

# NetVolanteシリーズ Web GUI

NVR700W Rev.15.00.03

NVR510 Rev.15.01.03

## Web GUIマニュアル

ヤマハ製品をお買い上げいただきありがとうございます。

Web GUIを使用する場合は、本書を参考にしてください。

## マニュアルのご案内

本書では、Web ブラウザーを使用してヤマハルーターの設定や管理を行う方を対象として、ヤマハルーターの Web GUI の使用方法を説明します。

弊社ではヤマハルーターの機能を十分に活用していただくために、様々なマニュアルを用意しています。

最新版のマニュアルは下記のヤマハネットワーク周辺機器技術情報ページに掲載します。

目的に合わせて適切なマニュアルをお読みください。

<http://www.rtpro.yamaha.co.jp/RT/manual.html>

ヤマハルーターをご使用中にトラブルが発生した場合は、以下の情報を参照して、問題を解決してください。

- ・ コマンドリファレンスを参照して、設定コマンドの使用方法を確認してください。
- ・ ヤマハネットワーク機器ホームページの設定例を参照して、設定を見直してください。  
<http://jp.yamaha.com/products/network/solution/>
- ・ ヤマハネットワーク機器技術情報ページで、障害の切り分け方法や設定事例集を参照して、設定を見直してください。  
<http://www.rtpro.yamaha.co.jp/RT/docs/>
- ・ 設定を見直してもトラブルが解決しない場合は、「取扱説明書」（製品付属の CD-ROM に収録）の「サポート窓口のご案内」を参照して、弊社のサポート窓口までご連絡ください。

- ◆ 本書の記載内容の一部または全部を無断で転載することを禁じます。
- ◆ この取扱説明書では、発行時点の最新仕様で説明をしております。取扱説明書の最新版につきましては、下記の Web サイトからダウンロードしてお読みいただけますよう、お願いいたします。  
<http://www.rtpro.yamaha.co.jp/RT/manual.html>
- ◆ ヤマハルーターを使用した結果により発生した情報の消失などの損失については、弊社ではいかなる責任も負いかねます。保証はヤマハルーターの物損の範囲に限ります。あらかじめご了承ください。

## 本書の表記について

### 表記の意味

本書では、ヤマハルーターを安全にお使いいただくため、以下のように表記します。


### ご注意


接続、操作、設定などで注意が必要なことを示します。

### メモ

操作や運用に関連した情報です。参考にお読みください。

NVR700W または NVR510 のみに関わる情報は以下のアイコンで表します。

: NVR700W のみに関わる記載を表します。

: NVR510 のみに関わる記載を表します。

### Web GUI の画面について

本書では、本書発行時点での Web GUI の画面を記載しています。実際の画面とは異なる場合があります。

### 例示用の IP アドレス / ドメイン名

本書では、グローバル IP アドレスやドメイン名を例示するとき、文書作成用途として RFC6890 / RFC6761 で予約されている IP アドレスとドメイン名の中から、以下に示す IP アドレス / ドメイン名を使用します。

IP アドレスの範囲 : 203.0.113.0/24

ドメイン名 : example.net

これらの IP アドレス / ドメイン名は通信で使用することはできません。実際に設定するときは、ご利用環境に合わせたものをお使いください。

### 略称について

本書ではそれぞれの製品について、以下のように略称で記載しています。

- ・ Microsoft® Windows® : Windows
- ・ Microsoft® Windows® 7 : Windows 7
- ・ Microsoft® Windows® 8.1 : Windows 8.1
- ・ Microsoft® Windows® 10 : Windows 10
- ・ 10BASE-T/100BASE-TX/1000BASE-T ケーブル : LAN ケーブル
- ・ 東日本電信電話株式会社 : NTT 東日本
- ・ 西日本電信電話株式会社 : NTT 西日本

### 商標について

- ・ Microsoft、Windows、Internet Explorer は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。
- ・ Google Chrome は、Google Inc. の登録商標です。
- ・ Mozilla、Firefox は、米国 Mozilla Foundation の米国およびその他の国における登録商標または商標です。
- ・ Apple、Macintosh、Safari は、米国および他の国々で登録された Apple Inc. の商標です。
- ・ iOS は、Apple Inc. の OS 名称です。
- ・ IOS は、Cisco Systems, Inc. またはその関連会社の米国およびその他の国における登録商標または商標です。
- ・ JavaScript は、Oracle Corporation およびその子会社、関連会社の米国およびその他の国における登録商標または商標です。

本書に記載されている会社名、製品名は各社の登録商標あるいは商標です。

# 目次

<b>第 1 章 はじめに</b> .....	<b>9</b>
1.1 Web GUI でできること .....	9
1.1.1 ダッシュボード .....	9
1.1.2 LAN マップ .....	9
1.1.3 かんたん設定 .....	10
1.1.4 詳細設定 .....	11
1.1.5 管理 .....	11
1.1.6 CONFIG .....	12
1.1.7 TECHINFO .....	12
1.1.8 ヘルプ .....	13
1.2 対応機器 / リビジョン .....	14
1.3 利用環境 .....	14
1.3.1 推奨 Web ブラウザー .....	14
1.3.2 JavaScript の設定 .....	14
1.4 ユーザーのアクセス権 .....	15
1.5 一般ユーザーと管理ユーザー .....	16
1.5.1 一般ユーザーと管理ユーザーのできることの違いや画面表示の違いなど .....	16
1.5.2 一般ユーザーと管理ユーザーの切り換え方法 .....	16
1.6 コマンド入力と併用する際のご注意 .....	16
<b>第 2 章 Web GUI へログインする</b> .....	<b>17</b>
<b>第 3 章 基本設定を行う</b> .....	<b>19</b>
3.1 日付と時刻を設定する .....	19
3.2 管理パスワードを設定する .....	21
3.3 LAN の IP アドレスを設定する .....	23
<b>第 4 章 IPv4 アドレスでインターネットに接続する</b> .....	<b>26</b>
4.1 ブロードバンド回線でインターネットへ接続する .....	26
4.1.1 接続方法を確認する .....	26
4.1.2 「PPPoE 接続」の場合 .....	30
4.1.3 「DHCP 接続」の場合 .....	35
4.2 無線 WAN 回線でインターネット接続する .....	39
4.2.1 内蔵無線 WAN でインターネットへ接続する (NVR700W) .....	39
4.2.2 USB 接続型データ通信端末でインターネットへ接続する .....	45
<b>第 5 章 IPv6 アドレスでインターネットに接続する</b> .....	<b>52</b>
5.1 フレッツ光 (IPv6 IPoE) でインターネットへ接続する .....	52
5.2 フレッツ光 (IPv6 PPPoE) でインターネットへ接続する .....	58
<b>第 6 章 ネットボランチ DNS サービスを利用する</b> .....	<b>64</b>
6.1 ネットボランチ DNS サービスとは? .....	64
6.2 ネットボランチ DNS サービスで取得できるホスト名 .....	65
6.3 ネットボランチ DNS ホスト名を取得する .....	65
6.4 ネットボランチ DNS ホスト名の登録を解除する .....	68
<b>第 7 章 拠点間を VPN で接続する</b> .....	<b>69</b>
7.1 VPN の設定をする前に .....	69



7.2	IPsec で接続する (NVR700W)	70
7.3	PPTP で接続する	76
7.4	IPIP で接続する	81
<b>第 8 章 外部から VPN 経由で LAN へアクセスする</b>		<b>86</b>
8.1	LAN 内のサーバーまたはパソコンの設定をする	87
8.2	L2TP/IPsec でリモートアクセスする	87
8.2.1	ヤマハルーターの設定 (L2TP/IPsec) をする	87
8.2.2	接続ユーザーを追加する	91
8.2.3	YMS-VPN8 の設定をする	93
8.2.4	YMS-VPN8 からヤマハルーターへリモートアクセスする	95
8.3	PPTP でリモートアクセスする	96
8.3.1	ヤマハルーターの設定 (PPTP) をする	96
8.3.2	接続ユーザーを追加する	100
8.3.3	Windows 7 でリモートアクセスする	102
8.3.4	Windows 8.1 でリモートアクセスする	106
8.3.5	Windows 10 でリモートアクセスする	110
<b>第 9 章 IP 電話を利用する</b>		<b>115</b>
9.1	基本設定をする	115
9.2	ひかり電話を設定する	117
9.3	SIP サーバーを設定する	121
9.3.1	楽天コミュニケーションズ系 SIP サーバーを設定する	121
9.3.2	その他の SIP サーバーを設定する	125
9.4	SIP 電話帳を設定する	129
9.5	ネットボランチ電話を設定する	133
<b>第 10 章 ダッシュボードを利用する</b>		<b>137</b>
10.1	ダッシュボードとは?	137
10.2	ダッシュボードの基本操作	138
10.2.1	ガジェットの追加と削除	138
10.2.2	ガジェットの移動	139
10.2.3	ガジェットの画面分離	140
10.2.4	ガジェットの最小化	141
10.2.5	ガジェットの位置情報の保存	141
10.2.6	ガジェットの自動更新	141
10.2.7	警告内容の確認	142
10.2.8	警告履歴表示	144
10.3	各ガジェットの説明	145
10.3.1	システム情報	145
10.3.2	リソース情報	146
10.3.3	インターフェース情報	147
10.3.4	トラフィック情報 (LAN/PP/TUNNEL)	149
10.3.5	プロバイダー接続状態	151
10.3.6	VPN 接続状態 (拠点間)	151
10.3.7	VPN 接続状態 (リモートアクセス)	152
10.3.8	NAT セッション数	152
10.3.9	ファストパスフロー数	152
10.3.10	動的フィルターセッション数	153
10.3.11	プロバイダー接続履歴	153
10.3.12	通話履歴	154

10.3.13 不正アクセス検知履歴 .....	154
10.3.14 SYSLOG .....	155

## **第 11 章 LAN マップを利用する..... 156**

11.1 LAN マップとは? .....	156
11.2 LAN マップの画面構成.....	156
11.2.1 マップページ.....	157
11.2.2 タグ VLAN ページ.....	157
11.2.3 マルチプル VLAN ページ .....	159
11.3 LAN マップを有効にする.....	160
11.4 スレーブの状態を確認する.....	162
11.5 ネットワークの異常を監視する.....	163
11.5.1 スレーブの動作状況と異常を監視する.....	164
11.5.2 ネットワークの接続状態を監視する.....	164
11.5.3 ネットワークの異常をメールで通知する.....	166
11.6 機器を検索する.....	167
11.7 ヤマハスイッチを設定する.....	169
11.7.1 スイッチの設定・保守ダイアログを表示する.....	169
11.7.2 ヤマハスイッチの機器名を変更する.....	172
11.7.3 省電力機能を設定する.....	172
11.7.4 ループ検出機能を設定する.....	173
11.7.5 ポートミラーリング機能を設定する.....	175
11.7.6 フレームカウンタをリセットする.....	176
11.7.7 ファームウェアを更新する.....	177
11.7.8 ヤマハスイッチを再起動する.....	180
11.7.9 ヤマハスイッチを初期化する.....	181
11.7.10 ポートの設定ダイアログを表示する.....	182
11.7.11 ポートの基本機能を設定する.....	184
11.7.12 QoS 機能を設定する.....	186
11.7.13 フレームカウンタを設定する.....	188
11.7.14 LAN ケーブル二重化機能を設定する.....	189
11.7.15 スイッチの指定方法を選択する.....	192
11.8 ヤマハ無線 AP の設定を行う.....	195
11.8.1 IP アドレスを変更する.....	195
11.8.2 無線 AP の指定方法を選択する.....	198
11.8.3 設定 (CONFIG) を保存する.....	200
11.8.4 設定 (CONFIG) を復元する.....	203
11.8.5 無線 AP の設定画面を表示する.....	206
11.9 タグ VLAN を設定する.....	207
11.9.1 タグ VLAN ページを表示する.....	208
11.9.2 タグ VLAN グループを作成する.....	209
11.9.3 タグ VLAN グループに参加させる.....	210
11.9.4 タグ VLAN グループを削除する.....	212
11.9.5 タグ VLAN 間フィルターを設定する.....	213
11.10 マルチプル VLAN を設定する.....	214
11.10.1 マルチプル VLAN ページを表示する.....	215
11.10.2 マルチプル VLAN グループを設定する.....	216
11.10.3 マルチプル VLAN グループの参加ポートを確認する.....	219
11.11 接続機器の一覧を見る.....	220
11.11.1 端末一覧画面を表示する.....	220
11.11.2 端末の情報を編集する.....	221

11.11.3	端末マスター画面を表示する	223
11.11.4	端末マスターに端末情報を新規登録する	224
11.11.5	端末マスターに登録されている端末情報を編集する	225
11.11.6	端末マスターファイルをパソコンへエクスポートする	227
11.11.7	端末マスターファイルをパソコンからインポートする	229
11.11.8	スレーブ一覧画面を表示する	230
11.11.9	スレーブの機器名を変更する	232
11.11.10	一覧マップで表示する	233
11.11.11	一覧マップを印刷する	235
<b>第 12 章</b>	<b>セキュリティを強化する</b>	<b>237</b>
12.1	不正アクセスとは?	237
12.1.1	グローバル IP アドレスが割り当てられている場合	237
12.1.2	パスワードを設定していない場合	238
12.2	不正アクセスに対抗する	238
12.2.1	不正アクセスによる侵入	238
12.2.2	OS やサーバソフトウェアのセキュリティホールからの侵入	238
12.2.3	電子メールの添付ファイルからの侵入	238
12.3	フィルターとは?	239
12.3.1	ヤマハルーターのフィルターの特徴	239
12.3.2	フィルター設定の基本	240
12.3.3	PING を許可する相手を限定する	241
12.3.4	PING をすべて破棄する	244
12.3.5	特定の端末だけ Web アクセスを許可する	248
12.4	ヤマハルーターへのアクセスを管理する	252
12.4.1	ログインを許可するユーザーを登録する	253
12.4.2	アクセス方法を変更する	255
12.4.3	パスワードを変更する	258
<b>第 13 章</b>	<b>詳細設定を行う</b>	<b>262</b>
13.1	LAN のアドレスを設定する	262
13.1.1	WAN のアドレスを設定する	264
13.1.2	セカンダリー IP アドレスも設定する	267
13.1.3	固定ではなく DHCP で設定する	269
13.2	ONU のアドレスを設定する	271
13.3	TEL ポートを設定する	274
13.4	グローバル IP アドレスを複数の端末でシェアする	276
13.5	外部にサーバーを公開する	281
13.5.1	IP アドレスの変換テーブルを登録する	282
13.5.2	IP アドレスの変換テーブルに合わせて静的フィルターを設定する	285
13.5.3	サーバーの公開先を限定する	289
13.6	複数のプロバイダーを使用する	293
13.6.1	複数のプロバイダーを設定する	293
13.6.2	端末ごとにプロバイダーを使い分ける	294
13.6.3	バックアップ回線を用意する	304
13.6.4	マルチホーミングによる負荷分散を行う	309
13.7	DNS サーバーを設定する	314
13.7.1	DNS サーバー機能の基本設定を行う	314
13.7.2	中継先 DNS サーバーを設定する	316
13.8	DHCP で端末に IP アドレスを割り当てる	320
13.9	異なるセグメントの DHCP サーバーから端末に IP アドレスを割り当てる	325

13.10 メール通知機能を使う.....	327
13.10.1 メールサーバーを設定する.....	327
13.10.2 メール通知を設定する.....	329
13.10.3 ヤマハルーターの内部状態をメールで通知する.....	331
<b>第 14 章 ヤマハルーターを管理する .....</b>	<b>333</b>
14.1 ヤマハルーターの日時を合わせる.....	333
14.1.1 日付と時刻を設定する.....	333
14.1.2 NTP サーバーと今すぐ同期する.....	335
14.2 ブザーを設定する.....	335
14.3 コマンドを実行する.....	337
14.4 ファームウェアを更新する.....	341
14.4.1 外部メモリを使用してファームウェアを更新する.....	341
14.4.2 ヤマハの Web サイトからネットワーク経由でファームウェアを更新する.....	344
14.4.3 社内サーバーからネットワーク経由でファームウェアを更新する.....	348
14.5 設定 (CONFIG) を管理する.....	351
14.5.1 設定 (CONFIG) を外部メモリにエクスポートする.....	352
14.5.2 設定 (CONFIG) を外部メモリからインポートする.....	354
14.6 SYSLOG を管理する.....	357
14.6.1 SYSLOG に出力する種別を変更する.....	357
14.6.2 SYSLOG をサーバーへ送信する.....	359
14.7 ヤマハルーターを再起動する.....	361
14.8 ヤマハルーターを工場出荷時の状態へ戻す.....	364
<b>第 15 章 独自の GUI を作成する (カスタム GUI) .....</b>	<b>367</b>
<b>第 16 章 付録 .....</b>	<b>368</b>
16.1 パソコンの IP アドレスを変更する.....	368
16.1.1 Windows 7 の場合.....	368
16.1.2 Windows 8.1 の場合.....	369
16.1.3 Windows 10 の場合.....	370
16.2 DNS サーバー機能にアクセスできるホストの設定を変更する.....	371
16.3 ヤマハルーターを譲渡 / 廃棄する際のご注意.....	374
16.3.1 設定内容を初期化する.....	374

# 第 1 章 はじめに

本章では、Web GUI の概要とお使いいただくために必要な事項を説明します。

## ご注意

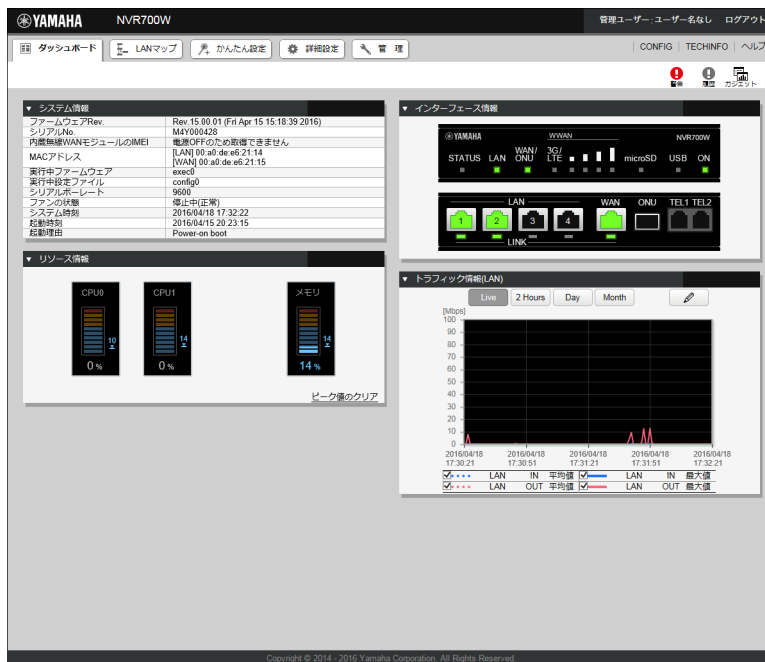
本書では、ヤマハルーター NVR700W の Web GUI の画面を使用しています。NVR510 をお使いの場合は、表示される画面が本書と異なる場合があります。

## 1.1 Web GUI でできること

ヤマハルーターは Web GUI を搭載しており、パソコンの Web ブラウザーを使って基本的な設定を行うことができます。また、設定だけでなく管理に便利な画面も搭載しています。Web GUI の画面構成について次節から説明します。

### 1.1.1 ダッシュボード

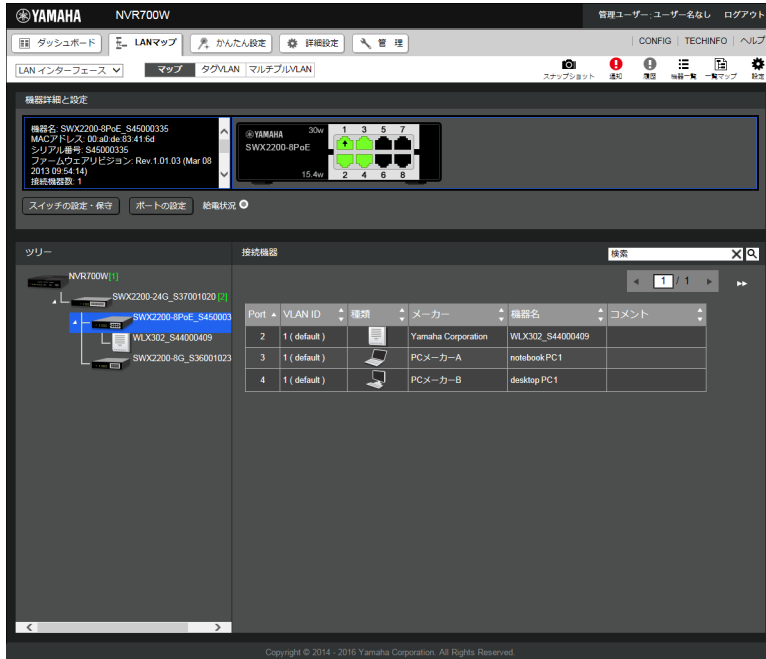
ダッシュボードページでは、各種システム情報やステータス情報を可視化、監視することができます。監視対象の各種パラメータが閾値以上の値になると警告メッセージが表示されるため、障害発生時の原因解析やトラブルシューティングにも利用できます。



### 1.1.2 LAN マップ

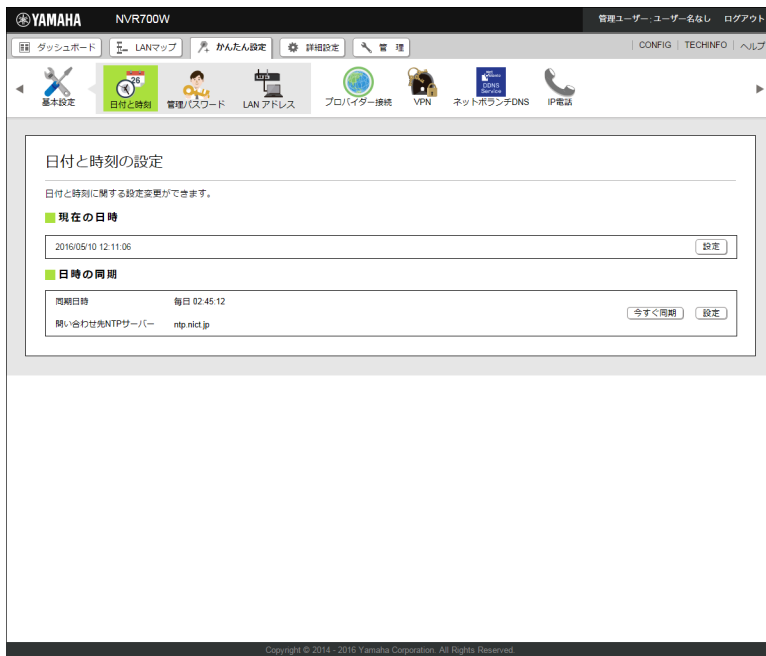
LAN マップページでは、LAN に接続されているヤマハネットワーク機器や通信端末の情報が表示され、LAN のネットワーク構成を確認することができます。また、ヤマハネットワーク機器の設定や VLAN の設定などを行うことができます。

ネットワークの異常も一目で把握することができるため、障害発生時の原因解析やトラブルシューティングにも利用できます。



### 1.1.3 かんたん設定

かんたん設定ページでは、ヤマハルーターの日付や時刻、管理パスワードなどのルーター本体に関する設定に加えて、インターネットに接続するための設定や VPN、ネットボランチ DNS、IP 電話に関する設定を行うことができます。ウィザード形式で設定できるため、専門知識がなくてもかんたんに設定することができます。



### 1.1.4 詳細設定

詳細設定ページでは、ヤマハルーターの NAT や IP フィルターなどの、ネットワークに関する詳細な設定を行うことができます。

現在の設定内容を表示しています。設定の追加、変更、削除ができます。

**ルーティング情報**

プロトコル	有効な経路数	無効な経路数
Static	2	0
implicit	2	0
Temporary	0	0
Redirect	0	0
RIP	0	0
OSPF	0	0
BGP	0	0
経路数の合計	4	0

**静的ルーティングの一覧**

優先ネットワーク	評価順	ゲートウェイ	オプション 有効基準	選択基準 フィルター型	メトリック
<input type="checkbox"/> default	1	dhcp lan2	-	500000	-
	2	pdp wan1	-	-	-

### 1.1.5 管理

管理ページでは、ヤマハルーターのファームウェアの更新や CONFIG ファイルの管理を行ったり、本体にアクセスするユーザーやパスワードの設定を行うことができます。

現在の設定内容を表示しています。

**CONFIGファイルのインポート**

CONFIGファイルを外部メモリからインポートします

**CONFIGファイルのエクスポート**

CONFIGファイルを外部メモリへエクスポートします

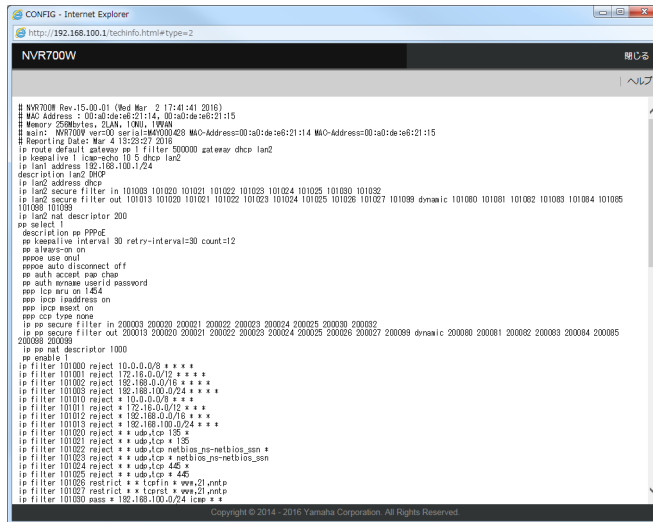
## 第 1 章 はじめに

### 1.1.6 CONFIG

CONFIG ページでは、ヤマハルーターの設定 (CONFIG) を Web ブラウザーで表示したり、テキストファイルで取得することができます。

ヤマハルーターは CONFIG に従って動作しています。CONFIG は複数のコマンドで構成されており、Web GUI から設定した内容もすべてコマンド形式で CONFIG に保存されます。

CONFIG ページを Web ブラウザーで表示するには、画面右上の「CONFIG」ボタンをクリックし、「ブラウザで表示」を選択します。



```
CONFIG - Internet Explorer
http://192.168.100.1/techinfo.html#type=2
NVR700W
# NVR700W Rev.15.00.01 (Wed Mar 2 17:41:41 2016)
# MAC Address : 00:sa0:de:ae:21:14, 00:sa0:de:ae:21:15
# Reentry 200000sec, 2LAN, 1LAN, 1WLAN
# Serial : NVR700W ver:00 ser:1a:9a:00:42:3 MAC-Address:00:sa0:de:ae:21:14 MIO-Address:00:sa0:de:ae:21:15
# Reentry Delay: Msr 4 15:25:27 2016
# route default gateway ip 1 filter 500000 gateway dhcp lan2
# hostname 1 | ipsec-echo 10 | dhcp lan2
# ip lan1 address 192.168.100.1/24
# description lan2 DHCP
# ip lan2 address dhcp
# ip lan2 secure filter in 101003 101020 101021 101022 101023 101024 101025 101090 101092
# ip lan2 secure filter out 101013 101020 101021 101022 101023 101024 101025 101026 101027 101099 dynamic 101080 101081 101082 101083 101084 101085
101090 101099
# ip lan2 nat descriptor 200
# ip nat 1
# description ip PPPoE
# ip nat ipsec Interval 30 retry-interval:30 count:12
# ip always-on on
# ipsec use on!
# ipsec auto disconnect off
# ip auth account pass chup
# ip auth monitor userid password
# ip tcp mru on 1634
# ip tcp ipaddress on
# ip tcp reset on
# ip tcp type none
# ip ps secure filter in 200003 200020 200021 200022 200023 200024 200025 200030 200032
# ip ps secure filter out 200013 200020 200021 200022 200023 200024 200025 200026 200027 200089 dynamic 200080 200081 200082 200083 200084 200085
200086 200089
# ip ps nat descriptor 1000
# ip enable 1
# ip filter 101000 reject 10.0.0.0/8 * * * *
# ip filter 101001 reject 172.16.0.0/16 * * * *
# ip filter 101002 reject 192.168.0.0/16 * * * *
# ip filter 101003 reject 192.168.100.0/24 * * * *
# ip filter 101010 reject * 10.0.0.0/8 * * *
# ip filter 101011 reject * 172.16.0.0/16 * * *
# ip filter 101012 reject * 192.168.0.0/16 * * *
# ip filter 101013 reject * 192.168.100.0/24 * * *
# ip filter 101020 reject * udb:tcp * 135
# ip filter 101021 reject * * udb:tcp * 135
# ip filter 101022 reject * * udb:tcp netbios_ns-netbios_ssn *
# ip filter 101023 reject * * udb:tcp * netbios_ns-netbios_ssn
# ip filter 101024 reject * * udb:tcp * 445
# ip filter 101025 reject * * udb:tcp * 445
# ip filter 101026 restrict * * tcp:in * www:21_ntlp
# ip filter 101027 restrict * * tcp:in * www:21_ntlp
# ip filter 101030 ssn * 192.168.100.0/24 |tcp * *
Copyright © 2014 - 2016 Yamaha Corporation. All Rights Reserved
```

#### メモ

テキストファイルで取得するには、画面右上の「CONFIG」ボタンをクリックし、「テキストファイルで取得」を選択します。取得したテキストファイルは UTF-8 でエンコードされています。

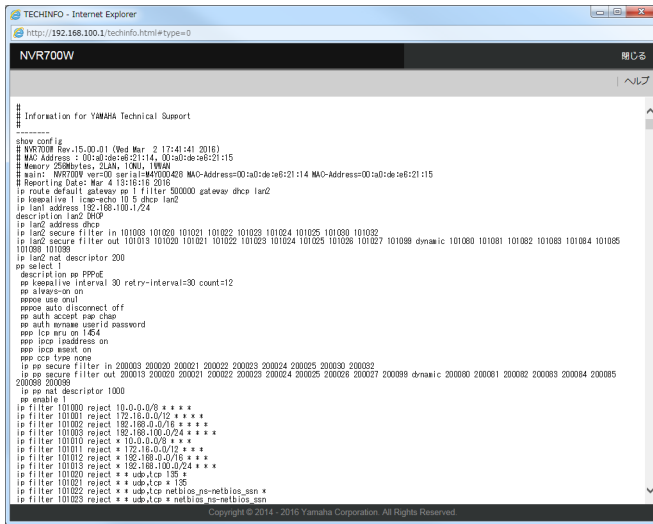
### 1.1.7 TECHINFO

TECHINFO ページでは、現在のヤマハルーターの設定や動作状態を Web ブラウザーで表示したり、テキストファイルで取得することができます。

お問い合わせ時にヤマハルーターの状態を把握するために、設定や動作状態を確認させていただくことがあります。



TECHINFO ページを Web ブラウザーで表示するには、画面右上の「TECHINFO」ボタンをクリックし、「ブラウザで表示」を選択します。



```
show conf #
NVR700W Rev.15.00.01 (Wed Mar 2 17:41:41 2016)
MAC Address : 00:a0:96:9e:21:14, 00:a0:96:9e:21:15
Memory : 256MB, CPU: 1000, 1000
Main: NVR700W ver=00 serial=M4Y030409 MAO-Address=00:a0:de:9e:21:14 MAO-Address=00:a0:de:9e:21:15
Recording Date: Mar 4 13:16:18 2016
ip route default gateway ip filter 500000 gateway dhcp lan2
ip forwarding ipsec-eth0 ip s dhcp lan2
ip lan1 address 192.168.100.1/24
description lan2 200
ip lan2 address dhcp
ip lan2 secure filter in 101003 101020 101021 101022 101023 101024 101025 101026 101027 101028 101029 101030
101008 101009
ip lan2 nat descriptor 200
no select 1
description sp PPPoE
no keepalive interval 30 retry-interval=30 count=12
no always-on on
no sleep on on
no auto disconnect off
no auto reconnect on
no auth name user id password
no ipsec on ipsec
no ipsec ip address on
no ipsec main on
no oca type none
ip secure filter in 200003 200020 200021 200022 200023 200024 200025 200030 200032
200033 200036
ip secure filter out 200013 200020 200021 200022 200023 200024 200025 200026 200027 200089 dynamic 200060 200061 200062 200063 200064 200065
200089 200090
ip nat descriptor 1000
no enable 1
ip filter 101000 reject 10.0.0.0/8 * * * *
ip filter 101001 reject 172.16.0.0/16 * * * *
ip filter 101002 reject 192.168.0.0/16 * * * *
ip filter 101003 reject 192.168.100.0/24 * * * *
ip filter 101004 reject 10.0.0.0 * * * *
ip filter 101005 reject * 192.168.0.0/16 * * * *
ip filter 101006 reject * 192.168.100.0/24 * * * *
ip filter 101007 reject * * udp tcp 135 *
ip filter 101008 reject * * udp tcp * 135
ip filter 101009 reject * * udp tcp * netbios-ssn *
ip filter 101020 reject * * udp tcp * netbios-ns-netbios-ssn *
Copyright © 2014 - 2016 Yamaha Corporation. All Rights Reserved.
```

## メモ

テキストファイルで取得するには、画面右上の「TECHINFO」ボタンをクリックし、「テキストファイルで取得」を選択します。取得したテキストファイルは UTF-8 でエンコードされています。

### 1.1.8 ヘルプ

ヘルプページでは、Web GUI の各設定画面の設定項目について、詳しい説明が記載されています。ヘルプページを表示するには、画面右上の「ヘルプ」ボタンをクリックしてください。



```
Copyright © 2014 - 2016 Yamaha Corporation. All Rights Reserved.
```

## 第 1 章 はじめに

### 1.2 対応機器 / リビジョン

本書は下記のヤマハネットワーク機器に対応しています。

対応機器	リビジョン
NVR700W	Rev.15.00.03
NVR510	Rev.15.01.03

### 1.3 利用環境

Web GUI を利用するための環境について説明します。

#### 1.3.1 推奨 Web ブラウザー

下記の Web ブラウザーでのご利用を推奨します。

##### Windows

- ・ Microsoft Internet Explorer 11
- ・ Mozilla Firefox
- ・ Google Chrome

##### Macintosh

- ・ Apple Safari

##### iOS

- ・ Apple Safari

##### メモ

Mozilla Firefox、Google Chrome、Apple Safari の推奨バージョンについては、下記の URL をご覧ください。

<http://www.rtpo.yamaha.co.jp/RT/FAQ/gui/browser.html>

##### ご注意

Web ブラウザーの「戻る」、「進む」ボタンは使用しないでください。使用すると意図しない動作につながる場合があります。

##### メモ

Web GUI の文字エンコードは UTF-8 になります。

#### 1.3.2 JavaScript の設定

Web GUI では JavaScript を利用しています。お使いの Web ブラウザーで JavaScript の設定が無効になっていると、Web GUI が利用できない場合があります。以下の手順で、JavaScript を有効に設定してからご利用ください。

##### Windows 版 Internet Explorer 11 の設定方法

1. Internet Explorer のメニューバーで「ツール」 - 「インターネットオプション」を順に選択する。

「インターネットオプション」画面が表示されます。

**メモ**

メニューバーが表示されていない場合は、キーボードの「Alt」キーを押すと表示されます。

2. 「セキュリティ」タブをクリックする。
3. 「インターネット」（地球マーク）が表示されているのを確認し、「既定のレベル」ボタンをクリックする。  
ボタンが押せない場合は「既定のレベル」が選択されているので、手順 4 に進みます。
4. 「OK」ボタンをクリックする。

**Windows 版 Mozilla Firefox の設定方法**

Firefox の JavaScript 設定については、Firefox のサポートページを参考にしてください。

<https://support.mozilla.org/ja/kb/javascript-settings-for-interactive-web-pages>

**Windows 版 Google Chrome の設定方法**

1. Google Chrome のツールバーの「Google Chrome の設定」アイコン - 「設定」を順に選択する。
2. 「詳細設定を表示」をクリックする。
3. 「プライバシー」項目の「コンテンツの設定」ボタンをクリックする。
4. 「Javascript」項目の「すべてのサイトで Javascript の実行を許可する（推奨）」を選択し、「完了」ボタンをクリックする。

**Macintosh 版 Safari 7 の設定方法**

1. Safari のメニューバーの「Safari」- 「環境設定」を選択します。
2. 「セキュリティ」ボタンをクリックする。
3. 「プラグインを許可」と「JavaScript を有効にする」にチェックを入れる。
4. 「セキュリティ」ウィンドウを閉じる。

**iOS 版 Safari の設定方法**

1. ホーム画面で、「設定」をタップする。
2. 「Safari」- 「詳細」を順に選択する。
3. 「JavaScript」のスライダーを右に動かして「オン」にする。

## 1.4 ユーザーのアクセス権

Web GUI にログインするユーザーは、一般ユーザーと管理ユーザーの 2 つに分類されます。これをアクセスレベルと呼びます。

アクセスレベルの違いは、以下のとおりです。

アクセスレベル	説明
一般ユーザー	ヤマハルーターの設定内容や通信ログを参照できます。設定の変更はできません。
管理ユーザー	ヤマハルーターの設定を行えます。また、設定内容や通信ログを参照できます。

### メモ

- ・ ログインパスワードを入力した場合は、一般ユーザーとしてログインします。
- ・ 管理パスワードを入力した場合は、管理ユーザーとしてログインします。
- ・ ログインパスワードと管理パスワードが同じ設定（もしくは工場出荷時のように何も設定されていない）の場合は、常に管理ユーザーとしてログインします。
- ・ 管理パスワードの設定は、「3.2 管理パスワードを設定する」（21 ページ）をご覧ください。
- ・ ユーザー登録とログインパスワードの設定は、「12.4.1 ログインを許可するユーザーを登録する」（253 ページ）をご覧ください。

## 1.5 一般ユーザーと管理ユーザー

本章では、一般ユーザー、管理ユーザーのログイン仕様について説明します。

### 1.5.1 一般ユーザーと管理ユーザーのできることの違いや画面表示の違いなど

#### 一般ユーザーとしてログインした場合：

ヤマハルーターの設定内容や動作状態を確認できます。ただし、ヤマハルーターの設定変更や初期化、再起動、ファームウェアの更新などの操作は行えません。これらの操作に関連するボタンはすべてグレイアウトされ、クリックすることができないようになっています。

#### 管理ユーザーとしてログインした場合：

Web GUI のすべての操作が可能となります。ヤマハルーターの設定内容や動作状態の確認だけでなく、ヤマハルーターの設定変更や初期化、再起動、ファームウェアの更新など、すべての操作を行うことができます。

### 1.5.2 一般ユーザーと管理ユーザーの切り換え方法

現在ログインしているアクセス権を切り替えるには、一度ログアウトした後に、切り替えたいアクセス権でログインしなおす必要があります。一般ユーザーから管理ユーザーに切り替える手順を例に説明します。

1. 画面右上の「ログアウト」ボタンをクリックし、ログアウトします。
2. Web ブラウザーを一旦終了し、再度 Web ブラウザーを起動します。
3. ヤマハルーターの Web GUI にアクセスし、ユーザー名とパスワードを入力する画面で、管理ユーザー権限を持ったユーザー名と管理パスワードを入力します。

### メモ

現在ログインしているアクセス権の情報やユーザー名は常に画面右上に表示されています。

## 1.6 コマンド入力と併用する際のご注意

ヤマハルーターは Web GUI による設定だけでなく、コマンドコンソール画面で直接コマンドを入力して設定することもできます。コマンド入力による設定では、Web GUI よりも多様な設定ができたり、Web GUI ではサポートしていない機能の設定を行ったりすることができます。ただし、コマンド入力による設定の後で Web GUI から設定を変更すると、入力したコマンドが削除されたり、コマンドの一部が書き換わったりすることがあります。コマンド入力と Web GUI を併用する際は、必ず画面右上の「CONFIG」ボタンから CONFIG を閲覧し、入力したコマンドが書き換わっていないことをご確認ください。

### メモ

Web GUI にもコマンド入力画面があり、そこからコマンド入力を行った場合も同様です。Web GUI のコマンド入力画面を表示するには、「管理」タブ - 「保守」 - 「コマンドの実行」を順に選択してください。また、コマンドの詳細については「コマンドリファレンス」（製品付属の CD-ROM に収録）をご覧ください。

## 第 2 章 Web GUI へログインする

本章では、Web GUI へのログイン方法を説明します。Web GUI にログインするには、ヤマハルーターに接続するためのパソコンと Web ブラウザーが必要です。なお、工場出荷状態ではユーザー名とパスワードは設定されていません。

本章では Windows 7 で Internet Explorer 11 を使用した場合の画面を例に説明します。他の環境の場合は画面表示が多少異なりますが基本的な操作は同じです。

1. ヤマハルーターの LAN ポートとパソコンを LAN ケーブルで接続する。
2. パソコンで Web ブラウザーを起動する。
3. アドレスバーに「<http://setup.netvolante.jp>」と半角英字で入力するか、または、「[http://\(ヤマハルーターに設定した IP アドレス\)/](http://(ヤマハルーターに設定した IP アドレス)/)」と半角英数字で入力して、Enter キーを押す。  
ユーザー名とパスワードを入力する画面が表示されます。

### メモ

工場出荷状態ではヤマハルーターの LAN ポートの IP アドレスは「192.168.100.1」に設定されているため、アドレスバーに「<http://192.168.100.1/>」と入力します。

4. 設定したユーザー名とパスワードを「ユーザー名」、「パスワード」に入力し、「OK」ボタンをクリックする。



パスワードには管理ユーザー用の管理パスワードと一般ユーザー用のログインパスワードの 2 種類が存在します。管理ユーザーとしてログインする場合は管理パスワードを、一般ユーザーとしてログインする場合はログインパスワードを入力してください。

### メモ

- ・ 工場出荷状態ではユーザー名とパスワードは設定されていません。ユーザー名とパスワードが設定されていない場合は、「ユーザー名」と「パスワード」は空欄のまま「OK」ボタンをクリックしてください。
- ・ ユーザー名を登録せず、管理パスワードまたはログインパスワードのみを設定している場合は、「ユーザー名」は空欄のまま、「パスワード」に管理パスワードまたはログインパスワードを入力し、「OK」ボタンをクリックしてください。
- ・ ユーザーのアクセス権については、「1.4 ユーザーのアクセス権」(15 ページ) をご覧ください。

### 工場出荷状態のヤマハルーターの Web GUI に Safari からログインする場合

「ユーザー名」に「anonymous」と半角英字で入力し「パスワード」は空欄のまま、「OK」ボタンをクリックしてください。

Web GUI のダッシュボードが表示されます。また、工場出荷状態からの初回ログイン時は「データ蓄積の設定」ダイアログが表示されますので「OK」ボタンをクリックしてください。

## 第2章 Web GUI へログインする

### パスワードについて

- ・ パスワードは必ず半角の英数字で入力してください。全角文字は使用できません。また大文字 / 小文字の違いも判別します。
- ・ 誤ったユーザー名 / パスワードが Web ブラウザーに記憶されていると、ユーザー名とパスワードを入力する画面が表示されないことがあります。Web ブラウザーを一旦終了させてから、もう一度 Web GUI にアクセスしてください。なお、自動ログイン用のユーザー情報を登録している場合は削除してください。
- ・ 設定したパスワードは忘れないようにしてください。万が一パスワードを忘れてしまった場合は、ヤマハルーターの設定を行った管理者に、正しいパスワードをお問い合わせください。

### ログアウトのしかた

画面右上の「ログアウト」ボタンをクリックしてください。また、他のユーザーでログインしなおす場合は、ログアウト後に Web ブラウザーを一旦終了させてから、再度本章の手順に従ってログインしてください。

## 第3章 基本設定を行う

本章では、ヤマハルーターの基本設定について説明します。

- ・ 日付と時刻を設定する …19 ページ
- ・ 管理パスワードを設定する …21 ページ
- ・ LAN の IP アドレスを設定する …23 ページ

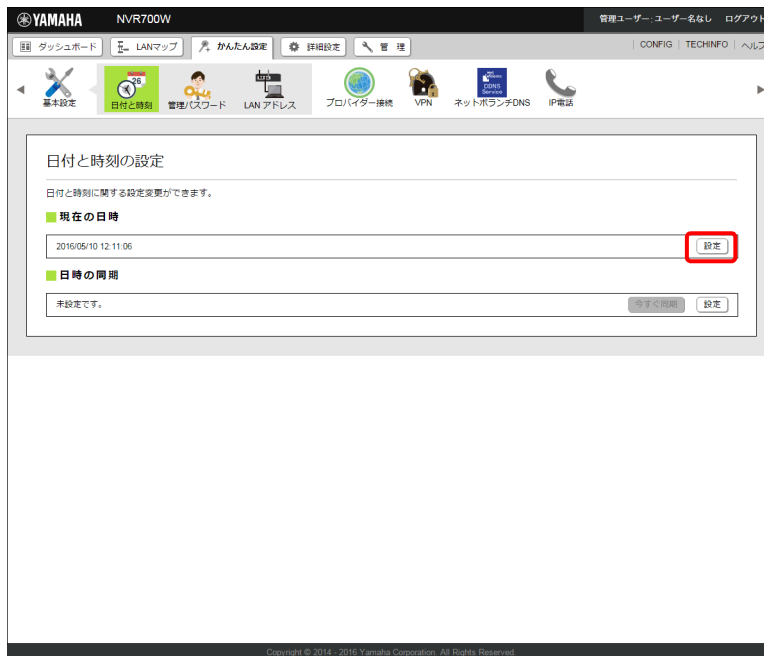
### 3.1 日付と時刻を設定する

ヤマハルーターの日付と時刻を合わせます。

#### メモ

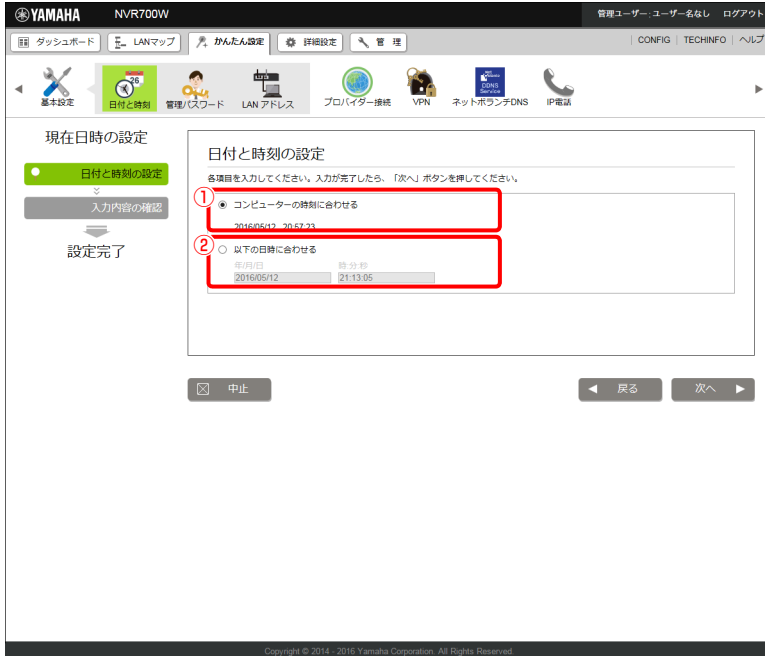
「日時の同期」については、「14.1 ヤマハルーターの日時を合わせる」(333 ページ) をご覧ください。

1. 「かんたん設定」タブ – 「基本設定」 – 「日付と時刻」 ボタンを順に選択する。  
「日付と時刻の設定」画面が表示されます。
2. 「現在の日時」項目の「設定」 ボタンをクリックする。



## 第3章 基本設定を行う

### 3. 日時を設定する。



#### ① コンピューターの時刻に合わせる：

現在お使いのコンピューターに設定されている時刻と、同じ時刻を設定します。

#### ② 以下の日時に合わせる：

設定する日時を入力します。

- ・「年 / 月 / 日」：日付を YYYY/MM/DD 形式で入力します。「年 / 月 / 日」欄にフォーカスを合わせるとカレンダーが表示され、カレンダーから日付を選択することもできます。
- ・「時 : 分 : 秒」：時刻を hh:mm:ss 形式で入力します。「時 : 分 : 秒」欄にフォーカスを合わせると時刻のリストが表示され、リストから時刻を選択することもできます。

### 4. 「次へ」 ボタンをクリックする。

「入力内容の確認」画面が表示されます。



## 5. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が変更され、「日付と時刻の設定」画面が表示されます。

## 3.2 管理パスワードを設定する

ヤマハルーターの管理パスワードを変更することができます。工場出荷状態ではヤマハルーターの管理パスワードは設定されていません。セキュリティ対策を行ううえでも、パスワードを設定することをおすすめします。

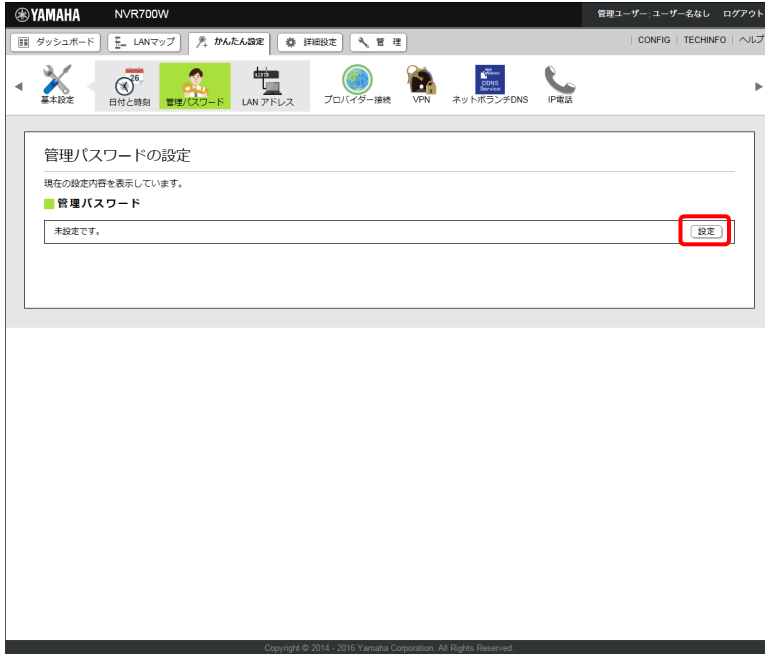
### メモ

- ・ パスワードを設定すると、ヤマハルーターにアクセスする際にパスワード入力が必要となるので、第三者がヤマハルーターの設定を変更することが困難になります。
- ・ ヤマハルーターのパスワードには管理パスワードとログインパスワードの2つがあります。ログインパスワードの設定方法については、「12.4 ヤマハルーターへのアクセスを管理する」(252ページ)をご覧ください。

1. 「かんたん設定」タブ - 「基本設定」 - 「管理パスワード」ボタンを順に選択する。  
「管理パスワードの設定」画面が表示されます。

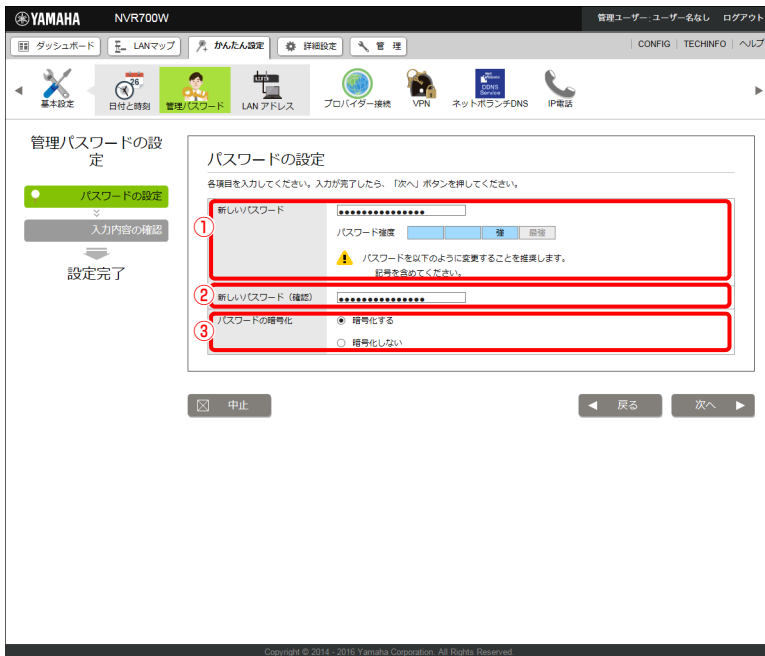
## 第3章 基本設定を行う

### 2. 「管理パスワード」項目の「設定」ボタンをクリックする。



「パスワードの設定」画面が表示されます。

### 3. 管理パスワードを設定する。



#### ① 新しいパスワード：

新しい管理パスワードを入力します。入力したパスワードは、●で表示されます。

#### ② 新しいパスワード (確認)：

新しい管理パスワードを再入力します。入力したパスワードは、●で表示されます。

## ③ パスワードの暗号化：

管理パスワードを暗号化して保存するか選択します。暗号化せずに保存すると、CONFIG を表示したときにパスワードがそのまま表示されます。すでに設定済みのパスワードに対して、暗号化の有無のみを変更することはできません。

4. 「次へ」 ボタンをクリックする。  
「入力内容の確認」画面が表示されます。
5. 内容を確認し、「設定の確定」 ボタンをクリックする。



設定が変更され、ユーザー名とパスワードを入力する画面が表示されます。

6. 設定したパスワードを「パスワード」に入力し、「OK」 ボタンをクリックする。



「管理パスワードの設定」画面が表示されます。

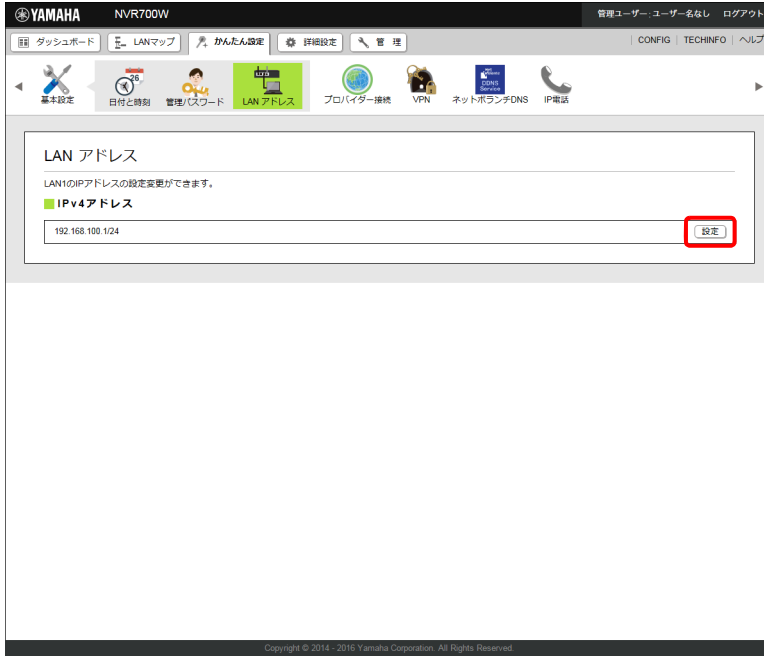
### 3.3 LAN の IP アドレスを設定する

ヤマハルーターの LAN の IP アドレスを変更することができます。すでに異なるネットワークアドレスが設定されているネットワークに設置する場合は、そのネットワークアドレスに応じた IP アドレスとネットマスクを

### 第3章 基本設定を行う

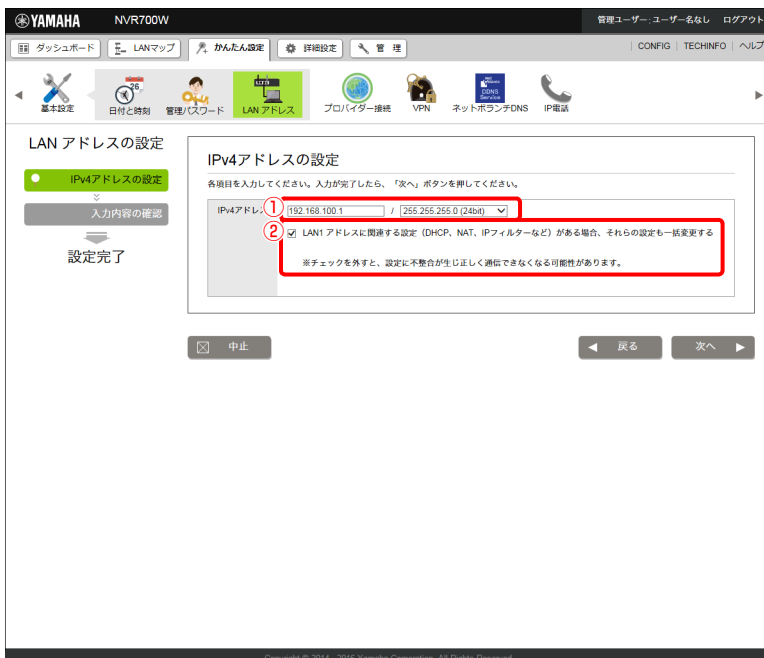
ヤマハルーターに設定してください。また、ヤマハルーターには、LAN内にすでに設置されている他の機器のIPアドレスと重複しないIPアドレスを設定してください。

1. 「かんたん設定」タブ - 「基本設定」 - 「LAN アドレス」 ボタンを順に選択する。  
「LAN アドレス」画面が表示されます。
2. 「IPv4 アドレス」項目の「設定」ボタンをクリックする。



「IPv4 アドレスの設定」画面が表示されます。

3. LAN の IP アドレスを設定する。



## ① アドレス入力欄：

新しく設定する IPv4 アドレスを入力します。ネットマスクは、「192.0.0.0 (2bit)」から「255.255.255.252 (30bit)」までの中から選択します。

## ② LAN1 アドレスに関連する設定 (DHCP、NAT、IP フィルターなど) がある場合、それらの設定も一括変更する：

選択すると、LAN インターフェースの IP アドレスの設定変更に合わせて、その他の設定に含まれる IP アドレスのパラメーターを自動的に変換します。

選択しないときは、IP アドレスの変更後に必要に応じて手動で設定を行ってください。

対象となる設定は以下のとおりです。

- ・ DHCP の設定
- ・ 静的 IP フィルター (始点 IP アドレス、終点 IP アドレス)
- ・ 動的 IP フィルター (始点 IP アドレス、終点 IP アドレス)
- ・ NAT ディスクリプター内側アドレス
- ・ NAT ディスクリプター静的 NAT (内側アドレス)
- ・ NAT ディスクリプター変換ルールに該当しないパケットの処理 (転送先端末のアドレス)
- ・ NAT ディスクリプター静的 IP マスカレード (内側アドレス)
- ・ DHCP で払い出す IP アドレス
- ・ IP キープアライブ (始点 IP アドレス)
- ・ トンネルインターフェース端点 IP アドレス (ローカル IP アドレス)

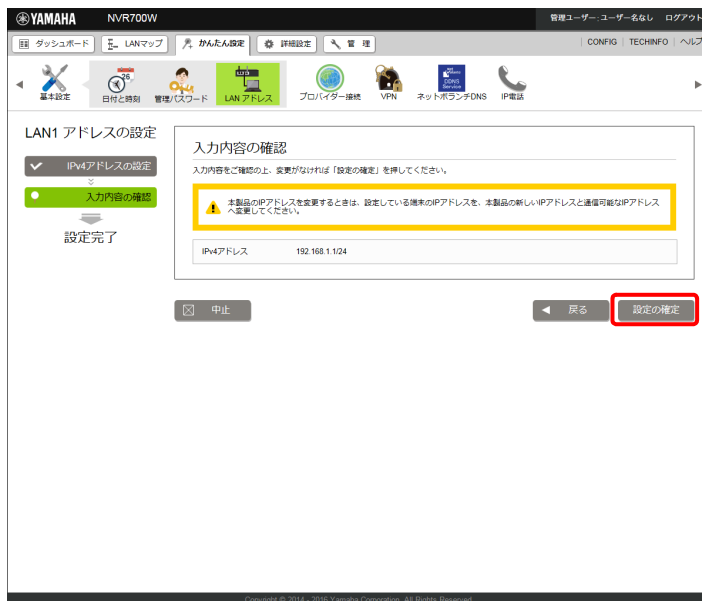
## ご注意

チェックを外すと設定に不整合が生じ、正しく通信できなくなる可能性があります。

## 4. 「次へ」 ボタンをクリックする。

「入力内容の確認」画面が表示されます。

## 5. 内容を確認し、「設定の確定」 ボタンをクリックする。



設定が変更され、「LAN アドレスの変更」画面が表示されます。「LAN アドレスの変更」画面の指示にしたがって、Web GUI に再ログインしてください。

## ご注意

LAN インターフェースの IP アドレスを変更するときや変更したあとは、LAN インターフェースのネットワークアドレスに合わせてパソコンなどの接続機器の IP アドレスも変更してください。

# 第 4 章 IPv4 アドレスでインターネットに接続する

本章では、IPv4 アドレスでインターネットに接続する方法について説明します。ヤマハルーターに接続するインターネット回線に合わせて、必要な接続方法を選んでください。

- ・ブロードバンド回線でインターネットへ接続する …26 ページ
- ・無線 WAN 回線でインターネット接続する …39 ページ

## メモ

本章では Windows 7 で Internet Explorer 11 を使用した場合の画面を例に説明します。他の環境の場合は画面表示が多少異なりますが基本的な操作は同じです。

## 4.1 ブロードバンド回線でインターネットへ接続する

ブロードバンド回線（PPPoE または CATV）を使用してインターネットに接続します。インターネット接続に使用するプロバイダーの設定資料を用意してください。

### ご注意

- ・プロバイダー契約を解除または変更したときは、必ずヤマハルーターの接続設定を削除または再設定してください。削除しないまま使っていると、回線業者やプロバイダーから意図しない料金を請求される場合があります。
- ・インターネットへ常時接続する場合は、インターネット側から不正なアクセスや攻撃を受ける危険性が高くなります。セキュリティには十分ご注意のうえ、お使いください。詳しくは「第 12 章 セキュリティを強化する」(237 ページ) をご覧ください。

### プロバイダーの設定資料

接続先を設定してインターネットに接続するには、プロバイダーから通知される以下の情報が必要です（接続方法によっては、必要のないものもあります）。

- ・ユーザー ID（認証 ID、アカウント名）
- ・パスワード（認証パスワード、初期パスワード）
- ・IP アドレス
- ・ネットマスク
- ・ネームサーバーアドレス
- ・デフォルト・ゲートウェイ・アドレス

## メモ

ネームサーバーアドレスはプロバイダーによって、DNS サーバーアドレスやネームサーバー IP アドレス、DNS サーバー IP アドレスなど呼び名が異なることがあります。

### 4.1.1 接続方法を確認する

1. LAN ケーブルで ONU やモデムとヤマハルーターの WAN ポートを接続する。  
または小型 ONU を ONU ポートに接続して、光ケーブルを小型 ONU に接続する。

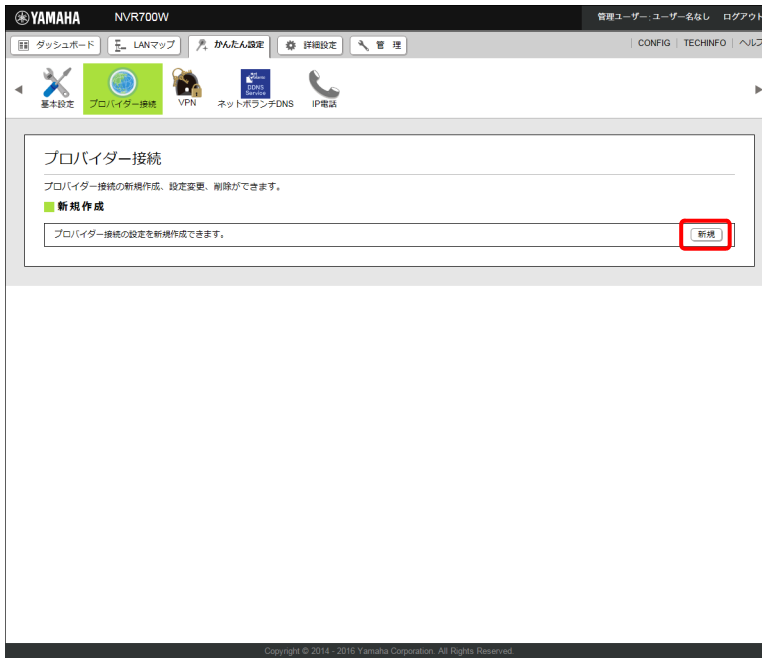
## メモ

本章ではプロバイダーから提供されたケーブルモデムや ADSL モデムをモデムと呼びます。

### ご注意

小型 ONU を使ってフレッツ光回線に接続する場合は、本製品の電源が切れた状態で小型 ONU を ONU ポートに接続し、光ケーブルを接続してから、本製品の電源を入れてください。

2. 「かんたん設定」タブを選択し、「プロバイダー接続」ボタンをクリックする。  
「プロバイダー接続」画面が表示されます。
3. 「新規」ボタンをクリックする。



「インターフェースの選択」画面が表示されます。

## 第4章 IPv4 アドレスでインターネットに接続する

### 4. 「WAN」または「ONU」を選択し、「次へ」ボタンをクリックする。



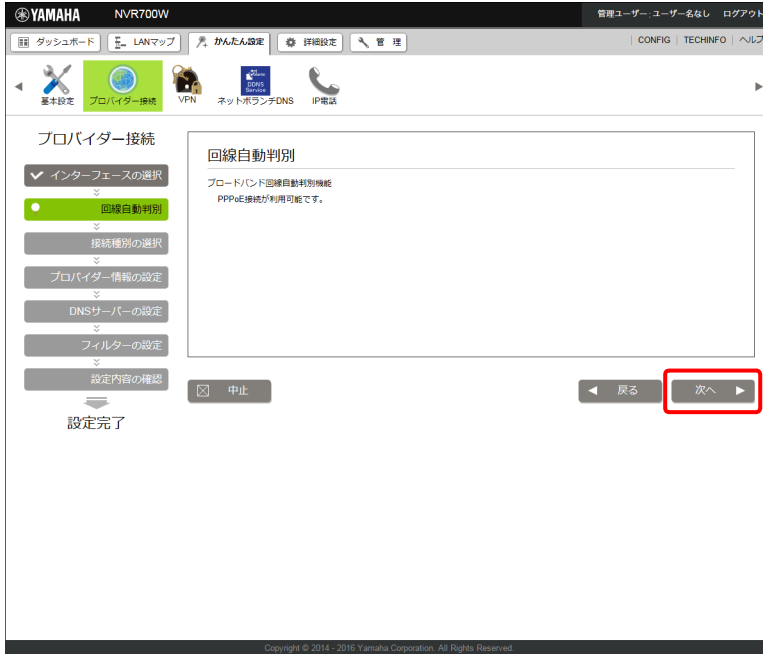
ヤマハルーターのブロードバンド回線自動判別機能が動作して、「回線自動判別」画面が表示されます。「回線自動判別」画面には、接続した回線に合わせた接続方法が表示されます。

### ご注意

- ・ 接続インターフェースで「WAN」または「ONU」を選択した場合、選択したポートに回線が接続されていないとブロードバンド回線自動判別機能は動作しません。
- ・ 「内蔵無線 WAN」は NVR700W をお使いの場合に表示されます。NVR510 では表示されません。



## 5. 自動判別された接続方法を確認し、「次へ」ボタンをクリックする。



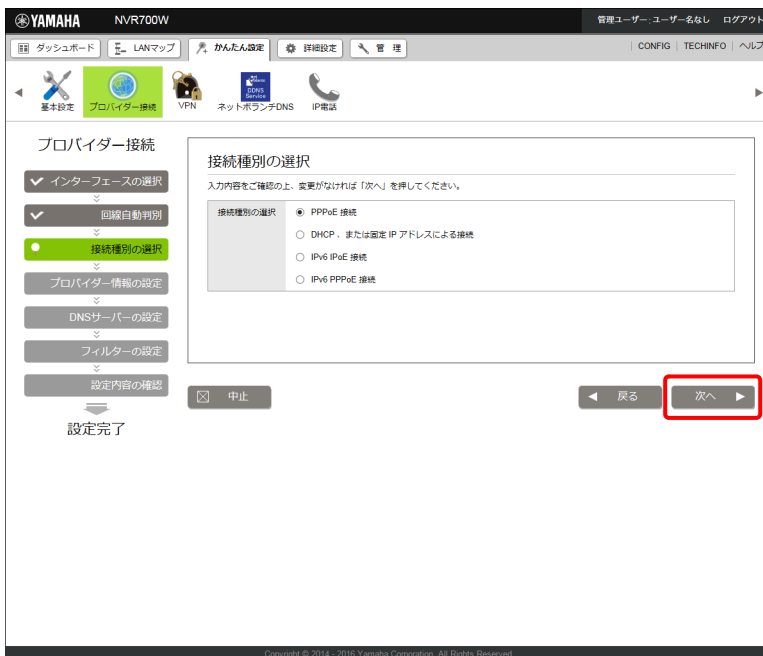
「接続種別の選択」画面が表示されます。

「ブロードバンド回線の自動判別に失敗しました。」が表示された場合

「接続種別の選択」画面で、接続回線に合わせ手動で「PPPoE 接続」または「DHCP 接続」を選択してください。

どちらかわからない場合は、プロバイダーとの契約書を確認するかプロバイダーにお問い合わせください。

## 6. 「次へ」ボタンをクリックする。



## 第4章 IPv4 アドレスでインターネットに接続する

接続回線に合わせた「プロバイダー情報の設定」画面が表示されます。

以下の設定は接続回線によって異なりますので、選んだ接続回線の説明をご覧ください。

- ・「PPPoE 接続」の場合…30 ページ
- ・「DHCP 接続」の場合…35 ページ

### 4.1.2 「PPPoE 接続」の場合

#### 1. プロバイダー情報を設定する。

YAMAHA NVR700W 管理ユーザー、ユーザー名なし ログアウト

ダッシュボード LANマップ かんたん設定 詳細設定 管理

基本設定 プロバイダー接続 VPN ネットポランテDNS IP電話

プロバイダー接続

インターネットの選択  
回線自動判別  
接続種別の選択  
● プロバイダー情報の設定  
DNSサーバーの設定  
フィルターの設定  
設定内容の確認

設定完了

プロバイダー情報の設定

入力内容をご確認の上、変更がなければ「次へ」を押してください。

① 設定名 PPPoE ※省略可

② ユーザーID ispid

③ 接続パスワード password

④ PP インターフェースのIPアドレス  
 自動取得する  
 指定する

中止 戻る 次へ

Copyright © 2014 - 2016 Yamaha Corporation. All Rights Reserved.

#### ① 設定名：

任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。

#### ② ユーザー ID：

プロバイダーから指定されたユーザー ID を入力します。

#### ③ 接続パスワード：

プロバイダーから指定されたパスワード（または自分で変更したパスワード）を入力します。

#### ④ PP インターフェースの IP アドレス：

PP インターフェースの IP アドレスを設定します。

プロバイダーから PP インターフェースの IP アドレスが指定されていない場合は「自動取得する」を選択します。

#### 2. 「次へ」 ボタンをクリックする。

「DNS サーバーの設定」画面が表示されます。

## 3. DNS サーバーアドレスを設定する。



① **DNS サーバーアドレスを指定しない、またはプロバイダーから自動取得：**  
 プロバイダーから DNS サーバーアドレスが指定されていない場合に選択します。

② **プロバイダーとの契約書に DNS サーバーアドレスの指定がある：**  
 プロバイダーから DNS サーバーアドレスが指定されている場合に選択し、以下の設定を行います。

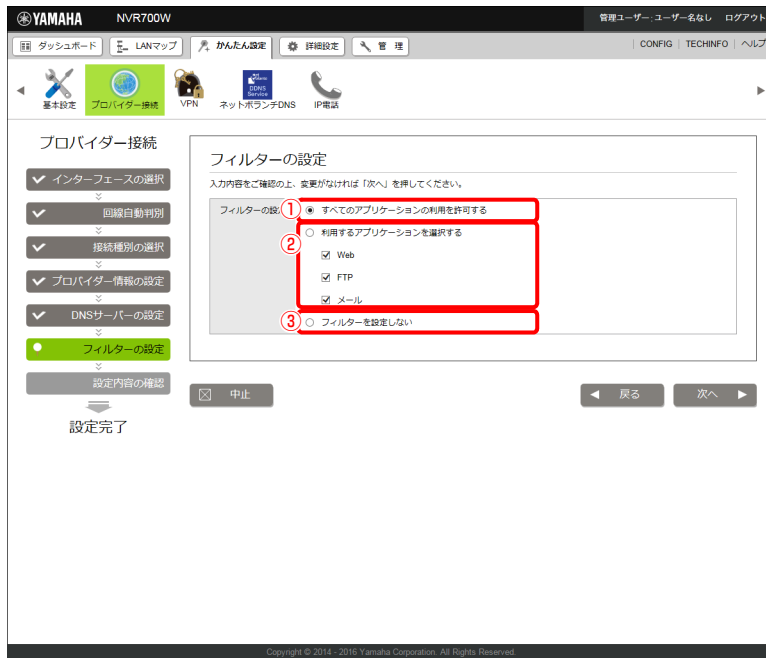
- ・ **プライマリー DNS サーバーアドレス：**プロバイダーから指定されている DNS サーバーアドレスを半角数字とドット (.) で入力します。
- ・ **セカンダリー DNS サーバーアドレス：**プロバイダーから指定されている DNS サーバーアドレスが 2 つある場合に入力します (1 つだけ指定されている場合は、この欄は空欄にしてください)。

## 4. 「次へ」 ボタンをクリックする。

「フィルターの設定」画面が表示されます。

## 第4章 IPv4 アドレスでインターネットに接続する

### 5. フィルターを設定する。



#### ① すべてのアプリケーションの利用を許可する：

LAN 側から利用するアプリケーションを制限せず、すべてのアプリケーションから WAN 側への通信が可能となります。

#### ② 利用するアプリケーションを選択する：

利用するアプリケーションに合わせて通信が許可されます。選択していないアプリケーションの通信は遮断されます。利用したいアプリケーションのチェックボックスにチェックを入れてください。

- ・ Web：Web 閲覧のために、http、https の通信が許可されます。
- ・ FTP：FTP の利用のために、ftp の通信が許可されます。
- ・ メール：メールの利用のために、pop3、smtp、submission の通信が許可されます。

#### ③ フィルターを設定しない：

フィルターの設定は行われません。

### 6. 「次へ」 ボタンをクリックする。

「設定内容の確認」画面が表示されます。

## 7. 内容を確認し、「設定の確定」ボタンをクリックする。



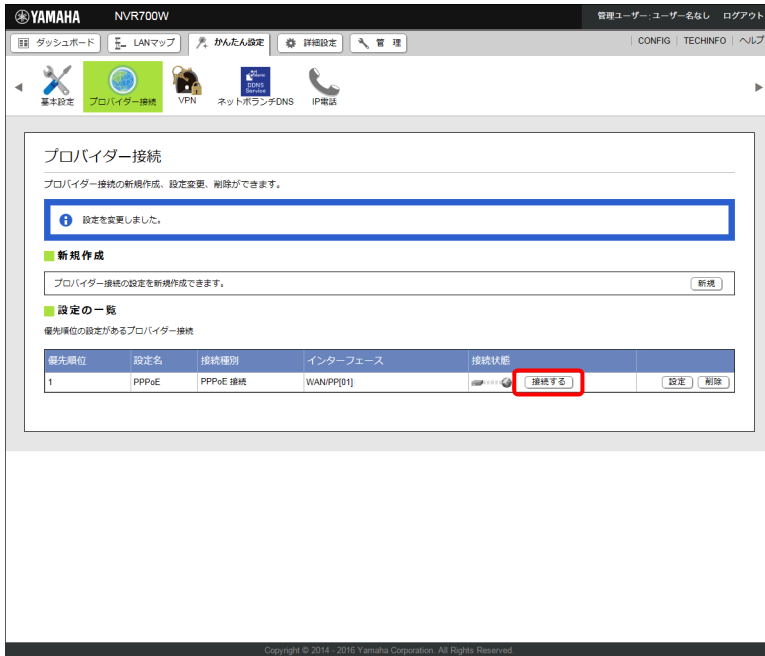
プロバイダー情報が設定され、「プロバイダー接続」画面が表示されます。

**ご注意**

プロバイダー情報が設定されると、自動的にヤマハルーターのDNSサーバー機能にアクセスできるホストがLANポートに接続されたホストに制限されます。ヤマハルーターのDNSサーバー機能にアクセスできるホストを変更する場合は、「16.2 DNSサーバー機能にアクセスできるホストの設定を変更する」(371 ページ) をご覧ください。

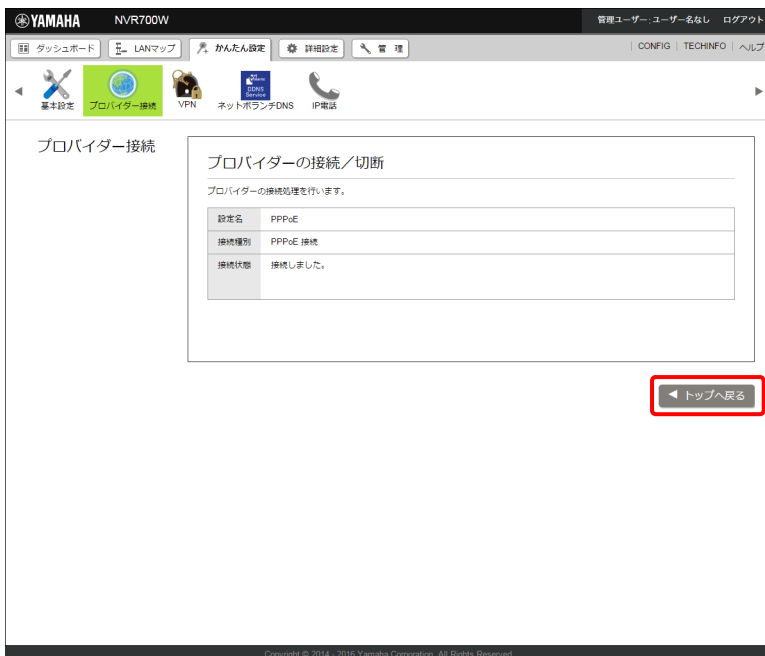
## 第4章 IPv4 アドレスでインターネットに接続する

8. 「設定の一覧」項目の中から設定したプロバイダー接続の「接続する」ボタンをクリックする。



プロバイダーへの接続処理が開始され、「プロバイダーの接続 / 切断」画面が表示されます。

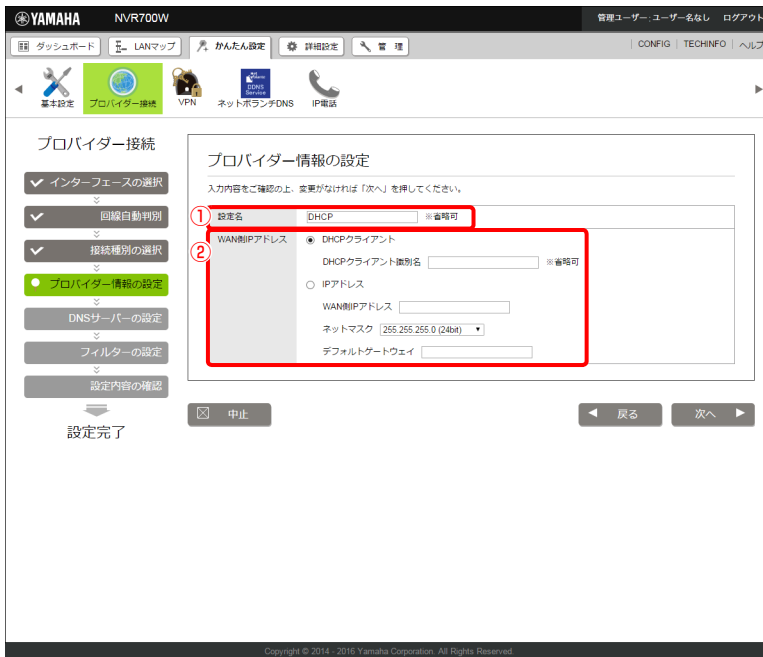
9. 「トップへ戻る」ボタンをクリックする。



「接続状態」の表示が に切り替わります。

## 4.1.3 「DHCP 接続」の場合

## 1. プロバイダー情報を設定する。



## ① 設定名：

任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。

## ② WAN 側 IP アドレス：

プロバイダーから指定された IP アドレスを設定します。

- ・ DHCP クライアント：プロバイダーから IP アドレスが指定されていない場合を選択します。DHCP クライアント識別名に任意の名前を入力します。
- ・ IP アドレス：プロバイダーから IP アドレスが指定されている場合を選択し、WAN 側 IP アドレス、ネットマスク、デフォルトゲートウェイを入力します。

## 2. 「次へ」 ボタンをクリックする。

「DNS サーバーの設定」画面が表示されます。

## 第4章 IPv4 アドレスでインターネットに接続する

### 3. DNS サーバーアドレスを設定する。



① DNS サーバーアドレスを指定しない、またはプロバイダーから自動取得：  
プロバイダーから DNS サーバーアドレスが指定されていない場合に選択します。

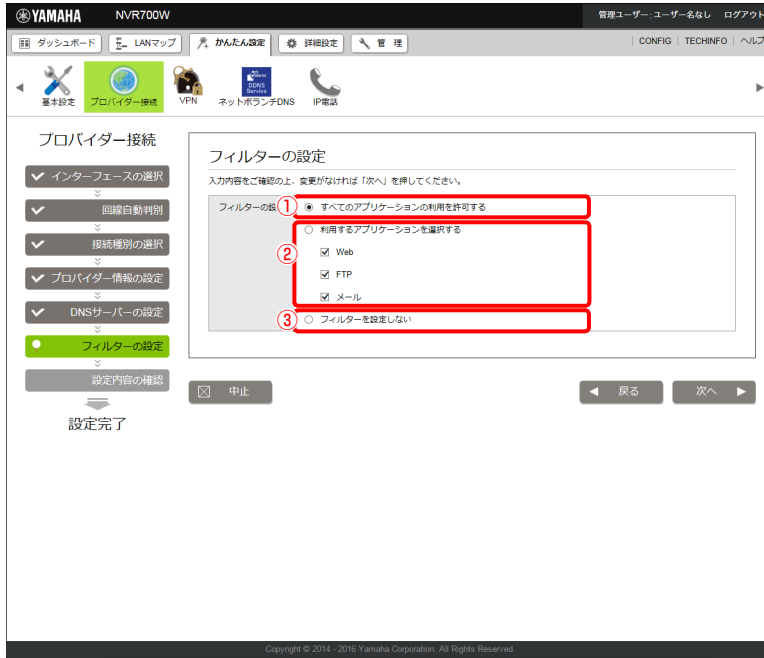
② プロバイダーとの契約書に DNS サーバーアドレスの指定がある：  
プロバイダーから DNS サーバーアドレスが指定されている場合に選択し、以下の設定を行います。

- ・ プライマリー DNS サーバーアドレス：プロバイダーから指定されている DNS サーバーアドレスを半角数字とドット (.) で入力します。
- ・ セカンダリー DNS サーバーアドレス：プロバイダーから指定されている DNS サーバーアドレスが2つある場合に入力します (1 つだけ指定されている場合は、この欄は空欄にしてください)。

4. 「次へ」 ボタンをクリックする。  
「フィルターの設定」画面が表示されます。



## 5. フィルターを設定する。



## ① すべてのアプリケーションの利用を許可する：

LAN 側から利用するアプリケーションを制限せず、すべてのアプリケーションから WAN 側への通信が可能となります。

## ② 利用するアプリケーションを選択する：

利用するアプリケーションに合わせて通信が許可されます。選択していないアプリケーションの通信は遮断されます。利用したいアプリケーションのチェックボックスにチェックを入れてください。

- ・ Web：Web 閲覧のために、http、https の通信が許可されます。
- ・ FTP：FTP の利用のために、ftp の通信が許可されます。
- ・ メール：メールの利用のために、pop3、smtp、submission の通信が許可されます。

## ③ フィルターを設定しない：

フィルターの設定は行われません。




## 6. 「次へ」 ボタンをクリックする。

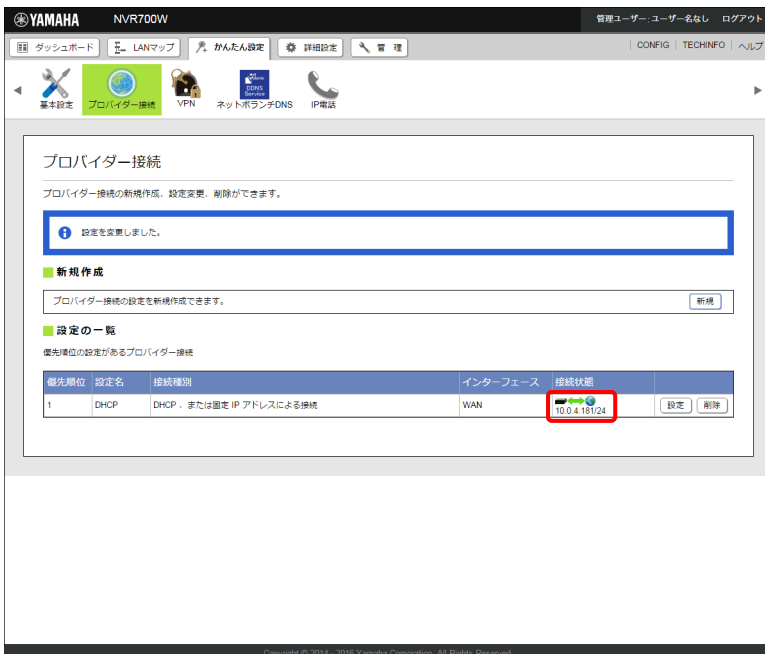
「設定内容の確認」画面が表示されます。

## 第4章 IPv4 アドレスでインターネットに接続する

### 7. 内容を確認し、「設定の確定」ボタンをクリックする。



プロバイダー情報が設定され、「プロバイダー接続」画面が表示されます。自動でインターネットに接続され、「接続状態」の表示が    に切り替わります。



### ご注意

プロバイダー情報が設定されると、自動的にヤマハルーターの DNS サーバー機能にアクセスできるホストが LAN ポートに接続されたホストに制限されます。ヤマハルーターの DNS サーバー機能にアクセスできるホストを変更する場合は、「16.2 DNS サーバー機能にアクセスできるホストの設定を変更する」(371 ページ)をご覧ください。

## 4.2 無線 WAN 回線でインターネット接続する

### 4.2.1 内蔵無線 WAN でインターネットへ接続する (NVR700W)

3G/LTE 携帯電話通信網に対応した SIM カードをヤマハルーターの SIM カードスロットに挿入してインターネットに接続します。

インターネット接続に使用するプロバイダーの設定資料を用意してください。

SIM カードの取り付け手順は、「取扱説明書」（製品付属の CD-ROM に収録）の「SIM カードの取り付け」をご覧ください。

#### ご注意

- ・ 本機能は NVR700W をお使いの場合に設定できます。NVR510 では設定できません。
- ・ プロバイダー契約を解除または変更したときは、必ずヤマハルーターの接続設定を削除または再設定してください。削除しないまま使っていると、回線業者やプロバイダーから意図しない料金を請求される場合があります。
- ・ データ通信（パケット通信）の契約が従量制である場合、あるいはデータ通信が定額制の契約の対象外である場合、長時間通信したり大量のデータをやりとりすると高額な料金が発生します。ご使用にあたっては、通信料金について十分ご注意ください。
- ・ インターネットへ常時接続する場合は、インターネット側から不正なアクセスや攻撃を受ける危険性が高くなります。セキュリティには十分ご注意のうえ、お使いください。詳しくは「第 12 章 セキュリティを強化する」（237 ページ）をご覧ください。

#### プロバイダーの設定資料

接続先を設定してインターネットに接続するには、プロバイダーから通知される以下の情報が必要です（接続方法によっては、必要のないものもあります）。

- ・ ユーザー ID（認証 ID、アカウント名）
- ・ パスワード（認証パスワード、初期パスワード）
- ・ IP アドレス
- ・ ネットマスク
- ・ ネームサーバーアドレス
- ・ アクセスポイント名

#### メモ

ネームサーバーアドレスはプロバイダーによって、DNS サーバーアドレスやネームサーバー IP アドレス、DNS サーバー IP アドレスなど呼び名が異なることがあります。

1. ヤマハルーターの SIM カードスロットに、SIM カードを挿入する。

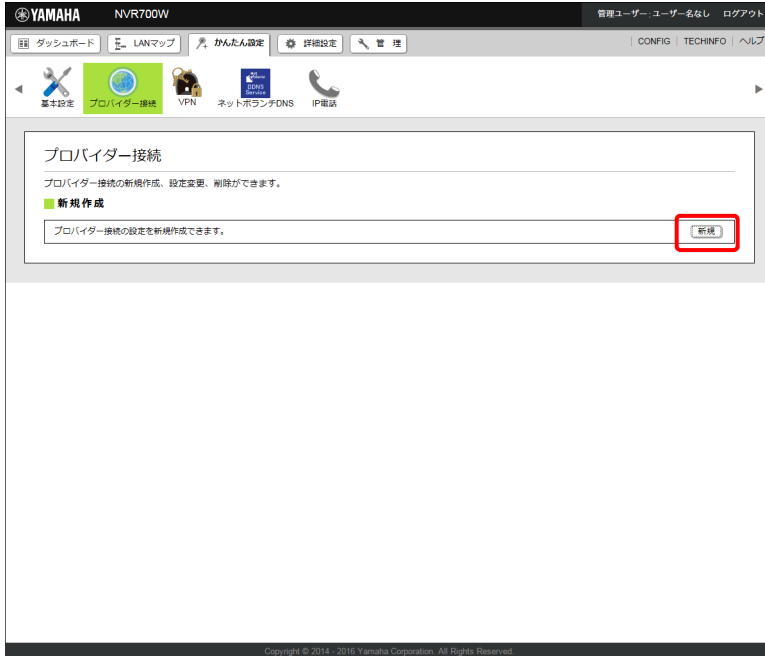
#### ご注意

SIM カードを挿入するときは、必ず本製品の電源を切った状態で行ってください。

2. 「かんたん設定」タブを選択し、「プロバイダー接続」ボタンをクリックする。  
「プロバイダー接続」画面が表示されます。

## 第 4 章 IPv4 アドレスでインターネットに接続する

### 3. 「新規」 ボタンをクリックする。



「インターフェースの選択」画面が表示されます。

### 4. 「内蔵無線 WAN」を選択し、「次へ」ボタンをクリックする。



「プロバイダー情報の設定」画面が表示されます。

## 5. プロバイダー情報を設定する。

## ① 設定名：

任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。

## ② アクセスポイント名：

キャリアまたはプロバイダーから指定された、アクセスポイント名を入力します。

## ③ ユーザー ID：

キャリアまたはプロバイダーから指定されたユーザー ID を入力します。

## ④ 接続パスワード：

キャリアまたはプロバイダーから指定されたパスワード（または自分で変更したパスワード）を入力します。

## ⑤ 通信制限：

従量課金制のサービスで通信を行っている場合などで、異常な通信量を制限するには「制限する (50Mbyte/30日)」を選択します。30日間で、50Mbyte 以内に累積送受信データ量を制限します。

## 6. 「次へ」 ボタンをクリックする。

「DNS サーバーの設定」画面が表示されます。

## 第4章 IPv4 アドレスでインターネットに接続する

### 7. DNS サーバーアドレスを設定する。



① DNS サーバーアドレスを指定しない、またはプロバイダーから自動取得：

プロバイダーから DNS サーバーアドレスが指定されていない場合に選択します。

② プロバイダーとの契約書に DNS サーバーアドレスの指定がある：

プロバイダーから DNS サーバーアドレスが指定されている場合に選択し、以下の設定を行います。

- ・ プライマリー DNS サーバーアドレス：プロバイダーから指定されている DNS サーバーアドレスを半角数字とドット (.) で入力します。
- ・ セカンダリー DNS サーバーアドレス：プロバイダーから指定されている DNS サーバーアドレスが 2 つある場合に入力します (1 つだけ指定されている場合は、この欄は空欄にしてください)。

### 8. 「次へ」 ボタンをクリックする。

「フィルターの設定」画面が表示されます。

## 9. フィルターを設定する。



## ① すべてのアプリケーションの利用を許可する：

LAN 側から利用するアプリケーションを制限せず、すべてのアプリケーションから WAN 側への通信が可能となります。

## ② 利用するアプリケーションを選択する：

利用するアプリケーションに合わせて通信が許可されます。選択していないアプリケーションの通信は遮断されます。利用したいアプリケーションのチェックボックスにチェックを入れてください。

- ・ Web：Web 閲覧のために、http、https の通信が許可されます。
- ・ FTP：FTP の利用のために、ftp の通信が許可されます。
- ・ メール：メールの利用のために、pop3、smtp、submission の通信が許可されます。

## ③ フィルターを設定しない：

フィルターの設定は行われません。


## 10. 「次へ」 ボタンをクリックする。

「設定内容の確認」画面が表示されます。

## 第 4 章 IPv4 アドレスでインターネットに接続する

### 11. 内容を確認し、「設定の確定」ボタンをクリックする。



プロバイダー情報が設定され、「プロバイダー接続」画面が表示されます。自動でインターネットに接続され、「接続状態」の表示が  に切り替わります。

### ご注意

- ・ 自動でインターネットに接続されるまでに数十秒かかることがあります。
- ・ プロバイダー情報が設定されると、自動的にヤマハルーターの DNS サーバー機能にアクセスできるホストが LAN ポートに接続されたホストに制限されます。ヤマハルーターの DNS サーバー機能にアクセスできるホストを変更する場合は、「16.2 DNS サーバー機能にアクセスできるホストの設定を変更する」(371 ページ) をご覧ください。



### 4.2.2 USB 接続型データ通信端末でインターネットへ接続する

3G/LTE 携帯電話通信網に対応した USB 接続型データ通信端末をヤマハルーターの USB ポートに接続してインターネットに接続します。

インターネット接続に使用するプロバイダーの設定資料を用意してください。

#### ご注意

- ・ プロバイダー契約を解除または変更したときは、必ずヤマハルーターの接続設定を削除または再設定してください。削除しないまま使っていると、回線業者やプロバイダーから意図しない料金を請求される場合があります。
- ・ データ通信（パケット通信）の契約が従量制である場合、あるいはデータ通信が定額制の契約の対象外である場合、長時間通信したり大量のデータをやりとりすると高額な料金が発生します。ご使用にあたっては、通信料金について十分ご注意ください。
- ・ インターネットへ常時接続する場合は、インターネット側から不正なアクセスや攻撃を受ける危険性が高くなります。セキュリティには十分ご注意のうえ、お使いください。詳しくは「第 12 章 セキュリティを強化する」(237 ページ) をご覧ください。
- ・ USB 接続型データ通信端末は、ご利用になる携帯端末の取扱説明書に指定されている使い方や、環境条件のもとでお使いください。
- ・ 本機能は 64k データ通信には対応しておりません。

#### プロバイダーの設定資料

接続先を設定してインターネットに接続するには、プロバイダーから通知される以下の情報が必要です（接続方法によっては、必要のないものもあります）。

- ・ ユーザー ID（認証 ID、アカウント名）
- ・ パスワード（認証パスワード、初期パスワード）
- ・ IP アドレス
- ・ ネットマスク
- ・ ネームサーバーアドレス
- ・ デフォルト・ゲートウェイ・アドレス
- ・ アクセスポイント名
- ・ CID (Context Identifier)

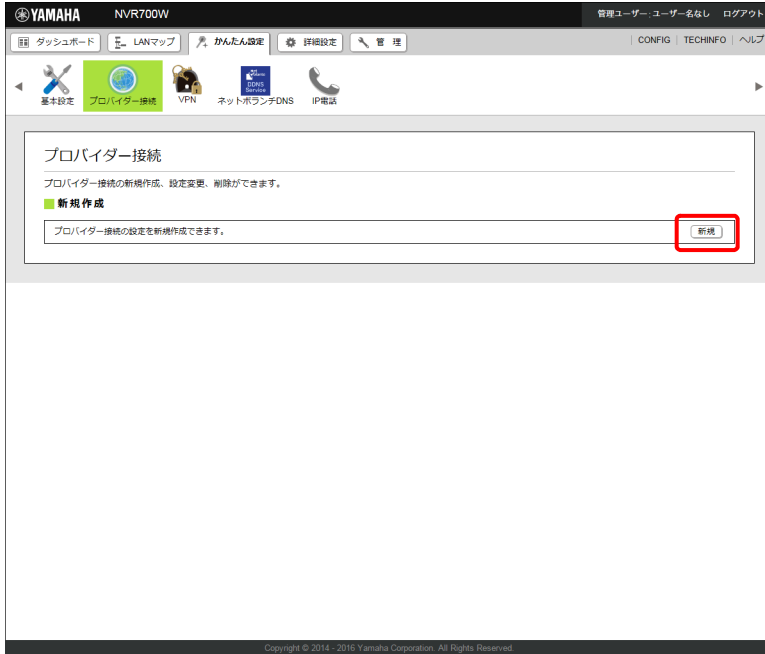
#### メモ

ネームサーバーアドレスはプロバイダーによって、DNS サーバーアドレスやネームサーバー IP アドレス、DNS サーバー IP アドレスなど呼び名が異なることがあります。

1. ヤマハルーターの USB ポートに、USB 接続型データ通信端末を接続する。
2. 「かんたん設定」タブを選択し、「プロバイダー接続」ボタンをクリックする。  
「プロバイダー接続」画面が表示されます。

## 第4章 IPv4 アドレスでインターネットに接続する

### 3. 「新規」 ボタンをクリックする。



「インターフェースの選択」画面が表示されます。

### 4. 「モバイル」を選択し、「次へ」ボタンをクリックする。



「プロバイダー情報の設定」画面が表示されます。

### ご注意

「内蔵無線 WAN」は NVR700W をお使いの場合に表示されます。NVR510 では表示されません。

## 5. プロバイダー情報を設定する。

## ① 接続インターフェース：

接続インターフェースを選択します。

## メモ

モデム方式 / イーサネット方式 (NDIS) のどちらを選択するかは、ご利用になる USB 接続型データ通信端末によって異なります。USB 接続型データ通信端末ごとに選択すべき接続インターフェースについて詳しくは、下記の URL をご覧ください。

<http://www.rtpro.yamaha.co.jp/RT/docs/mobile-internet/index.html>

## ② 設定名：

任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。

## ③ アクセスポイント名 (APN)：

キャリアまたはプロバイダーから指定された、アクセスポイント名を入力します。

## ④ CID (モデム方式選択時のみ)：

接続インターフェースで「モデム方式」を選択時に、キャリアまたはプロバイダーから指定された、CID 番号 (Context Identifier) を入力します。

## ⑤ ユーザー ID：

キャリアまたはプロバイダーから指定されたユーザー ID を入力します。

## ⑥ 接続パスワード：

キャリアまたはプロバイダーから指定されたパスワード (または自分で変更したパスワード) を入力します。

## ⑦ 通信制限：

従量課金制のサービスで通信を行っている場合などで、異常な通信量を制限するには「制限する (50Mbyte/30日)」を選択します。30日間で、50Mbyte 以内に累積受信データ量を制限します。

## 6. 「次へ」ボタンをクリックする。

「DNS サーバーの設定」画面が表示されます。

## 第4章 IPv4 アドレスでインターネットに接続する

### 7. DNS サーバーアドレスを設定する。



① DNS サーバーアドレスを指定しない、またはプロバイダーから自動取得：

プロバイダーから DNS サーバーアドレスが指定されていない場合に選択します。

② プロバイダーとの契約書に DNS サーバーアドレスの指定がある：

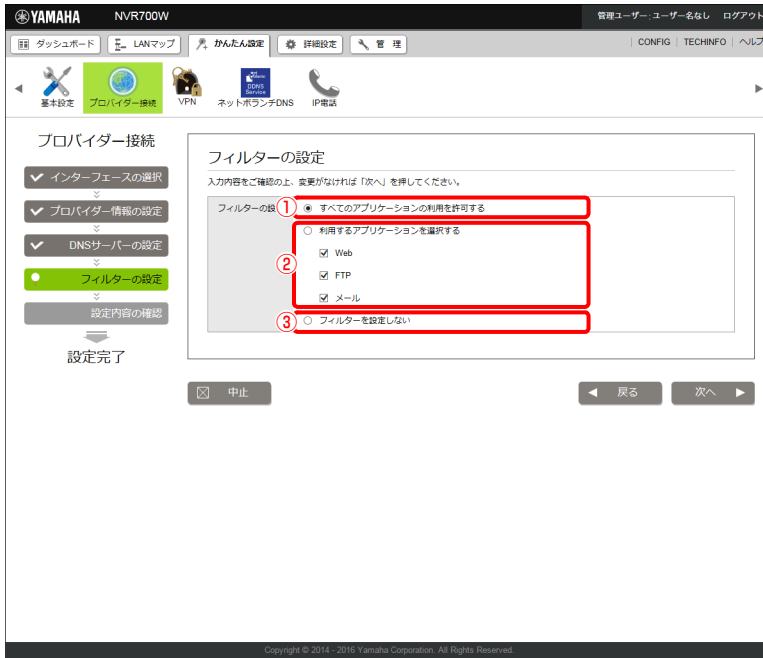
プロバイダーから DNS サーバーアドレスが指定されている場合に選択し、以下の設定を行います。

- ・ プライマリー DNS サーバーアドレス：プロバイダーから指定されている DNS サーバーアドレスを半角数字とドット (.) で入力します。
- ・ セカンダリー DNS サーバーアドレス：プロバイダーから指定されている DNS サーバーアドレスが2つある場合に入力します (1 つだけ指定されている場合は、この欄は空欄にしてください)。

### 8. 「次へ」 ボタンをクリックする。

「フィルターの設定」画面が表示されます。

## 9. フィルターを設定する。



## ① すべてのアプリケーションの利用を許可する：

LAN 側から利用するアプリケーションを制限せず、すべてのアプリケーションから WAN 側への通信が可能となります。

## ② 利用するアプリケーションを選択する：

利用するアプリケーションに合わせて通信が許可されます。選択していないアプリケーションの通信は遮断されます。利用したいアプリケーションのチェックボックスにチェックを入れてください。

- ・ Web：Web 閲覧のために、http、https の通信が許可されます。
- ・ FTP：FTP の利用のために、ftp の通信が許可されます。
- ・ メール：メールの利用のために、pop3、smtp、submission の通信が許可されます。

## ③ フィルターを設定しない：

フィルターの設定は行われません。

## 10. 「次へ」 ボタンをクリックする。

「設定内容の確認」画面が表示されます。

## 第4章 IPv4 アドレスでインターネットに接続する

### 11. 内容を確認し、「設定の確定」ボタンをクリックする。

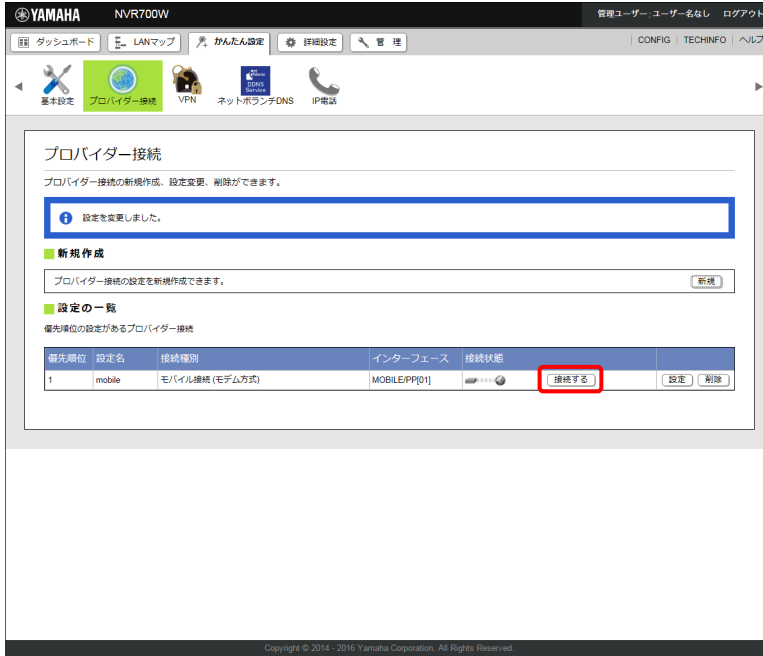


プロバイダー情報が設定され、「プロバイダー接続」画面が表示されます。

### ご注意

プロバイダー情報が設定されると、自動的にヤマハルーターのDNSサーバー機能にアクセスできるホストがLANポートに接続されたホストに制限されます。ヤマハルーターのDNSサーバー機能にアクセスできるホストを変更する場合は、「16.2 DNSサーバー機能にアクセスできるホストの設定を変更する」(371 ページ)をご覧ください。

12.「設定の一覧」項目の中から設定したプロバイダー接続の「接続する」ボタンをクリックする。



プロバイダーへの接続処理が開始され、「プロバイダーの接続 / 切断」画面が表示されます。

13.「トップへ戻る」ボタンをクリックする。



「接続状態」の表示が に切り替わります。

# 第 5 章 IPv6 アドレスでインターネットに接続する

本章では、IPv6 アドレスでインターネットに接続する方法について説明します。ヤマハルーターに接続するインターネット回線に合わせて、必要な接続方法を選んでください。

- ・ フレッツ光 (IPv6 IPoE) でインターネットへ接続する …52 ページ
- ・ フレッツ光 (IPv6 PPPoE) でインターネットへ接続する …58 ページ

## メモ

本章では Windows 7 で Internet Explorer 11 を使用した場合の画面を例に説明します。他の環境の場合は画面表示が多少異なりますが基本的な操作は同じです。

## 5.1 フレッツ光 (IPv6 IPoE) でインターネットへ接続する

フレッツ光 (IPv6 IPoE) を使用してインターネットに接続します。  
インターネット接続に使用するプロバイダーの設定資料を用意してください。

### ご注意

- ・ プロバイダー契約を解除または変更したときは、必ずヤマハルーターの接続設定を削除または再設定してください。削除しないまま使っていると、回線業者やプロバイダーから意図しない料金を請求される場合があります。
- ・ インターネットへ常時接続する場合は、インターネット側から不正なアクセスや攻撃を受ける危険性が高くなります。セキュリティには十分ご注意ください。詳しくは「第 12 章 セキュリティを強化する」(237 ページ)をご覧ください。
- ・ フレッツ光ネクストにおけるインターネット (IPv6 IPoE) 接続を用いてインターネット (IPv6) サービスをご利用いただくためには、IPv6 IPoE 接続に対応したプロバイダーとの契約とフレッツ・v6 オプションへのお申し込みが必要となります。

### プロバイダーの設定資料

接続先を設定してインターネットに接続するには、プロバイダーから通知される以下の情報が必要です。

- ・ ひかり電話の契約の有無

### WAN ポートを使用する場合

1. LAN ケーブルで ONU やモデムとヤマハルーターの WAN ポートを接続する。

### メモ

本章ではプロバイダーから提供されたケーブルモデムや ADSL モデムをモデムと呼びます。

### ONU ポートを使用する場合

1. 小型 ONU を ONU ポートに接続して、光ケーブルを小型 ONU に接続する。

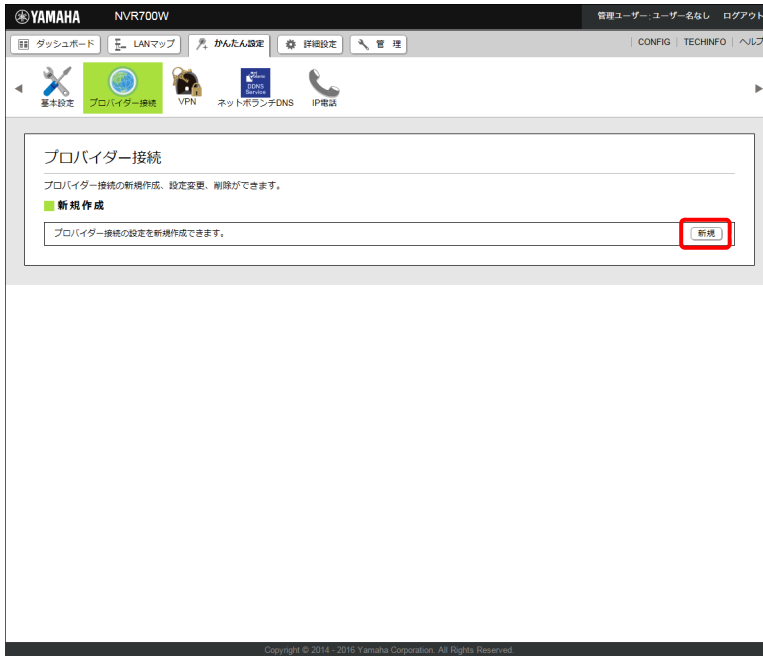
### ご注意

小型 ONU を使ってフレッツ光回線に接続する場合は、本製品の電源が切れた状態で小型 ONU を ONU ポートに接続し、光ケーブルを接続してから、本製品の電源を入れてください。



## 5.1 フレッツ光 (IPv6 IPoE) でインターネットへ接続する

2. 「かんたん設定」タブを選択し、「プロバイダー接続」ボタンをクリックする。  
「プロバイダー接続」画面が表示されます。
3. 「新規」ボタンをクリックする。



「インターフェースの選択」画面が表示されます。

4. 「WAN」または「ONU」を選択し、「次へ」ボタンをクリックする。



「回線自動判別」画面が表示されます。

### ご注意

- ・ IPv6 回線の自動判別は行えないため、手順5の「回線自動判別」画面では適切な種別が表示されません。手順6の「接続種別の選択」画面で、必ず手動で接続種別を選択し直してください。
- ・ 「内蔵無線 WAN」は NVR700W をお使いの場合に表示されます。NVR510 では表示されません。

### 5. 「次へ」ボタンをクリックする。



「接続種別の選択」画面が表示されます。

## 6. 「IPv6 IPoE 接続」を選択し、「次へ」ボタンをクリックする。



「プロバイダー情報の設定」画面が表示されます。

## 7. プロバイダー情報を設定する。



## ① 設定名：

任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。

## 第5章 IPv6 アドレスでインターネットに接続する

### ② ひかり電話の契約：

フレッツ光ネクスト回線の契約の「ひかり電話の契約の有無」に合わせて選択します。この設定を間違えると、インターネット接続ができなくなります。

### 8. 「次へ」 ボタンをクリックする。

「DNS サーバーの設定」画面が表示されます。

### 9. 「次へ」 ボタンをクリックする。






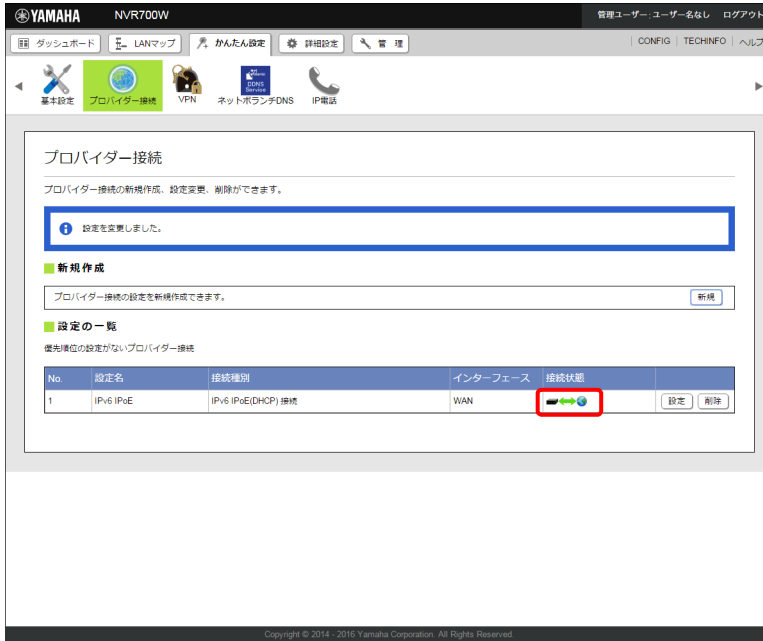
「設定内容の確認」画面が表示されます。

### 10. 内容を確認し、「設定の確定」ボタンをクリックする。



## 5.1 フレッツ光 (IPv6 IPoE) でインターネットへ接続する

プロバイダー情報が設定され、「プロバイダー接続」画面が表示されます。自動でインターネットに接続され、「接続状態」の表示が    に切り替わります。



### ご注意

プロバイダー情報が設定されると、自動的にヤマハルーターの DNS サーバー機能にアクセスできるホストが LAN ポートに接続されたホストに制限されます。ヤマハルーターの DNS サーバー機能にアクセスできるホストを変更する場合は、「16.2 DNS サーバー機能にアクセスできるホストの設定を変更する」(371 ページ) をご覧ください。

### 5.2 フレッツ光 (IPv6 PPPoE) でインターネットへ接続する

フレッツ光 (IPv6 PPPoE) を使用してインターネットに接続します。  
インターネット接続に使用するプロバイダーの設定資料を用意してください。

#### ご注意

- ・ プロバイダー契約を解除または変更したときは、必ずヤマハルーターの接続設定を削除または再設定してください。削除しないまま使っていると、回線業者やプロバイダーから意図しない料金を請求される場合があります。
- ・ インターネットへ常時接続する場合は、インターネット側から不正なアクセスや攻撃を受ける危険性が高くなります。セキュリティには十分ご注意のうえ、お使いください。詳しくは「第 12 章 セキュリティを強化する」(237 ページ) をご覧ください。
- ・ フレッツ光ネクストにおけるインターネット (IPv6 PPPoE) 接続を用いてインターネット (IPv6) サービスをご利用いただくためには、IPv6 PPPoE 接続に対応したプロバイダーとの契約が必要となります。なお、ヤマハルーターでは、フレッツ光ネクストにおけるインターネット (IPv6 PPPoE) 接続を用いたインターネット (IPv6) サービスは、ひかり電話やひかり TV などの一部のサービスと同時にご利用いただくことはできません。

#### プロバイダーの設定資料

接続先を設定してインターネットに接続するには、プロバイダーから通知される以下の情報が必要です。

- ・ ユーザー ID (認証 ID、アカウント名)
- ・ パスワード (認証パスワード、初期パスワード)

1. LAN ケーブルで ONU やモデムとヤマハルーターの WAN ポートを接続する。  
または小型 ONU を ONU ポートに接続して、光ケーブルを小型 ONU に接続する。

#### ご注意

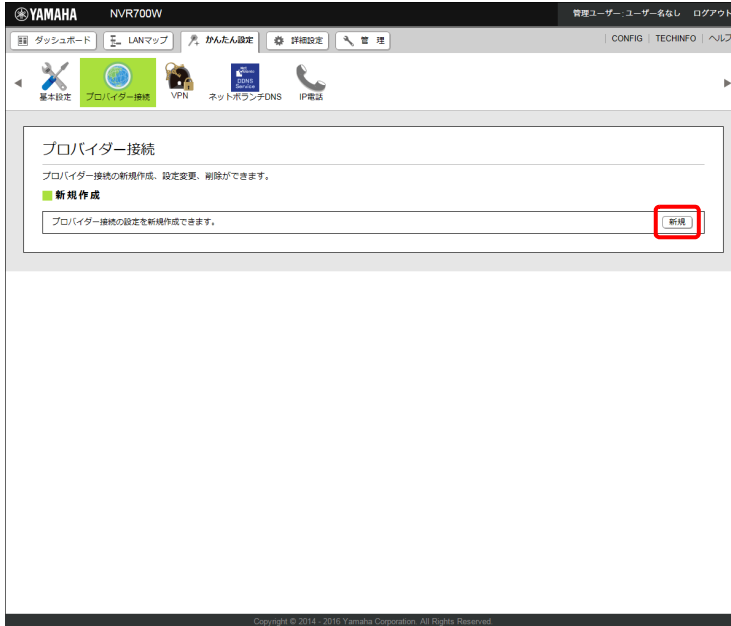
小型 ONU を使ってフレッツ光回線に接続する場合は、本製品の電源が切れた状態で小型 ONU を ONU ポートに接続し、光ケーブルを接続してから、本製品の電源を入れてください。

#### メモ

本章ではプロバイダーから提供されたケーブルモデムや ADSL モデムをモデムと呼びます。

2. 「かんたん設定」タブを選択し、「プロバイダー接続」ボタンをクリックする。  
「プロバイダー接続」画面が表示されます。

## 3. 「新規」 ボタンをクリックする。



「インターフェースの選択」画面が表示されます。

## 4. 「WAN」または「ONU」を選択し、「次へ」ボタンをクリックする。



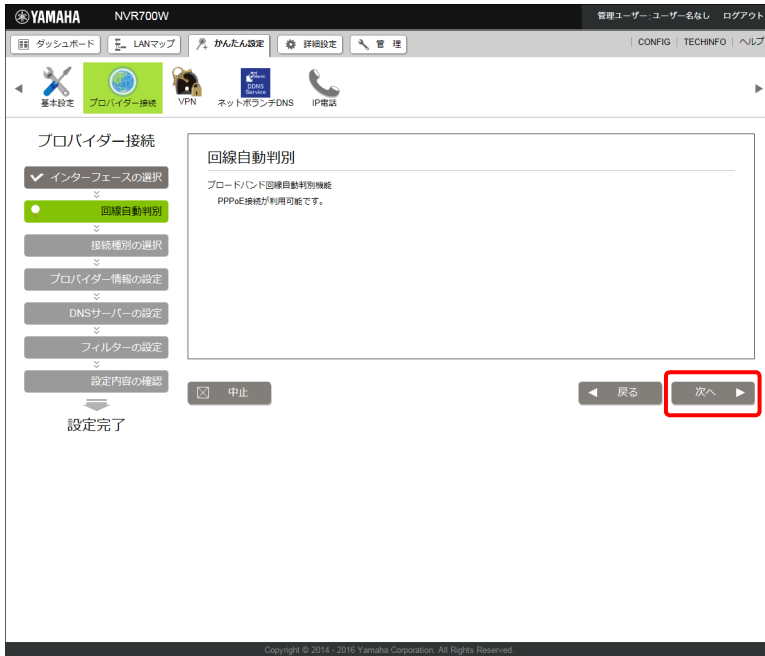
「回線自動判別」画面が表示されます。

### ご注意

- IPv6 回線の自動判別は行えないため、手順5の「回線自動判別」画面では適切な種別が表示されません。手順6の「接続種別の選択」画面で、必ず手動で接続種別を選択し直してください。
- 「内蔵無線WAN」は NVR700W をお使いの場合に表示されます。NVR510 では表示されません。

## 第5章 IPv6 アドレスでインターネットに接続する

### 5. 「次へ」 ボタンをクリックする。



「接続種別の選択」画面が表示されます。

### 6. 「IPv6 PPPoE 接続」を選択し、「次へ」ボタンをクリックする。



「プロバイダー情報の設定」画面が表示されます。



## 7. プロバイダー情報を設定する。



## ① 設定名：

任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。

## ② ユーザー ID：

プロバイダーから指定されたユーザー ID を入力します。

## ③ 接続パスワード：

プロバイダーから指定されたパスワード（または自分で変更したパスワード）を入力します。

## 8. 「次へ」 ボタンをクリックする。

「DNS サーバーの設定」画面が表示されます。

## 第5章 IPv6 アドレスでインターネットに接続する

### 9. 「次へ」 ボタンをクリックする。



「設定内容の確認」画面が表示されます。

### 10. 内容を確認し、「設定の確定」ボタンをクリックする。

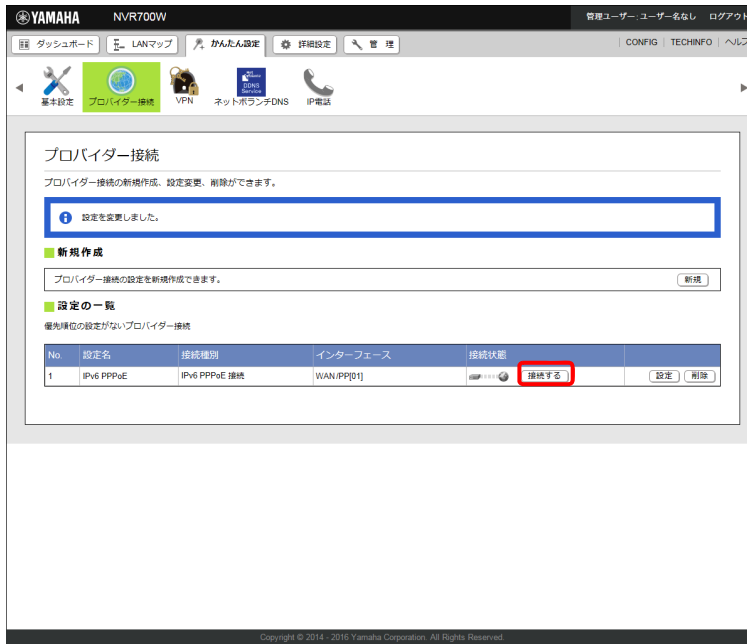


プロバイダー情報が設定され、「プロバイダー接続」画面が表示されます。

## ご注意

プロバイダー情報が設定されると、自動的にヤマハルーターの DNS サーバー機能にアクセスできるホストが LAN ポートに接続されたホストに制限されます。ヤマハルーターの DNS サーバー機能にアクセスできるホストを変更する場合は、「16.2 DNS サーバー機能にアクセスできるホストの設定を変更する」(371 ページ) をご覧ください。

11.「設定の一覧」項目の中から設定したプロバイダー接続の「接続する」ボタンをクリックする。



プロバイダーへの接続処理が開始され、「プロバイダーの接続 / 切断」画面が表示されます。

12.「トップへ戻る」ボタンをクリックする。



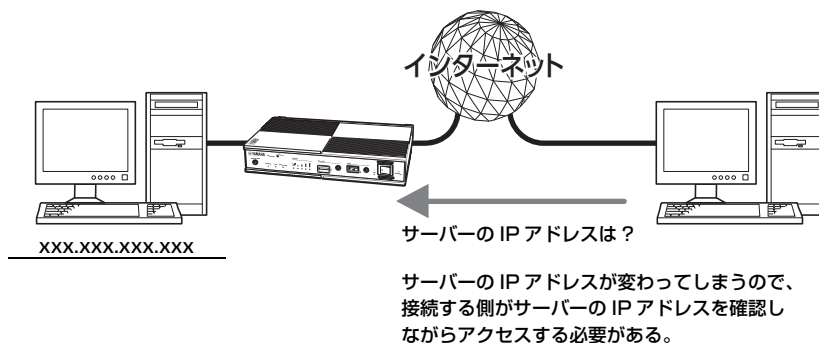
「接続状態」の表示が    に切り替わります。

# 第 6 章 ネットボランチ DNS サービスを利用する

## 6.1 ネットボランチ DNS サービスとは？

サーバーを構築してホームページを公開したり、作業用のファイルをインターネット経由で共有したりするためには、サーバーのグローバル IP アドレスがわかっている必要があります。

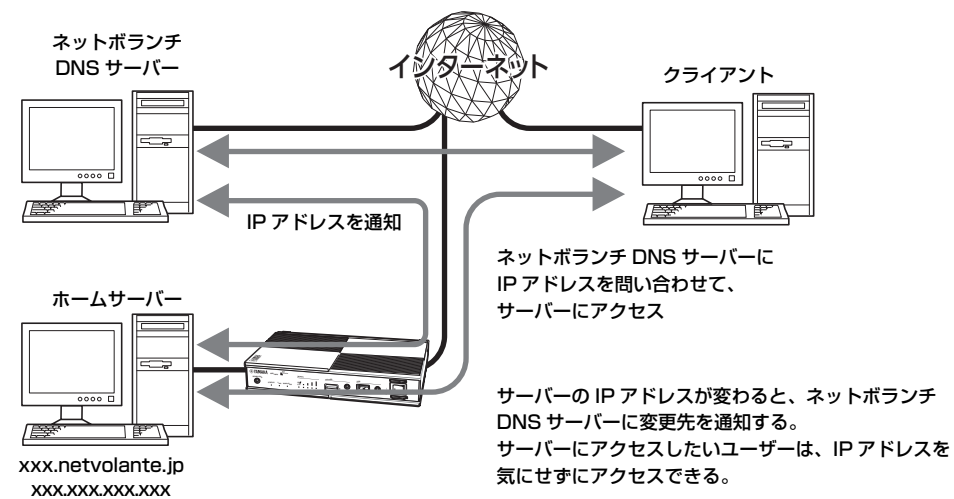
しかし、インターネットに常時接続している場合でも、割り当てられるグローバル IP アドレスは再接続時または一定時間経過時に変更される場合があります。そのため、固定グローバル IP アドレスサービスの契約をしていない環境では、サーバーを構築して公開することは困難です。



### ネットボランチ DNS サービスを利用すると

グローバル IP アドレスが変更されるたびに IP アドレスがネットボランチ DNS サーバーへ通知されるため、ネットボランチ DNS サーバーで取得できた固定のホスト名でアクセスできるようになります。

したがって、固定グローバル IP アドレスサービスの契約をしていない環境でも自宅サーバーで独自ドメインを使った各種サーバーを運用したり、IPsec や PPTP を利用して VPN を構築して、外部とデータをやり取りしたりできるようになります。



## 6.2 ネットボランチ DNS サービスで取得できるホスト名

ネットボランチ DNS サービスを利用すると、「(ユーザーの希望ホスト名).xxx.netvolante.jp」という形式のホスト名を取得できます。「xxx」の部分は、ネットボランチ DNS サーバーが任意に自動で割り当てます。ルーターの WAN 側 IP アドレスが変更されるたびに設定を変更する必要がなくなり、便利です。

### ご注意

- ・ ホストアドレスはルーター 1 台につき 1 つしか取得できません。
- ・ 希望のホスト名が取得できるとは限りません。あらかじめご了承ください。
- ・ 取得したホストアドレスに関しての正引きはできますが、逆引きはできません。
- ・ ネットボランチ DNS サービスはヤマハ独自のプロトコルを使用しているため、取得したホストアドレスを外部のダイナミック DNS サーバーに登録することはできません。
- ・ ネットボランチ DNS サービスは、プロバイダーからグローバル IP アドレスが割り当てられている環境でのみ利用できます。グローバル IP アドレスとは、下記以外の IP アドレスです。
  - 10.0.0.0 ~ 10.255.255.255
  - 172.16.0.0 ~ 172.31.255.255
  - 192.168.0.0 ~ 192.168.255.255
- ・ ご利用中のプロバイダーによっては、ホスト名の登録/更新内容がネットボランチ DNS サーバーにすぐに反映されないことがあります。あらかじめご了承ください。

## 6.3 ネットボランチ DNS ホスト名を取得する

ネットボランチ DNS サービスを利用するには、ホストアドレスを登録します。

### ご注意

ホストアドレスはルーター 1 台につき 1 つしか取得できません。

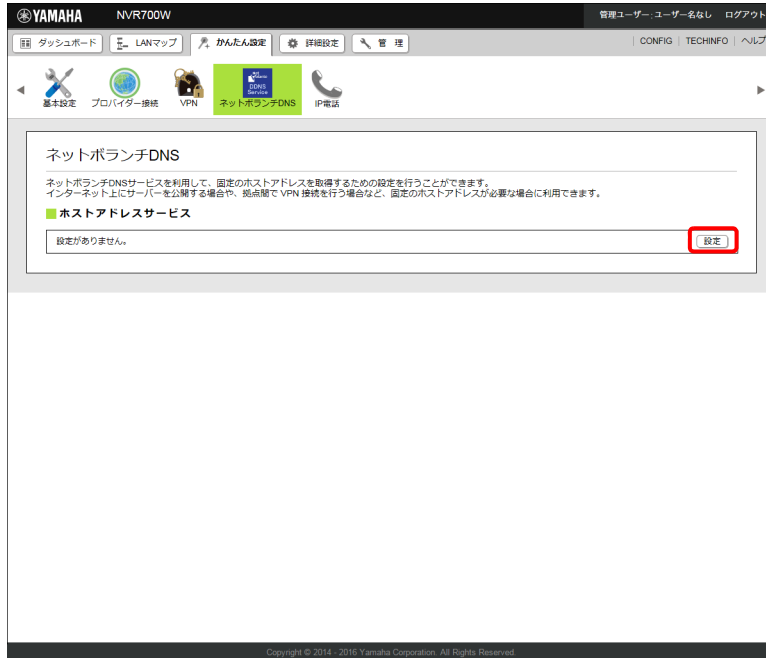
### メモ

本章では「かんたん設定」を使用して WAN インターフェースに DHCP 接続型のプロバイダーが設定されている状態（[4.1.3 「DHCP 接続」の場合]（35 ページ）の設定が完了している状態）から設定を行うという前提で説明します。

1. 「かんたん設定」タブ - 「ネットボランチ DNS」ボタンを順に選択する。  
「ネットボランチ DNS」画面が表示されます。

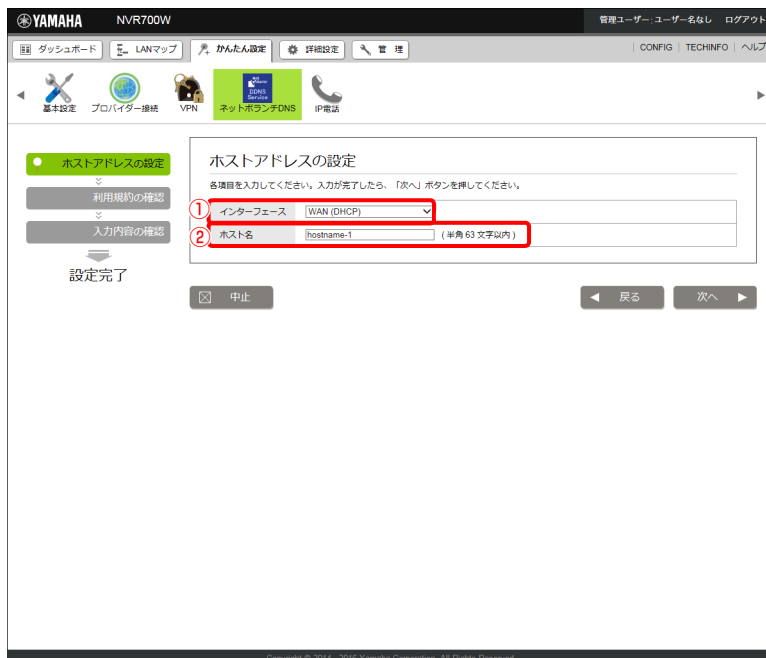
## 第6章 ネットボランチ DNS サービスを利用する

### 2. 「ホストアドレスサービス」項目の「設定」ボタンをクリックする。



「ホストアドレスの設定」画面が表示されます。

### 3. ホストアドレスを設定する。



#### ① インターフェース：

ホストアドレスを登録する対象のインターフェースを選択します。

#### ② ホスト名：

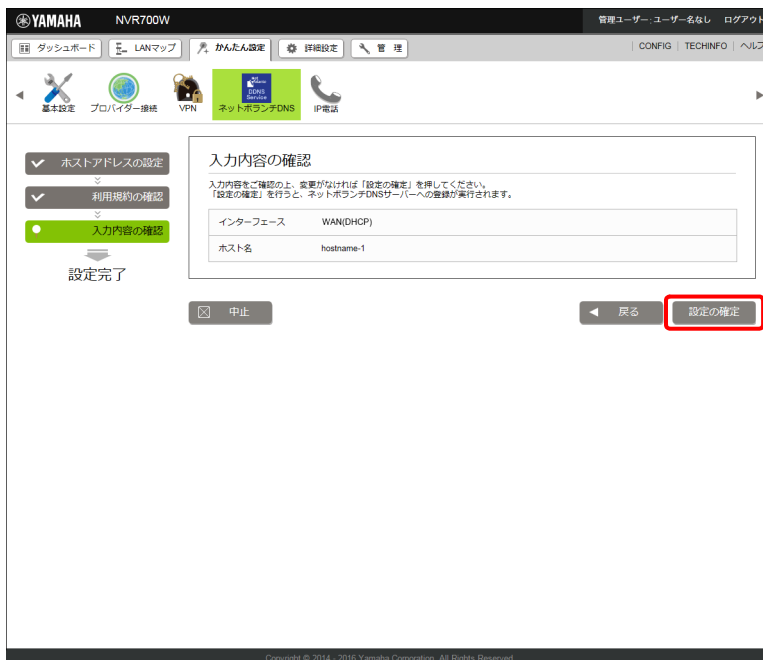
希望のホスト名 (63 文字以内) を半角英数字と '-' で入力します。

4. 「次へ」 ボタンをクリックする。  
「利用規約の確認」画面が表示されます。
5. 利用規約の内容をよく確認し、「同意する」ボタンをクリックする。



「入力内容の確認」画面が表示されます。

6. 内容を確認し、「設定の確定」ボタンをクリックする。



### 6.4 ネットボランチ DNS ホスト名の登録を解除する

ネットボランチ DNS サービスを効率良く運用するために、譲渡 / 廃棄前に不要となったネットボランチ DNS ホスト名の登録解除にご協力ください。

ネットボランチ DNS ホスト名の登録解除は、以下の手順に従って行ってください。

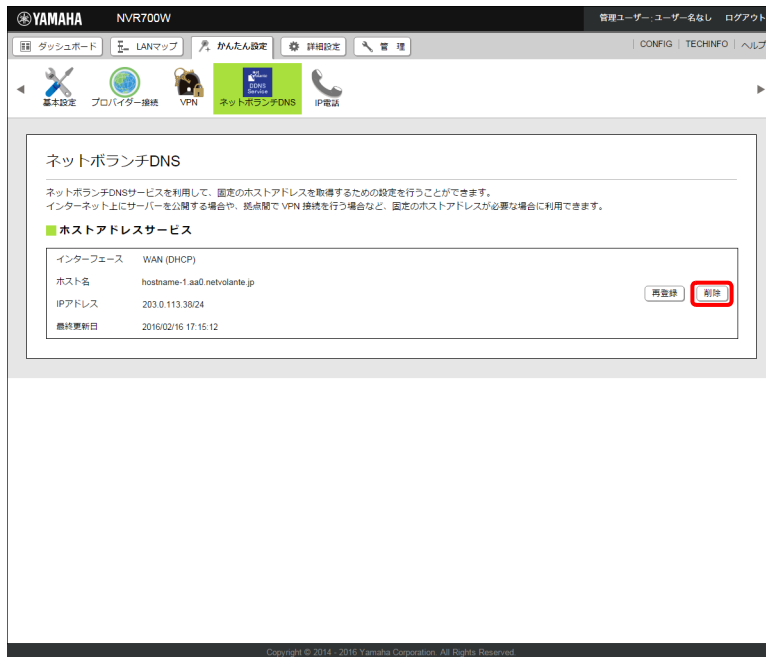
#### メモ

- ・本章では「かんたん設定」を使用して WAN インターフェースに DHCP 接続型のプロバイダーが設定されている状態（「4.1.3 「DHCP 接続」の場合」（35 ページ）の設定が完了している状態）から設定を行うという前提で説明します。
- ・本章ではネットボランチ DNS サービスのホストアドレスが、「hostname-1.aa0.netvolante.jp」で登録されている場合を例に説明します。ネットボランチ DNS ホスト名の取得について詳しくは、「6.3 ネットボランチ DNS ホスト名を取得する」（65 ページ）をご覧ください。

#### 1. 「かんたん設定」タブ - 「ネットボランチ DNS」ボタンを順に選択する。

「ネットボランチ DNS」画面が表示されます。

#### 2. 「ホストアドレスサービス」項目の「削除」ボタンをクリックする。



ネットボランチ DNS ホスト名の登録が削除されます。



## 第 7 章 拠点間を VPN で接続する

本章では、仮想プライベートネットワーク (VPN) を構築して、拠点間の LAN 同士を接続する方法について説明します。通常のインターネット回線をそのまま利用して VPN を構築できるため、専用線を導入する場合と比較して、低コストで VPN を実現できます。

拠点間を VPN で接続するには、少なくとも一方の拠点にプロバイダーからグローバル IP アドレスが割り当てられている必要があります。グローバル IP アドレスとは、下記以外の IP アドレスです。

- 10.0.0.0 ~ 10.255.255.255
- 172.16.0.0 ~ 172.31.255.255
- 192.168.0.0 ~ 192.168.255.255

VPN の設定をする前に …69 ページ

IPsec で接続する (NVR700W) …70 ページ

PPTP で接続する …76 ページ

IPIP で接続する …81 ページ

### ご注意

- ・ VPN の設定はインターネットに接続した状態で行う必要があるため、VPN を利用した拠点間接続の設定の前にインターネット接続の設定が必要です。
- ・ VPN を利用した拠点間接続を行うには、少なくとも一方の拠点に固定グローバル IP アドレスまたはネットボランチ DNS ホスト名が必要です。
- ・ ヤマハルーターの拠点間接続機能は、Windows の NetBEUI プロトコルおよび Macintosh の AppleTalk プロトコルには対応していません。
- ・ Windows でファイル共有をする場合は、NetBIOS over TCP/IP プロトコルを使用するか、または WINS サーバーを用意する必要があります。
- ・ Macintosh でファイル共有をする場合は、システム環境設定の「共有」で「パーソナルファイル共有」にチェックを入れます。

### メモ

本章では Windows 7 で Internet Explorer 11 を使用した場合の画面を例に説明します。他の環境の場合は画面表示が多少異なりますが基本的な操作は同じです。

### ネットボランチ DNS ホスト名とは

ネットボランチ DNS サービスにより取得できる固定のホスト名です。ネットボランチ DNS ホスト名は、ヤマハルーターのグローバル IP アドレスと結びつけられます。

インターネットに常時接続している場合でも、割り当てられるグローバル IP アドレスは再接続時または一定時間経過時に変更されることがあります。グローバル IP アドレスが変更されると IP アドレスがネットボランチ DNS サーバーへ通知され、ネットボランチ DNS ホスト名に結びつけられた IP アドレスが更新されます。ネットボランチ DNS ホスト名の取得について詳しくは「第 6 章 ネットボランチ DNS サービスを利用する」(64 ページ) をご覧ください。

## 7.1 VPN の設定をする前に

LAN 同士を接続する場合には、それぞれの LAN のネットワークアドレスが重複しないように、異なるアドレスを設定しておく必要があります。あらかじめ、ヤマハルーターの LAN のネットワークアドレスを変更してください。詳しくは「3.3 LAN の IP アドレスを設定する」(23 ページ) をご覧ください。

### 7.2 IPsecで接続する (NVR700W)

IPsecで拠点間を接続するために必要な設定と接続方法を説明します。IPsecで拠点間を接続するには、どちらかの拠点に固定グローバルIPアドレスまたはネットボランチDNSホスト名が必要になります。

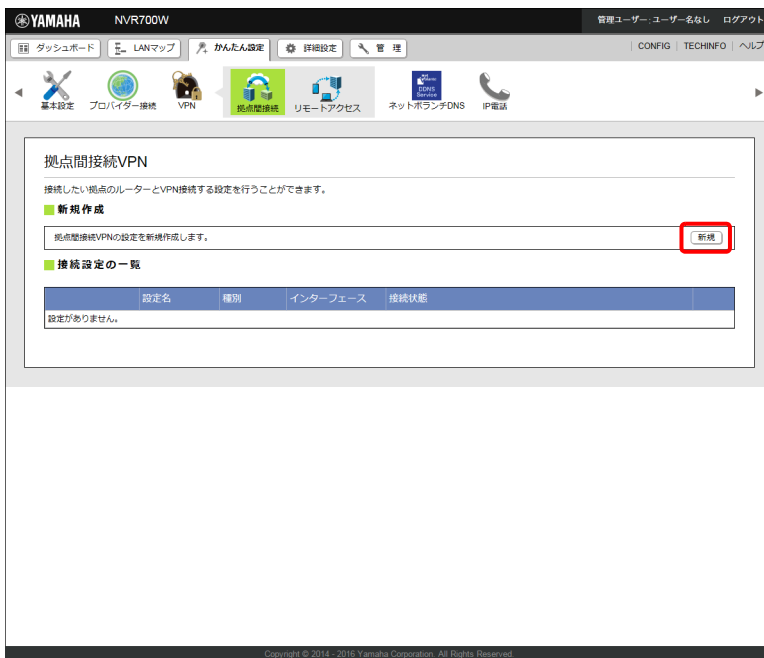
#### ご注意

本機能はNVR700Wをお使いの場合に設定できます。NVR510では設定できません。

#### メモ

ヤマハルーターのIPsecの仕様および設定コマンドについては、「コマンドリファレンス」(製品付属のCD-ROMに収録)をご覧ください。

1. 「かんたん設定」タブ - 「VPN」 - 「拠点間接続」ボタンを順に選択する。  
「拠点間接続VPN」画面が表示されます。
2. 「新規作成」項目の「新規」ボタンをクリックする。



「接続種別の選択」画面が表示されます。

## 3. 「IPsec」を選択し、「次へ」ボタンをクリックする。



「IPsecに関する設定」画面が表示されます。

## 4. IPsec の接続情報を設定する。

## ご注意

- IPsec 接続をするには、双方の拠点で同じ認証鍵 (pre-shared key) を設定する必要があります。
- 認証鍵 (pre-shared key) はパスワードに相当する重要な情報です。英大文字および英小文字、数字、記号を組み合わせた分りにくく長い値を設定し、十分に注意して管理してください。

## 第7章 拠点間をVPNで接続する

自分側と接続先の両方とも固定のグローバルアドレスまたはネットボランチ DNS ホスト名を持っている場合

YAMAHA NVR700W 管理ユーザー ユーザー名なし ログアウト

ダッシュボード LANマップ かんたん設定 詳細設定 管理

CONFIG | TECHNICO | ヘルプ

基本設定 プロバイダー接続 VPN 拡張接続 リモートアクセス ネットボランチDNS IP電話

### 拠点間接続VPN

接続種別の選択

- ✓ IPsecに関する設定
- 経路に関する設定
- 入力内容の確認

設定完了

#### IPsecに関する設定

各項目を入力してください。入力完了したら、「次へ」を押してください。

##### ネットワーク環境

①  自分側と接続先の両方とも固定のグローバルアドレスまたはネットボランチDNSホスト名を持っている

自分側のみの固定のグローバルアドレスまたはネットボランチDNSホスト名を持っている

接続先のみの固定のグローバルアドレスまたはネットボランチDNSホスト名を持っている

##### 自分側の設定

② 設定名 IPsec [※強制可]

##### 接続先の情報

③ 接続先のホスト名またはIPアドレス 203.0.113.2

##### 接続先と合わせる設定

④ 認証鍵 (pre-shared key) keyname

認証アルゴリズム HMAC-SHA

暗号アルゴリズム AES-CBC

中止 戻る 次へ

Copyright © 2014 - 2016 Yamaha Corporation. All Rights Reserved.

### ① ネットワーク環境：

「自分側と接続先の両方とも固定のグローバルアドレスまたはネットボランチ DNS ホスト名を持っている」を選択します。

### ② 自分側の設定：

自分側のヤマハルーターの設定を行います。

- 設定名：任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。

### ③ 接続先の情報：

接続先の情報を入力します。

- 接続先のホスト名または IP アドレス：ネットボランチ DNS ホスト名または接続先の IP アドレスを入力します。

### ④ 接続先と合わせる設定：

接続先と同じ値を設定します。

- 認証鍵 (pre-shared key)：データの暗号化に使用する事前共有鍵を入力します。
- 認証アルゴリズム：認証に使用するアルゴリズムを設定します。
- 暗号アルゴリズム：暗号化に使用するアルゴリズムを設定します。

## 自分側のみ固定のグローバルアドレスまたはネットボランチ DNS ホスト名を持っている場合

## ① ネットワーク環境：

「自分側のみ固定のグローバルアドレスまたはネットボランチ DNS ホスト名を持っている」を選択します。

## ② 自分側の設定：

自分側のヤマハルーターの設定を行います。

- 設定名：任意の名前を入力します。接続先がわかるような名前にしておく、設定の修正や削除をする場合に便利です。

## ③ 接続先の情報：

接続先の情報を入力します。

- 接続先の ID：接続先の「自分側の設定」項目の「自分側の ID」に設定された ID を入力します。

## ④ 接続先と合わせる設定：

接続先と同じ値を設定します。

- 認証鍵 (pre-shared key)：データの暗号化に使用する事前共有鍵を入力します。
- 認証アルゴリズム：認証に使用するアルゴリズムを設定します。
- 暗号アルゴリズム：暗号化に使用するアルゴリズムを設定します。

## 第7章 拠点間をVPNで接続する

### 接続先のみ固定のグローバルアドレスまたはネットボランチ DNS ホスト名を持っている場合



#### ① ネットワーク環境：

「接続先のみ固定のグローバルアドレスまたはネットボランチ DNS ホスト名を持っている」を選択します。

#### ② 自分側の設定：

自分側のヤマハルーターの設定を行います。

- 設定名：任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。
- 自分側の ID：他の拠点と重複しない ID（名前）を半角英数字で入力します。

#### ③ 接続先の情報：

接続先の情報を入力します。

- 接続先のホスト名または IP アドレス：ネットボランチ DNS ホスト名または接続先の IP アドレスを入力します。

#### ④ 接続先と合わせる設定：

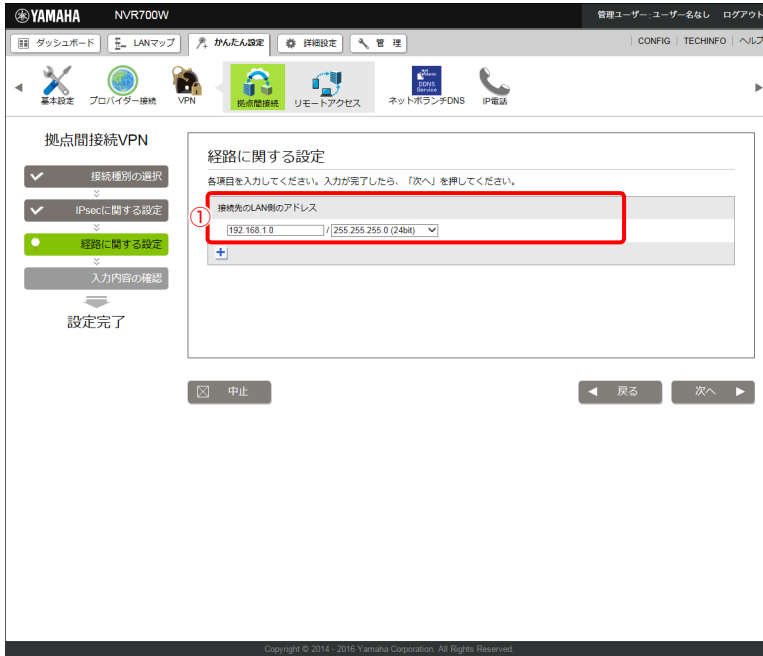
接続先と同じ値を設定します。

- 認証鍵（pre-shared key）：データの暗号化に使用する事前共有鍵を入力します。
- 認証アルゴリズム：認証に使用するアルゴリズムを設定します。
- 暗号アルゴリズム：暗号化に使用するアルゴリズムを設定します。

#### 5. 「次へ」 ボタンをクリックする。

「経路に関する設定」画面が表示されます。

## 6. 接続先の LAN 側のネットワークアドレスを設定する。



## ① 接続先の LAN 側のアドレス：

接続先の LAN 側のネットワークアドレスを入力します。双方でネットワークアドレスが重複している場合は、どちらかのネットワークアドレスを変更してください。

## 7. 「次へ」 ボタンをクリックする。

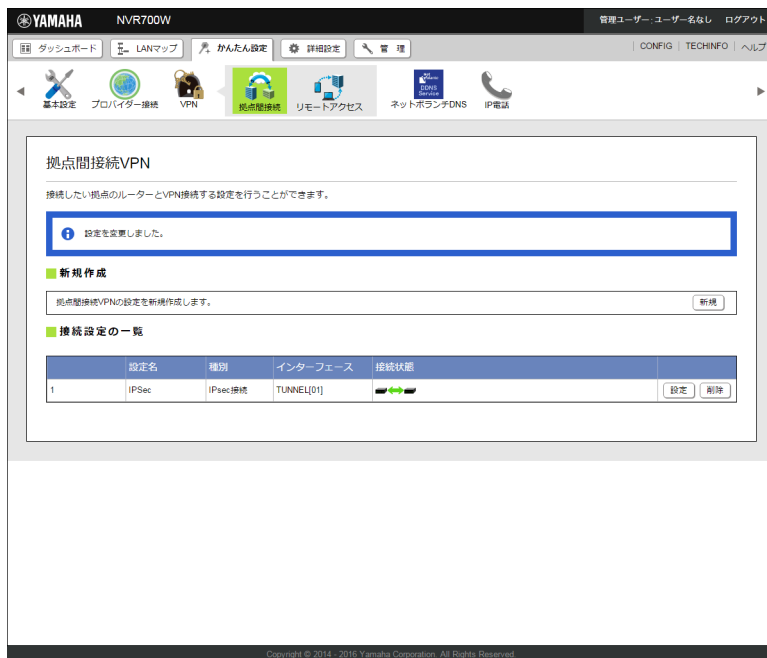
「入力内容の確認」画面が表示されます。

## 8. 内容を確認し、「設定の確定」ボタンをクリックする。



## 第7章 拠点間をVPNで接続する

設定が反映され、「拠点間接続 VPN」画面が表示されます。



双方の拠点で認証が成功すると、自動的に IPsec で拠点間が接続されます（特に操作は必要ありません）。IPsec 接続が完了すると、「拠点間接続 VPN」画面の「接続状態」の表示が 🟢🟢🟢 に切り替わります。

自動的に IPsec で拠点間が接続されない場合は下記の可能性があります。設定を見直してください。

- ・ 接続先の IP アドレス / ネットボランチ DNS ホスト名 / ID が間違っている
- ・ 接続先と認証鍵（pre-shared key） / 認証アルゴリズム / 暗号アルゴリズムの設定が一致していない

設定を見直しても接続されない場合は、ルーターのシリアルコンソール画面または TELNET コンソール画面から ping コマンドを実行し、接続先の IP アドレスに到達できるか確認してください。到達できない場合は、双方の拠点でインターネット接続ができるか確認してください。シリアルコンソール画面または TELNET コンソール画面へのログイン方法について詳しくは、取扱説明書（製品付属の CD-ROM に収録）をご覧ください。

### 7.3 PPTP で接続する

PPTP で拠点間を接続するために必要な設定と接続方法を説明します。PPTP で拠点間を接続するには、双方の拠点に固定グローバル IP アドレスまたはネットボランチ DNS ホスト名が必要になります。ヤマハルーターを PPTP サーバー / PPTP クライアントとして動作させるために必要な設定を行います。

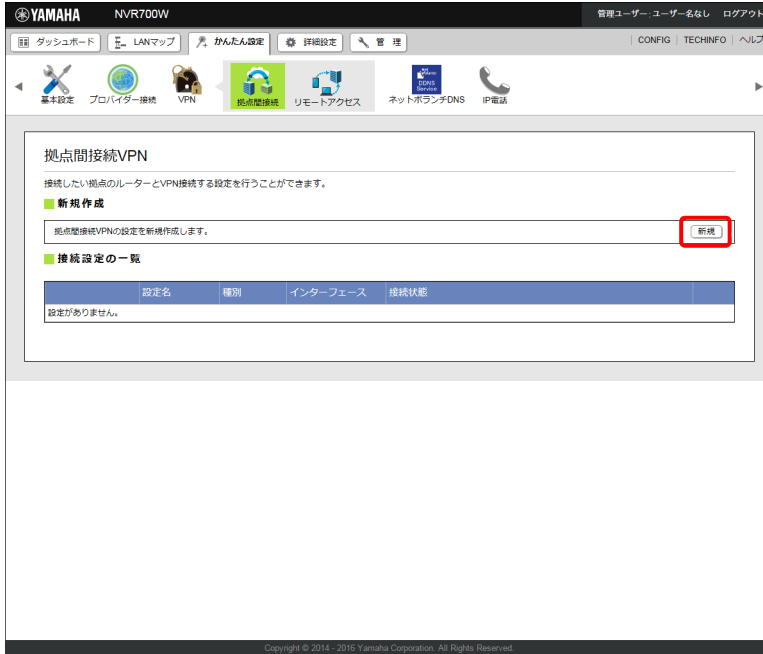
#### メモ

ヤマハルーターの PPTP の仕様および設定コマンドについて詳しくは、「コマンドリファレンス」（製品付属の CD-ROM に収録）をご覧ください。

1. 「かんたん設定」タブ - 「VPN」 - 「拠点間接続」ボタンを順に選択する。  
「拠点間接続 VPN」画面が表示されます。



## 2. 「新規作成」項目の「新規」ボタンをクリックする。



「接続種別の選択」画面が表示されます。

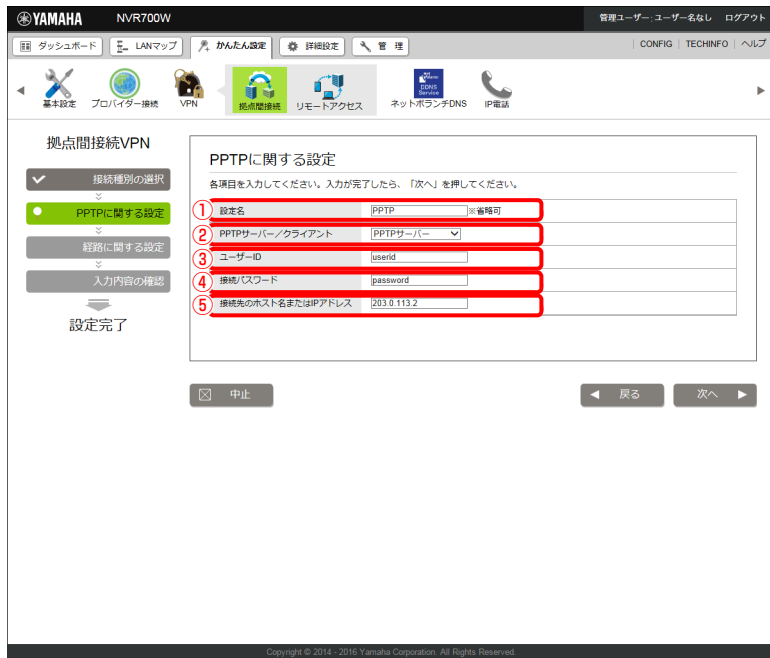
## 3. 「PPTP」を選択し、「次へ」ボタンをクリックする。



「PPTPに関する設定」画面が表示されます。

## 第7章 拠点間をVPNで接続する

### 4. PPTPの接続情報を設定する。



#### ① 設定名：

任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。

#### ② PPTP サーバー／クライアント：

自分側を VPN 接続のサーバー側にするかクライアント側にするかを選択します。

#### ③ ユーザー ID：

VPN 接続を行う際のユーザー認証で使用するユーザー ID を入力します。双方の拠点で同じユーザー ID を設定してください。

#### ④ 接続パスワード：

VPN 接続を行う際のユーザー認証で使用するパスワードを入力します。双方の拠点で同じパスワードを設定してください。

#### ⑤ 接続先のホスト名または IP アドレス：

接続先のネットボランチ DNS ホスト名または IP アドレスを入力します。

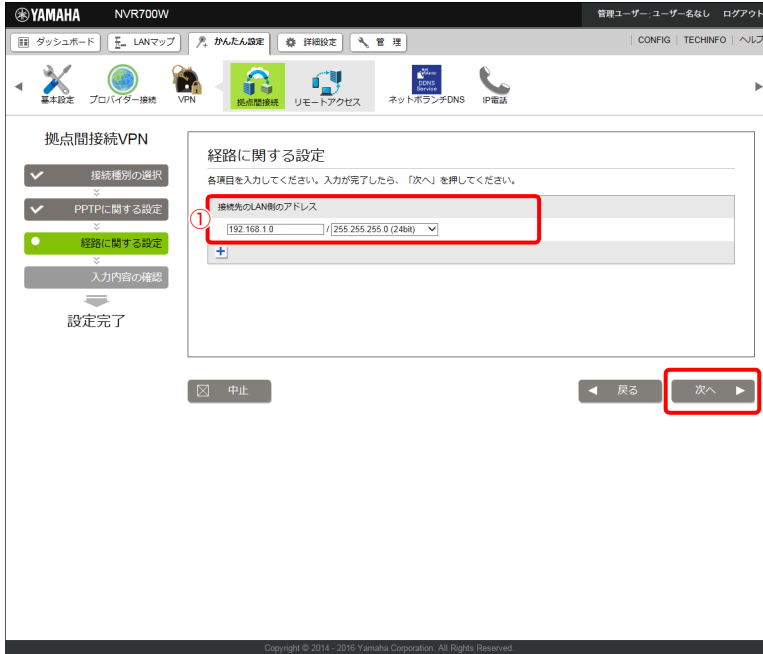
### ご注意

接続する側を PPTP クライアント、接続される側を PPTP サーバーとして設定してください。

### 5. 「次へ」ボタンをクリックする。

「経路に関する設定」画面が表示されます。

## 6. 接続先の LAN 側のネットワークアドレスを設定する。



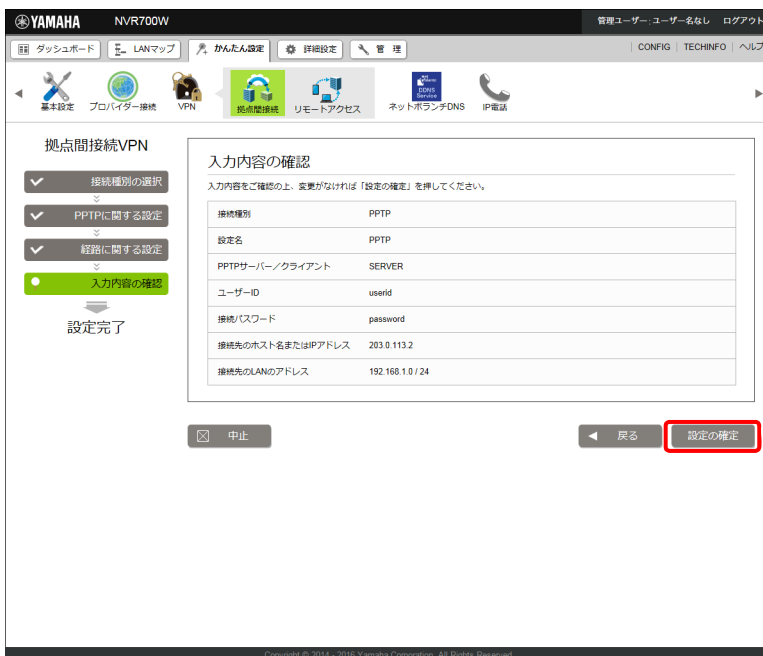
## ① 接続先の LAN 側のアドレス：

接続先の LAN 側のネットワークアドレスを入力します。双方でネットワークアドレスが重複している場合は、どちらかのネットワークアドレスを変更してください。

## 7. 「次へ」 ボタンをクリックする。

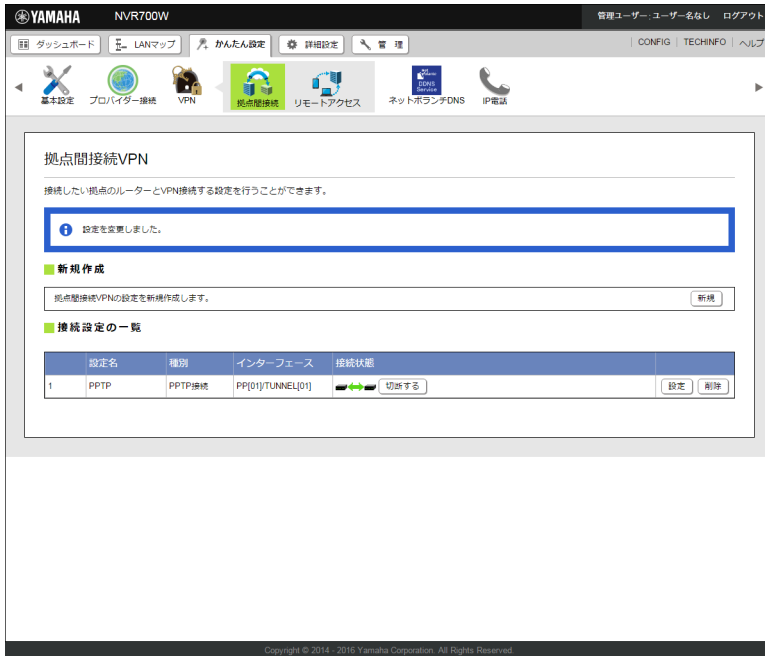
「入力内容の確認」画面が表示されます。


## 8. 内容を確認し、「設定の確定」 ボタンをクリックする。



## 第7章 拠点間をVPNで接続する

設定が反映され、「拠点間接続 VPN」画面が表示されます。



双方の拠点で認証が成功すると、自動的に PPTP で拠点間が接続されます（特に操作は必要ありません）。PPTP 接続が完了すると、「拠点間接続 VPN」画面の「接続状態」の表示が  に切り替わります。「拠点間接続 VPN」画面の「接続する」または「切断する」ボタンをクリックすると、手動で拠点間接続を接続または切断できます。

自動的に PPTP で拠点間が接続されない場合は下記の可能性があります。設定を見直してください。

- ・ 接続先の IP アドレス / ネットボランチ DNS ホスト名が間違っている
- ・ 接続先とユーザー ID / 接続パスワードの設定が一致していない

設定を見直しても接続されない場合は、ルーターのシリアルコンソール画面または TELNET コンソール画面から ping コマンドを実行し、接続先の IP アドレスに到達できるか確認してください。到達できない場合は、双方の拠点でインターネット接続ができるか確認してください。シリアルコンソール画面または TELNET コンソール画面へのログイン方法については、取扱説明書（製品付属の CD-ROM に収録）をご覧ください。

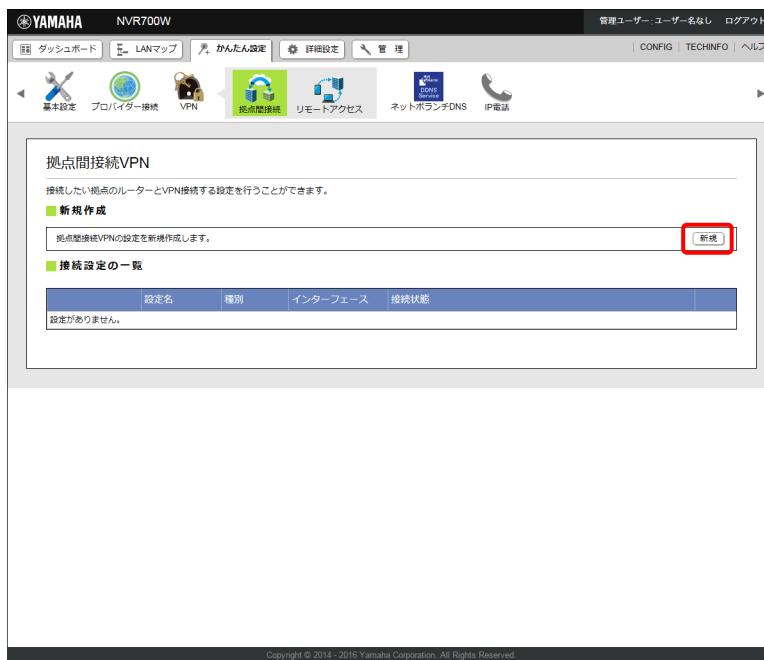
## 7.4 IPIP で接続する

IPIP で拠点間を接続するために必要な設定と接続方法を説明します。データは暗号化されないため、フレッツ網など機密性の高い閉域網が必要になります。

### メモ

ヤマハルーターの IPIP の仕様および設定コマンドについて詳しくは、「コマンドリファレンス」（製品付属の CD-ROM に収録）をご覧ください。

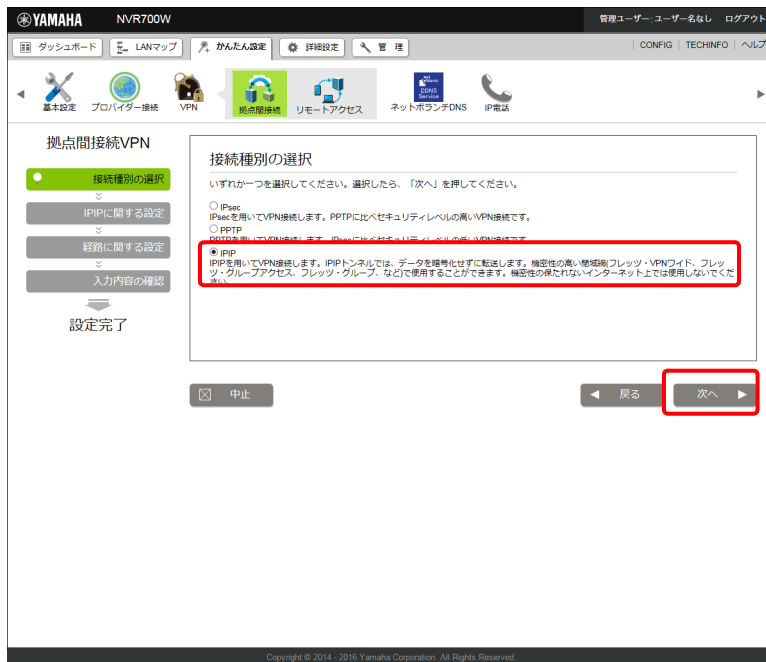
1. 「かんたん設定」タブ - 「VPN」 - 「拠点間接続」 ボタンを順に選択する。  
「拠点間接続 VPN」画面が表示されます。
2. 「新規作成」項目の「新規」 ボタンをクリックする。



「接続種別の選択」画面が表示されます。

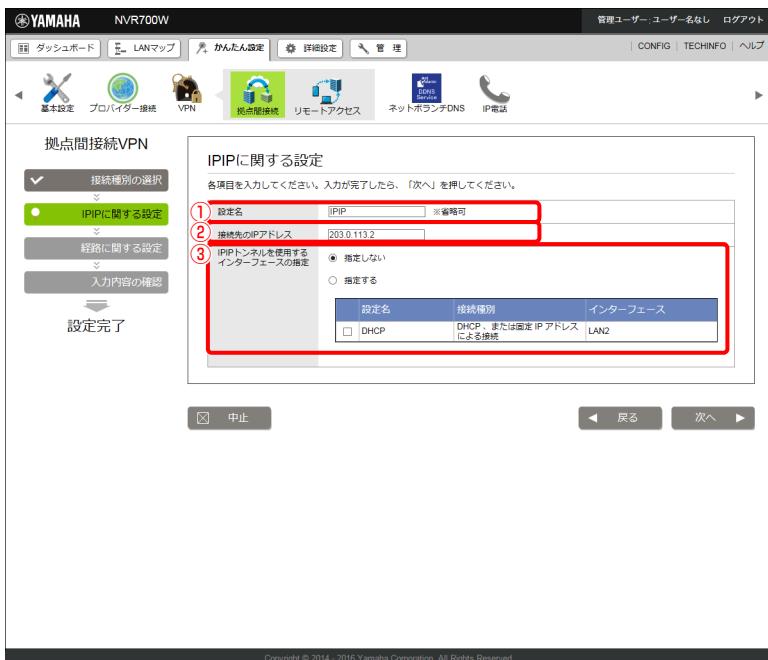
## 第7章 拠点間をVPNで接続する

### 3. 「IPIP」を選択し、「次へ」ボタンをクリックする。



「IPIPに関する設定」画面が表示されます。

### 4. IPIPの接続情報を設定する。



#### ① 設定名：

任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。

#### ② 接続先のIPアドレス：

接続先のIPアドレスを入力します。

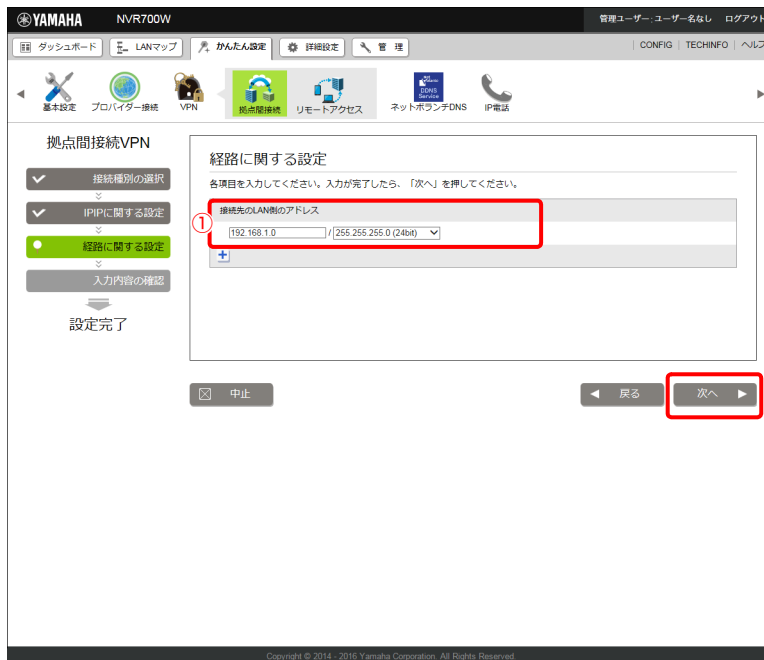
## ③ IPIP トンネルを使用するインターフェースの指定：

IPIP トンネルを使用するインターフェースを指定する場合は、「指定する」を選択し、使用するインターフェースを選択します。選択されたインターフェースに対して、IPIP トンネルによる通信に必要な IP フィルターと静的マスカレードの設定が追加されます。

## ご注意

IPIP トンネルを使用するインターフェースを設定すると、本画面で設定を変更することができなくなります。設定を変更する場合は、「詳細設定」タブ - 「IP フィルター」および「NAT」から行ってください。また、「かんたん設定」タブ - 「VPN」 - 「拠点間接続」のトップページから IPIP トンネルの設定をすべて削除すると、自動設定された IP フィルターと静的マスカレードの設定も一緒に削除されます。

5. 「次へ」ボタンをクリックする。  
「経路に関する設定」画面が表示されます。
6. 接続先の LAN 側のネットワークアドレスを設定する。



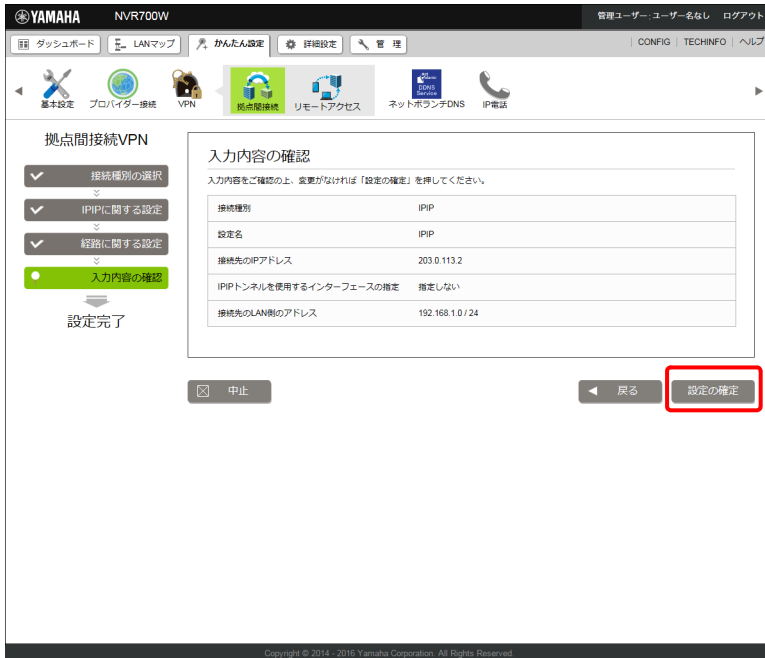
## ① 接続先の LAN 側のアドレス：

接続先の LAN 側のネットワークアドレスを入力します。双方でネットワークアドレスが重複している場合は、どちらかのネットワークアドレスを変更してください。

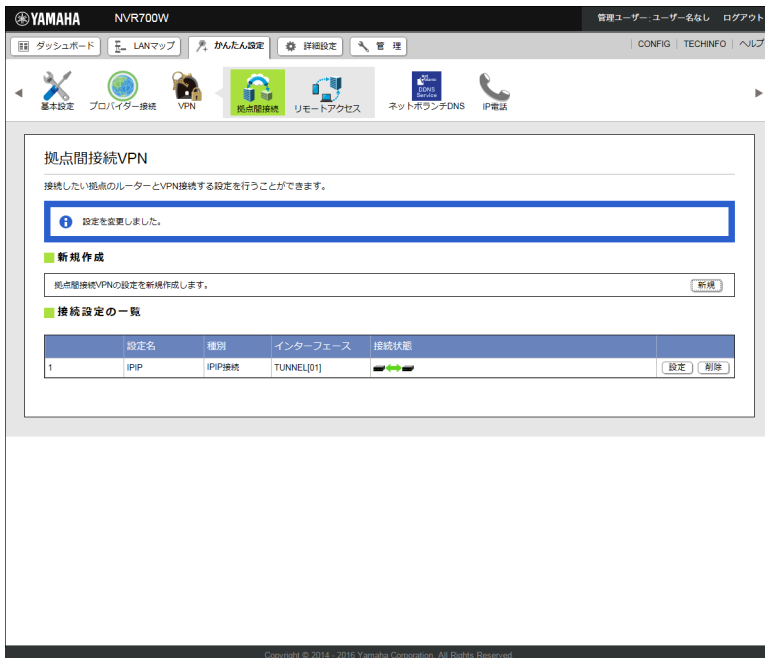
7. 「次へ」ボタンをクリックする。  
「入力内容の確認」画面が表示されます。

## 第7章 拠点間をVPNで接続する


### 8. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「拠点間接続 VPN」画面が表示されます。





双方の拠点で設定が完了すると、自動的に IPIP で拠点間が接続されます（特に操作は必要ありません）。IPIP 接続が完了すると、「拠点間接続 VPN」画面の「接続状態」の表示が  に切り替わります。

自動的に IPIP で拠点間が接続されない場合は下記の可能性があります。設定を見直してください。

- ・ 接続先の IP アドレスが間違っている

設定を見直しても接続されない場合は、ルーターのシリアルコンソール画面または TELNET コンソール画面から ping コマンドを実行し、接続先の IP アドレスに到達できるか確認してください。到達できない場合は、双方の拠点でインターネット接続ができるか確認してください。シリアルコンソール画面または TELNET コンソール画面へのログイン方法について詳しくは、取扱説明書（製品付属の CD-ROM に収録）をご覧ください。

# 第 8 章 外部から VPN 経由で LAN へアクセスする

本章では、仮想プライベートネットワーク（VPN）を構築して、外出先から LAN へリモートアクセスする方法について説明します。

外部の端末から VPN 経由でヤマハルーターにリモートアクセスするには、ヤマハルーター側にプロバイダーからグローバル IP アドレスが割り当てられている必要があります。グローバル IP アドレスとは、下記以外の IP アドレスです。

- 10.0.0.0 ~ 10.255.255.255
- 172.16.0.0 ~ 172.31.255.255
- 192.168.0.0 ~ 192.168.255.255

LAN 内のサーバーまたはパソコンの設定をする …87 ページ

L2TP/IPsec でリモートアクセスする …87 ページ

PPTP でリモートアクセスする …96 ページ

## ご注意

- ・ VPN の設定はインターネットに接続した状態で行う必要があるため、VPN を利用したリモートアクセスの設定の前にインターネット接続の設定が必要です。
- ・ 外部の端末から VPN 経由でヤマハルーターにリモートアクセスするには、ヤマハルーター側にプロバイダーからグローバル IP アドレスが割り当てられている必要があります。
- ・ リモートアクセスを利用するときは、データを保全するために十分なセキュリティ設定を行ってください。セキュリティ設定が不十分な場合は、LAN に接続されたパソコンが不正侵入や盗聴、妨害、データの消失、破壊などにあう可能性があります。
- ・ ヤマハルーターのリモートアクセス機能は、Windows の NetBEUI プロトコルおよび Macintosh の AppleTalk プロトコルには対応していません。
- ・ Windows でファイル共有をする場合は、NetBIOS over TCP/IP プロトコルを使用するか、または WINS サーバーを用意する必要があります。
- ・ Macintosh でファイル共有をする場合は、システム環境設定の「共有」で「パーソナルファイル共有」にチェックを入れます。

## メモ

- ・ 本章では Windows 7 で Internet Explorer 11 を使用した場合の画面を例に説明します。他の環境の場合は画面表示が多少異なりますが基本的な操作は同じです。
- ・ NVR510 の L2TP/IPsec はファームウェアリビジョン Rev.15.01.03 より対応しています。なお、IPsec による LAN 間接続 VPN および L2TPv3 を用いた L2VPN には対応していません。

## ネットボランチ DNS ホスト名とは

ネットボランチ DNS サービスにより取得できる固定のホスト名です。ネットボランチ DNS ホスト名は、ヤマハルーターのグローバル IP アドレスと結びつけられます。

インターネットに常時接続している場合でも、割り当てられるグローバル IP アドレスは再接続時または一定時間経過時に変更されることがあります。グローバル IP アドレスが変更されると IP アドレスがネットボランチ DNS サーバーへ通知され、ネットボランチ DNS ホスト名に結びつけられた IP アドレスが更新されます。ネットボランチ DNS ホスト名の取得について詳しくは「第 6 章 ネットボランチ DNS サービスを利用する」（64 ページ）をご覧ください。

## 8.1 LAN 内のサーバーまたはパソコンの設定をする

リモートアクセスするには、LAN 内のサーバーやパソコンに TCP/IP プロトコルでアクセスできるようにするための設定が必要です。

### ファイルサーバーソフトの設定を変更する

公開するサーバーまたはパソコンにファイルサーバーソフトやネットワーク共有を設定して、公開するフォルダーやユーザー ID、パスワードを設定します。

## 8.2 L2TP/IPsec でリモートアクセスする

パソコンやスマートフォンなどから L2TP/IPsec を利用してリモートアクセスを行うことができます。本章では YMS-VPN8 をインストールしたパソコンからアクセスする場合を例に説明します。

接続先のルーター側の設定：8.2.1 ヤマハルーターの設定（L2TP/IPsec）をする（87 ページ）

接続元のパソコン側の設定：8.2.3 YMS-VPN8 の設定をする（93 ページ）

### メモ

- ・ YMS-VPN8 について詳しくは、YMS-VPN8 の取扱説明書をご覧ください。
- ・ スマートフォンなど他のクライアントの設定方法はヤマハネットワーク周辺機器技術情報ページをご覧ください。  
[http://www.rtpro.yamaha.co.jp/RT/docs/l2tp\\_ipsec/](http://www.rtpro.yamaha.co.jp/RT/docs/l2tp_ipsec/)
- ・ NVR510 の L2TP/IPsec はファームウェアリビジョン Rev.15.01.03 より対応しています。なお、IPsec による LAN 間接続 VPN および L2TPv3 を用いた L2VPN には対応していません。

### 8.2.1 ヤマハルーターの設定（L2TP/IPsec）をする

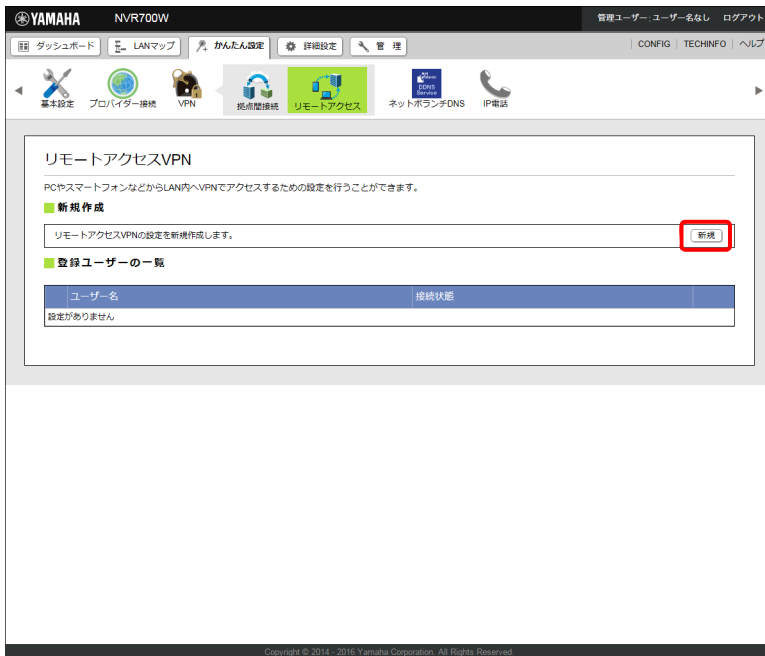
#### ご注意

ヤマハルーターの WAN 側または PP 側に固定グローバル IP アドレスまたはネットボランチ DNS で取得したホスト名が必要です。

1. 「かんたん設定」タブ - 「VPN」 - 「リモートアクセス」ボタンを順に選択する。  
「リモートアクセス VPN」画面が表示されます。

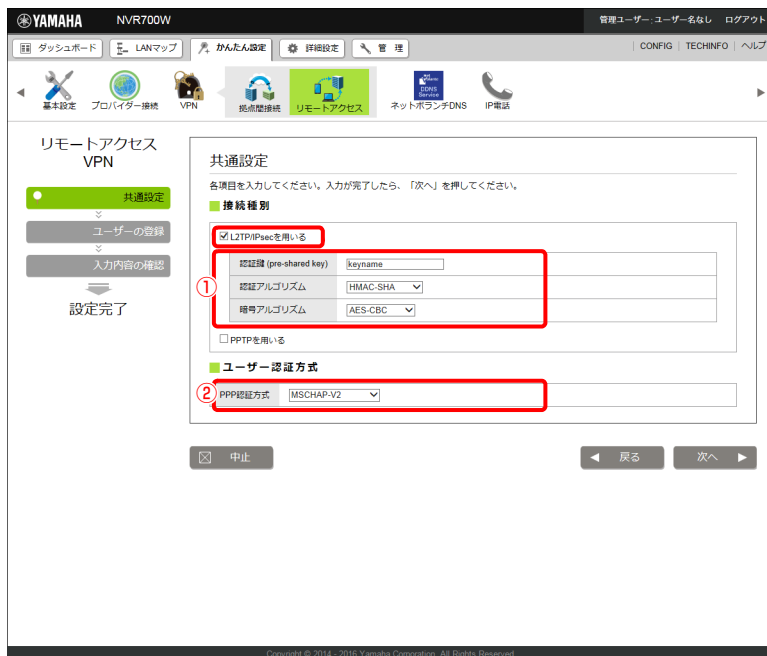
## 第8章 外部からVPN経由でLANへアクセスする

### 2. 「新規作成」項目の「新規」ボタンをクリックする。



「共通設定」画面が表示されます。

### 3. 「L2TP/IPsecを用いる」にチェックを入れ、VPNの接続情報を設定する。



#### ① 接続種別：

- ・ 認証鍵（pre-shared key）：データの暗号化に使用する事前共有鍵を入力します。
- ・ 認証アルゴリズム：認証に使用するアルゴリズムを設定します。
- ・ 暗号アルゴリズム：暗号化に使用するアルゴリズムを設定します。

## ② ユーザー認証方式：

- ・ PPP 認証方式：VPN 接続を行うユーザーの認証方式を設定します。

4. 「次へ」 ボタンをクリックする。  
「ユーザーの登録」画面が表示されます。

5. リモートアクセスするユーザー情報を設定する。



## ① ユーザー名：

VPN 接続を行う際のユーザー認証で使用するユーザー ID を入力します。

## ② パスワード：

VPN 接続を行う際のユーザー認証で使用するパスワードを入力します。

ユーザーを複数登録する場合は、「+」ボタンをクリックしてください。

6. 「次へ」 ボタンをクリックする。  
「入力内容の確認」画面が表示されます。

## 第8章 外部からVPN経由でLANへアクセスする

### 7. 内容を確認し、「設定の確定」ボタンをクリックする。

The screenshot shows the 'Remote Access VPN' configuration page in the Yamaha NVR700W Web GUI. The page is titled 'リモートアクセス VPN' and has a sidebar with navigation options: '共通設定' (Common Settings), 'ユーザーの登録' (User Registration), and '入力内容の確認' (Input Confirmation). The '入力内容の確認' section is active, displaying the following settings:

**入力内容の確認**  
入力内容をご確認の上、変更がなければ「設定の確定」を押してください。

**共通設定**

L2TP/IPsecを用いる	on
認証鍵 (pre-shared key)	keyname
認証アルゴリズム	SHA-HMAC
暗号アルゴリズム	AES-CBC
PPTPを用いる	off
PPP	MSCHAP-V2

**ユーザーの登録**

ユーザー名	パスワード
username	password

At the bottom of the page, there are three buttons: '中止' (Cancel), '戻る' (Back), and '設定の確定' (Confirm Settings), which is highlighted with a red box.

設定が反映され、「リモートアクセス VPN」画面が表示されます。

The screenshot shows the 'Remote Access VPN' configuration page in the Yamaha NVR700W Web GUI after the settings have been confirmed. The page is titled 'リモートアクセスVPN' and has a sidebar with navigation options: '基本設定' (Basic Settings), 'プロバイダー接続' (Provider Connection), 'VPN', '拠点間接続' (Site-to-Site Connection), 'リモートアクセス' (Remote Access), 'ネットホランチDNS' (Net Hologram DNS), and 'IP電話' (IP Phone). The 'リモートアクセス' section is active, displaying the following settings:

**リモートアクセスVPN**  
PCやスマートフォンなどからLAN内へVPNでアクセスするための設定を行うことができます。

設定を変更しました。

**設定**

登録ユーザーの追加、変更を行います。 [設定]

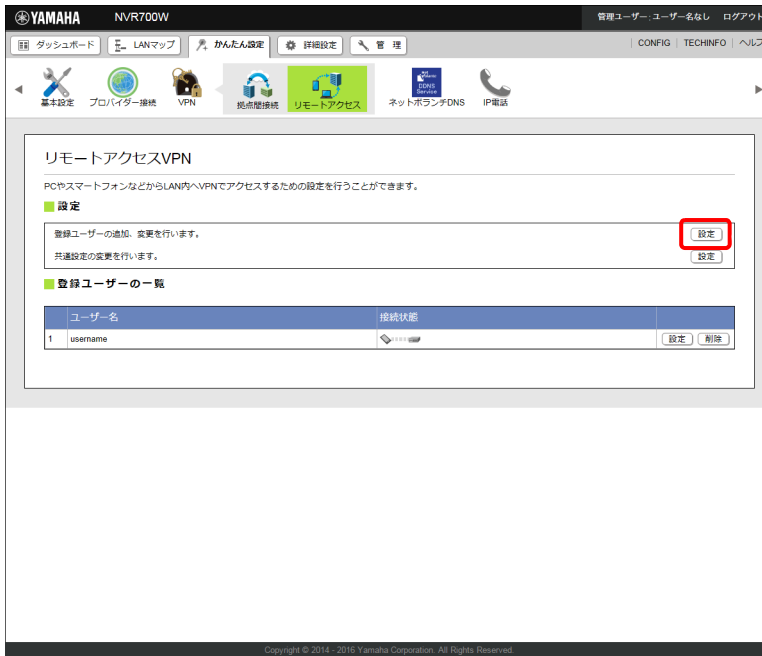
共通設定の変更を行います。 [設定]

**登録ユーザーの一覧**

ユーザー名	接続状態	
1 username	接続状態	[設定] [削除]

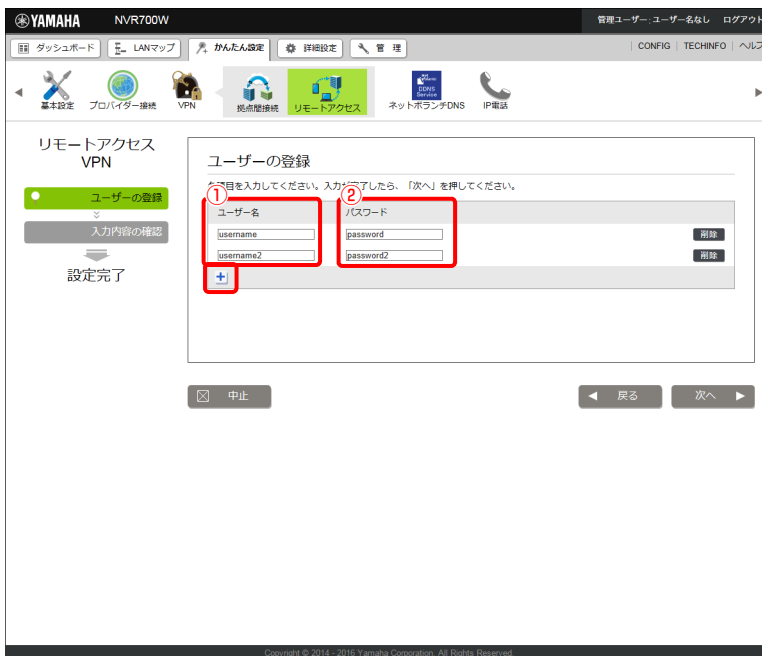
## 8.2.2 接続ユーザーを追加する

1. 「リモートアクセス VPN」画面で、「登録ユーザーの追加、変更を行います。」欄の「設定」ボタンをクリックする。



「ユーザーの登録」画面が表示されます。

2. 「+」ボタンをクリックし、リモートアクセスするユーザー情報を設定する。



## ① ユーザー名：

VPN 接続を行う際のユーザー認証で使用するユーザー ID を入力します。

## 第8章 外部からVPN経由でLANへアクセスする

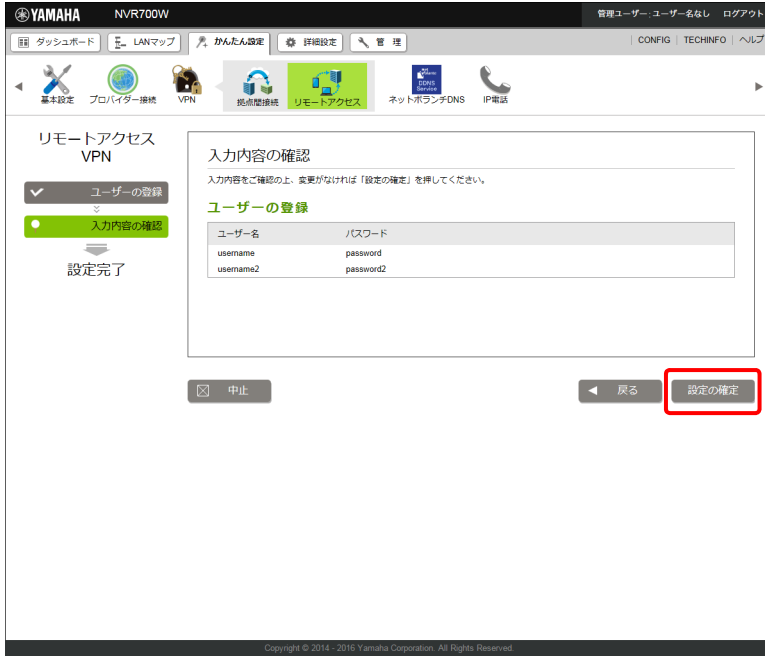
### ② パスワード：

VPN 接続を行う際のユーザー認証で使用するパスワードを入力します。

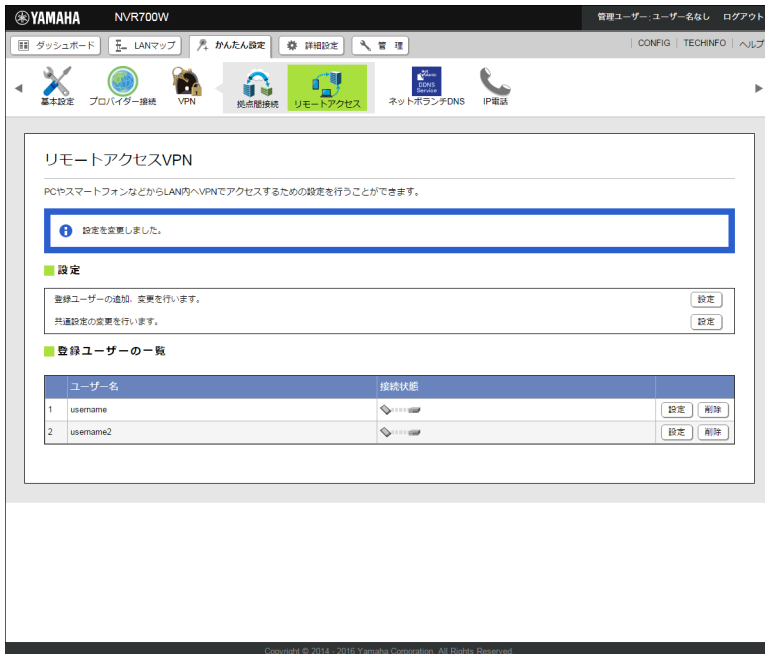
### 3. 「次へ」 ボタンをクリックする。

「入力内容の確認」画面が表示されます。

### 4. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「リモートアクセス VPN」画面が表示されます。





## 8.2.3 YMS-VPN8 の設定をする

## メモ

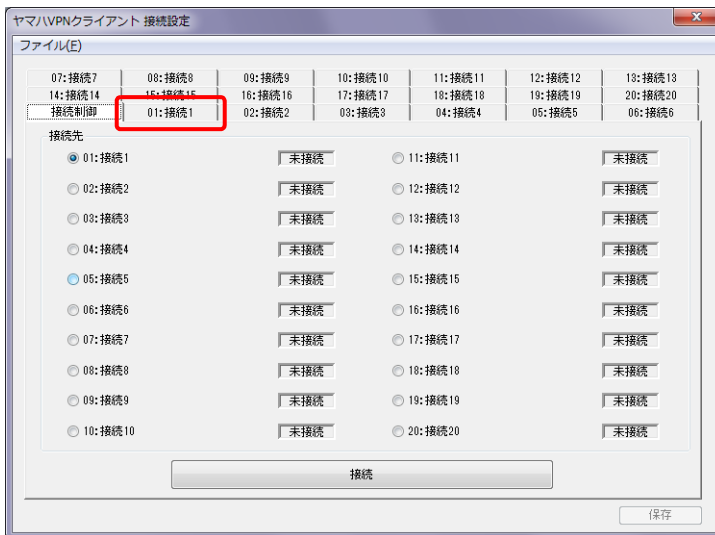
- ・ 本章では Windows 7 の画面を例に説明します。他の環境の場合は画面表示が多少異なりますが基本的な操作は同じです。
- ・ NVR510 の L2TP/IPsec はファームウェアリビジョン Rev.15.01.03 より対応しています。なお、IPsec による LAN 間接続 VPN および L2TPv3 を用いた L2VPN には対応していません。

1. 「スタート」メニューから「すべてのプログラム」－「YMS-VPN8」－「接続設定」を順に選択する。  
YMS-VPN8 が起動して、「接続設定」画面が表示されます。

## メモ

YMS-VPN8 が Windows のタスクトレイに常駐している場合は、「スタート」メニューから起動しても YMS-VPN8 の「接続設定」画面が表示されません。その場合は Windows のタスクトレイから YMS-VPN8 を起動してください。

2. 設定が登録されていないタブをクリックする。

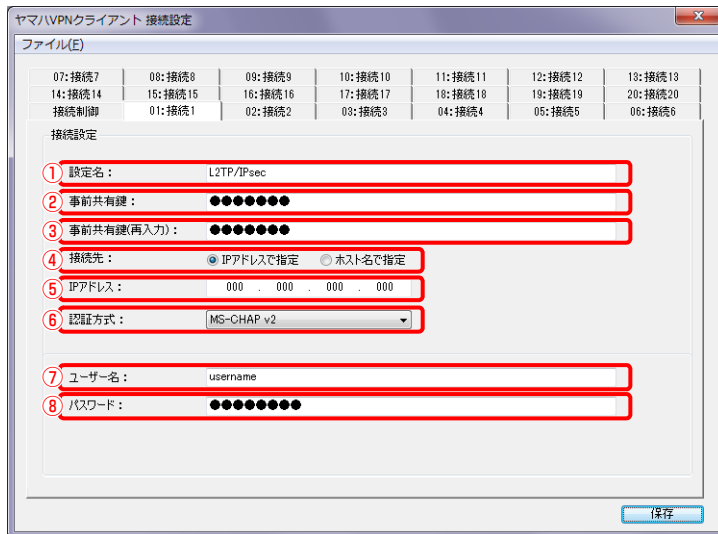


## メモ

- ・ 接続先は 20 件まで登録できます。
- ・ すでに登録した接続先の内容を変更したい場合は、変更したい接続先のタブをクリックします。

接続先の登録画面が表示されます。

### 3. VPN の接続情報を設定する。



#### ① 設定名：

任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。

設定を保存すると、入力した設定名はタブに反映されます（タブ内に設定名が表示しきれない場合は、一部省略して表示されます）。

#### ② 事前共有鍵：

「8.2.1 ヤマハルーターの設定（L2TP/IPsec）をする」（87 ページ）で設定した認証鍵（pre-shared key）を入力します。

入力した事前共有鍵は文字が「●」で表示されます。

#### ③ 事前共有鍵（再入力）：

「事前共有鍵」欄と同一の事前共有鍵を入力します。

入力した事前共有鍵は文字が「●」で表示されます。

#### ④ 接続先：

「IP アドレスで指定」または「ホスト名で指定」のどちらかを選択します。

#### ⑤ IP アドレス：

「接続先」欄で「IP アドレスで指定」を選んだ場合は、ヤマハルーターの WAN 側または PP 側の IP アドレスを入力します。

「ホスト名で指定」を選んだ場合は、「ホスト名」欄にヤマハルーターのネットボランチ DNS ホスト名を入力します。

#### ⑥ 認証方式：

「8.2.1 ヤマハルーターの設定（L2TP/IPsec）をする」（87 ページ）で設定した PPP 認証方式を選択します。

#### ⑦ ユーザー名：

「8.2.1 ヤマハルーターの設定（L2TP/IPsec）をする」（87 ページ）で設定したユーザー名を入力します。

#### ⑧ パスワード：

「8.2.1 ヤマハルーターの設定（L2TP/IPsec）をする」（87 ページ）で設定したパスワードを入力します。

### 4. 「保存」ボタンをクリックする。

設定内容が保存されます。

### ご注意

「保存」ボタンをクリックせずに他のタブで操作を続行した場合、設定内容が失われてしまいます。設定が終わったら、必ず「保存」ボタンをクリックしてください。

## 8.2.4 YMS-VPN8 からヤマハルーターへリモートアクセスする

### メモ

- ・本章では Windows 7 の画面を例に説明します。他の環境の場合は画面表示が多少異なりますが基本的な操作は同じです。
- ・NVR510 の L2TP/IPsec はファームウェアリビジョン Rev.15.01.03 より対応しています。なお、IPsec による LAN 間接続 VPN および L2TPv3 を用いた L2VPN には対応していません。

1. 「スタート」メニューから「すべてのプログラム」 - 「YMS-VPN8」 - 「接続設定」を順に選択する。YMS-VPN8 が起動して、「接続設定」画面が表示されます。

### メモ

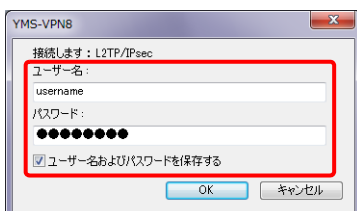
YMS-VPN8 が Windows のタスクトレイに常駐している場合は、「スタート」メニューから起動しても YMS-VPN8 の「接続設定」画面が表示されません。その場合は Windows のタスクトレイから YMS-VPN8 を起動してください。

2. 「接続制御」タブをクリックする。
3. 設定した接続先を選び、「接続」ボタンをクリックする。



接続時にユーザー名とパスワードの入力画面が表示されます。

4. 「7.2.1 ヤマハルーターの設定 (L2TP/IPsec) をする」で設定したユーザー名とパスワードを入力する。



### ご注意

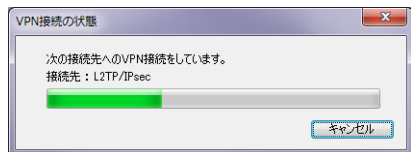
ユーザー名とパスワードは使用者の責任において安全に管理してください。

### メモ

ユーザー名とパスワードは接続設定で入力した設定を初期値として表示します。  
接続設定でユーザー名とパスワードを事前に設定しておくことで、VPN 接続時は「OK」ボタンをクリックするだけで接続できます。

#### 5. 「OK」ボタンをクリックする。

接続中は、「VPN 接続の状態」画面が表示されます。



選んだ接続先に VPN 接続を開始します。

#### リモートアクセスを切断する場合は

「接続設定」画面の「接続制御」タブで、「切断」ボタンをクリックします。

## 8.3 PPTP でリモートアクセスする

パソコンやスマートフォンなどから PPTP を利用してリモートアクセスを行うことができます。  
本章では Windows OS に標準搭載されている PPTP 接続機能を利用してアクセスする場合を例に説明します。

接続先のルーター側の設定：8.3.1 ヤマハルーターの設定（PPTP）をする …96 ページ

接続元のパソコン側の設定：8.3.3 Windows 7 でリモートアクセスする …102 ページ

8.3.4 Windows 8.1 でリモートアクセスする …106 ページ

8.3.5 Windows 10 でリモートアクセスする …110 ページ

### 8.3.1 ヤマハルーターの設定（PPTP）をする

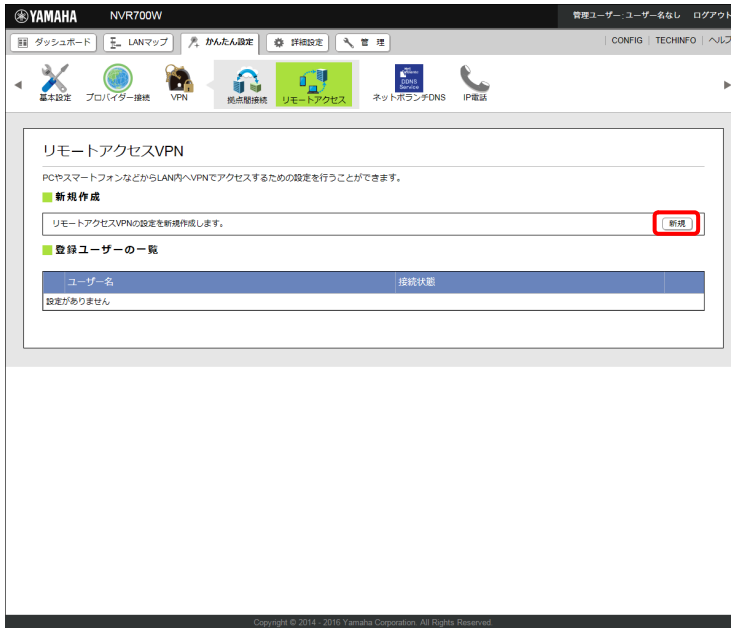
#### ご注意

ヤマハルーターの WAN 側または PP 側に固定グローバル IP アドレスまたはネットボランチ DNS ホスト名が必要です。

#### 1. 「かんたん設定」タブ - 「VPN」 - 「リモートアクセス」ボタンを順に選択する。

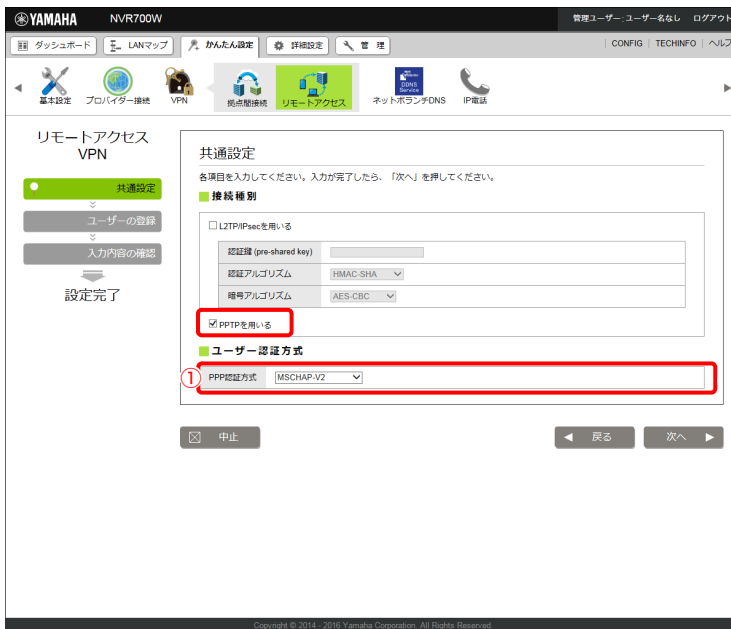
「リモートアクセス VPN」画面が表示されます。

## 2. 「新規作成」項目の「新規」ボタンをクリックする。



「共通設定」画面が表示されます。

## 3. 「PPTP を用いる」にチェックを入れ、VPN の接続情報を設定する。



## ① ユーザー認証方式：

PPP 認証方式：VPN 接続を行うユーザーの認証方式を設定します。

## ご注意

Windows Vista 以降の Windows OS では、Microsoft CHAP Version 1 (MS-CHAP) はサポートされていません。Windows Vista 以降の Windows OS からリモートアクセスする場合は、「MSCHAP-V2」を選択してください。

## 第 8 章 外部から VPN 経由で LAN へアクセスする

4. 「次へ」 ボタンをクリックする。  
「ユーザーの登録」画面が表示されます。
5. リモートアクセスするユーザー情報を設定する。



- ① ユーザー名：  
VPN 接続を行う際のユーザー認証で使用するユーザー ID を入力します。
- ② パスワード：  
VPN 接続を行う際のユーザー認証で使用するパスワードを入力します。

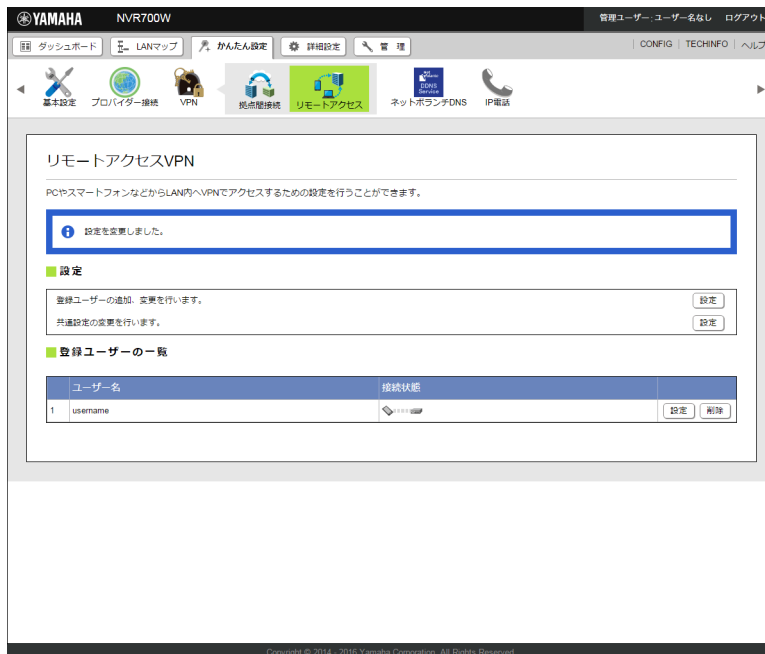
ユーザーを複数登録する場合は、「+」ボタンをクリックしてください。

6. 「次へ」 ボタンをクリックする。  
「入力内容の確認」画面が表示されます。

## 7. 内容を確認し、「設定の確定」ボタンをクリックする。



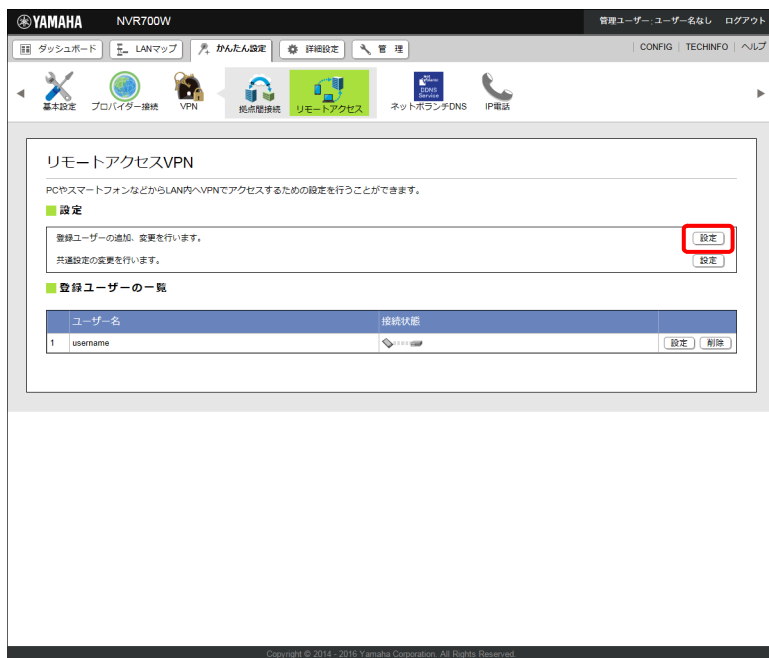
設定が反映され、「リモートアクセス VPN」画面が表示されます。



## 第8章 外部からVPN経由でLANへアクセスする

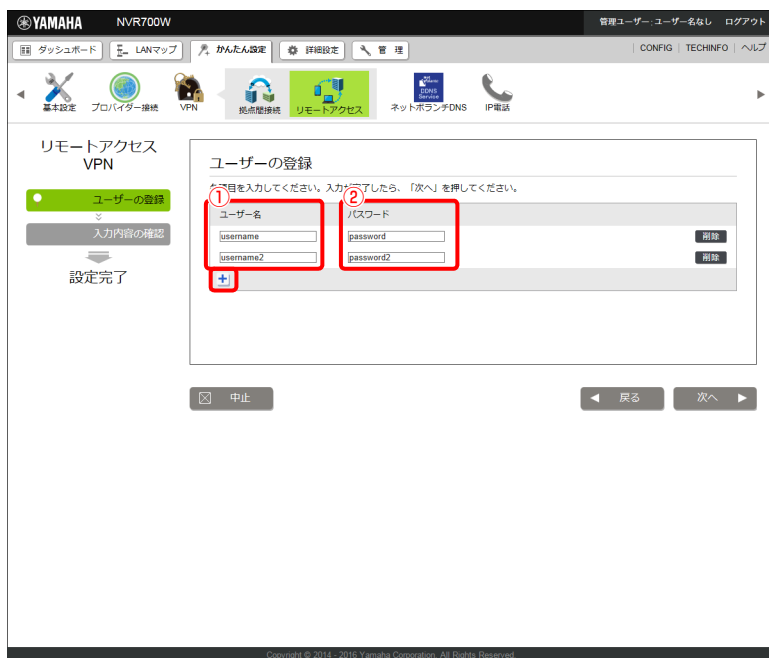
### 8.3.2 接続ユーザーを追加する

1. 「リモートアクセスVPN」画面で、「登録ユーザーの追加、変更を行います。」欄の「設定」ボタンをクリックする。



「ユーザーの登録」画面が表示されます。

2. 「+」ボタンをクリックし、リモートアクセスするユーザー情報を設定する。

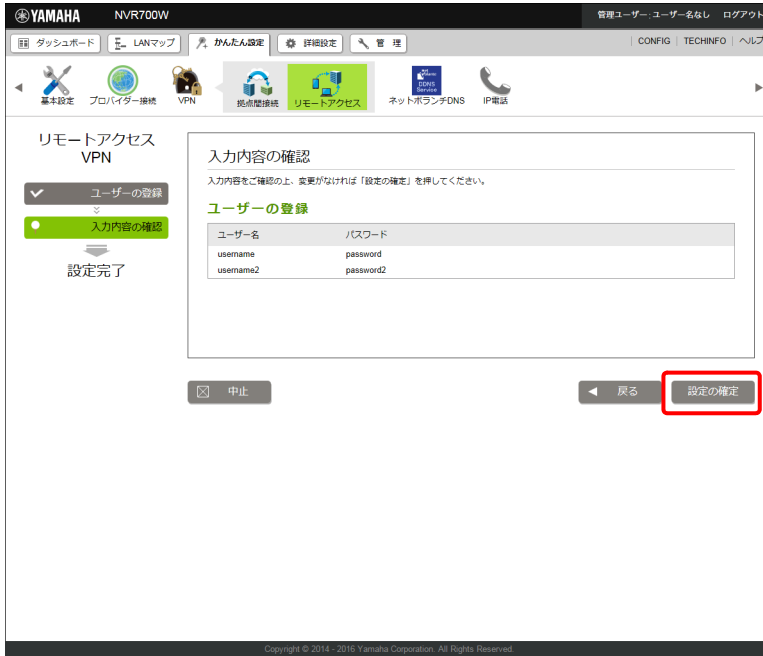


#### ① ユーザー名:

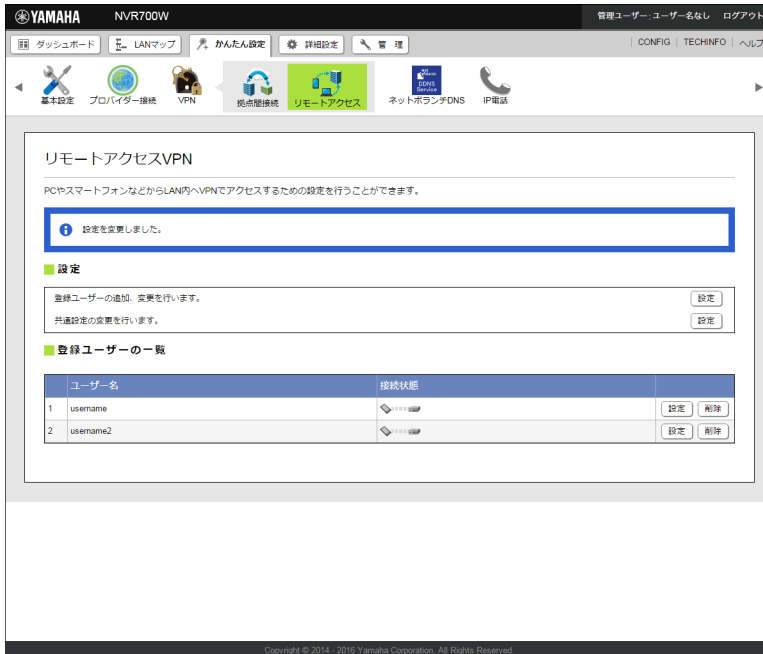
VPN接続を行う際のユーザー認証で使用するユーザーIDを入力します。



- ② パスワード：  
VPN 接続を行う際のユーザー認証で使用するパスワードを入力します。
3. 「次へ」ボタンをクリックする。  
「入力内容の確認」画面が表示されます。
4. 内容を確認し、「設定の確定」ボタンをクリックする。



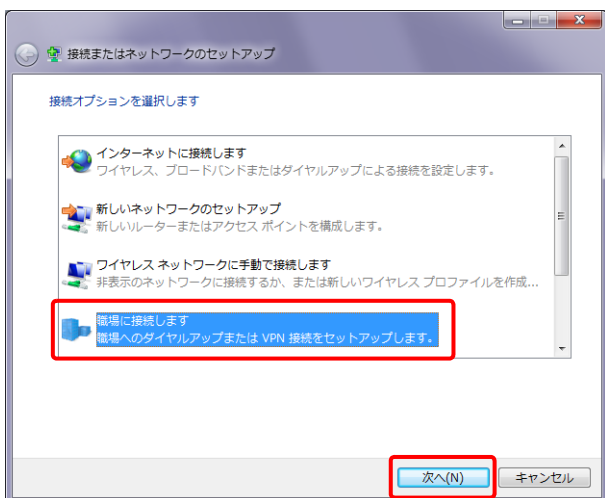
設定が反映され、「リモートアクセス VPN」画面が表示されます。



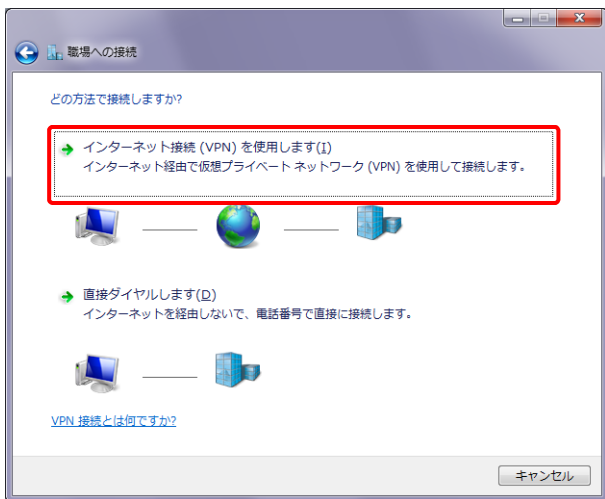
### 8.3.3 Windows 7 でリモートアクセスする

#### VPN の接続設定をする

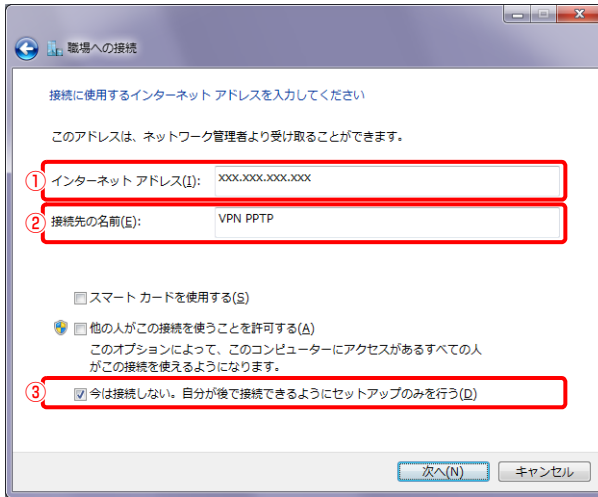
1. 「スタート」メニューから「コントロールパネル」 - 「ネットワークの状態とタスクの表示」の順に選択する。  
「ネットワークと共有センター」画面が表示されます。
2. 「新しい接続またはネットワークのセットアップ」をクリックする。
3. 「職場に接続します」を選択し、「次へ」ボタンをクリックする。



4. 「インターネット接続 (VPN) を使用します」をクリックする。



## 5. VPN の接続情報を設定する。



## ① インターネットアドレス：

ヤマハルーターのネットボランチ DNS ホスト名、もしくは、WAN 側または PP 側の IP アドレスを入力します。

## ② 接続先の名前：

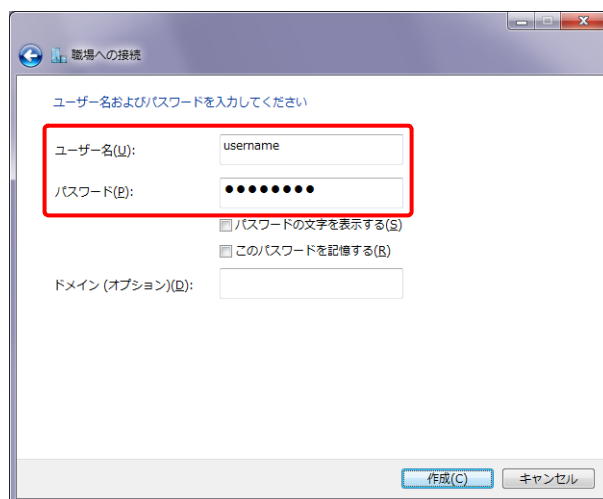
任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。

## ③ 今は接続しない。自分が後で接続できるようにセットアップのみを行う：

チェックボックスにチェックを入れます。

## 6. 「次へ」 ボタンをクリックする。

## 7. 「8.3.1 ヤマハルーターの設定 (PPTP) をする」 (96 ページ) で設定したユーザー名とパスワードを入力する。

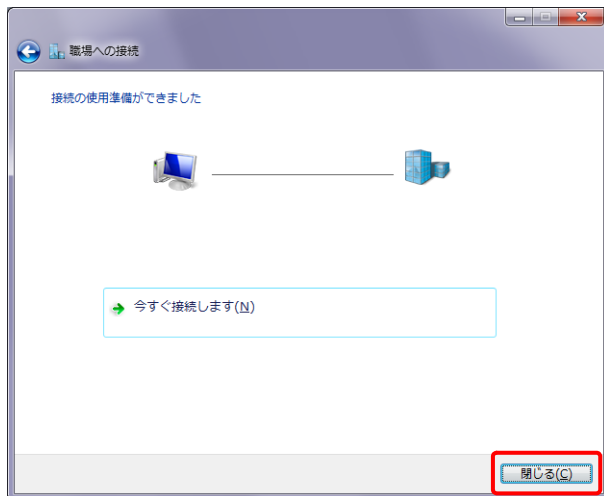


## 8. 「作成」 ボタンをクリックする。

設定内容が保存されます。

## 第 8 章 外部から VPN 経由で LAN へアクセスする

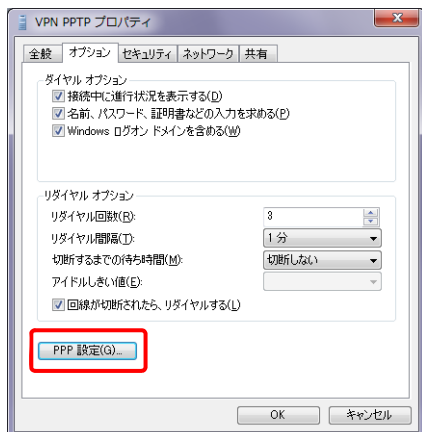
9. 「閉じる」ボタンをクリックする。



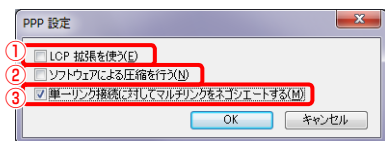
10. 「ネットワークと共有センター」画面で「アダプターの設定の変更」をクリックする。

11. 作成した VPN の接続設定を右クリックし、「プロパティ」を選択する。

12. 「オプション」タブ - 「PPP 設定」ボタンを順に選択する。



13. PPP 設定を変更する。



① LCP 拡張を使う：

チェックボックスのチェックを外します。

② ソフトウェアによる圧縮を行う：

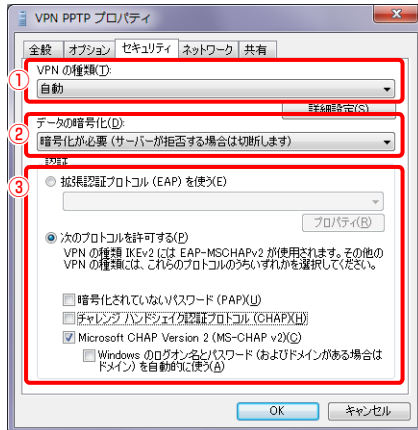
チェックボックスのチェックを外します。

③ 単一リンク接続に対してマルチリンクをネゴシエートする：

チェックボックスにチェックを入れます。

14. 「OK」ボタンをクリックし、「セキュリティ」タブを選択する。

## 15.セキュリティ設定を変更する。



## ① VPNの種類：

「自動」を選択します。

## ② データの暗号化：

「暗号化が必要 (サーバーが拒否する場合は切断します)」を選択します。

## ③ 認証：

「次のプロトコルを許可する」を選択し、以下のように設定します。

- ・ 暗号化されていないパスワード (PAP)：チェックボックスのチェックを外す。
- ・ チャレンジハンドシェイク認証プロトコル (CHAP)：チェックボックスのチェックを外す。
- ・ Microsoft CHAP Version 2 (MS-CHAPv2)：チェックボックスにチェックを入れる。
- ・ Windows のログオン名とパスワード (およびドメインがある場合はドメイン) を自動的に使う：チェックを外す。

## ご注意

Windows Vista 以降の Windows OS では、Microsoft CHAP Version 1 (MS-CHAP) はサポートされていません。「8.3.1 ヤマハルーターの設定 (PPTP) をする」の手順 4 で「MSCHAP-V2」を選択してください。

## 16.「OK」ボタンをクリックする。

## ヤマハルーターへリモートアクセスする

1. 「スタート」メニューから「コントロールパネル」－「ネットワークの状態とタスクの表示」の順に選択する。
2. 「ネットワークに接続」をクリックする。

## 第 8 章 外部から VPN 経由で LAN へアクセスする

3. 作成した VPN の接続設定を選択し、「接続」ボタンをクリックする。



4. 「8.3.1 ヤマハルーターの設定 (PPTP) をする」(96 ページ) で設定したユーザー名とパスワードを入力し、「接続」ボタンをクリックする。



### メモ

「次のユーザーが接続するとき使用するために、このユーザー名とパスワードを保存する」にチェックを入れると、次回からパスワードの入力が不要になります。チェックしない場合は、接続のたびにパスワード入力が必要になります。

ヤマハルーターへの VPN 接続を開始します。

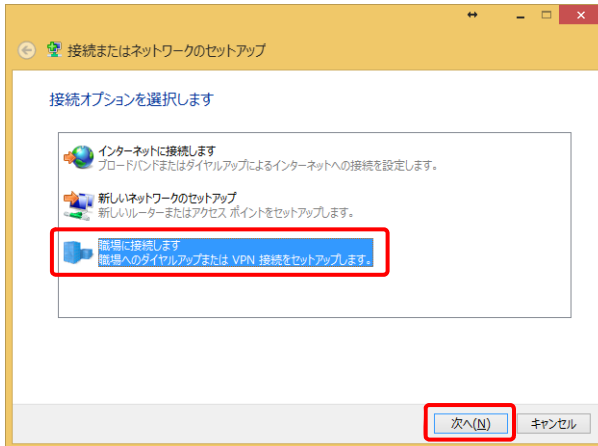
**リモートアクセスを切断する場合は**  
「切断」ボタンをクリックします。

## 8.3.4 Windows 8.1 でリモートアクセスする

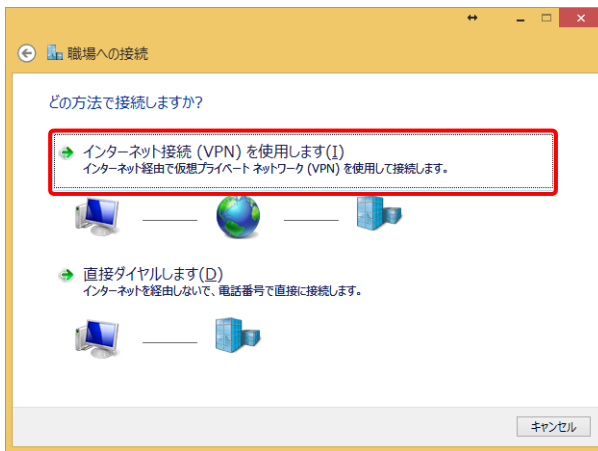
### VPN の接続設定をする

1. 「デスクトップ」画面で、マウスカーソルを右上隅または右下隅に移動する。
2. チャームから「設定」 - 「コントロールパネル」 - 「ネットワークの状態とタスクの表示」の順に選択する。「ネットワークと共有センター」画面が表示されます。
3. 「新しい接続またはネットワークのセットアップ」をクリックする。

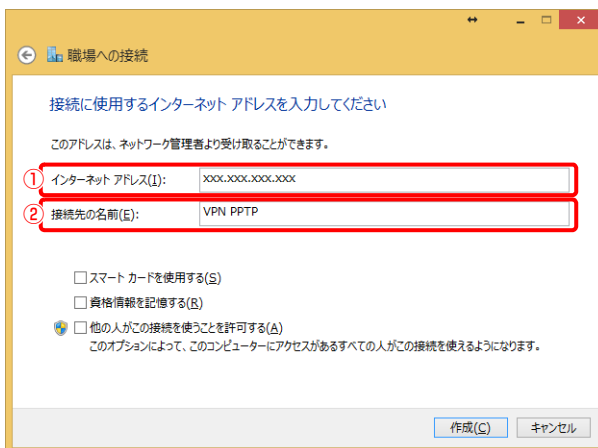
4. 「職場に接続します」を選択し、「次へ」ボタンをクリックする。



5. 「インターネット接続 (VPN) を使用します」をクリックする。



6. VPN の接続情報を設定する。



## 第 8 章 外部から VPN 経由で LAN へアクセスする

### ① インターネットアドレス：

ヤマハルーターのネットボランチ DNS ホスト名、もしくは、WAN 側または PP 側の IP アドレスを入力します。

### ② 接続先の名前：

任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。

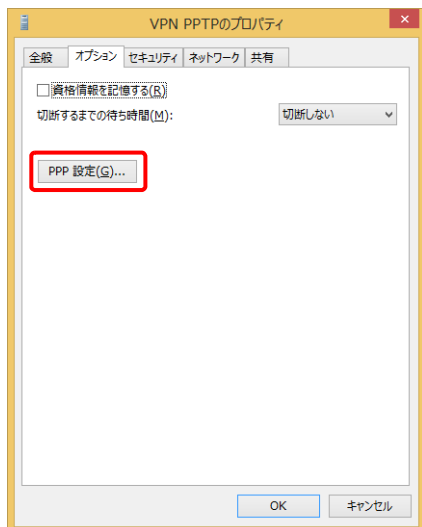
### 7. 「作成」 ボタンをクリックする。

設定内容が保存されます。

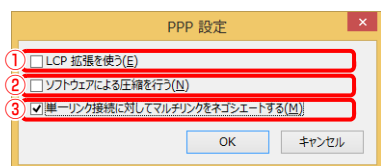
### 8. 「ネットワークと共有センター」 画面で「アダプターの設定の変更」をクリックする。

### 9. 作成した VPN の接続設定を右クリックし、「プロパティ」を選択する。

### 10. 「オプション」 タブを選択し、「PPP 設定」 ボタンをクリックする。



### 11. PPP 設定を変更する。



### ① LCP 拡張を使う：

チェックボックスのチェックを外します。

### ② ソフトウェアによる圧縮を行う：

チェックボックスのチェックを外します。

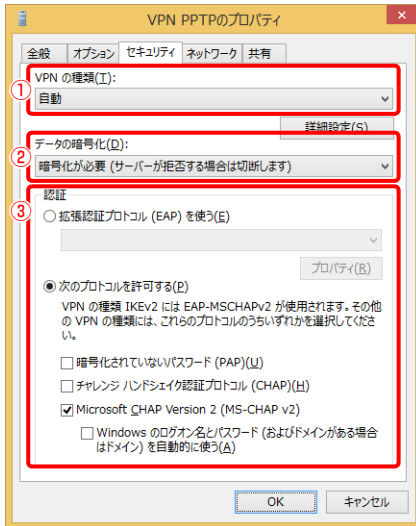
### ③ 単一リンク接続に対してマルチリンクをネゴシエートする：

チェックボックスにチェックを付けます。

### 12. 「OK」 ボタンをクリックし、「セキュリティ」 タブを選択する。



## 13. セキュリティー設定を変更する。



## ① VPNの種類：

「自動」を選択します。

## ② データの暗号化：

「暗号化が必要 (サーバーが拒否する場合は切断します)」を選択します。

## ③ 認証：

「次のプロトコルを許可する」を選択し、以下のように設定します。

- ・ 暗号化されていないパスワード (PAP)：チェックボックスのチェックを外す。
- ・ チャレンジハンドシェイク認証プロトコル (CHAP)：チェックボックスのチェックを外す。
- ・ Microsoft CHAP Version 2 (MS-CHAPv2)：チェックボックスにチェックを入れる。
- ・ Windows のログオン名とパスワード (およびドメインがある場合はドメイン) を自動的に使う：チェックボックスのチェックを外す。

## ご注意

Windows Vista 以降の Windows OS では、Microsoft CHAP Version 1 (MS-CHAP) はサポートされていません。「8.3.1 ヤマハルーターの設定 (PPTP) をする」(96 ページ) の手順 4 で「MSCHAP-V2」を選択してください。

## 14. 「OK」ボタンをクリックする

## ヤマハルーターへリモートアクセスする

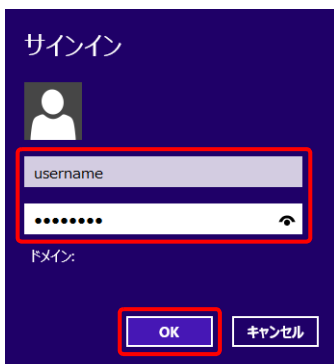
1. マウスカーソルを右上隅または右下隅に移動する。
2. チャームから「設定」 - 「ネットワーク」の順に選択する。

## 第 8 章 外部から VPN 経由で LAN へアクセスする

3. 作成した VPN の接続設定を選択し、「接続」ボタンをクリックする。



4. 「8.3.1 ヤマハルーターの設定 (PPTP) をする」(96 ページ) で設定したユーザー名とパスワードを入力し、「OK」ボタンをクリックする。  
ヤマハルーターへの VPN 接続を開始します。



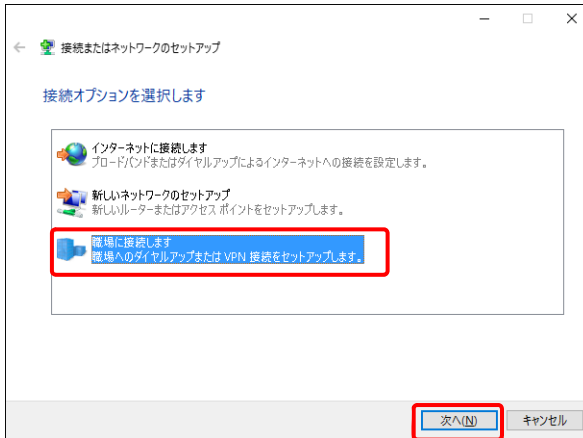
リモートアクセスを切断する場合は  
「切断」ボタンをクリックします。

### 8.3.5 Windows 10 でリモートアクセスする

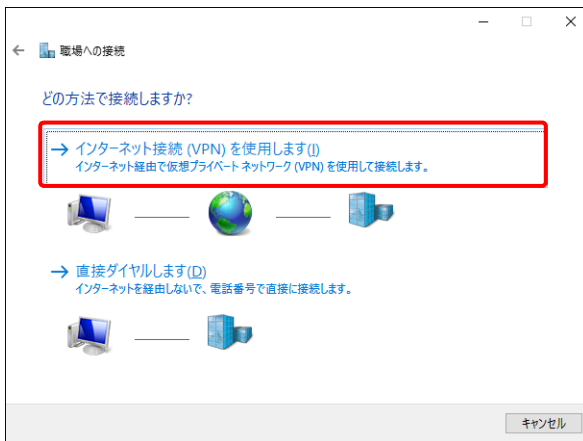
#### VPN の接続設定をする

1. 「スタート」ボタンを右クリックする。
2. 「コントロールパネル」 - 「ネットワークの状態とタスクの表示」の順に選択する。  
「ネットワークと共有センター」画面が表示されます。
3. 「新しい接続またはネットワークのセットアップ」をクリックする。

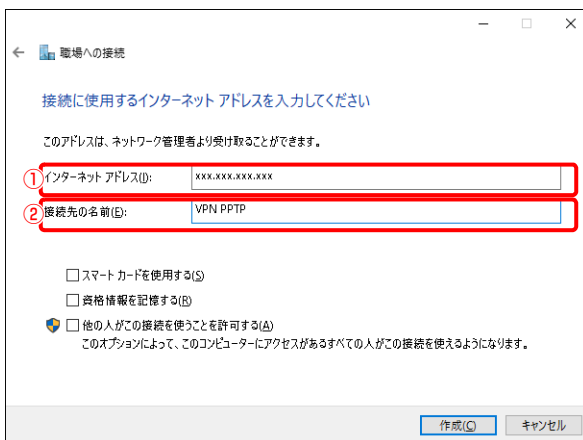
## 4. 「職場に接続します」を選択し、「次へ」ボタンをクリックする。



## 5. 「インターネット接続 (VPN) を使用します」をクリックする。



## 6. VPN の接続情報を設定する。



## 第 8 章 外部から VPN 経由で LAN へアクセスする

### ① インターネットアドレス：

ヤマハルーターのネットボランチ DNS ホスト名、もしくは、WAN 側または PP 側の IP アドレスを入力します。

### ② 接続先の名前：

任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。

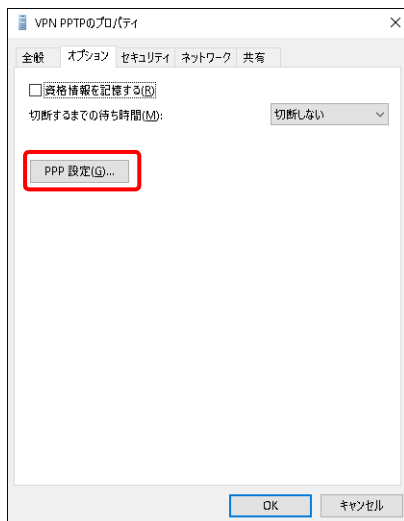
### 7. 「作成」 ボタンをクリックする。

設定内容が保存されます。

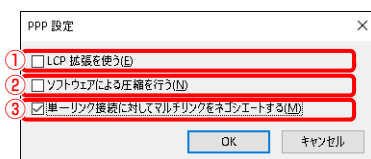
### 8. 「ネットワークと共有センター」 画面で「アダプターの設定の変更」をクリックする。

### 9. 作成した VPN の接続設定を右クリックし、「プロパティ」を選択する。

### 10. 「オプション」 タブを選択し、「PPP 設定」 ボタンをクリックする。



### 11. PPP 設定を変更する。



### ① LCP 拡張を使う：

チェックボックスのチェックを外します。

### ② ソフトウェアによる圧縮を行う：

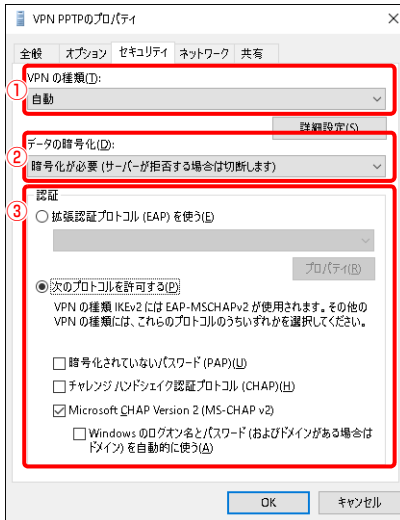
チェックボックスのチェックを外します。

### ③ 単一リンク接続に対してマルチリンクをネゴシエートする：

チェックボックスにチェックを付けます。

### 12. 「OK」 ボタンをクリックし、「セキュリティ」 タブを選択する。

## 13. セキュリティー設定を変更する。



## ① VPN の種類：

「自動」を選択します。

## ② データの暗号化：

「暗号化が必要（サーバーが拒否する場合は切断します）」を選択します。

## ③ 認証：

「次のプロトコルを許可する」を選択し、以下のように設定します。

- ・ 暗号化されていないパスワード（PAP）：チェックボックスのチェックを外す。
- ・ チャレンジハンドシェイク認証プロトコル（CHAP）：チェックボックスのチェックを外す。
- ・ Microsoft CHAP Version 2（MS-CHAPv2）：チェックボックスにチェックを入れる。
- ・ Windows のログオン名とパスワード（およびドメインがある場合はドメイン）を自動的に使う：チェックボックスのチェックを外す。

## ご注意

Windows Vista 以降の Windows OS では、Microsoft CHAP Version 1（MS-CHAP）はサポートされていません。「8.3.1 ヤマハルーターの設定（PPTP）をする」（96 ページ）の手順 4 で「MSCHAP-V2」を選択してください。

## 14. 「OK」ボタンをクリックする

## ヤマハルーターへリモートアクセスする

1. 「スタート」メニューから「設定」－「ネットワークとインターネット」－「VPN」の順に選択する。

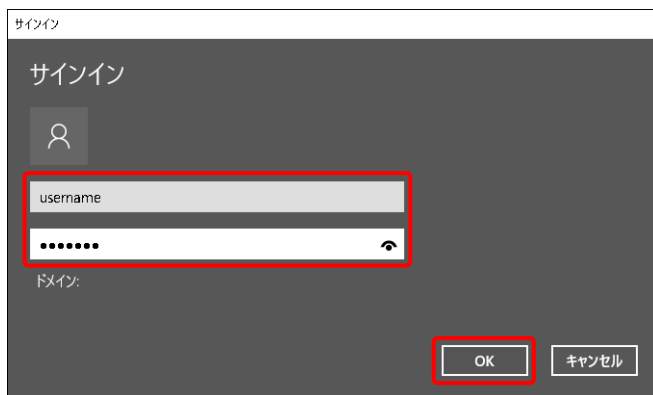
## 第 8 章 外部から VPN 経由で LAN へアクセスする

- 作成した VPN の接続設定を選択し、「接続」ボタンをクリックする。



- 「8.3.1 ヤマハルーターの設定 (PPTP) をする」で設定したユーザー名とパスワードを入力し、「OK」ボタンをクリックする。

ヤマハルーターへの VPN 接続を開始します。



リモートアクセスを切断する場合は「切断」ボタンをクリックします。

# 第9章 IP電話を利用する

本章では、VoIP 通話機能を使って IP 電話を利用する方法について説明します。お使いの環境に合わせて、さまざまな通話先に VoIP 通話することができます。

- ・ 基本設定をする …115 ページ
- ・ ひかり電話を設定する …117 ページ
- ・ SIP サーバーを設定する …121 ページ
- ・ SIP 電話帳を設定する …129 ページ
- ・ ネットボランチ電話を設定する …133 ページ

本製品は以下の VoIP 通話に対応しています。

## ひかり電話

NTT 東日本または NTT 西日本の提供するフレッツ光ネクストを利用してインターネットに接続している場合は、本製品をひかり電話の VoIP アダプターとして使用できます。ひかり電話サービスを利用するためには、ひかり電話サービスの提供会社（NTT 東日本または NTT 西日本）との契約および利用料金が必要です。

## SIP サーバー接続

楽天コミュニケーションズ系 SIP サーバーまたはその他の SIP サーバーを使用して構築された VoIP システムで通話します。楽天コミュニケーションズ系 SIP サーバーを使用すると、IP 加入電話番号で通話できるようになります。

## SIP 電話帳

SIP サーバーを利用せず、本製品の電話帳に登録した相手と VoIP 通話できるようになります。各種の VPN と併用すると、遠隔地の支社や営業所ともセキュリティーを保持した状態で内線 VoIP 通話できます。

## ネットボランチ電話

ネットボランチ DNS サービスを利用することでネットボランチ DNS サーバーから割り当てられた 8 ケタのネットボランチ電話番号を使用して、インターネットに接続したネットボランチシリーズのルーター間で、VoIP 通話ができます。

ネットボランチ電話を利用する場合は、プロバイダーへの通信料以外の通話料金はかかりません。

## メモ

本製品の電話機能で使用するプレフィックスとは、電話番号の前に付ける識別番号のことです。プレフィックスに任意の番号を設定しておき、電話をかけるときにダイヤルすると、利用したい VoIP 通話のサービスを選択して発信することができます。

## 9.1 基本設定をする

IP 電話を利用するための基本的な設定を行います。

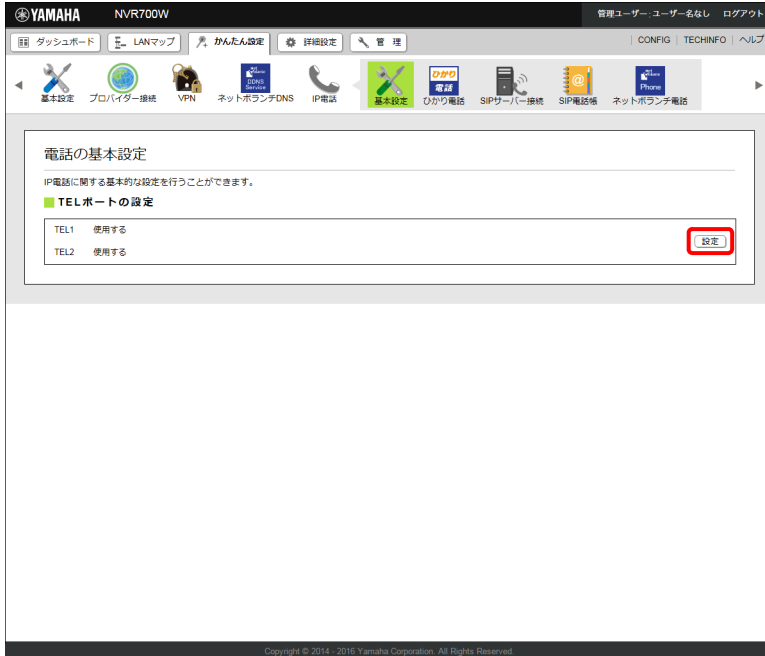
### ご注意

電話機や FAX などを接続していない TEL ポートが「使用する」または「使用する（着信のみ）」に設定されていると、かかってきた電話がその TEL ポートに着信してしまい、回線が話中にならない場合があります。何も接続していない TEL ポートは、「使用しない」に設定してください。

1. 「かんたん設定」タブー「IP 電話」－「基本設定」ボタンを順に選択する。  
「電話の基本設定」画面が表示されます。

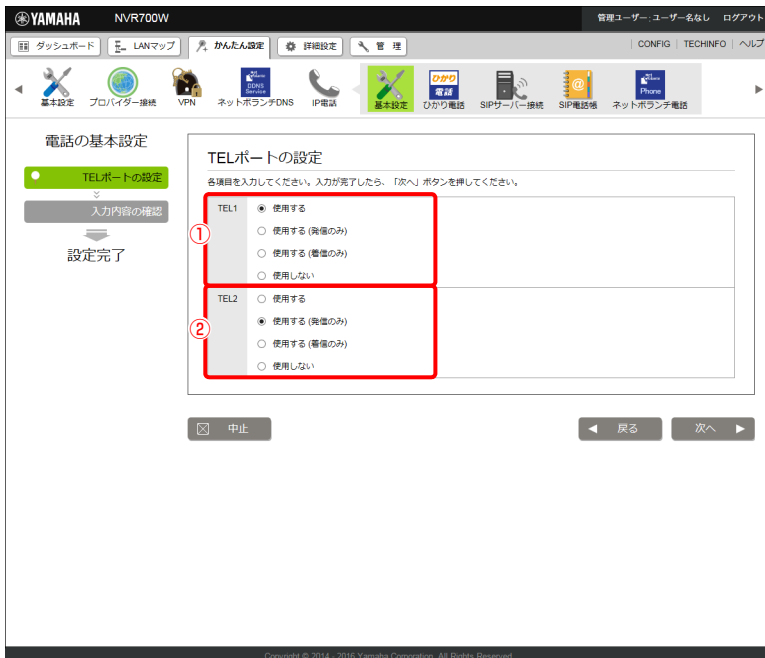
## 第9章 IP電話を利用する

### 2. 「TELポートの設定」項目の「設定」ボタンをクリックする。



「TELポートの設定」画面が表示されます。

### 3. TELポートを設定します。



① TEL1 :  
TEL1ポートの使用・不選択をします。

② TEL2 :  
TEL2ポートの使用・不選択をします。



## メモ

「使用する（発信のみ）」または「使用する（着信のみ）」を選択すると、TEL ポートの使用を、発信または着信のみに制限できます。

4. 「次へ」 ボタンをクリックする。  
「入力内容の確認」画面が表示されます。
5. 内容を確認し、「設定の確定」 ボタンをクリックする。



設定が反映され、「電話の基本設定」画面が表示されます。

## 9.2 ひかり電話を設定する

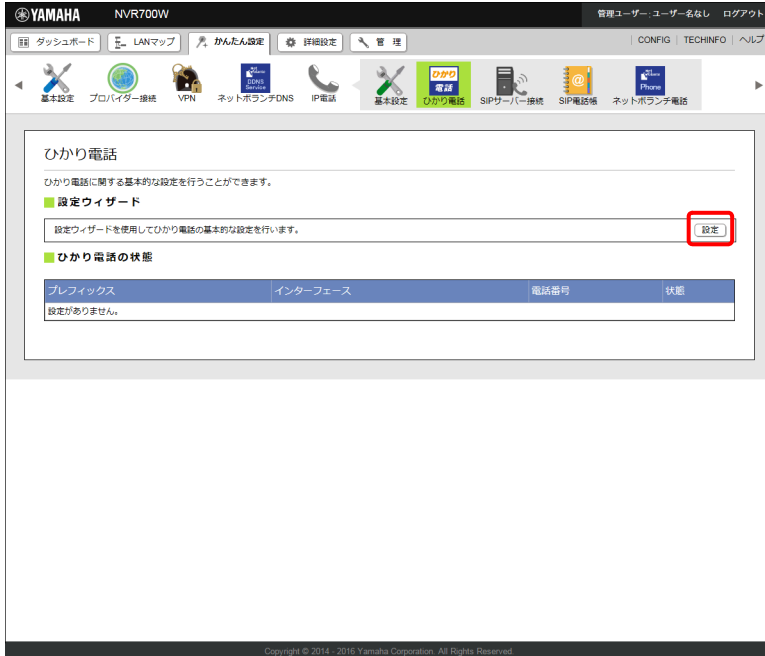
ひかり電話で通話するために必要な設定を説明します。

NTT 東日本または NTT 西日本の提供するフレッツ光ネクストを利用して接続している場合は、本製品をひかり電話（有料）の VoIP アダプターとして使用できます。

1. 「かんたん設定」タブ - 「IP 電話」 - 「ひかり電話」 ボタンを順に選択する。  
「ひかり電話」画面が表示されます。

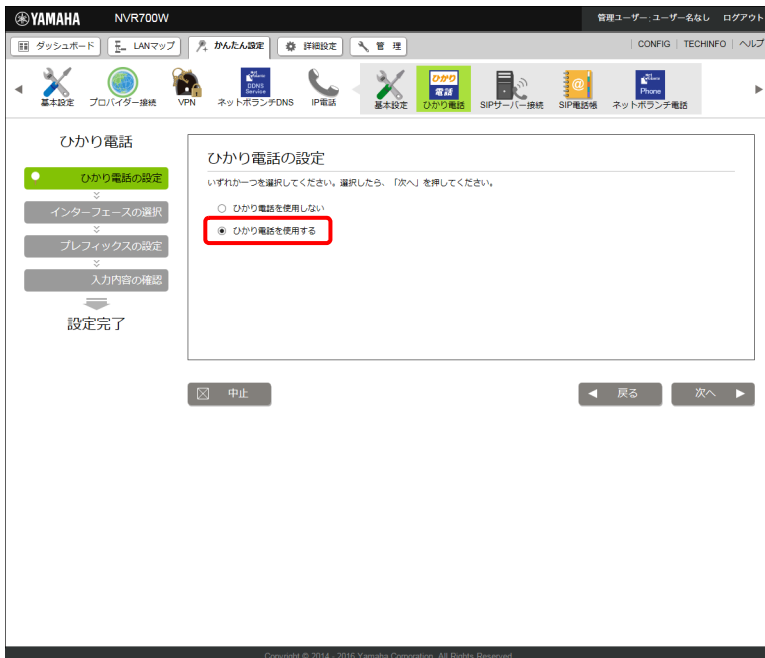
## 第9章 IP電話を利用する

### 2. 「設定ウィザード」項目の「設定」ボタンをクリックする。



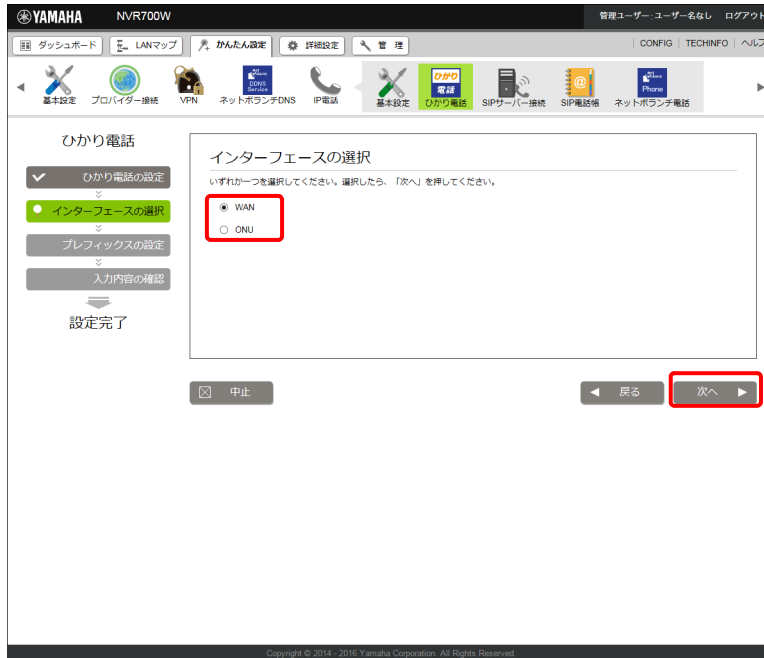
「ひかり電話の設定」画面が表示されます。

### 3. 「ひかり電話を使用する」を選択し、「次へ」ボタンをクリックする。



「インターフェースの選択」画面が表示されます。

## 4. 使用するインターフェースを選択し、「次へ」ボタンをクリックする。



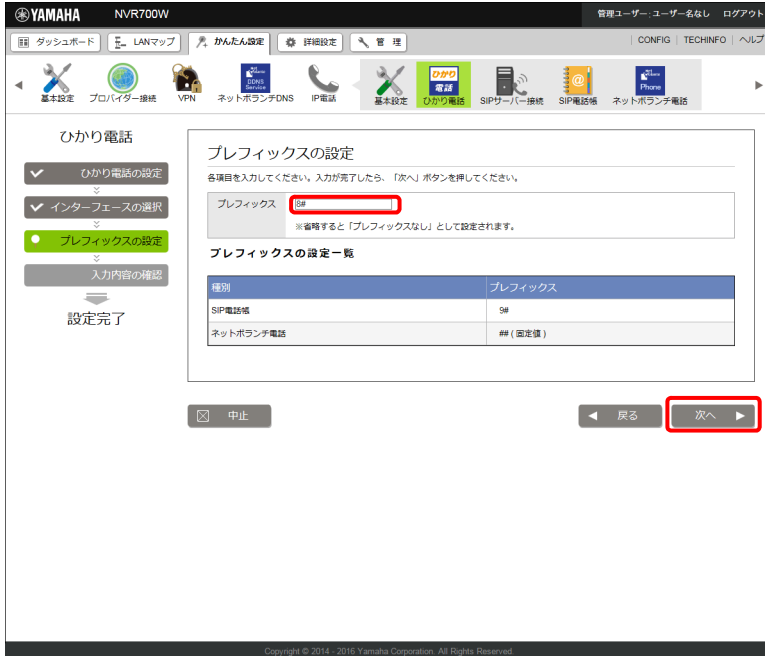
「プレフィックスの設定」画面が表示されます。

## メモ

- ・「WAN」を選択する場合は、ヤマハルーターの WAN ポートと接続した据え置き型の ONU 機器を使ってひかり電話設定を行います。
- ・「ONU」を選択する場合は、ヤマハルーターの ONU ポートに接続した小型 ONU を使ってひかり電話設定を行います。

## 第9章 IP電話を利用する

### 5. プレフィックスを入力し、「次へ」ボタンをクリックする。




「入力内容の確認」画面が表示されます。

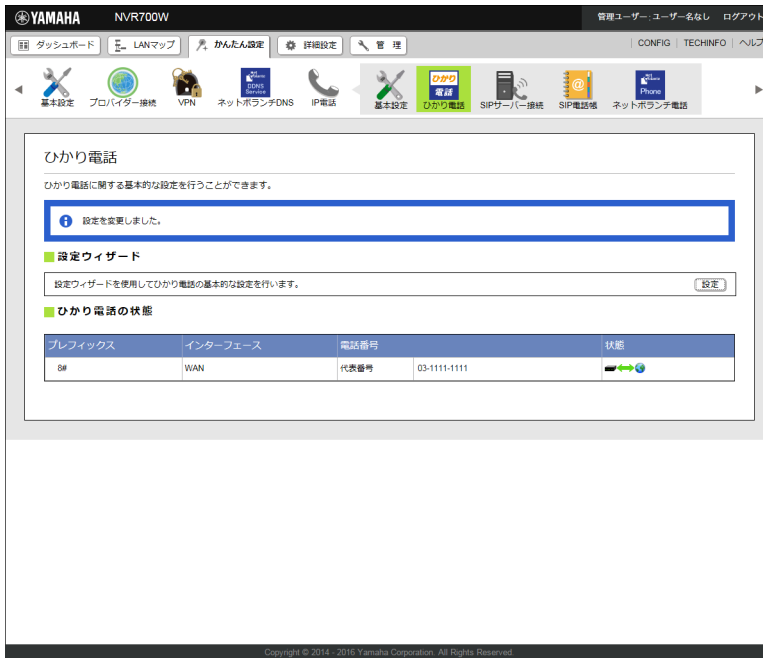
### メモ

プレフィックスを設定しない場合は、何も入力せずに「次へ」をクリックします。


### 6. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「ひかり電話」画面が表示されます。自動でインターネットに接続され、ひかり電話が使用できる状態になると、「状態」が  に切り替わります。



## メモ

ひかり電話接続が切断している場合は、「状態」に  が表示されます。アイコン下部の切断コードをクリックすると、「ヘルプページ」が表示され、切断コードごとの原因が確認できます。

## 9.3 SIP サーバーを設定する

SIP サーバーを使って IP 電話で通話するために必要な設定を説明します。

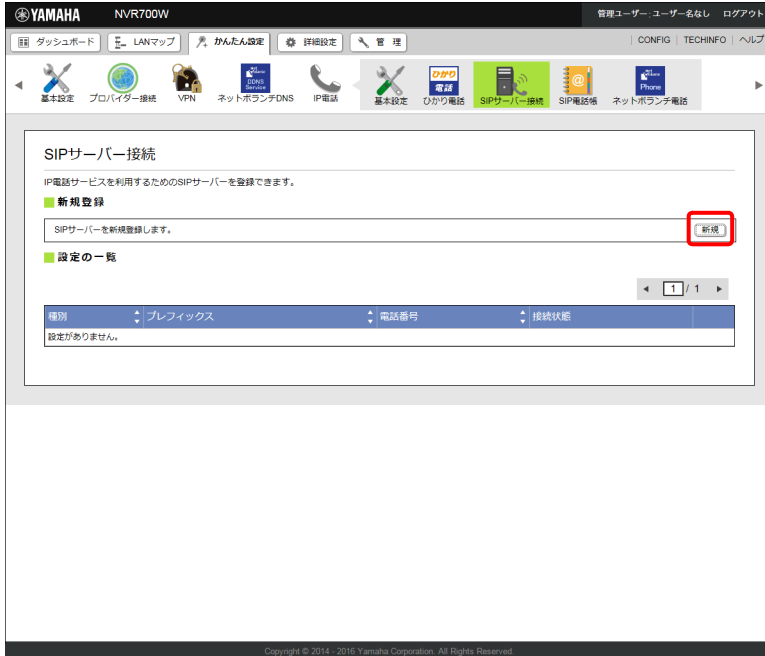
### 9.3.1 楽天コミュニケーションズ系 SIP サーバーを設定する

楽天コミュニケーションズ系 SIP サーバーを利用して、VoIP システムを構成できます。楽天コミュニケーションズ系 SIP サーバーで通話するために必要な設定を説明します。

1. 「かんたん設定」タブ「IP 電話」－「SIP サーバー接続」ボタンを順に選択する。  
「SIP サーバー接続」画面が表示されます。

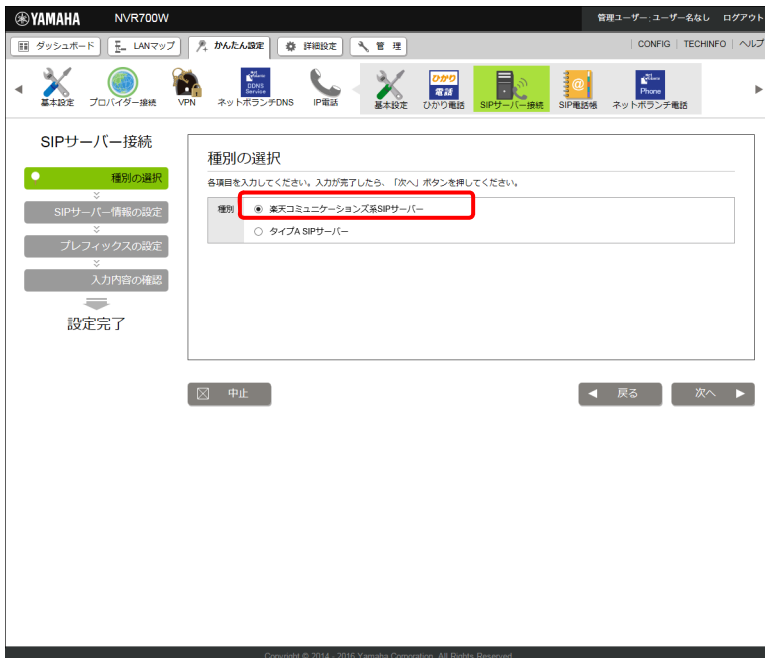
## 第9章 IP電話を利用する

### 2. 「新規登録」項目の「新規」ボタンをクリックする。



「種別の選択」画面が表示されます。

### 3. 「楽天コミュニケーションズ系 SIP サーバー」を選択し、「次へ」ボタンをクリックする。



「SIPサーバー情報の設定」画面が表示されます。

## 4. SIP サーバーの接続情報を設定する。



- ① **SIP ドメイン名 :**  
SIP サーバーのドメイン名を入力します。
- ② **SIP サーバーのアドレス :**  
SIP サーバーのアドレスを入力します。
- ③ **IP 加入電話番号 :**  
IP 電話番号を入力します。
- ④ **アカウント ID :**  
SIP サーバー接続を行う際のユーザー認証で使用するアカウント ID を入力します。
- ⑤ **IP 加入電話パスワード :**  
SIP サーバー接続を行う際のユーザー認証で使用するパスワードを入力します。

5. 「次へ」 ボタンをクリックする。  
「プレフィックスの設定」 画面が表示されます。

## 第9章 IP電話を利用する

### 6. プレフィックスを入力し、「次へ」ボタンをクリックする。

The screenshot shows the 'SIPサーバー接続' (SIP Server Connection) configuration page. The 'プレフィックスの設定' (Prefix Settings) section is active. The 'プレフィックス' (Prefix) field is highlighted with a red box. Below it, a table shows the prefix settings for different SIP services.

種別	プレフィックス
SIP電話帳	99
ネットボランチ電話	## (固定値)

「入力内容の確認」画面が表示されます。

### メモ

プレフィックスを設定しない場合は、何も入力せずに「次へ」をクリックします。

### 7. 内容を確認し、「設定の確定」ボタンをクリックする。

The screenshot shows the '入力内容の確認' (Confirmation of Input) page. The '設定の確定' (Confirm Settings) button is highlighted with a red box. The page displays the configuration details for the SIP server connection.

**種別の選択**

種別	※天コミュニケーション系SIPサーバー
----	---------------------

**SIPサーバー情報の設定**

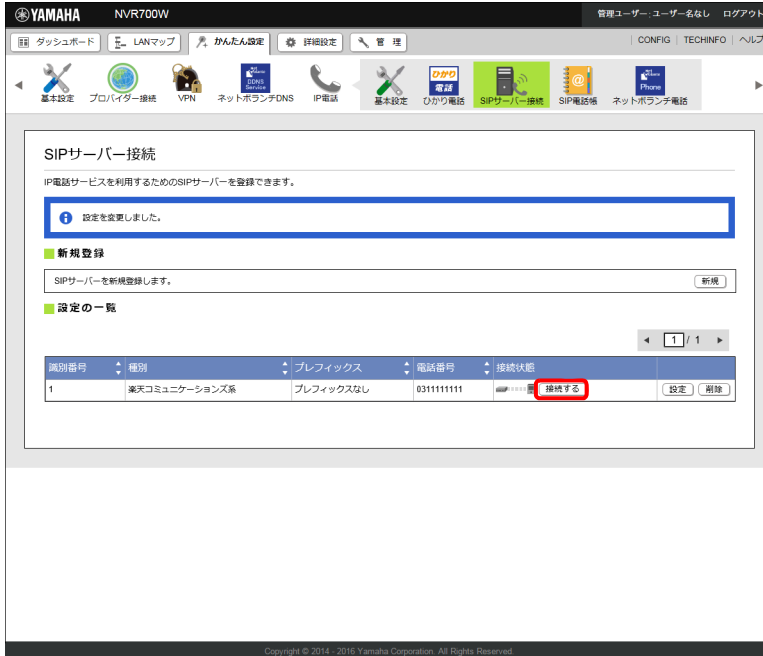
SIPドメイン名	xxxxxx
SIPサーバーのアドレス	xxxxxx
IP加入電話番号	0311111111
アカウントID	usend
IP加入電話/パスワード	password


**プレフィックスの設定**

プレフィックス	プレフィックスなし
---------	-----------



8. 「設定の一覧」項目の中から設定した SIP サーバー接続の「接続する」ボタンをクリックする。



SIP サーバー接続が完了すると、「接続状態」の表示が  に切り替わります。

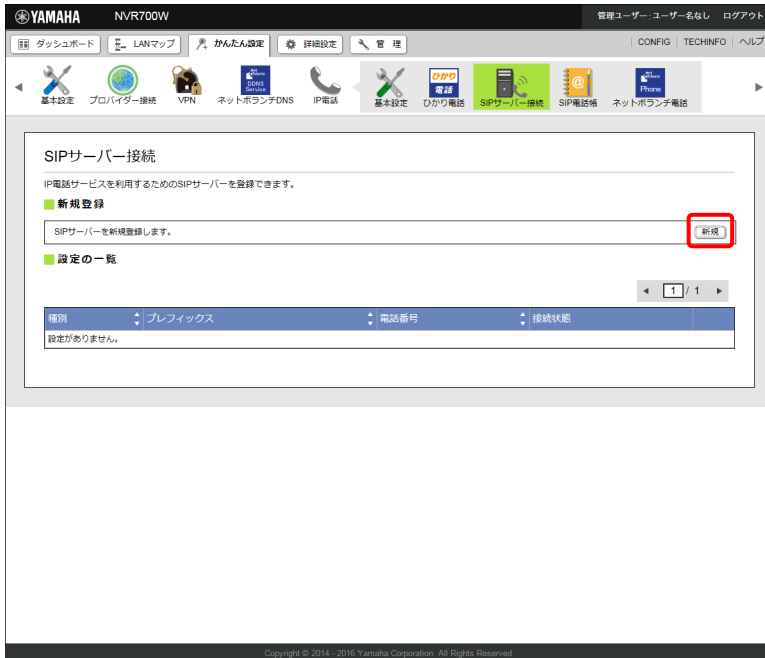
### 9.3.2 その他の SIP サーバーを設定する

その他の SIP サーバーを利用して、内線 VoIP システムを構成できます。その他の SIP サーバーにして通話するために必要な設定を説明します。

1. 「かんたん設定」タブで「IP 電話」 - 「SIP サーバー接続」ボタンを順に選択する。  
「SIP サーバー接続」画面が表示されます。

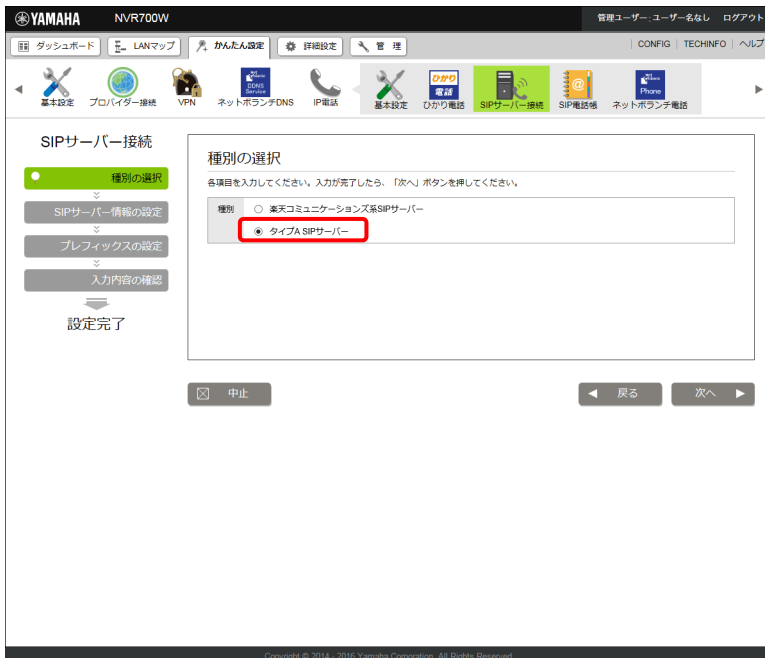
## 第9章 IP電話を利用する

### 2. 「新規登録」項目の「新規」ボタンをクリックする。



「種別の選択」画面が表示されます。

### 3. 「タイプ A SIP サーバー」を選択し、「次へ」ボタンをクリックする。



「SIP サーバー情報の設定」画面が表示されます。

## 4. SIP サーバーの接続情報を設定する。



## ① VoIP サーバー :

VoIP サーバーのアドレスを入力します。

## ② サービスドメイン :

サービスドメインを入力します。

## ③ VoIP ユーザー ID :

VoIP ユーザー名を入力します。

## ④ VoIP ユーザーパスワード :

VoIP サーバー接続を行う際のユーザー認証で使用するパスワードを入力します。

## ⑤ VoIP 電話番号 :

VoIP 電話番号を入力します。

## 5. 「次へ」 ボタンをクリックする。

「プレフィックスの設定」画面が表示されます。

## 第9章 IP電話を利用する

### 6. プレフィックスを入力し、「次へ」ボタンをクリックする。

YAMAHA NVR700W 管理ユーザー: ユーザー名なし ログアウト

ダッシュボード LANマップ かんたん設定 詳細設定 管理

基本設定 プロバイダー接続 VPN ネットボランチャDNS IP電話 基本設定 ひかり電話 SIPサーバー接続 SIP電話機 ネットボランチャ電話

SIPサーバー接続

- 種別の選択
- SIPサーバー情報の設定
- プレフィックスの設定**
- 入力内容の確認

設定完了

プレフィックスの設定

各項目を入力してください。入力が完了したら、「次へ」ボタンを押してください。

プレフィックス

※省略すると「プレフィックスなし」として設定されます。

プレフィックスの設定一覧

種別	プレフィックス
SIP電話機	99
ネットボランチャ電話	## (固定値)

中止 戻る 次へ

Copyright © 2014 - 2016 Yamaha Corporation. All Rights Reserved

「入力内容の確認」画面が表示されます。

### メモ

プレフィックスを設定しない場合は、何も入力せずに「次へ」をクリックします。

### 7. 内容を確認し、「設定の確定」ボタンをクリックする。

YAMAHA NVR700W 管理ユーザー: ユーザー名なし ログアウト

ダッシュボード LANマップ かんたん設定 詳細設定 管理

基本設定 プロバイダー接続 VPN ネットボランチャDNS IP電話 基本設定 ひかり電話 SIPサーバー接続 SIP電話機 ネットボランチャ電話

SIPサーバー接続

- 種別の選択
- SIPサーバー情報の設定
- プレフィックスの設定
- 入力内容の確認**

設定完了

入力内容の確認

入力内容をご確認の上、変更がなければ「設定の確定」を押してください。

種別の選択

種別 タイプA SIPサーバー

SIPサーバー情報の設定

VoIPサーバー xxxxxx

サービスドメイン xxxxxx

VoIPユーザーID userid

VoIPユーザーパスワード password

VoIP電話番号 05000000000

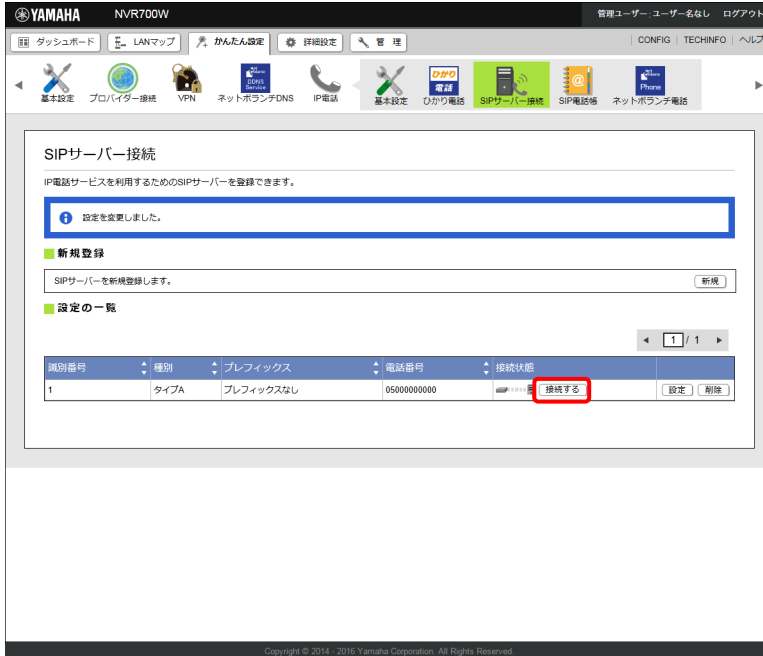
プレフィックスの設定

プレフィックス プレフィックスなし

中止 戻る 設定の確定

Copyright © 2014 - 2016 Yamaha Corporation. All Rights Reserved

8. 「設定の一覧」項目の中から設定した SIP サーバー接続の「接続する」ボタンをクリックする。




SIP サーバー接続が完了すると、「接続状態」の表示が 📞🔄📞 に切り替わります。

## 9.4 SIP 電話帳を設定する

SIP サーバーを利用せず、VoIP システムを構成できます。本製品に SIP 電話番号を登録して通話するために必要な設定を説明します。

VPN 接続と併用することで、ヤマハのネットボランチルーター同士であれば、セキュアな内線通話として利用できます。音声は暗号化されるため、通話が盗聴される心配はありません。

### メモ

設定ウィザードで設定する各項目は、「SIP 電話帳」画面で、それぞれの項目の「**設定**」ボタン、または「」ボタンで、個別に設定することもできます。

1. 「かんたん設定」タブー「IP 電話」－「SIP 電話帳」ボタンを順に選択する。  
「SIP 電話帳」画面が表示されます。

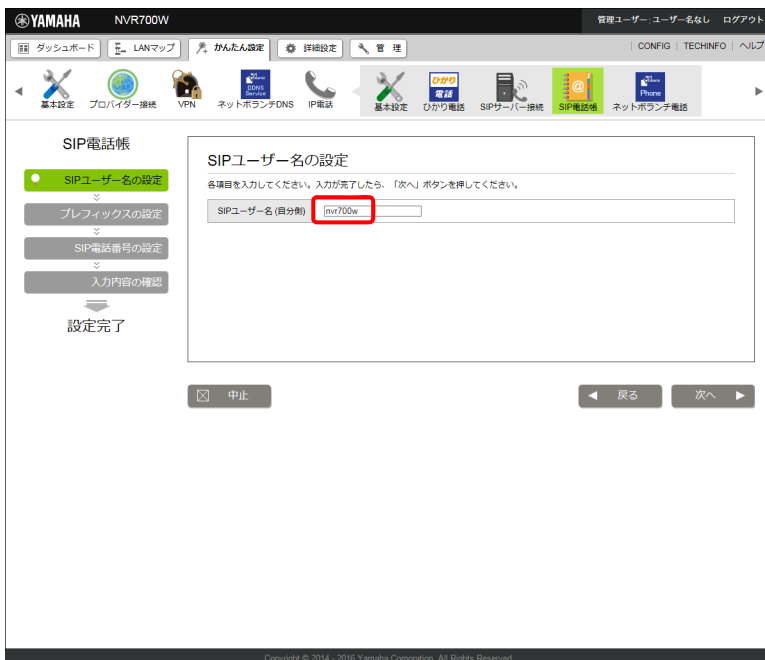
## 第9章 IP電話を利用する

### 2. 「設定ウィザード」項目の「設定」ボタンをクリックする。



「SIPユーザー名の設定」画面が表示されます。

### 3. 「SIPユーザー名 (自分側)」を入力し、「次へ」ボタンをクリックする。



「プレフィックスの設定」画面が表示されます。

## メモ

工場出荷状態では、「SIP ユーザー名 (自分側)」は使用しているヤマハルーターの名称が表示されます。「SIP ユーザー名 (自分側)」を変更した後に、「SIP 電話帳」画面で「初期設定に戻す」ボタンをクリックすると、再度ヤマハルーターの名称に戻ります。

4. プレフィックスを入力し、「次へ」ボタンをクリックする。



「SIP 電話番号の設定」画面が表示されます。

## メモ

プレフィックスを設定しない場合は、何も入力せずに「次へ」をクリックします。

## 第9章 IP電話を利用する

### 5. SIP電話番号を設定する。



① **宛先：**

通話対象の名称を入力します。

② **電話番号：**

通話対象の電話番号を入力します。

③ **SIP アドレス：**

相手側の SIP ユーザー名とホストアドレスを「@」で区切って入力します。

SIP 電話番号を複数登録する場合は、「+」ボタンをクリックしてください。

### 6. 「次へ」ボタンをクリックする。

「入力内容の確認」画面が表示されます。



## 7. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「SIP電話帳」画面が表示されます。



## 9.5 ネットボランチ電話を設定する

インターネット経由で本製品に接続した電話機間で会話（VoIP 通話）ができます。電話会社を通さずに通話するため、通常の電話料金はかかりません。

### ご注意

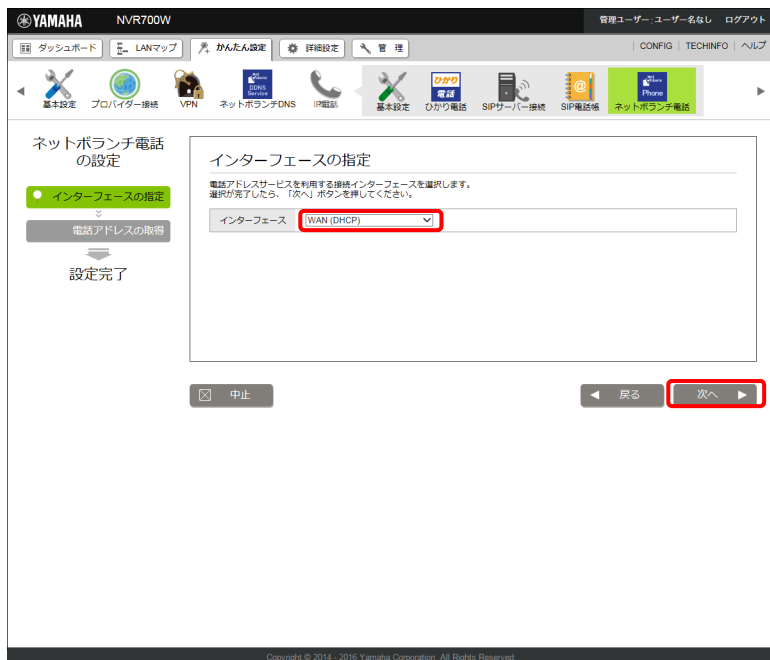
ネットボランチ電話を設定するには、事前に有効なインターフェース（WAN または ONU）を設定する必要があります。詳しくは、「ブロードバンド回線でインターネットへ接続する」（26 ページ）をご覧ください。

1. 「かんたん設定」タブー「IP 電話」－「ネットボランチ電話」ボタンを順に選択する。  
「ネットボランチ電話」画面が表示されます。
2. 「電話アドレスサービス」項目の「設定」ボタンをクリックする。



「インターフェースの指定」画面が表示されます。

## 3. インターフェースを選択し、「次へ」ボタンをクリックする。

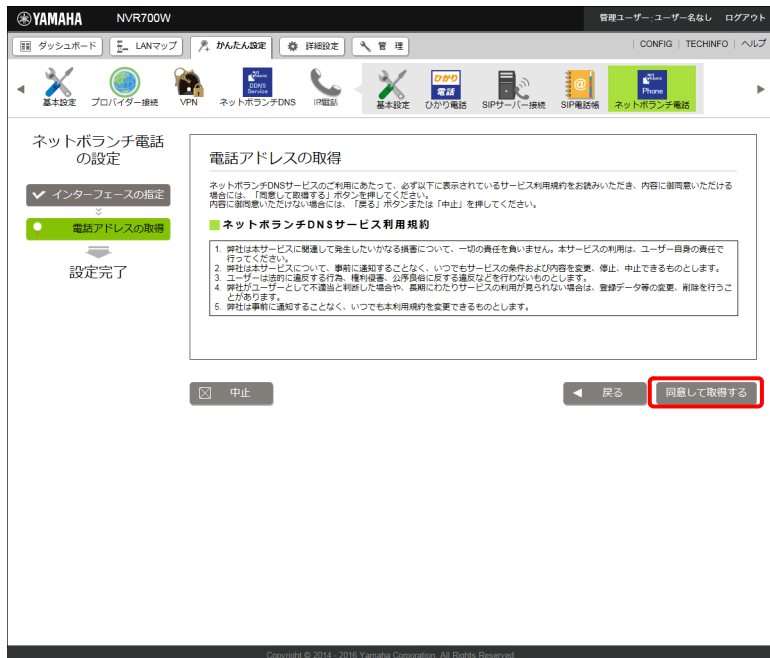


「電話アドレスの取得」画面が表示されます。

## メモ

有効なインターフェース（WANまたはONU）のみ選択できます。

## 4. ネットボランチ DNS サービス利用規約を確認し、「同意して取得する」ボタンをクリックする。



## 第9章 IP電話を利用する

設定が反映され、「ネットボランチ電話」画面が表示されます。



### メモ

工場出荷状態では、ネットボランチ電話のプレフィックスは「##」が固定値になります。プレフィックスを追加する場合は、「プレフィックス」の「**設定**」ボタンをクリックし、「プレフィックスの設定」画面で設定してください。

# 第 10 章 ダッシュボードを利用する

本章では、ダッシュボードの利用方法について説明します。

ダッシュボードとは？ …137 ページ

ダッシュボードの基本操作 …138 ページ

各ガジェットの説明 …145 ページ

## 10.1 ダッシュボードとは？

ダッシュボード機能とは、様々なガジェットを利用してシステムの状態や運用管理、トラブルシューティングに有用な情報を、Web ブラウザー上でよりグラフィカルに表示する機能のことです。

ガジェットは環境に応じて取捨選択して画面上に自由に配置することができます。

各ガジェットのパラメーターがある閾値を超えたら警告文が表示されるため、システムの監視も行うことが可能となります。

工場出荷状態ではダッシュボードに下記の 4 つのガジェットが表示されています。

- ・ システム情報
- ・ リソース情報
- ・ インターフェース情報
- ・ トラフィック情報 (LAN)

### ご注意

ログインユーザーごとに表示するガジェットを切り換えることはできません。


### メモ

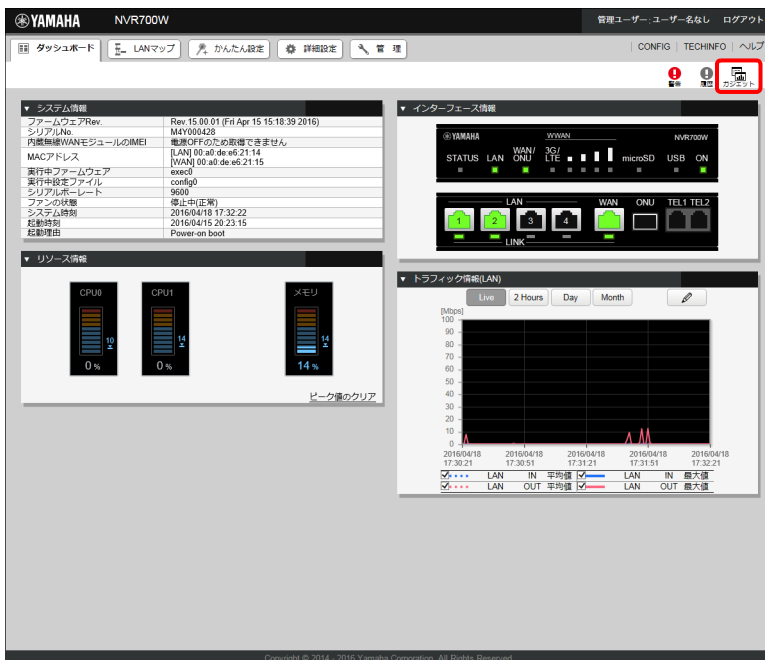
- ・ 各種システム情報やステータス情報を可視化、監視するページのことを「ダッシュボード」と呼びます。
- ・ ダッシュボードに表示される一つ一つのウィンドウのことを「ガジェット」と呼びます。各ガジェットの情報は定期的に自動更新されます。

## 10.2 ダッシュボードの基本操作

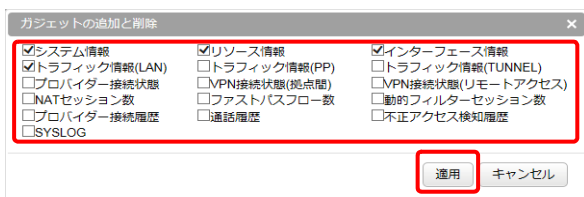
### 10.2.1 ガジェットを追加と削除

#### ガジェットを追加する

1. 「」 ボタンをクリックする。




2. ガジェットの一覧から追加するガジェットのチェックボックスにチェックを入れ、「適用」 ボタンをクリックする。



ガジェットは常にダッシュボードページ一番左上に追加されます。

#### ガジェットを削除する


ガジェットを削除する場合は、ガジェットの一覧から削除したいガジェットのチェックボックスのチェックを外し、「適用」 ボタンをクリックしてください。または、削除したいガジェットのタイトルバーにマウスカースルを重ね「」 ボタンをクリックしても削除することができます。



## メモ

ガジェットを削除すると、該当ガジェットに対する警告表示もクリアされます。

### 10.2.2 ガジェットの移動

1. 移動させたいガジェットのタイトルバーにマウスカーソルを重ねる。  
マウスカーソルが移動マーク「」に切り替わります。
2. ガジェットをドラッグアンドドロップし、任意の位置に移動する。





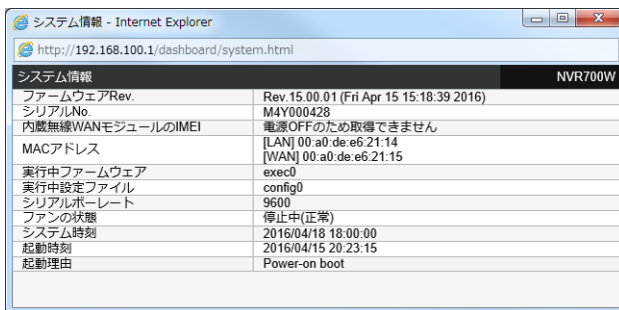
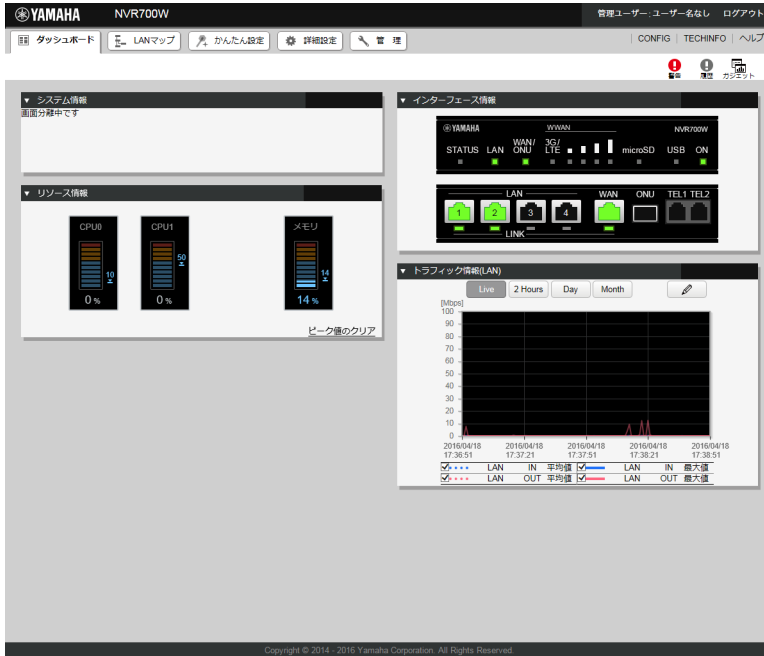
## メモ

ガジェットの移動先候補は灰色で表示されます。



## 第 10 章 ダッシュボードを利用する

### 10.2.3 ガジェット画面分離

1. 分離させたいガジェットのタイトルバーにマウスカーソルを重ねる。  
ガジェットのタイトルバーに「」が表示されます。
2. 「」ボタンをクリックする。  
ガジェットが別ウィンドウに分離されます。また、ダッシュボードでは「画面分離中です」と表示されます。





#### ガジェット分離中の動作

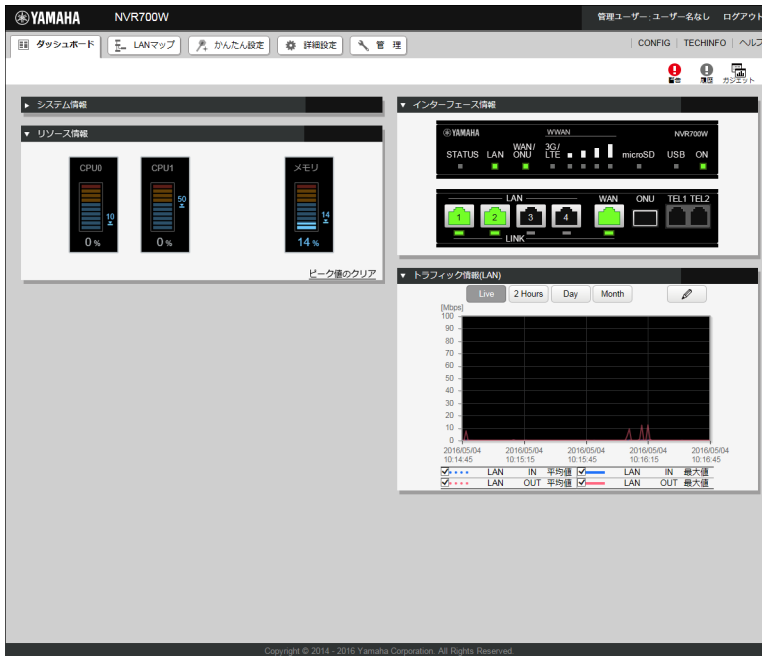
- ・ 分離元のガジェットには「」と「」は表示されません。
- ・ 分離中のガジェットを閉じると、ダッシュボードページの元の場所に戻ります。
- ・ ダッシュボードページの表示を更新すると、分離しているガジェットはすべてダッシュボードページに戻ります。
- ・ ダッシュボードページを閉じると、分離しているすべてのガジェットも閉じられます。
- ・ 分離したガジェットは、URL を直接 Web ブラウザーに指定して表示することができます。  
例：システム情報ガジェットは「[http://\(LAN アドレス\)/dashboard/system.html](http://(LAN アドレス)/dashboard/system.html)」



## 10.2.4 ガジェットの最小化

### 1. 最小化させたいガジェットの「」ボタンをクリックする。

ガジェットが最小化表示になります。また、アイコン表示が「」に切り替わります。「」ボタンをクリックすると、ガジェットは元の大きさに戻ります。



## 10.2.5 ガジェットの位置情報の保存

ガジェットの位置情報は下記の操作を行ったときにRTFSにファイルとして自動的に保存されます。RTFSとは、ヤマハルーターの不揮発性メモリに構築されるファイルシステムのことで、

- ・ ガジェットを追加、削除したとき
- ・ ガジェットを移動したとき
- ・ ガジェットを最小化 / 元に戻したとき

### ご注意

- ・ RTFSの空き容量が足りない場合、これらの情報は保存されません。
- ・ 工場出荷状態に戻したりRTFSをフォーマットすると、これらの情報も初期化されます。

### メモ

- ・ トラフィック情報のガジェットについては、表示するインターフェース情報、方向(IN/OUT)、グラフの種別(平均値 / 最大値)の設定を変更したときも保存されます。
- ・ 電源を再投入した後でもこれらの情報は保存されています。

## 10.2.6 ガジェットの自動更新

すべてのガジェットは定期的に自動更新されます。更新間隔はガジェットによって異なります。

### 10.2.7 警告内容の確認

#### ご注意

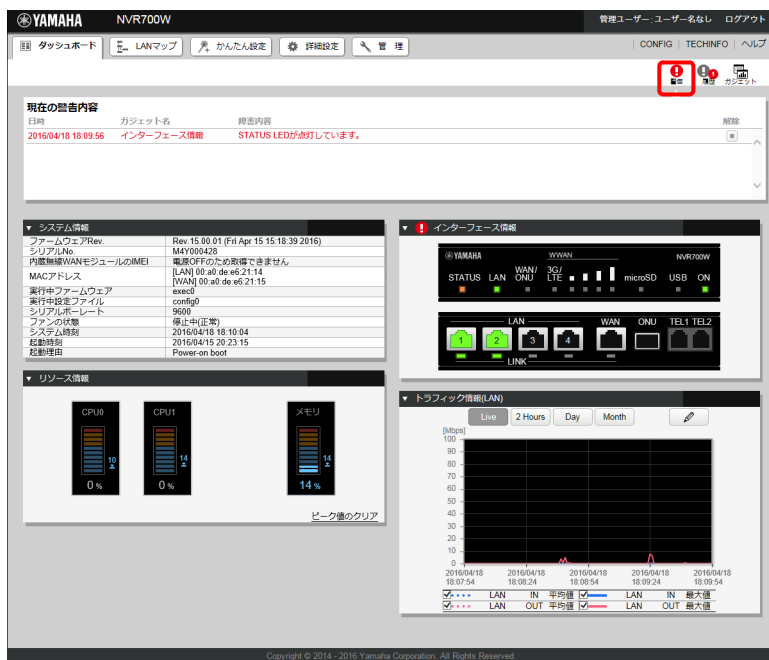
警告内容の一覧と警告履歴の一覧を同時に開くことはできません。

#### メモ

ダッシュボードに表示している各ガジェットで、異常状態または高負荷を検知すると「**!**」が点滅します。その際、該当ガジェットにも「**!**」アイコンが点滅しながら表示されます。

#### 1. 「**!**」ボタンをクリックする。

現在の警告内容が一覧で表示されます。



警告一覧には現在検出している警告内容が新しい順に表示されます。

- ・ 異常を検出した日時
- ・ 異常を検出したガジェット
- ・ 検出した内容

警告は、以下の条件を満たすと表示されなくなります。

- ・ 異常状態から復旧する（使用率やセッション数が閾値を下回った、など）
- ・ 状態をクリアする（設定を変更した、カウンタをクリアした、など）
- ・ 警告一覧の「解除」ボタンをクリックする

#### ご注意

「解除」ボタンをクリックして表示を消しても、異常状態が解消されたわけではありません。

#### メモ

すべての警告表示が消えると「**!**」の点滅は止まり、警告一覧の表示も消えます。

再度「**!**」ボタンをクリックすると警告内容の一覧は閉じられます。

## 警告の対象となる状態

ガジェット	トリガー
システム情報	起動理由でリブートを検出したとき ファンの異常状態を検出したとき (NVR700W)
リソース情報	CPU0 使用率が 80% 以上になったとき CPU1 使用率が 80% 以上になったとき メモリ使用率が 80% 以上になったとき
インターフェース情報	STATUS ランプが点灯したとき LAN/WAN/ONU でエラー (*) を検出したとき (*) 以下を LAN のエラーと判定します <ul style="list-style-type: none"> <li>- 送信アンダーフロー</li> <li>- 送信オーバーフロー</li> <li>- Late collision</li> <li>- Loss of carrier</li> <li>- 再送エラー</li> <li>- 受信フレーミングエラー</li> <li>- 受信オーバーフロー</li> <li>- 受信 CRC エラー</li> </ul> USB ポートで過電流が検出されたとき
トラフィック情報 (LAN/PP/TUNNEL)	[Live] のトラフィックが 800[Mbps] 以上になったとき
プロバイダー接続状態	エラーにより切断されたプロバイダーを検出したとき
VPN 接続状態 (拠点間 / リモートアクセス)	エラーにより切断された VPN を検出したとき
NAT セッション数	NAT のセッション数が最大同時セッション数の 80% 以上になったとき
ファストパスフロー数	ファストパスのフロー数が最大同時フロー数の 80% 以上になったとき
動的フィルターセッション数	動的フィルターのセッション数が最大同時セッション数の 80% 以上になったとき
不正アクセス検知履歴	不正アクセスを検知したとき

## 10.2.8 警告履歴表示


### ご注意


警告履歴の一覧と警告内容の一覧を同時に開くことはできません。

1. 「」 ボタンをクリックする。

警告履歴が一覧で表示されます。警告履歴は新しい順に最大で 30 件表示されます。

### メモ

- ・ 警告履歴は太字で表示されますが、警告一覧で「解除」ボタンをクリックすることにより解除された警告内容は細字で表示されます。
- ・ 解除されていない未確認の警告履歴がある場合は、 のように警告履歴の数が表示されます。この数字が表示されているときは、警告履歴の一覧で発生していた警告内容を確認してください。

再度「」 ボタンをクリックすると警告履歴の一覧は閉じられます。

### 警告履歴の操作

- ・ 各履歴の「確認」ボタンをクリックすると、確認済みの履歴として細字に切り替わり、「確認」の表示が消えます。
- ・ 「全て確認済」ボタンをクリックすると、すべての履歴が確認済みの状態になります。
- ・ 「全て削除」ボタンをクリックすると、すべての履歴が削除されます。

## 10.3 各ガジェットの説明

ダッシュボードに対応しているガジェットは以下のとおりです。

- ・ システム情報 … 145 ページ
- ・ リソース情報 … 146 ページ
- ・ インターフェース情報 … 147 ページ
- ・ トラフィック情報 (LAN/PP/TUNNEL) … 149 ページ
- ・ プロバイダー接続状態 … 151 ページ
- ・ VPN 接続状態 (拠点間) … 151 ページ
- ・ VPN 接続状態 (リモートアクセス) … 152 ページ
- ・ NAT セッション数 … 152 ページ
- ・ ファストパスフロー数 … 152 ページ
- ・ 動的フィルターセッション数 … 153 ページ
- ・ プロバイダー接続履歴 … 153 ページ
- ・ 通話履歴 … 154 ページ
- ・ 不正アクセス検知履歴 … 154 ページ
- ・ SYSLOG … 155 ページ

### 10.3.1 システム情報

システム情報	
ファームウェアRev.	Rev. 15.00.01 (Fri Apr 15 15:18:39 2016)
シリアルNo.	M4Y000428
内蔵無線WANモジュールのIMEI	電源OFFのため取得できません
MACアドレス	[LAN] 00:a0:de:e6:21:14 [WAN] 00:a0:de:e6:21:15
実行中ファームウェア	exec0
実行中設定ファイル	config0
シリアルボーレート	9600
ファンの状態	停止中(正常)
システム時刻	2016/04/18 17:32:22
起動時刻	2016/04/15 20:23:15
起動理由	Power-on boot

#### メモ

工場出荷状態ではダッシュボードの左上の位置に表示されます。

以下の情報が表示されます。

#### ファームウェア Rev.

- ・ ファームウェアのリビジョンが表示されます。

#### シリアル No.

- ・ 機器のシリアル番号が表示されます (筐体底面のシールにも記載されています)。

#### 内蔵無線 WAN モジュールの IMEI (NVR700W)

- ・ 内蔵無線 WAN モジュールの IMEI 番号が表示されます。

#### MAC アドレス

- ・ LAN と WAN/ONU の MAC アドレスが表示されます (筐体底面のシールにも記載されています)。

#### 実行中ファームウェア

- ・ 不揮発性メモリ内のファームウェアから起動している場合は「execN (N: 0-1)」(NVR700W) や「internal」(NVR510)、外部メモリ内に保存されているファームウェアから起動している場合は「usb1:/nvr700w.bin」または「usb1:/nvr510.bin」のように表示されます。

## 第 10 章 ダッシュボードを利用する

### 実行中設定ファイル

- ・ 不揮発性メモリ内の設定ファイルから起動している場合は「configN (N: 0-4.2)」、外部メモリ内に保存されている設定ファイルから起動している場合は「usb1:/config.txt」のように表示されます。

### シリアルボーレート

- ・ CONSOLE ポートのデータ転送速度が表示されます。

### ファンの状態 (NVR700W)

- ・ ファンの状態が表示されます。ファンが正常に動作、または停止しているか確認できます。

### システム時刻

- ・ 現在の機器の日時が表示されます。

### メモ

日時が合っていない場合は、「3.1 日付と時刻を設定する」を参照して日時を合わせてください。


### 起動時刻

- ・ ヤマハルーターの起動した日時が表示されます。

### 起動理由

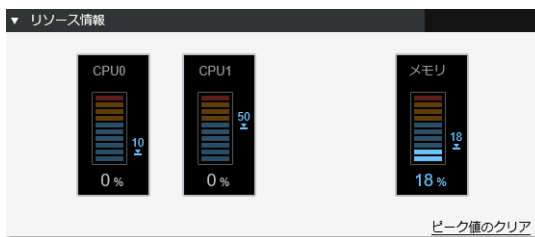
- ・ 起動した理由が表示されます（電源 OFF 状態からの起動、restart コマンド、リビジョンアップなどが表示されます）。

### メモ

起動理由でリポートを検出した場合や、ファンの異常を検出した場合 (NVR700W) は、背景が赤色に変わり  が表示されます。ネットワーク管理者に連絡してください。

また、警告一覧の「解除」ボタンをクリックして、警告表示を解除してください。

## 10.3.2 リソース情報



### メモ

工場出荷状態ではダッシュボードの左下の位置に表示されます。

CPU0、CPU1 使用率とメモリ使用率の現在の値とピーク値が表示されます。メーターの下側の数字は現在の使用率、右側はピーク値を示します。

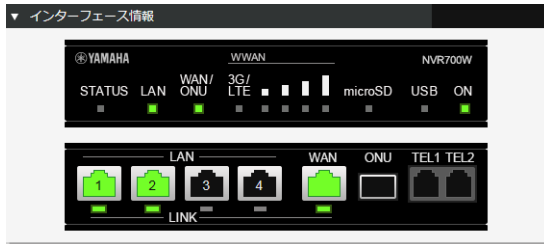
### メモ

- ・ 「ピーク値のクリア」ボタンをクリックすると、それまでのピーク値をクリアすることができます。また、ヤマハルーターを再起動してもピーク値はクリアされます。
- ・ それぞれのメーターにマウスカーソルを重ねると、ピーク値とピーク値を記録した日時が表示されず。

### ご注意

- ・ CPU0 または CPU1 使用率が 80% 以上になると **!** が表示されます。ピーク値を記録した日時を確認し、他のガジェットからその時間帯のトラフィックや各種セッション数を確認してください。
- ・ メモリ使用率が 80% 以上になると **!** が表示されます。ピーク値を記録した日時を確認し、他のガジェットからその時間帯のトラフィックや各種セッション数を確認してください。

### 10.3.3 インターフェース情報



### メモ

工場出荷状態ではダッシュボードの右上の位置に表示されます。

本体のランプの状態が表示されます。

### ランプ

#### STATUS

- ・ 常時接続の設定をしている接続先の機器との通信が途絶えたり、キープアライブで通信断を検出すると橙色に点灯します。
- ・ 点灯すると警告表示されます。マウスカーソルを重ねると障害を検出しているキープアライブの設定やインターフェースを確認できます。ケーブル抜けや回線の状態、アカウント情報の確認などを行ってください。キープアライブの到達性が回復したり、回線が接続状態になると警告表示は消えます。

#### LAN

- ・ LAN ポートがリンクアップしているときは緑色に点灯します。
- ・ マウスカーソルを重ねると LAN ポートのパケット送受信数やエラーパケット数が表示されます。
- ・ エラーパケットを検出すると警告表示されます。clear status lan1 コマンドを実行するとパケットの送受信数やエラーカウンタがリセットされ、警告表示も消すことができます。

#### WAN/ONU

- ・ WAN または ONU ポートがリンクアップしているときは緑色に点灯します。
- ・ マウスカーソルを重ねると WAN/ONU ポートのパケット送受信数やエラーパケット数が表示されます。
- ・ エラーパケットを検出すると警告表示されます。WAN の場合は clear status lan2、ONU の場合は clear status onu1 コマンドを実行するとパケットの送受信数やエラーカウンタがリセットされ、警告表示も消すことができます。

#### WWAN (NVR700W)

- ・ 3G/LTE ランプは、3G 接続されているときは橙色、LTE 接続されているときは緑色に点灯します。
- ・ アンテナランプは、受信レベルによって緑色に点灯または点滅します。
- ・ 左端のランプが点滅しているときは圏外状態であることを示します。
- ・ マウスカーソルを重ねるとモジュールの電源状態や RF 部の電源状態、SIM カードの有無などの情報が表示されます。

## 第 10 章 ダッシュボードを利用する

### microSD

- ・ microSD スロットに microSD が接続されていると緑色に点灯します。
- ・ マウスカーソルを重ねると給電状態や接続されているデバイス情報が表示されます。

### USB

- ・ USB ポートに USB メモリ、または USB 接続型データ通信端末が接続されていると緑色に点灯します。
- ・ マウスカーソルを重ねると給電状態や接続されているデバイス情報が表示されます。
- ・ 過電流を検出すると緑色で点滅し、警告表示されます。マウスカーソルを重ねると過電流の検出回数が表示されます。また、USB ポートに挿しているデバイスを抜き、USB ボタンを押すと警告表示も消すことができます。
- ・ USB ランプの点灯パターン
  - 点灯：USB メモリ、または USB 接続型データ通信端末が接続中
  - 点滅：過電流を検出

### ON

- ・ 電源が入っていると緑色に点灯します。

### LAN ポート

#### コネクタ部

- ・ リンクアップしているポートは緑色に点灯します。マウスカーソルを重ねると動作モードが表示されます。

#### LINK

- ・ リンクアップしているポートは緑色に点灯します。

### WAN ポート

#### コネクタ部

- ・ リンクアップしているポートは緑色に点灯します。マウスカーソルを重ねると動作モードが表示されます。

#### LINK

- ・ リンクアップしているポートは緑色に点灯します。

### ONU ポート

#### コネクタ部

- ・ リンクアップしているとき緑色に点灯します。マウスカーソルを重ねると動作モードが表示されます。

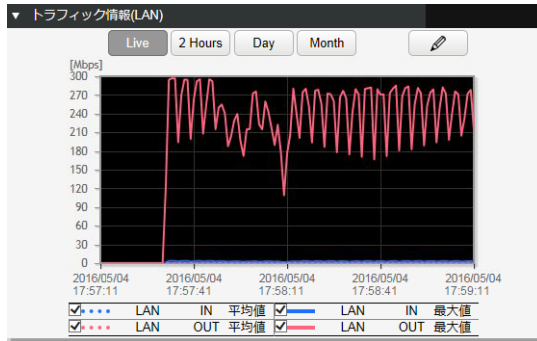
### TEL ポート

#### コネクタ部

- ・ 電話機や FAX などのアナログ機器をオフフックしたときや、着信があったときに緑色に点灯します。



### 10.3.4 トラフィック情報 (LAN/PP/TUNNEL)



#### メモ

工場出荷状態では、トラフィック情報 (LAN) がダッシュボードの右下の位置に表示されます。

有効になっているインターフェース (LAN/PP/TUNNEL) ごとのトラフィックがグラフで表示されます。各インターフェースに対して「IN 平均値」、「IN 最大値」、「OUT 平均値」、「OUT 最大値」のグラフを描画します。

グラフは最大で 8 本まで表示でき、グラフの線には [ 青、サーモンピンク、黄、緑、灰、スカイブルー、ピンク、紫 ] の 8 色が使用されます。この色は、グラフを描画するタイミングでインターフェースの若い順に割り当てられます。

**IN** : 該当インターフェースが受信するトラフィック

**OUT** : 該当インターフェースから送信されるトラフィック

#### メモ

- ・ 同一インターフェースかつ同一方向のグラフは、平均値は破線、最大値は実線で表示されます。
- ・ 有効になっている LAN/PP/TUNNEL インターフェースのトラフィックのみ表示されます。
- ・ トラフィック情報は、LAN 分割やタグ VLAN インターフェースには対応していません。

グラフの縦軸の上限はトラフィックに応じて 100[Mbps] 単位で最大 1000[Mbps] まで増えていきます。また、グラフの横軸の日時は以下の周期で更新されます。

- ・ Live : 30 秒
- ・ 2 Hours : 30 分
- ・ Day : 6 時間
- ・ Month : 約 1 週間

グラフの線上にマウスカーソルを重ねると、インターフェース情報や日時、トラフィック量が表示されます。グラフの下には現在表示されているグラフの線の色・スタイル、インターフェースの一覧 (凡例) が表示されます。

#### 凡例の使い方


凡例のチェックが入っている項目のみ表示されます。チェックを外すとグラフに表示されなくなります。複数の線が重なっていたり、特定のインターフェースを監視したい場合などに表示を切り替えてください。

## 第 10 章 ダッシュボードを利用する

### メモ

- ・ 現在監視の対象になっているインターフェースが存在しない場合は、「監視対象のインターフェースが選択されていません」と表示されます。
- ・ 画面を更新すると、すべての凡例にチェックが入り、描画期間が Live に切り替わります。

### ご注意

トラフィックが 800[Mbps] 以上になると  が表示されます。警告一覧や警告履歴からトラフィックが高くなっていった日時を確認し、その時間帯の各種セッション数を確認してください。

### 「」により別ウィンドウでガジェットを表示させた場合

- ・ 監視対象のインターフェースや方向の設定は分離前の設定が反映されます。ただし、すべての凡例にチェックが入り、描画期間が Live に切り替わります。
- ・ 分離したウィンドウ内で選択したインターフェースや方向の設定は、分離画面を閉じるとダッシュボードページのガジェットにも反映されます。

### 分離したウィンドウの URL を直接入力してガジェットを表示させた場合


監視対象のインターフェースや方向の設定は直接表示専用の設定が適用されるため、ダッシュボードページの設定とは異なります。ただし、すべての凡例にチェックが入り、描画期間が Live に切り替わります。

### グラフの描画期間を変更する

「Live」、「2 Hours」、「Day」、「Month」ボタンをクリックし、描画期間を変更します。

- ・ Live：過去 2 分間
- ・ 2 Hours：過去 2 時間
- ・ Day：過去 1 日間
- ・ Month：過去 1 ヶ月間

### グラフに描画するインターフェースを選択する

「」ボタンをクリックします。一覧から表示するインターフェースのチェックボックスにチェックを入れ、「適用」ボタンをクリックすると設定が反映されます。

### メモ

- ・ 有効になっていないインターフェースのチェックボックスは表示されません。
- ・ 現在有効になっているインターフェースが存在しない場合は、「有効なインターフェースが見つかりません」と表示されます。

### 10.3.5 プロバイダー接続状態

設定名	接続種別	インターフェース	状態
1 DHCP	DHCP, または固定IPアドレス	WAN	10.0.4.166/24
2 APN	Mobile WAN接続	MOBILE WAN	[Signal strength icon] [Globe icon]

プロバイダー接続の一覧とそれぞれの接続状態が表示されます。

通信中 (Up)、未接続 (Down)、エラー切断 (Error)、総数 (All) がカウントされます。また、「Up」、「Down」、「Error」、「All」 ボタンをクリックすると、各状態のプロバイダー接続のみを表示することができます。設定名、接続種別、インターフェース、接続状態が表示されます。状態欄にマウスカーソルを重ねると、そのプロバイダー接続の状態が表示されます。

#### ご注意

エラー切断を検出すると背景が赤色に変わり、**!** が表示されます。状態欄にマウスカーソルを重ね、切断された日時や切断理由を確認してください。

#### メモ

プロバイダーが一つも登録されていないときは「プロバイダーの設定がありません」と表示されます。

### 10.3.6 VPN 接続状態（拠点間）

設定名	接続種別	インターフェース	状態
1 Tokyo	IPsec接続	TUNNEL[03]	[Signal strength icon] [Globe icon]
2 Osaka	IPsec接続	TUNNEL[04]	[Signal strength icon] [Globe icon]

VPN 接続（拠点間）の一覧とそれぞれの接続状態が表示されます。

通信中 (Up)、未接続 (Down)、エラー切断 (Error)、総数 (All) がカウントされます。また、「Up」、「Down」、「Error」、「All」 ボタンをクリックすると、各状態の VPN 接続のみを表示することができます。

設定名、接続種別、インターフェース、接続状態が表示されます。状態欄にマウスカーソルを重ねると、その VPN 接続の状態が表示されます。

#### ご注意

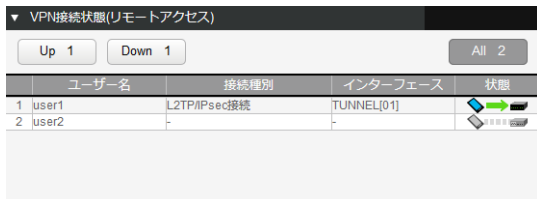
エラー切断を検出すると背景が赤色に変わり、**!** が表示されます。状態欄にマウスカーソルを重ね、切断された日時や切断理由を確認してください。

#### メモ

VPN 接続が一つも登録されていないときは「VPN の設定がありません」と表示されます。

## 第 10 章 ダッシュボードを利用する

### 10.3.7 VPN 接続状態 (リモートアクセス)



ユーザー名	接続種別	インターフェース	状態
1 user1	L2TP/IPsec接続	TUNNEL[01]	通信中
2 user2	-	-	未接続

VPN 接続 (リモートアクセス) の一覧とそれぞれの接続状態が表示されます。

通信中 (Up)、未接続 (Down)、総数 (All) がカウントされます。また、「Up」、「Down」、「All」 ボタンをクリックすると、各状態の VPN 接続のみを表示することができます。

ユーザー名、接続種別、インターフェース、接続状態が表示されます。状態欄にマウスカーソルを重ねると、その VPN 接続の状態が表示されます。

#### メモ

VPN 接続が一つも登録されていないときは「VPN の設定がありません」と表示されます。

### 10.3.8 NAT セッション数



NAT のセッション数が表示されます。

メーターの右側の数字は現在の利用率を示し、上部はピークの使用率を示します。

メーターの左上部にディスクリプタ ID、右上部に現在の接続数と最大数が表示されます。

メーターは現在の接続数が最も多いディスクリプタ ID の NAT セッション数を表示します。

#### ご注意

セッション数が最大同時セッション数の 80% 以上になると **!** が表示されます。ピーク値を記録した日時やセッションを大量に使用していたホストの IP アドレスを確認してください。

#### メモ

- ・ 「ピーク値のクリア」 ボタンをクリックすると、すべてのディスクリプタ ID のピーク値をクリアすることができます。また、ヤマハルーターを再起動してもピーク値はクリアされます。
- ・ メーターにマウスカーソルを重ねると、ピーク値 / ピーク時のセッション数上位 5 件のホストの IP アドレスとホストごとのセッション数 / ピーク値を記録した日時が表示されます。

### 10.3.9 ファストパスフロー数



ファストパスのフロー数が表示されます。

メーターの右側の数字は現在の利用率を示し、上部はピークの使用率を示します。

メーターの上部に現在のフロー数と最大数が表示されます。

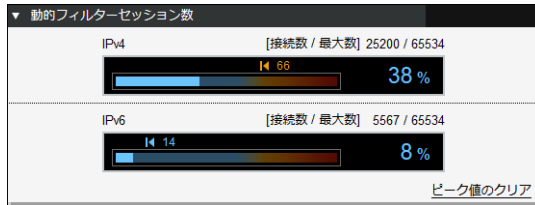
### ご注意

フロー数が最大同時フロー数の 80% 以上になると **!** が表示されます。ピーク値を記録した日時を確認し、他のガジェットからその時間帯のトラフィックや各種セッション数を確認してください。

### メモ

- ・「ピーク値のクリア」ボタンをクリックすると、IPv4/IPv6 のピーク値をクリアすることができます。また、ヤマハルーターを再起動してもピーク値はクリアされます。
- ・メーターにマウスカーソルを重ねると、ピーク値とピーク値を記録した日時が表示されます。

## 10.3.10 動的フィルターセッション数



動的フィルターで管理しているセッション数が表示されます。メーターの右側の数字は現在の使用率を示し、上部はピークの使用率を示します。メーターの上部に現在の接続数と最大数が表示されます。

### ご注意

セッション数が最大同時セッション数の 80% 以上になると **!** が表示されます。ピーク値を記録した日時を確認し、他のガジェットからその時間帯のトラフィックや各種セッション数を確認してください。

### メモ

- ・「ピーク値のクリア」ボタンをクリックすると、IPv4/IPv6 のピーク値をクリアすることができます。また、ヤマハルーターを再起動してもピーク値はクリアされます。
- ・メーターにマウスカーソルを重ねると、ピーク値とピーク値を記録した日時が表示されます。

## 10.3.11 プロバイダー接続履歴

開始日時	切断日時	インターフェース	状態
04/18 19:20	---	ONU/PP101	接続中
04/18 19:20	04/18 19:20	ONU/PP101	切断 (異常)
04/18 19:19	04/18 19:19	ONU/PP101	切断 (異常)

プロバイダー接続履歴は、通話履歴と合わせて 100 件まで最新の履歴が表示されます。

### メモ

- ・「接続中」、「切断」、「切断 (異常)」、「All」ボタンをクリックすると履歴を絞り込んで表示させることができます。
- ・1 件も履歴がないときは「プロバイダー接続は記録されていません」と表示されます。
- ・異常切断が発生した履歴は赤でハイライト表示されます。
- ・異常切断が発生した履歴の状態欄をマウスオーバーするとツールチップが表示され、切断コードと切断理由を確認することができます。

## 第 10 章 ダッシュボードを利用する

### 10.3.12 通話履歴

発信日時		相手番号	通話時間	
04/22 10:07	SIP	sip.xxxx@xxx.xxx.xxx	---	発信
04/22 10:06	SIP	sip.xxxx@xxx.xxx.xxx	4秒	着信
04/22 10:00	NGN(TEL)	09011111111	1分51秒	発信
04/22 09:58	NGN(TEL)	08011111111	6秒	発信

通話履歴は、プロバイダー接続履歴を合わせて 100 件まで最新の履歴が表示されます。

#### メモ

- ・「発信」、「着信」、「不在着信」、「All」ボタンをクリックすると履歴を絞り込んで表示させることができます。
- ・ 1 件も履歴がないときは「通話は記録されていません」と表示されます。
- ・ 異常切断が発生した履歴は赤でハイライト表示されます。
- ・ 異常切断が発生した履歴の状態欄をマウスオーバーするとツールチップが表示され、切断コードと切断理由を確認することができます。

### 10.3.13 不正アクセス検知履歴

日時	検知内容	送信元アドレス	宛先アドレス
2016/05/26 15:30:59	ICMP too large	192.168.100.5	> 192.168.100.1
2016/05/26 15:29:58	ICMP too large	192.168.100.5	> 192.168.100.1

不正アクセスの検知履歴が最新のものから 10 件分表示されます。

不正アクセス検知機能を有効に設定しておく必要があります。Web GUI から設定できないため、コンソールコマンドで設定してください。

検知した日時、検知した内容、送信元アドレス、宛先アドレスが表示されます。必要に応じて、送信元 IP アドレスからのアクセスを拒否するフィルターを設定してください。

すべてのインターフェースに対する検知結果が時系列にまとめて表示され、一番上が最新の履歴になります。

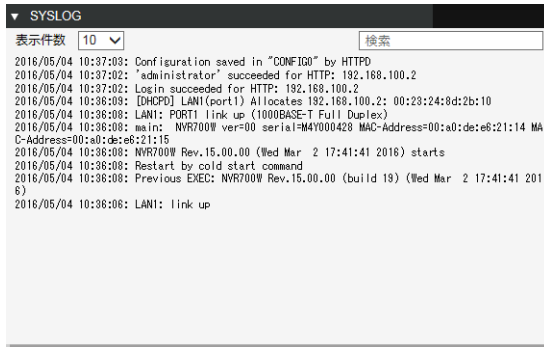
#### ご注意

- ・ 不正アクセス検知機能の設定を再設定すると履歴はクリアされます
- ・ 不正アクセスを検知すると **!** が表示されます。ネットワーク管理者に確認してください。

#### メモ

1 件も検知されていないときは「不正アクセスは検知していません」と表示されます。

## 10.3.14 SYSLOG



SYSLOG が最新のものから表示件数分表示されます。一番上が最新のログになります。

表示する件数（10件、50件、100件）をプルダウンメニューから変更することができます（初期値：10件）。

検索ボックスに検索したい文字列を入力すると、入力した文字列を含んだログのみを表示させることができます。なお、大文字、小文字は区別されます。

# 第 11 章 LAN マップを利用する

本章では、LAN マップの利用方法について説明します。本章では、LAN マップの制御を行うヤマハルーターのことを「コントローラー」、コントローラーが制御しているヤマハスイッチ、およびヤマハ無線 AP を「スレーブ」と呼びます。

- ・ LAN マップとは? …156 ページ
- ・ LAN マップの画面構成 …156 ページ
- ・ LAN マップを有効にする …160 ページ
- ・ スレーブの状態を確認する …162 ページ
- ・ ネットワークの異常を監視する …163 ページ
- ・ 機器を検索する …167 ページ
- ・ ヤマハスイッチを設定する …169 ページ
- ・ ヤマハ無線 AP の設定を行う …195 ページ
- ・ タグ VLAN を設定する …207 ページ
- ・ マルチプル VLAN を設定する …214 ページ
- ・ 接続機器の一覧を見る …220 ページ

## 11.1 LAN マップとは?

LAN マップでは、LAN 内に存在するスレーブと、その配下のパソコンやプリンター、ネットワークカメラ、POS 端末、スマートデバイスなどの通信端末の配置図を Web ブラウザー上に表示します。また、「LAN マップ」画面でスレーブの設定を変更したり、ネットワークの異常を一目で把握することもできるため、ネットワーク管理者の作業負荷を軽減します。

## 11.2 LAN マップの画面構成

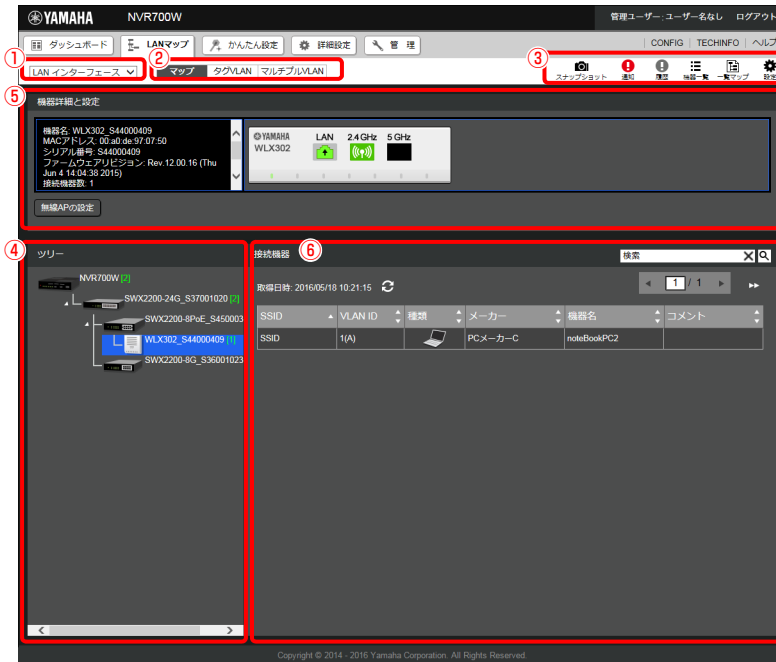
LAN マップは主に以下の画面で構成されており、画面上部の表示選択スイッチにより画面を切り替えることができます。

- マップページ …157 ページ
- タグ VLAN ページ …157 ページ
- マルチプル VLAN ページ …159 ページ



### 11.2.1 マップページ

ネットワークの状態が可視化されます。機器の接続状況を確認したり、スレーブの設定を変更することができます。



#### ① インターフェース選択プルダウンメニュー

LAN マップを表示したいインターフェースを選択します。LAN マップが有効になっていないインターフェースは選択できません。LAN マップを有効にする方法は、「11.3 LAN マップを有効にする」(160 ページ) をご覧ください。

#### ② 表示選択スイッチ

LAN マップで表示したいページを選択します。

#### ③ 各種ボタン

LAN マップの設定内容や通知メッセージなどを確認したり、スナップショットを保存したりするためのボタンが配置されています。

#### ④ ツリービュー

コントローラーを起点としたスレーブのトポロジーが表示されます。他社製ネットワーク機器は表示されません。「ツリービュー」で「機器」アイコンをクリックすると、「機器詳細と設定ビュー」と「接続機器ビュー」に機器の情報が表示されます。

#### ⑤ 機器詳細と設定ビュー

「ツリービュー」で選択したコントローラー、およびスレーブの詳細情報と機器の詳細画像が表示されます。

#### ⑥ 接続機器ビュー

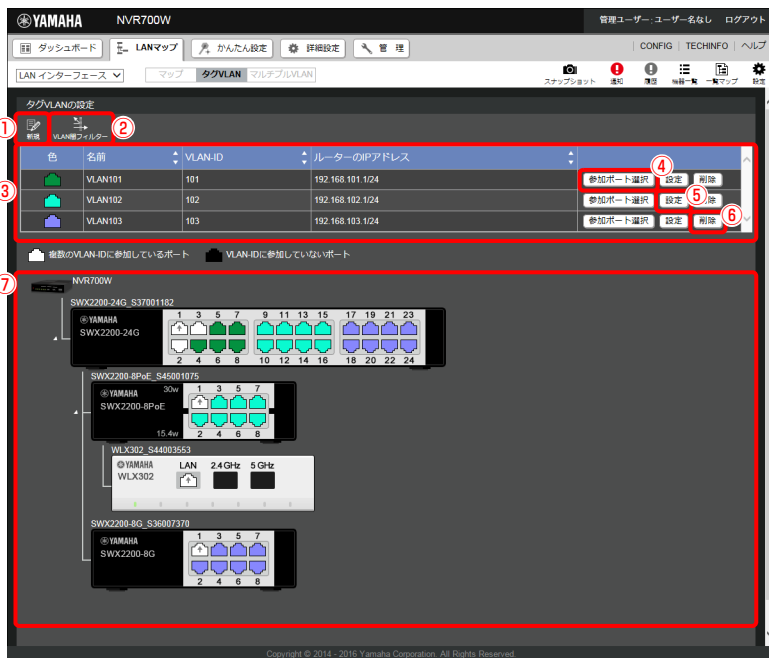
「ツリービュー」で選択したコントローラー、およびスレーブに接続されている機器が表示されます。端末管理が有効になっていない場合、端末の情報は表示されません。端末管理を有効にする方法は、「11.3 LAN マップを有効にする」(160 ページ) をご覧ください。

### 11.2.2 タグ VLAN ページ

VLAN を作成してスレーブのポートをグループ分けすることができます。また、VLAN ごとに IP アドレスを付加したり、すべての VLAN 間の通信を遮断することができます。

### ご注意

- ・ SWX2100 および SWX2300 は、タグ VLAN に対応していません。
- ・ SWX2300 は、「スイッチの設定・保守」ボタンをクリックすると設定画面が表示され、VLAN の設定を行うことができます。



#### ① 「新規」ボタン

VLAN グループを新たに作成します。ポートを VLAN グループに参加させるには、事前に VLAN グループを作成しておく必要があります。

#### ② 「VLAN 間フィルター」ボタン

すべての VLAN 間の通信について、全開放または全遮断を行います。新たに作成した VLAN と既存 VLAN 間の通信は開放されています。必要があれば全遮断を行ってください。

#### ③ タグ VLAN グループ一覧

登録されている VLAN グループの一覧が表示されます。VLAN グループごとにポートの色が割り当てられます。

#### ④ 「参加ポート選択」ボタン

ポートをタグ VLAN グループに参加させることができます。ボタンを押した後、トポロジー内にあるスレーブのポートを選択する必要があります。

#### ⑤ 「設定」ボタン

該当のタグ VLAN グループの設定を変更します。名前、ルーターの IP アドレスを変更することができます。

#### ⑥ 「削除」ボタン

該当のタグ VLAN グループを削除します。

#### ⑦ トポロジー

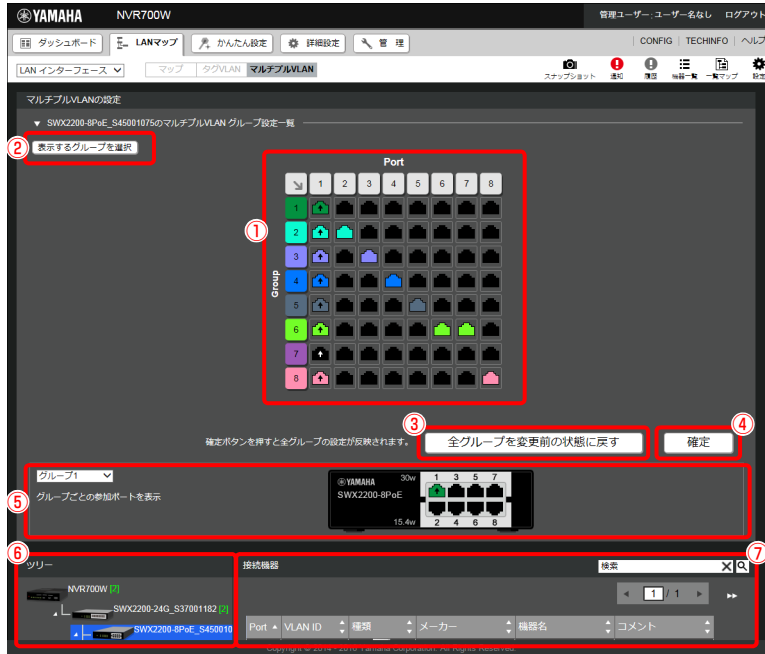
コントローラーを起点としたスレーブのトポロジーが表示されます。スレーブのポートの色を確認することによって、どの VLAN グループに参加しているかわかります。

### 11.2.3 マルチプル VLAN ページ




ひとつのスイッチのポートを複数のグループに分けて、グループ間の通信を遮断することができます。ポートを複数のグループに分けるだけでなく、ひとつのポートを複数のグループに参加させることもできます。たとえば、サーバーやルーターなど全グループと通信を行う必要がある端末が接続されるポートは、すべてのグループに重複して参加させます。なお、マルチプル VLAN ではグループが異なっても同じネットワークアドレスが使用されます。

#### ご注意

- ・ SWX2100 および SWX2300 は、マルチプル VLAN に対応していません。



#### ① マルチプル VLAN グループ設定一覧

マルチプル VLAN のグループごとの参加ポートの状態を、表の形式で表示します。表の横方向はスイッチのポート、縦方向はマルチプル VLAN グループを表し、表内の各ポートアイコン（   など）をクリックすることで各グループに参加させるポートを選択することができます。

#### ② 「表示するグループを選択」ボタン

「マルチプル VLAN グループ設定一覧」の表に表示するグループを選択することができます。

#### ③ 「全グループを変更前の状態に戻す」ボタン

各マルチプル VLAN グループに参加させるポートの編集内容を変更前の状態に戻します。

#### ④ 「確定」ボタン

各マルチプル VLAN グループに参加させるポートの編集内容を設定に反映します。

#### ⑤ 現在のマルチプル VLAN 設定内容

設定済みのマルチプル VLAN グループごとの設定内容を表示します。左側のプルダウンメニューで選択したグループに対する各ポートの参加状態を右側のスイッチ画像内に表示します。

#### ⑥ ツリービュー

マップページで表示されるものと同一です。マルチプル VLAN に対応しているスレーブを選択した場合は「マルチプル VLAN の設定ビュー」にマルチプル VLAN の設定が表示されます。

## 第 11 章 LAN マップを利用する

### ⑦ 接続機器ビュー

マップページで表示されるものと同一です。スイッチのどのポートにどのような機器が接続されているかが確認できるため、マルチプル VLAN グループ設定時の参考にすることができます。

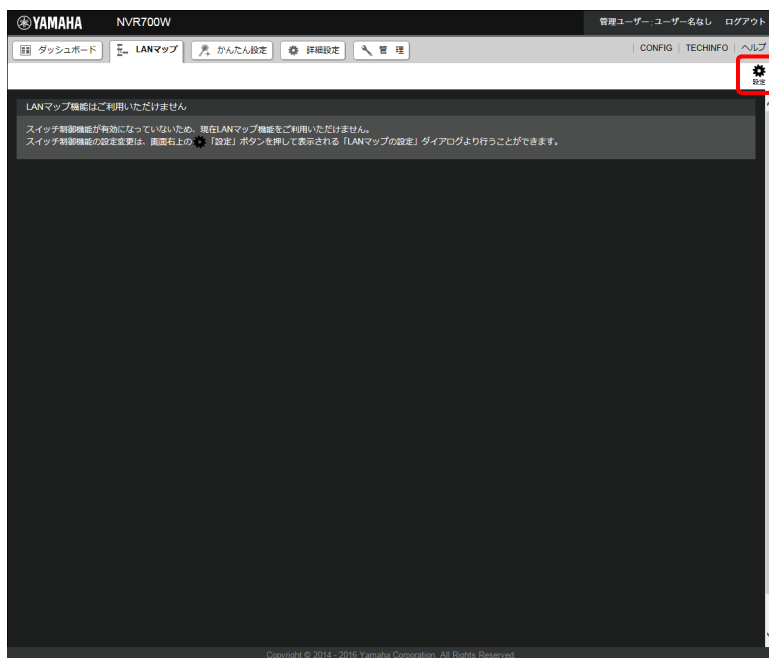
## 11.3 LAN マップを有効にする

LAN マップを使用するための設定方法を説明します。端末の検索を行う間隔を変更したり、スナップショット機能の設定を行ったりすることができます。

### ご注意

- ・ LAN 分割機能設定時は、LAN マップは使用できません。

#### 1. 「設定」ボタンをクリックする。



「LAN マップの設定」ダイアログが表示されます。

## 2. LAN マップを有効にしたいインターフェースで「LAN マップを使用する」を選択する。

**LANマップの設定**

LANマップでは、ネットワークに接続されているスレーブ(サーバ/スイッチ、ヤマハ/無線AP)、端末情報を可視化し、監視、管理することができます。  
LANマップを使用する場合は、基本設定の項目で「LANマップを使用する」を選択してください。

■ **基本設定**

LANマップの基本的な設定を行います。

①

LAN インターフェース	<input checked="" type="radio"/> LANマップを使用する <input checked="" type="checkbox"/> 端末も監視、管理する <input type="radio"/> LANマップを使用しない
WAN インターフェース	<input type="radio"/> LANマップを使用する <input type="checkbox"/> 端末も監視、管理する <input checked="" type="radio"/> LANマップを使用しない

スレーブの監視時間間隔	3 秒 (2-10)
スレーブの消失検出までの監視回数	3 回 (2-10)
端末情報の監視時間間隔	1800 秒 (1800-86400)
無線AP配下の端末情報の監視時間間隔	60 秒 (10-86400)

■ **スナップショット機能の設定**

スナップショット機能を使用するか否かの設定を行います。  
スナップショット機能は、現在のネットワークの接続状態と事前に保存したネットワークの接続状態(スナップショット)を比較して、変化を検知した場合に警告メッセージを表示します。スナップショットを保存するには、別途、「スナップショット」ボタンからスナップショットの保存を実行してください。

②

LAN インターフェース	<input type="radio"/> スナップショット機能を使用する <input type="checkbox"/> すべての端末を比較対象に含める <input type="checkbox"/> 有線接続されている端末のみ比較対象に含める <input checked="" type="checkbox"/> 端末を比較対象に含めない
WAN インターフェース	<input checked="" type="radio"/> スナップショット機能を使用しない <input type="radio"/> スナップショット機能を使用する <input type="checkbox"/> すべての端末を比較対象に含める <input type="checkbox"/> 有線接続されている端末のみ比較対象に含める <input checked="" type="checkbox"/> 端末を比較対象に含めない

## ① 基本設定：

LAN マップの基本的な設定を行います。

- ・ 各インターフェース：LAN マップ機能を使用するか否かを設定します。また、端末も管理したい場合は、「端末も監視、管理する」にチェックを入れてください。
- ・ スレーブの監視時間間隔：スレーブを探索するバケットの送信時間の間隔を設定します。設定した時間間隔でスレーブの管理情報が更新されます。
- ・ スレーブの消失検出までの監視回数：スレーブが消失したと判断するまでの探索バケット送信回数を設定します。
- ・ 端末情報の監視時間間隔：端末を検索する時間の間隔を設定します。設定した時間間隔で端末の管理情報が更新されます。
- ・ 無線 AP 配下の端末情報の監視時間間隔：無線 AP を経由する端末を検索する時間の間隔を設定します。設定した時間間隔で端末の管理情報が更新されます。

## ② スナップショット機能の設定：

スナップショット機能を使用するか否かを設定します。

スナップショット機能は、現在のネットワークの接続状態と事前に保存したネットワークの接続状態(スナップショット)を比較して、変化を検知した場合に警告メッセージを表示する機能です。

- ・ 各インターフェース：スナップショット機能を使用するか否かを設定します。また、無線接続端末と有線接続端末の両方を比較対象とする場合は、「すべての端末を比較対象に含める」にチェックを入れ、有線接続端末のみを比較対象とする場合は「有線接続されている端末のみ比較対象に含める」にチェックを入れます。

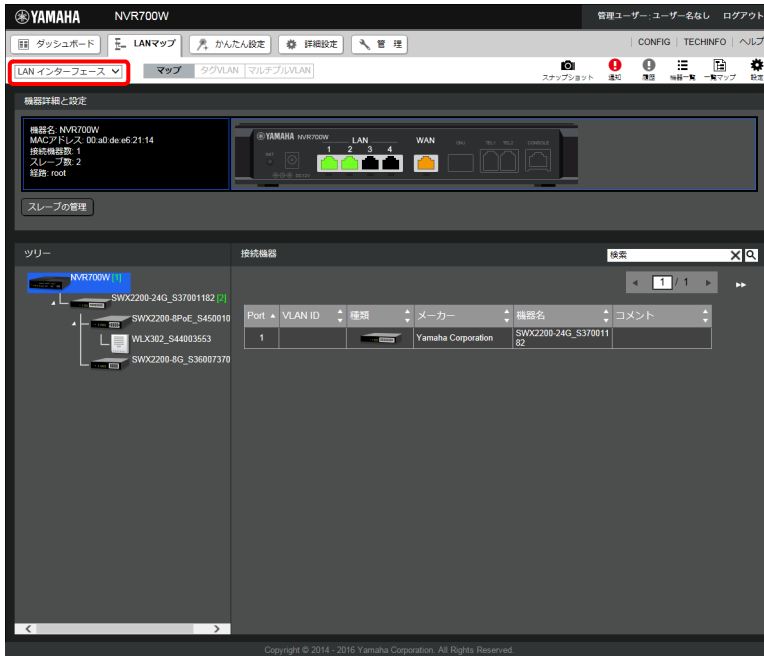
## 3. 「設定の確定」ボタンをクリックする。

設定が反映され、「LAN マップ」画面が表示されます。

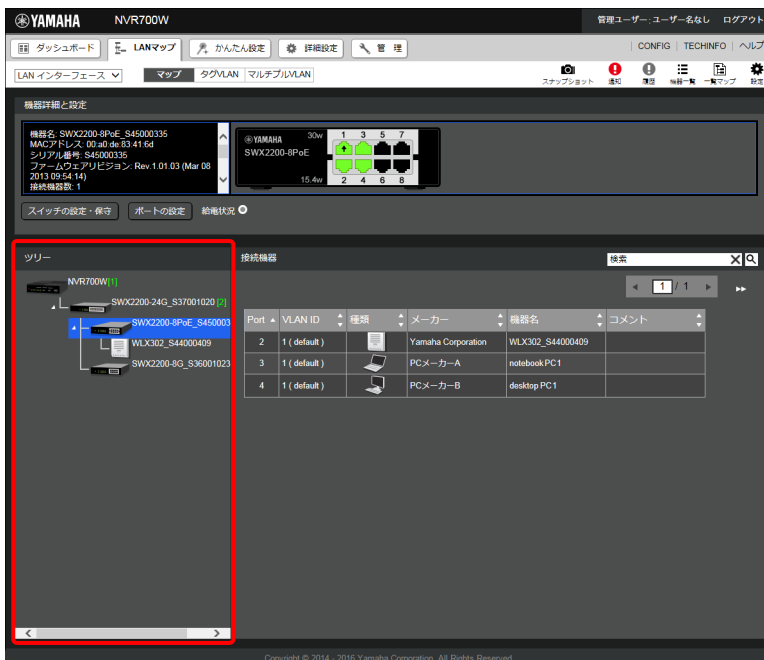
### 11.4 スレーブの状態を確認する

コントローラーに接続した、スレーブや端末の接続状況の確認方法を説明します。

1. 確認したいネットワークのインターフェースを、インターフェース選択プルダウンメニューから選択する。



2. ツリービューで確認したい機器を選択する。



機器詳細と設定ビューに機器の画像が表示され、ポートアイコンからリンク状態を確認することができます。また、ポートをクリックするとポートの詳細情報を確認することができます。

ポートアイコンはリンク状態によって下記のように表示されます。






アイコン	説明
	ポートスピード 1000BASE-T
	ポートスピード 100BASE-TX
	ポートスピード 10BASE-T
	異常発生
	リンクダウン

### メモ



ポートアイコンに上向き矢印が付いているポートはアップリンクポートを表しています。

#### PoE 対応スイッチを選択した場合

機器詳細と設定ビューの「給電状況」ボタンをクリックすると、PoE 給電状況を確認することができます。ポートアイコンは給電状況によって下記のように表示されます。

アイコン	説明
	PoE 給電中（給電 Class0 ～ 3）
	PoE 給電中（給電 Class4）
	PoE 給電は行わない
	給電停止（異常発生）
	給電停止

#### 無線 AP を選択した場合



機器詳細と設定ビューに表示された無線 AP の画像内にある  をクリックすると、無線通信状況を確認することができます。 は無線通信が有効になっている場合に、使用している周波数帯域（2.4GHz 帯、5GHz 帯）ごとに表示されます。

## 11.5 ネットワークの異常を監視する

ネットワークの異常を監視する方法を説明します。スレーブの動作状況の変化や異常を検知すると、通知エリアおよび履歴エリアにメッセージが表示されます。

## 第 11 章 LAN マップを利用する


### 通知エリア

現在のネットワークに対するメッセージが表示されます。通知エリアは新しいメッセージが追加されると自動的に表示され、「」ボタンをクリックすることでも表示することができます。また、メッセージが表示されている状態で「」ボタンをクリックすると通知エリアを閉じることができます。

### メモ

検知された状態が解消されるとメッセージの表示が消えます。その場合でもメッセージは履歴エリアに残ります。

### 履歴エリア

通知メッセージの履歴が表示されます。履歴は最大で 1000 件まで保存され、最大件数を超える場合は古いメッセージから削除されます。履歴エリアは「」ボタンをクリックすることで表示することができます。なお、通知エリアに表示されたメッセージが前回のメッセージから変化していない場合は履歴には追加されません。

### 11.5.1 スレーブの動作状況と異常を監視する

ヤマハスイッチの下記の動作や異常を検知すると、通知エリアおよび履歴エリアにメッセージが表示されます。両エリアに表示されるメッセージと片方のみに表示されるメッセージがあります。

検知項目	通知エリア	履歴エリア
ヤマハスイッチのファンが停止した	○	○
ヤマハスイッチのポートでループが発生した	○	○
ヤマハスイッチのポートの給電が停止した	×	○
ヤマハスイッチのポートで給電を開始した（給電 Class ごと）	×	○
ヤマハスイッチの給電が異常停止した	○	○
ヤマハスイッチの電源に異常が発生した	○	○
ヤマハスイッチの供給電力が最大供給電力を超えた	○	○
ヤマハスイッチがバックアップ経路で接続された	○	○
ヤマハスイッチがマスター経路で接続された	×	○

### 11.5.2 ネットワークの接続状態を監視する

スナップショット機能を使用してネットワークの接続状態を監視できます。スナップショット機能は、現在のネットワークの接続状態と事前に保存したネットワークの接続状態（スナップショット）を比較して、変化を検知した場合に警告メッセージを表示する機能です。事前に「11.3 LAN マップを有効にする」（160 ページ）を参照し、スナップショット機能を有効にしてください。スナップショット機能が有効になっている状態で、以下の操作を行ってはいじめてスナップショット機能が動作し始めます。

### メモ

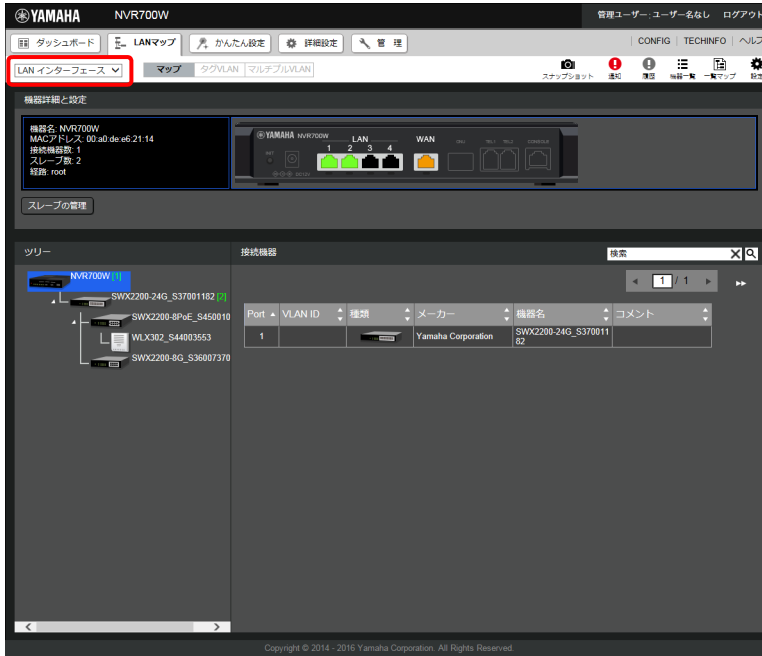
ベースとなるネットワークの接続状態（スレーブや端末の配置）が変わった場合は、その都度本操作を行ってスナップショットを保存し直してください。


### ネットワークの接続状態を保存する

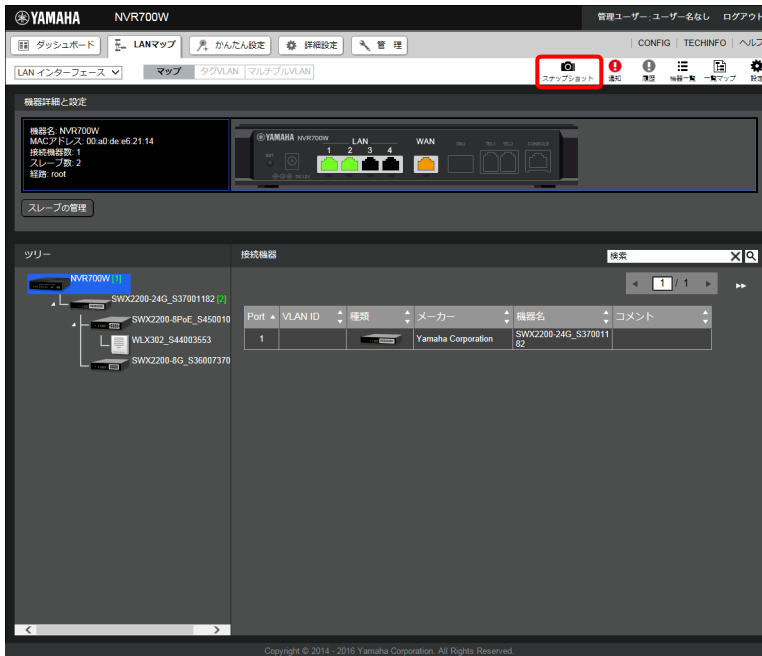
現在のネットワークの接続状態を保存します。



1. 監視したいネットワークのインターフェースを、インターフェース選択プルダウンメニューから選択する。



2. 「 スナップショット」ボタンをクリックする。



「スナップショットの保存」ダイアログが表示されます。

## 第 11 章 LAN マップを利用する

### 3. 「実行」 ボタンをクリックする。

スナップショットの保存

現在のヤマハスイッチとヤマハ無線APの接続状態、および通常の接続状態をスナップショットとして保存します。

スナップショット機能を使用している場合、保存されたスナップショットと現在のネットワークの接続状態を比較します。

スナップショット機能を使用する場合は、「設定」ボタンでスナップショット機能を「使用する」に設定してください。

「保存前にネットワークの接続状態を更新する」を有効にした場合、ネットワークの接続状態の情報を最新に更新した後に保存します。

※ネットワークの構成によっては保存が完了するまでに20分～30分程かかる場合があります。他の処理が実行できなくなることはありません。

保存前にネットワークの接続状態を更新する

#### メモ

「保存前にネットワークの接続状態を更新する」にチェックを入れた場合は、ネットワークの接続状態の情報を更新した後に保存します。ただし、ネットワークの構成によっては保存が完了するまでに 20 ～ 30 分程かかる場合があります。その間も他の操作は行えます。

### 変化を検知した場合

保存したネットワークの接続状態からの変化を検知すると、通知エリアおよび履歴エリアに下記のメッセージが表示されます。両エリアに表示されるメッセージと片方のみに表示されるメッセージがあります。

検知項目	通知エリア	履歴エリア
スナップショットに登録されていない機器が接続されている	○	○
機器の接続ポートがスナップショットと異なっている	○	○
スナップショットに登録されている機器が接続されていない	○	○
異常が検出されていた機器がスナップショットと一致した	×	○

### 11.5.3 ネットワークの異常をメールで通知する

ネットワークの異常を検知すると、登録した宛先にメールでお知らせします。

通知内容	通知方法
LAN マップの異常検知	LAN マップの異常を検知した場合、メールで通知します。
内部状態	内部状態については、自動で通知されません。「メール通知」画面の「いますぐ通知」の「進む」ボタンをクリックして、表示されるダイアログの「実行」ボタンをクリックすると、ヤマハルーターの内部状態を登録した宛先へ通知します。
インターフェース情報	
経路情報	
VPN 接続状態	
NAT	
ファイアウォール	
設定内容・ログ	

#### メモ

メール通知の設定について詳しくは、「13.10 メール通知機能を使う」（327 ページ）をご覧ください。

## 11.6 機器を検索する

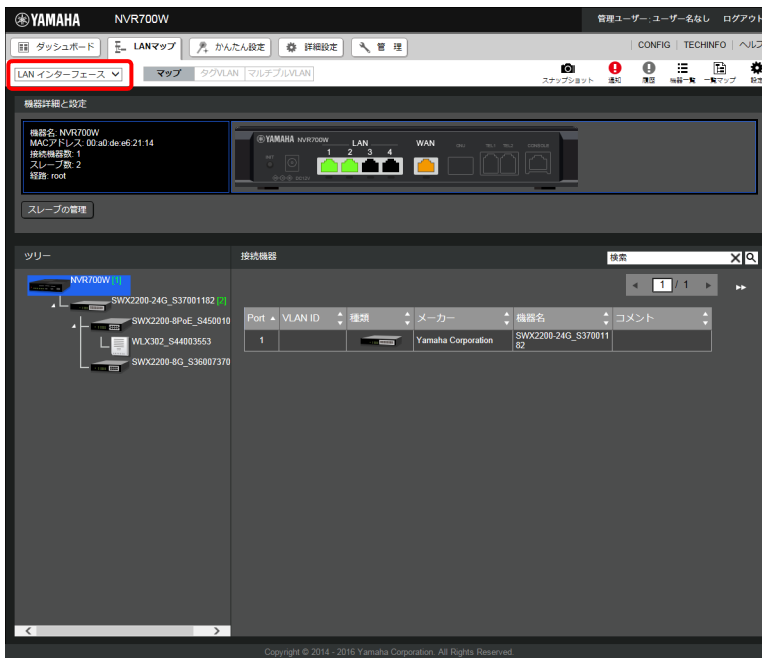
ネットワークに存在する機器を任意のキーワードで検索することができます。  
機器検索はキーワードと以下の機器情報を比較することで行われます。

- ・ 経路
- ・ SSID
- ・ VLAN ID
- ・ メーカー
- ・ 機器名
- ・ コメント
- ・ MAC アドレス
- ・ IP アドレス
- ・ 機種名
- ・ OS
- ・ 周波数

### ご注意

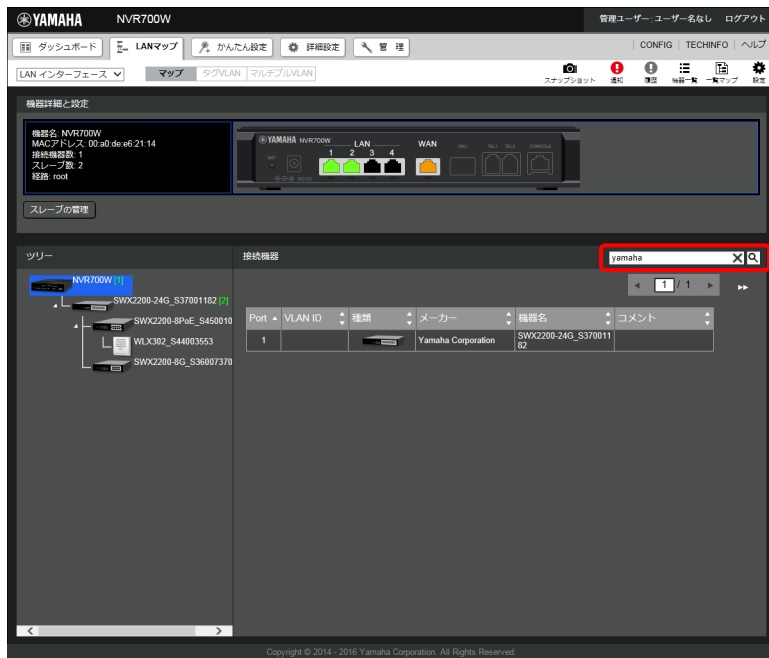
キーワードの大文字 / 小文字は区別されません。

1. 機器を検索したいネットワークのインターフェースを、インターフェース選択プルダウンメニューから選択する。



## 第 11 章 LAN マップを利用する

2. 接続機器ビューの検索ボックスに任意のキーワードを入力し、「**Q**」ボタンをクリックする。



検索結果が表示されます。



### ① ツリービュー：

検索でヒットした機器が接続されている機器アイコンがブルーグレーでハイライト表示されます。コントローラー、およびスレーブを選択すると「接続機器ビュー」に接続機器の一覧が表示されます。

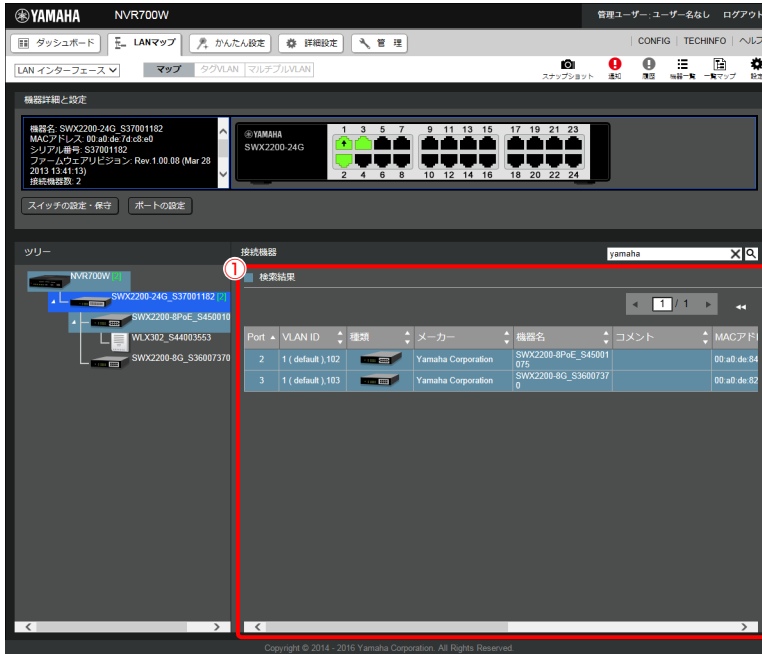
### ② 検索結果：

検索でヒットした機器の一覧が表示されます。

## メモ

検索結果の表示を解除するには、「**X**」ボタンをクリックしてください。

## 3. 検索でヒットした機器が接続されているスレーブをツリービューで選択する。



## ① 接続機器ビュー：

検索でヒットした機器アイコンがブルグレーでハイライト表示されます。異常検知による赤のハイライトと重なった場合は、ブルグレーが優先されます。

## メモ

検索結果の表示を解除するには、「**X**」ボタンをクリックしてください。

## 11.7 ヤマハスイッチを設定する

ヤマハスイッチの設定方法を説明します。

## 11.7.1 スイッチの設定・保守ダイアログを表示する

設定変更や保守機能を実行するヤマハスイッチの「スイッチの設定・保守」ダイアログを表示します。

## ご注意

ヤマハスイッチの種類によって、設定・保守ダイアログの設定内容や表示が異なります。

・ SWX2100 の場合

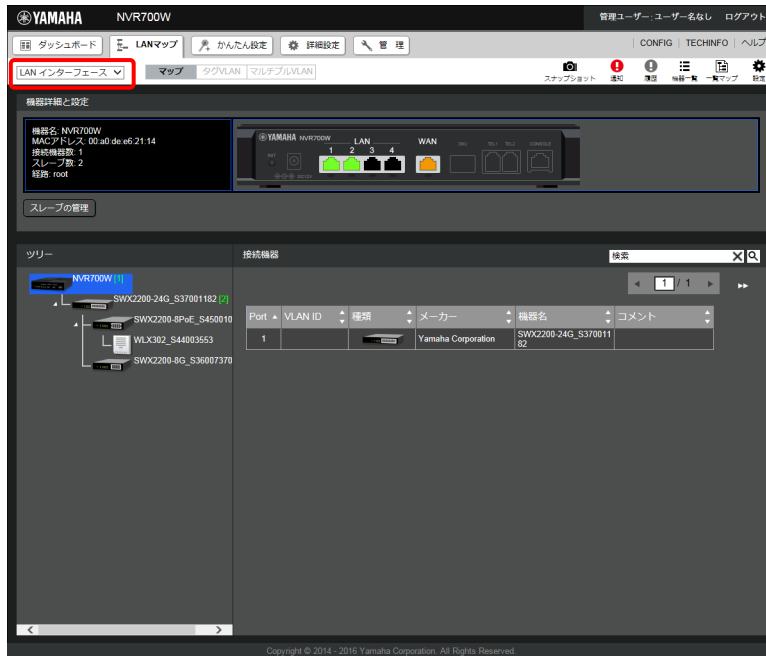
ヤマハスイッチ	できること	できないこと
SWX2100	<ul style="list-style-type: none"> <li>全ポートに共通の設定の表示</li> <li>フレームカウントのリセット</li> <li>ファームウェアの更新</li> <li>再起動</li> </ul>	<ul style="list-style-type: none"> <li>スイッチの設定変更</li> <li>スイッチの初期化</li> </ul>

## 第 11 章 LAN マップを利用する

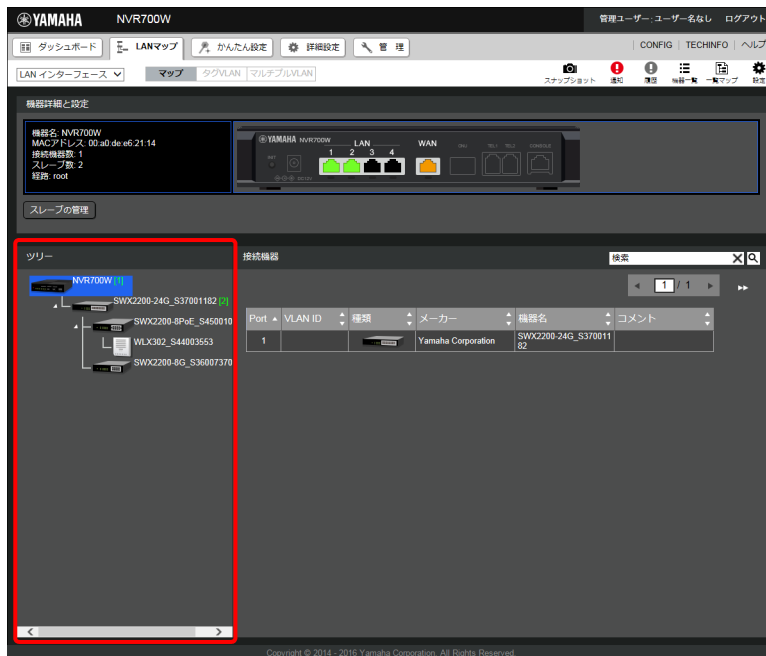
- ・ SWX2300 の場合

「スイッチの設定・保守」ボタンをクリックすると、Web 設定画面が別ウィンドウで表示され、設定を変更できます。

1. 設定・保守したいヤマハスイッチが接続されたインターフェースを、インターフェース選択プルダウンメニューから選択する。

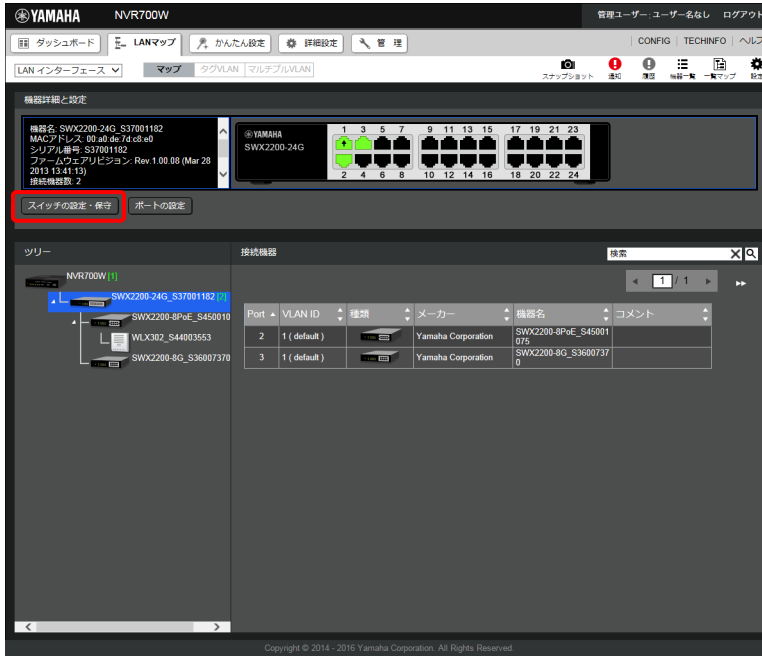


2. ツリービューでヤマハスイッチを選択する。



機器詳細と設定ビューと接続機器ビューの表示が切り替わります。

## 3. 機器詳細と設定ビューの「スイッチの設定・保守」ボタンをクリックする。



「スイッチの設定・保守」ダイアログが表示されます。

### スイッチの設定・保守

■ 機器名

SWX2200-24G\_S37001182 設定

■ 省電力機能

ノーマルモード 設定

■ ループ検出機能

ポートを自動シャットダウンしない 設定

■ ポートミラーリング機能

使用しない 設定

■ 保守

フレームカウンタをリセットする 進む

ファームウェアを更新する 進む

再起動を行う 進む

初期化を行う 進む

閉じる

## メモ

上記は、SWX2200の「スイッチの設定・保守」ダイアログです。SWX2100の場合、設定項目が異なります。

## 第 11 章 LAN マップを利用する

### 11.7.2 ヤマハスイッチの機器名を変更する

ヤマハスイッチの機器名を変更することができます。工場出荷時は、「機種名\_シリアル番号」という形式で機器名が付与されています。

1. 「スイッチの設定・保守」ダイアログを表示する。
2. 「機器名」項目の「設定」ボタンをクリックする。

スイッチの設定・保守

■ 機器名  
SWX2200-24G\_S37001182

■ 省電力機能  
ノーマルモード

■ ループ検出機能  
ポートを自動シャットダウンしない

■ ポートミラーリング機能  
使用しない

■ 保守  
フレームカウンタをリセットする   
ファームウェアを更新する   
再起動を行う   
初期化を行う

「機器名の設定」ダイアログが表示されます。

3. 任意の名称を入力し、「設定の確定」ボタンをクリックする。

機器名の設定

機器名  ※32文字以内

設定が反映され、「スイッチの設定・保守」ダイアログに戻ります。

### 11.7.3 省電力機能を設定する

省電力機能の設定を変更することができます。ヤマハスイッチには待機時の消費電力をカットする省電力機能が搭載され、動作モードをエコノミーモードに切り替えることで電力を節約することができます。

#### エコノミーモード時の動作

- ・ リンクダウンしているポートの待機電力の低減
- ・ ケーブル長検出による電力供給量の自動調節
- ・ ランプの明るさ調整

1. 「スイッチの設定・保守」ダイアログを表示する。



2. 「省電力機能」項目の「設定」ボタンをクリックする。

スイッチの設定・保守

■ 機器名  
SWX2200-24G\_S37001182 設定

■ 省電力機能  
ノーマルモード 設定

■ ループ検出機能  
ポートを自動シャットダウンしない 設定

■ ポートミラーリング機能  
使用しない 設定

■ 保守  
フレームカウンタをリセットする 進む  
ファームウェアを更新する 進む  
再起動を行う 進む  
初期化を行う 進む

閉じる

「省電力機能の設定」ダイアログが表示されます。

3. 動作モードでエコノミーモードを選択し、「設定の確定」ボタンをクリックする。

省電力機能の設定

この操作を行うと一時的にリンクダウンします。  
リンクダウン後に画面を再表示します。

動作モード  ノーマルモード  エコノミーモード

設定の確定 キャンセル

設定が反映され、「スイッチの設定・保守」ダイアログに戻ります。

#### 11.7.4 ループ検出機能を設定する

ループ検出機能の設定を変更することができます。ループ検出機能を有効にすると、誤ってループ状態が構成されブロードキャスト/マルチキャスト・ストームが発生した場合に自動的にループが発生したポートを一定時間シャットダウンすることができます。この動作により、ネットワーク全体が利用できなくなる状態を防ぐことができます。

1. 「スイッチの設定・保守」ダイアログを表示する。

## 第 11 章 LAN マップを利用する

### 2. 「ループ検出機能の設定」項目の「設定」ボタンをクリックする。

スイッチの設定・保守

■ 機器名  
SWX2200-24G\_S37001182 設定

■ 省電力機能  
ノーマルモード 設定

■ ループ検出機能  
ポートを自動シャットダウンしない 設定

■ ポートミラーリング機能  
使用しない 設定

■ 保守  
フレームカウンタをリセットする 進む  
ファームウェアを更新する 進む  
再起動を行う 進む  
初期化を行う 進む

閉じる

「ループ検出機能の設定」ダイアログが表示されます。

### 3. ループ検出機能を設定する。

ループ検出機能の設定

① MACアドレス移動回数閾値 3 回 (3-65535)

② ループ検出時の動作  
 ポートを自動シャットダウンして自動解除する  
300 秒 (1-98400)  
 ポートを自動シャットダウンしない

設定の確定 キャンセル

#### ① MAC アドレス移動回数閾値：

MAC アドレスのラーニング元ポートの移動回数の閾値を設定します。一定時間内にこの閾値に達するとループが発生したと判断されます。

#### ② ループ検出時の動作：

ループ検出時にポートを一定時間シャットダウンする場合は、「ポートを自動シャットダウンして自動解除する」を選択します。また、シャットダウンを解除する時間も設定します。

## メモ

「11.7.11 ポートの基本機能を設定する」（184 ページ）で、ループ検出機能を「使用する」に設定しているポートが対象となります。工場出荷状態ではすべてのポートで「使用する」が設定されています。

### 4. 「設定の確定」ボタンをクリックする。

設定が反映され、「スイッチの設定・保守」ダイアログに戻ります。

### 11.7.5 ポートミラーリング機能を設定する

ポートミラーリング機能の設定を変更することができます。ポートミラーリング機能を有効にすると、任意のポートのトラフィックを、指定したポートにコピーすることが可能になります。コピーされたパケットを採取することで通信状況の解析を行うことができます。

1. 「スイッチの設定・保守」ダイアログを表示する。
2. 「ポートミラーリング機能」項目の「設定」ボタンをクリックする。

スイッチの設定・保守

■ 機器名  
SWX2200-24G\_S37001182 設定

■ 省電力機能  
ノーマルモード 設定

■ ループ検出機能  
ポートを自動シャットダウンしない 設定

■ ポートミラーリング機能  
使用しない 設定

■ 保守  
フレームカウンタをリセットする 進む  
ファームウェアを更新する 進む  
再起動を行う 進む  
初期化を行う 進む

閉じる

「ポートミラーリング機能の設定」ダイアログが表示されます。

## 第 11 章 LAN マップを利用する

### 3. ポートミラーリング機能を設定する。

ポート番号	スニファポート	監視方向
1	<input checked="" type="radio"/>	監視しない
2	<input type="radio"/>	送信, 受信
3	<input type="radio"/>	送信
4	<input type="radio"/>	受信
5	<input type="radio"/>	監視しない
6	<input type="radio"/>	監視しない
7	<input type="radio"/>	監視しない
8	<input type="radio"/>	監視しない
9	<input type="radio"/>	監視しない
10	<input type="radio"/>	監視しない
11	<input type="radio"/>	監視しない
12	<input type="radio"/>	監視しない
13	<input type="radio"/>	監視しない
14	<input type="radio"/>	監視しない
15	<input type="radio"/>	監視しない
16	<input type="radio"/>	監視しない
17	<input type="radio"/>	監視しない
18	<input type="radio"/>	監視しない

#### ① 動作モード：

ポートミラーリング機能を使用するか否かを設定します。

#### ② スニファポート：

コピー先のポートを設定します。

#### ③ 監視方向：

各ポートのトラフィックの監視したい方向（コピーしたい方向）を設定します。

### 4. 「設定の確定」ボタンをクリックする。

設定が反映され、「スイッチの設定・保守」ダイアログに戻ります。

## 11.7.6 フレームカウンタをリセットする

「マップページ」の機器詳細と設定ビューで、機器画像内のポートを選択するとポートの情報が表示されます。その際に表示されるフレームカウンタ（統計情報）の値をリセットすることができます。

## メモ

フレームカウンタの設定について詳しくは、「11.7.13 フレームカウンタを設定する」（188 ページ）をご覧ください。

### 1. 「スイッチの設定・保守」ダイアログを表示する。

## 2. 「フレームカウンタをリセットする」欄の「進む」ボタンをクリックする。

スイッチの設定・保守

■ 機器名  
SWX2200-24G\_S37001182 設定

■ 省電力機能  
ノーマルモード 設定

■ ループ検出機能  
ポートを自動シャットダウンしない 設定

■ ポートミラーリング機能  
使用しない 設定

■ 保守

フレームカウンタをリセットする	進む
ファームウェアを更新する	進む
再起動を行う	進む
初期化を行う	進む

閉じる

「フレームカウンタをリセットする」ダイアログが表示されます。

## 3. 「実行」ボタンをクリックする。

フレームカウンタをリセットする

フレームカウンタをリセットします。

実行 キャンセル

フレームカウンタがリセットされ、「スイッチの設定・保守」ダイアログに戻ります。

## 11.7.7 ファームウェアを更新する

ヤマハスイッチのファームウェアを更新することができます。ヤマハスイッチでは市販の外部メモリ（USB メモリ / microSD カード）に保存したファームウェアをコントローラーに読み込ませて更新します。

## ご注意

- ・ ファームウェアの更新を始めたら、完了してヤマハスイッチが再起動するまで他の操作は絶対しないでください。万一、中断したときはヤマハスイッチが使えなくなることがあります。その場合は、持ち込み修理が必要となります。
- ・ ファームウェアの更新が完了すると、ヤマハスイッチは自動的に再起動されるため、すべての通信が切断されます。
- ・ ファームウェアの更新中は、絶対にケーブルを抜かないでください。ヤマハスイッチが使えなくなり、持ち込み修理が必要となる場合があります。
- ・ FAT または FAT32 形式でフォーマットされていない外部メモリは、コントローラーで使用できません。
- ・ USB ハブを介して、複数の USB メモリなどの外部メモリをコントローラーに接続することはできません。
- ・ コントローラーの USB ランプまたは microSD ランプが点灯 / 点滅している間は、外部メモリを取り外さないでください。外部メモリ内のデータを破損することがあります。USB ボタンまたは microSD ボタンを 2 秒間押し続けて、USB ランプまたは microSD ランプが消灯していることを確認してから外部メモリを取り外してください。

## 第 11 章 LAN マップを利用する

1. ヤマハスイッチのファームウェアを保存した外部メモリを用意する。
2. 外部メモリをコントローラーの USB ポートまたは microSD スロットに差し込む。
3. 「スイッチの設定・保守」ダイアログを表示する。
4. 「ファームウェアを更新する」欄の「進む」ボタンをクリックする。

スイッチの設定・保守

■ 機器名  
SWX2200-24G\_S37001182

■ 省電力機能  
ノーマルモード

■ ループ検出機能  
ポートを自動シャットダウンしない

■ ポートミラーリング機能  
使用しない

■ 保守

フレームカウンタをリセットする

ファームウェアを更新する

再起動を行う

初期化を行う

「ファームウェアを更新する」ダイアログが表示されます。

5. 外部メモリの種類を選択し、「参照」ボタンをクリックする。

ファームウェアを更新する

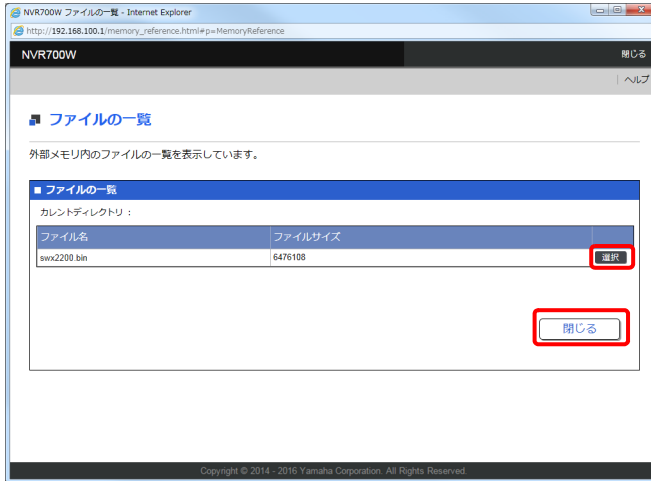
ファームウェアの更新を行います。  
この操作には数十秒かかります。その間、他の操作は絶対しないでください。  
ファームウェアの更新を行った後、自動で再起動します。  
この操作を行うと一時的にリンクダウンします。  
リンクダウン後に画面を再表示します。

ファームウェアファイルの指定

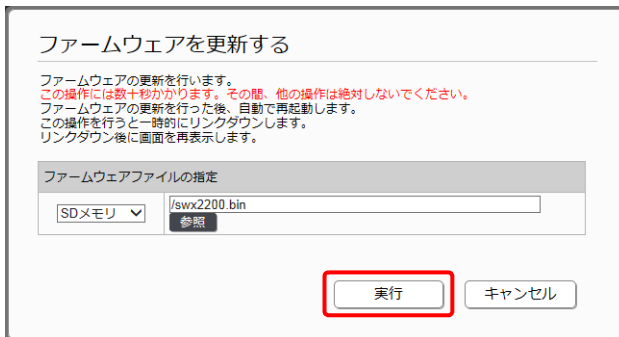
SDメモリ

「ファイルの一覧」画面が表示されます。

6. 更新に使用するファームウェアを選択し、「閉じる」ボタンをクリックする。



7. 「実行」ボタンをクリックする。



ファームウェアの更新が開始されます。ファームウェアの更新が終了すると、ヤマハスイッチは自動的に再起動します。

## 第 11 章 LAN マップを利用する

### 11.7.8 ヤマハスイッチを再起動する

ヤマハスイッチを再起動することができます。

1. 「スイッチの設定・保守」ダイアログを表示する。
2. 「再起動を行う」欄の「進む」ボタンをクリックする。

スイッチの設定・保守

■ 機器名  
SWX2200-24G\_S37001182

■ 省電力機能  
ノーマルモード

■ ループ検出機能  
ポートを自動シャットダウンしない

■ ポートミラーリング機能  
使用しない

■ 保守

フレームカウンタをリセットする	<input type="button" value="進む"/>
ファームウェアを更新する	<input type="button" value="進む"/>
再起動を行う	<input type="button" value="進む"/>
初期化を行う	<input type="button" value="進む"/>

「再起動を行う」ダイアログが表示されます。

3. 「実行」ボタンをクリックする。

再起動を行う

再起動を行います。  
この操作を行うと一時的にリンクダウンします。  
リンクダウン後に画面を再表示します。

ヤマハスイッチが再起動されます。



### 11.7.9 ヤマハスイッチを初期化する

ヤマハスイッチの設定内容を工場出荷状態に戻すことができます。

1. 「スイッチの設定・保守」ダイアログを表示する。
2. 「初期化を行う」欄の「進む」ボタンをクリックする。

スイッチの設定・保守

■ 機器名  
SWX2200-24G\_S37001182

■ 省電力機能  
ノーマルモード

■ ループ検出機能  
ポートを自動シャットダウンしない

■ ポートミラーリング機能  
使用しない

■ 保守

フレームカウンタをリセットする	<input type="button" value="進む"/>
ファームウェアを更新する	<input type="button" value="進む"/>
再起動を行う	<input type="button" value="進む"/>
初期化を行う	<input type="button" value="進む"/>

「初期化を行う」ダイアログが表示されます。

3. 「実行」ボタンをクリックする。

初期化を行う

初期化を行います。  
この操作には数十秒かかります。

ヤマハスイッチが初期化されます。

## 第 11 章 LAN マップを利用する

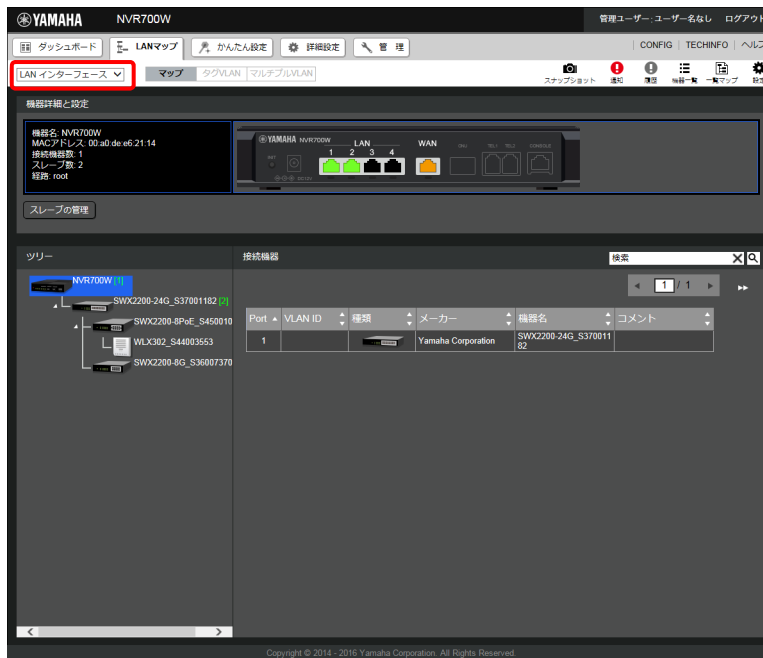
### 11.7.10 ポートの設定ダイアログを表示する

ヤマハスイッチのポートごとの設定を行うための「ポートの設定」ダイアログを表示します。

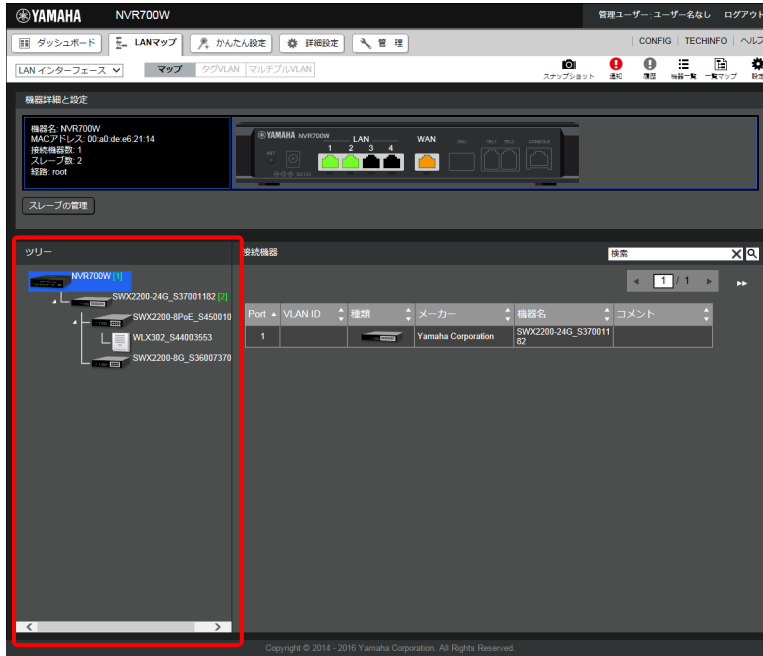
#### ご注意

ポートの設定は、SWX2200 をお使いの場合に設定できます。SWX2100 および SWX2300 では設定できません。

1. ポートの設定を行いたいヤマハスイッチが接続されたインターフェースを、インターフェース選択プルダウンメニューから選択する。

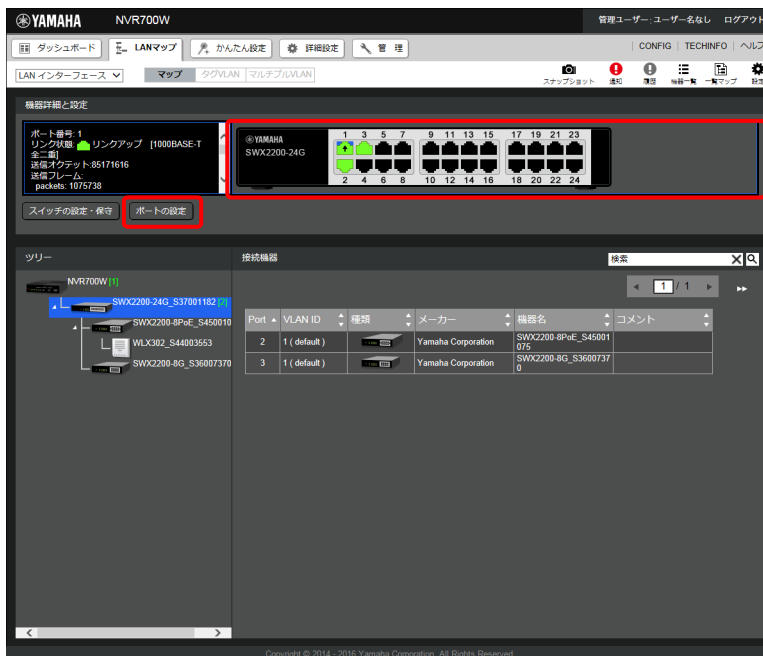


## 2. ツリービューでヤマハスイッチを選択する。



機器詳細と設定ビューと接続機器ビューの表示が切り替わります。

## 3. 機器詳細と設定ビューで設定するポートを選択し、「ポートの設定」ボタンをクリックする。



## 第 11 章 LAN マップを利用する

「ポートの設定」ダイアログが表示されます。

### ポート1の設定

■ 基本機能

設定項目	設定値	
ポートの動作		
クロスストレート自動判別	使用しない	
速度		設定
リンクスピードダウンシフト		
フロー制御		
ループ検出機能		

■ QoS

設定項目	設定値	
DSCPリマーカーキング		
送信シェーピング		設定
受信ポリシング		

■ タグVLAN

設定項目	設定値	
動作モード	アクセス	
アクセスVLAN ID	1 (default)	設定
トランクVLAN ID	-	

■ マルチプルVLAN

設定項目	設定値	
参加グループ	なし	設定

■ フレームカウンタ

設定項目	設定値	
------	-----	--

閉じる

### 11.7.11 ポートの基本機能を設定する

ポートごとに下記の設定を行うことができます。

- ・ ポートの動作
- ・ クロスストレート自動判別
- ・ 速度
- ・ リンクスピードダウンシフト
- ・ フロー制御
- ・ ループ検出機能

1. 「ポートの設定」ダイアログを表示する。

## 2. 「基本機能」項目の「設定」ボタンをクリックする。

ポート1の設定

■ 基本機能

設定項目	設定値	
ポートの動作		
クロスストレート自動判別	使用しない	
速度		<b>設定</b>
リンクスピードダウンシフト		
フロー制御		
ループ検出機能		

■ QoS

設定項目	設定値	
DSCPリマーカーキング		
送信シェーピング		<b>設定</b>
受信ポリシング		

■ タグVLAN

設定項目	設定値	
動作モード	アクセス	
アクセスVLAN ID	1 (default)	<b>設定</b>
トランクVLAN ID	-	

■ マルチプルVLAN

設定項目	設定値	
参加グループ	なし	<b>設定</b>

■ フレームカウンタ

設定項目	設定値	

閉じる

「基本機能の設定」ダイアログが表示されます。

## 3. ポートの基本機能を設定する。

基本機能の設定

この操作を行うと一時的にリンクダウンします。  
リンクダウン後に画面を再表示します。

① ポート動作	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
② クロスストレート自動判別	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
③ 速度	自動判別(auto) ▼
④ リンクスピードダウンシフト	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
⑤ フロー制御	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
⑥ ループ検出機能	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない

設定の確定      キャンセル

## ① ポートの動作：

ポートを使用するか否かを設定します。

## 第 11 章 LAN マップを利用する

### ② クロストレート自動判別：

LAN ケーブルの種類の自動判別機能を使用するか否かを設定します。

### ③ 速度：

ポートの速度を選択します。

### ④ リンクスピードダウンシフト：

速度ダウンシフト機能を使用するか否かを設定します。

### ⑤ フロー制御：

フロー制御機能を使用するか否かを設定します。

### ⑥ ループ検出機能：

ループ検出機能を使用するか否かを設定します。

#### 4. 「設定の確定」 ボタンをクリックする。

設定が反映され、「ポートの設定」 ダイアログが表示されます。

### 11.7.12 QoS 機能を設定する

QoS 機能の設定を変更することができます。ポートごとにポートを経由するパケットに DSCP 値を付加することで優先度を指定します。また、ポートごとに送信帯域や受信帯域を指定できます。

#### 1. 「ポートの設定」 ダイアログを表示する。

#### 2. 「QoS」 項目の「設定」 ボタンをクリックする。

ポート1の設定

■ 基本機能

設定項目	設定値	
ポートの動作		
クロストレート自動判別	使用しない	
速度		設定
リンクスピードダウンシフト		
フロー制御		
ループ検出機能		

■ QoS

設定項目	設定値	
DSCPリマーカーキング		
送信シェーピング		設定
受信ポリシング		

■ タグVLAN

設定項目	設定値	
動作モード	アクセス	
アクセスVLAN ID	1 (default)	設定
トランクVLAN ID	-	

■ マルチプルVLAN

設定項目	設定値	
参加グループ	なし	設定

■ フレームカウンタ

設定項目	設定値	
------	-----	--

閉じる

「QoS 機能の設定」 ダイアログが表示されます。

## 3. QoS 機能を設定する。

QoS機能の設定	
① DSCPリマーキング	使用しない ▼
② 送信シェーピング	使用しない ▼
③ 受信ポリシング	使用しない ▼

設定の確定    キャンセル

- ① **DSCP リマーキング**：  
DSCP 値に設定する優先度を選択します。
- ② **送信シェーピング**：  
送信帯域を選択します。
- ③ **受信ポリシング**：  
受信帯域を選択します。

**メモ**

送信シェーピングと受信ポリシングは、SWX2200-24G のみで設定できます。

## 4. 「設定の確定」 ボタンをクリックする。

設定が反映され、「ポートの設定」 ダイアログが表示されます。

## 第 11 章 LAN マップを利用する

### 11.7.13 フレームカウンタを設定する

フレームカウンタの設定を変更することができます。「マップページ」の機器詳細と設定ビューで、機器画像内のポートを選択するとポートの情報が表示されます。その際に表示されるフレームカウンタ（統計情報）にどの情報を表示するかを設定することができます。

1. 「ポートの設定」ダイアログを表示する。
2. 「フレームカウンタ」項目の「設定」ボタンをクリックする。

ポート1の設定

設定項目	設定値	
DSCPリマーカーキング		
送信シェーピング		設定
受信ポリシング		

■ タグVLAN

設定項目	設定値	
動作モード	アクセス	
アクセスVLAN ID	1 (default)	設定
トランクVLAN ID	-	

■ マルチプルVLAN

設定項目	設定値	
参加グループ	なし	設定

■ フレームカウンタ

設定項目	設定値	
送信フレーム	カウンタ1	packets
	カウンタ2	total-good-packets
	カウンタ3	total-error-packets
	カウンタ4	fifo-drops
	カウンタ5	collisions
受信フレーム	カウンタ1	packets
	カウンタ2	total-good-packets
	カウンタ3	total-error-packets
	カウンタ4	fifo-drops
	カウンタ5	crc-align-errors

閉じる

「フレームカウンタの設定」ダイアログが表示されます。



## 3. フレームカウンタの表示情報を設定する。

フレームカウンタの設定

■ 送信フレーム

① カウンタ1	packets
カウンタ2	total-good-packets
カウンタ3	total-error-packets
カウンタ4	fifo-drops
カウンタ5	collisions

■ 受信フレーム

② カウンタ1	packets
カウンタ2	total-good-packets
カウンタ3	total-error-packets
カウンタ4	fifo-drops
カウンタ5	crc-align-errors

設定の確定      キャンセル

① 送信フレーム：  
カウンタ 1 ～ 5 のそれぞれで表示する種別を設定します。

② 受信フレーム：  
カウンタ 1 ～ 5 のそれぞれで表示する種別を設定します。

## メモ

SWX2200-24G のみカウンタが 5 個設定できます。SWX2200-8G は 3 個まで設定できます。

## 4. 「設定の確定」ボタンをクリックする。

設定が反映され、「ポートの設定」ダイアログが表示されます。

## 11.7.14 LAN ケーブル二重化機能を設定する

LAN ケーブル二重化機能を設定することができます。コントローラーとヤマハスイッチの間で LAN ケーブルを二重化し、ネットワークの信頼性を向上させる機能です。二重化することで、主ケーブルの断線や抜けによって接続が切れてしまったときに、自動的にバックアップケーブルがリンクアップして、ネットワークを継続して利用することができます。

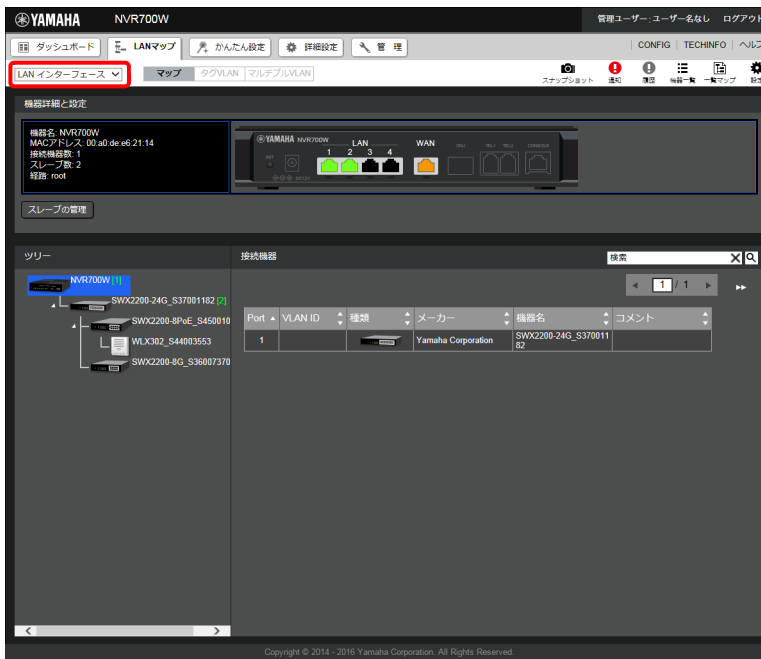
本機能では主ケーブルが接続されている機器間のことをマスター経路、バックアップケーブルが接続されている機器間のことをバックアップ経路と呼びます。

## ご注意

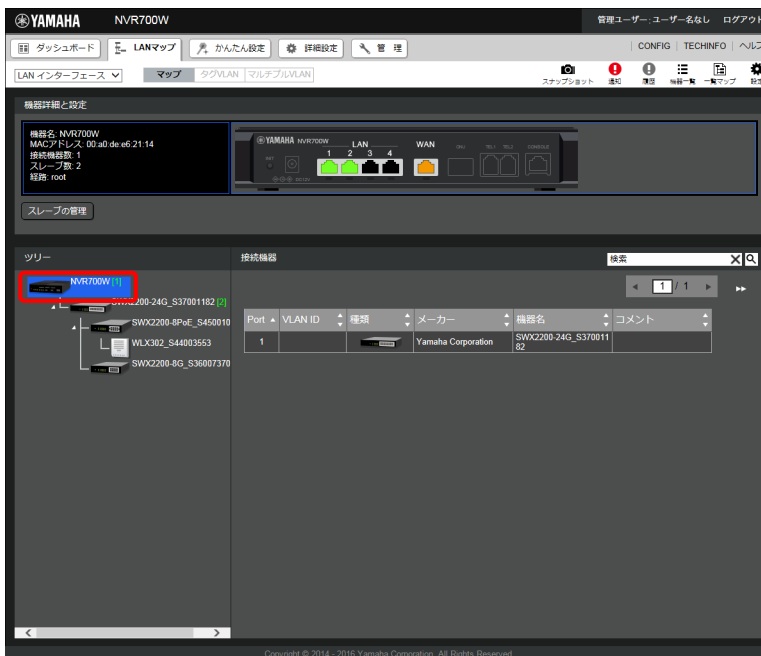
- ・ 本機能の設定前にバックアップ経路にケーブルを接続するとループが発生してしまうことがあります。ケーブルの接続は、本機能の設定後に行ってください。
- ・ LAN ケーブル二重化機能の設定は、設定対象の機器がコントローラー、あるいは SWX2200 のダウンリンクポートに接続されている場合のみ設定できます。

## 第 11 章 LAN マップを利用する

1. 対象のヤマハスイッチが接続されたインターフェースを、インターフェース選択プルダウンメニューから選択する。

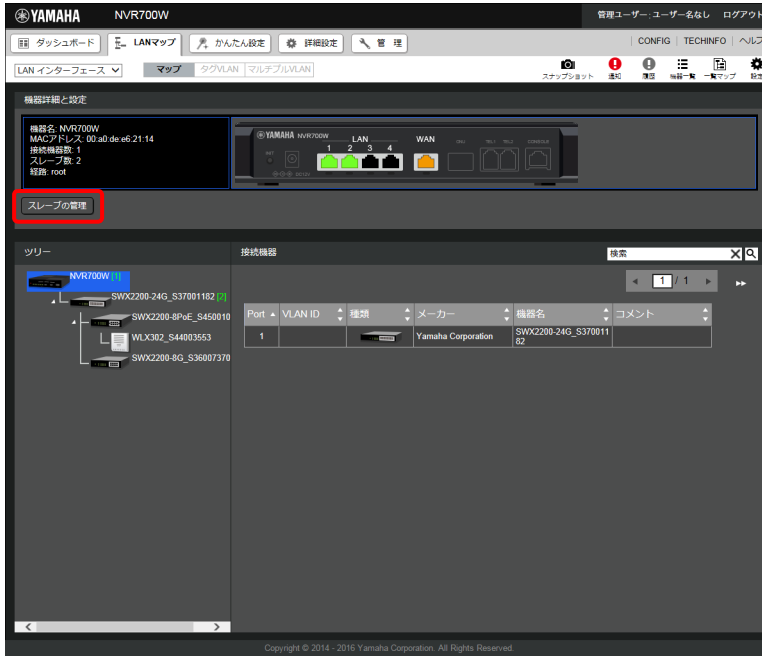


2. ツリービューでコントローラーを選択する。



機器詳細と設定ビューと接続機器ビューの表示が切り替わります。

## 3. 機器詳細と設定ビューの「スレーブの管理」ボタンをクリックする。



「スレーブの管理」ダイアログが表示されます。

## 4. 「スイッチの管理」項目の「バックアップ経路」欄の「設定」ボタンをクリックする。



「バックアップ経路の設定」ダイアログが表示されます。

## 第 11 章 LAN マップを利用する

### 5. バックアップ経路を設定する。

バックアップ経路の設定

バックアップ経路の設定を行います。  
この操作を行うと一時的にリンクダウンします。

マスター経路	lan1:1
① バックアップ経路	<input type="radio"/> 設定しない <input checked="" type="radio"/> 設定する lan1:2

設定の確定      キャンセル

#### ① バックアップ経路：

バックアップ経路を設定するか否かを設定します。「設定する」を選択した場合は、バックアップ経路に設定するポートを選択します。

### 6. 「設定の確定」ボタンをクリックする。

「完了」ダイアログが表示されます。

### 7. 「閉じる」ボタンをクリックする。

完了

設定を完了しました。

スイッチの設定反映には数十秒かかる場合があります。  
しばらく待ってから「スレーブの管理」画面を開いて、設定が反映されていることを確認してください。

閉じる

「スレーブの管理」ダイアログが表示されます。また、設定の反映には数十秒かかる場合があります。

## 11.7.15 スイッチの指定方法を選択する

ヤマハスイッチの設定は自動的にコントローラー内に保存されますが、その際にスイッチを経路で指定して管理するのか、MAC アドレスで指定して管理するのかをスイッチごとに選択することができます。経路指定で管理しているスイッチは、故障した場合でも新しいスイッチにリプレースするだけでリプレース前のスイッチと同じ設定が自動的に復元されます。

### 経路での管理

スイッチを経路と紐付けて管理します。故障などの理由でスイッチをリプレースした場合でも、同じ経路上に設置した新しいスイッチに対して、リプレース前の旧スイッチと同じ設定が自動的に復元されます。

### MAC アドレスでの管理

スイッチを MAC アドレスと紐付けて管理します。スイッチの設置場所（経路）を変更しても、スイッチの設定は変更されません。

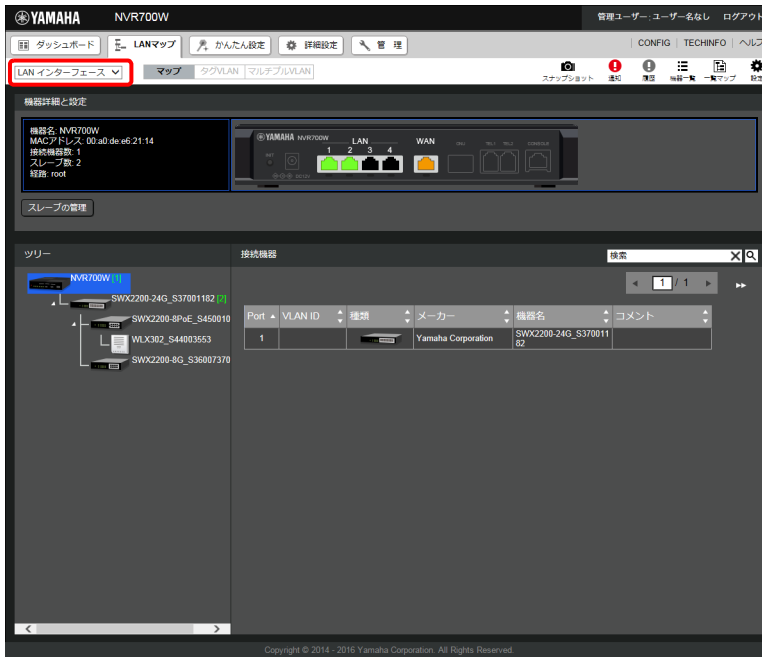
### ご注意

- ・ SWX2100 および SWX2300 の場合はコントローラー内にスイッチの設定が保存されないため、設定の復元は行われず、スイッチの指定方法の変更もできません。

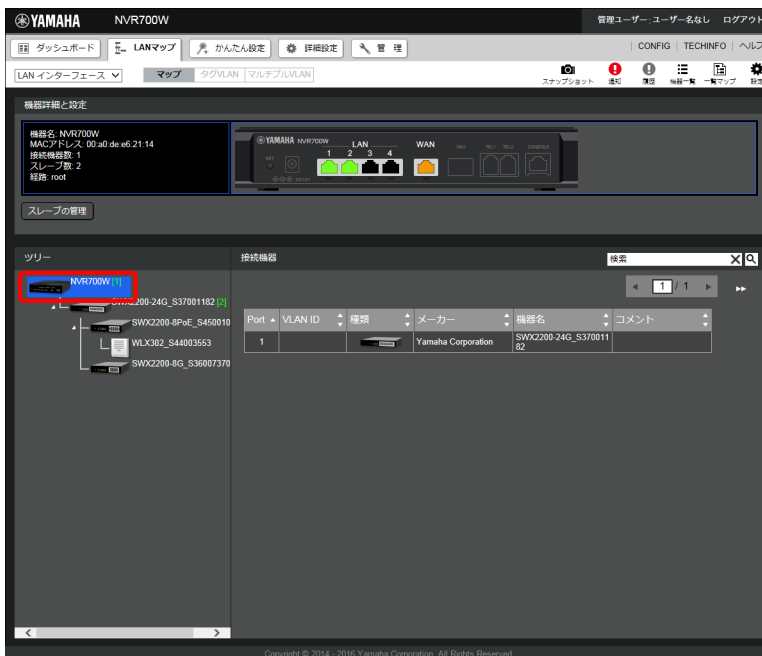
### メモ

工場出荷状態では MAC アドレスで指定されています。

1. 対象のヤマハスイッチが接続されたインターフェースを、インターフェース選択プルダウンメニューから選択する。



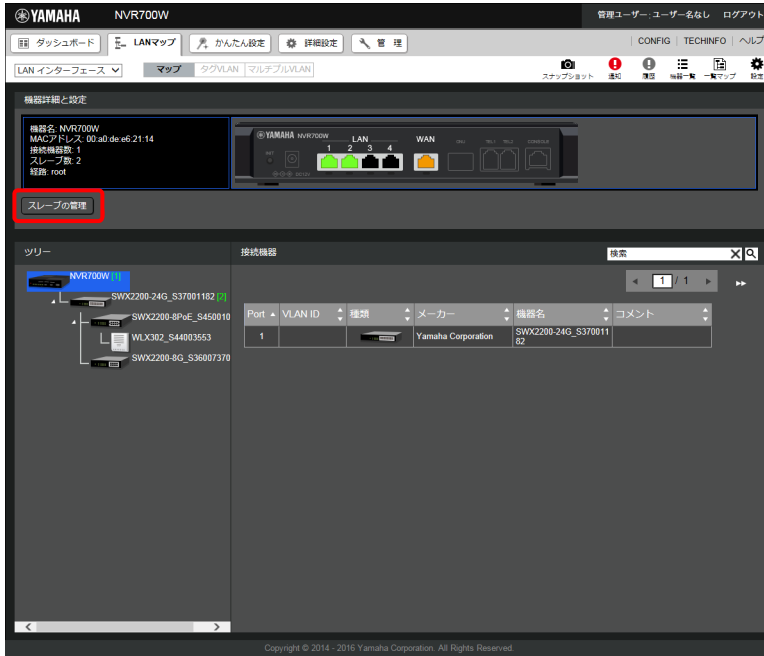
2. ツリービューでコントローラーを選択する。



機器詳細と設定ビューと接続機器ビューの表示が切り替わります。

## 第 11 章 LAN マップを利用する

### 3. 機器詳細と設定ビューの「スレーブの管理」ボタンをクリックする。



「スレーブの管理」ダイアログが表示されます。

### 4. 「スイッチの管理」項目の「スイッチの指定方法」欄の「設定」ボタンをクリックする。



「指定方法の変更」ダイアログが表示されます。

## 5. 「設定の確定」 ボタンをクリックする。

指定方法の変更

指定方法を経路指定(lan1:1)に変更しますか？

設定の確定
キャンセル

「設定の確定」 ボタンをクリックするたびに、「経路指定」と「MAC アドレス指定」が交互に切り替わります。

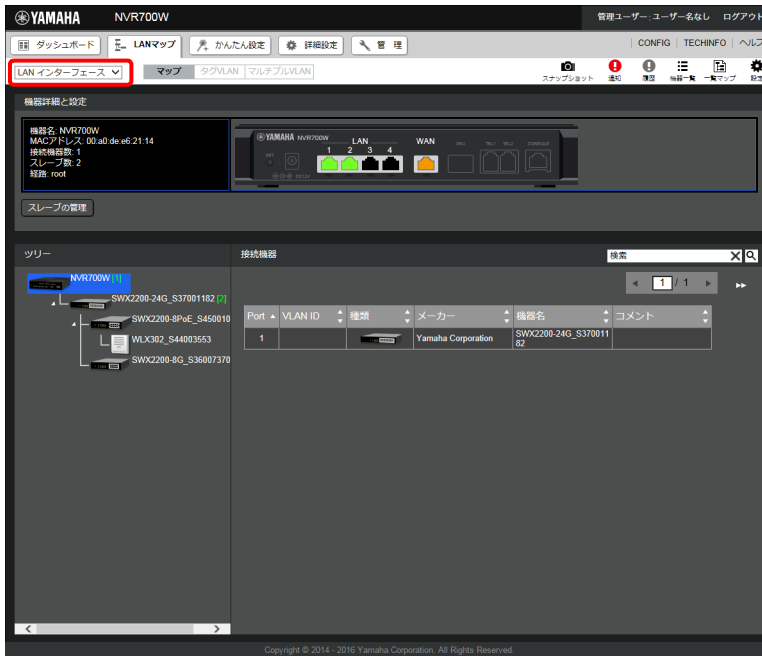
## 11.8 ヤマハ無線 AP の設定を行う

ヤマハ無線 AP の設定方法を説明します。

### 11.8.1 IP アドレスを変更する

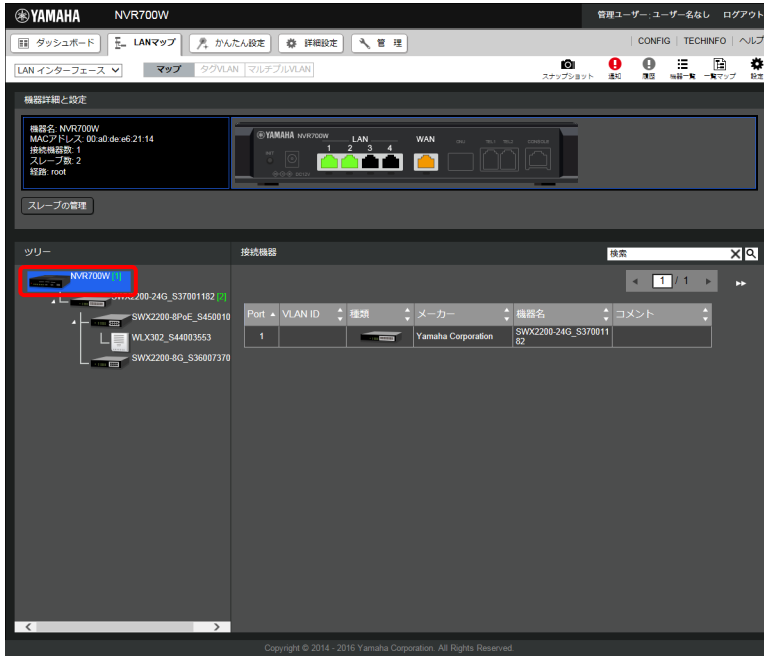
ヤマハ無線 AP の IP アドレスを変更することができます。

1. 設定したいヤマハ無線 AP が接続されたインターフェースを、インターフェース選択プルダウンメニューから選択する。



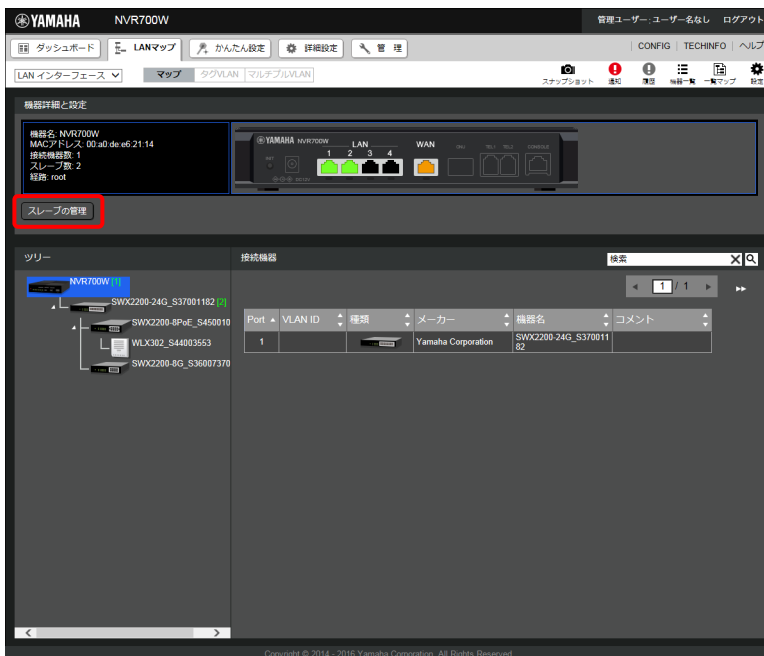
## 第 11 章 LAN マップを利用する

### 2. ツリービューでコントローラーを選択する。



機器詳細と設定ビューと接続機器ビューの表示が切り替わります。

### 3. 機器詳細と設定ビューの「スレーブの管理」ボタンをクリックする。



「スレーブの管理」ダイアログが表示されます。



## 4. 「無線 AP の管理」項目の「IP アドレス」欄の「設定」ボタンをクリックする。

スレーブの管理

■ スイッチの管理

機器名	機種名	経路	バックアップ経路	スイッチの指定方法
SWX2200-24G_S37001182	SWX2200-24G	lan1:1	- 設定	MACアドレス (00.a0.de.7d.c8.e0) 設定
SWX2200-8PoE_S45001075	SWX2200-8PoE	lan1:1-2	- 設定	MACアドレス (00.a0.de.84.2c.35) 設定
SWX2200-8G_S36007370	SWX2200-8G	lan1:1-3	- 設定	MACアドレス (00.a0.de.82.bb.75) 設定

■ 無線APの管理

無線APのCONFIGの一括操作

機器名	機種名	IPアドレス	経路	CONFIG	無線APの指定方法
WLX302_S44003553	WLX302	192.168.100.3 設定	lan1:1-2-2	- <input type="button" value="保存"/> <input type="button" value="復元"/> <input type="button" value="削除"/>	MACアドレス (00.a0.de.97.f2.a0) 設定

「IP アドレスの設定」ダイアログが表示されます。

## 5. IP アドレスを設定する。

IPアドレスの設定

① VLAN ID

② IPアドレス  
 DHCPで自動的に取得する  
 固定のアドレスを設定する  
 /

## ① VLAN ID :

VLAN ID を入力します。

## ② IP アドレス :

IP アドレスを DHCP から取得するか、固定 IP アドレスを設定するかを設定します。

- ・ DHCP で自動的に取得する：DHCP から IP アドレスを取得する場合に選択します。
- ・ 固定のアドレスを設定する：固定の IP アドレスを設定する場合に選択し、IP アドレスを入力します。

## 6. 「設定の確定」ボタンをクリックする。

IP アドレスが変更され、「スレーブの管理」ダイアログが表示されます。

### 11.8.2 無線 AP の指定方法を選択する

ヤマハ無線 AP の設定 (CONFIG) は手動でコントローラー内に保存することができますが、その際に無線 AP を経路で指定して管理するのか、MAC アドレスで指定して管理するのかを無線 AP ごとに選択することができます。コントローラー内に無線 AP の設定 (CONFIG) を保存しておけば、無線 AP をリプレースする際に、リプレース前の旧無線 AP と同じ設定 (CONFIG) を簡単な操作で復元させることができます。

#### 経路での管理

無線 AP を経路と紐付けて管理します。故障などの理由で無線 AP をリプレースした場合でも、同じ経路上に設置した新しい無線 AP に対して、リプレース前の旧無線 AP と同じ設定 (CONFIG) を簡単な操作で復元させることができます。

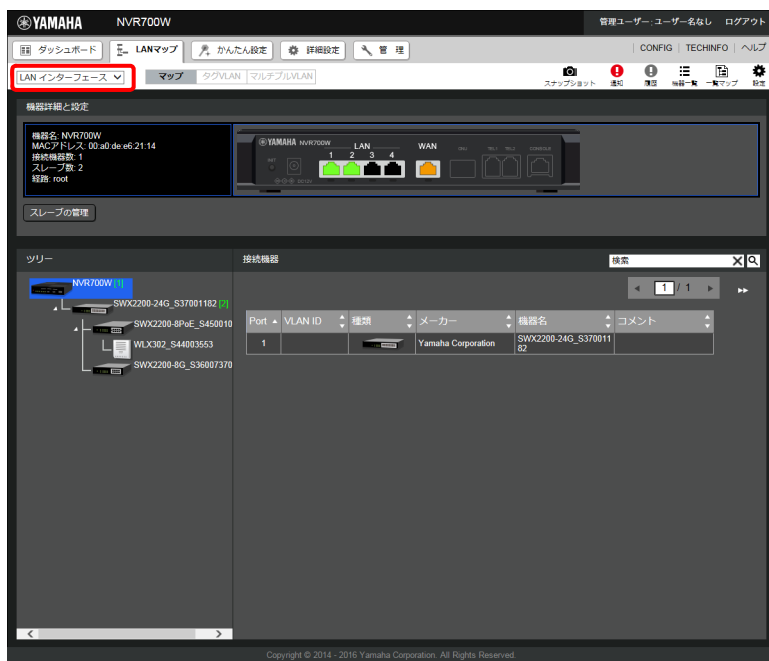
#### MAC アドレスでの管理

無線 AP を MAC アドレスと紐付けて管理します。コントローラーに保存されている設定 (CONFIG) ファイルは対象の無線 AP (MAC アドレスが同一の無線 AP) のみにしか復元できません。

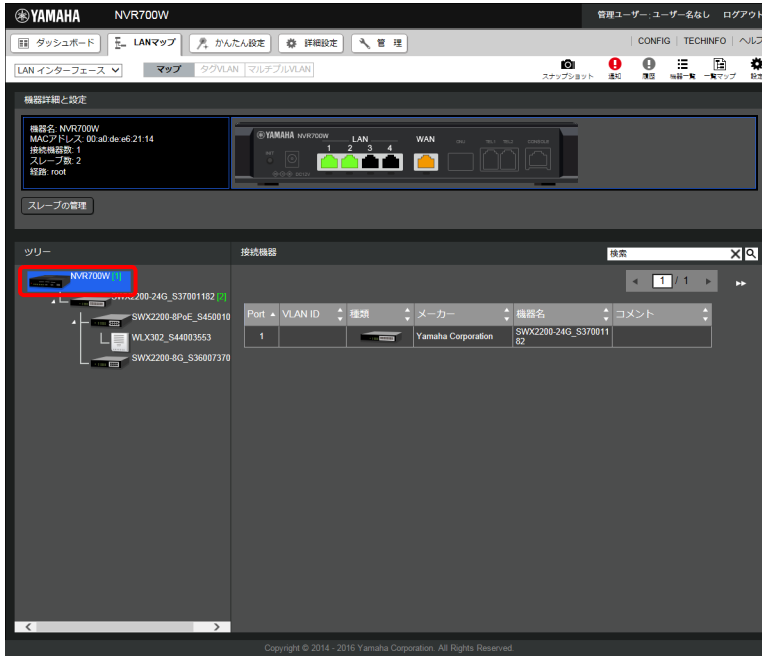
#### メモ

工場出荷状態では MAC アドレスで指定されています。

1. 設定したいヤマハ無線 AP が接続されたインターフェースを、インターフェース選択プルダウンメニューから選択する。

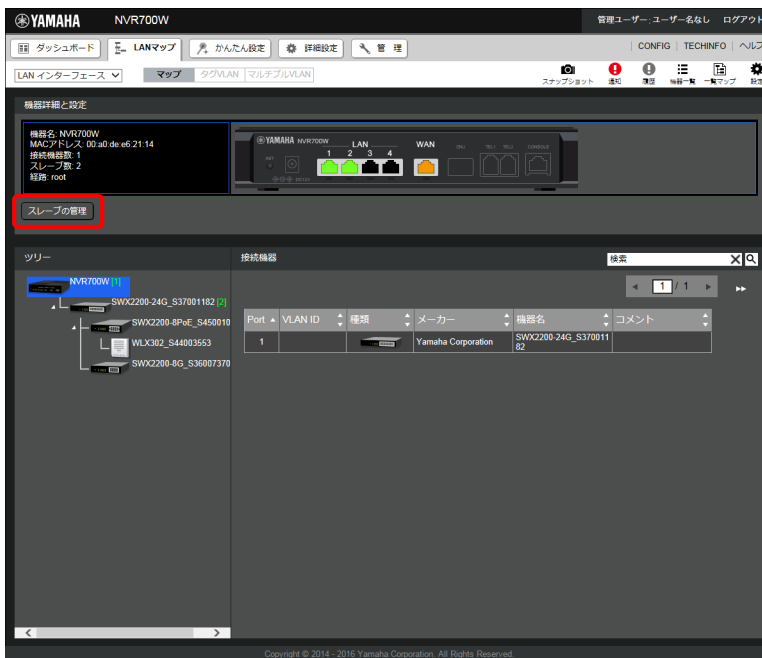


## 2. ツリービューでコントローラーを選択する。



機器詳細と設定ビューと接続機器ビューの表示が切り替わります。

## 3. 機器詳細と設定ビューの「スレーブの管理」ボタンをクリックする。



「スレーブの管理」ダイアログが表示されます。

## 第 11 章 LAN マップを利用する

4. 「無線 AP の管理」項目の「無線 AP の指定方法」欄の「設定」ボタンをクリックする。

スレーブの管理

■ スイッチの管理

機器名	機種名	経路	バックアップ経路	スイッチの指定方法
SWX2200-24G_S37001182	SWX2200-24G	lan1:1	- 設定	MACアドレス (00:a0:de:7d:c8:e0) 設定
SWX2200-8PoE_S45001075	SWX2200-8PoE	lan1:1-2	- 設定	MACアドレス (00:a0:de:84:2c:35) 設定
SWX2200-8G_S36007370	SWX2200-8G	lan1:1-3	- 設定	MACアドレス (00:a0:de:82:bb:75) 設定

■ 無線APの管理

無線APのCONFIGの一括操作

機器名	機種名	IPアドレス	経路	CONFIG	無線APの指定方法
WLX302_S44003553	WLX302	192.168.100.3 設定	lan1:1-2-2	- <input type="button" value="保存"/> <input type="button" value="復元"/> <input type="button" value="削除"/>	MACアドレス (00:a0:de:97:f2:a0) 設定

「指定方法の変更」ダイアログが表示されます。

5. 「設定の確定」ボタンをクリックする。

指定方法の変更

指定方法を経路指定(lan1:1-2-2)に変更しますか？

「設定の確定」ボタンをクリックするたびに、「経路指定」と「MAC アドレス指定」が交互に切り替わります。

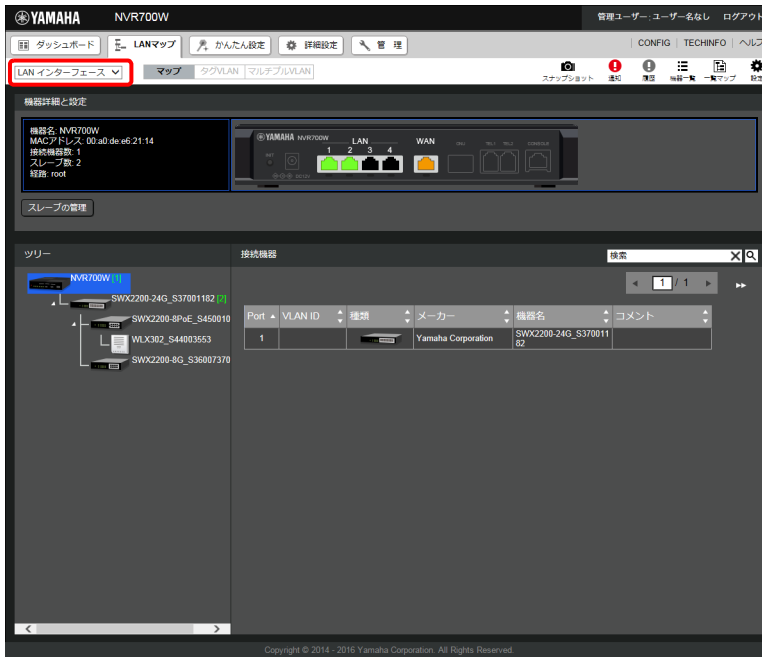
### 11.8.3 設定 (CONFIG) を保存する

ヤマハ無線 AP の設定 (CONFIG) をコントローラー内に保存します。

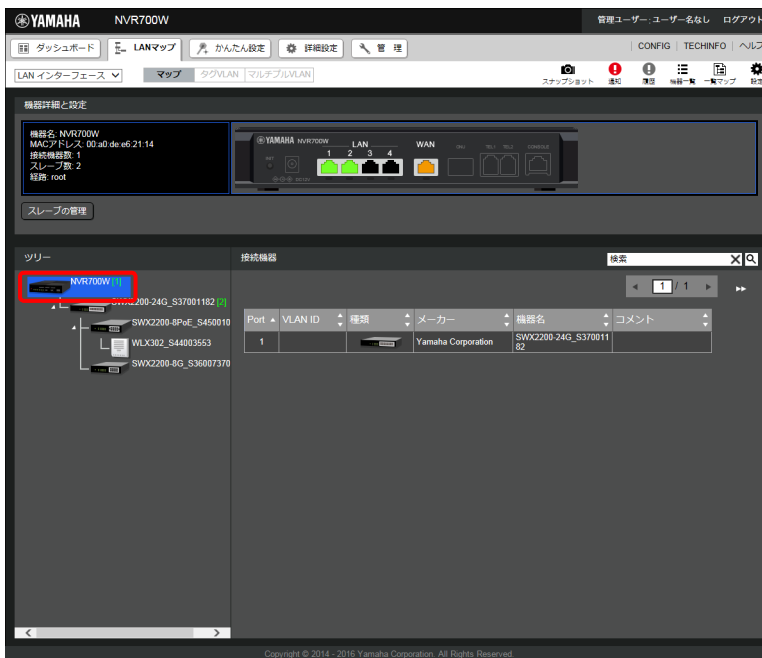
#### ご注意

ヤマハ無線 AP はヤマハスイッチと異なり、自動ではコントローラー内に設定が保存されません。

1. 設定 (CONFIG) を保存したいヤマハ無線 AP が接続されたインターフェースを、インターフェース選択プルダウンメニューから選択する。



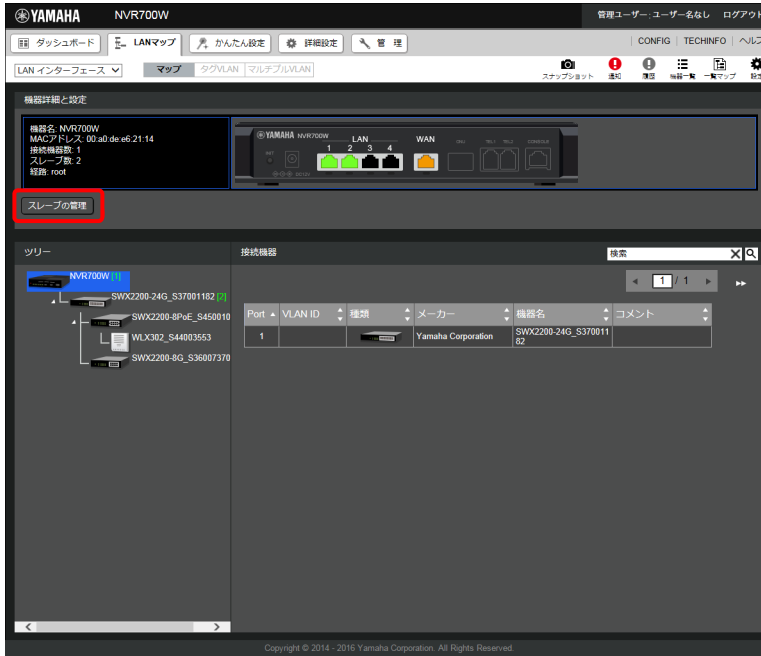
2. ツリービューでコントローラーを選択する。



機器詳細と設定ビューと接続機器ビューの表示が切り替わります。

## 第 11 章 LAN マップを利用する

### 3. 機器詳細と設定ビューの「スレーブの管理」ボタンをクリックする。



「スレーブの管理」ダイアログが表示されます。

### 4. 「無線 AP の管理」項目の「CONFIG」欄の「保存」ボタンをクリックする。

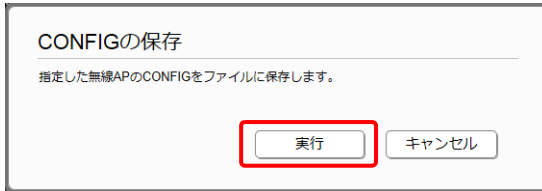


「CONFIG の保存」ダイアログが表示されます。

## メモ

ネットワーク内のすべてのヤマハ無線 AP の設定 (CONFIG) を保存するときは、「無線 AP の CONFIG の一括操作」欄の「保存」ボタンをクリックします。

## 5. 「実行」 ボタンをクリックする。



設定 (CONFIG) が保存され、「スレーブの管理」ダイアログが表示されます。

## 11.8.4 設定 (CONFIG) を復元する

コントローラー内に保存した設定 (CONFIG) から、ヤマハ無線 AP の設定を復元します。

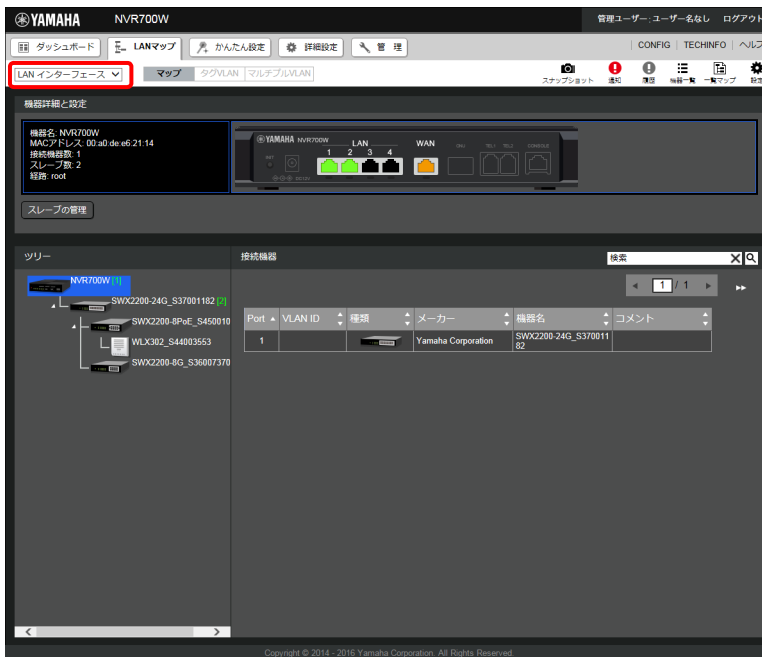
## ご注意

コントローラー内に設定 (CONFIG) が保存されていない場合は、復元することはできません。

## メモ

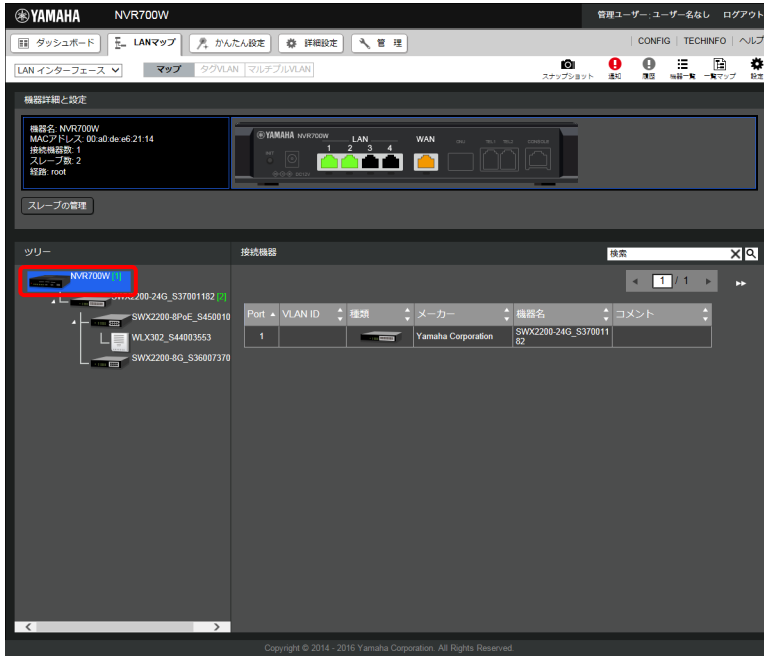
- ・ ヤマハ無線 AP の設定の復元は、「11.8.2 無線 AP の指定方法を選択する」(198 ページ) で指定したヤマハ無線 AP に対して実行されます。
- ・ 「11.8.2 無線 AP の指定方法を選択する」(198 ページ) で指定したヤマハ無線 AP の設定 (CONFIG) がコントローラー内に保存されている場合、対象のヤマハ無線 AP が工場出荷状態であれば設定 (CONFIG) が自動的に復元されます。工場出荷状態でない場合は、本章の復元操作を行う必要があります。

1. 設定 (CONFIG) を復元したいヤマハ無線 AP が接続されたインターフェースを、インターフェース選択プルダウンメニューから選択する。



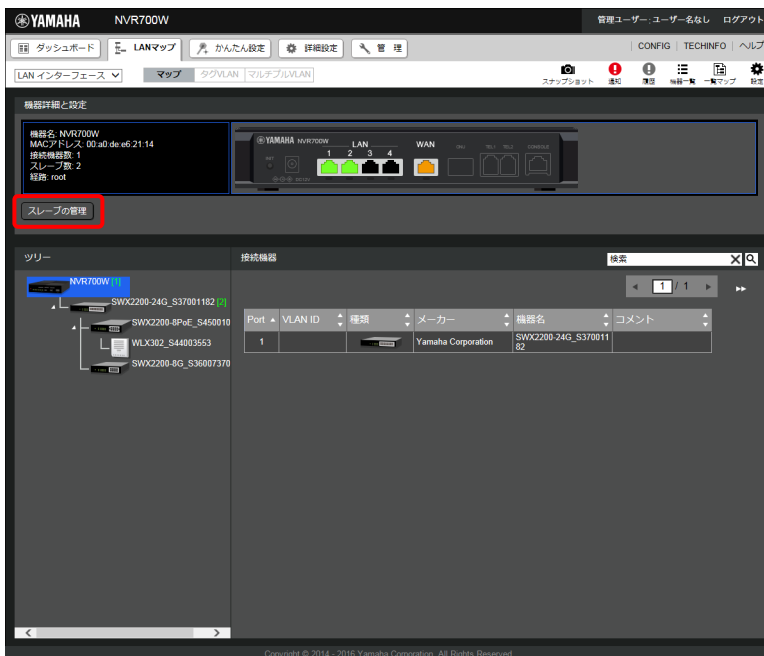
## 第 11 章 LAN マップを利用する

### 2. ツリービューでコントローラーを選択する。



機器詳細と設定ビューと接続機器ビューの表示が切り替わります。

### 3. 機器詳細と設定ビューの「スレーブの管理」ボタンをクリックする。



「スレーブの管理」ダイアログが表示されます。



4. 「無線 AP の管理」項目の「CONFIG」欄の「復元」ボタンをクリックする。

スレーブの管理

■ スイッチの管理

機器名	機種名	経路	バックアップ経路	スイッチの指定方法
SWX2200-24G_S37001182	SWX2200-24G	lan1:1	設定	MACアドレス (00:a0:de:7d:c8:e0) 設定
SWX2200-8PoE_S45001075	SWX2200-8PoE	lan1:1-2	設定	MACアドレス (00:a0:de:84:2c:35) 設定
SWX2200-8G_S36007370	SWX2200-8G	lan1:1-3	設定	MACアドレス (00:a0:de:82:bb:75) 設定

■ 無線APの管理

無線APのCONFIGの一括操作 **保存** **復元** **削除**

機器名	機種名	IPアドレス	経路	CONFIG	無線APの指定方法
WLX302_S44003553	WLX302	192.168.100.3 設定	lan1:1-2-2	00_a0_de_97_f2_a0.conf 保存 <b>復元</b> 削除	MACアドレス (00:a0:de:97:f2:a0) 設定

閉じる

「CONFIGの復元」ダイアログが表示されます。

## メモ

ネットワーク内のすべてのヤマハ無線 AP の設定 (CONFIG) を復元するときは、「無線 AP の CONFIG の一括操作」欄の「復元」ボタンをクリックします。

5. 「実行」ボタンをクリックする。

CONFIGの復元

指定した無線APのCONFIGへCONFIGファイルを送信します。

**実行** キャンセル

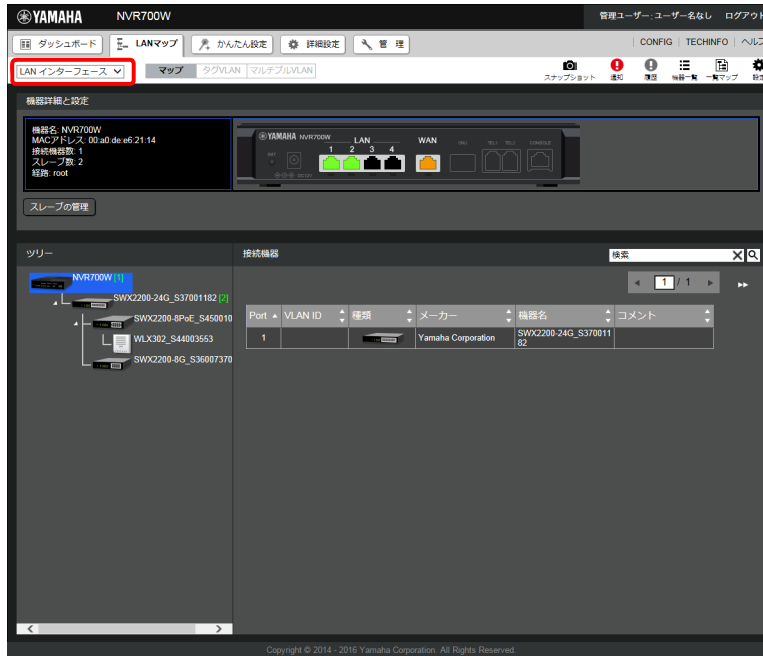
設定 (CONFIG) が復元され、「スレーブの管理」ダイアログが表示されます。

## 第 11 章 LAN マップを利用する

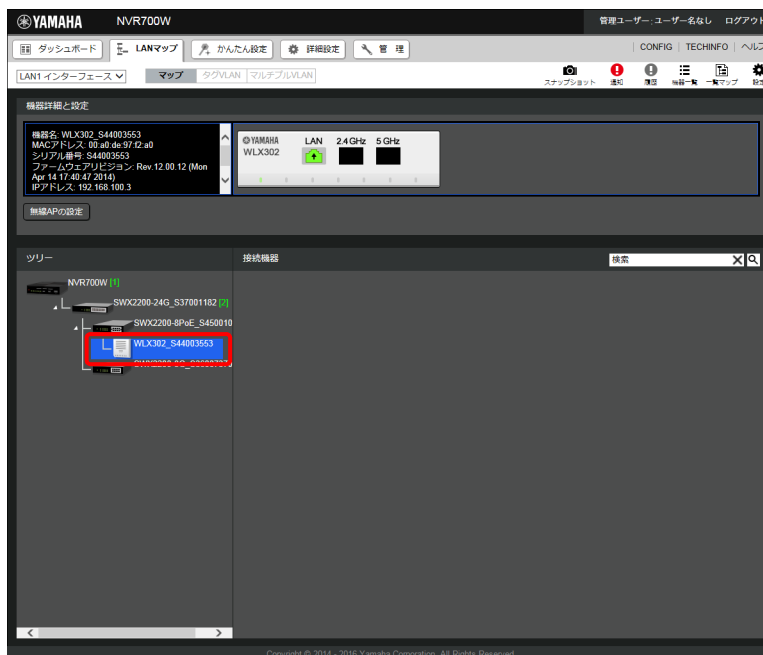
### 11.8.5 無線 AP の設定画面を表示する

ヤマハ無線 AP の詳細設定を変更するために、ヤマハ無線 AP の「Web 設定画面」を表示します。ヤマハ無線 AP の「Web 設定画面」の使い方について詳しくは、ヤマハ無線 AP の取扱説明書（製品付属の CD-ROM に収録）をご覧ください。

1. 設定したい無線 AP が接続されたインターフェースを、インターフェース選択プルダウンメニューから選択する。

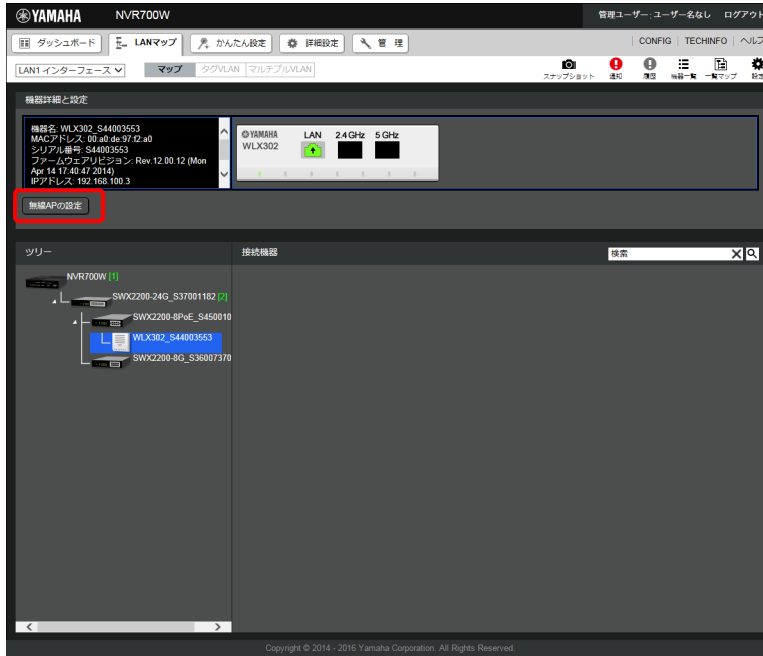


2. ツリービューで無線 AP を選択する。



機器詳細と設定ビューと接続機器ビューの表示が切り替わります。

## 3. 機器詳細と設定ビューの「無線 AP の設定」ボタンをクリックする。



無線 AP 機器の「Web 設定画面」が表示されます。

## 11.9 タグ VLAN を設定する

タグ VLAN の設定方法を説明します。タグ VLAN 機能とは、ヤマハスイッチのポートやヤマハ無線 AP の SSID をグループ分けし、グループごとにユニークな VLAN ID タグと IP アドレスを付与することで、物理的な配置に依存することなく、仮想的な LAN を形成する機能のことです。VLAN 間の通信はコントローラーを経由して行われます。

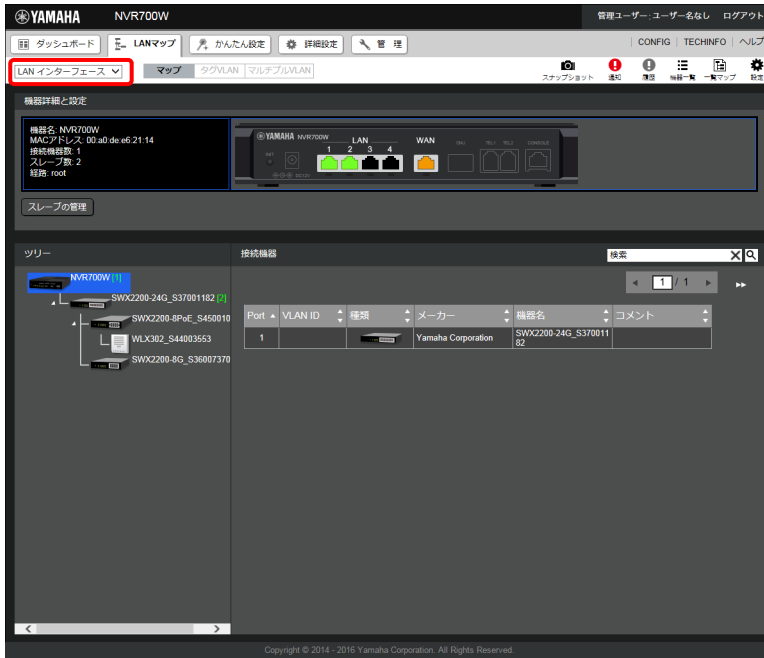
### ご注意

- ・ SWX2100 および SWX2300 では設定できません。SWX2300 は「スイッチの設定・保守」ボタンをクリックすると設定画面が表示され、VLAN の設定を行うことができます。

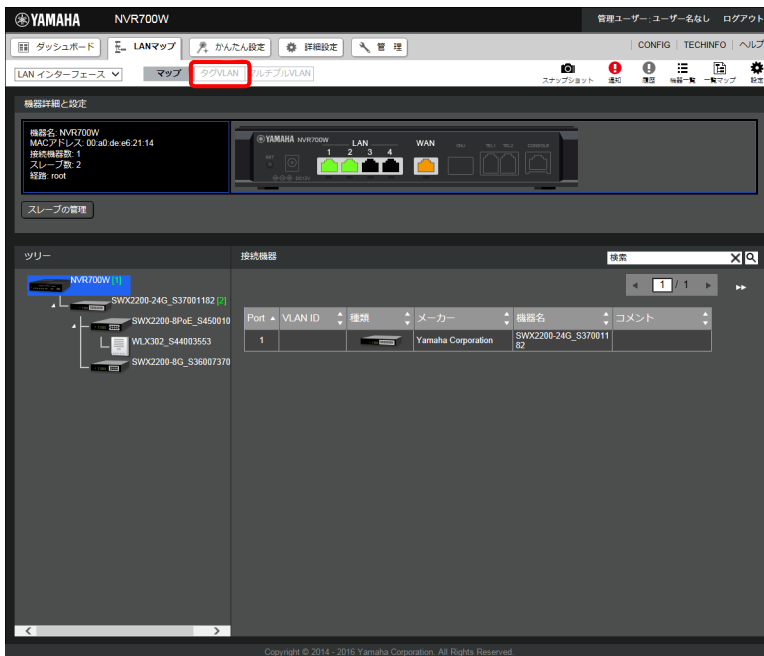
## 第 11 章 LAN マップを利用する

### 11.9.1 タグ VLAN ページを表示する

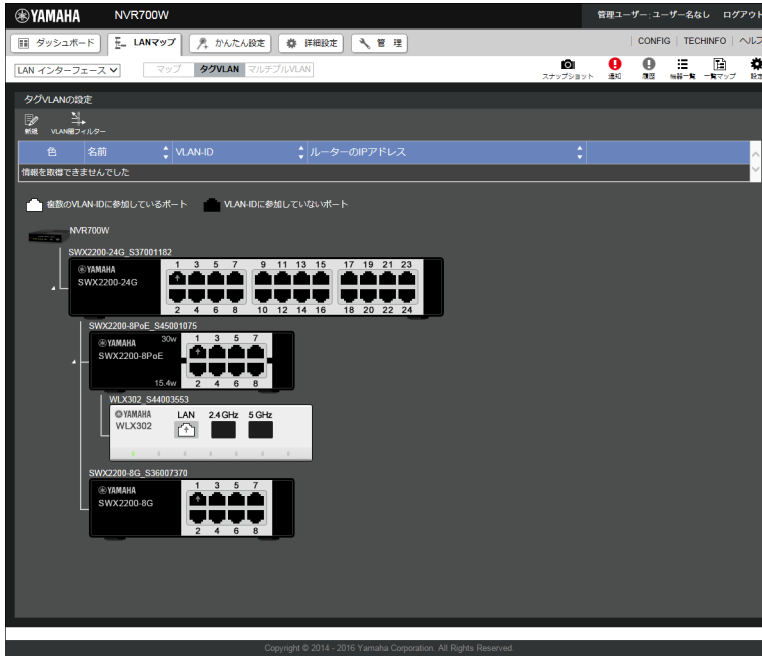
1. 設定したいネットワークのインターフェースを、インターフェース選択プルダウンメニューから選択する。



2. 表示選択スイッチで「タグ VLAN」を選択する。




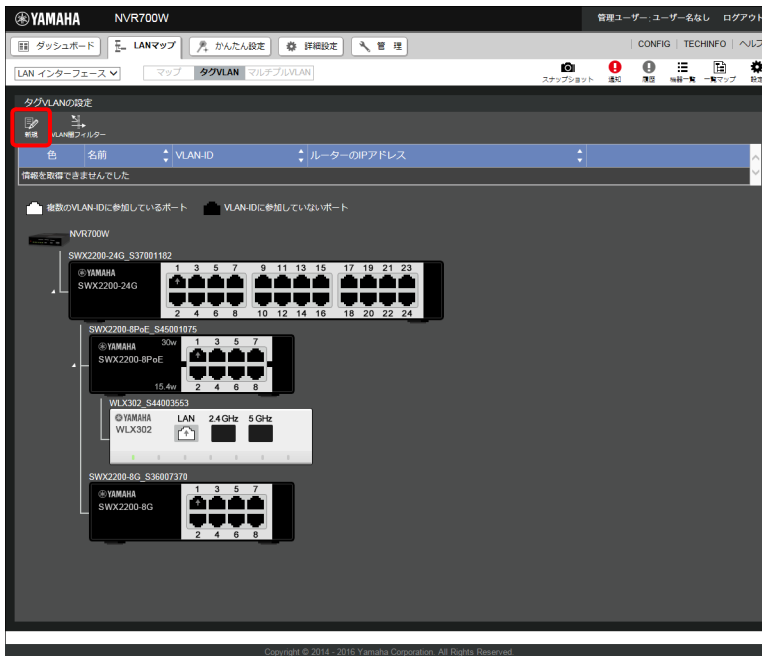
「タグ VLAN ページ」が表示されます。



## 11.9.2 タグ VLAN グループを作成する

タグ VLAN のグループを作成します。

1. 「タグ VLAN ページ」を表示する。
2. 「」ボタンをクリックする。



「VLAN グループの作成」ダイアログが表示されます。

## 第 11 章 LAN マップを利用する

### 3. タグ VLAN のグループ情報を入力する。

VLANグループの作成

① VLAN ID [ 101 ]

② 名前 [ VLAN101 ]

③ ルーターのIPアドレス [ 192.168.101.1 ] / [ 255.255.255.0 (24bit) ]

④ DHCPサーバー機能  使用する  使用しない  
[ 192.168.101.2 ] ~ [ 192.168.101.93 ] / [ 255.255.255.0 (24bit) ]

確定 キャンセル

① **VLAN ID :**

VLAN の ID を入力します。

② **名前 :**

任意の名前を入力します。区別しやすい名前を付けておくと、設定の修正や削除をする場合に便利です。

③ **ルーターの IP アドレス :**

VLAN で使用する IP アドレスを入力します。

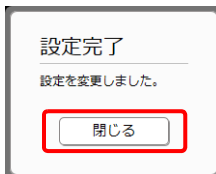
④ **DHCP サーバー機能 :**

VLAN 配下の端末に DHCP で IP アドレスを払い出す場合は、「使用する」を選択して IP アドレスを入力します。DHCP サーバー機能を使用しない場合は、「使用しない」を選択します。

### 4. 「確定」 ボタンをクリックする。

タグ VLAN のグループが登録され、「設定完了」ダイアログが表示されます。

### 5. 「閉じる」 ボタンをクリックする。



「タグ VLAN ページ」が表示されます。

## 11.9.3 タグ VLAN グループに参加させる

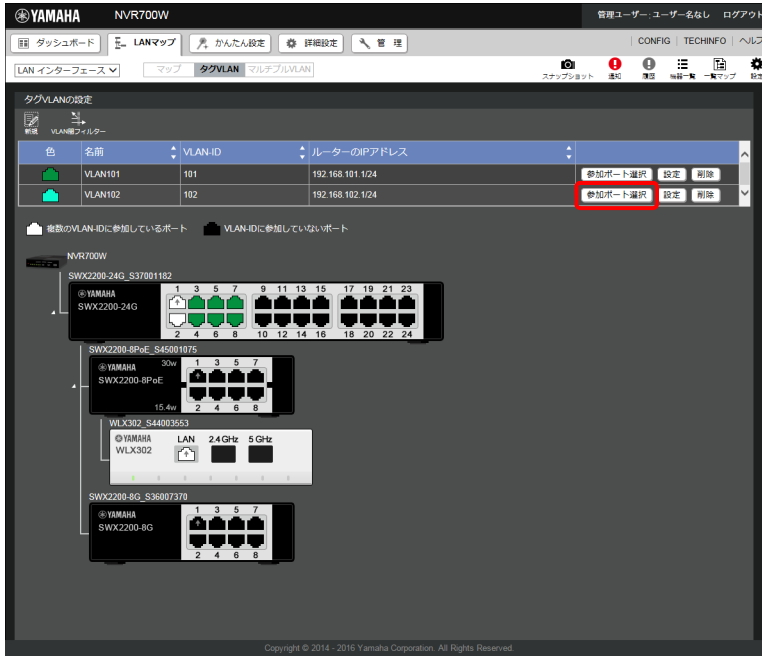
作成したタグ VLAN のグループごとに、参加させるポートを設定します。

### メモ

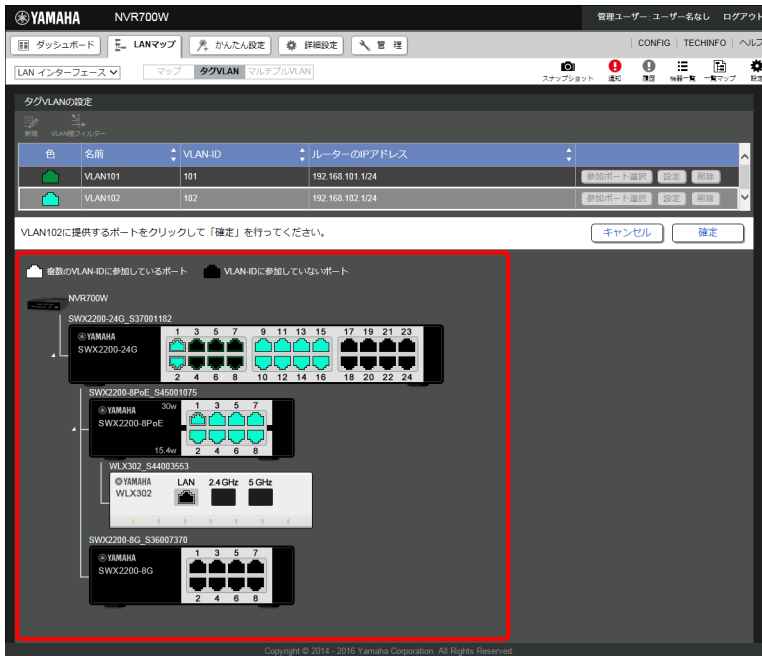
ヤマハ無線 AP の SSID も VLAN グループに参加させたい場合は、ヤマハ無線 AP の「Web 設定画面」で SSID ごとに VLAN ID を設定してください。また、「タグ VLAN ページ」でヤマハ無線 AP の LAN ポートも VLAN グループに参加させてください。ヤマハ無線 AP の「Web 設定画面」の使い方について詳しくは、ヤマハ無線 AP の取扱説明書（製品付属の CD-ROM に収録）をご覧ください。

#### 1. 「タグ VLAN ページ」を表示する。

2. 設定したいタグ VLAN グループの「参加ポート選択」ボタンをクリックする。



3. 機器アイコンからタグ VLAN グループに参加させたいポートを選択する。



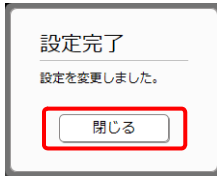
ポートを選択するとポートの色が変わり、指定の VLAN グループに参加させることができます。また、選択したポートを再選択すると参加をキャンセルすることができます。

## メモ

ポートを VLAN グループに参加させた場合、コントローラーから対象のスレーブまでをつなぐポート（アップリンク / ダウンリンク）も自動で選択されます。

## 第 11 章 LAN マップを利用する

4. 「確定」 ボタンをクリックする。  
設定が反映され、「設定完了」 ダイアログが表示されます。
5. 「閉じる」 ボタンをクリックする。

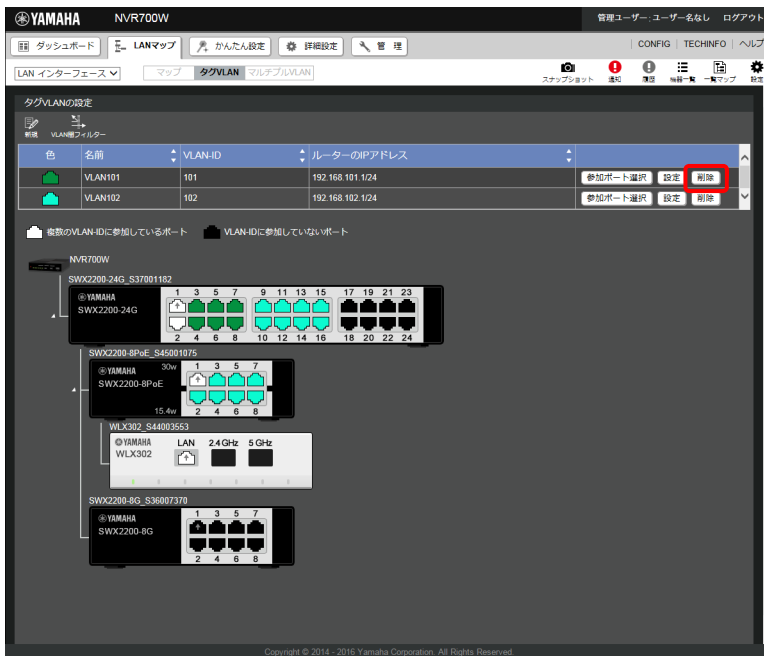


「タグ VLAN ページ」が表示されます。

### 11.9.4 タグ VLAN グループを削除する

作成したタグ VLAN グループを削除します。

1. 「タグ VLAN ページ」を表示する。
2. 削除したいタグ VLAN グループの「削除」ボタンをクリックする。



「VLAN グループの削除」ダイアログが表示されます。

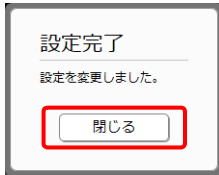
3. 「実行」ボタンをクリックする。



タグ VLAN グループが削除され、「設定完了」ダイアログが表示されます。



## 4. 「閉じる」 ボタンをクリックする。




「タグ VLAN ページ」が表示されます。

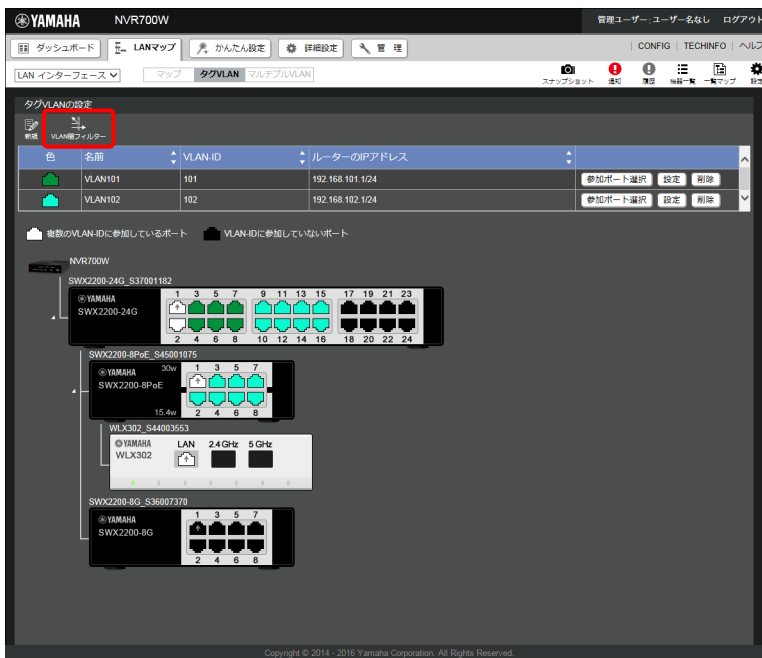
## 11.9.5 タグ VLAN 間フィルターを設定する

VLAN 間の通信を開放するか遮断するかを設定します。VLAN 間フィルターの設定操作を行わない場合は、VLAN 間の通信が常に全開放された状態になります。

## ご注意

タグ VLAN グループが 2 個以上作成されていなければ VLAN 間フィルターの設定はできません。

1. 「タグ VLAN ページ」を表示する。
2. 「」 ボタンをクリックする。



「VLAN 間フィルター」 ダイアログが表示されます。

## 第 11 章 LAN マップを利用する

### 3. タグ VLAN グループ間のフィルターを設定する。

#### ① 全遮断：

VLAN 間の通信をすべて遮断します。全遮断を選択した場合は、すべての VLAN 間の通信を遮断する IP フィルターが登録されます。

### ご注意

VLAN グループを追加した場合は、改めて全遮断のフィルター設定操作を行ってください。新規作成した VLAN グループは、既存の VLAN グループとの通信が開放されているためです。

VLAN グループで使用する IP アドレスを変更した場合も、改めて全遮断のフィルター設定操作を行ってください。

#### ② 全開放：

VLAN 間の通信をすべて開放します。全開放を選択した場合は、全遮断した際に追加した IP フィルターがすべて削除されます。

### 4. 「確定」 ボタンをクリックする。

設定が反映され、「設定完了」ダイアログが表示されます。

### 5. 「閉じる」 ボタンをクリックする。

「タグ VLAN ページ」が表示されます。

### メモ

全遮断の設定を行った後で VLAN グループを削除すると、削除した VLAN グループに関連する IP フィルターの設定が残ったままになりますが、全開放の設定を行えば IP フィルターの設定は削除されます。ただし、VLAN グループが 2 個以上作成されていなければ VLAN 間フィルターの設定は変更できないため、VLAN グループを削除する場合は、先に VLAN 間フィルターの全開放の設定を行っておくことで IP フィルターの設定を削除することができます。

## 11.10 マルチプル VLAN を設定する

マルチプル VLAN の設定方法を説明します。マルチプル VLAN 機能とは、ヤマハスイッチのポートをグループ分けし、グループ間の通信を遮断する機能のことです。マルチプル VLAN 機能はヤマハスイッチのみに設定することができます。

## ご注意

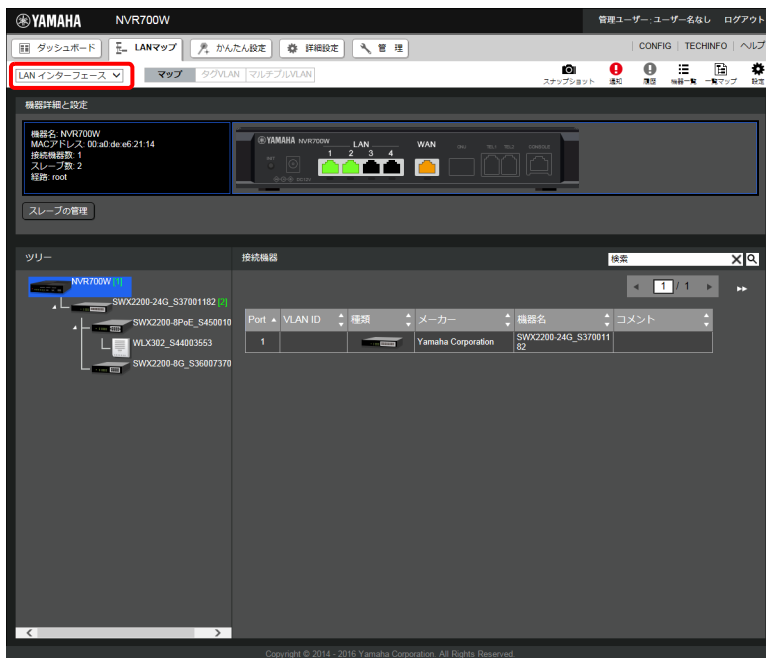
- マルチプル VLAN は、SWX2200 をお使いの場合に設定できます。SWX2100 および SWX2300 では設定できません。

## メモ

- サーバーやルーターなど全グループと通信を行う必要がある機器が接続されるポートについては、すべてのグループに参加させることで、すべてのグループとの通信を可能にすることができます。
- マルチプル VLAN 機能では、グループが異なっても同じネットワークアドレスが使用されます。

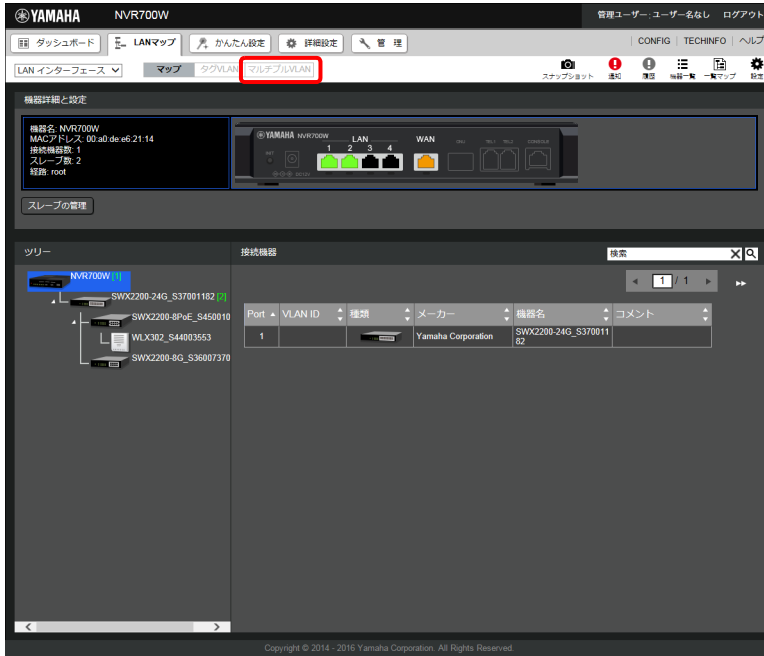
### 11.10.1 マルチプル VLAN ページを表示する

- 設定したいネットワークのインターフェースを、インターフェース選択プルダウンメニューから選択する。

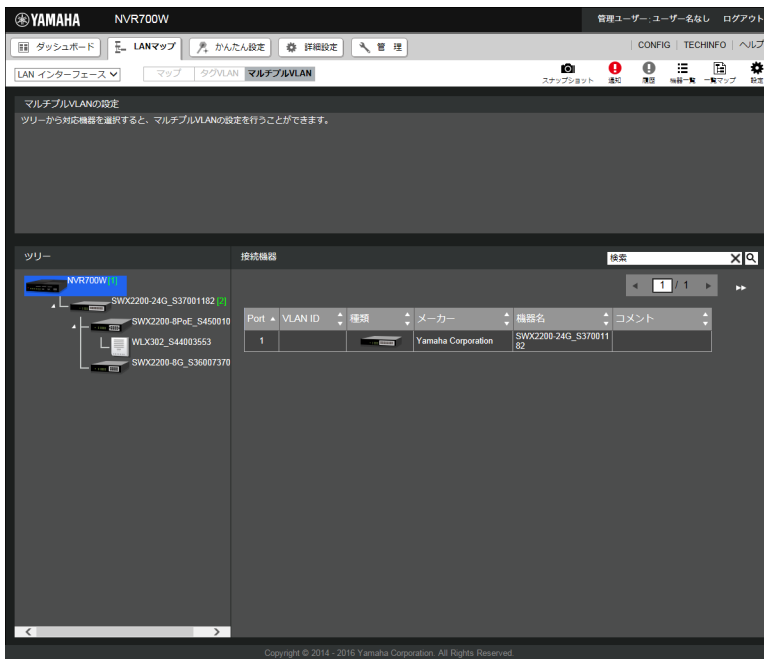


## 第 11 章 LAN マップを利用する

### 2. 表示選択スイッチで「マルチプル VLAN」を選択する。



「マルチプル VLAN ページ」が表示されます。

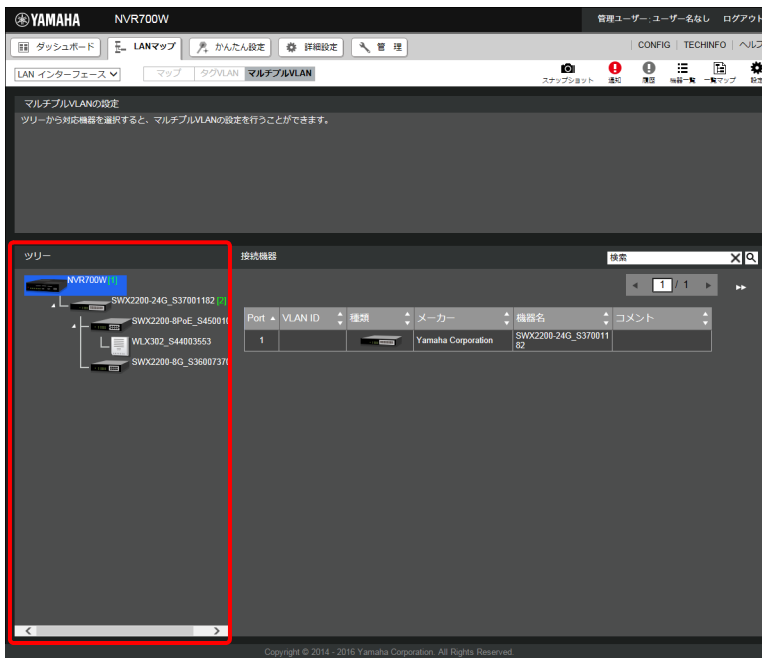


### 11.10.2 マルチプル VLAN グループを設定する

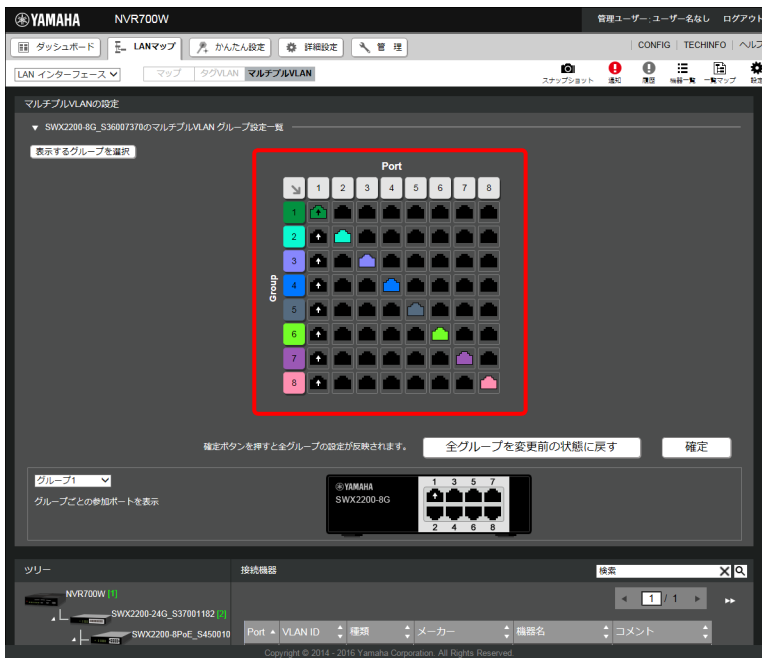
マルチプル VLAN のグループごとに、参加させるポートを設定します。

#### 1. 「マルチプル VLAN ページ」を表示する。

## 2. ツリービューで確認したいヤマハスイッチのアイコンを選択する。




## 3. マルチプル VLAN の設定ビューで、グループごとに参加ポートを選択する。



ポートを選択するとポートの色が変わり、指定のマルチプル VLAN グループに参加させることができます。また、選択したポートを再選択すると参加をキャンセルすることができます。

## メモ

- ・ポートの番号をクリックすると、Port 列のすべてのグループのポートを選択できます。
- ・グループの番号をクリックすると、Group 行のすべてのポートを選択できます。
- ・「」ボタンをクリックすると、左上から斜線上にポートを選択できます。

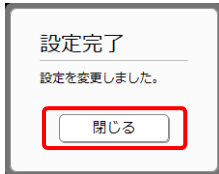
## 第 11 章 LAN マップを利用する

- ・「表示するグループを選択」ボタンをクリックすると、マルチプル VLAN の設定ビューに表示したいグループを設定することができます。表示したいグループのみにチェックを入れ「確定」ボタンをクリックすると、選択したマルチプル VLAN のグループのみが表示されます。
- ・「全グループを変更前の状態に戻す」ボタンをクリックすると、マルチプル VLAN に参加するポートを変更前の状態に戻すことができます。

### 4. 「確定」ボタンをクリックする。

マルチプル VLAN グループへの参加ポートが登録され、「設定完了」ダイアログが表示されます。

### 5. 「閉じる」ボタンをクリックする。

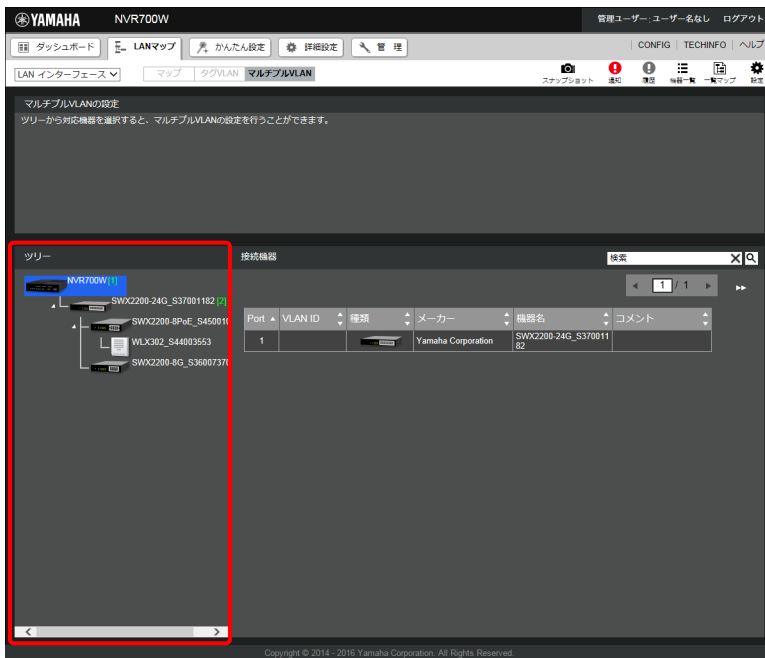


「マルチプル VLAN ページ」が表示されます。

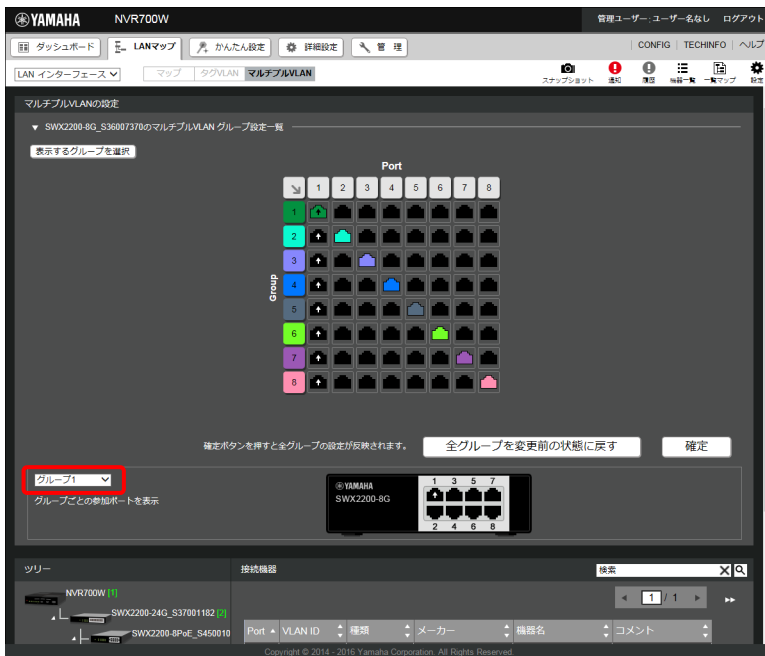
## 11.10.3 マルチプル VLAN グループの参加ポートを確認する

マルチプル VLAN のグループごとの参加ポートをスイッチ画像上で確認することができます。

1. 「マルチプル VLAN ページ」を表示する。
2. ツリービューで確認したいヤマハスイッチのアイコンを選択する。




3. 「グループごとの参加ポートを表示」項目のプルダウンメニューから、表示させたいグループを選択する。



右側のスイッチ画像で、選択したグループに参加しているポートがグループに対応した色に切り替わります。

### 11.11 接続機器の一覧を見る

LAN マップで管理している機器の一覧を表示することができます。端末情報の編集を行ったり、端末マスターをエクスポートしたりすることができます。端末マスターとは、端末ごとの詳細情報を記載した CSV 形式のファイルのことで、RTFS に自動的に保存されます。RTFS とは、ヤマハルーターの不揮発性メモリに構築されるファイルシステムのことです。端末マスターは Web GUI 上での編集に加え、エクスポートしてパソコン上で編集することもできます。端末の検索を行ったとき、端末マスターに登録された端末であれば端末情報が自動的に反映されます。端末ごとの情報を事前に設定しておくことができるため、検出された端末の管理が簡単になります。


また、「」ボタンをクリックすると、ネットワークに接続された機器全体を一覧マップで表示することができます。一覧マップについては、「11.11.10 一覧マップで表示する」(233 ページ) をご覧ください。

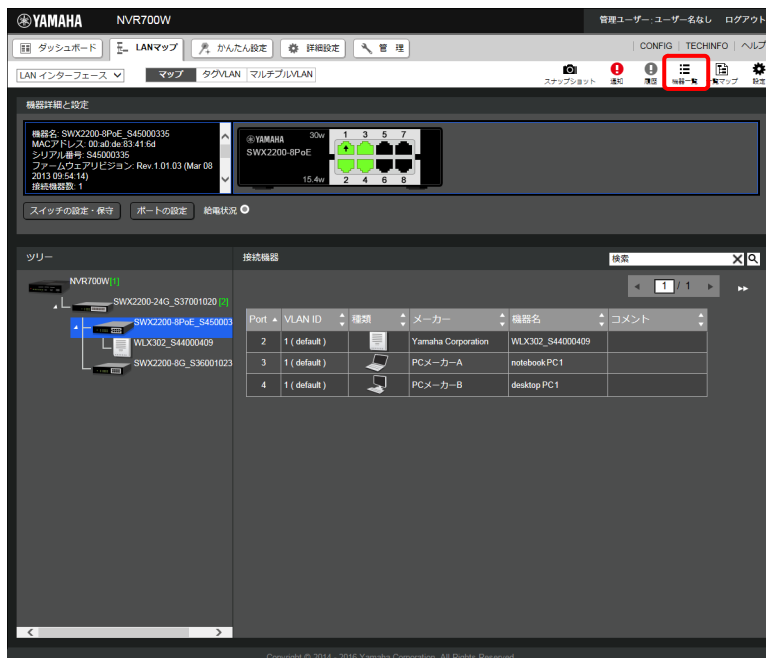
#### ご注意

- ・ RTFS の空き容量が足りない場合、端末マスターは保存されません。
- ・ 工場出荷状態に戻したり RTFS をフォーマットすると、端末マスターの情報も初期化されます。

#### 11.11.1 端末一覧画面を表示する

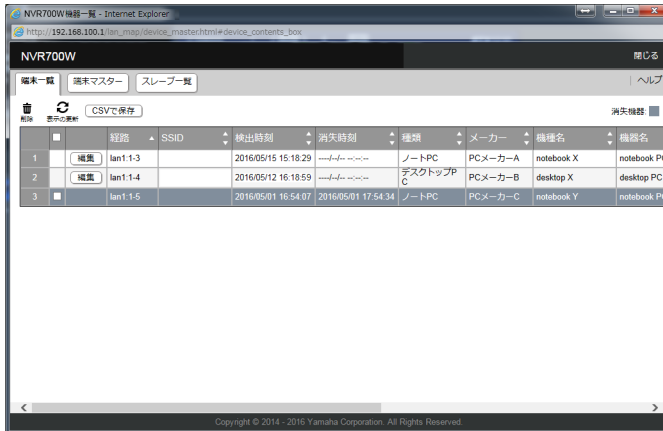
LAN マップで管理している端末を一覧表示します。「端末一覧」画面では、存在を確認できている端末だけでなく、存在を確認できなくなった端末も消失端末として表示され、消失した時刻が確認できます。LAN に接続されている端末であっても、無通信状態が長く続くと消失扱いになる場合があります。なお、消失扱いになった端末でも、存在が確認できた時点で消失扱いではなくなります。


1. 「」ボタンをクリックする。





「端末一覧」画面が表示され、LAN マップで管理している端末の情報が確認できます。





項目ごとの「」ボタンをクリックすることでリストを並び替えることができます。初期表示では経路順にソートされています。なお、消失している端末はグレーにハイライトされて表示されます。

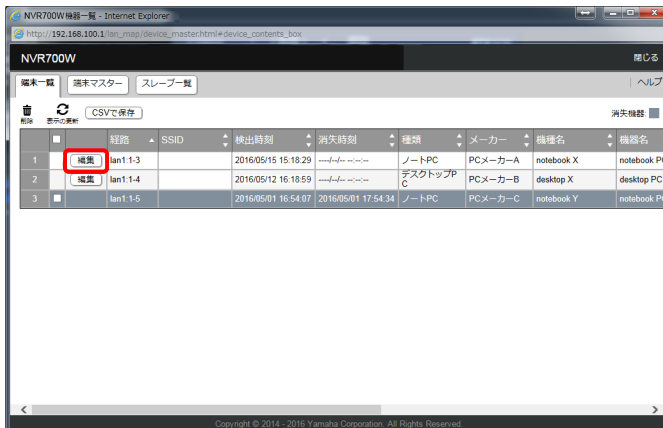
## メモ

- ・「」ボタンをクリックすると、選択した端末の情報が端末一覧から削除されます。消失端末の情報のみ削除することができます。実際に LAN から切断している端末で、情報が不要になった場合に削除します。
- ・「」ボタンをクリックすると、「端末一覧」画面の表示が、コントローラーが保持している最新の情報に更新されます。
- ・「CSVで保存」ボタンをクリックすると、端末一覧情報を CSV ファイル形式で保存することができます。

## 11.11.2 端末の情報を編集する

LAN マップで管理している端末の情報を編集することができます。編集した情報は自動的に端末マスターにも登録されます。

1. 「端末一覧」画面で編集したい端末の「編集」ボタンをクリックする。



「機器情報の編集」ダイアログが表示されます。

## 第 11 章 LAN マップを利用する

### 2. 端末の情報を編集する。

機器情報の編集	
MACアドレス	XXXXXXXXXX
① 種類	ノートPC
② メーカー	PCメーカーA
③ 機種名	notebook X
④ 機器名	notebook PC1
⑤ OS	Windows
⑥ コメント	work 1
⑦ スナップショット機能	<input checked="" type="radio"/> 監視対象に含める <input type="radio"/> 監視対象に含めない
確定      キャンセル	

#### ① 種類：

プルダウンメニューから端末の種類を選択します。選択した種類に合わせて接続機器ビューの端末アイコンが切り替わります。

#### ② メーカー：

メーカー名を入力します。

#### ③ 機種名：

機種名を入力します。

#### ④ 機器名：

機器名を入力します。

#### ⑤ OS：

OS 名を入力します。

#### ⑥ コメント：

任意のコメントを入力します。

#### ⑦ スナップショット機能：

スナップショット機能の監視対象に含める / 含めないを選択します。

## メモ

端末マスターに登録済みの端末情報の編集は、「端末マスター」画面でも行えます。

### 3. 「確定」 ボタンをクリックする。

端末の情報に変更され、「完了」ダイアログが表示されます。

### 4. 「閉じる」 ボタンをクリックする。

完了

編集を完了しました。  
この機器情報は端末マスターにも登録されました。

閉じる

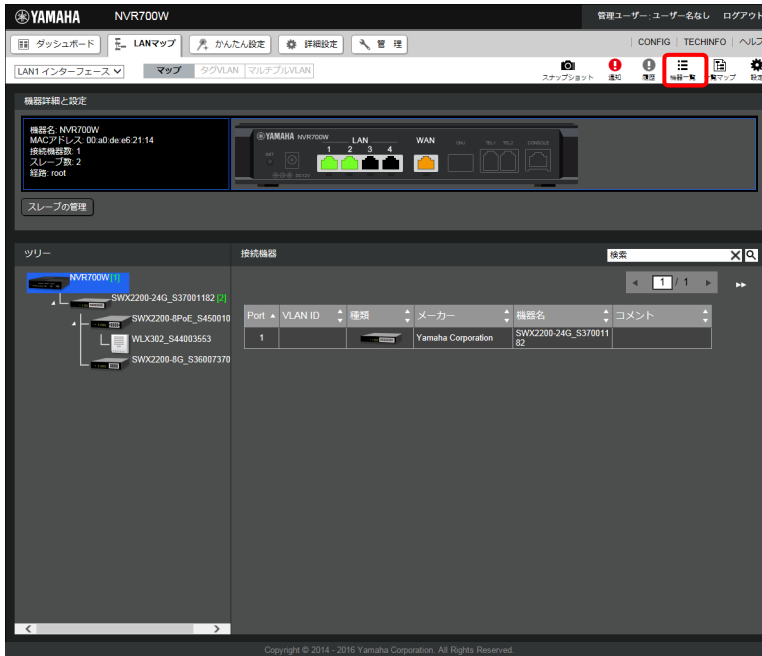
「端末一覧」画面が表示されます。

### 11.11.3 端末マスター画面を表示する

端末情報の基準となる情報を端末マスターと呼びます。LAN マップで検出された端末と MAC アドレスが一致する端末情報が端末マスターに登録されていれば、端末マスターの情報が接続機器ビューや「端末一覧」画面に表示されるようになります。

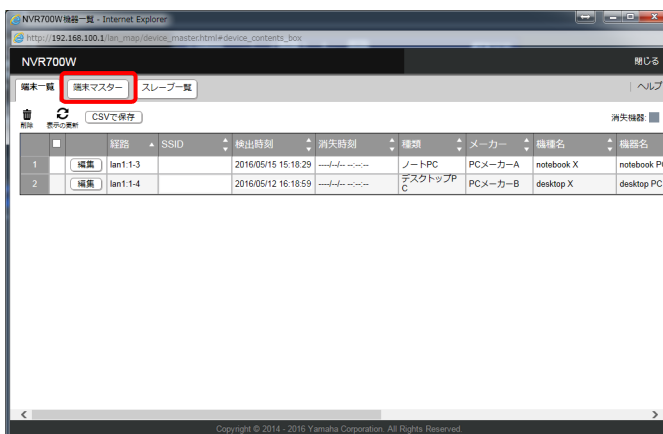
「端末マスター」画面では端末マスターに登録されている端末情報を一覧表示します。端末マスター情報を新規に登録したり、登録済みの情報を編集したりすることができます。

#### 1. 「」ボタンをクリックする。



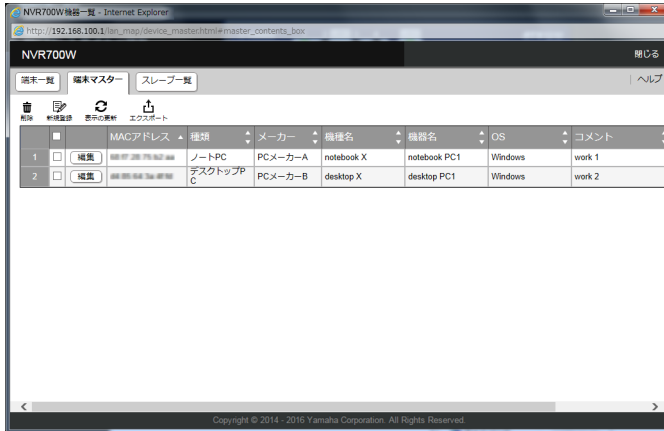
「端末一覧」画面が表示されます。


#### 2. 「端末マスター」タブをクリックする。






## 第 11 章 LAN マップを利用する

「端末マスター」画面が表示され、端末マスターに登録されている端末情報が確認できます。




項目ごとの「」ボタンをクリックすることでリストを並び替えることができます。初期表示では MAC アドレス順にソートされています。

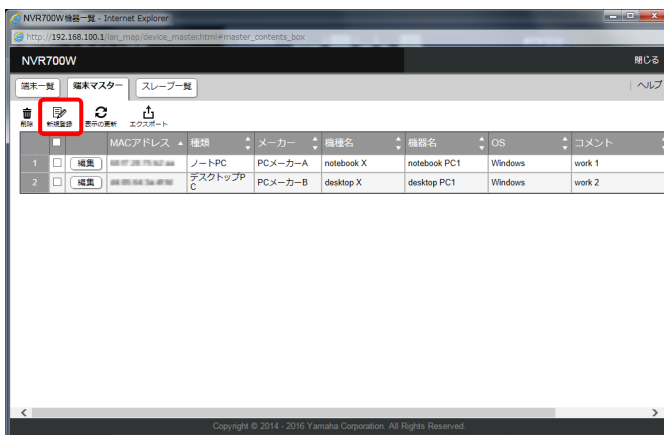
### メモ

- ・「」ボタンをクリックすると、選択した端末の情報が端末マスターから削除されます。
- ・「」ボタンをクリックすると、「端末マスター」画面の表示が更新されます。
- ・「」ボタンをクリックすると、端末マスター情報を CSV ファイル形式で保存することができます。

### 11.11.4 端末マスターに端末情報を新規登録する

端末の情報を端末マスターに新規登録することができます。

1. 「端末マスター」画面で「」ボタンをクリックする。



「機器情報の新規登録」ダイアログが表示されます。

## 2. 端末の情報を登録する。

## ① MAC アドレス：

MAC アドレスを「aa:bb:cc:dd:ee:ff」の形式で入力します。

## ② 種類：

プルダウンメニューから端末の種類を選択します。選択した種類に合わせて接続機器ビューの端末アイコンが切り替わります。

## ③ メーカー：

メーカー名を入力します。

## ④ 機種名：

機種名を入力します。

## ⑤ 機器名：

機器名を入力します。

## ⑥ OS：

OS 名を入力します。

## ⑦ コメント：

任意のコメントを入力します。

## ⑧ スナップショット機能：

スナップショット機能の監視対象に含める / 含めないを選択します。

## 3. 「確定」 ボタンをクリックする。

端末の情報が登録され、「完了」ダイアログが表示されます。

## 4. 「閉じる」 ボタンをクリックする。

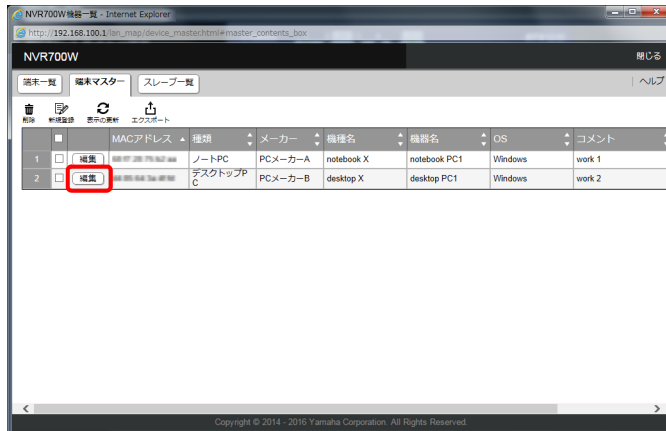
「端末マスター」画面が表示されます。

## 11.11.5 端末マスターに登録されている端末情報を編集する

端末マスターに登録されている端末の情報を編集することができます。

## 第 11 章 LAN マップを利用する

1. 「端末マスター」画面で編集したい端末の「編集」ボタンをクリックする。



「機器情報の編集」ダイアログが表示されます。

2. 端末の情報を編集する。

機器情報の編集	
① MACアドレス	aa:bb:cc:dd:ee:ff
② 種類	デスクトップPC
③ メーカー	PCメーカー-B
④ 機種名	desktop X
⑤ 機器名	desktop PC1
⑥ OS	Windows
⑦ コメント	work 2
⑧ スナップショット機能	<input checked="" type="radio"/> 監視対象に含める <input type="radio"/> 監視対象に含めない

① **MAC アドレス：**

MAC アドレスを「aa:bb:cc:dd:ee:ff」の形式で入力します。

② **種類：**

プルダウンメニューから端末の種類を選択します。選択した種類に合わせて接続機器ビューの端末アイコンが切り替わります。

③ **メーカー：**

メーカー名を入力します。

④ **機種名：**

機種名を入力します。

⑤ **機器名：**

機器名を入力します。

⑥ **OS：**

OS 名を入力します。

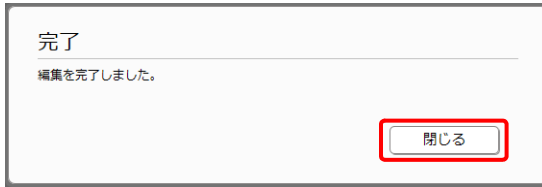
⑦ **コメント：**

任意のコメントを入力します。

⑧ **スナップショット機能：**

スナップショット機能の監視対象に含める / 含めないを選択します。

3. 「確定」 ボタンをクリックする。  
端末の情報が登録され、「完了」 ダイアログが表示されます。
4. 「閉じる」 ボタンをクリックする。



「端末マスター」画面が表示されます。

### 11.11.6 端末マスターファイルをパソコンへエクスポートする


端末マスターはファイル形式で RTFS に保存されており、ルーター間で移行することができます。ネットワーク全体で使用する端末の情報を一つの端末マスターファイルにまとめておき、各ルーターでその端末マスターを共有したり、ルーターをリプレースする際に新しいルーターへ端末マスターファイルを移行して端末情報を引き継ぐ、といった使い方ができます。

本章では、TFTP を使用して端末マスターファイルをパソコンへエクスポートする方法について説明します。

#### ご注意

工場出荷状態に戻したり、RTFS をフォーマットすると、端末マスターファイルも消去されてしまうため、定期的にバックアップしておくことをおすすめいたします。

#### メモ

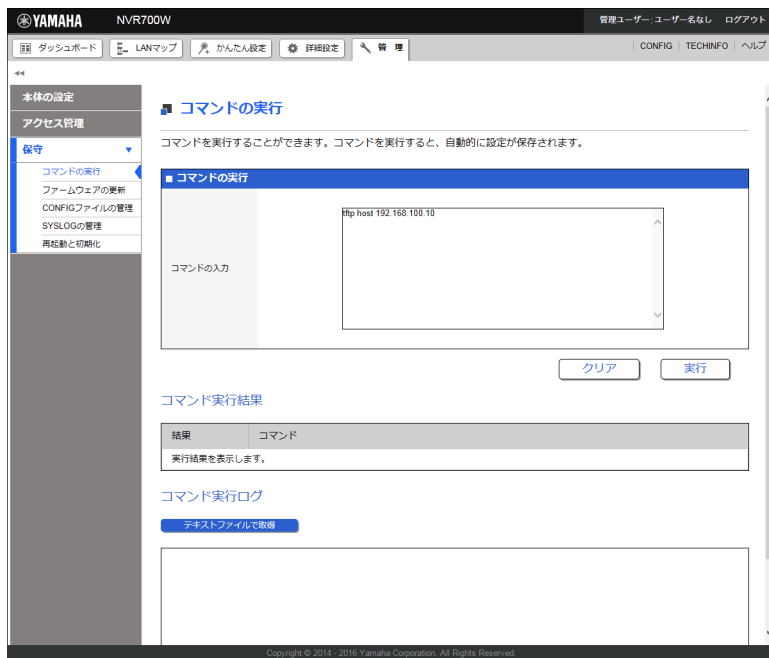
「端末マスター」画面の「」ボタンからエクスポートすることもできます。

1. 「管理」タブ - 「保守」 - 「コマンドの実行」を順に選択する。  
「コマンドの実行」画面が表示されます。

## 第 11 章 LAN マップを利用する

### 2. 「コマンドの実行」項目にコマンドを入力する。

tftp host コマンドでエクスポート先のパソコンの IP アドレスを設定します。



#### コマンドの入力例

- エクスポート先のパソコンの IP アドレス : 192.168.100.10

```
tftp host 192.168.100.10
```

### 3. 「実行」ボタンをクリックする。

### 4. パソコンのコマンドプロンプトを起動して、tftp コマンドを実行する。

- 使用するコマンドの形式は、OS に依存します。
- tftp コマンドのパラメーターに、ヤマハルーターの IP アドレスを指定します。
- 転送モードは「アスキー」または「文字」にします。
- ヤマハルーターに管理パスワードが設定されている場合は、ファイル名に続けて管理パスワードを指定します。

#### コマンドの入力例

- ヤマハルーターの IP アドレス : 192.168.100.1
- ヤマハルーターの管理パスワード : adM123
- 端末マスターファイルのファイルパス ( 固定 ) : /lanmap/devinfo\_master.csv

```
C:¥>tftp 192.168.100.1 get /lanmap/devinfo_master.csv/adM123
devinfo_master.csv
転送を正常に完了しました : 1 秒間に xxxx バイト、xxxx バイト / 秒

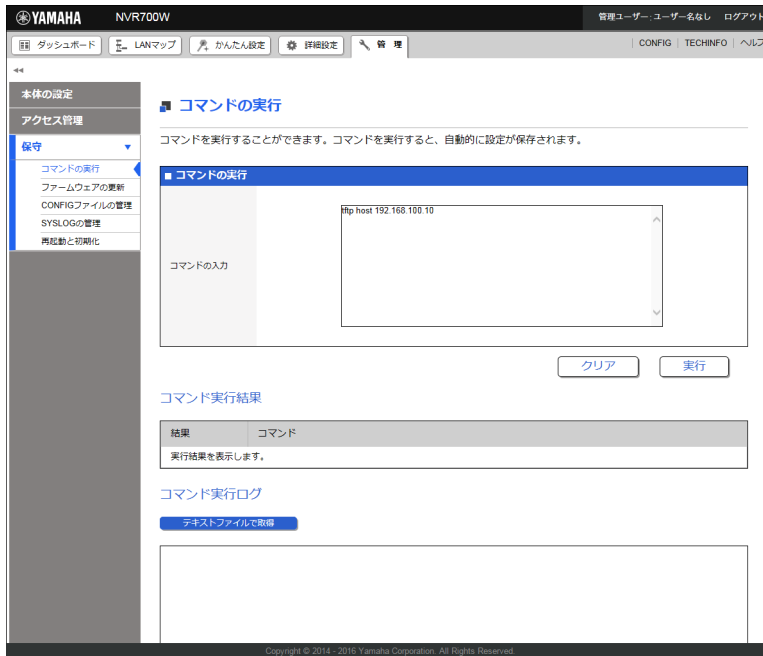
C:¥>
```



### 11.11.7 端末マスターファイルをパソコンからインポートする

本章では、TFTP を使用して端末マスターファイルをパソコンからインポートする方法について説明します。リプレースの際に端末マスターファイルを新しいルーターへ移行する場合などは、パソコンを新しいルーターに接続して本操作を行ってください。

1. 「管理」タブ - 「保守」 - 「コマンドの実行」を順に選択する。  
「コマンドの実行」画面が表示されます。
2. 「コマンドの実行」項目にコマンドを入力する。  
tftp host コマンドでインポート元のパソコンの IP アドレスを設定します。



#### コマンドの入力例

- インポート元のパソコンの IP アドレス : 192.168.100.10

```
tftp host 192.168.100.10
```

3. 「実行」ボタンをクリックする。
4. パソコンのコマンドプロンプトを起動して、tftp コマンドを実行する。
  - 使用するコマンドの形式は、OS に依存します。
  - tftp コマンドのパラメーターに、ヤマハルーターの IP アドレスを指定します。
  - 転送モードは「アスキー」または「文字」にします。
  - ヤマハルーターに管理パスワードが設定されている場合は、ファイル名に続けて管理パスワードを指定します。
  - 端末マスターファイルが保存されているディレクトリに移動します。

## 第 11 章 LAN マップを利用する

### コマンドの入力例

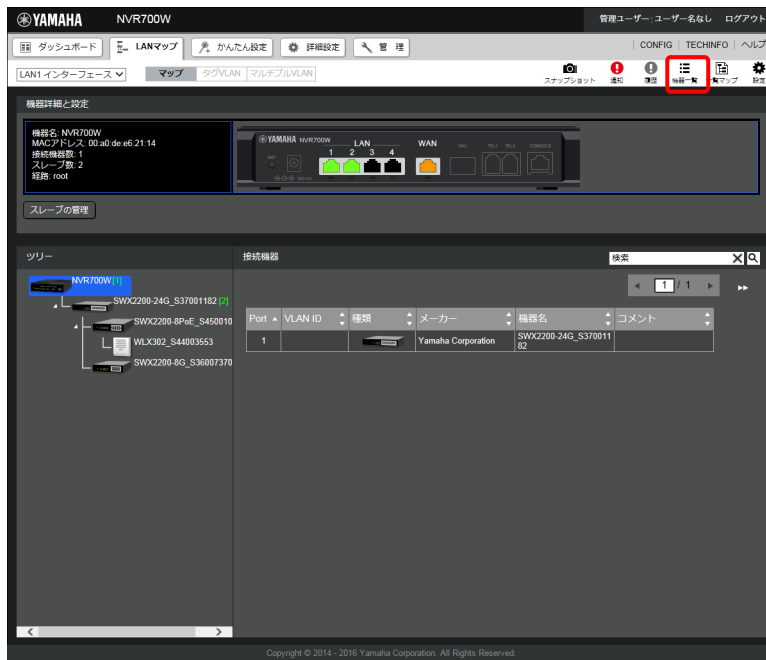
- ヤマハルーターの IP アドレス：192.168.100.1
- ヤマハルーターの管理パスワード：adM123
- 端末マスターファイルのファイルパス ( 固定 )：/lanmap/devinfo\_master.csv

```
C:¥>tftp 192.168.100.1 put devinfo_master.csv /lanmap/  
devinfo_master.csv/adM123  
転送を正常に完了しました： 1 秒間に xxxx バイト、xxxx バイト / 秒  
  
C:¥>
```

### 11.11.8 スレーブ一覧画面を表示する

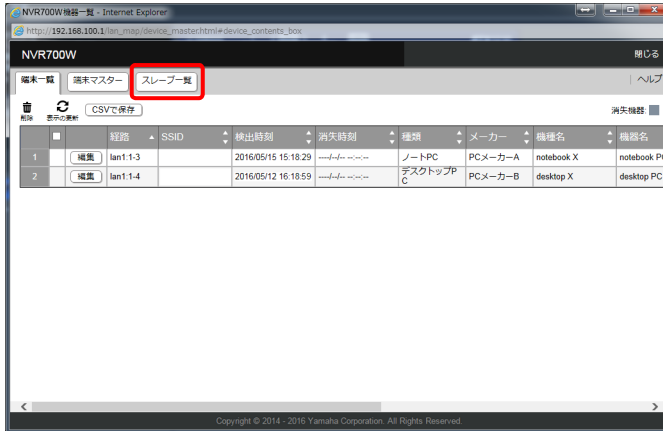
LAN マップで管理しているスレーブを一覧表示します。「スレーブ一覧」画面では、存在を確認できているスレーブだけでなく、存在を確認できなくなったスレーブも消失機器として表示され、消失した時刻が確認できます。LAN に接続されているスレーブであっても、応答がない状態が続くと消失扱いになる場合があります。なお、消失扱いになったスレーブでも、存在が確認できた時点で消失扱いではなくなります。

#### 1. 「」ボタンをクリックする。

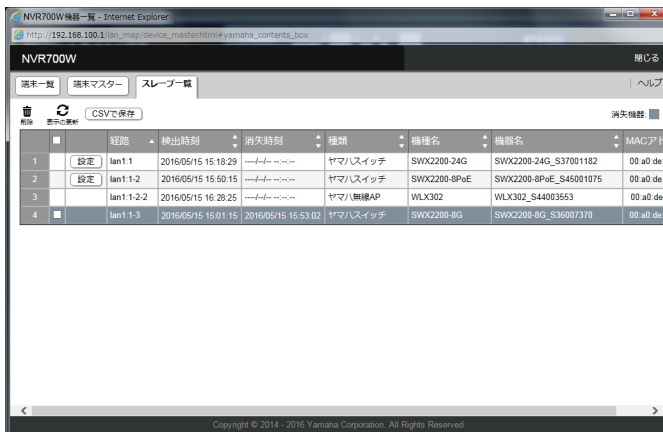



「端末一覧」画面が表示されます。

## 2. 「スレーブ一覧」タブをクリックする。





「スレーブ一覧」画面が表示され、LAN マップで管理しているスレーブの情報が確認できます。



項目ごとの「」ボタンをクリックすることでリストを並び替えることができます。初期表示では経路順にソートされています。なお、消失しているスレーブはグレーにハイライトされて表示されます。

## メモ

- ・「」ボタンをクリックすると、選択したスレーブの情報がスレーブ一覧から削除されます。消失しているスレーブの情報のみ削除することができます。実際に LAN から切断しているスレーブで、情報が不要になった場合に削除します。
- ・「」ボタンをクリックすると、「スレーブ一覧」画面の表示が、コントローラーが保持している最新の情報に更新されます。
- ・「CSV で保存」ボタンをクリックすると、スレーブ一覧情報を CSV ファイル形式で保存することができます。

## 第 11 章 LAN マップを利用する

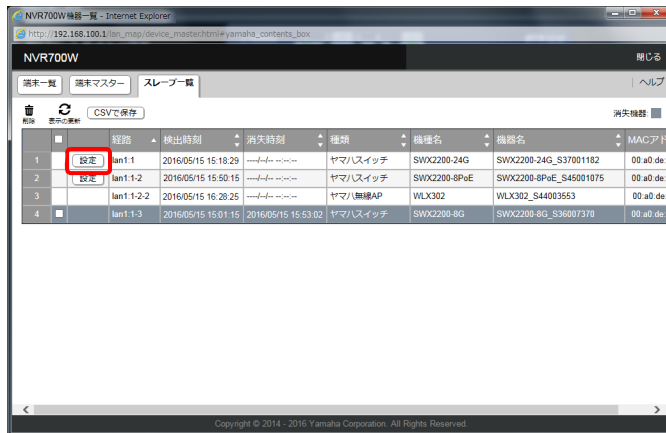
### 11.11.9 スレーブの機器名を変更する

LAN マップで管理しているスレーブの機器名を変更することができます。工場出荷時は、“機種名\_シリアル番号” という形式で機器名が付与されています。

#### ご注意

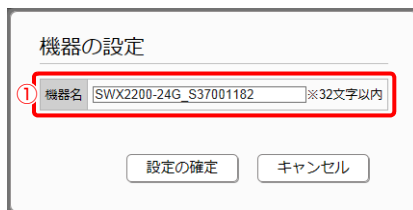
- ・ ヤマハスイッチの機器名は、SWX2200 のみ「スレーブ一覧」画面で変更できます。SWX2100 および SWX2300 の機器名は変更することができません。
- ・ 無線 AP の機器名は「スレーブ一覧」画面では変更することができません。無線 AP の機器名は無線 AP の Web 設定画面で変更することができます。Web 設定画面で、「管理機能」メニューの「基本設定」を開きます。「本製品の情報」の「名称」を任意の名称に変更し、「設定」ボタンをクリックすると、無線 AP の機器名を変更できます。無線 AP の Web 設定画面の開き方は「11.8.5 無線 AP の設定画面を表示する」（206 ページ）をご覧ください。

1. 「スレーブ一覧」画面で機器名を変更したいスレーブの「設定」ボタンをクリックする。



「機器の設定」ダイアログが表示されます。

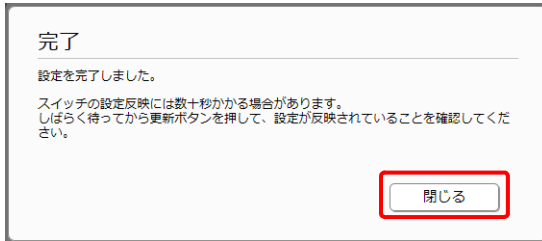
2. スレーブの機器名を変更する。



① 機器名：  
機器名を入力します。

3. 「設定の確定」ボタンをクリックする。  
機器名が変更され、「完了」ダイアログが表示されます。

## 4. 「閉じる」ボタンをクリックする。




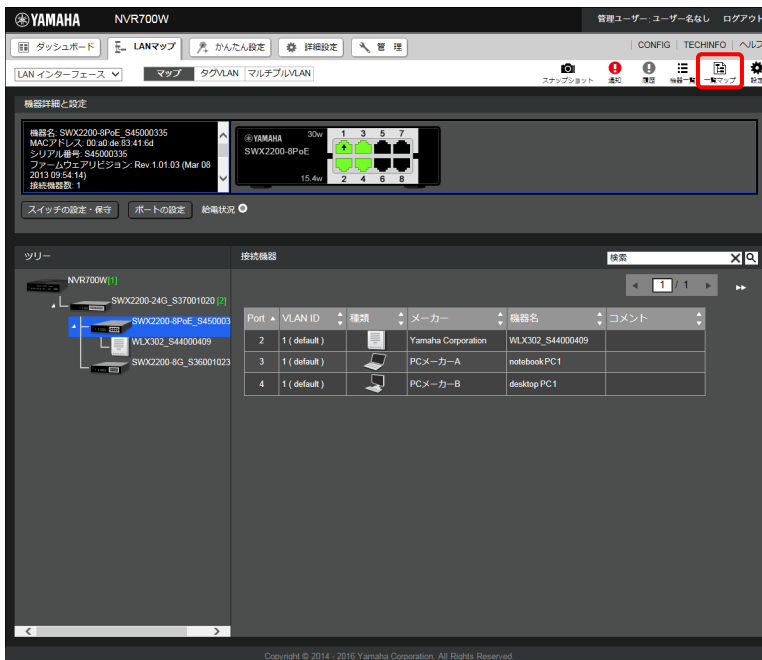
「スレーブ一覧」画面が表示されます。

## 11.11.10 一覧マップで表示する

ネットワークに接続されている機器全体を 1 つのトポロジーで表示します。トポロジーの表示範囲や機器情報の表示を切り替えることができ、自分が見やすいようにカスタマイズできます。さらに、印刷機能を使って表示している一覧マップを印刷でき、ネットワーク運用管理業務の様々な場面で活用することができます。

## ご注意



- ・ 一覧マップの表示設定は Cookie を用いて保存しています。一覧マップの表示設定を保存するには、Web ブラウザーの Cookie を有効にしてください。Web ブラウザーの設定を変更し、再度「一覧マップ」画面にアクセスしたときに設定変更が反映されていない場合は、Web ブラウザーの Cookie が無効になっているか、Cookie が削除された可能性があります。
- ・ 機器間のリンク速度（上位の機器のポートのリンク速度）は、機器アイコン間の接続線の色で確認できます。それぞれの色とリンク速度の対応については、画面右上の凡例をご確認ください。また、ヤマハ無線 AP 配下の端末、および機種を識別できないヤマハスイッチは、リンク速度を取得できないため、黒色（リンク速度が不明であることを示す色）の接続線で表示されます。

1. 「」ボタンをクリックする。

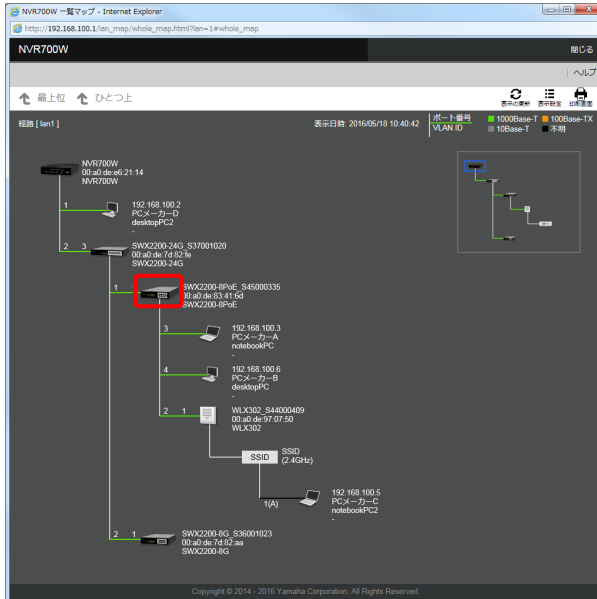
一覧マップが表示され、ネットワークに接続されている機器全体がトポロジーで確認できます。

## 第 11 章 LAN マップを利用する

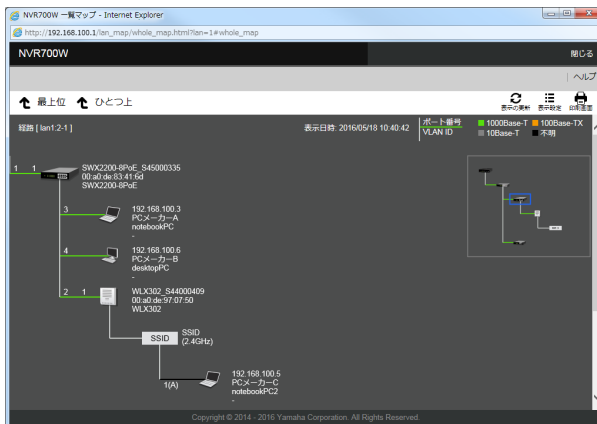
### メモ

- ・「」ボタンをクリックすると、「スレープ一覧」画面の表示が、コントローラーが保持している最新の情報に更新されます。
- ・「」ボタンをクリックすると、一覧マップで表示される機器の情報を設定することができます。




### 2. 各機器のアイコンをクリックする。



配下のスレープのみの表示に切り替わります。



### メモ

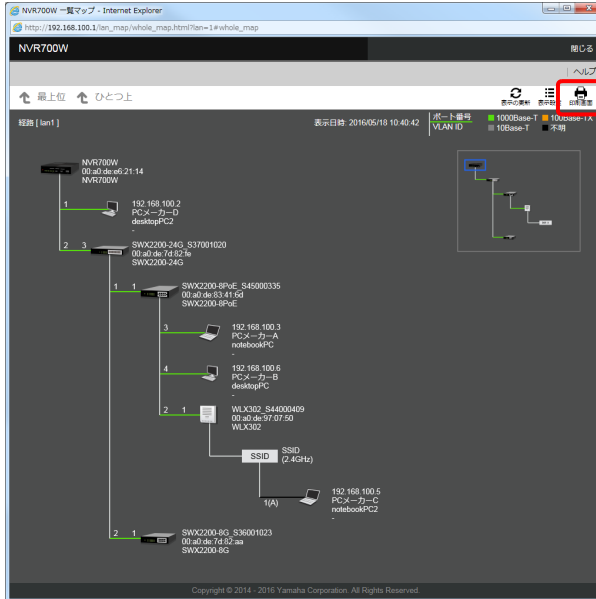
- ・画面右のマップ内で青枠で囲われている機器 () は、現在表示されているトポロジーの起点にあたる機器を示しています。
- ・「 最上位」ボタンまたは「 ひとつ上」ボタンをクリックすると、コントローラーを起点としたトポロジー全体や、ひとつ上の機器を起点とした範囲に戻ります。

### 11.11.11 一覧マップを印刷する

印刷画面を表示して、一覧マップを印刷することができます。

印刷機能を使用する場合は Firefox 以外の推奨 Web ブラウザーからご利用ください。一覧マップはひとつの SVG 画像となっています。Firefox はひとつの SVG 画像の複数枚印刷に対応していないため、印刷対象の一覧マップが大きく印刷枚数が 2 枚以上になる場合、正しく印刷されません。

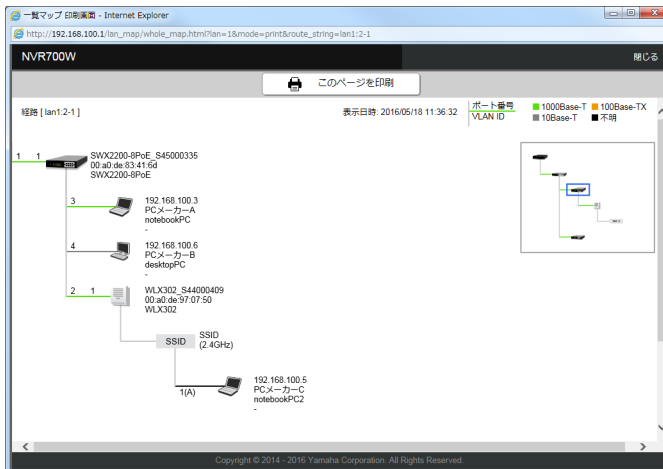
#### 1. 一覧マップで「印刷」ボタンをクリックする。



印刷画面が表示されます。

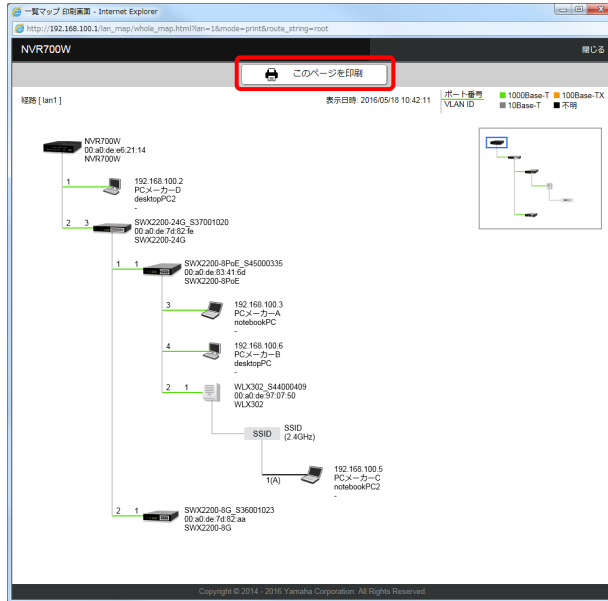
#### メモ

- 一覧マップでトポロジーの起点となる機器の表示を変えている場合は、印刷画面でも同じトポロジーが表示されます。



## 第 11 章 LAN マップを利用する

### 2. 「このページを印刷」 ボタンをクリックする。



プリンターの選択画面が表示されます。

### 3. プリンターを選択し、必要に応じて印刷設定をして印刷する。 一覧マップが印刷されます。



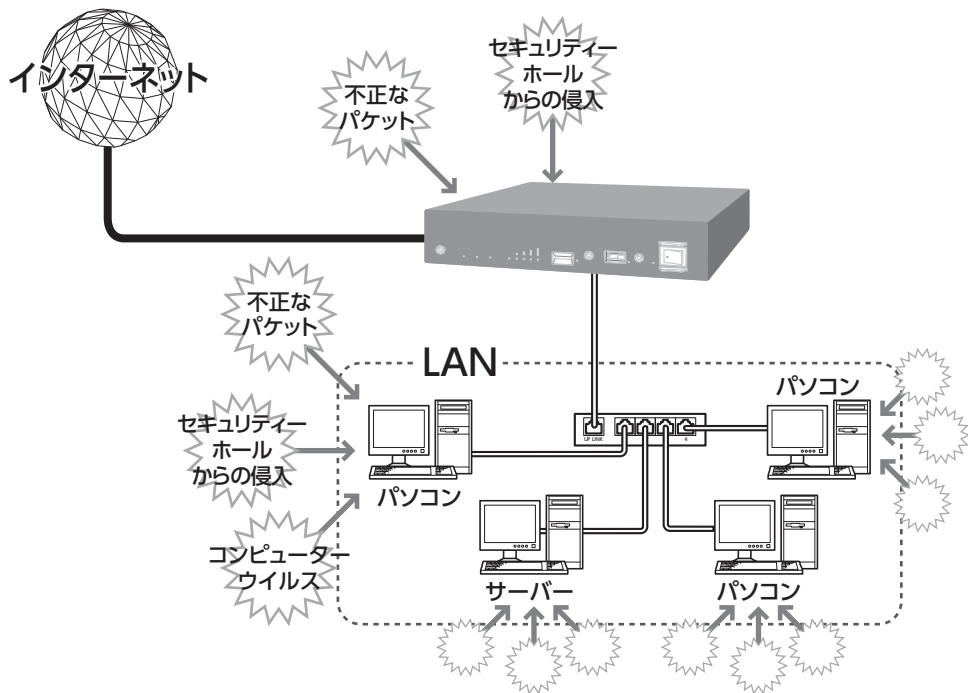
## 第 12 章 セキュリティーを強化する

本章では、セキュリティーについて説明します。インターネットに接続している間は、悪意のある者からルーターやパソコンがアタック（不正アクセス）される可能性があります。不正アクセスによりルーターの設定が変更されたり、パソコンのシステムやデータを破壊された場合、多大なデータの被害や金銭的被害に遭うことも十分に考えられます。ヤマハルーターのフィルター設定などのセキュリティー対策を行って、自己防衛してください。

- ・ 不正アクセスとは？ …237 ページ
- ・ 不正アクセスに対抗する …238 ページ
- ・ フィルターとは？ …239 ページ
- ・ ヤマハルーターへのアクセスを管理する …252 ページ

### 12.1 不正アクセスとは？

悪意のある者からルーターやパソコンがアタック（不正アクセス）され、ルーターの設定が変更されたり、パソコンのシステムやデータを破壊されたりします。ルーターを介してパソコンを接続している場合は、NAT や IP マスカレードといったアドレス変換機能によってインターネット側から内部の LAN へ侵入することができなくなるため、比較的安全が保たれますが、設定の誤りや不足によって、同様の危険にさらされる場合があります。また、インターネット経由の不正アクセスだけでなく、マルウェアによる攻撃にも注意が必要です。



#### 12.1.1 グローバル IP アドレスが割り当てられている場合

悪意を持った者がアタックを行うときに主な足がかりにするのが「グローバル IP アドレス」です。同じグローバル IP アドレスを長時間使用している場合は、不正アクセスの被害に遭う確率が高くなります。固定 IP アドレスサービスの利用時やネットワーク型接続、接続時に割り当てられた動的アドレスを使い続けるブロードバンド回線を使用する場合は、十分なセキュリティー対策を行うことをおすすめいたします。

## 第 12 章 セキュリティーを強化する

### 12.1.2 パスワードを設定していない場合

ヤマハルーターにパスワードを設定しない状態で使用することは、セキュリティ上大変危険です。単にパスワードを設定するだけでなく、定期的にパスワードを変更するようにしてください。

## 12.2 不正アクセスに対抗する

インターネットの不正アクセスは、いくつかの侵入経路に分けられます。それぞれの侵入経路に合った対策をしてください。

### ご注意

- ・ 不正アクセスの手段やセキュリティ上の抜け道 / 穴（セキュリティホール）は、日夜新たに発見されています。ヤマハルーターの機能を含めて、すべての問題を解決できる完璧なセキュリティ対策は存在せず、インターネット接続には常に危険があることをご理解ください。常に新しい情報入手し、お客様の自己責任でセキュリティ対策を強化することを強くおすすめいたします。
- ・ ヤマハルーターを使用した結果により発生したあらゆる損失について、弊社では一切その責任を負いかねますので、あらかじめご了承ください。

### 12.2.1 不正アクセスによる侵入

インターネット側から内部の LAN への侵入を防ぐには、以下の対応が効果的です。

- ・ インターネット接続の切断
- ・ グローバル IP アドレスの変更
- ・ パケットフィルタリング式ファイアウォールの導入
- ・ アプリケーション・ゲートウェイ式ファイアウォールソフトウェアの導入

#### ヤマハルーターで可能な対策

- ・ 自動切断機能の設定  
接続 / 切断のたびに動的 IP アドレスを変更できます。ただし、サーバー公開用途にヤマハルーターを使用する場合には、この対策を実施することは困難となりますので、サーバー側で対策を行ってください。
- ・ フィルターの設定  
攻撃に使用される特定の種類のパケットを通さないようにフィルターを設定する（239 ページ）ことで、その攻撃を防御できることがあります。

### 12.2.2 OS やサーバーソフトウェアのセキュリティホールからの侵入

OS やサーバーソフトウェアのバージョンアップや、適切な設定 / 運用を行うことが効果的です。

#### ヤマハルーターで可能な対策

- ・ Web GUI へのアクセス制限の設定  
ヤマハルーターの設定を変更できるホストを制限して、悪意のある第三者がヤマハルーターの設定を勝手に変更することを防止できます（252 ページ）。
- ・ フィルターの設定  
攻撃に使用される特定の種類のパケットを通さないようにフィルターを設定する（239 ページ）ことで、その攻撃を防御できることがあります。

### 12.2.3 電子メールの添付ファイルからの侵入

電子メールに添付されたコンピューターウイルスを開くことで感染します。不審な添付ファイルは開かないことを徹底するだけでなく、パソコンにウイルス検知ソフトウェアをインストールして、ウイルスを早期発見 / 早期駆除することで、被害を最小限に抑えることができます。

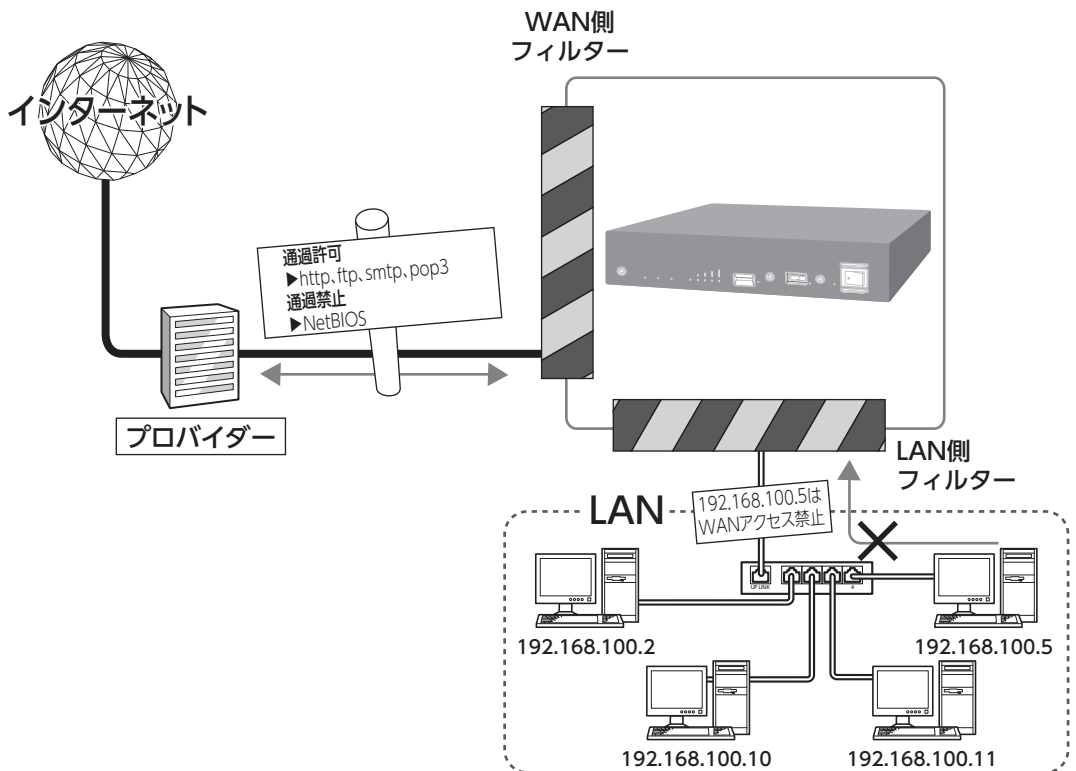
### ヤマハルーターで可能な対策

- ・ メールセキュリティ機能の使用

ヤマハのファイアウォール製品ではメールセキュリティ機能を搭載しています。ファイアウォール製品をヤマハルーターと併用することで、パソコンごとに個別にウイルス検知ソフトウェアをインストールしていない環境でも、コンピューターウイルスの感染を防御できるようになります。

## 12.3 フィルターとは？

ヤマハルーターでは、接続先ごとに 100 個までのフィルターを設定できます。それぞれのフィルターでパケットの送信元や宛先、パケットの種類、プロトコルの種類、方向によって、パケットを通さないよう設定できます。不正アクセスに使われやすいパケットや、正常な通信では発生しない作為的なパケットをルーター通過時に破棄するように設定することで、不正なパケットが LAN 内に入ることを防ぐことができます。



### 12.3.1 ヤマハルーターのフィルターの特徴

#### 静的フィルターと動的フィルター

ヤマハルーターで設定できるフィルターには、次の 2 種類があります。各々の利点を理解し、それぞれのフィルターを併用することをおすすめします。

- ・ 静的フィルター：一度設定を行うと、データや通信の有無にかかわらず常に有効になります。
- ・ 動的フィルター：通信状態を監視しながら、必要に応じてフィルターが有効になります。例えば「通常はインターネットから LAN への通信はすべて禁止にしておき、LAN 側から FTP の通信が発生したときに、インターネット側からはその応答だけ通過を許可する」といった設定ができます。

#### プロバイダー接続時のフィルター設定

「かんたん設定」からプロバイダー接続の設定を行った場合は、「フィルターの設定」画面（32 ページ）で選択した内容に応じて基本的なフィルターが自動的に適用されます。この基本的なフィルターに加え、必要に応じてフィルターを追加することができます。

### ご注意

コマンドコンソール画面からプロバイダー接続の設定を行った場合は、フィルターは何も登録されていない状態になります。

### フィルター番号

ヤマハルーターに設定できるフィルター番号は 1 ~ 21474836 ですが、Web GUI から自動的にフィルターが適用される際に不整合が生じないように、Web GUI では用途に応じて所定の番号範囲が予約されています。以下に Web GUI で予約されているフィルター番号を示します。コマンドコンソール画面からフィルターを追加していて、そのフィルターの番号がここに挙げられた番号と重複している場合は、Web GUI で設定変更を行うとフィルターの設定が意図せず上書きされることがあることにご注意ください。

使用用途	フィルター番号
LAN/WAN/ONU インターフェース用	100000 ~ 149999
PP インターフェース用	200000 ~ 299999
内蔵無線 WAN インターフェース用	300000 ~ 399999
フィルター型ルーティング用	500000 ~ 599999

### ご注意

- ・ 設定を間違えるとインターネットからのアクセスに対して無防備になってしまうことがあるため、フィルターの設定変更は機能を十分にご理解のうえ、慎重に行ってください。
- ・ フィルターを多く適用すると処理が複雑になり、インターネットへのアクセス速度が遅くなる場合があります。

## 12.3.2 フィルター設定の基本

フィルターを設定するときは、以下の考え方を基本にすることをおすすめします。

### LAN 側からインターネット側へのアクセス（出力方向）は原則許可し、必要に応じて禁止する

LAN 側からインターネット側へのアクセスを厳しく規制すると非常に使いにくいものになり、管理や設定変更の手間がかかります。原則自由としたうえで、問題があればその部分だけ制限します。

### インターネット側から LAN 側へのアクセス（入力方向）は原則禁止し、必要に応じて許可する

インターネット側から LAN 側へのアクセスは、原則禁止して外部からのアクセスを防ぎます。Web サーバーの公開など、必要がある場合にのみ、最低限のアクセスだけを許可します。

### ご注意

インターネット側からのアクセスとは、インターネット側から開始する通信のことを指します。

### 12.3.3 PING を許可する相手を限定する

静的フィルターを設定して、インターネット経由で PING を許可する外部の端末を限定します。固定 IP アドレスが設定されている端末からの PING を許可する場合を例に説明します。

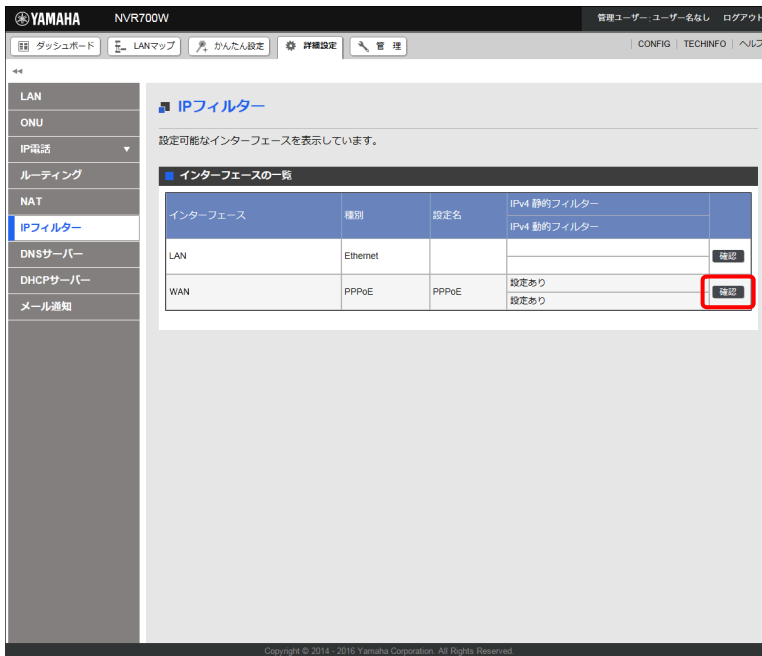
#### 設定例

PING を許可する外部端末の IP アドレス：203.0.113.2

#### メモ


- ・本章では「かんたん設定」を使用して WAN インターフェースに PPPoE 接続型のプロバイダーが設定されている状態（「4.1.2 「PPPoE 接続」の場合」（30 ページ）の設定が完了している状態）から設定を行うという前提で説明します。
- ・フィルターの設定を誤ると Web GUI へのアクセスもできなくなることがあります。Web GUI へのアクセスができなくなった場合は、シリアルケーブルでヤマハルーターに接続し、シリアルコンソール画面からフィルターの設定を修正するか、ヤマハルーターの設定を工場出荷状態に戻す必要があります。フィルターの設定は慎重に行ってください。

1. 「詳細設定」タブ - 「IP フィルター」を順に選択する。  
「IP フィルター」画面が表示されます。
2. 「インターフェースの一覧」項目の WAN インターフェースの「確認」ボタンをクリックする。



「適用されている IP フィルターの一覧」画面が表示されます。

## 第 12 章 セキュリティーを強化する

3. 「静的フィルター」項目の「」ボタンをクリックする。




「インターフェースへの適用の設定」画面が表示されます。

4. 「WANに適用する静的フィルター」項目でプロトコルが「ICMP」のフィルターの「設定」ボタンをクリックする。

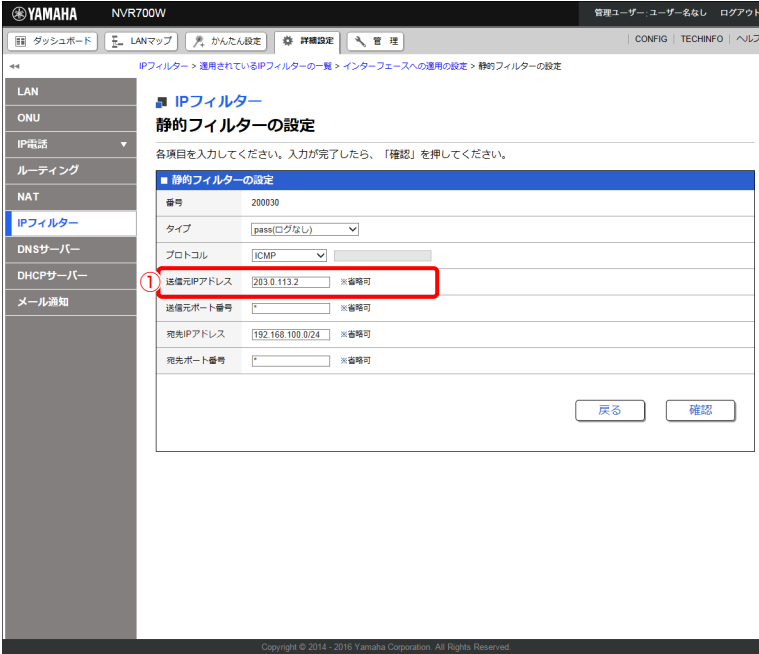


「静的フィルターの設定」画面が表示されます。

## メモ

「ICMP」のフィルターがない場合は、「静的フィルター」項目の「」ボタンをクリックし ICMP フィルターを追加してください。また、新規に追加した ICMP フィルターは、ドラッグ & ドロップで「静的フィルター」項目から「WAN に適用する静的フィルター」項目へ移動する必要があります。

## 5. 静的フィルターを編集する。



The screenshot shows the '静的フィルターの設定' (Static Filter Settings) page in the Yamaha NVR700W Web GUI. The page title is 'IPフィルター' (IP Filter). Below the title, there is a section for '静的フィルターの設定' (Static Filter Settings) with the following fields:

番号	200030
タイプ	pass(ログなし)
プロトコル	ICMP
送信元IPアドレス	203.0.113.2 ※省略可
送信元ポート番号	* ※省略可
宛先IPアドレス	192.168.100.0/24 ※省略可
宛先ポート番号	* ※省略可

The '送信元IPアドレス' (Send IP Address) field is highlighted with a red box and a circled '1'.

① 送信元 IP アドレス：  
「203.0.113.2」を入力します。

6. 「確認」ボタンをクリックする。  
「入力内容の確認」画面が表示されます。

## 第 12 章 セキュリティーを強化する

### 7. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「インターフェースへの適用の設定」画面が表示されます。

### 12.3.4 PING をすべて破棄する

静的フィルターを設定して、インターネット側から来た PING をすべて破棄します。

#### メモ

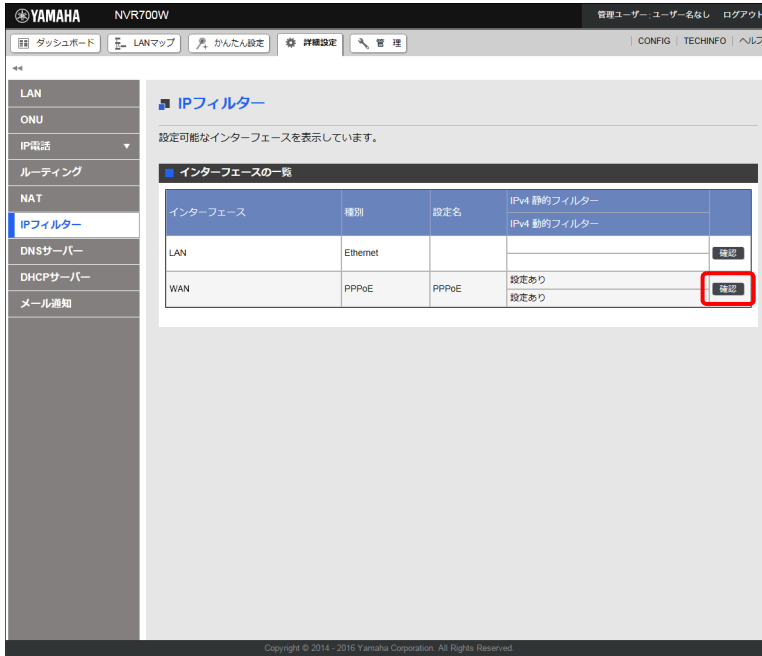
- ・本章では「かんたん設定」を使用して WAN インターフェースに PPPoE 接続型のプロバイダーが設定されている状態（「4.1.2 「PPPoE 接続」の場合」（30 ページ）の設定が完了している状態）から設定を行うという前提で説明します。
- ・フィルターの設定を誤ると Web GUI へのアクセスもできなくなることがあります。Web GUI へのアクセスができなくなった場合は、シリアルケーブルでヤマハルーターに接続し、シリアルコンソール画面からフィルターの設定を修正するか、ヤマハルーターの設定を工場出荷状態に戻す必要があります。フィルターの設定は慎重に行ってください。

#### 1. 「詳細設定」タブ - 「IP フィルター」を順に選択する。


「IP フィルター」画面が表示されます。



2. 「インターフェースの一覧」項目のWAN インターフェースの「確認」ボタンをクリックする。



「適用されている IP フィルターの一覧」画面が表示されます。

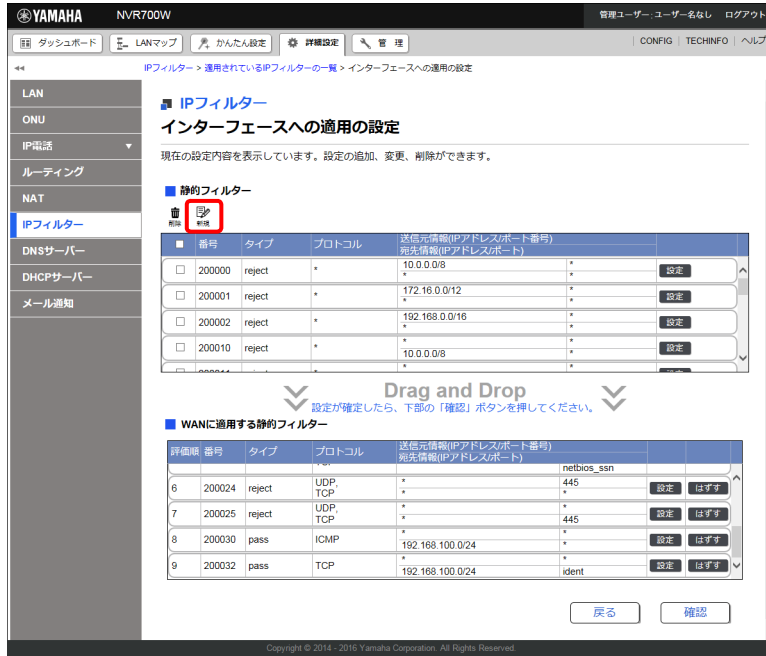
3. 「静的フィルター」項目の「」ボタンをクリックする。



「インターフェースへの適用の設定」画面が表示されます。

## 第 12 章 セキュリティーを強化する

### 4. 「静的フィルター」項目の「」ボタンをクリックする。



静的フィルター

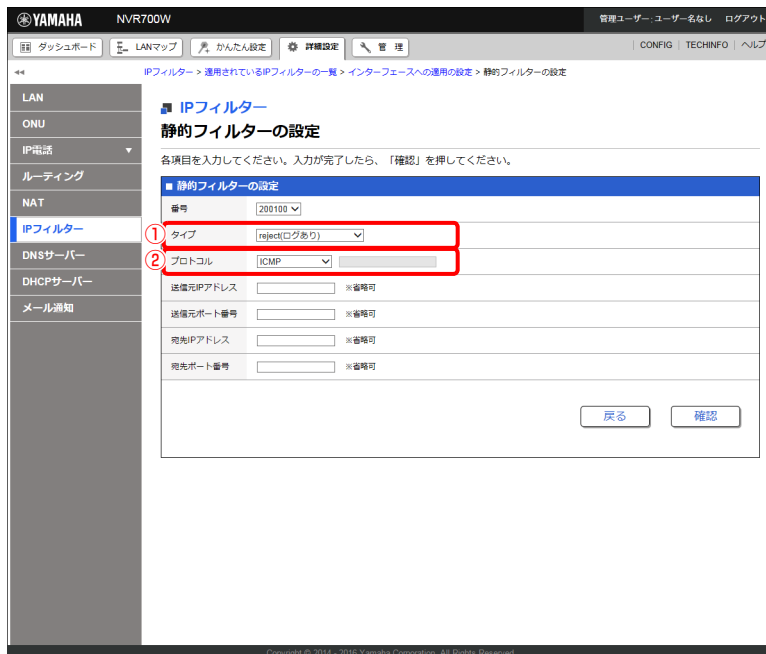
番号	タイプ	プロトコル	送信元情報(IPアドレス:ポート番号)	宛先情報(IPアドレス:ポート)	
200000	reject	*	10.0.0.0/8	*	設定
200001	reject	*	172.16.0.0/12	*	設定
200002	reject	*	192.168.0.0/16	*	設定
200010	reject	*	10.0.0.0/8	*	設定

静的フィルター

評価順	番号	タイプ	プロトコル	送信元情報(IPアドレス:ポート番号)	宛先情報(IPアドレス:ポート)		
6	200024	reject	UDP	*	445	設定	はずす
7	200025	reject	TCP	*	445	設定	はずす
8	200030	pass	ICMP	192.168.100.0/24	*	設定	はずす
9	200032	pass	TCP	192.168.100.0/24	ident	設定	はずす

「静的フィルターの設定」画面が表示されます。

### 5. 静的フィルターを設定する。



静的フィルターの設定

静的フィルターの設定

各項目を入力してください。入力が完了したら、「確認」を押してください。

静的フィルターの設定

番号: 200100

① タイプ: reject (ログあり)

② プロトコル: ICMP

送信元IPアドレス: ※省略可

送信元ポート番号: ※省略可

宛先IPアドレス: ※省略可

宛先ポート番号: ※省略可

① タイプ：  
「reject (ログあり)」を選択します。

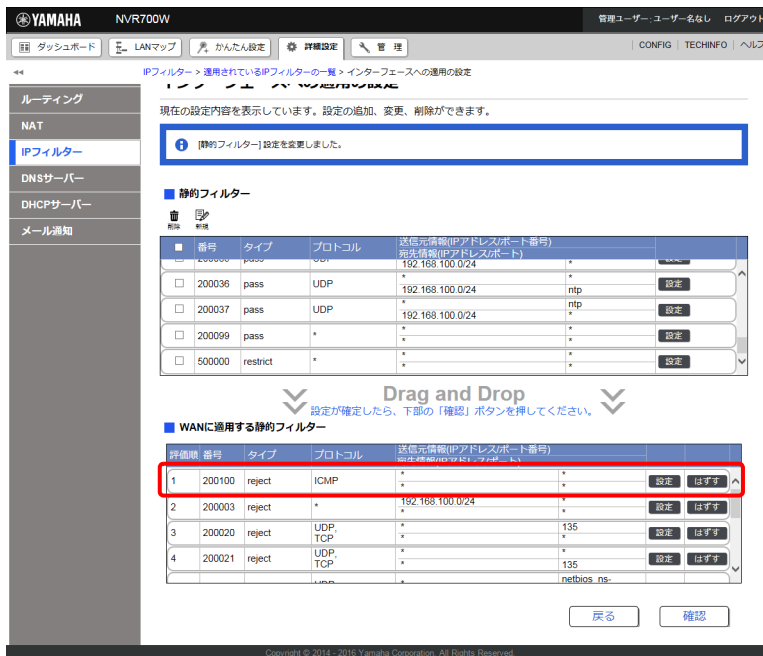
② プロトコル：  
「ICMP」を選択します。

6. 「確認」 ボタンをクリックする。  
「入力内容の確認」画面が表示されます。
7. 内容を確認し、「設定の確定」 ボタンをクリックする。



「インターフェースへの適用の設定」画面が表示されます。

8. 「静的フィルター」項目から「WANに適用する静的フィルター」項目の先頭に、作成したフィルター設定をドラッグ & ドロップする。



9. 「確認」 ボタンをクリックする。  
「入力内容の確認」画面が表示されます。

## 第 12 章 セキュリティーを強化する

### 10. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「インターフェースへの適用の設定」画面が表示されます。

### 12.3.5 特定の端末だけ Web アクセスを許可する

動的フィルターを設定して、LAN 内の特定の端末だけ、外部の Web サーバーへのアクセスを許可します。

#### 設定例

外部の Web サーバーへのアクセスを許可する端末の IP アドレス：192.168.100.2

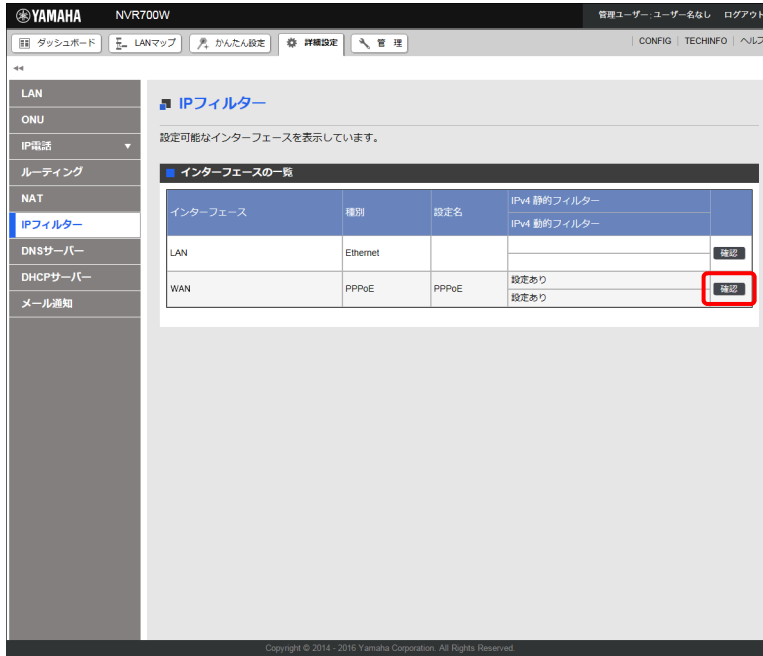
#### メモ

- ・ 本章では「かんたん設定」を使用して WAN インターフェースに PPPoE 接続型のプロバイダーが設定されている状態（「4.1.2 「PPPoE 接続」の場合」（30 ページ）の設定が完了している状態）から設定を行うという前提で説明します。
- ・ フィルターの設定を誤ると Web GUI へのアクセスもできなくなることがあります。Web GUI へのアクセスができなくなった場合は、シリアルケーブルでヤマハルーターに接続し、シリアルコンソール画面からフィルターの設定を修正するか、ヤマハルーターの設定を工場出荷状態に戻す必要があります。フィルターの設定は慎重に行ってください。

#### 1. 「詳細設定」タブ - 「IP フィルター」を順に選択する。

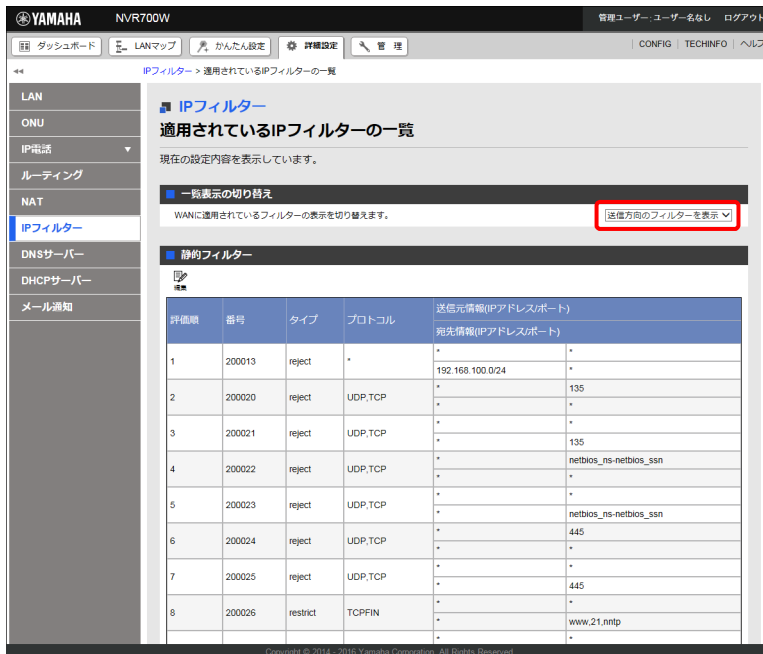
「IP フィルター」画面が表示されます。

2. 「インターフェースの一覧」項目のWAN インターフェースの「確認」ボタンをクリックする。




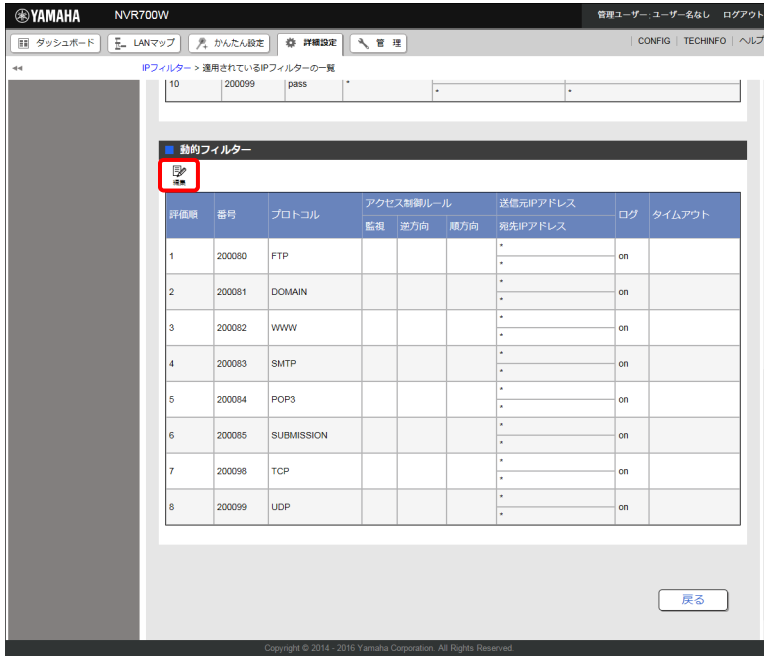
「適用されている IP フィルターの一覧」画面が表示されます。

3. 「一覧表示の切り替え」項目のプルダウンメニューから「送信方向のフィルターを表示」を選択する。



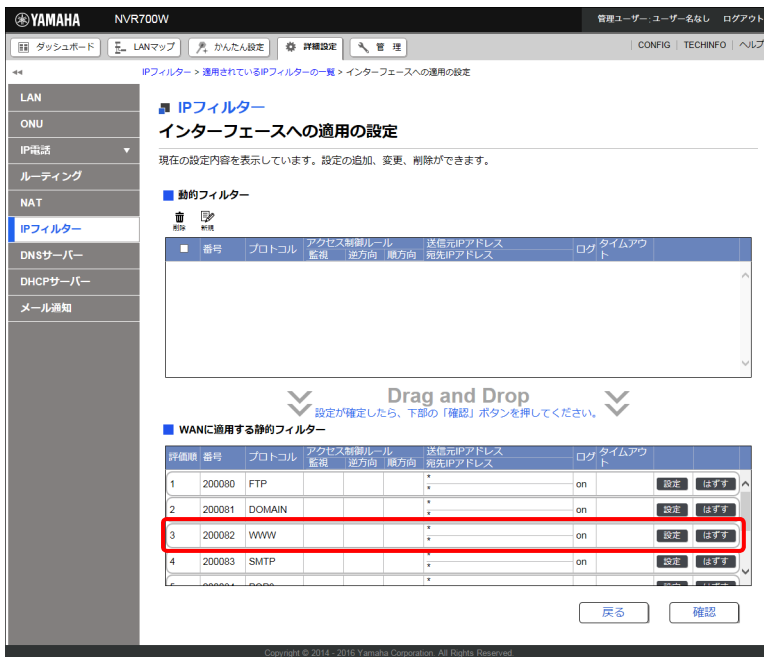
## 第 12 章 セキュリティーを強化する

4. 「動的フィルター」項目の「」ボタンをクリックする。




「インターフェースへの適用の設定」画面が表示されます。

5. 「WANに適用する動的フィルター」項目でプロトコルが「WWW」のフィルターの「設定」ボタンをクリックする。

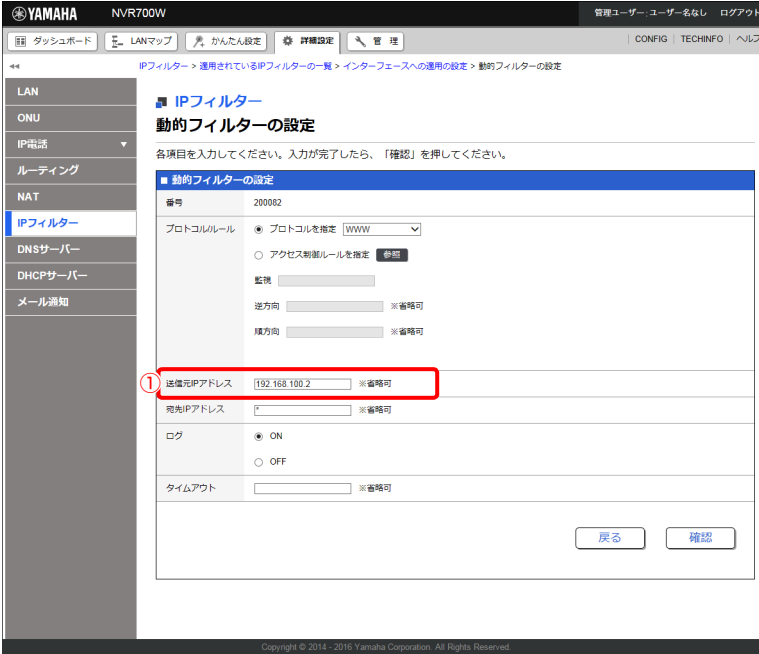


「動的フィルターの設定」画面が表示されます。

## メモ

「WWW」のフィルターがない場合は、「動的フィルター」項目の「」ボタンをクリックし WWW フィルターを追加してください。また、新規に追加した WWW 新規 フィルターは、ドラッグ & ドロップで「動的フィルター」項目から「WAN に適用する動的フィルター」項目へ移動する必要があります。

## 6. 動的フィルターを設定する。



The screenshot shows the '動的フィルターの設定' (Dynamic Filter Settings) page in the Yamaha NVR700W Web GUI. The page title is 'IPフィルター' (IP Filter). Below the title, there is a section for '動的フィルターの設定' (Dynamic Filter Settings) with the following fields and options:

- 番号 (Number): 200002
- プロトコルルール (Protocol Rule):  プロトコルを指定 | WWW (selected),  アクセス制御ルールを指定 | 伊部 (disabled)
- 監視 (Monitoring):
- 逆方向 (Reverse):  ※省略可
- 順方向 (Forward):  ※省略可
- 送信元IPアドレス (Send IP Address):  ※省略可 (highlighted with a red box and a circled '1')
- 宛先IPアドレス (Destination IP Address):  ※省略可
- ログ (Log):  ON,  OFF
- タイムアウト (Timeout):  ※省略可

At the bottom right, there are two buttons: '戻る' (Back) and '確認' (Confirm).

- ① 送信元 IP アドレス：  
「192.168.100.2」を入力します。

7. 「確認」ボタンをクリックする。  
「入力内容の確認」画面が表示されます。

## 第 12 章 セキュリティーを強化する

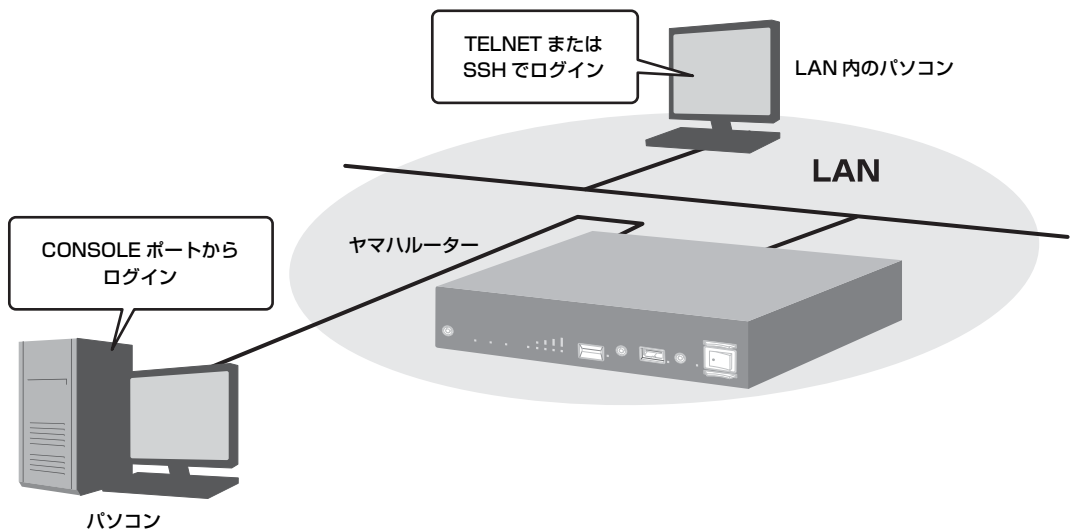
### 8. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「インターフェースへの適用の設定」画面が表示されます。

## 12.4 ヤマハルーターへのアクセスを管理する

ヤマハルーターへのアクセスを許可するユーザーを限定したり、接続手段を限定したりすることができます。セキュリティを確保するために、これらの機能を活用し、必要最低限のアクセスだけ許可するように設定することをおすすめいたします。





### 12.4.1 ログインを許可するユーザーを登録する

ユーザーを登録して、ヤマハルーターにログインできるユーザーを制限します。

#### 設定例


ユーザー名：user

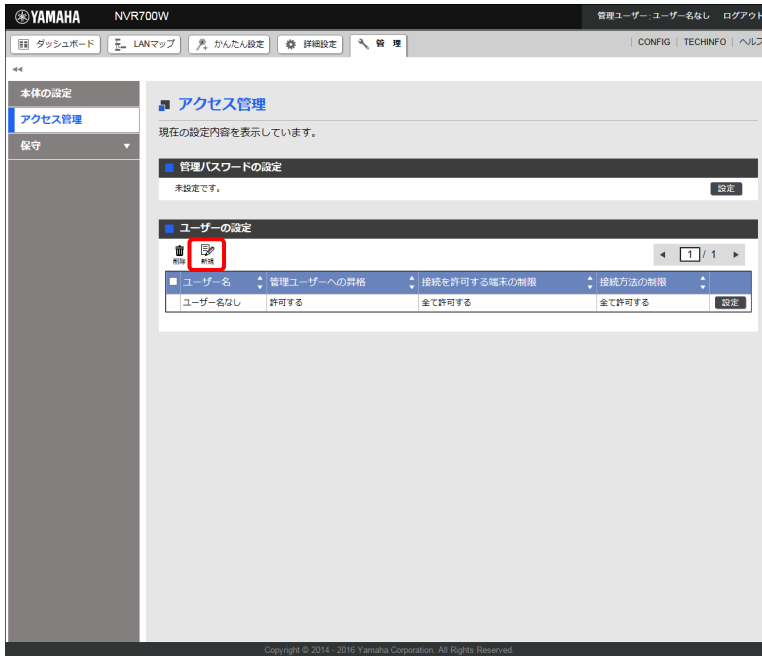
パスワード：password

管理ユーザーへの昇格：許可

Web GUI 画面の閲覧の許可：全て許可する

同一ユーザー名による複数接続：許可

1. 「管理」タブ - 「アクセス管理」を順に選択する。  
「アクセス管理」画面が表示されます。
2. 「ユーザーの設定」項目の「」ボタンをクリックする。



「ユーザーの設定」画面が表示されます。

## 第 12 章 セキュリティーを強化する

### 3. ユーザー情報を設定する。

① ユーザー名：

「user」を入力します。

② 新しいパスワード：

「password」を入力します。入力したパスワードは、●で表示されます。

③ 新しいパスワード（確認）：

「password」を入力します。入力したパスワードは、●で表示されます。

④ 管理ユーザーへの昇格：

「許可する」を選択します。

⑤ Web GUI 画面の閲覧の許可：

「全て許可する」を選択します。

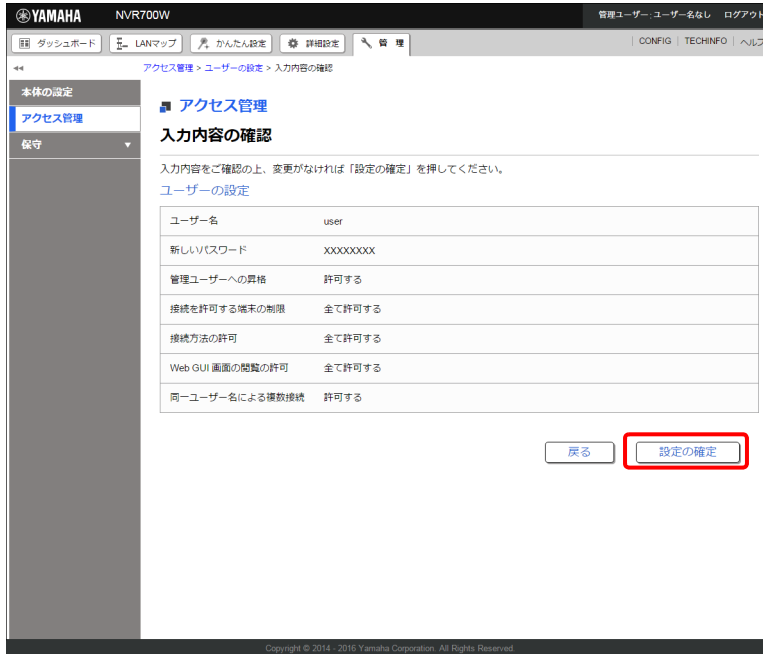
⑥ 同一ユーザー名による複数接続：

「許可する」を選択します。

## メモ

実際に設定するパスワードは、数字や記号を混ぜたり、できるだけ長くするなど、類推しにくい文字列にすることをおすすめいたします。

4. 「確認」 ボタンをクリックする。  
「入力内容の確認」画面が表示されます。
5. 内容を確認し、「設定の確定」 ボタンをクリックする。



設定が反映され、「アクセス管理」画面が表示されます。

### 12.4.2 アクセス方法を変更する

ユーザーごとに、ヤマハルーターへのアクセス方法を制限します。IP アドレスにより接続を許可する端末を制限したり、Web ブラウザー（HTTP）や TELNET など接続方法の制限をしたりします。

#### 設定例

アクセス制限を行うユーザー：user

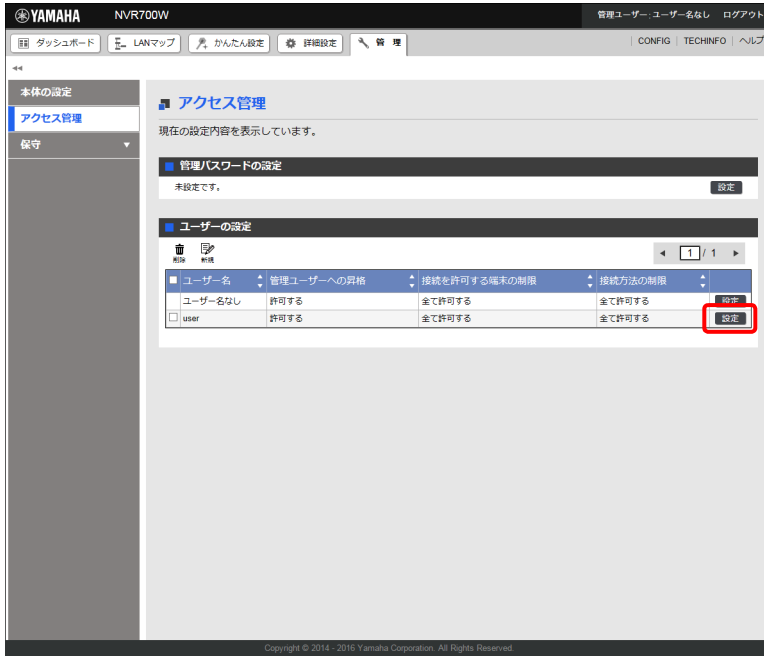
接続を許可する端末の IP アドレス：192.168.100.2

接続方法の制限：TELNET、HTTP

1. 「管理」タブ - 「アクセス管理」を順に選択する。  
「アクセス管理」画面が表示されます。

## 第 12 章 セキュリティーを強化する

### 2. 「ユーザーの設定」項目の user の「設定」ボタンをクリックする。



「ユーザーの設定」画面が表示されます。

## 3. ユーザー情報を設定する。

YAMAHA NVR700W 管理ユーザー ユーザー名なし ログアウト

ダッシュボード LANマップ かんたん設定 詳細設定 管理

アクセス管理 > ユーザーの設定

本体の設定  
アクセス管理  
保守

### アクセス管理 ユーザーの設定

各項目を入力してください。入力完了したら、「確認」を押してください。

#### 設定に必要な情報入力

ユーザー名

新しいパスワード

パスワード強度

新しいパスワード (確認)

管理ユーザーへの資格

許可する  
 許可しない

接続を許可する端末の制限

全て許可する  
 指定したIPアドレスを許可する

接続方法の許可

全て許可する  
 全て許可しない  
 指定した接続方法を許可する

シリアルコンソール  
 TELNET  
 SSH  
 SFTP  
 リモートセットアップ  
 HTTP

Web GUI 画面の閲覧の許可

全て許可する  
 指定した画面の閲覧を許可する

ダッシュボード画面  
 LANマップ画面  
 設定情報を閲覧できる画面 (かんたん設定、詳細設定、管理、CONFIG、TECHINFO)

同一ユーザー名による複数接続

許可する  
 許可しない

Copyright © 2014 - 2016 Yamaha Corporation. All Rights Reserved.

## ① 接続を許可する端末の制限：

「指定した IP アドレスを許可する」を選択し、「192.168.100.2」を入力します。

## ② 接続方法の許可：

「指定した接続方法を許可する」を選択し、「TELNET」と「HTTP」にチェックを入れます。

## 4. 「確認」ボタンをクリックする。

「入力内容の確認」画面が表示されます。

## 第 12 章 セキュリティーを強化する

### 5. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「アクセス管理」画面が表示されます。

### 12.4.3 パスワードを変更する

ユーザーのパスワードを変更します。定期的なパスワードの変更は、セキュリティ対策として効果的です。

#### 設定例

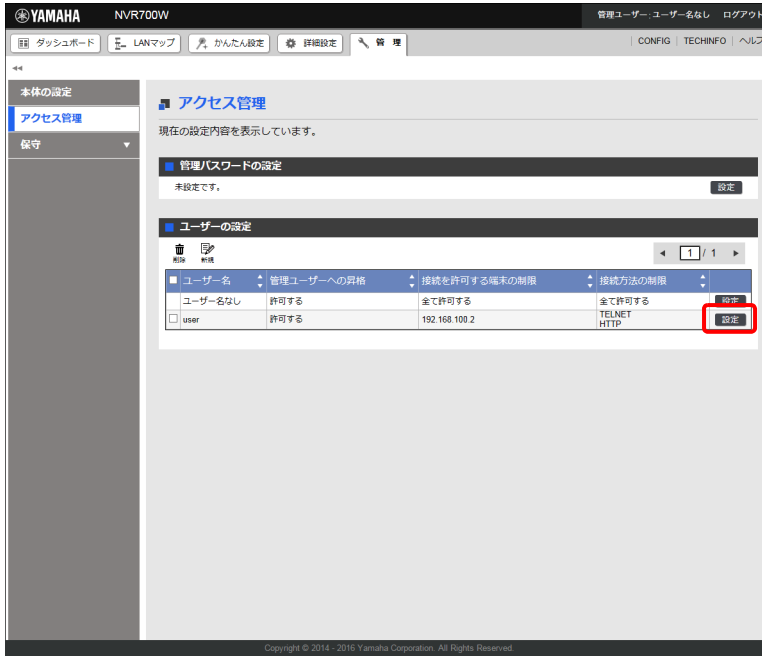
パスワードを変更するユーザー：user

パスワード：yamaha

#### 1. 「管理」タブ - 「アクセス管理」を順に選択する。

「アクセス管理」画面が表示されます。

## 2. 「ユーザーの設定」項目の user の「設定」ボタンをクリックする。



「ユーザーの設定」画面が表示されます。

## 第 12 章 セキュリティーを強化する

### 3. パスワードを設定する。

YAMAHA NVR700W 管理ユーザー ユーザー名なし ログアウト

ダッシュボード LANマップ かんたん設定 詳細設定 管理 CONFIG TECHINFO ヘルプ

アクセス管理 > ユーザーの設定

本体の設定  
アクセス管理  
保守

### アクセス管理 ユーザーの設定

各項目を入力してください。入力が完了したら、「確認」を押してください。

#### 設定に必要な情報入力

ユーザー名

新しいパスワード

パスワード強度 **弱** 中 強 最強

⚠️ パスワードを以下のように変更することを推奨します。  
パスワードが短いです。  
英大文字を含めてください。  
数字を含めてください。  
記号を含めてください。  
いろいろな文字を使用してください。

新しいパスワード (確認)

管理ユーザーへの権限  許可する  
 許可しない

接続を許可する端末の制限  全て許可する  
 指定したIPアドレスを許可する

接続方法の許可  全て許可する  
 全て許可しない  
 指定した接続方法を許可する  
 シリアルコンソール  
 TELNET  
 SSH  
 SFTP  
 リモートセットアップ  
 HTTP

Web GUI 画面の閲覧の許可  全て許可する  
 指定した画面の閲覧を許可する  
 ダッシュボード画面  
 LANマップ画面  
 設定情報を閲覧できる画面 (かんたん設定、詳細設定、管理、CONFIG、TECHINFO)

同一ユーザー名による複数接続  許可する  
 許可しない

Copyright © 2014 - 2016 Yamaha Corporation. All Rights Reserved.

#### ① 新しいパスワード：

「yamaha」を入力します。入力したパスワードは、●で表示されます。

#### ② 新しいパスワード (確認)：

「yamaha」を入力します。入力したパスワードは、●で表示されます。

### メモ

実際に設定するパスワードは、数字や記号を混ぜたり、できるだけ長くするなど、類推しにくい文字列にすることをおすすめいたします。

### 4. 「確認」 ボタンをクリックする。

「入力内容の確認」画面が表示されます。



## 5. 内容を確認し、「設定の確定」ボタンをクリックする。

The screenshot shows the Yamaha NVR700W Web GUI. The main menu on the left includes '本体の設定' (Device Settings), 'アクセス管理' (Access Management), and '保守' (Maintenance). The 'アクセス管理' section is expanded to show 'アクセス管理' (Access Management) and '入力内容の確認' (Confirm Input Content). The '入力内容の確認' section contains the following table:

ユーザーの設定	
ユーザー名	user
新しいパスワード	XXXXXX
管理ユーザーへの昇格	許可する
接続を許可する端末の制限	192.168.100.2
接続方法の許可	TELNET HTTP
Web GUI 画面の閲覧の許可	全て許可する
同一ユーザー名による複数接続	許可する

At the bottom right of the page, there are two buttons: '戻る' (Back) and '設定の確定' (Confirm Settings). The '設定の確定' button is highlighted with a red box.

設定が反映され、「アクセス管理」画面が表示されます。

# 第 13 章 詳細設定を行う

本章では、「詳細設定」画面にある各種設定メニューを活用して、外部にサーバーを公開したり、複数の WAN 回線を主回線とバックアップ回線で使い分けたりするなど、ヤマハルーターの応用的な設定について説明します。

- ・ LAN のアドレスを設定する …262 ページ
- ・ ONU のアドレスを設定する …271 ページ
- ・ TEL ポートを設定する …274 ページ
- ・ グローバル IP アドレスを複数の端末でシェアする …276 ページ
- ・ 外部にサーバーを公開する …281 ページ
- ・ 複数のプロバイダーを使用する …293 ページ
- ・ DNS サーバーを設定する …314 ページ
- ・ DHCP で端末に IP アドレスを割り当てる …320 ページ
- ・ 異なるセグメントの DHCP サーバーから端末に IP アドレスを割り当てる …325 ページ
- ・ メール通知機能を使う …327 ページ

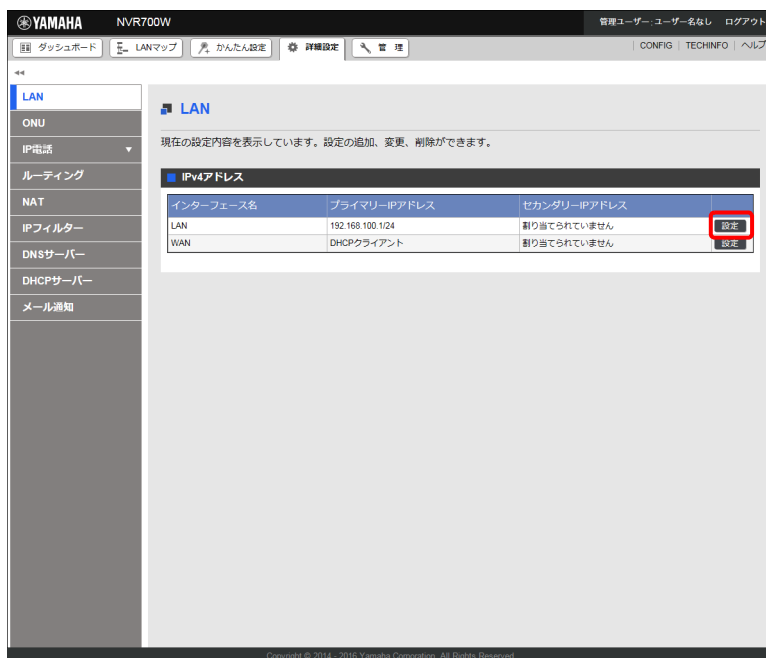
## 13.1 LAN のアドレスを設定する

ヤマハルーターの LAN のプライマリー IP アドレスを固定で設定します。

### メモ

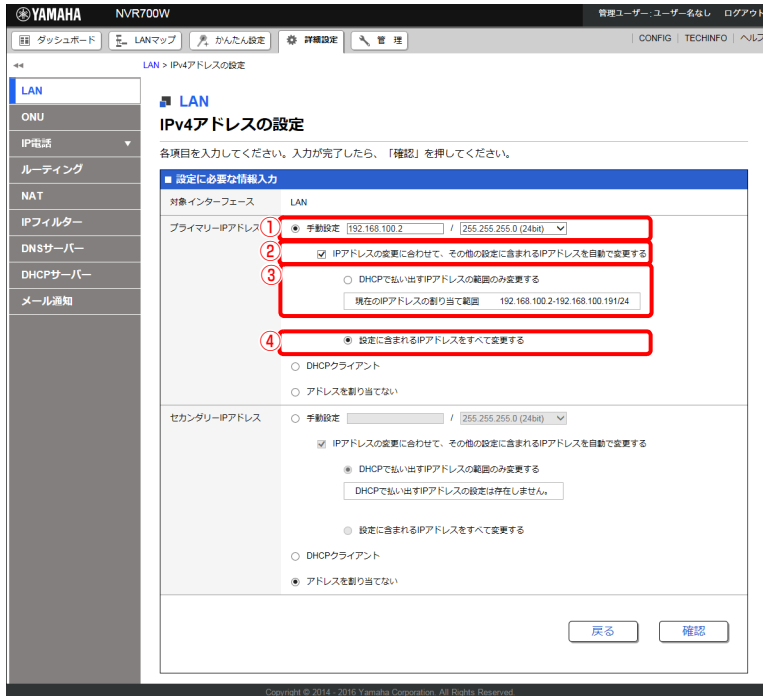
「かんたん設定」を使用してプロバイダー接続の設定が完了している場合は、プロバイダー接続の設定と同時に IP マスカレードも自動的に設定されるため、本章の操作は不要になります。

1. 「詳細設定」タブ - 「LAN」を順に選択する。  
「LAN」画面が表示されます。
2. 「LAN」の「設定」ボタンをクリックする。



「IPv4 アドレスの設定」画面が表示されます。

## 3. LAN の IP アドレスを設定する。



## ① アドレス入力欄：

「手動設定」を選択し、新しく設定するIPv4アドレスを入力します。ネットマスクは、「192.0.0.0 (2bit)」から「255.255.255.252(30bit)」までの中から選択します。

## ② IPアドレスの変更に合わせて、その他の設定に含まれるIPアドレスを自動で変更する：

選択するとLANインターフェースのIPアドレスの設定変更に合わせて、その他の設定に含まれるIPアドレスのパラメーターを自動的に変換します。

選択しないときは、IPアドレスの変更後に必要に応じて手動で設定を行ってください。

## ③ DHCPで払い出すIPアドレスの範囲のみ変更する：

選択すると、新しいIPアドレスに合わせてDHCPの設定を自動的に変更します。

## ④ 設定に含まれるIPアドレスをすべて変更する：

選択すると、新しいIPアドレスに合わせて各種設定のIPアドレス設定を自動的に変更します。対象となる設定は以下のとおりです。

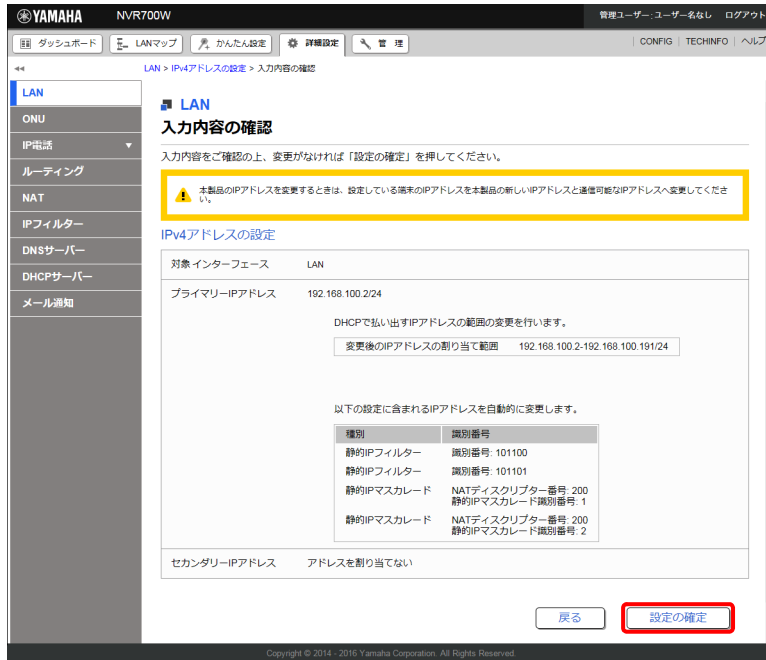
- 静的IPフィルター（始点IPアドレス、終点IPアドレス）
- 動的IPフィルター（始点IPアドレス、終点IPアドレス）
- NAT ディスクリプター内側アドレス
- NAT ディスクリプター静的NAT（内側アドレス）
- NAT ディスクリプター変換ルールに該当しないパケットの処理（転送先端末のアドレス）
- NAT ディスクリプター静的IPマスカレード（内側アドレス）
- DHCPで払い出すIPアドレス
- IPキーブライブ（始点IPアドレス）
- トンネルインターフェース 端点IPアドレス（ローカルIPアドレス）

## 4. 「確認」ボタンをクリックする。

「入力内容の確認」画面が表示されます。

## 第 13 章 詳細設定を行う

### 5. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が変更され、「LAN アドレスの変更」画面が表示されます。「LAN アドレスの変更」画面の指示にしたがって、Web GUI に再ログインしてください。

### 13.1.1 WAN のアドレスを設定する

ヤマハルーターの WAN のプライマリ IP アドレスを固定で設定します。

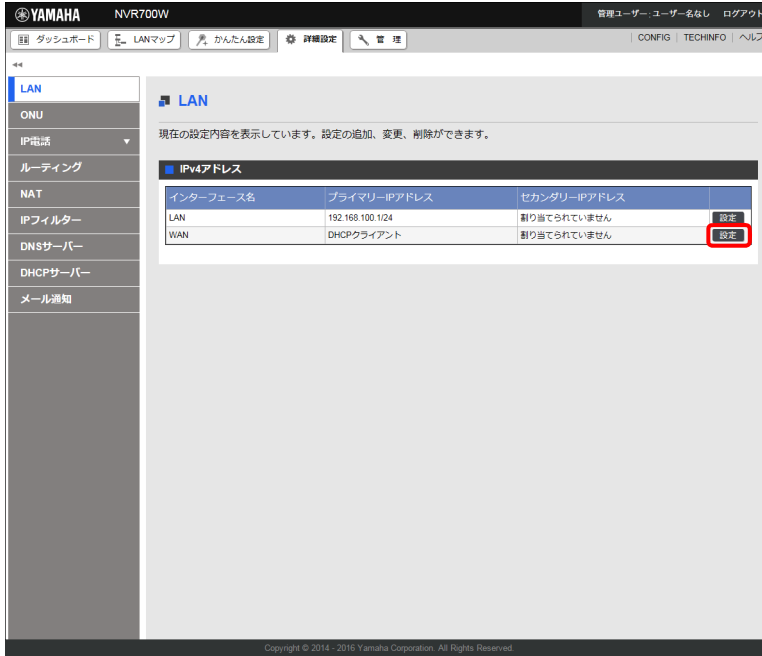
#### 設定例

設定するインターフェース：WAN

#### 1. 「詳細設定」タブ - 「LAN」を順に選択する。

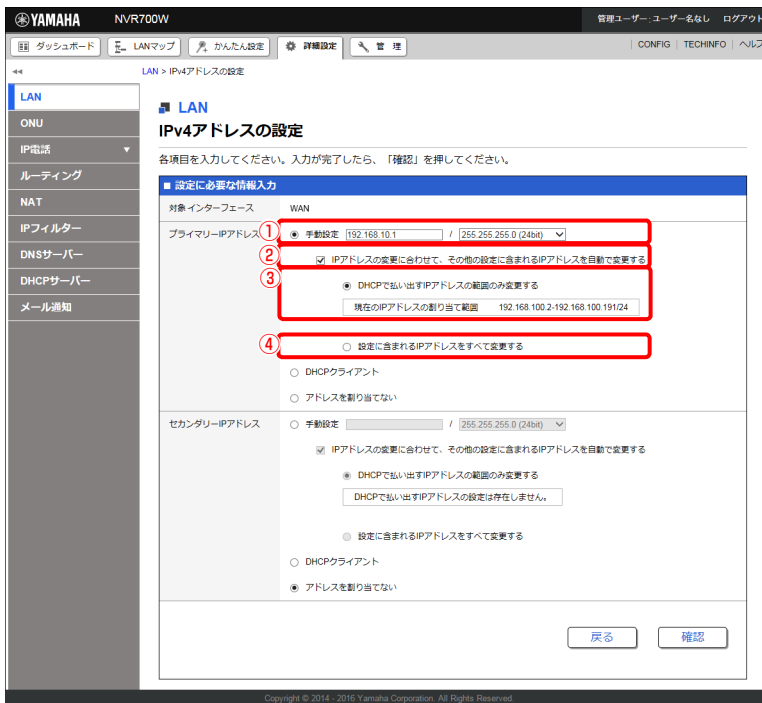
「LAN」画面が表示されます。

## 2. 「WAN」の「設定」ボタンをクリックする。



「IPv4 アドレスの設定」画面が表示されます。

## 3. WANのIPアドレスを設定する。



## ① アドレス入力欄：

「手動設定」を選択し、新しく設定するIPv4アドレスを入力します。ネットマスクは、「192.0.0.0 (2bit)」から「255.255.255.252(30bit)」までの中から選択します。

## 第 13 章 詳細設定を行う

### ② IP アドレスの変更に合わせて、その他の設定に含まれる IP アドレスを自動で変更する：

選択すると LAN インターフェースの IP アドレスの設定変更に合わせて、その他の設定に含まれる IP アドレスのパラメーターを自動的に変換します。

選択しないときは、IP アドレスの変更に必要に応じて手動で設定を行ってください。

### ③ DHCP で払い出す IP アドレスの範囲のみ変更する：

選択すると、新しい IP アドレスに合わせて DHCP の設定を自動的に変更します。

### ④ 設定に含まれる IP アドレスをすべて変更する：

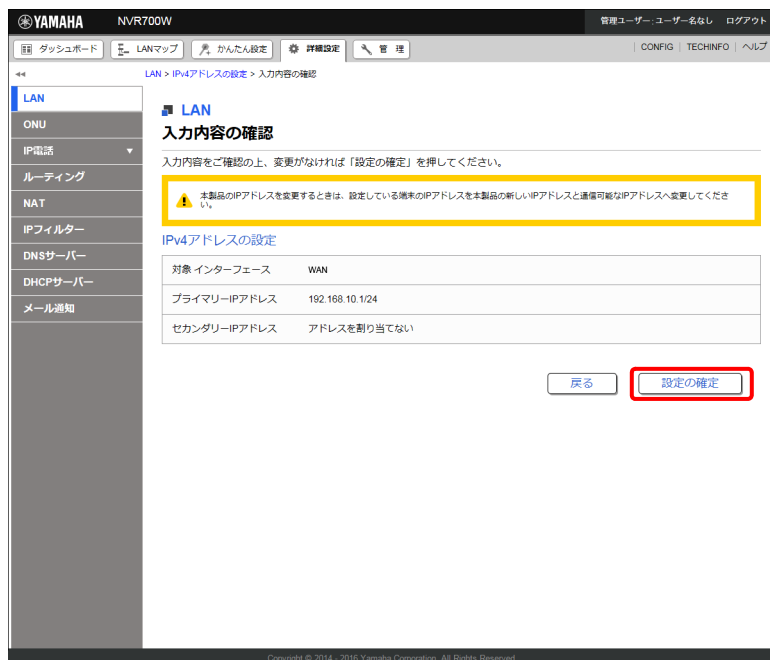
選択すると、新しい IP アドレスに合わせて各種設定の IP アドレス設定を自動的に変更します。対象となる設定は以下のとおりです。

- 静的 IP フィルター（始点 IP アドレス、終点 IP アドレス）
- 動的 IP フィルター（始点 IP アドレス、終点 IP アドレス）
- NAT ディスクリプター内側アドレス
- NAT ディスクリプター静的 NAT（内側アドレス）
- NAT ディスクリプター変換ルールに該当しないパケットの処理（転送先端末のアドレス）
- NAT ディスクリプター静的 IP マスカレード（内側アドレス）
- DHCP で払い出す IP アドレス
- IP キープアライブ（始点 IP アドレス）
- トンネルインターフェース 端点 IP アドレス（ローカル IP アドレス）

#### 4. 「確認」ボタンをクリックする。

「入力内容の確認」画面が表示されます。

#### 5. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が変更され、「WAN アドレスの変更」画面が表示されます。「WAN アドレスの変更」画面の指示にしたがって、Web GUI に再ログインしてください。

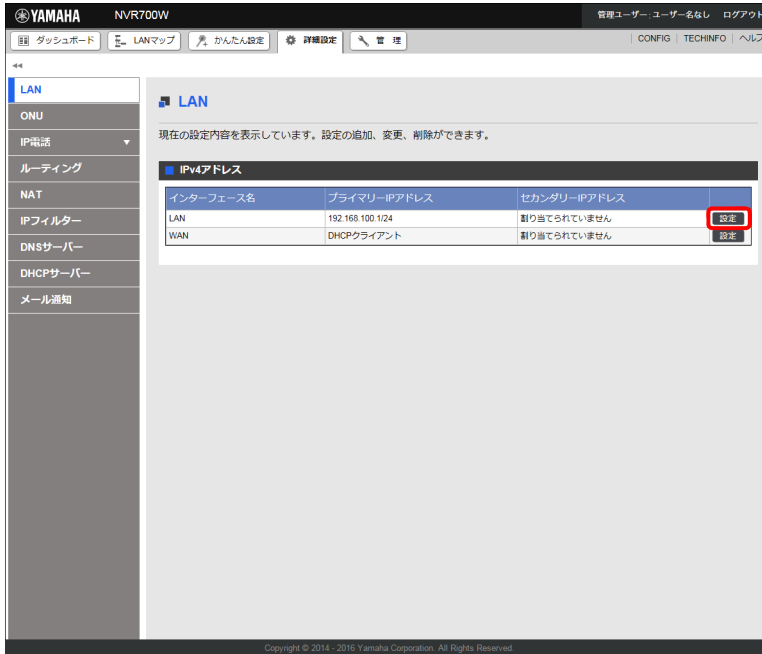
### 13.1.2 セカンダリー IP アドレスも設定する

ヤマハルーターの LAN または WAN のセカンダリー IP アドレスを固定で設定します。

#### 設定例

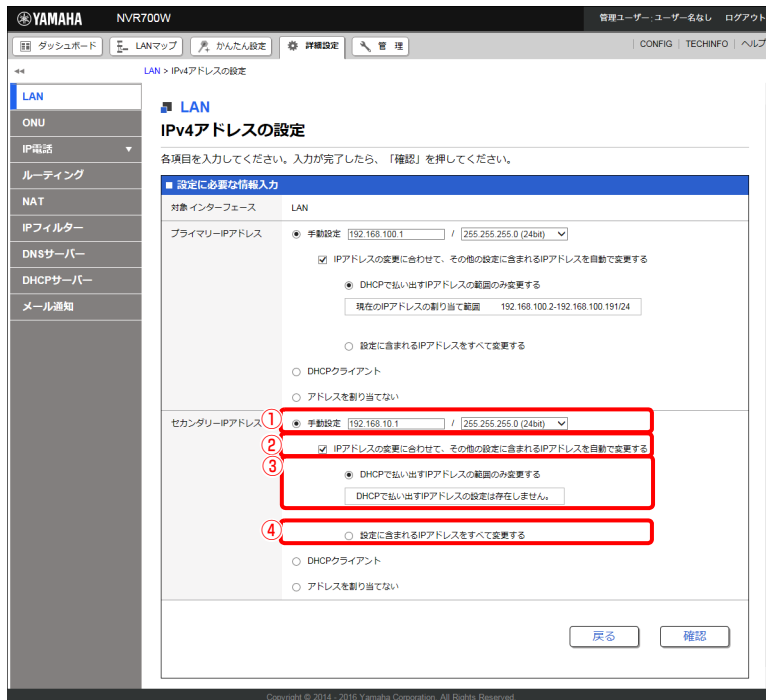
設定するインターフェース：LAN

1. 「詳細設定」タブ - 「LAN」を順に選択する。  
「LAN」画面が表示されます。
2. 「LAN」の「設定」ボタンをクリックする。



「IPv4 アドレスの設定」画面が表示されます。

3. LAN のセカンダリー IP アドレスを設定する。



① アドレス入力欄：

「手動設定」を選択し、新しく設定する IPv4 アドレスを入力します。ネットマスクは、「192.0.0.0 (2bit)」から「255.255.255.252(30bit)」までの中から選択します。

② IP アドレスの変更に合わせて、その他の設定に含まれる IP アドレスを自動で変更する：

選択すると LAN インターフェースの IP アドレスの設定変更に合わせて、その他の設定に含まれる IP アドレスのパラメーターを自動的に変換します。

選択すると、新しい IP アドレスに合わせて DHCP の設定を自動的に変更します。

③ DHCP で払い出す IP アドレスの範囲のみ変更する：

選択すると、新しい IP アドレスに合わせて DHCP の設定を自動的に変更します。

④ 設定に含まれる IP アドレスをすべて変更する：

選択すると、新しい IP アドレスに合わせて各種設定の IP アドレス設定を自動的に変更します。対象となる設定は以下のとおりです。

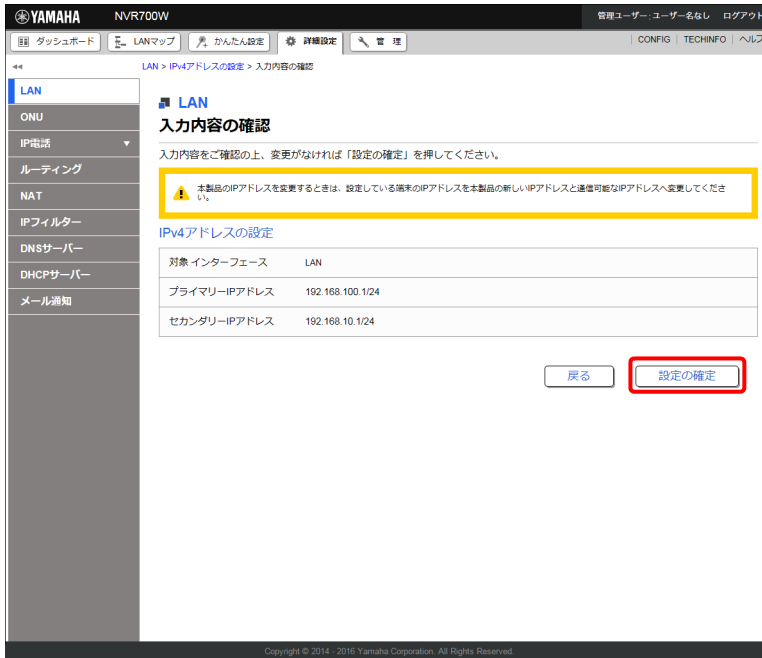
- 静的 IP フィルター（始点 IP アドレス、終点 IP アドレス）
- 動的 IP フィルター（始点 IP アドレス、終点 IP アドレス）
- NAT ディスクリプター内側アドレス
- NAT ディスクリプター静的 NAT（内側アドレス）
- NAT ディスクリプター変換ルールに該当しないパケットの処理（転送先端末のアドレス）
- NAT ディスクリプター静的 IP マスカレード（内側アドレス）
- DHCP で払い出す IP アドレス
- IP キープアライブ（始点 IP アドレス）
- トンネルインターフェース 端点 IP アドレス（ローカル IP アドレス）

4. 「確認」ボタンをクリックする。

「入力内容の確認」画面が表示されます。



## 5. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が変更され、「LAN アドレスの変更」画面が表示されます。「LAN アドレスの変更」画面の指示にしたがって、Web GUI に再ログインしてください。

## 13.1.3 固定ではなく DHCP で設定する

ヤマハルーターの LAN または WAN のプライマリー IP アドレスまたはセカンダリー IP アドレスを DHCP で取得します。

## 設定例

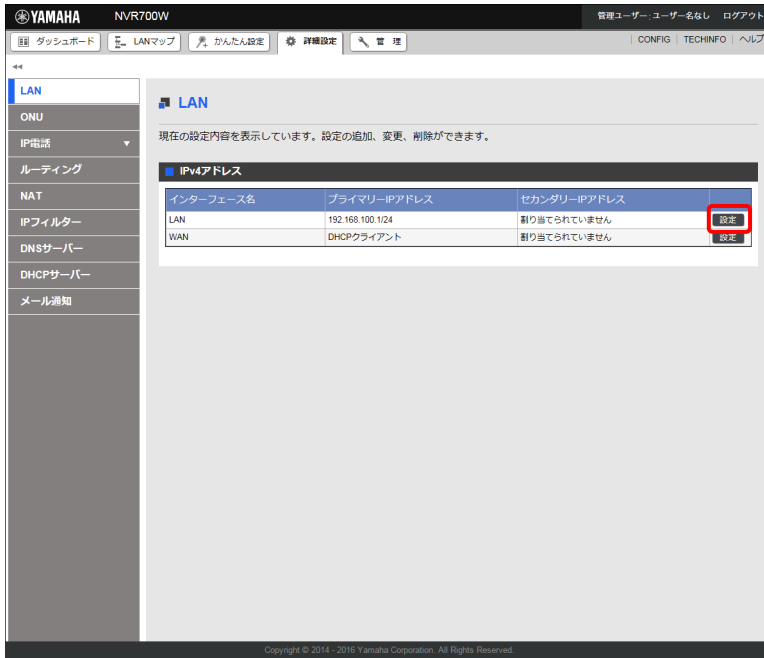
設定するインターフェース：LAN

DHCP で取得する IP アドレス：プライマリー IP アドレス

1. 「詳細設定」タブ - 「LAN」を順に選択する。  
「LAN」画面が表示されます。

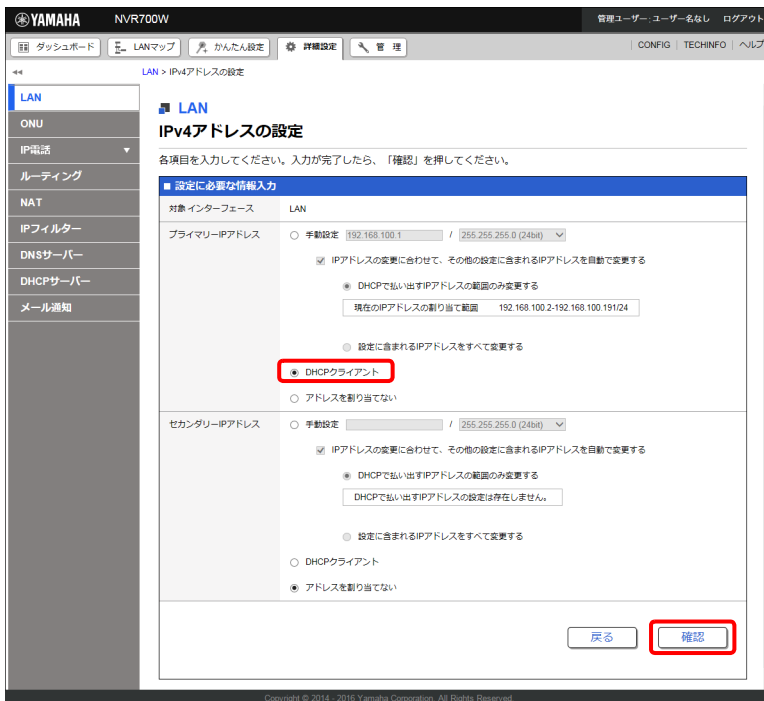
## 第 13 章 詳細設定を行う

### 2. 「LAN」の「設定」ボタンをクリックする。



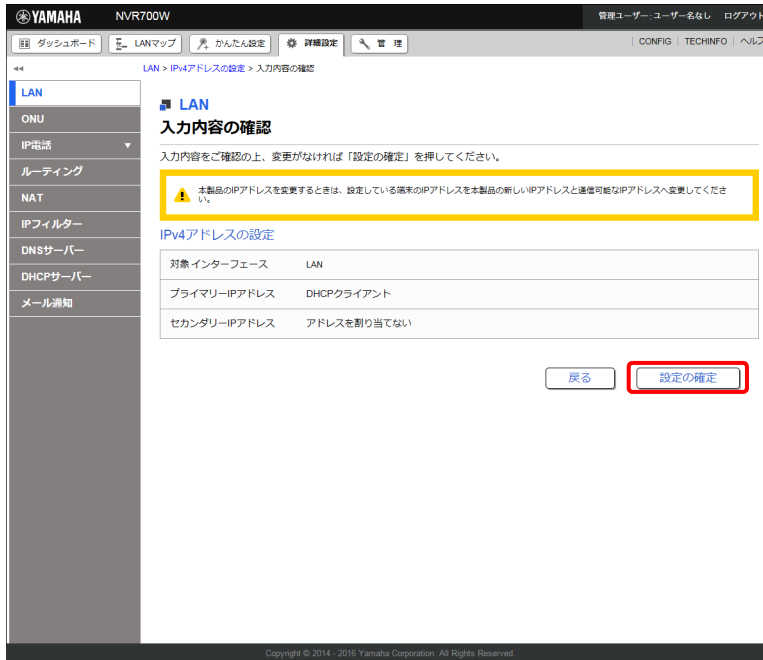
「IPv4 アドレスの設定」画面が表示されます。

### 3. プライマリ IP アドレスの「DHCP クライアント」を選択し、「確認」ボタンをクリックする。



「入力内容の確認」画面が表示されます。

## 4. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が変更され、「LAN アドレスの変更」画面が表示されます。「LAN アドレスの変更」画面の指示にしたがって、Web GUI に再ログインしてください。

**ご注意**

プライマリー IP アドレス、セカンダリー IP アドレスの両方を「DHCP クライアント」に設定することはできません。

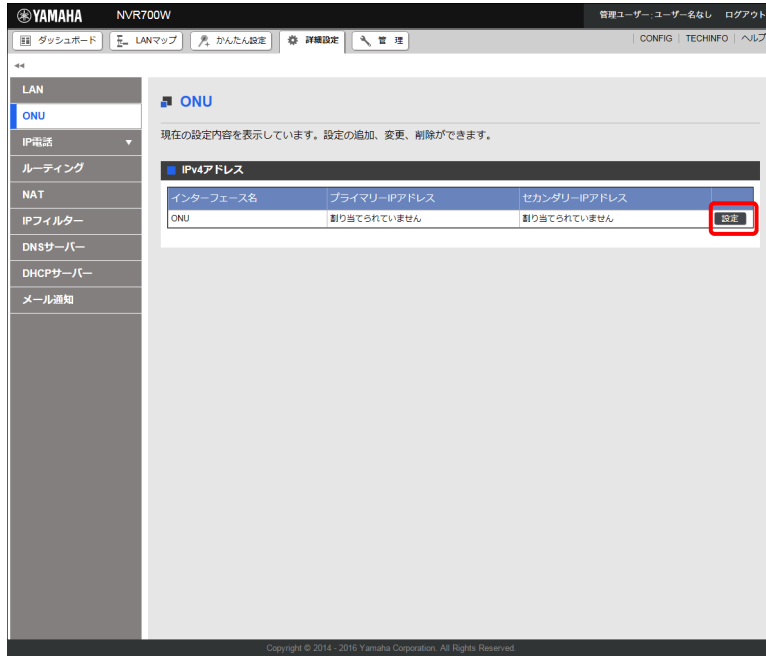
## 13.2 ONU のアドレスを設定する

ヤマハルーターの ONU ポートに接続した小型 ONU のプライマリー IP アドレスを固定で設定します。

1. 「詳細設定」タブ - 「ONU」を順に選択する。  
「ONU」画面が表示されます。

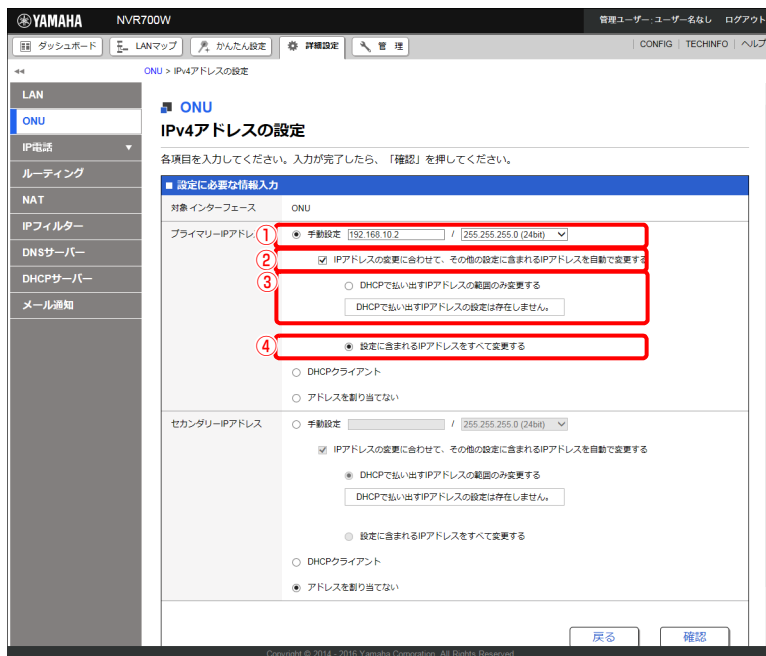
## 第 13 章 詳細設定を行う

### 2. 「ONU」の「設定」ボタンをクリックする。



「IPv4 アドレスの設定」画面が表示されます。

### 3. ONUのIPアドレスを設定する。



#### ① アドレス入力欄：

「手動設定」を選択し、新しく設定する IPv4 アドレスを入力します。ネットマスクは、「192.0.0.0 (2bit)」から「255.255.255.252(30bit)」までの中から選択します。

## ② IP アドレスの変更に合わせて、その他の設定に含まれる IP アドレスを自動で変更する：

選択すると ONU インターフェースの IP アドレスの設定変更に合わせて、その他の設定に含まれる IP アドレスのパラメーターを自動的に変換します。

選択しないときは、IP アドレスの変更後に必要に応じて手動で設定を行ってください。

## ③ DHCP で払い出す IP アドレスの範囲のみ変更する：

選択すると、新しい IP アドレスに合わせて DHCP の設定を自動的に変更します。

## ④ 設定に含まれる IP アドレスをすべて変更する：

選択すると、新しい IP アドレスに合わせて各種設定の IP アドレス設定を自動的に変更します。対象となる設定は以下のとおりです。

- 静的 IP フィルター (始点 IP アドレス、終点 IP アドレス)
- 動的 IP フィルター (始点 IP アドレス、終点 IP アドレス)
- NAT ディスクリプター内側アドレス
- NAT ディスクリプター静的 NAT (内側アドレス)
- NAT ディスクリプター変換ルールに該当しないパケットの処理 (転送先端末のアドレス)
- NAT ディスクリプター静的 IP マスカレード (内側アドレス)
- DHCP で払い出す IP アドレス
- IP キーブライブ (始点 IP アドレス)
- トンネルインターフェース 端点 IP アドレス (ローカル IP アドレス)

## 4. 「確認」 ボタンをクリックする。

「入力内容の確認」画面が表示されます。

## 5. 内容を確認し、「設定の確定」 ボタンをクリックする。

YAMAHA NVR700W 管理ユーザー:ユーザー名なし ログアウト

ONU > IPv4アドレスの設定 > 入力内容の確認

LAN

ONU

入力内容の確認

入力内容をご確認の上、変更があれば「設定の確定」を押してください。

⚠ 本製品のIPアドレスを変更するときは、設定している端末のIPアドレスを本製品の新しいIPアドレスと通信可能なIPアドレスへ変更してください。

IPv4アドレスの設定

対象 インターフェース ONU

プライマリIPアドレス 192.168.10.1/24

以下の設定については、IPアドレスを自動的に変更できません。  
設定を変更する必要がある場合は、各機能の設定ページから変更を行ってください。

リストを別ウィンドウで開く

種別	識別番号
静的IPフィルター	識別番号: 101002
静的IPフィルター	識別番号: 101012
静的IPフィルター	識別番号: 101100
静的IPフィルター	識別番号: 101101
静的IPフィルター	識別番号: 101102
静的IPマスカレード	NATディスクリプター番号: 200 静的IPマスカレード識別番号: 1
静的IPマスカレード	NATディスクリプター番号: 200 静的IPマスカレード識別番号: 2
静的IPマスカレード	NATディスクリプター番号: 200 静的IPマスカレード識別番号: 3

セカンダリーIPアドレス アドレスを割り当てない

戻る 設定の確定

Copyright © 2014 - 2016 Yamaha Corporation. All Rights Reserved.

設定が変更され、「ONU アドレスの変更」画面が表示されます。「ONU アドレスの変更」画面の指示にしたがって、Web GUI に再ログインしてください。

## 第 13 章 詳細設定を行う

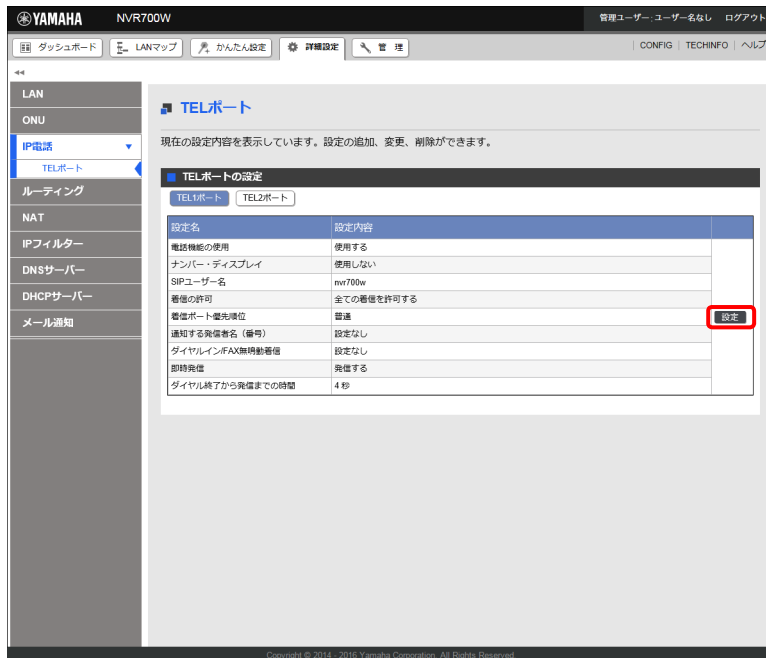
### メモ

ONU のアドレスも LAN 同様にセカンダリーアドレスと DHCP の設定ができます。「IPv4 アドレスの設定」画面を表示させ、「13.1.2 セカンダリー IP アドレスも設定する」(267 ページ) または「13.1.2 セカンダリー IP アドレスも設定する」(267 ページ) と同様の手順で設定してください。

## 13.3 TEL ポートを設定する

ヤマハルーターの TEL1 ポートおよび TEL2 ポートの詳細設定を行います。

1. 「詳細設定」タブ - 「IP 電話」 - 「TEL ポート」を順に選択する。  
「TEL ポート」画面が表示されます。
2. 「設定」ボタンをクリックする。



「TEL1 ポートの設定」画面が表示されます。

### メモ

TEL2 ポートを設定する場合は、「TEL2 ポート」ボタンをクリックしてください。

## 3. TEL1 ポートを設定する。

YAMAHA NVR700W 管理ユーザー-ユーザー名なし ログアウト

ダッシュボード LANマップ かんたん設定 詳細設定 管理

CONFIG TECHINFO ヘルプ

TELポート > TEL1ポートを設定

### TELポート

#### TELポートの設定

各項目を入力してください。入力が完了したら、「確認」を押してください。

TELポート 1

電話機能の使用 **①**

- 使用する
- 使用する (発信のみ)
- 使用する (着信のみ)
- 使用しない

ナンバー・ディスプレイ **②**

- 使用する
- 使用しない

SIPユーザー名 **③**

着信専用 1  ※省略可

着信専用 2  ※省略可

着信専用 3  ※省略可

着信の許可 **④**

- 全ての着信を許可する
- SIPユーザー名と一致した場合のみ許可する

着信ポート優先順位 **⑤**

- 高い
- 普通
- 低い

通知する発信者名 (番号) **⑥**  ※省略可

ダイヤルイン/FAX無鳴動着信 **⑦**

種別選択	サービス種別	ダイヤルイン時の出力番号/桁数
<input type="text"/>	<input type="text"/>	<input type="text"/>

即時発信 **⑧**

- 発信する
- 発信しない

ダイヤル終了から発信までの時間 **⑨**  秒

TEL1ポートと同じ設定をTEL2ポートに適用する

戻る 確認

**① 電話機能の使用：**

電話の発信、着信の設定を行います。TEL ポートの使用目的に合わせて選択します。

**② ナンバー・ディスプレイ：**

ナンバー・ディスプレイの表示を行うか選択します。

**③ SIP ユーザー名：**

発信時に使用する SIP ユーザー名と、着信専用の SIP ユーザー名を入力します。着信専用 SIP ユーザー名は 3 件まで入力可能です。

**④ 着信の許可：**

すべての着信を許可するか、SIP ユーザー名と一致した場合のみ許可するかを選択します。

**⑤ 着信ポート優先順位：**

TEL ポート通信の優先順位を選択します。「高い」に設定すると、他の TEL ポートよりも高い優先度で着信を行います。

**⑥ 通知する発信者名 (番号)：**

発信時に表示されるディスプレイ名を入力します。

**⑦ ダイヤルイン /FAX 無鳴動着信：**

アナログダイヤルインと無鳴動着信を設定します。

設定する SIP ユーザー名を入力し、使用するサービスを選択して、出力番号または出力桁数を入力します。設定項目を追加する場合は、「+」ボタンをクリックします。

**⑧ 即時発信：**

発信時に即時発信させるかどうかを選択します。

## 第 13 章 詳細設定を行う

### ⑨ ダイアル終了から発信までの時間：

相手先番号入力後、発信するまでの時間を入力します。

### メモ

画面下部のチェックボックスにチェックを入れると、TEL1 ポートと同じ設定が TEL2 ポートに適用されます。

#### 4. 「確認」ボタンをクリックする。

「入力内容の確認」画面が表示されます。

#### 5. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が変更され、「TEL ポートの設定」画面が表示されます。

## 13.4 グローバル IP アドレスを複数の端末でシェアする

グローバル IP アドレスとプライベート IP アドレスを透過的に相互変換することで、一つのグローバル IP アドレスを複数の端末でシェアすることができます (IP マスカレード)。TCP/UDP のポート番号まで動的に変換されるため、一つのグローバル IP アドレスで複数の端末から同時にインターネット接続することが可能です。

### 設定例

IP マスカレードを設定するインターフェース：WAN

NAT ディスクリプター番号：200

外側アドレス：プライマリアドレス


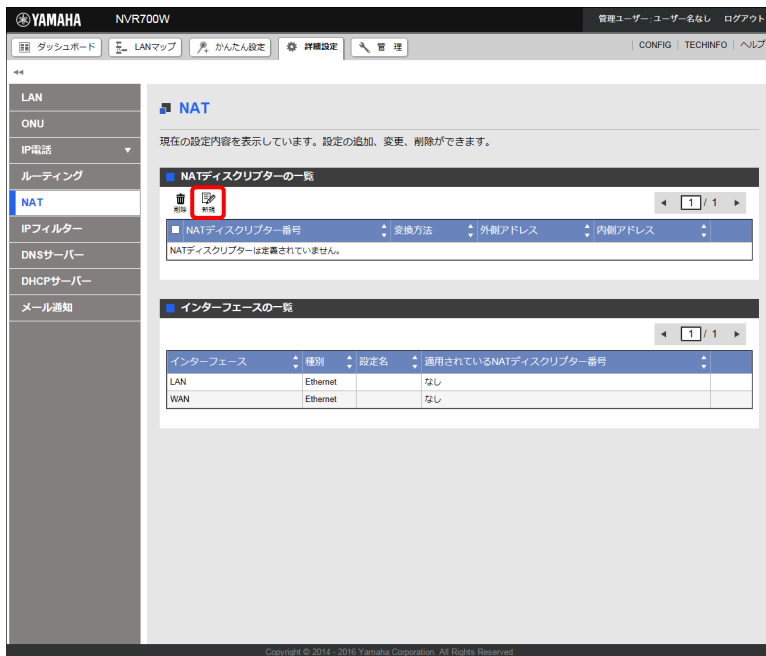
### メモ

「かんたん設定」を使用してプロバイダー接続の設定が完了している場合は、プロバイダー接続の設定と同時に IP マスカレードも自動的に設定されるため、本章の操作は不要になります。

#### 1. 「詳細設定」タブ - 「NAT」を順に選択する。

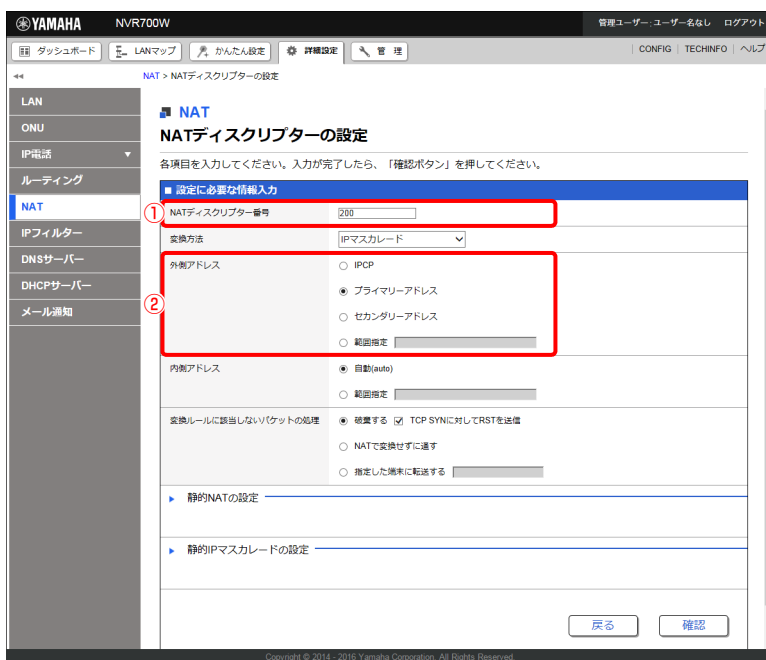
「NAT」画面が表示されます。



2. 「NAT ディスクリプターの一覧」項目の「」ボタンをクリックする。

「NAT ディスクリプターの設定」画面が表示されます。

## 3. IP マスカレードを設定する。



## ① NAT ディスクリプター番号：

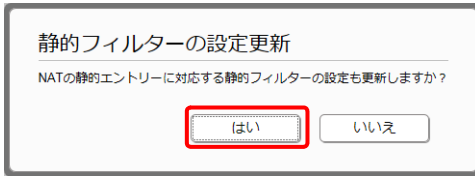
「200」を入力します。

## ② 外側アドレス：

「プライマリアドレス」を選択します。

## 第 13 章 詳細設定を行う

4. 「確認」 ボタンをクリックする。  
「静的フィルターの設定更新」 ダイアログが表示されます。
5. 「はい」 ボタンをクリックする。



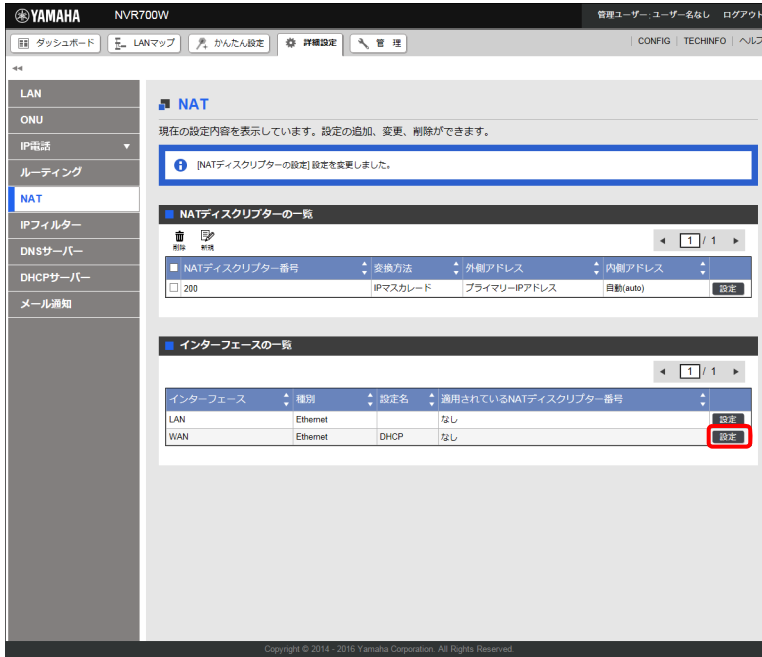
「入力内容の確認」画面が表示されます。

6. 内容を確認し、「設定の確定」ボタンをクリックする。



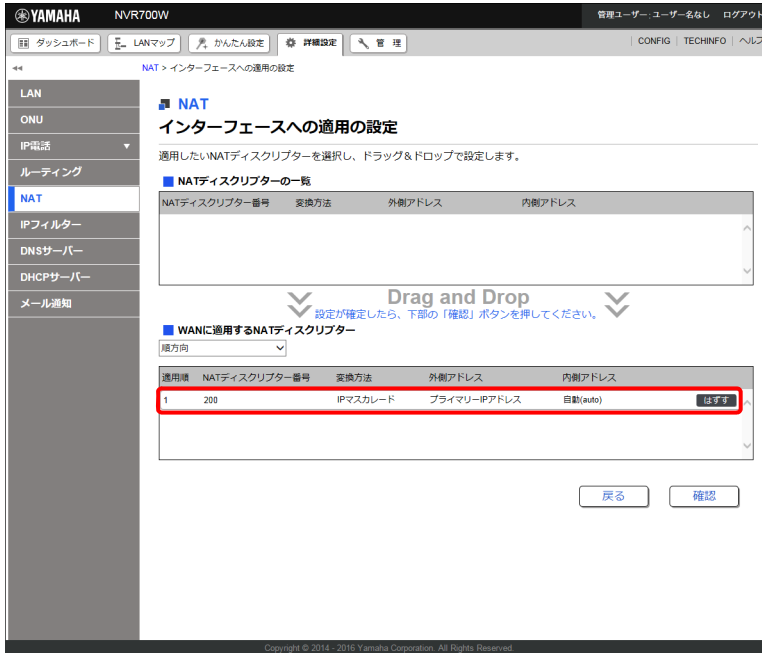
設定が反映され、「NAT」画面が表示されます。

## 7. 「インターフェースの一覧」項目のWANの「設定」ボタンをクリックする。



「インターフェースへの適用の設定」画面が表示されます。

## 8. 「NAT ディスクリプターの一覧」項目から「WANに適用するNAT ディスクリプター」項目の先頭に、作成したNAT ディスクリプターをドラッグ &amp; ドロップする。

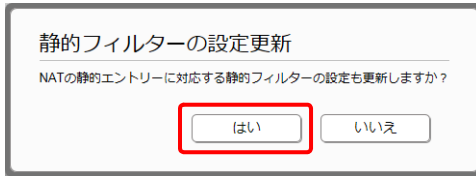


## 9. 「確認」ボタンをクリックする

「静的フィルターの設定更新」画面が表示されます。

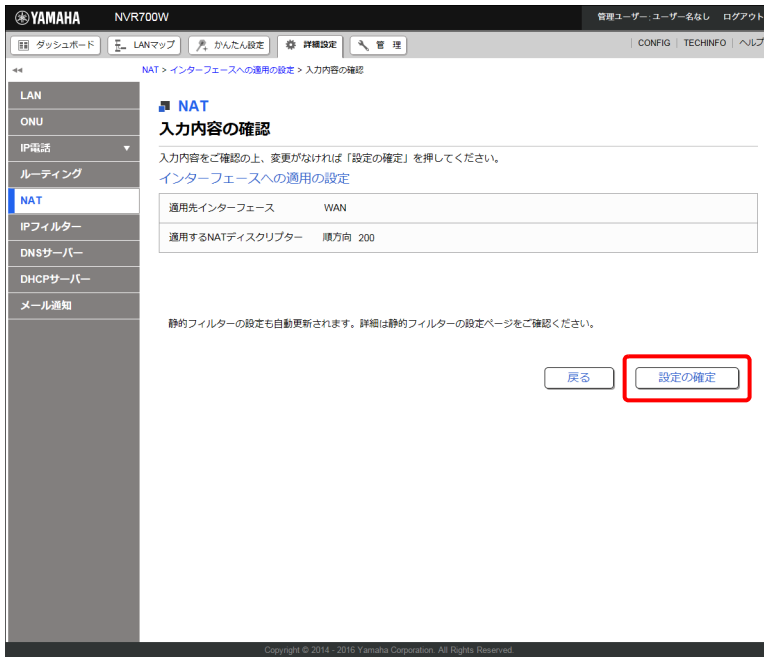
## 第 13 章 詳細設定を行う

### 10. 「はい」 ボタンをクリックする



「入力内容の確認」画面が表示されます。

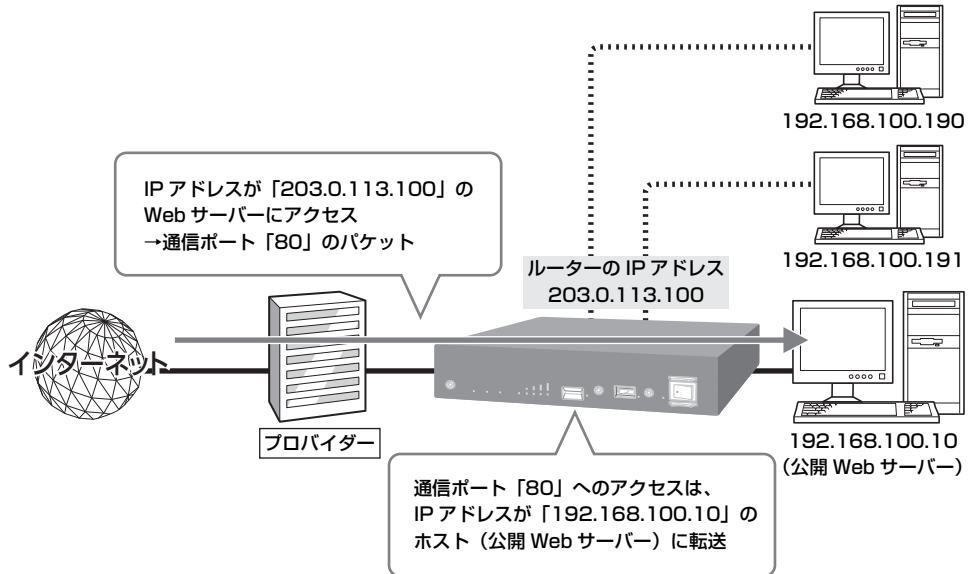
### 11. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「NAT」画面が表示されます。

## 13.5 外部にサーバーを公開する

インターネットへサーバーを公開したい場合は、公開したいサーバーに固定プライベート IP アドレスを設定してから、IP アドレスの変換テーブルを登録します（静的 IP マスカレード）。さらに、インターネットからのアクセスを許可するフィルターを設定すれば、特定のプロトコルのパケットを LAN 内のサーバーに送信できるようになるため、インターネットからサーバーにアクセスできるようになります。サーバーを公開するためには、次の設定が必要です。



### サーバーの設定

- ・ サーバーに固定 IP アドレスを設定する。
- ・ Web や FTP など、公開するサービスに合わせてファイルサーバーソフトの設定を変更する。

### ルーターの設定

- ・ プロトコルとポート番号、サーバーの IP アドレスの変換テーブルを登録する。（静的 IP マスカレード）（282 ページ）
- ・ 外部からのアクセスを許可するフィルターを設定する。（285 ページ）

### ご注意

インターネットへサーバーを公開するときは、データを保全するために十分なセキュリティ設定を行ってください。セキュリティ設定が不十分な場合は、LAN に接続されたパソコンが不正侵入や盗聴、妨害、データの消失、破壊などに遭う可能性があります。

### メモ

- ・ ネットボランチ DNS サービスを利用することで、固定グローバル IP アドレスが割り当てられない接続サービスでも、サーバーを公開して運用できます。ネットボランチ DNS サービスの設定について詳しくは、「第 6 章 ネットボランチ DNS サービスを利用する」（64 ページ）をご覧ください。
- ・ 本章では「かんたん設定」を使用して WAN インターフェイスに PPPoE 接続型のプロバイダーが設定されている状態「4.1.2 「PPPoE 接続」の場合」（30 ページ）の設定が完了している状態から設定を行うという前提で説明します。

## 第 13 章 詳細設定を行う

### 13.5.1 IP アドレスの変換テーブルを登録する

通信プロトコルとポート番号、サーバーの IP アドレスの変換テーブルを登録します。インターネットへ Web サーバーを公開する場合を例に説明します。

#### 設定例

NAT ディスクリプター番号：1000

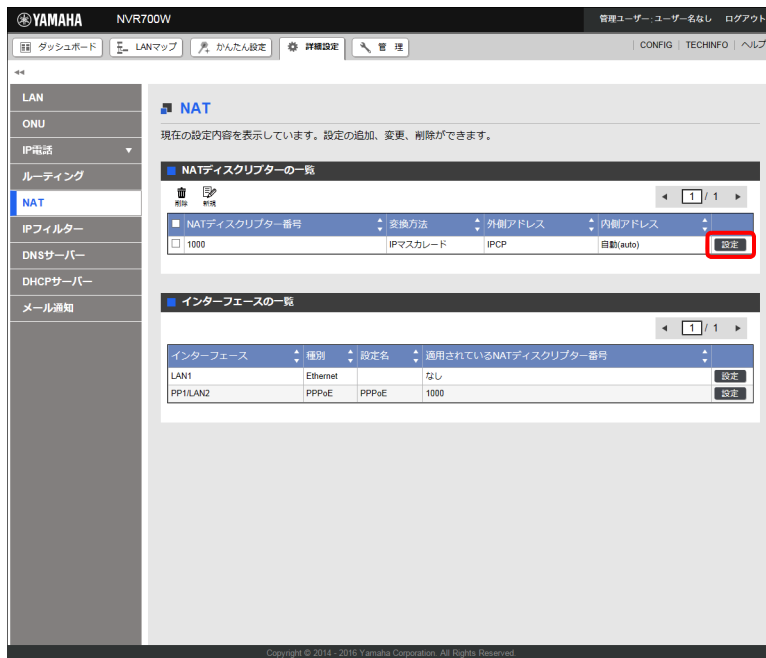
静的 IP マスカレードの識別番号：1

サーバーの IP アドレス：192.168.100.10

サーバーのプロトコル：TCP

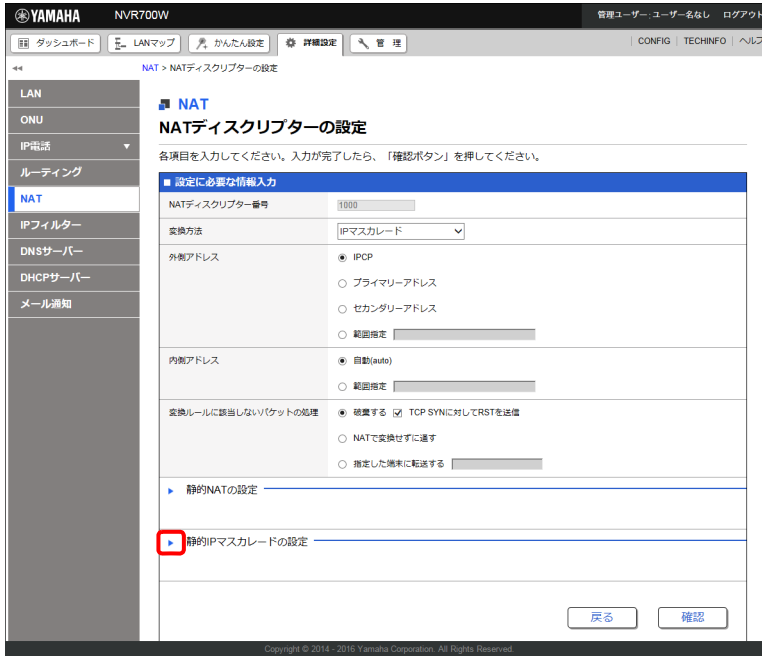
サーバーの使用ポート：80

1. 「詳細設定」タブ - 「NAT」を順に選択する。  
「NAT」画面が表示されます。
2. 「NAT ディスクリプターの一覧」項目の NAT ディスクリプター番号が 1000 の「設定」ボタンをクリックする。

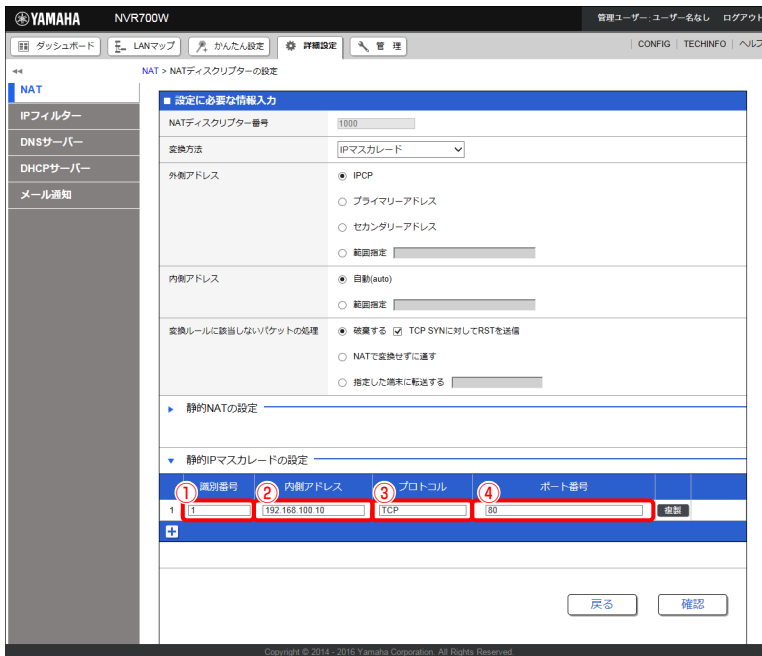


「NAT ディスクリプターの設定」画面が表示されます。

## 3. 「静的 IP マスカレードの設定」項目の「▶」ボタンをクリックする。



## 4. 静的 IP マスカレードを設定する。



- ① 識別番号：  
「1」を入力します。
- ② 内側アドレス：  
「192.168.100.10」を入力します。
- ③ プロトコル：  
「TCP」を入力します。

## 第 13 章 詳細設定を行う

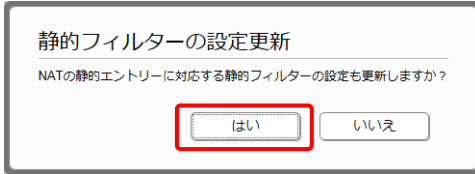
### ④ ポート番号：

「80」を入力します。

### 5. 「確認」 ボタンをクリックする。

「静的フィルターの設定更新」ダイアログが表示されます。

### 6. 「はい」 ボタンをクリックする。



WAN インターフェースに静的 IP フィルターが自動追加され、「入力内容の確認」画面が表示されます。

## メモ

静的フィルターを手動で設定する場合は「13.5.2 IP アドレスの変換テーブルに合わせて静的フィルターを設定する」(285 ページ) をご覧ください。

### 7. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「NAT」画面が表示されます。



## 13.5.2 IP アドレスの変換テーブルに合わせて静的フィルターを設定する

「11.2.1 IP アドレスの変換テーブルを登録する」の手順 6 で「いいえ」をクリックした場合は、IP アドレスの変換テーブルに合わせて静的フィルターを手動で設定します。

## 設定例

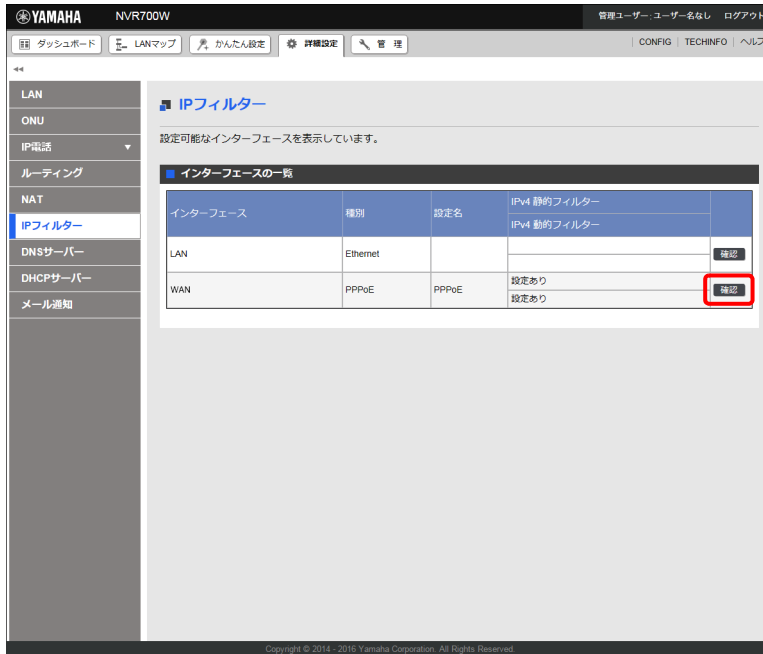
タイプ：pass（ログなし）

プロトコル：TCP

宛先 IP アドレス：192.168.100.10


宛先ポート番号：80


1. 「詳細設定」タブ - 「IP フィルター」を順に選択する。  
「IP フィルター」画面が表示されます。
2. 「インターフェースの一覧」項目の WAN インターフェースの「確認」ボタンをクリックする。



「適用されている IP フィルターの一覧」画面が表示されます。

## 第 13 章 詳細設定を行う

3. 「静的フィルター」項目の「」ボタンをクリックする。



静的フィルター

適用されているIPフィルターの一覧


現在の設定内容を表示しています。

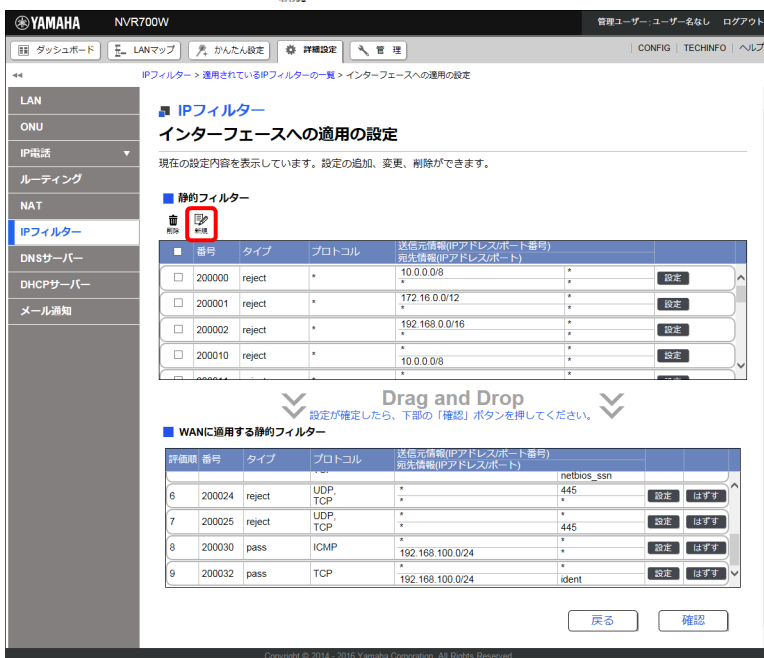
■ 一覧表示の切り替え  
WANに適用されているフィルターの表示を切り替えます。 受信方向のフィルターを表示

静的フィルター

評価順	番号	タイプ	プロトコル	送信元情報(IPアドレス/ポート)	宛先情報(IPアドレス/ポート)
1	200003	reject	*	192.168.100.0/24	*
2	200020	reject	UDP,TCP	*	135
3	200021	reject	UDP,TCP	*	135
4	200022	reject	UDP,TCP	*	netbios_ns-netbios_ssn
5	200023	reject	UDP,TCP	*	netbios_ns-netbios_ssn
6	200024	reject	UDP,TCP	*	445
7	200025	reject	UDP,TCP	*	445
8	200030	pass	ICMP	192.168.100.0/24	*

「インターフェースへの適用の設定」画面が表示されます。

4. 「静的フィルター」項目の「」ボタンをクリックする。



静的フィルター

インターフェースへの適用の設定

現在の設定内容を表示しています。設定の追加、変更、削除ができます。

静的フィルター

番号	タイプ	プロトコル	送信元情報(IPアドレス/ポート)	宛先情報(IPアドレス/ポート)	
<input type="checkbox"/> 200000	reject	*	10.0.0.0/8	*	設定
<input type="checkbox"/> 200001	reject	*	172.16.0.0/12	*	設定
<input type="checkbox"/> 200002	reject	*	192.168.0.0/16	*	設定
<input type="checkbox"/> 200010	reject	*	10.0.0.0/8	*	設定

Drag and Drop  
設定が確定したら、下部の「確認」ボタンを押してください。

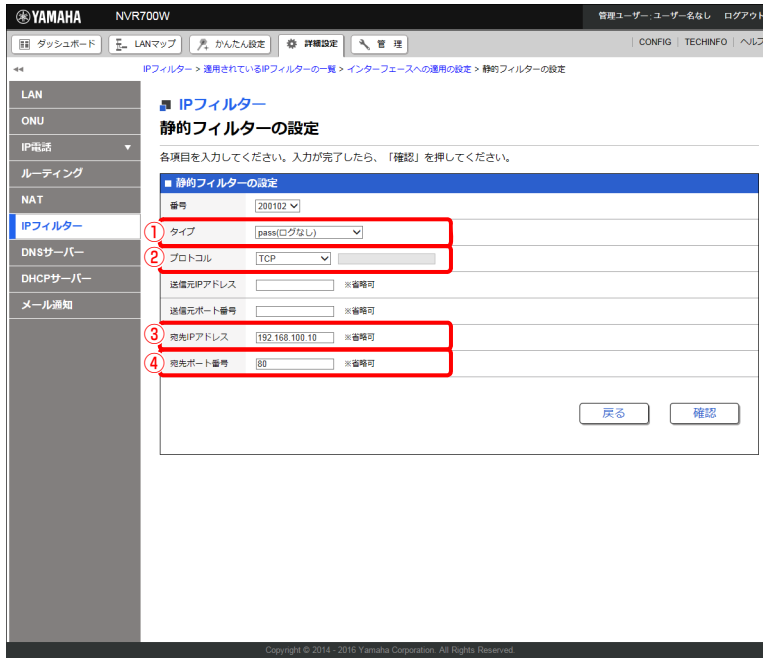
静的フィルター

評価順	番号	タイプ	プロトコル	送信元情報(IPアドレス/ポート)	宛先情報(IPアドレス/ポート)		
6	200024	reject	UDP,TCP	*	445	設定	はずす
7	200025	reject	UDP,TCP	*	445	設定	はずす
8	200030	pass	ICMP	192.168.100.0/24	*	設定	はずす
9	200032	pass	TCP	192.168.100.0/24	ident	設定	はずす

戻る 確認

「静的フィルターの設定」画面が表示されます。

## 5. 静的フィルターを設定する。



- ① **タイプ：**  
「pass (ログなし)」を選択します。
  - ② **プロトコル：**  
「TCP」を選択します。
  - ③ **宛先 IP アドレス：**  
「192.168.100.10」を入力します。
  - ④ **宛先ポート番号：**  
「80」を入力します。
6. 「確認」ボタンをクリックする。  
「入力内容の確認」画面が表示されます。

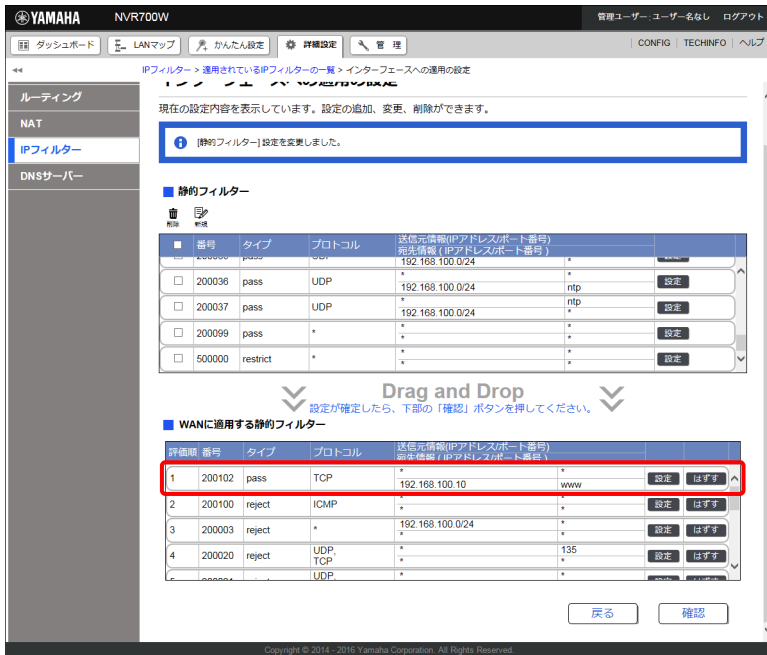
## 第 13 章 詳細設定を行う

### 7. 内容を確認し、「設定の確定」ボタンをクリックする。



「インターフェースへの適用の設定」画面が表示されます。

### 8. 「静的フィルター」項目から「WANに適用する静的フィルター」項目の先頭に、作成したフィルター設定をドラッグ&ドロップする。



### 9. 「確認」ボタンをクリックする。

「入力内容の確認」画面が表示されます。

10. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「インターフェースへの適用の設定」画面が表示されます。

### 13.5.3 サーバーの公開先を限定する

サーバーの公開先を限定します。「11.2.1 IP アドレスの変換テーブルを登録する」で設定した公開サーバーのアドレスに対して、下記のネットワークからのみアクセスできるようにする場合を例に説明します。

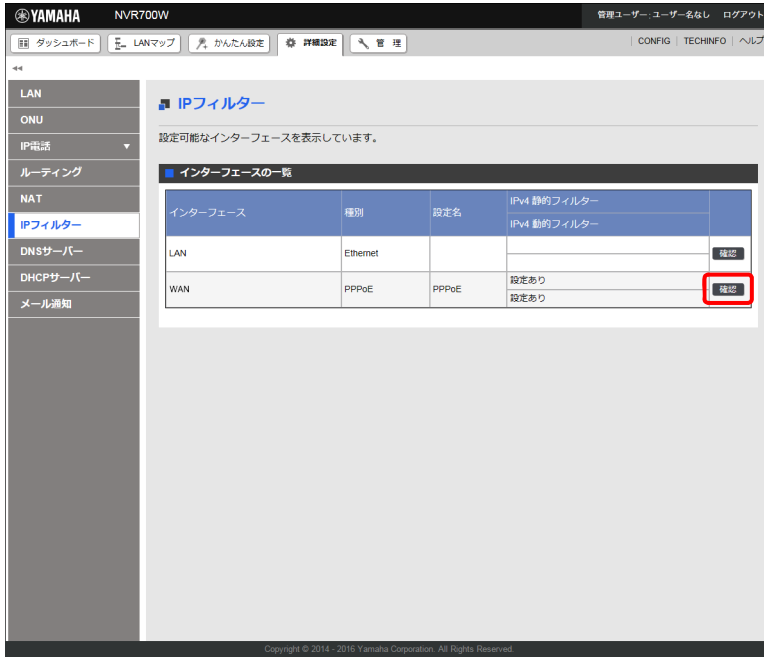
#### 設定例

公開先：203.0.113.0/24


1. 「詳細設定」タブ - 「IP フィルター」を順に選択する。  
「IP フィルター」画面が表示されます。

## 第 13 章 詳細設定を行う

2. 「インターフェースの一覧」項目の WAN インターフェースの「確認」ボタンをクリックする。



「適用されている IP フィルターの一覧」画面が表示されます。

3. 「静的フィルター」項目の「」ボタンをクリックする。



「インターフェースへの適用の設定」画面が表示されます。

4. 「WAN に適用する静的フィルター」項目で、以下の内容が合致するフィルターの「設定」ボタンをクリックする。
- タイプ : pass
  - プロトコル : TCP
  - 宛先アドレス : 192.168.100.10
  - 宛先ポート番号 : www

The screenshot shows the Web GUI for a Yamaha NVR700W. The left sidebar contains navigation options like LAN, ONU, IP電話, ルーティング, NAT, IPフィルター (selected), DNSサーバー, DHCPサーバー, and メール通知. The main content area is titled 'IPフィルター インターフェースへの適用の設定'. It features a '静的フィルター' table with columns for ID, Type, Protocol, and Destination/Port. Below this is a 'Drag and Drop' section and a 'WANに適用する静的フィルター' table. The 'WAN' table has columns for ID, Type, Protocol, Destination, and Port. The row with ID 1, Type 'pass', Protocol 'TCP', Destination '192.168.100.10', and Port 'www' has its '設定' button highlighted with a red box. At the bottom, there are '戻る' and '確認' buttons.

「静的フィルターの設定」画面が表示されます。

## 第 13 章 詳細設定を行う

### 5. 静的フィルターを編集する。

静的フィルターの設定

各項目を入力してください。入力完了したら、「確認」を押してください。

■ 静的フィルターの設定	
番号	200102
タイプ	pass(ログなし)
プロトコル	TCP
① 送信元IPアドレス	203.0.113.0/24 ※省略可
送信元ポート番号	* ※省略可
宛先IPアドレス	192.168.100.10 ※省略可
宛先ポート番号	www ※省略可

戻る 確認

① 送信元 IP アドレス：  
「203.0.113.0/24」を入力します。

6. 「確認」ボタンをクリックする。  
「入力内容の確認」画面が表示されます。

7. 内容を確認し、「設定の確定」ボタンをクリックする。

入力内容の確認

入力内容をご確認の上、変更がなければ「設定の確定」を押してください。

静的フィルターの設定

番号	200102
タイプ	pass(ログなし)
プロトコル	TCP
送信元IPアドレス	203.0.113.0/24
送信元ポート番号	*
宛先IPアドレス	192.168.100.10
宛先ポート番号	www

戻る 設定の確定

設定が反映され、「インターフェースへの適用の設定」画面が表示されます。



## 13.6 複数のプロバイダーを使用する

複数のプロバイダーを設定することで、端末ごとに接続プロバイダーを使い分けたり、障害時用のバックアップ回線を用意することができます。

### 13.6.1 複数のプロバイダーを設定する

複数のプロバイダーを用途に応じて使い分ける設定を行うためには、事前に「かんたん設定」の「プロバイダー接続」画面から複数のプロバイダーの設定を済ませておく必要があります。プロバイダーの設定方法について詳しくは、「第4章 IPv4 アドレスでインターネットに接続する」(26 ページ)をご覧ください。

13.6.2 ~ 13.6.4 の設定方法の説明では、WAN インターフェースに DHCP 接続型のプロバイダー、WWAN に内蔵無線 WAN 接続型のプロバイダーが設定されている状態（下記画像の状態）から設定を行うという前提で説明します。

YAMAHA NVR700W 管理ユーザー ユーザー名なし ログアウト

ダッシュボード LANマップ かんたん設定 詳細設定 管理

基本設定 プロバイダー接続 VPN ネットホストDNS IP電話

### プロバイダー接続

プロバイダー接続の新規作成、設定変更、削除ができます。

**■ 新規作成**

プロバイダー接続の設定を新規作成できます。

**■ 設定の一覧**

優先順位の設定があるプロバイダー接続

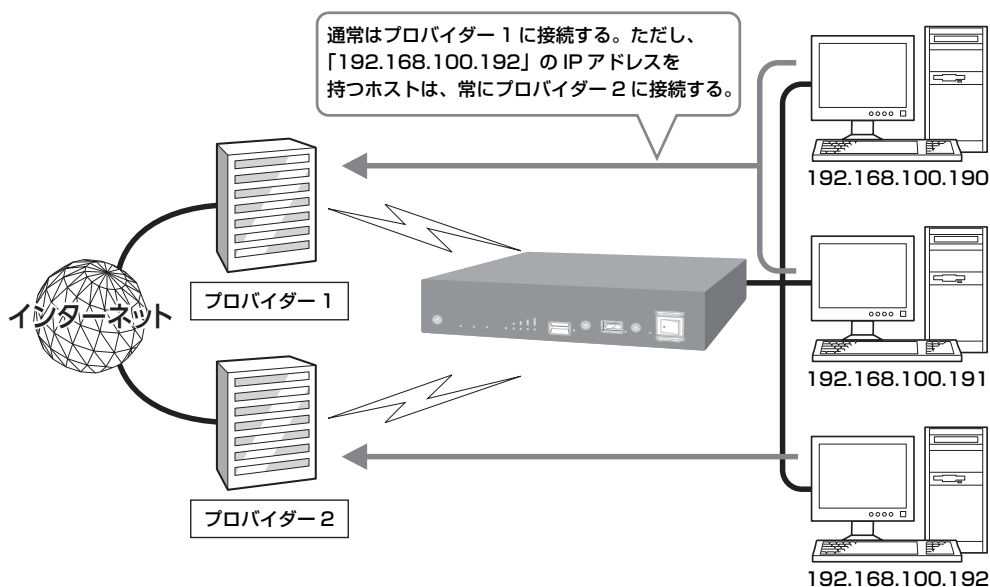
優先順位	設定名	接続種別	インターフェース	接続状態	
1	DHCP	DHCP、または固定 IP アドレスによる接続	WAN	10.0.4.166/24	<input type="button" value="設定"/> <input type="button" value="削除"/>
2	WWAN	内蔵無線 WAN 接続	WWAN1		<input type="button" value="接続する"/> <input type="button" value="設定"/> <input type="button" value="削除"/>

Copyright © 2014 - 2016 Yamaha Corporation. All Rights Reserved.

### 13.6.2 端末ごとにプロバイダーを使い分ける

端末の IP アドレスと使用する接続プロバイダーの関連づけを行い、端末ごとに接続するプロバイダーを使い分けます。

この場合は、LAN 上のすべての端末の IP アドレスをあらかじめ固定する必要があります。詳しくは、ネットワークの管理者にご相談ください。



#### 設定例

##### ゲートウェイ 1

プロバイダー：DHCP 接続型プロバイダー  
使用する端末の IP アドレス：192.168.100.2

##### ゲートウェイ 2

プロバイダー：内蔵無線 WAN 接続型プロバイダー  
使用する端末の IP アドレス：192.168.100.30

1. 「詳細設定」タブ - 「ルーティング」を順に選択する。  
「ルーティング」画面が表示されます。

## 2. 「静的ルーティングの一覧」項目の default 経路の「設定」ボタンをクリックする。

The screenshot shows the Web GUI for a Yamaha NVR700W device. The left sidebar contains navigation menus for LAN, ONU, IP電話, ルーティング (selected), NAT, IPフィルター, DNSサーバー, DHCPサーバー, and メール通知. The main content area is titled 'ルーティング' and displays routing information. Below the 'ルーティング情報' table, the '静的ルーティングの一覧' (Static Routing List) is shown. The table has columns for '優先ネットワーク' (Priority Network), '評価順' (Evaluation Order), 'ゲートウェイ' (Gateway), 'オプション有効基準' (Option Valid Criteria), '選路基準' (Routing Criteria), and 'メトリック' (Metric). The 'default' entry is selected, and its '設定' button is highlighted with a red box.

プロトコル	有効な経路数	無効な経路数
Static	2	0
Implicit	2	0
Temporary	0	0
Redirect	0	0
RIP	0	0
OSPF	0	0
BGP	0	0
経路数の合計	4	0

優先ネットワーク	評価順	ゲートウェイ	オプション有効基準	選路基準	メトリック
<input type="checkbox"/> default	1	dhcp lan2	-	アスタリスク型 500000	-
<input type="checkbox"/> default	2	pdp wan1	-	-	-

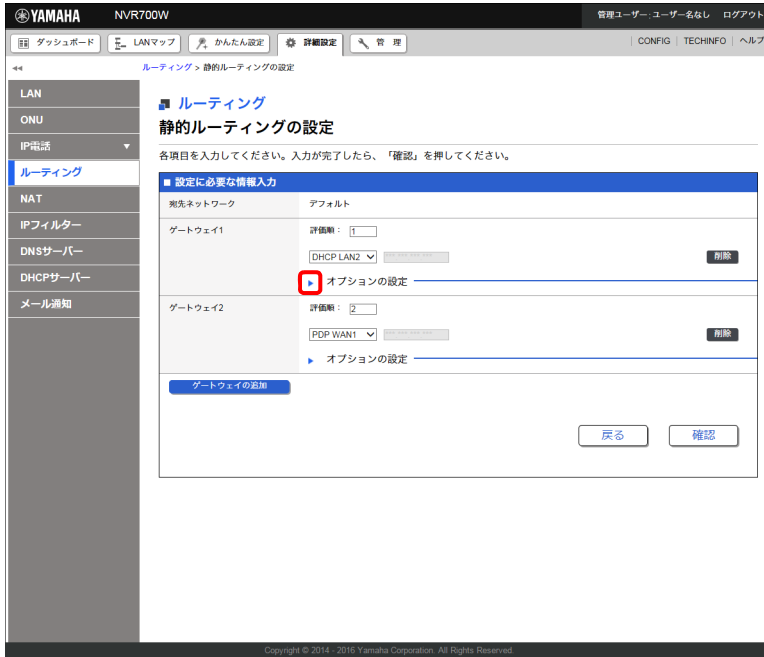
「静的ルーティングの設定」画面が表示されます。

## メモ

default 経路制御により、経路情報をコンパクトにすることができます。全ての TCP/IP ネットワークの経路情報をルーターが持とうとしても、経路情報が多過ぎて処理できません。default 経路により外側と内側を仕切り、未知のネットワークへのアクセスは default 経路に流すようになっています。

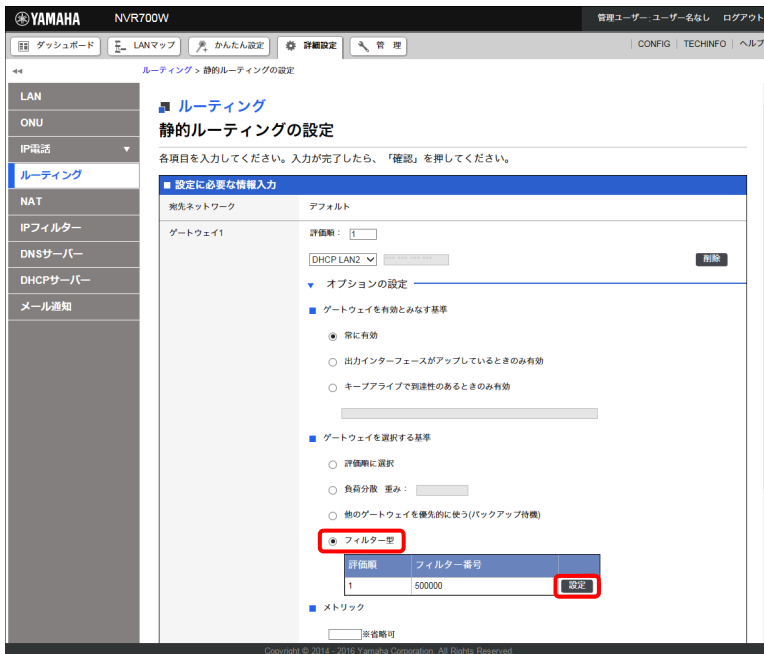
## 第 13 章 詳細設定を行う

3. 「ゲートウェイ 1」項目の「オプションの設定」の先頭にある「▶」ボタンをクリックする。




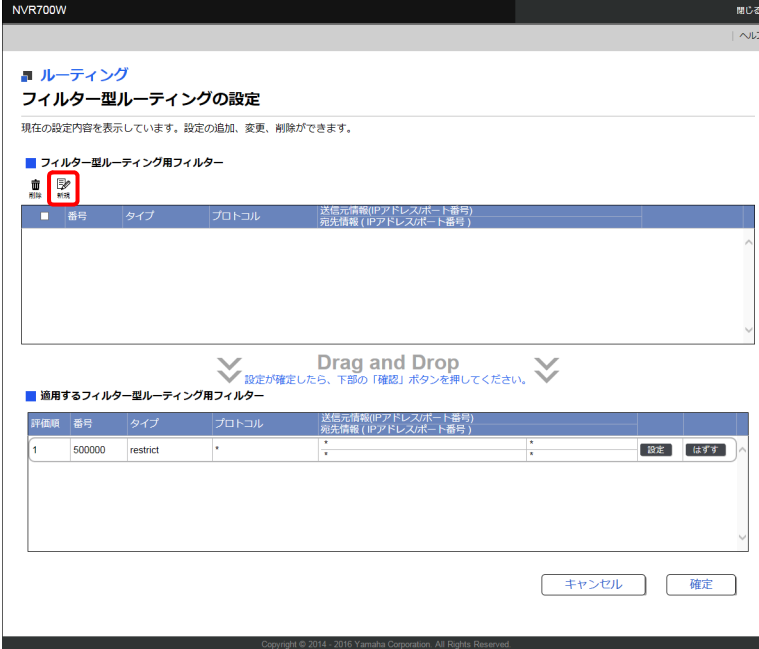
「オプションの設定」が表示されます。

4. 「ゲートウェイを選択する基準」欄で「フィルター型」を選択し、「設定」ボタンをクリックする。



「フィルター型ルーティングの設定」画面が表示されます。

5. 「フィルター型ルーティング用フィルター」項目の「」ボタンをクリックする。




NVR700W 閉じる ヘルプ

■ ルーティング  
フィルター型ルーティングの設定

現在の設定内容を表示しています。設定の追加、変更、削除ができます。

■ フィルター型ルーティング用フィルター



番号	タイプ	プロトコル	送信元情報 (IPアドレス/ポート番号)	宛先情報 (IPアドレス/ポート番号)

Drag and Drop  
設定が確定したら、下部の「確認」ボタンを押してください。

■ 適用するフィルター型ルーティング用フィルター

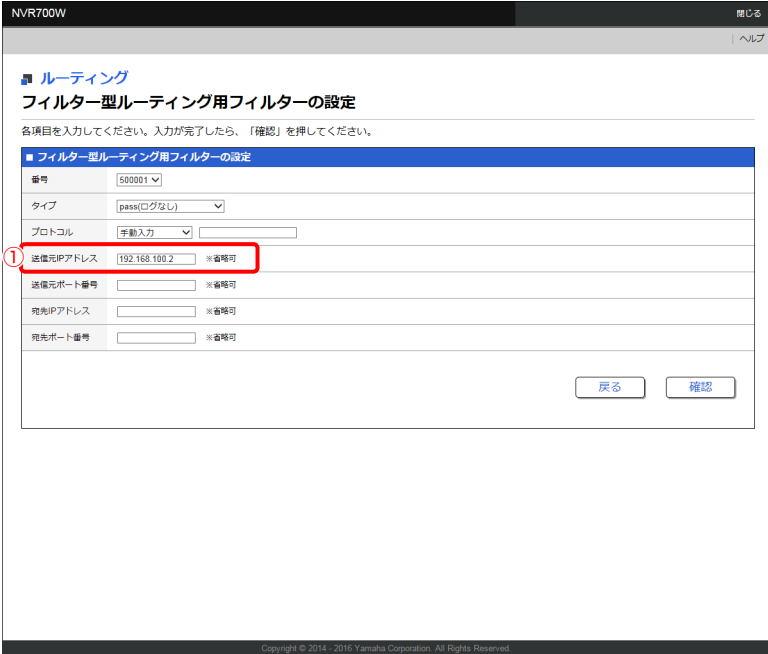
評価順	番号	タイプ	プロトコル	送信元情報 (IPアドレス/ポート番号)	宛先情報 (IPアドレス/ポート番号)	設定	はずす
1	500000	restrict	*	*	*	設定	はずす

キャンセル 確定

Copyright © 2014 - 2016 Yamaha Corporation. All Rights Reserved.

「フィルター型ルーティング用フィルターの設定」画面が表示されます。

6. ルーティング用フィルターを設定する。



NVR700W 閉じる ヘルプ

■ ルーティング  
フィルター型ルーティング用フィルターの設定

各項目を入力してください。入力が完了したら、「確認」を押してください。

■ フィルター型ルーティング用フィルターの設定

番号

タイプ

プロトコル

① 送信元IPアドレス  ※省略可

送信元ポート番号  ※省略可

宛先IPアドレス  ※省略可

宛先ポート番号  ※省略可

戻る 確認

Copyright © 2014 - 2016 Yamaha Corporation. All Rights Reserved.

- ① 送信元 IP アドレス：  
「192.168.100.2」を入力します。

7. 「確認」ボタンをクリックする。  
「入力内容の確認」画面が表示されます。

## 第 13 章 詳細設定を行う

### 8. 内容を確認し、「設定の確定」ボタンをクリックする。

NVR700W 閉じる ヘルプ

### ルーティング

#### 入力内容の確認

入力内容をご確認の上、変更がなければ「設定の確定」を押してください。

フィルター型ルーティング用フィルター

番号	500001
タイプ	pass(ログなし)
プロトコル	
送信元IPアドレス	192.168.100.2
送信元ポート番号	
宛先IPアドレス	
宛先ポート番号	

戻る 設定の確定

Copyright © 2014 - 2016 Yamaha Corporation. All Rights Reserved.

ルーティング用フィルターが作成され、「フィルター型ルーティングの設定」画面が表示されます。

### 9. 「フィルター型ルーティング用フィルター」項目から「適用するフィルター型ルーティング用フィルター」項目の先頭に、作成したフィルター設定をドラッグ & ドロップする。

NVR700W 閉じる ヘルプ

### フィルター型ルーティングの設定

現在の設定内容を表示しています。設定の追加、変更、削除ができます。

[i] [フィルター型ルーティング用フィルター] 設定を変更しました。

#### フィルター型ルーティング用フィルター

追加 削除

番号	タイプ	プロトコル	送信元情報(IPアドレス/ポート番号)	宛先情報(IPアドレス/ポート番号)

Drag and Drop  
設定が確定したら、下部の「確認」ボタンを押してください。

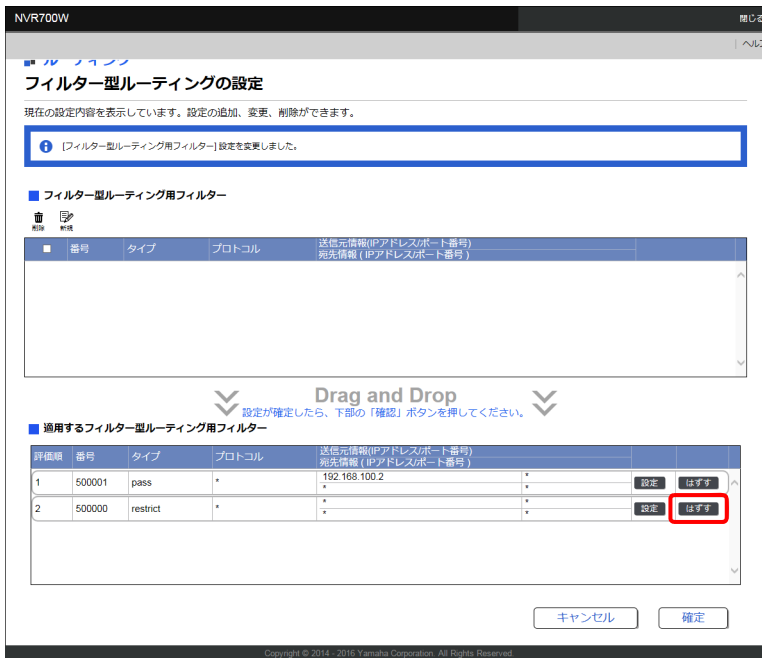
#### 適用するフィルター型ルーティング用フィルター

評価順	番号	タイプ	プロトコル	送信元情報(IPアドレス/ポート番号)	宛先情報(IPアドレス/ポート番号)	設定	はずす
1	500001	pass	*	192.168.100.2	*	設定	はずす
2	500000	restrict	*	*	*	設定	はずす

キャンセル 確定

Copyright © 2014 - 2016 Yamaha Corporation. All Rights Reserved.

10. 「適用するフィルター型ルーティング用フィルター」項目の 500000 番のフィルターの「はずす」ボタンをクリックする。



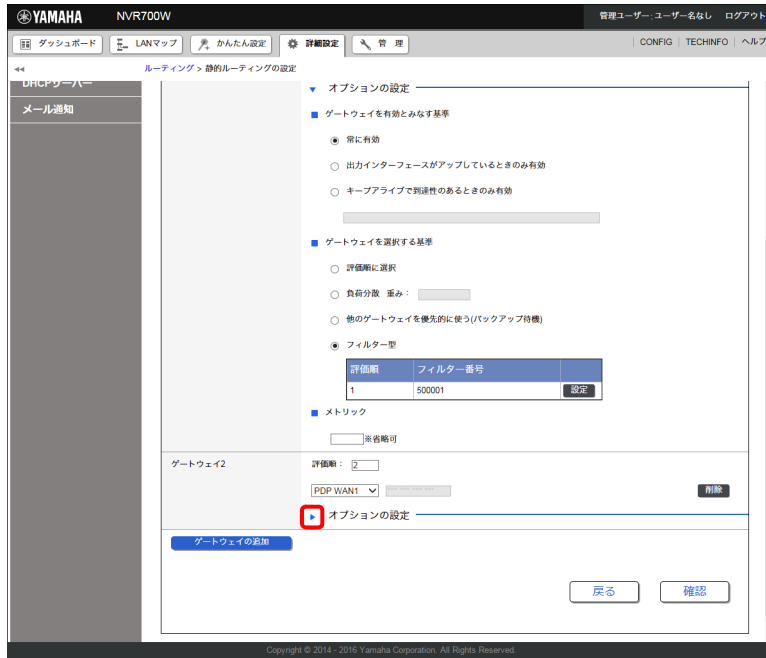
## ご注意

500000 番のフィルターが適用されたままになっていると、すべての端末がゲートウェイ 1 を使用してしまうため、端末ごとの使い分けができません。

11. 「確認」ボタンをクリックする。  
「フィルター型ルーティングの設定」画面が閉じられます。

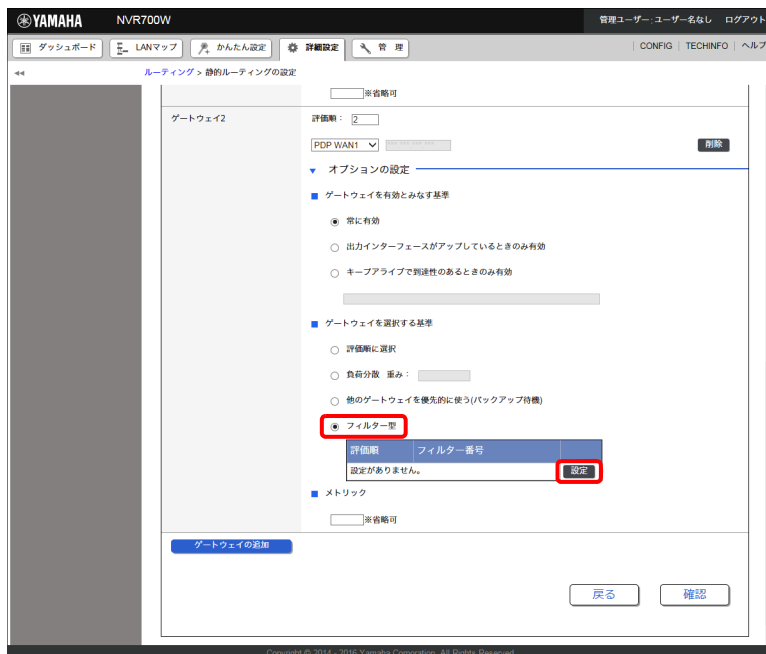
## 第 13 章 詳細設定を行う

12.「ゲートウェイ 2」項目の「オプションの設定」の先頭にある「▶」ボタンをクリックする。




「オプションの設定」が表示されます。

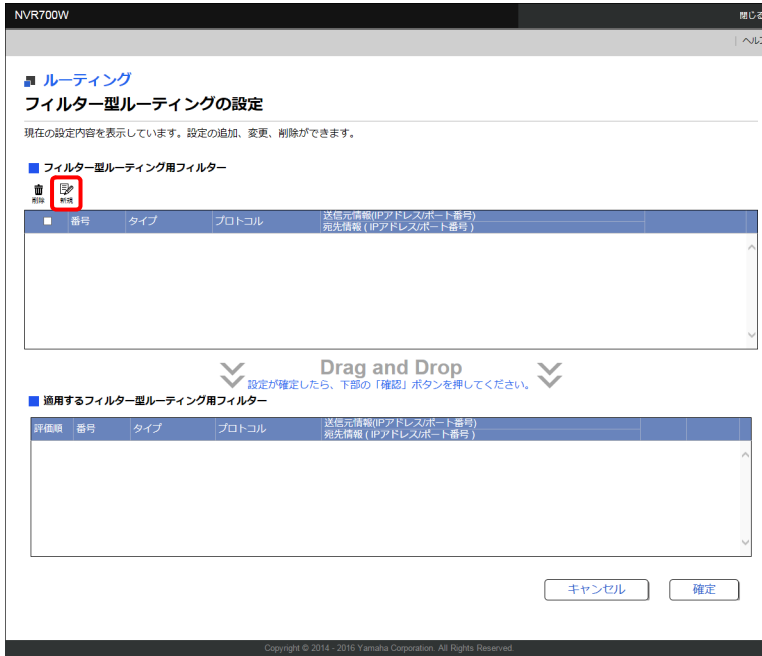
13.「ゲートウェイを選択する基準」欄で「フィルター型」を選択し、「設定」ボタンをクリックする。



「フィルター型ルーティングの設定」画面が表示されます。

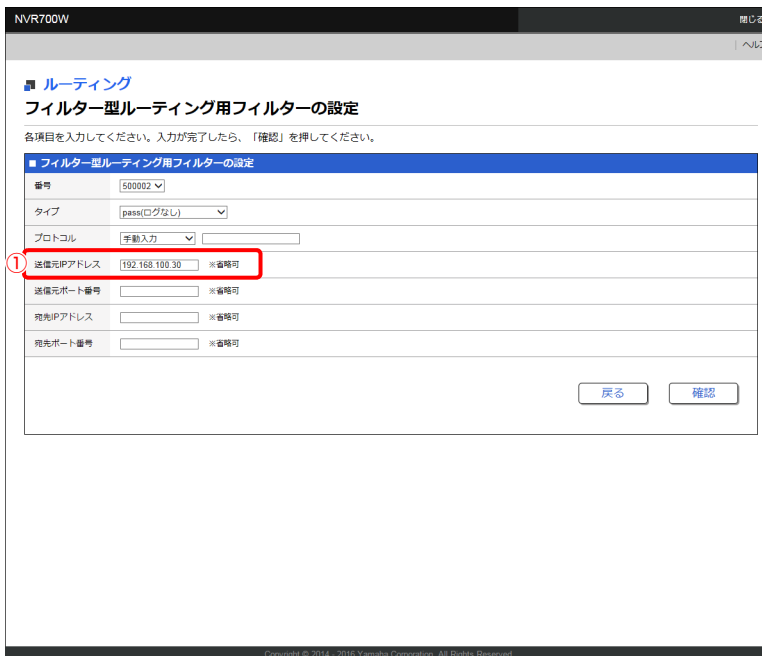


14.「フィルター型ルーティング用フィルター」項目の「」ボタンをクリックする。



「フィルター型ルーティング用フィルターの設定」画面が表示されます。

15.ルーティング用フィルターを設定する。



① 送信元 IP アドレス：  
「192.168.100.30」を入力します。

16.「確認」ボタンをクリックする。  
「入力内容の確認」画面が表示されます。

## 第 13 章 詳細設定を行う

17.内容を確認し、「設定の確定」ボタンをクリックする。

NVR700W 閉じる ヘルプ

### ルーティング

#### 入力内容の確認

入力内容をご確認の上、変更がなければ「設定の確定」を押してください。

フィルター型ルーティング用フィルター

番号	500002
タイプ	pass(ログなし)
プロトコル	
送信元IPアドレス	192.168.100.30
送信元ポート番号	
宛先IPアドレス	
宛先ポート番号	

戻る 設定の確定

Copyright © 2014 - 2016 Yamaha Corporation. All Rights Reserved.

ルーティング用フィルターが作成され、「フィルター型ルーティングの設定」画面が表示されます。

18.「フィルター型ルーティング用フィルター」項目から「適用するフィルター型ルーティング用フィルター」項目の先頭に、作成したフィルター設定をドラッグ & ドロップする。

NVR700W 閉じる ヘルプ

### フィルター型ルーティングの設定

現在の設定内容を表示しています。設定の追加、変更、削除ができます。

[i] [フィルター型ルーティング用フィルター] 設定を変更しました。

#### フィルター型ルーティング用フィルター

番号	タイプ	プロトコル	送信元情報(IPアドレス/ポート番号) 宛先情報 (IPアドレス/ポート番号)
----	-----	-------	--

Drag and Drop  
設定が確定したら、下部の「確認」ボタンを押してください。

#### 適用するフィルター型ルーティング用フィルター

評価順	番号	タイプ	プロトコル	送信元情報(IPアドレス/ポート番号) 宛先情報 (IPアドレス/ポート番号)	設定	はずす
1	500002	pass	*	192.168.100.30	設定	はずす

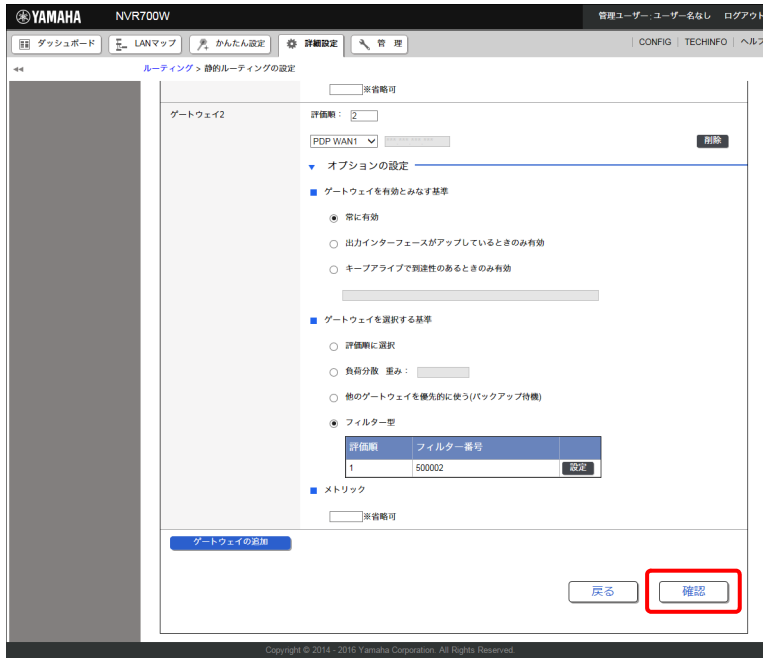
キャンセル 確認

Copyright © 2014 - 2016 Yamaha Corporation. All Rights Reserved.

19.「確認」ボタンをクリックする。

「フィルター型ルーティングの設定」画面が閉じられます。

## 20. 「確認」 ボタンをクリックする。



「入力内容の確認」画面が表示されます。

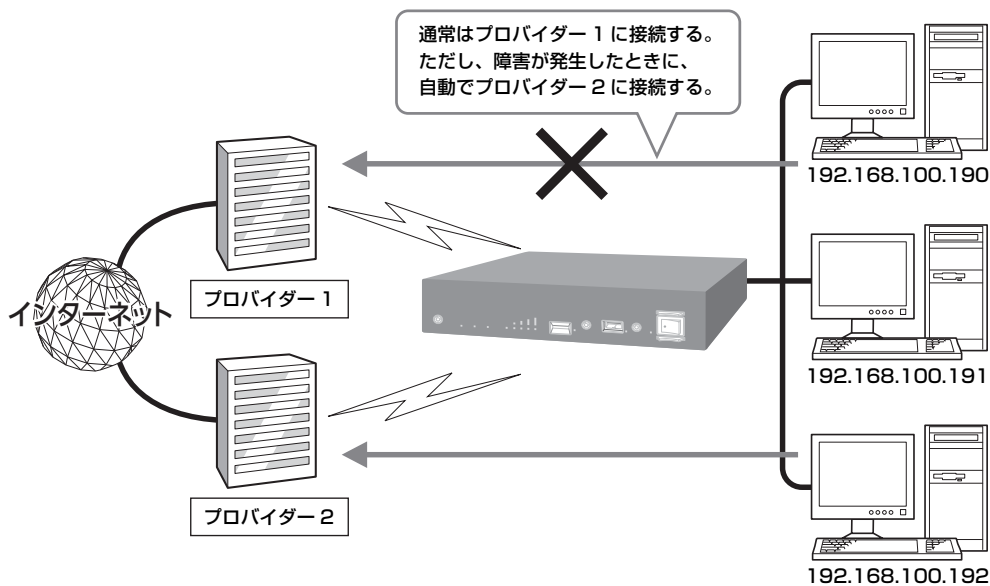
## 21. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「ルーティングの設定」画面が表示されます。

### 13.6.3 バックアップ回線を用意する

主のインターネット回線に障害が発生したときに、予備のインターネット回線に自動で切り替えることができます。



#### ご注意

本機能は NVR700W のみ利用できます。NVR510 では利用できません。

#### 設定例

##### ゲートウェイ 1

プロバイダー：PPPoE 接続型プロバイダー（主回線）  
キープアライブ機能で使用する IP アドレス：203.0.113.1

##### ゲートウェイ 2

プロバイダー：USB 接続型データ通信端末でプロバイダー接続（予備回線）

#### メモ

キープアライブ機能とは、指定の IP アドレスへ ICMP Echo を送信して到達性を確認し、到達性がある限り、そのゲートウェイを有効とみなす機能のことです。到達性がなくなった場合に予備回線のゲートウェイに切り換わります。宛先の IP アドレスには、安定的に稼動しているサーバーなどの固定グローバル IP アドレスを指定してください。

#### 1. 「詳細設定」タブ - 「ルーティング」を順に選択する。

「ルーティング」画面が表示されます。

## 2. 「静的ルーティングの一覧」項目の default 経路の「設定」ボタンをクリックする。

The screenshot shows the 'ルーティング' (Routing) configuration page for a Yamaha NVR700W device. The left sidebar contains navigation options like LAN, ONU, IP電話, ルーティング, NAT, IPフィルター, DNSサーバー, DHCPサーバー, and メール通知. The main content area is titled 'ルーティング' and includes a 'ルーティング情報' (Routing Information) table and a '静的ルーティングの一覧' (Static Routing List) table.

**ルーティング情報**

プロトコル	有効な経路数	無効な経路数
Static	2	0
Implicit	1	0
Temporary	0	0
Redirect	0	0
RIP	0	0
OSPF	0	0
BGP	0	0
経路数の合計	3	0

**静的ルーティングの一覧**

優先ネットワーク	評価値	ゲートウェイ	オプション 有効基準	選択基準 フェルティマス	メトリック	
<input type="checkbox"/> default	1	pp 1	-	500000	-	設定
<input type="checkbox"/> default	2	dhcp wan1	-	-	-	

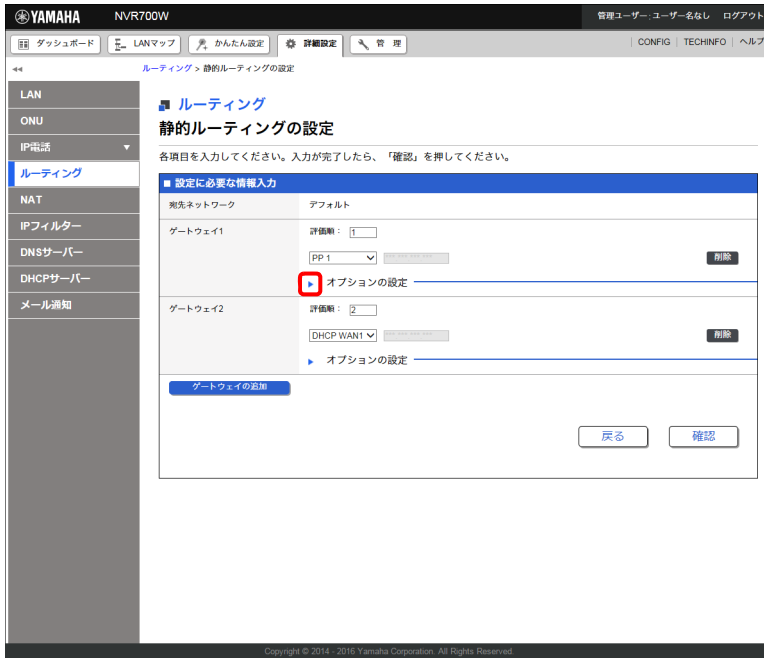
「静的ルーティングの設定」画面が表示されます。

## メモ

default 経路制御により、経路情報をコンパクトにすることができます。全ての TCP/IP ネットワークの経路情報をルーターが持とうとしても、経路情報が多過ぎて処理できません。default 経路により外側と内側を仕切り、未知のネットワークへのアクセスは default 経路に流すようになっています。

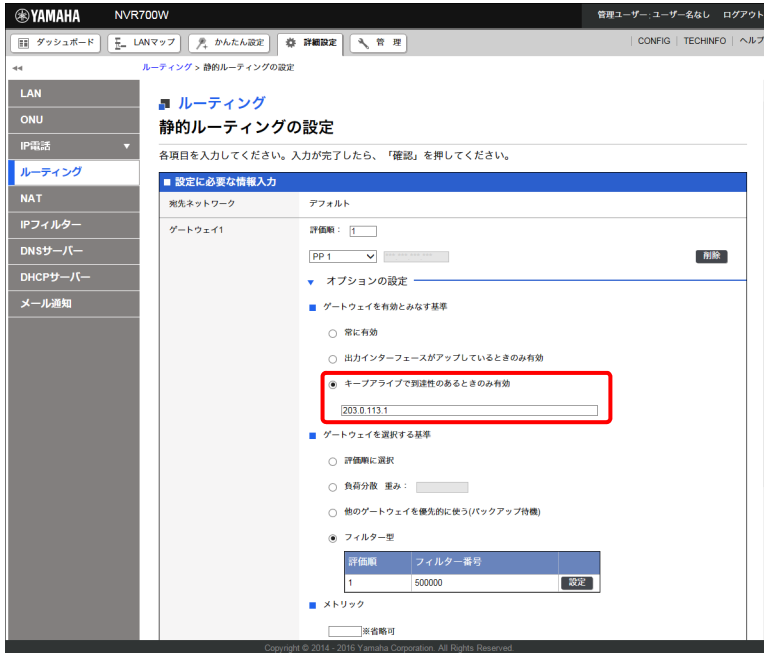
## 第 13 章 詳細設定を行う

3. 「ゲートウェイ 1」項目の「オプションの設定」の先頭にある「▶」ボタンをクリックする。

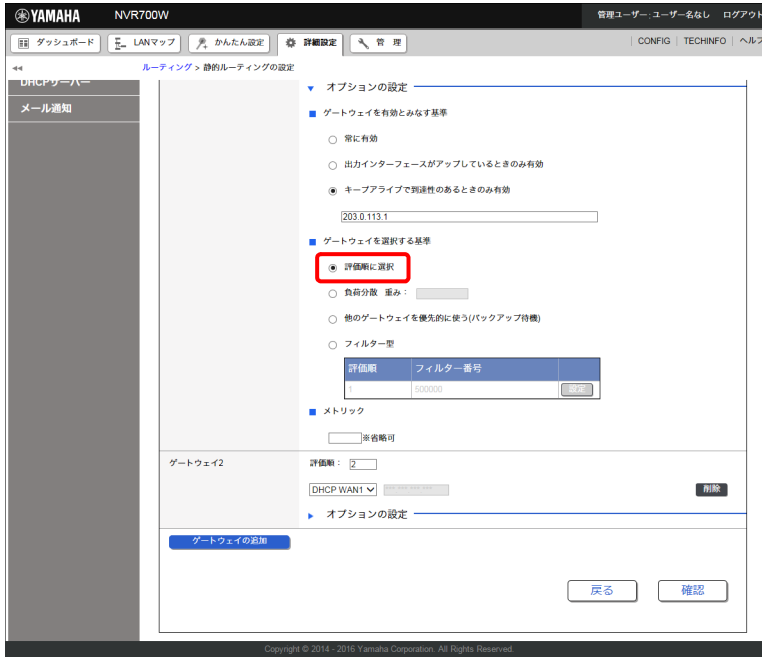


「オプションの設定」が表示されます。

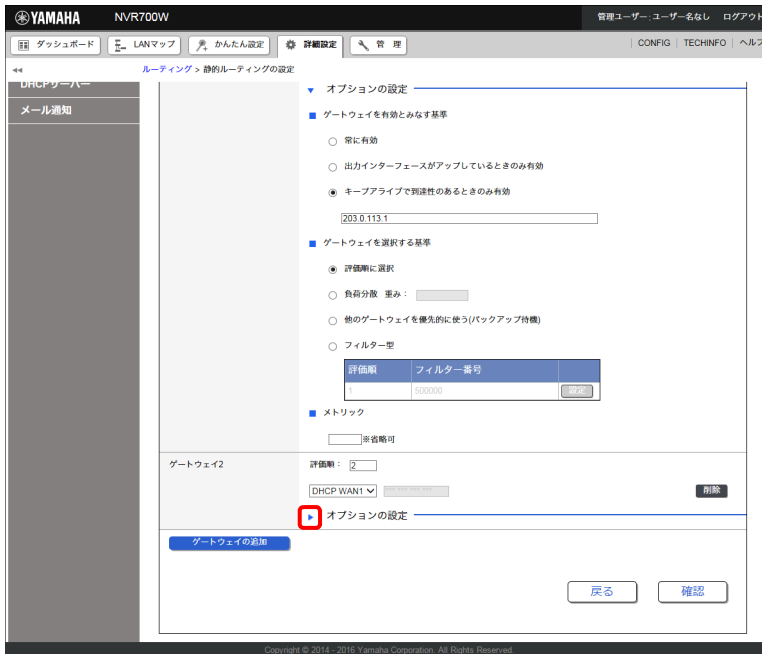
4. 「ゲートウェイを有効とみなす基準」欄で「キープアライブで到達性のあるときのみ有効」を選択し、「203.0.113.1」を入力する。



## 5. 「ゲートウェイを選択する基準」欄で「評価順に選択」を選択する。



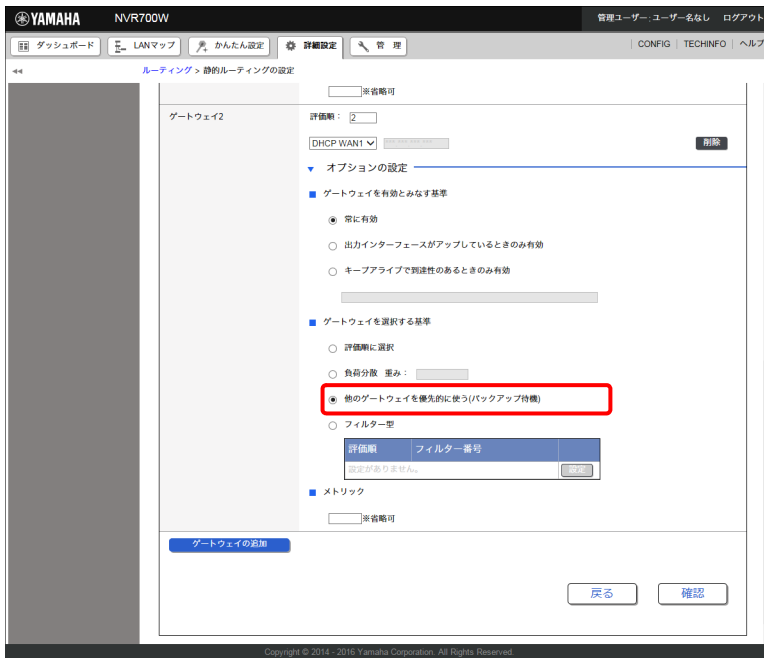
## 6. 「ゲートウェイ2」項目の「オプションの設定」の先頭にある「▶」ボタンをクリックする。



「オプションの設定」が表示されます。

## 第 13 章 詳細設定を行う

7. 「ゲートウェイを選択する基準」欄で「他のゲートウェイを優先的に使う（バックアップ待機）」を選択する。



8. 「確認」ボタンをクリックする。  
「入力内容の確認」画面が表示されます。
9. 内容を確認し、「設定の確定」ボタンをクリックする。

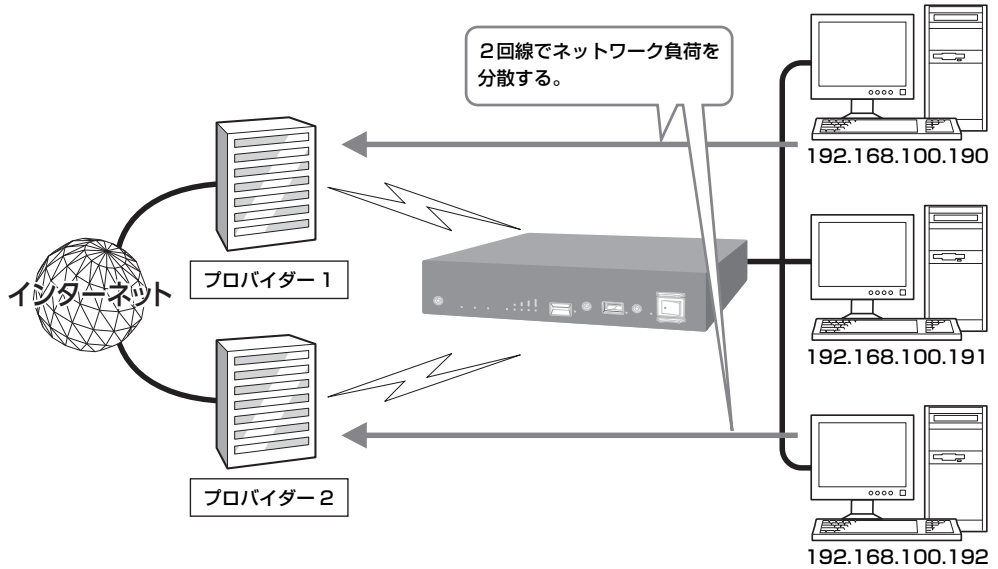


設定が反映され、「ルーティングの設定」画面が表示されます。



## 13.6.4 マルチホーミングによる負荷分散を行う

複数のインターネット回線を使用して、ネットワークの負荷を分散することができます。ネットワークの負荷を均等に分散する場合を例に説明します。



1. 「詳細設定」タブ - 「ルーティング」を順に選択する。  
「ルーティング」画面が表示されます。
2. 「静的ルーティングの一覧」項目の default 経路の「設定」ボタンをクリックする。

プロトコル	有効な経路数	無効な経路数
Static	2	0
Implicit	1	0
Temporary	0	0
Redirect	0	0
RIP	0	0
OSPF	0	0
BGP	0	0
経路数の合計	3	0

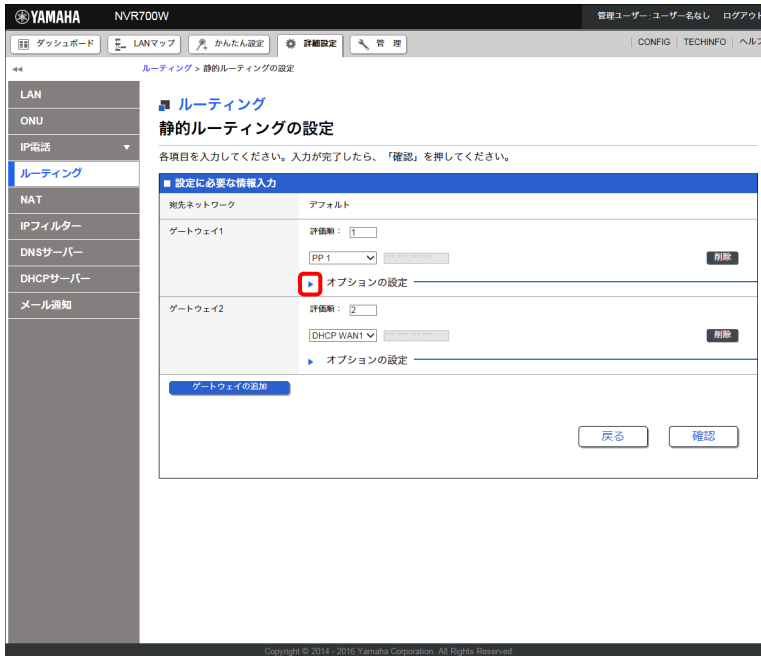
優先ネットワーク	詳細順	ゲートウェイ	オプション 有効基準	選択基準 フィルタースキーム	メトリック	
<input type="checkbox"/>	default	pp 1	-	500000	-	設定
<input type="checkbox"/>		dhcp wan1	-	-	-	

「静的ルーティングの設定」画面が表示されます。

### メモ

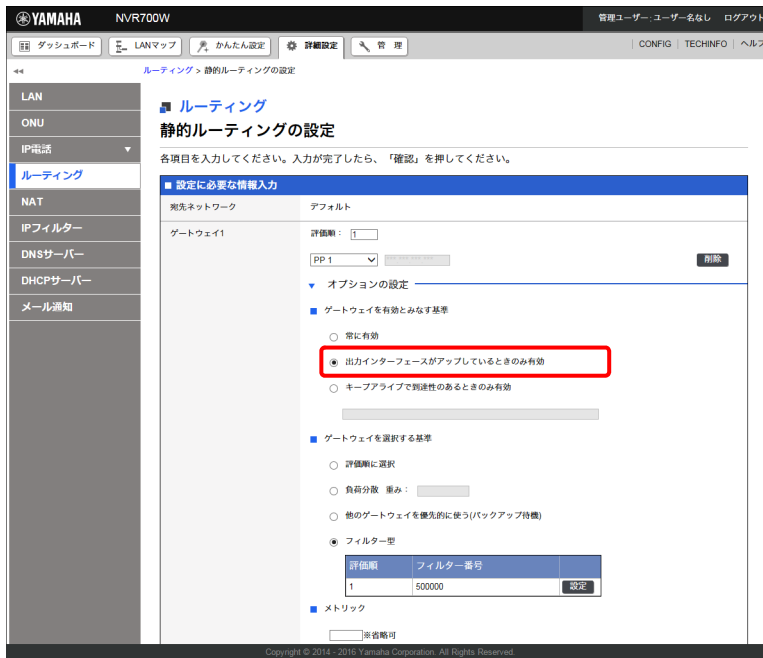
default 経路制御により、経路情報をコンパクトにすることができます。全ての TCP/IP ネットワークの経路情報をルーターが持とうとしても、経路情報が多過ぎて処理できません。default 経路により外側と内側を仕切り、未知のネットワークへのアクセスは default 経路に流すようになっています。

3. 「ゲートウェイ 1」項目の「オプションの設定」の先頭にある「▶」ボタンをクリックする。



「オプションの設定」が表示されます。

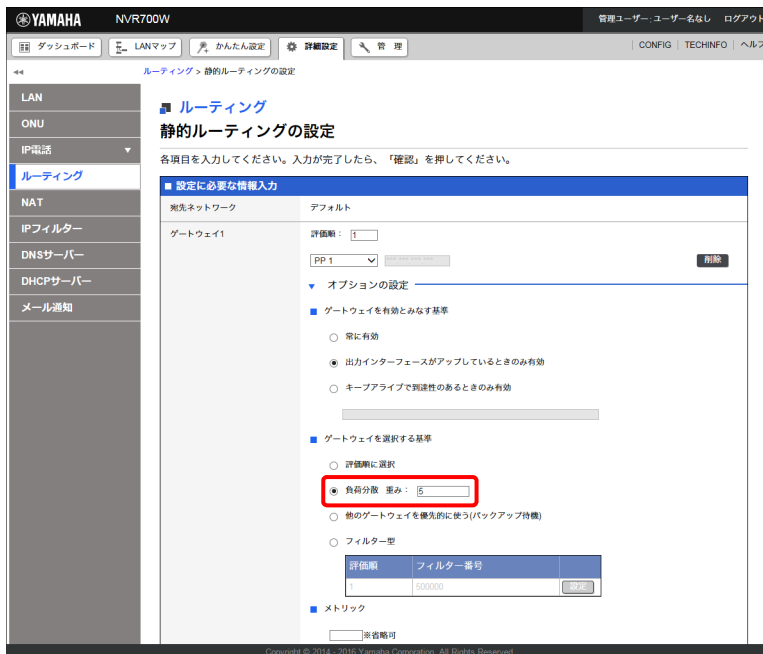
4. 「ゲートウェイを有効とみなす基準」欄で「出力インターフェースがアップしているときのみに有効」を選択する。



## メモ

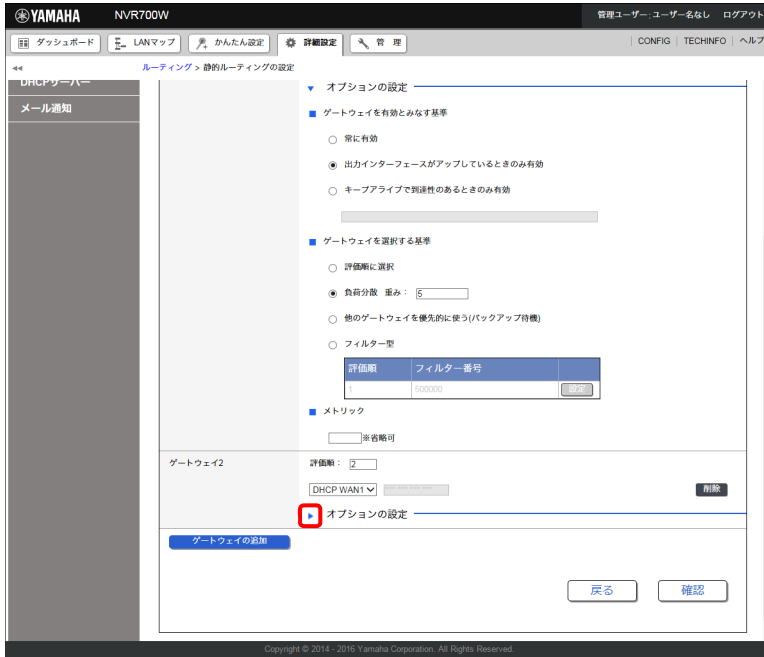
「出力インターフェースがアップしているときのみに有効」を選択することで、片方に障害が発生しても他方で通信を継続することができます。

5. 「ゲートウェイを選択する基準」欄で「負荷分散」を選択し、「5」を入力する。



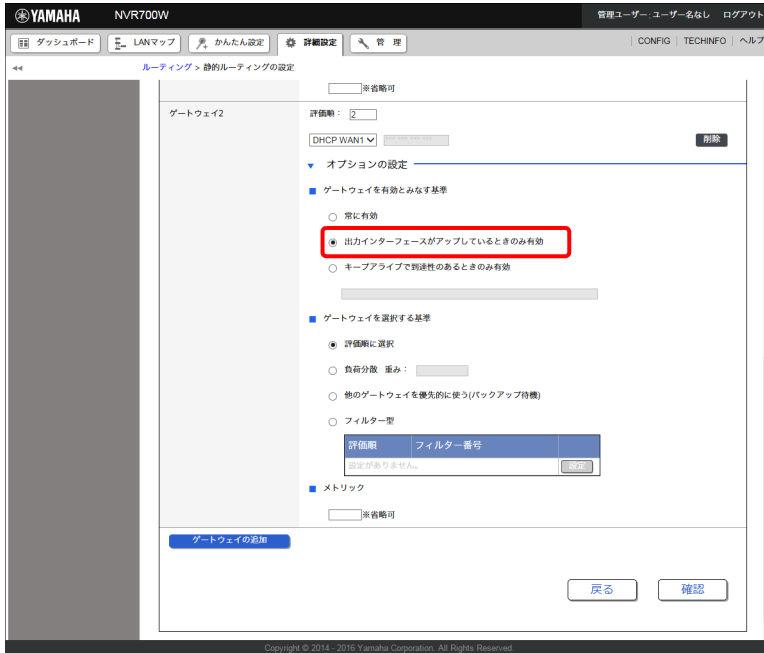
## 第 13 章 詳細設定を行う

6. 「ゲートウェイ 2」項目の「オプションの設定」の先頭にある「▶」ボタンをクリックする。



「オプションの設定」が表示されます。

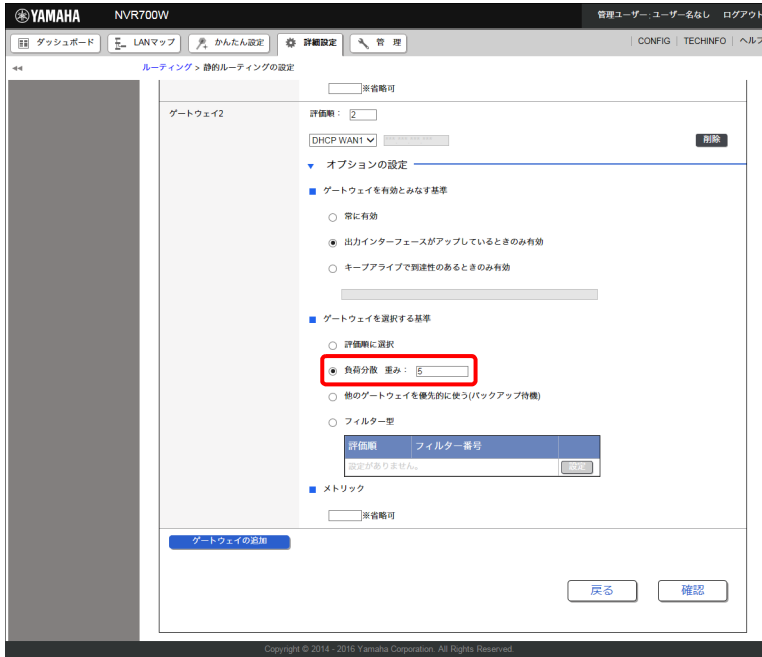
7. 「ゲートウェイを有効とみなす基準」欄で「出力インターフェースがアップしているときのみ有効」を選択する。



### メモ

「出力インターフェースがアップしているときのみ有効」を選択することで、片方に障害が発生しても他方で通信を継続することができます。

8. 「ゲートウェイを選択する基準」欄で「負荷分散」を選択し、「5」を入力する。



9. 「確認」ボタンをクリックする。  
「入力内容の確認」画面が表示されます。

10. 「設定の確定」ボタンをクリックする。



設定が反映され、「ルーティングの設定」画面が表示されます。

### 13.7 DNS サーバーを設定する

DNS サーバー機能の基本的な設定や上位の中継先 DNS サーバーの設定を行います。ヤマハルーターで DNS の名前解決ができなかった場合や、ヤマハルーターを介せずに端末が直接上位の DNS サーバーへ問い合わせを行う場合に、中継先 DNS サーバーの設定が必要になります。

#### 13.7.1 DNS サーバー機能の基本設定を行う

DNS サーバー機能の基本的な設定を行います。ヤマハルーターを DNS リカーシブサーバーとして動作させる場合を例に説明します。

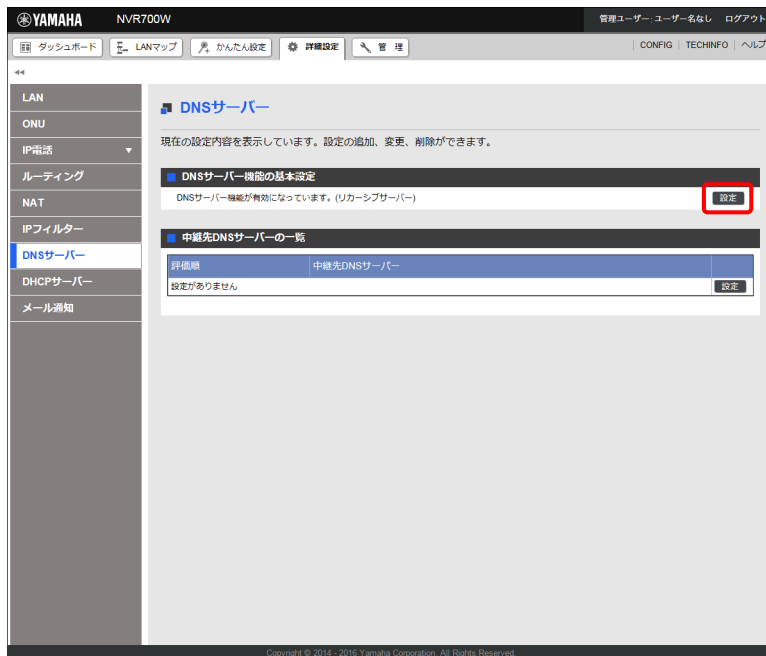
##### 設定例

DNS サーバー機能：リカーシブサーバーとして動作させる

DNS 問い合わせパケットの始点ポート番号：10000-10999

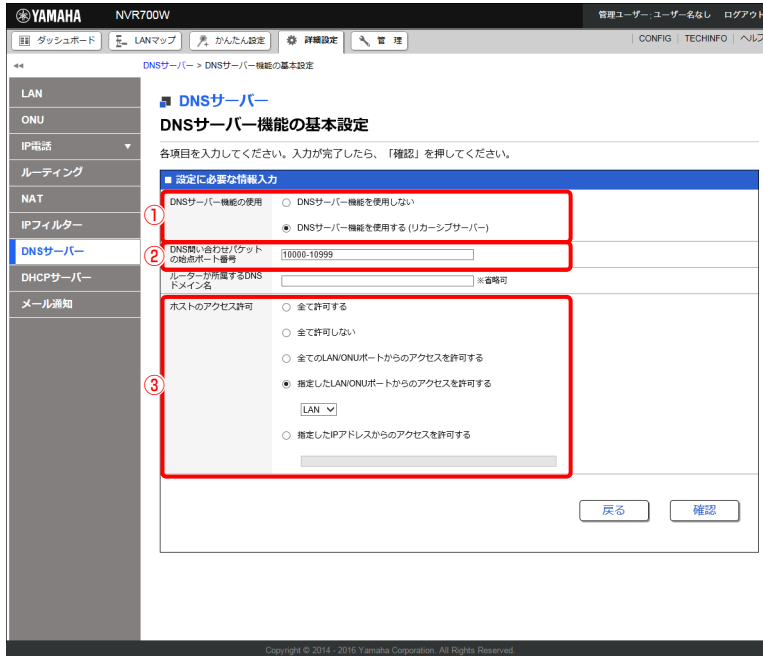
DNS 問い合わせを許可するホスト：LAN のネットワークに接続しているホスト

1. 「詳細設定」タブ - 「DNS サーバー」を順に選択する。  
「DNS サーバー」画面が表示されます。
2. 「DNS サーバー機能の基本設定」項目の「設定」ボタンをクリックする。



「DNS サーバー機能の基本設定」画面が表示されます。

## 3. DNS サーバーの基本機能を設定する。



- ① DNS サーバー機能の使用：  
「DNS サーバー機能を使用する」を選択します。
  - ② DNS 問い合わせパケットの始点ポート番号：  
「10000-10999」を入力します。
  - ③ ホストのアクセス許可：  
「指定した LAN/ONU ポートからのアクセスを許可する」を選択し、「LAN」を選択します。
4. 「確認」 ボタンをクリックする。  
「入力内容の確認」 画面が表示されます。

## 第 13 章 詳細設定を行う

### 5. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「DNS サーバー」画面が表示されます。

### 13.7.2 中継先 DNS サーバーを設定する

DNS 問い合わせの中継先の DNS サーバーを設定します。

#### プロバイダーから DNS サーバーが指定されている場合

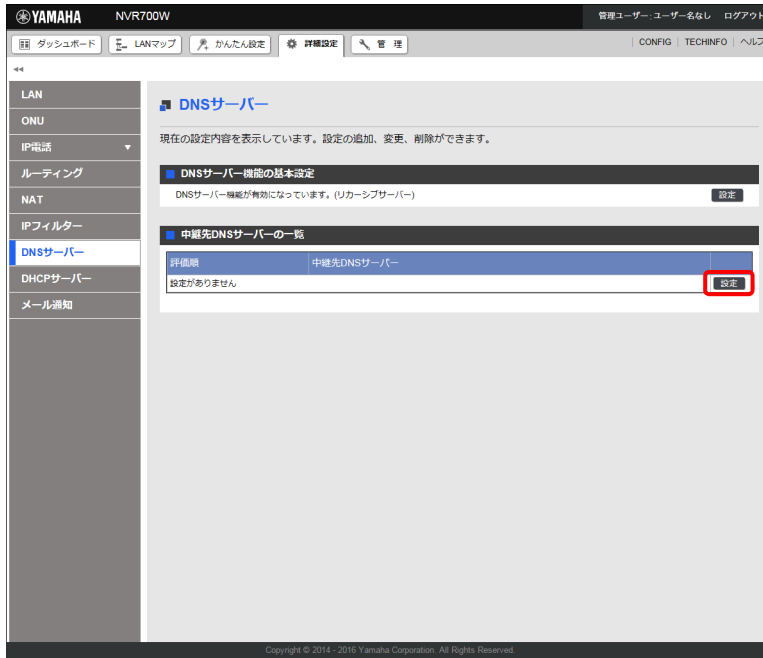
##### 設定例

DNS サーバーアドレス : 203.0.113.10、203.0.113.20

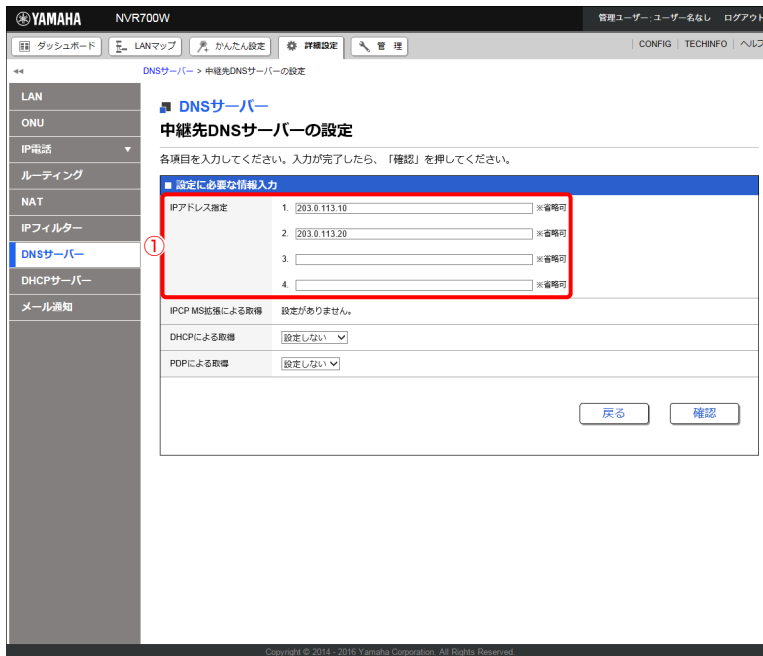
1. 「詳細設定」タブ - 「DNS サーバー」を順に選択する。  
「DNS サーバー」画面が表示されます。



## 2. 「中継先 DNS サーバーの一覧」項目の「設定」ボタンをクリックする。



## 3. 中継先 DNS サーバーを設定する。

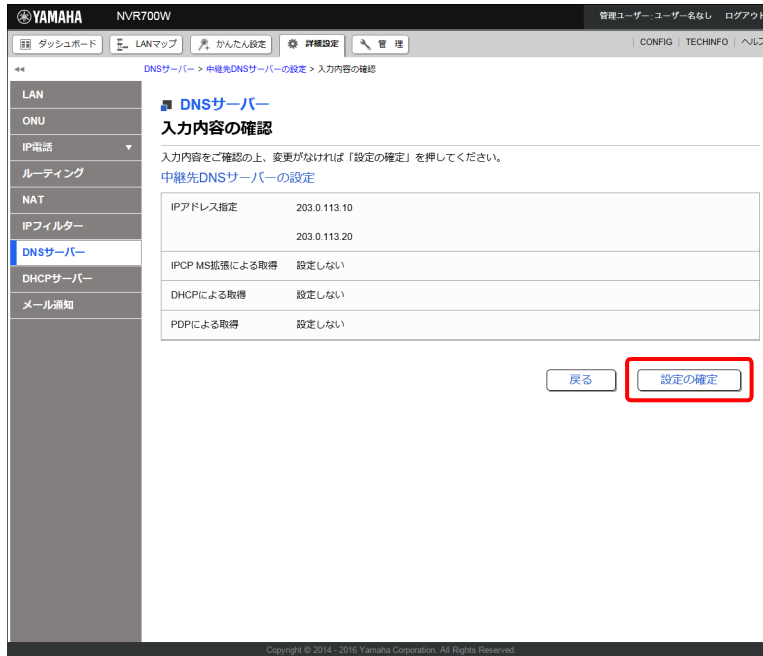


- ① IP アドレス指定：  
「203.0.113.10」と「203.0.113.20」を入力します。

4. 「確認」ボタンをクリックする。  
「入力内容の確認」画面が表示されます。

## 第 13 章 詳細設定を行う

### 5. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「DNS サーバー」画面が表示されます。

### DNS サーバーアドレスを自動取得する場合

#### 設定例

DNS サーバーアドレス：PPPoE 接続型のプロバイダー接続が設定されている PP1 インターフェースから DNS サーバーアドレスを取得

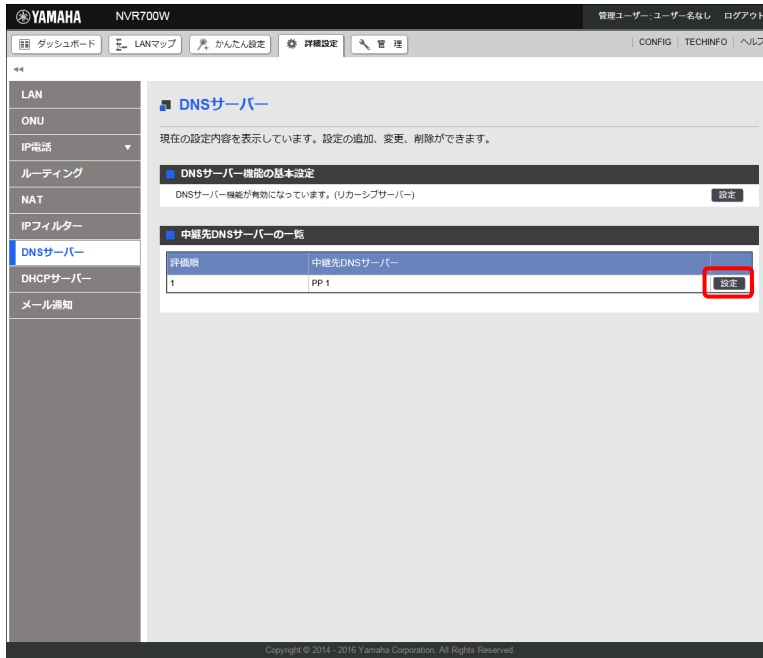
#### ご注意

プロバイダーから通知される DNS サーバーのアドレスを使用するため、事前にプロバイダー接続の設定を済ませておく必要があります。

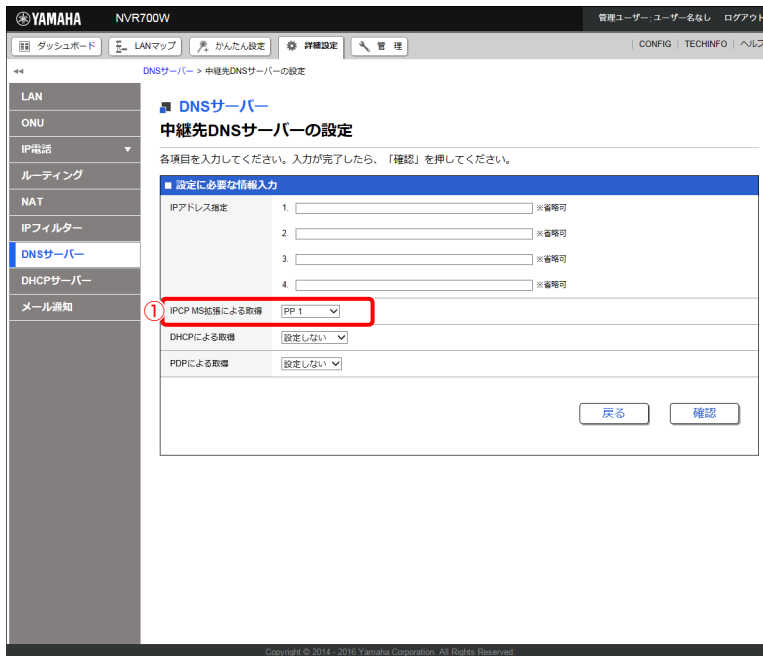
#### 1. 「詳細設定」タブ - 「DNS サーバー」を順に選択する。

「DNS サーバー」画面が表示されます。

## 2. 「中継先 DNS サーバーの一覧」項目の「設定」ボタンをクリックする。



## 3. 中継先 DNS サーバーを設定する。



① IPCP MS 拡張による取得：  
「PP 1」を選択します。

4. 「確認」ボタンをクリックする。  
「入力内容の確認」画面が表示されます。

## 第 13 章 詳細設定を行う

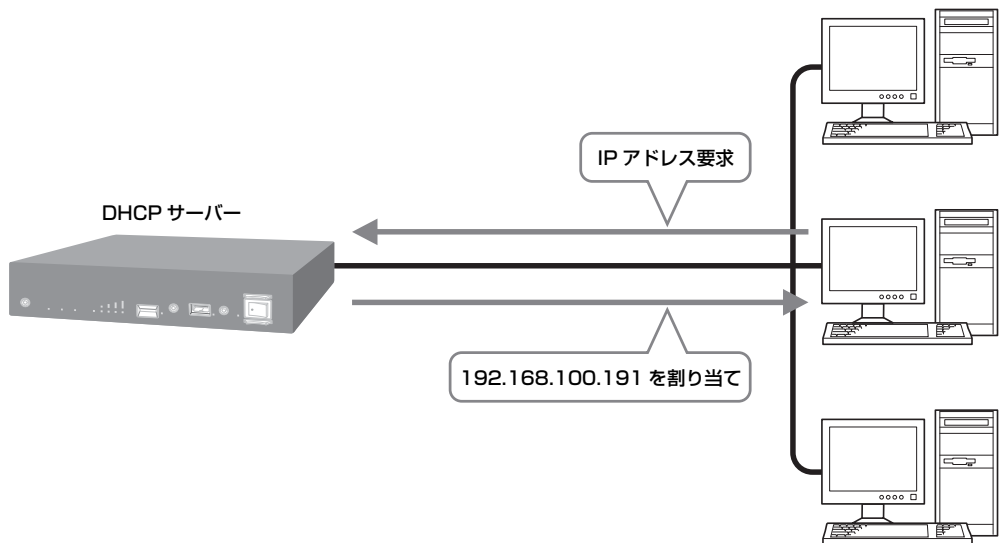
### 5. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「DNS サーバー」画面が表示されます。

## 13.8 DHCP で端末に IP アドレスを割り当てる

DHCP サーバー機能を使用して端末に IP アドレスを割り当てる設定を行います。



### 設定例

識別番号：1

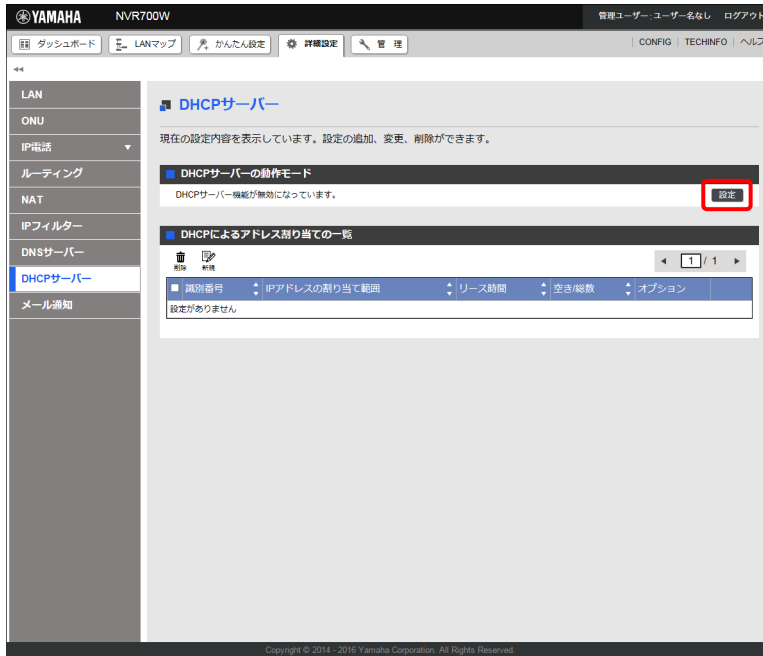
IP アドレスの割り当て範囲：192.168.100.100 - 192.168.100.200/24

リース時間：24 時間

## メモ

パソコン側の設定について詳しくは、「16.1 パソコンのIPアドレスを変更する」(368 ページ)をご覧ください。

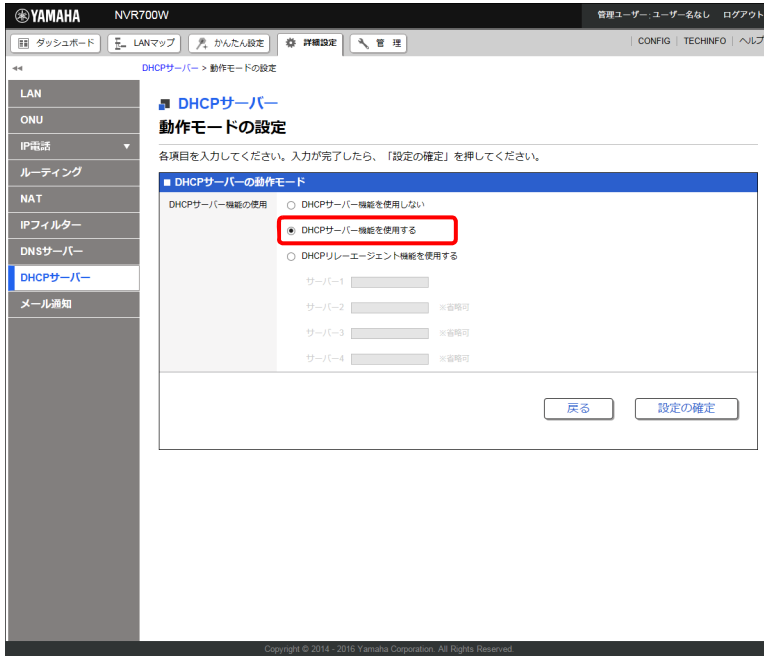
1. 「詳細設定」タブ - 「DHCP サーバー」を順に選択する。  
「DHCP サーバー」画面が表示されます。
2. 「DHCP サーバーの動作モード」項目の「設定」ボタンをクリックする。




「動作モードの設定」画面が表示されます。

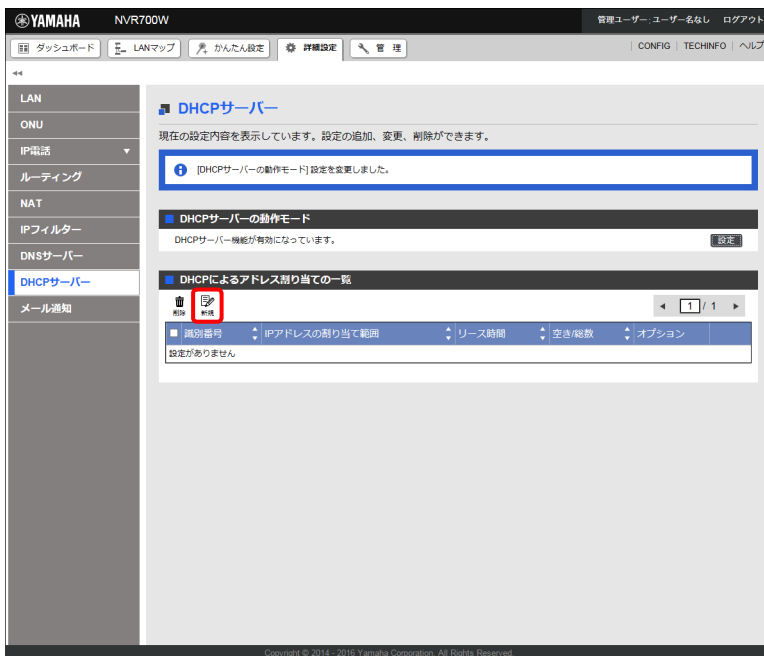
## 第 13 章 詳細設定を行う

3. 「DHCP サーバー機能を使用する」を選択し、「設定の確定」ボタンをクリックする。



設定が反映され、「DHCP サーバー」画面が表示されます。

4. 「DHCP によるアドレス割り当ての一覧」項目の「」ボタンをクリックする。



「アドレス割り当ての設定」画面が表示されます。

## 5. IPアドレスの割り当て範囲を設定する。

YAMAHA NVR700W 管理ユーザー-ユーザー名なし ログアウト

ダッシュボード LANマップ かんたん設定 詳細設定 管理

CONFIG TECHINFO ヘルプ

DHCPサーバー > アドレス割り当ての設定

LAN  
ONU  
IP電話  
ルーティング  
NAT  
IPフィルター  
DNSサーバー  
DHCPサーバー  
メール通知

**DHCPサーバー**  
アドレス割り当ての設定

各項目を入力してください。入力が完了したら、「確認」を押してください。

**設定に必要な情報入力**

① 識別番号

② IPアドレスの範囲 [192.168.100.100] ~ [192.168.100.200] / [255.255.255.0 (24bit)]

ゲートウェイ  ※省略可

③ リース時間  
 無制限  
 指定 [24] 時間 [0] 分

Copyright © 2014 - 2016 Yamaha Corporation. All Rights Reserved.

## ① 識別番号：

「1」を入力します。

## ② IPアドレスの範囲：

「192.168.100.100」と「192.168.100.200」を入力し、プルダウンメニューから「255.255.255.0 (24bit)」を選択します。

## ③ リース時間：

「指定」を選択し、「24 時間」と入力します。

## 6. 「確認」ボタンをクリックする。

「入力内容の確認」画面が表示されます。

## 第 13 章 詳細設定を行う

### 7. 内容を確認し、「設定の確定」ボタンをクリックする。

YAMAHA NVR700W 管理ユーザー ユーザー名なし ログアウト

ダッシュボード LANマップ かんたん設定 詳細設定 管理

CONFIG | TECHINFO | ヘルプ

DHCPサーバー > アドレス割り当ての設定 > 入力内容の確認

LAN  
ONU  
IP電話  
ルーティング  
NAT  
IPフィルター  
DNSサーバー  
DHCPサーバー  
メール通知

### DHCPサーバー

#### 入力内容の確認

入力内容をご確認の上、変更がなければ「設定の確定」を押してください。  
アドレス割り当ての設定

識別番号	1
IPアドレスの範囲	192.168.100.100 ~ 192.168.100.200 / 24
ゲートウェイ	
リース時間	指定 24 時間 0 分

戻る 設定の確定

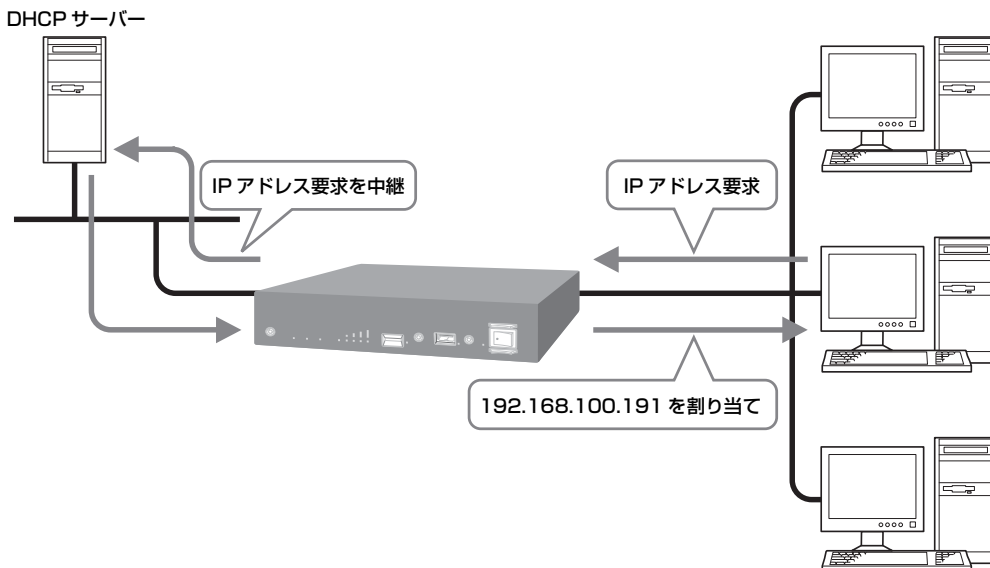
Copyright © 2014 - 2016 Yamaha Corporation. All Rights Reserved.

設定が反映され、「DHCP サーバー」画面が表示されます。



## 13.9 異なるセグメントの DHCP サーバーから端末に IP アドレスを割り当てる

DHCP はブロードキャストで通信を行うため、DHCP サーバーが端末の存在する LAN セグメントとは異なるネットワーク上に存在する場合、通常は端末に IP アドレスを割り当てることはできません。そのような環境においても、ヤマハルーターを DHCP リレーエージェントとして動作させれば、異なるセグメントに存在する DHCP サーバーから端末に IP アドレスを割り当てるできるようになります。本章では、ヤマハルーターを DHCP リレーエージェントとして動作させる設定方法について説明します。



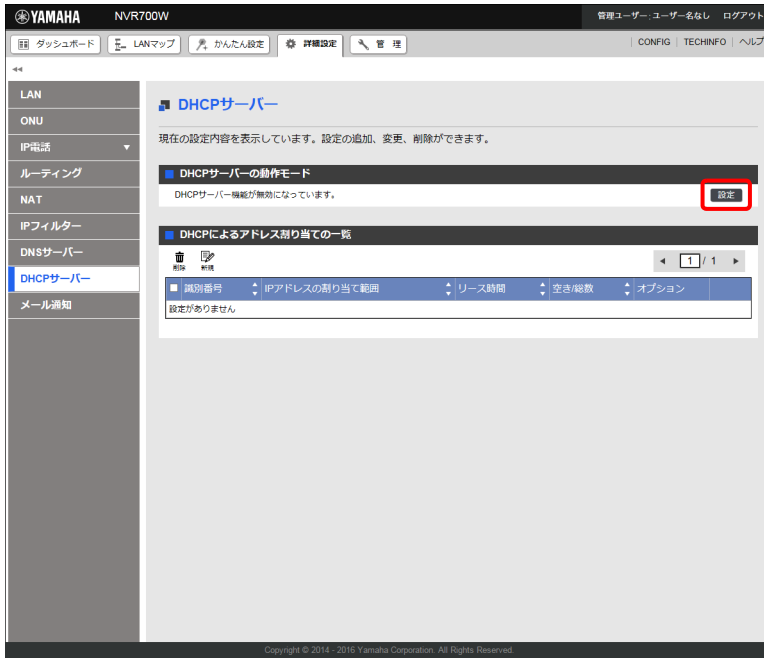
### 設定例

DHCP サーバーの IP アドレス : 192.168.1.1

1. 「詳細設定」タブ - 「DHCP サーバー」を順に選択する。  
「DHCP サーバー」画面が表示されます。

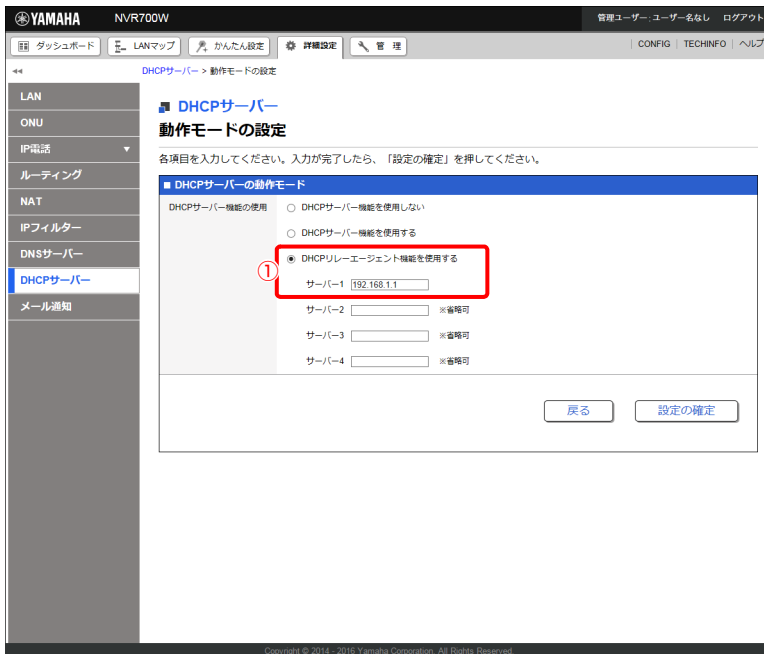
## 第 13 章 詳細設定を行う

### 2. 「DHCP サーバーの動作モード」項目の「設定」ボタンをクリックする。



「動作モードの設定」画面が表示されます。

### 3. DHCP リレーエージェント機能の設定をする。



#### ① DHCP サーバー機能の使用：

「DHCP リレーエージェント機能を使用する」を選択し、「192.168.1.1」を入力します。

### 4. 内容を確認し、「設定の確定」ボタンをクリックする。


設定が反映され、「DHCP サーバー」画面が表示されます。

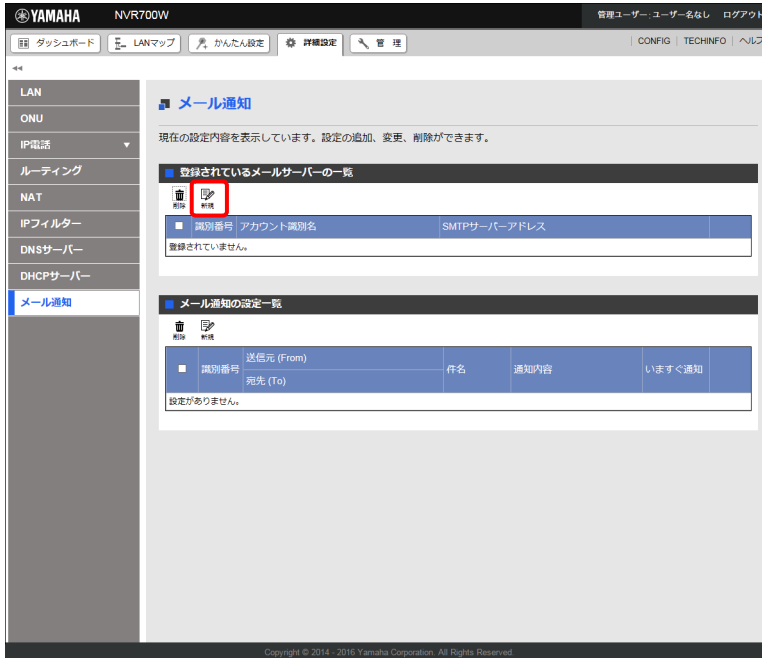
## 13.10 メール通知機能を使う

ネットワーク上で異常が検知されたときに、指定した宛先にメールで通知する設定を行います。また、インターフェースや経路の情報を、指定した宛先に手動で通知することもできます。

### 13.10.1 メールサーバーを設定する

宛先のメールサーバー（SMTP サーバー）を設定します。

1. 「詳細設定」タブ - 「メール通知」を順に選択する。  
「メール通知」画面が表示されます。
2. 「登録されているメールサーバーの一覧」項目の「 新視」ボタンをクリックする。



「メールサーバーの設定」画面が表示されます。

## 第 13 章 詳細設定を行う

### 3. メールサーバーを設定する。

YAMAHA NVR700W 管理ユーザー ユーザー名なし ログアウト

ダッシュボード LANマップ かんたん設定 詳細設定 管理

CONFIG | TECHINFO | ヘルプ

メール通知 > メールサーバーの設定

### メール通知

#### メールサーバーの設定

各項目を入力してください。入力が完了したら、「確認」を押してください。

識別番号	1
アカウント識別名	<input type="text"/> ※省略可
SMTPサーバーアドレス	<input type="text" value="192.168.100.1"/>
SMTPサーバーのポート番号	<input type="checkbox"/> サブミッションポート (587番ポート) <input type="text" value="25"/>
SMTP認証 (SMTP-AUTH)	認証方式: <input type="text" value="PLAIN"/> ユーザー名: <input type="text" value="yamaha"/> パスワード: <input type="text" value="yamaha"/>

Copyright © 2014 - 2016 Yamaha Corporation. All Rights Reserved.

#### ① SMTP サーバーアドレス：

メールを送信するときに使用する SMTP サーバーの IP アドレス、またはドメイン名を入力します。

#### ② SMTP サーバーのポート番号：

SMTP サーバーのポート番号を入力します。

「サブミッションポート (587 番ポート)」を選択すると、サブミッションポートの 587 番ポートが設定されます。

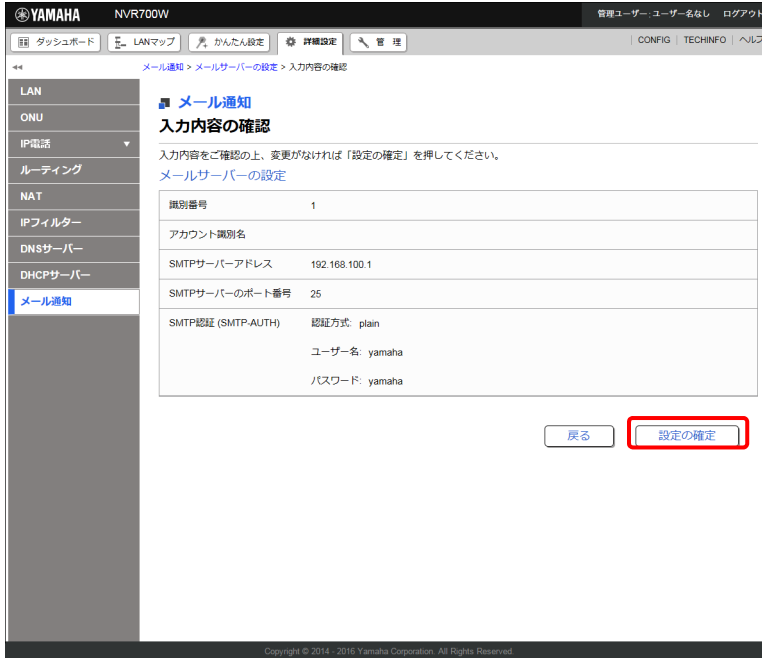
#### ③ SMTP 認証 (SMTP-AUTH)：

SMTP サーバーとの認証方式を選択し、ユーザー名とパスワードを入力します。

### 4. 「確認」ボタンをクリックする。

「入力内容の確認」画面が表示されます。


## 5. 内容を確認し、「設定の確認」ボタンをクリックする。

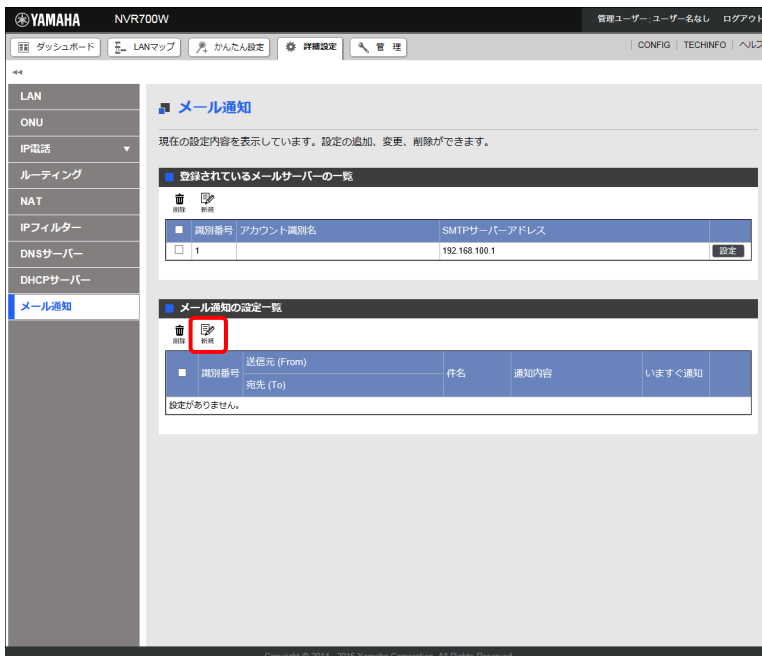


設定が反映され、「メール通知」画面が表示されます。

## 13.10.2 メール通知を設定する

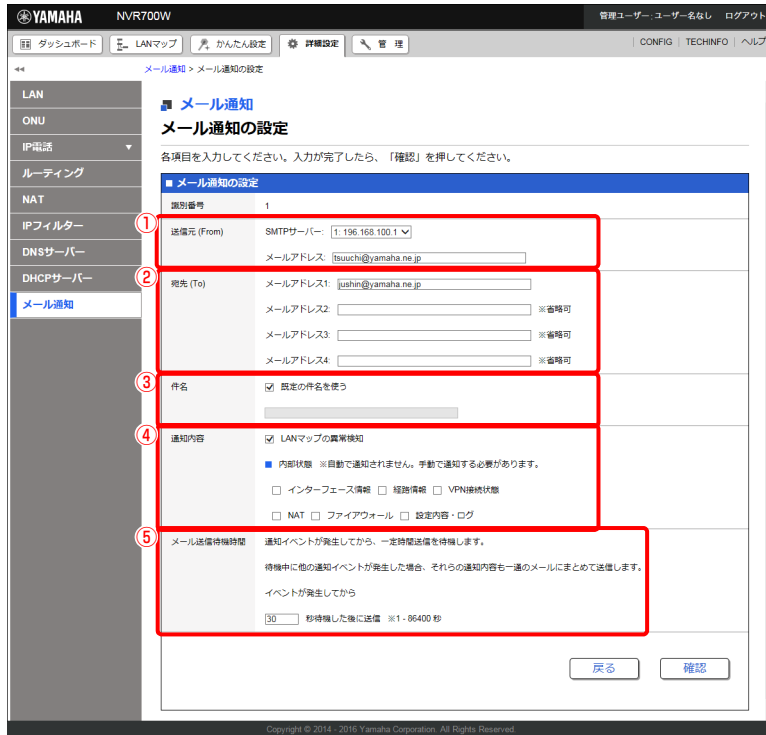
メール通知の送信元、宛先アドレスや、通知内容などを設定します。

1. 「詳細設定」タブ - 「メール通知」を順に選択する。  
「メール通知」画面が表示されます。
2. 「メール通知の設定一覧」項目の「」ボタンをクリックする。



「メール通知の設定」画面が表示されます。

3. メール通知を設定する。



① 送信元 (From) :

メールを送信するとき使用する SMTP サーバーの IP アドレス、またはドメイン名を入力します。

② 宛先 (To) :

送信するメールの宛先のメールアドレスを 4 件まで入力します。

③ 件名 :

送信するメールの件名を入力します。  
「既定の件名を使う」を選択すると、既定の件名で送信されます。

④ 通知内容 :

通知内容を選択します。

⑤ メール送信待機時間 :

通知イベントが発生してから、メール送信を待機する時間を入力します。待機中に他の通知イベントが発生した場合、それらの通知内容も一通のメールにまとめて送信されます。

メモ

内部状態は自動では送信されません。「メール通知」画面の「進む」ボタンをクリックして、「実行」ボタンをクリックすると、指定した宛先に内部状態が通知されます。

4. 「確認」ボタンをクリックする。

「入力内容の確認」画面が表示されます。

## 5. 内容を確認し、「設定の確定」ボタンをクリックする。

YAMAHA NVR700W 管理ユーザー-ユーザー名なし ログアウト

ダッシュボード LANマップ かんたん設定 詳細設定 管理 CONFIG TECHINFO ヘルプ

メール通知 > メール通知の設定 > 入力内容の確認

### メール通知

#### 入力内容の確認

入力内容をご確認の上、変更がなければ「設定の確定」を押してください。

#### メール通知の設定

識別番号	1
送信元 (From)	SMTPサーバー: 1: 196.168.100.1 メールアドレス: tsuchi@yamaha.ne.jp
宛先 (To)	メールアドレス1: jushin@yamaha.ne.jp メールアドレス2: メールアドレス3: メールアドレス4:
件名	(既定の件名を使う)
通知内容	LANマップの異常検知
メール送信待機時間	30 秒

戻る 設定の確定

Copyright © 2014 - 2016 Yamaha Corporation. All Rights Reserved.

設定が反映され、「メール通知」画面が表示されます。

### ご注意

メールサーバーが未設定の場合、メール通知の設定を行うことはできません。

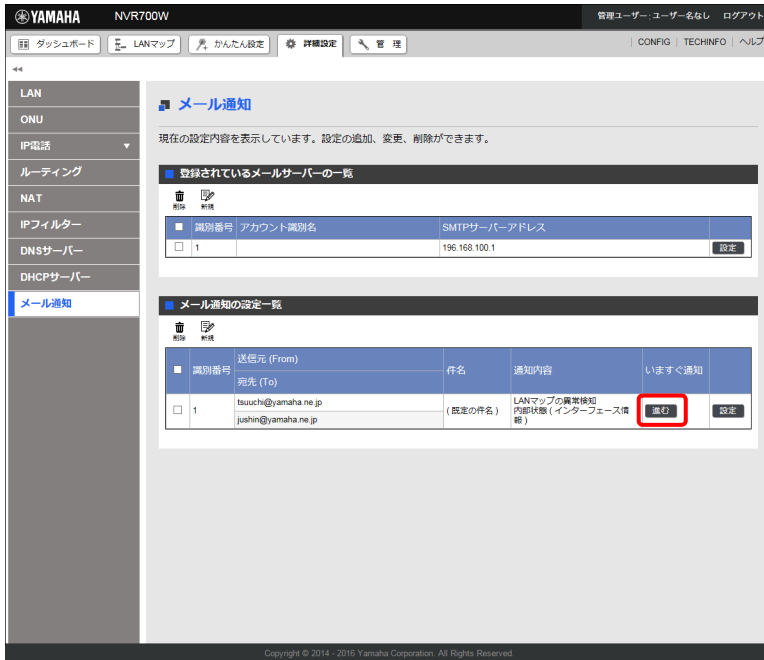
## 13.10.3 ヤマハルーターの内部状態をメールで通知する

ヤマハルーターの内部状態を登録した宛先へ通知します。

1. 「詳細設定」タブ - 「メール通知」を順に選択する。  
「メール通知」画面が表示されます。

## 第 13 章 詳細設定を行う

### 2. 「いますぐ通知」の「進む」ボタンをクリックする。

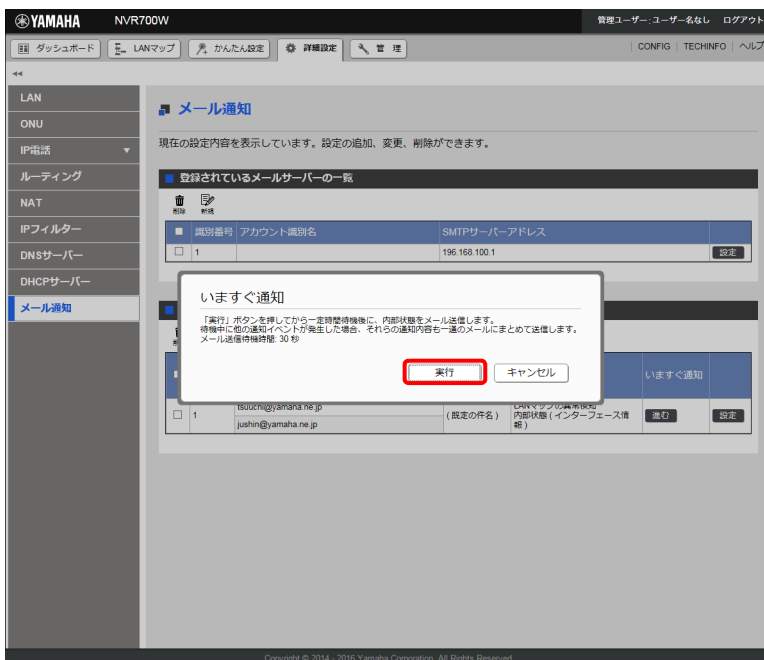


「いますぐ通知」ダイアログが表示されます。

### メモ

「進む」ボタンは、「メール通知の設定」画面の通知内容で内部状態を選択している場合にのみ表示されます。

### 3. 「いますぐ通知」ダイアログの「実行」ボタンをクリックする。



ヤマハルーターの内部状態が登録した宛先に通知されます。



# 第 14 章 ヤマハルーターを管理する

本章では、ファームウェアの更新を行ったり、CONFIG ファイルを外部メモリへエクスポートして保存するといった、ヤマハルーターの管理に関連する操作について説明します。

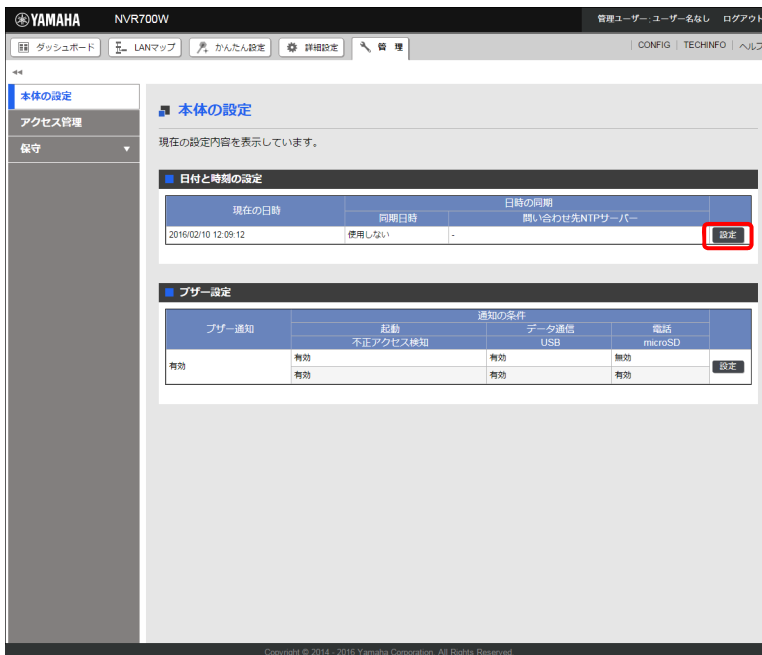
- ・ ヤマハルーターの日時を合わせる …333 ページ
- ・ ブザーを設定する …335 ページ
- ・ コマンドを実行する …337 ページ
- ・ ファームウェアを更新する …341 ページ
- ・ 設定 (CONFIG) を管理する …351 ページ
- ・ SYSLOG を管理する …357 ページ
- ・ ヤマハルーターを再起動する …361 ページ
- ・ ヤマハルーターを工場出荷時の状態へ戻す …364 ページ

## 14.1 ヤマハルーターの日時を合わせる

現在日時の設定や、NTP サーバーとの同期の設定を行います。

### 14.1.1 日付と時刻を設定する

1. 「管理」タブ – 「本体の設定」を順に選択する。  
「本体の設定」画面が表示されます。
2. 「日付と時刻の設定」項目の「設定」ボタンをクリックする。



「日付と時刻の設定」画面が表示されます。

## 第 14 章 ヤマハルーターを管理する

### 3. 日付と時刻を設定する。

#### ① 手動設定：

日時の設定を更新する場合は、「以下の日時に合わせる」にチェックを入れます。

- ・「年 / 月 / 日」：日付を YYYY/MM/DD 形式で入力します。「年 / 月 / 日」欄にフォーカスを合わせるとカレンダーが表示され、カレンダーから日付を選択することもできます。
- ・「時 : 分 : 秒」：時刻を hh:mm:ss 形式で入力します。「時 : 分 : 秒」欄にフォーカスを合わせると時刻のリストが表示され、リストから時刻を選択することもできます。

#### ② 日時の同期：

日時を自動的に補正したい場合は、日時同期のスケジュールと問い合わせ先の NTP サーバーを設定します。

- ・ 定期間隔：NTP サーバーとの同期する間隔を選択します。
- ・ 「時 : 分 : 秒」：時刻を hh:mm:ss 形式で入力します。「時 : 分 : 秒」欄にフォーカスを合わせると時刻のリストが表示され、リストから時刻を選択することもできます。
- ・ 問い合わせ先 NTP サーバー：同期を行う NTP サーバーのホスト名または IP アドレスを入力します。

### ご注意

NTP サーバーの負荷を分散させるためにも、00 分 00 秒のようにアクセスが集中しやすい時刻を同期日時に設定することはお控えください。

### メモ

日付と時刻の設定、および、NTP サーバーとの同期の設定は、「かんたん設定」－「基本設定」－「日付と時刻の設定」画面から行うこともできます。

### 4. 「設定の確定」ボタンをクリックする。

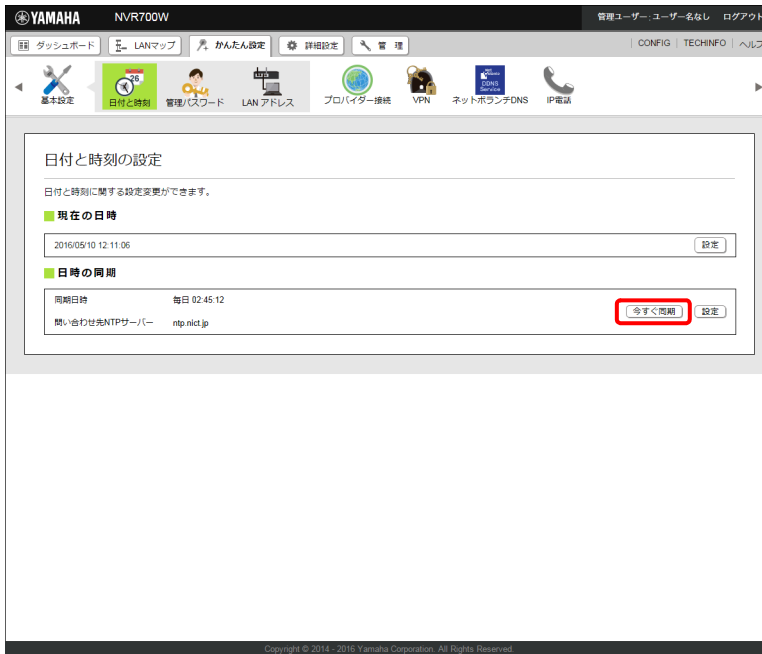
設定が反映され、「本体の設定」画面が表示されます。

### 14.1.2 NTP サーバーと今すぐ同期する

#### ご注意

日時同期のスケジュールと問い合わせ先 NTP サーバーが設定され、インターネットに接続している場合のみ行えます。

1. 「かんたん設定」タブ - 「基本設定」 - 「日付と時刻」ボタンを順に選択する。  
「日付と時刻の設定」画面が表示されます。
2. 「日時の同期」項目の「今すぐ同期」ボタンをクリックする。



NTP サーバーとの同期が開始されます。

## 14.2 ブザーを設定する

ブザーの有効 / 無効の切り換えや通知条件の設定を行います。

#### Web GUI で設定できるブザー

- ・ 本製品が起動したとき
- ・ データ通信が接続したとき、切断したとき
- ・ 電話をかけてつながったとき、通話を切ったとき
- ・ 不正アクセスを検出したとき
- ・ USB デバイスの状態が変化したとき
- ・ microSD デバイスの状態が変化したとき

#### メモ

Web GUI で設定できるブザーは、コマンドでも設定することができます。

#### コマンドで設定できるブザー

- ・ バッチファイル実行機能に関連するブザー (alarm batch)
- ・ HTTP リビジョンアップ機能に関連するブザー (alarm http revision-up)

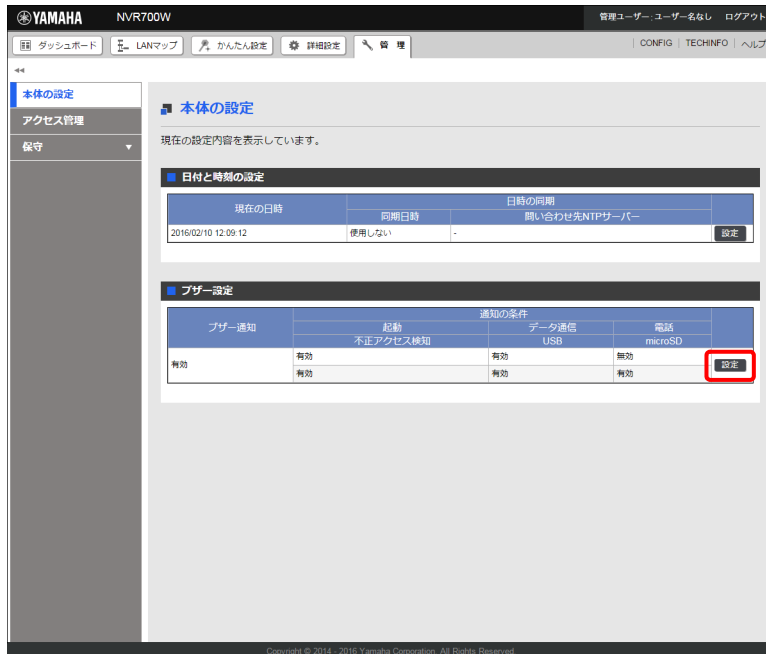
## 第 14 章 ヤマハルーターを管理する

- ・ HTTP アップロード機能に関連するブザー (alarm http upload)
- ・ Lua スクリプト機能に関連するブザー (alarm lua)
- ・ 携帯端末の接続時のブザー (alarm mobile)

### メモ

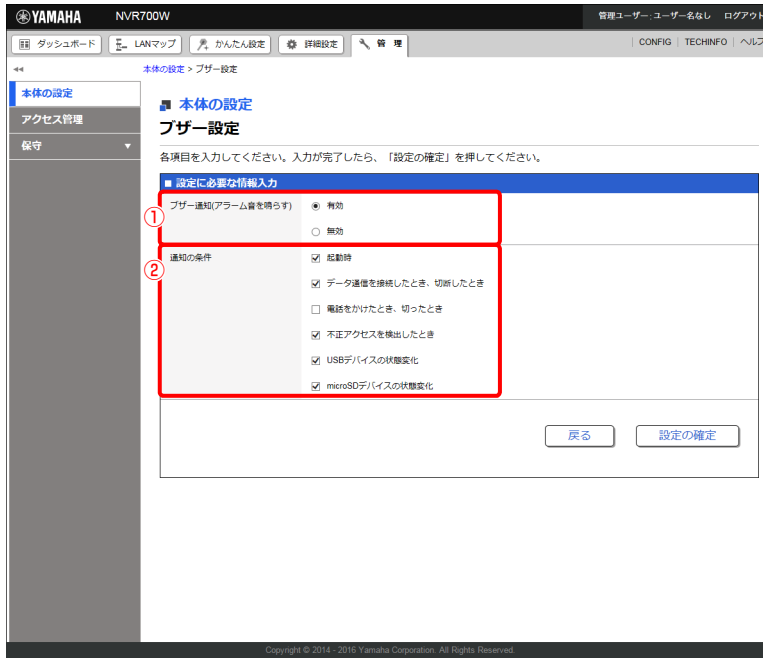
Web GUI で設定できないブザーの設定方法について詳しくは、「コマンドリファレンス」(製品付属の CD-ROM に収録)をご覧ください。

1. 「管理」タブ - 「本体の設定」を順に選択する。  
「本体の設定」画面が表示されます。
2. 「ブザー設定」項目の「設定」ボタンをクリックする。



「ブザー設定」画面が表示されます。

## 3. ブザーを設定する。



- ① **ブザー通知 (アラーム音を鳴らす) :**  
ブザー通知を有効にするか無効にするかを選択します。
- ② **通知の条件 :**  
ブザー通知を行う条件にチェックを入れます。

## 4. 「設定の確定」 ボタンをクリックする。

設定が反映され、「本体の設定」画面が表示されます。

## 14.3 コマンドを実行する

Web GUIのコマンド入力画面でコマンドを実行したり、コマンドの実行結果をテキスト形式で取得したりすることができます。Web GUIには設定項目がない機能を使用したい場合などに役立ちます。

まず、以下の条件で QoS (優先制御) を設定する場合を例に説明します。なお、WAN インターフェースに PPPoE 接続型のプロバイダーが設定されているものとします。

## 設定例

インターフェース速度 : 80Mbit/s

最高優先度 (クラス 4) : VoIP

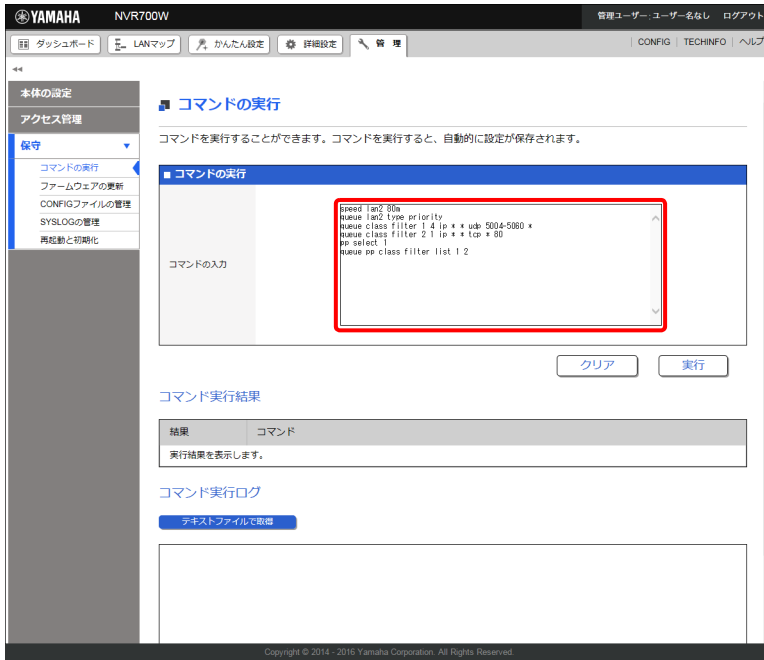
最低優先度 (クラス 1) : WWW

## 1. 「管理」タブ - 「保守」 - 「コマンドの実行」を順に選択する。

「コマンドの実行」画面が表示されます。

## 第 14 章 ヤマハルーターを管理する

### 2. 「コマンドの実行」項目にコマンドを入力する。



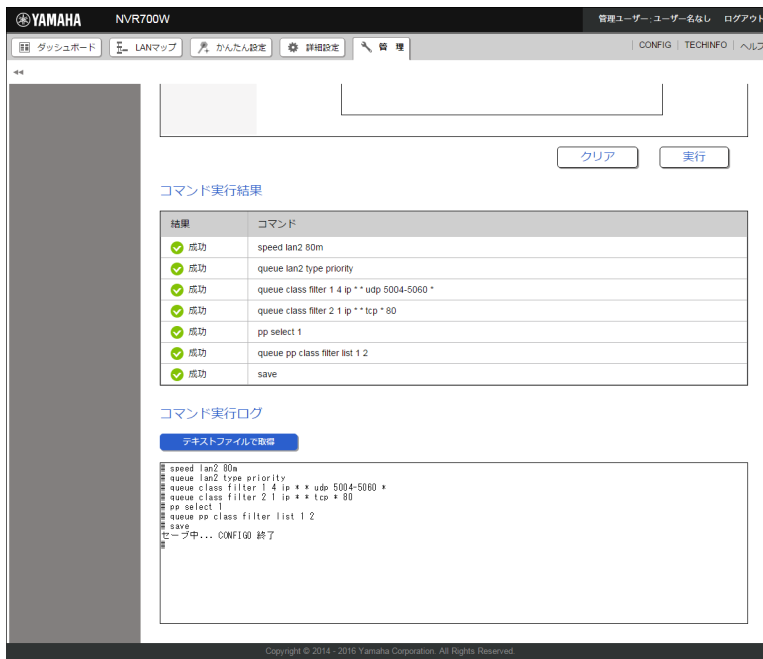
#### コマンドの入力例

```
speed lan2 80m
queue lan2 type priority
queue class filter 1 4 ip * * udp 5004-5060 *
queue class filter 2 1 ip * * tcp * 80
pp select 1
queue pp class filter list 1 2
```

#### メモ

改行で区切ることによって、複数のコマンドをまとめて入力することができます。

3. 「実行」 ボタンをクリックする。  
 コマンドの実行結果が表示されます。



## メモ

設定系コマンドを実行すると自動的に save コマンドも実行され、設定が自動的に保存されます。

次に、以下の表示系コマンドの実行例を示します。

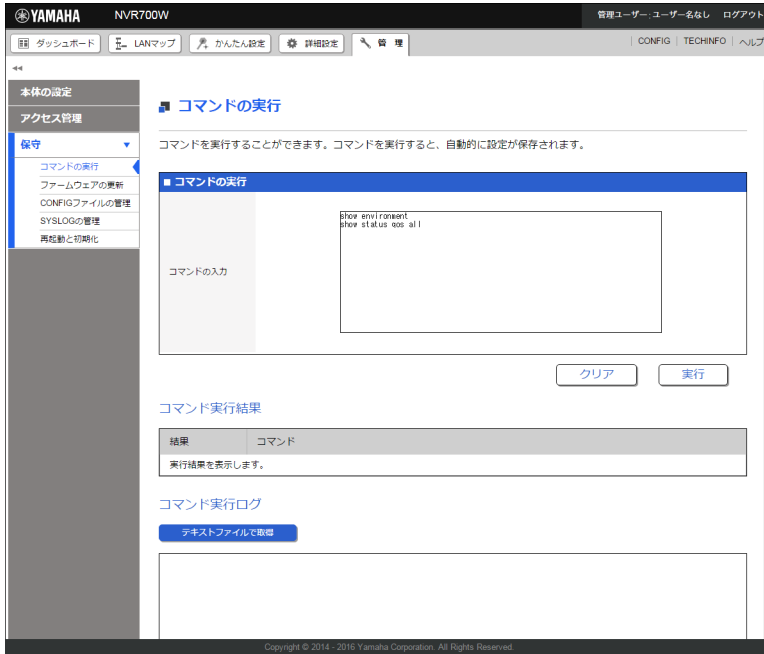
## 表示系コマンドの例

機器状態の表示 : show environment

QoS ステータスの表示 : show status qos all

## 第 14 章 ヤマハルーターを管理する

### 1. 「コマンドの実行」項目にコマンドを入力する。

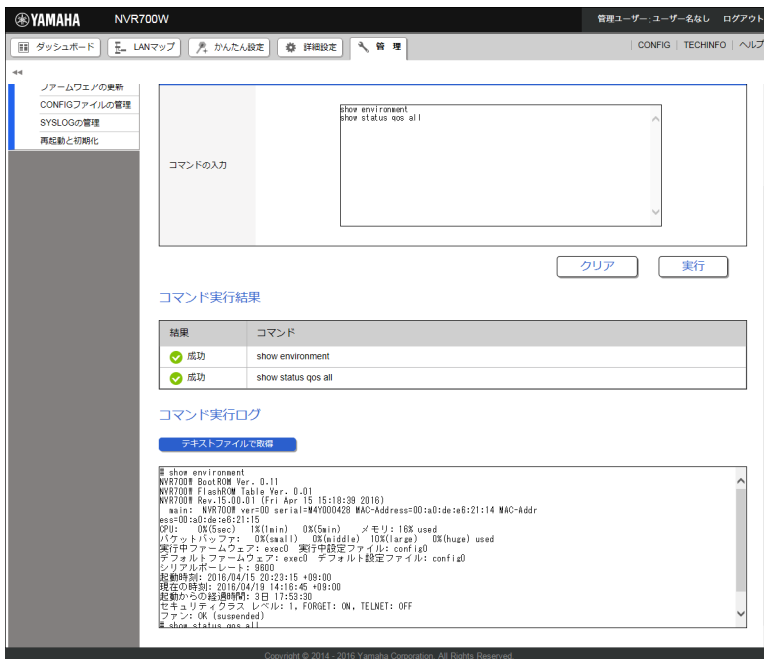


#### コマンドの入力例

```
show environment
show status qos all
```

### 2. 「実行」ボタンをクリックする。

コマンドの実行結果が表示されます。





## メモ

「テキストファイルで取得」ボタンをクリックすると、コマンドの実行結果をテキストファイルで取得することができます。取得したテキストファイルは UTF-8 でエンコードされています。

## 14.4 ファームウェアを更新する

ヤマハルーターのファームウェアを更新する方法について説明します。

### ご注意

使用中のファームウェアを更新する場合は、ファームウェアの更新が正常に完了すると自動的にヤマハルーターが再起動します。ヤマハルーターが再起動するまで他の操作は絶対に行わないでください。

### 14.4.1 外部メモリを使用してファームウェアを更新する

市販の外部メモリ（USB メモリ / microSD カード）に保存したファームウェアをヤマハルーターに読み込ませてファームウェアの更新を行います。

### ご注意

- ・ FAT または FAT32 形式でフォーマットされていない外部メモリは、ヤマハルーターで使用できません。
- ・ USB ハブを介して、複数の USB メモリなどの外部メモリをヤマハルーターに接続することはできません。
- ・ USB 延長ケーブルを介して接続した場合は、正常に動作しないことがあります。USB メモリはヤマハルーターの USB ポートに直接挿入してご使用ください。
- ・ ヤマハルーターの USB ランプまたは microSD ランプが点灯 / 点滅している間は、外部メモリを取り外さないでください。外部メモリ内のデータを破損することがあります。USB ボタンまたは microSD ボタンを 2 秒以上押し続けるとブザーが鳴り、USB ランプまたは microSD ランプが消灯し、外部メモリを取り外すことができるようになります。外部メモリを取り外す際は、USB ランプまたは microSD ランプが消灯していることを確認してから外部メモリを取り外してください。

#### 1. ファームウェアを保存した外部メモリを用意する。

ファームウェアはヤマハネットワーク周辺機器技術情報ページから入手できます。

<http://www.rtpro.yamaha.co.jp/>

#### 2. 外部メモリをヤマハルーターの USB ポートまたは microSD スロットに差し込む。

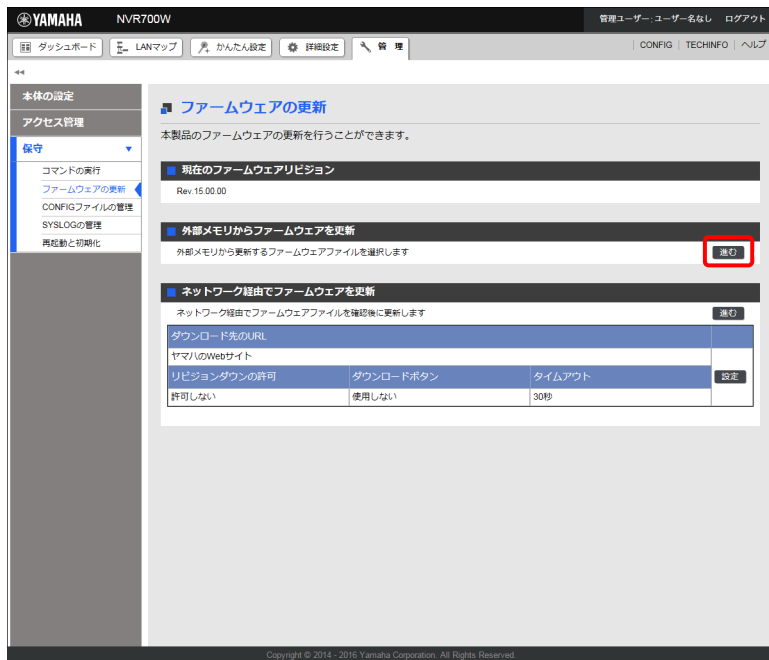
外部メモリを認識するとブザーが鳴り、ヤマハルーターの USB ランプまたは microSD ランプが点灯します。

#### 3. 「管理」タブ - 「保守」 - 「ファームウェアの更新」を順に選択する。

「ファームウェアの更新」画面が表示されます。

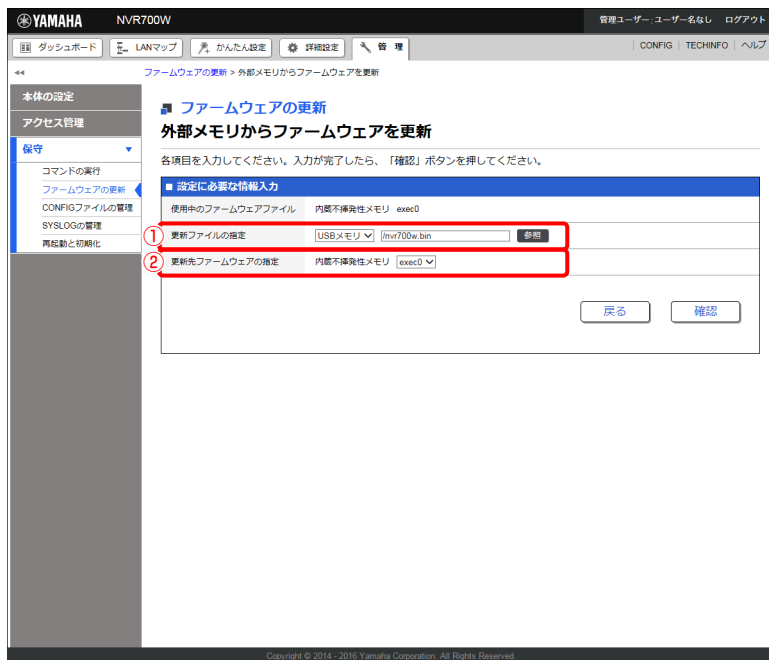
## 第 14 章 ヤマハルーターを管理する

### 4. 「外部メモリからファームウェアを更新」項目の「進む」ボタンをクリックする。



「外部メモリからファームウェアを更新」画面が表示されます。

### 5. 外部メモリから読み込みたいファームウェアを指定する。



#### ① 更新ファイルの指定：

差し込んだ外部メモリを選択し、「参照」ボタンをクリックします。「ファイルの一覧」画面で保存したファームウェアを選択します。

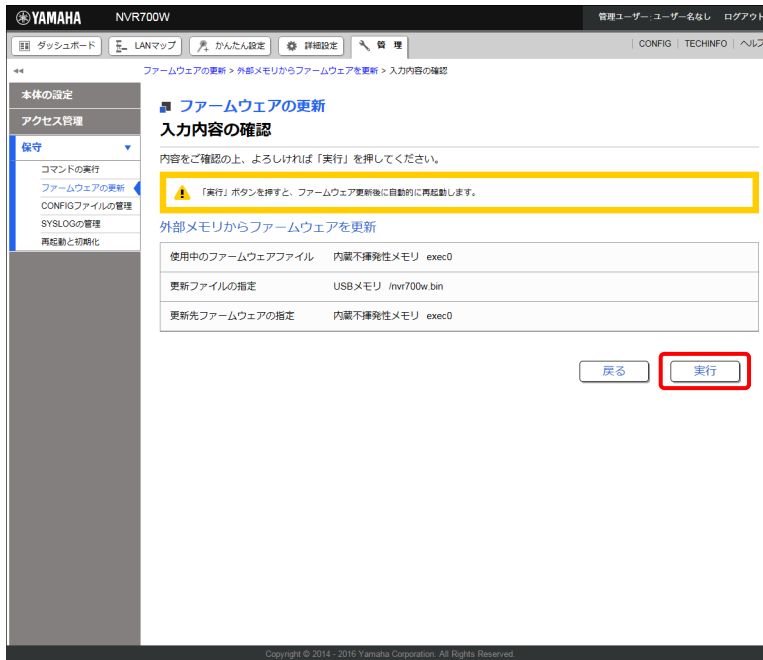
#### ② 更新先ファームウェアの指定：

更新先の内蔵不揮発性メモリのファームウェア番号を選択します。

## メモ

更新先ファームウェアの指定が使用中のファームウェアと同じ場合は、ファームウェアの更新の完了後にヤマハルーターが再起動します。また、指定が異なる場合は、再起動は行われず使用中のファームウェアも変化しません。

6. 「確認」 ボタンをクリックする。  
「入力内容の確認」画面が表示されます。
7. 内容を確認し、「実行」 ボタンをクリックする。



「ファームウェアの更新」ダイアログが表示され、ファームウェアの更新が開始されます。ファームウェアの更新が完了すると、ヤマハルーターは自動的に再起動します。

## ご注意

使用中のファームウェアと更新先ファームウェアの指定が異なる場合は、再起動は行われず、使用中のファームウェアも変化しません。手順 8 以降は、使用中のファームウェアと更新先ファームウェアの指定が同じ場合に行ってください。

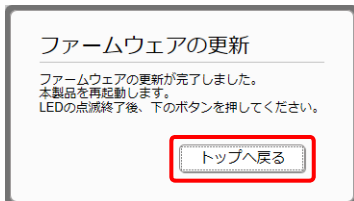
8. ヤマハルーターの再起動中に、外部メモリを取り外す。

## ご注意

ヤマハルーターのランプが全点灯している間に外部メモリを取り外してください。その際に USB ボタン /microSD ボタンを押す必要はありません。外部メモリを取り外さなかった場合、外部メモリ内にファームウェアまたは CONFIG ファイルが存在すると、その外部メモリ内のファイルを使用して起動します。

## 第 14 章 ヤマハルーターを管理する

9. ヤマハルーターの再起動が完了後、「トップへ戻る」ボタンをクリックする。



ダッシュボードページが表示されます。

### ご注意

再起動中は Web GUI を開いているパソコンがヤマハルーターと通信できない状態 (パソコンのネットワークアダプタの状態表示で「ネットワークケーブルが接続されていない」と表示されます) になりますが、再起動が完了すると通信状態が復旧します。ヤマハルーターのランプの点滅終了後に、Web GUI を開いているパソコンの通信状態が復旧していることを確認してから「トップへ戻る」をクリックしてください。

### 14.4.2 ヤマハの Web サイトからネットワーク経由でファームウェアを更新する

ヤマハの公式 Web サイト上に置かれたファームウェアファイルをダウンロードしてファームウェアの更新を行います。

### メモ

ヤマハの公式 Web サイトで公開されている NVR700W/NVR510 のファームウェアファイルの URL はそれぞれ以下になります。

NVR700W の場合：

<http://www.rtpro.yamaha.co.jp/firmware/revision-up/nvr700w.bin>

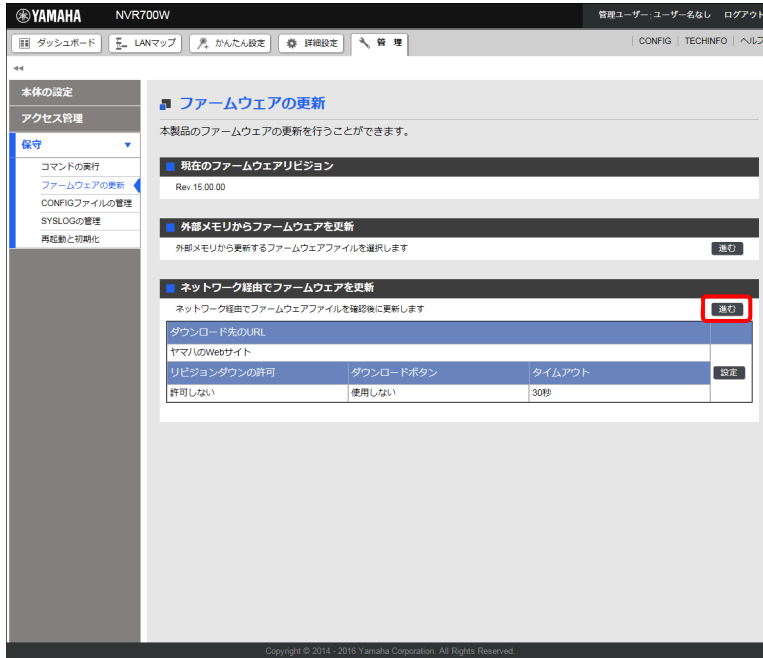
NVR510 の場合：

<http://www.rtpro.yamaha.co.jp/firmware/revision-up/nvr510.bin>

上記 URL は Web ブラウザーからアクセスすることはできません。

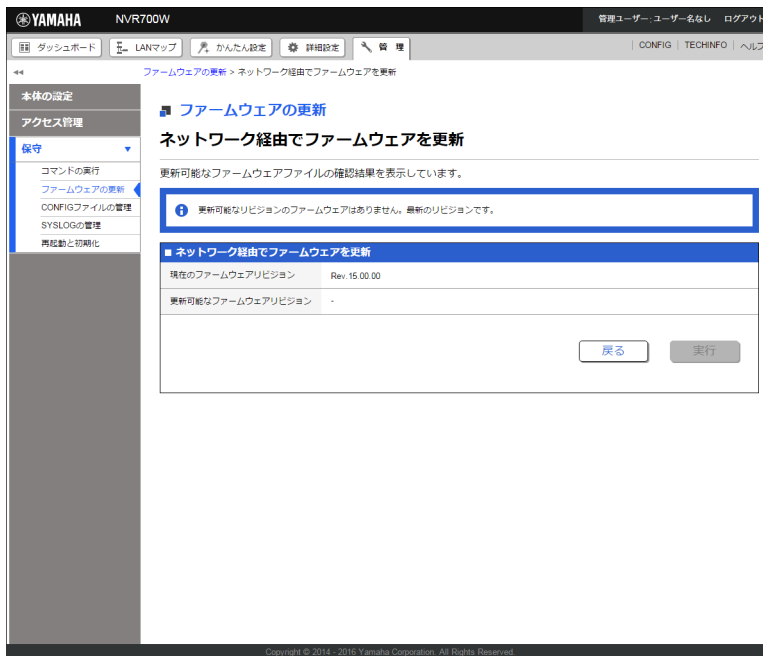
1. 「管理」タブ - 「保守」 - 「ファームウェアの更新」を順に選択する。  
「ファームウェアの更新」画面が表示されます。

## 2. 「ネットワーク経由でファームウェアを更新」項目の「進む」ボタンをクリックする。



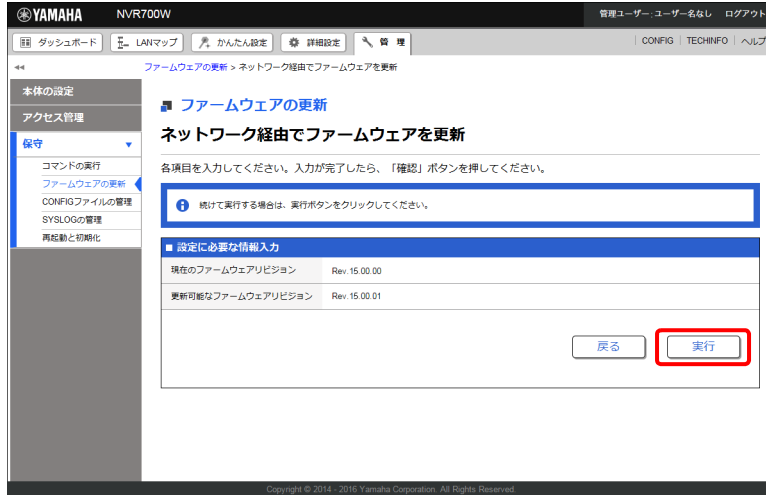
更新可能なファームウェアの確認が行われ、「ネットワーク経由でファームウェアを更新」画面が表示されま

す。最新のファームウェアを使用している場合は以下のような画面が表示されます。この場合はファームウェアを更新する必要はありません。



## 第 14 章 ヤマハルーターを管理する

### 3. 内容を確認し、「実行」ボタンをクリックする。



「ソフトウェアライセンス契約」画面が表示されます。

## 4. ソフトウェアライセンス契約の内容をよく確認し、「同意する」ボタンをクリックする。

YAMAHA NVR7000 管理ユーザー:ユーザー名なし ログアウト

ホーム ダッシュボード LANマップ かんたん設定 詳細設定 管理

CONFIG TECHINFO ヘルプ

ファームウェアの更新 > ネットワーク経由でファームウェアを更新 > ソフトウェアライセンス契約

本体の設定

アクセス管理

保守

コマンドの実行

ファームウェアの更新

CONFIGファイルの管理

SYSLLOGの管理

再起動と初期化

### ファームウェアの更新

#### ソフトウェアライセンス契約

以下に表示されているソフトウェアライセンス契約(以下、「本契約」といいます)の内容をお読みいただき、内容に御同意いただける場合には、「同意する」のボタンをクリックしてください。ファームウェアのダウンロードを開始します。内容に御同意いただけない場合には、「同意しない」のボタンをクリックしてください。ファームウェアの更新手順を中止します。

#### ソフトウェアライセンス契約

本契約は、お客様とヤマハ株式会社(以下、「ヤマハ」といいます)との間の契約であり、ヤマハルーター製品・サーバー製品(以下、「本製品」といいます)を用いてファームウェアおよびこれに関わるプログラム、印刷物、電子ファイル(以下、「本ソフトウェア」といいます)をヤマハがお客様に提供するにあたっての条件を規定するものです。

「本ソフトウェア」は、「本製品」で動作させる目的においてのみ使用することができます。本契約は、ヤマハがお客様に提供した「本ソフトウェア」および附属品1(家賃)1項の定めに従ってお客様が作成した「本ソフトウェア」の複製物に適用されます。

- 使用許諾**

(1) お客様は、「本ソフトウェア」をお客様が所有する「本製品」またはパーソナルコンピュータ等のデバイスにインストールして使用することができます。

(2) お客様は、本契約に明示的に定められる場合を除き、「本ソフトウェア」を、再使用許諾、販売、頒布、賃貸、リース、貸与もしくは譲渡し、特定もしくは不特定多数の者によるアクセスが可能なウェブ・サイトもしくはサーバー等にアップロードし、または、複製、翻訳、転載もしくは他のプログラム言語に書き換えしてはなりません。お客様はまた、「本ソフトウェア」の全部または一部を修正、改変、逆アセンブル、逆コンパイル、その他リバース・エンジニアリング等してはならず、また第三者にこのような行為をさせてはなりません。

(3) お客様は、「本ソフトウェア」に含まれるヤマハの著作権表示を複製、除去、または削除してはなりません。

(4) 本契約に明示的に定められる場合を除き、ヤマハは、「本ソフトウェア」に関するヤマハの知的財産権のいかなる権利もお客様に付与または許諾するものではありません。
- 所有権**

「本ソフトウェア」は、著作権法その他の法律により保護され、ヤマハにより所有されています。お客様は、ヤマハが、本契約に基づきまたはその他の手段により「本ソフトウェア」に係る所有権および知的財産権をお客様に譲渡するものはないことを、ここに同意するものとします。
- 輸出規制**

お客様は、当該国のすべての適用可能な輸出管理法規に準ずるものとし、また、かかる法規や規制に違反して「本ソフトウェア」の全部または一部を、いかなる国へ譲渡もしくは複製に輸出もしくは再輸出してはなりません。
- サポートおよびアップデート**

ヤマハ、ヤマハの子会社、それらの販売代理店および販売店、並びに、その他「本ソフトウェア」の取次者および頒布者は、「本ソフトウェア」のメンテナンスおよびお客様による「本ソフトウェア」の使用を支援することについて、いかなる責任を負うものでもありません。また、本契約に基づき「本ソフトウェア」に対してアップデート、パッチの修正あるいはサポートを行う義務もありません。
- 責任の制限**

(1) 「本ソフトウェア」は、「現状のまま(AS-IS)」の状態で使用許諾されます。ヤマハ、ヤマハの子会社、それらの販売代理店および販売店、並びに、その他「本ソフトウェア」の取次者および頒布者は、「本ソフトウェア」に関して、高度性及び特定の目的への適合性の保証を、いかなる保証も、明示したと認めたことと認む者一切しないものとします。

(2) ヤマハ、ヤマハの子会社、それらの販売代理店および販売店、並びに、その他「本ソフトウェア」の取次者および頒布者は、「本ソフトウェア」の使用または使用不能から生ずるいかなる損害(逸失利益およびその他の潜在的または付随的な損害を含む)がこれらに限定されないことについて、一切責任を負わないものとします。たとえ、ヤマハ、ヤマハの子会社、それらの販売代理店および販売店、並びに、その他「本ソフトウェア」の取次者および頒布者がかかる損害の可能性について知られていた場合でも同様です。

(3) ヤマハ、ヤマハの子会社、それらの販売代理店および販売店、並びに、その他「本ソフトウェア」の取次者および頒布者は、「本ソフトウェア」の使用に起因した賠償または賠償としてお客様と第三者との間に生じるいかなる紛争についても、一切責任を負わないものとします。
- 有効期間**

(1) 本契約は、下記(2)または(3)により終了されるまで有効に存続します。

(2) お客様は、「本製品」にインストール済みのすべての「本ソフトウェア」を消去することにより、本契約を終了させることができます。

(3) お客様が本契約のいずれかの条項に違反した場合、本契約は直ちに終了します。

(4) お客様は、上記(3)による本契約の終了後直ちに、「本製品」にインストール済みのすべての「本ソフトウェア」を消去するものとします。

(5) 本契約のいかなる条項にかかわらず、本契約第2条から第6条の規定は本契約の終了後も効力を有するものとします。
- 分離可能性**

本契約のいかなる条項が無効となった場合でも、本契約のそれ以外の部分は効力を有するものとします。
- U.S. GOVERNMENT RESTRICTED RIGHTS NOTICE**

The Software is a "commercial item," as that term is defined at 48 C.F.R. 2.101 (Oct 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users shall acquire the Software with only those rights set forth herein.
- 一般条項**

お客様は、本契約が本契約に規定されるすべての事項についての、お客様とヤマハとの間の完全かつ唯一の合意の声明であり、口頭あるいは書面による、すべての交渉、従前の契約またはその他のお客様とヤマハとのあらゆるコミュニケーションに優先するものであることに同意するものとします。本契約のいかなる修正も、ヤマハが正当に授權した代表者による署名がなければ効力を有しないものとします。
- 準拠法**

本契約は、日本の法に準拠し、これにもとじて解釈されるものとします。

同意しない

Copyright © 2014 - 2016 Yamaha Corporation. All Rights Reserved.

「ファームウェアの更新」ダイアログが表示され、ファームウェアの更新が開始されます。ファームウェアの更新が完了すると、ヤマハルーターは自動的に再起動します。

## 5. ヤマハルーターの再起動が完了後、「トップへ戻る」ボタンをクリックする。

ファームウェアの更新

ファームウェアの更新が完了しました。  
本製品を再起動します。  
LEDの点滅終了後、下のボタンを押してください。

ダッシュボードページが表示されます。

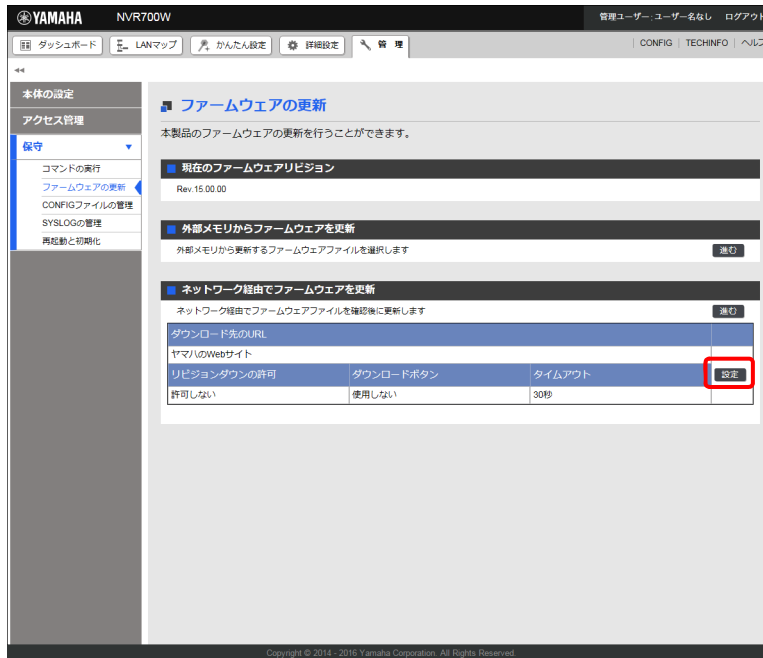
### ご注意

再起動中は Web GUI を開いているパソコンがヤマハルーターと通信できない状態（パソコンのネットワークアダプタの状態表示で「ネットワークケーブルが接続されていない」と表示されます）になりますが、再起動が完了すると通信状態が復旧します。ヤマハルーターのランプの点滅終了後に、Web GUI を開いているパソコンの通信状態が復旧していることを確認してから「トップへ戻る」をクリックしてください。

### 14.4.3 社内サーバーからネットワーク経由でファームウェアを更新する

社内サーバー上に置かれたファームウェアファイルをダウンロードしてファームウェアの更新を行います。

1. 「管理」タブ - 「保守」 - 「ファームウェアの更新」を順に選択する。  
「ファームウェアの更新」画面が表示されます。
2. 「ネットワーク経由でファームウェアを更新」項目の「設定」ボタンをクリックする。



「ファームウェア更新の基本設定」画面が表示されます。



## 3. ファームウェア更新の基本設定を行う。

The screenshot shows the 'ファームウェア更新の基本設定' (Firmware Update Basic Settings) page in the Yamaha NVR700W Web GUI. The page title is 'ファームウェア更新の基本設定'. Below the title, there is a section '設定に必要な情報入力' (Input information required for settings). The form contains the following items:

- ① **ダウンロード先のURL**: A radio button for 'ヤマハのWebサイト' (Yamaha website) is selected. Below it, a text input field contains 'http://www.example.net/yamaha/nvr700w.bin'.
- ② **リビジョンダウンの許可**: A radio button for '許可しない' (Do not allow) is selected.
- ③ **ダウンロードボタンの使用**: A radio button for '使用しない' (Do not use) is selected.
- ④ **タイムアウト**: A text input field contains '30' minutes, with a note '(1~180)'.

At the bottom of the form, there are two buttons: '戻る' (Back) and '確認' (Confirm).

## ① ダウンロード先のURL：

ファームウェアの置かれている URL を設定します。社内サーバーからダウンロードする場合は、「その他」を選択し社内サーバーの URL を入力します。

## ② リビジョンダウンの許可：

古いバージョンのファームウェアへの書き換えを許可するか否かを設定します。

## ③ ダウンロードボタンの使用：

ヤマハルーター本体の DOWNLOAD ボタンの使用を許可するか否かを設定します。

## メモ

ヤマハルーターは DOWNLOAD ボタンを使用してファームウェアの更新を行うこともできます。DOWNLOAD ボタンを使用してファームウェアを更新する場合も、本画面で設定した URL からファームウェアをダウンロードします。DOWNLOAD ボタンを用いた更新方法について詳しくは、「操作マニュアル」（製品付属の CD-ROM に収録）をご覧ください。

## ④ タイムアウト：

ネットワーク経由でファームウェアを更新する処理のタイムアウト時間を入力します。

## 4. 「確認」 ボタンをクリックする。

「入力内容の確認」画面が表示されます。

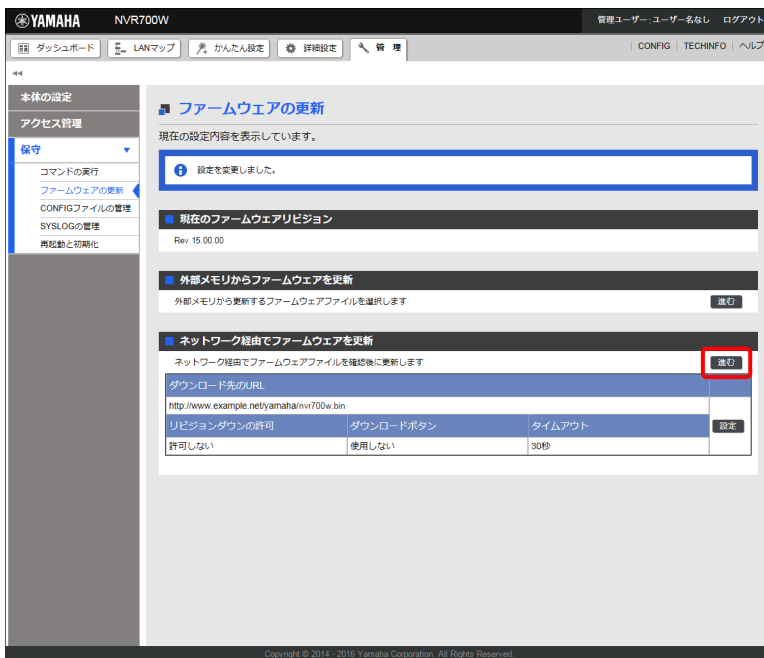
## 第 14 章 ヤマハルーターを管理する

### 5. 内容を確認し、「設定の確定」ボタンをクリックする。



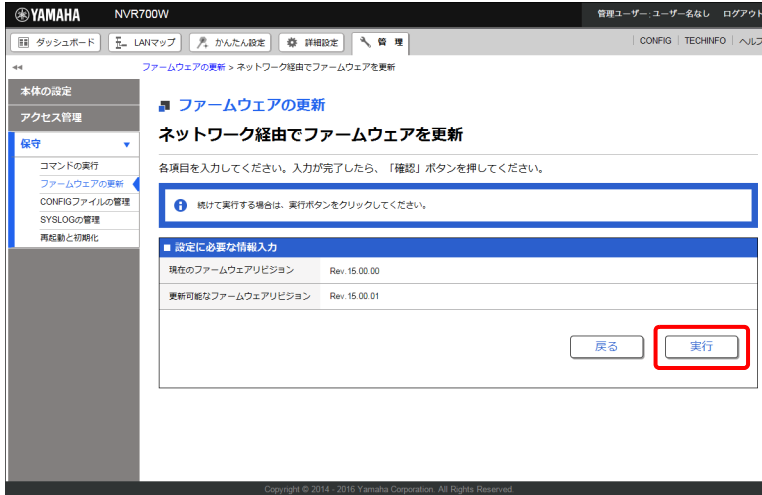
設定が反映され、「ファームウェアの更新」画面が表示されます。

### 6. 「ネットワーク経由でファームウェアを更新」項目の「進む」ボタンをクリックする。



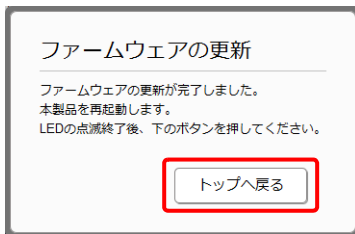
更新可能なファームウェアの確認が行われ、「ネットワーク経由でファームウェアを更新」画面が表示されます。

## 7. 内容を確認し、「実行」ボタンをクリックする。



「ファームウェアの更新」ダイアログが表示され、ファームウェアの更新が開始されます。ファームウェアの更新が完了すると、ヤマハルーターは自動的に再起動します。

## 8. ヤマハルーターの再起動が完了後、「トップへ戻る」ボタンをクリックする。



ダッシュボードページが表示されます。

## ご注意

再起動中は Web GUI を開いているパソコンがヤマハルーターと通信できない状態 (パソコンのネットワークアダプタの状態表示で「ネットワークケーブルが接続されていない」と表示されます) になりますが、再起動が完了すると通信状態が復旧します。ヤマハルーターのランプの点滅終了後に、Web GUI を開いているパソコンの通信状態が復旧していることを確認してから「トップへ戻る」をクリックしてください。

## 14.5 設定 (CONFIG) を管理する

設定 (CONFIG) を外部メモリへエクスポートしたり、外部メモリからインポートすることができます。ヤマハルーターは CONFIG に従って動作しています。CONFIG は複数のコマンドで構成されており、Web GUI から設定した内容もすべてコマンド形式で CONFIG に保存されます。

## ご注意

- ・ FAT または FAT32 形式でフォーマットされていない外部メモリは、ヤマハルーターで使用できません。
- ・ USB ハブを介して、複数の USB メモリなどの外部メモリをヤマハルーターに接続することはできません。

## 第 14 章 ヤマハルーターを管理する

- ・ USB 延長ケーブルを介して接続した場合は、正常に動作しないことがあります。USB メモリはヤマハルーターの USB ポートに直接挿入してご使用ください。
- ・ ヤマハルーターの USB ランプまたは microSD ランプが点灯 / 点滅している間は、外部メモリを取り外さないでください。外部メモリ内のデータを破損することがあります。USB ボタンまたは microSD ボタンを 2 秒以上押し続けるとブザーが鳴り、USB ランプまたは microSD ランプが消灯し、外部メモリを取り外すことができますようになります。外部メモリを取り外す際は、USB ランプまたは microSD ランプが消灯していることを確認してから外部メモリを取り外してください。

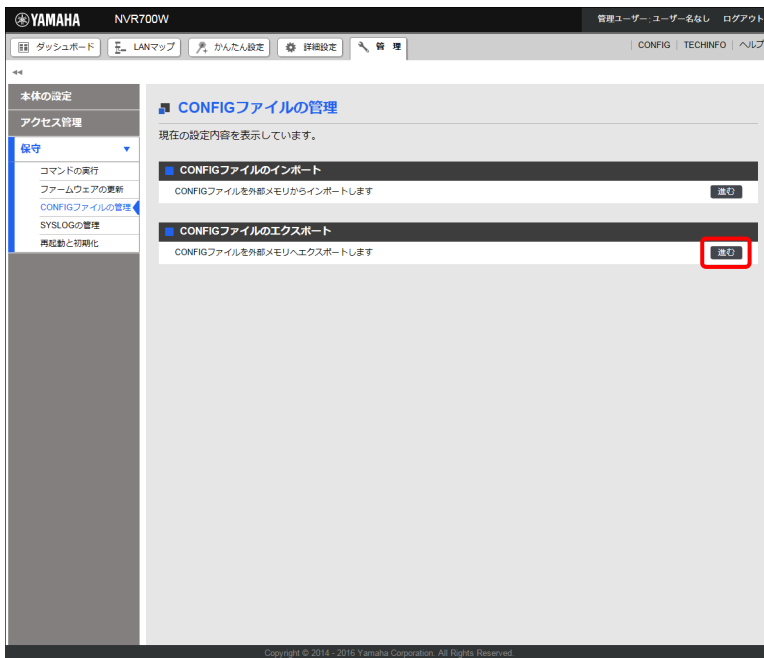
### メモ

コマンド仕様について詳しくは、「コマンドリファレンス」（製品付属の CD-ROM に収録）をご覧ください。

### 14.5.1 設定 (CONFIG) を外部メモリにエクスポートする

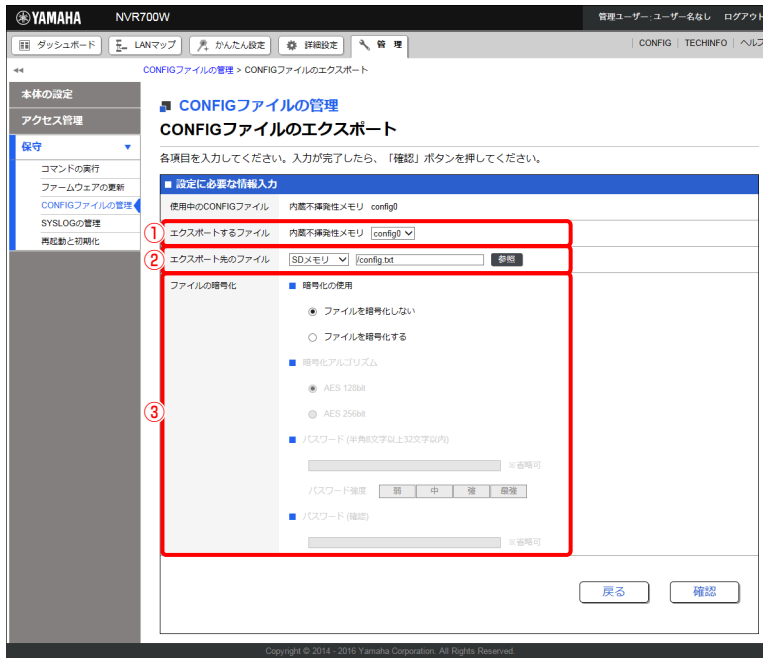
ヤマハルーター内に保存されている設定 (CONFIG) を外部メモリにエクスポートします。

1. 外部メモリをヤマハルーターの USB ポートまたは microSD スロットに差し込む。  
外部メモリを認識するとブザーが鳴り、ヤマハルーターの USB ランプまたは microSD ランプが点灯します。
2. 「管理」タブ - 「保守」 - 「CONFIG ファイルの管理」を順に選択する。  
「CONFIG ファイルの管理」画面が表示されます。
3. 「CONFIG ファイルのエクスポート」項目の「進む」ボタンをクリックする。



「CONFIG ファイルのエクスポート」画面が表示されます。

## 4. 設定 (CONFIG) ファイルのエクスポート方法を設定する。



## ① エクスポートするファイル：

エクスポートしたい内蔵不揮発性メモリの CONFIG 番号を選択します。

## ② エクスポート先のファイル：

差し込んだ外部メモリを選択し、エクスポート先のファイル名を入力します。

## ③ ファイルの暗号化：

エクスポートする際に CONFIG ファイルを暗号化するか否かを選択します。「ファイルを暗号化する」を選択した場合は、暗号化アルゴリズムを選択し、暗号化パスワードを入力します。パスワードを入力せずに暗号化することも可能です。暗号化パスワードを設定した場合は、CONFIG ファイルのインポート時に同じパスワードを入力して復号する必要があるため、パスワードは忘れないでください。

## 5. 「確認」 ボタンをクリックする。

「入力内容の確認」画面が表示されます。

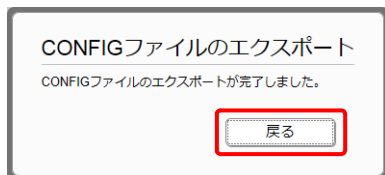
## 第 14 章 ヤマハルーターを管理する

### 6. 内容を確認し、「実行」ボタンをクリックする。



「CONFIG ファイルのエクスポート」ダイアログが表示され、外部メモリに CONFIG ファイルがエクスポートされます。

### 7. 「CONFIG ファイルのエクスポートが完了しました。」というメッセージが表示されたら、「戻る」ボタンをクリックする。



「CONFIG ファイルの管理」画面が表示されます。

## メモ

外部メモリに CONFIG ファイルが、正しくエクスポートされていることを確認してください。

### 14.5.2 設定 (CONFIG) を外部メモリからインポートする

外部メモリに保存されている設定 (CONFIG) をインポートし、ヤマハルーターの設定 (CONFIG) を更新します。

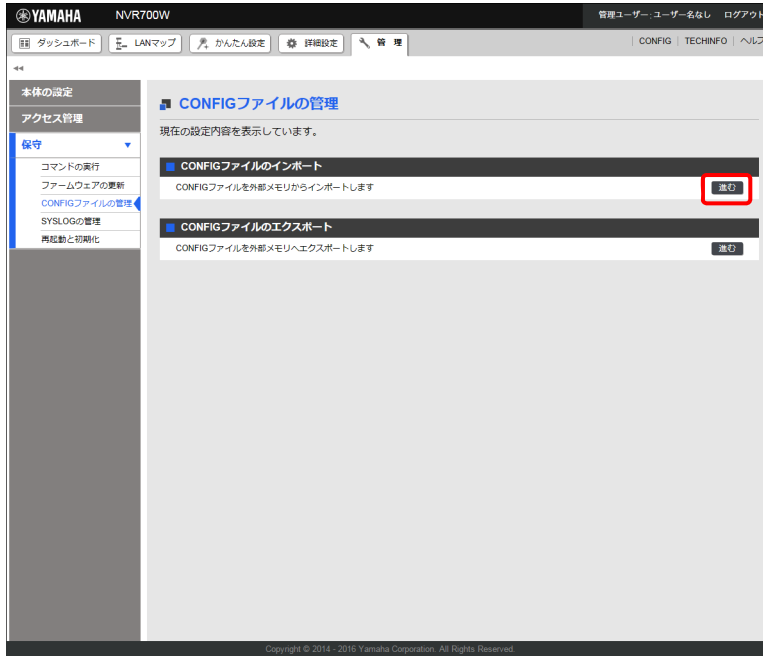
## ご注意

使用中の設定 (CONFIG) を更新する場合は、設定 (CONFIG) の更新が正常に完了すると自動的にヤマハルーターが再起動します。ヤマハルーターが再起動するまで他の操作は絶対に行わないでください。

1. CONFIG ファイルが保存されている外部メモリを用意する。
2. 外部メモリをヤマハルーターの USB ポートまたは microSD スロットに差し込む。

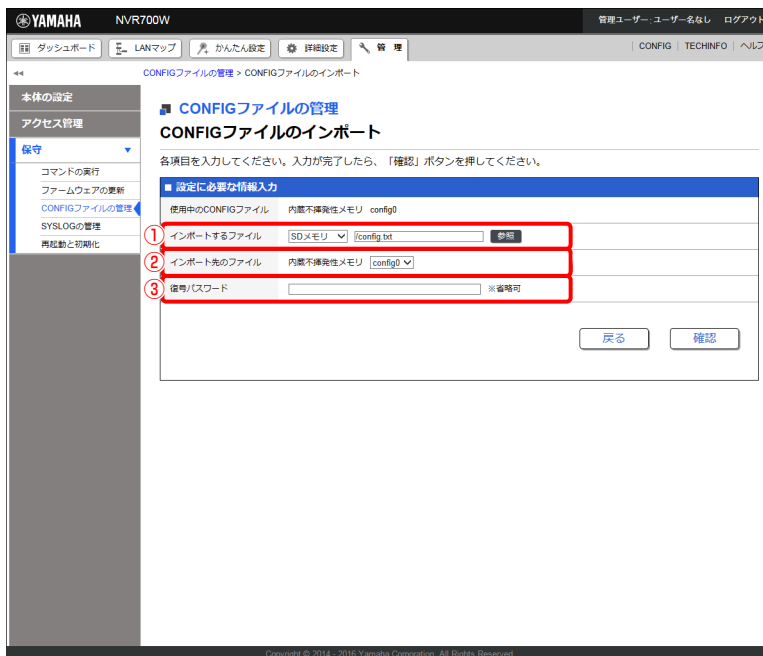
外部メモリを認識するとブザーが鳴り、ヤマハルーターの USB ランプまたは microSD ランプが点灯します。

3. 「管理」タブ - 「保守」 - 「CONFIG ファイルの管理」を順に選択する。  
「CONFIG ファイルの管理」画面が表示されます。
4. 「CONFIG ファイルのインポート」項目の「進む」ボタンをクリックする。



「CONFIG ファイルのインポート」画面が表示されます。

5. 設定 (CONFIG) ファイルのインポート方法を設定する。



## 第 14 章 ヤマハルーターを管理する

### ① インポートするファイル：

差し込んだ外部メモリを選択し、「参照」ボタンをクリックします。「ファイルの一覧」画面でインポートしたい CONFIG ファイルを選択します。

### ② インポート先のファイル：

インポート先の内蔵不揮発性メモリの CONFIG 番号を選択します。

## メモ

インポート先の CONFIG ファイルの指定が使用中の CONFIG ファイルと同じ場合は、インポートの完了後にヤマハルーターが再起動します。また、指定が異なる場合は、再起動は行われず使用中の CONFIG ファイルも変化しません。

### ③ 復号パスワード：

暗号化されている CONFIG ファイルをインポートする場合は、エクスポートする際に設定した暗号化パスワードを入力します。

## 6. 「確認」ボタンをクリックする。

「入力内容の確認」画面が表示されます。

## 7. 内容を確認し、「実行」ボタンをクリックする。



「CONFIG ファイルのインポート」ダイアログが表示され、設定 (CONFIG) ファイルがインポートされます。設定 (CONFIG) ファイルのインポートが完了すると、ヤマハルーターは自動的に再起動します。

## ご注意

使用中の CONFIG ファイルとインポート先の CONFIG ファイルの指定が異なる場合は、再起動は行われず、使用中の CONFIG も変化しません。手順 8 以降は、使用中の CONFIG ファイルとインポート先の CONFIG ファイルの指定が同じ場合に行ってください。

## 8. ヤマハルーターの再起動中に、外部メモリを取り外す。



**ご注意**

ヤマハルーターのランプが全点灯している間に外部メモリを取り外してください。その際に USB ボタン / microSD ボタンを押す必要はありません。  
外部メモリを取り外さなかった場合、外部メモリ内にファームウェアまたは CONFIG ファイルが存在すると、その外部メモリ内のファイルを使用して起動します。

9. ヤマハルーターの再起動が完了後、「トップへ戻る」ボタンをクリックする。



ダッシュボードページが表示されます。

**ご注意**

再起動中は Web GUI を開いているパソコンがヤマハルーターと通信できない状態 (パソコンのネットワークアダプタの状態表示で「ネットワークケーブルが接続されていない」と表示されます) になりますが、再起動が完了すると通信状態が復旧します。ヤマハルーターのランプの点滅終了後に、Web GUI を開いているパソコンの通信状態が復旧していることを確認してから「トップへ戻る」をクリックしてください。

## 14.6 SYSLOG を管理する

SYSLOG 機能の設定を行います。ヤマハルーターの動作履歴はログファイル (SYSLOG) に保存されています。SYSLOG はルーター内部に保存されるだけでなく、指定のサーバー (SYSLOG ホスト) へ送信することもできます。

**メモ**

SYSLOG でヤマハルーターの動作履歴を確認することで、ネットワーク障害を解決するヒントが得られる場合があります。

### 14.6.1 SYSLOG に出力する種別を変更する

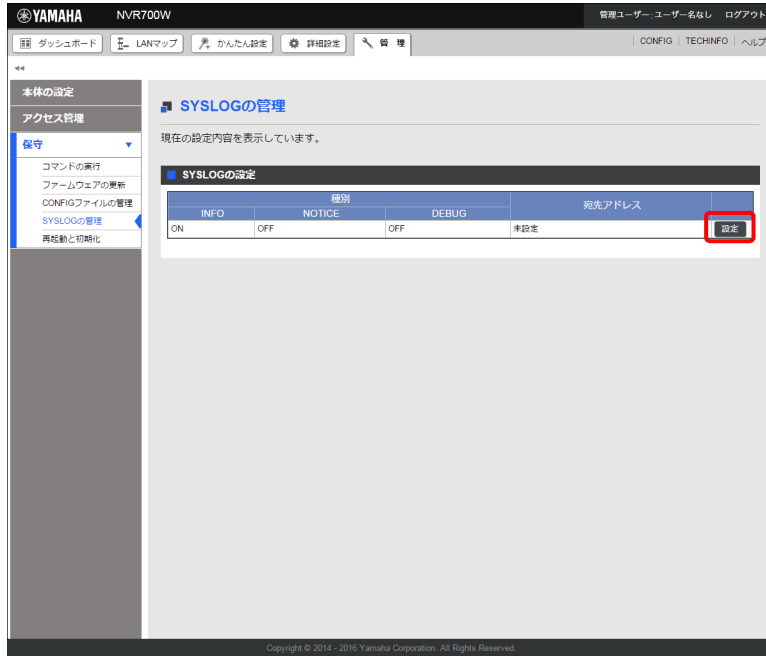
SYSLOG に出力する種別 (INFO / NOTICE / DEBUG) を変更します。

INFO : ヤマハルーターの動作状況に関する情報が出力されます。  
NOTICE : 各種フィルター機能などで検出したパケット情報が出力されます。  
DEBUG : デバッグ用の情報が出力されます。

1. 「管理」タブ - 「保守」 - 「SYSLOG の管理」を順に選択する。  
「SYSLOG の管理」画面が表示されます。

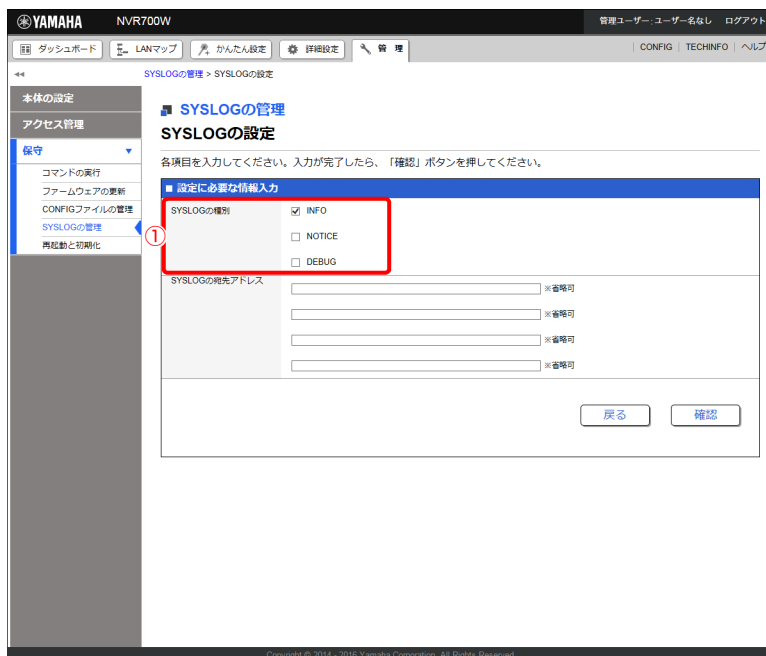
## 第 14 章 ヤマハルーターを管理する

### 2. 「SYSLOG の設定」項目の「設定」ボタンをクリックする。



「SYSLOG の設定」画面が表示されます。

### 3. SYSLOG に出力する種別を設定する。

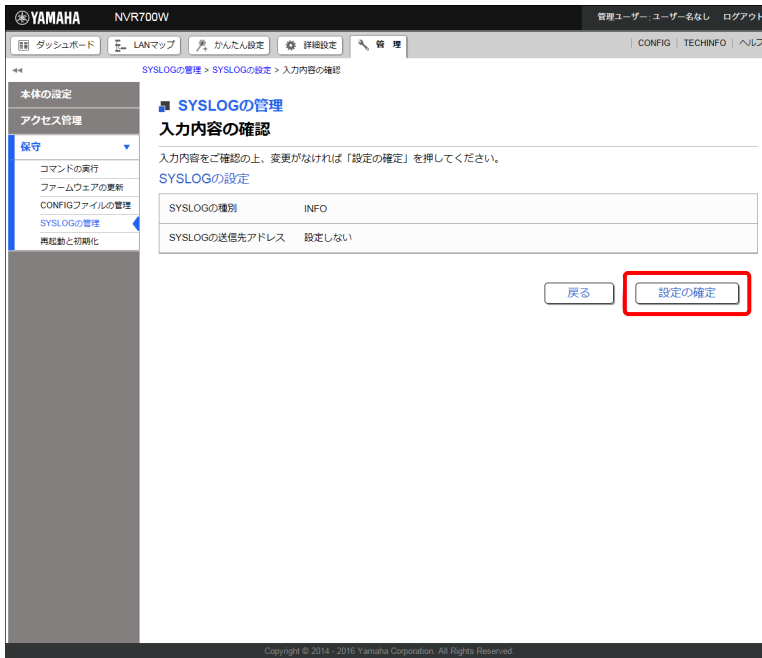


#### ① SYSLOG の種別：

SYSLOG に出力したい種別のチェックボックスにチェックを入れます。

- ・ INFO：ヤマハルーターの動作状況に関する情報を出力したい場合にチェックを入れます。
- ・ NOTICE：各種フィルター機能などで検出したパケット情報を出力したい場合にチェックを入れます。
- ・ DEBUG：デバッグ用の情報を出力したい場合にチェックを入れます。

4. 「確認」 ボタンをクリックする。  
「入力内容の確認」 画面が表示されます。
5. 内容を確認し、「設定の確定」 ボタンをクリックする。



設定が反映され、「SYSLOG の管理」画面が表示されます。

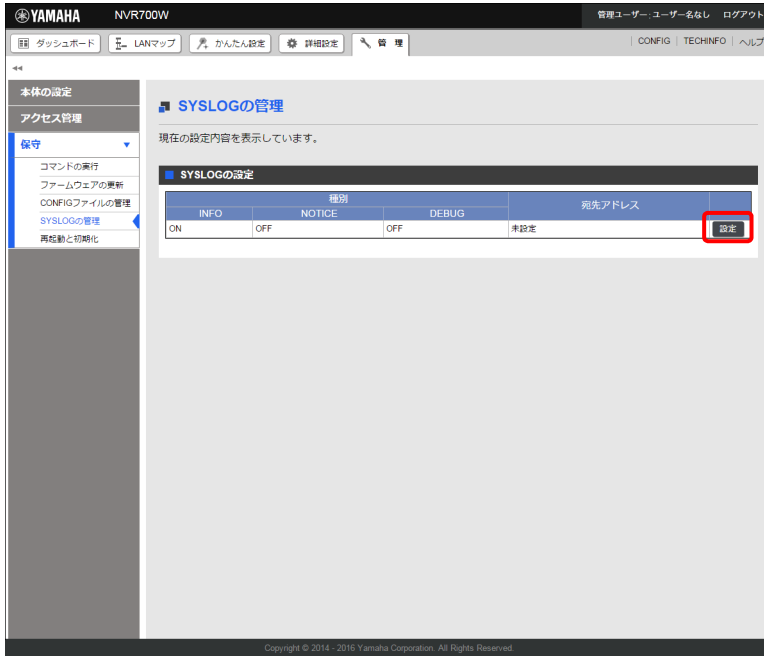
### 14.6.2 SYSLOG をサーバーへ送信する

SYSLOG を SYSLOG ホストに送信する場合に、宛先の SYSLOG ホストの IP アドレスを設定します。

1. 「管理」タブ - 「保守」 - 「SYSLOG の管理」を順に選択する。  
「SYSLOG の管理」画面が表示されます。

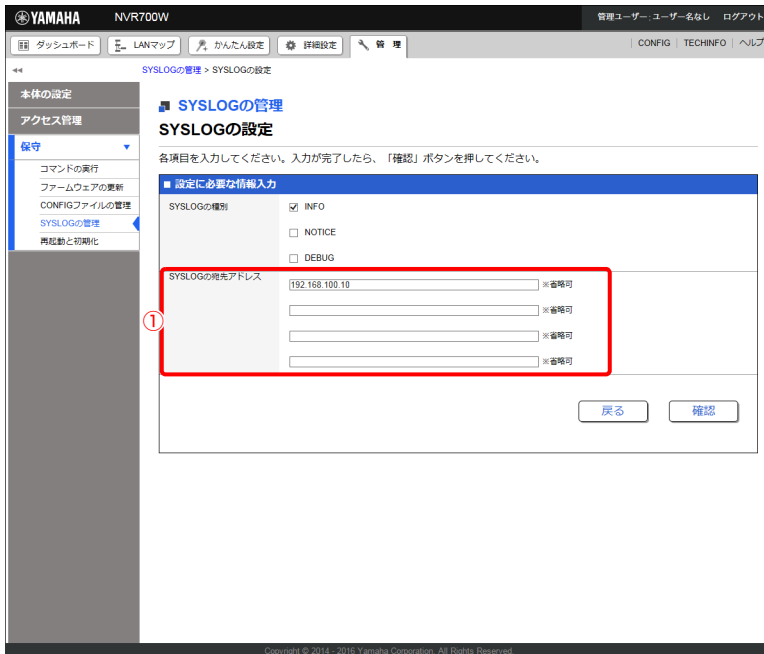
## 第 14 章 ヤマハルーターを管理する

### 2. 「SYSLOG の設定」項目の「設定」ボタンをクリックする。



「SYSLOG の設定」画面が表示されます。

### 3. SYSLOG の宛先アドレスを設定する。



#### ① SYSLOG の宛先アドレス :

SYSLOG の宛先のサーバー (SYSLOG ホスト) の IPv4 アドレスまたは IPv6 アドレスを入力します。最大で 4 つまで指定することができます。

### 4. 「確認」ボタンをクリックする。

「入力内容の確認」画面が表示されます。

## 5. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「SYSLOG の管理」画面が表示されます。

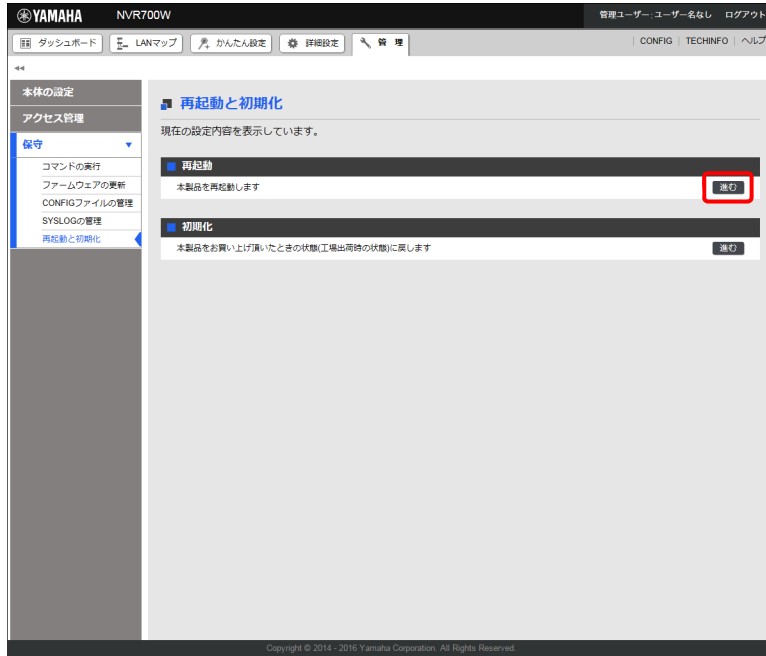
## 14.7 ヤマハルーターを再起動する

ヤマハルーターの再起動を行います。

1. 「管理」タブ - 「保守」 - 「再起動と初期化」を順に選択する。  
「再起動と初期化」画面が表示されます。

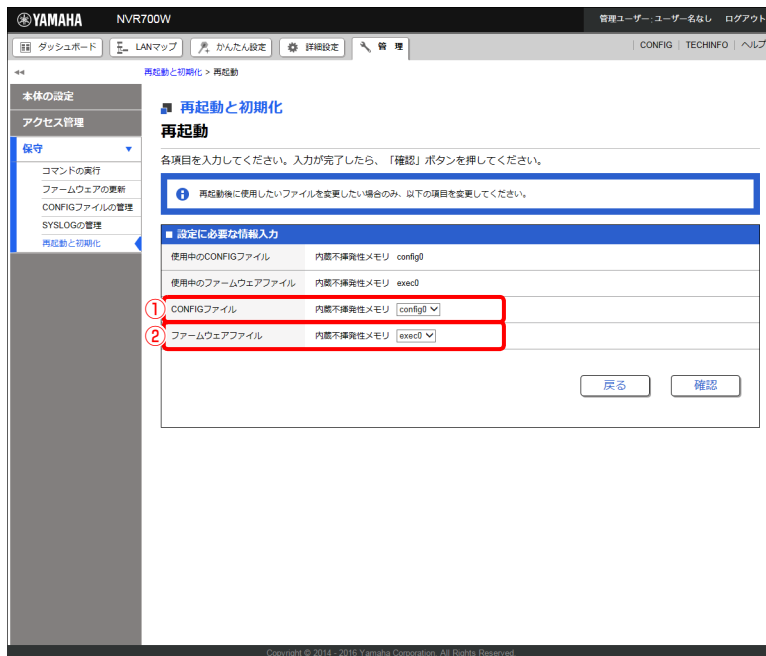
## 第 14 章 ヤマハルーターを管理する

### 2. 「再起動」項目の「進む」ボタンをクリックする。



「再起動」画面が表示されます。

### 3. 再起動後に使用するファイルを設定する。



#### ① CONFIG ファイル：

再起動後に使用したい設定（CONFIG）ファイルを選択します。

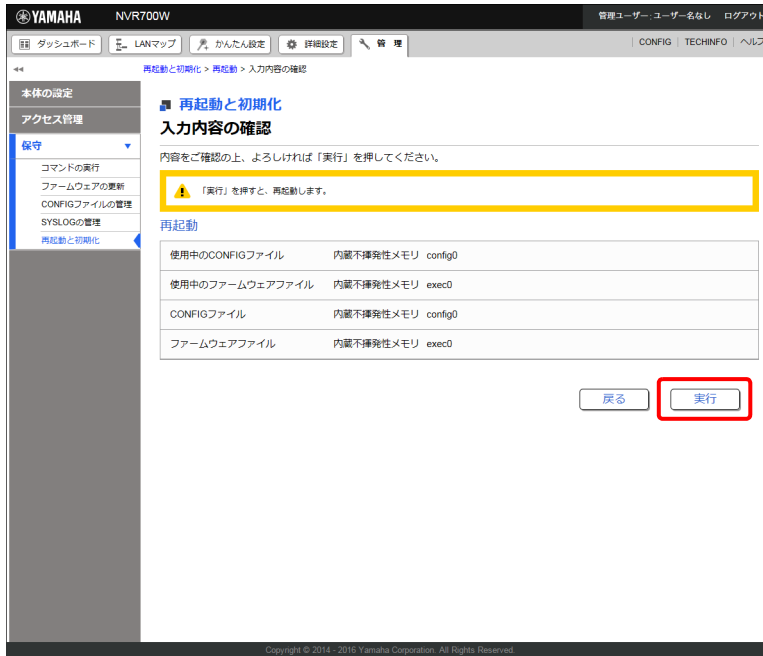
#### ② ファームウェアファイル：

再起動後に使用したいファームウェアファイルを選択します。

## メモ

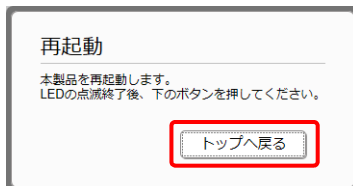
再起動後も現在使用中のものと同じ CONFIG ファイル / ファームウェアファイルを使用する場合は、設定を変更せずに手順 4 へ進んでください。

4. 「確認」 ボタンをクリックする。  
「入力内容の確認」画面が表示されます。
5. 内容を確認し、「実行」ボタンをクリックする。



「再起動」ダイアログが表示され、ヤマハルーターが再起動します。

6. ヤマハルーターの再起動の完了後、「トップへ戻る」ボタンをクリックする。



ダッシュボードページが表示されます。

## ご注意

再起動中は Web GUI を開いているパソコンがヤマハルーターと通信できない状態 (パソコンのネットワークアダプタの状態表示で「ネットワークケーブルが接続されていない」と表示されます) になりますが、再起動が完了すると通信状態が復旧します。ヤマハルーターのランプの点滅終了後に、Web GUI を開いているパソコンの通信状態が復旧していることを確認してから「トップへ戻る」をクリックしてください。

### 14.8 ヤマハルーターを工場出荷時の状態へ戻す

設定内容や SYSLOG などを消去し、ヤマハルーターを工場出荷時の状態へ戻します。なお、ファームウェアは変更されません。

#### ご注意

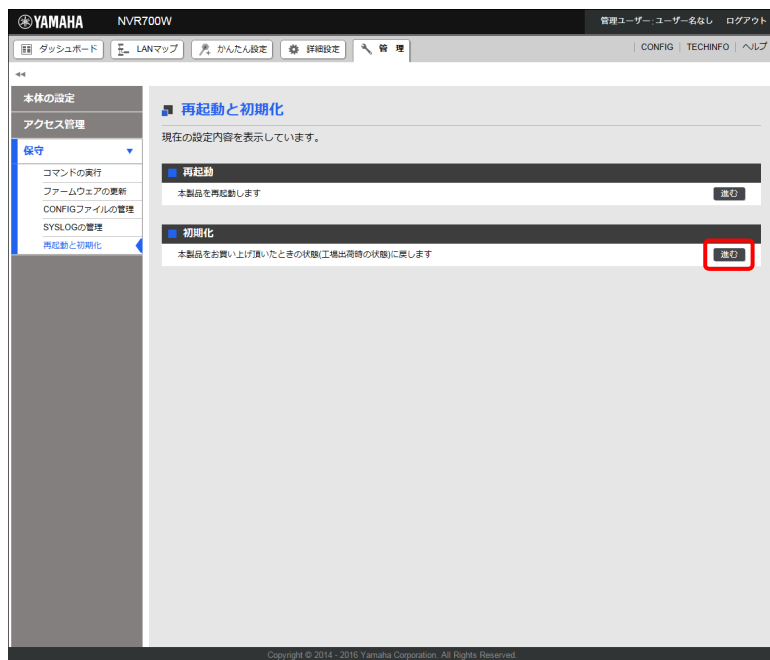
工場出荷時の状態へ戻す場合は、以下の点にご注意ください。

- ・ 実行した直後にすべての通信が切断されます。
- ・ ヤマハルーターの LAN アドレスが初期設定値（192.168.100.1）に戻ります。
- ・ 工場出荷時の状態に戻した後は設定内容を復元することはできません。必要に応じて、事前に外部メモリなどに設定内容を退避してください。外部メモリにエクスポートする方法については、「14.5.1 設定（CONFIG）を外部メモリにエクスポートする」（352 ページ）をご覧ください。

1. 「管理」タブ - 「保守」 - 「再起動と初期化」を順に選択する。

「再起動と初期化」画面が表示されます。

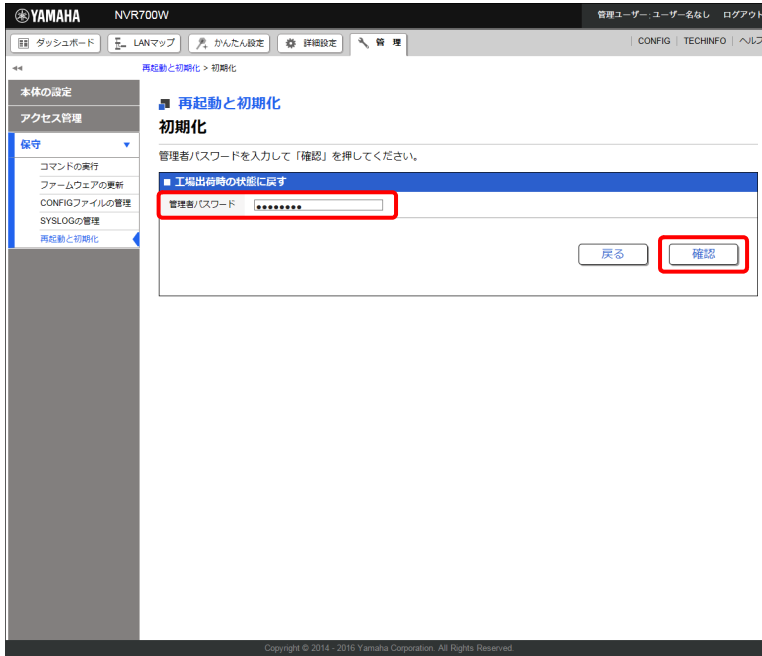
2. 「初期化」項目の「進む」ボタンをクリックする。



「初期化」画面が表示されます。

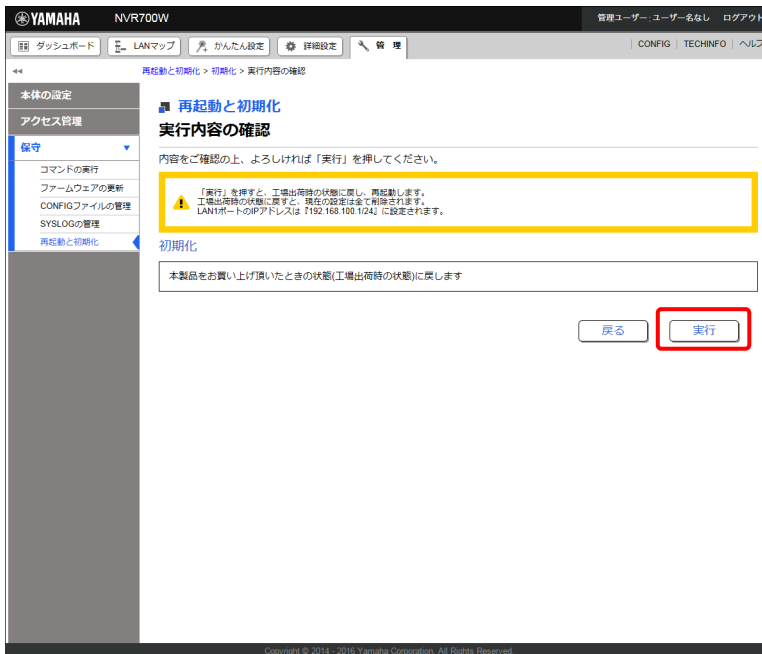


## 3. 管理パスワードを入力し、「確認」ボタンをクリックする。



「実行内容の確認」画面が表示されます。

## 4. 内容を確認し、「実行」ボタンをクリックする。



ヤマハルーターが工場出荷時の状態へ戻されます。また、「初期化」ダイアログが表示され、ヤマハルーターが再起動します。

## 第 14 章 ヤマハルーターを管理する

5. ヤマハルーターの再起動の完了後、Web GUI へ再度アクセスする。

### メモ

ヤマハルーターの LAN アドレスが 192.168.100.1 に戻ります。Web GUI へ再度アクセスする際には 192.168.100.1 へアクセスしてください。

### ご注意

再起動中は Web GUI を開いているパソコンがヤマハルーターと通信できない状態（パソコンのネットワークアダプタの状態表示で「ネットワークケーブルが接続されていない」と表示されます）になりますが、再起動が完了すると通信状態が復旧します。ヤマハルーターのランプの点滅終了後に、Web GUI を開いているパソコンの通信状態が復旧していることを確認してから「192.168.100.1/24」をクリックしてください。

# 第 15 章 独自の GUI を作成する（カスタム GUI）

ヤマハルーターに標準搭載されている Web GUI 画面とは別に、独自の Web GUI 画面を作成してヤマハルーターに組み込むことができます（カスタム GUI）。カスタム GUI を利用すれば、以下のようなことが実現できるようになります。

- ・ ログインするユーザーに応じて個別のトップページを表示させる
- ・ ユーザーごとに GUI でできることを変更する
- ・ 必要最低限の機能に関してのみ、GUI から設定や情報参照ができるようにする
- ・ 標準の GUI では対応していない機能の設定を行う
- ・ GUI 画面上のボタンを一回クリックするだけで、全拠点に共通する基本的な設定（複数のコマンド群）を登録させる

カスタム GUI の使用方法については、以下の URL をご覧ください。

<http://www.rtpro.yamaha.co.jp/RT/docs/custom-gui/>

なお、カスタム GUI を使用するためには、HTTP プロトコルや HTML、JavaScript に関する基礎的な知識が必要となります。

# 第 16 章 付録

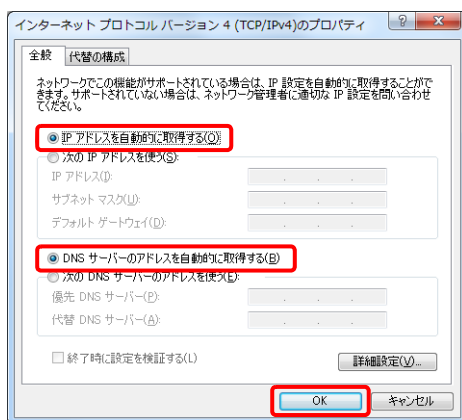
## 16.1 パソコンの IP アドレスを変更する

パソコンの IP アドレスを変更するには、以下の手順で操作します。

### 16.1.1 Windows 7 の場合

#### IP アドレスを自動取得するように設定する

1. 「スタート」 - 「コントロールパネル」 - 「ネットワークの状態とタスクの表示」 - 「アダプターの設定の変更」を順に選択する。
2. 変更する接続を右クリックし、「プロパティ」をクリックする。
3. 「インターネットプロトコル (TCP/IP)」を選択し、「プロパティ」ボタンをクリックする。
4. 「IP アドレスを自動的に取得する」と「DNS サーバーのアドレスを自動的に取得する」を選択し、「OK」ボタンをクリックする。



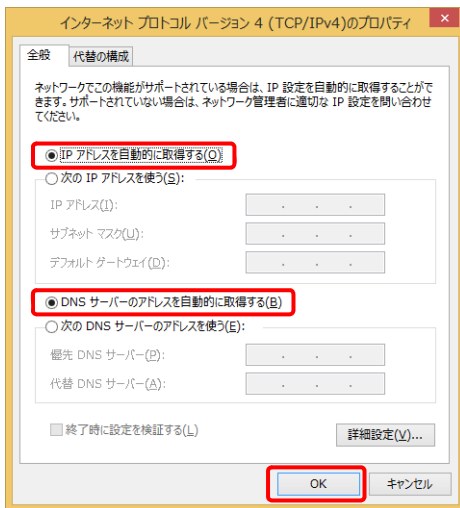
#### 動的 IP アドレスの再割り当てを行う

1. 「スタート」 - 「すべてのプログラム」 - 「アクセサリ」 - 「コマンドプロンプト」を選択する。
2. 「ipconfig /release」と入力し、Enter キーを押す。  
パソコンに割り当てられていた IP アドレスが解放されます。
3. 「ipconfig /renew」と入力し、Enter キーを押す。  
新たな IP アドレスがパソコンに割り当てられます。

## 16.1.2 Windows 8.1 の場合

## IP アドレスを自動取得するように設定する

1. 「デスクトップ」画面で、マウスカースルを右上隅または右下隅に移動する。
2. チャームから「設定」－「コントロールパネル」－「ネットワークの状態とタスクの表示」－「アダプターの設定の変更」の順に選択する。  
「ネットワーク接続」画面が表示されます。
3. 変更する接続を右クリックし、「プロパティ」をクリックする。
4. 「IP アドレスを自動的に取得する」と「DNS サーバーのアドレスを自動的に取得する」を選択し、「OK」ボタンをクリックする。



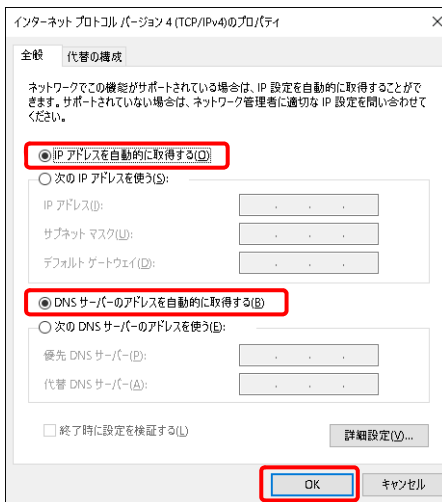
## 動的 IP アドレスの再割り当てを行う

1. 「デスクトップ」画面で、「スタート」を右クリックし、「コマンドプロンプト」を選択する。
2. 「ipconfig /release」と入力し、Enter キーを押す。  
パソコンに割り当てられていた IP アドレスが解放されます。
3. 「ipconfig /renew」と入力し、Enter キーを押す。  
新たな IP アドレスがパソコンに割り当てられます。

### 16.1.3 Windows 10 の場合

#### IP アドレスを自動取得するように設定する

1. 「スタート」 ボタンを右クリックする。
2. 「コントロールパネル」 - 「ネットワークの状態とタスクの表示」 - 「アダプターの設定の変更」 を順に選択する。
3. 変更する接続を右クリックし、「プロパティ」 をクリックする。
4. 「インターネットプロトコル (TCP/IP)」 を選択し、「プロパティ」 ボタンをクリックする。
5. 「IP アドレスを自動的に取得する」と「DNS サーバーのアドレスを自動的に取得する」 を選択し、「OK」 ボタンをクリックする。



#### 動的 IP アドレスの再割り当てを行う

1. 「スタート」 を右クリックし、「コマンドプロンプト」 を選択する。
2. 「ipconfig /release」と入力し、Enter キーを押す。  
パソコンに割り当てられていた IP アドレスが解放されます。
3. 「ipconfig /renew」と入力し、Enter キーを押す。  
新たな IP アドレスがパソコンに割り当てられます。

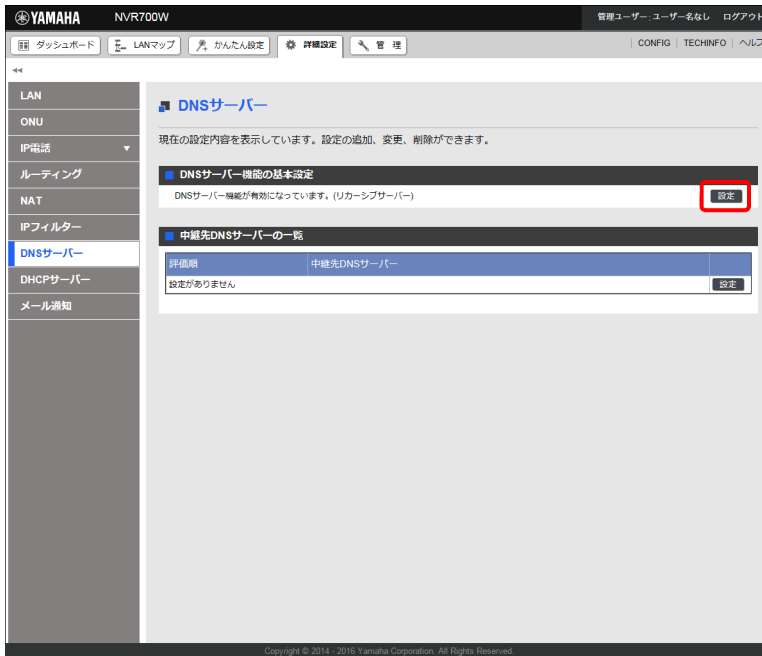
## 16.2 DNS サーバー機能にアクセスできるホストの設定を変更する

ヤマハルーターの DNS サーバー機能にアクセスできるホストを変更します。

### メモ

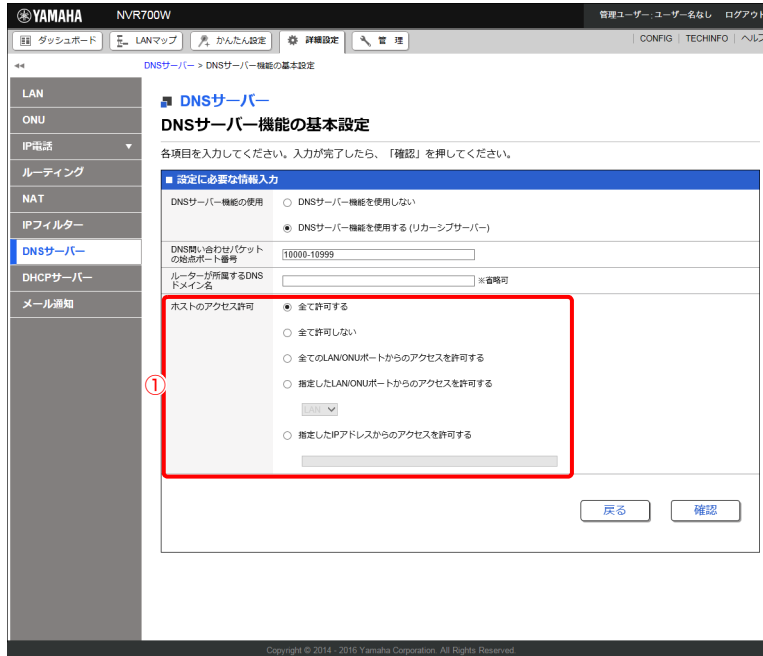
プロバイダー情報を設定すると、ヤマハルーターの DNS サーバー機能にアクセスできるホストは、自動的に LAN ポートに接続されているホストに制限されます。

1. 「詳細設定」タブ - 「DNS サーバー」を順に選択する。  
「DNS サーバー」画面が表示されます。
2. 「DNS サーバー機能の基本設定」項目の「設定」ボタンをクリックする。



「DNS サーバー機能の基本設定」画面が表示されます。

3. ホストのアクセス許可を設定する。



① ホストのアクセス許可：

- **全て許可する**  
すべてのホストからの DNS サーバー機能へのアクセスを許可します。
- **全て許可しない**  
すべてのホストからの DNS サーバー機能へのアクセスを禁止します。
- **全ての LAN/ONU ポートからのアクセスを許可する**  
すべての LAN ポート側ネットワーク内からの DNS サーバー機能へのアクセスを許可します。
- **指定した LAN/ONU ポートからのアクセスを許可する**  
1 つの任意の LAN ポート側ネットワーク内からの DNS サーバー機能へのアクセスを許可します。
- **指定した IP アドレスからのアクセスを許可する**  
指定した IP アドレスからの DNS サーバー機能へのアクセスを許可します。範囲指定する場合は、'-' で区切って入力してください。IP アドレス及び IP アドレスの範囲を複数設定する場合は、'|' で区切って入力してください。

4. 「確認」ボタンをクリックする。

「入力内容の確認」画面が表示されます。



5. 内容を確認し、「設定の確定」ボタンをクリックする。

The screenshot shows the Yamaha NVR700W Web GUI. The left sidebar contains navigation options: LAN, ONU, IP電話, ルーティング, NAT, IPフィルター, DNSサーバー (highlighted), DHCPサーバー, and メール通知. The main content area is titled "DNSサーバー 入力内容の確認". Below the title, there is a message: "入力内容をご確認の上、変更がなければ「設定の確定」を押してください。" and a link for "DNSサーバー機能の基本設定". A table displays the current configuration:

DNSサーバー機能の使用	DNSサーバー機能を使用する (リカーブサーバー)
始点ポート番号	10000-10999
ドメイン名	
ホストのアクセス許可	指定したLAN/ONUポートからのアクセスを許可する
	LAN

At the bottom right, there are two buttons: "戻る" and "設定の確定". The "設定の確定" button is highlighted with a red rectangle.

設定が反映され、「DNS サーバー」画面が表示されます。

## 16.3 ヤマハルーターを譲渡 / 廃棄する際のご注意

ヤマハルーターを譲渡 / 廃棄する際は、以下の操作を行ってください。

1. ネットボランチ DNS ホスト名の登録を解除する
2. 設定内容を初期化する

### ご注意

- ・ 先に設定内容を初期化してしまうと、ネットボランチ DNS サーバーに登録されたホストアドレスを削除できなくなります。必ずネットボランチ DNS ホスト名の登録を解除してから、設定内容を初期化するようにしてください。
- ・ ネットボランチ DNS ホスト名の登録の解除は、ネットボランチ DNS ホスト名を登録したお客様のみ行ってください。
- ・ ヤマハルーターを譲渡する際は、製品付属のマニュアル類もあわせて譲渡してください。

### 16.3.1 設定内容を初期化する

保存されている設定内容には、プロバイダーへの接続に必要な ID やパスワードも含まれています。設定内容を初期化せずに譲渡 / 廃棄すると、これらの情報が悪意のある第三者によって悪用されるおそれがあります。初期化の方法については、「14.8 ヤマハルーターを工場出荷時の状態へ戻す」(364 ページ) をご覧ください。

**ネットボランチ・コールセンター**

TEL: 03-5715-0350

**ご相談受付時間**

9:00~12:00、13:00~17:00

(土・日・祝日、年末年始は休業とさせていただきます)

**お問合せページ**

<http://jp.yamaha.com/products/network/> から  
サポートページにお進みください。