NEC

UNIVERGE

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
ご使用の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 NAPT 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

⑴ 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」をご覧になり、正しくお使いいただきますようお願い致します。
⑵ 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。
⑶ 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。
⑷ 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。
⑸ 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。
⑹ 運用した結果については、⑸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 NAPT 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
注意	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。
メモ	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

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

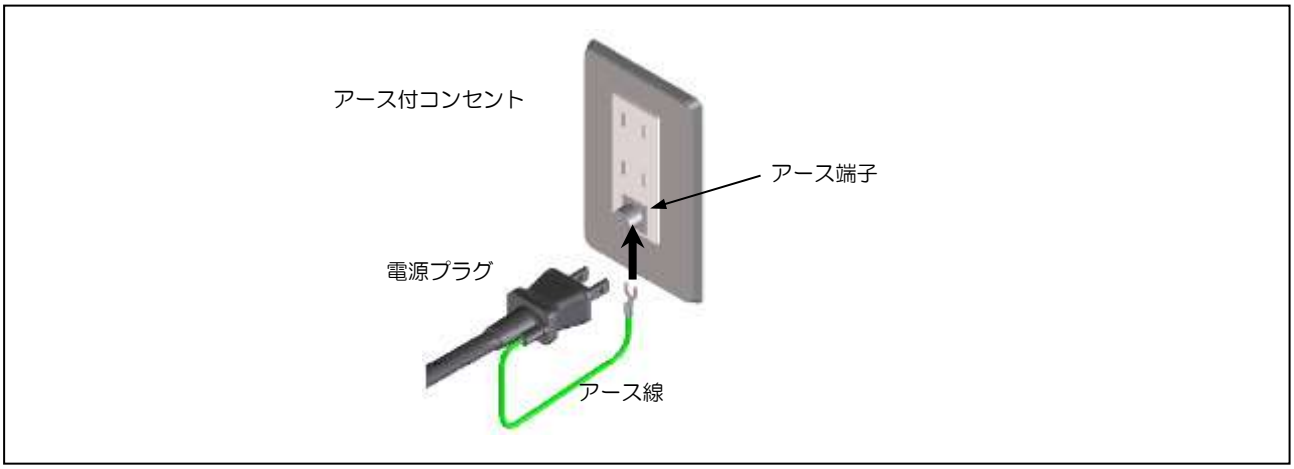
1.1 IX2107/IX2235 をお使いの方

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

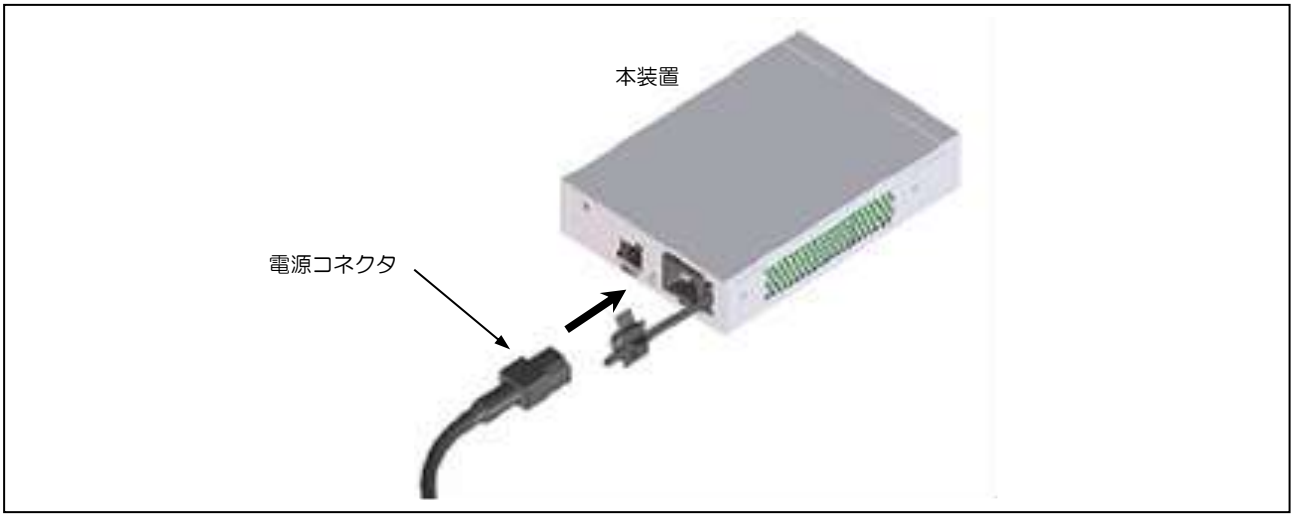
(1) 添付の電源ケーブルに付いているアース線をコンセントのアース端子に確実に接続します。なお、その際、アース線についている保護キャップを外してから接続してください。

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。

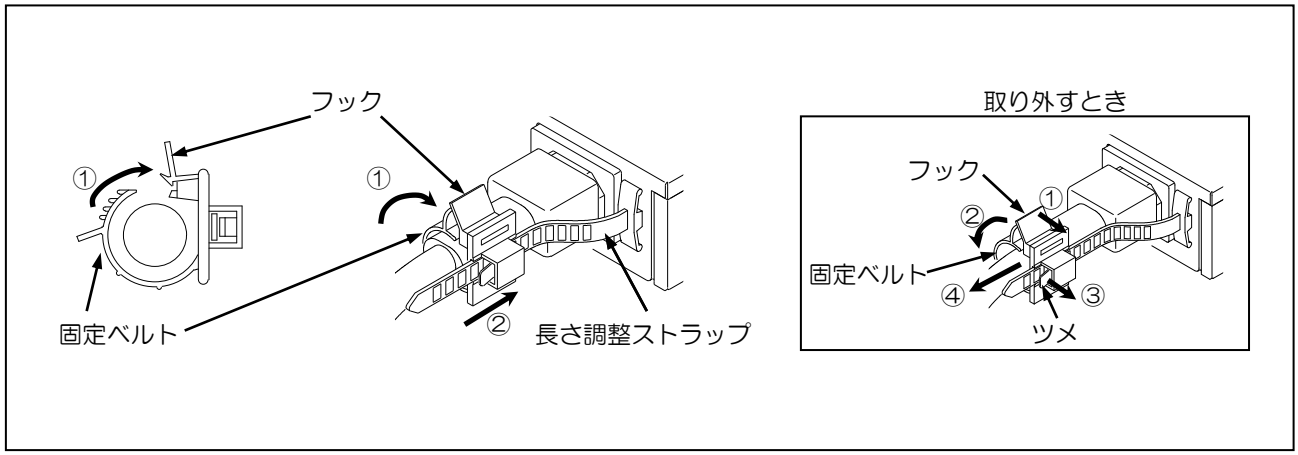


⑵　電源コネクタを本装置に接続します。

注意　緩みのないように確実に挿し込みます。



⑶　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。



⑷　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。

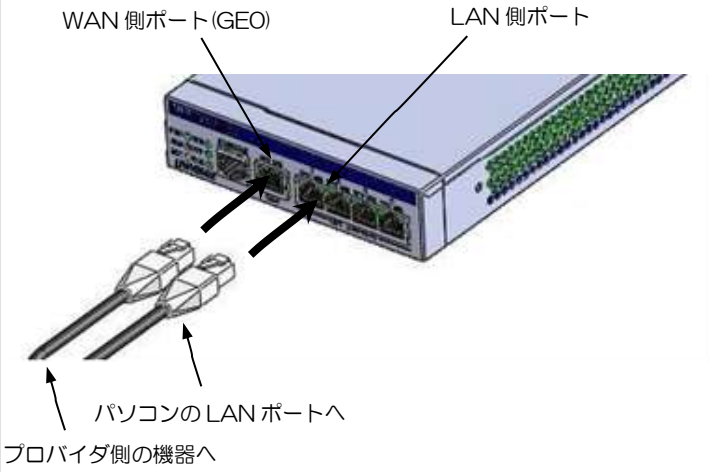
メモ　本装置は、ストレート結線／クロス結線を自動認識します。

1. Web 設定の準備

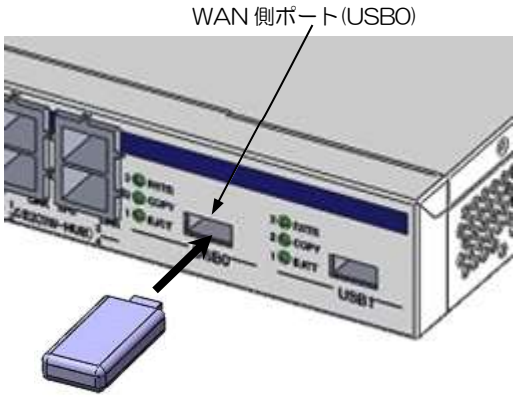
(5) 本装置の WAN 側ポート(GE0/USB0)とプロバイダ側の機器(ONU 等)、または、データ通信端末を接続します。

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。

［有線回線接続の場合］



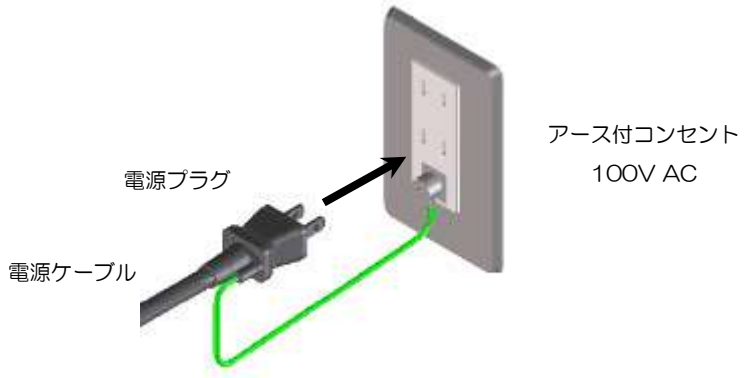
［モバイル回線接続の場合］
※IX2215/IX2235 のみ



(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。

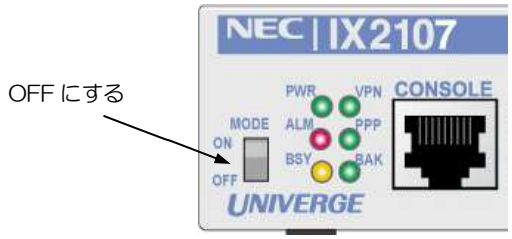


1. Web 設定の準備

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。

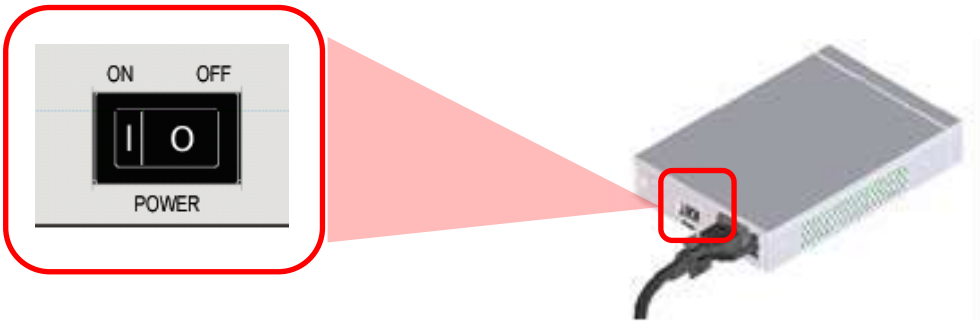


1.1.3 本装置の電源を入れる

(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。

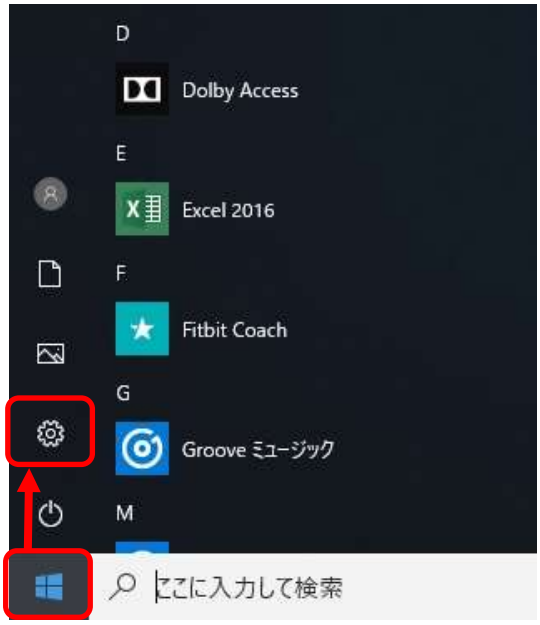
メモ 起動には 30 秒程度かかります。



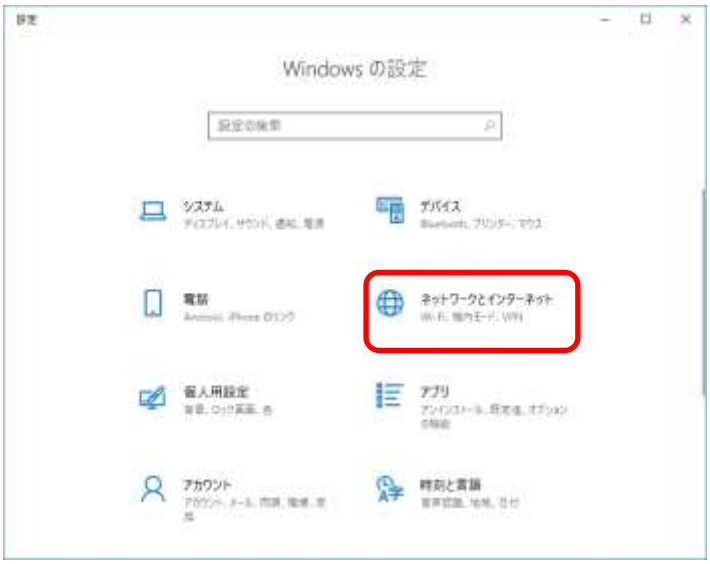
1. Web 設定の準備

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。



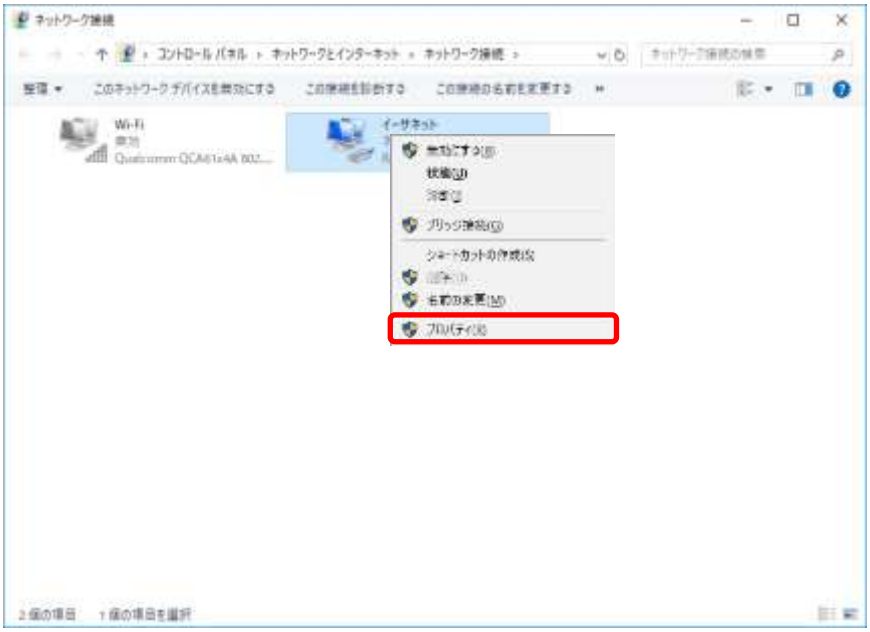
(2) [ネットワークとインターネット]をクリックします。



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。

(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。

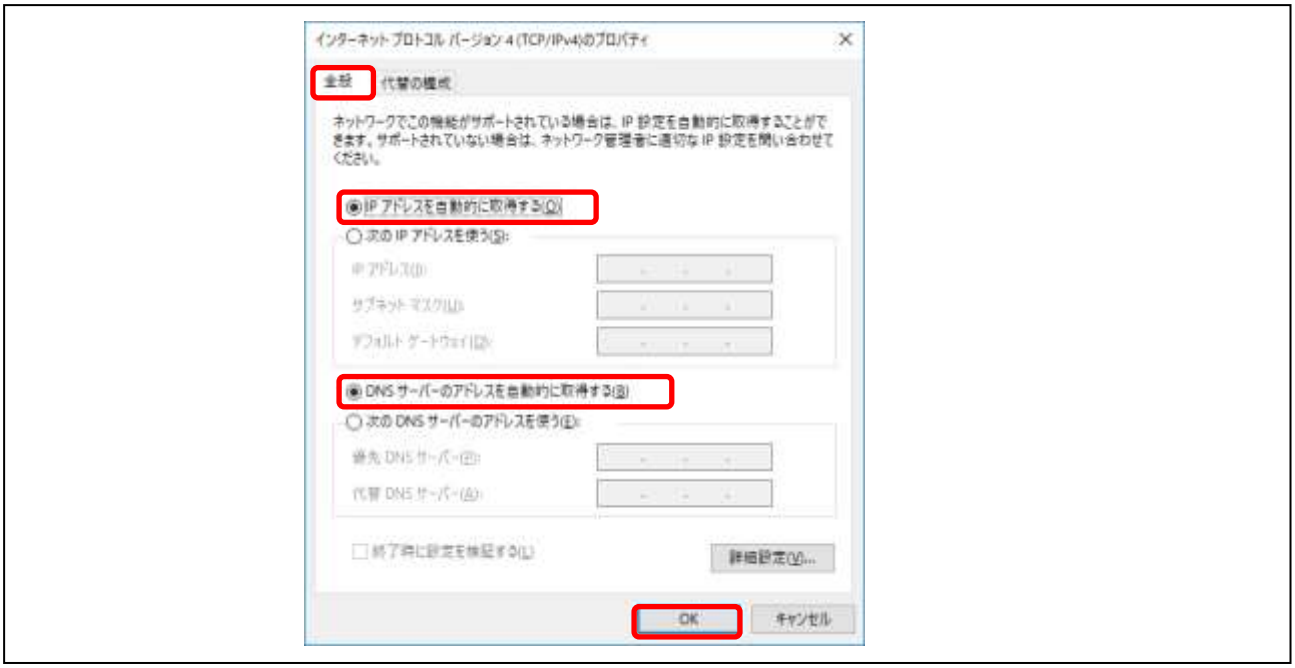
(6) [プロパティ(R)]をクリックします。

(7) [全般]タブをクリックします。

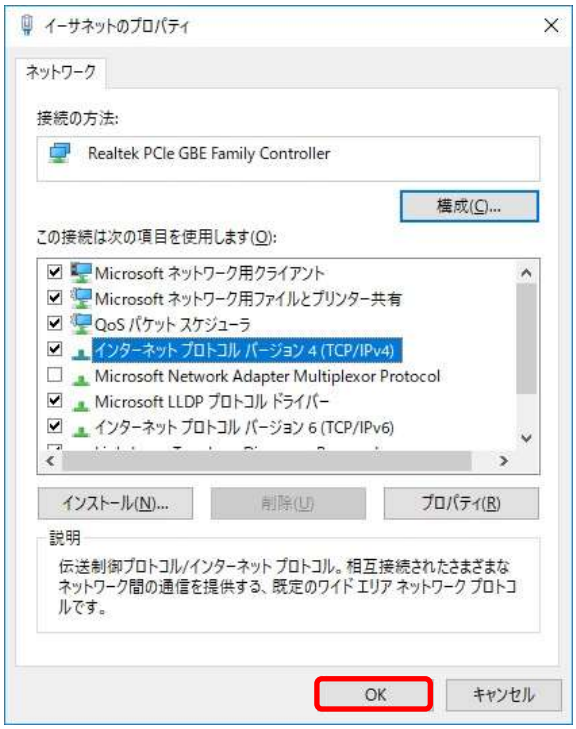
(8) [IP アドレスを自動的に取得する(O)] のラジオボタンをチェックします。

(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。



(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。

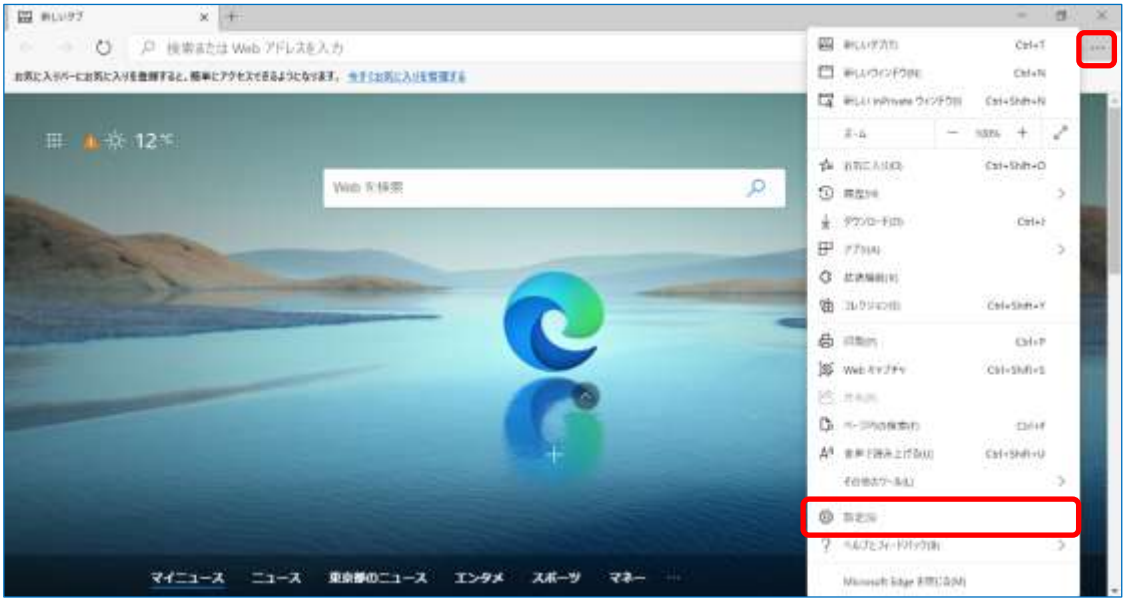


1.1.5 パソコンのブラウザを設定する

メモ 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。

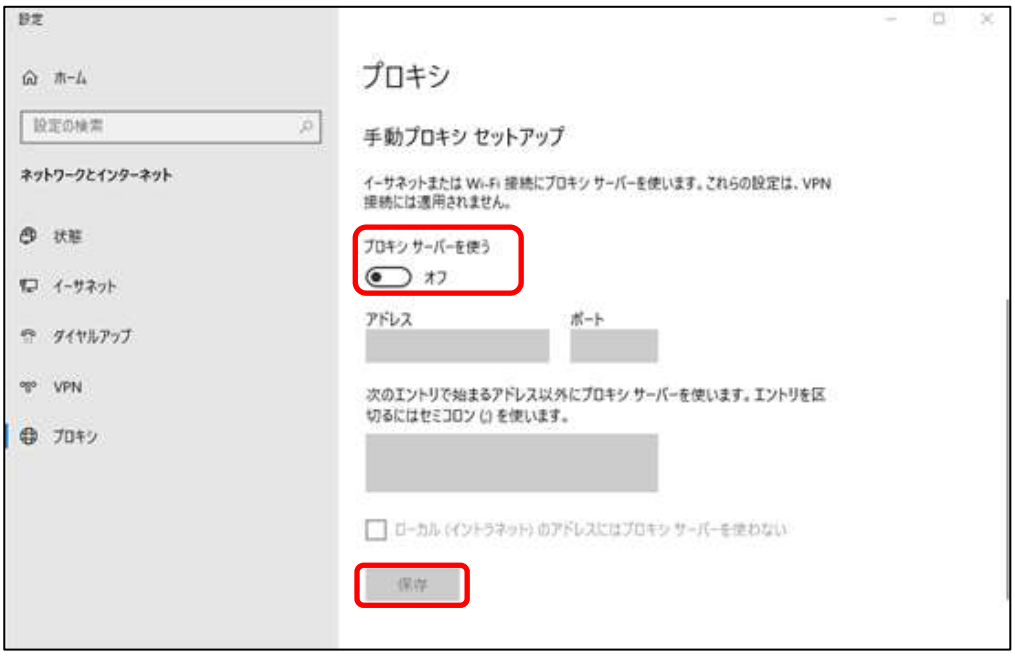


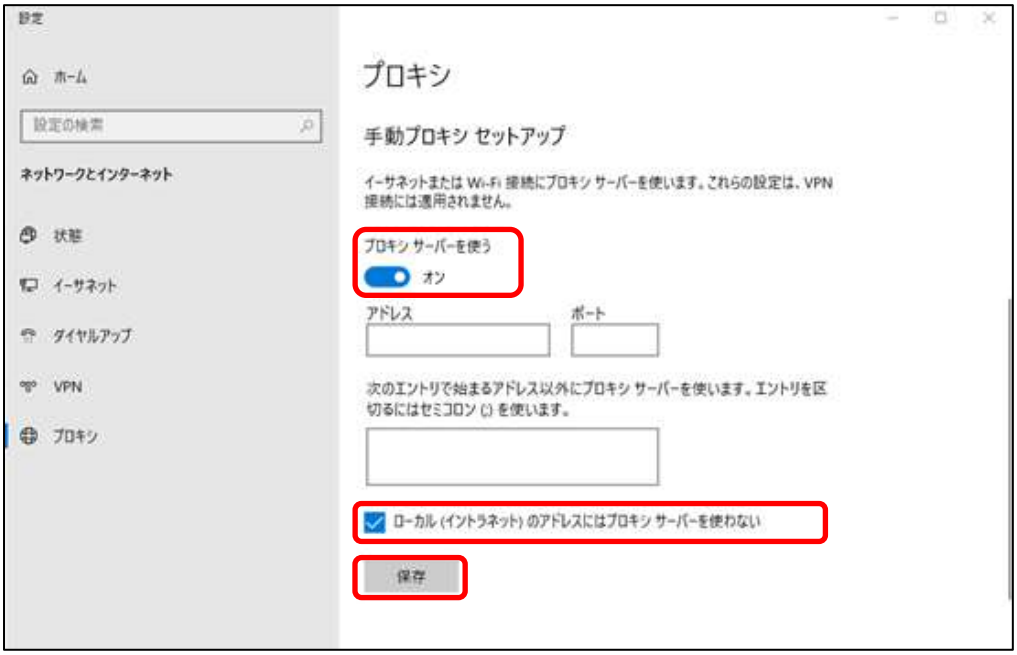
1. Web 設定の準備

(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。

メモ 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。

(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。

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

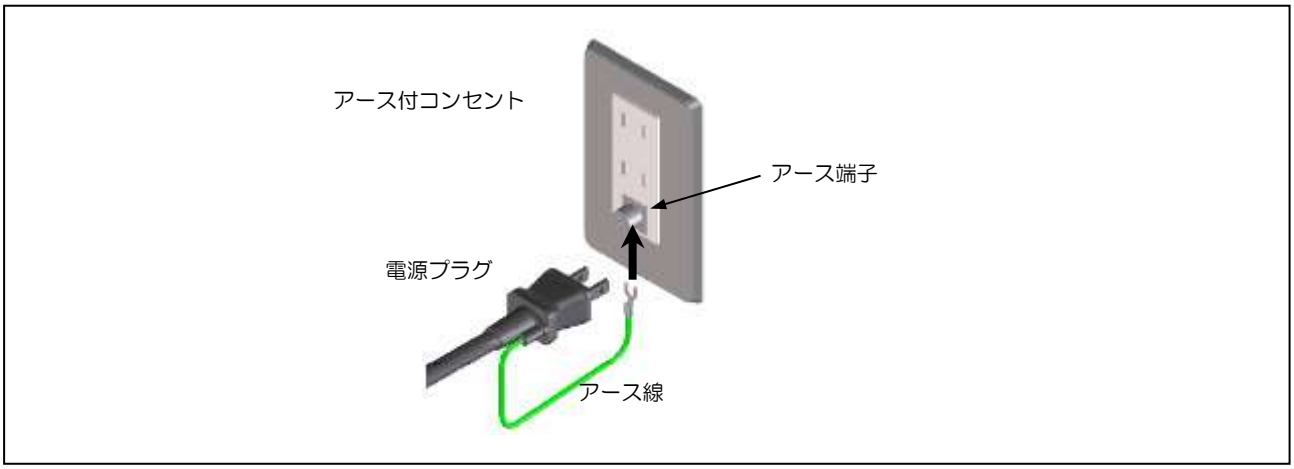
IX2215/IX2310/IX3315 で Web 設定を利用する場合、Web 設定を使用できるようにするための設定を別途投入する必要があります。

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。

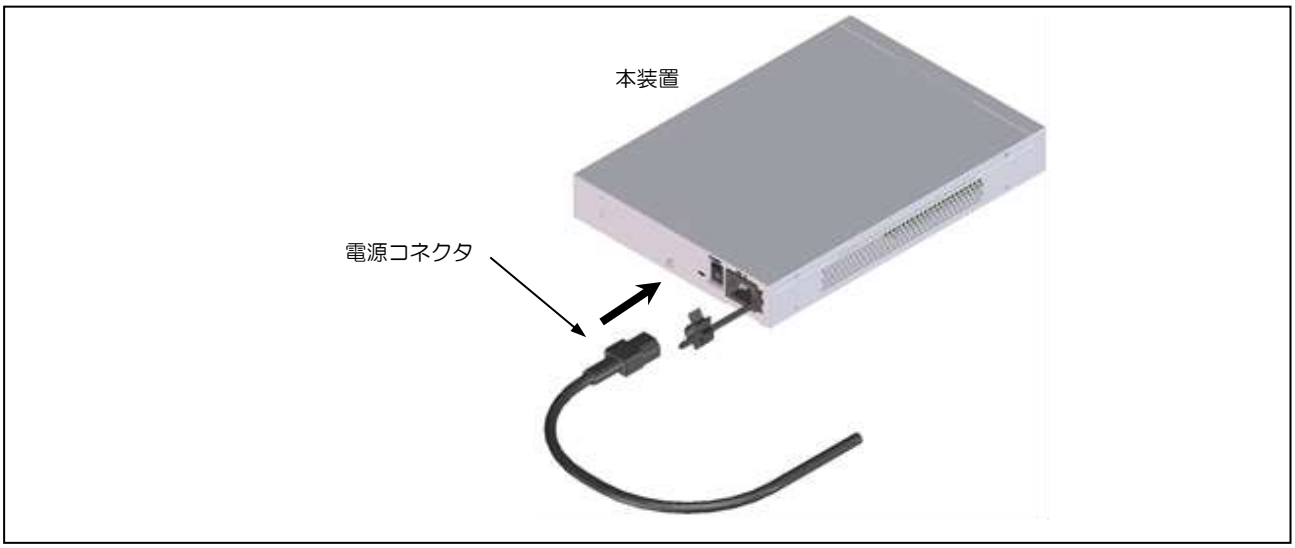
注意 接続するのはアース線のみです。(1)では電源プラグはコンセントに絶対に接続しないでください。

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。

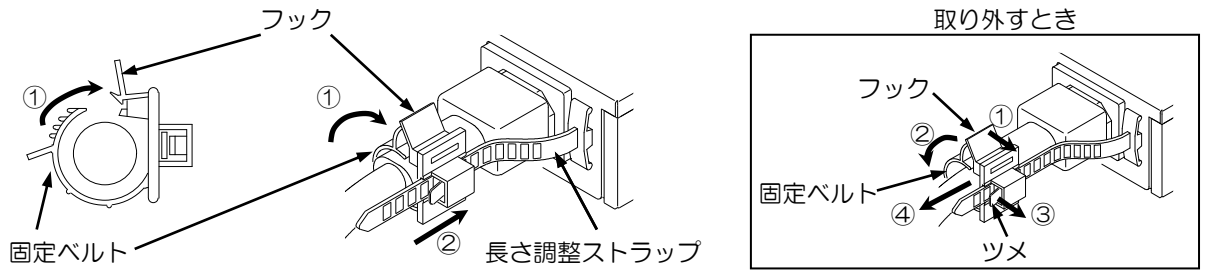


(2) 電源コネクタを本装置に接続します。

注意 緩みのないように確実に挿し込みます。



(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。

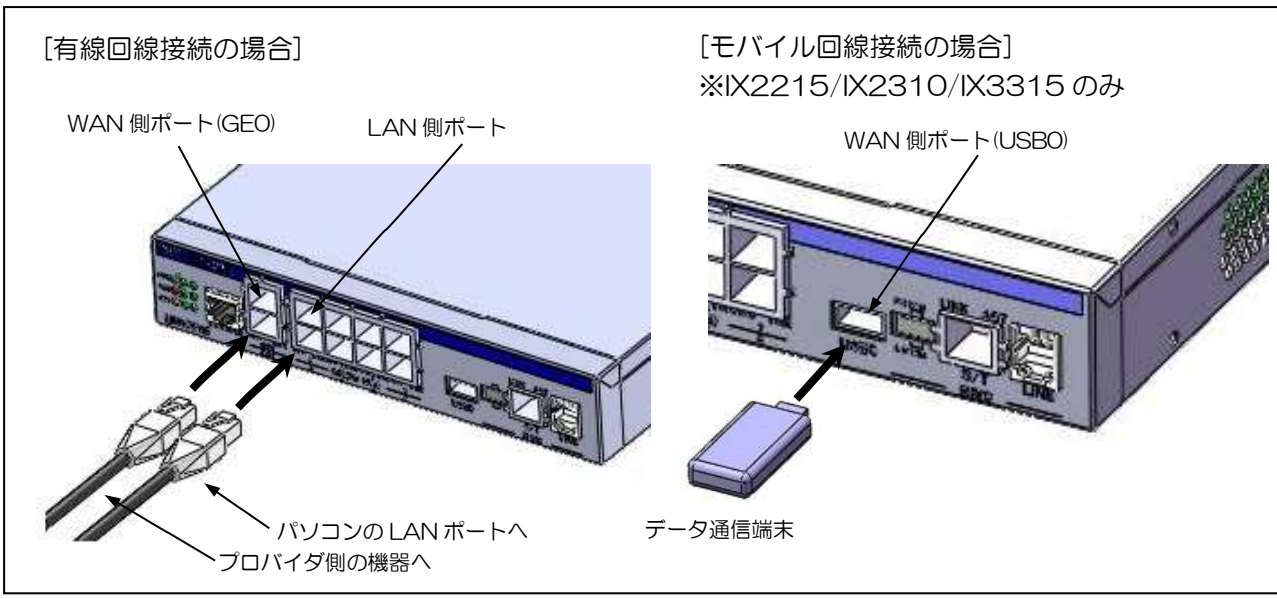
注意 カテゴリ 5 以上のストレート結線またはクロス結線の UTP または STP ケーブルを使用してください。

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(GE0/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。

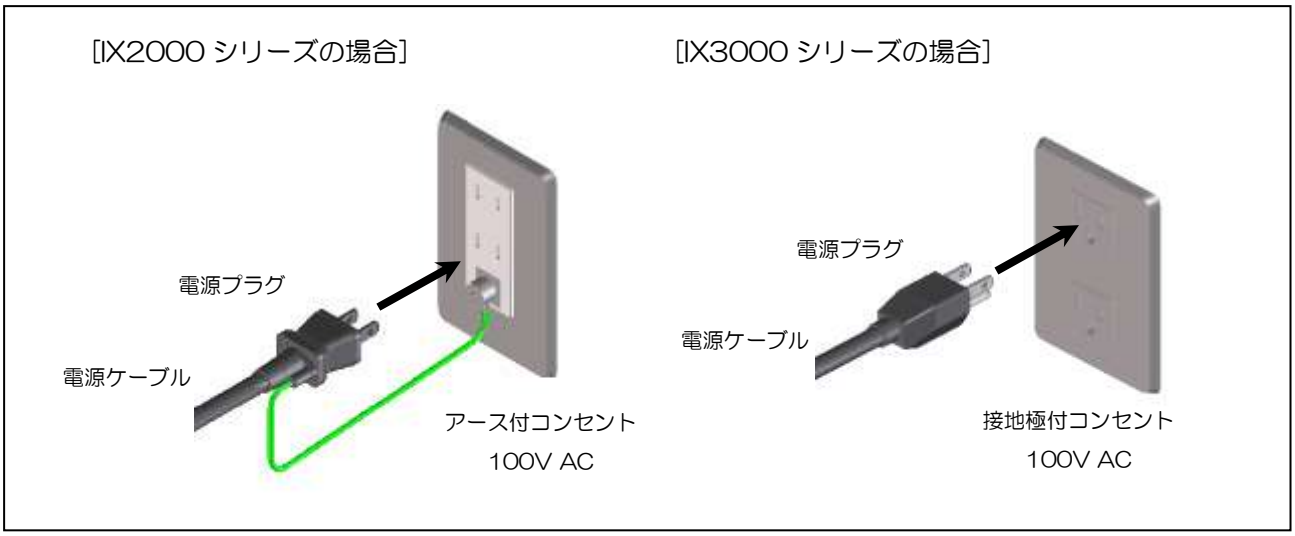
注意 ケーブルは、カテゴリ 5 以上のストレート結線またはクロス結線の UTP または STP ケーブルを使用してください。



(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。

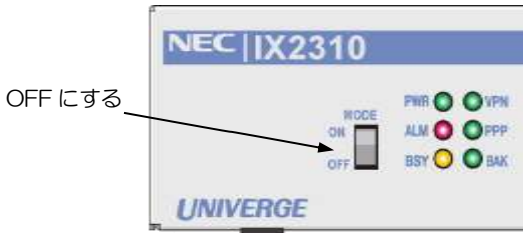


1.2.2 MODE スイッチを設定する(IX2310)

(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。

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



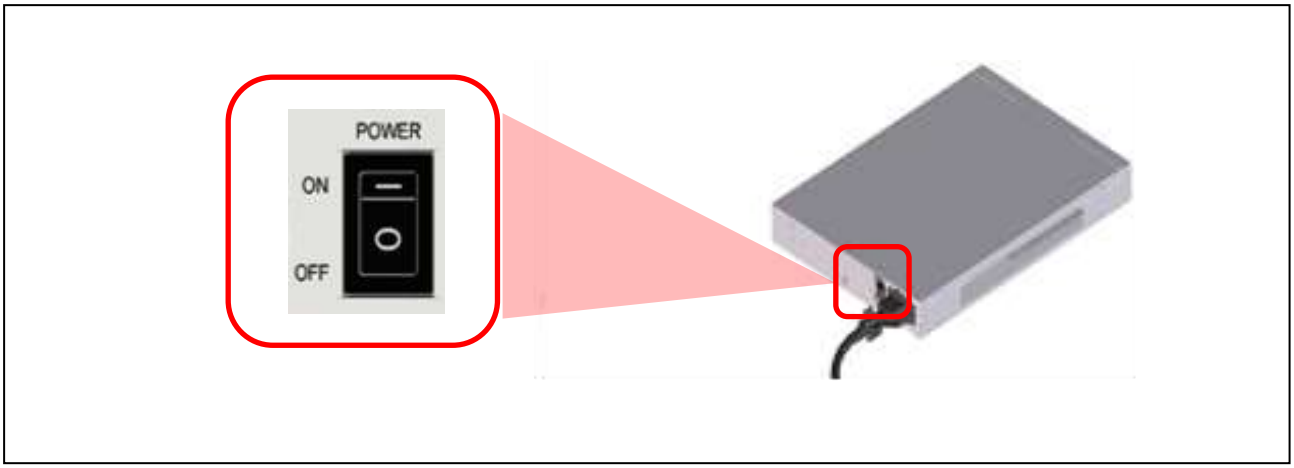
1.2.3 本装置の電源を入れる

(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。

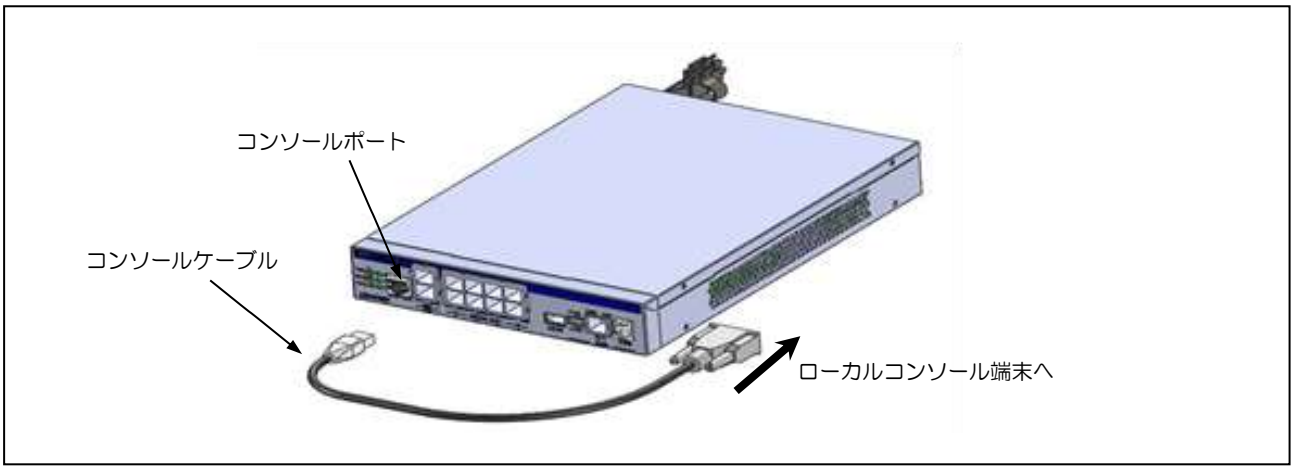
メモ IX3000 シリーズの場合、電源スイッチの[|]を押して ON にします。

メモ 起動には 30 秒～120 秒程度かかります。



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。



メモ 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

(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

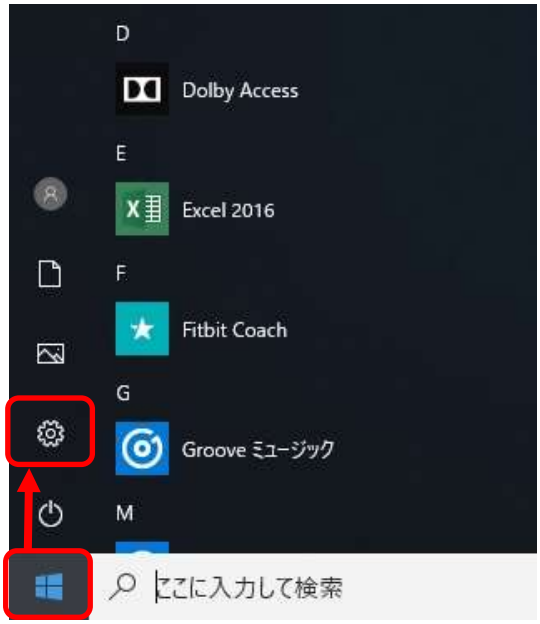
【IX3315 の場合】

```
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
```

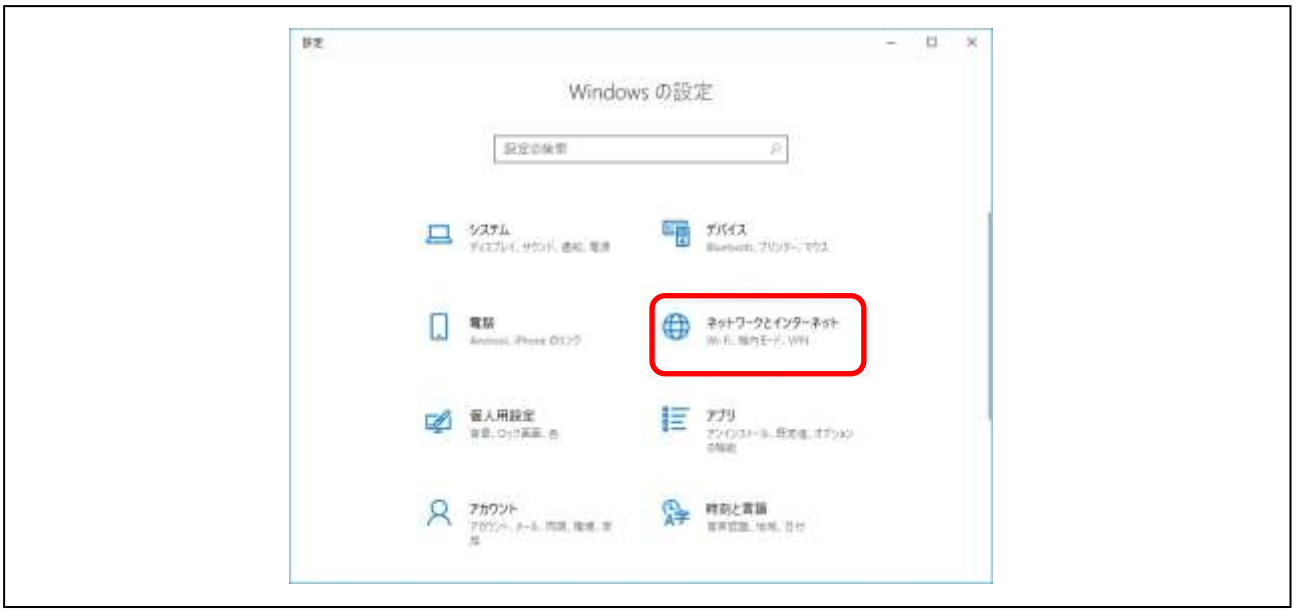
メモ ソフトウェアバージョンによって、上記で入力したコマンドが自動的に変換される場合があります。

1.2.5 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。

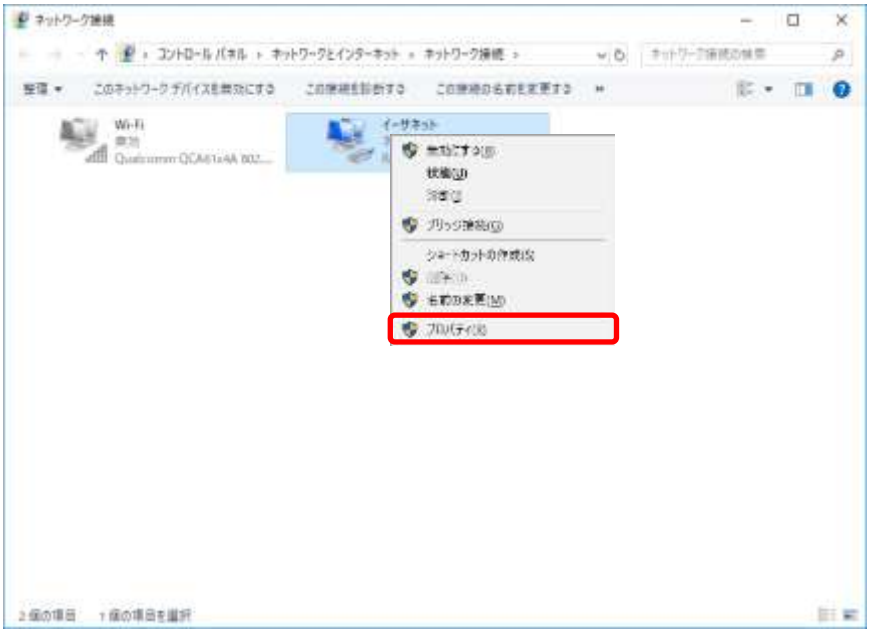


⑵ [ネットワークとインターネット]をクリックします。



⑶ [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。

(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。

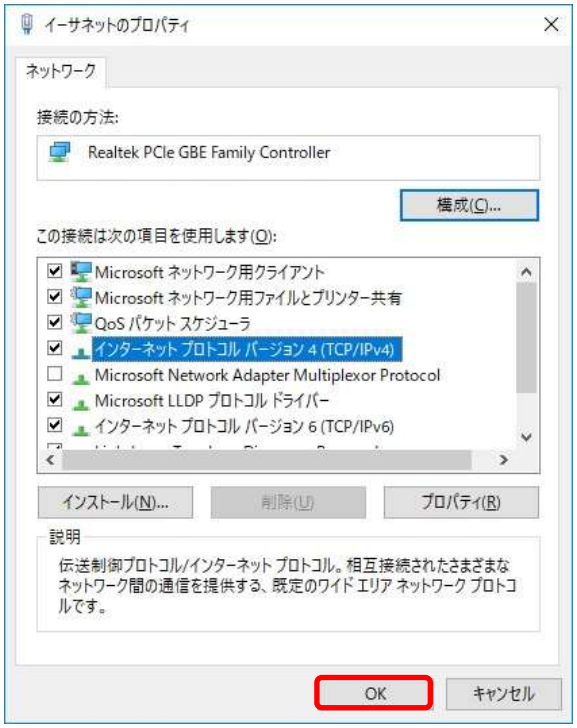
(7) [全般]タブをクリックします。

(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。

(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

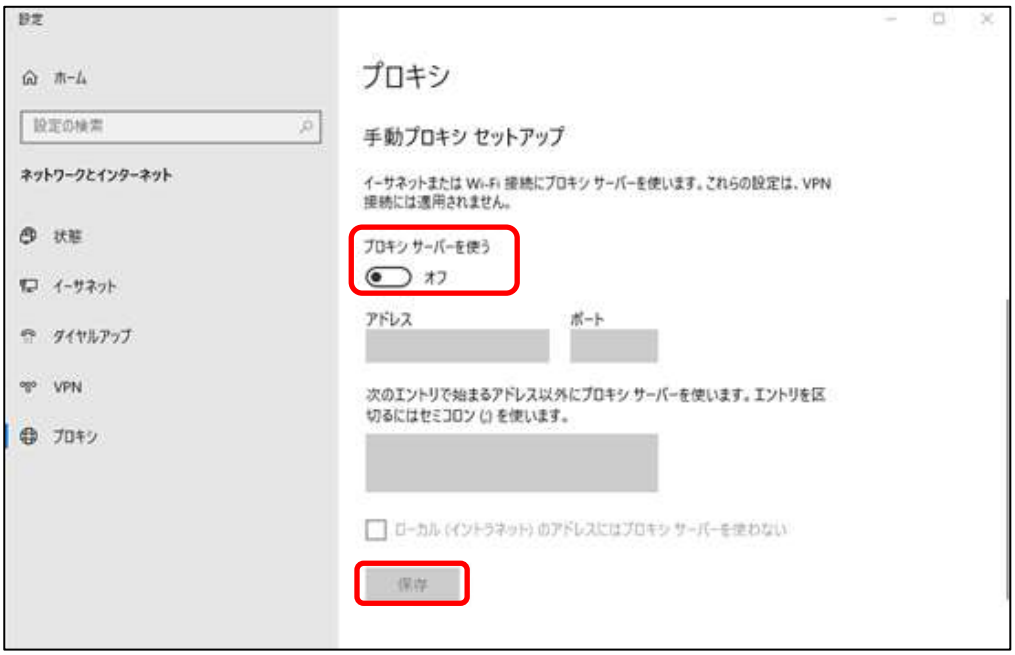
メモ Microsoft Edge のバージョンにより、画面の表示内容が異なる場合があります。

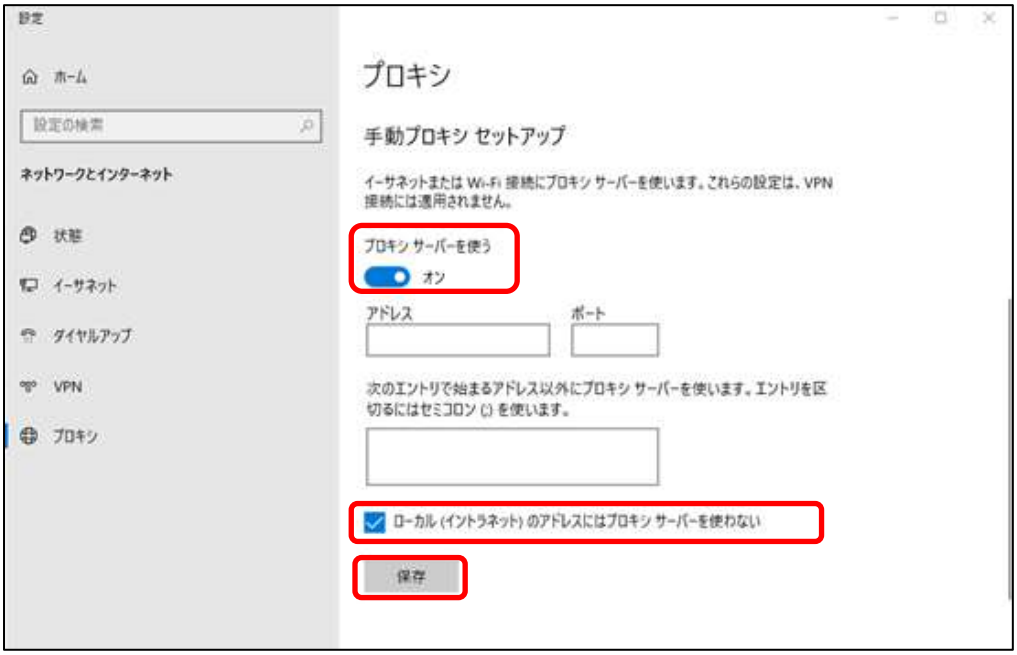
(1) パソコンで、Web ブラウザ(Microsoft Edge)を起動します。

(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。

(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。



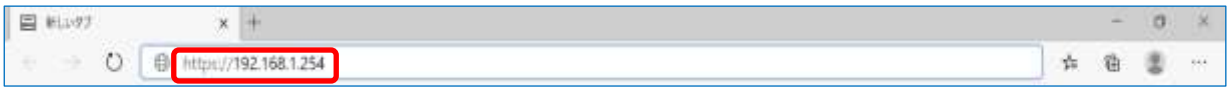


注意 本装置は Cookie を使用しています。「すべての Cookie をブロック」または「高」にすると、本装置で使用する Cookie がブロックされ、設定を行うことができません。

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。



メモ 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。

(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。

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

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. 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

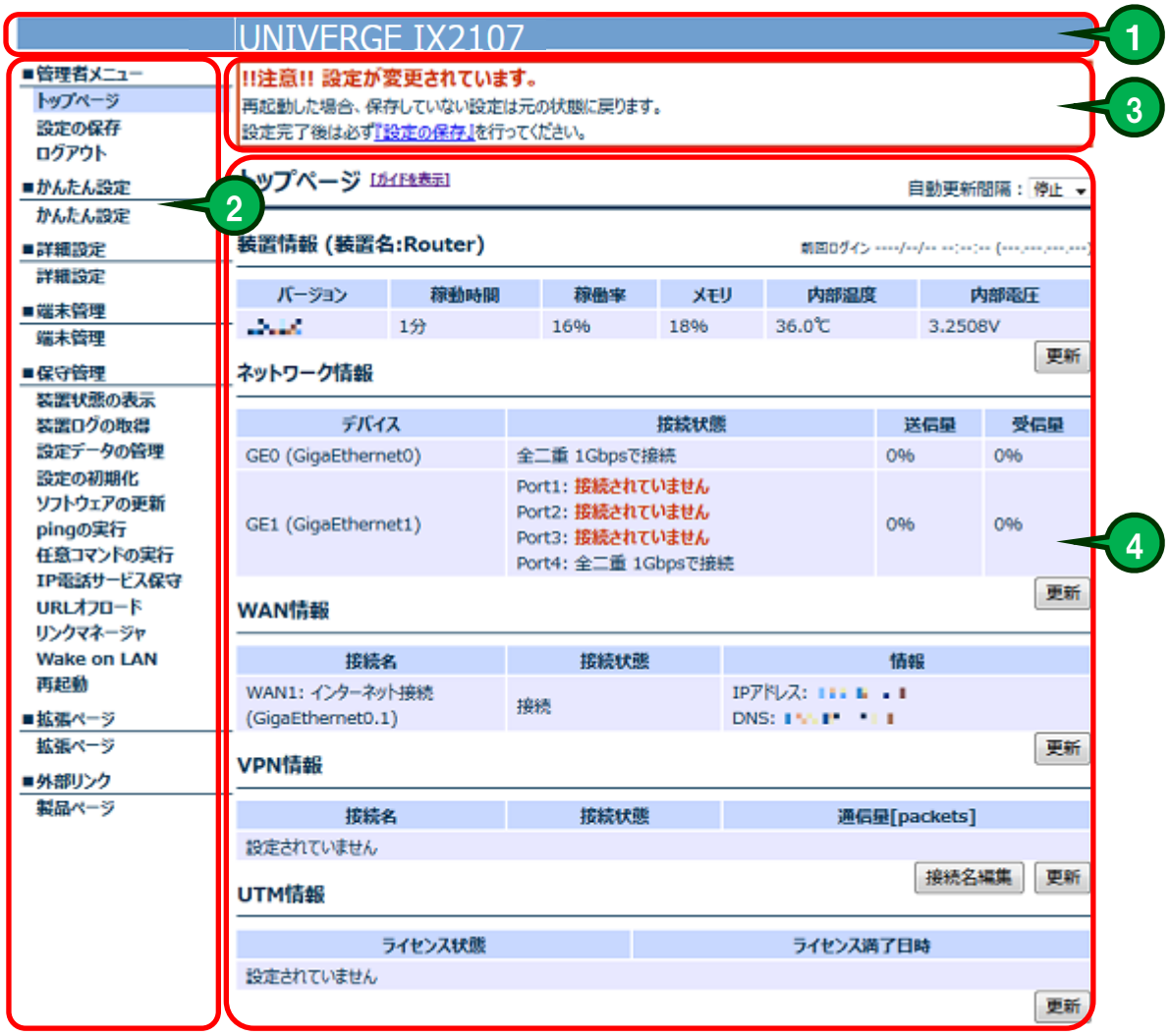
③ メッセージエリア（ログイン時のみ表示）

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。



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。

メモ　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。

2. メニュー

2.2 ログインする

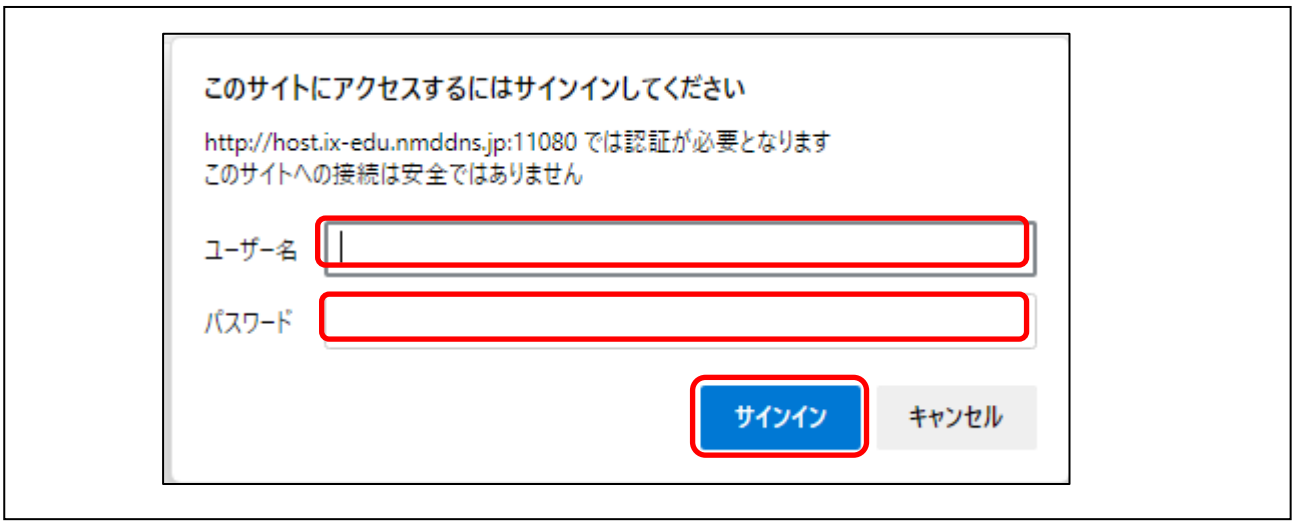
(1) トップページのメニューエリアから[ログイン]、または、設定・表示エリアから設定したい項目のリンクをクリックします。

(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。

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]をクリックしてください。

メモ 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。

メモ 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。

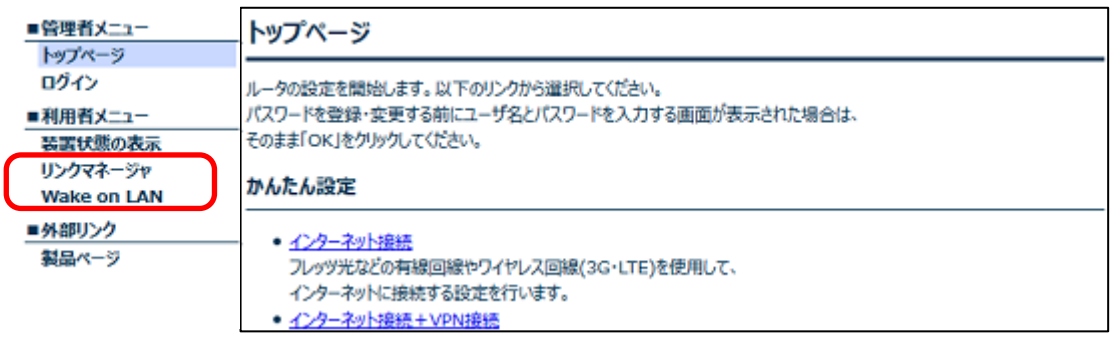


(3) パスワードの設定画面が表示されますので、各項目を設定し、[反映]ボタンをクリックします。

2. メニュー

番号	項目	内容
①	ユーザ名	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。 • 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。 • 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。 メモ • 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。 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) 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	利用者ユーザ	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。 • 「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。 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。 メモ • 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	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。 メモ • 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

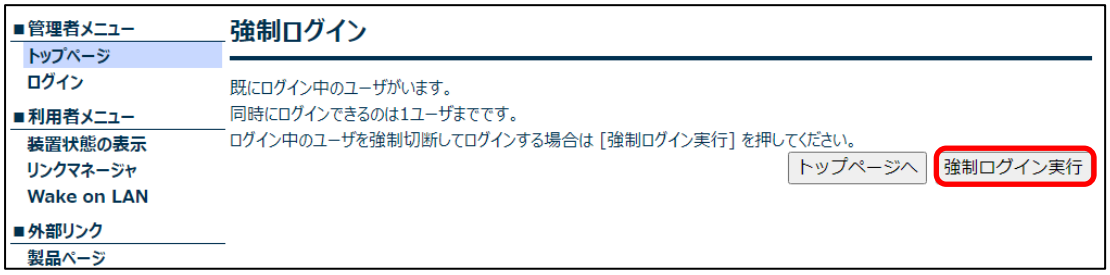


(4)　ログイン後のトップページが表示されることを確認します。

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。

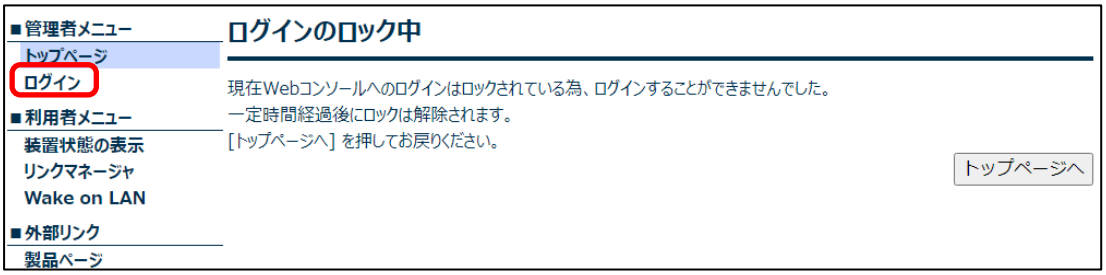
すでに本装置にログインしているユーザがいるときは、【強制ログイン】画面が表示されます。ログイン中のユーザを強制切断してログインする場合は、[強制ログイン実行]を押してください。



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。

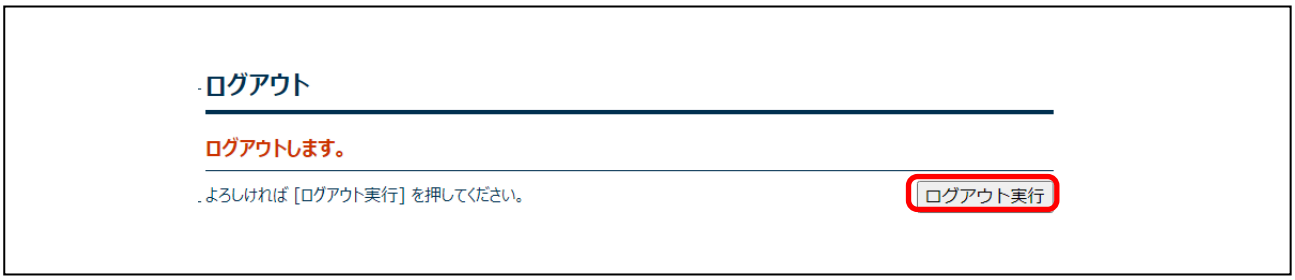
60 秒以上経過後、再度ログインを実行してください。



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。

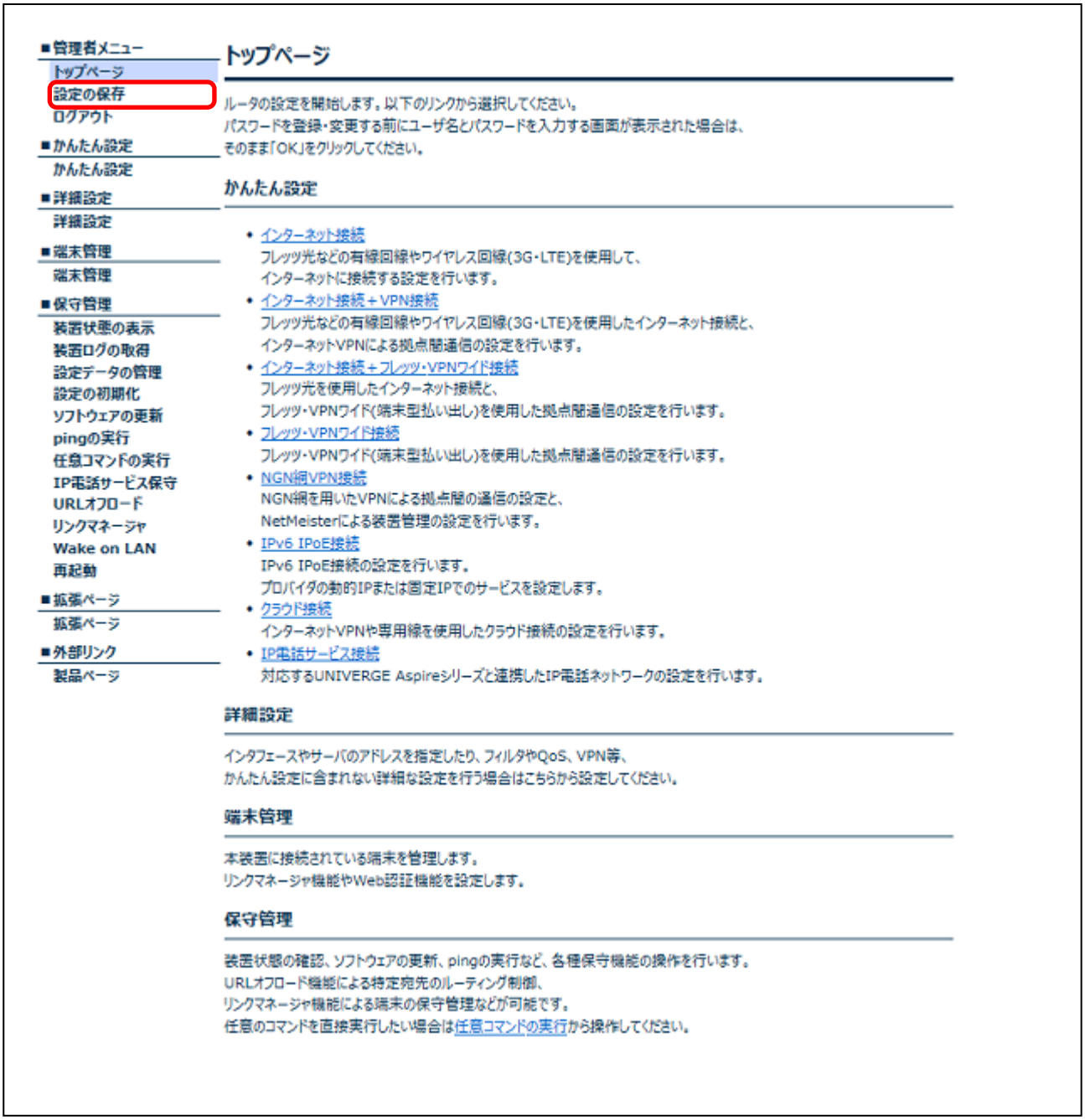
⑵　[ログアウト実行]ボタンをクリックします。



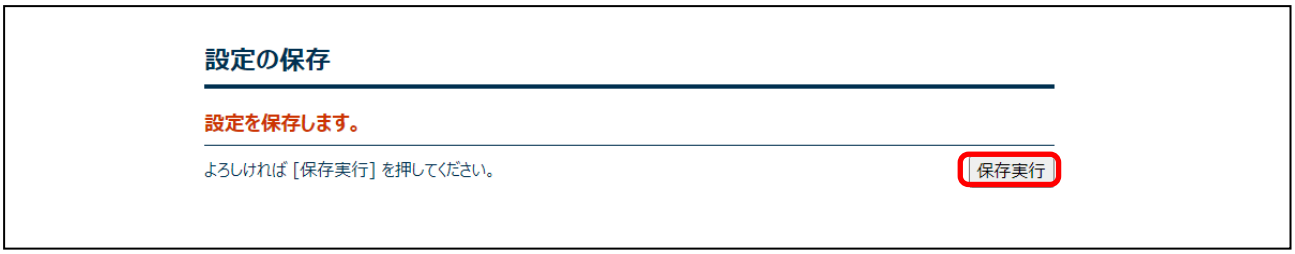
⑶　ログアウト後のトップページが表示されることを確認します。

2.4 設定の保存

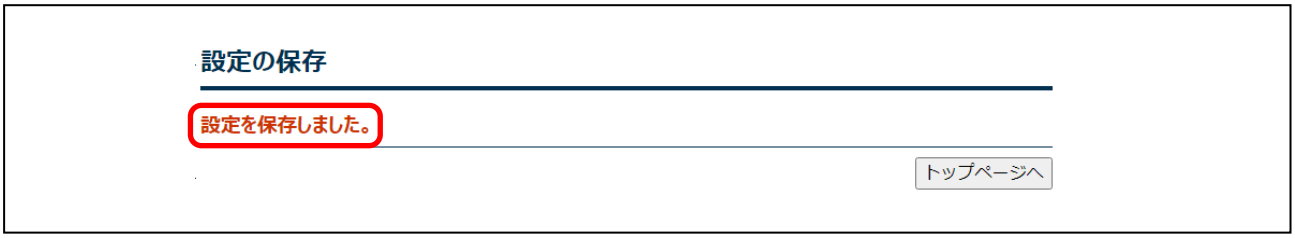
(1) ログイン後のメニューエリアから[設定の保存]をクリックします。



(2) [保存実行]ボタンをクリックします。



(3) 「設定を保存しました。」のメッセージを確認します。



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。

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。

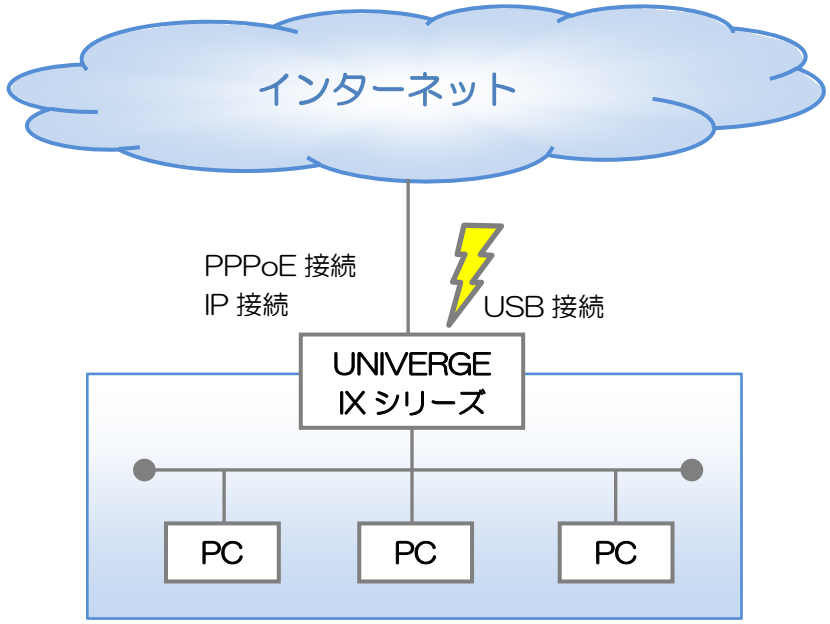
メモ IX2107/IX2235/IX2310 の場合、ゼロタッチプロビジョニングモードが ON（装置前面の MODE スイッチが ON）に設定されていると、かんたん設定を利用できません。ゼロタッチプロビジョニング機能は利用せず、かんたん設定を利用する場合は、MODE スイッチを OFF に設定してください。MODE スイッチの設定を変更したときは、装置を再起動してください。
工場出荷時は、MODE スイッチは ON に設定されています。

3. かんたん設定

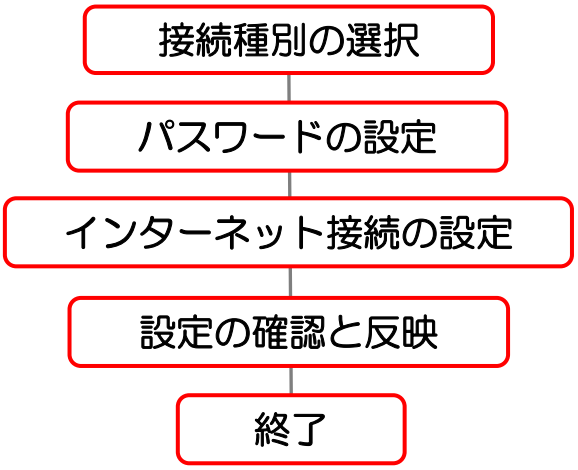
3.1 インターネット接続

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。

(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。

(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。 ・ 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。

(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。

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。

PPPoE 接続の場合(フレッツ光回線利用の場合)

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。

<table>
<tr><td>⑥</td><td>セキュリティ強度</td><td>通信セキュリティの強度を設定します。
・ 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。
「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>
<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>
メモセキュリティ強度は、以下を参照してください。
<table>
<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></td></tr>
<tr><td>⑦</td><td>LAN 側 IP アドレス</td><td>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。</td></tr>
</table>

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		○ PPPoE接続（フレッツ光回線利用の場合） ◉ 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		◉ 自動取得 ○ 手動設定
DNSアドレス		◉ 自動取得 ○ 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	◉ 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。 ○ 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

戻る 次へ

<table>
<tr><th>番号</th><th>項目</th><th>内容</th></tr>
<tr><td>①</td><td>接続形態</td><td>「IP 接続（ケーブルテレビ回線利用の場合）」を選択します。</td></tr>
<tr><td>②</td><td>WAN 側 IP アドレス</td><td>IP 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。</td></tr>
<tr><td>③</td><td>DNS アドレス</td><td>IP 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。</td></tr>
<tr><td>④</td><td>セキュリティ強度</td><td>通信セキュリティの強度を設定します。
• 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。
「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>
<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>
メモセキュリティ強度は、以下を参照してください。
<table>
<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></td></tr>
<tr><td>⑤</td><td>LAN 側 IP アドレス</td><td>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。</td></tr>
</table>

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

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。

<table>
<tr><td>⑧</td><td>セキュリティ強度</td><td>通信セキュリティの強度を設定します。
・ 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。
「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>
<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>
メモセキュリティ強度は、以下を参照してください。
<table>
<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></td></tr>
<tr><td>⑨</td><td>LAN 側 IP アドレス</td><td>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。</td></tr>
</table>

(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。

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。

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。

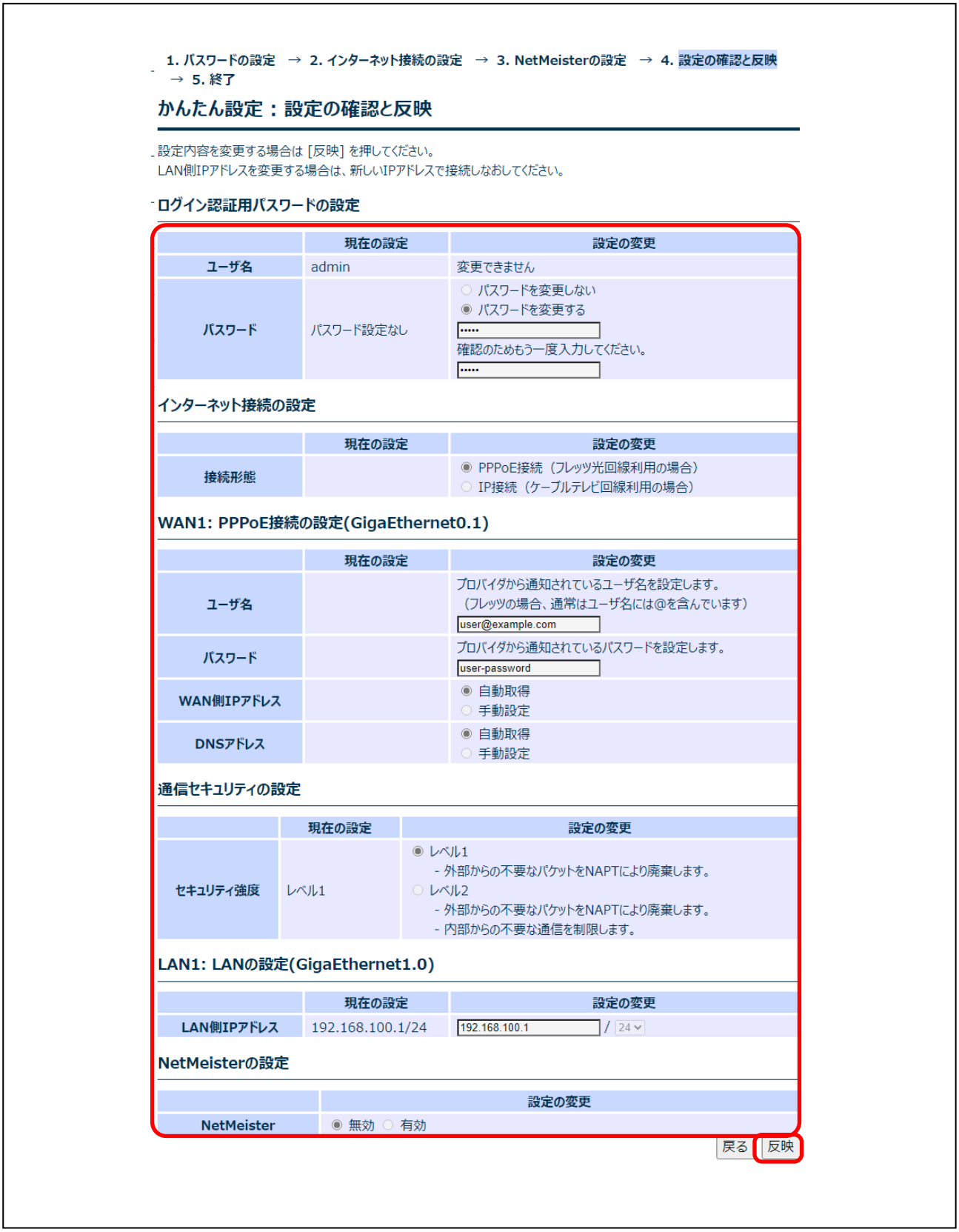
「有効」を選択するとアカウント名等の設定項目が表示されますので、各項目を設定し、[設定の確認]ボタンをクリックします。

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。

⑹　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	○ パスワードを変更しない ◉ 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		◉ PPPoE接続（フレッツ光回線利用の場合） ○ 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		◉ 自動取得 ○ 手動設定
DNSアドレス		◉ 自動取得 ○ 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	◉ 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。 ○ 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	◉ 無効 ○ 有効

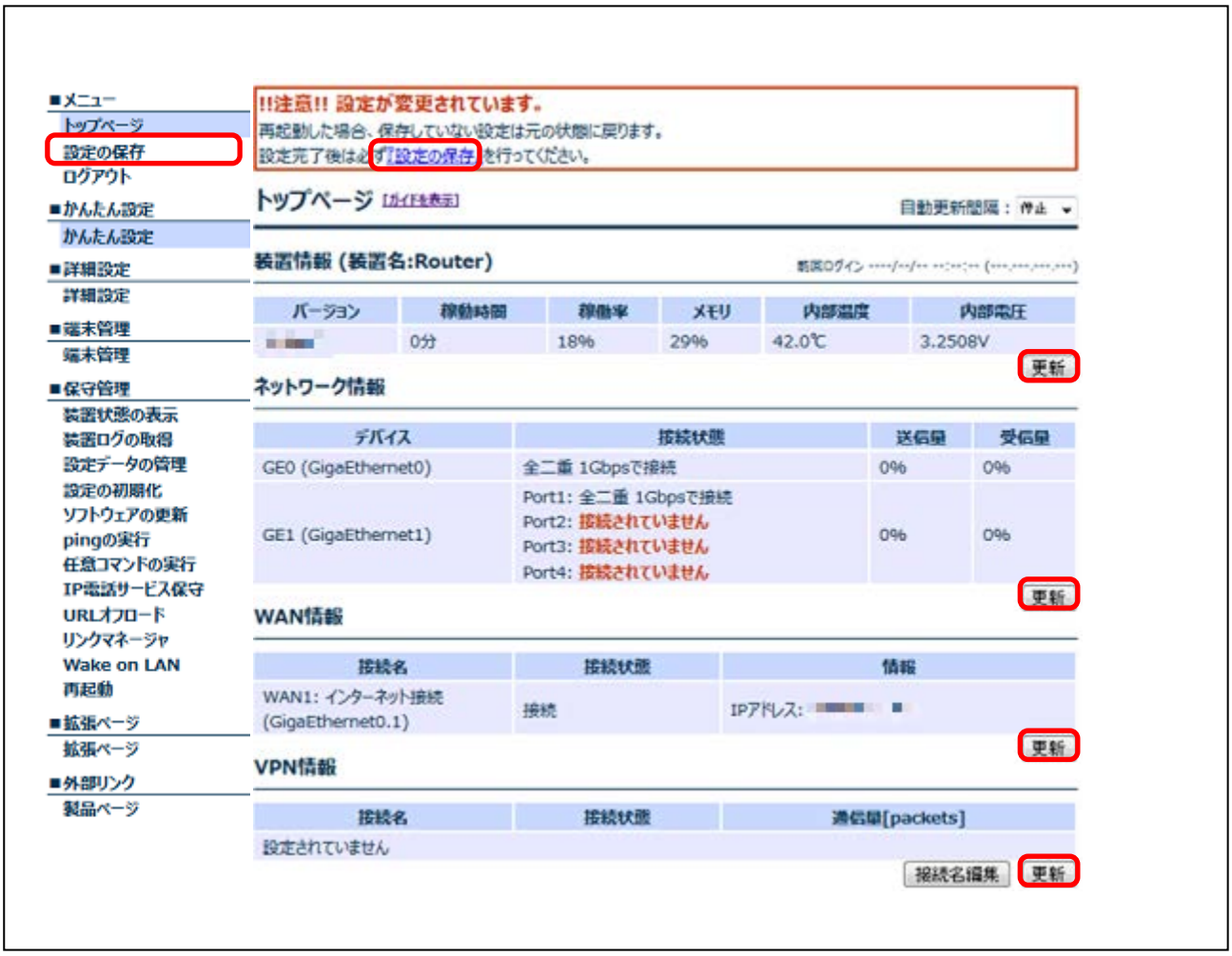
戻る　反映

(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。

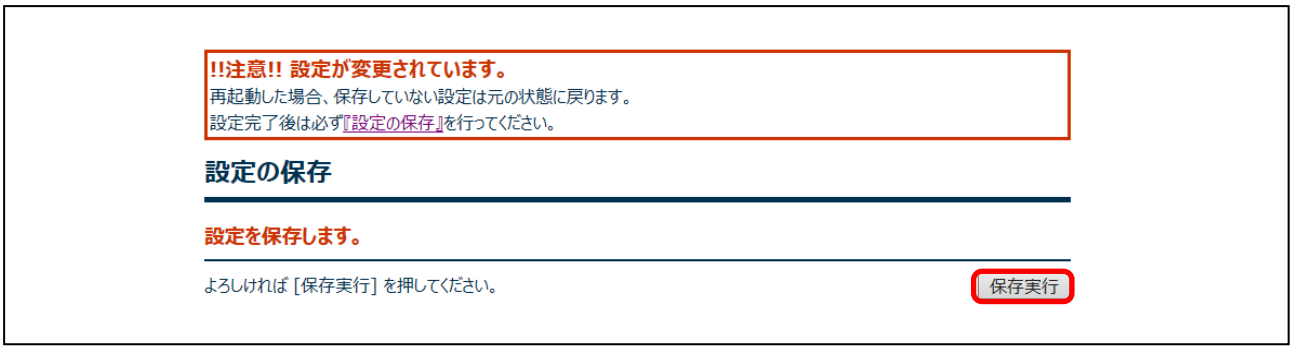
⑻　トップページで WAN 情報の接続状態を確認します。

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。

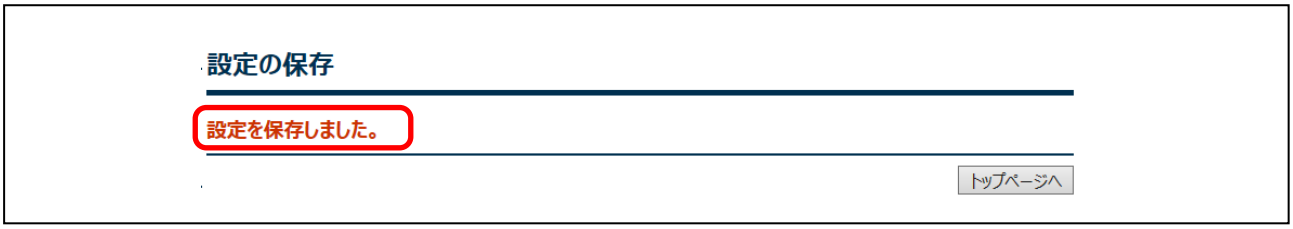
⑼　メニューエリア、または、メッセージエリアから[設定の保存]をクリックします。



(10) [保存実行]ボタンをクリックします。



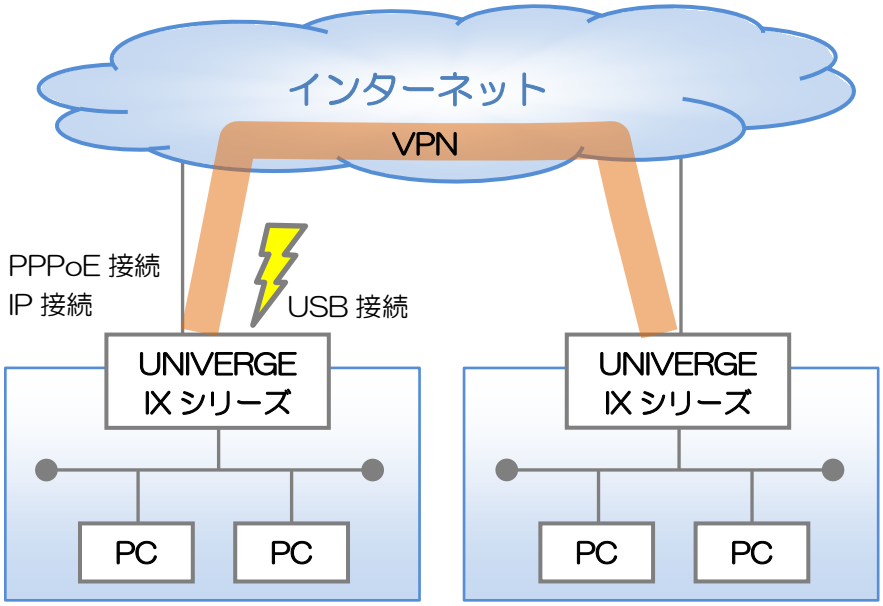
(11)「設定を保存しました。」のメッセージを確認します。



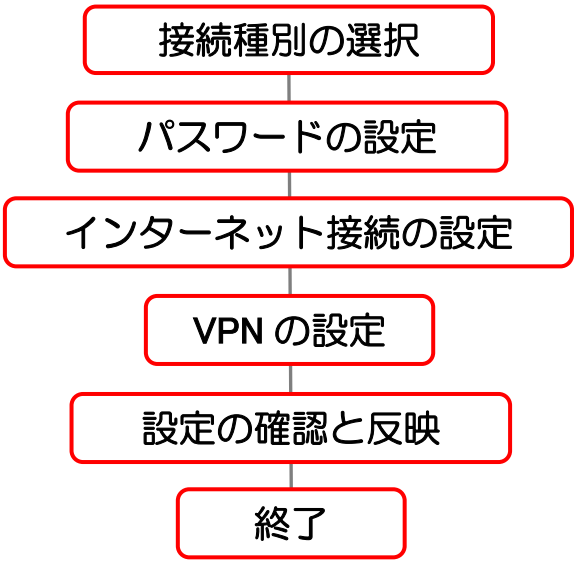
3.2 インターネット接続＋VPN 接続

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。

(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。

(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。 ・ 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。

(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。

PPPoE 接続の場合(フレッツ光回線利用の場合)

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。

<table>
<tr>
<td>⑥</td>
<td>セキュリティ強度</td>
<td>
通信セキュリティの強度を設定します。
・ 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。
「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>
<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>
メモセキュリティ強度は、以下を参照してください。
<table>
<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>
</td>
</tr>
</table>

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)

<table>
<tr><th>番号</th><th>項目</th><th>内容</th></tr>
<tr><td>①</td><td>接続形態</td><td>「IP 接続（ケーブルテレビ回線利用の場合）」を選択します。</td></tr>
<tr><td>②</td><td>WAN 側 IP アドレス</td><td>IP 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。
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。</td></tr>
<tr><td>③</td><td>DNS アドレス</td><td>IP 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。</td></tr>
<tr><td>④</td><td>セキュリティ強度</td><td>通信セキュリティの強度を設定します。
• 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。
「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>
<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>
メモセキュリティ強度は、以下を参照してください。
<table>
<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></td></tr>
</table>

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

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。

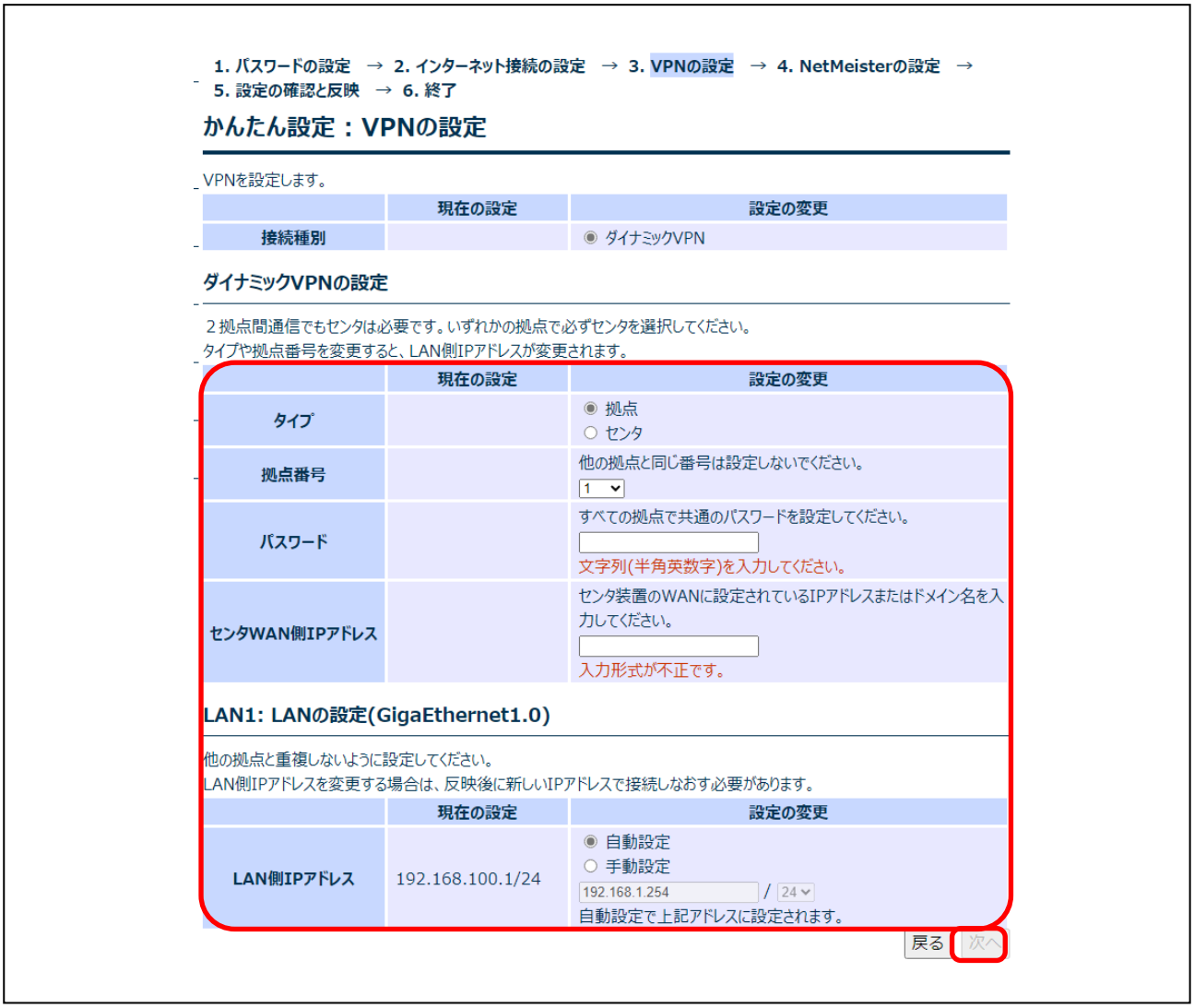
<table>
<tr>
<td>⑧</td>
<td>セキュリティ強度</td>
<td>
通信セキュリティの強度を設定します。
・ 外部からの不要なパケットを NAPT により廃棄する場合は「レベル 1」を選択します。
・ 外部からの不要なパケットを NAPT により廃棄し、さらに内部からの不要な通信を制限する場合は、「レベル 2」を選択します。
「レベル 2」を選択したときは、送信時に以下に該当する通信を廃棄します。
<table>
<tr><td rowspan="4">宛先 IP アドレス</td><td>0.0.0.0/8</td></tr>
<tr><td>127.0.0.0/8</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>
メモセキュリティ強度は、以下を参照してください。
<table>
<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>
</td>
</tr>
</table>

⑸ [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 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。

メモ 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



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

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。

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。

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。

(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。

⑻ 「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. 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	○ パスワードを変更しない ◉ 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		◉ PPPoE接続（フレッツ光回線利用の場合） ○ 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		◉ 自動取得 ○ 手動設定
DNSアドレス		◉ 自動取得 ○ 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	◉ 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。 ○ 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		◉ 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		◉ 拠点 ○ 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	[redacted]	◉ 自動設定 ○ 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

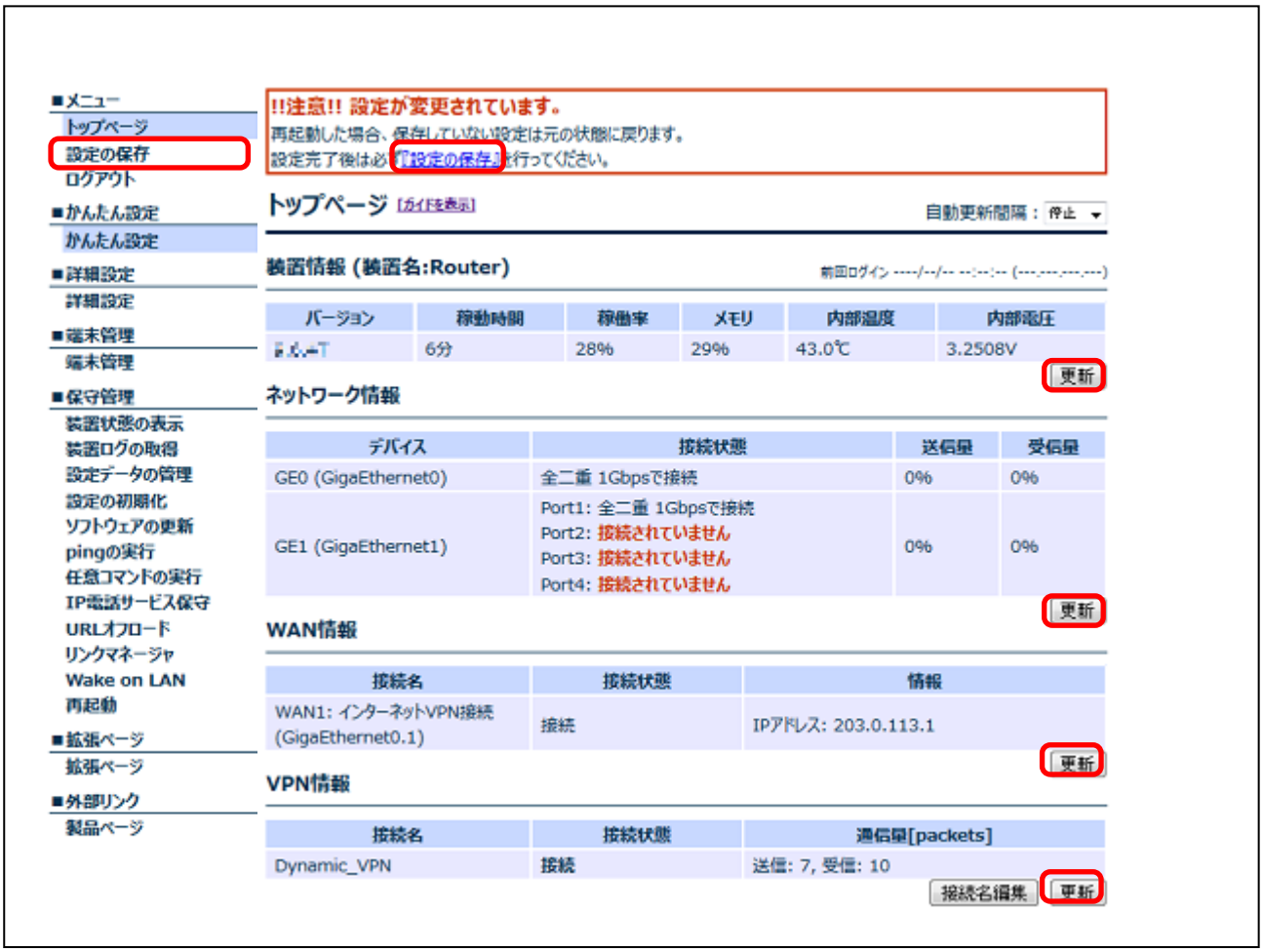
	設定の変更
NetMeister	◉ 無効 ○ 有効

トップページへ

(9) 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。

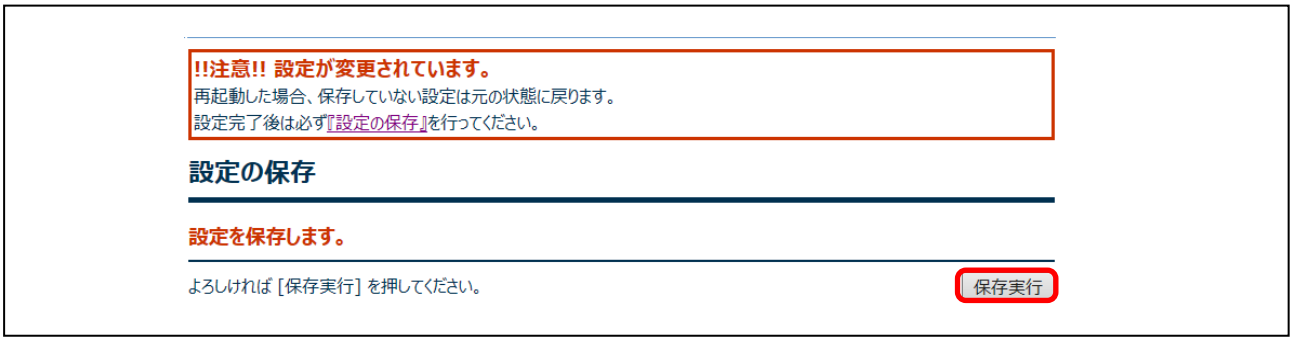
(10) メニューエリア、または、メッセージエリアから[設定の保存]をクリックします。



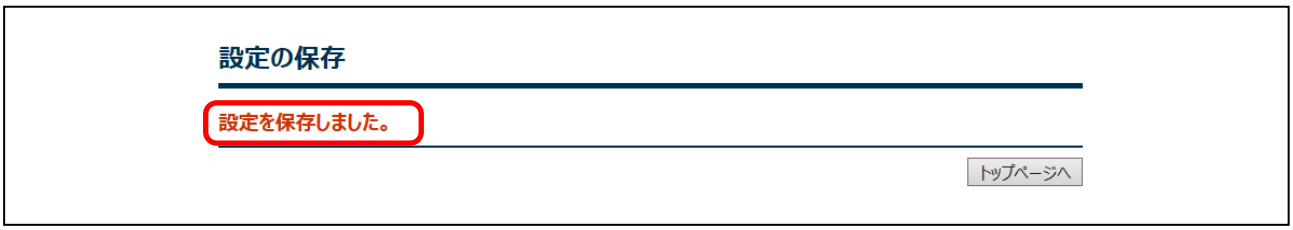
(11) VPN 情報は、接続名にマウスカーソルを近づけることで、詳細情報を確認することができます。また、接続名をわかりやすいように変更することができます。

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。



(13) 「設定を保存しました。」のメッセージを確認します。

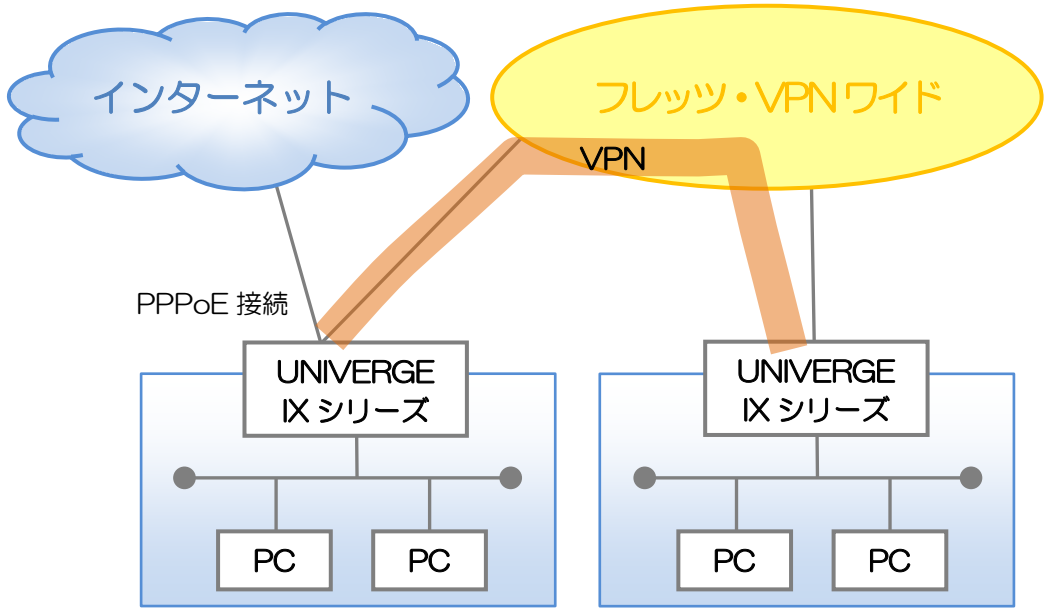


メモ　確実に VPN 接続するため、設定の保存後、再起動実行を推奨します。

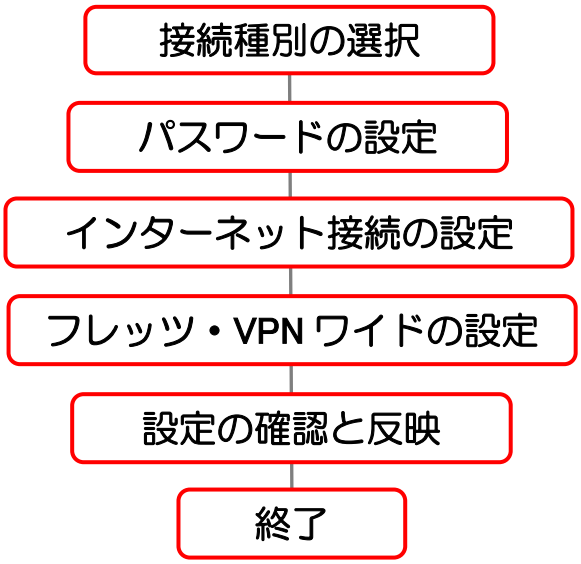
3.3 インターネット接続＋フレッツ・VPN ワイド接続

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。

(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。

(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。

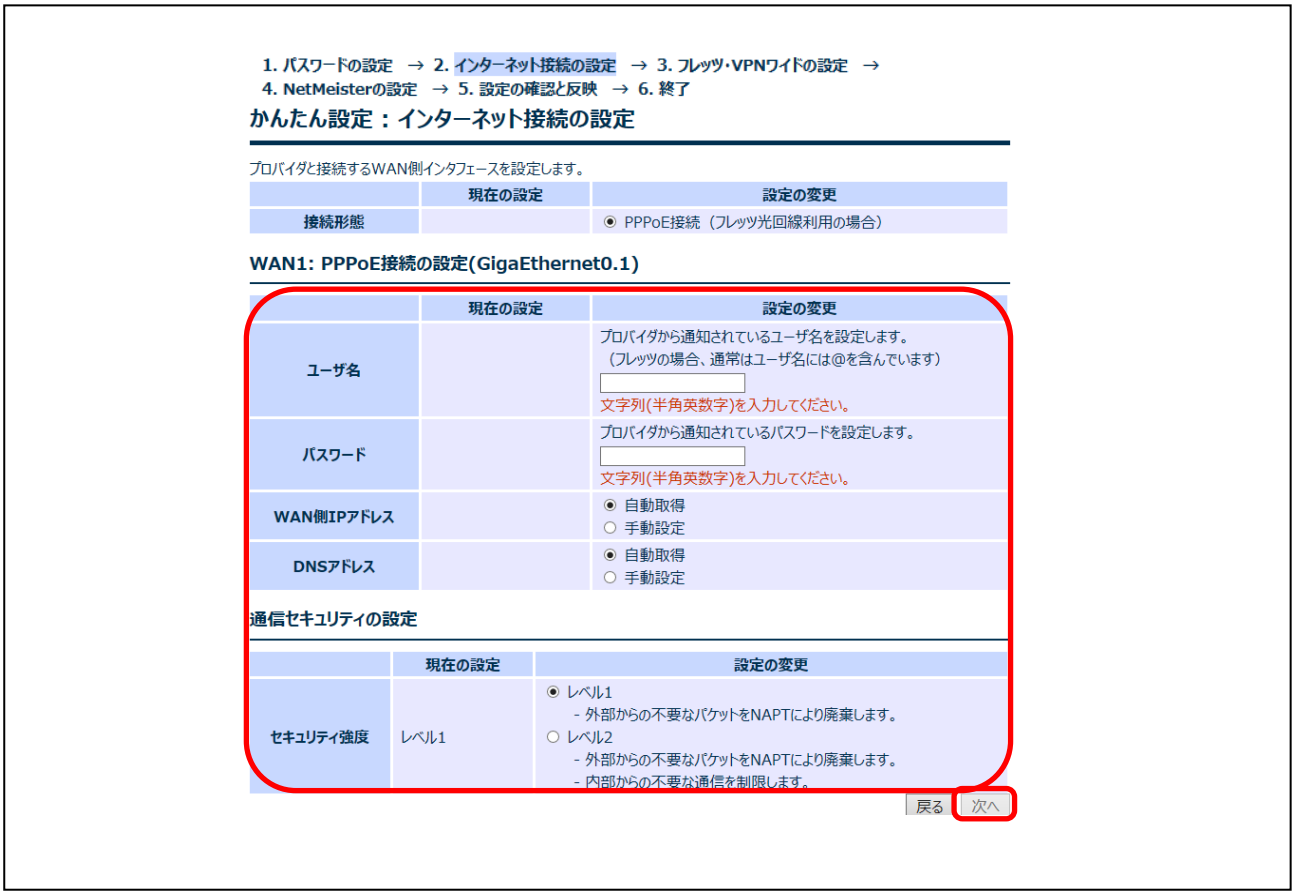
メモ　管理者パスワードを変更する必要が無い場合は、そのまま[次へ]ボタンをクリックします。

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。 ・ 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。

(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。



<table>
<tr><th>番号</th><th>項目</th><th>内容</th></tr>
<tr><td>①</td><td>ユーザ名</td><td>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。</td></tr>
<tr><td>②</td><td>パスワード</td><td>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。</td></tr>
<tr><td>③</td><td>WAN 側 IP アドレス</td><td>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。</td></tr>
<tr><td>④</td><td>DNS アドレス</td><td>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。</td></tr>
<tr><td>⑤</td><td>セキュリティ強度</td><td>通信セキュリティの強度を設定します。
・ 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。
「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>
<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>
メモセキュリティ強度は、以下を参照してください。
<table>
<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></td></tr>
</table>

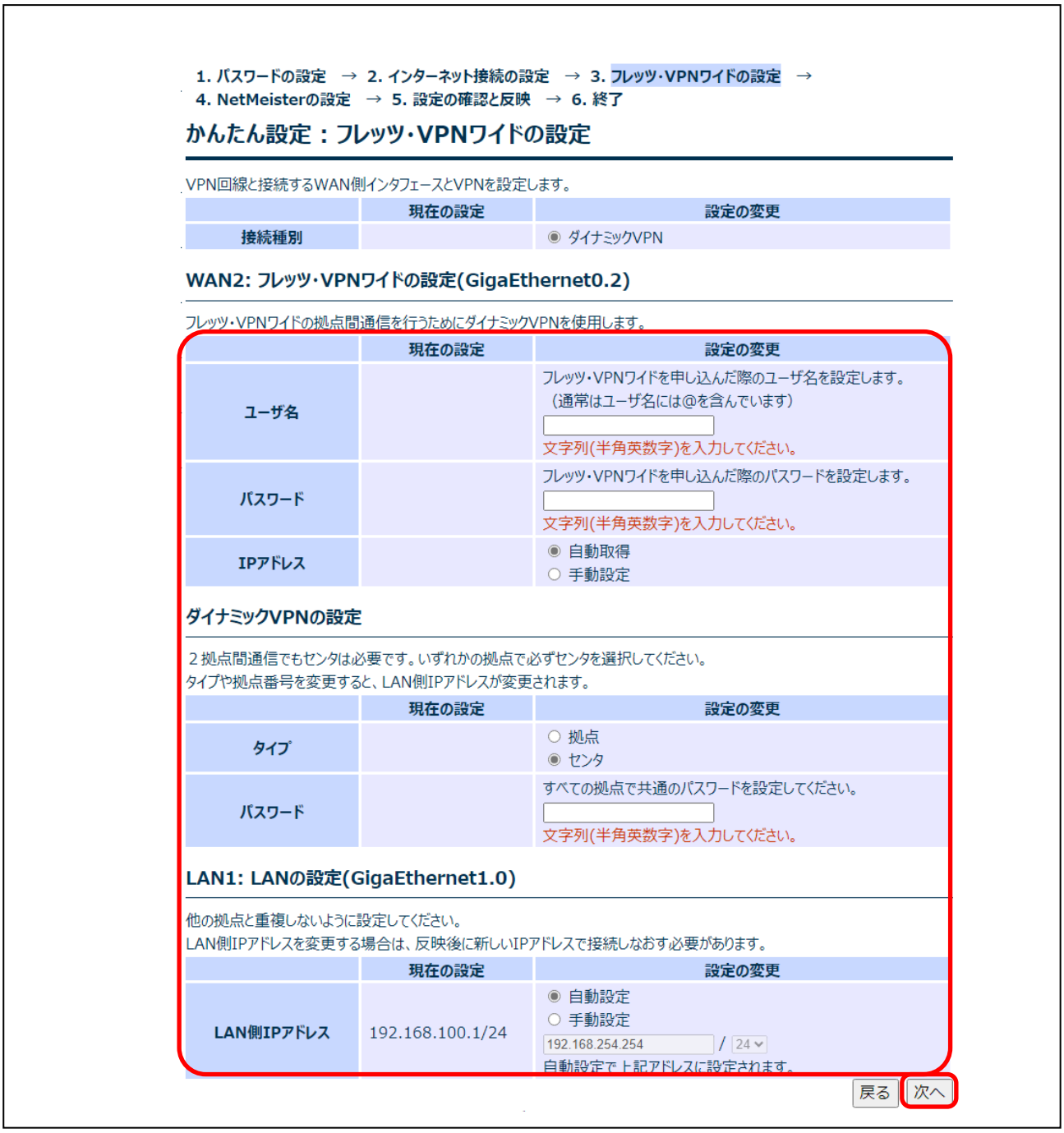
⑸ [フレッツ・VPN ワイドの設定]の各項目を設定し、[次へ]ボタンをクリックします。

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

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。

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		◉ 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） [ ] 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。 [ ] 文字列(半角英数字)を入力してください。
IPアドレス		◉ 自動取得 ○ 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		○ 拠点 ◉ 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。 [ ] 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。

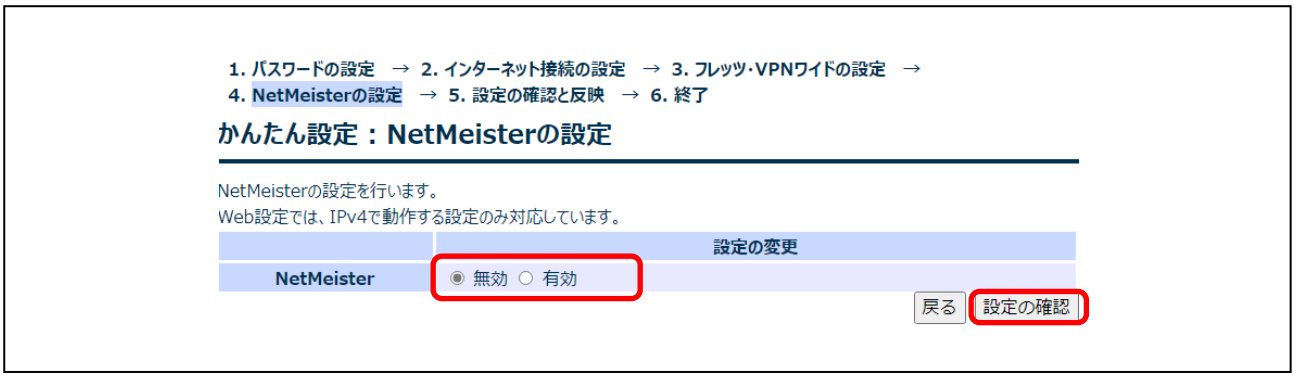
	現在の設定	設定の変更
LAN側IPアドレス	192.168.100.1/24	◉ 自動設定 ○ 手動設定 192.168.254.254 / 24 自動設定で上記アドレスに設定されます。

戻る　次へ

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。



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。

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。

(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	○ パスワードを変更しない ◉ 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		◉ 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		◉ 自動取得 ○ 手動設定
DNSアドレス		◉ 自動取得 ○ 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	◉ 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。 ○ 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		◉ 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		◉ 自動取得 ○ 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		◉ 拠点 ○ 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	[redacted]	◉ 自動設定 ○ 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。

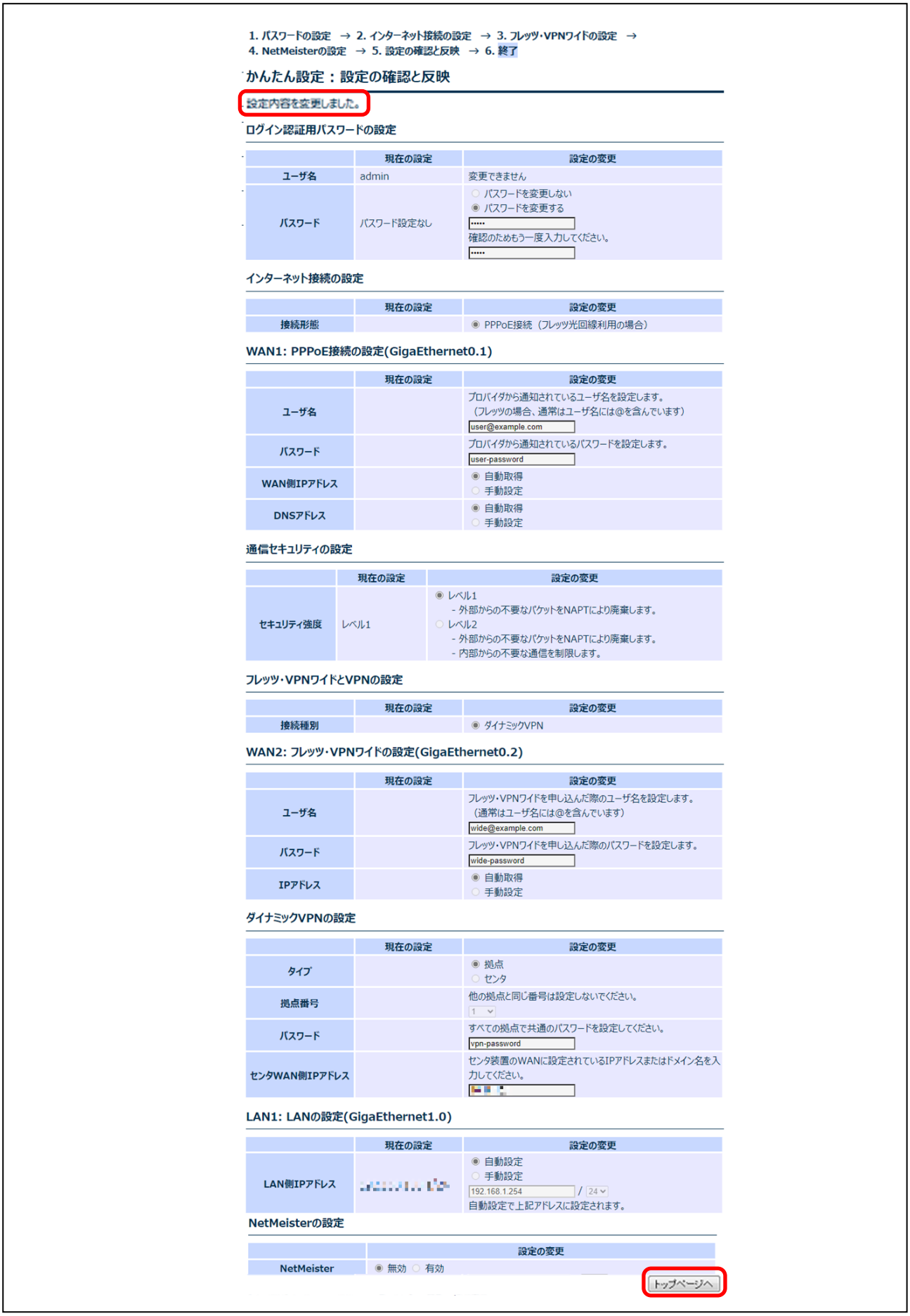
NetMeisterの設定

	設定の変更
NetMeister	◉ 無効 ○ 有効

戻る 反映

⑻ 「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. 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	○ パスワードを変更しない ◉ 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		◉ 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		◉ 自動取得 ○ 手動設定
DNSアドレス		◉ 自動取得 ○ 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	◉ 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。 ○ 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		◉ 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		◉ 自動取得 ○ 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		◉ 拠点 ○ 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	[redacted]	◉ 自動設定 ○ 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	◉ 無効 ○ 有効

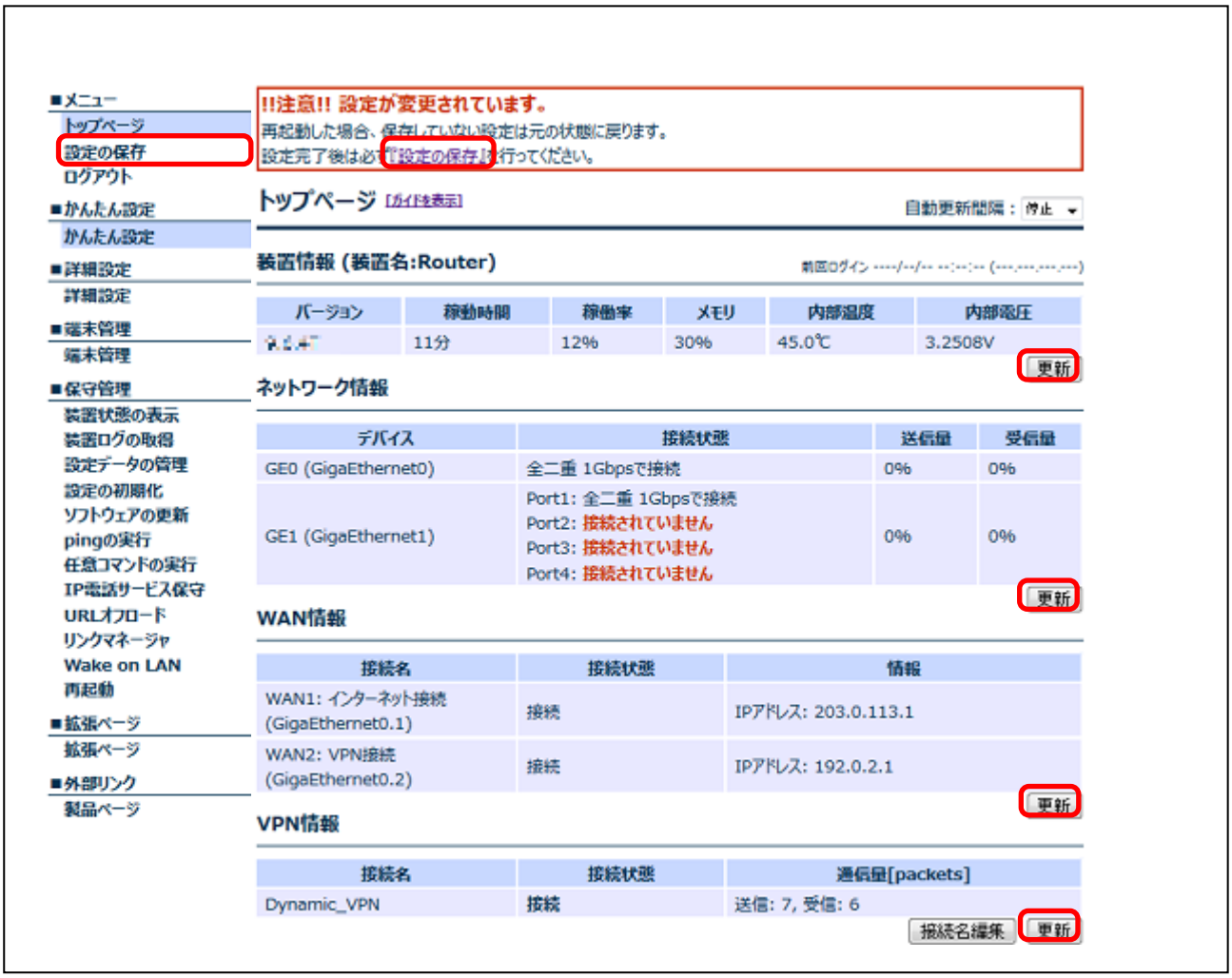
トップページへ

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。

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。

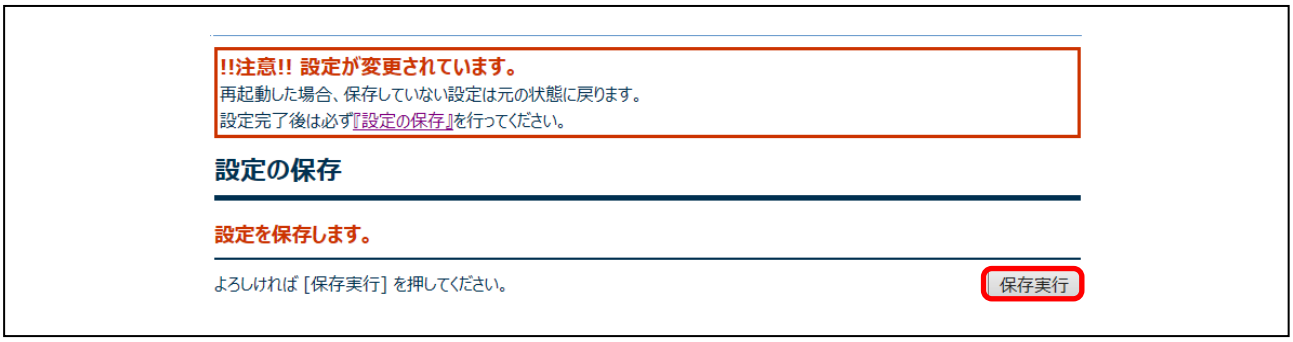
(10) メニューエリア、または、メッセージエリアから[設定の保存]をクリックします。



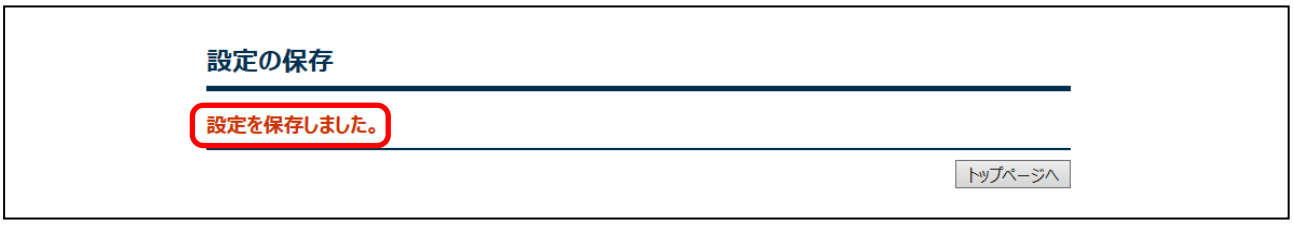
(11) VPN 情報は、接続名にマウスカーソルを近づけることで、詳細情報を確認することができます。また、接続名をわかりやすいように変更することができます。

	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。



(13) 「設定を保存しました。」のメッセージを確認します。

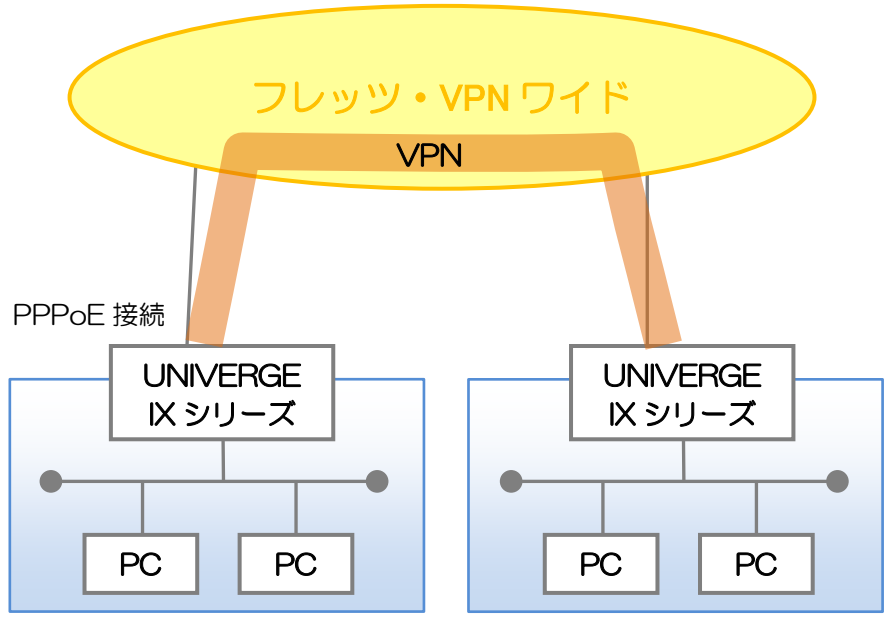


メモ　確実に VPN 接続するため、設定の保存後、再起動実行を推奨します。

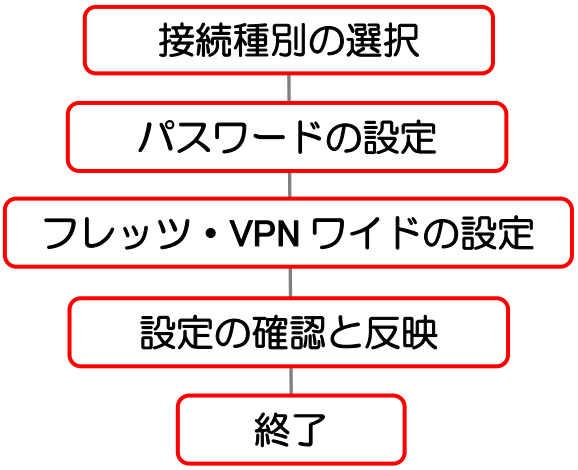
3.4 フレッツ・VPN ワイド接続

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。

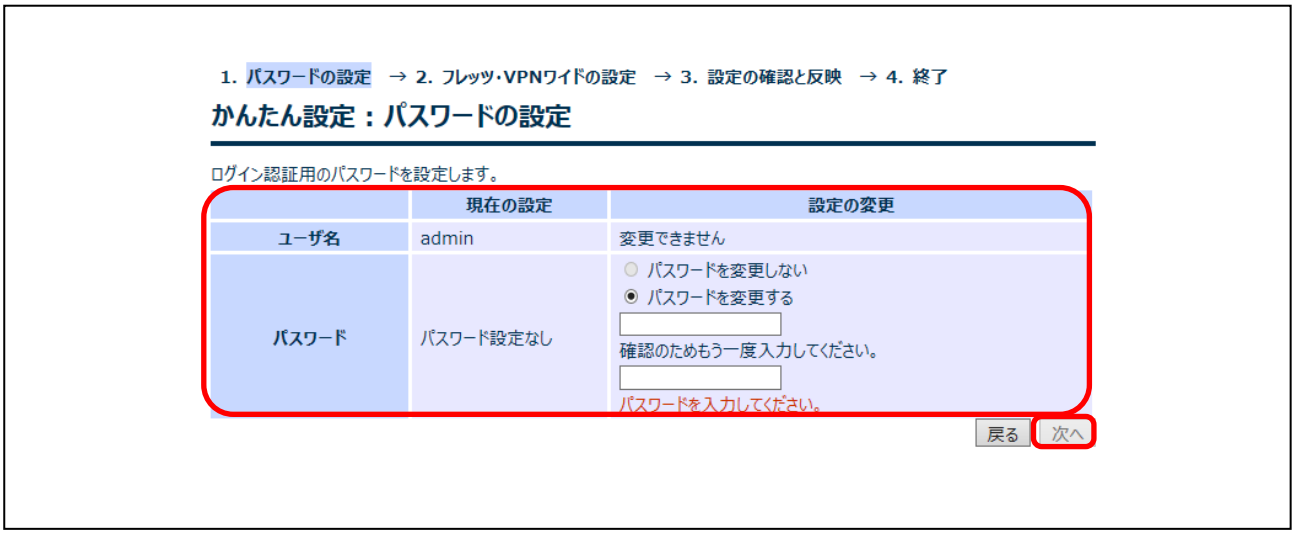
(2) 接続種別の選択で「フレッツ・VPN ワイド接続」にチェックを入れ、[次へ] ボタンをクリックします。

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。

(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。 ・ 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 1～249 文字で入力します。 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) [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。

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。

拠点の場合

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		◉ 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） 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。 文字列(半角英数字)を入力してください。
IPアドレス		◉ 自動取得 ○ 手動設定
DNSアドレス		◉ 自動設定 ○ 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		○ 拠点 ◉ 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。 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	◉ 自動設定 ○ 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

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(*)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. 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
パスワードを変更しない
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
接続種別
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
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
自動取得
手動設定
DNSアドレス
自動設定
手動設定
ダイナミックVPNの設定
タイプ
拠点
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。
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)
LAN側IPアドレス
自動設定
手動設定
192.168.1.254
/ 24
*
戻る
反映

⑹　「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。

(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。

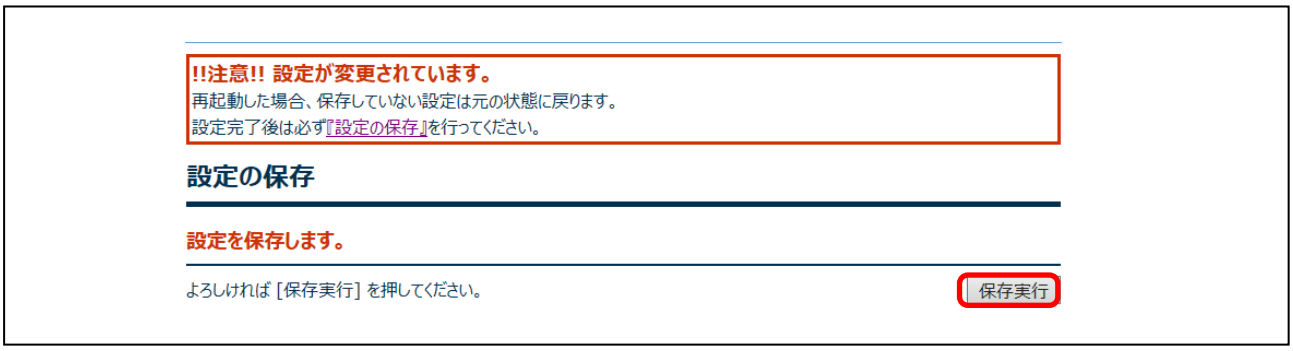
メモ [更新]ボタンをクリックすると、情報を更新することが可能です。

(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。

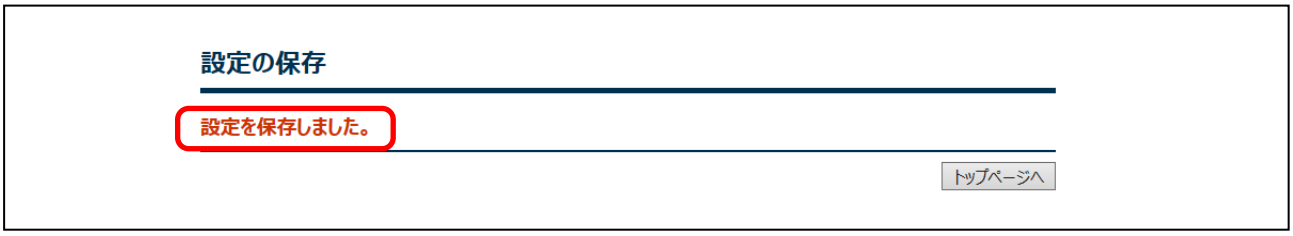
(9) VPN 情報は、接続名にマウスカーソルを近づけることで、詳細情報を確認することができます。また、接続名をわかりやすいように変更することができます。

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。



(11)「設定を保存しました。」のメッセージを確認します。

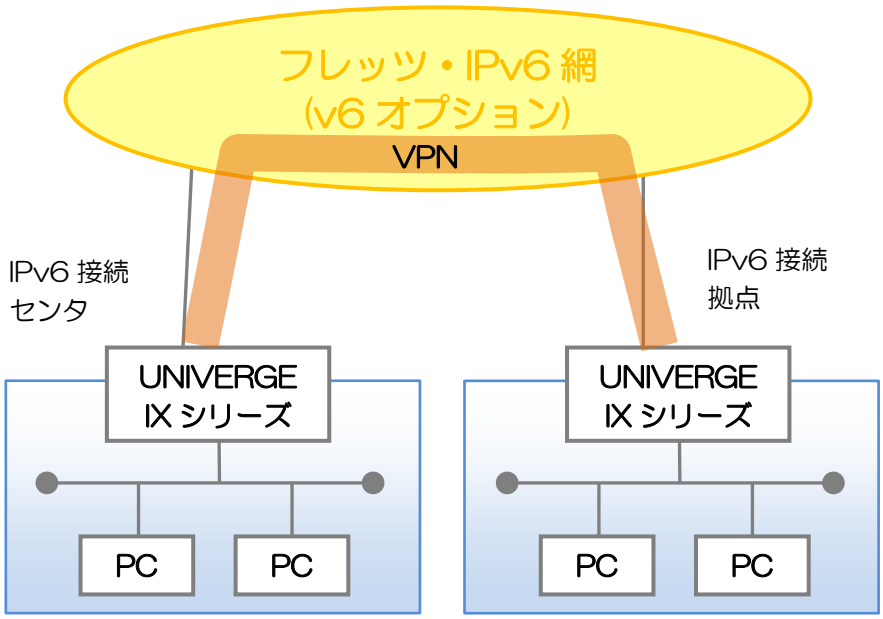


3.5 NGN VPN 接続

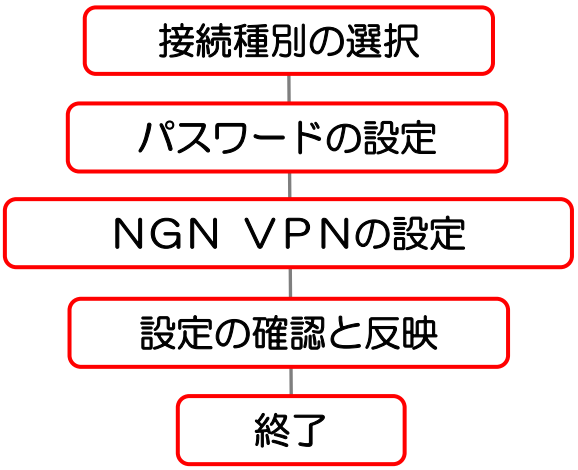
フレッツ・IPv6 網を使用した拠点間 VPN 通信の設定を行います。

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】



3.5.1 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。

メモ　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。

メモ 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。

3.5.2 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。

メモ　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。

(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。

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。

(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。

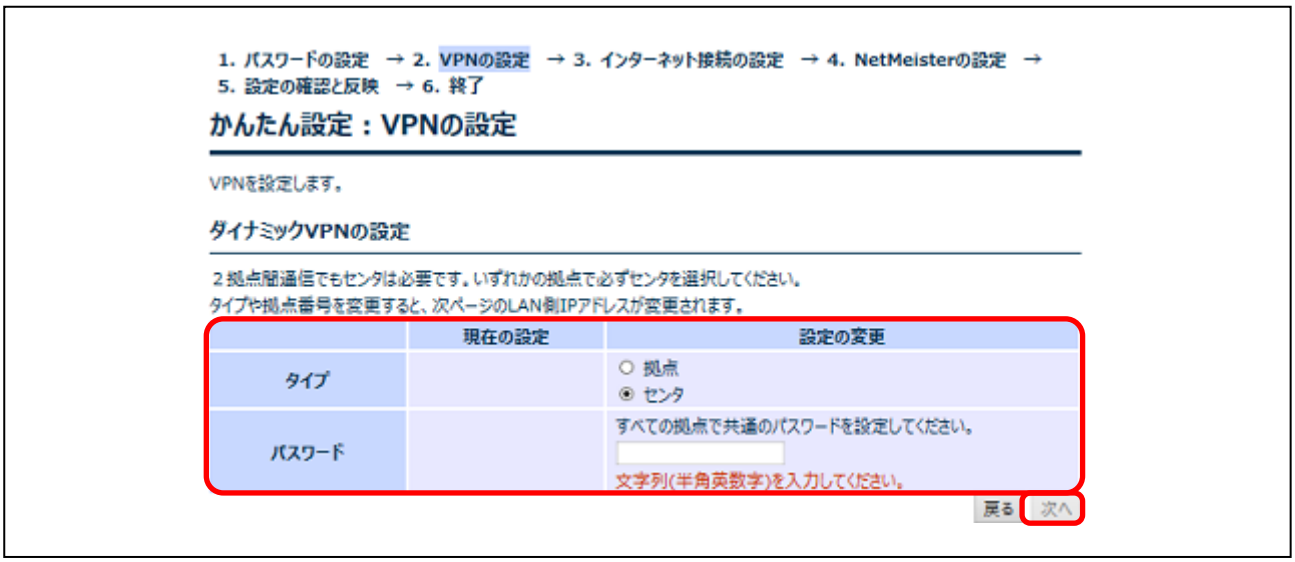
番号	項目	内容
①	ユーザ名	本装置にログインするときのユーザ名です。 ・ 初期状態ではユーザ名は設定されていません。 ・ パスワード設定後のユーザ名は「admin」です。Web 設定からは変更できません。
②	パスワード	本装置にログインするときのパスワードです。 ・ 初期状態ではパスワードは設定されていません。 ・ 半角英数字 1～249 文字で入力します。 注意 ・ 大文字／小文字は区別されます。 ・ パスワードの入力文字は表示されません。●●●のように伏せ文字で表示されます。 ・ パスワードは、第三者に推測されにくく、忘れないような文字列を入力してください。

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。

3.5.3 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。

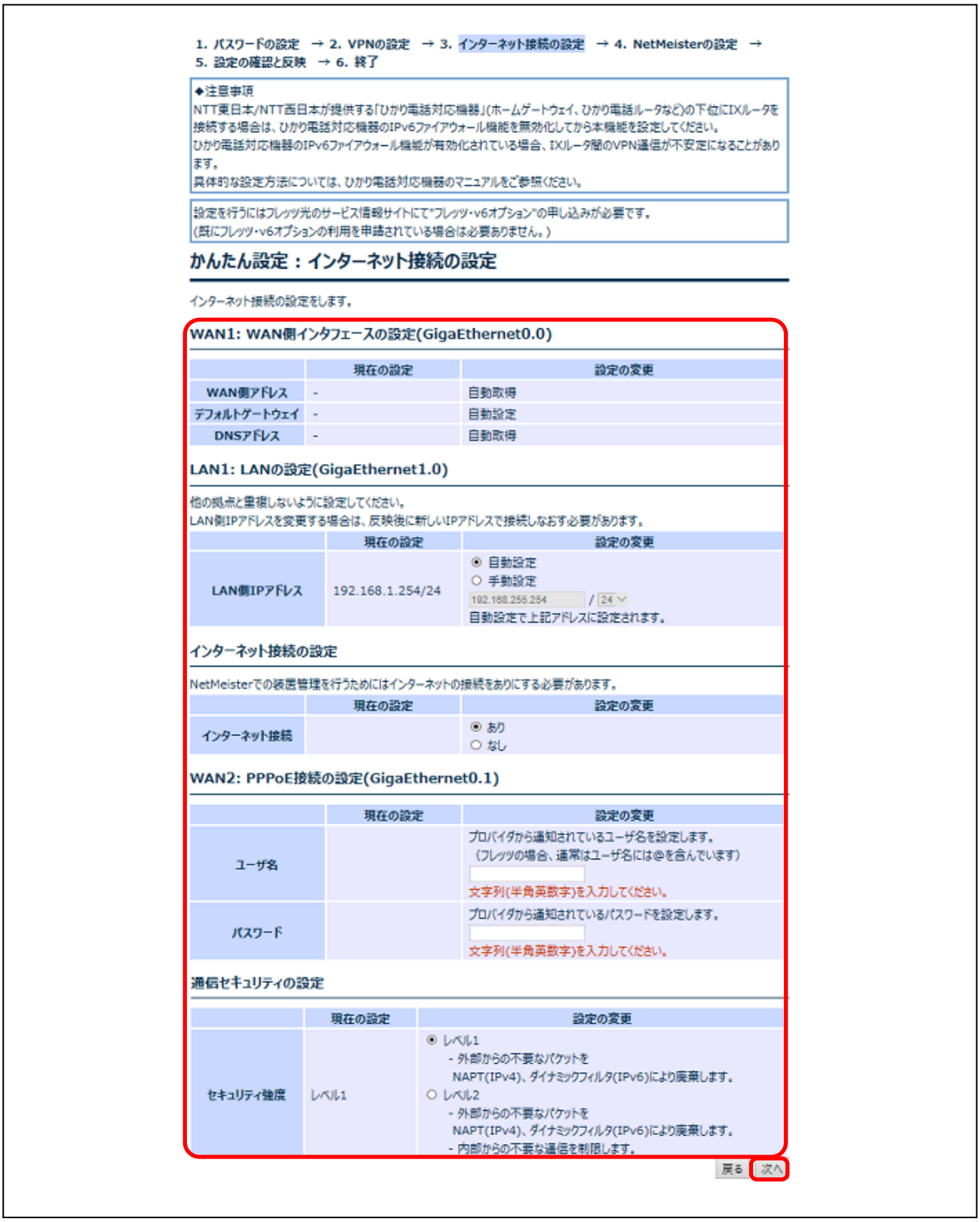
メモ　パスワードの設定に戻る場合は、[戻る]ボタンをクリックしてください。



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。

(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。



3. かんたん設定

<table>
<tr><th>番号</th><th>項目</th><th>内容</th></tr>
<tr><td>①</td><td>LAN 側 IP アドレス</td><td>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。</td></tr>
<tr><td>②</td><td>インターネット接続</td><td>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。
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。
・ 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。</td></tr>
<tr><td>③</td><td>ユーザ名</td><td>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)
・ 半角英数字で 1～59 文字まで入力できます。</td></tr>
<tr><td>④</td><td>パスワード</td><td>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。
・ 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。</td></tr>
<tr><td>⑤</td><td>セキュリティ強度</td><td>セキュリティ強度を選択します。
・ 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>
<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>
</td></tr>
</table>

(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。

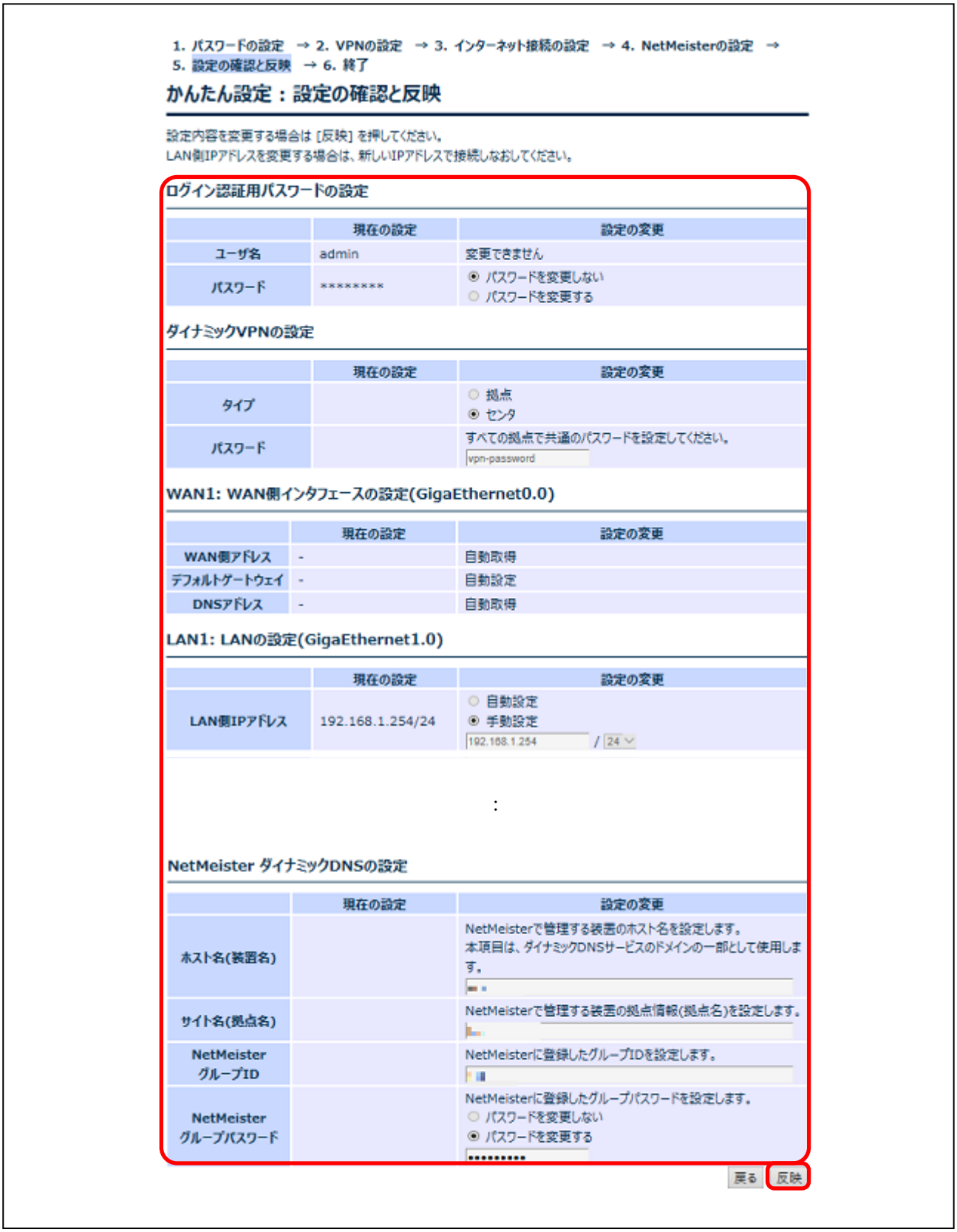
メモ　インターネット接続の設定に戻る場合は、[戻る]ボタンをクリックしてください。

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。 • 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 • 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。
②	サイト名(拠点名)	NetMeister に通知するサイト名を設定します。 • 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 • 大文字は、小文字に変換して 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	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。 • 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 • 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。 • 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 • 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) 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。



⑸　「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	********	◉ パスワードを変更しない ○ 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	○ 拠点 ◉ 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。 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	○ 自動設定 ◉ 手動設定 192.168.1.254 / 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。
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。
NetMeister グループID	■■	NetMeisterに登録したグループIDを設定します。
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。 ◉ パスワードを変更しない ○ パスワードを変更する

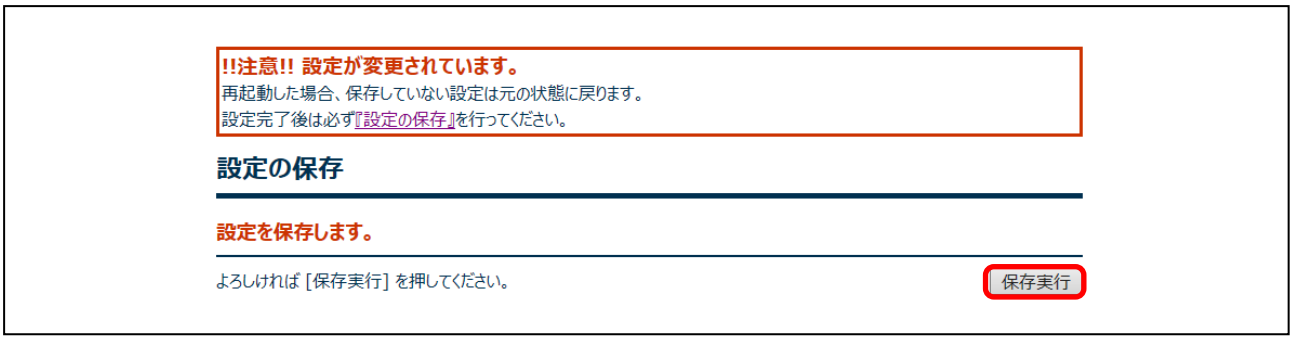
トップページへ

⑹　トップページで WAN 情報の接続状態を確認します。

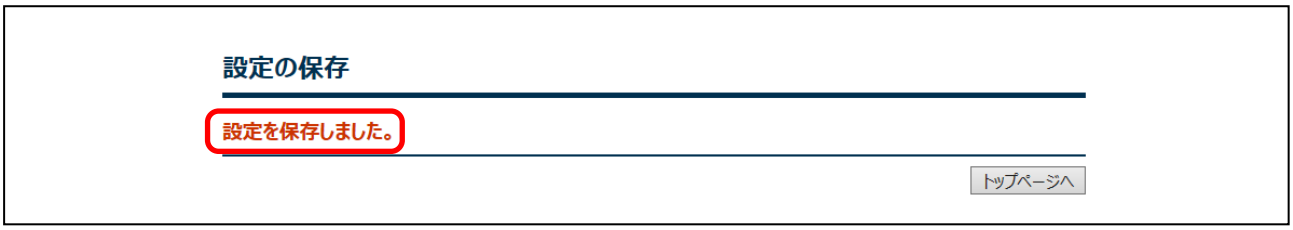
メモ　[更新]ボタンをクリックすると、情報を更新することが可能です。

⑺　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。

⑻　[保存実行]ボタンをクリックします。



⑼　「設定を保存しました。」のメッセージを確認します。



3.5.4 拠点の場合の設定

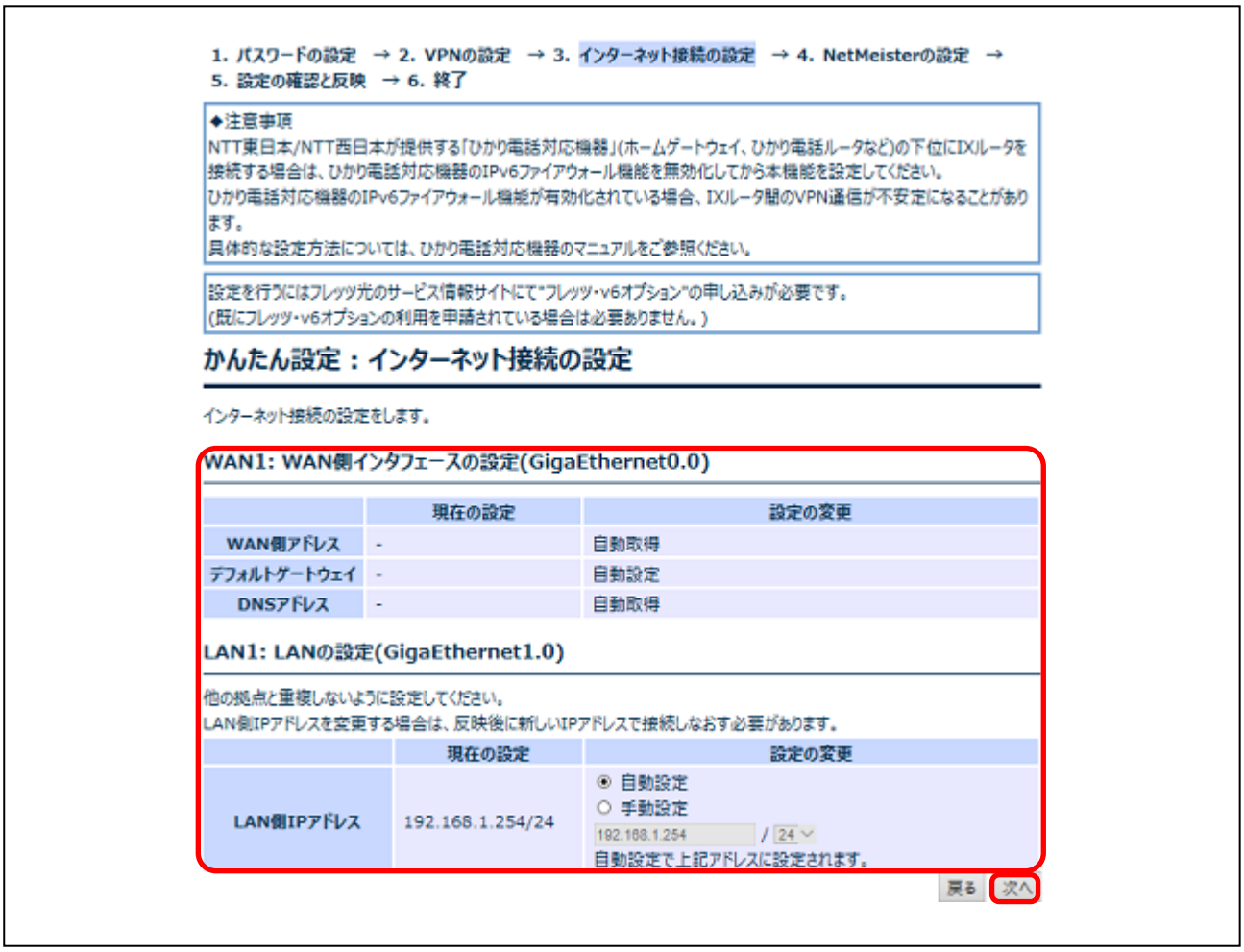
(1) ダイナミック VPN の設定で、[VPN の設定]の各項目を設定し、[次へ]ボタンをクリックします。

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。

⑵ [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。



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) [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。

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。 • 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 • 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。
②	サイト名(拠点名)	NetMeister に通知するサイト名を設定します。 • 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 • 大文字は、小文字に変換して 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	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。 • 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 • 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。 • 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 • 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) 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。

⑸　「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	********	◉ パスワードを変更しない ○ 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	◉ 拠点 ○ 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	[redacted]	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。 [redacted] .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)	[redacted]	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。 [redacted]
サイト名(拠点名)	[redacted]	NetMeisterで管理する装置の拠点情報(拠点名)を設定します。 [redacted]
NetMeister グループID	[redacted]	NetMeisterに登録したグループIDを設定します。 [redacted]
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。 ◉ パスワードを変更しない ○ パスワードを変更する

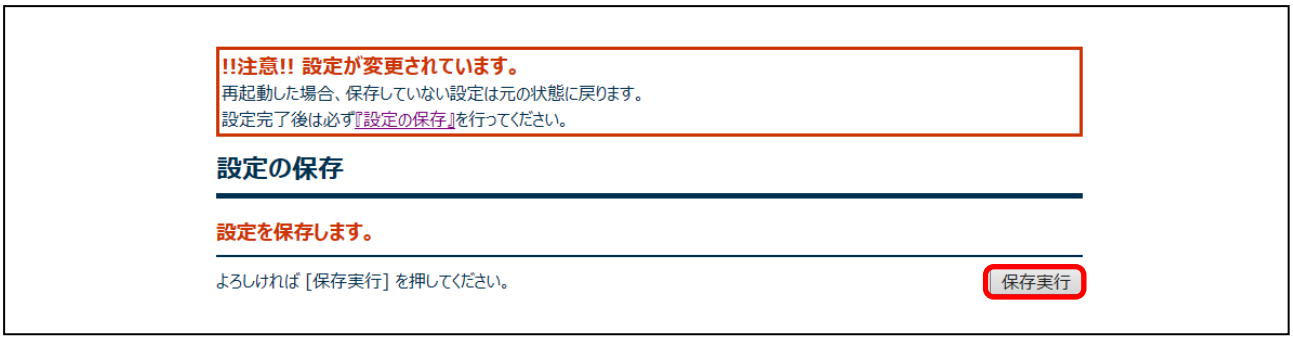
トップページへ

⑹　トップページで WAN 情報の接続状態を確認します。

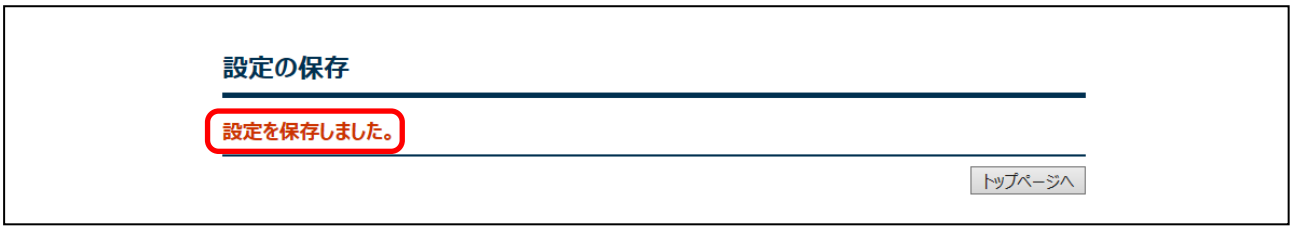
メモ　[更新]ボタンをクリックすると、情報を更新することが可能です。

⑺　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。

⑻　[保存実行]ボタンをクリックします。



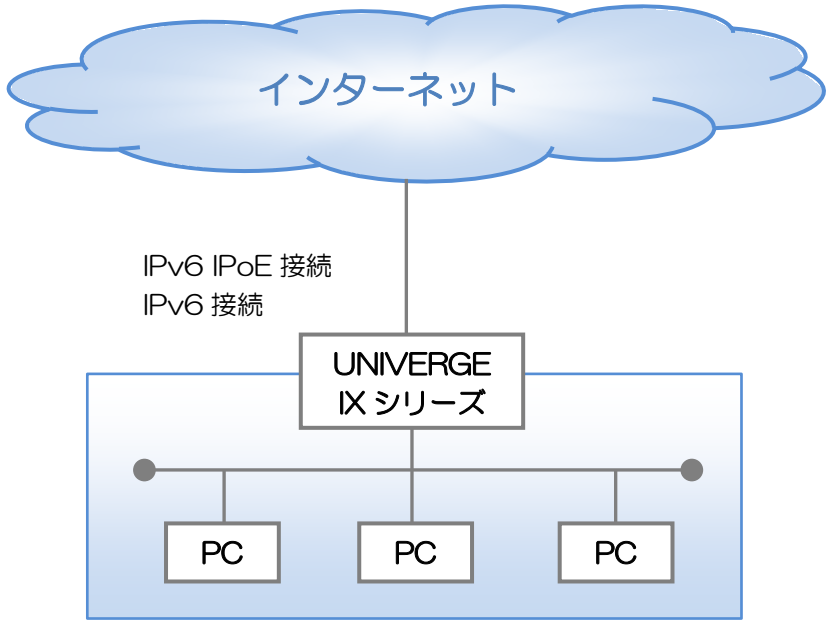
⑼　「設定を保存しました。」のメッセージを確認します。



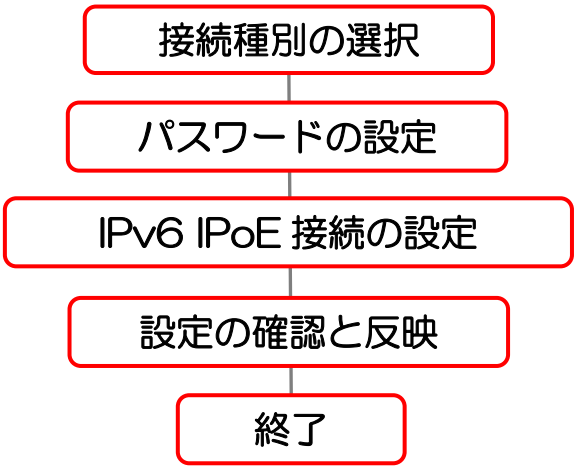
3.6 IPv6 IPoE 接続

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。

(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。

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。

(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。 ・ 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 1～249 文字で入力します。 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) [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。

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		○ OCN(OCNバーチャルコネクト) ◉ JPIX(v6プラス) ○ 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		◉ PD/RA自動判別 ○ 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		○ 動的 ◉ 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。 https://www.example.com:port URLを入力してください。
ユーザ名		文字列(半角英数字)を入力してください。
パスワード		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		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		IPアドレスを入力してください。

戻る　次へ

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。

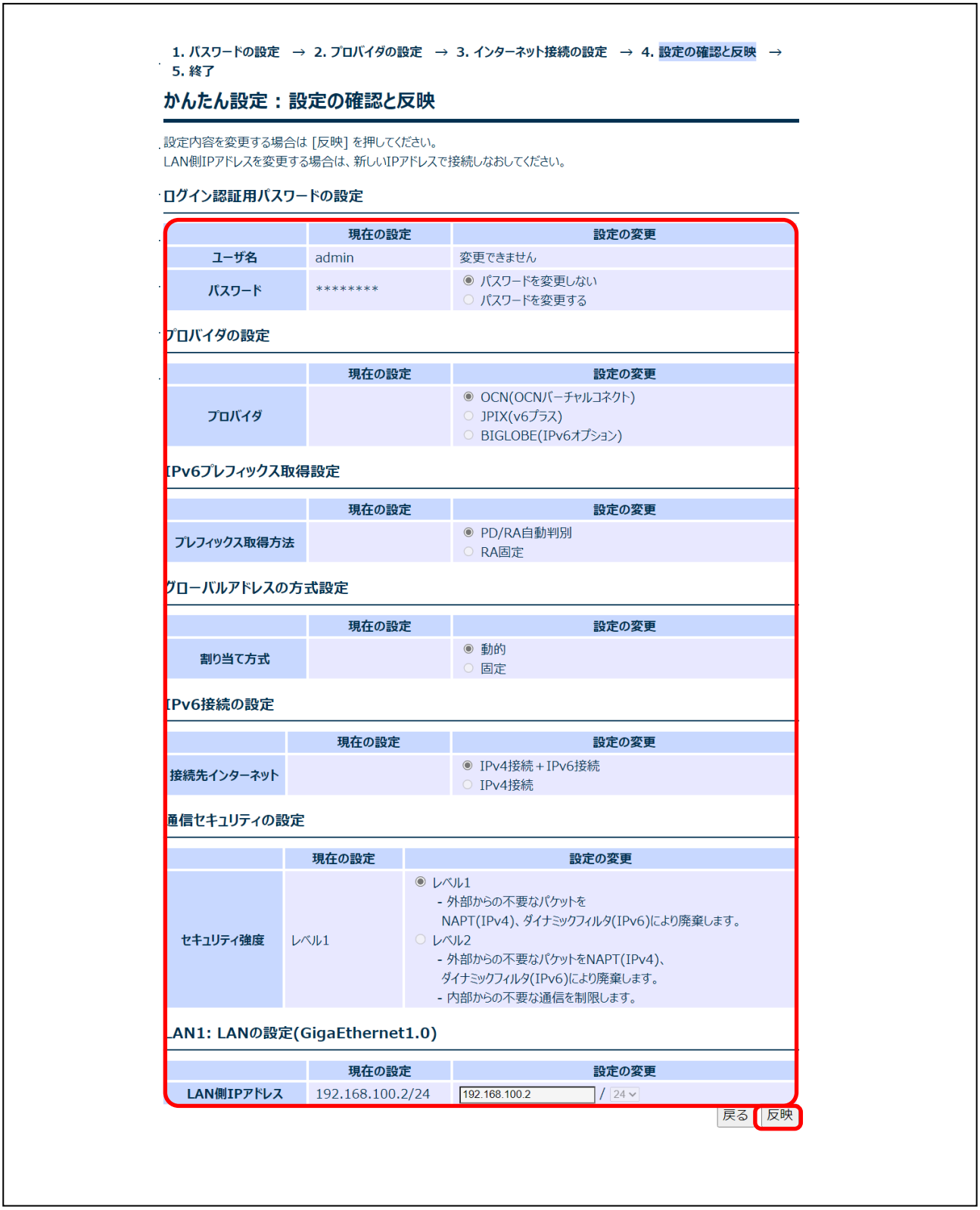
(5) [インターネット接続の設定]の項目を設定し、[設定の確認]ボタンをクリックします。

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。

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。 ・「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。 ・ 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。 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。

⑹　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。



(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	********	◉ パスワードを変更しない ○ 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)	○ OCN(OCNバーチャルコネクト) ◉ JPIX(v6プラス) ○ 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		◉ PD/RA自動判別 ○ 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	◉ 動的 ○ 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	◉ IPv4接続＋IPv6接続 ○ 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	◉ 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。 ○ 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	192.168.1.254 / 24

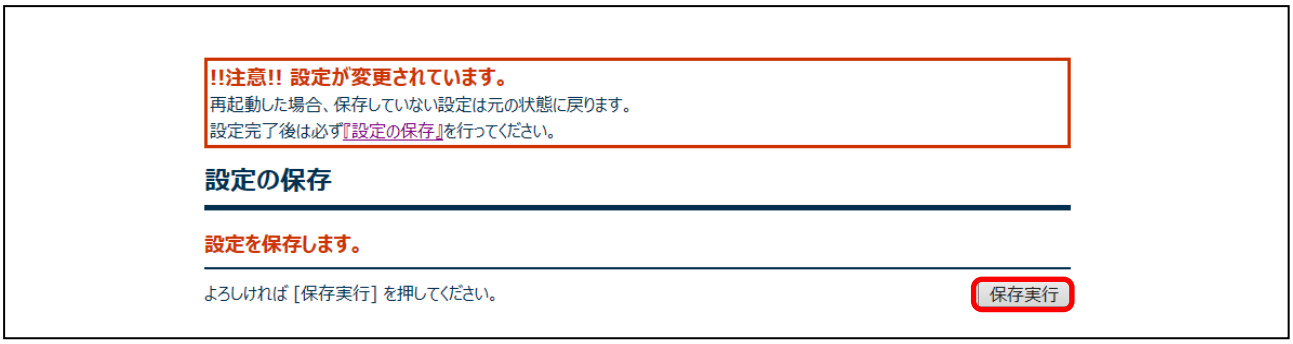
トップページへ

⑻　トップページで WAN 情報の接続状態を確認します。

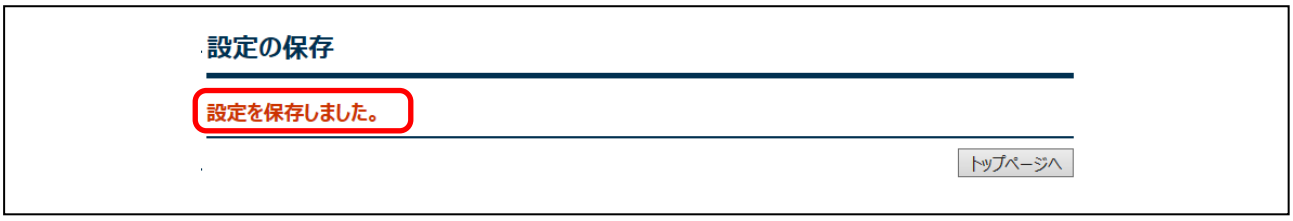
メモ　[更新]ボタンをクリックすると、情報を更新することが可能です。

⑼　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。

(10) [保存実行]ボタンをクリックします。



(11)「設定を保存しました。」のメッセージを確認します。

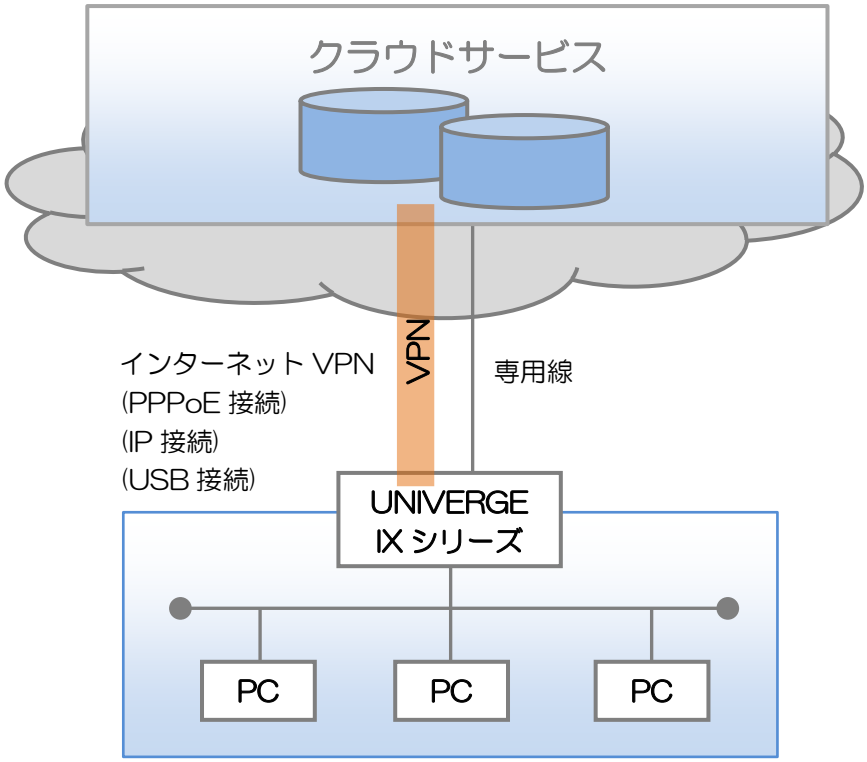


3. かんたん設定

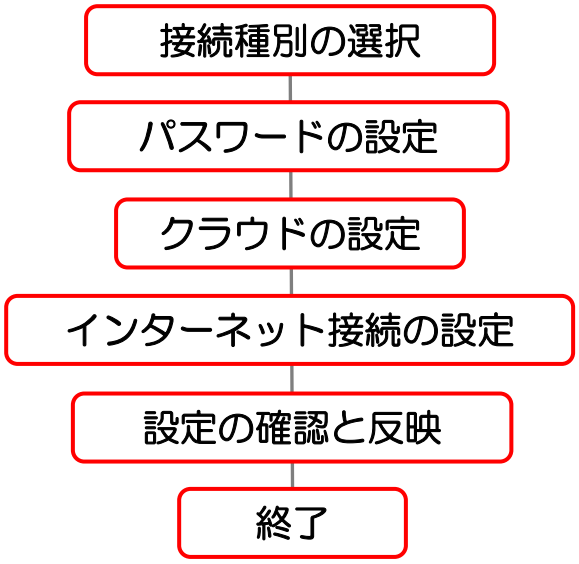
3.7 クラウド接続

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。

(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。

(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。 ・ 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。 ・ 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。

(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。

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		◉ AWS (Amazon Web Services) ○ Microsoft Azure ○ NEC Cloud IaaS
接続形態		◉ インターネットVPN ○ 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。 [ ] 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。 [ ] 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。 [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。 [ ] / [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。 [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。 [ ]
	VPNアドレス		**Inside IP Addresses:**の Virtual Private Gateway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。 [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。 [ ] / [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。 [ ] 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。 [ ]

戻る 次へ

<table>
<tr><th>番号</th><th>項目</th><th>内容</th></tr>
<tr><td>①</td><td>サービス種別</td><td>「AWS (Amazon Web Services)」を選択します。</td></tr>
<tr><td>②</td><td>接続形態</td><td>「インターネット VPN」を選択します。</td></tr>
<tr><td>③</td><td>IPsec Tunnel#1
接続先(クラウド)
WAN 側 IP アドレス</td><td>IPsec Tunnel#1 の Outside IP Addresses:の Virtual Private Gateway を入力します。</td></tr>
<tr><td>④</td><td>IPsec Tunnel#1
接続先(クラウド)
VPN アドレス</td><td>IPsec Tunnel#1 の Inside IP Addresses:の Virtual Private Gateway を入力します。</td></tr>
<tr><td>⑤</td><td>IPsec Tunnel#1
接続先(クラウド)
AS 番号</td><td>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。</td></tr>
<tr><td>⑥</td><td>IPsec Tunnel#1
接続元(IX)
VPN アドレス</td><td>IPsec Tunnel#1 の Inside IP Addresses:の Customer Gateway を入力します。</td></tr>
<tr><td>⑦</td><td>IPsec Tunnel#1
接続元(IX)
AS 番号</td><td>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。</td></tr>
<tr><td>⑧</td><td>IPsec Tunnel#2
接続先(クラウド)
WAN 側 IP アドレス</td><td>IPsec Tunnel#2 の Outside IP Addresses:の Virtual Private Gateway を入力します。
メモ
・ 複数 VPN を使用しない場合は、本設定は不要です。</td></tr>
<tr><td>⑨</td><td>IPsec Tunnel#2
接続先(クラウド)
VPN アドレス</td><td>IPsec Tunnel#2 の Inside IP Addresses:の Virtual Private Gateway を入力します。
メモ
・ 複数 VPN を使用しない場合は、本設定は不要です。</td></tr>
<tr><td>⑩</td><td>IPsec Tunnel#2
接続先(クラウド)
AS 番号</td><td>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。
メモ
・ 複数 VPN を使用しない場合は、本設定は不要です。</td></tr>
<tr><td>⑪</td><td>IPsec Tunnel#2
接続元(IX)
VPN アドレス</td><td>IPsec Tunnel#2 の Inside IP Addresses:の Customer Gateway を入力します。
メモ
・ 複数 VPN を使用しない場合は、本設定は不要です。</td></tr>
<tr><td>⑫</td><td>IPsec Tunnel#1
IKE 事前共有鍵</td><td>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>
<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></td></tr>
</table>

<table>
<tr>
<td>⑬</td>
<td>IPsec Tunnel#2
IKE 事前共有鍵</td>
<td>IPsec Tunnel#2 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>
<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>
メモ
・ 複数 VPN を使用しない場合は、本設定は不要です。</td>
</tr>
</table>

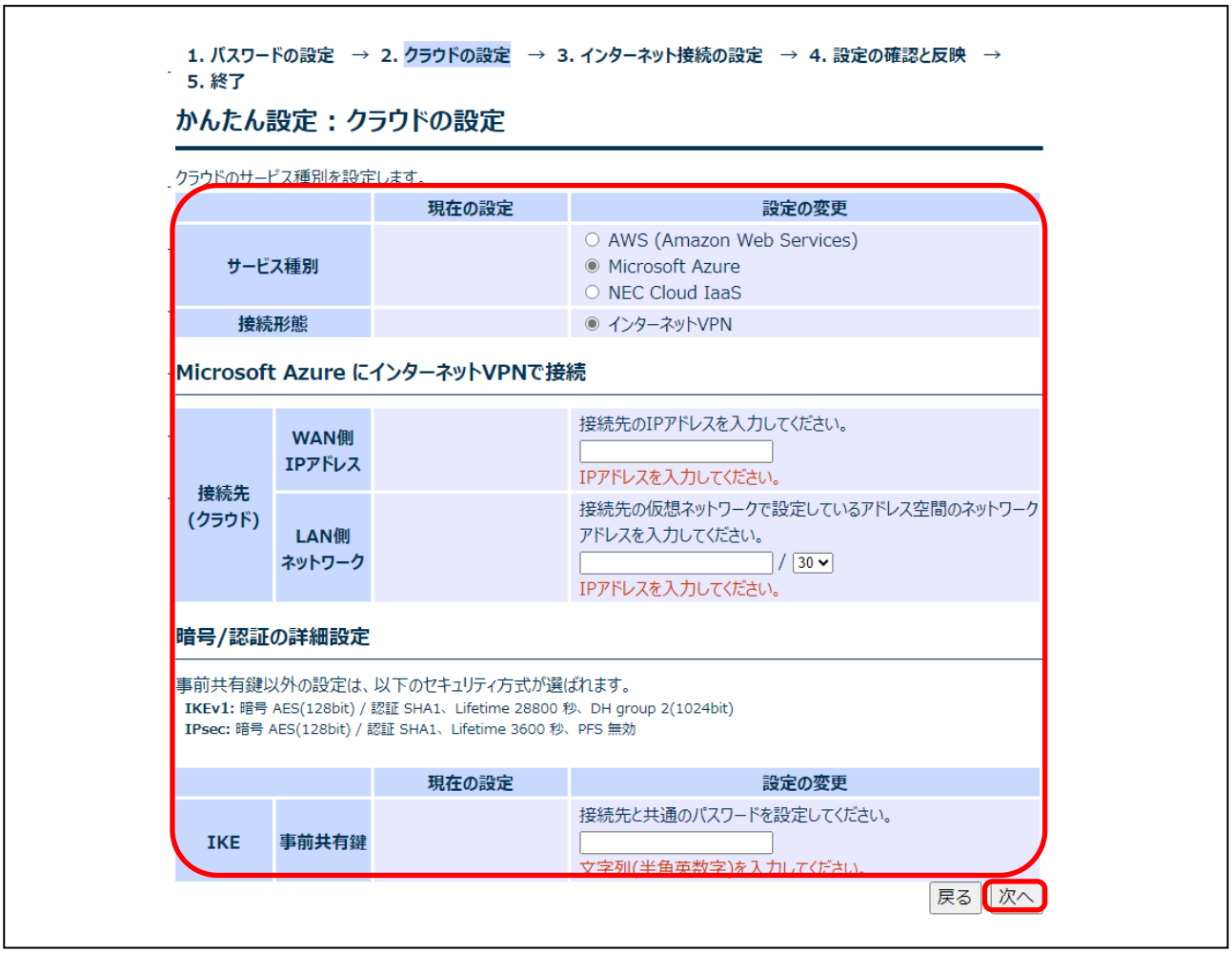
AWS(Amazon Web Services)に専用線で接続する場合

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。

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。

Microsoft Azure に接続する場合



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。

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

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。

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

⑸ [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。

メモ　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)

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。

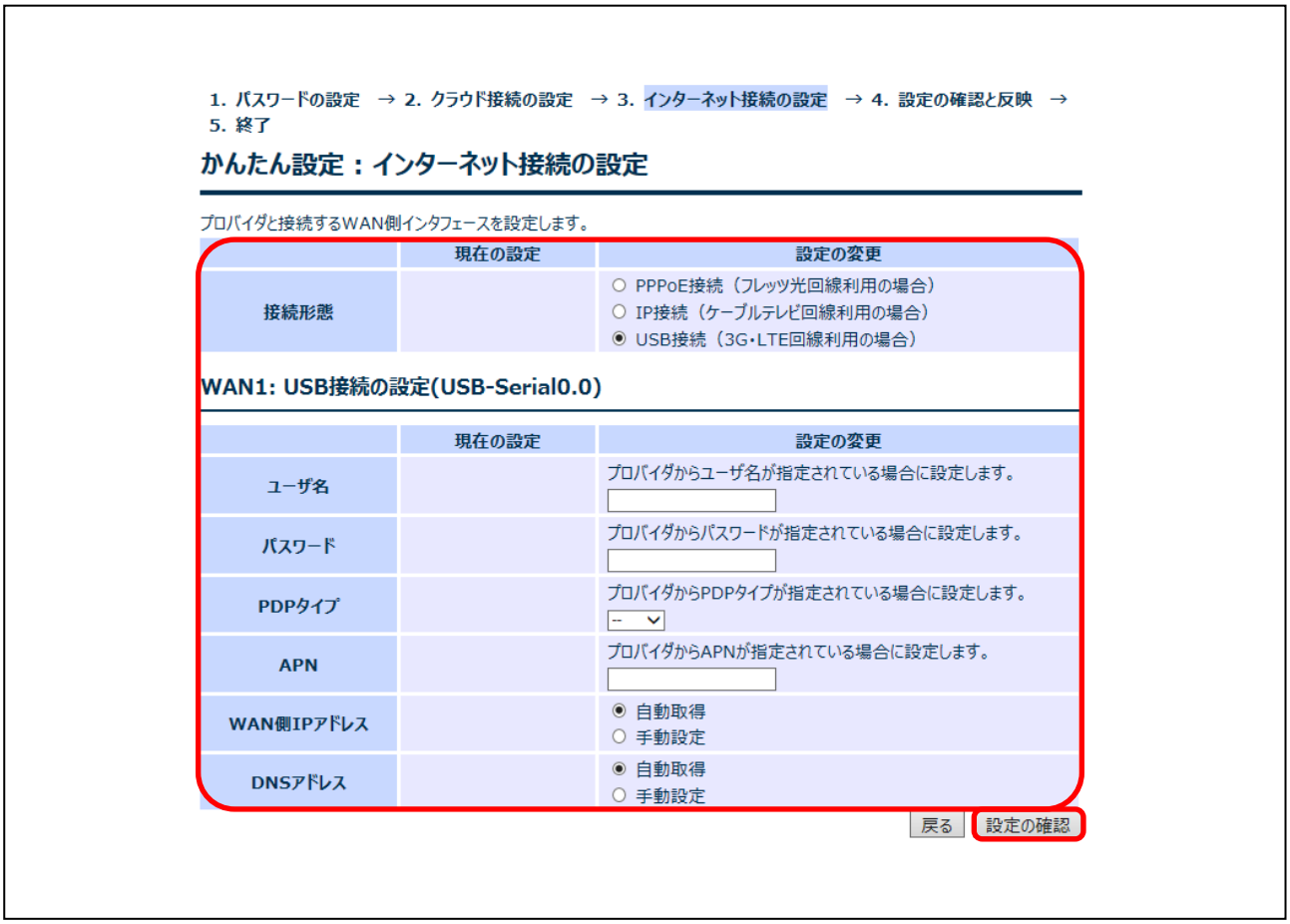
3. かんたん設定

IP 接続の場合(ケーブルテレビ回線利用の場合)

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。 • 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。
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。 • 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。

USB 接続の場合(3G・LTE 回線利用の場合)

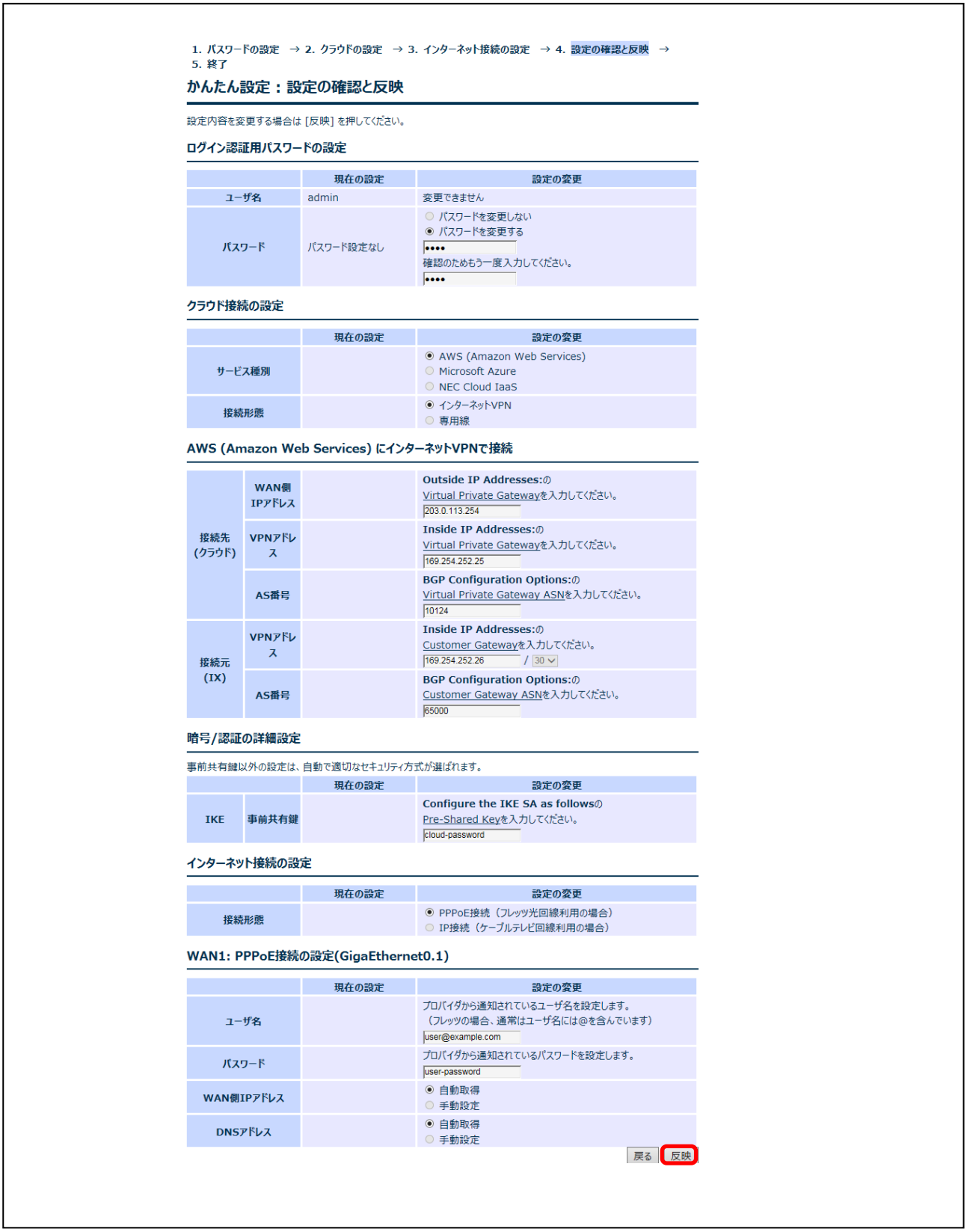
※IX2215/IX2235/IX2310/IX3315 のみ



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。

⑹　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. 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	○ パスワードを変更しない ◉ 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 (Amazon Web Services) ○ Microsoft Azure ○ NEC Cloud IaaS
接続形態		◉ インターネットVPN ○ 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		◉ PPPoE接続（フレッツ光回線利用の場合） ○ 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		◉ 自動取得 ○ 手動設定
DNSアドレス		◉ 自動取得 ○ 手動設定

戻る　反映

(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	********	○ パスワードを変更しない ◉ 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	◉ AWS (Amazon Web Services) ○ Microsoft Azure ○ NEC Cloud IaaS
接続形態	インターネットVPN	◉ インターネットVPN ○ 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	◉ PPPoE接続（フレッツ光回線利用の場合） ○ 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)

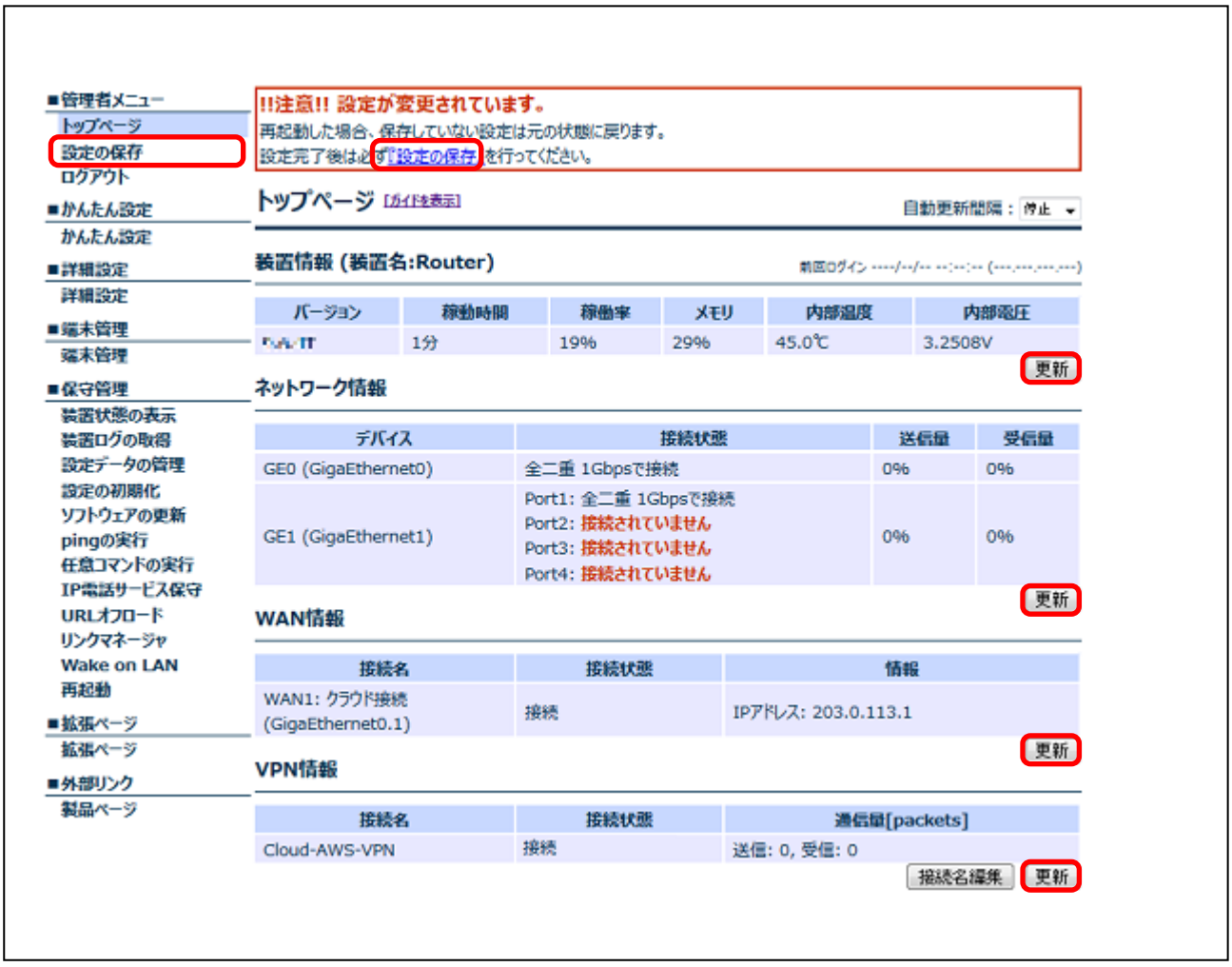
	現在の設定	設定の変更
ユーザ名	user@example.com	プロバイダから通知されているユーザ名を設定します。（フレッツの場合、通常はユーザ名には@を含んでいます） user@example.com
パスワード	user-password	プロバイダから通知されているパスワードを設定します。 user-password
WAN側IPアドレス	自動取得	◉ 自動取得 ○ 手動設定
DNSアドレス	自動取得	◉ 自動取得 ○ 手動設定

トップページへ

(8) 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。

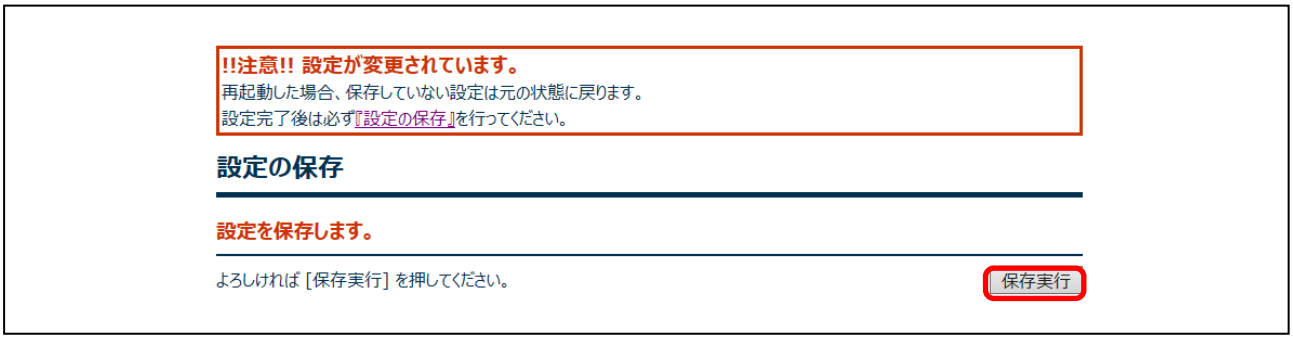
(9) メニューエリア、または、メッセージエリアから[設定の保存]をクリックします。



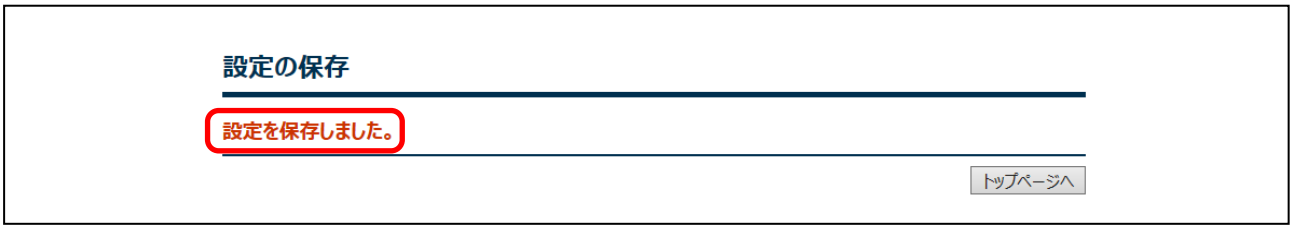
(10) VPN 情報は、接続名にマウスカーソルを近づけることで、詳細情報を確認することができます。また、接続名をわかりやすいように変更することができます。

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。



(12) 「設定を保存しました。」のメッセージを確認します。

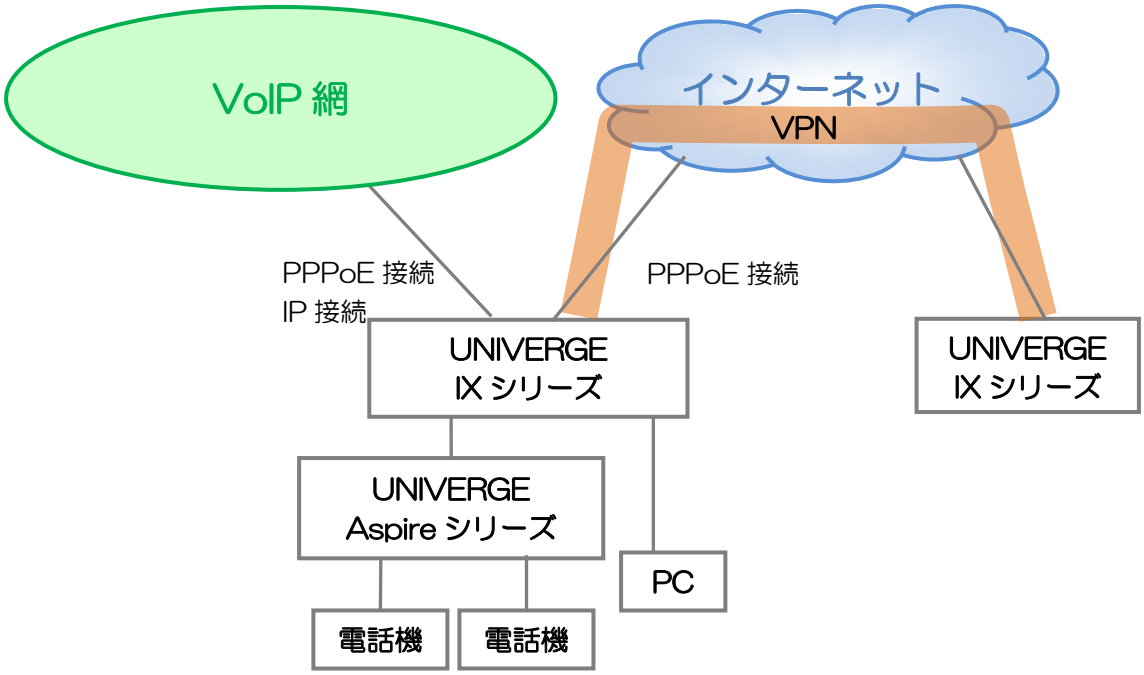


3.8 IP 電話サービス接続

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。

(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。

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。

(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。

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入力します。 • 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を入力します。 • 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 1～249 文字で入力します。 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	回線種別	契約内容にあわせて選択します。 注意 • 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。 • 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。 • 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。

(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

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。

au ひかりビジネス、FT フォン（0ABJ 番号）、スマートひかりの場合

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。

ひかり電話オフィスＡ（エース）の場合

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

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。

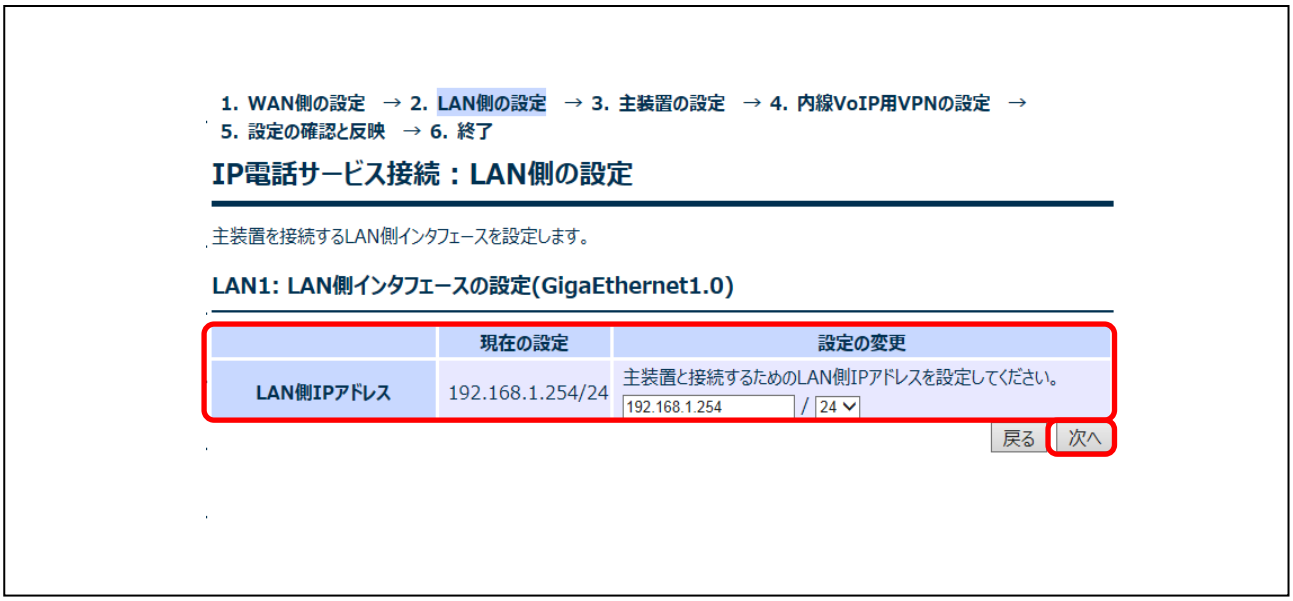
おとく光電話の場合

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。

⑸ [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。

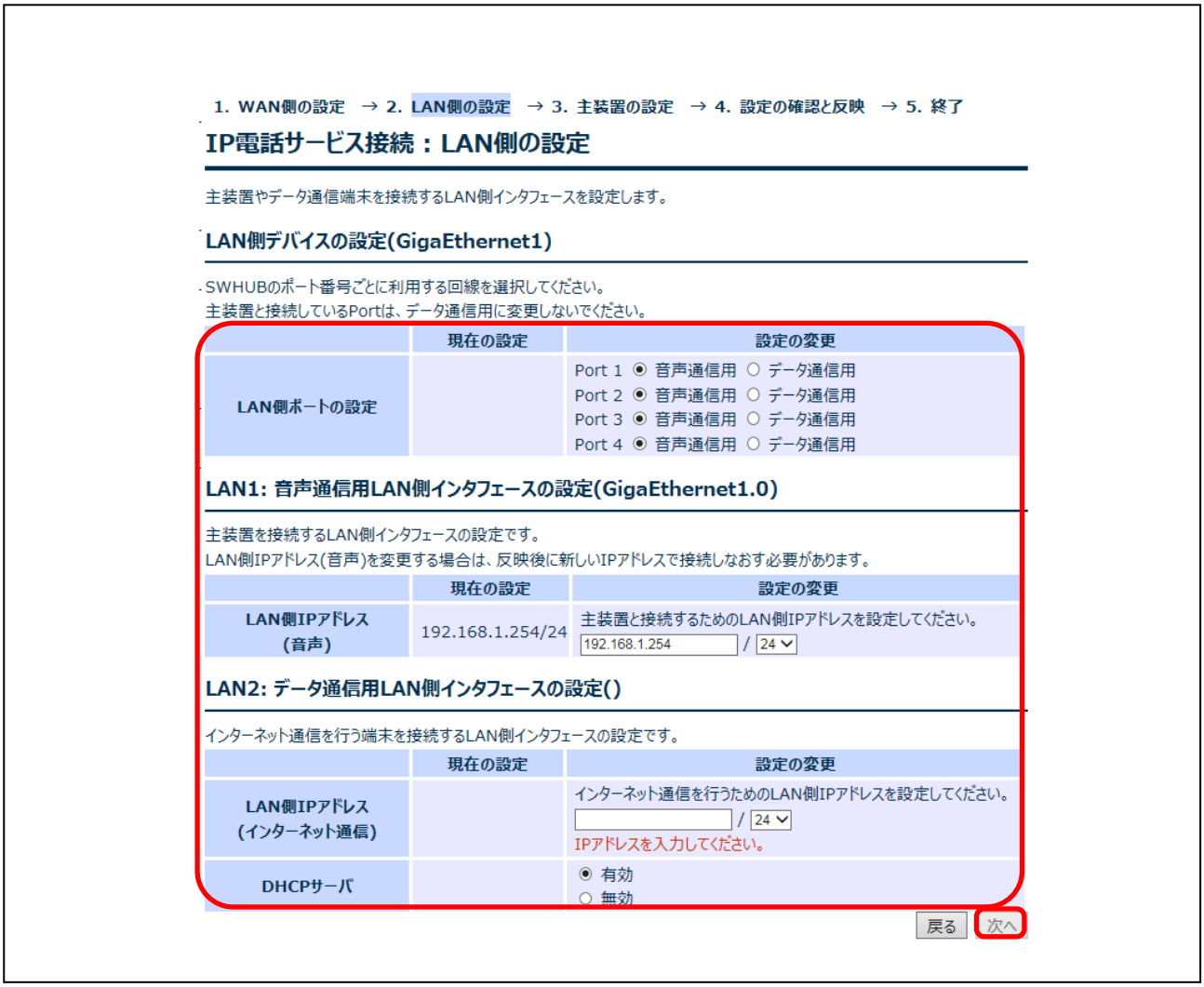
別回線でインターネットを利用しない場合



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



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。

⑹ [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

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。

別回線でインターネットを利用する場合

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。

(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

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。

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		◉ 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		◉ 自動取得 ○ 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		◉ 拠点 ○ 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。

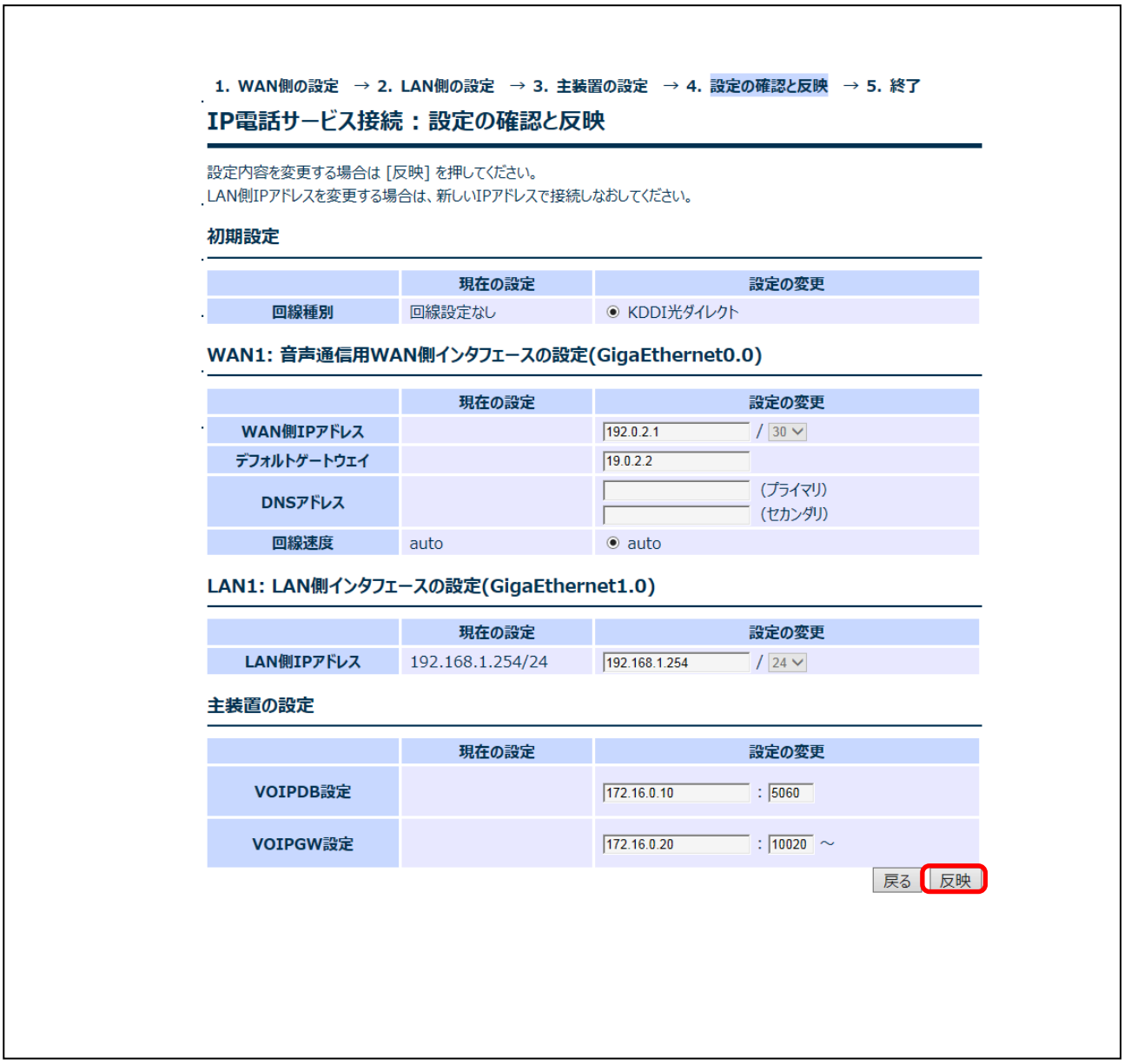
戻る　設定の確認

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。

⑻　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　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。

メモ　下記は KDDI 光ダイレクトの場合の例です。



⑼　「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。

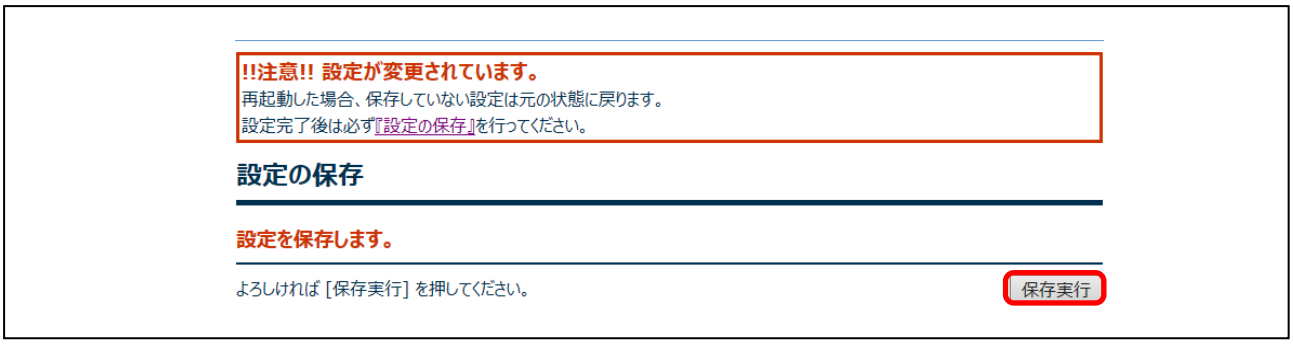
メモ　下記は KDDI 光ダイレクトの場合の例です。

(10) トップページで WAN 情報の接続状態を確認します。

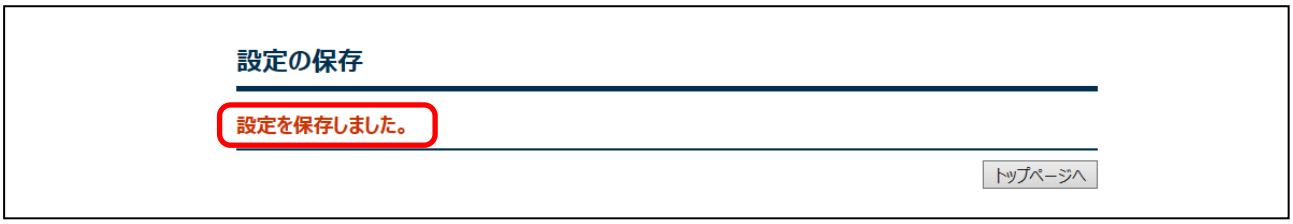
メモ　[更新]ボタンをクリックすると、情報を更新することが可能です。

(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。

(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

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 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。

- 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 NAPT 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

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。

4.1.1 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。

(3) 各項目を設定し、[反映]ボタンをクリックします。

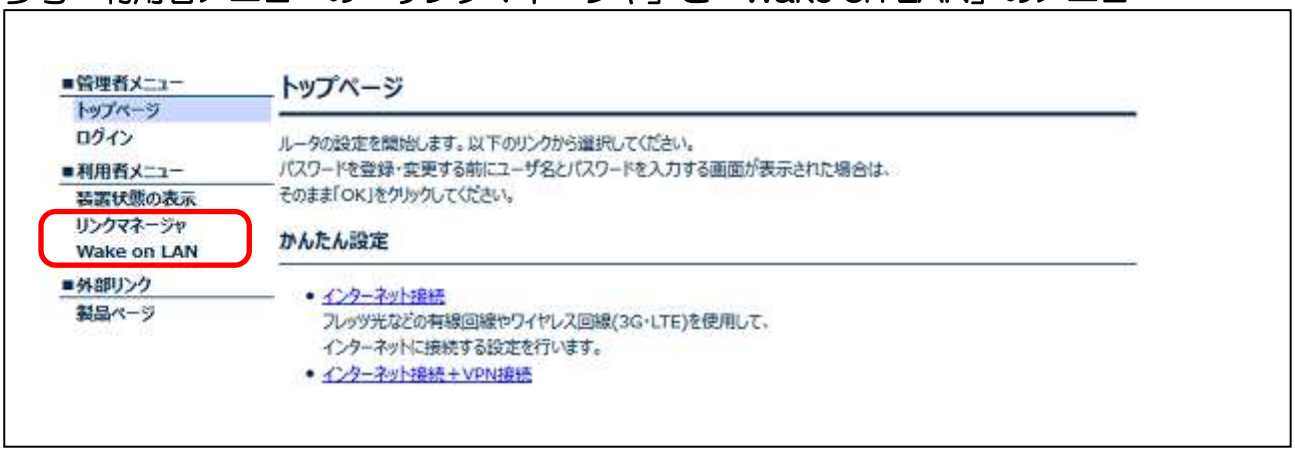
4. 詳細設定


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
パスワードを変更しない
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。
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
利用者ユーザを設定しない
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
『装置状態の表示』は認証が不要
『装置状態の表示』に認証が必要

4. 詳細設定

番号	項目	内容
①	ユーザ名	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。 ・ 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。 ・ 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。 メモ ・ 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。 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) 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	利用者ユーザ	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。 ・ 「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。 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。 メモ ・ 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	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。

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



(4) 「設定内容を変更しました。」のメッセージを確認します。

4.1.2 装置名の設定

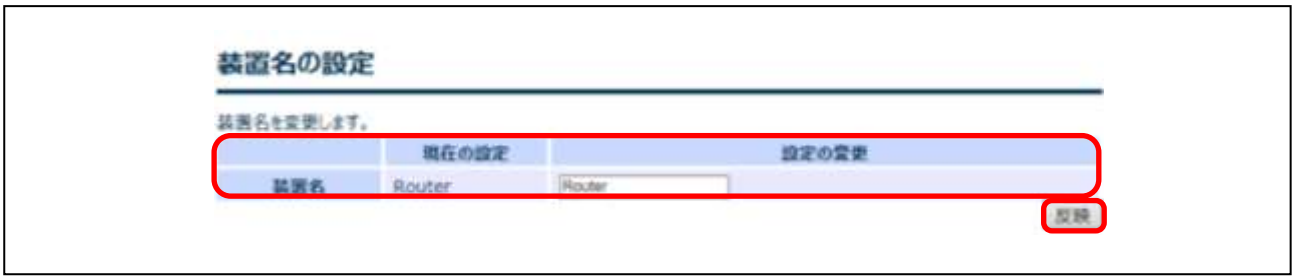
装置名を変更します。

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。

(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。

(3) 各項目を設定し、[反映]ボタンをクリックします。



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。 ・ 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。

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。

⑶　各項目を設定し、[反映]ボタンをクリックします。

番号	項目	内容
①	装置時刻	本装置の時刻を設定します。 • 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：0～59 • NTP 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。

⑷　「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。

4. 詳細設定

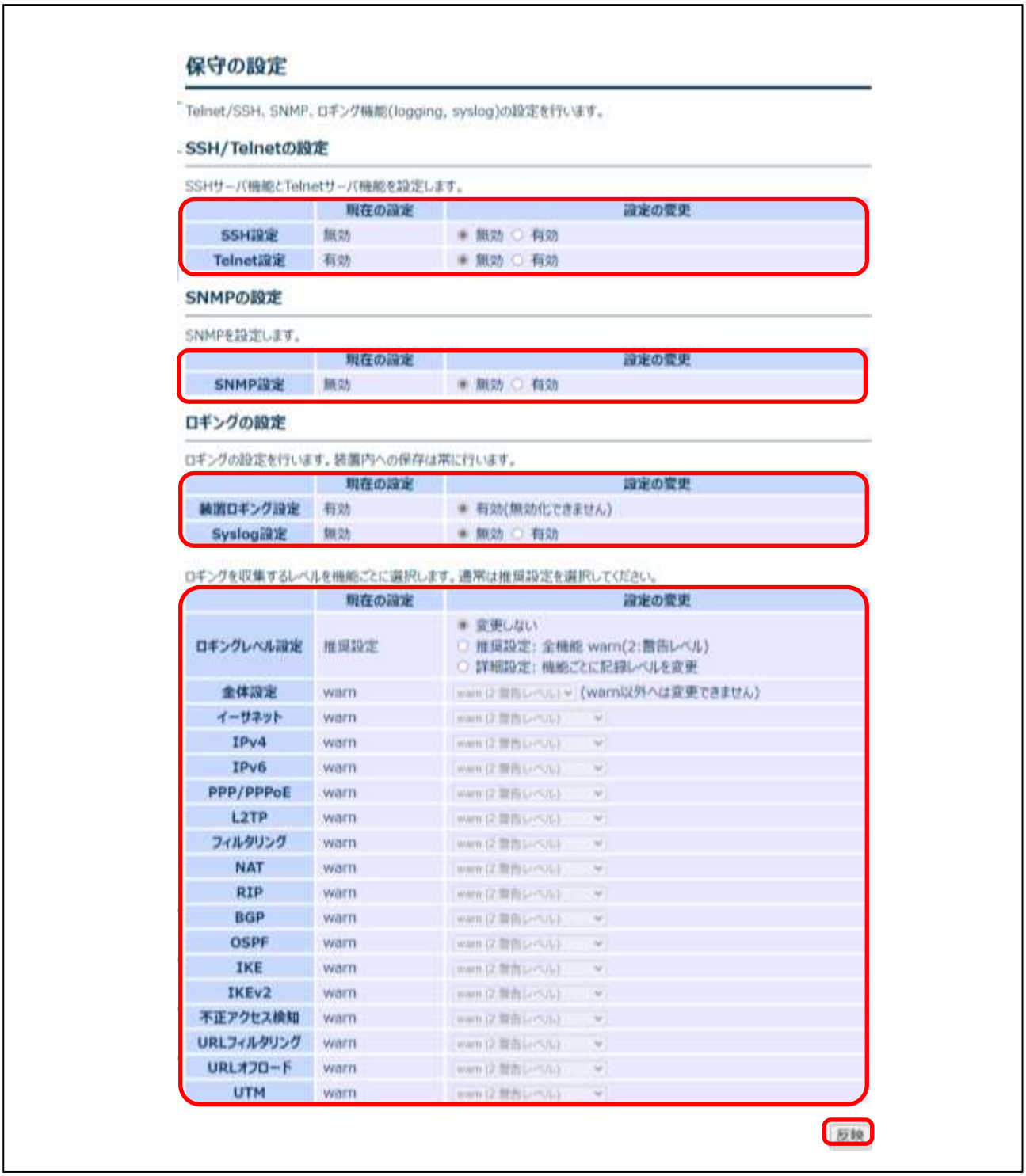
4.1.4 保守の設定

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。

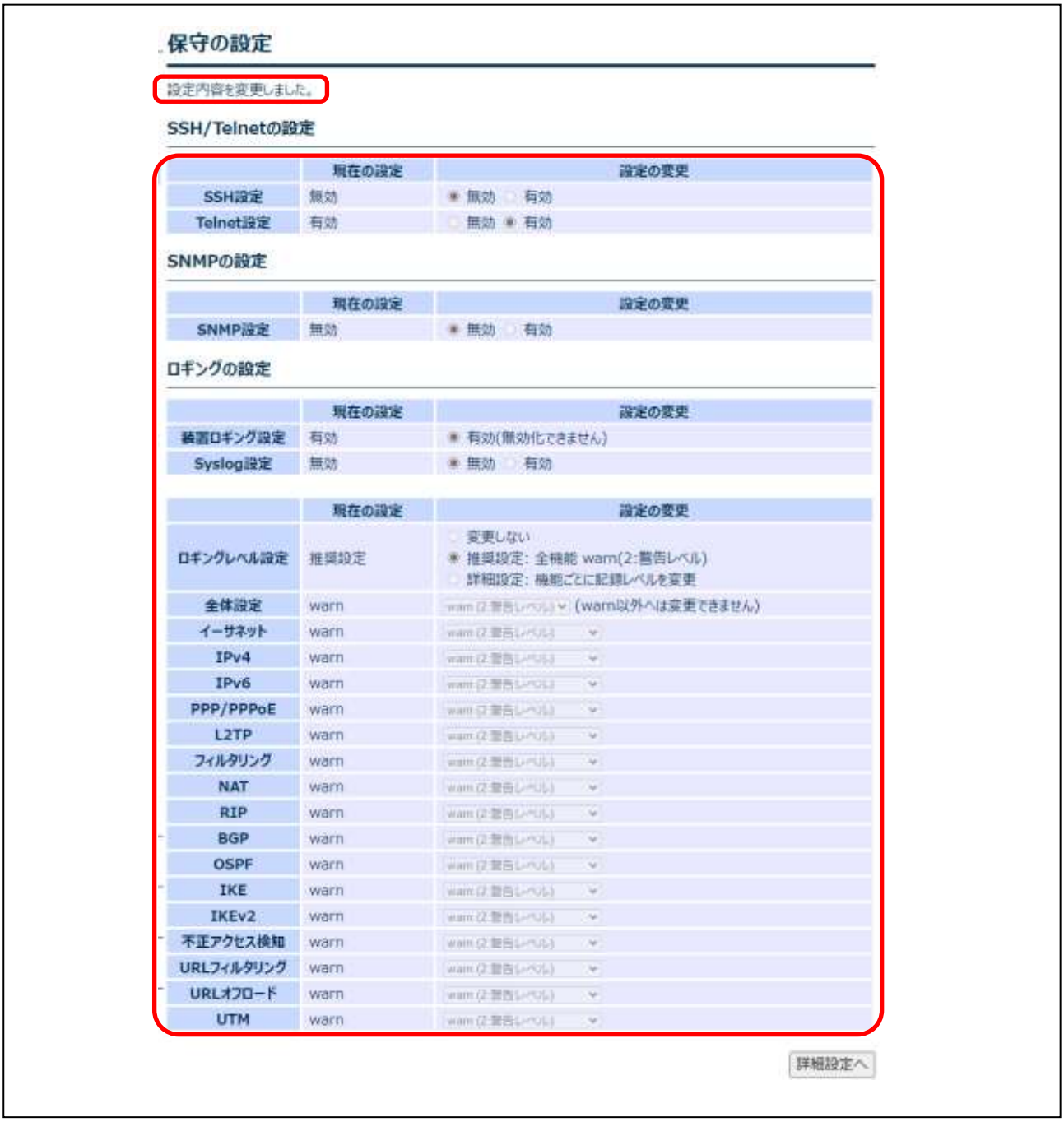
(3) 各項目を設定し、[反映]ボタンをクリックします。



4. 詳細設定

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。 • 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。 • 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。 • 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。 • 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。 • 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。 • 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。 • 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) 「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	◉ 無効 ○ 有効
Telnet設定	有効	○ 無効 ◉ 有効

SNMPの設定

	現在の設定	設定の変更
SNMP設定	無効	◉ 無効 ○ 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	◉ 有効(無効化できません)
Syslog設定	無効	◉ 無効 ○ 有効

	現在の設定	設定の変更
ロギングレベル設定	推奨設定	○ 変更しない ◉ 推奨設定: 全機能 warn(2:警告レベル) ○ 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

4.1.5 NetMeister の設定

NetMeister を設定します。

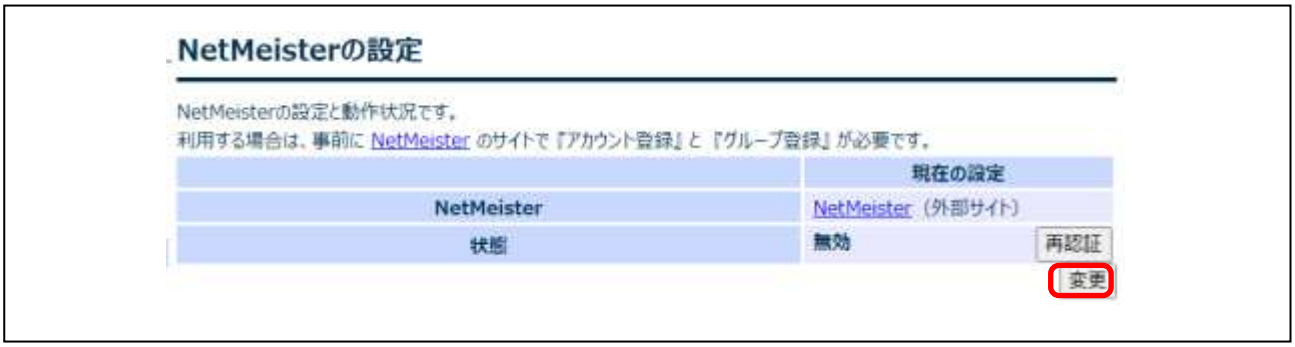
メモ NetMeister を利用しない場合、NetMeister の設定は不要です。

メモ 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。

(3) [変更]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。

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。

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

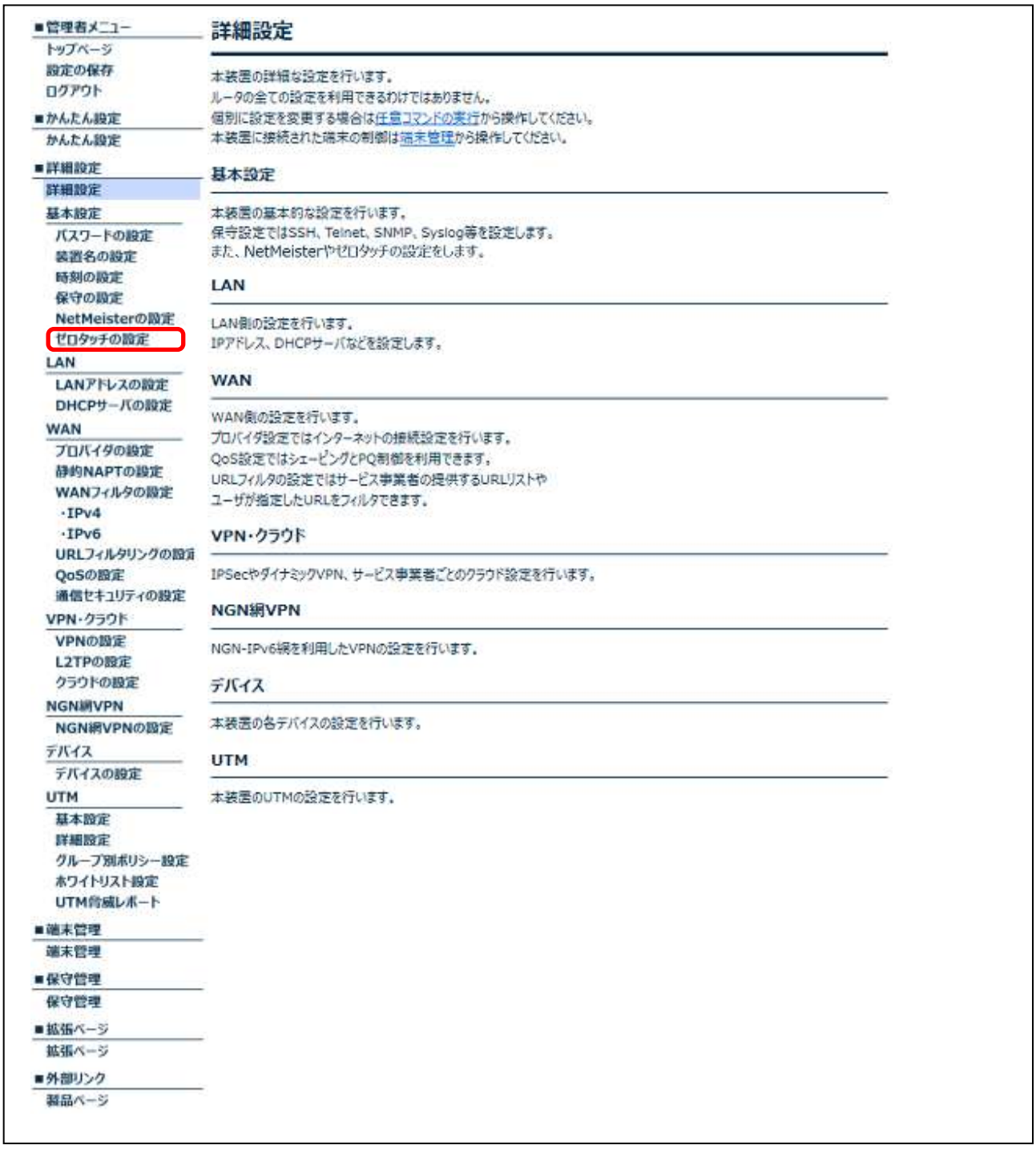
ゼロタッチプロビジョニング機能を設定します。

メモ　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。

メモ　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。



(3) 各項目を設定し、[反映]ボタンをクリックします。

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

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

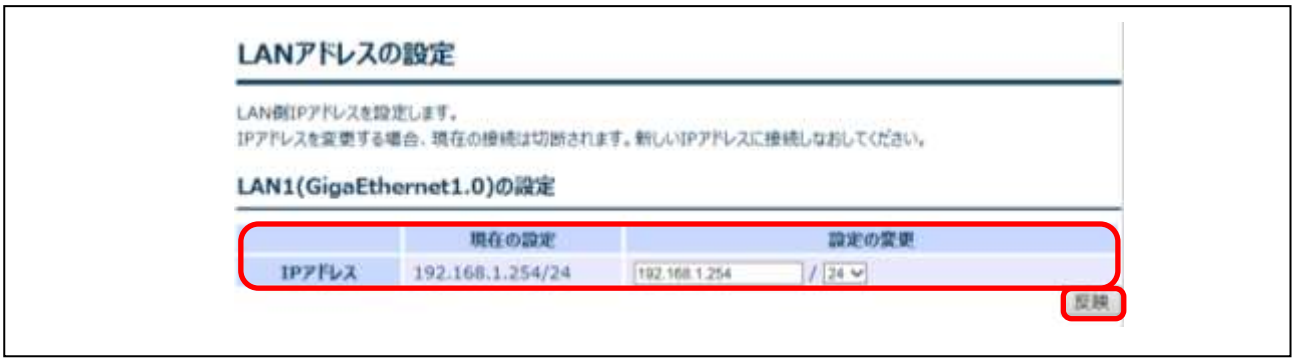
(1) ログイン後のメニューエリアから[詳細設定]をクリックします。

(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


■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
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。

(3) 各項目を設定し、[反映]ボタンをクリックします。



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。

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。

⑶　各項目を設定し、[反映]ボタンをクリックします。

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。

⑷　「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。

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。

(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)

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。 • 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) • 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。 • 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。 • 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。
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。 • 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。
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。

IPv4、IP 接続の場合(ケーブルテレビ回線利用の場合)

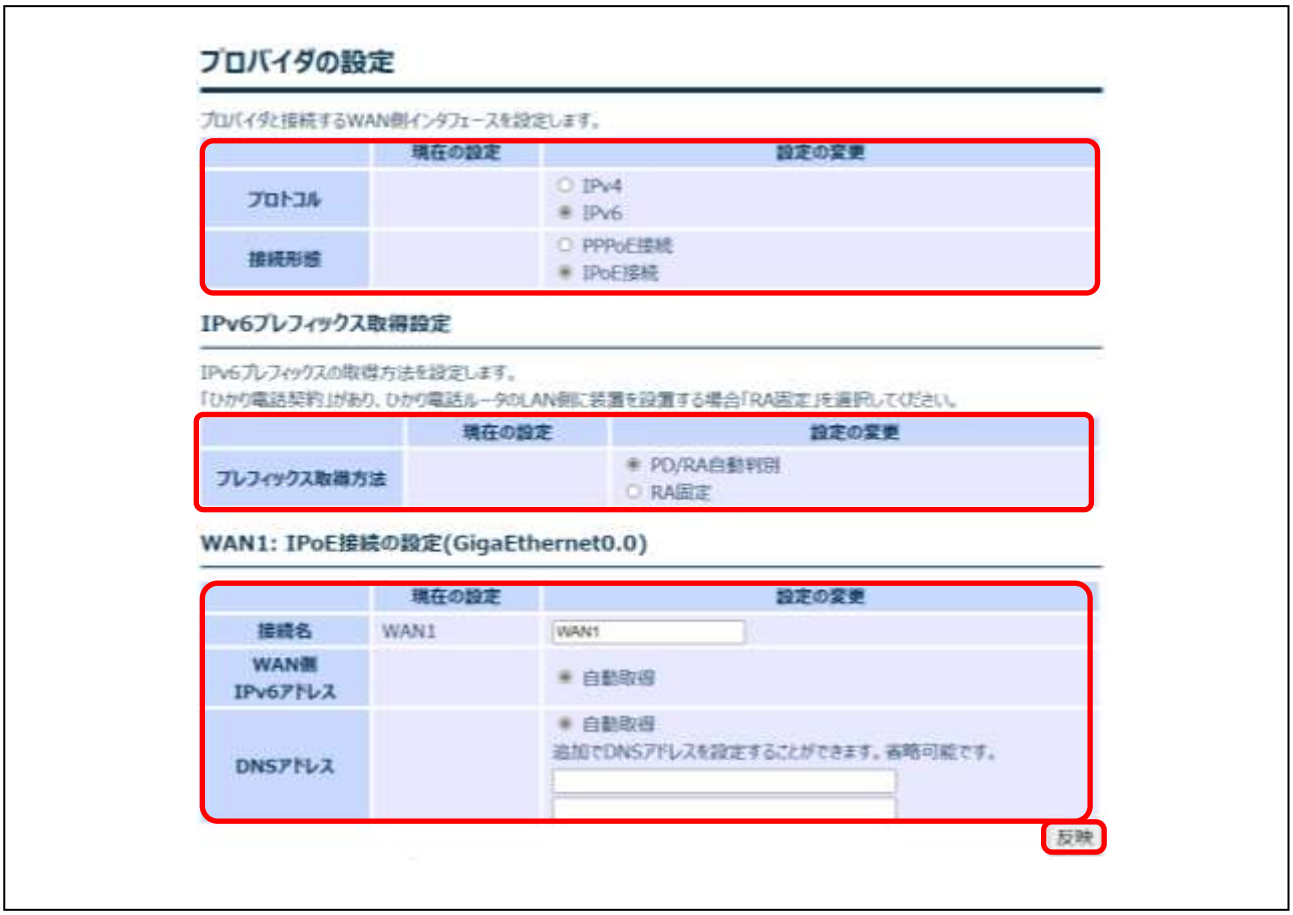
4. 詳細設定

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。 • 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。 • 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	IP 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。
⑥	NAPT	NAPT の利用を設定します。 • 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 • 特殊な環境で無い限りは、「有効」に設定してください。

IPv6、PPPoE 接続の場合(フレッツ光回線利用の場合)

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。 • 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) • 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。 • 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 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。

IPv6、IP 接続の場合(ケーブルテレビ回線利用の場合)

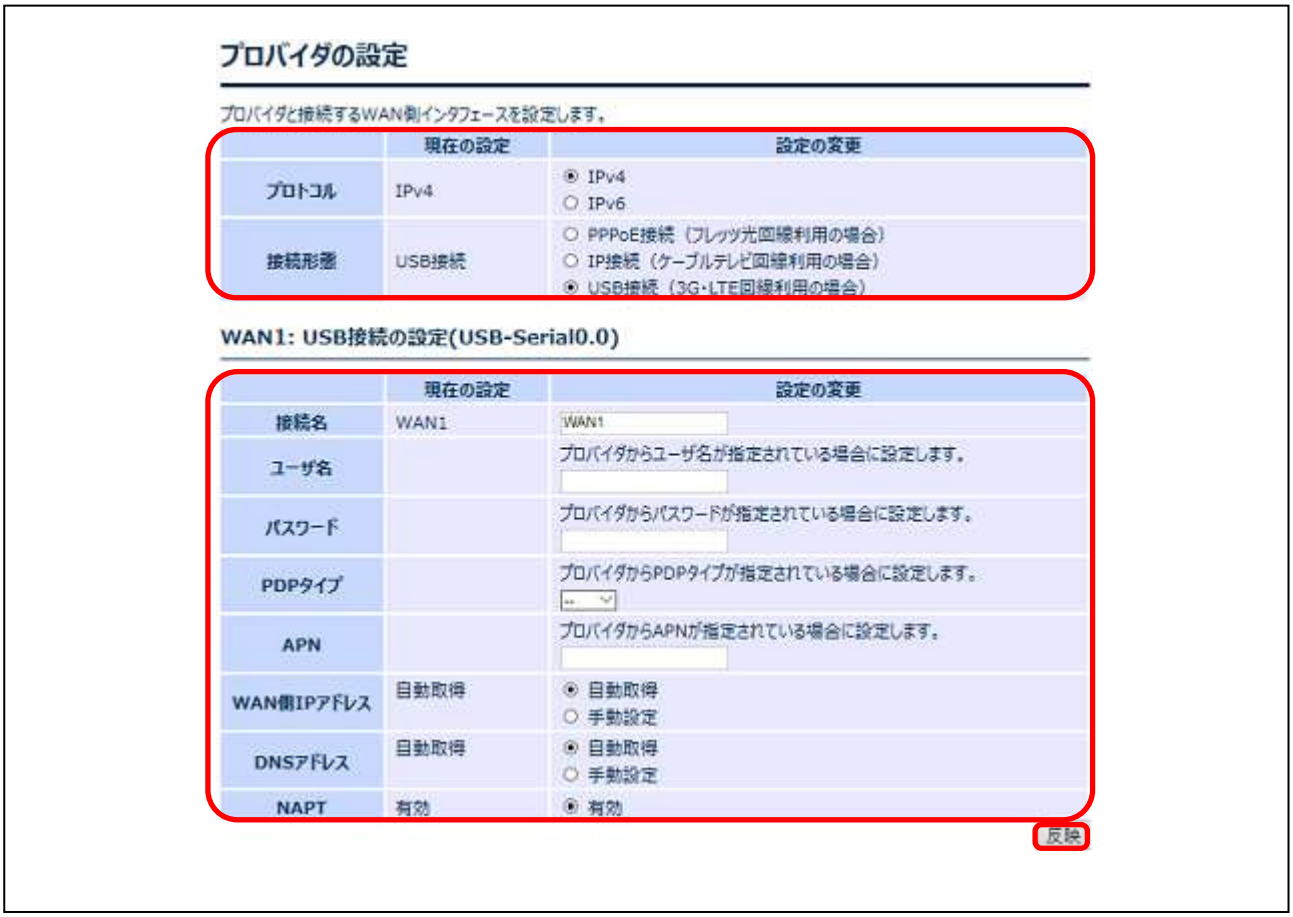


番号	項目	内容
①	プロトコル	「IPv6」を選択します。
②	接続形態	「IPoE 接続」を選択します。
③	プレフィックス取得方法	RA 固定とPD/RA 自動判別のいずれかを選択します。
④	接続名	接続名を識別するための名称を入力します。 ・ 任意の接続名を付けることができます。 ・ 半角英数字で 1～79 文字まで入力できます。 ・ 初期値は「WAN1」です。
⑤	WAN 側 IPv6 アドレス	WAN 側 IPv6 アドレスは常に「自動取得」です。設定を変更することはできません。
⑥	DNS アドレス	PPPoE 接続の DNS サーバのアドレスを設定します。「自動選択」の他、DNS 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



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。 • 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。 • 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。 • 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。 • 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。 • 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。
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。 • 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。
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) 設定が反映されたことを確認します。

4.3.2 静的 NAPT の設定

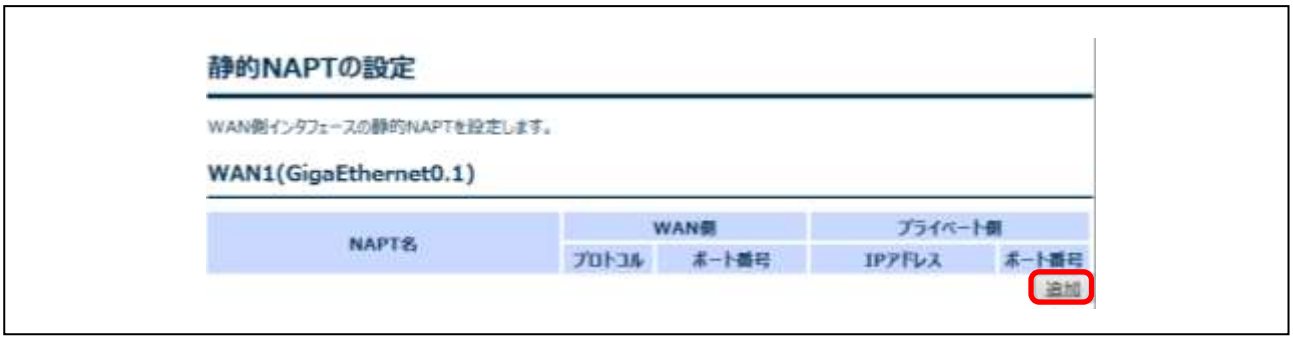
WAN 側インタフェースに静的 NAPT を設定します。

メモ 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。

(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。

メモ 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。

ポート番号指定の場合

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。

(5) 設定が追加されたことを確認します。

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。

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。

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。

メモ 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


■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
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。

(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。

メモ 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。

メモ 「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。

(4) 各項目を設定し、[反映]ボタンをクリックします。

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。 • 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。 • 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。 • 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。 • 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。 注意 • 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。 • 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。 • 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。 注意 • 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。

(5) 設定が追加されたことを確認します。

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
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。

(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。

メモ 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。

(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。

メモ 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。

⑸　各項目を設定し、[反映]ボタンをクリックします。

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。 • 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。 • 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。 • 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。 • 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。 注意 • 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。 • 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。 • 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。 注意 • 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。 • 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。

⑸　設定が追加されたことを確認します。

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）

メモ 設定するには、「プロバイダの設定」が必要です。

メモ 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。

メモ 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。

メモ 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
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。

(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。

(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。

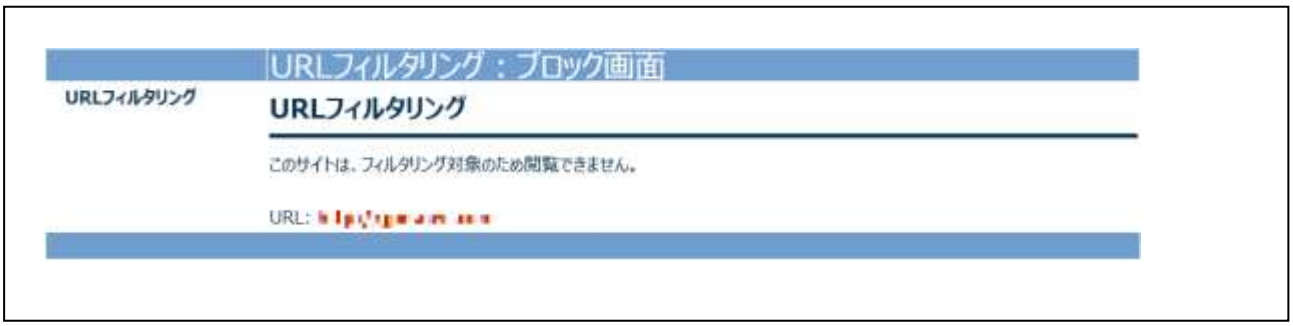
番号	項目	内容
①	番号	フィルタの番号を選択します。 • 1 から順に割り当てられます。 • 現在の設定内容と同じ番号を選択した場合は、新たに追加した内容をその順番に挿入します。
②	動作	該当の URL に対する処理動作を「透過」／「廃棄」から選択します。
③	ドメイン名 または IPv4 アドレス形式	フィルタリング対象とする宛先のドメイン名または IPv4 アドレスを設定します。 • カンマで区切って、複数設定することができます。その場合、[追加]ボタンをクリックすると、複数の番号で追加されます。

⑸ 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。

⑹ 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。

メモ 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。

メモ 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。



4.3.6 QoS の設定

QoS を設定します。

メモ 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。

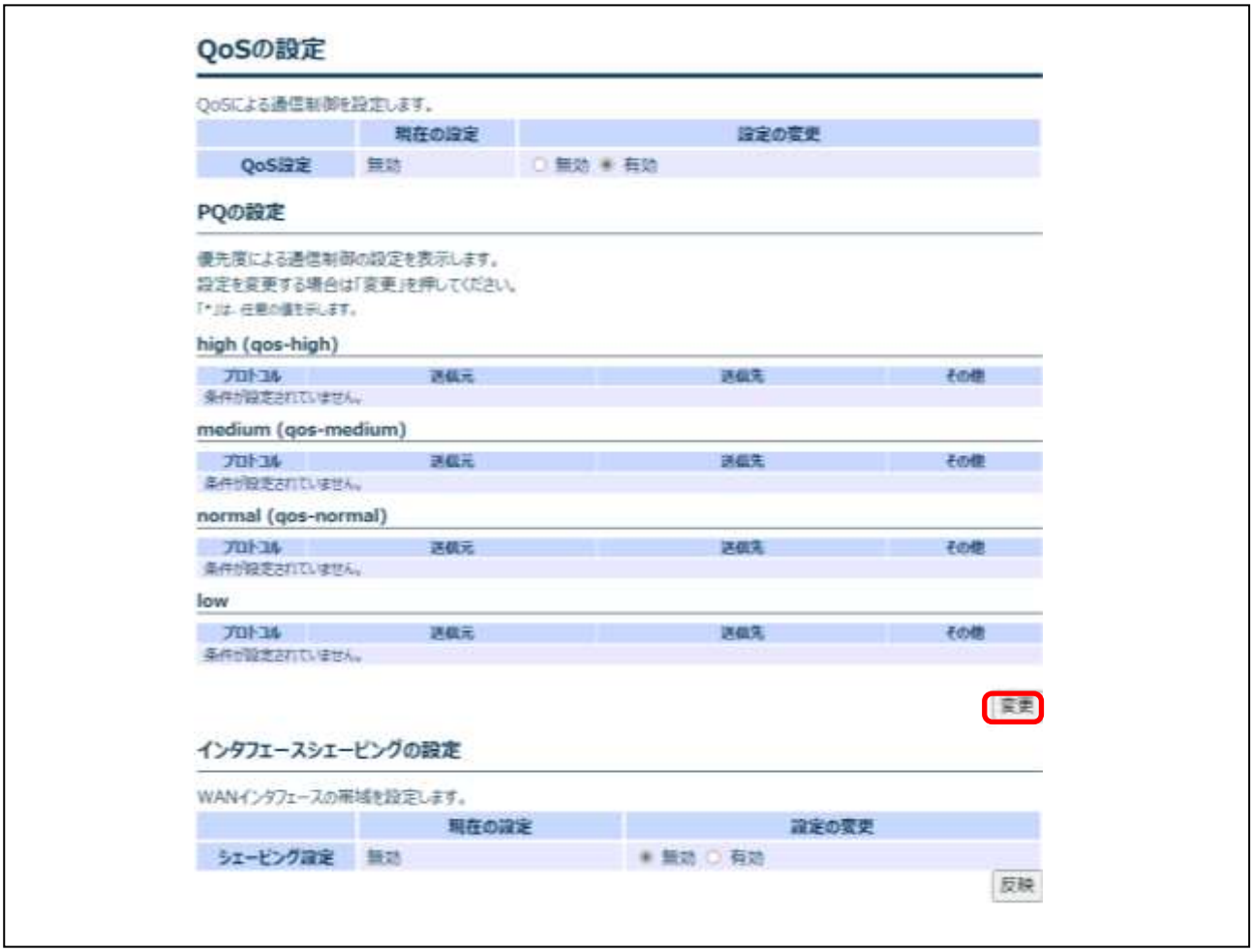
(3) QoS 設定の「有効」／「無効」を設定します。

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フェースシェーピングの設定が表示されます。

(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。

メモ PQ を利用しない場合は、PQ の設定の変更は不要です。



⑹　各項目を設定し、[追加]ボタンをクリックします。

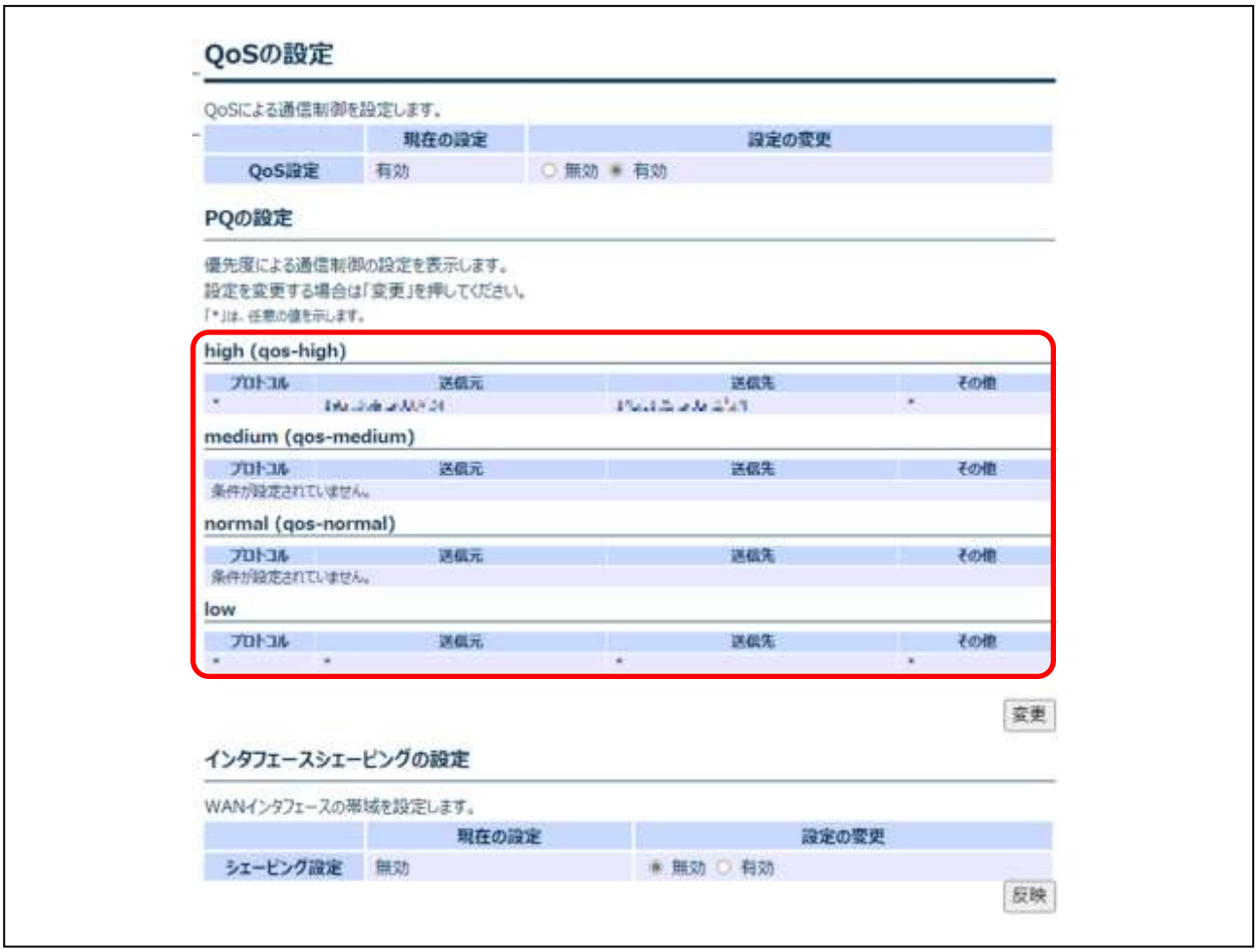
メモ　PQ を利用しない場合は、PQ の設定の変更は不要です。

4. 詳細設定

番号	項目	内容
①	優先度	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。 • 優先度は、[high]、[medium]、[normal]から選択します。 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。
②	プロトコル	プロトコルをプルダウンメニューから選択します。 • 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	送信元の IPv4 アドレスを設定します。 • 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。 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。 • 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	送信先の IPv4 アドレスを設定します。 • 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。 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。 • 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	対象となる ToS 値を設定します。 • 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。

(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。

(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。

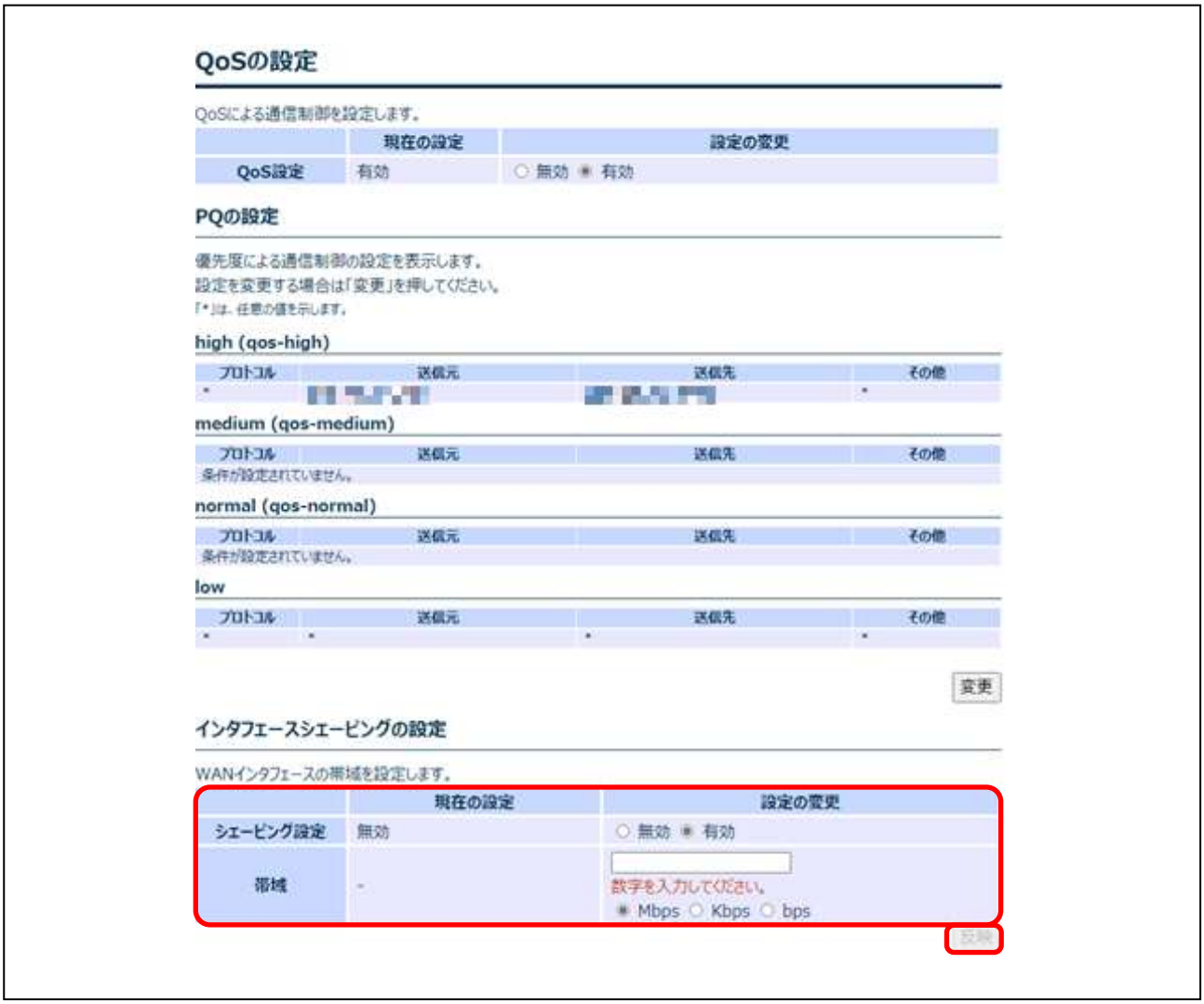


⑼ インタフェースシェーピングを設定する場合は、シェーピング設定の「無効」／「有効」を設定し、[反映]ボタンをクリックします。

メモ 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。

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。

(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。



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。

（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。

4.3.7 通信セキュリティの設定

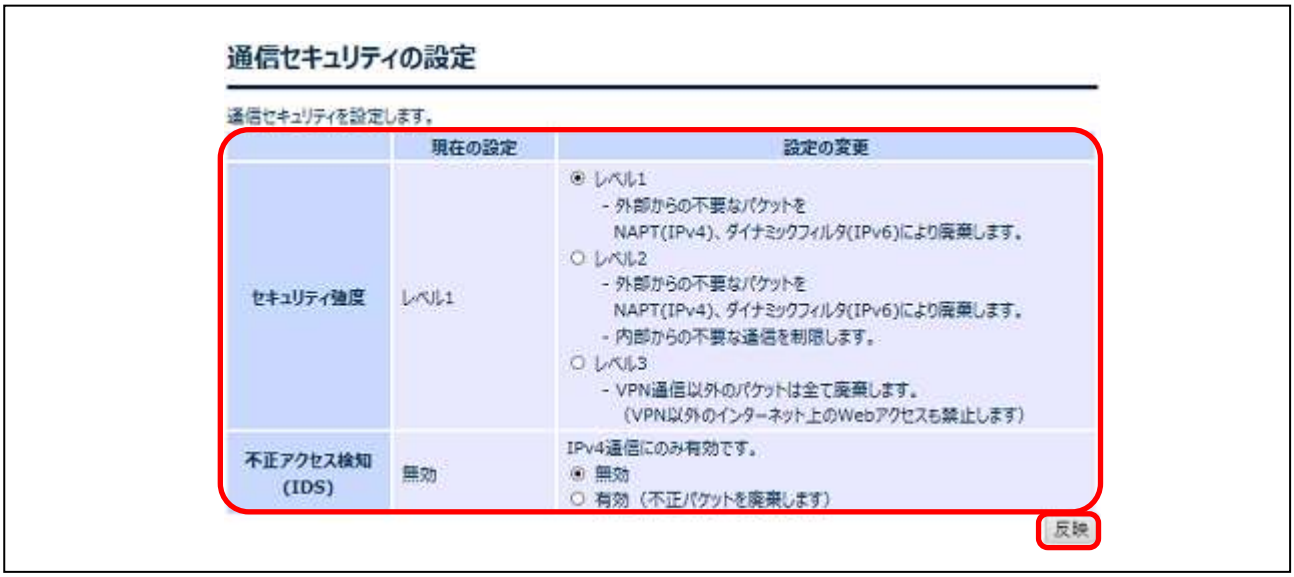
通信セキュリティを設定します。

メモ 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。

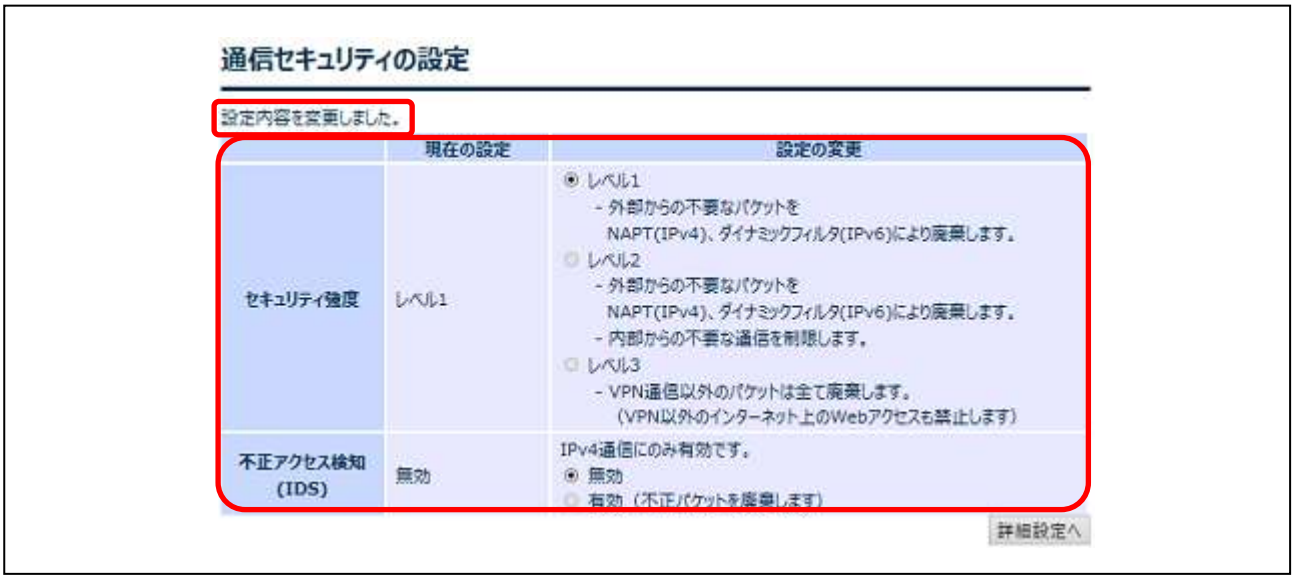
(3) セキュリティ強度や不正アクセス検知(IDS)の「有効」／「無効」を設定し、[反映]ボタンをクリックします。



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。 • 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。
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。

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

(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。



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。

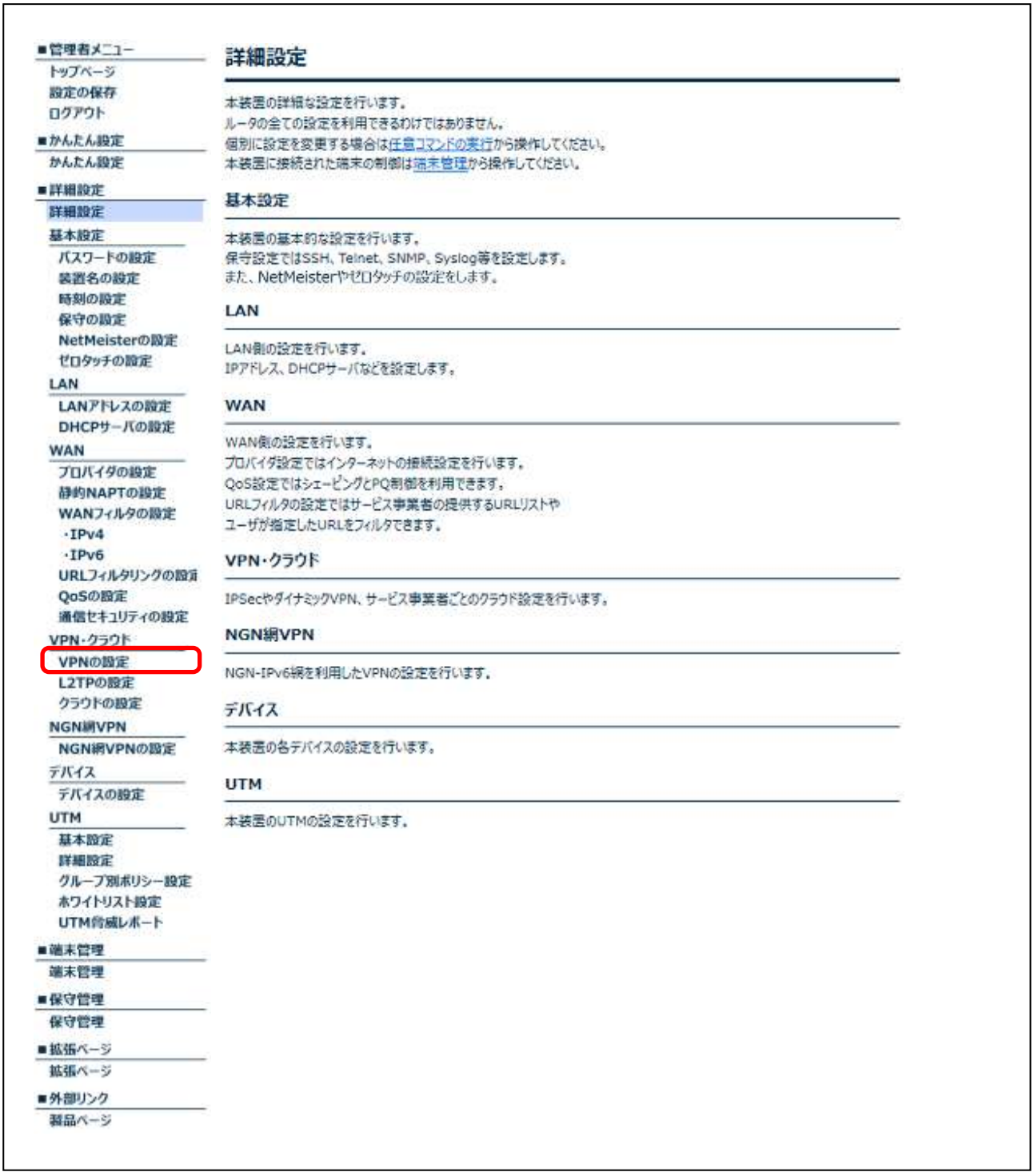
メモ 設定するには、「プロバイダの設定」が必要です。

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
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。

(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。

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。

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。

IPsec の場合

メモ 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。

メモ 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。

メモ 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。

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。

IP トンネルの場合

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。

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。

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 • 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。 • 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。 • 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。

4.4.2 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。

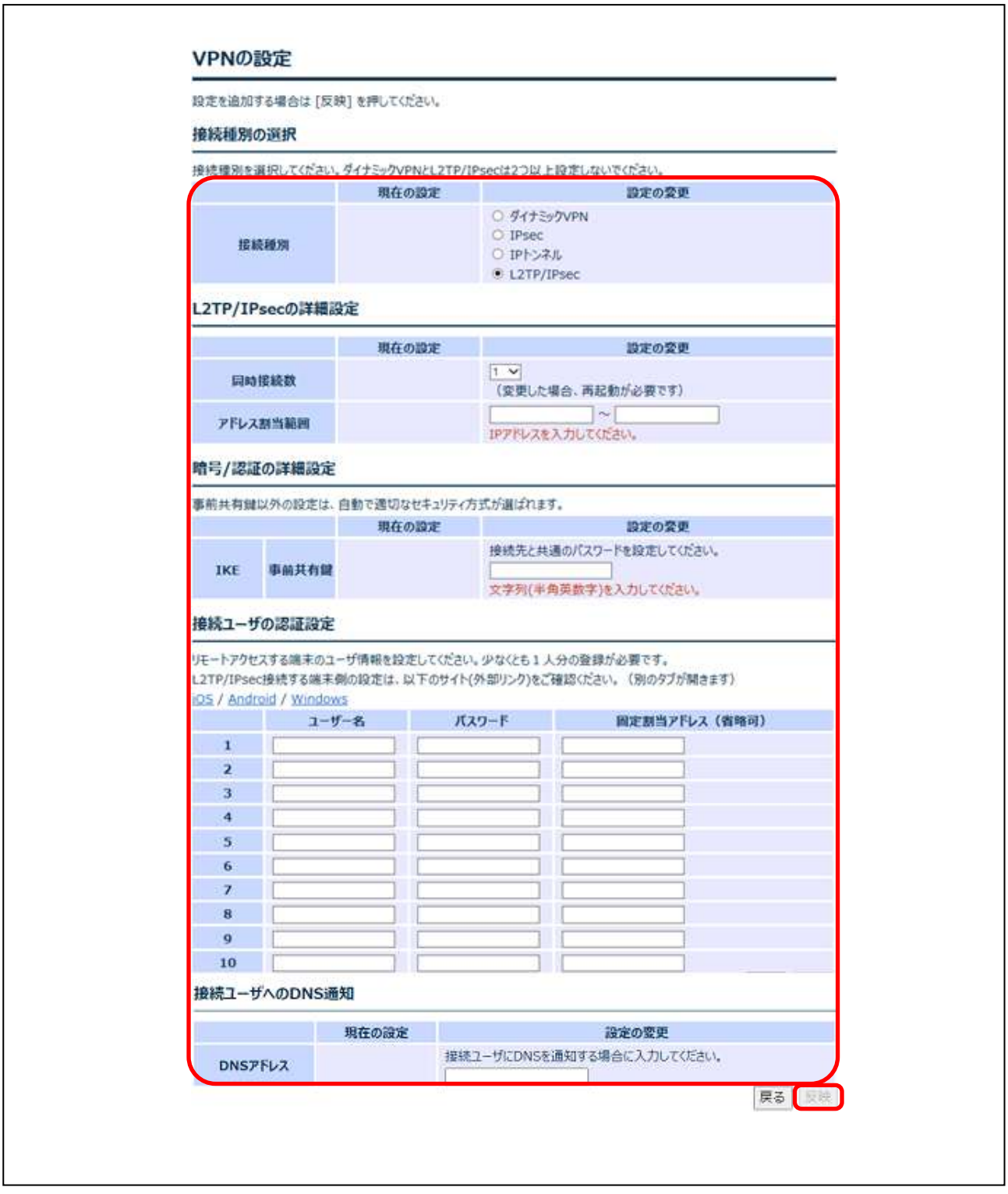
メモ L2TP/IPsec は 2 つ以上設定しないでください。

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。

(3) 各項目を設定し、[反映]ボタンをクリックします。



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 • 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。 • 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。 • 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。

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。

4.4.3 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。

メモ 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
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。

(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。

4. 詳細設定

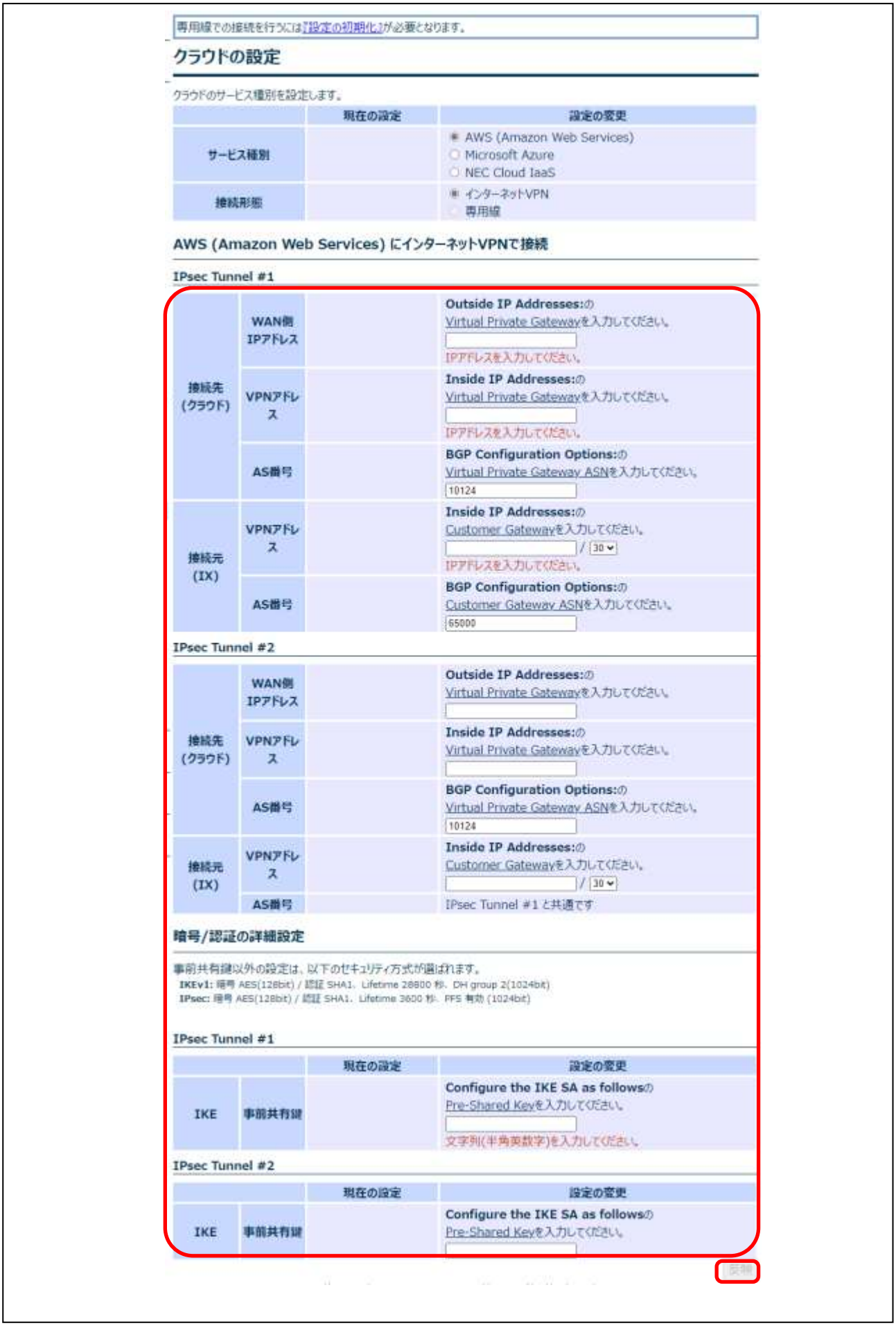
番号	項目	内容
①	サービス種別	「AWS (Amazon Web Services)」を選択します。
②	接続形態	「専用線」を選択します。
③	接続先(クラウド) WAN 側 IP アドレス	接続先の IP アドレスを入力します。
④	接続先(クラウド) AS 番号	接続先の BGP ピアの AS 番号(1～65534)を入力します。 • 初期値は「10124」です。
⑤	接続先(クラウド) BGP パスワード	接続先と共通のパスワードを設定します。 • 半角英数字で 1～218 文字まで入力できます。
⑥	接続元(IX) WAN 側 IP アドレス	接続元の IP アドレスを入力します。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

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
AWS (Amazon Web Services)
Microsoft Azure
NEC Cloud IaaS
接続形態
インターネットVPN
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。
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。
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。
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。
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。
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。
VPNアドレス
Inside IP Addresses:の
Virtual Private Gateway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。
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。
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。
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。

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(IX) 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(IX) 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。 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。 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。 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(IX) VPN アドレス	IPsec Tunnel#2 の Inside IP Addresses:の Customer Gateway を入力します。 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。

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

<table>
<tr>
<td>⑬</td>
<td>IPsec Tunnel#2
IKE 事前共有鍵</td>
<td>IPsec Tunnel#2 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>
<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>
メモ
• 複数 VPN を使用しない場合は、本設定は不要です。</td>
</tr>
</table>

Microsoft Azure に接続する場合

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。

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

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。

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

⑸　「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。

4.5 NGN 網 VPN の設定

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。

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。

メモ 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。

メモ 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
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

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。

メモ 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

メモ 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。

メモ 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。

(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。

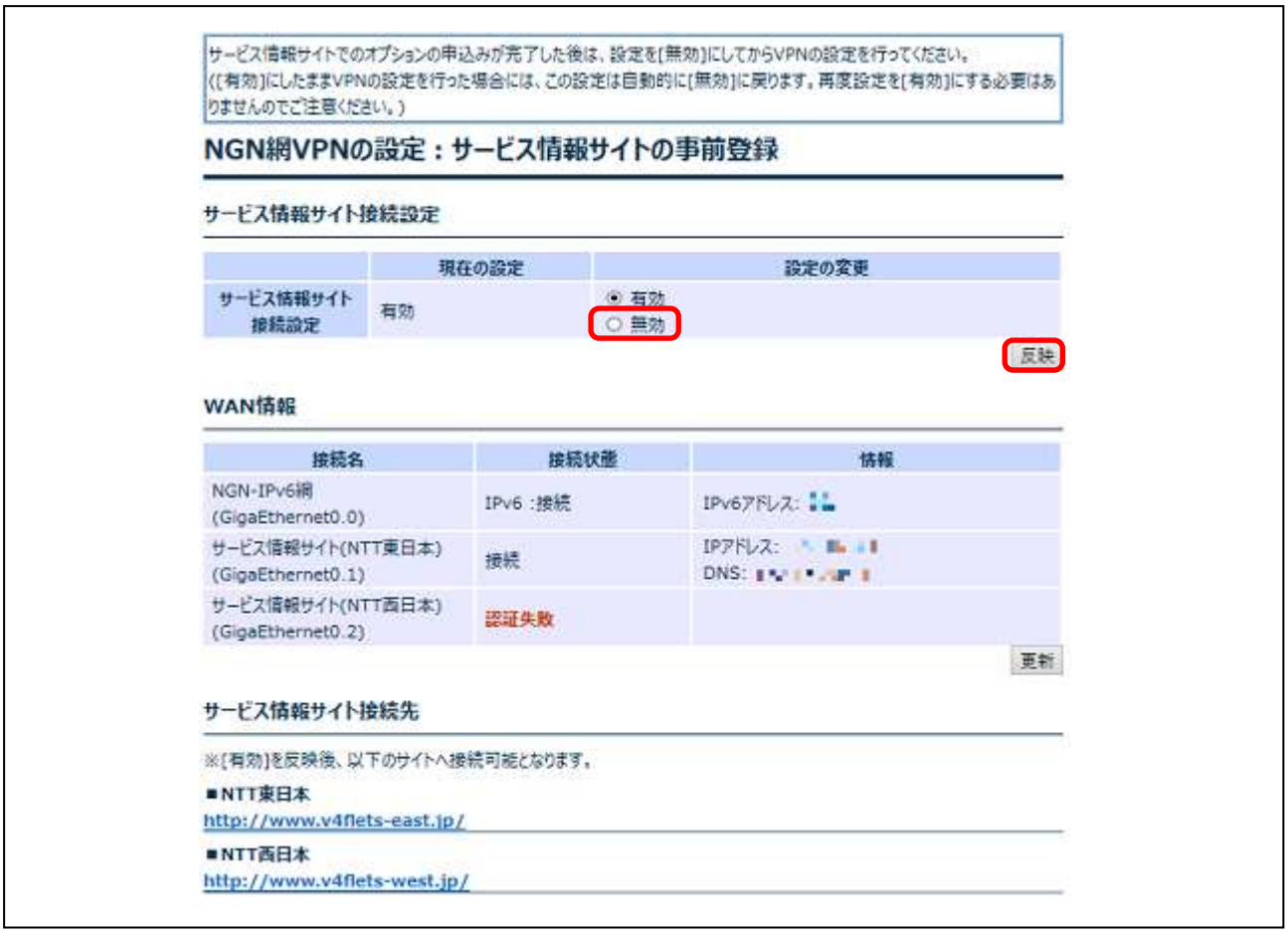
(3) サービス情報サイトにアクセスできるようにするため、サービス情報サイト接続設定の有効を選択し、[反映]をクリックします。

(4) 設定が反映されたことを確認します。

メモ 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。

⑸ 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。

⑹ 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。



⑺ 設定が反映されたことを確認します。

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。

:

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 ・ 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) NGN 網 VPN 設定の VPN の設定を行います。

センタの設定の場合

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

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。

(3) NGN 網 VPN 設定の NetMeister ダイナミック DNS の設定を行います。

：

：

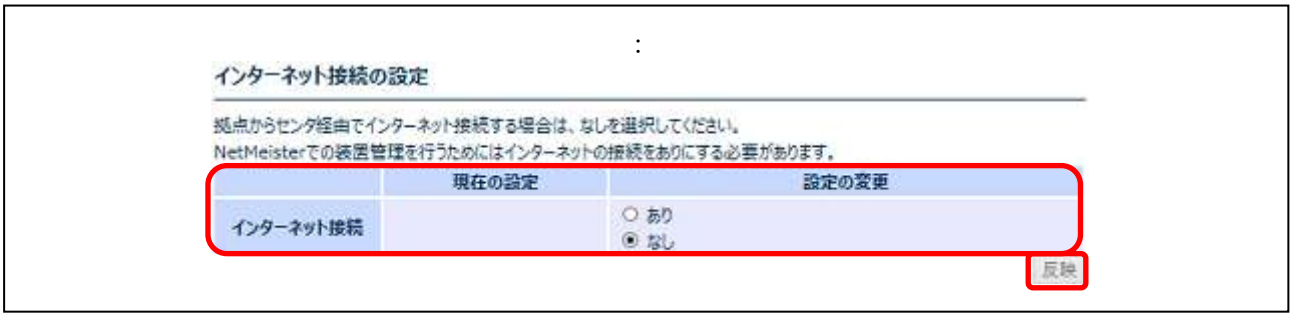
番号	項目	内容
①	ホスト名(装置名)	装置のホスト名を設定します。設定したホスト名は NetMeister に通知されます。 ・ 半角英数字または-(ハイフン)で 2～63 文字まで入力できます。 メモ ・ 大文字は、小文字に変換して NetMeister に通知されます。 注意 ・ ホスト名の先頭と最後には-(ハイフン)を利用することができません。
②	サイト名(拠点名)	NetMeister に通知するサイト名を設定します。 ・ 半角英数字または-(ハイフン)で 2～31 文字まで入力できます。 メモ ・ 大文字は、小文字に変換して NetMeister に通知されます。 注意 ・ サ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	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。 ・ 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 ・ 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。 ・ 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 ・ 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) 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

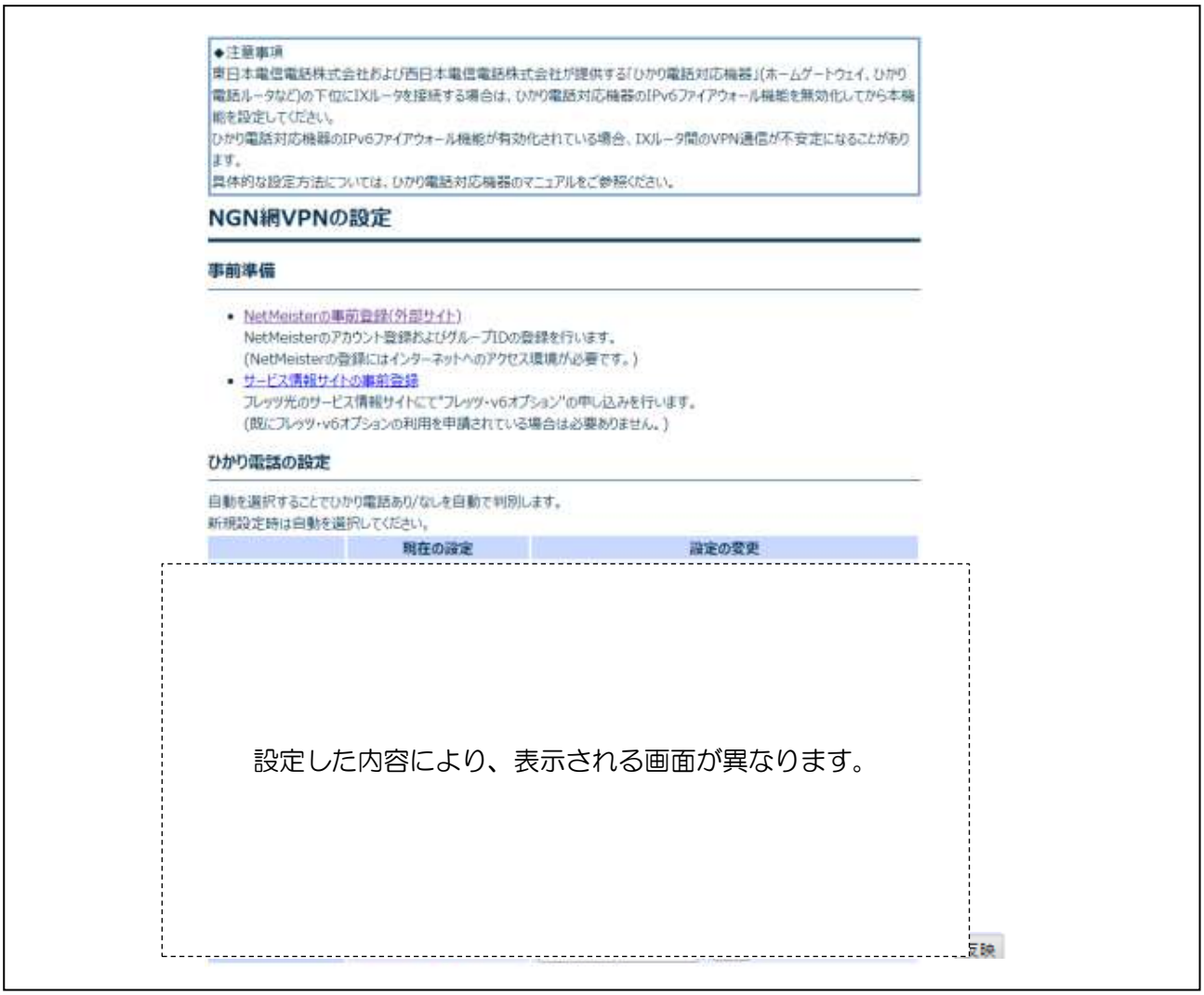
番号	項目	内容
①	インターネット接続	[あり]を選択します。 メモ ・ インターネット接続[あり]の場合、NetMeister によるダイナミック DNS を利用可能となります。また、NetMeister による装置管理も利用可能となります。
②	ユーザ名	プロバイダから通知されているユーザ名を設定します。 (フレッツの場合、通常はユーザ名には@を含んでいます) ・ 半角英数字で 1～59 文字まで入力できます。
③	パスワード	プロバイダから通知されているパスワードを設定します。 ・ 半角英数字で 1～79 文字まで入力できます。 注意 ・ 大文字／小文字は区別されます。

インターネット接続[なし]の場合



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。

⑸　設定が反映されたことを確認します。



4.6 デバイス

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。

4.6.1 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
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。

(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。

(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。

メモ 回線速度は、Ethernet デバイス選択時のみ表示されます。

メモ 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。

(5)　設定が反映されたことを確認します。

メモ 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。

4.7 UTM

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。

4.7.1 トップページ

UTM の状態を確認します。

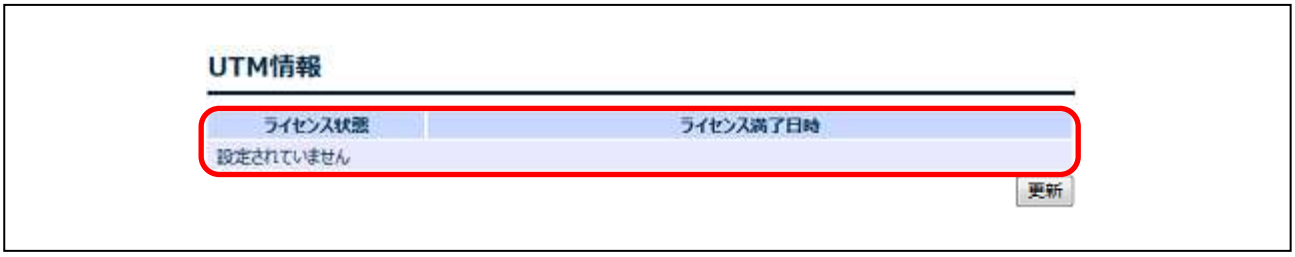
注意 UTM を利用する場合、インターネット上にあるライセンスサーバでライセンス認証を行ったり、シグネチャサーバとの通信、アンチウイルスサーバおよび URL フィルタリングデータベースサーバで通信のチェックを行ったりするため、インターネットへの経路到達性が必須となります。あらかじめ、インターネットへ接続するための設定を行ってください。

(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。

(2) UTM 情報より、UTM の状態を確認します。

メモ [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）

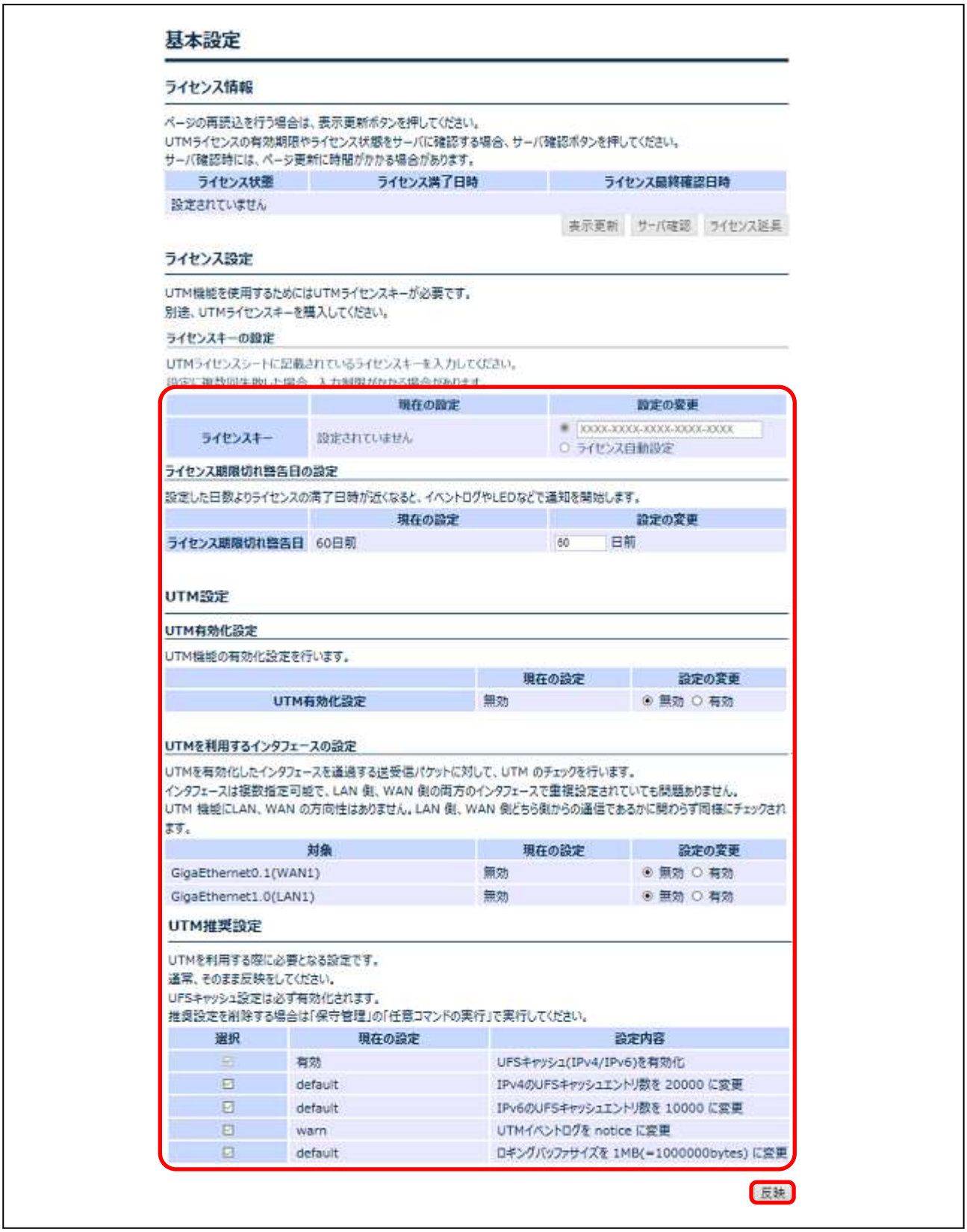
上記のように接続が確認できない場合、更新ボタンを押下いただき、正常状態になるかご確認ください。正常状態にならない場合は、インターネットに接続されていることと「ライセンスキー」「UTM 機能の有効化」が正しく設定されていることを確認してください。

4.7.2 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。

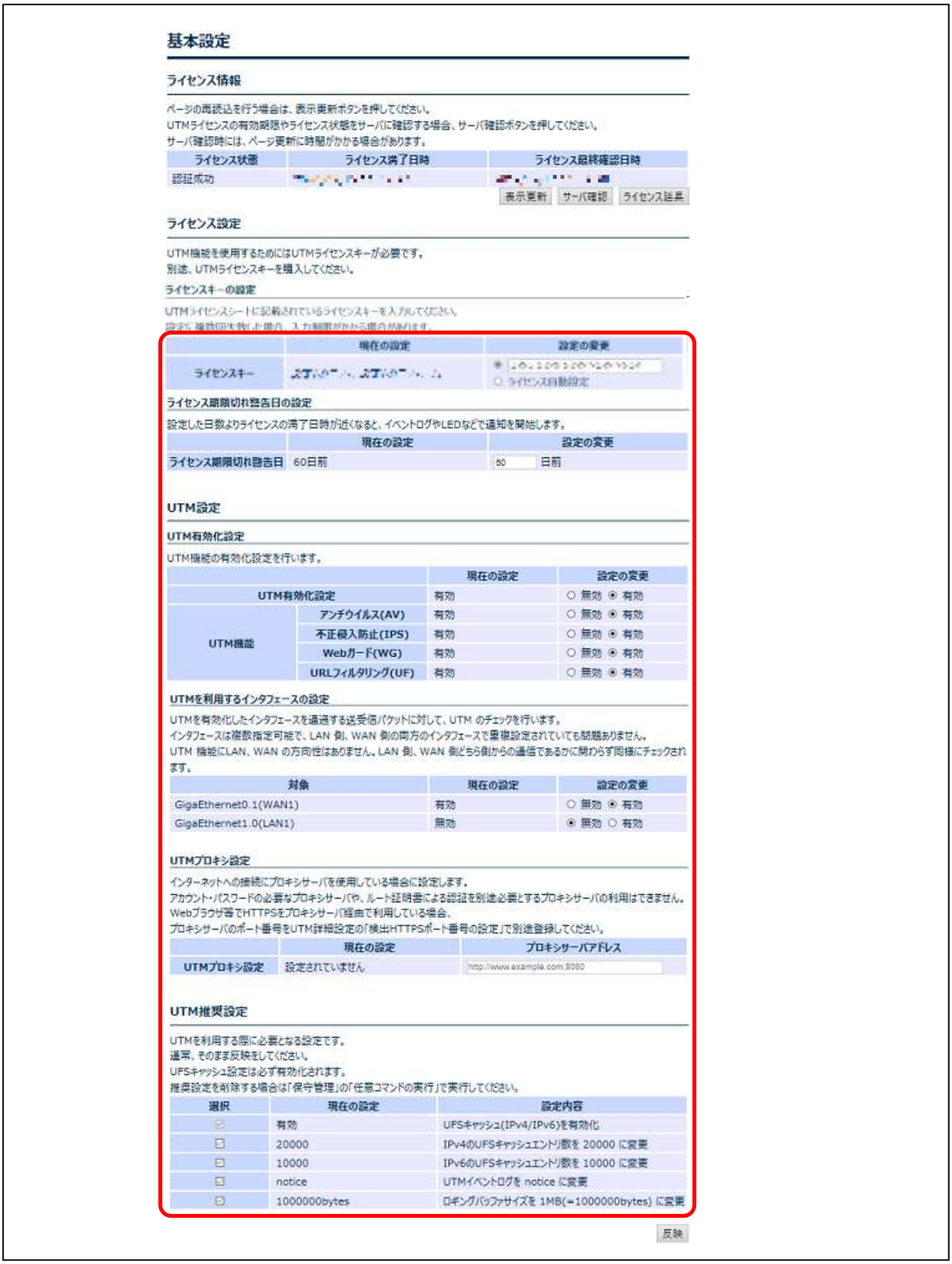
(2) 各項目を設定し、[反映]ボタンをクリックします。



4. 詳細設定

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。 ・ 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。 ・ 半角数字で 1～1000 の間で入力できます。 メモ ・ 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 などで通知を開始します。
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。 メモ ・ 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。 ・ http://FQDN 名/形式で、214 文字まで入力できます。 メモ ・ 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。 ・ 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。

(3)　設定が反映されたことを確認します。



(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。

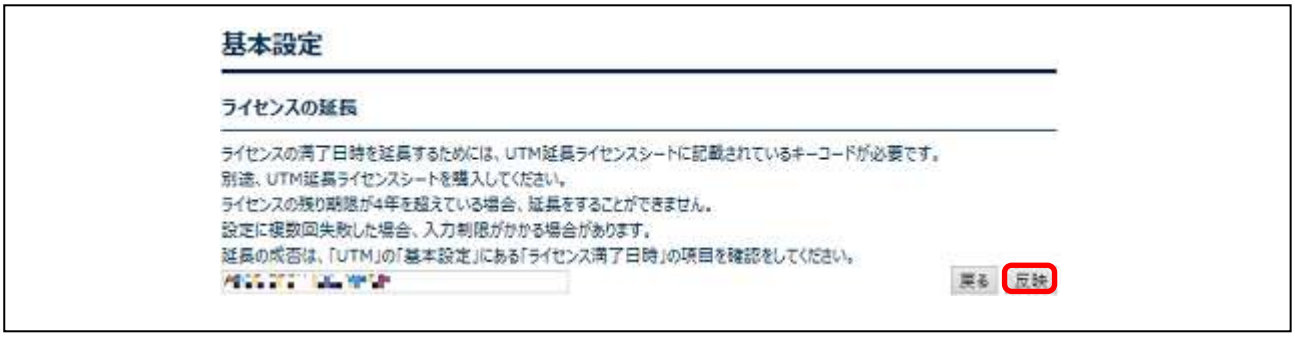
(6) UTM ライセンスの有効期限を延長する場合は、[ライセンス延長]をクリックします。

メモ 別売の延長ライセンスを購入する必要があります。

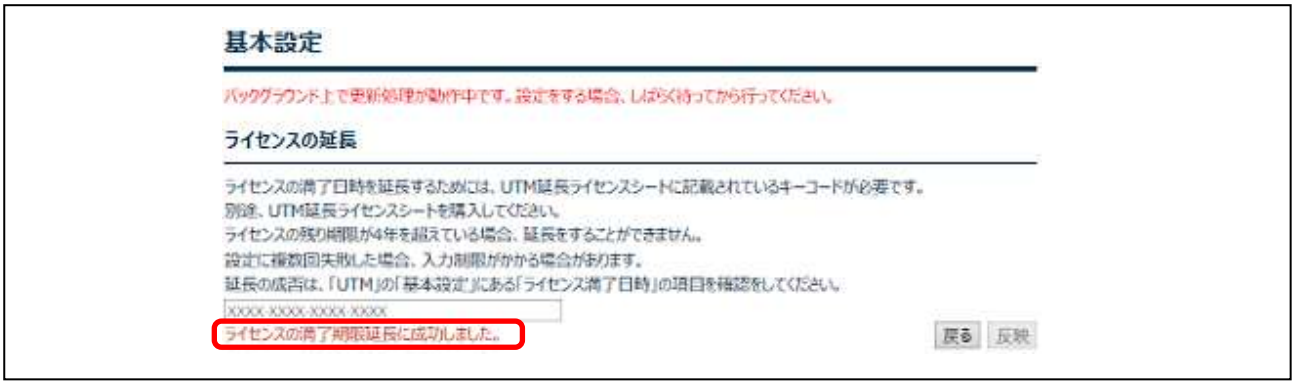
メモ サーバで管理されている情報を更新するため、サーバとの通信が確立している必要があります。

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。



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。



[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。

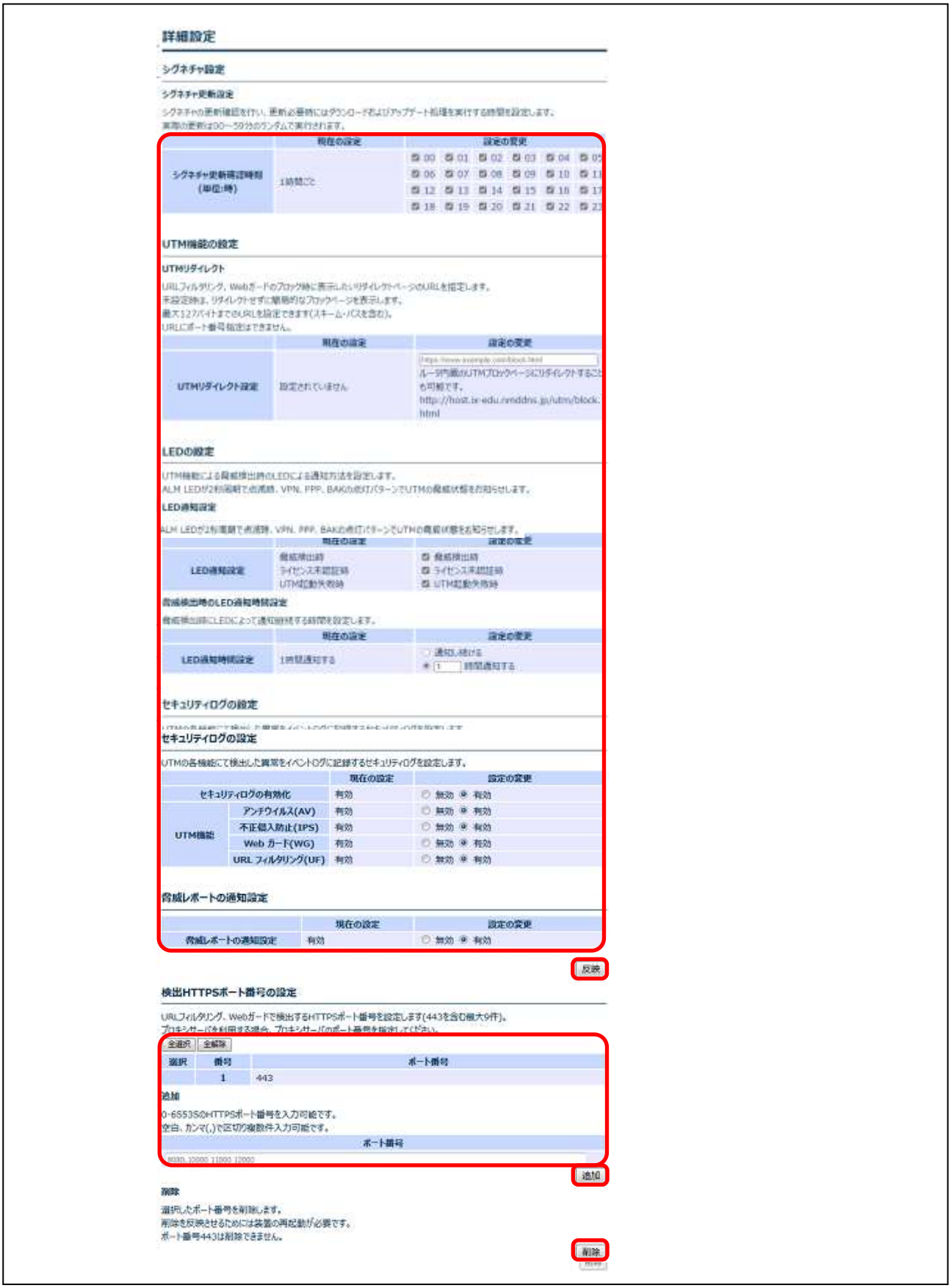
4.7.3 UTM の詳細設定

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。

⑵ 各項目を設定し、[反映]ボタンをクリックします。

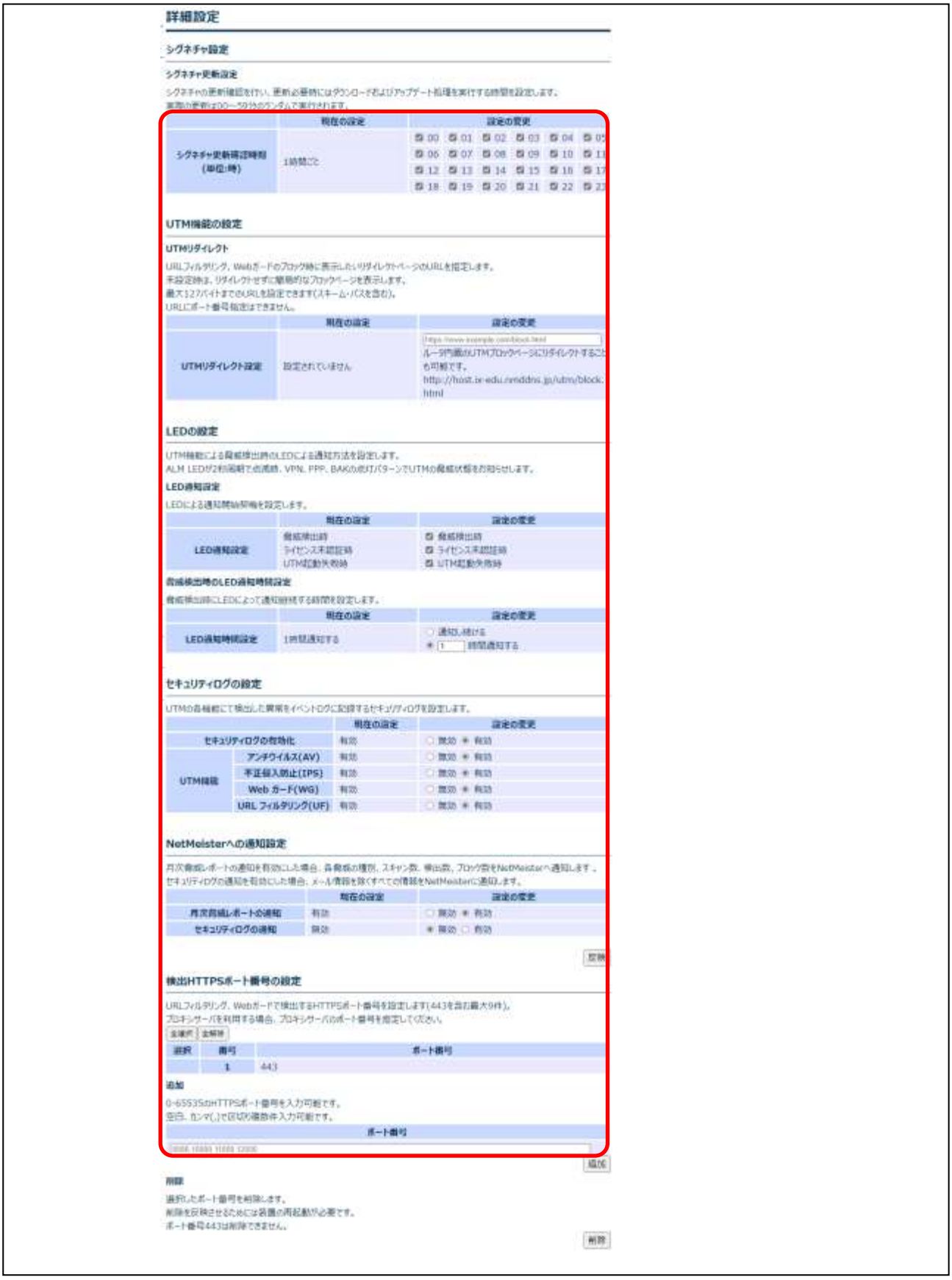
注意 [反映]をクリックする前に検出 HTTPS ポート番号の設定の[追加]または[削除]をクリックした場合、それまで入力した値はリセットされます。



4. 詳細設定

番号	項目	内容
①	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。 ・ 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。 メモ ・ 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	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。 ・ 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	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。 ・ 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。 メモ ・ 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	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。 ・ 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。 メモ ・ 443 を削除することはできません。 注意 ・ [反映]をクリックしなくても設定されます。

(3) 設定が反映されたことを確認します。



4. 詳細設定

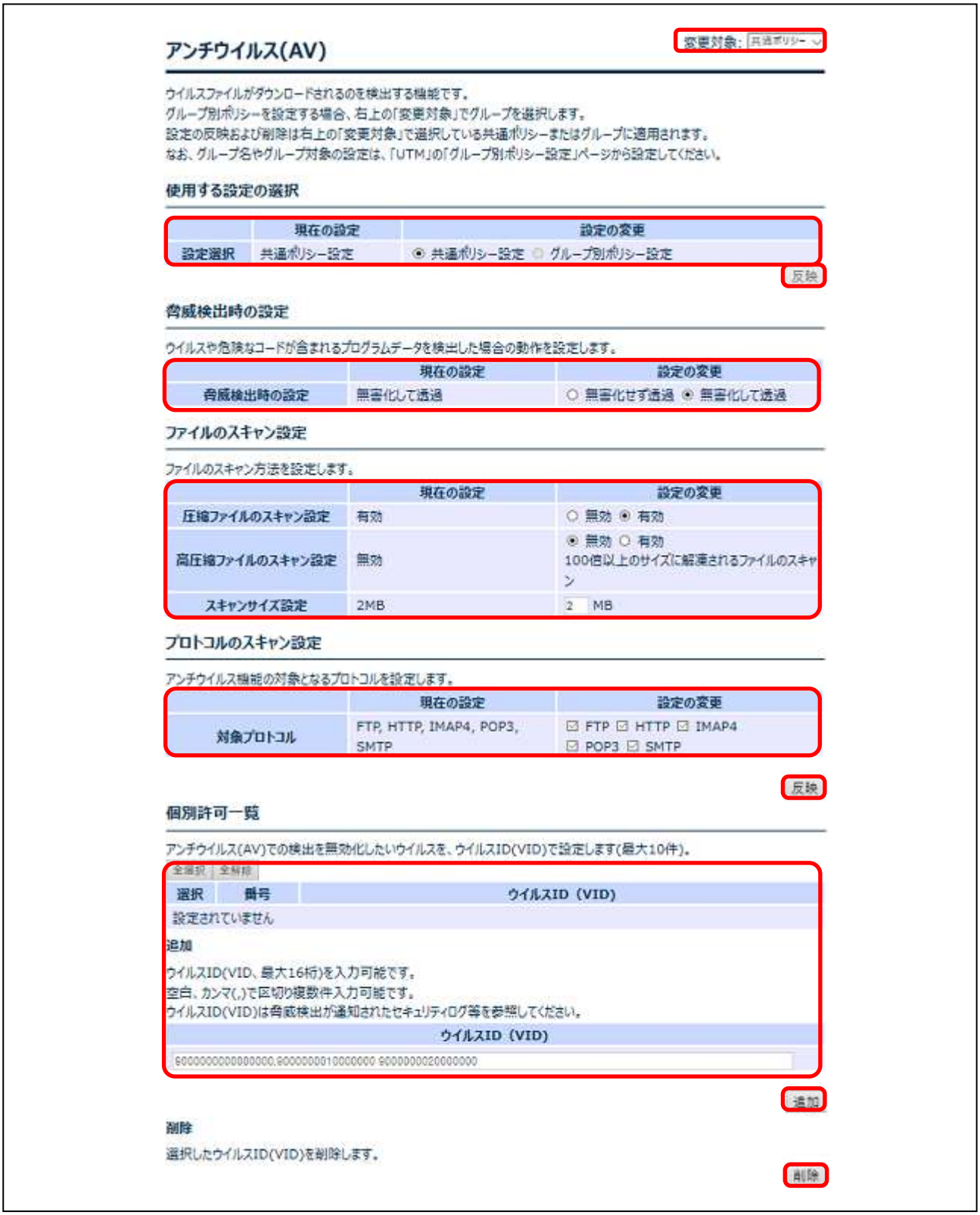
4.7.4 アンチウイルス(AV)の設定

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。

(2) 各項目を設定し、[反映]ボタンをクリックします。

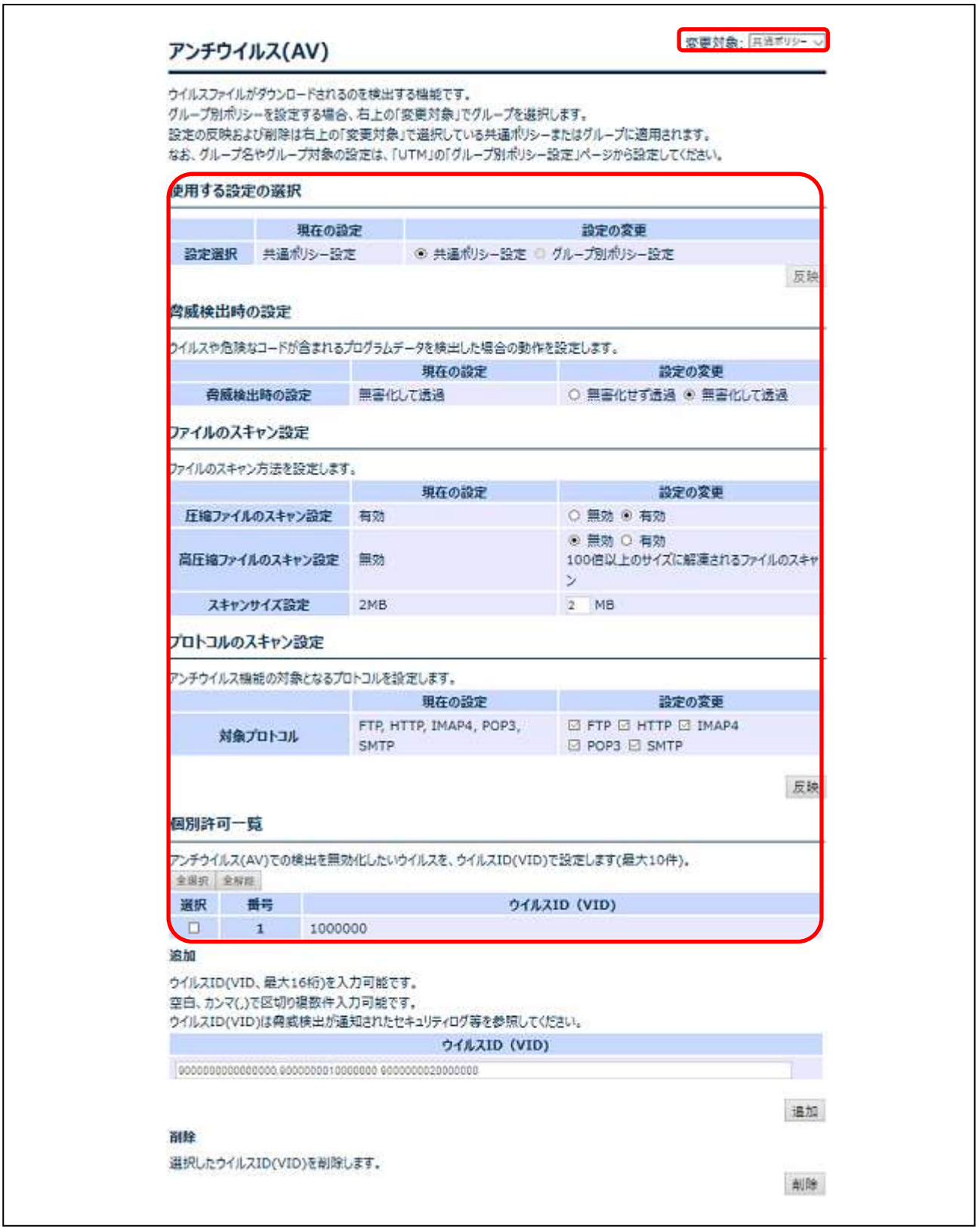
注意 [反映]をクリックする前に個別許可一覧の[追加]または[削除]をクリックした場合、それまで入力した値はリセットされます。



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 • 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	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。 メモ • 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	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。 • 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	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。 メモ • 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	選択したウイルス ID をすべて解除します。 メモ • 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	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。 ウイルスID単位で、個々に選択します。 メモ • 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	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。 • 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。 メモ • 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。

(3) 設定が反映されたことを確認します。

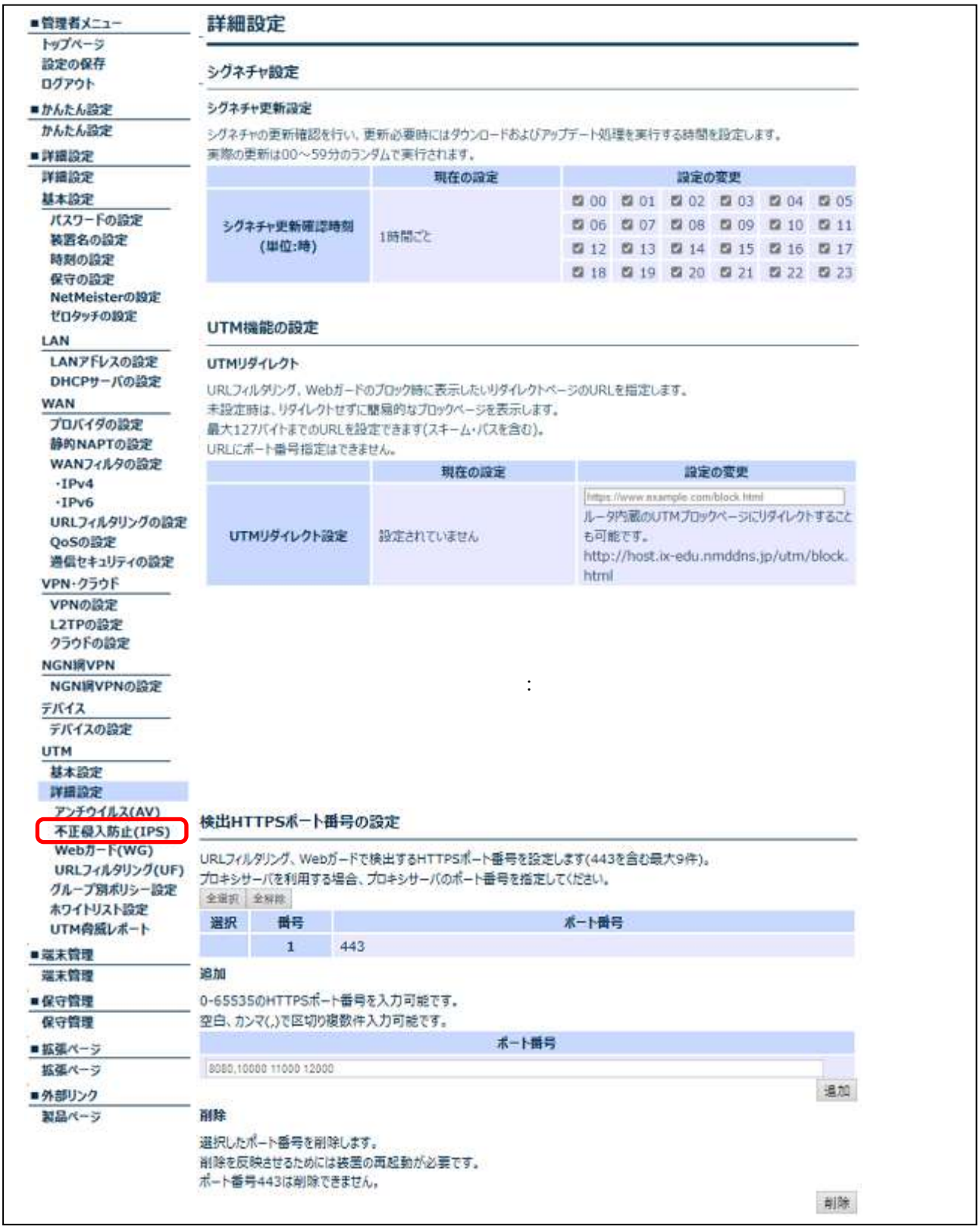


4. 詳細設定

4.7.5 不正侵入防止(IPS)の設定

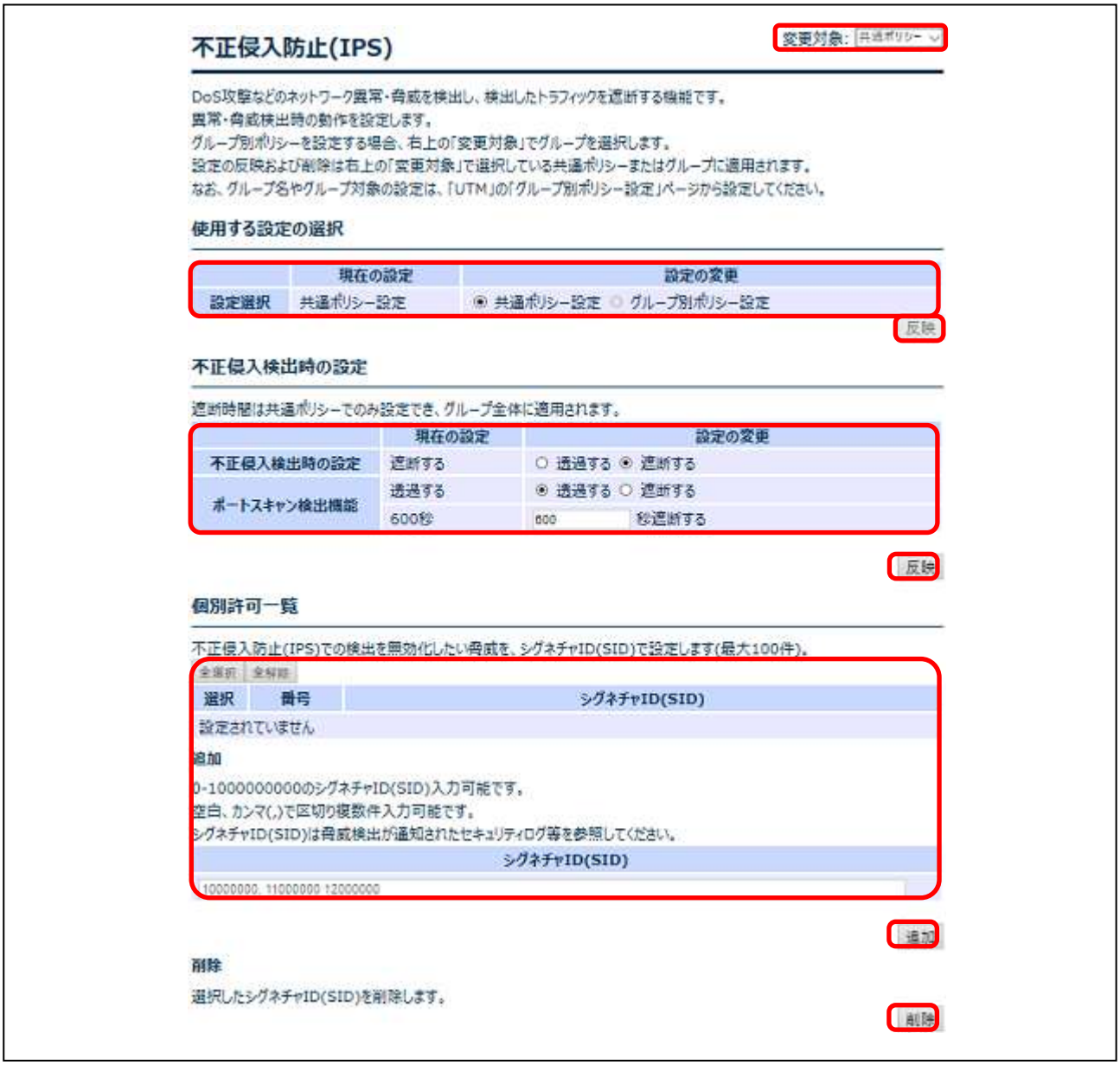
不正侵入防止（Intrusion Prevention System）を設定します。

(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。



⑵　各項目を設定し、[反映]ボタンをクリックします。

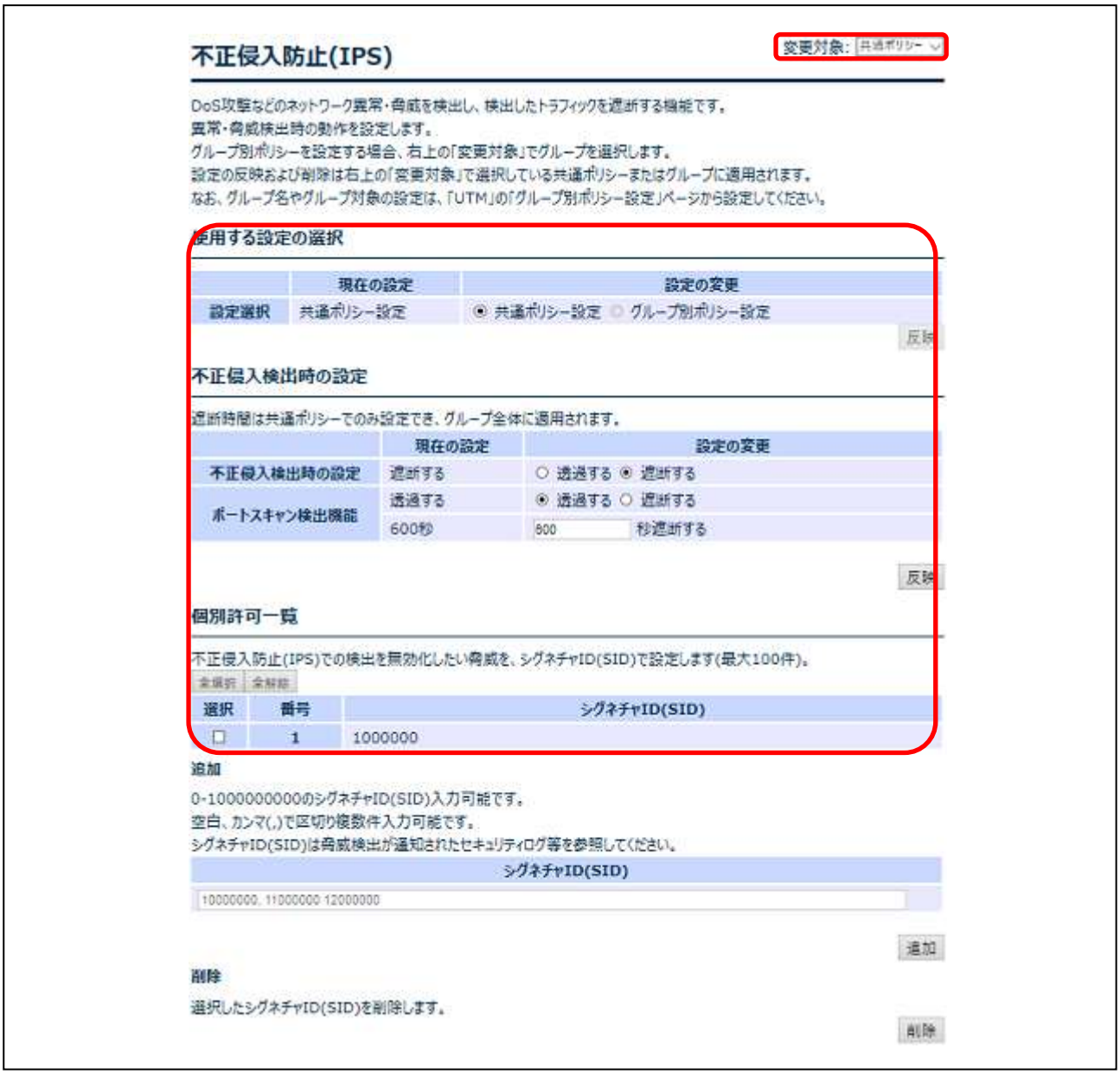
注意　[反映]をクリックする前に個別許可一覧の[追加]または[削除]をクリックした場合、それまで入力した値はリセットされます。



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 • 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	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。 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。 ・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	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。 メモ • 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	選択したシグネチャ ID をすべて解除します。 メモ • 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	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。 シグネチャID単位で、個々に選択します。 メモ • 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	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。 • 最大 100 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。 メモ • 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。

(3) 設定が反映されたことを確認します。

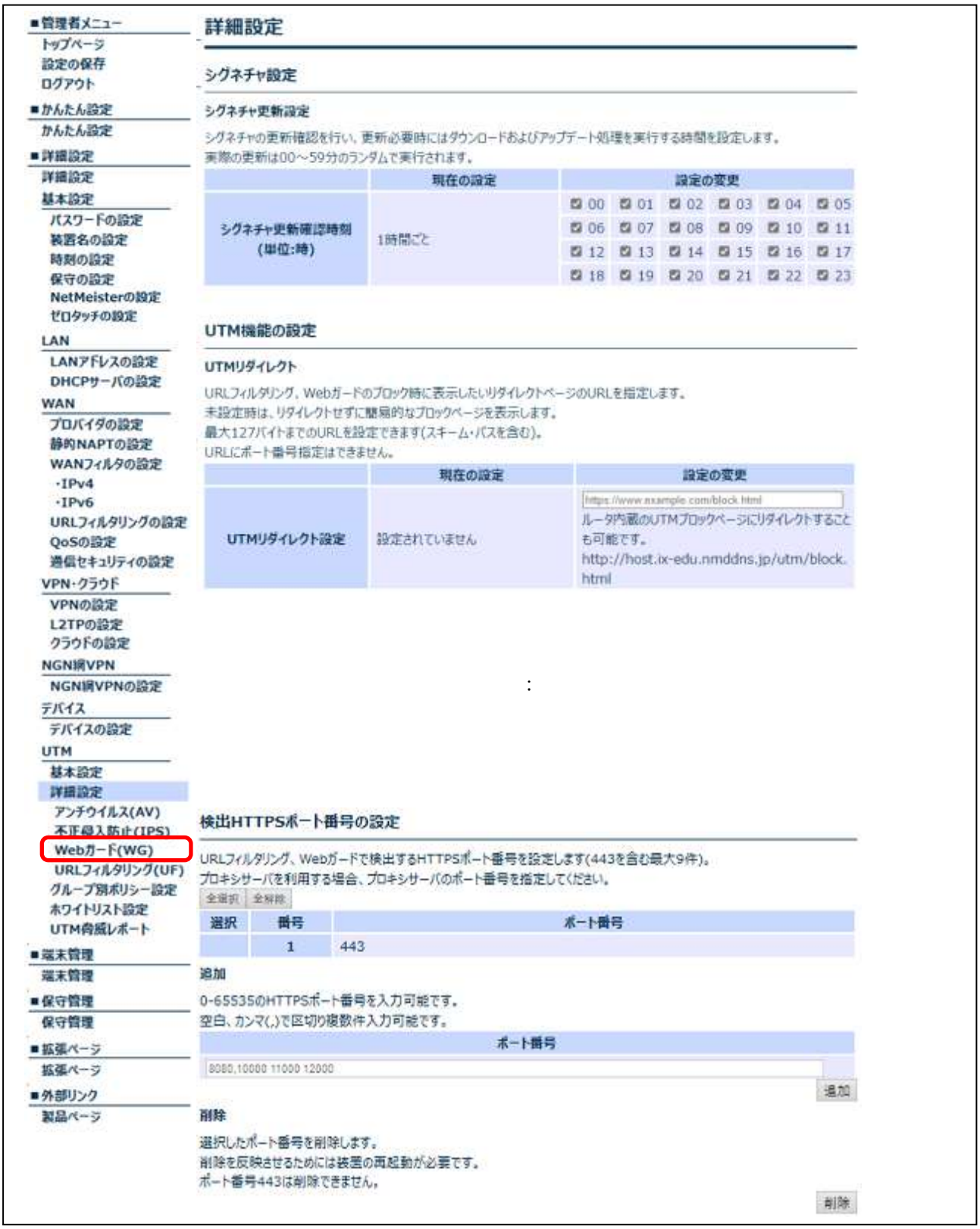


4. 詳細設定

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。



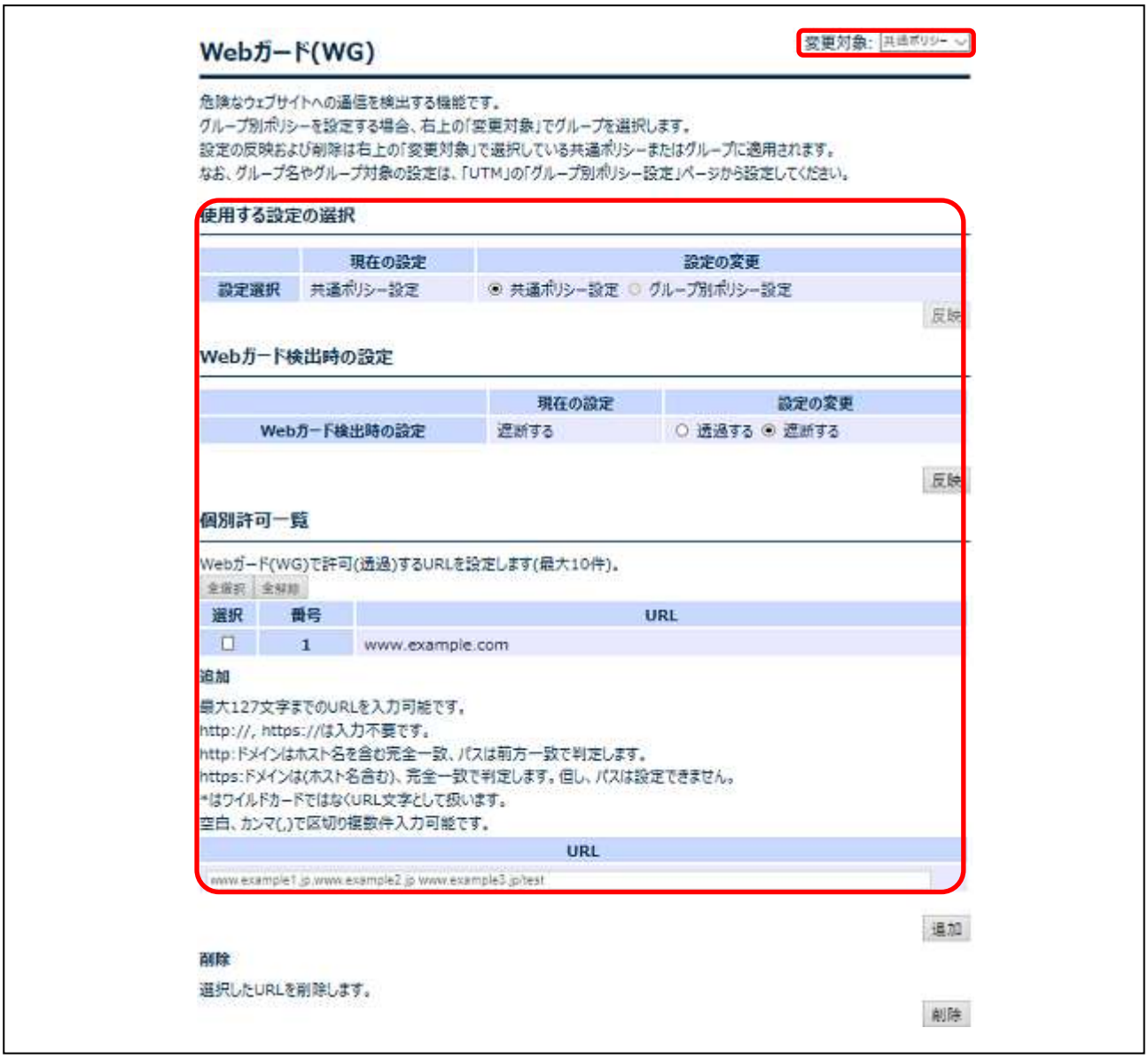
⑵　各項目を設定し、[反映]ボタンをクリックします。

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。

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 • 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。 • 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 • 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。

(3)　設定が反映されたことを確認します。

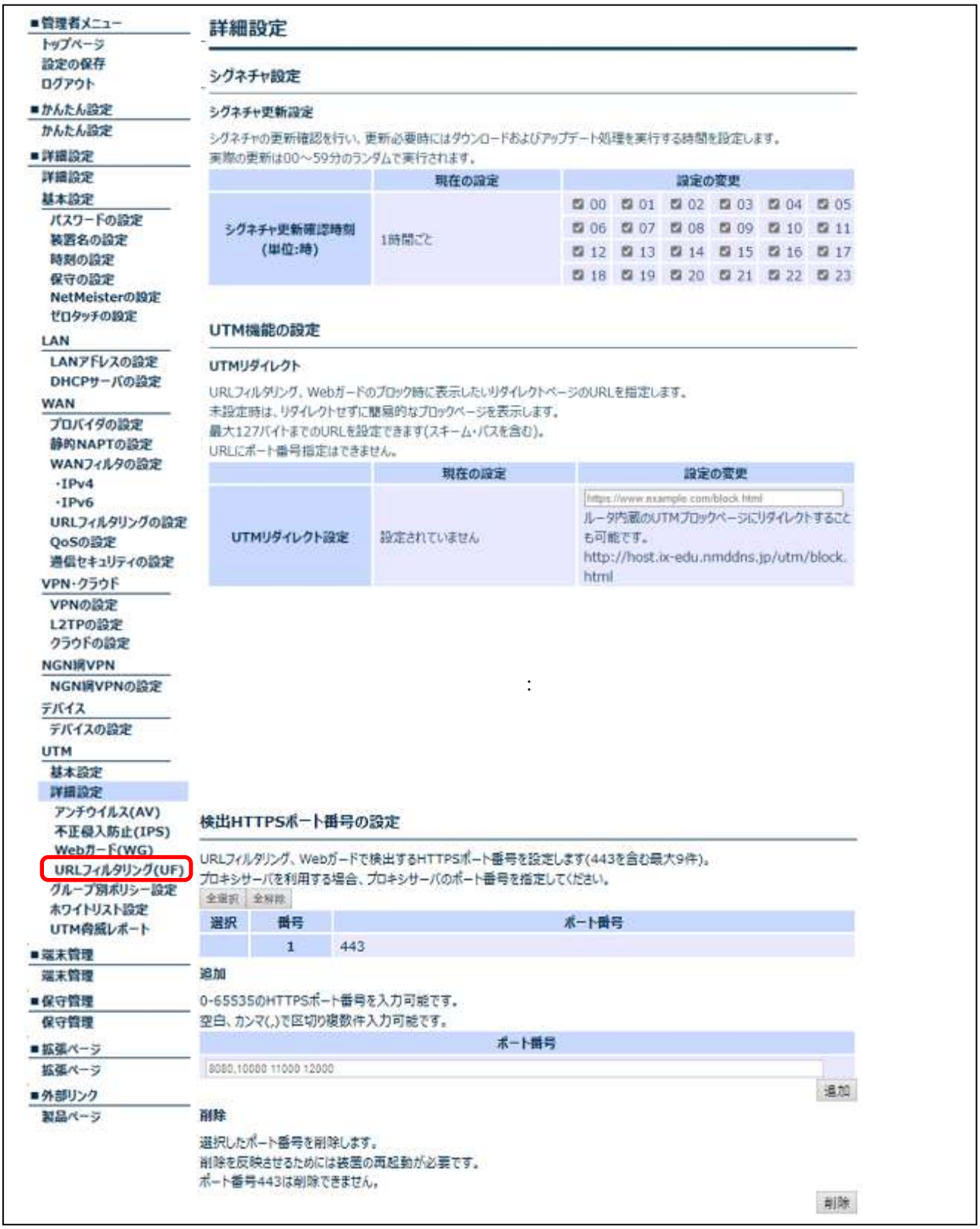


4. 詳細設定

4.7.7 URL フィルタリング(UF)の設定

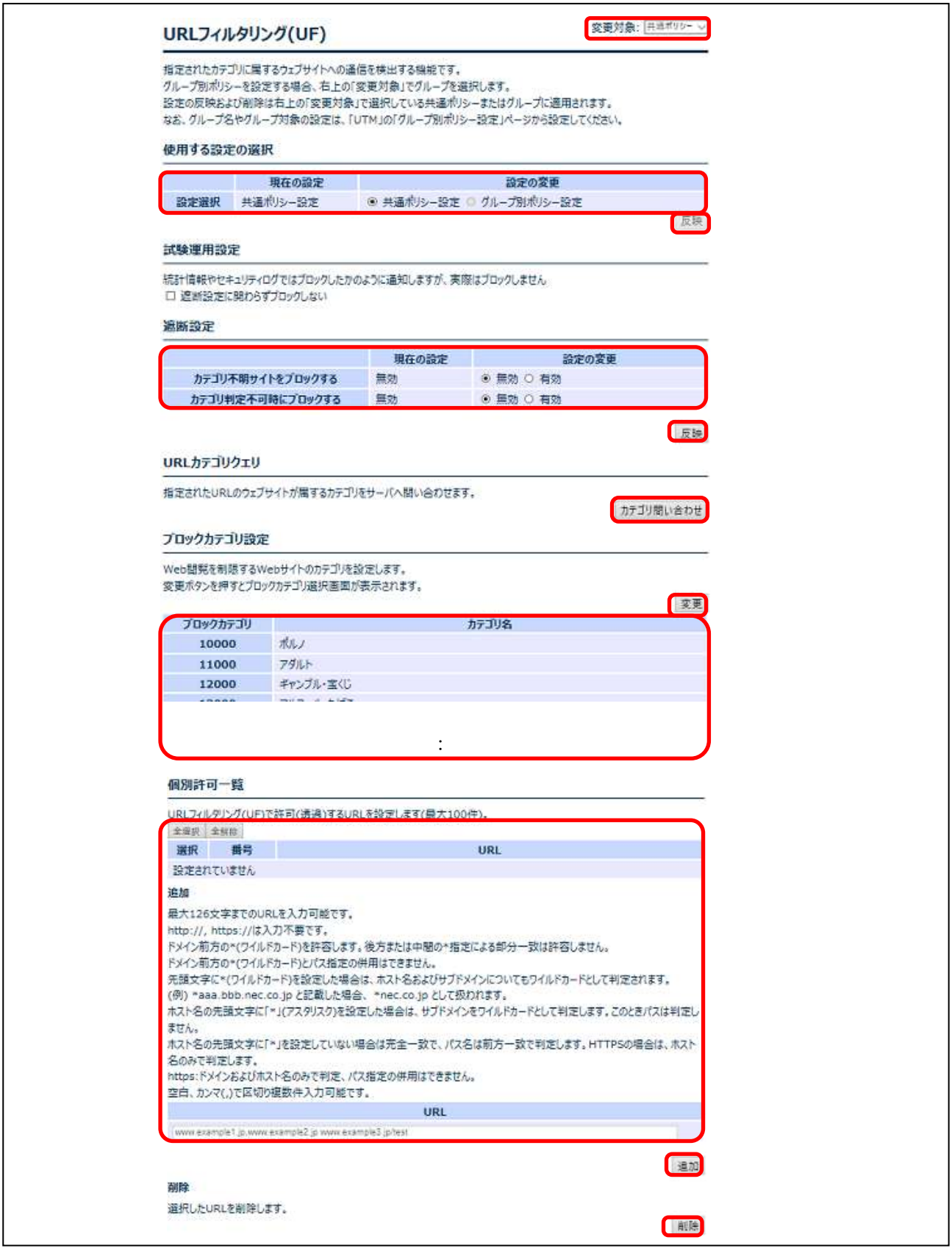
URL フィルタリング（URL Filtering）を設定します。

(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。



⑵ 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。



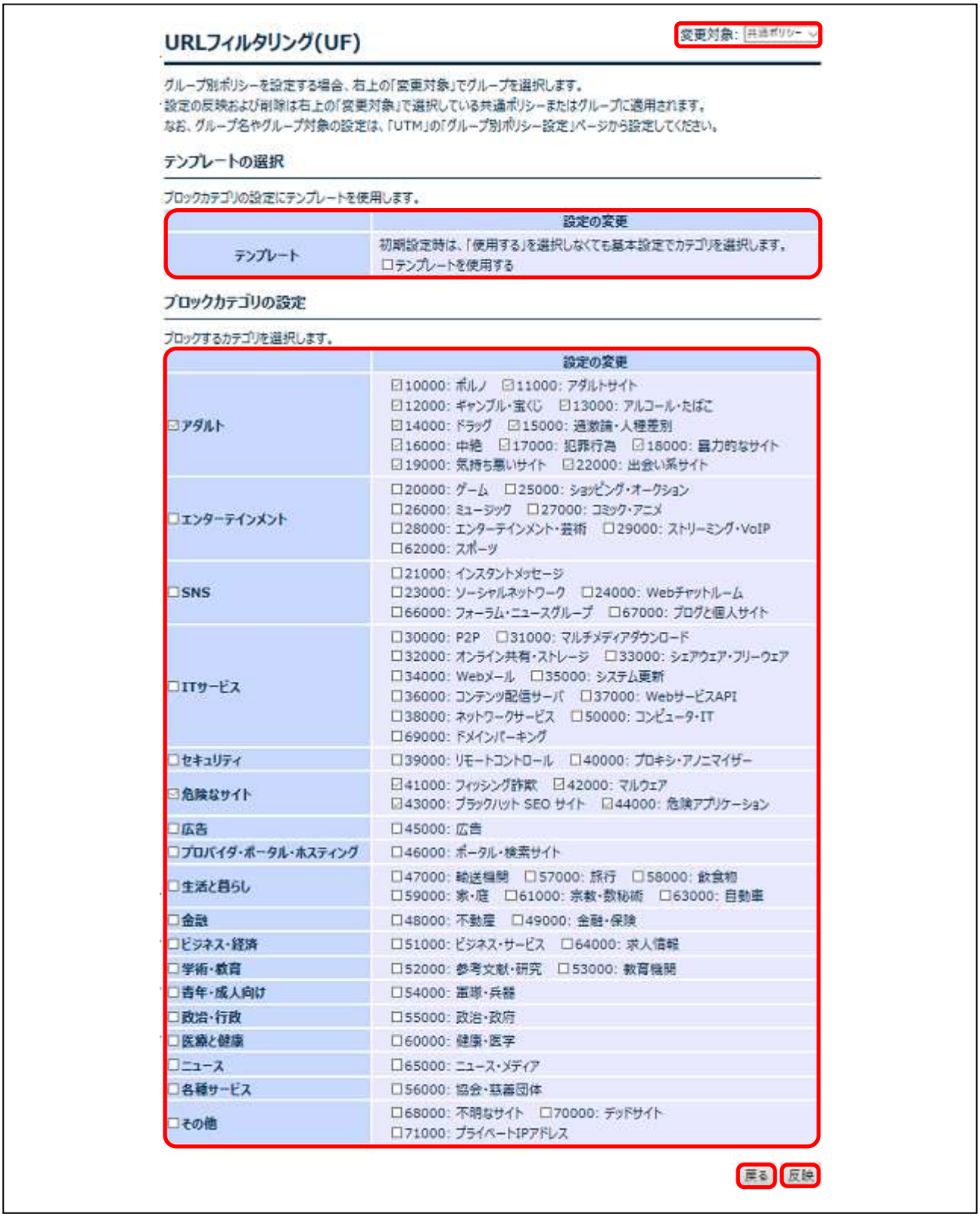
4. 詳細設定

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 • 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	URL カテゴリクエリ画面に遷移します。 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。
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	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。
⑩	個別許可一覧 追加	URL フィルタリングで許可(透過)する URL を設定します。 • 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。

[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。

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。

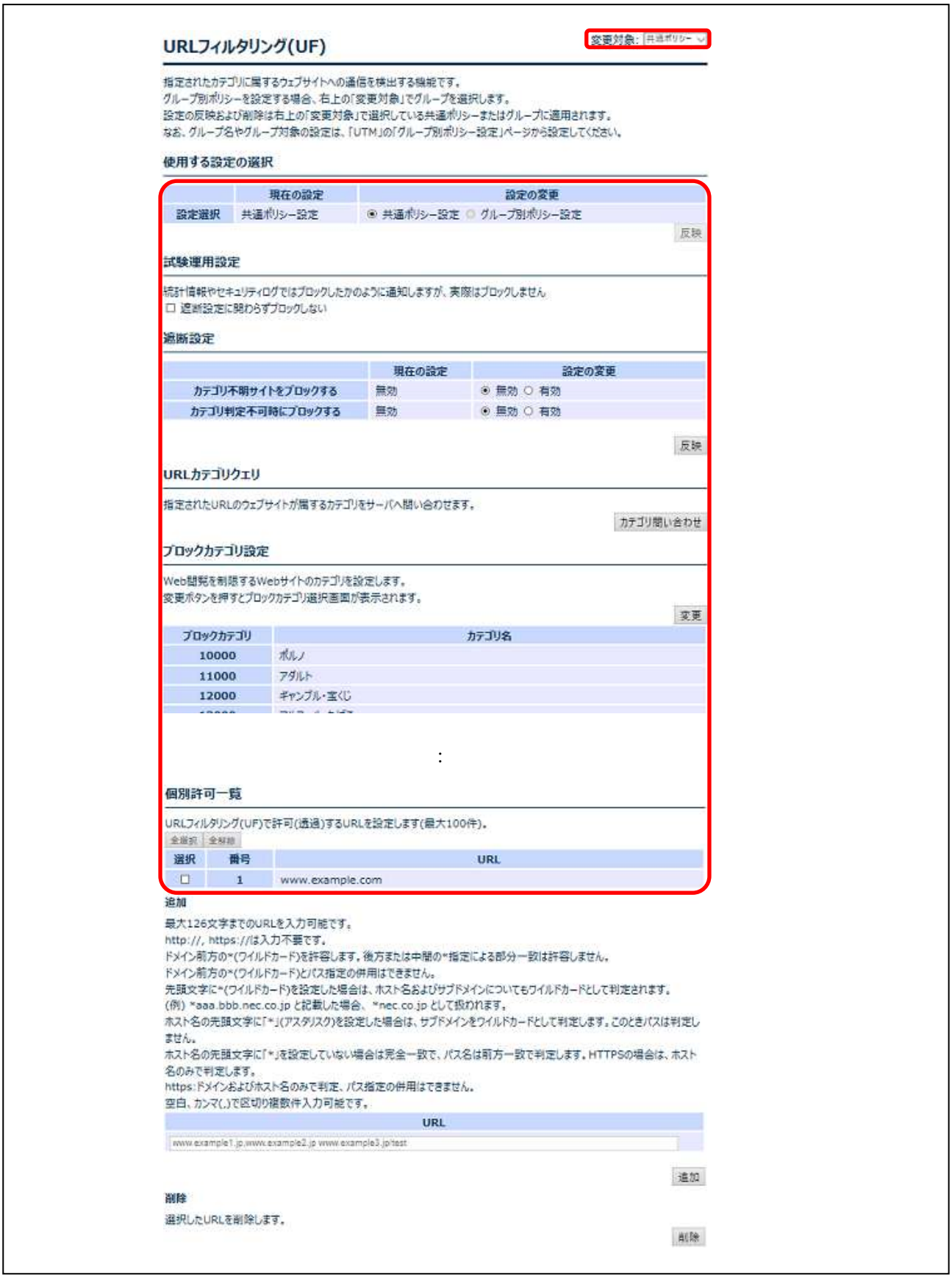
(3) [変更]ボタンをクリックし、ブロックカテゴリを選択し、[反映]をクリックします。



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。 • 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) 設定が反映されたことを確認します。

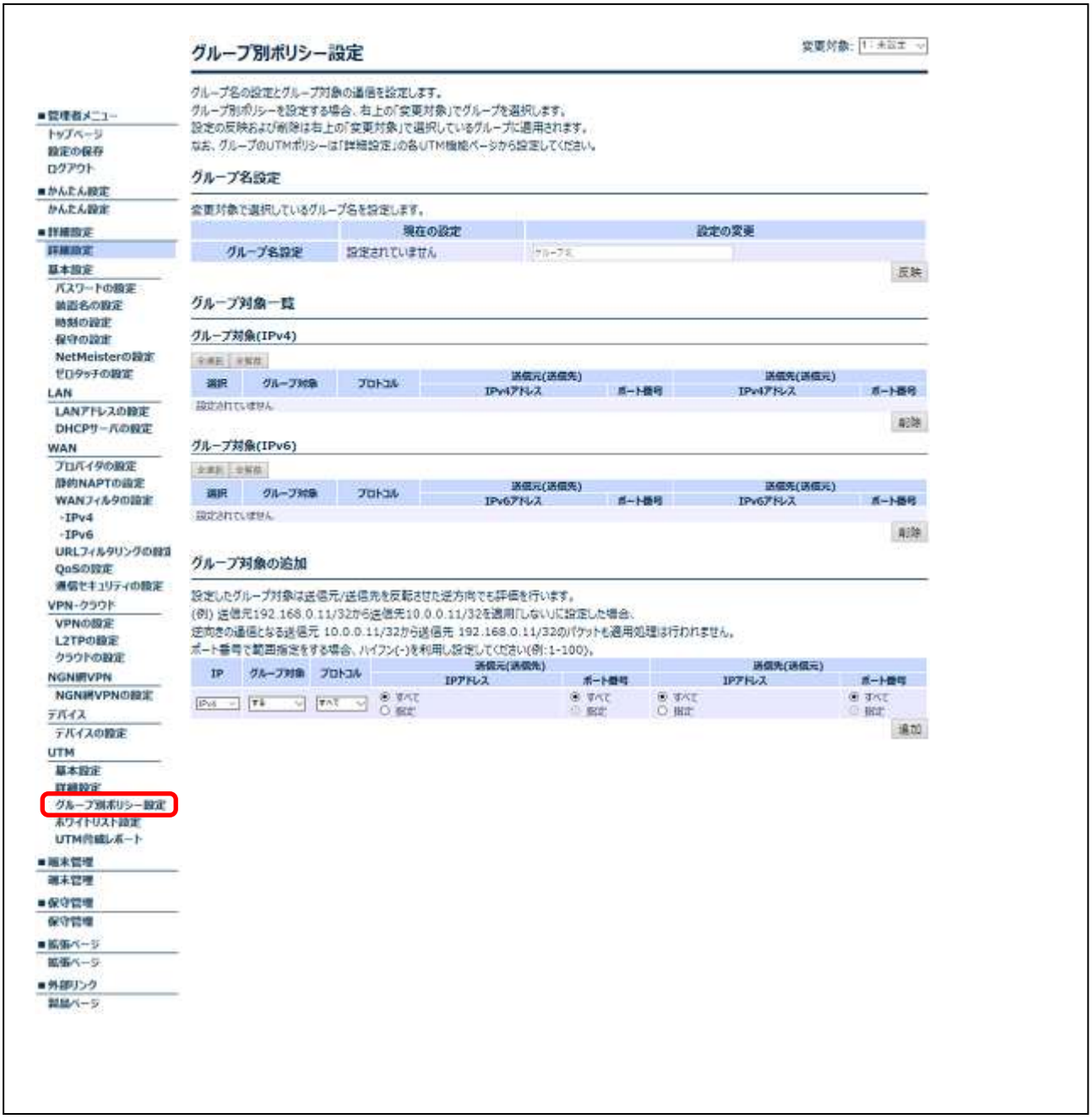


4. 詳細設定

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。



(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。

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。

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。 ・ 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。
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。

(3)　設定が反映されたことを確認します。

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。

(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。

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。

(3)　設定が反映されたことを確認します。

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。

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. 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。

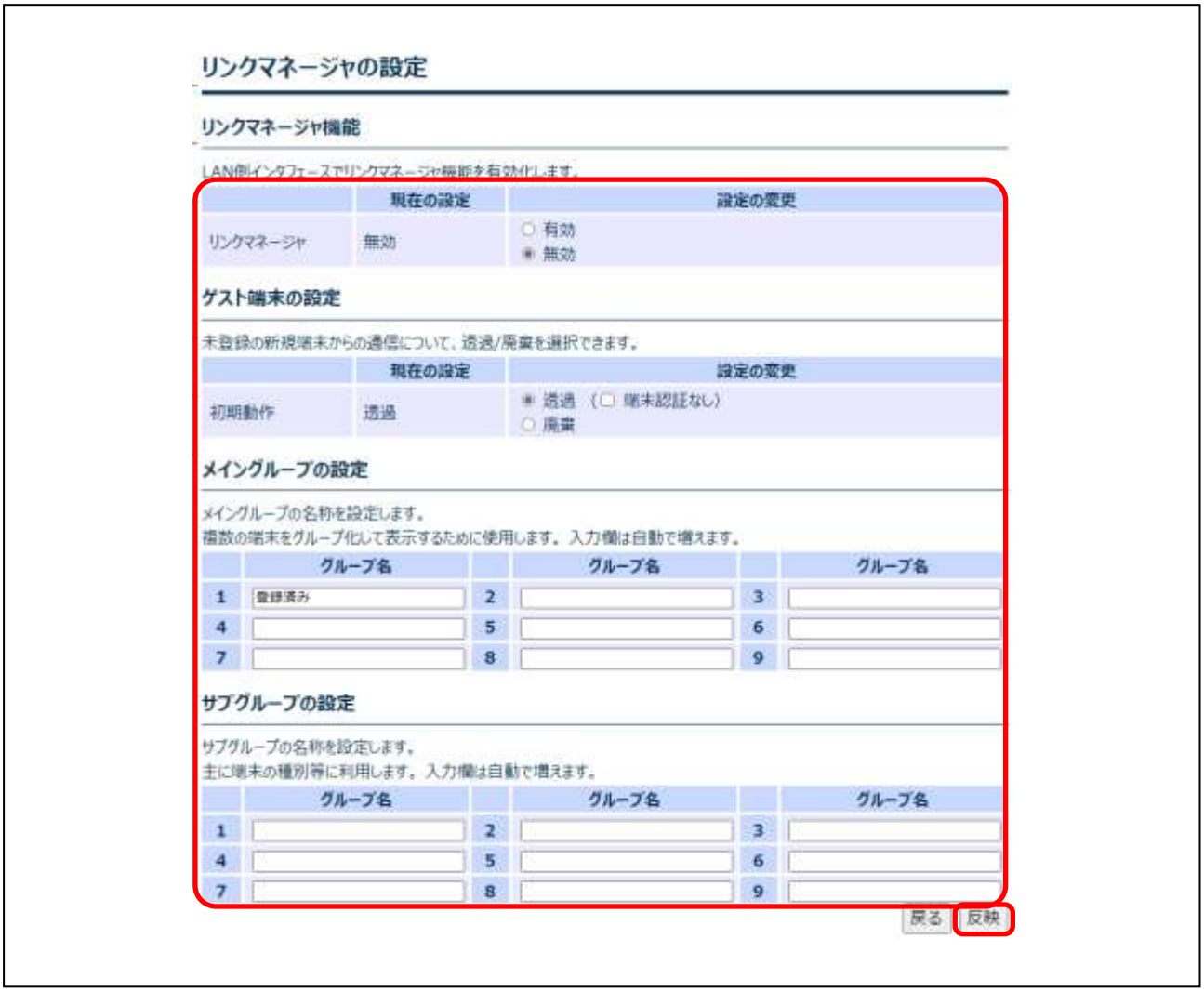
(1)　ログイン後のメニューエリアから[端末管理]をクリックします。

(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

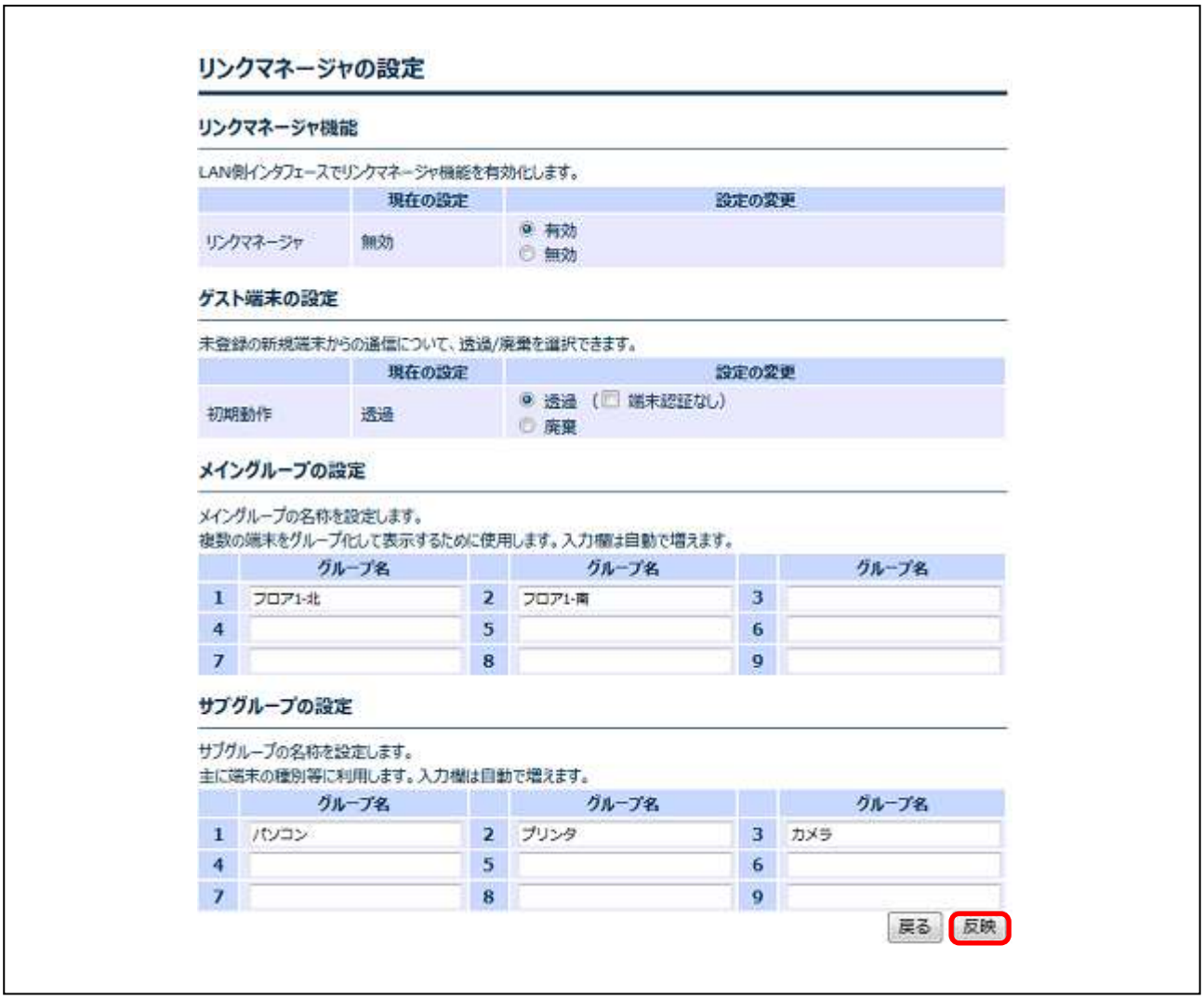
(4) 各項目を設定し、[反映]ボタンをクリックします。



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。 • 「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。 • 「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。 • 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 • 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。 • 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 • 全角文字を利用することができます。 注意 • 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で、サブグループのみを設定することはできません。

⑸　各項目を設定する一例を示します。



⑹　各項目の設定が反映されたことを確認します。

⑺　「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。

(8)　各項目を設定し、[反映]をクリックします。

5. 端末管理

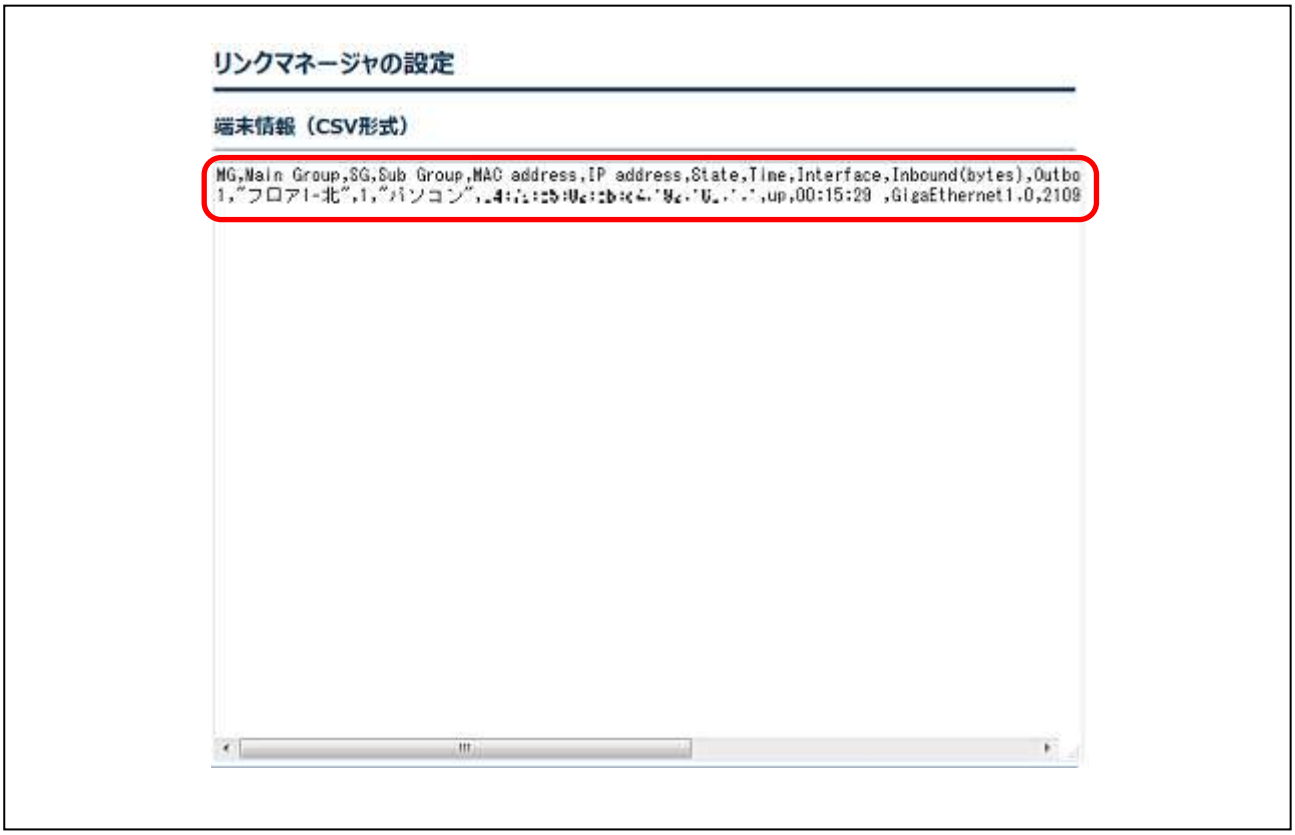
番号	項目	内容
①	グループ 全選択	選択した端末情報に対して、一括変更、一括統計クリアおよび一括削除することができます。 [全選択]をクリックすると、端末の選択を全選択します。
②	グループ 全解除	[全解除]をクリックすると、端末の選択を全解除します。
③	グループ 表示範囲	ハイフン(-)で指定された範囲の番号の端末情報を表示させることができます。
④	グループ 選択	選択した端末情報に対して、一括変更、一括統計クリアおよび一括削除することができます。 端末単位で、個々に選択します。 注意 ・ 設定を反映させる場合は、該当の端末の選択がチェックされている必要があります。
⑤	グループ 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で、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。

(9) 各項目の設定が反映されたことを確認します。

(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。

5. 端末管理

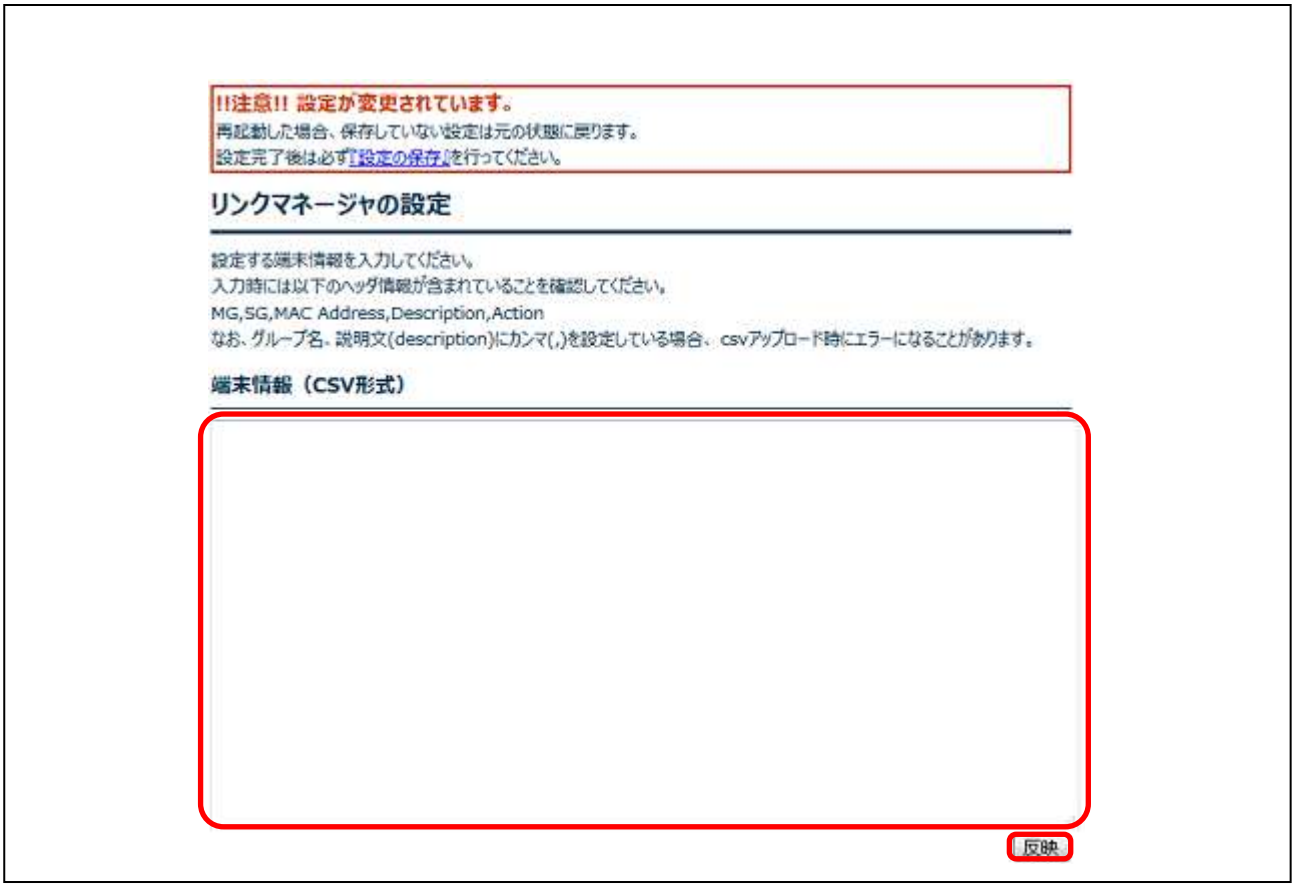
(11) 端末情報が CSV 形式で表示されたことを確認します。マウスで必要箇所をなぞり、コピーして利用してください。



(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。

(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。



5. 端末管理

(14) 設定が反映されたことを確認します。

(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。

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。

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。

(4) 各項目を設定し、[反映]をクリックします。

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。

⑸　各項目の設定が反映されたことを確認します。

⑹ 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。

メモ 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。

メモ 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。

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. 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。

メモ 更新ボタンを押すと、最新の装置状態が表示されます。

メモ ログイン前の場合、VPN 情報は表示されません。

6. 保守管理

番号	項目	内容
①	装置情報	本装置の名称と稼働状態を表示しています。 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。 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。 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。 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。 稼働率 ： CPU の使用率を表示しています。 メモリ ： 内部メモリの使用率を表示しています。 内部温度 ： 本装置内部の温度を表示しています。 内部電圧 ： 内部装置への入力電圧を表示しています。
②	ネットワーク情報	ネットワークの状態を表示しています。 デバイス ： 物理デバイスの接続種類を表示しています。 接続状態 ： デバイスの接続状態を表示しています。 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。 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。
③	WAN 情報	WAN 接続の状態を表示しています。 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。 接続状態 ： 接続状態を表示しています。 情報 ： WAN 接続の情報を表示しています。
④	VPN 情報	VPN 接続の状態を表示しています。 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。 接続状態 ： VPN 接続の接続状態を表示しています。 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。
⑤	UTM 情報	UTM の状態を表示しています。 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。 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。

(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。

メモ 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。

(5) 接続名を入力し、[反映]ボタンをクリックします。

メモ 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。

⑹　VPN 情報の接続名が反映されたことを確認します。

メモ　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。

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。

6. 保守管理

6.3 設定データの管理

6.3.1 設定データのダウンロード(バックアップ)

装置の設定データ(不揮発メモリに保存されているスタートアップコンフィグ)をテキストデータ形式で確認することができます。また、パソコンにダウンロードして保存し、バックアップとすることができます。

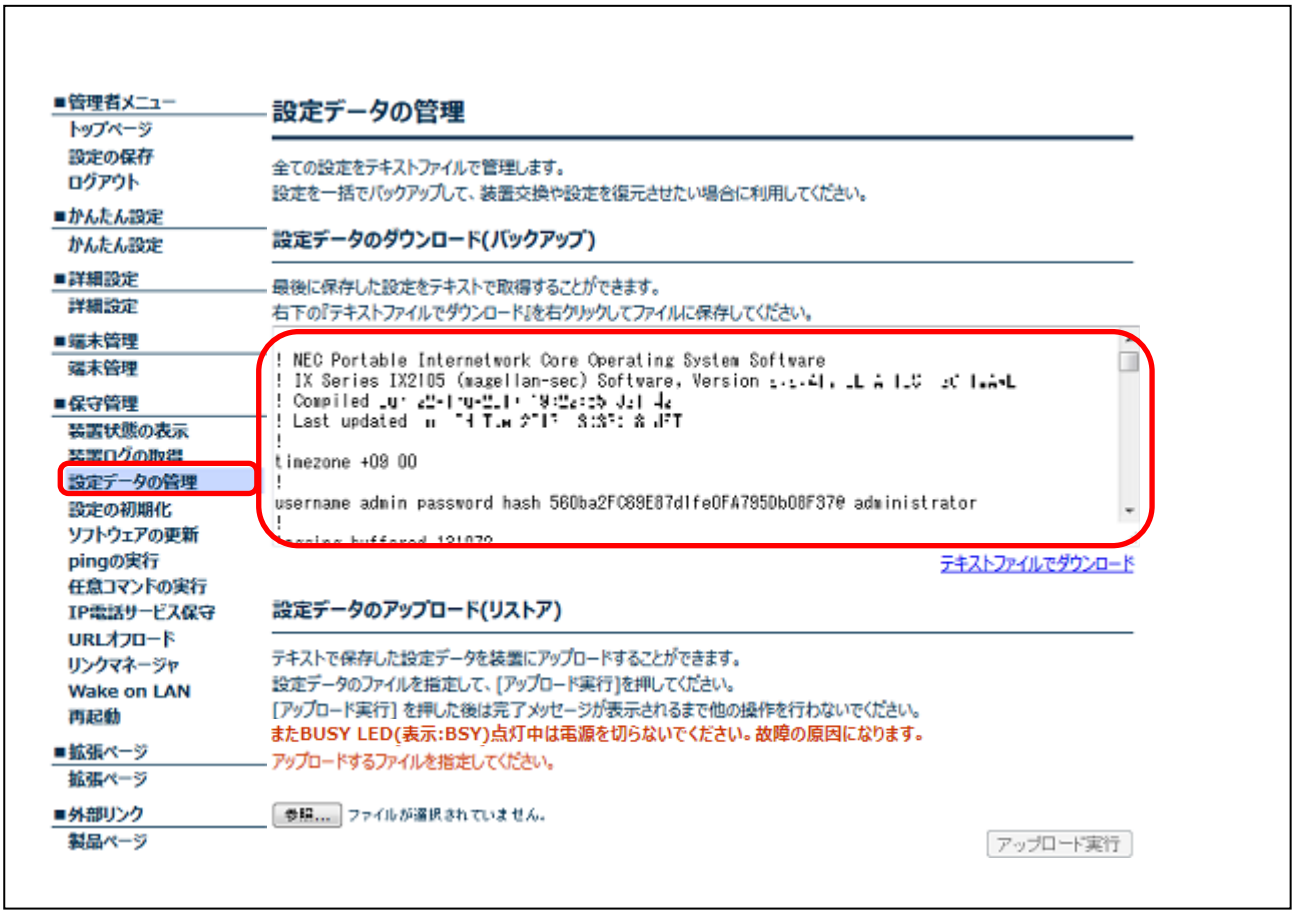
メモ　実行中の設定データ(running-config)を確認したいときは、メニューエリアの「設定の保存」を実行してから、確認を行ってください。

(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。

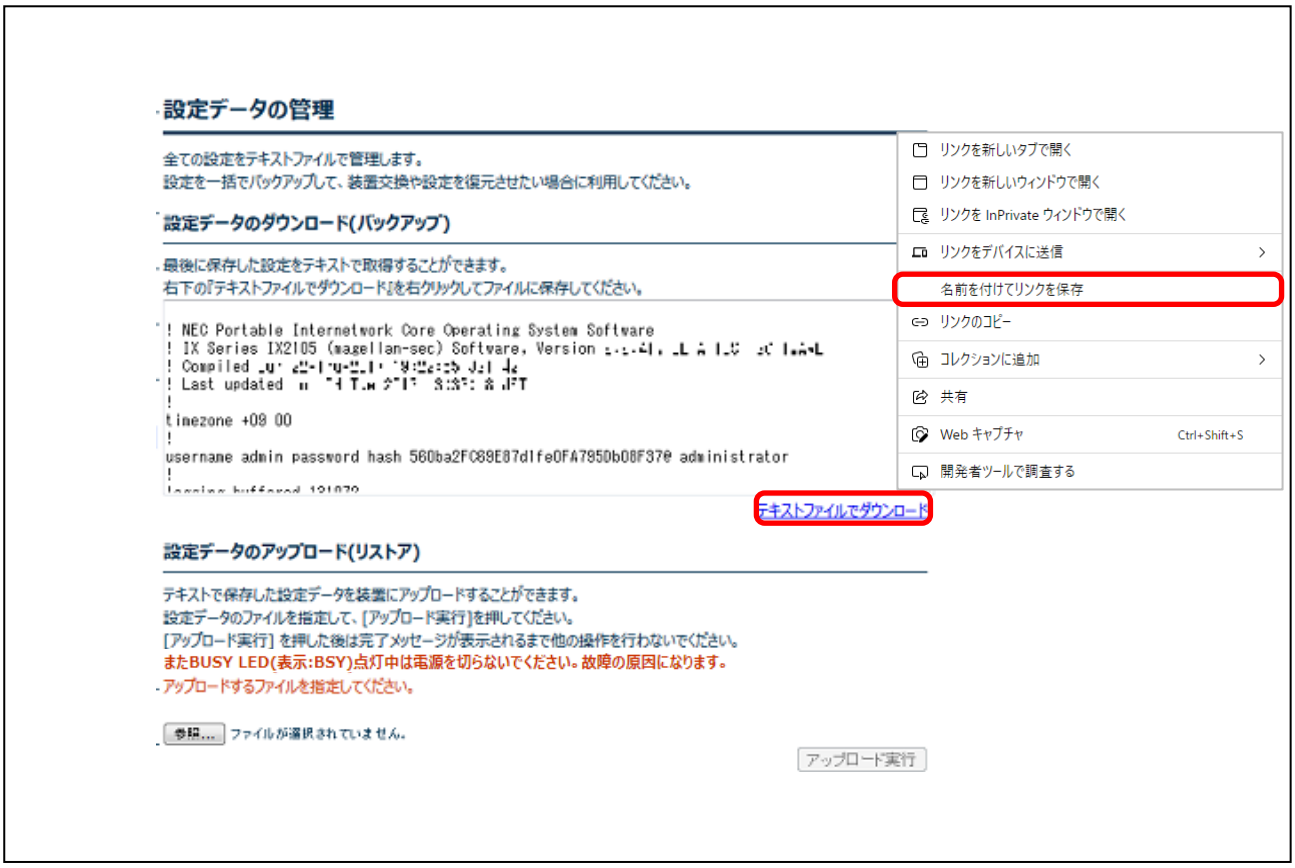
(2)　[設定データの管理]をクリックします。

(3)　「設定データのダウンロード(バックアップ)」の枠内に表示された設定データを確認します。

メモ　保存されている設定データがない場合、設定データは表示されません。



(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。



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

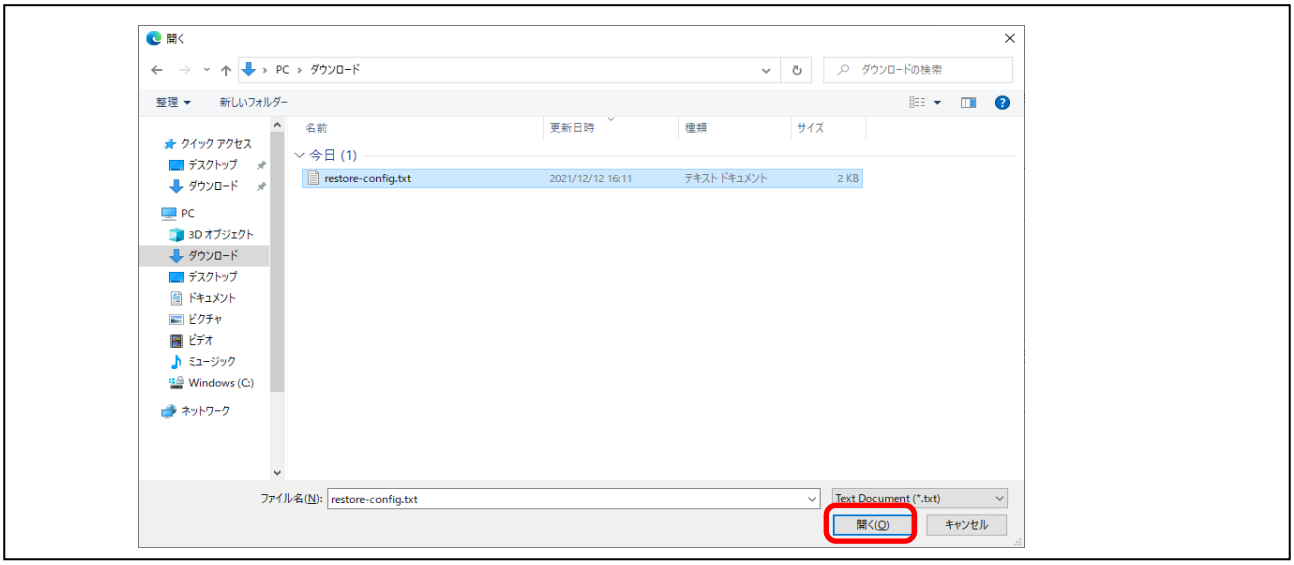
(1)　ログイン後のメニューエリアから[保守管理]をクリックします。

(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。

(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。

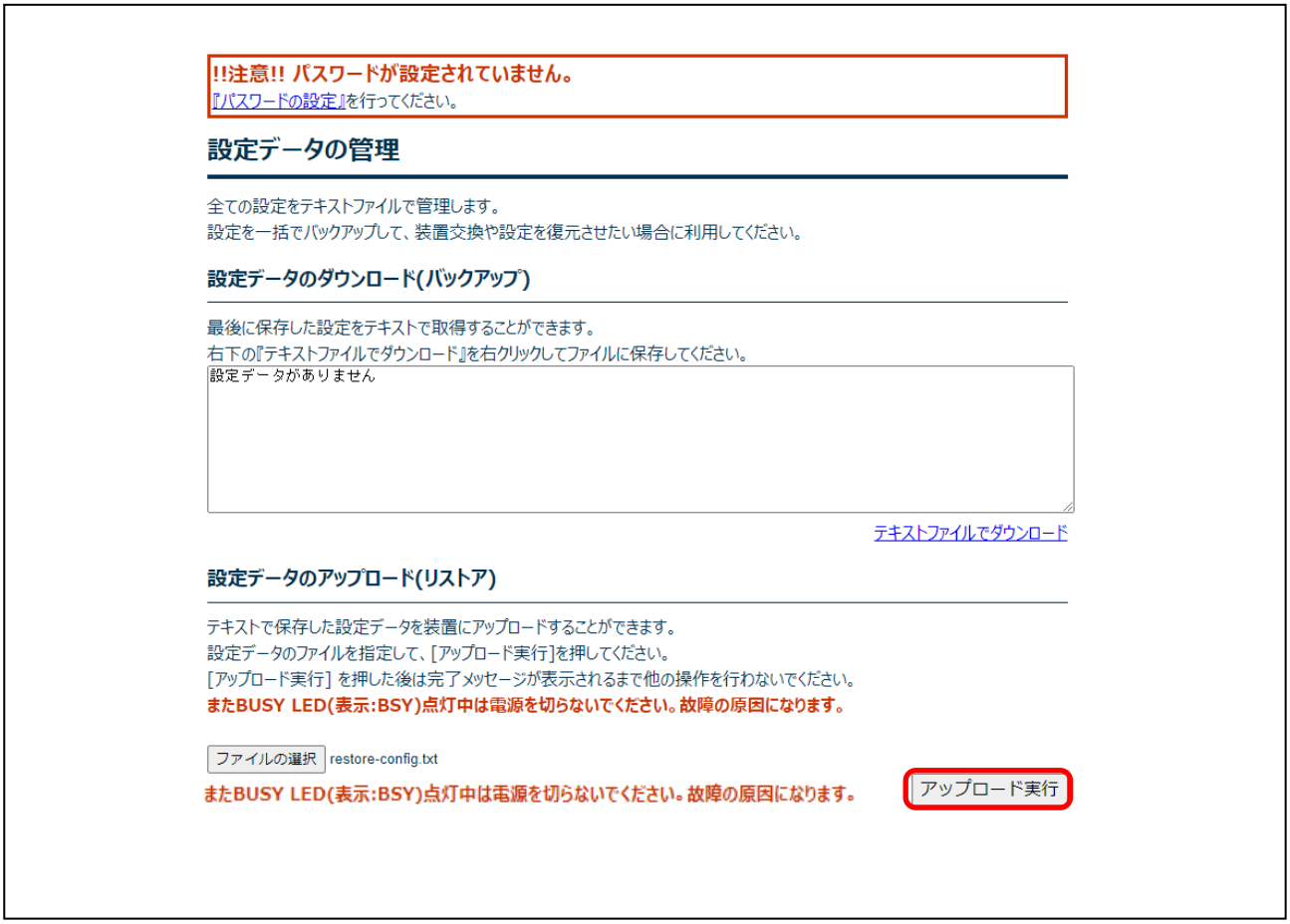
メモ　Windows の設定によってはファイル名に拡張子が表示されません。



⑸ ［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。

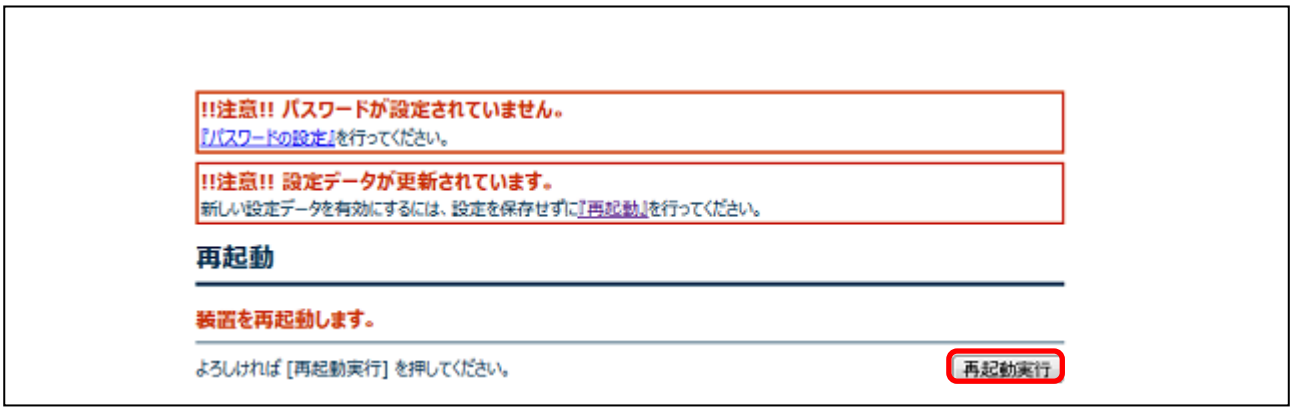


⑹　メッセージが「設定データのアップロード中です。」から「設定データのアップロードが完了しました。」に変わったことを確認します。

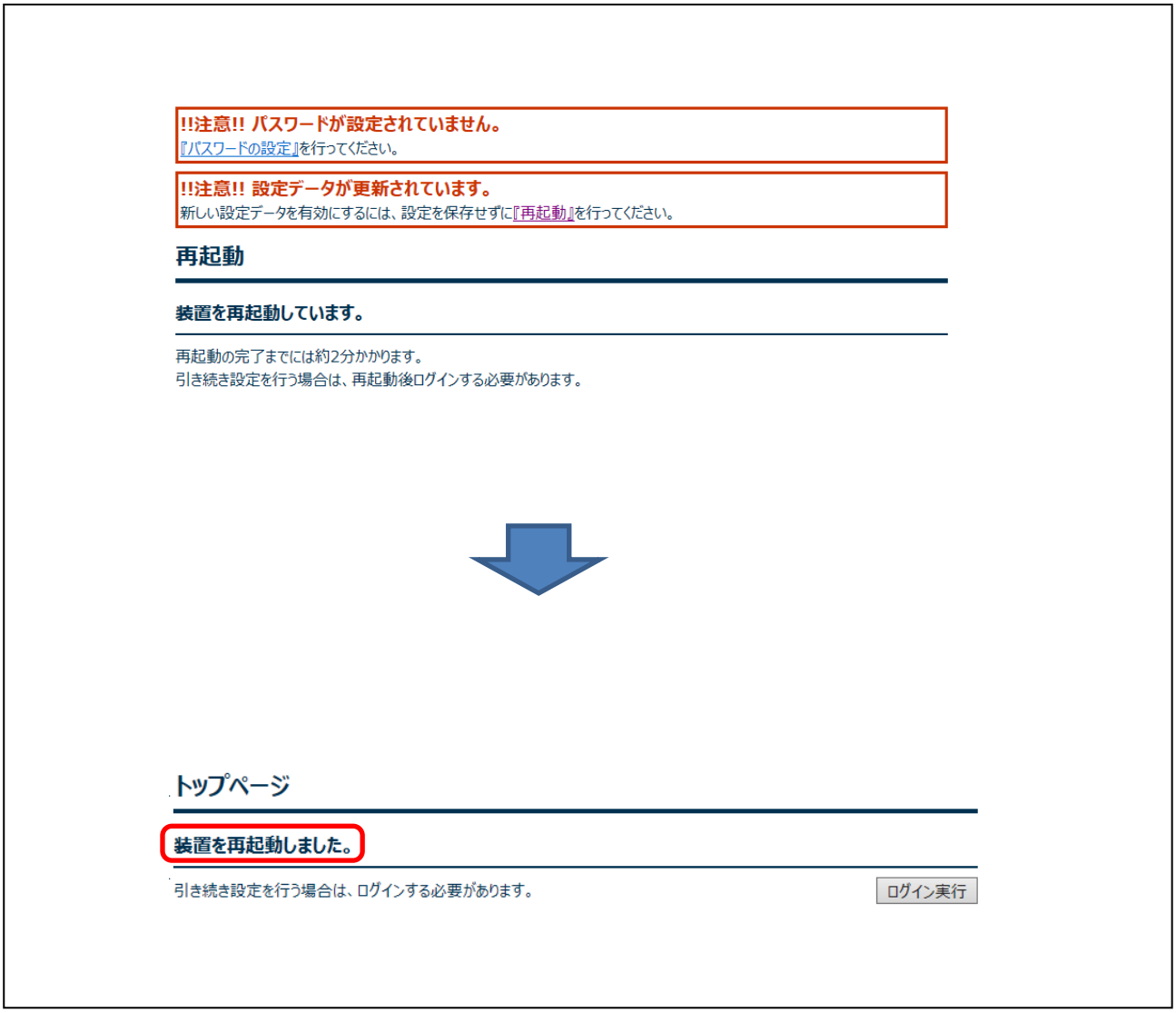
6. 保守管理

(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。

(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。



⑼　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。



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。

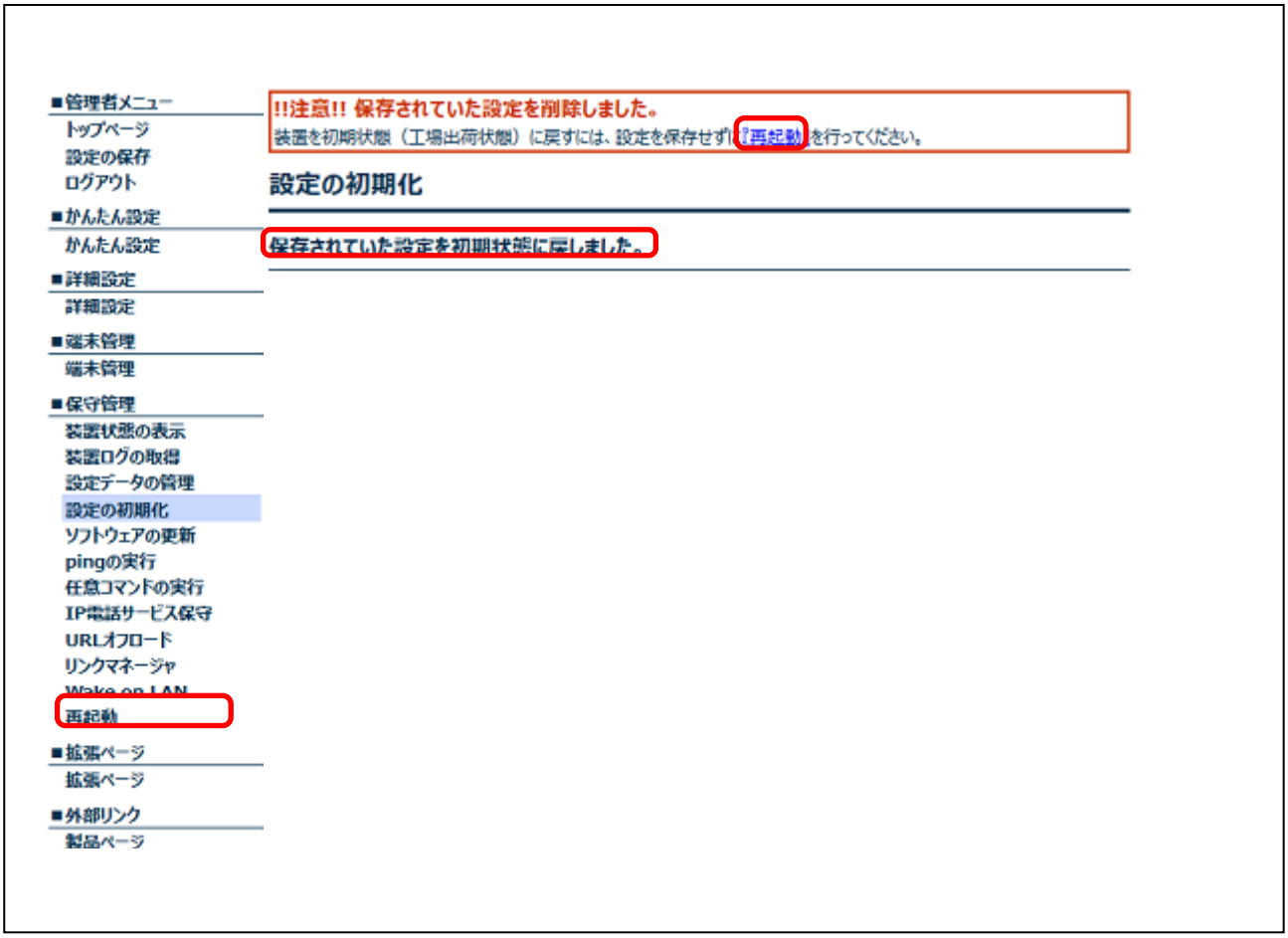
(2) [設定の初期化]をクリックします。

(3) [初期化実行]ボタンをクリックします。

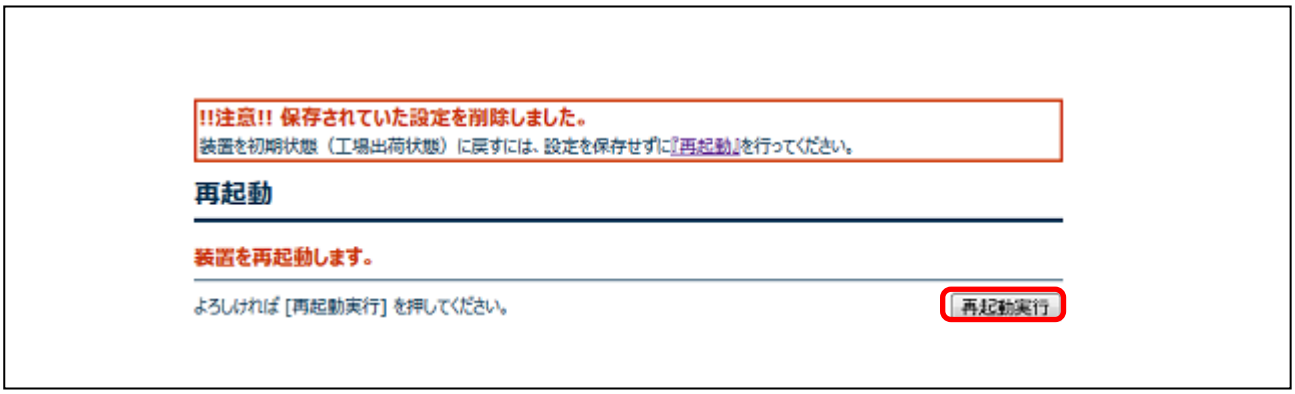
(4) 「保存されていた設定を初期状態に戻しました。」が表示されたことを確認します。

6. 保守管理

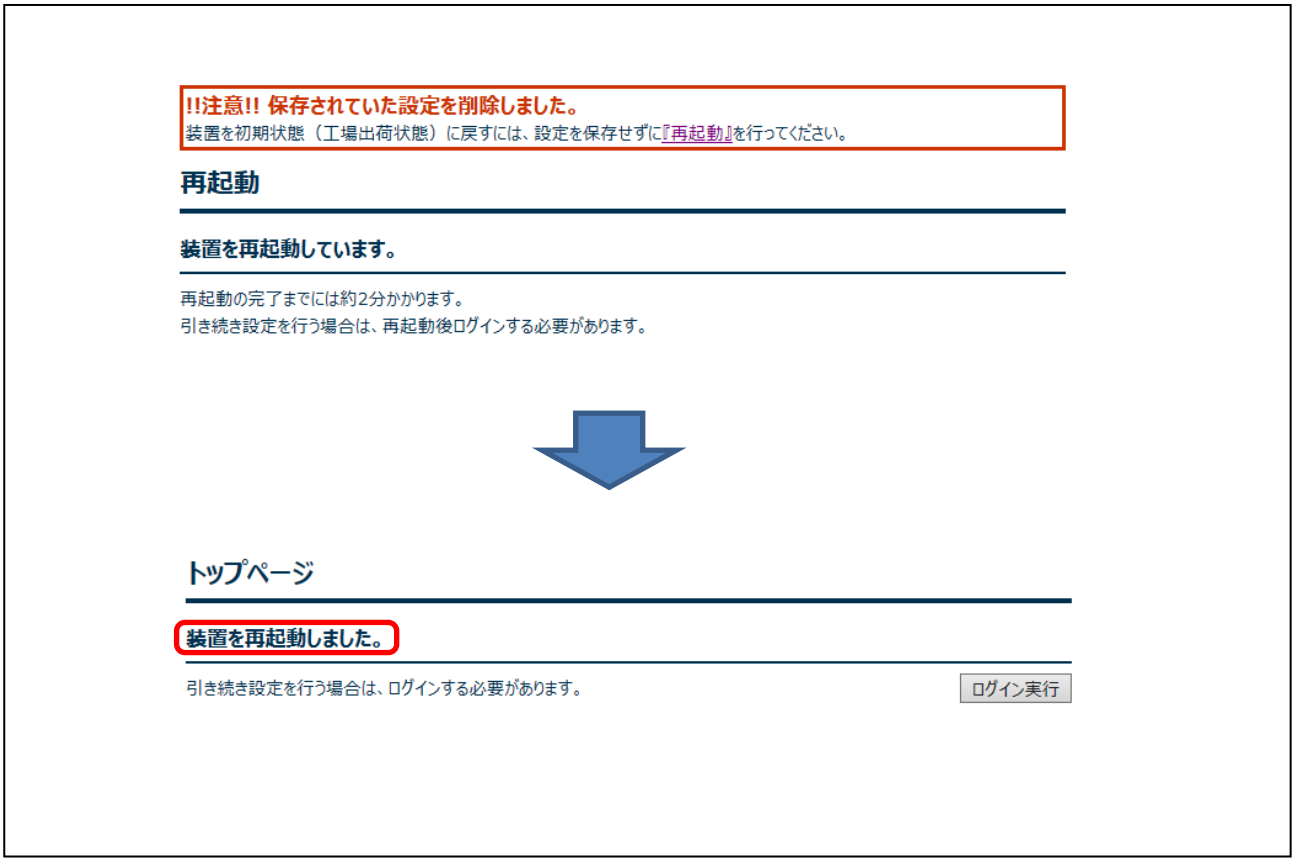
⑸　メニューエリアの「保守管理」、または、メッセージエリアから[再起動]をクリックします。



⑹　[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。



(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。



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。

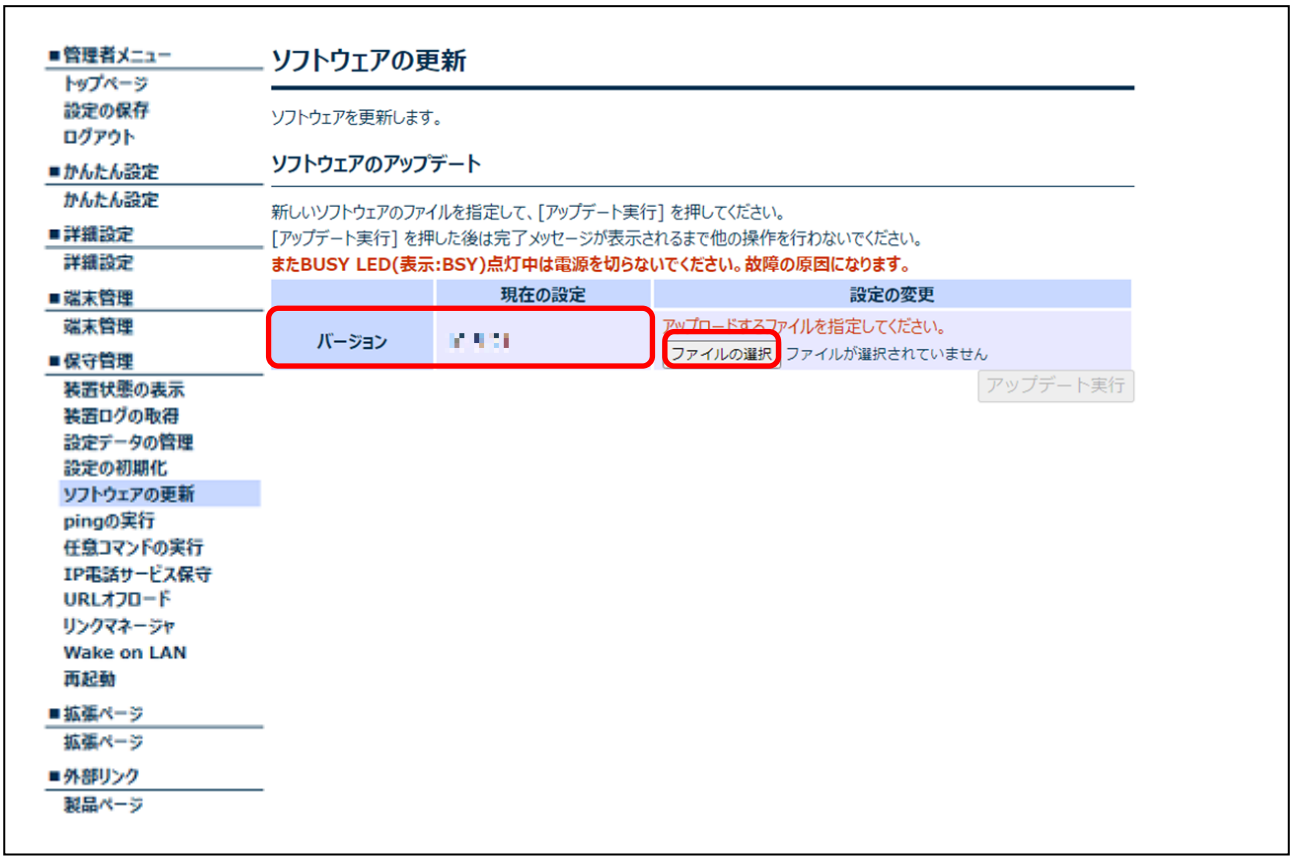
メモ　あらかじめ、ソフトウェアのプログラムファイル(拡張子が「.rap」のファイル)を入手し、パソコンに保存しておく必要があります。

(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。

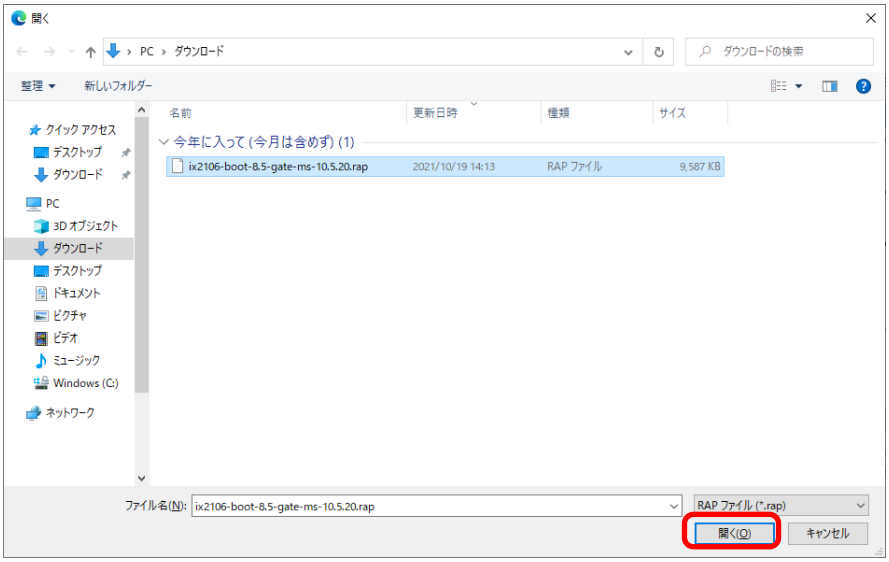
(2)　[ソフトウェアの更新]をクリックします。

(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。



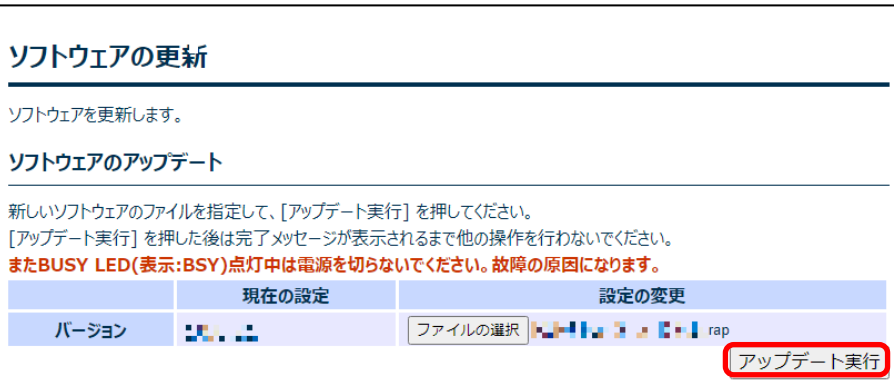
(5) 保存しておいたソフトウェアのプログラムファイル(拡張子が「.rap」のファイル)を選択します。



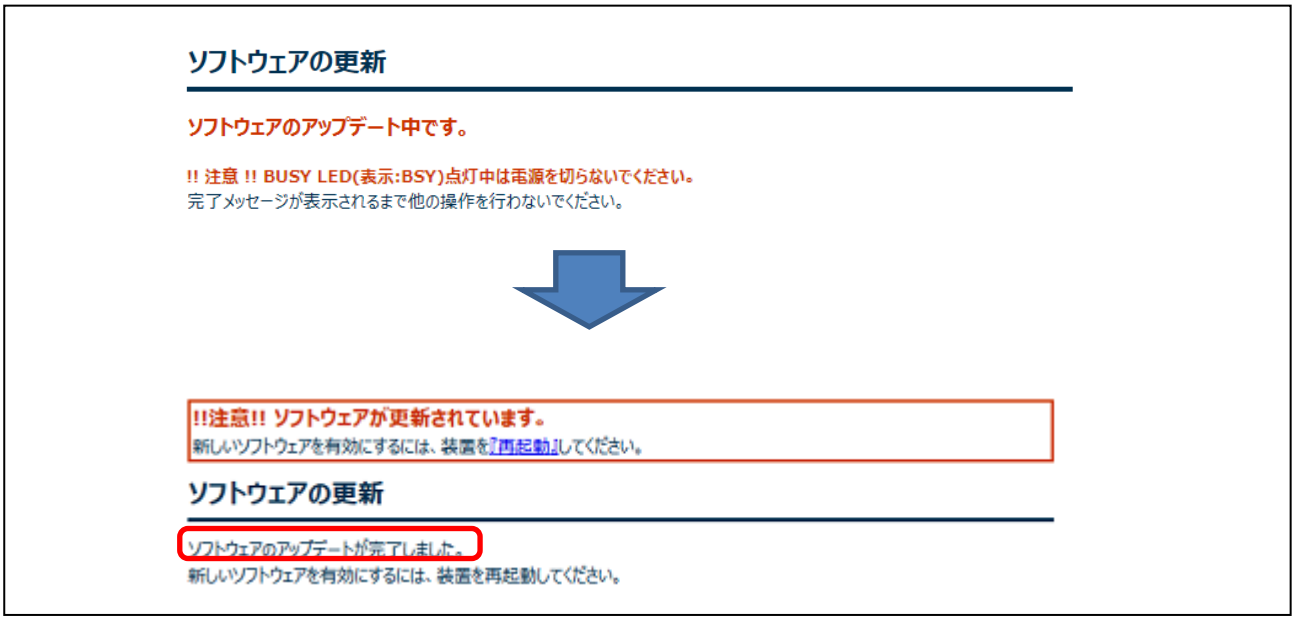
(6) [アップデート実行]ボタンをクリックします。

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。

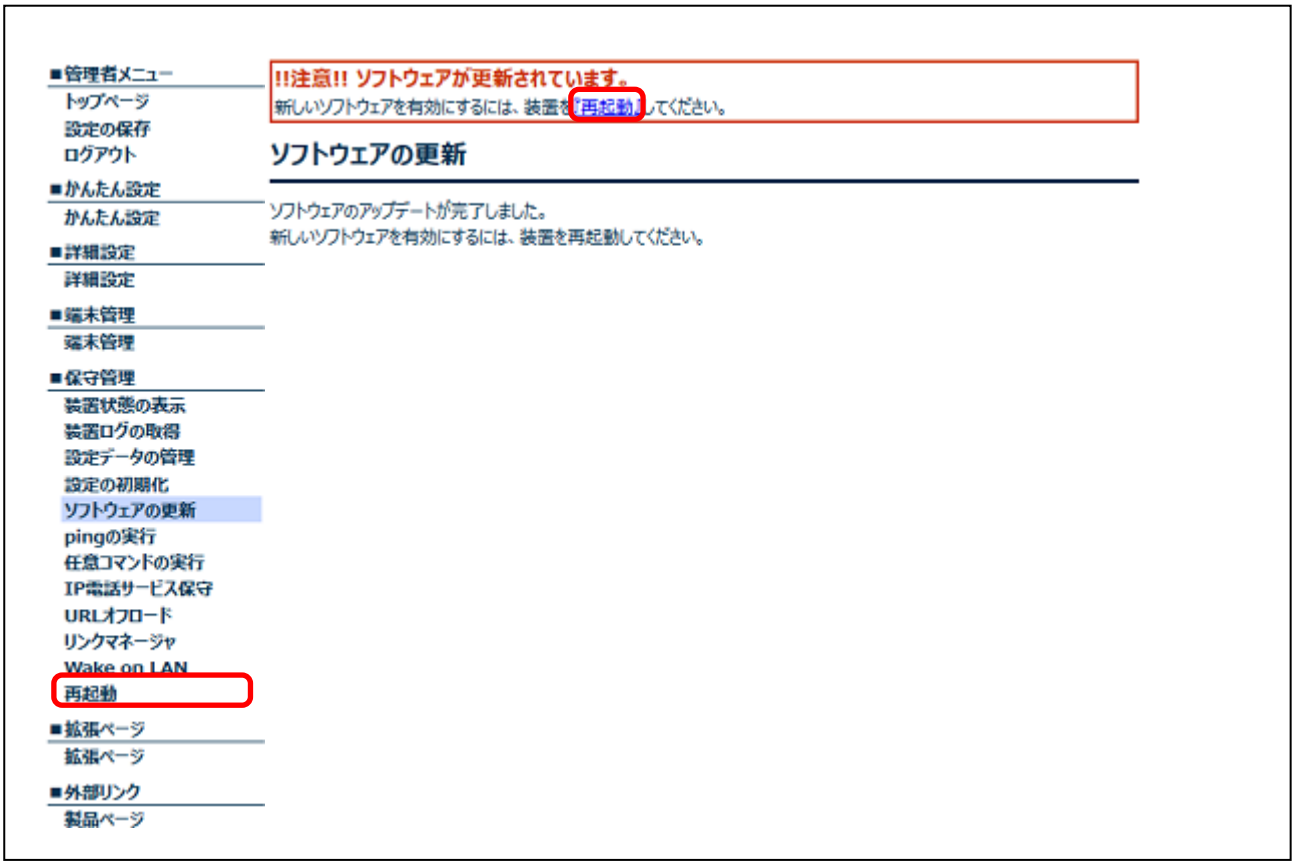
注意 「BUSY LED」点灯中は電源を切らないでください。故障の原因になります。



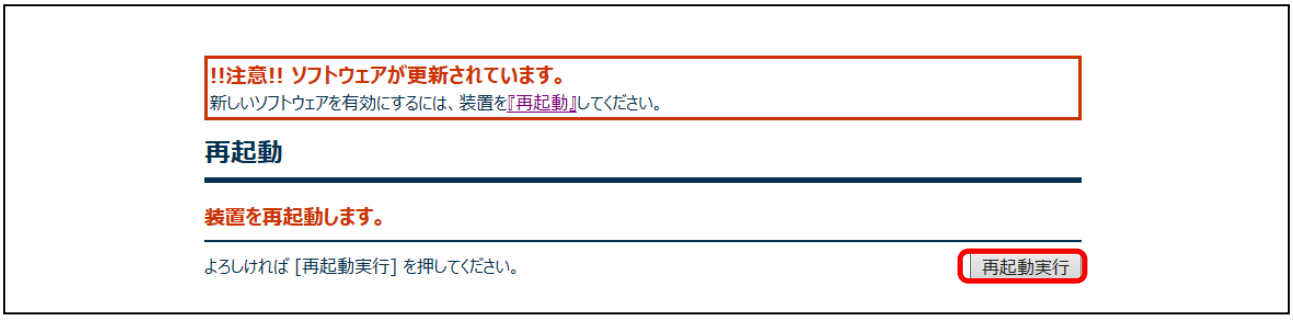
(7) メッセージが「ソフトウェアのアップデート中です。」から「ソフトウェアのアップデートが完了しました。」に変わったことを確認します。



(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。



(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。



(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。

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。

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。

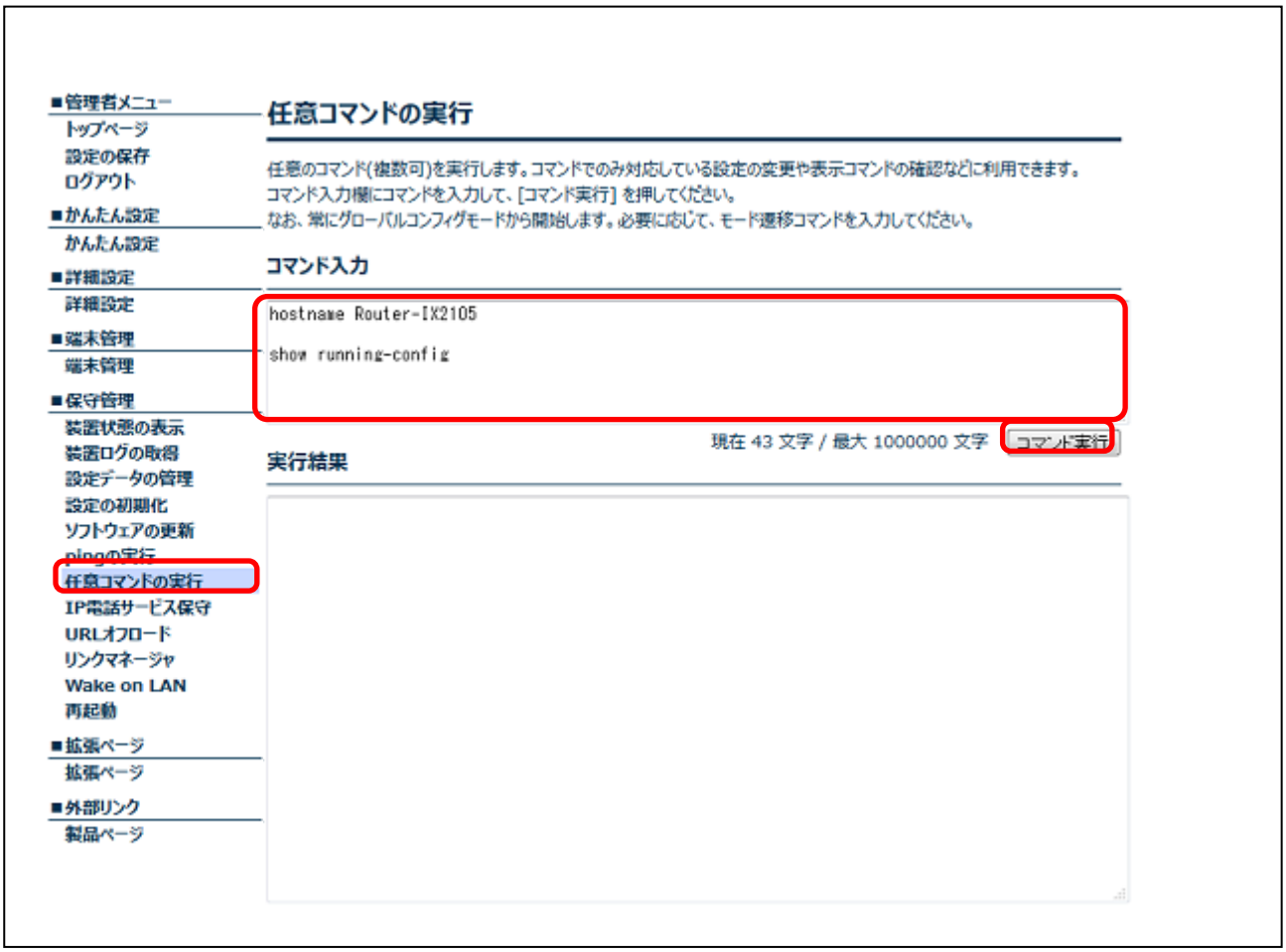
メモ 対話形式で実行するコマンドや自律的なメッセージ出力を行わせるコマンドは、動作保証の対象外です。

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。

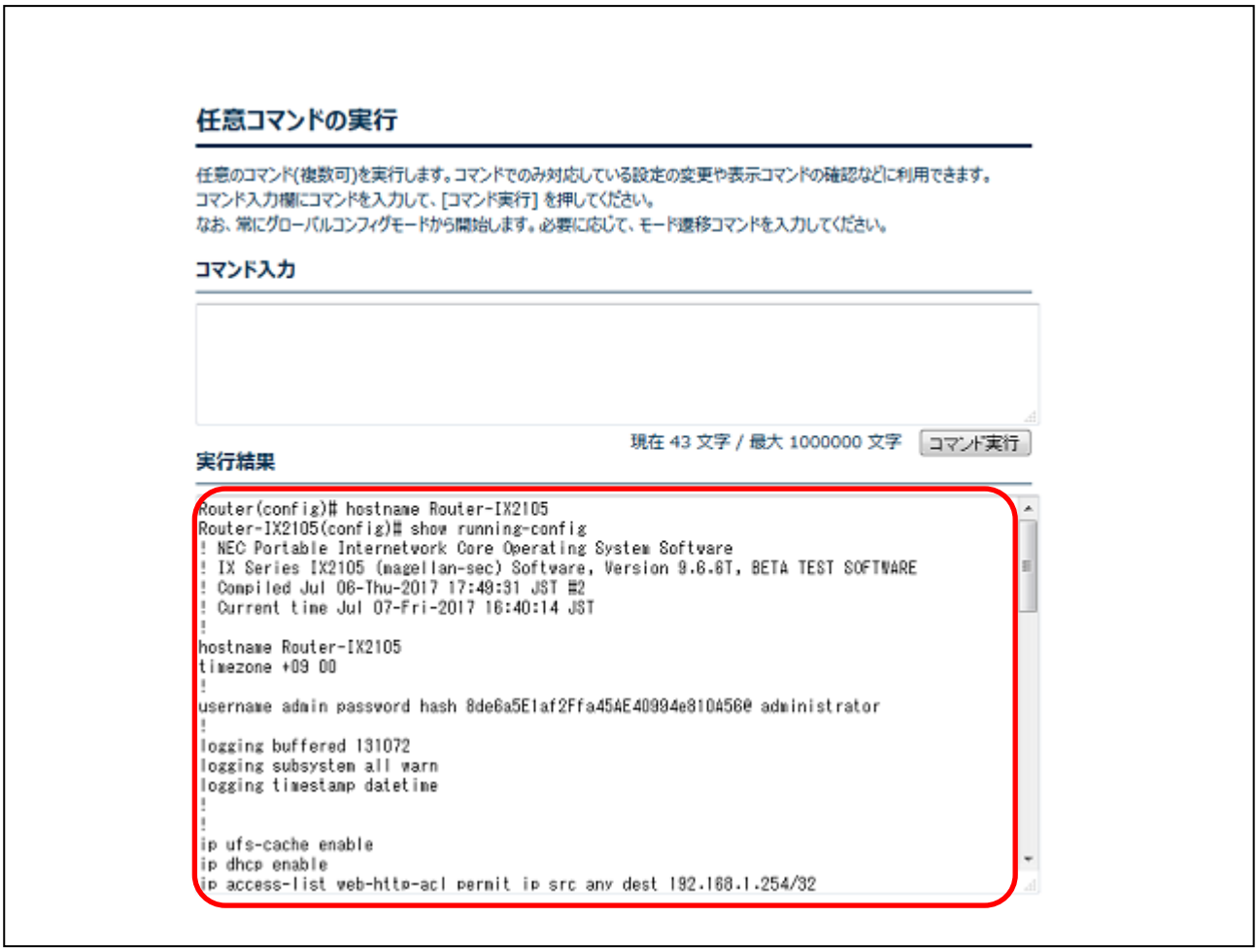
(1) ログイン後のメニューエリアから[保守管理]をクリックします。

(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。



(4) コマンドの実行結果を確認します。



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。

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。

メモ 「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。

メモ [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。

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。 • 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。 • 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。 • 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。 • 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。 • 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。 • 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。
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。

メモ [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。
メモ 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。

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。

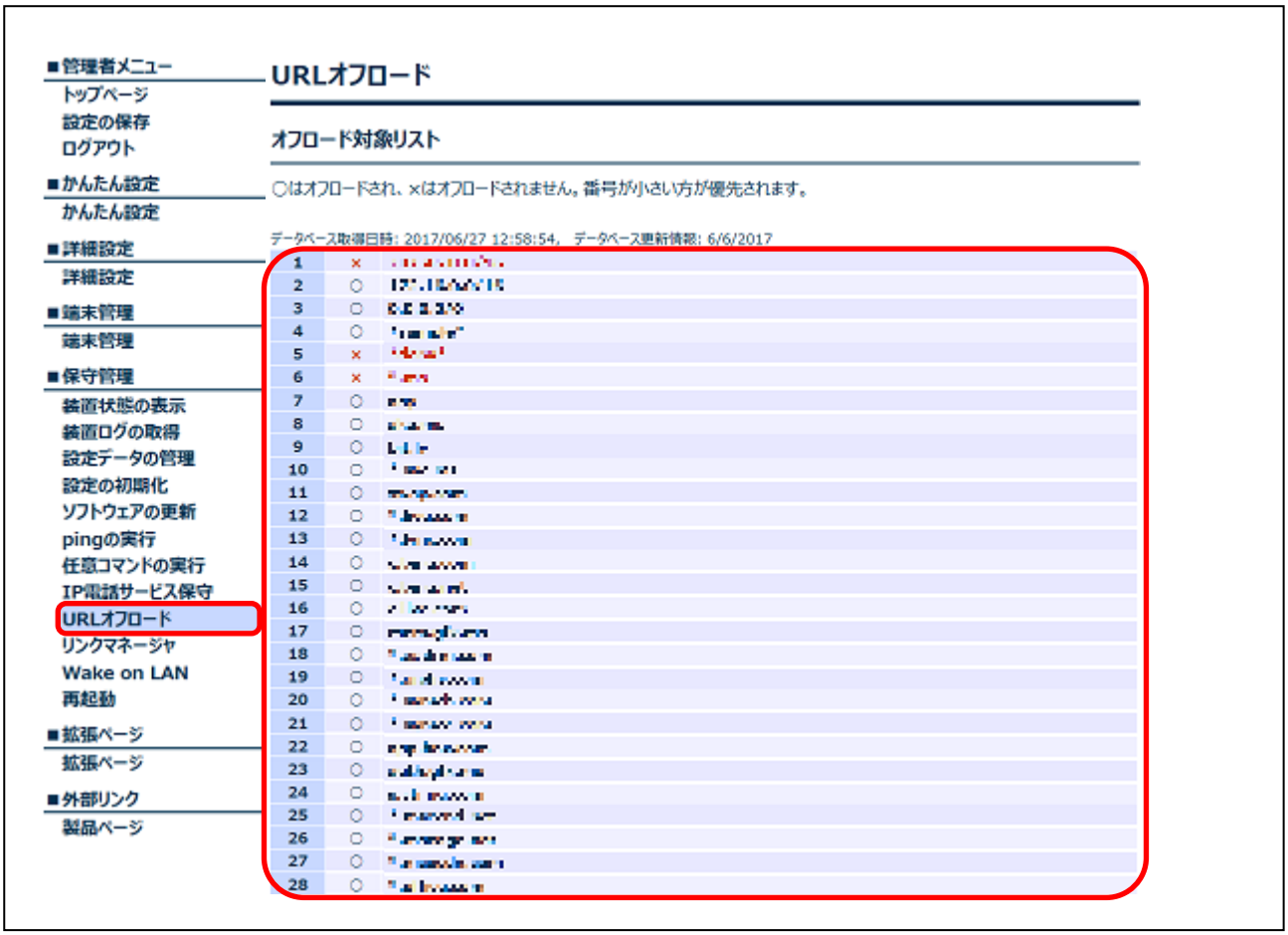
(1) ログイン後のメニューエリアから[保守管理]をクリックします。

(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。



6. 保守管理

6.10 リンクマネージャ

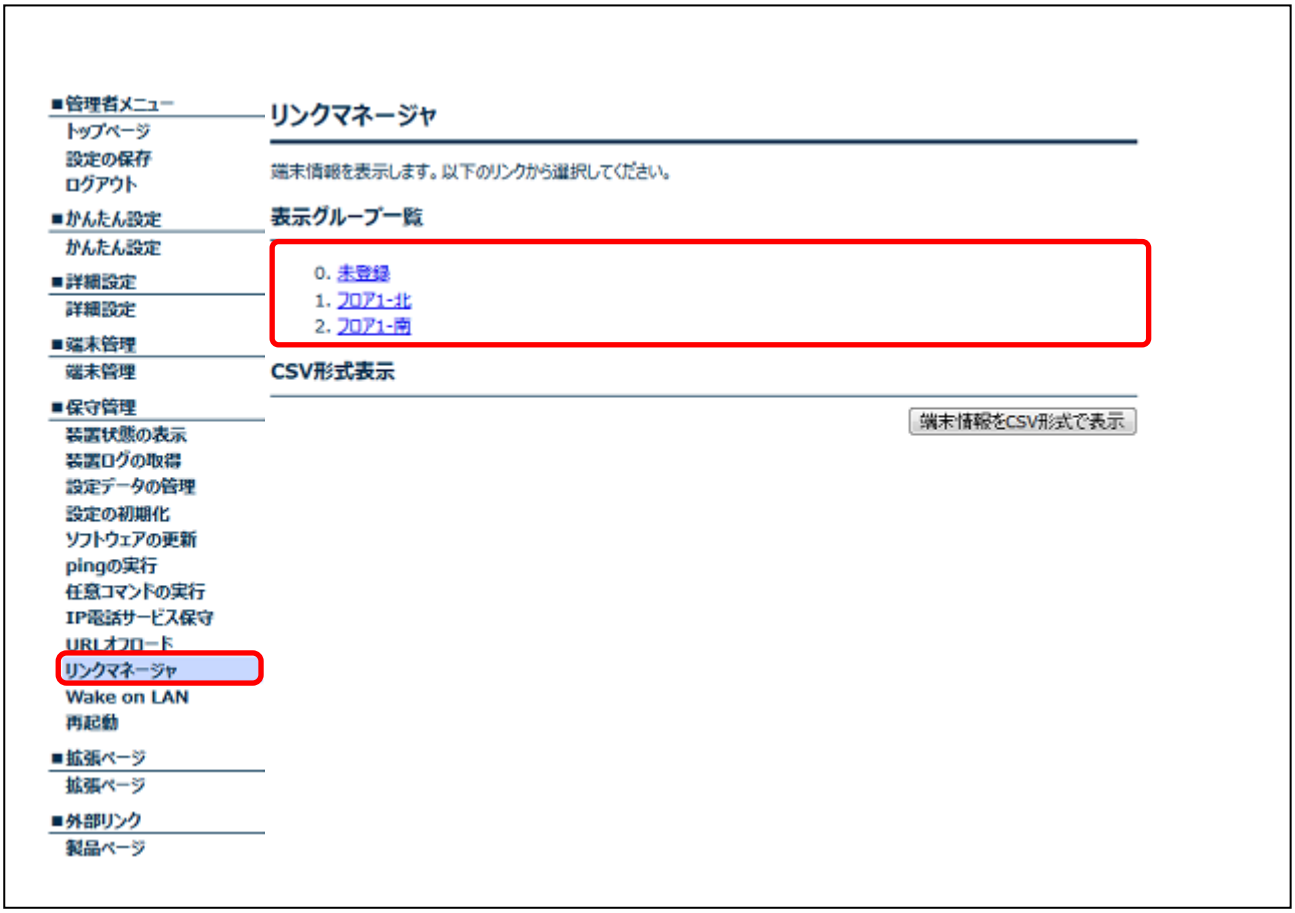
端末管理のリンクマネージャを登録している場合、端末の状態を確認することができます。

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し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[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。



(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。

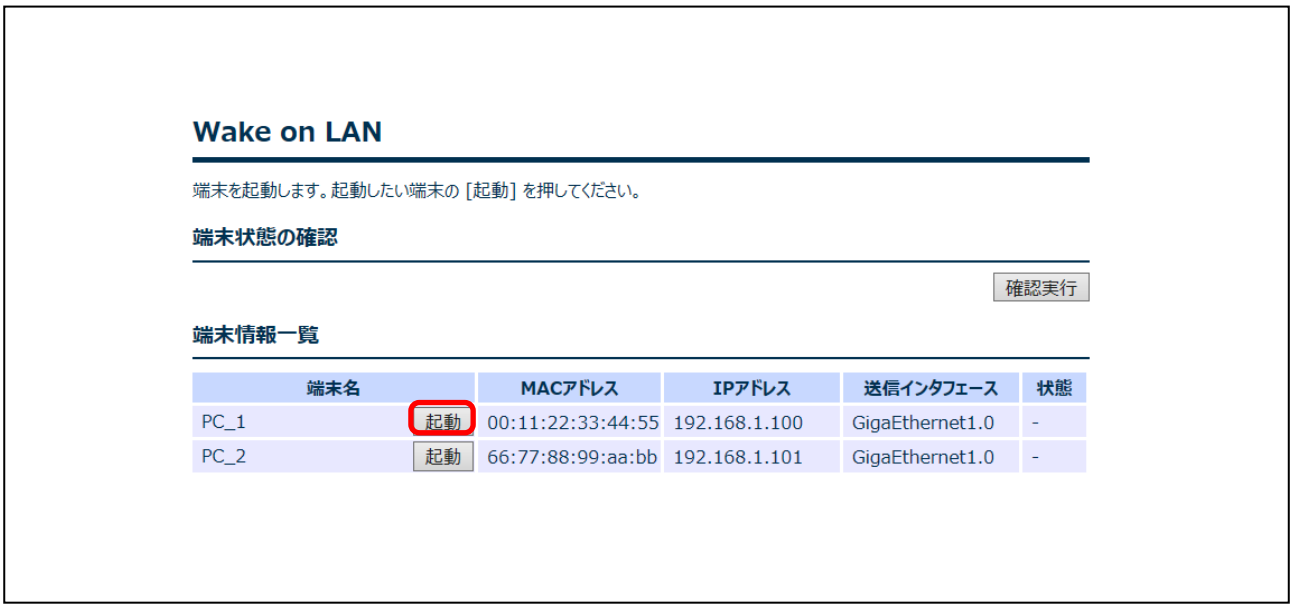
(1) メニューエリアの「保守管理」から[Wake on LAN]をクリックします。

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。



(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。

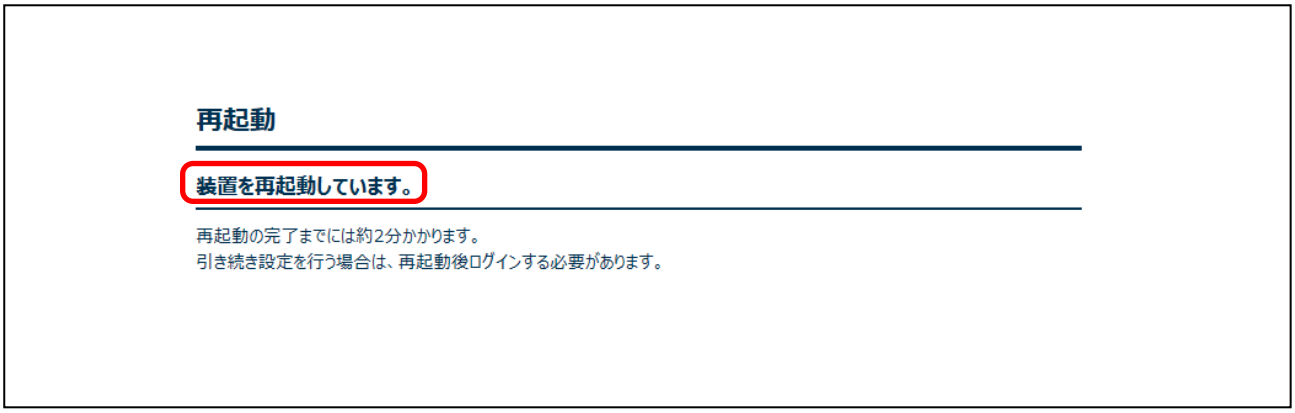
メモ　設定を変更したときは、設定の保存を行ってから再起動してください。

(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。

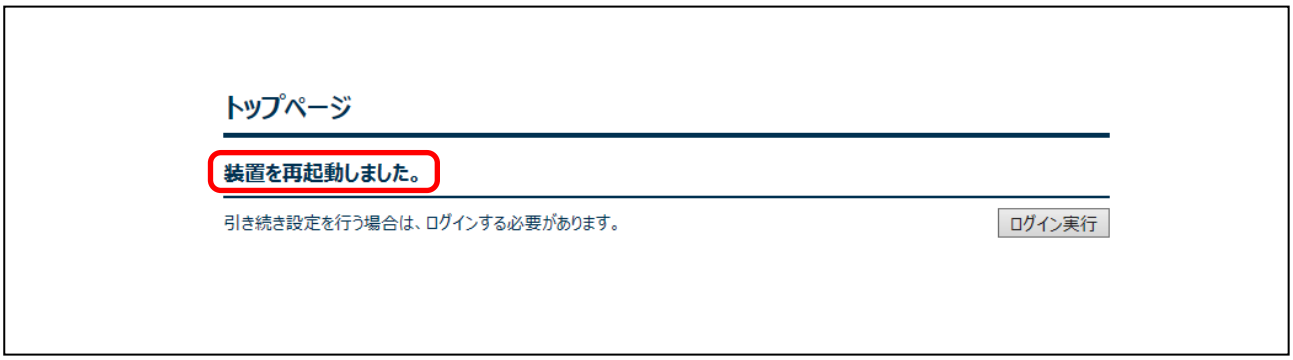
(2)　[再起動]をクリックします。

(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。

(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

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. 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。

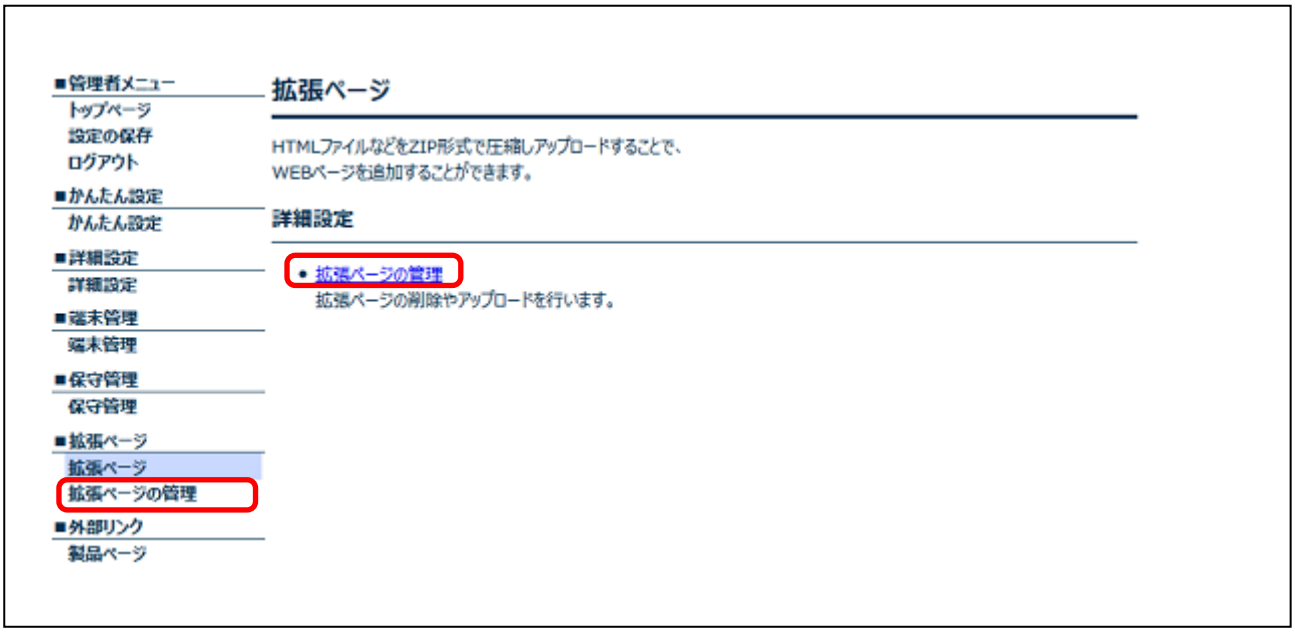
- html、htm、css、js
- jpeg、jpg、gif、png、bmp、ico

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。

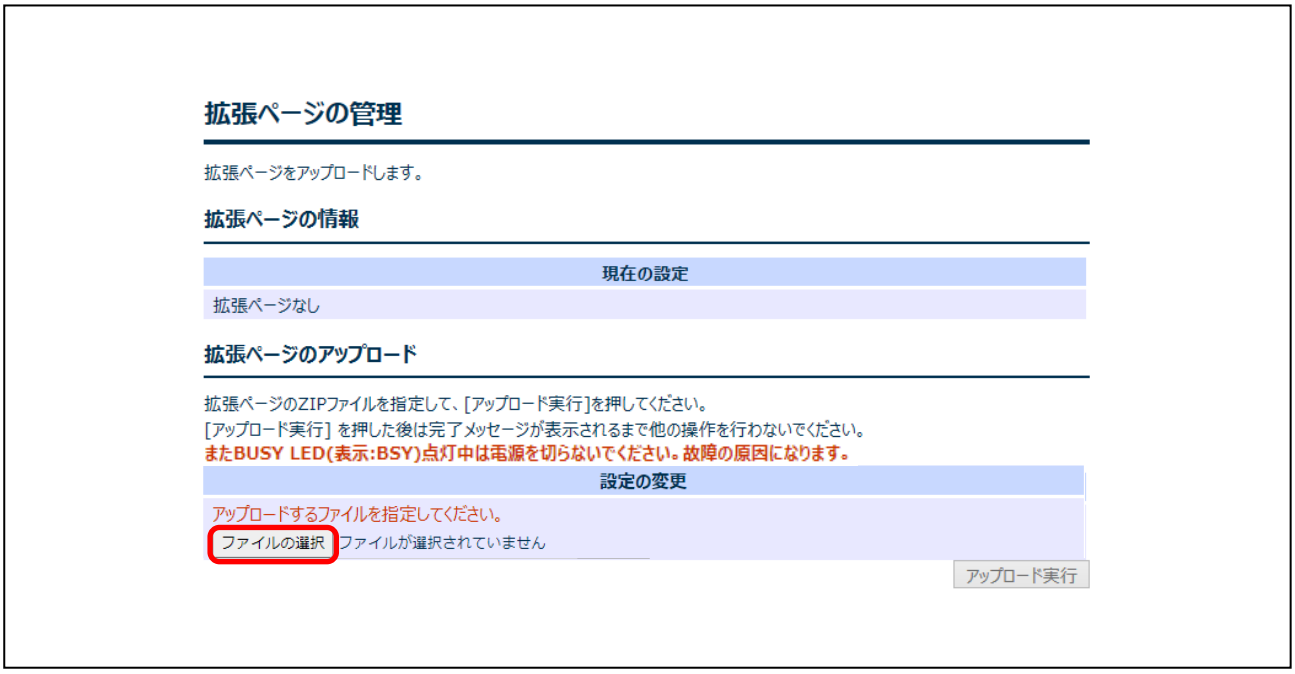
(2) 拡張ページの[拡張ページの管理]をクリックします。



7. 拡張ページ

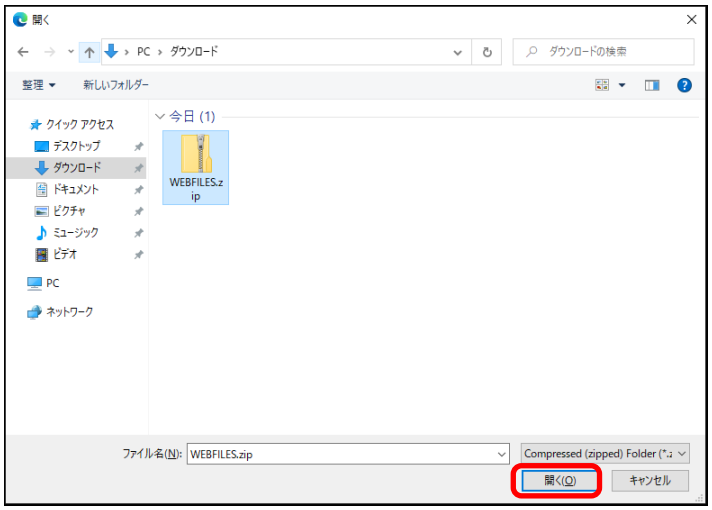
(3) 「拡張ページのアップロード」の[ファイルの選択]ボタンをクリックします。

メモ 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。

メモ 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。

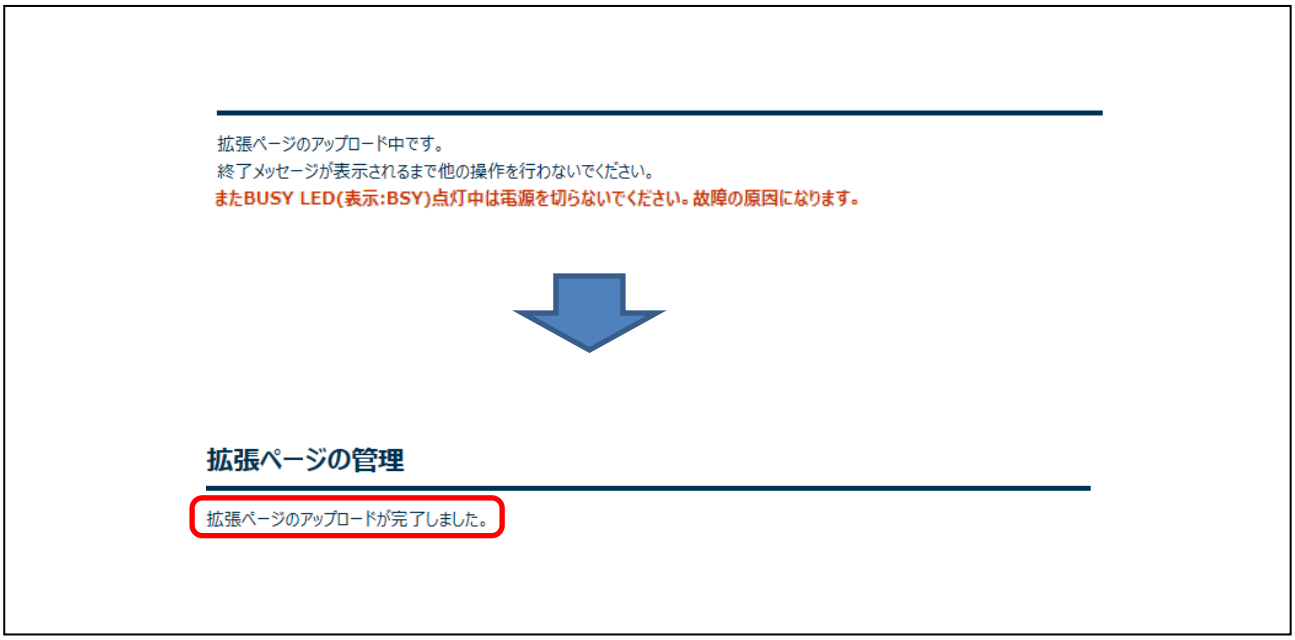


⑸ [アップロード実行]ボタンをクリックします。

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。

⑹ 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。



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。

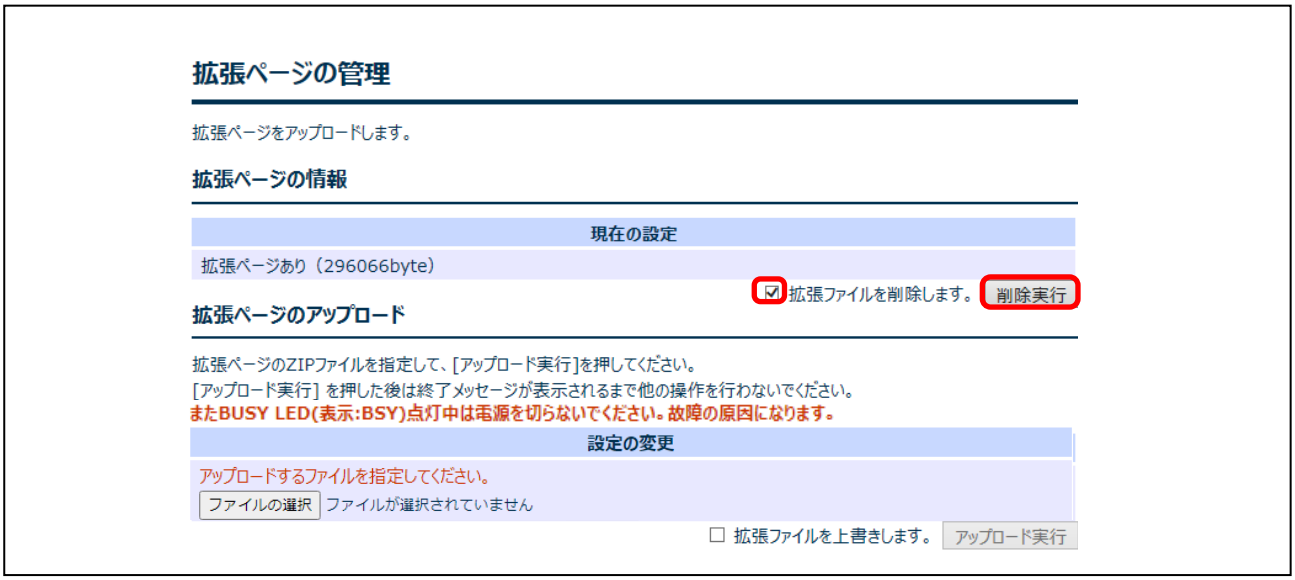
(1) ログイン後のメニューエリアから[拡張ページ]をクリックします。

(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。



(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

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。

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ました。
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ました。

UNIVERGE IX2000/IX3000シリーズ
Web設定マニュアル
GYS-096530-004-00

2026年4月 第1.1版
日本電気株式会社

日本電気株式会社

GYS-096530-004-00