



EchoLife HN8055Q

V300R016C00

取扱説明書

発行 01

日付 2015-05-30

Copyright © Huawei Technologies Co., Ltd. 2015. All rights reserved.

文書による華為の事前承諾なしに、本書のいかなる部分も、いかなる形式またはいかなる手段によっても複製または転載は許可されません。

商標および許諾



HUAWEIおよびその他のファーウェイ(華為)の商標は華為技術有限公司の商標です。
このドキュメントに記載されているその他の商標はすべて、それぞれの所有者に帰属します。

注意

購入した製品、サービスおよび機能は華為とお客様の間の契約によって規定されます。本文書に記載されている製品、サービスおよび機能の全体または一部は、購入範囲または使用範囲に含まれない場合があります。契約で規定しない場合、本文書内の記述、情報、推奨事項はすべて「無保証(AS IS)」で提供されており、明示的または暗黙的ないかなる保証も約束も行いません。

この文書の記載内容は、予告なく変更されることがあります。この文書作成にあたっては内容の正確性に最大限の注意を払っておりますが、この文書内のいかなる説明、情報、推奨事項も、明示的または暗黙的に何らかの保証を行うものではありません。

Huawei Technologies Co., Ltd.

住所: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Webサイト: <http://www.huawei.com>

Eメール: support@huawei.com

本章について

目的

ギガビット対応パッシブ光ネットワーク(XG-PON)端末EchoLife HN8055Q(以降 HN8055Qと呼ぶ)は、ホームユーザー向けに設計された屋内光ネットワークユニット(ONU)です。本書では、HN8055Qの外観と仕様、およびその設定と使用方法について説明します。これにより、HN8055Qについての知識を短期間で得ることができます。




製品バージョン



以下の表に、本書に関連する製品バージョンを示します。

製品名	製品バージョン
EchoLife HN8055Q	V300R016C00

マークの表記

本書で使用するマークは、以下のように定義されています。

 危険	回避しなければ、死亡または重傷につながる、危険が差し迫った状況を示しています。
 警告	回避しなければ、死亡または重傷につながるおそれのある、危険を伴う状況を示しています。
 注意	回避しなければ、軽傷または中程度の負傷につながるおそれのある、危険を伴う状況を示しています。

マーク	説明
 注意事項	<p>回避しなければ、機器の損傷、データの喪失、パフォーマンスの低下、予期しない結果につながるおそれのある、危険を伴う状況を示します。</p> <p>注意事項は、人体の損傷に関係のない行為に対処するために使用されます。</p>
 注記	<p>重要な情報、ベストプラクティス、ヒントなどを示します。</p> <p>注記は、人体の損傷、機器の損傷、環境悪化に関係のない情報に対処するために使用されます。</p>

目次

本章について.....	ii
1 安全上のご注意.....	1
2 システム概要.....	3
2.1 製品概要.....	4
2.2 仕様.....	8
2.2.1 物理的仕様.....	8
2.2.2 プロトコルおよび規格.....	9
2.3 代表的なネットワークアプリケーション.....	9
3 同梱品一覧.....	10
4 設置.....	12
4.1 HN8055Q の設置.....	13
4.2 電源ケーブルの接続およびボタン設定.....	13
5 管理画面へのログイン方法.....	16
6 Web ページでのインターネットアクセスサービスの設定.....	30
7 Web ページでの Wi-Fi アクセスサービスの設定.....	32
8 Web ページのリファレンス.....	40
8.1 高速設定.....	41
8.2 ホームページ.....	43
8.3 ワンクリック診断.....	44
8.4 システム情報.....	45
8.4.1 デバイス情報.....	45
8.4.2 WAN 情報.....	46
8.4.3 光学情報.....	47
8.4.4 サービスプロビジョニングステータス.....	48
8.4.5 Eth ポート情報.....	49
8.4.6 WLAN 情報.....	49
8.4.7 スマート WiFi カバレッジ.....	50
8.5 詳細設定.....	51
8.5.1 WAN 設定.....	51

8.5.2 LAN 設定.....	53
8.5.2.1 レイヤ 2/3 ポート設定.....	54
8.5.2.2 LAN ホスト設定.....	54
8.5.2.3 DHCP サーバ設定.....	55
8.5.2.4 DHCP スタティック IP 設定.....	58
8.5.2.5 DHCPv6 サーバ設定.....	59
8.5.2.6 DHCPv6 スタティック IP 設定.....	61
8.5.2.7 DHCPv6 情報.....	61
8.5.3 セキュリティ設定.....	62
8.5.3.1 DoS 設定.....	62
8.5.3.2 IPv4 アドレスフィルタリング.....	63
8.5.3.3 MAC アドレスフィルタリング.....	65
8.5.3.4 Wi-Fi MAC アドレスフィルタリング.....	66
8.5.3.5 ペアレンタルコントロール.....	67
8.5.3.6 ONT アクセス制御設定.....	68
8.5.4 ルート.....	69
8.5.4.1 デフォルトの IPv4 ルート設定.....	69
8.5.4.2 IPv4 スタティックルート設定.....	70
8.5.4.3 IPv4 VLAN バインディング設定.....	71
8.5.4.4 IPv4 サービスルート設定.....	72
8.5.4.5 IPv4 ルーティングテーブル.....	72
8.5.4.6 デフォルトの IPv6 ルート設定.....	73
8.5.4.7 IPv6 スタティックルート設定.....	73
8.5.5 転送ルール.....	74
8.5.5.1 DMZ 設定.....	74
8.5.5.2 IPv4 ポートマッピング.....	76
8.5.5.3 ポートトリガ設定.....	77
8.5.6 アプリケーション.....	79
8.5.6.1 時間設定.....	79
8.5.6.2 メディア共有.....	80
8.5.6.3 DDNS 設定.....	81
8.5.6.4 UPnP 設定.....	83
8.5.6.5 IGMP 設定.....	83
8.5.6.6 スタティック DNS.....	84
8.5.7 WLAN.....	85
8.5.7.1 2.4G 基本ネットワーク設定.....	85
8.5.7.2 2.4G 詳細ネットワーク設定.....	88
8.5.7.3 5G 基本ネットワーク設定.....	90
8.5.7.4 5G 詳細ネットワーク設定.....	93
8.5.7.5 WiFi 自動切断.....	95
8.5.7.6 スマート WiFi カバレッジ管理.....	96

8.5.8 システム管理.....	96
8.5.8.1 TR-069.....	96
8.5.8.2 アカウント管理.....	99
8.5.8.3 ご利用上の注意.....	99
8.5.8.4 ONT 認証.....	101
8.5.9 保守診断.....	101
8.5.9.1 ファームウェアアップグレード.....	101
8.5.9.2 設定ファイル管理.....	102
8.5.9.3 保守.....	102
8.5.9.4 ログ.....	104
8.5.9.5 障害情報の収集.....	104
8.5.9.6 リモートミラーリング.....	105

1 安全上のご注意

本製品を正しく安全にお使いいただくために、ご使用前にこの「安全上のご注意」をよくお読みください。

基本的な要件

- 本製品は保管、輸送、および稼働時は乾燥した状態を保ってください。
- 本製品は保管、輸送、および稼働時は他の物体にぶつからないようにしてください。
- 本製品を設置するにはメーカーの要件を必ず守ってください。
- 本製品を勝手に分解しないでください。本製品に異常がある場合は、サービス提供元が指定するお問い合わせ先にご連絡ください。
- 本製品の構造、安全設計、性能設計を許可なく変更しないでください。
- 本製品を使用するには各国・地域の法令を遵守し、他者の法的権利を尊重してください。
- 本製品がご不要になった際は、サービス提供元が指定するお問い合わせ先にご連絡ください。

環境要件

- 本製品は直射日光の当たらない、風通しの良い場所に設置してください。
- 本製品は清潔な状態を保ってください。
- 本製品は水周りまたは湿った場所のそばに置かないでください。
- 本製品の上に物を置かないでください。熱や歪みにより本製品が損傷する場合があります。
- 放熱のため、機器の周囲に少なくとも10cm以上のスペースを確保してください。
- 本製品はヒーターやろうそくなどの熱源や火気の近くに置かないでください。
- 本製品を電子レンジ、冷蔵庫、携帯電話など、強力な磁場や磁界が発生する電子機器のそばに置かないでください。

使用上のご注意

- 付属の電源アダプタ以外は使用しないでください。
- 利用電圧は本製品の入力電圧の要件に適合している必要があります。

- 本製品の電源アダプタは、たこ足配線にしないでください。たこ足配線にするとテーブルタップなどが過熱、劣化する可能性があります。危険です。
- 感電またはその他の危険を回避するために、電源プラグは清潔で乾燥した状態を保ってください。
- ケーブルの抜き差しは、必ず機器を停止して、電源を切ってから行ってください。
- 雷が発生した場合には、電源を切って、電源ケーブル、モジュラーケーブル、電話線などすべてのケーブルを抜いてください。
- 本製品を長期間使用しない場合には、電源を切って電源プラグを抜いてください。
- 本製品は水や液体で濡らさないようにしてください。水や他の液体で濡れた場合には、すぐに電源を切って、本製品から電源ケーブルやモジュラーケーブルなどすべてのケーブルを抜いてください。本製品が故障した場合にはサービス提供元が指定するお問い合わせ先にご連絡ください。
- 損傷するおそれがあるため、ケーブルを踏みつけたり、引っ張ったり、引きずったり、無理やり曲げたりしないでください。ケーブルが損傷すると、本製品が故障するおそれがあります。
- 損傷または劣化したケーブルは使用しないでください。
- 保護メガネを着用せずに直接光ポートを覗き込んだりしないでください。光ポートから放射されるレーザーによって目を痛めるおそれがあります。
- 発煙、異常な音、異臭などが発生したら、ただちに本製品の使用を中止して、電源を切り、全てのケーブル(電源ケーブルやモジュラーケーブルなど)を抜いてください。本製品に異常がある場合は、サービス提供元が指定するお問い合わせ先にご連絡ください。
- 金属部品などの異物が通気孔から本製品に入らないようにしてください。
- 引っかいた場所からはがれた塗装によって本製品に異常が発生するおそれがあるため、本製品の外装を引っかいたりしないでください。塗装が本製品に入ると、ショートするおそれがあります。また、はがれた塗装によって人体にアレルギー反応が発生するおそれがあります。
- 部品や付属品を誤って飲み込むことがないように幼児の手の届かないところに設置してください。

清掃上のご注意

- 本製品を清掃する前に、本製品を停止し、電源を切って、本製品から電源ケーブルやモジュラーケーブルなどすべてのケーブルを抜いてください。
- クリーニング液またはスプレー式洗剤を使用して本製品の外装を清掃しないでください。柔らかい布を使用して清掃してください。

2 システム概要

本章について

本章では、HN8055Qの概要を示します。

2.1 製品概要

ここでは、HN8055Qの外観を示し、そのポートとLED種別について説明します。

2.2 仕様

ここでは、HN8055Qの物理的仕様やHN8055Qが準拠している規格およびプロトコルなどの仕様について説明します。

2.3 代表的なネットワークアプリケーション

ここでは、HN8055Qの代表的なネットワークアプリケーションについて説明します。

2.1 製品概要

ここでは、HN8055Qの外観を示し、そのポートとLED種別について説明します。

HN8055Qは、個人宅向の屋内光ネットワーク端末です。筐体は自然放熱材でできていて、光ポートは防塵設計を採用し、ラバープラグがついています。このため外観がすっきりしていて、エネルギー効率に優れています。設置場所に縦置きで設置できるため、様々な環境でのユーザーの設置要件に適合します。



注意事項

HN8055Qは屋内での使用に限定されます。HN8055Qを屋外または屋外のキャビネットに設置しないでください。

外観

図 2-1に、縦置きスタンドに設置したHN8055Qの外観を示します。

図 2-1 HN8055Q 正面の外観

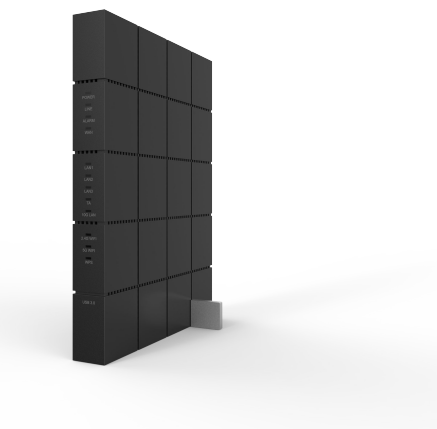


図 2-2 HN8055Q 背面の外観



表 2-1では、HN8055Qの各ポートおよびボタンの機能について説明します。

表 2-1 HN8055Q のポートおよびボタンの機能

ポート/ボタン	機能
POWER	電源アダプタまたはバックアップ電源ユニットに接続するために使用する電源ポート。
TA	関連パラメータを設定した後に電話機またはファクシミリに接続するために使用するオートセンシング10/100/1000M Base-Tイーサネットポート(RJ-45)。
LAN1-LAN3/10G LAN	PCやTV等に接続するために使用するオートセンシング10/100/1000M Base-Tイーサネットポート(RJ-45)。
USB1-USB2	USBストレージデバイスに接続するために使用するUSBポート。
RESET	リセットボタン。このボタンを数秒間押下すると、本製品がリセットされます。このボタンを長時間(10秒以上)押し続けると、本製品が工場出荷時の設定に戻った後、リセットされます。
WLAN	無線LAN機能(Wi-Fi)を有効または無効にするために使用するボタンです。この機能はデフォルトで有効になっています。
WPS	無線LANデータ暗号化機能を有効または無効にするために使用するWi-Fi保護設定(WPS)ボタンです。この機能はデフォルトで無効になっています。

LED 種別

図 2-3に、HN8055QのLED種別を示します。

図 2-3 HN8055Q のLED種別

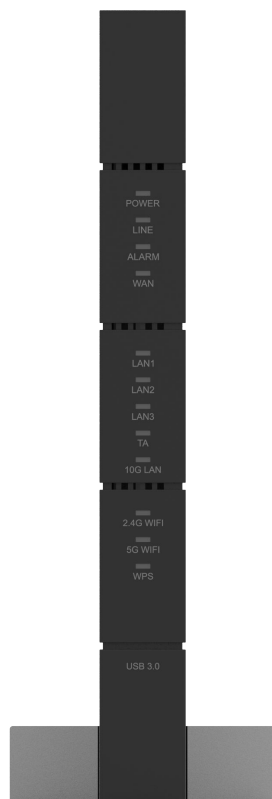


表 2-2では、HN8055QのLED種別の意味について説明します。

表 2-2 HN8055Q のLED種別の意味

LED種別	LED色	LED状態	説明
POWER	緑	点灯	HN8055Qの電源がオンになっています。
		オフ	電源が切れています。
LINE	緑	点灯	HN8055Qの認証に成功しています。
		点滅	HN8055Qの認証中です。
		オフ	HN8055Qが認証されていません。
ALARM	赤	点灯	光リンクで障害が発生しています。
		点滅	システムをアップグレードしています。

LED種別	LED色	LED状態	説明
		オフ	光リンクが正常です。
WAN	緑	点灯	インターネットに正常に接続されています。
		点滅	DHCPを使用して、HN8055QはIPアドレスを取得しています。
		オフ	HN8055QはIPアドレスを取得していません。
LAN1-LAN3/10G LAN	緑	点灯	LAN接続されています。
		点滅	LAN接続でデータ通信中です。
		オフ	LANポートに機器が接続されていません。
TA	緑	点灯	TA接続されています。
		点滅	TA接続でデータ通信中です。
		オフ	TAポートに機器が接続されていません。
2.4G WiFi	緑	点灯	Wi-Fi機能は2.4GHzで利用可能です。
		点滅	Wi-Fi端末が2.4GHzでHN8055Qにアクセスしています。
		オフ	Wi-Fi機能は2.4GHzでは利用できません。
5G WiFi	緑	点灯	Wi-Fi機能は5GHzで利用可能です。

LED種別	LED色	LED状態	説明
		点滅	Wi-Fi端末が5GHzでHN8055Qにアクセスしています。
		オフ	Wi-Fi機能は5GHzで利用できません。
WPS	緑	点灯	WPS機能が有効になっていて、Wi-Fi端末がHN8055Qに正常にアクセスしています。
	黄色	点滅	Wi-Fi端末がHN8055Qにアクセスしています。
	赤	点滅	Wi-Fi端末がHN8055Qへのアクセスに失敗しています。
	-	オフ	WPS機能が有効になっていません。

2.2 仕様

ここでは、HN8055Qの物理的仕様やHN8055Qが準拠している規格およびプロトコルなどの仕様について説明します。

2.2.1 物理的仕様

ここでは、寸法、重量、電圧範囲、動作環境パラメータなど、HN8055Qの物理的仕様について説明します。

表 2-3に、HN8055Qの物理的仕様を示します。

表 2-3 HN8055Q の物理的仕様

項目	仕様
寸法(幅 x 奥行き x 高さ)	HN8055Q: 238 mm x 26 mm x 190 mm 縦置きスタンド: 23 mm x 6mm x 80mm
重量	約2000 g
システム全体の電源	12V DC、3A

項目	仕様
電源アダプタ入力	100 V – 240 V、50 Hz / 60 Hz
最大消費電力	36 W 以下
周囲温度	0°C - + 40°C
保管および輸送温度	-40°C - +70°C
周囲湿度	5% – 95%(結露なし)

2.2.2 プロトコルおよび規格

ここでは、HN8055Qが準拠しているプロトコルおよび規格を示します。

- XG-PON: ITU-T勧告G.987.2
- ルーティング: ネットワークアドレス変換(NAT)およびアプリケーションレベルゲートウェイ(ALG)
- LANインターフェース: IEEE 802.3/IEEE 802.3u/IEEE 802.3ab
- USB: USB 3.0
- Wi-Fi: IEEE 802.11a/b/g/n/ac

2.3 代表的なネットワークアプリケーション

ここでは、HN8055Qの代表的なネットワークアプリケーションについて説明します。

HN8055Qはネットワーク端末としてXG-PONアクセスレイヤに配備され、上り光ポートを介して個人宅ユーザーをインターネットに接続します。ローカルエリアネットワーク(LAN)側(すなわち、ユーザー側)から見ると、HN8055Qには豊富なハードウェアポートが用意されていて、個人宅ユーザーのさまざまなネットワーク要件が満たされます。

3 同梱品一覧

本章では、[図 3-1](#)に示すように、HN8055Q、縦置きスタンド、電源アダプタなど、荷箱に入っているものについて説明します。

図 3-1 荷箱

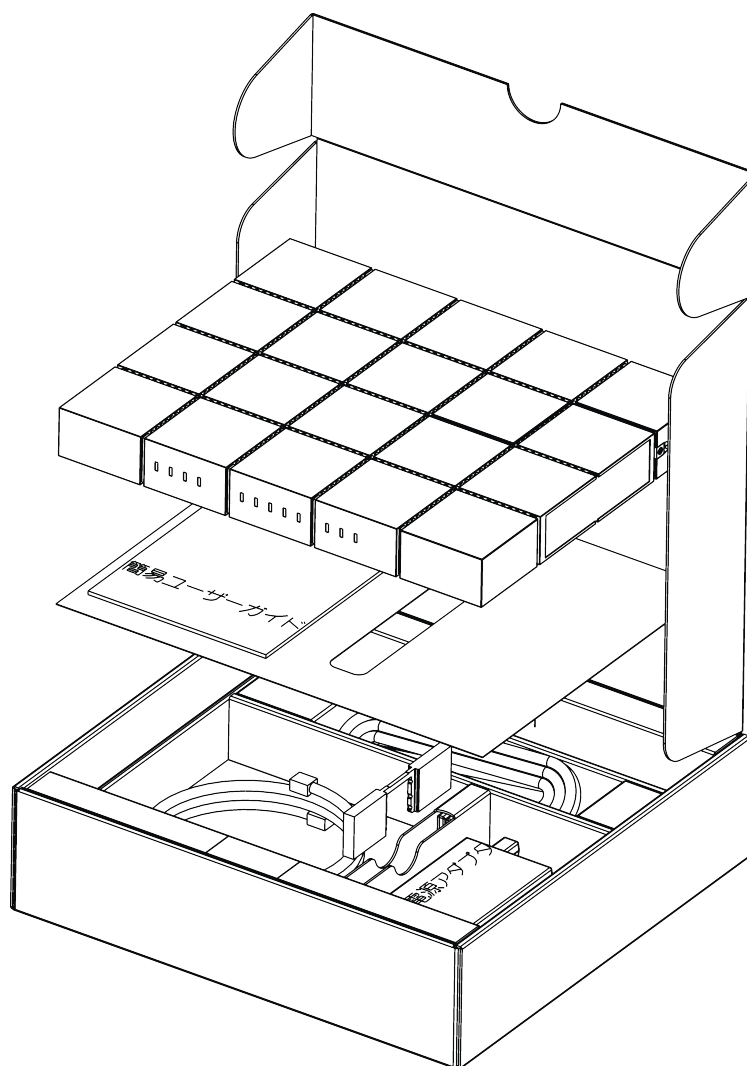

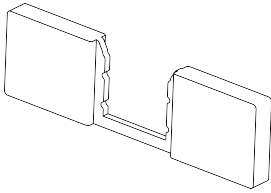






表 3-1 同梱品一覧

名前	図				
HN8055Q本体					
縦置きスタンド					
電源ケーブルおよび電源アダプタ					
LANケーブル(1本)(ストレート)					
簡易ユーザーガイド	<p data-bbox="1010 1198 1181 1243">EchoLife HN8055Q 簡易ユーザーガイド</p>  <div data-bbox="933 1496 1181 1545"> <p>同梱品一覧</p> <table border="1"> <tr> <td>HN8055Q本体</td> <td>電源ケーブルおよび電源アダプタ</td> </tr> <tr> <td>LANケーブル(1本)(ストレート)</td> <td>簡易ユーザーガイド</td> </tr> </table>  </div>	HN8055Q本体	電源ケーブルおよび電源アダプタ	LANケーブル(1本)(ストレート)	簡易ユーザーガイド
HN8055Q本体	電源ケーブルおよび電源アダプタ				
LANケーブル(1本)(ストレート)	簡易ユーザーガイド				

4 設置

本章について

本章では、HN8055Qを設置し、ケーブルを接続する手順について説明します。

4.1 HN8055Qの設置

ここでは、HN8055Qの設置方法について説明します。

4.2 電源ケーブルの接続およびボタン設定

ここでは、HN8055Qのポートを他のデバイスに接続する手順について説明します。

4.1 HN8055Q の設置

ここでは、HN8055Qの設置方法について説明します。

はじめに

ご使用前に本体にスタンドを取り付けて縦置きにしてください。壁や天井など別の場所に設置したり、屋外または屋外のキャビネットに設置したりしないでください。

手順

ステップ1 矢印の方向にHN8055Qを設置してください。



ステップ2 縦置きスタンドを取り付けたHN8055Qを設置場所に縦置きにします。

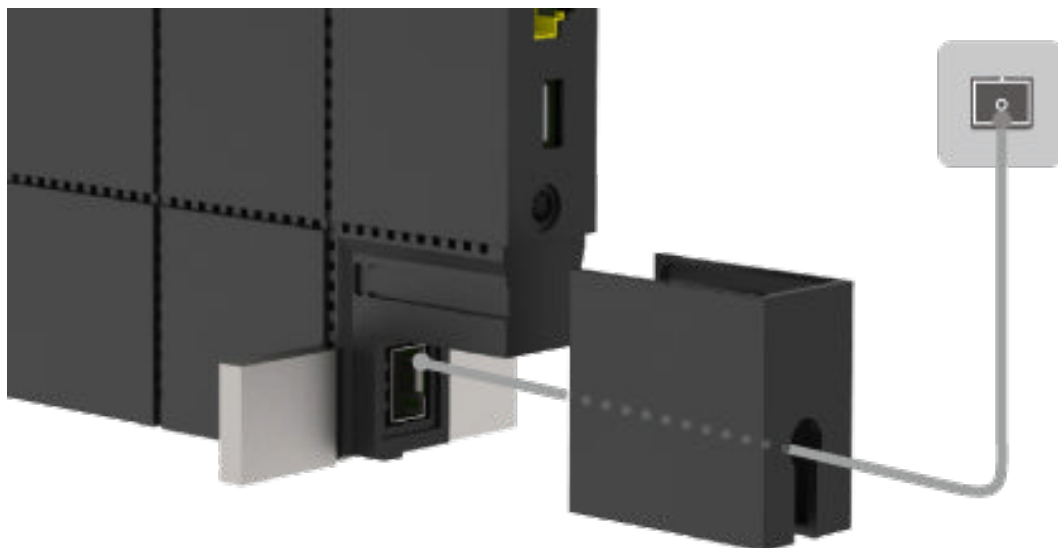
4.2 電源ケーブルの接続およびボタン設定

ここでは、HN8055Qのポートを他のデバイスに接続する手順について説明します。

手順

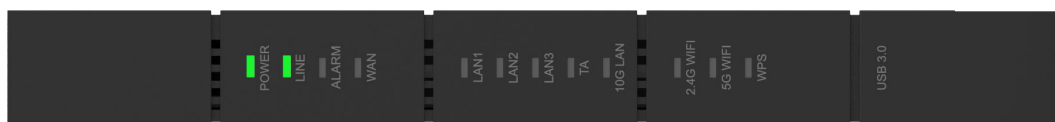
ステップ1 装置カバーを矢印の方向に沿って押します。光ファイバを使用してXG-PON終端装置のOPTICALポートと壁面にある光ポートを接続します。

図 4-1 光ポートの接続



ステップ 2 電源アダプタをDC INポートに接続し、電源ケーブルをAC電源コンセントに接続します。HN8055Qの電源が正常にオンになると、LED が以下の図のように点灯します。

図 4-2 HN8055Q の電源が正常にオンになると点灯する LED



ステップ 3 イーサネットケーブルでLANポートにPCまたはTVを接続します。

ステップ 4 USBデータケーブルでUSBポートにUSBストレージデバイスを接続します。

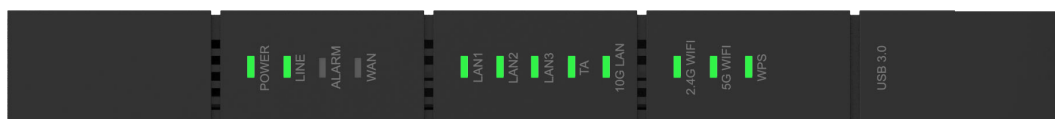
ステップ 5 Wi-Fi機能はデフォルトで有効になっています。Wi-Fi無線アクセス機能を有効/無効にするには、上面のWLANボタンを押します。

ステップ 6 無線アクセス用WPS(Wi-Fi 保護設定)暗号化機能を有効にするには、上面の WPSボタンを押します。



注記
WPS暗号化機能を有効にするには、あらかじめソフトウェア内でWPS暗号化機能が設定されている必要があります。WPSボタンを押してもWPS暗号化機能が有効にならない場合、サービス提供元の指定するお問い合わせ先にお問い合わせください。HN8055Qが外部デバイスへの接続に成功し、WPS機能が有効になっている場合、LEDは以下の図のように点灯します。

図 4-3 HN8055Q が外部デバイスへの接続に成功すると点灯する LED





注記

LAN1、LAN2、LAN3、TAが接続されていて、2.4G Wi-Fiおよび5G Wi-Fiそれぞれについて有効化(「WLANの有効化」)設定をしている場合、上記の図のように点灯します。

WANデータをWebページで設定し、インターネットに正常に接続されると、WANインジケータが緑色に点灯します。

5 管理画面へのログイン方法

本章では、Webページを介してHN8055Qにログインするためのユーザー名/パスワードおよび手順について説明します。

はじめに

管理画面へのログインを行う前に表 5-1 初期設定情報一覧「PCのIPアドレスとサブネットマスク」に記載した設定が完了していることを確認してください。

表 5-1 初期設定情報一覧

項目	説明
ユーザー名とパスワード	デフォルト設定: <ul style="list-style-type: none">● ユーザー:<ul style="list-style-type: none">- ユーザー名: admin_nt_ikyo- パスワード: nt_ikyo_admin_+"MACアドレスの下4桁" 注意事項 <ul style="list-style-type: none">● ログインしてから5分間何も操作が実行されないと、ログインがタイムアウトして自動的にログアウトされ、ログイン待ち状態に戻ります。ユーザー名とパスワードを入力すると、ユーザーアカウントのロックを解除できます。● 間違ったユーザー名とパスワードが3回続けて入力されると、システムはロックされます。1分後に自動的にシステムのロックが解除されます。
LAN IPアドレスとサブネットマスク	デフォルト設定: <ul style="list-style-type: none">● IPアドレス: 192.168.1.1● サブネットマスク: 255.255.255.0

項目	説明
PCのIPアドレスとサブネットマスク	<p>PCで自動的にIPアドレスを取得するよう設定して、PCのIPアドレスがHN8055QのLAN IPアドレスと同じサブネット内に属するよう設定します。</p> <p>例:</p> <ul style="list-style-type: none"> ● IPアドレス:192.168.1.100 ● サブネットマスク:255.255.255.0

手順

ステップ1 付属のLANケーブルを使用して、HN8055Q本体のLANポートとPC端末を接続します。

ステップ2 PCで自動的にIPアドレスを取得します。また、PCのIPアドレスがHN8055Qの管理用IPアドレスと同じサブネット内に属していることを確認します。

本書はPCで自動的にIPアドレスを取得する方法について、Windows 8、Windows 7、Windows XP、Mac OS X 10.8.2の各OSごとに説明しています。

- Windows 8のケース

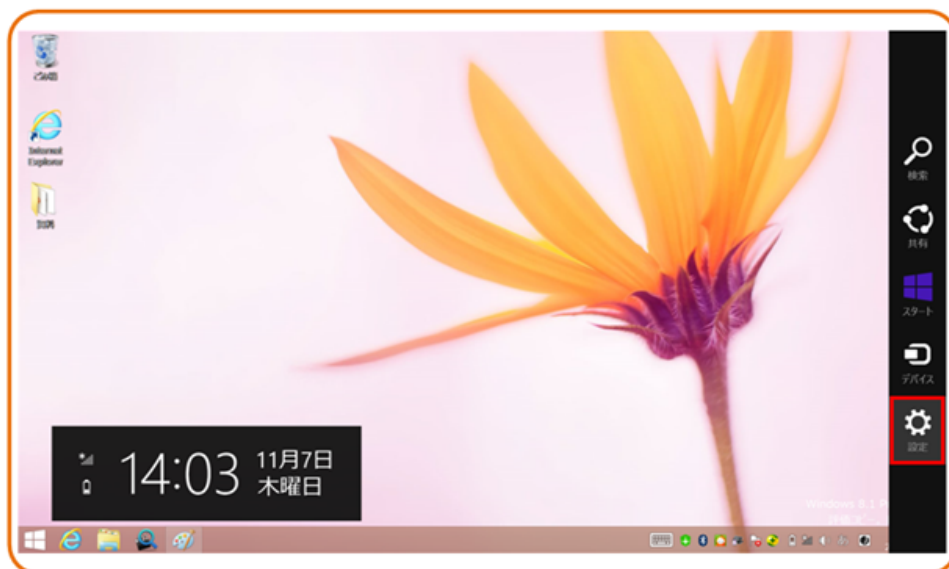
1. OSにログインした後、[図 5-1](#)に示すように[デスクトップ]を選択します。

図 5-1 スタート画面



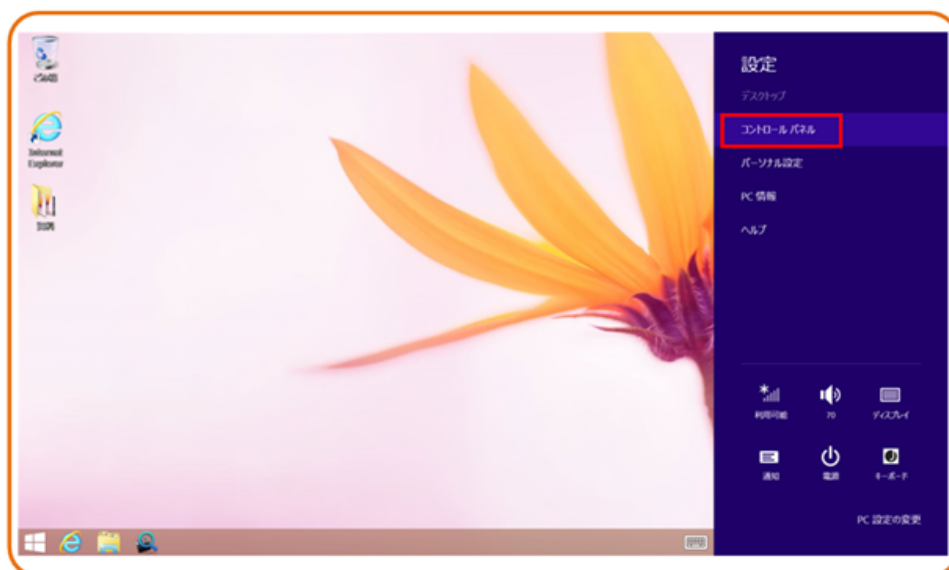
2. [デスクトップ]画面に入り、画面の右下または右上にマウスポインターを移動すると、チャームが表示されます。チャームから[設定]ボタンを選択します。

図 5-2 [設定]ボタン



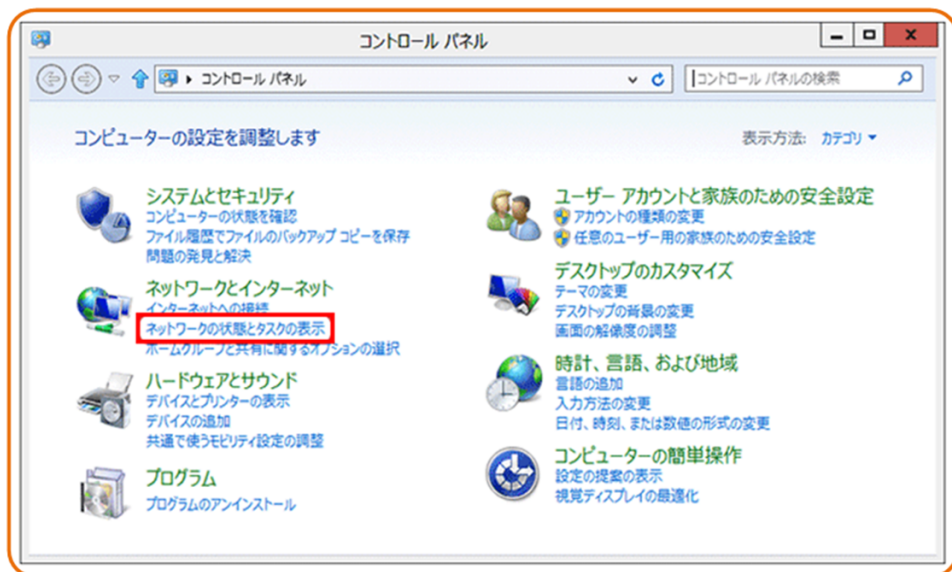
3. [設定]画面からコントロールパネルを選択します。

図 5-3 [コントロールパネル]ボタン



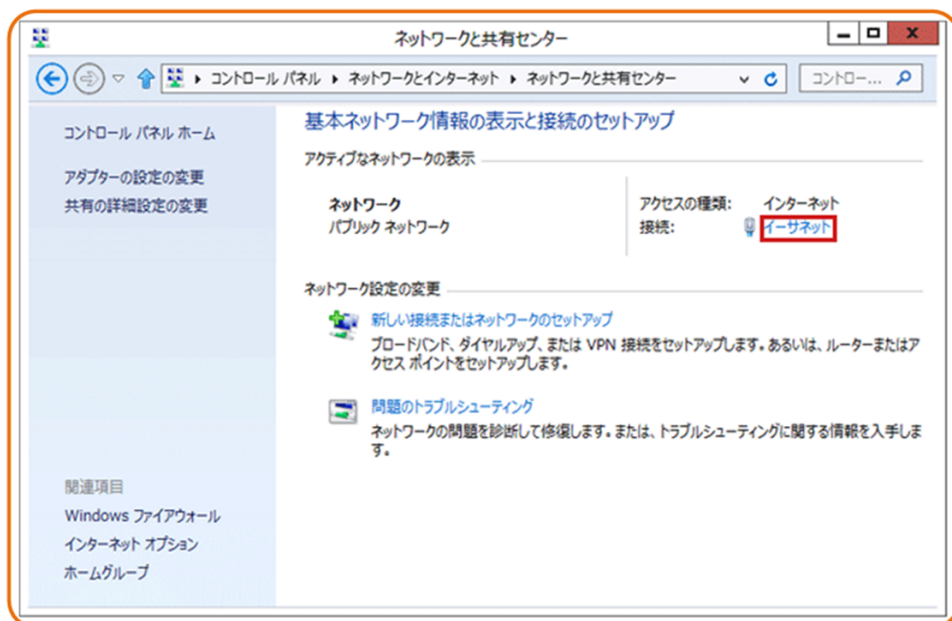
4. [コントロールパネル]を表示したら、図 5-4に示すように[ネットワークとインターネット]の下の[ネットワークの状態とタスクの表示]を選択します。

図 5-4 [コントロール パネル]ウィンドウ



5. [ネットワークの状態とタスクの表示]を選択したら、図 5-5に示すような[ネットワークと共有センター]ウィンドウが表示されます。

図 5-5 [ネットワークと共有センター]ウィンドウ



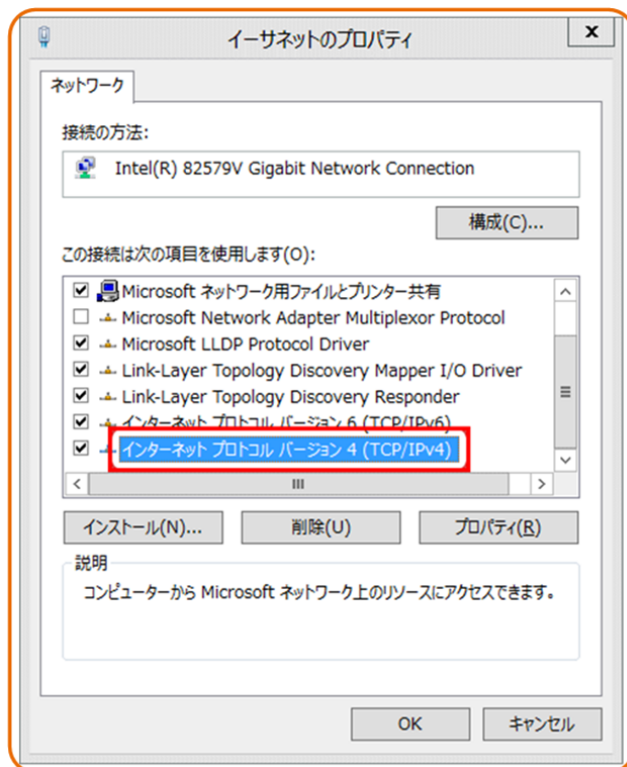
6. [アクティブなネットワークの表示]エリアの[イーサネット]を選択します。図 5-6に示すような[イーサネットの状態]ダイアログボックスが表示されます。

図 5-6 [イーサネットの状態]ウィンドウ



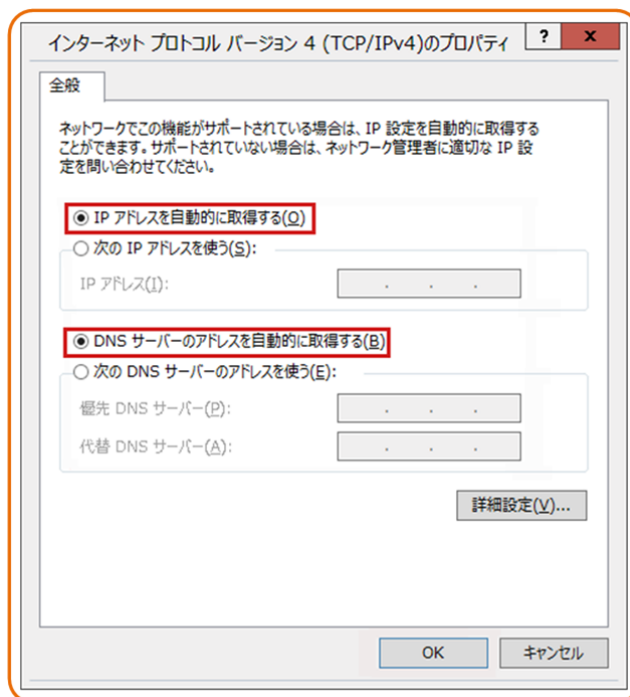
7. [プロパティ]を選択すると、図 5-7のような[イーサネットのプロパティ]ダイアログボックスが表示されます。

図 5-7 [イーサネットのプロパティ]ダイアログボックス



8. [ネットワーク]タブを選択して、[この接続は次の項目を使用します]リストボックス内の[インターネット プロトコル バージョン 4 (TCP/IPv4)]をダブル選択します。図 5-8 のような[インターネット プロトコル バージョン 4 (TCP/IPv4)のプロパティ]ダイアログボックスが表示されます。

図 5-8 [インターネット プロトコル バージョン 4 (TCP/IPv4)のプロパティ]ダイアログボックス



9. [全般]タブを選択して、図 5-8に示すような[IP アドレスを自動的に取得する]と[DNS サーバのアドレスを自動的に取得する]を選択します。
 10. [OK]を選択して設定を完了して、[イーサネットの状態]ダイアログボックスに戻ります。
 11. [OK]を選択して設定を完了します。
- Windows 7のケース


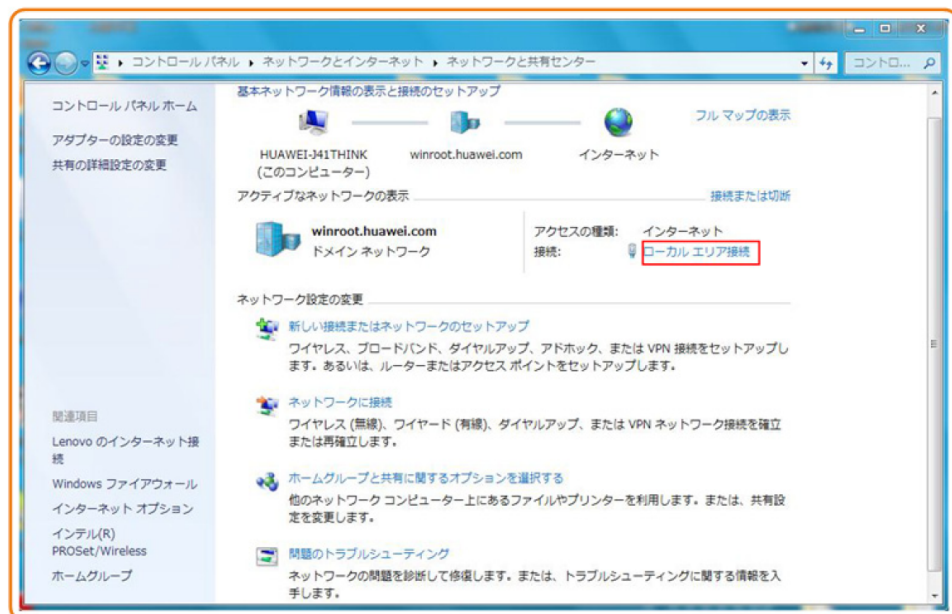
1. OSにログインした後、[スタートボタン](デスクトップの左下隅の  ボタン)を選択し、[コントロール パネル]を選択すると、図 5-9に示すような[コントロール パネル]ウィンドウが表示されます。

図 5-9 [コントロール パネル]ダイアログボックス



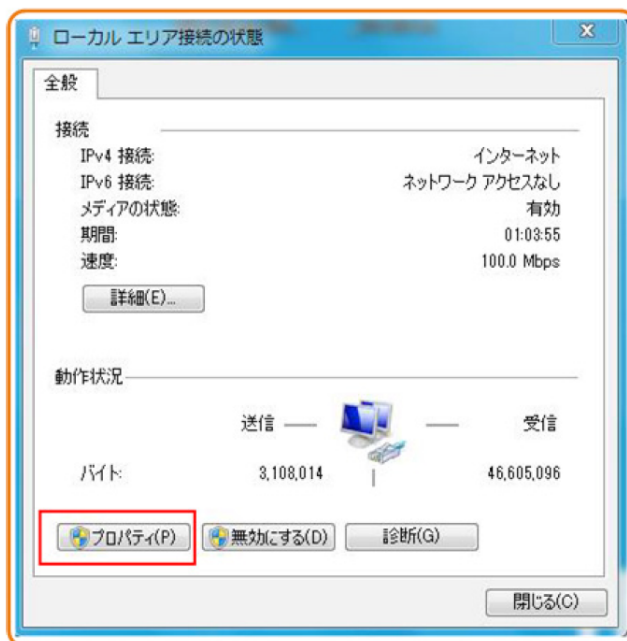
2. [ネットワークとインターネット]の下の[ネットワークの状態とタスクの表示]を選択します。図 5-10に示すような[ネットワークと共有センター]ウィンドウが表示されます。

図 5-10 [ネットワークと共有センター]ウィンドウ



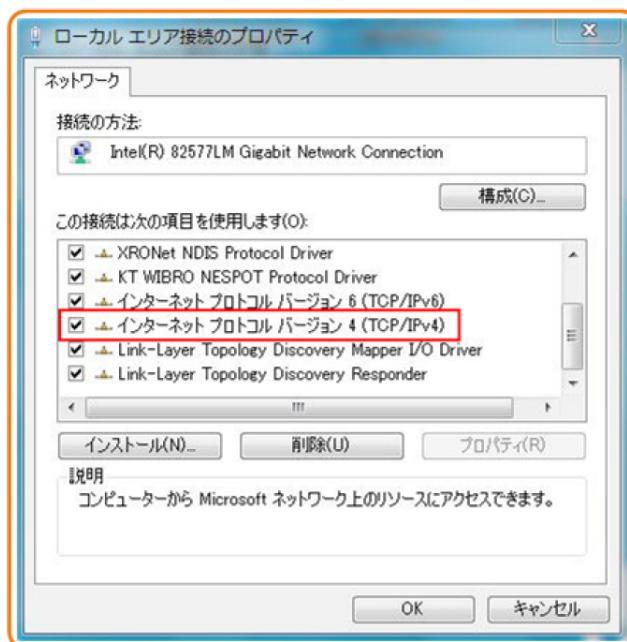
3. [アクティブなネットワークの表示]エリアの[ローカル エリア接続]を選択します。図 5-11に示すような[ローカル エリア接続の状態]ダイアログボックスが表示されます。

図 5-11 [ローカル エリア接続の状態]ダイアログボックス



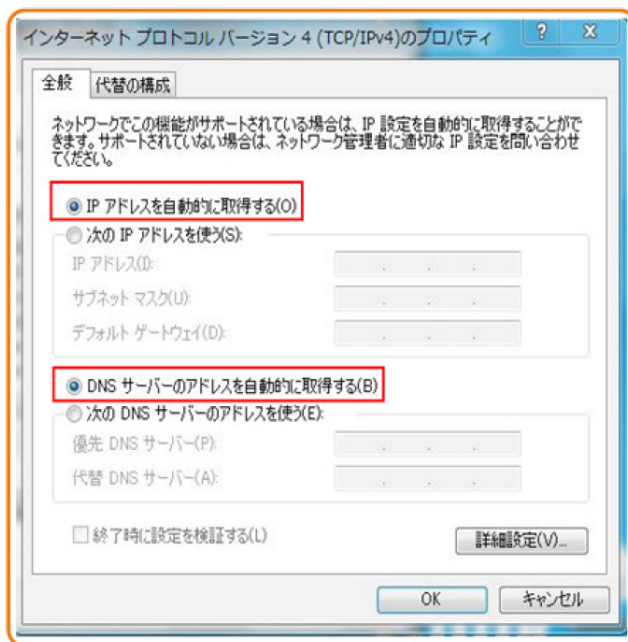
4. [プロパティ]を選択すると、図 5-12のような[ローカル エリア接続のプロパティ]ダイアログボックスが表示されます。

図 5-12 [ローカル エリア接続のプロパティ]ダイアログボックス



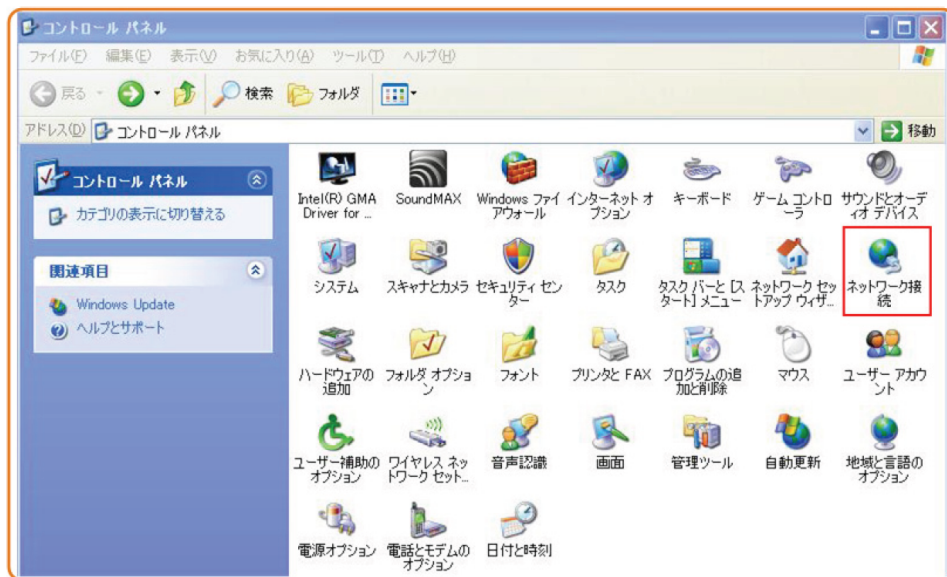
5. [ネットワーク]タブを選択して、[この接続は次の項目を使用します]リストボックス内の[インターネット プロトコル バージョン 4 (TCP/IPv4)]をダブル選択します。図 5-13のような[インターネット プロトコル バージョン 4 (TCP/IPv4)のプロパティ]ダイアログボックスが表示されます。
6. [全般]タブを選択して、図 5-13に示すような[IP アドレスを自動的に取得する]と[DNS サーバのアドレスを自動的に取得する]を選択します。

図 5-13 [インターネット プロトコル バージョン 4 (TCP/IPv4)のプロパティ]ダイアログボックス



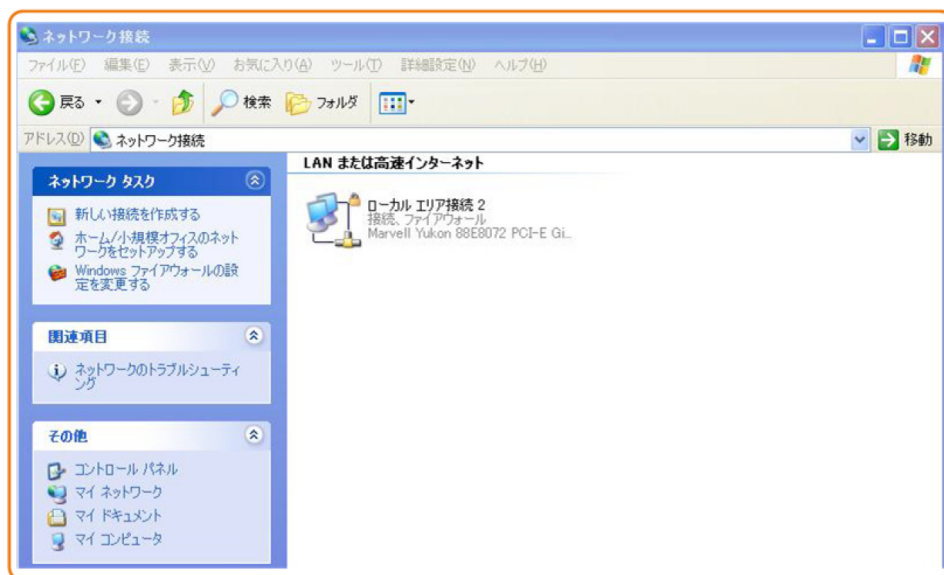
7. [OK]を選択して設定を完了して、[ローカルエリア接続の状態]ダイアログボックスに戻ります。
 8. [OK]を選択して設定を完了します。
- Windows XPのケース
 1. OSにログインした後、デスクトップの左下隅の[スタート]から[コントロール パネル]を選択すると、図 5-14のような[コントロール パネル]ウィンドウが表示されます。

図 5-14 [コントロール パネル]ダイアログボックス



2. [ネットワーク接続]をダブル選択すると、図 5-15のような[ネットワーク接続]ウィンドウが表示されます。

図 5-15 [ネットワーク接続]ウィンドウ



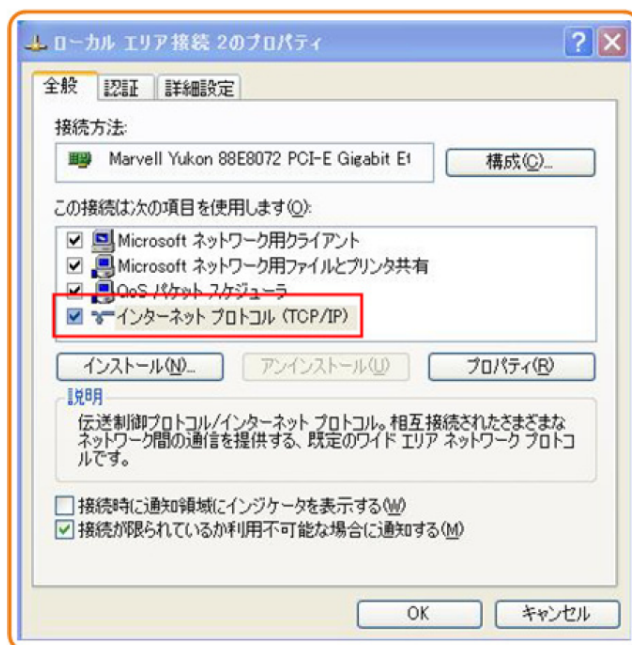
3. [ローカル エリア接続]をダブル選択すると、図 5-16のような[ローカル エリア接続の状態]ダイアログボックスが表示されます。

図 5-16 [ローカル エリア接続の状態]ダイアログボックス



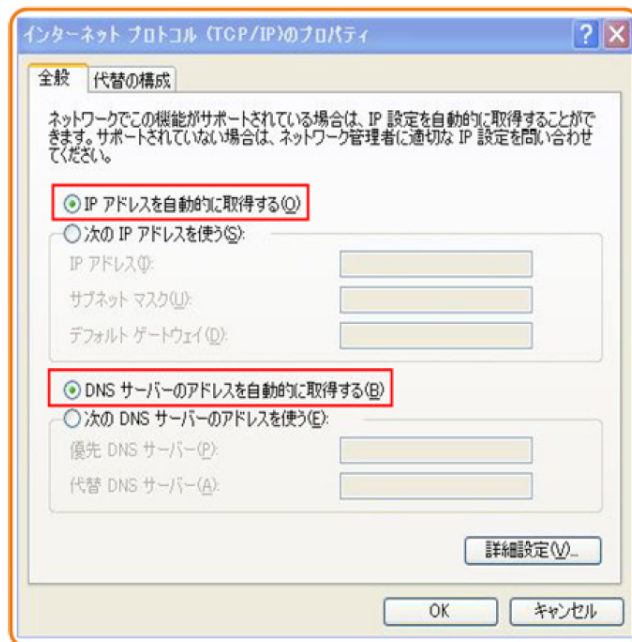
4. [全般]タブを選択して、[プロパティ]を選択します。図 5-17のような[ローカル エリア接続のプロパティ]ダイアログボックスが表示されます。

図 5-17 [ローカル エリア接続のプロパティ]ダイアログボックス



5. [全般]タブを選択して、[この接続は次の項目を使用します]リストボックス内の[インターネット プロトコル (TCP/IP)]をダブル選択します。図 5-18 のような[インターネット プロトコル (TCP/IP)のプロパティ]ダイアログボックスが表示されます。
6. [全般]タブを選択して、図 5-18 に示すような[IP アドレスを自動的に取得する]と[DNS サーバのアドレスを自動的に取得する]を選択します。

図 5-18 [インターネット プロトコル (TCP/IP)のプロパティ]ダイアログボックス



7. [OK]を選択して設定を完了して、[ローカル エリア接続のプロパティ]ダイアログボックスに戻ります。
8. [OK]を選択して設定を完了します。

- Mac OS X 10.8.2
 1. OSにログインした後、デスクトップ下部の[システム環境設定]を選択すると、[図 5-19](#)と[図 5-20](#)に示すような[システム環境設定]ウィンドウが表示されます。

図 5-19 [システム環境設定]ラベル

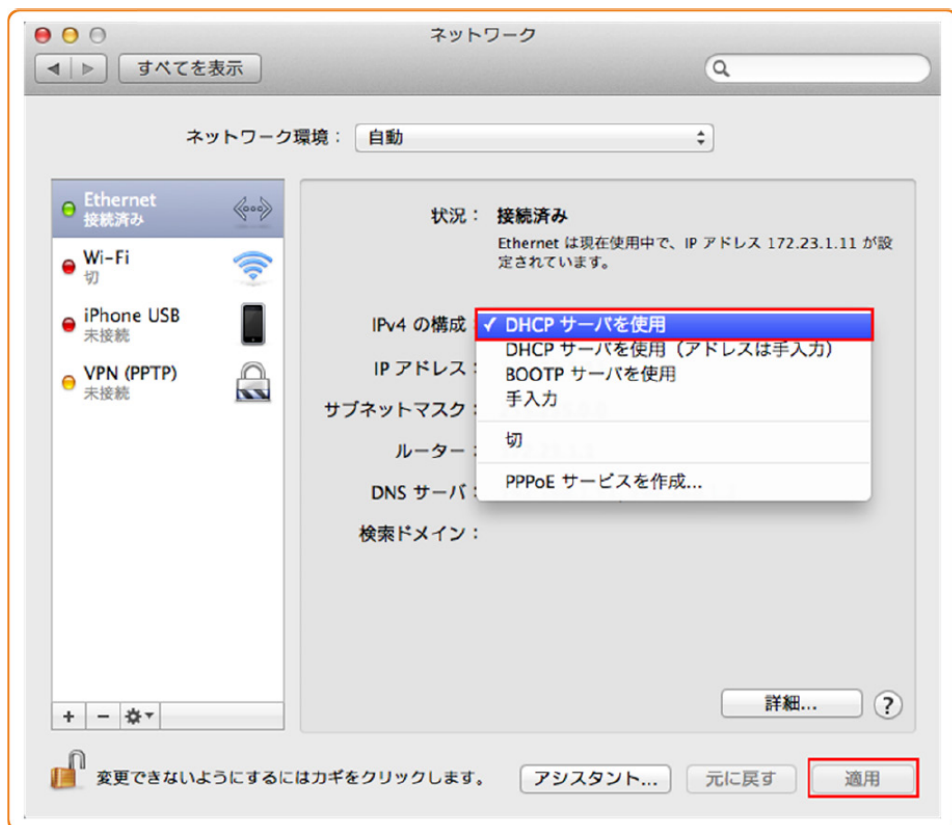


図 5-20 [システム環境設定]ウィンドウ



2. [インターネットとワイヤレス]エリアの[ネットワーク]を選択します。[図 5-21](#)に示すような[ネットワーク]ダイアログボックスが表示されます。
3. [図 5-21](#)に示すように[IPv4の構成]メニューから[DHCPサーバを使用]を選択し、[適用]を選択して設定を完了します。

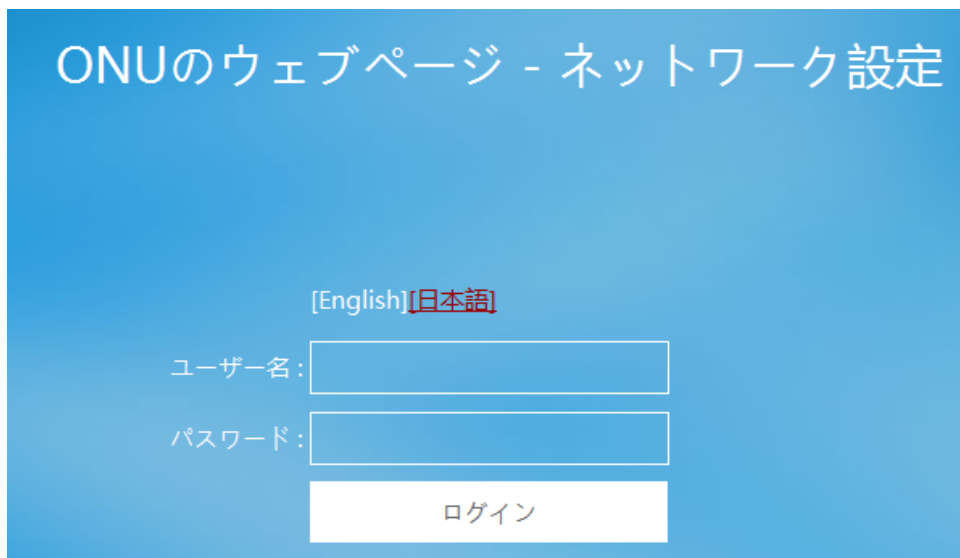
図 5-21 [ネットワーク]ダイアログボックス



ステップ 3 Webページにログインします。

1. WebブラウザのアドレスバーにHN8055Qの管理用IPアドレスを入力して、Enterを押します。ログイン画面が表示されます。デフォルトのIPアドレスは 192.168.1.1です。ログイン画面で言語を選択し、ユーザー名とパスワード(デフォルトのユーザー名: admin、デフォルトのパスワード: admin)を入力して、「ログイン」を選択します。

図 5-22 [ログイン画面]



2. 以下の画面で新しいパスワードを設定してください。

アカウント管理

このページでは、あなたが一般ユーザのログインパスワードを変更することができ、あなたがアクセス ONT HTTPS SSL証明書の認証用パスワードと、対応するインポートSSL証明書を設定することができます。

パスワードの変更

ユーザー名:	admin	1.パスワードは少なくとも6文字で設定してください。 2.パスワードは次の条件を少なくとも2つ組み合わせて設定してください。 数字、大文字、小文字 特殊文字 (~!@#\$%^&*()-_+=\ []{};:'"<.,>/?)。 3.パスワードにはユーザー名やユーザー名の順序を逆にしたものは使用できません。
新しいパスワード:	●●●●●●	
パスワードの確認:	●●●●●●	

証明書認証の有効化と秘密鍵パスワードの設定

証明書認証を有効にする:

秘密鍵パスワード: (1-127文字。このパスワードはデバイスを再起動すると有効になります。)

パスワードの確認: (1-127文字。このパスワードはデバイスを再起動すると有効になります。)

証明書のインポート

証明書:

6 Web ページでのインターネットアクセスサービスの設定

本章では、Webページでインターネットアクセスサービスを設定する方法の例を示します。

事前の要件

- Webページにログインしてサービス設定を行うための環境設定が完了しており、Webページへのログインに成功していること。詳細は、[5 管理画面へのログイン方法](#)をご参照ください。
- ユーザーPCがモジュラーケーブルでHN8055QのLANポートに接続されていること。詳細は、[4.2 電源ケーブルの接続およびボタン設定](#)をご参照ください。

はじめに

インターネットアクセスサービス: ONUのLAN1~3・10GE及び無線LANにて提供されます。この際のIPアドレスはONUのDHCP IPアドレスプールから割り当てられます。ONUは先ずキャリアネットワークに接続され、その後ルータモードで高速インターネットアクセスサービスを提供します。

手順

ステップ1 DHCPサーバのパラメータを設定します。

左側のナビゲーションツリーから[[詳細設定](#)] > [[LAN設定](#)] > [[DHCPサーバ設定](#)]を選択します。右側のメイン表示部分で、ゲートウェイとして機能するONTの、LAN側のDHCPアドレスプールを設定できます。設定後、[図 6-1](#)に示すように、LANポートに接続されたPCはアドレスプールからIPアドレスを自動的に取得できます。

図 6-1 DHCP サーバ設定

DHCPサーバ設定

このページでは、LAN側デバイスのDHCPサーバのパラメータを設定し、IPアドレスを取得することができます。

プライマリアドレスプール

プライマリDHCPサーバを有効にする:

DHCPリレーを有効にする:

Option125を有効にする:

LANホストIPアドレス: 192.168.1.1

サブネットマスク: 255.255.255.0

IPアドレスの開始: *(LANホストのIPアドレスと同一のサブネット上にある必要があります。)

IPアドレスの終了: *

リース時間: 時間

プライマリDNSサーバ:

セカンダリDNSサーバ:

セカンダリアドレスプール

セカンダリDHCPサーバを有効にする:

IPアドレス: 192.168.2.1

サブネットマスク: 255.255.255.0

IPアドレスの開始: *

IPアドレスの終了: *

リース時間: 日

Option 60: *

Option 43:

NTPサーバ:

プライマリDNSサーバ:

セカンダリDNSサーバ:

結果

インターネットアクセスサービス: PCはDHCPモードでONUによって割り当てられたIPアドレスを自動で取得します。IPアドレスを正常に取得すると、ユーザはインターネットにアクセスできるようになります。

7 Web ページでの Wi-Fi アクセスサービスの設定

本章では、WebページでWi-Fiアクセスサービスを設定する方法の例を示します。

事前の要件

- Webページにログインしてサービス設定を行うための環境設定が完了しており、Webページへのログインに成功していること。詳細は、[5 管理画面へのログイン方法](#)をご参照ください。
- Wi-Fi機能を搭載した端末が用意されていること。

はじめに

Wi-Fiワイヤレスアクセスサービスは、レイヤ3ルーティングWi-Fiサービスです。

サービスセットID (SSID) 検索がPC上で実行されます。認証に成功すると、PCはONUのDHCPアドレスプールからIPアドレスを割当てられます。

HN8055Qは2.4GHzおよび5GHz Wi-Fi機能をサポートします。2.4GHz Wi-Fiと5GHz Wi-Fiの設定方法は同じです。本書では例として、2.4GHz Wi-Fiの設定を使用します。

手順

ステップ 1 2.4GHz Wi-Fiサービスを設定します。

左側のナビゲーションツリーから[[詳細設定](#)] > [[WLAN](#)] > [[2.4G基本ネットワーク設定](#)]を選択します。右側のメイン表示部分で、[図 7-1](#)に示すように、2.4G Wi-Fiネットワークの基本パラメータを設定します。

図 7-1 2.4G 基本ネットワーク設定

2.4G基本ネットワーク設定

このページでは、2.4GHz帯ワイヤレスネットワークの基本パラメータの設定ができます。2.4GHz帯ワイヤレスネットワークが無効化されている場合、このページは空白です。

警告:

- ワイヤレスネットワークパラメータを変更するとワイヤレスネットワークサービスが一時的に中断される可能性があります。
- セキュリティ保護のため、WPA2または WPA/WPA2認証モードを使用することをお勧めします。

WLANの有効化

新規作成 削除

	SSIDインデックス	SSID名	SSIDの状態	接続デバイス数	SSIDのブロードキャスト	セキュリティ設定
<input type="checkbox"/>	1	Huawei-XXXX-XXXX	有効	32	有効	設定済み

SSID設定詳細

SSID名: * (1-32文字)

SSIDの有効化:

接続デバイス数: * (1-32)

SSIDのブロードキャスト:

WMMの有効化:

認証モード:

暗号化モード:

WPA PreSharedKey: 非表示 *(8-63文字または64文字(16進文字))

WPAグループキー更新間隔: *(600 ~ 86400秒)

WPSを有効にする:

WPSモード:


PBC:

表 7-1で、2.4G基本ワイヤレスネットワーク設定について説明します。

表 7-1 2.4G 基本ワイヤレスネットワーク設定

パラメータ	説明
WLANの有効化	ワイヤレスネットワークを有効にするかどうかを指定します。以下のパラメータは、ワイヤレスネットワークが有効になっている場合にのみ設定できます。
SSID名	ワイヤレスネットワークの名前を指定します。これは、各種ワイヤレスネットワークを区別するために使用されます。タブ文字無しで、最大32文字から構成されます。
SSIDの有効化	接続を有効にするかどうかを指定します。
接続デバイス数	STAの数を指定します。1 ~ 32の範囲で指定します。
SSIDのブロードキャスト	ブロードキャストを有効にするか非表示にするかを指定します。 <ul style="list-style-type: none"> ● このオプションボックスを選択した場合、SSIDのブロードキャスト機能が有効になるように指定されます。ONTは、SSID、すなわちワイヤレスネットワークの名前を定期的にブロードキャストします。このような方法で、STAはワイヤレスネットワークを検索できます。 ● このオプションボックスを選択しなかった場合は、SSIDのブロードキャスト機能が無効になるように指定されます。SSIDを非表示にすると、STAはワイヤレスネットワークを検索できなくなり、SSIDは要求しない限り取得できなくなります。
WMMの有効化	Wi-Fiマルチメディアを有効にするかどうかを指定します。
認証モード	ワイヤレスネットワークへのアクセスを要求するSTAの認証モードを指定します。このモードは、オープン、共有、WPA Pre-Shared Key、WPA2 Pre-Shared Key、WPA/WPA2 Pre-Shared Key、WPAエンタープライズ、WPA2エンタープライズ、WPA/WPA2エンタープライズから指定できます。これは、デフォルトでは、WPA/WPA2 Pre-Shared Keyに設定されています。
暗号化モード	ワイヤレスネットワークへのアクセスを要求するSTAの暗号化モードを指定します。暗号化モードと暗号化パラメータは、認証モードによって異なります。 <ul style="list-style-type: none"> ● 認証モードがオープンに設定されている場合、暗号化モードはNoneまたはWEPに設定できます。 ● 認証モードが共有に設定されている場合、暗号化モードはWEPに設定できます。 ● 認証モードがWPA Pre-Shared Key、WPA2 Pre-Shared Key、WPA/WPA2 Pre-Shared Key、WPAエンタープライズ、WPA2エンタープライズ、WPA/WPA2エンタープライズに設定されている場合、暗号化モードはAES、TKIP、TKIP&AESに設定できます。

パラメータ	説明
WPA PreSharedKey	WPA共有キーを指定します。有効な値は、8 ~ 63のASCIIコードまたは64の16進数字から構成されます。
WPAグループキー更新 間隔	WPAグループキーを生成する間隔を指定します。単位は秒です。有効な値の範囲は600 ~ 86400です。
WPSを有効にする	WPSを有効にするかどうかを指定します。
WPSモード	WPSモードを指定します。有効な値は、PBC、PIN、AP-PINです。
PBC	WPSモードがPBCに設定されている場合は、WPSを起動を選択してPBCモードを開始することができます。

左側のナビゲーションツリーから[詳細設定] > [WLAN] > [2.4G詳細ネットワーク設定]を選択します。右側のメイン表示部分で、 7-2に示すように、2.4G Wi-Fiネットワークの拡張パラメータを設定します。



[WLANの有効化]が[2.4G基本ネットワーク設定]で選択されていない場合、このページは空白になります。

図 7-2 2.4G 詳細ネットワーク設定

2.4G詳細ネットワーク設定

このページでは、2.4GHz帯ワイヤレスネットワークの拡張パラメータの設定ができます。2.4GHz帯ワイヤレスネットワークが無効化されている場合、このページは空白です。

⚠警告:
ワイヤレスネットワークパラメータを変更するとワイヤレスネットワークサービスが一時的に中断される可能性があります。

詳細設定

送信出力:	<input type="text" value="100%"/>	
規制区域:	<input type="text"/>	
チャンネル:	<input type="text" value="自動"/>	
チャンネル幅:	<input type="text" value="Auto 20/40 MHz"/>	
モード:	<input type="text" value="802.11b/g/n"/>	
DTIM間隔:	<input type="text" value="1"/>	(1~255、デフォルト: 1)
ビーコン間隔:	<input type="text" value="100"/>	(20~1000ミリ秒、デフォルト: 100)
RTS閾値:	<input type="text" value="2346"/>	(1~2346バイト、デフォルト: 2346)
フラグメント閾値:	<input type="text" value="2346"/>	(256~2346バイト、デフォルト: 2346)

表 7-2で、ワイヤレスネットワークの拡張パラメータについて説明します。

表 7-2 ワイヤレスネットワークの拡張パラメータ

パラメータ	説明
送信出力	無線信号の送信光出力を指定します。これは、20%、40%、60%、80%、100%に設定できます。値が大きくなればなるほど、無線信号のカバレッジが向上します。
チャンネル	ワイヤレスネットワークのチャンネルを指定します。チャンネルは、自動の値によって異なります。
チャンネル幅	無線のチャンネル幅を指定します。これは、Auto 20/40 MHz、20 MHz、40 MHz、Auto 20/40/80 MHzに設定できません。

パラメータ	説明
モード	サポートされるワイヤレスネットワークモードを指定します。これは、802.11b、802.11g、802.11b/g、802.11b/g/nに設定できます。
DTIM間隔	DTIMの送信間隔を指定します。値の範囲は1 ~ 255で、デフォルト値は1です。
ビーコン間隔	ビーコンの送信間隔を指定します。ビーコンは、他のアクセスポイントデバイスまたはネットワーク制御デバイスとの通信に使用されます。値の範囲は20ms ~ 1000msで、デフォルト値は100msです。
RTS閾値	送信要求(RTS)の閾値を指定します。これは、無線LANのデータ伝送での競合を回避するために使用されます。 RTS閾値が小さければ小さいほど、RTSパケットの伝送周波数が高くなり、中断や競合からのシステム復旧が早くなります。ただし、使用される帯域幅が大きくなり、これは他のネットワークデータパケットのスループットに影響します。 値の範囲は1バイト ~ 2346バイトで、デフォルト値は2346バイトです。
フラグメント閾値	フラグメント閾値を指定します。パケットのサイズがこの閾値よりも大きい場合、パケットは分割されます。フラグメントの伝送が中断されると、正常に伝送されなかった部分のみ、再伝送される必要があります。 値の範囲は256バイト ~ 2346バイトで、デフォルト値は 2346バイトです。

ステップ2 2.4GHz Wi-Fi 接続のステータスを確認します。

左側のナビゲーションツリーから[システム情報] > [WLAN情報]を選択します。それにより、右側のメイン表示部分で、WLAN情報、WLAN/パケット統計情報、SSID情報などの情報を、[図 7-3](#)に示すように照会できます。

図 7-3 WLAN 情報

WLAN情報

このページではWLAN情報、WLANパケット統計情報、SSID情報を照会することができます。

2.4GHz帯ワイヤレスネットワーク情報
 5GHz帯ワイヤレスネットワーク情報

WLAN情報

WLANステータス: 有効

WLANチャンネル: 36

WLANパケット統計情報

SSIDインデックス	SSID名	受信(RX)				送信(TX)			
		バイト	パケット	エラー	削除済み	バイト	パケット	エラー	削除済み
5	Sonet-5G	125748945	2306565	0	0	2207947641	4630866	343	0

SSID情報

SSIDインデックス	SSID名	セキュリティ設定	認証モード	暗号化モード
5	Sonet-5G	設定済み	WPA/WPA2 PreSharedKey	TKIP&AES

STA情報

検索

MACアドレス	SSID名	接続時間(秒)	送信速度(Mbit/s)	受信速度(Mbit/s)	信号強度(dBm)	ノイズ(dBm)	S/N比(dB)	信号品質(dBm)
---------	-------	---------	--------------	--------------	-----------	----------	----------	-----------

近くのアクセスポイント情報

検索

注記: 近くのAP情報を検索すると全ての局接続が切断される可能性があります。

SSID名	MACアドレス	ネットワークの種類	チャンネル	信号強度(dBm)	ノイズ(dBm)	DTIM間隔	ビーコン間隔(ms)	認証モード	作業モード	最大速度(Mbit/s)
-------	---------	-----------	-------	-----------	----------	--------	------------	-------	-------	--------------

結果

レイヤ3ルーティングWi-Fiサービス: SSID無線信号はPCによって検出できます。ユーザーが認証キーを入力し、認証に成功すると、PCはONUのDHCP IPアドレスプールから割り当てられたIPアドレスを取得できます。アドレス割り当てが正常に実行されると、ユーザーはインターネットにアクセスできます。



注記

Wi-Fi端末に設定するセキュリティモードおよび暗号化モードは、ONUのセキュリティモードおよび暗号化モードと同じでなければなりません。Wi-Fi端末にTKIP&AESまたはAES暗号化モードがない場合、Wi-Fi端末のWi-Fiドライバが初期バージョンのものである可能性があります。このような場合、ドライバをバージョンアップしてください。

8 Web ページのリファレンス

本章について

ここでは、Webページのパラメータの使用方法と意味について説明します。

Webページのパラメータを設定したり表示したりするには、Webページにログインします。Webページへのログイン方法についての詳細は、[5 管理画面へのログイン方法](#)をご参照ください。

8.1 高速設定

ここでは、ONTを簡単に設定する方法について説明します。

8.2 ホームページ

ここでは、Wi-Fi設定、宅内共有、ネットワーク状態の確認など、ONTの共通設定について説明します。

8.3 ワンクリック診断

ここでは、ONTのネットワーク障害を迅速に診断する方法について説明します。ワンクリック診断の動作中は、ONUの処理が重くなる場合があります。ONUの正常動作時は使用しないでください。

8.4 システム情報

ここでは、WebページからWANインターフェース、Wi-Fiポートに関する情報を照会する方法について説明します。

8.5 詳細設定

ここでは、次のような詳細な設定の実行方法について説明します：[LAN設定](#)、[セキュリティ設定](#)、[転送ルール](#)、[アプリケーション](#)、[WLAN](#)、[システム管理](#)、[保守診断](#)

8.1 高速設定

ここでは、ONTを簡単に設定する方法について説明します。

1. ホームページの右上部の[高速設定]をクリックします。表示されたページ(図 8-1)で、[OLT]、[EMS]、[ACS]、[ONUのウェブページ]を選択して、ONTのサービスプロビジョニング方法を指定できます。

図 8-1 高速設定



2. サービスプロビジョニング方法を選択したら、図 8-2に示すように[次へ]をクリックします。

図 8-2 高速設定 - ONT 認証



図 8-3 高速設定 - WAN 設定

ONU - 家族や友人への接続

ONU認証



WAN設定



設定完了



新規作成 削除

	接続名	VLAN/優先度	プロトコルの種類
<input type="checkbox"/>	1_TR069_INTERNET_R_VID_10	10/0	IPv4/IPv6
<input type="checkbox"/>	2_INTERNET_B_VID_1001	1001/0	IPv6

基本情報

WANを有効にする:

カプセル化方法: IPoE PPPoE

プロトコルの種類:

WANの種類:

サービスの種類:

VLANを有効にする:

VLAN ID: *(1-4094)

802.1pポリシー: 指定の値を使用する IP Precedenceからコピーする

802.1p優先:

バインディングオプション: LAN1 LAN2 LAN3 LAN4 LAN5
 SSID1 SSID2 SSID3 SSID4 SSID5 SSID6 SSID7 SSID8

IPv6情報

マルチキャストVLAN ID: (1-4094)



注記
ONTのWebページのみでONT WAN設定が可能です。

図 8-4 高速設定 - 設定完了



設定が完了したら、サービスは自動的にONTに対してプロビジョニングされます。プロビジョニング中に、[ホームページに戻る]をクリックすると、ホームページに移動できます。



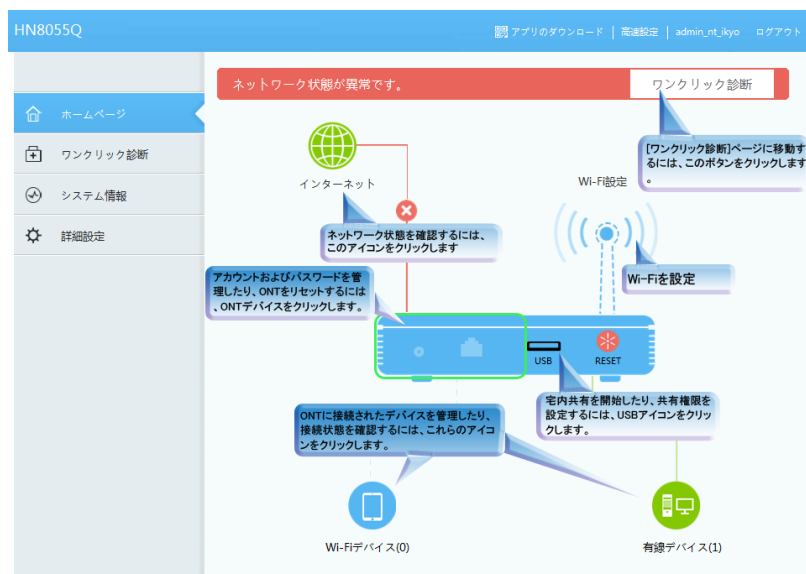
- 設定をスキップする場合は、[スキップ]をクリックして次の設定に移動します。
- [ONT認証]および[WAN設定]の設定方法については、[8.5.8.4 ONT認証](#)および[8.5.1 WAN設定](#)をご参照ください。

8.2 ホームページ

ここでは、Wi-Fi設定、宅内共有、ネットワーク状態の確認など、ONTの共通設定について説明します。

1. ONTにログインすると、[図 8-5](#)が表示されます。このページでは、ネットワーク接続状態、音声サービス情報、デバイスの接続情報などを確認できます。さらに、ページ上のONTデバイスをクリックすると、通常ユーザーのログインパスワードを変更できます。ネットワーク接続に異常がある場合、ページの右上部にメッセージが表示されます。この場合、[ワンクリック診断]ページに移動して、ネットワークの障害を診断できます。以下の図はONTの詳細な機能を示しています。

図 8-5 ホームページ



2. ページの右上部のボタン([アプリのダウンロード]、[高速設定]など)から様々なページに移動できます。

8.3 ワンクリック診断

ここでは、ONTのネットワーク障害を迅速に診断する方法について説明します。ワンクリック診断の動作中は、ONUの処理が重くなる場合があります。ONUの正常動作時は使用しないでください。

1. 左側のナビゲーションツリーから、[ワンクリック診断]を選択します。次に、右側のページの[ワンクリック診断]をクリックして、図 8-6に示すようにネットワーク状態を診断します。

図 8-6 ワンクリック診断



2. 図 8-7は診断結果を示しています。

図 8-7 診断結果



障害を再診断する必要がある場合、[再診断]をクリックします。

8.4 システム情報

ここでは、WebページからWANインターフェース、Wi-Fiポートに関する情報を照会する方法について説明します。

8.4.1 デバイス情報

左側のナビゲーションツリーから[システム情報] > [デバイス情報]を選択します。右側のメイン表示部分に、図 8-8に示すように、製品名、ハードウェアのバージョン、ソフトウェアのバージョンが表示されます。

図 8-8 デバイス情報

デバイス情報	
このページでは基本デバイス情報を表示することができます。	
デバイスの種類:	HN8055Q
種類:	EchoLife HN8055Q XG_PON Terminal (N2a/PRODUCT ID:0000000001)
SN:	6877687700000001 (hwhw00000001)
ハードウェアバージョン:	788.A
ソフトウェアバージョン:	V3R016C005007
製造情報:	.00020000000000000000000001
ONT登録ステータス:	0%(未登録)
ONT ID:	0
CPU使用率:	1%
メモリ使用率:	20%
カスタマイズ情報:	SONET
システム時間:	05/22/2015 09:14



図 8-8は、例として使用されています。照会結果は、実際の状況によって異なります。

8.4.2 WAN 情報

左側のナビゲーションツリーから[システム情報] > [WAN情報]を選択します。右側のメイン表示部分に、図 8-9に示すように、WANインターフェース、IPアドレスを取得する方法、IPアドレス、サブネットマスクが表示されます。

図 8-9 WAN 情報

WAN情報

このページでは、WANポートの接続と回線の状態を確認することができます。

IPv4情報

WAN名	状態	IPアドレス	VLAN/優先度	接続
1_TR069_INTERNET_R_VID_1290	接続	171.240.99	1290/0	AlwaysOn

WAN情報

MACアドレス: 00:25:9E:23:33:49

VLAN: 1290

ポリシー: 指定値を使用

優先度: 0

NAT: 有効

IP取得方法: DHCP

IPアドレス/サブネットマスク: 171.240.99/255.255.255.0

ゲートウェイ: 171.240.254

DNSサーバ: 10.11.10.1,10.11.11.1

リース時間: 180 秒

残りのリース時間: 109 秒

NTPサーバ:

タイムゾーン情報:

スタティックルート:

24.11.11.1/32>171.240.254 24.11.11.2/32>171.240.254
 34.11.11.1/32>171.2.20.254 12.11.11.1/32>171.2.20.254
 13.11.11.1/32>171.2.20.254 17.11.11.1/32>171.2.20.254
 19.11.11.1/32>171.2.20.254 20.11.11.1/32>171.2.20.254
 22.11.11.1/32>171.2.20.254

ベンダー情報:

接続時間 (dd:hh:mm:ss): 00:03:13:31



WANリストのレコードを選択します。WANリストのレコードを選択すると、詳細が表示されます。

8.4.3 光学情報

左側のナビゲーションツリーから[システム情報] > [光学情報]を選択します。右側のメイン表示部分に、図 8-10に示すように、光モジュールの光ステータス、送信光出力、受信光出力が表示されます。

図 8-10 光学情報

光学情報		
このページでは光モジュールの情報を照会することができます。		
ONT情報		
	現在値	参考値
光信号送信ステータス:	--	自動
送信光出力:	-- dBm	2~7dBm
受信光出力:	-- dBm	-28~-8dBm
動作電圧:	3261 mV	3100~3500mV
バイアス電流:	5 mA	0~90mA
動作温度:	42 °C	-10~+85°C
OLT情報		
	現在値	参考値
光モジュールの種類:	--	--
送信光出力:	-- dBm	--
PONポート識別子:	--	--

8.4.4 サービスプロビジョニングステータス

左側のナビゲーションツリーから[システム情報] > [サービスプロビジョニングステータス]を選択します。右側のペインで、図 8-11に示すようにONTサービスプロビジョニング状態が表示されます。

図 8-11 サービスプロビジョニングステータス

サービスプロビジョニングステータス	
このページではサービスプロビジョニングのステータスを照会することができます。	
ONT登録ステータス:	ONTがOLTに登録されました。
OLTサービス設定ステータス:	OLTサービスが設定されました。
EMS設定ステータス:	XML設定が適用されていません。
ACS登録ステータス:	ACSサーバにONTを登録中です。しばらくお待ちください。
<input type="button" value="更新"/>	

8.4.5 Eth ポート情報

左側のナビゲーションツリーから[システム情報] > [Ethポート情報]を選択します。右側のメイン表示部分に、[図 8-12](#)に示すように、Ethポートのデュプレックスモード、速度、ステータスが表示されます。

図 8-12 Eth ポート情報

Ethポート情報							
このページではユーザー側のイーサネットポート情報を照会することができます。							
イーサネットポートのステータス							
ポート	ステータス			受信(RX)		送信(TX)	
	モード	速度	リンク	バイト	パケット	バイト	パケット
1	半二重	10 Mbit/s	ダウン	0	0	19171	169
2	半二重	10 Mbit/s	ダウン	0	0	19171	169
3	全二重	1000 Mbit/s	アップ	1560222	8275	10193988	11232
4	半二重	10 Mbit/s	ダウン	0	0	0	0
5	半二重	100 Mbit/s	ダウン	0	0	19171	169

8.4.6 WLAN 情報

左側のナビゲーションツリーから[システム情報] > [WLAN情報]を選択します。その後、右側のメイン表示部分で、[図 8-13](#)に示すように、Wi-Fiポートステータス、Wi-Fiパケット統計、SSIDなどの情報を照会することができます。

図 8-13 WLAN 情報

WLAN情報

このページではWLAN情報、WLANパケット統計情報、SSID情報を照会することができます。

2.4GHz帯ワイヤレスネットワーク情報
 5GHz帯ワイヤレスネットワーク情報

WLAN情報

WLANステータス: 有効

WLANチャンネル: 36

WLANパケット統計情報

SSIDインデックス	SSID名	受信(RX)				送信(TX)			
		バイト	パケット	エラー 済み	エラー 済み	バイト	パケット	エラー 済み	エラー 済み
5	Sonet-5G	125748945	2306565	0	0	2207947641	4630866	343	0

SSID情報

SSIDインデックス	SSID名	セキュリティ設定	認証モード	暗号化モード
5	Sonet-5G	設定済み	WPA/WPA2 PreSharedKey	TKIP&AES

STA情報

検索

MACアドレス	SSID名	接続時間(秒)	送信速度(Mbit/s)	受信速度(Mbit/s)	信号強度(dBm)	ノイズ(dBm)	S/N比(dB)	信号品質(dBm)

近くのアクセスポイント情報

検索 注記：近くのAP情報を検索すると全ての再接続が切断される可能性があります。

SSID名	MACアドレス	ネットワークの種類	チャンネル	信号強度(dBm)	ノイズ(dBm)	DTIM間隔	ビーコン間隔(ms)	認証モード	作業モード	最大速度(Mbit/s)

8.4.7 スマート WiFi カバレッジ

左側のナビゲーションツリーから[システム情報] > [スマートWiFiカバレッジ]を選択します。
 図 8-14に示すように、右側のペインから、デバイス状態、統計情報、WiFiネットワーク内の外部APの隣接AP情報を確認します。

図 8-14 スマート WiFi カバレッジ

スマートWiFiカバレッジ

このページでは、WiFiネットワークにおけるデバイス状態、統計情報、隣接AP情報を照会できます。

オンライン外部AP

モデル	シリアル番号	ハードウェアバージョン	ソフトウェアバージョン	オンライン時間	動作モード	接続モード	SSID接続	キャンセル	送信電力
--	--	--	--	--	--	--	--	--	--

外部APからアクセスされたWiFiデバイス			外部APの隣接情報			外部APのWiFi統計		
SSID名	MACアドレス	接続時間(秒)	受信速度(Mbit/s)	送信速度(Mbit/s)	信号強度(dBm)	ノイズ(dBm)	S/N比(dB)	信号品質(dBm)
--	--	--	--	--	--	--	--	--

8.5 詳細設定

ここでは、次のような詳細な設定の実行方法について説明します：**LAN設定**、**セキュリティ設定**、**転送ルール**、**アプリケーション**、**WLAN**、**システム管理**、**保守診断**

8.5.1 WAN 設定

1. 左側のナビゲーションツリーから[**詳細設定**] > [**WAN設定**]を選択します。右側のメイン表示部分で、WAN設定情報が 図 8-15 に示すように表示されます。

図 8-15 WAN 設定

WAN設定

このページではWANポートパラメータの設定ができます。ONT(ホームゲートウェイ)はWANポートを使用して上位レイヤのネットワーク機器と通信します。そのため、これらのパラメータはONTとネットワーク機器間で一致している必要があります。

	接続名	VLAN/優先度	プロトコルの種類
<input type="checkbox"/>	1_TR069_INTERNET_R_VID_10	10/0	IPv4/IPv6

基本情報

WANを有効にする:

カプセル化方法: IPoE PPPoE

プロトコルの種類:

WANの種類:

サービスの種類:

VLANを有効にする:

VLAN ID: *(1-4094)

802.1pポリシー: 指定の値を使用する IP Precedenceからコピーする

802.1p優先:

MTU: (1280-1540)

バインディングオプション:
 LAN1 LAN2 LAN3 LAN4 LAN5
 SSID1 SSID2 SSID3 SSID4 SSID5 SSID6 SSID7 SSID8

IPv4情報

IP取得方法: スタティック DHCP PPPoE

NATを有効にする:

NATの種類:

ベンダーID: (ベンダーIDは0-64文字で構成されます。)

ユーザーID: (オプション61、範囲0-64)

マルチキャストVLAN ID: (1-4094)

IPv6情報

プレフィックス取得方法: DHCPv6-PD スタティック None

IP取得方法: DHCPv6 自動 スタティック None

予約済みプレフィックスアドレス: (例::FFFF:0:FF:FF00:1)

マルチキャストVLAN ID: (1-4094)

2. [適用]をクリックします。

表 8-1 で、ルートモードのWANに関するパラメータについて説明します。パラメータのうち。

表 8-1 ルートモードの WAN に関するパラメータ

パラメータ	説明
WANを有効にする	WAN接続を有効にするかどうかを指定します。
カプセル化方法	WANインターフェースのカプセル化方法を指定します。
プロトコルの種類	WANインターフェースのプロトコルの種類を指定します。
サービスの種類	WANインターフェースのサービスの種類を指定します。
MTU	IPoEパケットの最大伝送単位(MTU)を指定します。
IPv4情報	
IP取得方法	ONT上でIPv4アドレスを取得する方法を指定します。これは、 DHCP 、 スタティック または PPPoE に設定できます。
NATを有効にする	NAT機能を有効にするかどうかを指定します。
NATの種類	NATの種類を指定します。これは、 [ポート制限コーンNAT] または [フルコーンNAT] に設定できます。このパラメータは、NAT機能が有効になっている場合にのみ設定します。 <ul style="list-style-type: none">● [ポート制限コーンNAT]: 内部アドレスAが外部アドレスBにマップされた後、Aが以前にパケットをホストに送信したことがある場合に限り、外部ホストはパケットをBに送信することによってAに送信できます。ホストによって送信されたメッセージ内の送信元IPおよびポート番号は、以前Aによって送信されたメッセージの送信先IPおよびポート番号と同じである必要があります。● [フルコーンNAT]: 内部アドレスAが外部アドレスBにマップされた後、外部ホストはパケットを Bに送信することによってAに送信できます。
IPv6情報	
プレフィックス取得方法	プレフィックス取得方法を指定します。これは、 DHCPv6-PD 、 自動 、 スタティック 、 RA 、 なし に設定できます。
IP取得方法	IP取得方法を指定します。これは、 DHCPv6 、 自動 、 スタティック 、 なし に設定できます。
予約済みプレフィックスアドレス	IPv6アドレスのプレフィックスを指定します。

8.5.2 LAN 設定

ここでは、WebページでのDHCPパラメータの設定方法について説明します。

8.5.2.1 レイヤ 2/3 ポート設定

1. 左側のナビゲーションツリーから[詳細設定] > [LAN設定][レイヤ2/3ポート設定]を選択します。右側のペインで、**図 8-16**に示すようにLANポートがレイヤ3モードで動作するかを指定します。

図 8-16 レイヤ 2/3 ポート設定



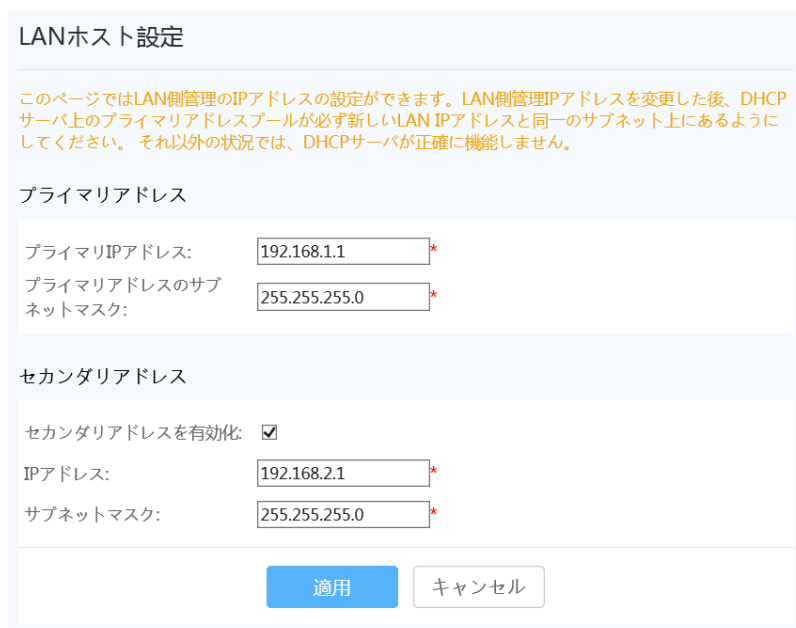
注記
LANポートに対応するチェックボックスを選択すると、LANポートがレイヤ3モード(ゲートウェイモード)で動作します。LANポートに対応したチェックボックスの選択を解除すると、LANポートがレイヤ2モード(ブリッジモード)で動作します。

2. [適用]をクリックします。

8.5.2.2 LAN ホスト設定

1. 左側のナビゲーションツリーから[詳細設定] > [LAN設定] > [LANホスト設定]を選択します。右側のメイン表示部分で、**図 8-17**に示すように、LANホストの管理IPアドレスおよびサブネットマスクを設定します。

図 8-17 LAN ホスト設定





注記

LANポートに接続されているデバイスのIPアドレスは、管理IPアドレスと同一のサブネットにある必要があります。こうすることによって、WebページからONTにアクセスし、照会と管理を行うことができます。LANポートに接続されているデバイスのIPアドレスが管理IPアドレスと同一のネットワークセグメント上にあるように手動で設定したり、DHCPサーバを起動して、DHCPアドレスプールのIPアドレスが管理IP アドレスと同一のネットワークセグメント上にあるように設定することができます。詳細は、[8.5.2.3 DHCPサーバ設定](#)をご参照ください。

2. **[適用]**をクリックします。

8.5.2.3 DHCP サーバ設定

1. 左側のナビゲーションツリーから**[詳細設定]** > **[LAN設定]** > **[DHCPサーバ設定]**を選択します。右側のメイン表示部分で、ゲートウェイとして機能するONTの、LAN側のDHCPアドレスプールを設定できます。設定後、[図 8-18](#)に示すように、LANポートに接続されたPCがアドレスプールからIPアドレスを自動的に取得できます。

図 8-18 DHCP サーバ設定

DHCPサーバ設定

このページでは、LAN側デバイスのDHCPサーバのパラメータを設定し、IPアドレスを取得することができます。

プライマリアドレスプール

プライマリDHCPサーバを有効にする:

DHCPリレーを有効にする:

Option125を有効にする:

LANホストIPアドレス: 192.168.1.1

サブネットマスク: 255.255.255.0

IPアドレスの開始: *(LANホストのIPアドレスと同一のサブネット上にある必要があります。)

IPアドレスの終了: *

リース時間: 時間

プライマリDNSサーバ:

セカンダリDNSサーバ:

セカンダリアドレスプール

セカンダリDHCPサーバを有効にする:

IPアドレス: 192.168.2.1

サブネットマスク: 255.255.255.0

IPアドレスの開始: *

IPアドレスの終了: *

リース時間: 日

Option 60: *

Option 43:

NTPサーバ:

プライマリDNSサーバ:

セカンダリDNSサーバ:

2. [適用]をクリックします。

表 8-2で、DHCPサーバに関するパラメータについて説明します。

表 8-2 DHCP サーバに関するパラメータ

パラメータ	説明
プライマリDHCPサーバを有効にする	プライマリDHCPサーバを有効にするかどうかを指定します。チェックボックスを選択すると、プライマリDHCPサーバを設定できます。
DHCPリレーを有効にする	DHCP L2リレーを有効にするかどうかを指定します。 DHCPリレーは、DHCPブロードキャストパケットのクロスサブネット転送がDHCPクライアントとDHCPサーバの間に実装されるプロセスです。この方法では、異なる物理サブネットのDHCPクライアントが、同じDHCPサーバから動的に割り当てられたIPアドレスを取得できます。
IPアドレスの開始	プライマリDHCPサーバ上のIPアドレスプールの開始IPアドレスを指定します。この開始IPアドレスは、LANホスト設定で設定したIPアドレスと同一のサブネットにある必要があります。そうでない場合、DHCPサーバは正常に動作しません。
IPアドレスの終了	有効なDHCPサーバ上のIPアドレスプールの終了IPアドレスを指定します。この終了IPアドレスは、LANホスト設定で設定したIPアドレスと同一のサブネットにある必要があります。そうでない場合、DHCPサーバは動作しません。
リース時間	有効なDHCPサーバ上のIPアドレスプールのリース時間を指定します。分、時間、日、週を選択できます。
セカンダリDHCPサーバを有効にする	セカンダリDHCPサーバを有効にするかどうかを指定します。チェックボックスを選択すると、セカンダリDHCPサーバを設定できます。
IPアドレス	セカンダリDHCPサーバのIPアドレスを指定します。
サブネットマスク	セカンダリDHCPサーバのサブネットマスクを指定します。
IPアドレスの開始	セカンダリDHCPサーバ上のIPアドレスプールの開始IPアドレスを指定します。
IPアドレスの終了	セカンダリDHCPサーバ上のIPアドレスプールの終了IPアドレスを指定します。

パラメータ	説明
リース時間	セカンダリDHCPサーバ上のIPアドレスプールのリース時間を指定します。分、時間、日、週を選択できます。
Option 60	セカンダリDHCPサーバのOption 60フィールドを指定します。ユーザー側のDHCPクライアントによって伝達されるOption 60フィールドがこの設定と同じである場合に限り、ユーザー側DHCPクライアントがセカンダリDHCPサーバ上のIPアドレスプールからIPアドレスを取得できます。
Option 43	セカンダリDHCPサーバのOption 43フィールドを指定し、TFTPサーバを識別します。
NTPサーバ	NTPサーバのIPアドレスを入力します。
プライマリDNSサーバ	プライマリDNSサーバのIPアドレスを入力します。
セカンダリDNSサーバ	セカンダリDNSサーバのIPアドレスを入力します。

8.5.2.4 DHCP スタティック IP 設定

1. 左側のナビゲーションツリーから[詳細設定] > [LAN設定] > [DHCPスタティックIP設定]を選択します。右側のメイン表示部分で、[新規作成]を選択します。表示されるダイアログボックスで、[図 8-19](#)に示すように、[MACアドレス]および[IPアドレス]を設定します。

図 8-19 DHCP スタティック IP 設定

DHCPスタティックIP設定

このページでは、指定のMACアドレスにDHCPを介して割り当てられた予約済みIPアドレスを設定できません。

新規作成
削除

	MACアドレス	IPアドレス
<input type="checkbox"/>	A7:9B:39:D2:E7:F1	192.168.1.20

MACアドレス: *(AA:BB:CC:DD:EE:FF)

IPアドレス: *

適用
キャンセル

2. [適用]をクリックします。

8.5.2.5 DHCPv6 サーバ設定

1. 左側のナビゲーションツリーから[詳細設定] > [LAN設定] > [DHCPv6サーバ設定]を選択します。右側のメイン表示部分で、[図 8-20](#)に示すように、ゲートウェイとして機能するONTの、LAN側のアドレスプールを設定できます。

図 8-20 DHCPv6 サーバ設定

DHCPv6サーバ設定

このページではIPv6関連機能のパラメータの設定ができます。

インターフェースのアドレス情報

IPv6アドレス: *

プレフィックス取得方法:

親プレフィックス:

子プレフィックスマスク: *(IPv6アドレス/64)

DNS情報

LAN側のDNSソース:

リソース割り当て情報

ルータ広告を有効にする:

DHCPv6サーバを有効にする:

リソース割り当てモード:

アドレス/プレフィックスの割り当て方法: DHCPv6 SLAAC

その他の情報の割り当て方法: DHCPv6 SLAAC

ULA情報

ULAモード:

2. [適用]をクリックします。

[表 8-3](#)に、DHCPv6サーバ設定パラメータを一覧表示します。

表 8-3 DHCPv6 サーバ設定パラメータ

パラメータ	説明
LAN側のDNSソース	IPv6のLAN側のDNSソースを選択します。

パラメータ	説明
アドレス/プレフィックスの割り当て方法	<p>アドレス/プレフィックスの割り当て方法を指定します。これは、DHCPv6またはステートレスアドレス自動設定 (SLAAC) に設定できます。SLAACに設定した場合は、[ULAモード]を設定する必要があります。</p> <ul style="list-style-type: none"> ● DHCPv6: LAN側のホストがDHCPv6モードでアドレスを取得するように指定します。 ● SLAAC: LAN側のホストがNDモードでアドレスを取得するように指定します。SLAACモードでは、ホストによってアドレスが自動的に設定されます。このアドレス情報には、ローカルルータによって示されるプレフィックスおよびホストのインターフェース識別子が含まれます。リンク上にルータがない場合、ホストはローカルノードと通信するためにリンクのローカルアドレスを自動的に設定する必要があります。
その他の情報の割り当て方法	<p>その他の情報の割り当て方法を指定します。その他の情報とは、DNSパケットなど、パケットのペイロードにおけるIPアドレスを指します。</p> <ul style="list-style-type: none"> ● DHCPv6: アドレスがDHCPv6モードで取得されるように指定します。 ● SLAAC: アドレスがNDモードで取得されるように指定します。
ULA情報	<p>一意のローカルIPv6アドレス(ULA)情報を指定します。ULAアドレスは、プレフィックスfdから始まります。予約済みIPv4アドレスと同様に、予約済みIPv6アドレスはプライベートネットワーク向けに使用されます。これはプロトコルの整合性を確保するためのものです。</p> <p>このパラメータは、手動、自動、無効、無効をお勧めします。</p> <ul style="list-style-type: none"> ● 無効: この機能が無効になります。 ● 自動: アドレスが自動的に割り当てられます。 ● 手動: アドレスを入力する必要があります。このオプションを選択した場合は、プレフィックス、プレフィックス長、優先耐用期間、有効耐用期間も設定する必要があります。
プレフィックス	<p>ネットワークアドレス空間を指定します。IPv6では、プレフィックスを使用して、ネットワークアドレス空間が指定されます。たとえば、2001:251:e000::/48により、48ビットのプレフィックスを使用してアドレス空間が指定されます。</p>
プレフィックス長	<p>プレフィックス長を指定します。これは10進値です。アドレス内にプレフィックスを形成するために使用される左端のビット数を指定します。アドレスプレフィックスは、「IPv6アドレス/プレフィックス長」の形式で表されます。たとえば、2001:251:e000::/48により、48ビットのプレフィックスを使用してアドレス空間が指定されます。</p>
優先耐用期間	<p>有効なアドレスが優先状態にある期間を指定します。優先耐用期間が過ぎると、アドレスは無効になります。</p>

パラメータ	説明
有効耐用期間	アドレスが有効な期間を指定します。有効耐用期間は、優先耐用期間よりも長くなければなりません。有効耐用期間が過ぎると、アドレスは無効になります。

8.5.2.6 DHCPv6 スタティック IP 設定

1. 左側のナビゲーションツリーから[詳細設定] > [LAN設定] > [DHCPv6スタティックIP設定]を選択します。右側のメイン表示部分で、MACアドレスにインターフェースIDおよびIPv6 GUAアドレスを使用してIPアドレスを割り当てることができます。IPv6 GUAアドレスは、[図 8-21](#)に示すように、LAN側に設定されたインターフェースIDとプレフィックスの組み合わせです。

図 8-21 DHCPv6 スタティック IP 設定

DHCPv6スタティックIP設定

このページでは予約済みインターフェースIDとIPv6 GUAアドレスを使用してMACにIPアドレスを割り当てることができます。IPv6 GUAアドレスはLAN側に設定されたインターフェースIDとプレフィックスの組み合わせです。LANアドレスの取得方法がSLAACに設定されている場合、このページの設定は有効になりません。

	MACアドレス	インターフェースID
<input type="checkbox"/>	A7:9B:39:D2:E7:F1	2012:1111:2222:3333

MACアドレス: *(AA:BB:CC:DD:EE:FF)

インターフェースID: *(XXXX:XXXX:XXXX:XXXX)

2. [適用]をクリックします。

8.5.2.7 DHCPv6 情報

左側のナビゲーションツリーから[詳細設定] > [LAN設定] > [DHCPv6情報]を選択します。[図 8-22](#)に示すように、右側のメイン表示部分に、アドレスの総数、残りのIPアドレスの数、DUID、IPv6アドレス/プレフィックスが表示されます。

図 8-22 DHCPv6 情報

DHCPv6情報

このページでは、DUID、IPv6アドレス、プレフィックス、残りリース時間など、DHCPv6の基本情報を照会することができます。

IPアドレス総数:	256
残りのIPアドレス:	256

DUID	IPv6アドレス/プレフィックス	残りリース時間
--	--	--

8.5.3 セキュリティ設定

ここでは、IPフィルタリング、MACフィルタリング、DoSオプションの設定方法について説明します。

8.5.3.1 DoS 設定

1. 左側のナビゲーションツリーから[詳細設定] > [セキュリティ設定] > [DoS設定]を選択します。右側のメイン表示部分で、[図 8-23](#)に示すように、DoS攻撃防止設定を有効にするかどうかを指定します。

図 8-23 DoS 設定

DoS設定

このページではDoSパラメータの設定ができます。

SYNフラッド攻撃の防止:	<input checked="" type="checkbox"/>
ICMP ECHO攻撃の防止:	<input checked="" type="checkbox"/>
ICMPリダイレクト攻撃の防止:	<input checked="" type="checkbox"/>
LAND攻撃の防止:	<input checked="" type="checkbox"/>
Smurf攻撃の防止:	<input checked="" type="checkbox"/>
WinNuke攻撃の防止:	<input checked="" type="checkbox"/>
Pingスイープ攻撃の防止:	<input checked="" type="checkbox"/>

2. [適用]をクリックします。

サービス拒否(DoS)攻撃は、インターネットへのユーザーのアクセスを拒否するネットワークベースの攻撃です。DoS攻撃は、多数のネットワーク接続を開始し、サーバまたはサーバ

上で動作するプログラムを停止させたり、サーバリソースを枯渇させたり、インターネットサービスへのユーザーのアクセスを拒否したりします。その結果、ネットワークサービスが機能しなくなります。

8.5.3.2 IPv4 アドレスフィルタリング

1. 左側のナビゲーションツリーから[詳細設定] > [セキュリティ設定][DoS設定]を選択します。右側のメイン表示部分の[IPv4アドレスフィルタリング]を有効にします。[フィルタリング方法]の選択後、[新規作成]を選択します。その後、[図 8-24](#)のように表示されたダイアログボックスで、WANインターフェースからLANポートまでのIPアドレスをフィルタリングする際のルールを設定します。

図 8-24 IPv4 アドレスフィルタリング

IPv4アドレスフィルタリング

このページでは、WAN-to-LANフィルタを設定し、WANにある特定のIPアドレスがLANにアクセスしないようにすることができます。

有効 IP フィルタ: (IPフィルタリング機能を有効にしている場合、デバイスの転送性能が低下します。)

フィルタリング方法: ブラックリスト ▼

新規作成 削除

ルール名	プロトコル	方向	LAN側IPアドレス	WAN側IPアドレス
----	----	----	----	----

ルール名: *

プロトコル: 全て ▼

方向: 双方向 ▼

LAN側の開始IPアドレス: ▼

LAN側の終了IPアドレス: ▼

WAN側IPアドレス: --

適用 キャンセル

2. **[適用]**をクリックします。

IPアドレスのフィルタリング機能は、宅内ゲートウェイで設定するセキュリティ対策です。外部IPアドレスセグメントのすべてのポートまたは一部のポートと通信するために、イントラネットのIPアドレスセグメントのすべてのポートまたは一部のポートを有効/無効にします。IPアドレスのフィルタリング設定は、イントラネット内のデバイスと外部デバイス間の通信を制限するために使用されます。

[表 8-4](#)で、IPアドレスのフィルタリングに関するパラメータについて説明します。

表 8-4 IP アドレスのフィルタリングに関するパラメータ

パラメータ	説明
有効IPフィルタ	IPアドレスのフィルタリング機能を有効にするかどうかを指定します。
フィルタリング方法	<p>ブラックリストまたはホワイトリストのIPアドレスのフィルタリングルールを指定します。</p> <ul style="list-style-type: none"> ● ブラックリスト: フィルタリングルールリストのルールを満たしているデータが通過できないように指定します。 ● ホワイトリスト: フィルタリングルールリストのルールを満たしているデータが通過できるように指定します。 ● ハイブリッド: 上り方向であるか下り方向であるかに基づいて、パケットがフィルタリングされるように指定します。上り方向または下り方向の特定のIPパケットが通過できます（通過できません）。 <p>上述の方法の1つだけを選択できます。</p>
ルール名	ルールの名前を指定します。このパラメータは必須であり、数字と文字のみが使用できます。ルール名は一意である必要があります。
プロトコル	プロトコルのタイプを指定します。TCP/UDP、TCP、UDP、ICMP、全てを指定できます。
方向	<p>フィルタリングルールを適用する方向を指定します。</p> <ul style="list-style-type: none"> ● 双方向: この値を使用できるのは、フィルタリング方法がブラックリストまたはホワイトリストの場合のみです。この値は変更できません。 ● 上り方向: この値をハイブリッドモードで選択すると、フィルタリングルールは上り方向に適用されます。ハイブリッドフィルタリングモードでは、[Upstream]または[Downstream]のいずれか1つのみを選択できます。 ● 下り方向: この値をハイブリッドモードで選択すると、フィルタリングルールは下り方向に適用されます。
優先度	IPフィルタリングルールの優先度を指定します。このパラメータは、[Filter Mode]が[Hybrid]に設定されている場合にのみ設定可能です。値の範囲は0 - 255です。値が小さいほど、優先度が高くなります。デフォルト値は255です。
LAN側の開始IPアドレス	LAN側の開始IPアドレスを指定します。
LAN側の終了IPアドレス	LAN側の終了IPアドレスを指定します。
WAN側IPアドレス	WAN側のIPアドレスを指定します。

パラメータ	説明
処理	<p>IPフィルタリング処理を指定します。</p> <ul style="list-style-type: none"> ● 許可: IPフィルタリングルールを満たしたパケットを許可します。 ● 破棄: IPフィルタリングルールを満たしたパケットを破棄します。

8.5.3.3 MAC アドレスフィルタリング

1. 左側のナビゲーションツリーから[詳細設定] > [セキュリティ設定] > [MACアドレスフィルタリング]を選択します。右側のメイン表示部分で、[MACアドレスフィルタリング]を有効にし、[フィルタリング方法]を選択した後、[新規作成]を選択します。図 8-25のように表示されるダイアログボックスで、PCがインターネットにアクセスする際のMACフィルタリングルールを設定します。

図 8-25 MAC アドレスフィルタリング

2. [適用]をクリックします。

ネットワーク上のPCのMACアドレスリストは、ONT上に保存されます。MACフィルタリングルールを設定することにより、そのルールに準拠するPCがインターネットサービスにアクセスできるようにしたり、そのルールに準拠しないPCがインターネットサービスにアクセスできないようにしたりすることができます。1台のPCが複数のIPアドレスを持つ場合がありますが、MACアドレスは一意です。そのため、MACフィルタリングルールを設定すると、LAN上のPCのインターネットサービスのアクセス権限が効果的に制御されます。

表 8-5で、MACフィルタリングに関するパラメータについて説明します。

表 8-5 MAC アドレスのフィルタリングに関するパラメータ

パラメータ	説明
MACフィルタを有効にする	MACアドレスのフィルタリング機能を有効にするかどうかを指定します。
フィルタリング方法	<p>ブラックリストまたはホワイトリストのMACアドレスのフィルタリングルールを指定します。</p> <ul style="list-style-type: none"> ● ブラックリスト: フィルタリングルールリストのルールを満たしているデータが通過できないように指定します。 ● ホワイトリスト: フィルタリングルールリストのルールを満たしているデータが通過できるように指定します。 <p>フィルタリング方法はグローバルな設定方法です。そのため、ブラックリストとホワイトリストを同時に使用することはできません。</p>
送信元MACアドレス	MACアドレスのフィルタリングルールでの送信元MACアドレスを指定します。

8.5.3.4 Wi-Fi MAC アドレスフィルタリング

1. 左側のナビゲーションツリーから[詳細設定] > [セキュリティ設定] > [Wi-Fi MACアドレスフィルタリング]を選択します。右側のメイン表示部分で、[WLAN MACフィルタを有効にする]を選択し、フィルタリング方法を設定し、[新規作成]を選択します。表示されるダイアログボックスで、[図 8-26](#)に示すように、SSIDベースのMACアドレスフィルタリングルールを設定します。

図 8-26 Wi-Fi MAC アドレスフィルタリング

Wi-Fi MACアドレスフィルタリング

このページではMACフィルタを設定し特定のPCのインターネットアクセスを禁止することができます。

WLAN MACフィルタを有効にする:

フィルタリング方法: ブラックリスト ▼

新規作成 削除

	SSIDインデックス	送信元MACアドレス
----	----	----

SSIDインデックス: SSID5 ▼

送信元MACアドレス: A7:9B:39:D2:E7:F1 *(AA:BB:CC:DD:EE:FF)

適用
キャンセル

2. [適用]をクリックします。

表 8-6で、ワイヤレスネットワークのMACアドレスフィルタリングの設定パラメータについて説明します。

表 8-6 ワイヤレスネットワークの MAC フィルタリングのパラメータ

パラメータ	説明
WLAN MACフィルタを有効にする	WLAN MACフィルタリング機能の有効/無効を切り替えます。
フィルタリング方法	<p>MACフィルタリング方法を指定します。これは、ブラックリスト または ホワイトリストに設定できます。</p> <ul style="list-style-type: none"> ● ブラックリスト: ブラックリストのルールに一致するデータパケットの通過を禁止します。 ● ホワイトリスト: ホワイトリストのルールに一致するデータパケットの通過を許可します。 <p>ブラックリスト または ホワイトリスト モードはグローバルな設定です。この2つの方法を同時に使用することはできません。</p>
SSIDインデックス	MACアドレスフィルタリングのWLANのSSIDインデックスが設定されるように指定します。
送信元MACアドレス	MACフィルタリングルールでの送信元MACアドレスを指定します。

8.5.3.5 ペアレンタルコントロール

1. 左側のナビゲーションツリーから、[詳細設定] > [セキュリティ設定] > [ペアレンタルコントロール]を選択します。右側のペインで、ネットワーク閲覧時間や平日や休日におけるWebサイトへのアクセスに関する様々な制限を設定できます。図 8-27に示すように、お子様が指定の時間帯のみネットワークにアクセスすることを許可したり、年齢制限のある不適切なコンテンツにアクセスさせないように設定できます。

図 8-27 ペアレンタルコントロール

ペアレンタルコントロール

このページでは、インターネットのアクセス制限を設定し、直接監視をしなくても子どもが安全にインターネットを使用できるようにします。ペアレンタルコントロールにより、子どもがインターネットを使用できる時間やアクセスできるウェブサイトの指定ができます。

概要 | テンプレート | 統計 [ヘルプ](#)

全てのデバイスに適用 指定したデバイスに適用

	デバイス	説明	テンプレートの関連付け
----	----	----	----

デバイス

指定されたデバイス

説明

デバイスの説明

テンプレートの関連付け

テンプレート

2. [適用]をクリックします。



ウィザードでの説明に従ってテンプレートを設定します。右上部の [ヘルプ] をクリックすると、必要に応じてテンプレートの設定方法に関するオンラインヘルプを確認できます。

8.5.3.6 ONT アクセス制御設定

1. 左側のナビゲーションツリーから[詳細設定] > [セキュリティ設定] > [ONTアクセス制御設定]を選択します。右側のペインで、図 8-28に示すようにONTアクセス制御ルールを設定します。



危険

リモートアクセス制御を有効にする前にネットワークセキュリティ計画を完了して、ONTがセキュアなネットワーク状態でログインしていることを確認してください。ONTのログイン操作が完了したら、リモートアクセス制御を適宜無効にしてください。ネットワークセキュリティ計画を完了していない場合や適宜リモートアクセス制御を無効にしていない状態でネットワーク障害やネットワークが攻撃を受けた場合、Huaweiは付随する結果に対して一切の責任を負いません。

図 8-28 ONT アクセス制御設定

ONTアクセス制御設定

このページではONTアクセスの許可や拒否ができます。

LANサービス

LAN側PCによるTelnetを介したONTアクセスを有効にする:

WiFiサービス

WiFi側デバイスによるウェブページへのアクセスを有効にする:

WiFi側PCによるTelnetを介したONTへのアクセスを有効にする:

適用 キャンセル

2. [適用]をクリックします。

8.5.4 ルート

ここでは、Webページでのルートの設定方法について説明します。

8.5.4.1 デフォルトのIPv4 ルート設定

1. 左側のナビゲーションツリーから[詳細設定] > [ルート] > [デフォルトのIPv4ルート設定]を選択します。右側のペインで、システムのデフォルトルートを有効/無効にするには、図 8-29に示すように[デフォルトルートを有効にする]オプションボタンを選択/選択解除します。

図 8-29 デフォルトの IPv4 ルート設定

デフォルトのIPv4ルート設定

このページではデフォルトルートを設定できます。

デフォルトルートを有効にする:

WAN名: 1_TR069_INTERNET_R_VID_10

適用 キャンセル



パケット受信後にONTで一致するルーティングエントリが見つからない場合、デフォルトルート設定で指定されたWANインターフェースによりパケットがネットワークデバイスに送信されます。システムのデフォルトルートを有効にする前に、WANインターフェースではIPアドレスを取得する必要があります。そのため、WANインターフェースのパラメータは正しく設定する必要があります。詳細は、[8.5.1 WAN設定](#)をご参照ください。

2. [適用]をクリックします。

8.5.4.2 IPv4 スタティックルート設定

1. 左側のナビゲーションツリーから[詳細設定] > [ルート] > [IPv4スタティックルート設定]を選択します。右側のペインで、[新規作成]をクリックします。表示されたダイアログボックスで、[図 8-30](#)に示すようにスタティックルートに関するパラメータを設定します。

図 8-30 IPv4 スタティックルート設定

IPv4スタティックルート設定

このページでは、ドメイン名、IPアドレス、サブネットマスク、ゲートウェイIPアドレス、WANポート名など、スタティックルートの設定ができます。スタティックルートを設定する際、指定のWANポートがオフラインの場合、ゲートウェイIPアドレスは空白のままにしてください。

	WAN名	IPアドレス/ドメイン名	ゲートウェイ	サブネットマスク
<input type="checkbox"/>	1_TR069_INTERNET_R_VID_10	10.167.166.55		255.255.255.255

アドレス形式: IP ドメイン名

IPアドレス: *(宛先IPアドレスとマスクが設定されている場合、ドメイン設定は有効化されません。)

サブネットマスク: *

ゲートウェイ: 空白: 自動でゲートウェイを選択します

WAN名:

2. [適用]をクリックします。

[表 8-7](#)では、スタティックルートに関するパラメータについて説明します。

表 8-7 スタティックルートに関するパラメータ

パラメータ	説明
アドレス形式	アドレスの形式を指定します。IPアドレスまたはドメイン名の形式を指定可能です。宛先IPアドレスおよびドメイン名の両方を設定する場合、宛先IPアドレスのみが有効になります。
IPアドレス	スタティックルートの宛先IPアドレスを指定します。このパラメータは、IPアドレスの形式が[アドレス形式]で指定されている場合に設定する必要があります。

パラメータ	説明
ドメイン名	<p>スタティックルートのドメイン名を指定します。このパラメータは、ドメイン名の形式が[アドレス形式]で指定されている場合に設定する必要があります。</p> <p>次のような形式のワイルドカードによるドメイン名の指定が可能です： *.abc.com、abc.com.*、abc.*.com。次のような形式でのワイルドカードによるドメイン名の指定はできません： *abc.com、abc*.com、a*c.com</p>
サブネットマスク	スタティックルートのサブネットマスクを指定します。
ゲートウェイ	スタティックルートのゲートウェイIPアドレスを指定します。
WAN名	ルートが通過するWANインターフェースを指定します。

8.5.4.3 IPv4 VLAN バインディング設定

1. 左側のナビゲーションツリーから[詳細設定] > [ルート] > [IPv4 VLANバインディング設定]を選択します。ポートVLANバインディング関係を設定するには、[図 8-31](#)に示すように右側のペインで、タブ内でポートVLANバインディングコラムを設定する必要があります。

図 8-31 IPv4 VLAN バインディング設定

IPv4 VLANバインディング設定

このページではVLANをバインドすることができます。VLANをバインドする際は、m1/n1の形式で設定してください。(m1はユーザー側のVLAN、n1はイグレスVLAN) 複数のVLANペアをカンマで区切ります。

ポート	バインディング方法	VLANペア
LAN1	VLANバインディング	20/10
LAN2	ポートバインディング	--
LAN3	ポートバインディング	--
LAN4	ポートバインディング	--
LAN5	ポートバインディング	--
SSID1	ポートバインディング	--
SSID5	ポートバインディング	--

ポート:

ポート方法:

VLANペア: *(ユーザー-VLAN/WAN VLAN)

2. [適用]をクリックします。

8.5.4.4 IPv4 サービスルート設定

1. 左側のナビゲーションツリーから[詳細設定] > [ルート] > [IPv4サービスルート設定]を選択します。右側のペインで、[新規作成]をクリックします。表示されたダイアログボックスで、[図 8-32](#)に示すように関連するサービスルートパラメータを設定します。

図 8-32 IPv4 サービスルート設定

IPv4サービスルート設定

このページではサービスのルーティングを設定できます。設定後、サービスパケットは指定のWANポートを経由してOLTに送信されます。

新規作成
削除

サービスの種類	WAN名
<input type="checkbox"/> PPPoE	2_INTERNET_B_VID_1001

サービスの種類: PPPoE

WAN名: 2_INTERNET_B_VID_1001

適用
キャンセル



この設定は、デバイスがブリッジモードで動作している場合に有効です。対応するWANはブリッジタイプのWANにする必要があります。

2. [適用]をクリックします。

8.5.4.5 IPv4 ルーティングテーブル

左側のナビゲーションツリーから[詳細設定] > [ルート] > [IPv4ルーティングテーブル]を選択します。[図 8-33](#)に示すように、右側のペインに宛先IPアドレス、宛先サブネットマスク、ゲートウェイ、送出インターフェースなどのデバイスのルーティング情報が表示されます。

図 8-33 IPv4 ルーティングテーブル

IPv4ルーティングテーブル

このページでは、宛先IPアドレス、宛先サブネットマスク、ゲートウェイ、出力インターフェースなどのルーティング情報を照会することができます。

No.	宛先IPアドレス	宛先サブネットマスク	ゲートウェイ	インターフェース
1	192.168.1.0	255.255.255.0	0.0.0.0	br0

<< < 1/1 > >>

ページ 移動

8.5.4.6 デフォルトの IPv6 ルート設定

1. 左側のナビゲーションツリーから[詳細設定] > [ルート] > [デフォルトのIPv6ルート設定]を選択します。右側のペインで、システムのデフォルトルートの有効/無効にするには、[図 8-34](#)に示すように[デフォルトルートを有効にする]オプションボタンを選択/選択解除します。

図 8-34 デフォルトの IPv6 ルート設定



注記
パケット受信後にONTで一致するルーティングエントリが見つからない場合、デフォルトルート設定で指定されたWANインターフェースによりパケットがネットワークデバイスに送信されます。システムのデフォルトルートを有効にする前に、WANインターフェースではIPアドレスを取得する必要があります。そのため、WANインターフェースのパラメータは正しく設定する必要があります。詳細は、[8.5.1 WAN設定](#)をご参照ください。

2. [適用]をクリックします。

8.5.4.7 IPv6 スタティックルート設定

1. 左側のナビゲーションツリーから[詳細設定] > [ルート] > [IPv6スタティックルート設定]を選択します。右側のペインで[新規作成]をクリックします。表示されたダイアログボックスで、[図 8-35](#)に示すようにスタティックルートに関するパラメータを設定します。

図 8-35 IPv6 スタティックルート設定

IPv6スタティックルート設定

このページでは、IPアドレスプレフィックスとネクストホップなどのスタティックルートを設定することができます。

	WAN名	宛先IPプレフィックス	ネクストホップ
<input type="checkbox"/>	1_TR069_INTERNET_R_VID_10	2012:1111:2222::/64	2012:1111:2222:3333:.....

宛先IPプレフィックス: *(IPv6アドレス/n 1 <= n <= 128)

ネクストホップ: (IPv6アドレス)

WAN名:

2. [適用]をクリックします。

表 8-8にスタティックルートの設定パラメーター一覧を示します。

表 8-8 スタティックルートパラメータ

パラメータ	説明
宛先IPプレフィックス	このパラメータは取得されたプレフィックスが64ビットより短い場合に設定する必要があります。これはLAN IPアドレス割当に使用されます。
ネクストホップ	スタティックルートの宛先IPアドレスを指定します。
WAN名	スタティックルートが通るWANインターフェースを指定します。

8.5.5 転送ルール

ここでは、WebページからDMZ、ポートマッピング、ポートトリガを設定する方法について説明します。

8.5.5.1 DMZ 設定

1. 左側のナビゲーションツリーから[詳細設定] > [転送ルール] > [DMZ設定]を選択します。右側のメイン表示部分で、[新規作成]を選択します。表示されるダイアログボックスで、図 8-36に示すように、DMZに関するパラメータを設定します。

図 8-36 DMZ 設定

DMZ設定

このページではDMZパラメータの設定ができます。DMZデバイスは信頼できない外部からの接続がデバイスに確立されるのを制限します。これは安全なシステムと安全ではないシステム間のバッファとなります。WANポートがポートマッピングテーブルに登録されていない場合、WAN接続からのアプリケーション要求はDMZデバイスに転送されます。

新規作成
削除

WAN名	DMZの有効化	ホストアドレス
----	----	----

DMZを有効にする:

WAN名:

ホストアドレス:

適用
キャンセル

2. [適用]をクリックします。

非武装地帯 (DMZ) は、ONTが受信したすべてのパケットを指定した内部サーバを介して転送できるようにする技術です。この技術により、LAN上のコンピュータをインターネット上のすべてのユーザーに完全に公開することや、指定したIPアドレスを持つホストとインターネット上の他のユーザーまたは他のサーバの間で制限なしに相互に通信することが可能になります。このような方法で、指定したIPアドレスを持つホスト上で多くのアプリケーションが動作できます。指定したIPアドレスを持つホストは、識別可能なすべての接続とファイルを受け入れます。



注意事項

LAN側のデバイスがWebサイトサービスや他のネットワークサービスを提供しない場合は、デバイスをDMZホストに設定しないでください。DMZホストのポートはすべて、インターネットに対して開かれているからです。

表 8-9 で、DMZに関するパラメータについて説明します。

表 8-9 DMZ に関するパラメータ

パラメータ	説明
DMZを有効にする	DMZを有効にするかどうかを指定します。
WAN名	WANインターフェースの名前を指定します。WANインターフェースがポートマッピングテーブルにない場合、WAN接続からのアプリケーション要求は、DMZのホストに直接転送されます。
ホストアドレス	DMZホストのIPアドレスを指定します。

8.5.5.2 IPv4 ポートマッピング

1. 左側のナビゲーションツリーから[詳細設定] > [転送ルール] > [IPv4ポートマッピング]を選択します。右側のメイン表示部分で、[新規作成]を選択します。表示されるダイアログボックスで、[図 8-37](#)に示すように、ポートマッピングに関するパラメータを設定します。

図 8-37 IPv4 ポートマッピング

IPv4ポートマッピング

このページではポートマッピングパラメータを設定して、LANネットワーク上に仮想サーバを設定し、これらのサーバをインターネットからアクセスできるようにします。
注: 既存の音声サービス用のポートはマッピングポートの範囲に入れることはできません。

---	マッピング名	WAN名	内部ホスト	外部ホスト	有効
---	---	---	---	---	---

種別: カスタム設定 アプリケーション

アプリケーション:

ポートマッピングを有効にする:

マッピング名:

WAN名:

内部ホスト: *

外部送信元IPアドレス: --

プロトコル: 内部ポート番号: -- *

外部ポート番号: -- * 外部送信元ポート番号: --

2. [適用]をクリックします。

ポートマッピングは、イントラネットサーバをエクストラネットに対して開くことができるように指定します(たとえば、イントラネットがエクストラネットに WWWサーバまたはFTPサーバを提供します)。ポートマッピングは、エクストラネットのユーザーがイントラネットサーバにアクセスできるように、イントラネットのホストのIPアドレスおよびポートIDをエクストラネットのIPアドレスおよび対応するポートIDにマップします。ポートマッピングでは、ユーザーは、イントラネットのIPアドレスを参照することはできず、エクストラネットのIPアドレスを参照します。

[表 8-10](#)で、ポートマッピングに関するパラメータについて説明します。

表 8-10 ポートマッピングに関するパラメータ

パラメータ	説明
ポートマッピングを有効にする	ポートマッピングを有効にするかどうかを指定します。
マッピング名	ポートマッピングルールの名前を指定します。
WAN名	ポートマッピングを有効にするWANインタフェースの名前を指定します。
内部ホスト	ポートがマップされるホストのIPアドレスを指定します。
外部送信元IPアドレス	外部データパケットの送信元IPアドレスを指定します。
プロトコル	ポートマッピングパケットのプロトコルの種類を指定します。 TCP、UDP、TCP/UDPを指定できます。
内部ポート番号	ポートマッピングパケットの内部宛先ポートを示しています。
外部ポート番号	外部データパケットの宛先ポートを示しています。
外部送信元ポート番号	外部データパケットの送信元ポートを示しています。

8.5.5.3 ポートトリガ設定

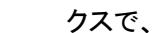
1. 左側のナビゲーションツリーから[詳細設定] > [転送ルール] > [ポートトリガ設定]を選択します。右側のメイン表示部分で、[新規作成]を選択します。表示されるダイアログボックスで、 8-38に示すように、ポートトリガに関するパラメータを設定します。

図 8-38 ポートトリガ設定

ポートトリガ設定

このページでは、インターネットにアクセスするためLAN側アプリケーションにより使用されるポートの範囲を設定することができます。ポートを自動で有効にすることもできます。
注: 既存の音声サービス用のポートはオープンポートの範囲に入れることはできません。

	WAN名	ポートトリガの有効化	トリガポート	オープンポート	トリガプロトコル	オープンプロトコル
<input type="checkbox"/>	1_TR069_INTERNET_R_VID_10	有効	200-201	145-147	UDP	UDP

ポートトリガを有効にする:

WAN名:

トリガプロトコル:

オープンプロトコル:

開始トリガポート: *

終了トリガポート: *

開始オープンポート: *

終了オープンポート: *

2. [適用]をクリックします。

ポートトリガは、対応するイントラネットポートがパケットを送信し、そのパケットがホスト上のイントラネットポートにマップされたときに、特定のエクストラネットポートが自動的に有効になるように指定します。特定のマッピングパケットは、エクストラネットのパケットが対応するホストにマップされるように、イントラネットを介してONTから送信されます。ゲートウェイファイアウォール上で指定したポートが、リモートアクセスのために一部のアプリケーションに対して開かれます。ポートトリガは、ファイアウォールのオープンポートを動的に有効にできます。

表 8-11 で、ポートトリガに関するパラメータについて説明します。

表 8-11 ポートトリガに関するパラメータ

パラメータ	説明
ポートトリガを有効にする	ポートトリガを有効にするかどうかを指定します。
WAN名	ポートトリガを有効にするWANインタフェースの名前を指定します。
トリガプロトコル	ポートトリガパケットのプロトコルの種類を指定します。TCP、UDP、TCP/UDPを指定できます。

パラメータ	説明
オープンプロトコル	オープンデータパケットのプロトコルの種類を指定します。
開始トリガポート	ポートトリガパケットの送信先開始ポートを指定します。
終了トリガポート	ポートトリガパケットの送信先終了ポートを指定します。
開始オープンポート	オープンパケットの送信先開始ポートを指定します。
終了オープンポート	オープンパケットの送信先終了ポートを指定します。

8.5.6 アプリケーション

ここでは、WebページからUSB、UPnP、DDNSを設定する方法について説明します。

8.5.6.1 時間設定

1. 左側のナビゲーションツリーから[詳細設定] > [アプリケーション] > [時間設定]を選択します。右側のメイン表示部分で、[図 8-39](#)に示すように、SNTPサーバ、タイムゾーン、サマータイム(DST)など、システム時間に関するパラメータを設定します。

図 8-39 時間設定

時間設定

このページでは正確な時刻を取得するため、SNTPプロトコル、タイムゾーン、DSTを設定することができます。

ネットワーク時刻サーバを自動
で同期する

プライマリSNTPサーバ:

セカンダリSNTPサーバ:

タイムゾーン:

時刻同期の時間: (秒)

WAN名:

DSTを有効にする

DST開始時間:

時間: 分: 秒:

DST終了時間:

時間: 分: 秒:

2. [適用]をクリックします。

表 8-12で、システム時間に関するパラメータについて説明します。

表 8-12 システム時間に関するパラメータ

パラメータ	説明
ネットワーク時刻サーバを自動で同期する	ネットワーク時刻サーバ、すなわちSNTPサーバの自動同期を有効にするかどうかを指定します。
プライマリSNTPサーバ	プライマリSNTPサーバを指定します。
セカンダリSNTPサーバ	セカンダリSNTPサーバを指定します。
タイムゾーン	タイムゾーンを指定します。
時刻同期の時間	時刻同期の時間を指定します。
DSTを有効にする	DSTを有効にするかどうかを指定します。
DST開始時間	DST開始時間を指定します。
DST終了時間	DST終了時間を指定します。

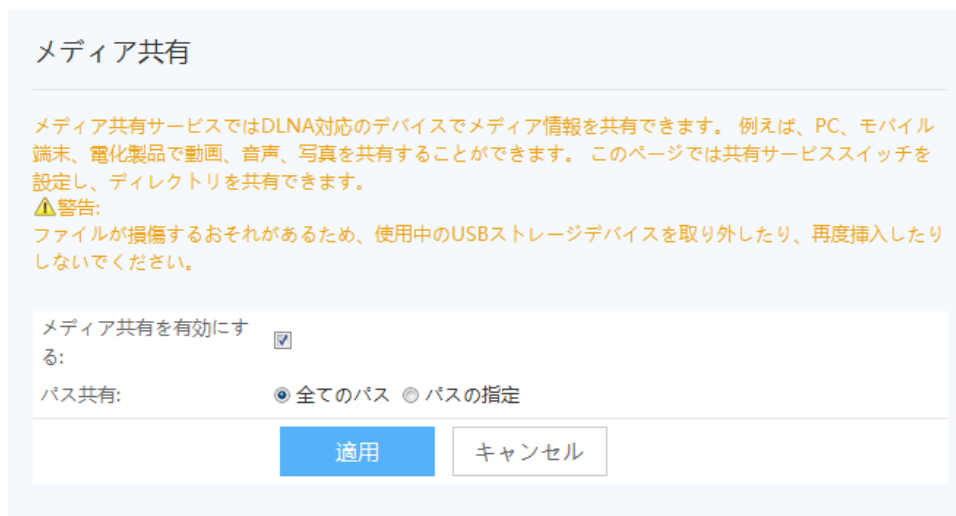


SNTPサーバをドメイン名形式に基づいて設定する場合は、スタティックルートまたはデフォルトルートを設定する必要があります。スタティックルートまたはデフォルトルートが設定されていない場合、ONTはSNTPサーバから時間を取得できません。SNTPサーバをIPアドレス形式に基づいて設定する場合、上述した操作は省略できます。

8.5.6.2 メディア共有

1. 左側のナビゲーションツリーから[詳細設定] > [アプリケーション] > [メディア共有]を選択します。右側のメイン表示部分で、図 8-40に示すように、メディア共有を設定できます。

図 8-40 メディア共有



2. [適用]を選択します。

8.5.6.3 DDNS 設定

1. 左側のナビゲーションツリーから[詳細設定] > [アプリケーション] > [DDNS設定]を選択します。右側のペインで、図 8-41 に示すように[サービスプロバイダ]、[ホスト名]、[サービスポート]、[ドメイン名]、[ユーザー名]、[パスワード]などのDDNSパラメータを設定します。

8.5.6.4 UPnP 設定

1. 左側のナビゲーションツリーから[詳細設定] > [アプリケーション] > [UPnP設定]を選択します。右側のメイン表示部分で、[図 8-42](#)に示すように、UPnPを有効にするかどうかを指定します。

図 8-42 UPnP 設定

UPnP設定

このページではユニバーサルプラグアンドプレイ (UPnP)機能の有効化や無効化を設定し、複数種類のネットワークデバイスの自動検出を実施することができます。この機能が有効化されていると、デバイスはネットワークへのアクセス、IPアドレスの取得、データ転送、他のデバイスの検出、他のデバイスデータの取得を実施することができます。

UPnPを有効にする:

No.	説明	外部ポート	内部ポート	プロトコル	IPアドレス	ステータス
--	--	--	--	--	--	--

2. [適用]をクリックします。

ユニバーサルプラグアンドプレイ (UPnP) は、プロトコルのグループ名です。UPnPでは、ゼロコンフィギュレーションネットワークと、各種ネットワークデバイスの自動検出がサポートされています。UPnPを有効にすると、UPnP対応デバイスがネットワークに動的に接続して、IPアドレスの取得、転送性能の取得、他のデバイスの検出、他のデバイスの性能の把握を行うことができます。UPnP対応デバイスは、このデバイスまたは他のデバイスに影響を与えずに、ネットワークから自動的に切断されます。

UPnPを有効にすると、LAN側のPCはONTを自動的に検出します。ONTは、PCの周辺機器とみなされ、プラグアンドプレイです。PC上でアプリケーションソフトウェアの実行後、ONT上でUPnPプロトコルを介してポートマッピングエントリが自動的に生成されるため、実行速度が向上します。

8.5.6.5 IGMP 設定

1. 左側のナビゲーションツリーから[詳細設定] > [アプリケーション] > [IGMP設定]を選択します。右側のペインで、[図 8-43](#)に示すようにIGMPパラメータを設定します。

図 8-43 IGMP 設定

IGMP設定

このページではIGMPパラメータの設定ができます。IGMP機能はIGMPがゲートウェイとして機能している場合に限りWANポートで有効にすることができます。ONTがゲートウェイとして機能し、IGMPプロキシが有効化されている場合のみ、ロバスト性、IGMPプロキシバージョン、一般的なクエリとグループ特定クエリに関するパラメータを設定することができます。

IGMPを有効にする:	<input type="text" value="はい"/>
IGMPモード:	<input type="text" value="プロキシ"/>
ブリッジWANプロキシを有効化:	<input type="text" value="はい"/>
PPPoE WANプロキシモード:	<input type="text" value="PPPoE"/>
PPPoE WANスヌーピングモード:	<input type="text" value="IPoEとPPPoE"/>
IGMPプロキシバージョン:	<input type="text" value="V2"/>
IP Precedenceの再マーク:	<input type="text" value=""/> (0-7)
802.1p優先度の再マーク:	<input type="text" value=""/> (0-7)
ロバスト性:	<input type="text" value="2"/> *(範囲: 1-10、デフォルト: 2)
一般的なクエリ間隔:	<input type="text" value="125"/> *(範囲: 1-5000、単位: 秒、デフォルト: 125)
一般的なクエリ応答タイムアウト時間:	<input type="text" value="100"/> *(範囲: 1-255、単位: 0.1秒、デフォルト: 100)
グループ特定クエリ時間:	<input type="text" value="2"/> *(範囲: 1-10、デフォルト: 2)
グループ特定クエリ間隔:	<input type="text" value="10"/> *(範囲: 1-5000、単位: 0.1秒、デフォルト: 10)
グループ特定クエリ応答タイムアウト時間:	<input type="text" value="10"/> *(範囲: 1-255、単位: 0.1秒、デフォルト: 10)

2. [適用]をクリックします。

WANポートのIGMP機能は、IGMPがゲートウェイモードで動作している場合にのみ有効にできます。

8.5.6.6 スタティック DNS

1. 左側のナビゲーションツリーから[詳細設定] > [アプリケーション] > [スタティックDNS]を選択します。右側のメイン表示部分で、図 8-44に示すように、DNSパラメータを設定し、スタティックDNSのドメイン名解決を設定できます。

図 8-44 スタティック DNS

スタティック DNS

このページでは、DNSサーバ、スタティックドメイン名解決を設定できます。

DNS検索リスト設定

新規作成 削除

ドメイン名	WAN名	DNSサーバ
----	----	----

ドメイン名: *

WAN名:

DNSサーバ:

適用 キャンセル

スタティック DNS設定

新規作成 削除

ドメイン名	IPアドレス
----	----

ドメイン名: *

IPアドレス: *

適用 キャンセル

2. [適用]をクリックします。

8.5.7 WLAN

ここでは、WebページからWLANの基本設定および詳細設定を行う方法について説明します。

8.5.7.1 2.4G 基本ネットワーク設定

1. 左側のナビゲーションツリーから[詳細設定] > [WLAN] > [2.4G基本ネットワーク設定]を選択します。右側のメイン表示部分で、[WLANの有効化]オプションボックスを選択します。表示されるダイアログボックスで、図 8-45に示すように、SSID、認証モード、暗号化モードなどの基本Wi-Fiパラメータを設定します。

図 8-45 2.4G 基本ネットワーク設定

2.4G基本ネットワーク設定

このページでは、2.4GHz帯ワイヤレスネットワークの基本パラメータの設定ができます。2.4GHz帯ワイヤレスネットワークが無効化されている場合、このページは空白です。

⚠警告:

- ワイヤレスネットワークパラメータを変更するとワイヤレスネットワークサービスが一時的に中断される可能性があります。
- セキュリティ保護のため、WPA2または WPA/WPA2認証モードを使用することをお勧めします。

WLANの有効化

新規作成
削除

	SSIDインデックス	SSID名	SSIDの状態	接続デバイス数	SSIDのプロードキャスト	セキュリティ設定
<input type="checkbox"/>	1	HN8055Q-XXXX-XX	有効	32	有効	設定済み

SSID設定詳細

SSID名: * (1-32文字)

SSIDの有効化:

接続デバイス数: * (1-32)

SSIDのプロードキャスト:

WMMの有効化:

認証モード:

暗号化モード:

WPA PreSharedKey: 非表示 * (8-63文字または64文字(16進文字))

WPAグループキー更新間隔: * (600 ~ 86400秒)

WPSを有効にする:

WPSモード:

PBC:

適用
キャンセル

2. [適用]をクリックします。

表 8-13で、2.4G基本ワイヤレスネットワーク設定について説明します。

表 8-13 2.4G 基本ワイヤレスネットワーク設定

パラメータ	説明
WLANの有効化	ワイヤレスネットワークを有効にするかどうかを指定します。以下のパラメータは、ワイヤレスネットワークが有効になっている場合にのみ設定できます。
SSID名	ワイヤレスネットワークの名前を指定します。これは、各種ワイヤレスネットワークを区別するために使用されます。タブ文字無しで、最大32文字から構成されます。
SSIDの有効化	接続を有効にするかどうかを指定します。
接続デバイス数	STAの数を指定します。1 ~ 32の範囲で指定します。
SSIDのブロードキャスト	ブロードキャストを有効にするか非表示にするかを指定します。 <ul style="list-style-type: none"> ● このオプションボックスを選択した場合、SSIDのブロードキャスト機能が有効になるように指定されます。ONTは、SSID、すなわちワイヤレスネットワークの名前を定期的にブロードキャストします。このような方法で、STAはワイヤレスネットワークを検索できます。 ● このオプションボックスを選択しなかった場合は、SSIDのブロードキャスト機能が無効になるように指定されます。SSIDを非表示にすると、STAはワイヤレスネットワークを検索できなくなり、SSIDは要求しない限り取得できなくなります。
WMMの有効化	Wi-Fiマルチメディアを有効にするかどうかを指定します。
認証モード	ワイヤレスネットワークへのアクセスを要求するSTAの認証モードを指定します。このモードは、オープン、共有、WPA Pre-Shared Key、WPA2 Pre-Shared Key、WPA/WPA2 Pre-Shared Key、WPAエンタープライズ、WPA2エンタープライズ、WPA/WPA2エンタープライズから指定できます。これは、デフォルトでは、WPA/WPA2 Pre-Shared Keyに設定されています。
暗号化モード	ワイヤレスネットワークへのアクセスを要求するSTAの暗号化モードを指定します。暗号化モードと暗号化パラメータは、認証モードによって異なります。 <ul style="list-style-type: none"> ● 認証モードがオープンに設定されている場合、暗号化モードはNoneまたはWEPに設定できます。 ● 認証モードが共有に設定されている場合、暗号化モードはWEPに設定できます。 ● 認証モードがWPA Pre-Shared Key、WPA2 Pre-Shared Key、WPA/WPA2 Pre-Shared Key、WPAエンタープライズ、WPA2エンタープライズ、WPA/WPA2エンタープライズに設定されている場合、暗号化モードはAES、TKIP、TKIP&AESに設定できます。

パラメータ	説明
WPA PreSharedKey	WPA共有キーを指定します。有効な値は、8 ～ 63のASCIIコードまたは64の16進数字から構成されます。
WPAグループキー更新 間隔	WPAグループキーを生成する間隔を指定します。単位は秒です。有効な値の範囲は600 ～ 86400です。
WPSを有効にする	WPSを有効にするかどうかを指定します。
WPSモード	WPSモードを指定します。有効な値は、PBC、PIN、AP-PINです。
PBC	WPSモードがPBCに設定されている場合は、WPSを起動を選択してPBCモードを開始することができます。

8.5.7.2 2.4G 詳細ネットワーク設定

1. 左側のナビゲーションツリーから[詳細設定] > [WLAN] > [2.4G詳細ネットワーク設定]を選択します。右側のメイン表示部分で、[図 8-46](#)に示すように、パラメータを設定します。



[WLANの有効化] が [2.4G詳細ネットワーク設定]で選択されていない場合、このページは空白になります。

図 8-46 2.4G 詳細ネットワーク設定

2.4G詳細ネットワーク設定

このページでは、2.4GHz帯ワイヤレスネットワークの拡張パラメータの設定ができます。2.4GHz帯ワイヤレスネットワークが無効化されている場合、このページは空白です。

⚠警告:
ワイヤレスネットワークパラメータを変更するとワイヤレスネットワークサービスが一時的に中断される可能性があります。

詳細設定

送信出力:	<input type="text" value="100%"/>	▼
規制区域:	<input type="text"/>	▼
チャンネル:	<input type="text" value="自動"/>	▼
チャンネル幅:	<input type="text" value="Auto 20/40 MHz"/>	▼
モード:	<input type="text" value="802.11b/g/n"/>	▼
DTIM間隔:	<input type="text" value="1"/>	(1~255、デフォルト: 1)
ビーコン間隔:	<input type="text" value="100"/>	(20~1000ミリ秒、デフォルト: 100)
RTS閾値:	<input type="text" value="2346"/>	(1~2346バイト、デフォルト: 2346)
フラグメント閾値:	<input type="text" value="2346"/>	(256~2346バイト、デフォルト: 2346)

2. [適用]をクリックします。

表 8-14 で、ワイヤレスネットワークの拡張パラメータについて説明します。

表 8-14 ワイヤレスネットワークの拡張パラメータ

パラメータ	説明
送信出力	無線信号の送信光出力を指定します。これは、20%、40%、60%、80%、100%に設定できます。値が大きくなればなるほど、無線信号のカバレッジが向上します。
チャンネル	ワイヤレスネットワークのチャンネルを指定します。チャンネルは、自動の値によって異なります。
チャンネル幅	無線のチャンネル幅を指定します。これは、Auto 20/40 MHz、20 MHz、40 MHz、Auto 20/40/80 MHzに設定できます。
モード	サポートされるワイヤレスネットワークモードを指定します。これは、802.11b、802.11g、802.11b/g、802.11b/g/nに設定できます。

パラメータ	説明
DTIM間隔	DTIMの送信間隔を指定します。値の範囲は1 ~ 255で、デフォルト値は1です。
ビーコン間隔	ビーコンの送信間隔を指定します。ビーコンは、他のアクセスポイントデバイスまたはネットワーク制御デバイスとの通信に使用されます。値の範囲は20ms ~ 1000msで、デフォルト値は100msです。
RTS閾値	送信要求(RTS)の閾値を指定します。これは、無線LANのデータ伝送での競合を回避するために使用されます。 RTS閾値が小さければ小さいほど、RTSパケットの伝送周波数が高くなり、中断や競合からのシステム復旧が早くなります。ただし、使用される帯域幅が大きくなり、これは他のネットワークデータパケットのスループットに影響します。 値の範囲は1バイト ~ 2346バイトで、デフォルト値は2346バイトです。
フラグメント閾値	フラグメント閾値を指定します。パケットのサイズがこの閾値よりも大きい場合、パケットは分割されます。フラグメントの伝送が中断されると、正常に伝送されなかった部分のみ、再伝送される必要があります。 値の範囲は256バイト ~ 2346バイトで、デフォルト値は 2346バイトです。

8.5.7.3 5G 基本ネットワーク設定

1. 左側のナビゲーションツリーから[詳細設定] > [WLAN] > [5G基本ネットワーク設定]を選択します。右側のメイン表示部分で、[WLANの有効化]オプションボックスを選択します。表示されるダイアログボックスで、[図 8-47](#)に示すように、SSID、認証モード、暗号化モードなどの基本Wi-Fiパラメータを設定します。

図 8-47 5G 基本ネットワーク設定

5G基本ネットワーク設定

このページでは、5GHz帯ワイヤレスネットワークの基本パラメータの設定ができます。5GHz帯ワイヤレスネットワークが無効化されている場合、このページは空白です。

警告:

- ワイヤレスネットワークパラメータを変更するとワイヤレスネットワークサービスが一時的に中断される可能性があります。
- セキュリティ保護のため、WPA2または WPA/WPA2認証モードを使用することをお勧めします。

WLANの有効化

新規作成
削除

	SSIDインデックス	SSID名	SSIDの状態	接続デバイス数	SSIDのブロードキャスト	セキュリティ設定
<input type="checkbox"/>	5	realtalk-5000-kg	有効	32	有効	設定済み

SSID設定詳細

SSID名: * (1-32文字)

SSIDの有効化:

接続デバイス数: * (1-32)

SSIDのブロードキャスト:

WMMの有効化:

認証モード: ▼

暗号化モード: ▼

WPA PreSharedKey: 非表示 * (8-63文字または64文字(16進文字))

WPAグループキー更新間隔: * (600 ~ 86400秒)

WPSを有効にする:

WPSモード: ▼

PBC:

2. [適用]をクリックします。

表 8-15で、5G基本ワイヤレスネットワーク設定について説明します。

表 8-15 5G 基本ワイヤレスネットワーク設定

パラメータ	説明
WLANの有効化	ワイヤレスネットワークを有効にするかどうかを指定します。以下のパラメータは、ワイヤレスネットワークが有効になっている場合にのみ設定できます。
SSID名	ワイヤレスネットワークの名前を指定します。これは、各種ワイヤレスネットワークを区別するために使用されます。タブ文字無しで、最大32文字から構成されます。
SSIDの有効化	接続を有効にするかどうかを指定します。
接続デバイス数	STAの数を指定します。1 ~ 32の範囲で指定します。
SSIDのブロードキャスト	ブロードキャストを有効にするか非表示にするかを指定します。 <ul style="list-style-type: none"> ● このオプションボックスを選択した場合、SSIDのブロードキャスト機能が有効になるように指定されます。ONTは、SSID、すなわちワイヤレスネットワークの名前を定期的にブロードキャストします。このような方法で、STAはワイヤレスネットワークを検索できます。 ● このオプションボックスを選択しなかった場合は、SSIDのブロードキャスト機能が無効になるように指定されます。SSIDを非表示にすると、STAはワイヤレスネットワークを検索できなくなり、SSIDは要求しない限り取得できなくなります。
WMMの有効化	Wi-Fiマルチメディアを有効にするかどうかを指定します。
認証モード	ワイヤレスネットワークへのアクセスを要求するSTAの認証モードを指定します。このモードは、Open、Shared、WPA Pre-Shared Key、WPA2 Pre-Shared Key、WPA/WPA2 Pre-Shared Key、WPAエンタープライズ、WPA2エンタープライズ、WPA/WPA2エンタープライズから指定できます。これは、デフォルトでは、WPA/WPA2 Pre-Shared Keyに設定されています。
暗号化モード	ワイヤレスネットワークへのアクセスを要求するSTAの暗号化モードを指定します。暗号化モードと暗号化パラメータは、認証モードによって異なります。 <ul style="list-style-type: none"> ● 認証モードがOpenに設定されている場合、暗号化モードはNoneまたはWEPに設定できます。 ● 認証モードがSharedに設定されている場合、暗号化モードはWEPに設定できます。 ● 認証モードがWPA Pre-Shared Key、WPA2 Pre-Shared Key、WPA/WPA2 Pre-Shared Key、WPAエンタープライズ、WPA2エンタープライズ、WPA/WPA2エンタープライズに設定されている場合、暗号化モードはAES、TKIP、TKIP&AESに設定できます。

パラメータ	説明
WPA PreSharedKey	WPA共有キーを指定します。有効な値は、8 ～ 63のASCIIコードまたは64の16進数字から構成されます。
WPAグループキー更新間隔	WPAグループキーを生成する間隔を指定します。単位は秒です。有効な値の範囲は600 ～ 86400です。
WPSを有効にする	WPSを有効にするかどうかを指定します。
WPSモード	WPSモードを指定します。有効な値は、PBC、PIN、AP-PINです。
PIN	WPSモードがPINに設定されている場合は、PINのパスワードを入力する必要があります。

8.5.7.4 5G 詳細ネットワーク設定

1. 左側のナビゲーションツリーから[詳細設定] > [WLAN] > [5G詳細ネットワーク設定]を選択します。右側のメイン表示部分で、[図 8-48](#)に示すように、パラメータを設定します。



[WLANの有効化] が [5G詳細ネットワーク設定] で選択されていない場合、このページは空白になります。

図 8-48 5G 詳細ネットワーク設定

5G詳細ネットワーク設定

このページでは、5GHz帯ワイヤレスネットワークの拡張パラメータの設定ができます。5GHz帯ワイヤレスネットワークが無効化されている場合、このページは空白です。

警告:
ワイヤレスネットワークパラメータを変更するとワイヤレスネットワークサービスが一時的に中断される可能性があります。

詳細設定

送信出力:	<input type="text" value="100%"/>	▼
規制区域:	<input type="text"/>	▼
チャンネル:	<input type="text" value="自動"/>	▼
チャンネル幅:	<input type="text" value="Auto 20/40/80 MHz"/>	▼
モード:	<input type="text" value="802.11a/n/ac"/>	▼
DTIM間隔:	<input type="text" value="1"/>	(1~255、デフォルト: 1)
ビーコン間隔:	<input type="text" value="100"/>	(20~1000ミリ秒、デフォルト: 100)
RTS閾値:	<input type="text" value="2346"/>	(1~2346バイト、デフォルト: 2346)
フラグメント閾値:	<input type="text" value="2346"/>	(256~2346バイト、デフォルト: 2346)

2. [適用]をクリックします。

表 8-16で、ワイヤレスネットワークの拡張パラメータについて説明します。

表 8-16 5G ワイヤレスネットワークの拡張パラメータ

パラメータ	説明
送信出力	無線信号の送信光出力を指定します。これは、20%、40%、60%、80%、100%に設定できます。値が大きくなればなるほど、無線信号のカバレッジが向上します。
チャンネル	ワイヤレスネットワークのチャンネルを指定します。チャンネルは、自動の値によって異なります。
チャンネル幅	無線のチャンネル幅を指定します。これは、Auto 20/40 MHz、20 MHz、40 MHz、Auto 20/40/80 MHzに設定できます。
モード	サポートされるワイヤレスネットワークモードを指定します。これは、802.11a、802.11a/n、802.11acに設定できます。

パラメータ	説明
DTIM間隔	DTIMの送信間隔を指定します。値の範囲は1 ~ 255で、デフォルト値は1です。
ビーコン間隔	ビーコン送信間隔を指定します。ビーコンは、他のアクセスポイントデバイスまたはネットワーク制御デバイスとの通信に使用されます。値の範囲は20ms ~ 1000msで、デフォルト値は100msです。
RTS閾値	送信要求(RTS)の閾値を指定します。これは、無線LANのデータ伝送での競合を回避するために使用されます。 RTS閾値が小さければ小さいほど、RTSパケットの伝送周波数が高くなり、中断や競合からのシステム復旧が早くなります。ただし、使用される帯域幅が大きくなり、これは他のネットワークデータパケットのスループットに影響します。 値の範囲は1バイト ~ 2346バイトで、デフォルト値は2346バイトです。
フラグメント閾値	フラグメント閾値を指定します。パケットのサイズがこの閾値よりも大きい場合、パケットは分割されます。フラグメントの伝送が中断されると、正常に伝送されなかった部分のみ、再伝送される必要があります。 値の範囲は256バイト ~ 2346バイトで、デフォルト値は 2346バイトです。

8.5.7.5 WiFi 自動切断

1. 左側のナビゲーションツリーから[詳細設定] > [WLAN] > [WiFi自動切断]を選択します。右側のペインで、予定されたWiFi停止時間を設定し、WiFiネットワークが使用されていない場合は、WiFiネットワークが自動的に停止されます(図 8-49を参照)。

図 8-49 WiFi 自動切断

WiFi自動切断

この画面では、WiFi機能を使用していない間、自動で停止するように設定することができます。

自動停止の設定

WiFi自動停止を有効にする

	開始	終了	月曜日	火曜日	水曜日	木曜日	金曜日	土曜日	日曜日
1	18 : 00	23 : 00	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	07 : 00	09 : 00	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

2. [適用]をクリックします。

8.5.7.6 スマート WiFi カバレッジ管理

1. 左側のナビゲーションツリーから[詳細設定] > [WLAN] > [スマートWiFiカバレッジ管理]を選択します。右側のペインで、スマートWiFiカバレッジに使用するSSIDを指定し、特定の外部APデバイスを追加します(図 8-50を参照)。

図 8-50 スマート WiFi カバレッジ管理

スマートWiFiカバレッジ管理

このページでは、スマートWiFiカバレッジを管理できます。特にONTが外部のAPと連携し、WiFiネットワークを構築したり、WiFiのカバレッジを拡張することができます。

自動的にデフォルトSSIDを使用して、WiFi接続をAPにまで延長する
HN8055-XXXX-a

ローミングと切替設定

ローミングと切替を有効化:

強制的なRSSI切替閾値: dBm (範囲: -100 dBm ~ -66 dBm、デフォルト: -79 dBm)

条件によるRSSI切替閾値: dBm (範囲: -84 dBm ~ -60 dBm、デフォルト: -75 dBm)

外部APリスト

No.	デバイスモデル	シリアル番号	状態	オンライン時間	設定状態
--	--	--	--	--	--

2. [適用]をクリックします。

8.5.8 システム管理

ここでは、TR-069、アカウント管理、ご利用上の注意、ONT認証など、Webページでのシステムの管理方法について説明します。

8.5.8.1 TR-069

1. 左側のナビゲーションツリーから[詳細設定] > [システム管理] > [TR-069]を選択します。右側のペインで、図 8-51に示すようにONTとTR-069サーバ間の相互接続に関するパラメータを設定します。

図 8-51 TR-069

ACS設定

このページでは、ACSパラメータの設定、SSL証明書による認証用パスワードの設定、必要なSSL証明書のインポートが可能です。

ACSパラメータ設定

定期通知を有効にする:

通知間隔: *[1 - 2147483647](s)

通知時間: yyyy-mm-ddThh:mm:ss (例: 2009-12-20T12:23:34)

ACS URL: *

ACSユーザー名: *

ACSパスワード: *

接続要求ユーザー名: *

接続要求パスワード: *

DSCP: (0~63)

証明書認証の有効化と秘密鍵パスワードの設定

証明書認証を有効にする:

秘密鍵パスワード: (1-32文字。このパスワードはデバイスを再起動すると有効になります。)

パスワードの確認: (1-32文字。このパスワードはデバイスを再起動すると有効になります。)

証明書のインポート

証明書:



注記
ONTとTR-069サーバ間の相互接続を設定するには、WANインターフェースを作成する必要があります。また、WANインターフェースの[サービスの種類]にはTR069が含まれている必要があります。詳細は、[8.5.1 WAN設定](#)をご参照ください。

2. [適用]をクリックします。

表 8-17ではTR-069パラメータについて説明します。

表 8-17 TR-069 パラメータ

パラメータ	説明
ACSパラメータ設定	

パラメータ	説明
定期通知を有効にする	<p>通知機能を有効にするかどうかを指定します。</p> <ul style="list-style-type: none"> ● 通知機能を有効にすると、ONTが接続要求をTR-069サーバに自律的に送信します。 ● 通知機能を無効にすると、ONTが接続要求をTR-069サーバに自律的に送信しません。 <p>通知機能を有効にした場合、[通知間隔]および[通知時間]パラメータを設定できます。</p>
通知間隔	ONTがTR-069サーバに接続要求を送信する間隔を指定します。
通知時間	ONTがTR-069サーバに接続要求を送信する時間を指定します。
ACS URL	ONTが接続要求を送信するTR-069サーバのアドレスを指定します。
ACSユーザー名	ONTでTR-069サーバを登録する際のユーザー名を指定します。
ACSパスワード	ONTでTR-069サーバを登録する際のパスワードを指定します。
接続要求ユーザー名	TR-069サーバでONTに接続要求を発行する際のユーザー名を指定します。
接続要求パスワード	TR-069サーバでONTに接続要求を発行する際に送信されるパスワードを指定します。
DSCP	RFC2474 "Definition of the Differentiated Services Field"で定義されています。DSCP (Differentiated Services Code Point)では、優先度マーキングにコード値を使用します。DSCPでは、サービス要件に基づいて通信事業者ごとにカスタマイズ可能であるため、ネットワーク上のデバイスがDSCP値に基づいてQoSを実行できます。
証明書認証の有効化と秘密鍵パスワードの設定	
証明書認証を有効にする	ACSがSSL経由で接続されている場合に証明書を有効にします。
秘密鍵パスワード	証明書を有効にした後に秘密鍵パスワードを設定します。
パスワードの確認	パスワードを確認し、[秘密鍵パスワード]と同じであることを確認してください。
証明書のインポート	
証明書	通信事業者から提供された証明書ファイルを指定します。

8.5.8.2 アカウント管理

1. 左側のナビゲーションツリーから[詳細設定] > [システム管理] > [アカウント管理]を選択します。右側のメイン表示部分で、[図 8-52](#)に示すように、[admin]ユーザーのパスワードを変更します。

図 8-52 アカウント管理

アカウント管理

このページでは、あなたが一般ユーザのログインパスワードを変更することができ、あなたがアクセス ONT HTTPS SSL証明書の認証用パスワードと、対応するインポートSSL証明書を設定することができます。

パスワードの変更

ユーザー名:	admin	1.パスワードは少なくとも6文字で設定してください。 2.パスワードは次の条件を少なくとも2つ組み合わせて設定してください。 数字、大文字、小文字 特殊文字 (~!@#\$%^&*()-_+=+\\[{}];' "<, > / ?).
新しいパスワード:	●●●●	
パスワードの確認:	●●●●	3.パスワードにはユーザー名やユーザー名の順序を逆にしたものは使用できません。

証明書認証の有効化と秘密鍵パスワードの設定

証明書認証を有効にする:

秘密鍵パスワード: ●●●● (1-127文字。このパスワードはデバイスを再起動すると有効になります。)

パスワードの確認: ●●●● (1-127文字。このパスワードはデバイスを再起動すると有効になります。)

証明書のインポート

証明書:

2. [適用]をクリックします。

8.5.8.3 ご利用上の注意

左側のナビゲーションツリーから[詳細設定] > [システム管理] > [ご利用上の注意]を選択します。タブの右側に、[図 8-53](#)に示すような製品のご利用上の注意を表示できます。

図 8-53 ご利用上の注意

⚠ 危険
<ul style="list-style-type: none"> ■本製品は水や液体で濡らさないようにしてください。また、ケーブルの抜き差しは濡れた手でを行わないでください。ケーブルの抜き差しは、必ず機器を停止して、電源を切ってから行ってください。 ■万が一、本製品が濡れたり、発煙や異常な音、異臭などが発生した場合は、ただちに本製品の使用を中止して、電源を切り、全てのケーブル（電源ケーブルやネットワークケーブルなど）を抜いてください。本製品に異常がある場合は、サービス提供元が指定するお問い合わせ先にご連絡ください。 ■本製品を火気の近く、または高温になる場所で使用しないようにしてください。本体やケーブルが破損して火災や感電の原因となる可能性があります危険です。また、本製品は水周りまたは湿った場所のそばに置かないでください。 ■本製品を使用中に、あやまって落としてしまい故障した場合には、電源を切って、電源ケーブル、イーサネットケーブル、ネットワークケーブルなど全てのケーブルを抜いてください。また、本製品をぐらついた台の上や傾いたところなど、不安定な場所に置かないでください。 ■利用電圧は本製品の入力電圧の要件に適合している必要があります。また、付属の電源アダプタ以外は使用しないでください。使用すると本製品で異常が発生する可能性があります、危険です。 ■本製品の電源アダプタは、たこ足配線にしないでください。たこ足配線にするとテーブルタップなどが過熱、劣化する可能性があります、危険です。 ■感電またはその他の危険を回避するために、電源プラグは清潔で乾燥した状態を保ってください。 ■本製品は、縦置き設置として設計されていますので、横置きでの設置をしないでください。また横置きをして、他の物をその上に重ね置きをしないでください。熱や歪みにより本製品が損傷する場合があります。また、放熱のため、機器の周囲に少なくとも10cm以上のスペースを確保してください。 ■金属部品などの異物が通気孔から本製品に入らないようにしてください。また、通気孔を他の物で塞がないようにしてください。 ■引っかけた場所からはがれた塗装によって本製品に異常が発生するおそれがあるため、本製品の外装を引っかけたりしないでください。塗装が本製品に入ると、ショートするおそれがあります。また、はがれた塗装によって人体にアレルギー反応が発生するおそれがあります。 ■雷が発生した場合には、電源を切って、電源ケーブル、イーサネットケーブル、ネットワークケーブルなど全てのケーブルを抜いてください。 ■本製品を電子レンジ、冷蔵庫、携帯電話等、強力な磁場や磁界が発生する電子機器のそばに置かないでください。 ■部品や付属品を誤って飲み込むことがないように幼児の手の届かないところに設置してください。
⚠ 注意
<ul style="list-style-type: none"> ■本製品を設置する際にはメーカーの要件を必ず守ってください。 ■本製品はレーザー製品です。保護メガネを着用せずに光ポートを直接覗きこんだりしないでください。 ■本製品を使用する環境温度については、本製品の“周囲温度”の仕様範囲内で使用してください。 ■本製品を移動する場合には、かならず電源ケーブルをコンセントからはずして移動してください。また、電源ケーブルをコンセントからはずす場合は、ケーブルをひっぱらずに電源プラグをつかんでコンセントからはずしてください。 ■本製品を長期間使用しない場合には、電源を切って電源プラグを抜いてください。 ■損傷のおそれがあるため、ケーブルを踏みつけたり、引っ張ったり、引きずったり、無理やり曲げたりしないでください。ケーブルが損傷すると、本製品が故障するおそれがあります。 ■損傷または劣化したケーブルは使用しないでください。 ■本製品を勝手に分解しないでください。本製品に異常がある場合は、サービス提供元が指定するお問い合わせ先にご連絡ください。 ■本製品を使用するにあたり、ほこりの多い場所に置かないでください。 ■本製品は清潔な状態に保ってください。本製品のほこり、よごれをふきとる場合、濡れた布ではなく乾いた布などでふきとってください。なお、本製品を清掃する前に、本製品を停止し、電源を切って、本製品から電源ケーブルやネットワークケーブルなどすべてのケーブルを抜いてください。 ■クリーニング液またはスプレー式洗浄剤を使用して本製品の外装を清掃しないでください。柔らかい布を使用して清掃してください。 ■本製品をテレビ、ラジオなどの近くで使用する場合、影響を与えることがあります。 ■本製品がご不要になった際は、サービス提供元が指定するお問い合わせ先にご連絡ください。 ■ネットワークケーブル、電源アダプタ、電源アダプタケーブルは屋外に設置しないでください。こうした対策をしておくことで、雷の場合に発生しやすい機器の損傷や人体への損傷を防ぐことができます。

図 8-54 ソフトウェア情報

⚠ ソフトウェア情報
<p>本製品に関するソフトウェア情報については こちら をご参照ください。</p>

8.5.8.4 ONT 認証

1. 左側のナビゲーションツリーから[詳細設定] > [システム管理] > [ONT認証]を選択します。右側のペインで、[図 8-55](#)に示すようにOLT上でのONTの登録時の認証モードを確認または変更できます。

図 8-55 ONT 認証

2. [適用]をクリックします。

8.5.9 保守診断

ここでは、システムの保守や診断方法について説明します。

8.5.9.1 ファームウェアアップグレード

1. 左側のナビゲーションツリーから[詳細設定] > [保守診断] > [ファームウェアアップグレード]を選択します。右側のペインで[参照...]をクリックします。表示されたダイアログボックスで、デバイスの対象ソフトウェアバージョンを選択します。[図 8-56](#)に示すように[アップグレード]をクリックして、デバイスのソフトウェアをアップグレードします。

図 8-56 ファームウェアアップグレード

 [参照...] [アップグレード]"/>

2. アップグレードに成功すると、デバイスのリセットが必要であることを示すメッセージが表示されます。[再起動]をクリックします。設定データはデバイスのリセット後に有効になります。

8.5.9.2 設定ファイル管理

左側のナビゲーションツリーから[詳細設定] > [保守診断] > [設定ファイル管理]を選択します。右側のメイン表示部分で、[図 8-57](#)に示すように、必要に応じてボタンを選択します。

図 8-57 設定ファイル管理



- 設定ファイルをフラッシュメモリに保存するには、[保存]を選択します。これにより、本機器の再起動によってデータが失われなくなります。
- 設定ファイルを保存し、ONTを再起動するには、[保存と再起動]を選択します。
- [設定ファイルのダウンロード]をクリックします。表示されたダイアログボックスで、[保存]をクリックし、設定ファイルの保存先を指定し、ファイルをローカルディスクにバックアップします。
- [設定ファイル]テキストボックスの横に表示されている[参照...]をクリックします。表示されたダイアログボックスから、アップロードする設定ファイルを選択します。[設定ファイルのアップデート]をクリックして、ローカルディスクに保存されている設定ファイルをアップロードします。設定ファイルのアップロードに成功すると、デバイスは自動的に再起動され、新しい設定が有効になります。



注意事項

設定ファイルをアップロードする際には、必ず正しい種類の設定ファイルを選択してください。ただし、選択された設定ファイルの種類および名前は本デバイス内に保存されているファイルと同じにすることはできません。同じにすると、設定ファイルはアップロードできません。

8.5.9.3 保守

左側のナビゲーションツリーから[詳細設定] > [保守診断] > [保守]を選択します。

1. 右側のメイン表示部分で、[ターゲット] および [WAN名]に、[図 8-58](#)に示すように、ターゲットのIPアドレスまたはホスト名を入力し、[開始]を選択します。

図 8-58 Ping テスト

保守

このページではLANやインターネット接続を確認する保守診断機能とメインチップの基本機能を使用することができます。

注意：ハードウェア障害検出では、一部のハードウェア障害を検出できない場合があります。この操作はHuaweiの保守エンジニアのみが対象です。この操作は注意して行う必要があります。ハードウェアの障害検出時は、データ通信サービスが中断されます。

Pingテスト

ターゲット:	<input type="text" value="10.167.166.50"/>	*
WAN名:	<input type="text" value="1_TR069_INTERNET_R_VID_10"/>	
データブロックサイズ:	<input type="text" value="56"/>	(32-65500、入力なしのデフォルト: 56)
繰り返し:	<input type="text" value="4"/>	(1-3600、入力なしのデフォルト: 4)
最大タイムアウト時間:	<input type="text" value="10"/>	(1-4294967s、入力なしのデフォルト: 10)
DSCP値:	<input type="text" value="0"/>	(0-63、入力なしのデフォルト: 0)

トレースルートテスト

ターゲット:	<input type="text" value="10.167.166.50"/>	*
WAN名:	<input type="text" value="1_TR069_INTERNET_R_VID_10"/>	
データブロックサイズ:	<input type="text" value="38"/>	(38-32768、入力なしのデフォルト: 38)

- Pingテストが成功した場合、テスト結果が表示されます。すなわち、ONTは送信先のIPアドレスを使用して本機器と相互作用できます。
 - Pingテストが失敗した場合、[結果]が[失敗]として表示されます。すなわち、ONTは送信先のIPアドレスを使用して本機器と相互作用できません。
2. 右側のメイン表示部分で、[図 8-59](#)に示すように、[ハードウェア障害検出]を選択してハードウェア障害検出を開始します。

図 8-59 ハードウェア障害検出

ハードウェア障害検出

8.5.9.4 ログ

左側のナビゲーションツリーから[詳細設定] > [保守診断] > [ログ]を選択します。右側のメイン表示部分で、[ログファイルのダウンロード]を選択します。表示されるダイアログボックスで、[図 8-60](#)に示すように、[保存]を選択し、ログファイルの保存パスを指定し、そのログファイルをローカルディスクに保存します。

図 8-60 ログ

ユーザーログ

このページでは、ユーザーログの設定、ダウンロード、照会が可能です。

ログ保存の有効化

ログの保存:

ログレベル: デバッグ ▾

適用 キャンセル

ログのダウンロードと表示

ログファイルのダウンロード

ログ種別: 全てのログ ▾

```
Manufacturer:Huawei Technologies Co., Ltd;
ProductClass:HN8055Q;
SerialNumber:6877687700000001;
IP:192.168.1.1;
HWVer:788.A;
SWVer:V3R016C00S007;
1970-01-01 00:00:14 [Error][アラームログ] AlarmID:104001,AlarmLevel:Error,Device reset. Cause: ONU
1970-01-01 00:01:12 [Critical][構成ログ] Terminal:CLI(127.0.0.1),Result:Fail,Type:Login,Username:
1970-01-01 00:01:15 [Critical][構成ログ] Terminal:CLI(127.0.0.1),Result:Success,Type:Login,Username:roc
1970-01-01 00:00:14 [Error][アラームログ] AlarmID:104001,AlarmLevel:Error,Device reset. Cause: ONU
1970-01-01 00:00:15 [Error][アラームログ] AlarmID:104001,AlarmLevel:Error,Device reset. Cause: ONU
1970-01-01 00:00:17 [Error][アラームログ] AlarmID:104001,AlarmLevel:Error,Device reset. Cause: ONU
1970-01-01 00:01:11 [Critical][構成ログ] Terminal:CLI(127.0.0.1),Result:Success,Type:Login,Username:roc
1970-01-01 00:01:12 [Critical][シェルログ] Terminal:CLI(127.0.0.1),Result:Success,Cmd:su
1970-01-01 00:01:13 [Critical][シェルログ] Terminal:CLI(127.0.0.1),Result:Success,Cmd:shell
1970-01-01 00:08:06 [Critical][シェルログ] Terminal:CLI(127.0.0.1),Result:Success,Cmd:exit
```

8.5.9.5 障害情報の収集

左側のナビゲーションツリーから[詳細設定] > [保守診断] > [障害情報の収集]を選択します。[図 8-61](#)に示すように右側のペインで、[開始]をクリックしてONT障害情報を収集します。

図 8-61 障害情報の収集



情報を収集したら、[ダウンロード]をクリックして収集された情報をローカルのディレクトリにダウンロードします。

8.5.9.6 リモートミラーリング

1. 左側のナビゲーションツリーから[詳細設定] > [保守診断] > [リモートミラーリング]を選択します。

図 8-62 リモートミラーリング



この設定に基づいて、CPUで送受信されるパケットをリモートでキャプチャして分析できます。

- 送信元IPアドレス: リモートミラーリングを実行するWANポートのIPアドレスを指定します。
- 宛先IPアドレス: 結果を保存するホストのIPアドレスを指定します。

2. [開始]をクリックします。



ユーザーの要件に基づいて、この機能ではネットワーク操作とサービス保護を目的としてユーザーの通信に関する情報を使用、取得、保存する場合があります。ただし、Huaweiのみでユーザーの通信内容の収集または保存はできません。傍受関連の機能については、目的や使用範囲の観点で適用法や規制に基づいて有効にすることをお勧めします。内容の利用中および保存中にユーザーの通信内容を完全に保護できる有効な対策を行うことが必要です。