反映]をクリックします。

サービス情報サイトでのオプションの申込みが完了した後は、設定を[無効]にしてからVPNの設定を行ってください。
([有効]にしたままVPNの設定を行った場合には、この設定は自動的に[無効]に戻ります。再度設定を[有効]にする必要はありませんのでご注意ください。)

NGN網VPNの設定：サービス情報サイトの事前登録

サービス情報サイト接続設定

	現在の設定	設定の変更	
サービス情報サイト 接続設定	無効	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効	<input type="button" value="反映"/>

WAN情報

接続名	接続状態	情報
設定されていません		


サービス情報サイト接続先

※[有効]を反映後、以下のサイトへ接続可能となります。

- NTT東日本
<http://www.v4flets-east.jp/>
- NTT西日本
<http://www.v4flets-west.jp/>

4. 詳細設定

(4) 設定が反映されたことを確認します。

 NTT回線の地域が対応していないサービス情報サイトとの接続状態は、「認証失敗」と表示されます。

サービス情報サイトでのオプションの申込みが完了した後は、設定を[無効]にしてからVPNの設定を行ってください。
([有効]にしたままVPNの設定を行った場合には、この設定は自動的に[無効]に戻ります。再度設定を[有効]にする必要はありませんのでご注意ください。)

NGN網VPNの設定：サービス情報サイトの事前登録

サービス情報サイト接続設定

	現在の設定	設定の変更
サービス情報サイト 接続設定	有効	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効

WAN情報

接続名	接続状態	情報
NGN-IPv6網 (GigaEthernet0.0)	IPv6 : 接続	IPv6アドレス: 
サービス情報サイト(NTT東日本) (GigaEthernet0.1)	接続	IPアドレス:  DNS: 
サービス情報サイト(NTT西日本) (GigaEthernet0.2)	認証失敗	

サービス情報サイト接続先

※[有効]を反映後、以下のサイトへ接続可能となります。

- NTT東日本
<http://www.v4flets-east.jp/>
- NTT西日本
<http://www.v4flets-west.jp/>

4. 詳細設定

- (5) 画面下の「サービス情報サイト接続先」より、NTT 東日本またはNTT 西日本にアクセスし、フレッツ・v6 オプションの申し込みを行ってください。
- (6) フレッツ・v6 オプションの申し込みが完了した後、サービス情報サイト接続設定を無効にします。

サービス情報サイトでのオプションの申し込みが完了した後は、設定を[無効]にしてからVPNの設定を行ってください。
（[有効]にしたままVPNの設定を行った場合には、この設定は自動的に[無効]に戻ります。再度設定を[有効]にする必要はありませんのでご注意ください。）

NGN網VPNの設定：サービス情報サイトの事前登録

サービス情報サイト接続設定

	現在の設定	設定の変更	
サービス情報サイト 接続設定	有効	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効	<input type="button" value="反映"/>

WAN情報

接続名	接続状態	情報
NGN-IPv6網 (GigaEthernet0.0)	IPv6 : 接続	IPv6アドレス:
サービス情報サイト(NTT東日本) (GigaEthernet0.1)	接続	IPアドレス: DNS:
サービス情報サイト(NTT西日本) (GigaEthernet0.2)	認証失敗	

サービス情報サイト接続先

※[有効]を反映後、以下のサイトへ接続可能となります。

- NTT東日本
<http://www.v4flets-east.jp/>
- NTT西日本
<http://www.v4flets-west.jp/>

- (7) 設定が反映されたことを確認します。

サービス情報サイトでのオプションの申し込みが完了した後は、設定を[無効]にしてからVPNの設定を行ってください。
（[有効]にしたままVPNの設定を行った場合には、この設定は自動的に[無効]に戻ります。再度設定を[有効]にする必要はありませんのでご注意ください。）

NGN網VPNの設定：サービス情報サイトの事前登録

サービス情報サイト接続設定

	現在の設定	設定の変更	
サービス情報サイト 接続設定	無効	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効	<input type="button" value="反映"/>

サービス情報サイトへの接続完了

※[無効]を反映後、サービス情報サイトへの接続は削除されます。
引き続き設定を行う場合は「NGN網VPNの設定」に移動してください。
[NGN網VPNの設定](#)

4. 詳細設定

4.5.3 NGN 網 VPN 設定

NGN 網 VPN の設定を行います。

- (1) NGN 網 VPN の設定のひかり電話の設定および LAN 側インタフェースの設定を行います。

◆注意事項
東日本電信電話株式会社および西日本電信電話株式会社が提供する「ひかり電話対応機器」(ホームゲートウェイ、ひかり電話ルータなど)の下位にIXルータを接続する場合は、ひかり電話対応機器のIPv6ファイアウォール機能を無効化してから本機能を設定してください。
ひかり電話対応機器のIPv6ファイアウォール機能が有効化されている場合、IXルータ間のVPN通信が不安定になることがあります。
具体的な設定方法については、ひかり電話対応機器のマニュアルをご参照ください。

NGN網VPNの設定

事前準備

- [NetMeisterの事前登録\(外部サイト\)](#)
NetMeisterのアカウント登録およびグループIDの登録を行います。
(NetMeisterの登録にはインターネットへのアクセス環境が必要です。)
- [サービス情報サイトの事前登録](#)
フレッツ光のサービス情報サイトにて「フレッツ・v6オプション」の申し込みを行います。
(既にフレッツ・v6オプションの利用を申請されている場合は必要ありません。)

ひかり電話の設定

自動を選択することでひかり電話あり/なしを自動で判別します。
新規設定時は自動を選択してください。

	現在の設定	設定の変更
ひかり電話		<input checked="" type="radio"/> 自動 <input type="radio"/> あり <input type="radio"/> なし

WAN1: WAN側インタフェースの設定(GigaEthernet0.0)

	現在の設定	設定の変更
WAN側アドレス	-	自動取得
デフォルトゲートウェイ	-	自動設定
DNSアドレス	-	自動取得

LAN1: LAN側インタフェースの設定(GigaEthernet2.0)

他の拠点と重複しないように設定してください。
LAN側IPアドレスを変更する場合、現在のWEBページへの接続が切断されます。新しいIPアドレスで接続しなおしてください。

	現在の設定	設定の変更
LAN側IPアドレス	192.168.1.254	LAN側IPアドレスを設定してください。 192.168.1.254 / 24

番号	項目	内容
①	ひかり電話	NTT 東日本またはNTT 西日本フレッツ光サービスのひかり電話サービスの契約有無を選択します。[自動]は、ルータで自動判定します。
②	LAN 側 IP アドレス	LAN 側 IP アドレスを設定します。 IP アドレスを変更する場合、現在の接続は切断されます。新しい IP アドレスに接続しなおしてください。 注意 <ul style="list-style-type: none"> 他のセンタ・拠点と異なる IP アドレスを設定する必要があります。

4. 詳細設定

(2) NGN 網 VPN 設定の VPN の設定を行います。

センタの設定の場合

:

VPNの設定

	現在の設定	設定の変更
タイプ		<input type="radio"/> 拠点 <input checked="" type="radio"/> センタ
VPNパスワード		センタとすべての拠点で共通のパスワードを設定してください。 <input type="text"/> 文字列(半角英数字)を入力してください。

:

番号	項目	内容
①	タイプ	センタを選択します。
②	パスワード	すべてのセンタと拠点で共通のパスワードを設定します。 ・ 半角英数字で 1~128 文字まで入力できます。

拠点の設定の場合

:

VPNの設定

	現在の設定	設定の変更
タイプ		<input checked="" type="radio"/> 拠点 <input type="radio"/> センタ
拠点番号		他の拠点と同じ番号は設定しないでください。 <input type="text" value="1"/>
VPNパスワード		センタとすべての拠点で共通のパスワードを設定してください。 <input type="text"/> 文字列(半角英数字)を入力してください。
センタのFQDN		センタで設定したNetMeisterの「装置のホスト名」と「グループID」を入力してください。 <input type="text" value="hostname"/> . <input type="text" value="group-id"/> <input type="text" value=".v6.nmddns.jp"/> 文字列を入力してください。[2-63文字](装置のホスト名) 文字列を入力してください。[2-63文字](グループID)

:

番号	項目	内容
①	タイプ	拠点を選択します。
②	拠点番号	拠点の識別番号です。 他の拠点と重複しない任意の番号(1~64)を設定します。
③	パスワード	すべてのセンタと拠点で共通のパスワードを設定します。 ・ 半角英数字で 1~128 文字まで入力できます。
④	センタの FQDN	センタ装置に設定された NetMeister の「ホスト名」と「グループ ID」を設定します。 ・ ホスト名およびグループ ID は、半角英数字で 2~63 文字まで入力できます。

4. 詳細設定

(3) NGN 網 VPN 設定の NetMeister ダイナミック DNS の設定を行います。

:

NetMeister ダイナミックDNSの設定

	現在の設定	設定の変更
NTT回線の地域	-	自動取得
ホスト名(装置名)		NetMeisterで管理する装置のホスト名を設定します。 本項目は、ダイナミックDNSサービスのドメインの一部として使用します。 <input type="text"/> 文字列を入力してください。[2-63文字]
サイト名(拠点名)		NetMeisterで管理する装置の拠点情報(拠点名)を設定します。 <input type="text"/> 文字列を入力してください。[2-31文字]
NetMeister グループID		NetMeisterに登録したグループIDを設定します。 <input type="text"/> 文字列を入力してください。[2-63文字]
NetMeister グループパスワード		NetMeisterに登録したグループパスワードを設定します。 <input type="radio"/> パスワードを変更しない <input checked="" type="radio"/> パスワードを変更する <input type="text"/> 文字列を入力してください。[8-31文字]

:

番号	項目	内容
①	ホスト名(装置名)	装置のホスト名を設定します。設定したホスト名は NetMeister に通知されます。 <ul style="list-style-type: none"> 半角英数字または-(ハイフン)で2~63 文字まで入力できます。 メモ <ul style="list-style-type: none"> 大文字は、小文字に変換して NetMeister に通知されます。 注意 <ul style="list-style-type: none"> ホスト名の先頭と最後には-(ハイフン)を利用することができません。
②	サイト名(拠点名)	NetMeister に通知するサイト名を設定します。 <ul style="list-style-type: none"> 半角英数字または-(ハイフン)で2~31 文字まで入力できます。 メモ <ul style="list-style-type: none"> 大文字は、小文字に変換して NetMeister に通知されます。 注意 <ul style="list-style-type: none"> サイト名の先頭と最後には-(ハイフン)を利用することができません。
③	NetMeister グループ ID	NetMeister の登録ページで申請した「グループ ID」を設定します。 <ul style="list-style-type: none"> 半角英数字または-(ハイフン)で2~63 文字まで入力できます。 注意 <ul style="list-style-type: none"> NetMeister グループ ID の先頭と最後には-(ハイフン)を利用することができません。
④	NetMeister グループパスワード	NetMeister の登録ページで申請した「グループパスワード」を設定します。 <ul style="list-style-type: none"> 半角英数字または-(ハイフン)で2~31 文字まで入力できます。 注意 <ul style="list-style-type: none"> 大文字/小文字は区別されます。 パスワードの入力文字は表示されません。●●●のように伏せ文字で表示されます。

4. 詳細設定

- (4) NGN 網 VPN 設定のインターネット接続の設定を行い、[反映]をクリックします。

インターネット接続[あり]の場合

:

インターネット接続の設定

拠点からセンタ経由でインターネット接続する場合は、なしを選択してください。
NetMeisterでの装置管理を行うためにはインターネットの接続をありにする必要があります。

	現在の設定	設定の変更
インターネット接続		<input checked="" type="radio"/> あり <input type="radio"/> なし

WAN2: PPPoE接続の設定(GigaEthernet0.1)

	現在の設定	設定の変更
ユーザ名		プロバイダから通知されているユーザ名を設定します。 (フレッツの場合、通常はユーザ名に@を含んでいます) <input type="text"/> 文字列(半角英数字)を入力してください。
パスワード		プロバイダから通知されているパスワードを設定します。 <input type="text"/> 文字列(半角英数字)を入力してください。

反映

番号	項目	内容
①	インターネット接続	[あり]を選択します。 メモ ・ インターネット接続[あり]の場合、NetMeister によるダイナミック DNS を利用可能となります。また、NetMeister による装置管理も利用可能となります。
②	ユーザ名	プロバイダから通知されているユーザ名を設定します。 (フレッツの場合、通常はユーザ名には@を含んでいます) ・ 半角英数字で1~59 文字まで入力できます。
③	パスワード	プロバイダから通知されているパスワードを設定します。 ・ 半角英数字で1~79 文字まで入力できます。 注意 ・ 大文字/小文字は区別されます。

4. 詳細設定

インターネット接続[なし]の場合

インターネット接続の設定

拠点からセンタ経由でインターネット接続する場合は、なしを選択してください。
NetMeisterでの装置管理を行うためにはインターネットの接続をありにする必要があります。

	現在の設定	設定の変更
インターネット接続		<input type="radio"/> あり <input checked="" type="radio"/> なし

反映

番号	項目	内容
①	インターネット接続	[なし]を選択します。 メモ ・ インターネット接続[なし]の場合、NetMeister によるダイナミック DNS を利用可能となります。NetMeister による装置管理は利用できません。

4. 詳細設定

(5) 設定が反映されたことを確認します。

◆注意事項
東日本電信電話株式会社および西日本電信電話株式会社が提供する「ひかり電話対応機器」(ホームゲートウェイ、ひかり電話ルータなど)の下位にIXルータを接続する場合は、ひかり電話対応機器の「IPv6ファイアウォール機能」を無効化してから本機能を設定してください。
ひかり電話対応機器のIPv6ファイアウォール機能が有効化されている場合、IXルータ間のVPN通信が不安定になることがあります。
具体的な設定方法については、ひかり電話対応機器のマニュアルをご参照ください。

NGN網VPNの設定

事前準備

- **Net Meisterの事前登録(外部サイト)**
Net Meisterのアカウント登録およびグループIDの登録を行います。
(Net Meisterの登録にはインターネットへのアクセス環境が必要です。)
- **サービス情報サイトの事前登録**
フレッツ光のサービス情報サイトで「フレッツ・v6オプション」の申し込みを行います。
(既にフレッツ・v6オプションの利用を申請されている場合は必要ありません。)

ひかり電話の設定

自動を選択することでひかり電話あり/なしを自動で判別します。
新規設定時は自動を選択してください。


	現在の設定	設定の変更
--	-------	-------

設定した内容により、表示される画面が異なります。

反映

4. 詳細設定

4.6 デバイス

 設定を変更したときは、設定の保存を実行してください。

4.6.1 デバイスの設定

デバイスの状態を変更します。

- (1) ログイン後のメニューエリアから[詳細設定]をクリックします。
- (2) 「デバイス」の項目から[デバイスの設定]をクリックします。

4. 詳細設定

■ 管理者メニュー	詳細設定
トップページ	本装置の詳細な設定を行います。
設定の保存	ルータの全ての設定を利用できるわけではありません。
ログアウト	個別に設定を変更する場合は任意コマンドの実行から操作してください。
■ かんたん設定	本装置に接続された端末の制御は 端末管理 から操作してください。
かんたん設定	
■ 詳細設定	基本設定
詳細設定	本装置の基本的な設定を行います。
基本設定	保守設定ではSSH、Telnet、SNMP、Syslog等を設定します。
パスワードの設定	また、NetMeisterやゼロタッチの設定をします。
装置名の設定	
時刻の設定	
保守の設定	
NetMeisterの設定	
ゼロタッチの設定	
LAN	LAN
LANアドレスの設定	LAN側の設定を行います。
DHCPサーバの設定	IPアドレス、DHCPサーバなどを設定します。
WAN	WAN
プロバイダの設定	WAN側の設定を行います。
静的NAPTの設定	プロバイダ設定ではインターネットの接続設定を行います。
WANフィルタの設定	QoS設定ではシェーピングとPQ制御を利用できます。
IPv4	URLフィルタの設定ではサービス事業者の提供するURLリストや
IPv6	ユーザが指定したURLをフィルタできます。
URLフィルタリングの設定	
QoSの設定	
通信セキュリティの設定	
VPN・クラウド	VPN・クラウド
VPNの設定	IPSecやダイナミックVPN、サービス事業者ごとのクラウド設定を行います。
L2TPの設定	
クラウドの設定	
NGN網VPN	NGN網VPN
NGN網VPNの設定	NGN-IPv6網を利用したVPNの設定を行います。
デバイス	デバイス
デバイスの設定	本装置の各デバイスの設定を行います。
UTM	UTM
基本設定	本装置のUTMの設定を行います。
詳細設定	
グループ別ポリシー設定	
ホワイトリスト設定	
UTM脅威レポート	
■ 端末管理	
端末管理	
■ 保守管理	
保守管理	
■ 拡張ページ	
拡張ページ	
■ 外部リンク	
製品ページ	

4. 詳細設定

(3) 状態を変更したいデバイスの[変更]ボタンをクリックします。

デバイスの設定

デバイスの状態を変更します。

デバイス	接続状態		送信量	受信量
GE0 (GigaEthernet0)	全二重 100Mbpsで接続	変更	0%	0%
GE1 (GigaEthernet1)	Port1: 全二重 1Gbpsで接続	変更	0%	0%
	Port2: 接続されていません	変更		
	Port3: 接続されていません	変更		
	Port4: 接続されていません	変更		

更新

(4) デバイスの利用や回線速度を選択し、[反映]ボタンをクリックします。

☒ 回線速度は、Ethernet デバイス選択時のみ表示されます。

☒ IX3315 の 10GigaEthernet(GE2/GE3) では、「10Mbps 固定」と「100Mbps 固定」の回線速度項目は表示されません。

デバイスの設定

選択したデバイスの設定を変更します。

GE1 (GigaEthernet1) Port4

	現在の設定	設定の変更
デバイスの利用	使用する	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない(シャットダウン)
回線速度	auto	速度をauto以外に設定した場合、duplexは全二重固定です。 <input checked="" type="radio"/> auto (自動設定) <input type="radio"/> 1Gbps固定 <input type="radio"/> 100Mbps固定 <input type="radio"/> 10Mbps固定

戻る 反映

4. 詳細設定

(5) 設定が反映されたことを確認します。

ケーブルが接続されていない場合、回線速度は表示されません。


デバイスの設定

デバイスの状態を変更します。

デバイス	接続状態	送信量	受信量
GE0 (GigaEthernet0)	全二重 100Mbpsで接続 <input type="button" value="変更"/>	0%	0%
	Port1: 全二重 1Gbpsで接続 <input type="button" value="変更"/>		
GE1 (GigaEthernet1)	Port2: 接続されていません <input type="button" value="変更"/>	0%	0%
	Port3: 接続されていません <input type="button" value="変更"/>		
	Port4: 未使用(シャットダウン) <input type="button" value="変更"/>		


4. 詳細設定

4.7 UTM

 設定を変更したときは、設定の保存を実行してください。

4.7.1 トップページ

UTMの状態を確認します。

 UTMを利用する場合、インターネット上にあるライセンスサーバでライセンス認証を行ったり、シグネチャサーバとの通信、アンチウイルスサーバおよびURLフィルタリングデータベースサーバで通信のチェックを行ったりするため、インターネットへの経路到達性が必須となります。あらかじめ、インターネットへ接続するための設定を行ってください。

(1) ログイン後のメニューエリアから[トップページ]をクリックします。



The screenshot shows the UTM management interface. On the left is a navigation menu with 'トップページ' (Top Page) highlighted in red. The main content area shows the following sections:

- 装置情報 (装置名:Router)**

バージョン	稼働時間	稼働率	メモリ	内部温度	内部電圧
	1分	16%	18%	36.0℃	3.2506V

更新
- ネットワーク情報**

デバイス	接続状態	送信量	受信量
GE0 (GigaEthernet0)	全二重 1Gbpsで接続	0%	0%
GE1 (GigaEthernet1)	Port1: 接続されていません Port2: 接続されていません Port3: 接続されていません Port4: 全二重 1Gbpsで接続	0%	0%

更新
- WAN情報**

接続名	接続状態	情報
WAN1: インターネット接続 (GigaEthernet0.1)	接続	IPアドレス: ■■■■■■■■ DNS: ■■■■■■■■

更新
- VPN情報**

接続名	接続状態	通信量[packets]
設定されていません		


接続名編集 更新
- UTM情報**

ライセンス状態	ライセンス満了日時
設定されていません	

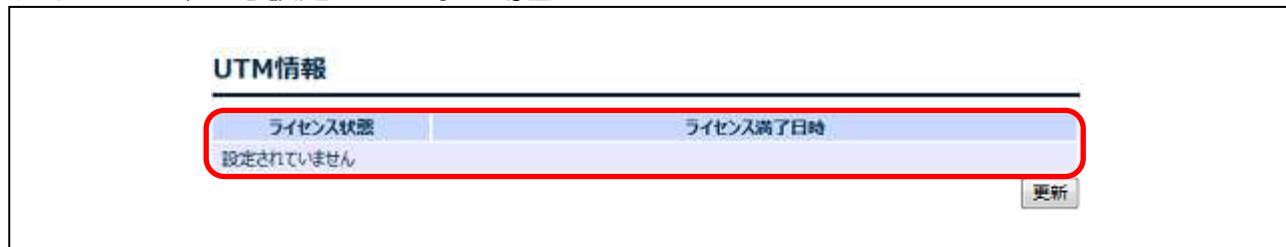
更新

4. 詳細設定

(2) UTM 情報より、UTM の状態を確認します。

 [更新]ボタンをクリックすると、最新の状態を表示することができます。

ライセンスキーを設定していない場合



次章を参照いただき、UTM 機能を有効化してください。

ライセンスが有効となっている場合（正常状態）



上記のように接続が確認できない場合、更新ボタンを押下いただき、正常状態になるかご確認ください。正常状態にならない場合は、インターネットに接続されていることと「ライセンスキー」「UTM 機能の有効化」が正しく設定されていることを確認してください。

4. 詳細設定

4.7.2 基本設定

UTM を設定します。

- (1) ログイン後のメニューエリアから[詳細設定]を選択し、「UTM」の項目から[基本設定]をクリックします。

<ul style="list-style-type: none">■ 管理者メニュー<ul style="list-style-type: none">トップページ設定の保存ログアウト■ かんたん設定<ul style="list-style-type: none">かんたん設定■ 詳細設定<ul style="list-style-type: none">詳細設定基本設定パスワードの設定装置名の設定時刻の設定保守の設定NetMeisterの設定ゼロタッチの設定LAN<ul style="list-style-type: none">LANアドレスの設定DHCPサーバの設定WAN<ul style="list-style-type: none">プロバイダの設定静的NAPTの設定WANフィルタの設定<ul style="list-style-type: none">・IPv4・IPv6URLフィルタリングの設定QoSの設定通信セキュリティの設定VPN・クラウド<ul style="list-style-type: none">VPNの設定L2TPの設定クラウドの設定NGN網VPN<ul style="list-style-type: none">NGN網VPNの設定デバイス<ul style="list-style-type: none">デバイスの設定UTM<ul style="list-style-type: none">基本設定詳細設定グループ別ポリシー設定ホワイトリスト設定UTM脅威レポート■ 端末管理<ul style="list-style-type: none">端末管理■ 保守管理<ul style="list-style-type: none">保守管理■ 拡張ページ<ul style="list-style-type: none">拡張ページ■ 外部リンク<ul style="list-style-type: none">製品ページ	<h3>詳細設定</h3> <p>本装置の詳細な設定を行います。 ルータの全ての設定を利用できるわけではありません。 個別に設定を変更する場合は任意コマンドの実行から操作してください。 本装置に接続された端末の制御は端末管理から操作してください。</p> <hr/> <h3>基本設定</h3> <p>本装置の基本的な設定を行います。 保守設定ではSSH、Telnet、SNMP、Syslog等を設定します。 また、NetMeisterやゼロタッチの設定をします。</p> <hr/> <h3>LAN</h3> <p>LAN側の設定を行います。 IPアドレス、DHCPサーバなどを設定します。</p> <hr/> <h3>WAN</h3> <p>WAN側の設定を行います。 プロバイダ設定ではインターネットの接続設定を行います。 QoS設定ではシェーピングとPQ制御を利用できます。 URLフィルタの設定ではサービス事業者の提供するURLリストや ユーザが指定したURLをフィルタできます。</p> <hr/> <h3>VPN・クラウド</h3> <p>IPSecやダイナミックVPN、サービス事業者ごとのクラウド設定を行います。</p> <hr/> <h3>NGN網VPN</h3> <p>NGN-IPv6網を利用したVPNの設定を行います。</p> <hr/> <h3>デバイス</h3> <p>本装置の各デバイスの設定を行います。</p> <hr/> <h3>UTM</h3> <p>本装置のUTMの設定を行います。</p>
---	---

4. 詳細設定

(2) 各項目を設定し、[反映]ボタンをクリックします。

基本設定

ライセンス情報

ページの再読み込みを行う場合は、表示更新ボタンを押してください。
UTMライセンスの有効期限やライセンス状態をサーバに確認する場合、サーバ確認ボタンを押してください。
サーバ確認時には、ページ更新に時間がかかる場合があります。

ライセンス状態	ライセンス満了日時	ライセンス最終確認日時
設定されていません		

ライセンス設定

UTM機能を使用するためにはUTMライセンスキーが必要です。
別途、UTMライセンスキーを購入してください。

ライセンスキーの設定

UTMライセンスシートに記載されているライセンスキーを入力してください。
設定に重複が発生した場合、入力制限がかかる場合があります。

	現在の設定	設定の変更
ライセンスキー	設定されていません	<input checked="" type="radio"/> XXXX-XXXX-XXXX-XXXX-XXXX <input type="radio"/> ライセンス自動設定

ライセンス期限切れ警告日の設定

設定した日数よりライセンスの満了日時が近くなると、イベントログやLEDなどで通知を開始します。

	現在の設定	設定の変更
ライセンス期限切れ警告日	60日前	60 <input type="text"/> 日前

UTM設定

UTM有効化設定

UTM機能の有効化設定を行います。

	現在の設定	設定の変更
UTM有効化設定	無効	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効

UTMを利用するインタフェースの設定

UTMを有効化したインタフェースを通過する送受信パケットに対して、UTM のチェックを行います。
インタフェースは複数指定可能で、LAN 側、WAN 側の両方のインタフェースで重複設定されていても問題ありません。
UTM 機能にLAN、WAN の方向性はありません。LAN 側、WAN 側どちら側からの通信であるかに関わらず同様にチェックされます。

対象	現在の設定	設定の変更
GigaEthernet0.1(WAN1)	無効	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
GigaEthernet1.0(LAN1)	無効	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効

UTM推奨設定

UTMを利用する際に必要となる設定です。
通常、そのまま反映してください。
UFSキャッシュ設定は必ず有効化されます。
推奨設定を削除する場合は「保守管理」の「任意コマンドの実行」で実行してください。

選択	現在の設定	設定内容
<input checked="" type="checkbox"/>	有効	UFSキャッシュ(IPv4/IPv6)を有効化
<input checked="" type="checkbox"/>	default	IPv4のUFSキャッシュエントリ数を 20000 に変更
<input checked="" type="checkbox"/>	default	IPv6のUFSキャッシュエントリ数を 10000 に変更
<input checked="" type="checkbox"/>	warn	UTMイベントログを notice に変更
<input checked="" type="checkbox"/>	default	ロギングバッファサイズを 1MB(=1000000bytes) に変更

4. 詳細設定

番号	項目	内容
①	ライセンスキー	UTM ライセンスキーを設定します。 <ul style="list-style-type: none">別売のライセンスシートに記載されているライセンスキーを入力します。 ライセンス自動設定を選択することで、NetMeister から自動的に UTM ライセンスを適用することもできます。
②	ライセンス期限切れ警告日	UTM ライセンスの期限切れ警告を何日前から通知するかを設定します。 <ul style="list-style-type: none">半角数字で 1~1000 の間で入力できます。 <input type="text" value="×モ"/> <ul style="list-style-type: none">設定した日数よりライセンスの満了日時が近くなると、イベントログおよび LED などて通知を開始します。
③	UTM 有効化設定	UTM の有効化/無効化を設定します。
④	UTM を利用するインタフェースの設定	UTM によるチェックを行うインタフェースを選択します。 <input type="text" value="×モ"/> <ul style="list-style-type: none">インタフェースは複数指定可能で、LAN 側、WAN 側の両方のインタフェースで重複設定されていても問題ありません。UTM 機能に LAN、WAN の方向性はありません。LAN 側、WAN 側どちら側からの通信であるかに関わらず同様にチェックされます。
⑤	UTM プロキシ設定	インターネットへの接続にプロキシサーバを使用している場合に設定します。 <ul style="list-style-type: none">http://FQDN 名/形式で、214 文字まで入力できます。 <input type="text" value="×モ"/> <ul style="list-style-type: none">アカウント・パスワードの必要なプロキシサーバや、ルート証明書による認証を別途必要とするプロキシサーバの利用はできません。
⑥	UTM 推奨設定	UTM を利用する際に推奨される設定です。 <ul style="list-style-type: none">選択がチェックされている場合、「現在の設定」値から「設定内容」に表示される推奨設定値に変更されます。

4. 詳細設定

- (4) UTM ライセンス情報の最新の状態を確認する場合は、[表示更新]をクリックします。



- (5) UTM ライセンスの有効期限またはライセンス状態をサーバに確認する場合は、[サーバ確認]をクリックします。

メモ サーバ確認では、画面の更新に時間がかかる場合があります。



- (6) UTM ライセンスの有効期限を延長する場合は、[ライセンス延長]をクリックします。

メモ 別売の延長ライセンスを購入する必要があります。

メモ サーバで管理されている情報を更新するため、サーバとの通信が確立している必要があります。



4. 詳細設定

ご購入いただいた延長ライセンスのシートに記載される延長キーコードを入力し、[反映]をクリックします。

基本設定

ライセンスの延長

ライセンスの満了日時を延長するためには、UTM延長ライセンスシートに記載されているキーコードが必要です。
別途、UTM延長ライセンスシートを購入してください。
ライセンスの残り期限が4年を超えている場合、延長をすることができません。
設定に複数回失敗した場合、入力制限がかかる場合があります。
延長の成否は、「UTM」の「基本設定」にある「ライセンス満了日時」の項目を確認してください。

戻る **反映**

延長キーコードが正常にサーバに反映された場合、下記のように表示されます。下記のように表示されない場合、延長キーコードの入力誤りあるいはサーバとの通信が正常に行われていないなどが考えられます。

基本設定

バックグラウンド上で更新処理が動作中です。設定をする場合、しばらく待ってから行ってください。

ライセンスの延長

ライセンスの満了日時を延長するためには、UTM延長ライセンスシートに記載されているキーコードが必要です。
別途、UTM延長ライセンスシートを購入してください。
ライセンスの残り期限が4年を超えている場合、延長をすることができません。
設定に複数回失敗した場合、入力制限がかかる場合があります。
延長の成否は、「UTM」の「基本設定」にある「ライセンス満了日時」の項目を確認してください。

XXXXX XXXXX XXXXX XXXXX

ライセンスの満了期限延長に成功しました。

戻る 反映

[戻る]をクリックし、ライセンス情報のライセンス満了日時が延長されたことを確認します。

基本設定

ライセンス情報

ページの再読み込みを行う場合は、表示更新ボタンを押してください。
UTMライセンスの有効期限やライセンス状態をサーバに確認する場合、サーバ確認ボタンを押してください。
サーバ確認時には、ページ更新に時間がかかる場合があります。

ライセンス状態	ライセンス満了日時	ライセンス最終確認日時
認証成功	2024.12.31	2024.12.31

表示更新 サーバ確認 ライセンス延長

4. 詳細設定

4.7.3 UTMの詳細設定

UTMの詳細を設定します。

- (1) ログイン後のメニューエリアから[詳細設定]を選択し、「UTM」の項目から[詳細設定]をクリックします。

<ul style="list-style-type: none">■ 管理者メニュー<ul style="list-style-type: none">トップページ設定の保存ログアウト■ かんたん設定<ul style="list-style-type: none">かんたん設定■ 詳細設定<ul style="list-style-type: none">詳細設定基本設定<ul style="list-style-type: none">パスワードの設定装置名の設定時刻の設定保守の設定NetMeisterの設定ゼロタッチの設定LAN<ul style="list-style-type: none">LANアドレスの設定DHCPサーバの設定WAN<ul style="list-style-type: none">プロバイダの設定静的NAPTの設定WANフィルタの設定<ul style="list-style-type: none">・IPv4・IPv6URLフィルタリングの設定QoSの設定通信セキュリティの設定VPN・クラウド<ul style="list-style-type: none">VPNの設定L2TPの設定クラウドの設定NGN網VPN<ul style="list-style-type: none">NGN網VPNの設定デバイス<ul style="list-style-type: none">デバイスの設定UTM<ul style="list-style-type: none">基本設定詳細設定グループ別ポリシー設定ホワイトリスト設定UTM脅威レポート■ 端末管理<ul style="list-style-type: none">端末管理■ 保守管理<ul style="list-style-type: none">保守管理■ 拡張ページ<ul style="list-style-type: none">拡張ページ■ 外部リンク<ul style="list-style-type: none">製品ページ	<h3>詳細設定</h3> <p>本装置の詳細な設定を行います。 ルータの全ての設定を利用できるわけではありません。 個別に設定を変更する場合は任意コマンドの実行から操作してください。 本装置に接続された端末の制御は端末管理から操作してください。</p> <hr/> <h3>基本設定</h3> <p>本装置の基本的な設定を行います。 保守設定ではSSH、Telnet、SNMP、Syslog等を設定します。 また、NetMeisterやゼロタッチの設定をします。</p> <hr/> <h3>LAN</h3> <p>LAN側の設定を行います。 IPアドレス、DHCPサーバなどを設定します。</p> <hr/> <h3>WAN</h3> <p>WAN側の設定を行います。 プロバイダ設定ではインターネットの接続設定を行います。 QoS設定ではシェーピングとPQ制御を利用できます。 URLフィルタの設定ではサービス事業者の提供するURLリストやユーザが指定したURLをフィルタできます。</p> <hr/> <h3>VPN・クラウド</h3> <p>IPSecやダイナミックVPN、サービス事業者ごとのクラウド設定を行います。</p> <hr/> <h3>NGN網VPN</h3> <p>NGN-IPv6網を利用したVPNの設定を行います。</p> <hr/> <h3>デバイス</h3> <p>本装置の各デバイスの設定を行います。</p> <hr/> <h3>UTM</h3> <p>本装置のUTMの設定を行います。</p>
--	--

4. 詳細設定

番号	項目	内容
①	シグネチャ更新設定	<p>シグネチャの更新確認を行い、更新必要時にはダウンロードおよびアップデート処理を実行する時間を設定します。</p> <ul style="list-style-type: none"> 0を設定した場合は、毎日00時台の時刻で実行します。1を設定した場合は、毎日01時台の時刻で実行します。以下同様に、23時台まで設定することができます。 <p>メモ</p> <ul style="list-style-type: none"> サーバの負荷軽減のため、実際の更新は00～59分のいずれかでランダムに実行されます。 0から23までのすべてがチェックされている場合は、現在の設定に「1時間ごと」と表示されます。
②	UTMリダイレクト設定	<p>URLフィルタリング、Webガードのブロック時に表示したいリダイレクトページのURLを指定します。</p> <ul style="list-style-type: none"> 半角英数字で127文字まで入力できます。(スキーム・パスを含む) ルータに設定されたLAN側IPアドレスを指定することにより、ルータ内蔵のブロックページにリダイレクトすることもできます。 未設定時は、リダイレクトせずに、簡易的なブロックページを表示します。
③	LED通知設定	UTMで検出した場合の、LEDによる通知対象を指定します。
④	LED通知時間設定	<p>UTMによる脅威を検出した際に、LED点灯を継続する時間を設定します。</p> <ul style="list-style-type: none"> 半角数字で1～256時間まで入力できます。 「通知し続ける」を指定した場合は、手動で消灯を設定するまで点灯し続けます。 <p>メモ</p> <ul style="list-style-type: none"> 本設定は、LED通知設定で「脅威検出時」を選択したときに有効です。
⑤	セキュリティログの設定	UTMの各機能にて検出した異常をイベントログに記録するセキュリティログの[有効]/[無効]を選択します。
⑥	脅威レポートの通知設定	UTMによる脅威を検出した際に、イベントログに記録する脅威レポートの[有効]/[無効]を選択します。
⑦	検出HTTPSポート番号の設定 全選択	選択したHTTPSポートに対して、一括削除することができます。[全選択]をクリックすると、HTTPSポートを全選択します。
⑧	検出HTTPSポート番号の設定 全解除	選択したHTTPSポートをすべて解除します。
⑨	検出HTTPSポート番号の設定 選択	選択したHTTPSポートに対して、一括削除することができます。 HTTPSポート単位で、個々に選択します。
⑩	検出HTTPSポート番号の設定 追加	<p>URLフィルタリング、Webガードで検出するHTTPSポート番号を設定します。追加する場合は、数値を入力した後、[追加]をクリックします。削除する場合は、ポート番号に該当する選択ボックスをチェックし、[削除]をクリックします。</p> <ul style="list-style-type: none"> 443を含め、最大9件まで入力できます。 半角数字0～65535までを入力できます。 空白またはカンマで区切って複数のポート番号を同時に入力することもできます。 <p>メモ</p> <ul style="list-style-type: none"> 443を削除することはできません。 <p>注意</p> <ul style="list-style-type: none"> [反映]をクリックしなくても設定されます。

4. 詳細設定

(3) 設定が反映されたことを確認します。

詳細設定

シグネチャ設定

シグネチャ更新設定

シグネチャの更新確認を行い、更新必要時にはダウンロードおよびアップロード処理を実行する時間を設定します。更新の更新は00〜59分のランダムで実行されます。

現在の設定	設定の変更
シグネチャ更新確認時刻 (単位:時)	<input type="checkbox"/> 00 <input type="checkbox"/> 01 <input type="checkbox"/> 02 <input type="checkbox"/> 03 <input type="checkbox"/> 04 <input type="checkbox"/> 05 <input type="checkbox"/> 06 <input type="checkbox"/> 07 <input type="checkbox"/> 08 <input type="checkbox"/> 09 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23

UTM機能の設定

UTMリダイレクト

URLフィルタリング、Webガードのブロック時に表示したリダイレクトページのURLを指定します。未設定時は、リダイレクトせずに標準的なブロックページを表示します。最大127バイトまでのURLを設定できます(スキーム/パスを含む)。URLにポート番号指定はできません。

現在の設定	設定の変更
UTMリダイレクト設定	設定されていません <input type="text" value="http://www.example.com/block.html"/> <small>ルーティングがUTMブロックページにリダイレクトすることも可能です。 http://host.be.edu/reddns.jp/utm/block.html</small>

LEDの設定

UTM機能による検出時のLEDによる通知方法を設定します。ALM、LEDが2秒間連続で点滅時、VPN、PPP、BAKの点灯パターンでUTMの機能状態を知らせます。

LED通知設定

LEDによる通知開始時間を設定します。

現在の設定	設定の変更
LED通知設定	<input type="checkbox"/> 検出時 <input checked="" type="checkbox"/> ライセンス承認時 <input type="checkbox"/> UTM起動失敗時

検出時のLED通知時間設定

検出時にLEDによって通知継続する時間を設定します。

現在の設定	設定の変更
LED通知時間設定	<input type="radio"/> 通知し続ける <input checked="" type="radio"/> * [1] 時間通知する

セキュリティログの設定

UTMの各種機能で検出した異常をイベントログに記録するセキュリティログを設定します。

現在の設定	設定の変更
セキュリティログの有効化	<input checked="" type="checkbox"/> 有効 <input type="checkbox"/> 無効 * 有効
アンチウイルス(AV)	<input checked="" type="checkbox"/> 有効 <input type="checkbox"/> 無効 * 有効
不正侵入防止(IPS)	<input checked="" type="checkbox"/> 有効 <input type="checkbox"/> 無効 * 有効
Webガード(WG)	<input checked="" type="checkbox"/> 有効 <input type="checkbox"/> 無効 * 有効
URLフィルタリング(UF)	<input checked="" type="checkbox"/> 有効 <input type="checkbox"/> 無効 * 有効

NetMeisterへの通知設定

主要検出レポートの通知を有効にした場合、各機能の種類、スキャン数、検出数、ブロック数をNetMeisterへ通知します。セキュリティログの通知を有効にした場合、メール内容を除くすべての情報をNetMeisterへ通知します。

現在の設定	設定の変更
主要検出レポートの通知	<input checked="" type="checkbox"/> 有効 <input type="checkbox"/> 無効 * 有効
セキュリティログの通知	<input checked="" type="checkbox"/> 有効 <input type="checkbox"/> 無効

[戻り](#)

検出HTTPSポート番号の設定

URLフィルタリング、Webガードで検出するHTTPSポート番号を設定します(443を指定最大9件)。プロキシサーバを利用する場合、プロキシサーバのポート番号を指定してください。

[追加](#) [削除](#)

選択	番号	ポート番号
<input checked="" type="checkbox"/>	1	443

追加

0-65535のHTTPSポート番号を入力可能です。
空白、カンマ(,)で区切り複数件入力可能です。

[追加](#)

削除

選択したポート番号を削除します。
削除を反映させるためには装置の再起動が必要です。
ポート番号443は削除できません。

[削除](#)

4. 詳細設定

4.7.4 アンチウイルス(AV)の設定

アンチウイルス (AntiVirus) を設定します。

- (1) ログイン後のメニューエリアから[詳細設定]を選択し、「UTM」の詳細設定から[アンチウイルス (AV) の設定]をクリックします。

■管理者メニュー
トップページ
設定の保存
ログアウト

■かんたん設定
かんたん設定

■詳細設定
詳細設定
基本設定
パスワードの設定
装置名の設定
時刻の設定
保守の設定
NetMeisterの設定
ゼロタッチの設定

LAN
LANアドレスの設定
DHCPサーバの設定

WAN
プロバイダの設定
静的NAPTの設定
WANフィルタの設定
・IPv4
・IPv6
URLフィルタリングの設定
QoSの設定
通信セキュリティの設定

VPN・クラウド
VPNの設定
L2TPの設定
クラウドの設定

NGN網VPN
NGN網VPNの設定

デバイス
デバイスの設定

UTM
基本設定
詳細設定
アンチウイルス(AV)
不正侵入防止 (IPS)
Webガード(WG)
URLフィルタリング(UF)
グループポリシー設定
ホワイトリスト設定
UTM脅威レポート

■端末管理
端末管理

■保守管理
保守管理

■拡張ページ
拡張ページ

■外部リンク
製品ページ

詳細設定

シグネチャ設定

シグネチャ更新設定

シグネチャの更新確認を行い、更新必要時にはダウンロードおよびアップデート処理を実行する時間を設定します。実際の更新は00～59分のランダムで実行されます。

	現在の設定	設定の変更
シグネチャ更新確認時刻 (単位:時)	1時間ごと	<input type="checkbox"/> 00 <input type="checkbox"/> 01 <input type="checkbox"/> 02 <input type="checkbox"/> 03 <input type="checkbox"/> 04 <input type="checkbox"/> 05 <input type="checkbox"/> 06 <input type="checkbox"/> 07 <input type="checkbox"/> 08 <input type="checkbox"/> 09 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23

UTM機能の設定

UTMリダイレクト

URLフィルタリング、Webガードのブロック時に表示したいリダイレクトページのURLを指定します。未設定時は、リダイレクトせずに簡易的なブロックページを表示します。最大127バイトまでのURLを設定できます(スキーム・パスを含む)。URLにポート番号指定はできません。

	現在の設定	設定の変更
UTMリダイレクト設定	設定されていません	<input type="text" value="https://www.example.com/block.html"/> ルータ内蔵のUTMブロックページにリダイレクトすることも可能です。 <input type="text" value="http://host.ix-edu.nmddns.jp/utm/block.html"/>

検出HTTPSポート番号の設定

URLフィルタリング、Webガードで検出するHTTPSポート番号を設定します(443を含む最大9件)。プロキシサーバを利用する場合、プロキシサーバのポート番号を指定してください。

選択	番号	ポート番号
<input type="checkbox"/>	1	443

追加

0-65535のHTTPSポート番号を入力可能です。
空白、カンマ(,)で区切り複数件入力可能です。

削除

選択したポート番号を削除します。
削除を反映させるためには装置の再起動が必要です。
ポート番号443は削除できません。

4. 詳細設定

(2) 各項目を設定し、[反映]ボタンをクリックします。

注意 [反映]をクリックする前に個別許可一覧の[追加]または[削除]をクリックした場合、それまで入力した値はリセットされます。

アンチウイルス(AV) 変更対象: 共通ポリシー

ウイルスファイルがダウンロードされるのを検出する機能です。
グループ別ポリシーを設定する場合、右上の「変更対象」でグループを選択します。
設定の反映および削除は右上の「変更対象」で選択している共通ポリシーまたはグループに適用されます。
なお、グループ名やグループ対象の設定は、「UTM」の「グループ別ポリシー設定」ページから設定してください。

使用する設定の選択

	現在の設定	設定の変更
設定選択	共通ポリシー設定	<input checked="" type="radio"/> 共通ポリシー設定 <input type="radio"/> グループ別ポリシー設定

反映

脅威検出時の設定

ウイルスや危険なコードが含まれるプログラムデータを検出した場合の動作を設定します。

	現在の設定	設定の変更
脅威検出時の設定	無害化して透過	<input type="radio"/> 無害化せず透過 <input checked="" type="radio"/> 無害化して透過

ファイルのスキャン設定

ファイルのスキャン方法を設定します。

	現在の設定	設定の変更
圧縮ファイルのスキャン設定	有効	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
高圧縮ファイルのスキャン設定	無効	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効 100倍以上のサイズに解凍されるファイルのスキャン
スキャンサイズ設定	2MB	2 MB

プロトコルのスキャン設定

アンチウイルス機能の対象となるプロトコルを設定します。

	現在の設定	設定の変更
対象プロトコル	FTP, HTTP, IMAP4, POP3, SMTP	<input checked="" type="checkbox"/> FTP <input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> IMAP4 <input checked="" type="checkbox"/> POP3 <input checked="" type="checkbox"/> SMTP

反映

個別許可一覧

アンチウイルス(AV)での検出を無効化したいウイルスを、ウイルスID(VID)で設定します(最大10件)。

全選択 全解除

選択	番号	ウイルスID (VID)
<input type="checkbox"/>		設定されていません

追加

ウイルスID(VID、最大16桁)を入力可能です。
空白、カンマ(,)で区切り複数件入力可能です。
ウイルスID(VID)は脅威検出が通知されたセキュリティログ等を参照してください。

ウイルスID (VID)

900000000000000000.9000000010000000 9000000020000000

追加

削除

選択したウイルスID(VID)を削除します。

削除

4. 詳細設定

番号	項目	内容
①	変更対象	ポリシーを設定するグループを選択します。
②	設定選択	<p>変更対象で選択したグループに、共通ポリシーまたはグループ別ポリシーを設定します。</p> <p>メモ</p> <ul style="list-style-type: none"> 変更対象で共通ポリシーを選択した場合は、「共通ポリシー設定」のみが選択できます。 変更対象で共通ポリシー以外のグループを選択し、「共通ポリシーの設定」を選択した場合は該当のグループに共通ポリシーが適用され、「グループ別ポリシーの設定」を選択した場合はグループ別ポリシーが適用されます。 グループ別ポリシーを設定する場合は、あらかじめ「UTM」の「グループ別ポリシー設定」でグループ名およびグループ対象を設定してください。
③	脅威検出時の設定	ウイルスや危険なコードが含まれるプログラムデータを検出した場合の動作を設定します。
④	圧縮ファイルのスキャン設定	圧縮ファイルのウイルススキャンを有効化/無効化します。
⑤	高圧縮ファイルのスキャン設定	<p>高圧縮ファイルのウイルススキャンを有効化/無効化します。</p> <p>メモ</p> <ul style="list-style-type: none"> 高圧縮ファイルとは、解凍時に 100 倍以上のサイズに解凍されるファイルを表します。
⑥	スキャンサイズ設定	<p>ウイルススキャンするファイルの先頭からのサイズを設定します。</p> <ul style="list-style-type: none"> 半角数字で 1~20 まで入力できます。単位は MB です。
⑦	対象プロトコル	アンチウイルスの対象となるプロトコルを選択します。
⑧	個別許可一覧 全選択	<p>選択したウイルス ID に対して、一括削除することができます。[全選択]をクリックすると、ウイルス ID を全選択します。</p> <p>メモ</p> <ul style="list-style-type: none"> ウイルス ID (VID) は、脅威検出が通知されたセキュリティログ等を参照してください。
⑨	個別許可一覧 全解除	<p>選択したウイルス ID をすべて解除します。</p> <p>メモ</p> <ul style="list-style-type: none"> ウイルス ID (VID) は、脅威検出が通知されたセキュリティログ等を参照してください。
⑩	個別許可一覧 選択	<p>選択したウイルス ID に対して、一括削除することができます。</p> <p>ウイルス ID 単位で、個々に選択します。</p> <p>メモ</p> <ul style="list-style-type: none"> ウイルス ID (VID) は、脅威検出が通知されたセキュリティログ等を参照してください。
⑪	個別許可一覧 追加	<p>アンチウイルスでの検出を無効化したいウイルスを、ウイルス ID で設定します。</p> <ul style="list-style-type: none"> 最大 10 件まで入力できます。 半角数字 0~1000000000 を入力できます。 空白またはカンマで区切って複数のポート番号を同時に入力することもできます。 <p>メモ</p> <ul style="list-style-type: none"> ウイルス ID (VID) は、脅威検出が通知されたセキュリティログ等を参照してください。

4. 詳細設定

(3) 設定が反映されたことを確認します。

アンチウイルス(AV) 変更対象: [共通ポリシー]

ウイルスファイルがダウンロードされるのを検出する機能です。
グループ別ポリシーを設定する場合、右上の「変更対象」でグループを選択します。
設定の反映および削除は右上の「変更対象」で選択している共通ポリシーまたはグループに適用されます。
なお、グループ名やグループ対象の設定は、「UTM」の「グループ別ポリシー設定」ページから設定してください。

使用する設定の選択

	現在の設定	設定の変更
設定選択	共通ポリシー設定	<input checked="" type="radio"/> 共通ポリシー設定 <input type="radio"/> グループ別ポリシー設定

反映

脅威検出時の設定

ウイルスや危険なコードが含まれるプログラムデータを検出した場合の動作を設定します。

	現在の設定	設定の変更
脅威検出時の設定	無害化して透過	<input type="radio"/> 無害化せず透過 <input checked="" type="radio"/> 無害化して透過

ファイルのスキャン設定

ファイルのスキャン方法を設定します。

	現在の設定	設定の変更
圧縮ファイルのスキャン設定	有効	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
高圧縮ファイルのスキャン設定	無効	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効 100倍以上のサイズに解凍されるファイルのスキャン
スキャンサイズ設定	2MB	2 MB

プロトコルのスキャン設定

アンチウイルス機能の対象となるプロトコルを設定します。

	現在の設定	設定の変更
対象プロトコル	FTP, HTTP, IMAP4, POP3, SMTP	<input checked="" type="checkbox"/> FTP <input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> IMAP4 <input checked="" type="checkbox"/> POP3 <input checked="" type="checkbox"/> SMTP

反映

個別許可一覧

アンチウイルス(AV)での検出を無効化したいウイルスを、ウイルスID(VID)で設定します(最大10件)。

選択	番号	ウイルスID (VID)
<input type="checkbox"/>	1	1000000

追加

ウイルスID(VID、最大16桁)を入力可能です。
空白、カンマ(,)で区切り複数件入力可能です。
ウイルスID(VID)は脅威検出が通知されたセキュリティログ等を参照してください。

ウイルスID (VID)
90000000000000000000,9000000010000000 9000000020000000

削除

選択したウイルスID(VID)を削除します。

4. 詳細設定

4.7.5 不正侵入防止 (IPS) の設定

不正侵入防止 (Intrusion Prevention System) を設定します。

- (1) ログイン後のメニューエリアから[詳細設定]を選択し、「UTM」の詳細設定から[不正侵入防止 (IPS) の設定]をクリックします。

The screenshot shows a web-based configuration interface. On the left is a navigation menu with categories like 'Management Menu', 'Simple Settings', 'Detailed Settings', 'LAN', 'WAN', 'VPN', 'NGN', 'Device', 'UTM', and 'Terminal Management'. The 'Detailed Settings' section is expanded, and 'Intrusion Prevention (IPS)' is highlighted with a red box. The main content area is titled 'Detailed Settings' and is divided into sections: 'Signature Settings', 'UTM Function Settings', and 'Detection of HTTPS Port Number Settings'. The 'Signature Settings' section includes a table for 'Signature Update Confirmation Time (Unit: Hour)' with a grid of checkboxes for hours 00 through 23. The 'UTM Function Settings' section includes a table for 'UTM Redirect Settings' with a text input field for the URL. The 'Detection of HTTPS Port Number Settings' section includes a table for port numbers, a text input field for adding ports, and a 'Delete' button.

■管理者メニュー
トップページ
設定の保存
ログアウト

■かんたん設定
かんたん設定

■詳細設定
詳細設定
基本設定
パスワードの設定
装置名の設定
時刻の設定
保守の設定
NetMeisterの設定
ゼロタッチの設定

LAN
LANアドレスの設定
DHCPサーバの設定

WAN
プロバイダの設定
静的NAPTの設定
WANフィルタの設定
・IPv4
・IPv6
URLフィルタリングの設定
QoSの設定
通信セキュリティの設定

VPN・クラウド
VPNの設定
L2TPの設定
クラウドの設定

NGN網VPN
NGN網VPNの設定

デバイス
デバイスの設定

UTM
基本設定
詳細設定
アンチウイルス(AV)
不正侵入防止(IPS)
Webガード(WG)
URLフィルタリング(UF)
グループ別ポリシー設定
ホワイトリスト設定
UTM脅威レポート

■端末管理
端末管理

■保守管理
保守管理

■拡張ページ
拡張ページ

■外部リンク
製品ページ

詳細設定

シグネチャ設定

シグネチャ更新設定

シグネチャの更新確認を行い、更新必要時にはダウンロードおよびアップデート処理を実行する時間を設定します。実際の更新は00～59分のランダムで実行されます。

	現在の設定	設定の変更																							
シグネチャ更新確認時刻 (単位:時)	1時間ごと	<input type="checkbox"/> 00	<input type="checkbox"/> 01	<input type="checkbox"/> 02	<input type="checkbox"/> 03	<input type="checkbox"/> 04	<input type="checkbox"/> 05	<input type="checkbox"/> 06	<input type="checkbox"/> 07	<input type="checkbox"/> 08	<input type="checkbox"/> 09	<input type="checkbox"/> 10	<input type="checkbox"/> 11	<input type="checkbox"/> 12	<input type="checkbox"/> 13	<input type="checkbox"/> 14	<input type="checkbox"/> 15	<input type="checkbox"/> 16	<input type="checkbox"/> 17	<input type="checkbox"/> 18	<input type="checkbox"/> 19	<input type="checkbox"/> 20	<input type="checkbox"/> 21	<input type="checkbox"/> 22	<input type="checkbox"/> 23

UTM機能の設定

UTMリダイレクト

URLフィルタリング、Webガードのブロック時に表示したいリダイレクトページのURLを指定します。未設定時は、リダイレクトせずに簡易的なブロックページを表示します。最大127バイトまでのURLを設定できます(スキーム・パスを含む)。URLにポート番号指定はできません。

	現在の設定	設定の変更
UTMリダイレクト設定	設定されていません	<input type="text" value="https://www.example.com/block.html"/> ルータ内蔵のUTMブロックページにリダイレクトすることも可能です。 <input type="text" value="http://host.ix-edu.nmddns.jp/utm/block.html"/>

検出HTTPSポート番号の設定

URLフィルタリング、Webガードで検出するHTTPSポート番号を設定します(443を含む最大9件)。プロキシサーバを利用する場合、プロキシサーバのポート番号を指定してください。

選択	番号	ポート番号
<input type="checkbox"/>	1	443

追加

0-65535のHTTPSポート番号を入力可能です。
空白、カンマ(,)で区切り複数件入力可能です。

削除

選択したポート番号を削除します。
削除を反映させるためには装置の再起動が必要です。
ポート番号443は削除できません。

4. 詳細設定

(2) 各項目を設定し、[反映]ボタンをクリックします。

注意 [反映]をクリックする前に個別許可一覧の[追加]または[削除]をクリックした場合、それまで入力した値はリセットされます。

不正侵入防止(IPS) 変更対象: 共通ポリシー

DoS攻撃などのネットワーク異常・脅威を検出し、検出したトラフィックを遮断する機能です。
異常・脅威検出時の動作を設定します。
グループ別ポリシーを設定する場合、右上の「変更対象」でグループを選択します。
設定の反映および削除は右上の「変更対象」で選択している共通ポリシーまたはグループに適用されます。
なお、グループ名やグループ対象の設定は、「UTM」の「グループ別ポリシー設定」ページから設定してください。

使用する設定の選択

	現在の設定	設定の変更
設定選択	共通ポリシー設定	<input checked="" type="radio"/> 共通ポリシー設定 <input type="radio"/> グループ別ポリシー設定

反映

不正侵入検出時の設定

遮断時間は共通ポリシーでのみ設定でき、グループ全体に適用されます。

	現在の設定	設定の変更
不正侵入検出時の設定	遮断する	<input type="radio"/> 透過する <input checked="" type="radio"/> 遮断する
ポートスキャン検出機能	透過する 600秒	<input checked="" type="radio"/> 透過する <input type="radio"/> 遮断する 600 秒遮断する

反映

個別許可一覧

不正侵入防止(IPS)での検出を無効化したい脅威を、シグネチャID(SID)で設定します(最大100件)。

全選択 全解除

選択	番号	シグネチャID(SID)
		設定されていません

追加

0-1000000000のシグネチャID(SID)入力可能です。
空白、カンマ(,)で区切り複数件入力可能です。
シグネチャID(SID)は脅威検出が通知されたセキュリティログ等を参照してください。

シグネチャID(SID)
10000000, 11000000, 12000000

追加

削除

選択したシグネチャID(SID)を削除します。

削除

4. 詳細設定

番号	項目	内容
①	変更対象	ポリシーを設定するグループを選択します。
②	設定選択	<p>変更対象で選択したグループに、共通ポリシーまたはグループ別ポリシーを設定します。</p> <p>メモ</p> <ul style="list-style-type: none"> 変更対象で共通ポリシーを選択した場合は、「共通ポリシー設定」のみが選択できます。 変更対象で共通ポリシー以外のグループを選択し、「共通ポリシーの設定」を選択した場合は該当のグループに共通ポリシーが適用され、「グループ別ポリシーの設定」を選択した場合はグループ別ポリシーが適用されます。 グループ別ポリシーを設定する場合は、あらかじめ「UTM」の「グループ別ポリシー設定」でグループ名およびグループ対象を設定してください。
③	不正侵入検出時の設定	不正侵入を検出した場合に、検出したトラフィックを透過するか遮断するかを設定します。
④	ポートスキャン検出機能	<p>ポートスキャン攻撃を検出した場合に、検出したトラフィックを透過するか遮断するかを設定します。</p> <p>遮断する場合、検出したトラフィックを遮断する時間を設定します。</p> <ul style="list-style-type: none"> 半角数字で 600~1215752191 秒まで入力できます。
⑤	個別許可一覧 全選択	<p>選択したシグネチャIDに対して、一括削除することができます。[全選択]をクリックすると、シグネチャIDを全選択します。</p> <p>メモ</p> <ul style="list-style-type: none"> シグネチャID (SID) は、脅威検出が通知されたセキュリティログ等を参照してください。
⑥	個別許可一覧 全解除	<p>選択したシグネチャIDをすべて解除します。</p> <p>メモ</p> <ul style="list-style-type: none"> シグネチャID (SID) は、脅威検出が通知されたセキュリティログ等を参照してください。
⑦	個別許可一覧 選択	<p>選択したシグネチャIDに対して、一括削除することができます。</p> <p>シグネチャID単位で、個々に選択します。</p> <p>メモ</p> <ul style="list-style-type: none"> シグネチャID (SID) は、脅威検出が通知されたセキュリティログ等を参照してください。
⑧	個別許可一覧 追加	<p>不正侵入防止での検出を無効化したい脅威を、シグネチャIDで設定します。</p> <ul style="list-style-type: none"> 最大 100 件まで入力できます。 半角数字 0~10000000000 を入力できます。 空白またはカンマで区切って複数のポート番号を同時に入力することもできます。 <p>メモ</p> <ul style="list-style-type: none"> シグネチャID (DID) は、不正侵入が通知されたセキュリティログ等を参照してください。

4. 詳細設定

(3) 設定が反映されたことを確認します。

不正侵入防止(IPS) 変更対象: 共通ポリシー

DoS攻撃などのネットワーク異常・脅威を検出し、検出したトラフィックを遮断する機能です。
異常・脅威検出時の動作を設定します。
グループ別ポリシーを設定する場合、右上の「変更対象」でグループを選択します。
設定の反映および削除は右上の「変更対象」で選択している共通ポリシーまたはグループに適用されます。
なお、グループ名やグループ対象の設定は、「UTM」の「グループ別ポリシー設定」ページから設定してください。

使用する設定の選択

	現在の設定	設定の変更
設定選択	共通ポリシー設定	<input checked="" type="radio"/> 共通ポリシー設定 <input type="radio"/> グループ別ポリシー設定

反映

不正侵入検出時の設定

遮断時間は共通ポリシーでのみ設定でき、グループ全体に適用されます。

	現在の設定	設定の変更
不正侵入検出時の設定	遮断する	<input type="radio"/> 透過する <input checked="" type="radio"/> 遮断する
ポートスキャン検出機能	透過する	<input checked="" type="radio"/> 透過する <input type="radio"/> 遮断する
	600秒	800 <input type="text"/> 秒遮断する

反映

個別許可一覧

不正侵入防止(IPS)での検出を無効化したい脅威を、シグネチャID(SID)で設定します(最大100件)。

選択	番号	シグネチャID(SID)
<input type="checkbox"/>	1	1000000

追加

0-1000000000のシグネチャID(SID)入力可能です。
空白、カンマ(,)で区切り複数件入力可能です。
シグネチャID(SID)は脅威検出が通知されたセキュリティログ等を参照してください。

シグネチャID(SID)
<input type="text" value="10000000, 11000000 12000000"/>

追加

削除

選択したシグネチャID(SID)を削除します。

削除

4. 詳細設定

4.7.6 Web ガード (WG) の設定

Web ガード (Web Guard) を設定します。

- (1) ログイン後のメニューエリアから[詳細設定]を選択し、「UTM」の詳細設定から[Web ガード (WG) の設定]をクリックします。

The screenshot shows a configuration page with a left sidebar menu and a main content area. The sidebar menu includes sections like '管理者メニュー', 'かんたん設定', '詳細設定', 'LAN', 'WAN', 'VPN・クラウド', 'NGN網VPN', 'デバイス', 'UTM', '端末管理', '保守管理', '拡張ページ', and '外部リンク'. The '詳細設定' section is expanded, and 'Webガード(WG)' is highlighted with a red box. The main content area is titled '詳細設定' and contains several sub-sections: 'シグネチャ設定', 'UTM機能の設定', and '検出HTTPSポート番号の設定'. The 'シグネチャ設定' section includes a table for 'シグネチャ更新確認時刻 (単位:時)' with columns for '現在の設定' and '設定の変更'. The 'UTM機能の設定' section includes a table for 'UTMリダイレクト設定' with columns for '現在の設定' and '設定の変更'. The '検出HTTPSポート番号の設定' section includes a table for '検出HTTPSポート番号の設定' with columns for '選択', '番号', and 'ポート番号'. The 'Webガード(WG)' section is currently selected, and the '検出HTTPSポート番号の設定' section is visible below it.

管理者メニュー

- トップページ
- 設定の保存
- ログアウト

かんたん設定

- かんたん設定

詳細設定

- 詳細設定
- 基本設定
 - パスワードの設定
 - 装置名の設定
 - 時刻の設定
 - 保守の設定
 - NetMeisterの設定
 - ゼロタッチの設定
- LAN
 - LANアドレスの設定
 - DHCPサーバの設定
- WAN
 - プロバイダの設定
 - 静的NAPTの設定
 - WANフィルタの設定
 - IPv4
 - IPv6
 - URLフィルタリングの設定
 - QoSの設定
 - 通信セキュリティの設定
- VPN・クラウド
 - VPNの設定
 - L2TPの設定
 - クラウドの設定
- NGN網VPN
 - NGN網VPNの設定
- デバイス
 - デバイスの設定
- UTM
 - 基本設定
 - 詳細設定
 - アンチウイルス(AV)
 - 不正侵入防止(IPS)
 - Webガード(WG)**
 - URLフィルタリング(UF)
 - グループ別ポリシー設定
 - ホワイトリスト設定
 - UTM脅威レポート
- 端末管理
 - 端末管理
- 保守管理
 - 保守管理
- 拡張ページ
 - 拡張ページ
- 外部リンク
 - 製品ページ

詳細設定

シグネチャ設定

シグネチャ更新設定

シグネチャの更新確認を行い、更新必要時にはダウンロードおよびアップデート処理を実行する時間を設定します。実際の更新は00～59分のランダムで実行されます。

	現在の設定	設定の変更
シグネチャ更新確認時刻 (単位:時)	1時間ごと	<input type="checkbox"/> 00 <input type="checkbox"/> 01 <input type="checkbox"/> 02 <input type="checkbox"/> 03 <input type="checkbox"/> 04 <input type="checkbox"/> 05 <input type="checkbox"/> 06 <input type="checkbox"/> 07 <input type="checkbox"/> 08 <input type="checkbox"/> 09 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23

UTM機能の設定

UTMリダイレクト

URLフィルタリング、Webガードのブロック時に表示したいリダイレクトページのURLを指定します。未設定時は、リダイレクトせずに簡易的なブロックページを表示します。最大127バイトまでのURLを設定できます(スキーム・パスを含む)。URLにポート番号指定はできません。

	現在の設定	設定の変更
UTMリダイレクト設定	設定されていません	<input type="text" value="https://www.example.com/block.html"/> ルータ内蔵のUTMブロックページにリダイレクトすることも可能です。 <input type="text" value="http://host.ix-edu.nmddns.jp/utm/block.html"/>

検出HTTPSポート番号の設定

URLフィルタリング、Webガードで検出するHTTPSポート番号を設定します(443を含む最大9件)。プロキシサーバを利用する場合、プロキシサーバのポート番号を指定してください。

全選択	全解除	選択	番号	ポート番号
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	443

追加

0-65535のHTTPSポート番号を入力可能です。空白、カンマ(,)で区切り複数件入力可能です。

ポート番号
<input type="text" value="8080,10000 11000 12000"/>

追加

削除

選択したポート番号を削除します。削除を反映させるためには装置の再起動が必要です。ポート番号443は削除できません。

削除

4. 詳細設定

(2) 各項目を設定し、[反映]ボタンをクリックします。

注意 [反映]をクリックする前に個別許可一覧の[追加]または[削除]をクリックした場合、それまで入力した値はリセットされます。

Webガード(WG) 変更対象: 共通ポリシー

危険なウェブサイトへの通信を検出する機能です。
グループ別ポリシーを設定する場合、右上の「変更対象」でグループを選択します。
設定の反映および削除は右上の「変更対象」で選択している共通ポリシーまたはグループに適用されます。
なお、グループ名やグループ対象の設定は、「UTM」の「グループ別ポリシー設定」ページから設定してください。

使用する設定の選択

	現在の設定	設定の変更
設定選択	共通ポリシー設定	<input checked="" type="radio"/> 共通ポリシー設定 <input type="radio"/> グループ別ポリシー設定

Webガード検出時の設定

	現在の設定	設定の変更
Webガード検出時の設定	遮断する	<input type="radio"/> 透過する <input checked="" type="radio"/> 遮断する

個別許可一覧

Webガード(WG)で許可(透過)するURLを設定します(最大10件)。

選択	番号	URL
		設定されていません

追加
最大127文字までのURLを入力可能です。
http://, https://は入力不要です。
http:ドメインはホスト名を含む完全一致、パスは前方一致で判定します。
https:ドメインは(ホスト名含む)、完全一致で判定します。但し、パスは設定できません。
*はワイルドカードではなくURL文字として扱います。
空白、カンマ(,)で区切り複数件入力可能です。

URL
www.example1.jp www.example2.jp www.example3.jp/test

削除
選択したURLを削除します。

4. 詳細設定

番号	項目	内容
①	変更対象	ポリシーを設定するグループを選択します。
②	設定選択	変更対象で選択したグループに、共通ポリシーまたはグループ別ポリシーを設定します。 メモ <ul style="list-style-type: none">変更対象で共通ポリシーを選択した場合は、「共通ポリシー設定」のみが選択できます。変更対象で共通ポリシー以外のグループを選択し、「共通ポリシーの設定」を選択した場合は該当のグループに共通ポリシーが適用され、「グループ別ポリシーの設定」を選択した場合はグループ別ポリシーが適用されます。グループ別ポリシーを設定する場合は、あらかじめ「UTM」の「グループ別ポリシー設定」でグループ名およびグループ対象を設定してください。
③	Web ガード検出時の設定	危険な Web サイトへの通信を検出した場合に、検出したトラフィックを透過するか遮断するかを設定します。
④	個別許可一覧 全選択	選択した URL に対して、一括削除することができます。[全選択]をクリックすると、URL を全選択します。
⑤	個別許可一覧 全解除	選択した URL をすべて解除します。
⑥	個別許可一覧 選択	選択した URL に対して、一括削除することができます。 URL 単位で、個々に選択します。
⑦	個別許可一覧 追加	Web ガードでの検出を無効化したい通信を、URL で設定します。 <ul style="list-style-type: none">最大 10 件まで入力できます。最大 127 文字までの URL を入力できます。空白またはカンマで区切って複数のポート番号を同時に入力することもできます。 注意 <ul style="list-style-type: none">http://、https://は入力しないでください。* (アスタリスク) は、ワイルドカードではなく、URL 文字として扱います。

4. 詳細設定

(3) 設定が反映されたことを確認します。

Webガード(WG) 変更対象: 共通ポリシー

危険なウェブサイトへの通信を検出する機能です。
グループ別ポリシーを設定する場合、右上の「変更対象」でグループを選択します。
設定の反映および削除は右上の「変更対象」で選択している共通ポリシーまたはグループに適用されます。
なお、グループ名やグループ対象の設定は、「UTM」の「グループ別ポリシー設定」ページから設定してください。

使用する設定の選択

	現在の設定	設定の変更
設定選択	共通ポリシー設定	<input checked="" type="radio"/> 共通ポリシー設定 <input type="radio"/> グループ別ポリシー設定

Webガード検出時の設定

	現在の設定	設定の変更
Webガード検出時の設定	遮断する	<input type="radio"/> 透過する <input checked="" type="radio"/> 遮断する

個別許可一覧

Webガード(WG)で許可(透過)するURLを設定します(最大10件)。

選択	番号	URL
<input type="checkbox"/>	1	www.example.com

追加

最大127文字までのURLを入力可能です。
http://, https://は入力不要です。
http:ドメインはホスト名を含む完全一致、パスは前方一致で判定します。
https:ドメインは(ホスト名含む)、完全一致で判定します。但し、パスは設定できません。
*はワイルドカードではなくURL文字として扱います。
空白、カンマ(,)で区切り複数件入力可能です。

URL

削除

選択したURLを削除します。

4. 詳細設定

4.7.7 URL フィルタリング(UF)の設定

URL フィルタリング (URL Filtering) を設定します。

- (1) ログイン後のメニューエリアから[詳細設定]を選択し、「UTM」の詳細設定から[URL フィルタリング (UF) の設定]をクリックします。

■管理者メニュー
トップページ
設定の保存
ログアウト

■かんたん設定
かんたん設定

■詳細設定
詳細設定
基本設定
パスワードの設定
装置名の設定
時刻の設定
保守の設定
NetMeisterの設定
ゼロタッチの設定

LAN
LANアドレスの設定
DHCPサーバの設定

WAN
プロバイダの設定
静的NAPTの設定
WANフィルタの設定
・IPv4
・IPv6
URLフィルタリングの設定
QoSの設定
通信セキュリティの設定

VPN・クラウド
VPNの設定
L2TPの設定
クラウドの設定

NGN網VPN
NGN網VPNの設定

デバイス
デバイスの設定

UTM
基本設定
詳細設定
アンチウイルス(AV)
不正侵入防止(IPS)
Webガード(WG)
URLフィルタリング(UF)
グループ別ポリシー設定
ホワイトリスト設定
UTM脅威レポート

■端末管理
端末管理

■保守管理
保守管理

■拡張ページ
拡張ページ

■外部リンク
製品ページ

詳細設定

シグネチャ設定

シグネチャ更新設定
シグネチャの更新確認を行い、更新必要時にはダウンロードおよびアップデート処理を実行する時間を設定します。
実際の更新は00～59分のランダムで実行されます。

	現在の設定	設定の変更
シグネチャ更新確認時刻 (単位:時)	1時間ごと	<input type="checkbox"/> 00 <input type="checkbox"/> 01 <input type="checkbox"/> 02 <input type="checkbox"/> 03 <input type="checkbox"/> 04 <input type="checkbox"/> 05 <input type="checkbox"/> 06 <input type="checkbox"/> 07 <input type="checkbox"/> 08 <input type="checkbox"/> 09 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23

UTM機能の設定

UTMリダイレクト

URLフィルタリング、Webガードのブロック時に表示したいリダイレクトページのURLを指定します。
未設定時は、リダイレクトせずに簡易的なブロックページを表示します。
最大127バイトまでのURLを設定できます(スキーム・パスを含む)。
URLにポート番号指定はできません。

	現在の設定	設定の変更
UTMリダイレクト設定	設定されていません	<input type="text" value="https://www.example.com/block.html"/> ルータ内蔵のUTMブロックページにリダイレクトすることも可能です。 http://host.ix-edu.nmddns.jp/utm/block.html

検出HTTPSポート番号の設定

URLフィルタリング、Webガードで検出するHTTPSポート番号を設定します(443を含む最大9件)。
プロキシサーバを利用する場合、プロキシサーバのポート番号を指定してください。

選択	番号	ポート番号
<input checked="" type="checkbox"/>	1	443

追加

0-65535のHTTPSポート番号を入力可能です。
空白、カンマ(,)で区切り複数件入力可能です。

削除

選択したポート番号を削除します。
削除を反映させるためには装置の再起動が必要です。
ポート番号443は削除できません。

4. 詳細設定

(2) 各項目を設定し、[反映]ボタンをクリックします。

注意 [反映]をクリックする前に個別許可一覧の[追加]、[削除]、[変更]または[カテゴリ問い合わせ]をクリックした場合、それまで入力した値はリセットされます。

URLフィルタリング(UF) 変更対象: [共通ポリシー]

指定されたカテゴリに属するウェブサイトへの通信を弾く機能です。
グループ別ポリシーを設定する場合、右上の「変更対象」でグループを選択します。
設定の反映および削除は右上の「変更対象」で選択している共通ポリシーまたはグループに適用されます。
なお、グループ名やグループ対象の設定は、「UTM」の「グループ別ポリシー設定」ページから設定してください。

使用する設定の選択

	現在の設定	設定の変更
設定選択	共通ポリシー設定	<input checked="" type="radio"/> 共通ポリシー設定 <input type="radio"/> グループ別ポリシー設定

[反映]

試験運用設定

統計情報やセキュリティログではブロックしたかのように通知しますが、実際はブロックしません。
 遮断設定に関わらずブロックしない

遮断設定

	現在の設定	設定の変更
カテゴリ不明サイトをブロックする	無効	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
カテゴリ判定不可時にブロックする	無効	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効

[反映]

URLカテゴリクエリ

指定されたURLのウェブサイトが属するカテゴリをサーバへ問い合わせます。

[カテゴリ問い合わせ]

ブロックカテゴリ設定

Web閲覧を制限するWebサイトのカテゴリを設定します。
変更ボタンを押すとブロックカテゴリ選択画面が表示されます。

[変更]

ブロックカテゴリ	カテゴリ名
10000	ポルノ
11000	アダルト
12000	ギャンブル・盗くじ
...	...

個別許可一覧

URLフィルタリング(UF)で許可(透過)するURLを設定します(最大100件)。

全選択	全解除	選択	番号	URL
				設定されていません
		<input type="checkbox"/>		追加

最大126文字までのURLを入力可能です。
http://, https://は入力不要です。
ドメイン前方の*(ワイルドカード)を許可します。後方または中間の*指定による部分一致は許可しません。
ドメイン前方の*(ワイルドカード)とパス指定の併用はできません。
先頭文字に*(ワイルドカード)を設定した場合は、ホスト名およびサブドメインについてもワイルドカードとして判定されます。
(例) *aaa.bbb.nec.co.jp と記載した場合、*nec.co.jp として扱われます。
ホスト名の先頭文字に*(アスタリスク)を設定した場合は、サブドメインをワイルドカードとして判定します。このときパスは判定しません。
ホスト名の先頭文字に*を設定していない場合は完全一致で、パスは前方一致で判定します。HTTPSの場合は、ホスト名のみで判定します。
https:ドメインおよびホスト名のみで判定、パス指定の併用はできません。
空白、カンマ(,)で区切り複数件入力可能です。

URL
www.example1.jp, www.example2.jp, www.example3.jp/test

[追加]

削除
選択したURLを削除します。

[削除]

4. 詳細設定

番号	項目	内容
①	変更対象	ポリシーを設定するグループを選択します。
②	設定選択	<p>変更対象で選択したグループに、共通ポリシーまたはグループ別ポリシーを設定します。</p> <p>メモ</p> <ul style="list-style-type: none"> 変更対象で共通ポリシーを選択した場合は、「共通ポリシー設定」のみが選択できます。 変更対象で共通ポリシー以外のグループを選択し、「共通ポリシーの設定」を選択した場合は該当のグループに共通ポリシーが適用され、「グループ別ポリシーの設定」を選択した場合はグループ別ポリシーが適用されます。 グループ別ポリシーを設定する場合は、あらかじめ「UTM」の「グループ別ポリシー設定」でグループ名およびグループ対象を設定してください。
③	カテゴリ不明サイトをブロックする	URL フィルタリングを実施した結果、カテゴリが定義されていないサイトをアクセスしたと判断された場合に、その URL アクセスを透過するか遮断(ブロック)するかを設定します。
④	カテゴリ判定不可時にブロックする	URL フィルタリングを実施した結果、URL フィルタリングサーバから応答が無かった場合に該当の URL アクセスを透過するか遮断(ブロック)するかを設定します。
⑤	カテゴリ問い合わせ	<p>URL カテゴリクエリ画面に遷移します。</p> <p>URL を指定して、その Web サイトが属するカテゴリをサーバに問い合わせることができます。</p>
⑥	ブロックカテゴリ設定	Web 閲覧を制限する Web サイトのカテゴリを設定します。[変更]ボタンをクリックして、ブロックカテゴリを設定します。
⑦	個別許可一覧 全選択	選択した URL に対して、一括削除することができます。[全選択]をクリックすると、URL を全選択します。
⑧	個別許可一覧 全解除	選択した URL をすべて解除します。
⑨	個別許可一覧 選択	<p>選択した URL に対して、一括削除することができます。</p> <p>URL 単位で、個々に選択します。</p>
⑩	個別許可一覧 追加	<p>URL フィルタリングで許可(透過)する URL を設定します。</p> <ul style="list-style-type: none"> 最大 100 件まで入力できます。 最大 126 文字の URL を入力できます。 空白またはカンマで区切って複数のポート番号を同時に入力することもできます。

4. 詳細設定

[カテゴリ問い合わせ]をクリックした場合は、URL を指定して、その Web サイトが属するカテゴリをサーバに問い合わせることができます。問い合わせ内容を入力して、[反映]をクリックします。

URLフィルタリング(UF)

URLカテゴリクエリ

指定されたURLのウェブサイトが属するカテゴリをサーバへ問い合わせます。
URLのドメイン部のみ入力してください。
最大127文字までのURLを入力可能で、使用可能文字列は半角英数字、.(ドット)、-(ハイフン)です。
http://, https://は不要です。
UTMライセンスの認証に成功していない場合、問い合わせをすることはできません。

戻る 反映

問い合わせ結果	
カテゴリ番号	
カテゴリ	
URL	

番号	項目	内容
①	問い合わせ内容	URL のドメイン部までを入力します。 ・ 半角英数字、.(ドット)、-(ハイフン)で、127 文字まで入力できます。

4. 詳細設定

(3) [変更]ボタンをクリックし、ブロックカテゴリを選択し、[反映]をクリックします。

URLフィルタリング(UF) 変更対象: 共通ポリシー

グループ別ポリシーを設定する場合、右上の「変更対象」でグループを選択します。
設定の反映および削除は右上の「変更対象」で選択している共通ポリシーまたはグループに適用されます。
なお、グループ名やグループ対象の設定は、「UTM」の「グループ別ポリシー設定」ページから設定してください。

テンプレートの選択

ブロックカテゴリの設定にテンプレートを使用します。

テンプレート	設定の変更
	初期設定時は、「使用する」を選択しなくても基本設定でカテゴリを選択します。 <input type="checkbox"/> テンプレートを使用する

ブロックカテゴリの設定

ブロックするカテゴリを選択します。

	設定の変更
<input type="checkbox"/> アダルト	<input type="checkbox"/> 10000: ポルノ <input type="checkbox"/> 11000: アダルトサイト <input type="checkbox"/> 12000: キャンブル・宝くじ <input type="checkbox"/> 13000: アルコール・たばこ <input type="checkbox"/> 14000: ドラッグ <input type="checkbox"/> 15000: 過激論・人種差別 <input type="checkbox"/> 16000: 中絶 <input type="checkbox"/> 17000: 犯罪行為 <input type="checkbox"/> 18000: 暴力的なサイト <input type="checkbox"/> 19000: 気持ち悪いサイト <input type="checkbox"/> 22000: 出会い系サイト
<input type="checkbox"/> エンターテインメント	<input type="checkbox"/> 20000: ゲーム <input type="checkbox"/> 25000: ショッピング・オークション <input type="checkbox"/> 26000: ミュージック <input type="checkbox"/> 27000: コミック・アニメ <input type="checkbox"/> 28000: エンターテインメント・芸術 <input type="checkbox"/> 29000: ストリーミング・VoIP <input type="checkbox"/> 62000: スポーツ
<input type="checkbox"/> SNS	<input type="checkbox"/> 21000: インスタントメッセージ <input type="checkbox"/> 23000: ソーシャルネットワーク <input type="checkbox"/> 24000: Webチャットルーム <input type="checkbox"/> 66000: フォーラム・ニュースグループ <input type="checkbox"/> 67000: ブログと個人サイト
<input type="checkbox"/> ITサービス	<input type="checkbox"/> 30000: P2P <input type="checkbox"/> 31000: マルチメディアダウンロード <input type="checkbox"/> 32000: オンライン共有・ストレージ <input type="checkbox"/> 33000: シェアウェア・フリーウェア <input type="checkbox"/> 34000: Webメール <input type="checkbox"/> 35000: システム更新 <input type="checkbox"/> 36000: コンテンツ配信サーバ <input type="checkbox"/> 37000: WebサービスAPI <input type="checkbox"/> 38000: ネットワークサービス <input type="checkbox"/> 50000: コンピュータ・IT <input type="checkbox"/> 69000: ドメインパーキング
<input type="checkbox"/> セキュリティ	<input type="checkbox"/> 39000: リモートコントロール <input type="checkbox"/> 40000: プロキシ・匿名化
<input type="checkbox"/> 危険なサイト	<input type="checkbox"/> 41000: フィッシング詐欺 <input type="checkbox"/> 42000: マルウェア <input type="checkbox"/> 43000: ブラックハット SEO サイト <input type="checkbox"/> 44000: 危険アプリケーション
<input type="checkbox"/> 広告	<input type="checkbox"/> 45000: 広告
<input type="checkbox"/> プロバイダ・ポータル・ホスティング	<input type="checkbox"/> 46000: ポータル・検索サイト
<input type="checkbox"/> 生活と暮らし	<input type="checkbox"/> 47000: 輸送機関 <input type="checkbox"/> 57000: 旅行 <input type="checkbox"/> 58000: 飲食初 <input type="checkbox"/> 59000: 家・庭 <input type="checkbox"/> 61000: 宗教・数秘術 <input type="checkbox"/> 63000: 自動車
<input type="checkbox"/> 金融	<input type="checkbox"/> 48000: 不動産 <input type="checkbox"/> 49000: 金融・保険
<input type="checkbox"/> ビジネス・経済	<input type="checkbox"/> 51000: ビジネス・サービス <input type="checkbox"/> 64000: 求人情報
<input type="checkbox"/> 学術・教育	<input type="checkbox"/> 52000: 参考文献・研究 <input type="checkbox"/> 53000: 教育機関
<input type="checkbox"/> 青年・成人向け	<input type="checkbox"/> 54000: 軍事・兵器
<input type="checkbox"/> 政治・行政	<input type="checkbox"/> 55000: 政治・政府
<input type="checkbox"/> 医療と健康	<input type="checkbox"/> 60000: 健康・医学
<input type="checkbox"/> ニュース	<input type="checkbox"/> 65000: ニュース・メディア
<input type="checkbox"/> 各種サービス	<input type="checkbox"/> 56000: 協会・慈善団体
<input type="checkbox"/> その他	<input type="checkbox"/> 68000: 不明なサイト <input type="checkbox"/> 70000: テッドサイト <input type="checkbox"/> 71000: プライベートIPアドレス

戻る 反映

4. 詳細設定

番号	項目	内容
①	変更対象	ポリシーを設定するグループを選択します。
②	テンプレートの選択	「テンプレートを使用する」を選択した場合、「基本設定」「全選択」「全解除」のいずれかを選択できるようになります。 <ul style="list-style-type: none">• 基本設定は、最も基本的なカテゴリが一括で選択されます。• 全選択は、すべてのカテゴリが一括で選択されます。• 全解除は、すべてのカテゴリが一括で選択解除されます。
③	ブロックカテゴリの設定	ブロックするカテゴリを個別に選択あるいは解除します。

4. 詳細設定

(4) 設定が反映されたことを確認します。

URLフィルタリング(UF) 変更対象: [共通ポリシー]

指定されたカテゴリに属するウェブサイトへの通信を検出する機能です。
グループ別ポリシーを設定する場合、右上の「変更対象」でグループを選択します。
設定の反映および削除は右上の「変更対象」で選択している共通ポリシーまたはグループに適用されます。
なお、グループ名やグループ対象の設定は、「UTM」の「グループ別ポリシー設定」ページから設定してください。

使用する設定の選択

	現在の設定	設定の変更
設定選択	共通ポリシー設定	<input checked="" type="radio"/> 共通ポリシー設定 <input type="radio"/> グループ別ポリシー設定

試験運用設定

統計情報やセキュリティログではブロックしたかのように通知しますが、実際はブロックしません。

遮断設定に関わらずブロックしない

遮断設定

	現在の設定	設定の変更
カテゴリ不明サイトをブロックする	無効	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
カテゴリ判定不可時にブロックする	無効	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効

URLカテゴリクエリ

指定されたURLのウェブサイトが属するカテゴリをサーバへ問い合わせます。

ブロックカテゴリ設定

Web閲覧を制限するWebサイトのカテゴリを設定します。
変更ボタンを押すとブロックカテゴリ選択画面が表示されます。

ブロックカテゴリ	カテゴリ名
10000	ポルノ
11000	アダルト
12000	キャンブル・宝くじ
...	...

個別許可一覧

URLフィルタリング(UF)で許可(透過)するURLを設定します(最大100件)。

選択	番号	URL
<input type="checkbox"/>	1	www.example.com

追加

最大126文字までのURLを入力可能です。
http://, https://は入力不要です。
ドメイン前方の*(ワイルドカード)を許可します。後方または中間の*指定による部分一致は許可しません。
ドメイン前方の*(ワイルドカード)とパス指定の併用はできません。
先頭文字に*(ワイルドカード)を設定した場合は、ホスト名およびサブドメインについてもワイルドカードとして判定されます。
(例) *aaa.bbb.nec.co.jp と記載した場合、*nec.co.jp として扱われます。
ホスト名の先頭文字に*(アスタリスク)を設定した場合は、サブドメインをワイルドカードとして判定します。このときパスは判定しません。
ホスト名の先頭文字に*(アスタリスク)を設定していない場合は完全一致で、パス名は前方一致で判定します。HTTPSの場合は、ホスト名のみで判定します。
https:ドメインおよびホスト名のみで判定。パス指定の併用はできません。
空白、カンマ(,)で区切り複数件入力可能です。

www.example1.jp, www.example2.jp, www.example3.jp/test

削除

選択したURLを削除します。

4. 詳細設定

4.7.8 グループ別ポリシー設定

グループを作成して、それぞれのグループに UTM のポリシーを設定します。

- (1) ログイン後のメニューエリアから[詳細設定]を選択し、「UTM」の項目から[グループ別ポリシー設定]をクリックします。

グループ別ポリシー設定 変更対象: 1:未設定

グループ名の設定とグループ対象の通信を設定します。
グループ別ポリシーを設定する場合、右上の「変更対象」でグループを選択します。
設定の反映および削除は右上の「変更対象」で選択しているグループに適用されます。
なお、グループのUTMポリシーは「詳細設定」の各UTM機能ページから設定してください。

グループ名設定

変更対象で選択しているグループ名を設定します。

	現在の設定	設定の変更
グループ名設定	設定されていません	グループ名

グループ対象一覧

グループ対象(IPv4)

選択	グループ対象	プロトコル	送信元(送信先) IPv4アドレス	ポート番号	送信先(送信元) IPv4アドレス	ポート番号
設定されていません						

グループ対象(IPv6)

選択	グループ対象	プロトコル	送信元(送信先) IPv6アドレス	ポート番号	送信先(送信元) IPv6アドレス	ポート番号
設定されていません						

グループ対象の追加

設定したグループ対象は送信元/送信先を反転させた逆方向でも評価を行います。
(例) 送信元192.168.0.11/32から送信先10.0.0.11/32を適用しないに設定した場合、
逆方向の通信となる送信元 10.0.0.11/32から送信先 192.168.0.11/32のパケットも適用処理は行われません。
ポート番号で範囲指定をする場合、ハイフン(-)を利用し設定してください(例:1-100)。

IP	グループ対象	プロトコル	送信元(送信先)		送信先(送信元)	
			IPアドレス	ポート番号	IPアドレス	ポート番号
IPv4	すべて	すべて	<input checked="" type="radio"/> すべて <input type="radio"/> 指定	<input checked="" type="radio"/> すべて <input type="radio"/> 指定	<input checked="" type="radio"/> すべて <input type="radio"/> 指定	<input checked="" type="radio"/> すべて <input type="radio"/> 指定

4. 詳細設定

- (2) グループ設定は、グループ名を入力して[反映]ボタンをクリックします。グループ対象一覧で項目を削除する場合は、各項目を選択し、[削除]ボタンをクリックします。グループ対象を追加する場合は、グループ対象の追加で各項目を設定し、[追加]ボタンをクリックします。

グループ別ポリシー設定 変更対象: [1:未設定]

グループ名の設定とグループ対象の通信を設定します。
 グループ別ポリシーを設定する場合、右上の「変更対象」でグループを選択します。
 設定の反映および削除は右上の「変更対象」で選択しているグループに適用されます。
 なお、グループのUTMポリシーは「詳細設定」の各UTM機能ページから設定してください。

グループ名設定

変更対象で選択しているグループ名を設定します。

グループ名設定	現在の設定	設定の変更
	設定されていません	グループ名 <input type="text"/>

反映

グループ対象一覧

グループ対象(IPv4)

選択	グループ対象	プロトコル	送信元(送信先)	ポート番号	送信先(送信元)	ポート番号
<input type="checkbox"/>			IPv4アドレス		IPv4アドレス	

削除

グループ対象(IPv6)

選択	グループ対象	プロトコル	送信元(送信先)	ポート番号	送信先(送信元)	ポート番号
<input type="checkbox"/>			IPv6アドレス		IPv6アドレス	

削除

グループ対象の追加

設定したグループ対象は送信元/送信先を反転させた逆方向でも評価を行います。
 (例) 送信元192.168.0.11/32から送信先10.0.0.11/32を適用しないに設定した場合、
 逆方向の通信となる送信元 10.0.0.11/32から送信先 192.168.0.11/32のパケットも適用処理は行われません。
 ポート番号で範囲指定する場合、ハイフン(-)を利用し設定してください(例:1-100)。

IP	グループ対象	プロトコル	送信元(送信先)	ポート番号	送信先(送信元)	ポート番号
IPv4	<input type="text"/>	<input type="text"/>	IPアドレス	ポート番号	IPアドレス	ポート番号
			<input checked="" type="radio"/> すべて <input type="radio"/> 指定	<input checked="" type="radio"/> すべて <input type="radio"/> 指定	<input checked="" type="radio"/> すべて <input type="radio"/> 指定	<input checked="" type="radio"/> すべて <input type="radio"/> 指定

追加

4. 詳細設定

番号	項目	内容
①	変更対象	ポリシーを設定するグループを選択します。
②	グループ名設定 グループ名設定	変更対象にグループ名称を設定します。 ・ 任意の文字列でグループ名を入力します。
③	グループ名設定 反映	設定されたグループ名を設定に反映します。
④	グループ対象 (IPv4) グループ対象	グループ対象に[する]、[しない]を選択します。 ・ [する]はグループ対象とし、[しない]はグループ対象から除外します。
⑤	グループ対象 (IPv4) 全選択	選択したグループ対象 (IPv4) に対して、一括削除することができます。[全選択]をクリックすると、グループ対象 (IPv4) を全選択します。
⑥	グループ対象 (IPv4) 全解除	選択したグループ対象 (IPv4) をすべて解除します。
⑦	グループ対象 (IPv4) 選択	選択したグループ対象 (IPv4) に対して、一括削除することができます。 グループ対象 (IPv4) 単位で、個々に選択します。
⑧	グループ対象 (IPv6) グループ対象	グループ対象に[する]、[しない]を選択します。 ・ [する]はグループ対象とし、[しない]はグループ対象から除外します。
⑨	グループ対象 (IPv6) 全選択	選択したグループ対象 (IPv6) に対して、一括削除することができます。[全選択]をクリックすると、グループ対象 (IPv6) を全選択します。
⑩	グループ対象 (IPv6) 全解除	選択したグループ対象 (IPv6) をすべて解除します。
⑪	グループ対象 (IPv6) 選択	選択したグループ対象 (IPv6) に対して、一括削除することができます。 グループ対象 (IPv6) 単位で、個々に選択します。
⑫	グループ対象の追加 IP	IPv4 か、IPv6 かを選択します。
⑬	グループ対象の追加 グループ対象	グループ対象をチェック対象とするか、否かを選択します。 ・ [しない] / [する] から選択します。
⑭	グループ対象の追加 プロトコル	プロトコルを、[すべて]、[TCP]、[UDP]、[ICMP] または [指定] から選択します。 ・ 「指定」を選択したときは、プロトコル番号 (1~255) を入力します。
⑮	グループ対象の追加 送信元 (送信先) IP アドレス	IP アドレスを設定します。 ・ IP アドレスは、[すべて]、[指定] から選択します。 ・ [すべて]を選択した場合、すべての IP アドレスが対象となります。 ・ [指定]を選択した場合、ネットワークアドレスを入力するボックスが表示されるため、ネットワークアドレスを入力します。
⑯	グループ対象の追加 送信元 (送信先) ポート番号	ポート番号を設定します。 ・ ポートは、[すべて]、[指定] から選択します。 ・ [すべて]を選択した場合、すべてのポートが対象となります。 ・ [指定]を選択した場合、ポート番号を入力するボックスが表示されるため、そのボックスで番号の範囲を指定することができます。 メモ ・ プロトコルが TCP または UDP 以外が指定されている場合は、ポート番号の指定はできません。
⑰	グループ対象の追加 送信先 (送信元) IP アドレス	IP アドレスを設定します。 ・ IP アドレスは、[すべて]、[指定] から選択します。 ・ [すべて]を選択した場合、すべての IP アドレスが対象となります。 ・ [指定]を選択した場合、ネットワークアドレスを入力するボックスが表示されるため、ネットワークアドレスを入力します。

4. 詳細設定

⑱	グループ対象の追加 送信先(送信元) ポート番号	ポート番号を設定します。 <ul style="list-style-type: none">• ポートは、[すべて]、[指定]から選択します。• [すべて]を選択した場合、すべてのポートが対象となります。• [指定]を選択した場合、ポート番号を入力するボックスが表示されるため、そのボックスで番号の範囲を指定することができます。 <div data-bbox="568 387 616 421" style="border: 1px solid black; padding: 2px;">メモ</div> <ul style="list-style-type: none">• プロトコルが TCP または UDP 以外が指定されている場合は、ポート番号の指定はできません。
⑲	グループ対象の追加 追加	設定されたグループ対象を追加します。

4. 詳細設定

(3) 設定が反映されたことを確認します。

グループ別ポリシー設定

変更対象: [1:グループ1]

グループ名の設定とグループ対象の通信を設定します。
 グループ別ポリシーを設定する場合、右上の「変更対象」でグループを選択します。
 設定の反映および削除は右上の「変更対象」で選択しているグループに適用されます。
 なお、グループのUTMポリシーは「詳細設定」の各UTM機能ページから設定してください。

グループ名設定

変更対象で選択しているグループ名を設定します。

グループ名設定	現在の設定	設定の変更
	グループ1	<input type="text" value="グループ1"/>

[反映]

グループ対象一覧

グループ対象 (IPv4)

[全選択] [全解除]

選択	グループ対象	プロトコル	送信元(送信元)		送信先(送信先)	
			IPv4アドレス	ポート番号	IPv4アドレス	ポート番号
<input type="checkbox"/>	する	TCP	<input type="text" value="10.0.0.0/24"/>	すべて	<input type="text" value="10.0.0.0/24"/>	すべて
<input type="checkbox"/>	する	TCP	<input type="text" value="10.0.0.0/24"/>	すべて	<input type="text" value="10.0.0.0/24"/>	すべて

[削除]

グループ対象 (IPv6)

[全選択] [全解除]

選択	グループ対象	プロトコル	送信元(送信元)		送信先(送信先)	
			IPv6アドレス	ポート番号	IPv6アドレス	ポート番号
<input type="checkbox"/>	する	TCP	<input type="text" value=":::1"/>	すべて	<input type="text" value=":::1"/>	すべて

[削除]

グループ対象の追加

設定したグループ対象は送信元/送信先を反転させた応方向でも評価を行います。
 (例) 送信元192.168.0.11/32から送信先10.0.0.11/32を適用「しない」に設定した場合、
 応向きの通信となる送信元 10.0.0.11/32から送信先 192.168.0.11/32の/ケットも適用処理は行われません。
 ポート番号で範囲指定をする場合、ハイフン(-)を利用し設定してください(例: 1-100)。

IP	グループ対象	プロトコル	送信元(送信元)		送信先(送信先)	
			IPアドレス	ポート番号	IPアドレス	ポート番号
IPv4	する	すべて	<input checked="" type="radio"/> すべて <input type="radio"/> 指定	<input checked="" type="radio"/> すべて <input type="radio"/> 指定	<input checked="" type="radio"/> すべて <input type="radio"/> 指定	<input checked="" type="radio"/> すべて <input type="radio"/> 指定

[追加]

4. 詳細設定

4.7.9 ホワイトリスト設定

UTM を通さず、無条件で許可するトラフィックやホストをホワイトリストとして設定します。

- (1) ログイン後のメニューエリアから[詳細設定]を選択し、「UTM」の項目から[ホワイトリスト設定]をクリックします。

ホワイトリスト設定 変更対象:

UTMを通さず、無条件で許可するトラフィックやホストを設定します。
個別機能を設定をする場合、右上にある「変更対象」にて選択してください。
設定の反映および削除は右上の「変更対象」で選択しているすべてまたは個別機能の設定に適用されます。

IPv4ホワイトリスト一覧

選択	UTMチェック	プロトコル	送信元(送信先)		送信先(送信元)	
			IPv4アドレス	ポート番号	IPv4アドレス	ポート番号
設定されていません						
<input type="button" value="削除"/>						

IPv6ホワイトリスト一覧

選択	UTMチェック	プロトコル	送信元(送信先)		送信先(送信元)	
			IPv6アドレス	ポート番号	IPv6アドレス	ポート番号
設定されていません						
<input type="button" value="削除"/>						

ホワイトリストの追加

設定したホワイトリストは送信元/送信先を反転させた逆方向でも評価を行います。
(例) 送信元192.168.0.11/32から送信先10.0.0.11/32をUTMチェックしないに設定した場合、
逆方向の送信となる送信元 10.0.0.11/32から送信先 192.168.0.11/32の/パケットもUTM(個別機能)処理は行われません。
ポート番号で範囲指定をする場合、ハイフン(-)を利用し設定してください(例:1-100)。
「変更対象: "すべて"」で UTMチェックを「しない」にした場合、個別機能の設定にかかわらずUTMチェックをしません。
「変更対象: "すべて"」で UTMチェックを「する」にした場合、個別機能でUTMをチェック「しない」にするとUTMチェックをしません。

IP	UTMチェック	プロトコル	送信元(送信先)		送信先(送信元)	
			IPアドレス	ポート番号	IPアドレス	ポート番号
<input type="text" value="IPv4"/>	<input type="text" value="しない"/>	<input type="text" value="すべて"/>	<input type="radio"/> すべて <input type="radio"/> 指定	<input type="radio"/> すべて <input type="radio"/> 指定	<input type="radio"/> すべて <input type="radio"/> 指定	<input type="radio"/> すべて <input type="radio"/> 指定
<input type="button" value="追加"/>						

4. 詳細設定

(2) 各項目を設定し、[追加]または[削除]ボタンをクリックします。

ホワイトリスト設定

UTMを通さず、無条件で許可するトラフィックのホストを設定します。

IPv4ホワイトリスト一覧

選択	UTMチェック	プロトコル	送信元(送信先) IPv4アドレス	ポート番号	送信先(送信元) IPv4アドレス	ポート番号
<input type="checkbox"/>						

削除

IPv6ホワイトリスト一覧

選択	UTMチェック	プロトコル	送信元(送信先) IPv6アドレス	ポート番号	送信先(送信元) IPv6アドレス	ポート番号
<input type="checkbox"/>						

削除

ホワイトリストの追加

設定したホワイトリストは送信元/送信先を反転させた逆方向でも評価を行います。
(例) 送信元192.168.0.11/32から送信先10.0.0.11/32をUTMチェック「しない」に設定した場合、
逆方向の通信となる送信元 10.0.0.11/32から送信先 192.168.0.11/32のパケットもUTM処理は行われません。
ポート番号で範囲を設定する場合は、ハイフン(-)を利用し、設定して(例えば例:1-100)。

IP	UTMチェック	プロトコル	送信元(送信先) IPアドレス	ポート番号	送信先(送信元) IPアドレス	ポート番号
IPv4	しない	すべて	<input checked="" type="radio"/> すべて <input type="radio"/> 指定	<input checked="" type="radio"/> すべて <input type="radio"/> 指定	<input checked="" type="radio"/> すべて <input type="radio"/> 指定	<input checked="" type="radio"/> すべて <input type="radio"/> 指定

追加

4. 詳細設定

番号	項目	内容
①	IPv4 ホワイトリスト 全選択	選択した IPv4 ホワイトリストに対して、一括削除することができます。[全選択]をクリックすると、IPv4 ホワイトリストを全選択します。
②	IPv4 ホワイトリスト 全解除	選択した IPv4 ホワイトリストをすべて解除します。
③	IPv4 ホワイトリスト 選択	選択した IPv4 ホワイトリストに対して、一括削除することができます。 IPv4 ホワイトリスト単位で、個々に選択します。
④	IPv6 ホワイトリスト 全選択	選択した IPv6 ホワイトリストに対して、一括削除することができます。[全選択]をクリックすると、IPv6 ホワイトリストを全選択します。
⑤	IPv6 ホワイトリスト 全解除	選択した IPv6 ホワイトリストをすべて解除します。
⑥	IPv6 ホワイトリスト 選択	選択した IPv6 ホワイトリストに対して、一括削除することができます。 IPv6 ホワイトリスト単位で、個々に選択します。
⑦	ホワイトリストの追加 IP	IPv4 か、IPv6 かを選択します。
⑧	ホワイトリストの追加 UTM チェック	UTM のチェック対象とするか、否かを選択します。 ・ [しない]/[する]から選択します。
⑨	ホワイトリストの追加 プロトコル	プロトコルを、[すべて]、[TCP]、[UDP]、[ICMP]または[指定]から選択します。 ・ 「指定」を選択したときは、プロトコル番号(1~255)を入力します。
⑩	ホワイトリストの追加 送信元(送信先) IP アドレス	IP アドレスを設定します。 ・ IPアドレスは、[すべて]、[指定]から選択します。 ・ [すべて]を選択した場合、すべてのIPアドレスが対象となります。 ・ [指定]を選択した場合、ネットワークアドレスを入力するボックスが表示されるため、ネットワークアドレスを入力します。
⑪	ホワイトリストの追加 送信元(送信先) ポート番号	ポート番号を設定します。 ・ ポートは、[すべて]、[指定]から選択します。 ・ [すべて]を選択した場合、すべてのポートが対象となります。 ・ [指定]を選択した場合、ポート番号を入力するボックスが表示されるため、そのボックスで番号の範囲を指定することができます。 メモ ・ プロトコルが TCP または UDP 以外が指定されている場合は、ポート番号の指定はできません。
⑫	ホワイトリストの追加 送信先(送信元) IP アドレス	IP アドレスを設定します。 ・ IPアドレスは、[すべて]、[指定]から選択します。 ・ [すべて]を選択した場合、すべてのIPアドレスが対象となります。 ・ [指定]を選択した場合、ネットワークアドレスを入力するボックスが表示されるため、ネットワークアドレスを入力します。
⑬	ホワイトリストの追加 送信先(送信元) ポート番号	ポート番号を設定します。 ・ ポートは、[すべて]、[指定]から選択します。 ・ [すべて]を選択した場合、すべてのポートが対象となります。 ・ [指定]を選択した場合、ポート番号を入力するボックスが表示されるため、そのボックスで番号の範囲を指定することができます。 メモ ・ プロトコルが TCP または UDP 以外が指定されている場合は、ポート番号の指定はできません。
⑭	ホワイトリストの追加 追加	設定されたホワイトリストを追加します。

4. 詳細設定

(3) 設定が反映されたことを確認します。

ホワイトリスト設定

UTMを通さず、無条件で許可するトラフィックやホストを設定します。

IPv4ホワイトリスト一覧

選択	UTMチェック	プロトコル	送信元(送信先)		送信先(送信元)	
			IPv4アドレス	ポート番号	IPv4アドレス	ポート番号
<input type="checkbox"/>	しない	TCP	10.0.0.11/32	すべて	10.0.0.11/32	80
<input type="checkbox"/>	しない	TCP	10.0.0.11/32	すべて	10.0.0.11/32	443

IPv6ホワイトリスト一覧

選択	UTMチェック	プロトコル	送信元(送信先)		送信先(送信元)	
			IPv6アドレス	ポート番号	IPv6アドレス	ポート番号
<input type="checkbox"/>	しない	TCP	すべて	すべて	すべて	すべて

ホワイトリストの追加

設定したホワイトリストは送信元/送信先を反転させた逆方向でも評価を行います。
(例) 送信元192.168.0.11/32から送信先10.0.0.11/32をUTMチェック「しない」に設定した場合、
逆方向の送信元となる送信元 10.0.0.11/32から送信先 192.168.0.11/32の/ケットもUTM処理は行われません。
ポート番号で範囲指定をする場合、ハイフン(-)を利用し設定してください(例:1-100)。

IP	UTMチェック	プロトコル	送信元(送信先)		送信先(送信元)	
			IPv4アドレス	ポート番号	IPv4アドレス	ポート番号
IPv4	しない	すべて	<input checked="" type="radio"/> すべて <input type="radio"/> 指定	<input checked="" type="radio"/> すべて <input type="radio"/> 指定	<input checked="" type="radio"/> すべて <input type="radio"/> 指定	<input checked="" type="radio"/> すべて <input type="radio"/> 指定

4. 詳細設定

4.7.10 UTM 脅威レポート

UTM 各機能の脅威検出状況を表示します。

- (1) ログイン後のメニューエリアから[詳細設定]を選択し、「UTM」の項目から[UTM 脅威レポート]をクリックすることで、UTM 各機能の脅威検出状況を表示します。

- 管理者メニュー
 - トップページ
 - 設定の保存
 - ログアウト
- かんたん設定
 - かんたん設定
- 詳細設定
 - 詳細設定
 - 基本設定
 - パスワードの設定
 - 装置名の設定
 - 時刻の設定
 - 保守の設定
 - NetMeisterの設定
 - ゼロタッチの設定
 - LAN
 - LANアドレスの設定
 - DHCPサーバの設定
 - WAN
 - プロバイダの設定
 - 静的NAPTの設定
 - WANフィルタの設定
 - IPv4
 - IPv6
 - URLフィルタリングの設定
 - QoSの設定
 - 通信セキュリティの設定
 - VPN・クラウド
 - VPNの設定
 - L2TPの設定
 - クラウドの設定
 - NGN網VPN
 - NGN網VPNの設定
 - デバイス
 - デバイスの設定
 - UTM
 - 基本設定
 - 詳細設定
 - グループ別ポリシー設定
 - ホワイトリスト設定
 - UTM脅威レポート**
- 端末管理
 - 端末管理
- 保守管理
 - 保守管理
- 拡張ページ
 - 拡張ページ
- 外部リンク
 - 製品ページ

UTM脅威レポート

集計期間： 累計

各機能ごとの脅威検出状況を表示します。

各機能の脅威検出状況概要

機能名	スキャン数	検出数	ブロック数	最終検出日時
アンチウイルス(AV)	3-days	undefined	undefined	undefined undefined
不正侵入防止(IPS)	3-days	undefined	undefined	undefined undefined
Webガード(WG)	3-days	-	undefined	undefined undefined
URLフィルタリング(UF)	3-days	undefined	undefined	undefined undefined

アンチウイルス(AV)機能の脅威検出状況詳細

ウイルスID	ウイルス名	スキャン数	検出数	ブロック数	最終検出日時
--------	-------	-------	-----	-------	--------

不正侵入防止(IPS)機能の脅威検出状況詳細

シグネチャID	脅威名	スキャン数	検出数	ブロック数	最終検出日時
---------	-----	-------	-----	-------	--------

URLフィルタリング(UF)機能の脅威検出状況詳細

カテゴリID	カテゴリ名	スキャン数	検出数	ブロック数	最終検出日時
--------	-------	-------	-----	-------	--------

5. 端末管理

5 端末管理

本章では、IoT デバイスや LAN 内の端末の管理、あるいは Web 認証によるセキュリティ設定や Wake on LAN などの『端末管理』について説明します。端末管理では、以下の操作を行うことができます。

5.1 リンクマネージャの設定

5.2 Web 認証の設定

5. 端末管理

5.1 リンクマネージャの設定

リンクマネージャを設定します。

- (1) ログイン後のメニューエリアから[端末管理]をクリックします。
- (2) 「端末管理」の項目から[リンクマネージャの設定]をクリックします。



- (3) リンクマネージャの設定で、[変更]ボタンをクリックします。



5. 端末管理

(4) 各項目を設定し、[反映]ボタンをクリックします。

リンクマネージャの設定

リンクマネージャ機能

LAN側インタフェースでリンクマネージャ機能を有効化します。

	現在の設定	設定の変更
リンクマネージャ	無効	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

ゲスト端末の設定

未登録の新規端末からの通信について、透過/廃棄を選択できます。

	現在の設定	設定の変更
初期動作	透過	<input checked="" type="radio"/> 透過 (<input type="checkbox"/> 端末認証なし) <input type="radio"/> 廃棄

メイングループの設定

メイングループの名称を設定します。
複数の端末をグループ化して表示するために使用します。入力欄は自動で増えます。

	グループ名		グループ名		グループ名
1	登録済み	2		3	
4		5		6	
7		8		9	

サブグループの設定

サブグループの名称を設定します。
主に端末の種別等に利用します。入力欄は自動で増えます。

	グループ名		グループ名		グループ名
1		2		3	
4		5		6	
7		8		9	

5. 端末管理

番号	項目	内容
①	リンクマネージャ	リンクマネージャの利用を選択します。 <ul style="list-style-type: none">・ 「有効」 / 「無効」 から選択します。
②	ゲスト端末の設定	端末管理で登録されていない新たな端末が接続された場合に、その通信を透過するか、廃棄するかを選択します。 <ul style="list-style-type: none">・ 「透過」 / 「廃棄」 から選択します。・ 「透過」 を選択し、「端末認証なし」 をチェックした場合、IEEE802.1X 認証、MAC 認証、Web 認証のいずれかが設定されていても、その設定を無視して送受信します。
③	メイングループの設定	複数の端末をグループ化して表示することができます。 <ul style="list-style-type: none">・ 任意の文字列でメイングループ名を入力します。・ メイングループを削除する場合は、文字列を削除します。 メモ <ul style="list-style-type: none">・ 全角文字を利用することができます。
④	サブグループの設定	複数の端末をグループ化して表示することができます。 <ul style="list-style-type: none">・ 任意の文字列でサブグループ名を入力します。・ サブグループを削除する場合は、文字列を削除します。 メモ <ul style="list-style-type: none">・ 全角文字を利用することができます。 注意 <ul style="list-style-type: none">・ 端末をグループ化する際は、メイングループが未登録のまま、サブグループのみを設定することはできません。

5. 端末管理

(5) 各項目を設定する一例を示します。

リンクマネージャの設定

リンクマネージャ機能

LAN側インタフェースでリンクマネージャ機能を有効化します。

	現在の設定	設定の変更
リンクマネージャ	無効	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効

ゲスト端末の設定

未登録の新規端末からの通信について、透過/廃棄を選択できます。

	現在の設定	設定の変更
初期動作	透過	<input checked="" type="radio"/> 透過 (<input type="checkbox"/> 端末認証なし) <input type="radio"/> 廃棄

メイングループの設定

メイングループの名称を設定します。
複数の端末をグループ化して表示するために使用します。入力欄は自動で増えます。

	グループ名		グループ名		グループ名
1	フロア1-北	2	フロア1-南	3	
4		5		6	
7		8		9	

サブグループの設定

サブグループの名称を設定します。
主に端末の種別等に利用します。入力欄は自動で増えます。

	グループ名		グループ名		グループ名
1	パソコン	2	プリンタ	3	カメラ
4		5		6	
7		8		9	

5. 端末管理

(6) 各項目の設定が反映されたことを確認します。

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず「設定の保存」を行ってください。

リンクマネージャの設定

接続端末の可視化および制御を行います。

有効/無効	デフォルト受信動作	メイングループ数	サブグループ数
有効	透過	2	3

[変更](#)

表示グループ: [すべて](#)

[端末情報をCSV形式で追加](#) [端末情報をCSV形式で表示](#)

未登録

メイングループ	サブグループ	端末情報	説明	インターフェース(ポート番号)	状態	受信 [Mbyte]	送信 [Mbyte]	動作
		子登録	24c7b0c3b052c010c4 (204.205.2.1)	GEL.0	up	0.17	0.0074	透過

[編集](#) [更新](#)

フロア1-北

端末情報がありません。

[追加](#) [編集](#) [更新](#)

フロア1-南

端末情報がありません。

[追加](#) [編集](#) [更新](#)

(7) 「未登録」グループの端末を登録済みのグループに登録するため、[編集]をクリックします。

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず「設定の保存」を行ってください。

リンクマネージャの設定

接続端末の可視化および制御を行います。

有効/無効	デフォルト受信動作	メイングループ数	サブグループ数
有効	透過	2	3

[変更](#)

表示グループ: [すべて](#)

[端末情報をCSV形式で追加](#) [端末情報をCSV形式で表示](#)

未登録

メイングループ	サブグループ	端末情報	説明	インターフェース(ポート番号)	状態	受信 [Mbyte]	送信 [Mbyte]	動作
		子登録	24c7b0c3b052c010c4 (204.205.2.1)	GEL.0	up	0.17	0.0074	透過

[編集](#) [更新](#)

フロア1-北

端末情報がありません。

[追加](#) [編集](#) [更新](#)

フロア1-南

端末情報がありません。

[追加](#) [編集](#) [更新](#)

5. 端末管理

(8) 各項目を設定し、[反映]をクリックします。

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず「設定の保存」を行ってください。

リンクマネージャの設定

グループ:未登録

端末情報を変更します。選択した端末のみ反映されます。

全選択 全解除 表示範囲: 1-1 / 1

選択	端末名称 説明	メイングループ サブグループ	インタフェース(ポート番号)	状態 経過時間	動作	端末詳細
<input type="checkbox"/>	110701020700004 (147 176 1 1)	未登録	GE10	UP 00:04:53	変更	<input type="checkbox"/>

一括変更

選択した端末の設定を一括変更します。

	設定
メイングループ	(変更しない)
サブグループ	(変更しない)
動作	(変更しない)
端末認証なし	(変更しない)

統計クリア

選択した端末の統計情報をクリアします。

削除

選択した端末を削除します。

5. 端末管理

番号	項目	内容
①	グループ 全選択	選択した端末情報に対して、一括変更、一括統計クリアおよび一括削除することができます。 [全選択]をクリックすると、端末の選択を全選択します。
②	グループ 全解除	[全解除]をクリックすると、端末の選択を全解除します。
③	グループ 表示範囲	ハイフン(-)で指定された範囲の番号の端末情報を表示させることができます。
④	グループ 選択	選択した端末情報に対して、一括変更、一括統計クリアおよび一括削除することができます。 端末単位で、個々に選択します。 注意 ・ 設定を反映させる場合は、該当の端末の選択がチェックされている必要があります。
⑤	グループ 端末情報説明	端末の MAC アドレス情報と登録されている説明(端末名称等)が表示されます。説明が未登録の場合は、ハイフン(-)が表示されます。 ・ 任意の文字列で詳細を入力します。 メモ ・ DHCP により端末の情報が収集できた場合は、自動的に詳細が表示されます。 ・ 全角文字を利用することができます。 注意 ・ 設定を反映させる場合は、該当の端末の選択がチェックされている必要があります。
⑥	メイングループ	端末にメイングループを設定することができます。上段にメイングループを設定します。 ・ メイングループをリストから選択します。 注意 ・ 設定を反映させる場合は、該当の端末の選択がチェックされている必要があります。
⑦	サブグループ	端末にグループを設定することができます。下段にサブグループを設定します。 ・ サブグループをリストから選択します。 注意 ・ メイングループが未登録のまま、サブグループのみを設定することはできません。 設定を反映させる場合は、該当の端末の選択がチェックされている必要があります。
⑧	グループ 動作	該当の端末の通信を透過するか、廃棄するかを選択します。 ・ 「透過」/「廃棄」から選択します。 注意 ・ 設定を反映させる場合は、該当の端末の選択がチェックされている必要があります。
⑨	グループ 端末認証なし	「動作」で該当の端末の通信の「透過」を選択し、「端末認証なし」をチェックした場合、該当の端末が IEEE802.1X 認証、MAC 認証、Web 認証のいずれかが設定されていても、その設定を無視して送受信します。
⑩	一括変更 メイングループ	選択されているすべての端末のメイングループを一括で設定します。 ・ メイングループをリストから選択します。
⑪	一括変更 サブグループ	選択されているすべての端末のサブグループを一括で設定します。 ・ サブグループをリストから選択します。
⑫	一括変更 動作	選択されているすべての端末の動作を一括で設定します。 ・ 「透過」/「廃棄」から選択します。
⑬	一括変更 L2 認証なし	選択されているすべての端末の「端末認証なし」を一括で設定します。 ・ 「有効」/「無効」から選択します。
⑭	一括統計クリア	選択した端末の統計情報を一括クリアします。
⑮	一括削除	選択した端末を一括削除します。

5. 端末管理

(9) 各項目の設定が反映されたことを確認します。

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず「設定の保存」を行ってください。

リンクマネージャの設定

接続端末の可視化および制御を行います。

有効/無効	デフォルト受信動作	メイングループ数	サブグループ数
有効	透過	2	3

変更

表示グループ: すべて

端末情報をCSV形式で追加 端末情報をCSV形式で表示

未登録

メイングループ	サブグループ	端末情報	説明	インターフェース(ポート番号)	状態	受信 [Mbyte]	送信 [Mbyte]	動作
端末情報がありません。								

検索 実行

フロア1-北

メイングループ	サブグループ	端末情報	説明	インターフェース(ポート番号)	状態	受信 [Mbyte]	送信 [Mbyte]	動作
フロア1-北	パソコン	14:76ac5c82-ehant (04 / 05 / 1)	OAパソコン	GE1.0	up	0.08	0.12	透過

追加 編集 実行

フロア1-南

メイングループ	サブグループ	端末情報	説明	インターフェース(ポート番号)	状態	受信 [Mbyte]	送信 [Mbyte]	動作
端末情報がありません。								

追加 編集 実行

(10) 端末情報を市販の表計算ソフトなどで利用する場合は、[端末情報をCSV形式で表示]ボタンで表示させます。

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず「設定の保存」を行ってください。

リンクマネージャの設定

接続端末の可視化および制御を行います。

有効/無効	デフォルト受信動作	メイングループ数	サブグループ数
有効	透過	2	3

変更

表示グループ: すべて

端末情報をCSV形式で追加 端末情報をCSV形式で表示

未登録

メイングループ	サブグループ	端末情報	説明	インターフェース(ポート番号)	状態	受信 [Mbyte]	送信 [Mbyte]	動作
端末情報がありません。								

検索 実行

フロア1-北

メイングループ	サブグループ	端末情報	説明	インターフェース(ポート番号)	状態	受信 [Mbyte]	送信 [Mbyte]	動作
フロア1-北	パソコン	14:76ac5c82-ehant (04 / 05 / 1)	OAパソコン	GE1.0	up	0.08	0.12	透過

追加 編集 実行

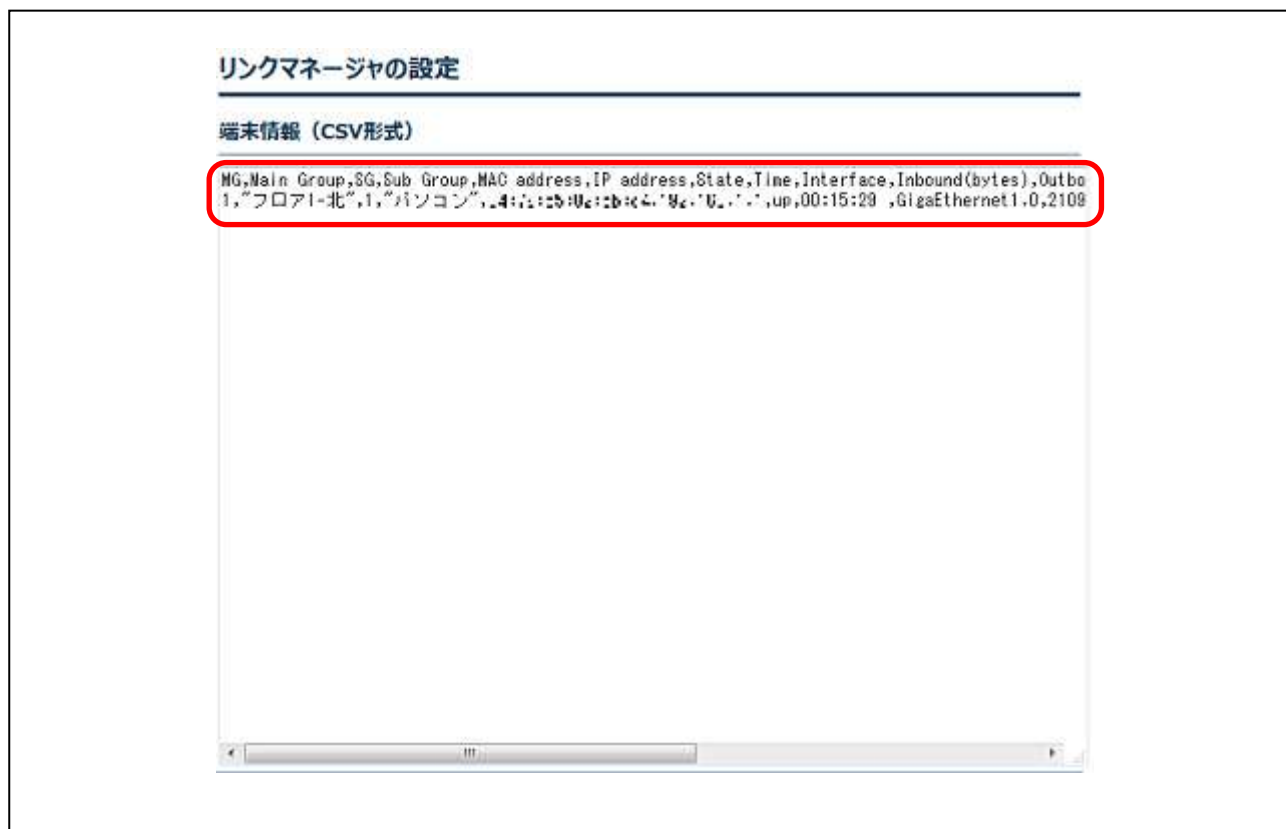
フロア1-南

メイングループ	サブグループ	端末情報	説明	インターフェース(ポート番号)	状態	受信 [Mbyte]	送信 [Mbyte]	動作
端末情報がありません。								

追加 編集 実行

5. 端末管理

- (11) 端末情報が CSV 形式で表示されたことを確認します。マウスで必要箇所をなぞり、コピーして利用してください。



5. 端末管理

(12) 市販の表計算ソフトなどで作成した端末情報から追加する場合は、[端末情報を CSV 形式で追加] ボタンをクリックします。

注意 メイングループ名 (Main Group) およびサブグループ名 (Sub Group) は CSV 形式のファイルからは反映されず、グループ番号 (MG、SG) に反映されます。メイングループ名およびサブグループ名は、あらかじめ設定画面から設定した後に、「端末情報を CSV 形式で追加」を利用してください。

注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず「設定の保存」を行ってください。

リンクマネージャの設定

接続端末の可視化および制御を行います。

有効/無効	デフォルト受信動作	メイングループ数	サブグループ数
有効	透過	2	3

表示グループ: すべて

未登録

メイングループ	サブグループ	端末情報	説明	インターフェース(ポート番号)	状態	受信 [Mbyte]	送信 [Mbyte]	動作

端末情報がありません。

フロア1-北

メイングループ	サブグループ	端末情報	説明	インターフェース(ポート番号)	状態	受信 [Mbyte]	送信 [Mbyte]	動作
フロア1-北		14:76ac%540rhant (4) (15 1)		GE1.0	up	0.08	0.12	透過

フロア1-南

メイングループ	サブグループ	端末情報	説明	インターフェース(ポート番号)	状態	受信 [Mbyte]	送信 [Mbyte]	動作

端末情報がありません。

5. 端末管理

- (13) CSV 形式の端末情報をテキスト形式でコピーし、「端末情報 (CSV 形式)」に貼り付け (ペースト) して[反映]ボタンをクリックしてください。

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず「[設定の保存](#)」を行ってください。

リンクマネージャの設定

設定する端末情報を入力してください。
入力時には以下のヘッダ情報が含まれていることを確認してください。
MG,SG,MAC Address,Description,Action
なお、グループ名、説明文(description)にカンマ(,)を設定している場合、csvアップロード時にエラーになることがあります。

端末情報 (CSV形式)

5. 端末管理

(14) 設定が反映されたことを確認します。

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず「設定の保存」を行ってください。

リンクマネージャの設定

接続端末の可視化および制御を行います。

有効/無効	デフォルト受信動作	メイングループ数	サブグループ数
有効	透過	2	3

表示グループ: すべて

未登録

メイングループ	サブグループ	端末情報	説明	インターフェース(ポート番号)	状態	受信 [Mbyte]	送信 [Mbyte]	経過時間	透過	動作
端末情報がありません。										

フロア1-北

メイングループ	サブグループ	端末情報	説明	インターフェース(ポート番号)	状態	受信 [Mbyte]	送信 [Mbyte]	経過時間	透過	動作
フロア1-北	パソコン	74:76:1c:07:20:04 (142 10)	OAパソコン	GE1.0	up	3.27	0.41	00:44:39	透過	<input type="button" value="追加"/> <input type="button" value="編集"/> <input type="button" value="更新"/>

フロア1-南

メイングループ	サブグループ	端末情報	説明	インターフェース(ポート番号)	状態	受信 [Mbyte]	送信 [Mbyte]	経過時間	透過	動作
フロア1-南	パソコン	74:76:1c:07:20:04 (142 10)	OAパソコン	-	down	0	0	-	透過	<input type="button" value="追加"/> <input type="button" value="編集"/> <input type="button" value="更新"/>
フロア1-南	パソコン	74:76:1c:07:20:04 (142 10)	OAパソコン	-	down	0	0	-	透過	<input type="button" value="追加"/> <input type="button" value="編集"/> <input type="button" value="更新"/>

(15) 登録済みの端末情報を削除する場合は、[編集]をクリックします。

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず「設定の保存」を行ってください。

リンクマネージャの設定

接続端末の可視化および制御を行います。

有効/無効	デフォルト受信動作	メイングループ数	サブグループ数
有効	透過	2	3

表示グループ: すべて

未登録

メイングループ	サブグループ	端末情報	説明	インターフェース(ポート番号)	状態	受信 [Mbyte]	送信 [Mbyte]	経過時間	透過	動作
端末情報がありません。										

フロア1-北

メイングループ	サブグループ	端末情報	説明	インターフェース(ポート番号)	状態	受信 [Mbyte]	送信 [Mbyte]	経過時間	透過	動作
フロア1-北	パソコン	74:76:1c:07:20:04 (142 10)	OAパソコン	GE1.0	up	3.27	0.41	00:44:39	透過	<input type="button" value="追加"/> <input type="button" value="編集"/> <input type="button" value="更新"/>

フロア1-南

メイングループ	サブグループ	端末情報	説明	インターフェース(ポート番号)	状態	受信 [Mbyte]	送信 [Mbyte]	経過時間	透過	動作
フロア1-南	パソコン	74:76:1c:07:20:04 (142 10)	OAパソコン	-	down	0	0	-	透過	<input type="button" value="追加"/> <input type="button" value="編集"/> <input type="button" value="更新"/>
フロア1-南	パソコン	74:76:1c:07:20:04 (142 10)	OAパソコン	-	down	0	0	-	透過	<input type="button" value="追加"/> <input type="button" value="編集"/> <input type="button" value="更新"/>

5. 端末管理

- (16) 端末の「選択」をチェックし、端末を選択します。削除する場合は、[削除]をクリックします。統計情報をクリアする場合は、[クリア]をクリックします。

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず「設定の保存」を行ってください。

リンクマネージャの設定

グループ: フロア1-南

端末情報を変更します。選択した端末のみ反映されます。

全選択 全解除

表示範囲: 1-2 / 2

選択	端末情報 説明	メイングループ サブグループ	インタフェース(ポート番号)	状態 経過時間	動作	詳細設定
<input type="checkbox"/>	24-7/bnub/82:cd1c1b 04/1/10/10	フロア1南 パソコン	-	down -	通信	<input type="checkbox"/>
<input type="checkbox"/>	24-7/bnub/82:cd1c1b 04/1/10/10	フロア1南 パソコン	-	down -	通信	<input type="checkbox"/>

一括変更

選択した端末の設定を一括変更します。

	設定
メイングループ	<変更しない>
サブグループ	<変更しない>
動作	<変更しない>
端末認証なし	<変更しない>

一括変更

統計クリア

選択した端末の統計情報をクリアします。

クリア

削除

選択した端末を削除します。

削除

5. 端末管理

5.2 Web 認証の設定

Web 認証を設定します。

- (1) ログイン後のメニューエリアから[端末管理]をクリックします。
- (2) 「端末管理」の項目から[Web 認証の設定]をクリックします。



- (3) Web 認証の設定で、[設定変更]をクリックします。



5. 端末管理

(4) 各項目を設定し、[反映]をクリックします。

Web認証の設定

Web認証を設定します。

Web認証の設定

	現在の設定	設定の変更
Web認証	無効	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
HTTPSの透過	認証が必要	<input checked="" type="radio"/> 認証が必要 <input type="radio"/> 常に透過

認証アカウントの設定

Web認証アカウントの情報を設定してください。少なくとも1人分の登録が必要です。

	ユーザ名	パスワード
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>

認証対象外の設定

	MACアドレス		MACアドレス
1	<input type="text"/>	2	<input type="text"/>
3	<input type="text"/>	4	<input type="text"/>
5	<input type="text"/>	6	<input type="text"/>
7	<input type="text"/>	8	<input type="text"/>
9	<input type="text"/>	10	<input type="text"/>

戻る **反映**

5. 端末管理

番号	項目	内容
①	Web 認証	Web 認証の設定を選択します。 ・ 「無効」 / 「有効」 から選択します。 注意 ・ 「有効」 を選択した場合は、少なくとも 1 人分の認証アカウントを設定してください。
②	https の透過	https 通信を、Web 認証無しで透過するか、Web 認証後に透過するかを選択します。 ・ 「認証が必要」 / 「常に透過」 から選択します。
③	認証アカウントの設定 ユーザ名	Web 認証の対象となるユーザ名を設定します。 メモ ・ 半角英数字の文字列を入力してください。
④	認証アカウントの設定 パスワード	Web 認証の対象となるユーザ名のパスワードを設定します。 メモ ・ 半角英数字または半角記号の文字列を入力してください。
⑤	認証対象外の設定 MAC アドレス	プリンタや IoT デバイスなど、Web 認証の対象外とする端末を設定します。 ・ XX:XX:XX:XX:XX:XX 形式で入力します。 注意 ・ 登録可能な MAC アドレスは最大 10 件です。

5. 端末管理

(5) 各項目の設定が反映されたことを確認します。

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず「設定の保存」を行ってください。

Web認証の設定

Web認証の情報

現在の設定	総数	認証済み	未認証
有効	1	0	1

端末の情報

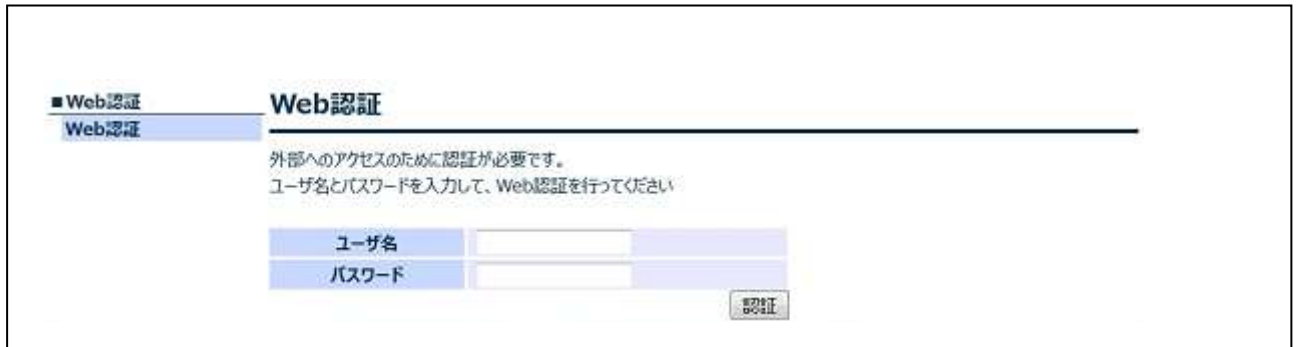
MACアドレス	状態	有効期限	受信 [Mbyte]
ユーザ名			送信 [Mbyte]
14: 14: 14: 14: 14: 14	未認証	---	0.00059
			0.0015

5. 端末管理

(6) 端末から http によって URL をアクセスしようとした際、Web 認証によって、端末の画面に以下のような認証画面が表示されます。

☒ http によるアクセス時のみ認証画面が表示され、https によるアクセス時は認証画面が表示されずタイムアウトになります。

☒ 認証画面は、お客様の環境に合わせ、拡張ページ機能を利用してカスタマイズすることができます。



■ Web認証

Web認証

外部へのアクセスのために認証が必要です。
ユーザ名とパスワードを入力して、Web認証を行ってください。

ユーザ名

パスワード

認証

6. 保守管理

6 保守管理

本章では、『保守管理』について説明します。

保守管理では、以下の操作を行うことができます。

- 6.1 装置状態の表示
- 6.2 装置ログの取得
- 6.3 設定データの管理
 - 設定データのダウンロード(バックアップ)
 - 設定データのアップロード(リストア)
- 6.4 設定の初期化
- 6.5 ソフトウェアの更新
- 6.6 ping の実行
- 6.7 任意コマンドの実行
- 6.8 IP 電話サービス保守
- 6.9 URL オフロード
- 6.10 リンクマネージャ
- 6.11 Wake on LAN
- 6.12 再起動

6. 保守管理

6.1 装置状態の表示

装置状態を確認することができます。

- (1) ログイン後のメニューエリアから[保守管理]をクリックします。
- (2) [装置状態の表示]をクリックします。
- (3) 装置状態を確認します。

更新ボタンを押すと、最新の装置状態が表示されます。

ログイン前の場合、VPN 情報は表示されません。

■ 管理者メニュー
トップページ
設定の保存
ログアウト

■ かんたん設定
かんたん設定

■ 詳細設定
詳細設定

■ 端末管理
端末管理

■ 保守管理
装置状態の表示
装置ログの取得
設定データの管理
設定の初期化
ソフトウェアの更新
pingの実行
任意コマンドの実行
IP電話サービス保守
URLオフロード
リンクマネージャ
Wake on LAN
再起動

■ 拡張ページ
拡張ページ

■ 外部リンク
製品ページ

装置状態の表示

自動更新間隔: 停止

装置情報 (装置名: Router) 前回ログイン: ----/--/--:--:-- (-----)

バージョン	稼働時間	稼働率	メモリ	内部温度	内部電圧
全点	8分	11%	29%	45.0℃	3.2508V

ネットワーク情報 更新

デバイス	接続状態	送信量	受信量
GE0 (GigaEthernet0)	全二重 1Gbpsで接続	0%	0%
GE1 (GigaEthernet1)	Port1: 全二重 1Gbpsで接続 Port2: 接続されていません Port3: 接続されていません Port4: 接続されていません	0%	0%

WAN情報 更新

接続名	接続状態	情報
WAN1: IP電話サービス接続 (GigaEthernet0.0)	接続	IPアドレス: 192.0.2.1

VPN情報 更新

接続名	接続状態	通信量[packets]
設定されていません		

UTM情報 更新


ライセンス状態	ライセンス満了日時
設定されていません	

6. 保守管理

番号	項目	内容
①	装置情報	<p>本装置の名称と稼働状態を表示しています。</p> <p>装置名 : 本装置の名称です。初期値は「Router」です。 名称は任意に付けることができ、変更するときは、「4.詳細設定」の「4.1.2 装置名の設定」を参照してください。</p> <p>前回ログイン : 前回装置にログインを行った日時と、パソコンのIPアドレスを表示しています。</p> <p>バージョン : 現在稼働中のソフトウェアのバージョンを表示しています。 ソフトウェアの更新は、本章の「6.5 ソフトウェアの更新」を参照してください。</p> <p>稼働時間 : 本装置の電源スイッチをONにしたときや、本装置の再起動を実行してからの経過時間を表示しています。</p> <p>稼働率 : CPUの使用率を表示しています。</p> <p>メモリ : 内部メモリの使用率を表示しています。</p> <p>内部温度 : 本装置内部の温度を表示しています。</p> <p>内部電圧 : 内部装置への入力電圧を表示しています。</p>
②	ネットワーク情報	<p>ネットワークの状態を表示しています。</p> <p>デバイス : 物理デバイスの接続種類を表示しています。</p> <p>接続状態 : デバイスの接続状態を表示しています。</p> <p>送信量 : 物理ポート(デバイス)における送信方向の回線使用率を表示しています。</p> <p>受信量 : 物理ポート(デバイス)における受信方向の回線使用率を表示しています。</p>
③	WAN 情報	<p>WAN 接続の状態を表示しています。</p> <p>接続名 : 「プロバイダの設定」で設定した接続名、または、「かんたん設定」で指定した接続種別が表示されます。</p> <p>接続状態 : 接続状態を表示しています。</p> <p>情報 : WAN 接続の情報を表示しています。</p>
④	VPN 情報	<p>VPN 接続の状態を表示しています。</p> <p>接続名 : 「VPN の設定」で設定した接続名、または、「かんたん設定」で自動設定された接続名が表示されます。</p> <p>接続状態 : VPN 接続の接続状態を表示しています。</p> <p>通信量[packets] : VPN 接続で利用された通信量(送信量、受信量)を表示しています。</p>
⑤	UTM 情報	<p>UTM の状態を表示しています。</p> <p>ライセンス状態 : UTM ライセンスの認証状態を表示しています。</p> <p>ライセンス終了日時 : 適用中 UTM ライセンスの終了日時を表示しています。</p>

6. 保守管理

- (4) VPN 情報の接続名を変更したい場合は、[接続名編集]ボタンをクリックします。

 VPN 情報の接続名を変更する必要が無い場合は、接続名編集は不要です。

装置状態の表示

自動更新間隔: 停止

装置情報 (装置名:Router)

前回ログイン: ****/**/** **:*:* (**,***,***,***)

バージョン	稼働時間	稼働率	メモリ	内部温度	内部電圧
	2分	11%	29%	42.0℃	3.2508V

ネットワーク情報 更新

デバイス	接続状態	送信量	受信量
GE0 (GigaEthernet0)	全二重 1Gbpsで接続	0%	0%
GE1 (GigaEthernet1)	Port1: 接続されていません Port2: 接続されていません Port3: 接続されていません Port4: 全二重 1Gbpsで接続	0%	0%

WAN情報 更新

接続名	接続状態	情報
WAN1: インターネットVPN接続 (GigaEthernet0.1)	接続	IPアドレス:

VPN情報 更新

接続名	接続状態	通信量[packets]
Dynamic_VPN	接続	送信: 31, 受信: 45


接続名編集 更新

UTM情報

ライセンス状態	ライセンス満了日時
設定されていません	

更新

- (5) 接続名を入力し、[反映]ボタンをクリックします。

 VPN 情報の接続名を変更する必要が無い場合は、接続名編集は不要です。

VPN情報 接続名の編集

接続名	接続状態	IPアドレス/通信量[packets]
<input type="text"/>	接続	IPアドレス:
Tunnelアドレス:	ダイナミックVPN(センタ)	送信: 152 受信: 210

反映 戻る

6. 保守管理

(6) VPN情報の接続名が反映されたことを確認します。

☒ VPN情報の接続名を変更する必要が無い場合は、接続名編集は不要です。

!!注意!! 設定が変更されています。
再起動した場合、保存していない設定は元の状態に戻ります。
設定完了後は必ず「設定の保存」を行ってください。

装置状態の表示 自動更新間隔: 停止 ▼

装置情報 (装置名:Router) 前回ログイン: 2023/10/27 10:00:00 (.....)

バージョン	稼働時間	稼働率	メモリ	内部温度	内部電圧
1.0.0	17分	28%	29%	43.0℃	3.2508V

ネットワーク情報 更新

デバイス	接続状態	送信量	受信量
GE0 (GigaEthernet0)	全二重 1Gbpsで接続	0%	0%
GE1 (GigaEthernet1)	Port1: 接続されていません Port2: 接続されていません Port3: 接続されていません Port4: 全二重 1Gbpsで接続	0%	0%

WAN情報 更新

接続名	接続状態	情報
WAN1: インターネットVPN接続 (GigaEthernet0.1)	接続	IPアドレス: 1.1.1.1

VPN情報 更新

接続名	接続状態	通信量[packets]
東京本社	接続	送信: 281, 受信: 404

[接続名編集](#) [更新](#)

UTM情報

ライセンス状態	ライセンス満了日時
設定されていません	

[更新](#)

6. 保守管理

6.2 装置ログの取得

装置のログを閲覧することができます。また、パソコンにダウンロードしてテキストファイルで保存することができます。

- (1) ログイン後のメニューエリアから[保守管理]をクリックします。
- (2) [装置ログの取得]をクリックします。
- (3) 取得したい情報の[テキストファイルでダウンロード]を左クリック、または、右クリックしたメニューから[名前を付けてリンクを保存]をクリックし、【名前を付けて保存】ダイアログから保存します。

■管理者メニュー	装置ログの取得	
トップページ	装置のログを閲覧・ダウンロードします。	
設定の保存	[テキストファイルでダウンロード]を右クリックしてファイルに保存してください。	
ログアウト		
■かんたん設定		
かんたん設定		
■詳細設定	テクニカルサポート情報	
詳細設定	テクニカルサポートに必要な情報を取得します。	テキストファイルでダウンロード
show tech-support, show logging		
■端末管理		
端末管理		
■保守管理	個別情報	
装置状態の表示	インタフェース/デバイス情報	
装置ログの取得	インタフェースとデバイスの情報を取得します。	テキストファイルでダウンロード
設定データの管理	show interface detail, show devices detail	
設定の初期化		
ソフトウェアの更新	ルーティング情報	
pingの実行	ルーティング情報を取得します。	テキストファイルでダウンロード
任意コマンドの実行	show ip route, show ip cache, show ipv6 route, show ipv6 cache	
IP電話サービス保守		
URLオフロード	NAT/NAPT情報	
リンクマネージャ	NATとNAPTの変換情報を取得します。	テキストファイルでダウンロード
Wake on LAN	show ip nat translation, show ip napt translation	
再起動		
■拡張ページ	DHCPサーバ情報	
拡張ページ	DHCPサーバ情報を取得します。	テキストファイルでダウンロード
■外部リンク	show ip dhcp lease	
製品ページ		
	VRRP情報	
	VRRP情報を取得します。	テキストファイルでダウンロード
	show vrrp	
	:	
	不正アクセス監視情報	
	不正アクセス監視情報を取得します。	テキストファイルでダウンロード
	show ids statistics	
	ロギング情報	
	ロギング情報を取得します。	テキストファイルでダウンロード
	show logging	

6. 保守管理

- (4) [テキストファイルでダウンロード]を左クリック、または、右クリックしたメニューから[名前を付けてリンクを保存]をクリックし、【名前を付けて保存】ダイアログから保存します。

設定データの管理

全ての設定をテキストファイルで管理します。
設定を一括でバックアップして、装置交換や設定を復元させたい場合に利用してください。

設定データのダウンロード(バックアップ)

最後に保存した設定をテキストで取得することができます。
右下の「テキストファイルでダウンロード」を右クリックしてファイルに保存してください。

```
! NEC Portable Internetwork Core Operating System Software
! IX Series IX2105 (magellan-sec) Software, Version 1.1.0.1
! Compiled on 2014.04.11 10:00:00 JST
! Last updated on 2014.04.11 10:00:00 JST
!
! timezone +08 00
!
username admin password hash 560ba2f068e87d1fe0fa7950b08f37e administrator
!
! session timeout 1200
```

テキストファイルでダウンロード

- リンクを新しいタブで開く
- リンクを新しいウィンドウで開く
- リンクを InPrivate ウィンドウで開く
- リンクをデバイスに送信
- 名前を付けてリンクを保存**
- リンクのコピー
- コレクションに追加
- 共有
- Web キャプチャ (Ctrl+Shift+S)
- 開発者ツールで調査する

設定データのアップロード(リストア)

テキストで保存した設定データを装置にアップロードすることができます。
設定データのファイルを指定して、[アップロード実行]を押してください。
[アップロード実行]を押した後は完了メッセージが表示されるまで他の操作を行わないでください。
またBUSY LED(表示:BSY)点灯中は電源を切らないでください。故障の原因になります。
アップロードするファイルを指定してください。

参照... ファイルが選択されていません。

アップロード実行

6. 保守管理

6.3.2 設定データのアップロード(リストア)

テキスト形式で保存した設定データを装置にアップロード(リストア)することで、設定データを元の状態に戻すことができます。

注意 アップロード可能な設定データは、拡張子が「.txt」のテキストファイルです。「.txt」以外のファイルは動作保証の対象外です。

注意 設定データを本装置にアップロードする際には、事前に誤記やコマンドの入力順序に誤りがないことを確認してください。また、設定データ内に使用不可能な文字(※)が含まれていないことを確認してください。

(※)使用不可能な文字については、「はじめに」の「Web 設定で利用可能な文字について」を参照してください。

注意 アップロードを実行すると現在の設定データは上書きされ、再起動後に有効になります。

注意 アップロードした設定データに、現在と異なる IP アドレスが設定されていた場合には、本装置の再起動後に Web 接続が切断されます。

アップロードした設定データと同じネットワークの IP アドレスで再接続してください。

■ 設定データ内に含まれてはいけないコマンドについて

- 再起動が実行されるコマンドが含まれる場合は、本装置を正常に立ち上げることができません。

例：「reload」「restart」など

- Web 設定画面を起動している端末の通信を制限するコマンドが含まれている場合は、Web 設定画面を表示することができなくなります。

例：「filter」「access-list」など

- Web 設定画面を起動している端末が接続されているインタフェースを無効化するコマンドが含まれている場合は、Web 設定画面を表示することができなくなります。

例：「shutdown」など

- ※ 上記のコマンドは一例です。コマンドの組み合わせによっては、正しく動作しない場合があります。

6. 保守管理

- (1) ログイン後のメニューエリアから[保守管理]をクリックします。
- (2) [設定データの管理]をクリックします。
- (3) 「設定データのアップロード(リストア)」の[参照]ボタンをクリックします。



■管理者メニュー
トップページ
設定の保存
ログアウト

■かんたん設定
かんたん設定

■詳細設定
詳細設定

■端末管理
端末管理

■保守管理
装置状態の表示
装置ログの取得
設定データの管理
設定の初期化
ソフトウェアの更新
pingの実行
任意コマンドの実行
IP電話サービス保守
URLオフロード
リンクマネージャ
Wake on LAN
再起動

■拡張ページ
拡張ページ

■外部リンク
製品ページ

**!!注意!! パスワードが設定されていません。
パスワードの設定を行ってください。**

設定データの管理

全ての設定をテキストファイルで管理します。
設定を一括でバックアップして、装置交換や設定を復元させたい場合に利用してください。

設定データのダウンロード(バックアップ)

最後に保存した設定をテキストで取得することができます。
右下の「テキストファイルでダウンロード」を右クリックしてファイルに保存してください。
設定データがありません

[テキストファイルでダウンロード](#)

設定データのアップロード(リストア)

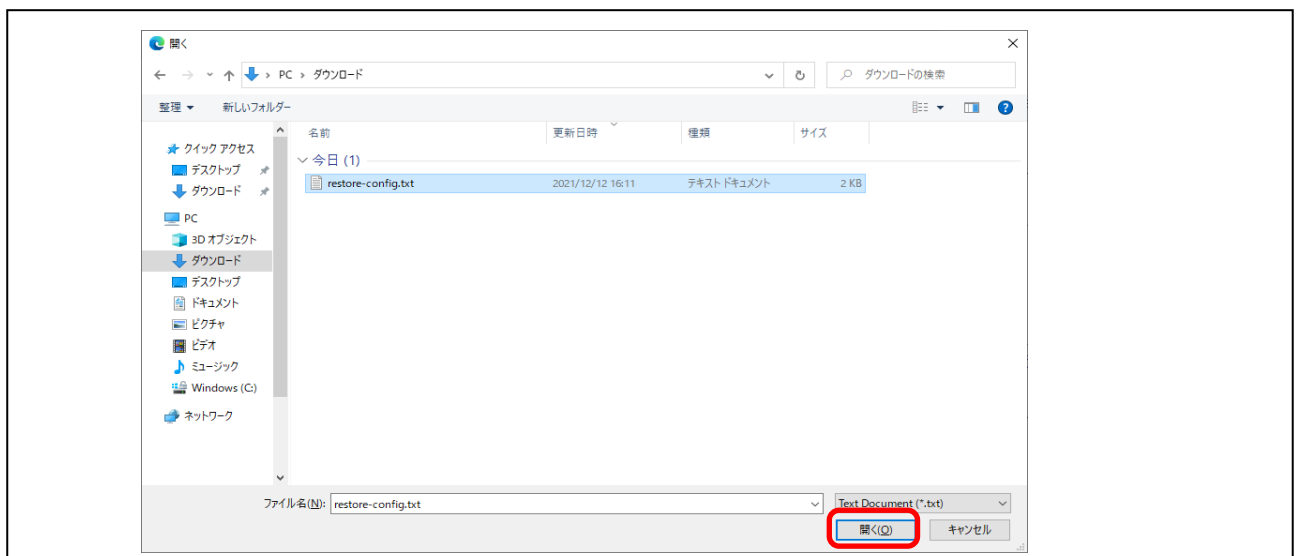
テキストで保存した設定データを装置にアップロードすることができます。
設定データのファイルを指定して、[アップロード実行]を押してください。
[アップロード実行]を押した後は完了メッセージが表示されるまで他の操作を行わないでください。
またBUSY LED(表示:BSY)点灯中は電源を切らないでください。故障の原因になります。
アップロードするファイルを指定してください。

参照 ファイルが選択されていません。

[アップロード実行](#)

- (4) 保存しておいた設定データ(拡張子が「.txt」のファイル)を選択します。

☒ Windows の設定によってはファイル名に拡張子が表示されません。



開く

← → ↑ ↓ PC > ダウンロード

ダウンロードの検索

整理 新しいフォルダ

名前	更新日時	種類	サイズ
▼ 今日 (1)			
restore-config.txt	2021/12/12 16:11	テキストドキュメント	2 KB

ファイル名(四): restore-config.txt

Text Document (*.txt)

開く(O) キャンセル

6. 保守管理

(5) [アップロード実行]ボタンをクリックします。

注意 [アップロード実行]ボタンをクリックしたあとは、「設定ファイルのアップロードが完了しました。」のメッセージが表示されるまで、他の操作を行わないでください。

注意 アップロードの実行中は、電源スイッチを絶対にOFFにしないでください。故障の原因になります。

!!注意!! パスワードが設定されていません。
[『パスワードの設定』](#)を行ってください。

設定データの管理

全ての設定をテキストファイルで管理します。
設定を一括でバックアップして、装置交換や設定を復元させたい場合に利用してください。

設定データのダウンロード(バックアップ)

最後に保存した設定をテキストで取得することができます。
右下の『テキストファイルでダウンロード』を右クリックしてファイルに保存してください。
設定データがありません

[テキストファイルでダウンロード](#)

設定データのアップロード(リストア)

テキストで保存した設定データを装置にアップロードすることができます。
設定データのファイルを指定して、[アップロード実行]を押してください。
[アップロード実行]を押した後は完了メッセージが表示されるまで他の操作を行わないでください。
またBUSY LED(表示:BSY)点灯中は電源を切らないでください。故障の原因になります。

restore-config.txt

またBUSY LED(表示:BSY)点灯中は電源を切らないでください。故障の原因になります。

アップロード実行

6. 保守管理


- (6) メッセージが「設定データのアップロード中です。」から「設定データのアップロードが完了しました。」に変わったことを確認します。

!!注意!! パスワードが設定されていません。
『パスワードの設定』を行ってください。

!!注意!! 設定データが更新されています。
新しい設定データを有効にするには、設定を保存せずに『再起動』を行ってください。

設定データの管理

設定データのアップロード中です。
完了メッセージが表示されるまで他の操作を行わないでください。
またBUSY LED(表示:BSY)点灯中は電源を切らないでください。故障の原因になります。



!!注意!! パスワードが設定されていません。
『パスワードの設定』を行ってください。

!!注意!! 設定データが更新されています。
新しい設定データを有効にするには、設定を保存せずに『再起動』を行ってください。

設定データの管理

設定データのアップロードが完了しました。

6. 保守管理

- (7) メニューエリアの「保守管理」、または、メッセージエリアから[再起動]をクリックします。

The screenshot shows a management menu on the left with the following items: ■管理者メニュー (トップページ, 設定の保存, ログアウト), ■かんたん設定 (かんたん設定), ■詳細設定 (詳細設定), ■端末管理 (端末管理), ■保守管理 (装置状態の表示, 装置ログの取得, 設定データの管理, 設定の初期化, ソフトウェアの更新, pingの実行, 任意コマンドの実行, IP電話サービス保守, URLオフロード, リンクマネージャ, Wake on LAN, 再起動), ■拡張ページ (拡張ページ), ■外部リンク (製品ページ). The '再起動' item is circled in red. Two warning messages are displayed in red boxes: '!!注意!! パスワードが設定されていません。【パスワードの設定】を行ってください。' and '!!注意!! 設定データが更新されています。新しい設定データを有効にするには、設定を保存せずに【再起動】を行ってください。'. The main content area is titled '設定データの管理' and shows '設定データのアップロードが完了しました。'.

- (8) [再起動実行]ボタンをクリックして、装置の再起動を行います。

The screenshot shows the '再起動' page. It features the same two warning messages as the previous screenshot. Below the warnings, the title '再起動' is displayed. The text '装置を再起動します。' is followed by 'よろしければ [再起動実行] を押してください。'. The '再起動実行' button is circled in red.

6. 保守管理

- (9) メッセージが「装置を再起動しています。」から「装置を再起動しました。」に変わったら、再度、ログインし、設定データを確認します。

!!注意!! パスワードが設定されていません。
『パスワードの設定』を行ってください。

!!注意!! 設定データが更新されています。
新しい設定データを有効にするには、設定を保存せずに『再起動』を行ってください。

再起動

装置を再起動しています。

再起動の完了までには約2分かかります。
引き続き設定を行う場合は、再起動後ログインする必要があります。



トップページ

装置を再起動しました。

引き続き設定を行う場合は、ログインする必要があります。

6. 保守管理

6.4 設定の初期化

装置の設定を初期状態に戻します。

- (1) ログイン後のメニューエリアから[保守管理]をクリックします。
- (2) [設定の初期化]をクリックします。
- (3) [初期化実行]ボタンをクリックします。



- (4) 「保存されていた設定を初期状態に戻しました。」が表示されたことを確認します。

6. 保守管理

- (5) メニューエリアの「保守管理」、または、メッセージエリアから[再起動]をクリックします。

The screenshot shows a web interface with a left-hand navigation menu and a main content area. The navigation menu includes sections like '管理者メニュー', 'かんたん設定', '詳細設定', '端末管理', '保守管理', '拡張ページ', and '外部リンク'. Under '保守管理', '設定の初期化' is highlighted. A red box highlights the '再起動' option. The main content area has a warning message: '!!注意!! 保存されていた設定を削除しました。装置を初期状態（工場出荷状態）に戻すには、設定を保存せずに『再起動』を行ってください。' Below this is the title '設定の初期化' and another red box containing the message: '保存されていた設定を初期状態に戻しました。'

- (6) [再起動実行]ボタンをクリックして、装置の再起動を行います。

The screenshot shows the '再起動' (Restart) page. It features a warning message at the top: '!!注意!! 保存されていた設定を削除しました。装置を初期状態（工場出荷状態）に戻すには、設定を保存せずに『再起動』を行ってください。' Below the title '再起動', there is a sub-heading '装置を再起動します。' and a text prompt: 'よろしければ [再起動実行] を押してください。' A red box highlights the '再起動実行' button.

6. 保守管理


- (7) メッセージが「装置を再起動しています。」から「装置を再起動しました。」に変わったら、再度、ログインし、設定データを確認します。

!!注意!! 保存されていた設定を削除しました。
装置を初期状態（工場出荷状態）に戻すには、設定を保存せずに『再起動』を行ってください。

再起動

装置を再起動しています。

再起動の完了までには約2分かかります。
引き続き設定を行う場合は、再起動後ログインする必要があります。



トップページ

装置を再起動しました。

引き続き設定を行う場合は、ログインする必要があります。

[ログイン実行](#)

6. 保守管理

6.5 ソフトウェアの更新

ソフトウェアのバージョン確認とアップデートが可能です。

☒ あらかじめ、ソフトウェアのプログラムファイル(拡張子が「.rap」のファイル)を入手し、パソコンに保存しておく必要があります。

- (1) ログイン後のメニューエリアから[保守管理]をクリックします。
- (2) [ソフトウェアの更新]をクリックします。
- (3) 現在のソフトウェアのバージョンを確認します。
- (4) [ファイルの選択]ボタンをクリックします。

■管理者メニュー

- トップページ
- 設定の保存
- ログアウト

■かんたん設定

- かんたん設定

■詳細設定

- 詳細設定

■端末管理

- 端末管理

■保守管理

- 装置状態の表示
- 装置ログの取得
- 設定データの管理
- 設定の初期化
- ソフトウェアの更新
- pingの実行
- 任意コマンドの実行
- IP電話サービス保守
- URLオフロード
- リンクマネージャ
- Wake on LAN
- 再起動

■拡張ページ

- 拡張ページ

■外部リンク

- 製品ページ

ソフトウェアの更新

ソフトウェアを更新します。

ソフトウェアのアップデート

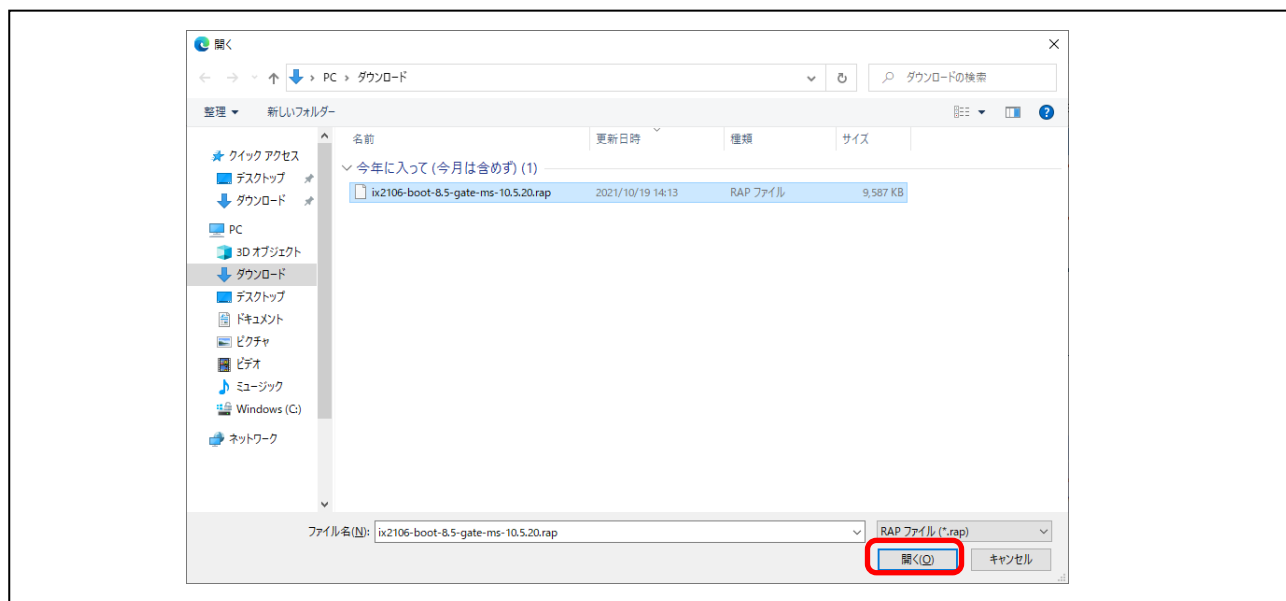
新しいソフトウェアのファイルを指定して、[アップデート実行]を押してください。
[アップデート実行]を押した後は完了メッセージが表示されるまで他の操作を行わないでください。
またBUSY LED(表示:BSY)点灯中は電源を切らないでください。故障の原因になります。

	現在の設定	設定の変更
バージョン	1.1.1	アップロードするファイルを指定してください。
ファイルの選択		ファイルが選択されていません

アップデート実行

6. 保守管理

- (5) 保存しておいたソフトウェアのプログラムファイル(拡張子が「.rap」のファイル)を選択します。



- (6) [アップデート実行]ボタンをクリックします。

注意 [アップデート実行]を押した後は完了メッセージが表示されるまで他の操作を行わないでください。アップデートには数分(3~4分)かかります。

注意 「BUSY LED」点灯中は電源を切らないでください。故障の原因になります。

ソフトウェアの更新



ソフトウェアを更新します。

ソフトウェアのアップデート

新しいソフトウェアのファイルを指定して、[アップデート実行]を押してください。

[アップデート実行]を押した後は完了メッセージが表示されるまで他の操作を行わないでください。

またBUSY LED(表示:BSY)点灯中は電源を切らないでください。故障の原因になります。

	現在の設定	設定の変更
バージョン		ファイルの選択  rap
		アップデート実行


6. 保守管理

- (7) メッセージが「ソフトウェアのアップデート中です。」から「ソフトウェアのアップデートが完了しました。」に変わったことを確認します。

ソフトウェアの更新

ソフトウェアのアップデート中です。

!! 注意 !! BUSY LED(表示:BSY)点灯中は電源を切らないでください。
完了メッセージが表示されるまで他の操作を行わないでください。



!! 注意 !! ソフトウェアが更新されています。
新しいソフトウェアを有効にするには、装置を再起動してください。

ソフトウェアの更新

ソフトウェアのアップデートが完了しました。
新しいソフトウェアを有効にするには、装置を再起動してください。

- (8) メニューエリアの「保守管理」、または、メッセージエリアから[再起動]をクリックします。

- 管理者メニュー
 - トップページ
 - 設定の保存
 - ログアウト
- かんたん設定
 - かんたん設定
- 詳細設定
 - 詳細設定
- 端末管理
 - 端末管理
- 保守管理
 - 装置状態の表示
 - 装置ログの取得
 - 設定データの管理
 - 設定の初期化
 - ソフトウェアの更新
 - pingの実行
 - 任意コマンドの実行
 - IP電話サービス保守
 - URLオフロード
 - リンクマネージャ
 - Wake on LAN
 - 再起動
- 拡張ページ
 - 拡張ページ
- 外部リンク
 - 製品ページ

!! 注意 !! ソフトウェアが更新されています。
新しいソフトウェアを有効にするには、装置を再起動してください。

ソフトウェアの更新

ソフトウェアのアップデートが完了しました。
新しいソフトウェアを有効にするには、装置を再起動してください。

6. 保守管理

(9) [再起動実行]ボタンをクリックして、装置の再起動を行います。

!!注意!! ソフトウェアが更新されています。
新しいソフトウェアを有効にするには、装置を『再起動』してください。

再起動

装置を再起動します。

よろしければ [再起動実行] を押してください。 [再起動実行]

(10) メッセージが「装置を再起動しています。」から「装置を再起動しました。」に変わったら、再度、ログインし、ソフトウェアのバージョンを確認します。

!!注意!! ソフトウェアが更新されています。
新しいソフトウェアを有効にするには、装置を『再起動』してください。

再起動

装置を再起動しています。

再起動の完了までには約2分かかります。
引き続き設定を行う場合は、再起動後ログインする必要があります。



トップページ

装置を再起動しました。

引き続き設定を行う場合は、ログインする必要があります。 [ログイン実行]

6. 保守管理

6.6 ping の実行

他の IP アドレスへの到達性を確認します。

- (1) ログイン後のメニューエリアから[保守管理]をクリックします。
- (2) [ping の実行]をクリックします。
- (3) 各項目を入力し、[ping 実行]ボタンをクリックします。
- (4) 実行結果を確認します。

pingの実行

IPv4またはIPv6のアドレスを入力してください。
他のIPアドレスへの到達性を確認します。
以下のフォームに入力して、[ping実行]を押してください。

実行内容

実行内容	
送信先 IPアドレス	192.168.1.1
送信元 IPアドレス	IPアドレスを指定する場合に入力してください。省略可能です。 (省略時はLANのIPアドレスが使用されます)
パケットサイズ	サイズを指定する場合に入力してください。省略可能です。

ping実行

実行結果

```
Router(config)# ping 192.168.1.1 source 192.168.1.254
PING 192.168.1.254 > 192.168.1.1 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=128 time=0.247 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=128 time=0.373 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=128 time=0.358 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=128 time=0.324 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=128 time=0.533 ms

--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 0.247/0.367/0.533
Router(config)#
```

番号	項目	内容
①	送信先 IP アドレス	送信先(到達性を確認したい宛先)の IP アドレスを入力します。
②	送信元 IP アドレス	IP アドレスを指定する場合に入力してください。省略可能です。 ・ 省略した場合、LAN の IP アドレスが使用されます。
③	パケットサイズ	サイズ(byte)を指定する場合に入力してください。省略可能です。 ・ 省略した場合、56byte のパケットが送信されます。 ・ 4~65507byte の範囲で指定することができます。

6. 保守管理

6.7 任意コマンドの実行

任意のコマンド(複数可)を実行します。コマンド対応のみの設定の変更や表示コマンドの確認などに利用できます。

- メモ** 実行できるコマンドは最大 1000000 文字(改行含む)です。
- メモ** 常にグローバルコンフィグモードから開始します。必要に応じて、モード遷移コマンドを入力してください。
- メモ** 対話形式で実行するコマンドや自律的なメッセージ出力を行わせるコマンドは、動作保証の対象外です。
- 注意** コマンドによっては本装置の設定が変更されるため、必要に応じて、設定の保存を行ってください。

- (1) ログイン後のメニューエリアから[保守管理]をクリックします。
- (2) [任意コマンドの実行]をクリックします。
- (3) 「コマンド入力」ボックスにコマンドを入力し、[コマンド実行]ボタンをクリックします。



6. 保守管理

(4) コマンドの実行結果を確認します。

任意コマンドの実行

任意のコマンド(複数可)を実行します。コマンドでのみ対応している設定の変更や表示コマンドの確認などに利用できます。
コマンド入力欄にコマンドを入力して、[コマンド実行] を押してください。
なお、常にグローバルコンフィグモードから開始します。必要に応じて、モード遷移コマンドを入力してください。

コマンド入力

現在 43 文字 / 最大 1000000 文字 コマンド実行

実行結果

```
Router(config)# hostname Router-IX2105
Router-IX2105(config)# show running-config
!
! NEC Portable Internetwork Core Operating System Software
! IX Series IX2105 (magellan-sec) Software, Version 9.6.8T, BETA TEST SOFTWARE
! Compiled Jul 06-Thu-2017 17:49:31 JST #2
! Current time Jul 07-Fri-2017 16:40:14 JST
!
hostname Router-IX2105
timezone +09 00
!
username admin password hash 8de6a5E1af2Ffa454E40994e810A56e administrator
!
logging buffered 131072
logging subsystem all warn
logging timestamp datetime
!
!
ip ufs-cache enable
ip dhcp enable
ip access-list web-http-acl permit ip src any dest 192.168.1.254/32
```

6. 保守管理

6.8 IP 電話サービス保守

他拠点の UNIVERGE Aspire シリーズへ VPN を経由してリモートでアクセスし、リモートメンテナンスの接続/切断の操作ができます。

- (1) ログイン後のメニューエリアから[保守管理]をクリックします。
- (2) [IP 電話サービス保守]をクリックします。
- (3) 各項目を入力し、[反映]ボタンをクリックします。

- 本 Web 設定機能に対応する UNIVERGE Aspire シリーズおよび設定内容の詳細については、UNIVERGE Aspire シリーズの販売店にご相談ください。
- 「リモートメンテナンス接続先の設定」は、省略して設定することが可能です。ただし、リモートメンテナンスの[接続]や[切断]が実行できなくなります。
- [反映]と[接続]ボタンクリック後は、約 5 秒間の待機画面が表示されます。

IP電話サービス保守：リモートメンテナンス接続

他拠点のUNIVERGE Aspire UXへVPNを経由してリモートでアクセスしたい場合に利用します。

リモートメンテナンスの状態

リモートメンテナンスの接続/切断の操作を行います。

接続状態	設定されていません
------	-----------

リモートメンテナンス接続先の設定

リモートメンテナンス接続先の情報を設定します。

	現在の設定	設定の変更
接続先電話番号		接続先の電話番号を入力してください。 <input type="text"/>
接続先ネットワークアドレス		接続先のLAN側のネットワークアドレスを入力してください。 <input type="text"/> / <input type="text"/>
VPN接続用パスワード		接続先と共通のパスワードを設定してください。 <input type="text"/>

ルータの設定

本装置のリモートメンテナンス用設定情報を変更する/しないを選択します。

	現在の設定	設定の変更
ルータの設定	未設定	<input type="radio"/> ルータの設定を変更しない <input checked="" type="radio"/> ルータの設定を変更する

パスワードの設定

本装置のログイン認証用パスワードを設定します。

	現在の設定	設定の変更
ユーザ名	admin	変更できません
パスワード	パスワード設定なし	<input type="radio"/> パスワードを変更しない <input checked="" type="radio"/> パスワードを変更する <input type="text"/> 確認のためもう一度入力してください。 <input type="text"/>

WAN1: WAN側インタフェースの設定(GigaEthernet0.0)

「WAN側IPアドレス」「デフォルトゲートウェイ」「DNSアドレス」は自動取得します。
接続タイプを指定してください。

	現在の設定	設定の変更
接続タイプ		<input checked="" type="radio"/> ひかり電話回線直結 <input type="radio"/> ゲートウェイ (HGW,OGW等) 配下

LAN: LAN側インタフェースの設定(GigaEthernet1.0)


本装置のLAN側IPアドレスを設定します。


	現在の設定	設定の変更
LAN側IPアドレス	192.168.1.254/24	LAN側IPアドレスを設定してください。 <input type="text"/> / <input type="text"/>

6. 保守管理

番号	項目	内容
①	接続状態	リモートメンテナンスの接続状態を表示します。 <ul style="list-style-type: none"> 各接続先と「接続」や「切断」の実行ができます。 「更新」により、接続状態の更新ができます。
②	接続先電話番号	リモートメンテナンスを行う接続先の電話番号を入力してください。 <ul style="list-style-type: none"> 電話番号のハイフン(-)などは省略して入力することもできます。
③	接続先ネットワークアドレス	リモートメンテナンスを行う接続先のLAN側のネットワークアドレスを入力してください。
④	VPN 接続用パスワード	リモートメンテナンスを行う接続先と共通のパスワードを入力してください。 <ul style="list-style-type: none"> 半角英数字で1~128文字まで入力できます。
⑤	ルータの設定	リモートメンテナンスを行う本装置の設定を行います。 <ul style="list-style-type: none"> 未設定の場合、「ルータの設定を変更しない」を選択できません。 一度設定した後は「ルータの設定を変更しない」が選択され、表示内容が省略されます。
⑥	ユーザ名	本装置にログインするときのユーザ名です。 <ul style="list-style-type: none"> 初期状態ではユーザ名は設定されていません。 パスワード設定後のユーザ名は「admin」です。Web設定からは変更できません。
⑦	パスワード	本装置にログインするときのパスワードです。 <ul style="list-style-type: none"> 初期状態ではパスワードは設定されていません。 半角英数字で1~249文字まで入力できます。 注意 <ul style="list-style-type: none"> 大文字/小文字は区別されます。 パスワードの入力文字は表示されません。●●●のように伏せ文字で表示されます。 パスワードは、第三者に推測されにくく、忘れないような文字列を入力してください。
⑧	接続タイプ	接続のタイプを選択してください。
⑨	LAN側IPアドレス	LAN側IPアドレスを設定します。 IPアドレスを変更する場合、現在の接続は切断されます。新しいIPアドレスに接続しなおしてください。

(4) 「接続状態」が「接続」となることを確認します。

 [切断]をクリックすると、リモートアクセスの接続を切断できます。

 接続ができなかった場合は、「接続状態」に表示されるメッセージにしたがって操作してください。

IP電話サービス保守：リモートメンテナンス接続

他拠点の対応するUNIVERGE AspireシリーズへVPNを経由してリモートでアクセスしたい場合に利用します。

リモートメンテナンスの状態

リモートメンテナンスの接続/切断の操作を行います。

接続状態
接続
接続開始 2018/03/01 12:34:56

リモートメンテナンス接続先の設定

6. 保守管理

6.9 URL オフロード

URL オフロードが設定されている場合、そのオフロード対象となる宛先（URL/IP アドレス）を確認することができます。

注意 URL オフロードは、Web 設定画面から簡易的に設定することはできません。あらかじめ保守管理の任意コマンドの実行画面あるいはコマンドラインから設定してからご利用ください。

- (1) ログイン後のメニューエリアから[保守管理]をクリックします。
- (2) [URL オフロード]をクリックします。
- (3) 「オフロード対象リスト」に、オフロード対象となる宛先（URL/IP アドレス）が表示されます。

メモ オフロード対象は XML 形式のファイルを取得した結果の他、あらかじめ本装置に設定することができます。

メモ オフロード対象の除外で登録された URL あるいは IP アドレスは、「×」と表示されます。

URL オフロード		
オフロード対象リスト		
○はオフロードされ、×はオフロードされません。番号が小さい方が優先されます。		
データベース取得日時: 2017/06/27 12:58:54, データベース更新情報: 6/6/2017		
1	×	http://www.example.com
2	○	http://www.example.com
3	○	http://www.example.com
4	○	http://www.example.com
5	×	http://www.example.com
6	×	http://www.example.com
7	○	http://www.example.com
8	○	http://www.example.com
9	○	http://www.example.com
10	○	http://www.example.com
11	○	http://www.example.com
12	○	http://www.example.com
13	○	http://www.example.com
14	○	http://www.example.com
15	○	http://www.example.com
16	○	http://www.example.com
17	○	http://www.example.com
18	○	http://www.example.com
19	○	http://www.example.com
20	○	http://www.example.com
21	○	http://www.example.com
22	○	http://www.example.com
23	○	http://www.example.com
24	○	http://www.example.com
25	○	http://www.example.com
26	○	http://www.example.com
27	○	http://www.example.com
28	○	http://www.example.com

6. 保守管理

6.10 リンクマネージャ

端末管理のリンクマネージャを登録している場合、端末の状態を確認することができます。

注意 あらかじめ端末管理のリンクマネージャで端末を登録する必要があります。

- (1) ログイン後のメニューエリアから[保守管理]をクリックします。
- (2) [リンクマネージャ]をクリックします。
- (3) 登録されている端末のグループが「表示グループ一覧」に表示されます。

The screenshot shows a web interface with a left sidebar menu and a main content area. The sidebar menu includes sections like '管理者メニュー', 'かんたん設定', '詳細設定', '端末管理', '保守管理', '拡張ページ', and '外部リンク'. The '保守管理' section is expanded, and 'リンクマネージャ' is highlighted. The main content area is titled 'リンクマネージャ' and contains the text '端末情報を表示します。以下のリンクから選択してください。' Below this, there is a section titled '表示グループ一覧' which contains a list of groups: '0. 未登録', '1. 2021-北', and '2. 2021-南'. This list is enclosed in a red rectangular box. At the bottom right of the main content area, there is a button labeled '端末情報をCSV形式で表示'.

6. 保守管理

(4) 「表示グループ一覧」から、確認するグループをクリックします。

メモ [端末情報を CSV 形式で表示]をクリックすることで、CSV 形式で表示させることもできます。



(5) 各グループに登録されている端末一覧が表示されたことを確認します。



6. 保守管理

6.11 Wake on LAN

Wake on LAN 機能を使い、指定した端末の電源を ON にすることが可能です。また、端末毎の IP アドレスを登録しておくことで、端末の電源状態が ON になっているかを制御画面から確認することができます。

注意 本機能では、ルータに直接接続されている同一リンク上の端末以外を起動することはできません。

注意 Wake on LAN 機能の利用にはコマンドラインからの設定が必要です。本章ではあらかじめ設定コマンドが投入されているものとして操作画面の紹介をしています。コマンドライン設定については、『コマンドリファレンスマニュアル』をご覧ください。

注意 Wake on LAN 機能の利用には端末側にも設定が必要な場合があります。端末側の設定方法については、ご利用になる端末の説明書やメーカーサイトをご参照ください。

(1) メニューエリアの「保守管理」から[Wake on LAN]をクリックします。

メモ ログイン前の場合、ユーザ名とパスワードを入力する画面が表示されます。“ユーザ名”と“パスワード”を入力し、[OK]ボタンをクリックします。

メモ 利用者パスワードを設定している場合、ユーザ名とパスワードを入力する画面が表示されます。“ユーザ名”と“パスワード”を入力し、[OK]ボタンをクリックします。Web 設定からパスワードを登録・変更した場合、ユーザ名の初期設定は「monitor」です。

メモ パスワードを登録・変更する前にユーザ名とパスワードを入力する画面が表示された場合、そのまま「OK」ボタンをクリックしてください。

(2) 起動したい端末の[起動]ボタンをクリックします。

Wake on LAN

端末を起動します。起動したい端末の [起動] を押してください。

端末状態の確認

端末情報一覧

端末名	MACアドレス	IPアドレス	送信インターフェース	状態	
PC_1	<input type="button" value="起動"/>	00:11:22:33:44:55	192.168.1.100	GigaEthernet1.0	-
PC_2	<input type="button" value="起動"/>	66:77:88:99:aa:bb	192.168.1.101	GigaEthernet1.0	-

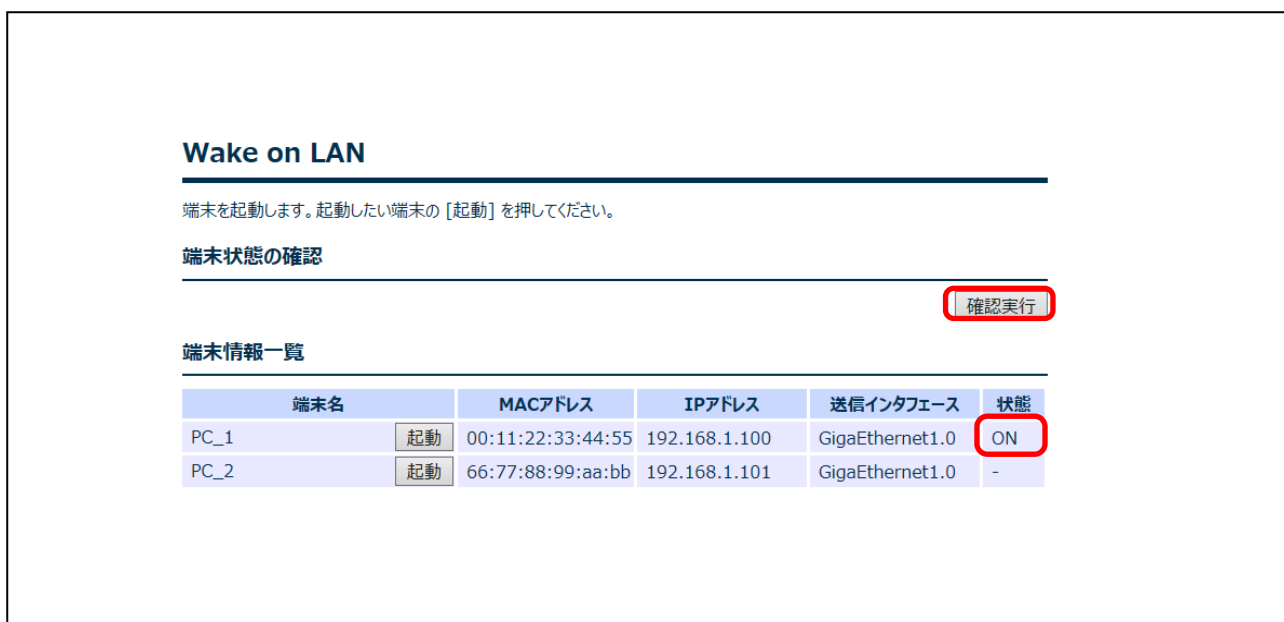
6. 保守管理

- (3) [起動実行]ボタンをクリックします。
指定した端末の電源をONにして、【端末の起動制御】画面に切り替わります。



- (4) [確認実行]ボタンを押すと、IP アドレスを登録している端末の電源状態を確認することができます。

メモ 端末の電源状態は、IX ルータから ping パケットを送信することで確認を行っています。そのため IP アドレスを登録していない端末は、電源の状態が表示されません。また、端末のファイアウォールやウイルスソフトの設定によって表示されない場合があります。



6. 保守管理

6.12 再起動

装置を再起動します。

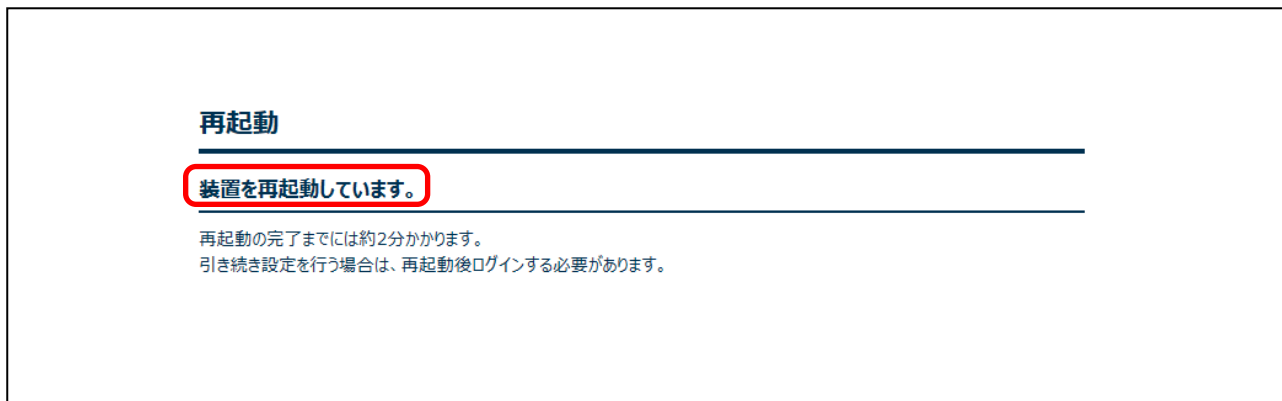
 設定を変更したときは、設定の保存を行ってから再起動してください。

- (1) ログイン後のメニューエリアから[保守管理]をクリックします。
- (2) [再起動]をクリックします。
- (3) [再起動実行]ボタンをクリックして、装置の再起動を行います。

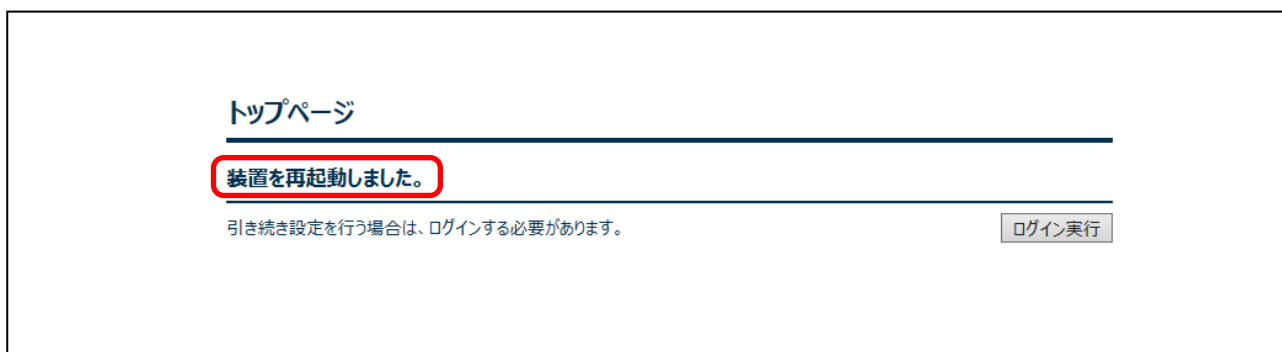


6. 保守管理

- (4) 「装置を再起動しています。」のメッセージを確認し、数分待ちます。



- (5) 「装置を再起動しました。」のメッセージを確認します。



7. 拡張ページ

7 拡張ページ

本章では、HTML や画像ファイルなどをまとめた zip ファイルをアップロードすることで、Web ページの追加・置き換えが可能な『拡張ページ』について説明します。

7.1 拡張ページのアップロード

7.2 拡張ページの削除

7. 拡張ページ

7.1 拡張ページのアップロード

拡張ページをアップロードします。

注意 対応する拡張子は以下の通りです。

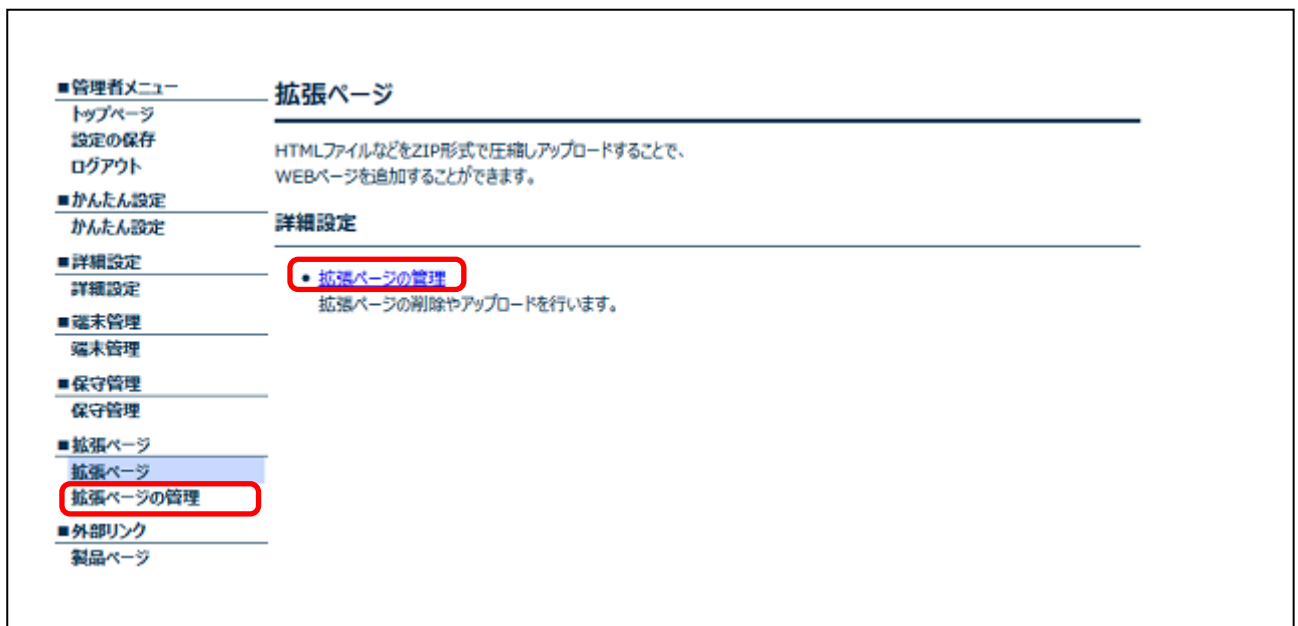
- html、htm、css、js
- jpeg、jpg、gif、png、bmp、ico

これらの拡張子ファイルをフォルダ(フォルダ名は「custom」)にまとめて、圧縮ファイル(拡張子が「.zip」のファイル)を作成して、パソコンに保存してください。

注意 圧縮後のファイル名は任意の名前に変更可能(日本語不可)ですが、圧縮前のフォルダ名は「custom」としてください。

(1) ログイン後のメニューエリアから[拡張ページ]をクリックします。

(2) 拡張ページの[拡張ページの管理]をクリックします。



7. 拡張ページ

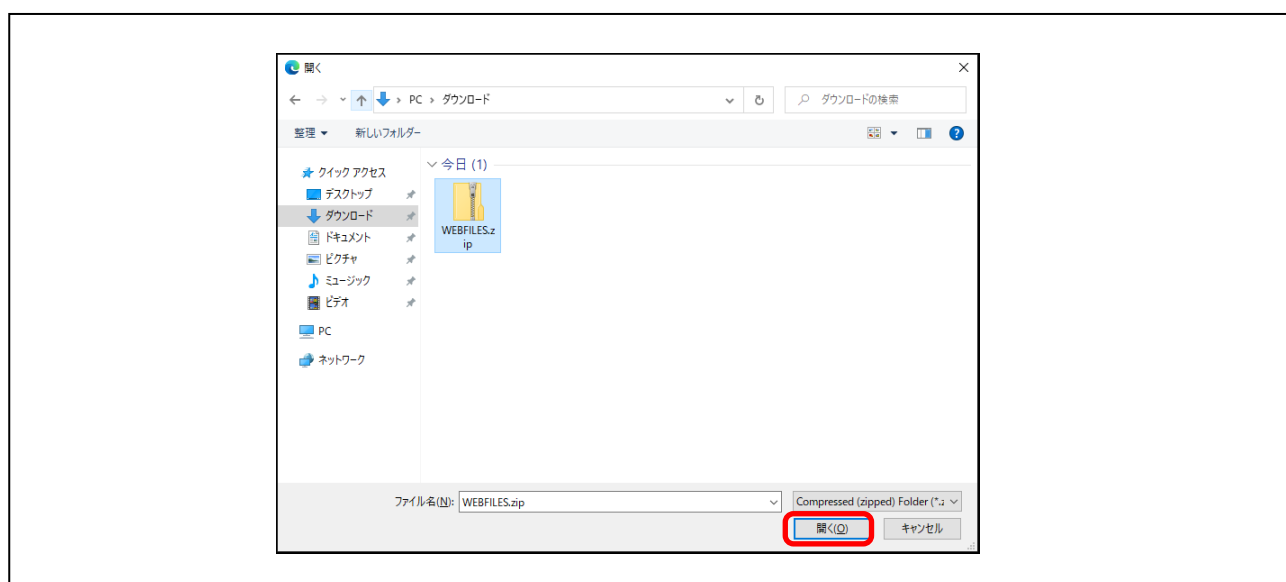
(3) 「拡張ページのアップロード」の[ファイルの選択]ボタンをクリックします。

拡張ページを上書きする場合は、「拡張ファイルを上書きします。」にチェックを入れてください。



(4) 保存しておいた拡張ページの圧縮ファイル(拡張子が「.zip」のファイル)を選択します。

Windows の設定によってはファイル名に拡張子が表示されません。



7. 拡張ページ

(5) [アップロード実行]ボタンをクリックします。

注意 [アップロード実行]をクリックした後は完了メッセージが表示されるまで他の操作を行わないでください。

注意 「BUSY LED」点灯中は電源を切らないでください。故障の原因になります。

拡張ページの管理

拡張ページをアップロードします。

拡張ページの情報

現在の設定
拡張ページなし

拡張ページのアップロード

拡張ページのZIPファイルを指定して、[アップロード実行]を押してください。
[アップロード実行]を押した後は完了メッセージが表示されるまで他の操作を行わないでください。
またBUSY LED(表示:BSY)点灯中は電源を切らないでください。故障の原因になります。

設定の変更

ファイルの選択   .zip

アップロード実行

(6) メッセージが「拡張ページのアップロード中です。」から「拡張ページのアップロードが完了しました。」に変わったことを確認します。

拡張ページのアップロード中です。
終了メッセージが表示されるまで他の操作を行わないでください。
またBUSY LED(表示:BSY)点灯中は電源を切らないでください。故障の原因になります。

↓

拡張ページの管理

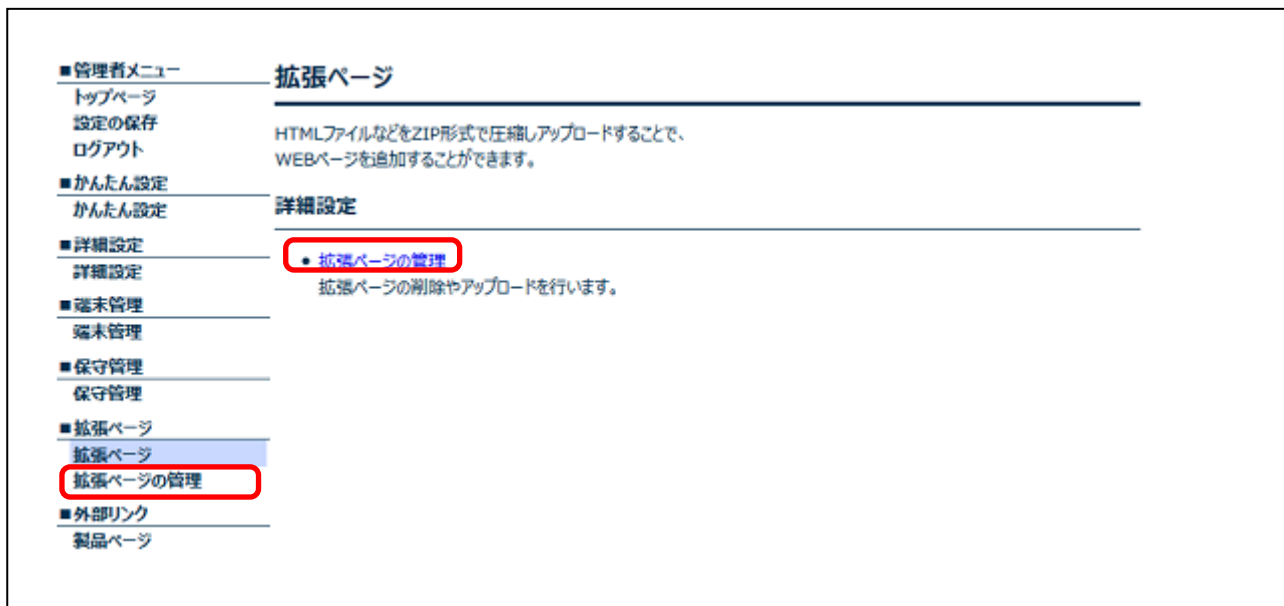
拡張ページのアップロードが完了しました。

7. 拡張ページ

7.2 拡張ページの削除

拡張ページを削除します。

- (1) ログイン後のメニューエリアから[拡張ページ]をクリックします。
- (2) 拡張ページの[拡張ページの管理]ボタンをクリックします。



- (3) 「拡張ページの情報」の「拡張ファイルを削除します。」にチェックを入れ、[削除実行]ボタンをクリックします。

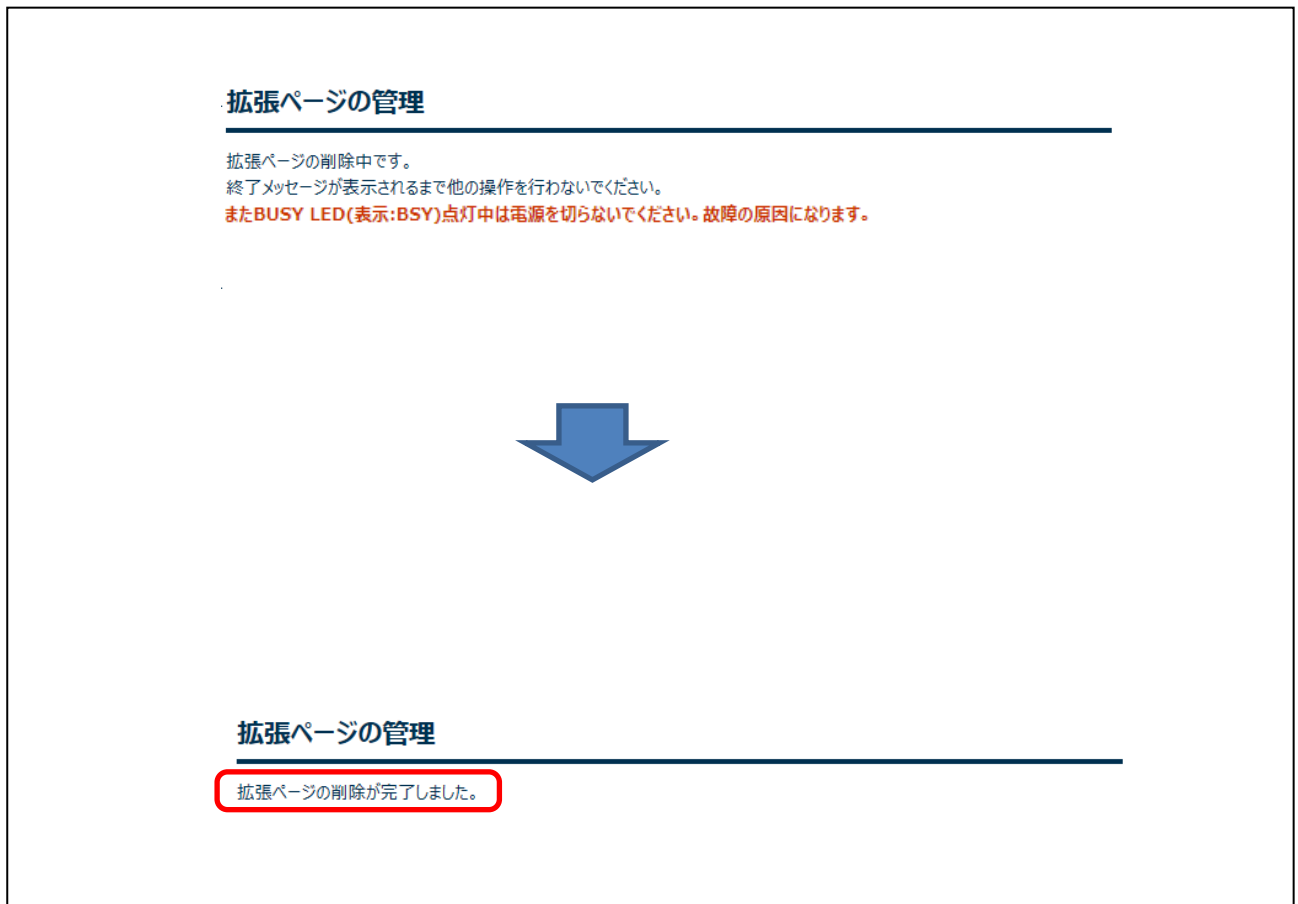
注意 [削除実行]をクリックした後は完了メッセージが表示されるまで他の操作を行わないでください。

注意 「BUSY LED」点灯中は電源を切らないでください。故障の原因になります。



7. 拡張ページ

- (4) メッセージが「拡張ページの削除中です。」から「拡張ページの削除が完了しました。」に変わったことを確認します。



8. 困ったときには

8 困ったときには

本章では、『困ったときには』について説明します。

画面に表示されるメッセージについて、それぞれの理由を確認できます。

8.1 メッセージエリアの警告メッセージ

8.2 入力エラーメッセージ

8.1 メッセージエリアの警告メッセージ

メッセージエリアに表示される警告メッセージの一覧です。

画面に表示される警告メッセージと、表示した理由を説明しています。

画面表示	表示理由
!!注意!! パスワードが設定されていません。 『パスワードの設定』を行ってください	ログインパスワードが設定されていません。
!!注意!! パスワードの再設定が必要です。 『パスワードの設定』でパスワードの再設定を行ってください	ログインパスワードが削除されています。 パスワードの再設定を行ってください。
!!注意!! パスワードの再設定が必要です。 『Wake on LAN の設定』でパスワードの再設定を行ってください	Wake on LAN のログインパスワードが削除されています。 パスワードの再設定を行ってください。
!!注意!! 保存されていた設定を削除しました。 装置を初期状態(工場出荷状態)に戻すには、設定を保存せずに装置を『再起動』を行ってください。	本装置の初期化が実行されました。
!!注意!! 設定が変更されています。 再起動した場合、保存していない設定は元の状態に戻ります。設定完了後は必ず『設定の保存』を行ってください。	各設定ページで設定情報が変更されています。
!!注意!! 設定データが更新されています。 新しい設定データを有効にするには、設定を保存せずに『再起動』を行ってください。	設定データが本装置へアップロードされましたが、有効になっていません。
!!注意!! 再起動が必要な設定の変更がされています。 設定を反映するためには、『設定の保存』したうえで、『再起動』してください。再起動を行わない場合や設定を保存せずに再起動した場合には設定が反映されません。	再起動が必要な設定変更が行われました。
!!注意!! ソフトウェアが更新されています。 新しいソフトウェアを有効にするには、装置を『再起動』してください。	ソフトウェアのアップデートが正常に終了しました。
!!注意!! BUSY LED 点灯中は電源を切らないでください。 完了メッセージが表示されるまで他の操作を行わないでください。	ソフトウェアのアップデート中です。メッセージ表示中に電源を切ると、本装置を起動できなくなるなど、故障の原因となります。
!!注意!! VPN (IPsec) 向けのデフォルトルートが変更された可能性があります。 『VPN の設定』を行っていた場合、再設定する必要があります。『VPN の設定』を選択し、入力値を変更せず[反映]を押してください。	VPN(IPsec)設定後にプロバイダの設定を実行したため、デフォルトルートに問題があります。
!!注意!! 設定の保存に失敗しました。 再起動した場合、設定は元の状態に戻ります。	設定の保存に失敗しました。
設定の反映に失敗しました。	入力した値や文字列に問題があります。

8. 困ったときには

入力値を見直してください。	
ソフトウェアの更新に失敗しました。 ファイル名が長すぎます。	ソフトウェアファイル名が長すぎます。
ソフトウェアの更新に失敗しました。 ファイル名に使用できない文字があります。	ソフトウェアファイル名に使用できない文字が含まれています。
ソフトウェアの更新に失敗しました。 ファイルサイズが制限を超えています。	ソフトウェアファイルのサイズ異常を検出しました。
ソフトウェアの更新に失敗しました。 ファイル形式が異常です。	ソフトウェアファイルが正しくありません。
ソフトウェアの更新に失敗しました。 ファイルが破損しています(CRC エラー)。	ソフトウェアファイルの CRC エラーを検出しました。
ソフトウェアの更新に失敗しました。 ファイルが破損しています。	ソフトウェアファイルの破損を検出しました。
ソフトウェアの更新に失敗しました。 起動中のファイルと同じです。	起動中のソフトウェアと同じソフトウェアを指定しました。
ソフトウェアの更新に失敗しました。 不明なエラーです。	ソフトウェア更新時に内部エラーが発生しました。
設定データのアップロードに失敗しました。 ファイルサイズが制限を超えています。	設定データのサイズ異常を検出しました。
設定データのアップロードに失敗しました。 設定ファイルのアップロードに失敗しました。	設定データのアップロードに失敗しました。
拡張ページのアップロードに失敗しました。 拡張ファイルのアップロードに失敗しました。	拡張ファイルのアップロードに失敗しました。
拡張ページのアップロードに失敗しました。 拡張ファイルが ZIP ファイルではないか、破損しています。	アップロードした拡張ファイルが ZIP ファイルではないか、破損しています。

8. 困ったときには

8.2 入力エラーメッセージ

入力画面で入力内容に間違いがあったとき、入力ボックス下やページ右下付近に表示されるメッセージです。

画面に表示される入力エラーメッセージと、エラーの理由を説明しています。

画面表示	表示理由
使用できない文字があります。	使用不可能な文字がフォームに入力されました。
文字列長が長すぎます。	フォームに入力している文字数が入力可能な範囲を越えています。
コマンド長が長すぎます。	フォームに入力しているコマンドの文字数が入力可能な範囲を越えています。
文字列(半角英数字)を入力してください。	文字列の入力形式が間違っています。
IP アドレスを入力してください。	IP アドレスが未記入、あるいは入力形式が間違っています。
IP アドレスとプレフィックスの組み合わせが不正です。	ネットワーク指定時の IP アドレス(プレフィックス)とサブネットマスクが不一致です。
パスワードを入力してください。	ログインパスワードが入力されていません
確認用パスワードを入力してください。	確認用のログインパスワードが入力されていません
パスワードが一致していません。	設定したパスワードと確認のためのパスワードの文字列が一致していません。
数字を入力してください。	ポート番号が入力されていません。
範囲が異常です。	ポート番号の範囲指定が異常です。
範囲外の数字です。	入力範囲外の値を入力しました。
PDP を選択してください。	USB 接続の PDP タイプが選択されていません。
FQDN の形式が不正です。	FQDN の入力値が正しくありません。
年を入力してください。 月を入力してください。 日を入力してください。 時を入力してください。 分を入力してください。 秒を入力してください。	時刻設定に値が入力されていません。
範囲外の年です。 範囲外の月です。 範囲外の日です。 範囲外の時です。 範囲外の分です。 範囲外の秒です。	時刻設定に入力範囲外の値を入力しました。
DNS アドレスの自動取得は、WAN 側 IP アドレスが自動取得の場合のみ選択可能です。	プロバイダの設定の接続形態で IP 接続を選択時、WAN 側 IP アドレスは手動設定していますが、DNS アドレスは自動取得を選択しています。
シーケンス番号が重複しています。	フィルタの設定で、既に使われているシーケンス番号を登録しようとした。
他の VPN で Tunnel インタフェースが使用中です。	L2TP の設定で、既に使われているトンネル番号を登録しようとした。

UNIVERGE IX2000/IX3000シリーズ
Web設定マニュアル
GYS-096530-004-00

© NEC Corporation 2026
2026年4月 第1.1版
日本電気株式会社
(禁無断複製)

NEC