

ZXHN F660A
取扱説明書
V1.0

Copy Right

本資料の著作権はZTE Corporationが有します。弊社の許可なく書類をコピー、引用あるいは翻訳は違反となります。

本製品は環境保護および人身安全保護視点から設計されています。製品の保存、使用と廃棄はユーザーマニュアル、関連契約および所在国の法律に基づいて行ってください。
本製品の更新および技術変更は、別途通知しないものとさせていただきます。

Copyright © 2013 ZTE CORPORATION.

注意事項

本機器の最新のファームウェアが提供された場合、最新バージョンにアップデートされます。
その際は、機器が自動的に再起動されその間、一時的にインターネットなどのご利用がいただけません。
実施のお知らせなど詳しくは、サービス提供元が指定するお問い合わせ先にご確認ください。

資料コード: SJ-20150325134200-001

リリース日: 2015/03/31 (R1.0.1)

目次

1	製品概要	1
1.1	安全注意事項	1
1.2	包装明細書	2
1.3	LED 表示	3
1.4	ポート	4
1.5	製品仕様	5
1.6	技術仕様	7
1.7	スタンドとファイバーカバーの取り付け	7
2	設定の準備	11
2.1	設定の準備作業	11
2.2	TCP/IP 設定	11
2.3	本製品のログイン	13
3	デバイスの状態	13
3.1	デバイス情報	13
3.2	ネットワークインタフェース情報	13
3.2.1	WAN 接続情報	14
3.2.2	PON 情報	14
3.3	ユーザーインタフェース情報	15
3.3.1	イーサネットインタフェース情報	15
3.3.2	無線 LAN RF2.4G インタフェース情報	17
3.3.3	無線 LAN RF5G インタフェース情報	17
3.3.4	USB インタフェース情報	18
4	ネットワーク設定	19
4.1	無線 LAN RF2.4G の設定	19
4.1.1	無線 LAN RF2.4G 基本パラメータの設定	19
4.1.2	SSID の設定	20
4.1.3	無線 LAN セキュリティ属性の設定	21
4.1.4	アクセス制御リストの設定	22
4.1.5	接続中の機器の確認	23
4.1.6	WPS 機能の設定	24
4.2	無線 LAN RF5G の設定	24
4.2.1	無線 LAN RF5G 基本パラメータの設定	25
4.2.2	SSID の設定	26
4.2.3	無線 LAN セキュリティ属性の設定	27
4.2.4	アクセス制御リストの設定	28
4.2.5	接続中の機器の確認	28
4.2.6	WPS 機能の設定	29
4.3	LAN の設定	30
4.3.1	静的アドレスの設定	30
4.3.2	動的 IPv4 アドレスの設定	31
4.3.3	動的 IPv6 アドレスの設定	33

4.3.4	スタティックプレフィックスの設定	35
4.3.5	プレフィックスデリゲーション方式の設定	36
4.3.6	RA サービスの設定	37
5	セキュリティ設定	38
5.1	ファイアウォールの設定	38
5.2	IP フィルタの設定	39
5.3	MAC フィルタの設定	40
5.4	URL フィルタの設定	42
5.5	アクセス制御の設定	42
5.6	ALG スイッチの設定	44
6	アプリケーションの設定	44
6.1	DMZ の設定	44
6.2	UPnP の設定	45
6.3	UPnP ポートマッピングの確認	46
6.4	仮想ホストの設定	47
6.5	DNS サービスの設定	48
6.5.1	ドメイン名の設定	48
6.5.2	ホスト名の設定	49
6.5.3	DNS サーバの設定	50
6.6	SNTP(時刻同期)設定	50
6.7	USB ストレージの容量確認	51
6.8	メディア共有	52
6.9	FTP 設定	53
6.9.1	FTP サーバ設定	53
6.9.2	FTP クライアント設定	53
6.10	ポートトリガーの設定	55
6.11	ポートフォワーディング(アプリケーションリスト)の設定	56
6.12	アプリケーションリストの設定	57
6.13	ホーム共有(samba)	59
7	管理の設定	60
7.1	ユーザー管理の設定	60
7.2	システム管理	61
7.2.1	リモートアップデートの設定	61
7.2.2	リセット	62
7.3	ログ管理の設定	62
7.4	診断メンテナンス	63
7.4.1	Ping 診断の設定	63
7.4.2	Trace Route 診断の設定	64
8	Q&A	66
8.1	Q&A	66
9	略語リスト	67

1 製品概要

1.1 安全注意事項

注意事項

- ・同梱されている電源アダプタとLANケーブル等をお使いください。
- ・ACアダプタとその電源コードを傷つけたり、破損、加工、無理な力(曲げる、引っ張る、ねじる、束ねる)を加えないでください。火災、感電の原因となります。
- ・利用電圧は本製品の入力電圧を満たす必要があります(電圧フリッカ10%以下)。
- ・感電等の危険を防ぐため、電源プラグを清潔にかつ、乾いた状態を保ってください。
- ・落雷による事故を防ぐため、雷雨時は必ず電源プラグを抜いてください。
- ・長時間設備を使用しない場合は、電源を切り、電源プラグを抜いてください。
- ・本製品を分解しないでください。通電したとき危険です。
- ・視力保護のため、光ポートを直接目で見ないでください。
- ・万が一、使用中に煙、異常な音、異常な匂い等が出た場合、すぐに本製品のACアダプタをコンセントから抜き、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。

※ご利用前に上記注意事項をお読みください。上記注意事項以外の利用方法で事故が発生した場合は、原則免責とさせていただきます。

使用環境

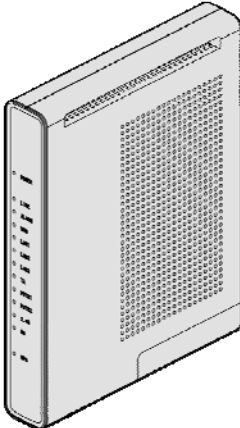
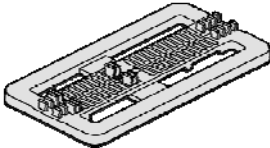
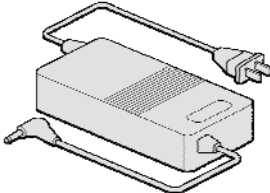
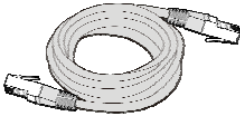

- ・直射日光を避け、本製品を通気性の良い場所に設置してください。
- ・本製品を乾燥している場所に設置し、熱源、水回りの近くへの設置は避けてください。。
- ・本製品の上にはものを置かないでください。圧力による破損の恐れがあります。
- ・熱源、水周りの近くに設置しないでください。
- ・本製品設置時は電気製品・AV・OA機器などの磁気を帯びている場所や電磁波が発生している場所(電子レンジ、スピーカ、テレビ、ラジオ、蛍光灯、電気こたつ、インバータエアコン、電磁調理器など)を避けてください。

本製品についてのご願い

本製品がご不要になった際には、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。

1.2 包装明細書

下記の部品が同梱されていることをご確認ください。

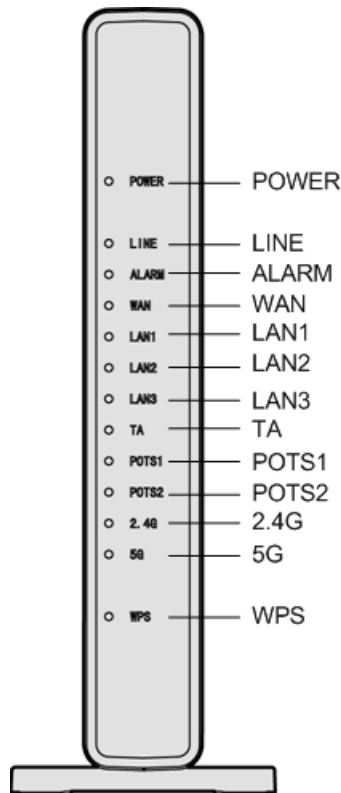
名前	数量	図
ZXHN F660A本体	1台	
ZXHN F660Aスタンド	1個	
電源アダプタ	1個	
RJ-45ケーブル	1本	
簡易ユーザーガイド	1冊	

※設置を始める前に、構成部品がすべてそろっていることを確認してください。

不足しているもの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。

1.3 LED表示

図 1-1 ZXHN F660A LED



LEDの内容については表1-1を参照してください。

表 1-1 正面 LED 表示説明

LED表示	色	説明
POWER	緑	消灯:電源オフ 点灯:電源オン
LINE	緑	消灯:回線がアクティブではありません 点灯:回線がアクティブになっています 早い点滅(2回/秒):回線の認証中です 遅い点滅(1回/秒):ONUがファームアップ中です
ALARM	赤	消灯:ONUが受信した光信号の出力が正常です 点灯:ONU PONポート光出力が電源オフになっています 点滅:ONUが受信した光信号の出力が光受信機の感度を下回っています
WAN	緑	消灯:インターネット接続がありません 点灯:接続が確立され、IPアドレスを取得しました 点滅:データ受信中です
LAN1、LAN2、LAN3、	緑	消灯:LANポートに設備が接続されていません

LED表示	色	説明
TA		点灯: LANポートに設備が接続されていますが、データ 受送信がありません 点滅: データ受送信中です
2.4G	緑	消灯: WIFI機能オフ 点灯: WIFI機能オン 点滅: データ受送信中です
5G	緑	消灯: WIFI機能オフ 点灯: WIFI機能オン 点滅: データ受送信中です
WPS	赤、黄、緑	消灯: WPSのオートネゴシエーションがされていません 黄色点灯: オートネゴシエーション中 緑色点灯: オートネゴシエーションが成功しました 赤色点灯: セッション・オーバーラッピング検査または オートネゴシエーションが失敗しました

1.4 ポート

図 1-2 ZXHN F660A 背面ポートとボタン

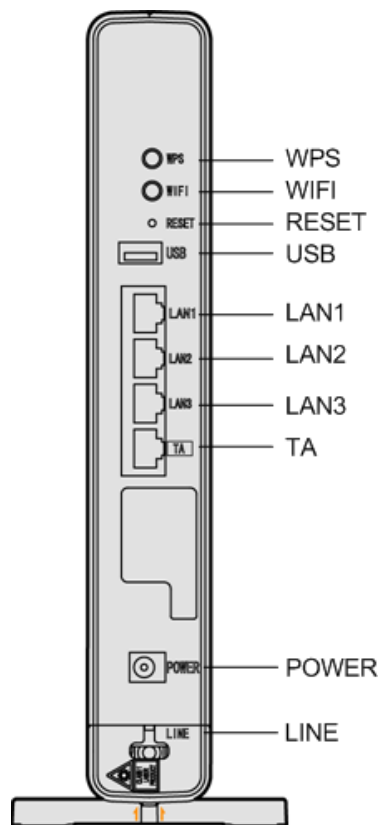


表 1-2 裏面ポートとボタンの説明

ポート、ボタン	説明
LINE	PON接続ポート、光ファイバーでインターネットに接続します。
POWER	電源入力。電源アダプタに接続します。
TA	IP電話ポート、RJ-45ケーブル経由でIP電話機に接続します。
LAN1、LAN2、LAN3	イーサネットポート、RJ-45ケーブル経由でPCに接続します。
WIFI	WIFI機能ボタン、WIFI機能のオン/オフを行います。
WPS	WIFI保護設置機能ボタン、WPS対応端末との接続時に本ボタンを押すことで接続を容易に行うことができます。
RESET	リセットボタンです。設備が通電した状態で細い針などで押し、5秒以内に離せば、設備がリセットされます。リセット後もユーザー設定情報は失われません。5秒以上長押しすれば、工場出荷設定に戻してリセットします。
USB	標準USB2.0ポート、USB 2.0互換設備に接続できます。

1.5 製品仕様

表 1-3 製品仕様

WAN インターフェイス	
ポート数	GPON Port × 1
通信方式	ITU-T G.984 準拠
物理インタフェース	UPC/SC
LAN インターフェイス	
ポート数	10BASE-T/100BASE-TX/1000BASE-T × 3
規格	IEEE802.3/IEEE802.3u/IEEE802.3ab
全二重/半二重	自動検出
MDI/MDI-X	自動検出
物理インタフェース	RJ-45
VOIP インターフェイス	
ポート数	10BASE-T/100BASE-TX/1000BASE-T × 1
規格	IEEE802.3/IEEE802.3u/IEEE802.3ab

規格	自動検出
全二重/半二重	自動検出
MDI/MDI-X	自動検出
無線LANインタフェース	
IEEE802.11n	
周波数帯域/チャンネル	2.4GHz帯 (2,400-2,484 MHz) / 1~13ch
伝送方式	OFDM(直交周波数分割方式)/搬送波数[HT20] 56、 [HT40] 114 MIMO(空間多重)方式
伝送速度	2.4GHz帯 最大450 Mbps
周波数帯域/チャンネル	5GHz帯(5.15-5.729 MHz) 5.2G ch 36/40/44/48 5.3G ch 52/56/60/64 5.6G ch 100/104/108/112/116/120/124/128/132/136/140
伝送方式	OFDM(直交周波数分割方式)/搬送波数[HT20] 56、 [HT40] 114 MIMO(空間多重)方式
伝送速度	5GHz帯 最大450 Mbps
IEEE802.11b	
周波数帯域/チャンネル	2.4GHz帯 (2,400-2,484 MHz) / 1~13ch
伝送方式	DS-SS(スペクトラム直接拡散)方式
伝送速度	11/5.5/2/1 Mbps(自動フォールバック)
IEEE802.11g	
周波数帯域/チャンネル	2.4GHz帯 (2,400-2,484 MHz)/1~13ch
伝送方式	OFDM(直接周波数分割多重)方式/搬送波数 52
伝送速度	54/48/36/24/18/12/9/6 Mbps(自動フォールバック)
IEEE802.11a	
周波数帯域/チャンネル	5GHz帯(5.15-5.729 MHz) 5.2G ch 36/40/44/48 5.3G ch 52/56/60/64 5.6G ch 100/104/108/112/116/120/124/128/132/136/140
伝送方式	OFDM(直接周波数分割多重)方式/搬送波数 52

伝送速度	54/48/36/24/18/12/9/6 Mbps(自動フォールバック)
アンテナ	送信3×受信3(内蔵アンテナ)
セキュリティ	SSID MAC address filtering、WEP(128/64bit)、WPA-PSK(TKIP、AES)、WPA2-PSK(TKIP、AES)
IEEE802.11ac	
周波数帯域/チャンネル	5GHz帯(5.15-5.729 MHz, W52/W53/W56) 5.2G ch 36/40/44/48 5.3G ch 52/56/60/64 5.5G-5.7G ch 100/104/108/112/116/120/124/128/132/136/140
伝送方式	OFDM(直接周波数分割多重)方式/搬送波数 [VHT20]56/[VHT40]114/[VHT80]242 MIMO
伝送速度	5GHz帯(最大1.3Gbps)
アンテナ	送信3×受信3(内蔵アンテナ)
セキュリティ	SSID MAC address filtering、WEP(128/64bit)、WPA-PSK(TKIP、AES)、WPA2-PSK(TKIP、AES)

※規格による理論上の速度であり、ご利用の環境や接続機器などにより実際のデータ伝送速度は異なります。

1.6 技術仕様

表 1-4 技術仕様

項目	仕様
外観寸法	245 mm × 190 mm × 38 mm (H × W × D)
定格電流	2 A
定格電圧	12 V DC
動作温度	-5 °C ~ 40 °C
動作湿度	5% ~ 95%

1.7 スタンドとファイバーカバーの取り付け

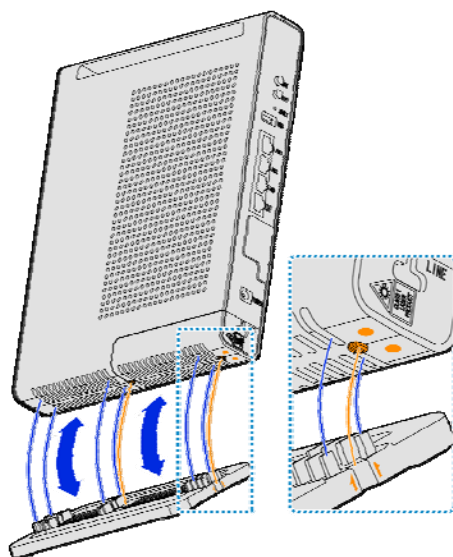
スタンドの取り付け

本製品はスタンドが付属しています。ご使用前にスタンドを取り付けて縦置きにしてください。

本体とスタンドの取り付け手順:

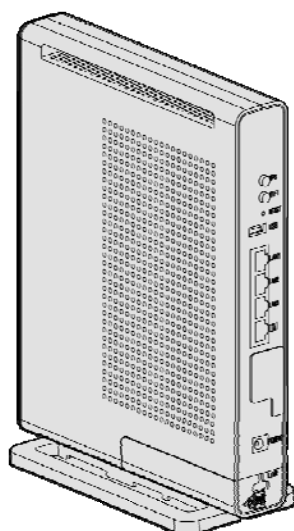
1. スタンドの矢印側を裏面(各ポートが入っている方向)に合わせ、散熱口に差し込みます。(図1-3)

図 1-3 スタンドの取り付け方



2.取り付けが正常に完了した場合、図1-4のようになります。

図 1-4 スタンドの取り付け完了



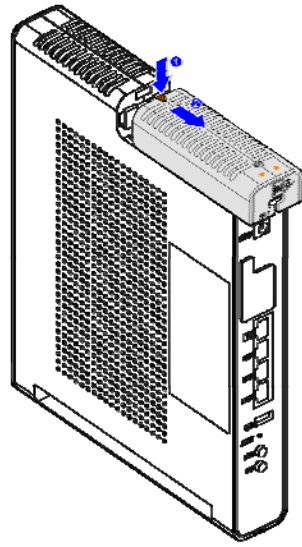
ファイバーカバーの取り付け

本製品はファイバー保護のため、ファイバーカバーを用意しています。

下記手順通りにファイバーカバーの開閉ができます。

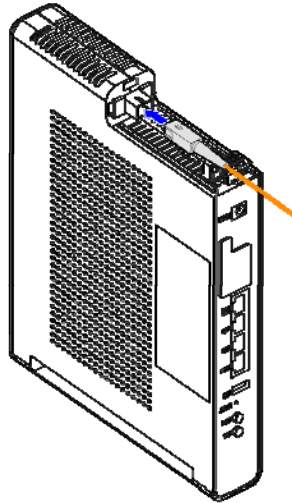
- 1.外に押しながら外側にファイバーカバーをスライドさせます。(図1-5)

図 1-5 ファイバーカバーの取り外し



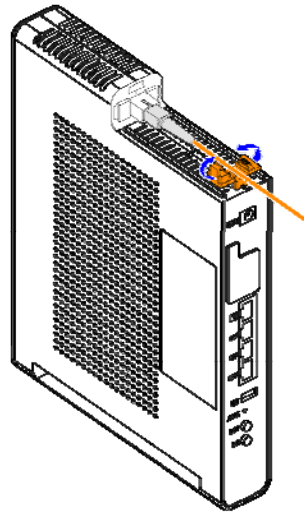
2.ファイバー末端部分をコネクタ端子に差し込みます。(図1-6)

図 1-6 ファイバー端子の差し込み



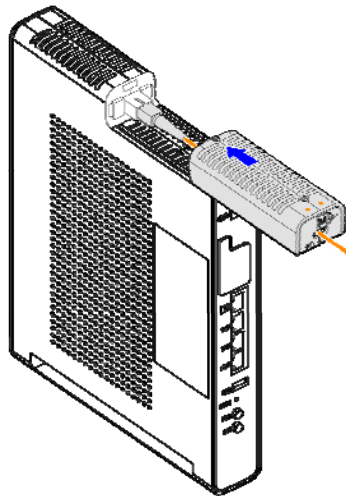
3.ファイバーを固定します。(図1-7)

図 1-7 ファイバーの固定



4.ファイバーカバーを閉めます。(図1-8)

図 1-8 ファイバーカバーの取り付け



2 設定の準備

2.1 設定の準備作業

サービス提供元で初期設定が完了している為、接続後そのままご使用いただけます。設定を行う必要がある場合は、下記内容をご確認ください。

- ・本製品のいずれかのインターネットポートがパソコンと直接接続されていることをご確認ください。
- ・パソコンの TCP/IP 設定に問題ないかをご確認ください。
- ・ブラウザのプロキシ設定を無効にしてください。
- ・設定に必要な関連情報については、サービス提供元にお問い合わせください。

2.2 TCP/IP 設定

Windows XP 環境下での設定:

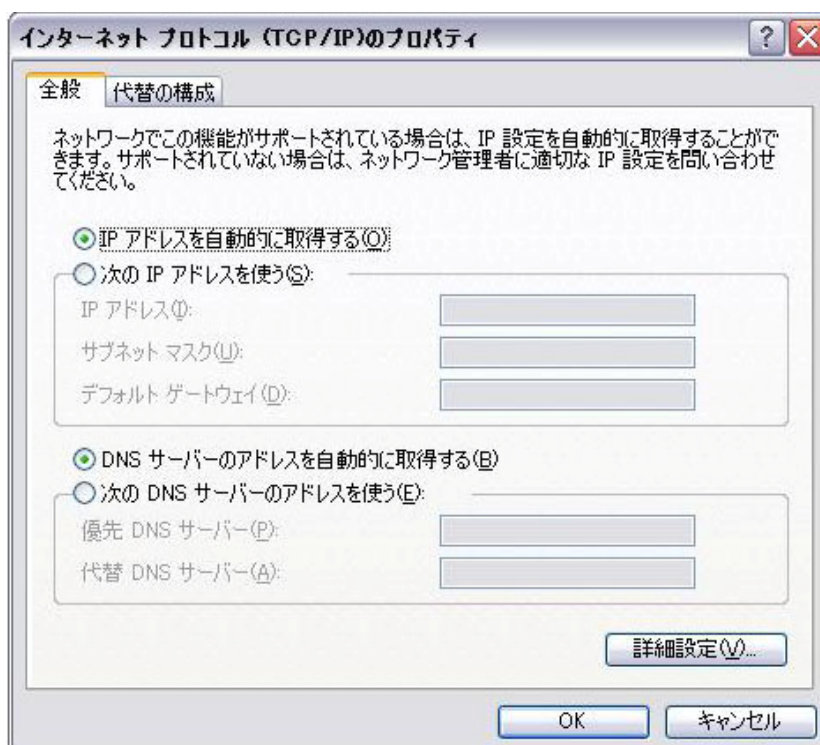
本製品のデフォルトネットワーク設定は以下の通りです。

- ・ IP アドレス: 192.168.1.1
- ・ サブネットマスク: 255.255.255.0

PC が本製品にアクセスできることをご確認ください。PC で設定する IP アドレスは本製品と同一の IP セグメント内にある必要があります。

1. Windows XP システムで、**スタート** > **コントロールパネル**を選択し、**コントロールパネル**ウィンドウを開きます。
2. **コントロールパネル**ウィンドウ内で**ネットワーク接続**をダブルクリックして、**ネットワーク接続**ウィンドウを開きます。
3. ネットワーク接続ウィンドウ内で、**ローカルエリア接続**をダブルクリックし、**ローカルエリア接続の状態**ダイアログボックスがポップアップ表示されることをご確認ください。
4. **全般**タブで**インターネットプロトコル(TCP/IP)**を選択し、**プロパティ**ボタンをクリックし、**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ポップアップ表示されることをご確認ください。
5. 図 2-1 のように IP アドレスを自動的に取得する、DNS サーバーのアドレスを自動的に取得する を選択してください。

図 2-1 インターネットプロトコル(TCP/IP)のプロパティ画面



6. OK ボタンをクリックします。

Windows 7環境下での設定：

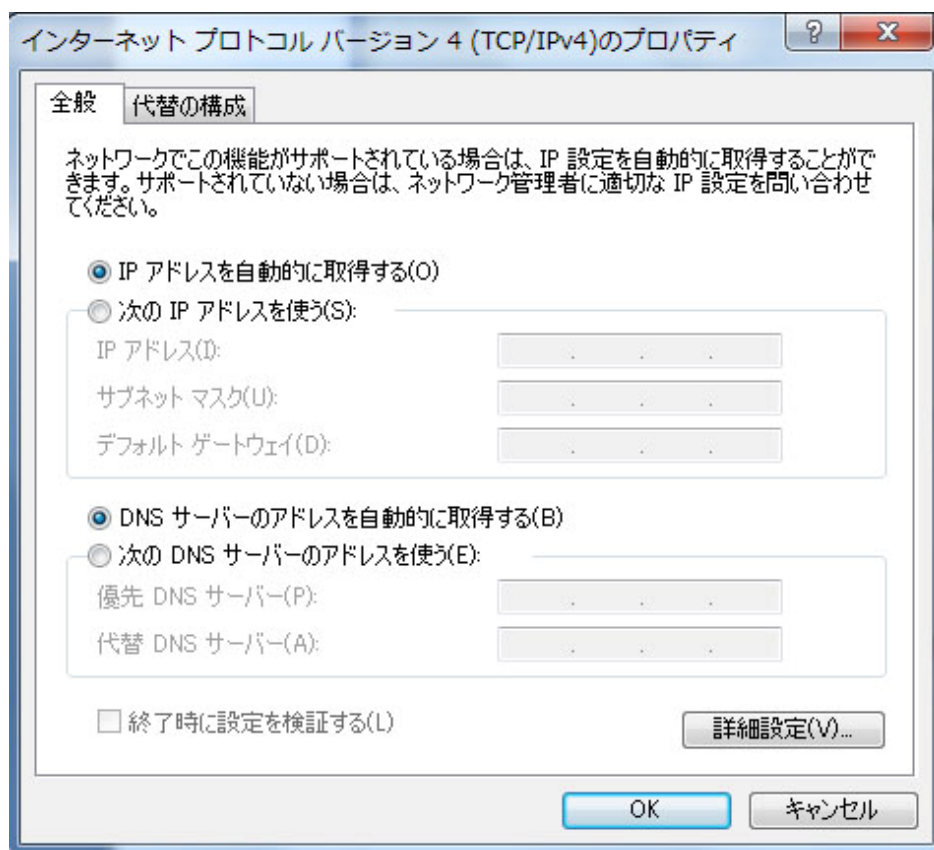
本製品のデフォルトネットワーク設定は以下の通りです。

- ・ IPアドレス：192.168.1.1
- ・ サブネットマスク：255.255.255.0

PCが本製品にアクセスできることをご確認ください。PCで設定するIPアドレスは本製品と同一のIPセグメント内にある必要があります。

1. Windows 7で、**スタート**> **コントロールパネル**を選択し、**コントロールパネル**ウィンドウを開きます。
2. **コントロールパネル**ウィンドウ内で**ネットワークと共有センター**をダブルクリックして、**ネットワークと共有センター**ウィンドウを開きます。
3. **ネットワークと共有センター**ウィンドウ内で、**ローカルエリア接続**をダブルクリックし、**ローカルエリア接続の状態**ダイアログボックスがポップアップ表示されることをご確認ください。
4. **全般**タブで**プロパティ**を選択し、出てきたウィンドウ内で**ネットワーク**タブを選択します。**インターネットプロトコル(TCP/IP)**を選択し、**プロパティ**ボタンをクリックし、**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ポップアップ表示されることをご確認ください。
5. 図 2-2 のように **IP アドレスを自動的に取得する**、**DNS サーバーのアドレスを自動的に取得する** を選択してください。

図 2-2 インターネットプロトコル(TCP/IP)のプロパティ画面



6. OK ボタンをクリックします。

2.3 本製品のログイン

本製品ではWEBブラウザを通じて本製品設定・管理ができます。

事前確認事項

- ・本製品が正しく接続されていることをご確認ください。
- ・PCのTCP/IP設定が完了していることをご確認ください。

1. IEブラウザの画面を開き、http://192.168.1.1 (デフォルトIPアドレス)を入力しログイン画面を表示します。(図2-3)

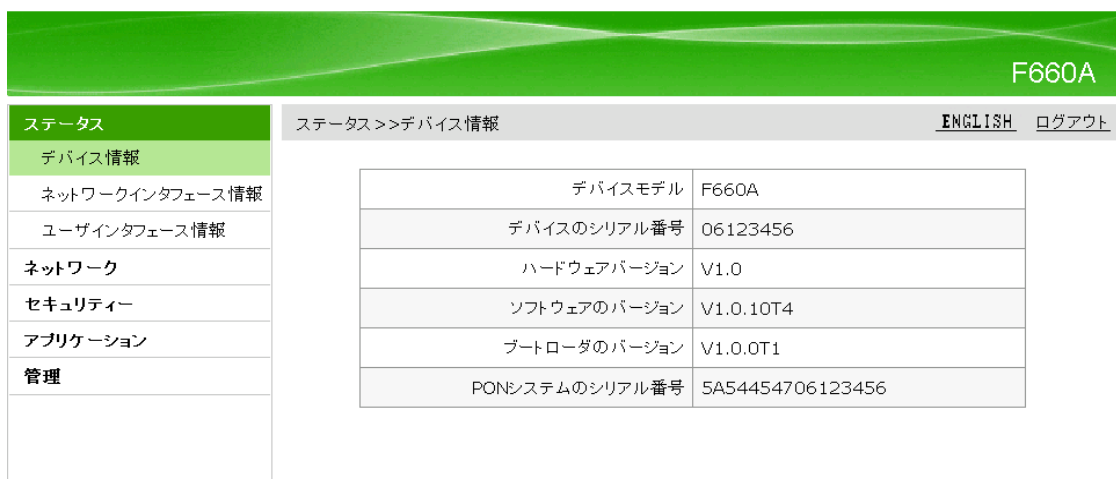
図 2-3 ログイン画面



2. ユーザー名とパスワードを入力してログインボタンをクリックするとデバイス情報画面に進みます。

(図2-4)

図 2-4 デバイス情報画面



3 デバイスの状態

3.1 デバイス情報

WEB画面の左側でステータスを選択すると、デバイス情報画面に進み、デバイスの基本情報が表示されます。(図3-1)

図 3-1 デバイス情報画面



3.2 ネットワークインタフェース情報

本製品のネットワークインタフェース情報には以下の内容が含まれます。

- ・WAN接続情報
- ・PON情報

3.2.1 WAN 接続情報

WEB画面の左側でステータス>ネットワークインタフェース>WAN接続を選択すると、WAN接続情報画面に進みネットワーク側の接続情報が表示されます。(図3-2)

図 3-2 WAN 接続情報画面

ステータス	ステータス >> ネットワークインタフェース情報 >> WAN接続情報	ENGLISH	ログアウト
デバイス情報			
ネットワークインタフェース情報			
WAN接続情報			
PON接続情報			
ユーザインタフェース情報			
ネットワーク			
セキュリティ			
アプリケーション			
管理			

モード	IP
接続名	omci_dhcp
IPプロトコルのバージョン	IPv4/v6
NAT	有効
IPv4アドレス	198.51.100.100/255.255.255.0
IPv4 DNS	203.0.113.33/203.0.113.49/0.0.0.0
IPv4ゲートウェイ	198.51.100.1
IPv4接続ステータス	接続中
IPv4のオンライン時間	406秒
IPv4リース残存期間	10394秒
IPv6 LLA	fe80::fec8:97ff:feaf:1ec
IPv6 DNS	::/::/::
IPv6ゲートウェイ	::
IPv6 プレフィックスデリゲーション	使用
IPv6 プロキシアドレス	::
IPv6接続ステータス	接続中
IPv6のオンライン時間	409秒
WAN MAC	fc:c8:97:af:01:ec

更新

3.2.2 PON 情報

WEB画面の左側でステータス>ネットワークインタフェース>PONの情報を選択すると、PONの情報画面に進み、PON状態の情報が表示されます。(図3-3)

図 3-3 PON 情報画面

ステータス	ステータス >> ネットワークインタフェース情報 >> PON接続情報	ENGLISH	ログアウト
デバイス情報			
ネットワークインタフェース情報			
WAN接続情報			
PON接続情報			
ユーザインタフェース情報			
ネットワーク			
セキュリティ			
アプリケーション			
管理			

PONの状態	認証完了
光モジュールの入力電力 (dBm)	-16.9
光モジュールの出力パワー (dBm)	3.28
光モジュールの電源電圧 (V)	3.306
光送信バイアス電流 (A)	0.009996
光モジュールの動作温度 (°C)	43.152

更新

3.3 ユーザーインタフェース情報

本製品のユーザーインタフェース情報には以下の内容が含まれます。

- ・イーサネットインタフェース情報
- ・無線LAN RF2.4Gインタフェース情報

- ・ 無線LAN RF5Gインタフェース情報
- ・ USBインタフェース情報

3.3.1 イーサネットインタフェース情報

WEB画面の左側メニューでステータス>ユーザーインタフェース情報を選択すると、デフォルトではイーサネットインタフェース情報画面に進み、イーサネットインタフェースに送受信パケット情報が表示されます。(図3-4)

図 3-4 イーサネットインタフェース画面

ステータス	ステータス>>ユーザインタフェース情報>>イーサネットインタフェース情報	ENGLISH ログアウト
デバイス情報		
ネットワークインタフェース情報		
ユーザインタフェース情報		
イーサネットインタフェース情報		
無線LAN RF2.4G		
無線LAN RF5G		
USBインタフェース情報		
ネットワーク		
セキュリティ		
アプリケーション		
管理		

ポート名	LAN1
受信したデータ量(byte)	0
受信したパケットの総数	0
マルチキャストパケットの受信数	0
ブロードキャストパケットの受信数	0
送信したデータ量(byte)	0
送信されたパケットの総数	0
マルチキャストパケットの送信数	0
ブロードキャストパケットの送信数	0

ポート名	LAN2
受信したデータ量(byte)	10708
受信したパケットの総数	126
マルチキャストパケットの受信数	6
ブロードキャストパケットの受信数	0
送信したデータ量(byte)	1215974
送信されたパケットの総数	8143
マルチキャストパケットの送信数	2027
ブロードキャストパケットの送信数	5971

ポート名	LAN3
受信したデータ量(byte)	0
受信したパケットの総数	0
マルチキャストパケットの受信数	0
ブロードキャストパケットの受信数	0
送信したデータ量(byte)	0
送信されたパケットの総数	0
マルチキャストパケットの送信数	0
ブロードキャストパケットの送信数	0

ポート名	TA
受信したデータ量(byte)	0
受信したパケットの総数	0
マルチキャストパケットの受信数	0
ブロードキャストパケットの受信数	0
送信したデータ量(byte)	0
送信されたパケットの総数	0
マルチキャストパケットの送信数	0
ブロードキャストパケットの送信数	0

更新

3.3.2 無線 LAN RF2.4G インタフェース情報

WEB画面の左側メニューでステータス>ユーザーインタフェース情報>無線LAN RF2.4Gを選択すると、無線LAN RF2.4G画面に進み、無線スイッチの情報、送受信パケット情報、認証情報が表示されます。(図3-5)

図 3-5 無線 LAN RF 2.4G インタフェース情報画面

ステータス	ステータス >> ユーザーインターフェイス情報 >> 無線LAN RF2.4G	ENGLISH	ログアウト
デバイス情報			
ネットワークインターフェイス情報			
ユーザーインターフェイス情報			
イーサネットインターフェイス情報			
無線LAN RF2.4G			
無線LAN RF5G			
USBインターフェイス情報			
ネットワーク			
セキュリティ			
アプリケーション			
管理			

無線の状態	有効
チャンネル	1

SSID1の状態	有効
SSID1名	F660A-QG05-G
認証方法	WPA/WPA2-PSK
暗号化	TKIP+AES
MACアドレス	00:20:30:70:11:05
受信パケット/バイト数	649863/84778417
送信パケット/バイト数	742669/810109166
受信エラーパケット数	9
送信エラーパケット数	0
受信パケットの廃棄数	9
送信パケットの廃棄数	6289

SSID2の状態	無効
----------	----

SSID3の状態	無効
----------	----

SSID4の状態	無効
----------	----

3.3.3 無線 LAN RF5G インタフェース情報

WEB画面の左側メニューでステータス>ユーザーインターフェイス情報>無線LAN RF5Gを選択すると、無線LAN RF5G画面に進み、無線スイッチの情報、送受信パケット情報、認証情報が表示されます。(図3-6)

図 3-6 無線 LAN RF 5G インタフェース情報画面

ステータス	ステータス >> ユーザーインターフェイス情報 >> 無線LAN RF5G	ENGLISH ログアウト
デバイス情報		
ネットワークインターフェイス情報		
ユーザーインターフェイス情報		
イーサネットインターフェイス情報		
無線LAN RF2.4G		
無線LAN RF5G		
USBインターフェイス情報		
ネットワーク		
セキュリティ		
アプリケーション		
管理		

無線の状態	有効
チャンネル	100

SSID5の状態	有効
SSID5名	F660A-QG05-A
認証方法	WPA/WPA2-PSK
暗号化	TKIP+AES
MACアドレス	00:20:30:70:11:06
受信パケット/バイト数	356/35733
送信パケット/バイト数	245/64253
受信エラーパケット数	0
送信エラーパケット数	17915
受信パケットの廃棄数	0
送信パケットの廃棄数	0

SSID6の状態	無効
----------	----

SSID7の状態	無効
----------	----

SSID8の状態	無効
----------	----

3.3.4 USB インタフェース情報

WEB画面の左側メニューでステータス>ユーザーインターフェイス情報>USBインターフェイス情報を選択すると、USBインターフェイス情報画面に進み、USBインターフェイス情報が表示されます。(図3-7)

図 3-7 USB 情報画面

ステータス	ステータス >> ユーザーインターフェイス情報 >> USBインターフェイス情報	ENGLISH ログアウト
デバイス情報		
ネットワークインターフェイス情報		
ユーザーインターフェイス情報		
イーサネットインターフェイス情報		
無線LAN RF2.4G		
無線LAN RF5G		
USBインターフェイス情報		
ネットワーク		
セキュリティ		
アプリケーション		
管理		

ポート番号	1
装置名	USB DISK
デバイスの種類	USB Mass Storage
デバイスID	090c_1000
デバイス速度	不明
接続ステータス	接続されている
アクセスアドレス	ftp://192.168.1.1

4 ネットワーク設定

4.1 無線 LAN RF2.4G の設定

本製品の無線LAN設定には以下の内容が含まれます。

- ・無線LAN基本パラメータの設定
- ・SSIDの設定
- ・無線LANセキュリティ属性の設定
- ・アクセス制御リストの設定
- ・関連付けられているデバイスの表示
- ・WPS機能の設定

4.1.1 無線 LAN RF2.4G 基本パラメータの設定

無線LAN RF2.4Gの基本パラメータ調整により、無線LANの動作条件および動作状態を設定できます。

- 1.WEB画面左側のメニューでネットワーク>無線LAN RF2.4Gを選択すると、デフォルトでは基本設定画面に進みます。(図4-1)

図 4-1 無線 LAN 基本設定画面

ネットワーク>>無線LAN RF2.4G>>基本設定

無線LANを有効にする

他SSIDとの分離を有効にする

動作モード

チャンネル帯域幅

無線チャンネル

ShortGIを有効にする

ビーコン間隔 ミリ秒

電波出力

QoSタイプ

RTSしきい値

DTIM

設定 キャンセル

- 2.必要に応じて無線LAN RF2.4Gの基本パラメータを設定し、設定ボタンをクリックします。

無線LAN基本パラメータについては下の表を参照してください。

パラメータ	説明
2.4G無線LANを有効にする	無線LAN機能のオンとオフを行います。
他SSIDとの分離を有効にする	チェックを入れると他SSIDとの分離機能が有効になり、各SSIDのユーザーとの相互接続がなくなります。

パラメータ	説明
動作モード	以下のモードをサポートしています。 IEEE 802.11b Only IEEE 802.11g Only IEEE 802.11n Only Mixed(802.11b+802.11g) Mixed(802.11g+802.11n) Mixed(802.11b+802.11g+802.11n) : デフォルト
チャンネル帯域幅	無線ブロードバンドの帯域幅を設定します。以下の設定が可能です。 自動 20Mhz 40Mhz : デフォルト
無線チャンネル	国コードから適当なチャンネルチャンネルを選択できます。 自動(デフォルト)または1~13が選択できます。 無線アクセスポイントと基地局の通信時に使用する帯域です。
ShortGI	ショートガードインターバル(Short Guard Interval)を有効にします。
ビーコンギャップ	ビーコンの間隔時間です。デフォルトでは100ミリ秒です。
電波出力	電波出力のレベルは以下のように設定できます。 100% 80% 60% 40% 20%
QoSタイプ	不使用、WMM、SSIDが選択できます。
RTSしきい値	RTS(Request To Send)しきい値(送信するリクエスト回数の上限)
DTIM	DTIM(Delivery Traffic Indication Message、配信トラフィック表示メッセージ)の時間間隔です。

4.1.2 SSID の設定

本製品1台に複数のSSIDが設定でき、それぞれのSSIDに異なるSSID名とオン/オフが設定できます。

- 1.WEB画面の左側でネットワーク>無線LAN RF2.4G>SSID設定を選択すると、SSID設定画面に進みます。(図4-2)

図 4-2 SSID 基本設定画面

2.SSIDに関するパラメータを設定して、**設定ボタン**をクリックします。

SSIDのパラメータについては下の表を参照してください。

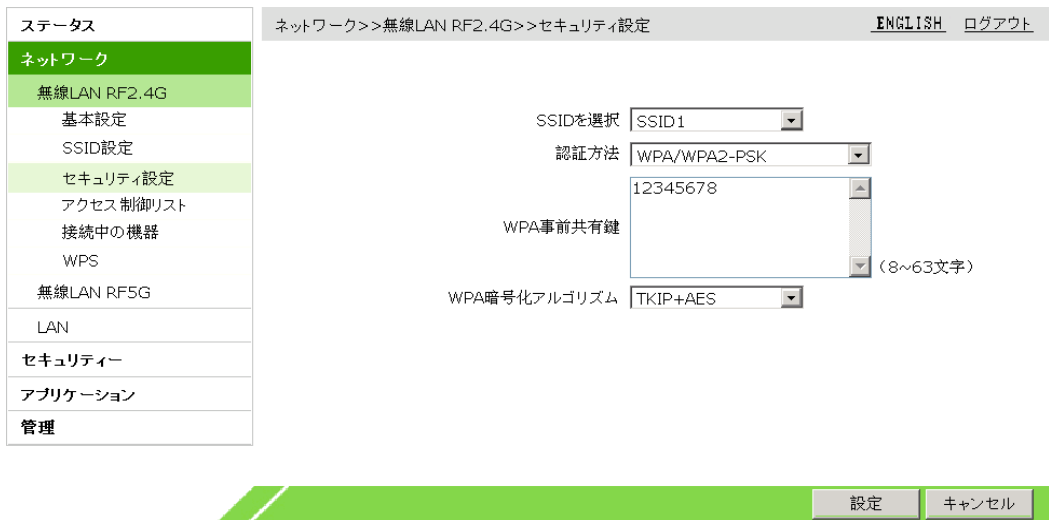
パラメータ	説明
SSIDを選択	設定するSSIDを選択します。SSID1～SSID4が選択できます。
有効にする	チェックを入れるとSSIDが有効になります。
ステルス機能を有効にする	チェックをいれるとSSIDが非表示になります。
SSID内の端末間での通信を無効にする	チェックを入れると他SSIDとの分離機能が有効になり、各SSIDのユーザーとの相互接続がなくなります。
最大ユーザー数	SSIDに接続できる最大ユーザー数を設定します。設定値の範囲は1～10です。
SSID名	選択中のSSIDの名称を設定します。設定できる範囲は0～32文字です。 ※選択中のSSIDの名称を設定します。設定できる範囲は0～32文字で、次の文字が使えます：A-Z,a-z,0-9,`~!@#\$%^&*()_+ =¥[]:;"/<>?
プライオリティ	SSIDのプライオリティを設定します。設定値の範囲は0～7です。デフォルトでは0となり、プライオリティを設定していません。この値が大きいほどプライオリティが高くなります。

4.1.3 無線 LAN セキュリティ属性の設定

無線LANセキュリティ属性を設定すると、SSIDごとに異なる暗号化方式が設定できます。

1.WEB画面の左側メニューでネットワーク>無線LAN RF2.4G>セキュリティ設定を選択すると、セキュリティ設定画面に進みます。(図4-3)

図 4-3 セキュリティ設定画面



2. 認証方式を設定して、**設定ボタン**をクリックします。

SSIDがサポートしている認証方式はOpen System(オープンシステム)、Shared Key(共有鍵方式)、WPA-PSK、WPA2-PSK、WPA/WPA2-PSKの5種類です。

4.1.4 アクセス制御リストの設定

無線LANアクセス制御機能を有効にして無線LANアクセスのブラック/ホワイトリストを設定すると、無線LANアクセスの制御を実現できます。モードを「阻止」に設定すると、リスト外の無線端末が当該SSIDにアクセスできるようになります。モードを「許可」に設定すると、リスト内の無線端末だけが当該SSIDにアクセスできるようになります。

1. WEB画面の左側メニューで**ネットワーク>無線LAN RF2.4G>アクセス制御リスト**を選択すると、**アクセス制御リスト設定画面**に進みます。(図4-4)

図 4-4 アクセス制御リストの設定画面




2. アクセス制御リストに関するパラメータを設定して、**追加ボタン**をクリックします。

アクセス制御リストの設定パラメータについては下の表を参照してください。

パラメータ	説明

パラメータ	説明
SSIDを選択	設定するSSIDを選択します。SSID1～SSID4が選択できます。
モード	サポートするモードは以下の3種類です。 ・「制限しない」: SSIDのアクセス制御を行いません(デフォルトモード)。 ・「制限する」: 登録するMACアドレスのデバイスからの接続を阻止するとき使用します。 ・「許可する」: 登録するMACアドレスのデバイスからの接続を許可するとき使用します。 ※設定ミスによりアクセスができない恐れがあります。
MACアドレス	無線LANにアクセスするデバイスのMACアドレスです。

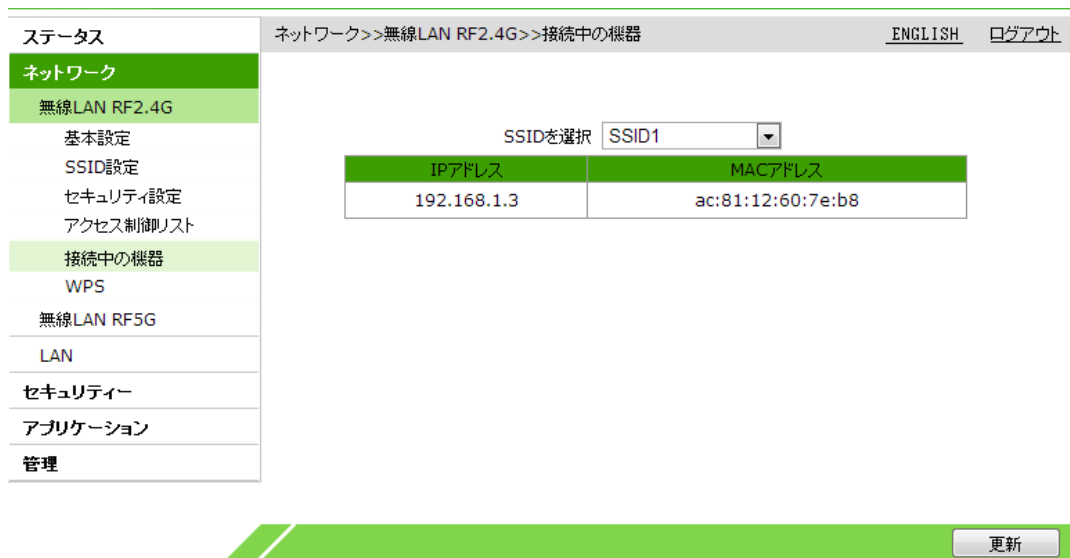
3.(オプション)SSIDの後に表示される  アイコンをクリックすると設定データを削除できます。

4.1.5 接続中の機器の確認

WEB画面で各SSID上に関連付けられているデバイス(そのSSIDを使用しているデバイス)のIPアドレスとMACアドレスを確認できます。

1.WEB画面の左側メニューでネットワーク>無線LAN RF2.4G>接続中の機器を選択すると、接続中の機器画面に進みます。(図4-5)

図 4-5 接続中の機器画面



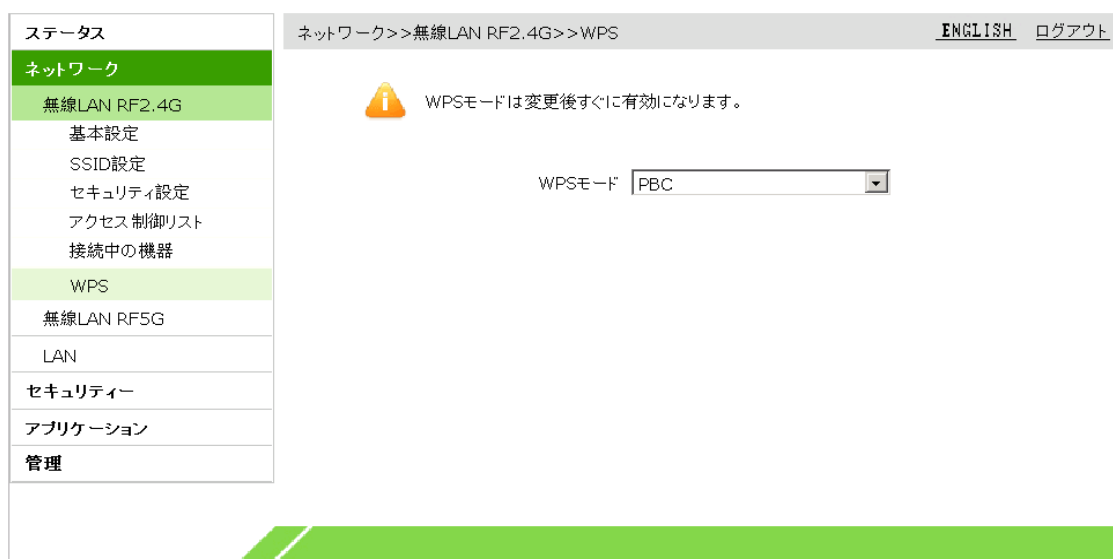
2.SSIDを選択プルダウンリストからSSID番号を選択して更新ボタンをクリックすると、接続中の機器のIPアドレスとMACアドレスが表示されます。

4.1.6 WPS 機能の設定

2.4G 無線LANモードの保護設定(Wi-Fi Protected Setup)機能に関するパラメータです。この機能をオンにすると、端末(パソコン、スマートフォン等)はONUと自動的に接続し、ユーザーがその都度SSIDを検索しパスワードを入力する必要がなくなります。通常、変更する必要はありません。

1.WEB画面の左側メニューでネットワーク>無線LAN RF2.4G>WPSを選択すると、WPS設定画面に進みます。(図4-6)

図 4-6 WPS 設定画面



2.必要に応じてWPSモードを設定します。設定は完了後すぐ有効になります。

WPSの設定パラメータについては下の表を参照してください。

パラメータ	説明
WPSモード	PBCモード: プッシュボタンモードです。本製品パネル上のWPSボタンをクリックするとWPS機能が有効になります。
	<p>PINモード: PIN番号の使い方によってDevice PINとEnrollee PINに分けられます。</p> <p>Device PIN: デバイスが自動で生成する8ビットのPIN番号です。無線ネットワークカード管理ソフトウェア上でデバイスの生成したPIN番号を入力することで関連付けを行います。生成ボタンをクリックすると、デバイスは新たに8ビットのPIN番号を取得します。</p> <p>Enrollee PIN: 無線ネットワークカードが生成する8ビットのPIN番号です。Enrollee PIN入力枠にPIN番号を入力すると無線ネットワークカードとデバイスとの関連付けが有効になります。</p>

4.2 無線 LAN RF5G の設定

本製品の無線LAN設定には以下の内容が含まれます。

- ・無線LAN基本パラメータの設定
- ・SSIDの設定
- ・無線LANセキュリティ属性の設定
- ・アクセス制御リストの設定
- ・関連付けられているデバイスの表示
- ・WPS機能の設定

4.2.1 無線 LAN RF5G 基本パラメータの設定

無線LAN RF5Gの基本パラメータを設定すると、無線LANの動作条件および動作状態を設定できます。

- 1.WEB画面の左側メニューでネットワーク>無線LAN RF5Gを選択すると、基本設定画面に進みます。(図4-7)

図 4-7 無線 LAN RF5G 基本設定画面

ステータス ネットワーク >> 無線LAN RF5G >> 基本設定 ENGLISH ログアウト

無線LAN RF5G

基本設定

無線LANを有効にする

他SSIDとの分離を有効にする

動作モード Mixed(802.11a+802.11n+802.11ac) ▼

チャンネル帯域幅 20/40/80Mhz 自動 ▼

無線チャンネル 自動 ▼

ShortGIを有効にする

ビーコン間隔 100 ミリ秒

電波出力 100% ▼

QoSタイプ WMM ▼

RTS/CTSしきい値 2347

DTIM 1

設定 キャンセル

2.必要に応じて無線LAN RF5Gの基本パラメータを設定し、**設定ボタン**をクリックします。

無線LAN基本パラメータについては下の表を参照してください。

パラメータ	説明
5G無線LANを有効にする	無線LAN機能のオン/オフを行います。
他SSIDとの分離を有効にする	チェックを入れると他SSIDとの分離機能が有効になり、各SSIDのユーザーとの相互接続がなくなります。
動作モード	以下のモードをサポートしています。 IEEE 802.11a Only IEEE 802.11n Only Mixed(802.11a+802.11n) Mixed(802.11a+802.11n+802.11ac) : デフォルト
チャンネル帯域幅	無線ブロードバンドの帯域幅を設定します。以下の設定が可能です。 20Mhz 40Mhz 20/40/80Mhz 自動: デフォルト
無線チャンネル	5G帯域Wi-Fiチャンネルを設定します。ONUが無線信号の状況に応じてチャンネルを自動選択する方式または手動でチャンネルを指定する方式に設定できます。以下の設定が可能です。 自動: デフォルト 36 40 44 48 52

パラメータ	説明
	56 60 64 100 104 108 112 116 120 124 128 132 136 140 デフォルトではONUによるチャンネル自動選択方式となっています。
ShortGI	ショートガードインターバル(Short Guard Interval)を有効にします。
ビーコンギャップ	ビーコンの間隔時間です。システムのデフォルトでは100ミリ秒です。
電波出力	電波出力のレベルは以下のように設定できます。 100% 80% 60% 40% 20%
QoSタイプ	不使用、WMM、SSIDが選択できます。
RTSしきい値	RTS(Request To Send)しきい値(送信するリクエスト回数の上限)
DTIM	DTIM(Delivery Traffic Indication Message、配信トラフィック表示メッセージ)の時間間隔です。

4.2.2 SSID の設定

1台の本製品上に複数のSSIDが設定でき、それぞれのSSIDに異なるSSID名とオン/オフを設定することができます。

- 1.WEB画面の左側でネットワーク>無線LAN RF5G>SSID設定を選択すると、SSID設定画面に進みます。(図4-8)

図 4-8 SSID 設定画面

2.SSIDに関するパラメータを設定して、**設定ボタン**をクリックします。

SSIDのパラメータについては下の表を参照してください。

パラメータ	説明
SSIDを選択	設定するSSIDを選択します。SSID5～SSID8が選択できます。
有効にする	チェックを入れるとそのSSIDが有効になります。
ステルス機能を有効にする	チェックをいれるとそのSSIDが非表示になります。
SSID内の端末間での通信を無効にする	チェックを入れると他SSIDとの分離機能が有効になり、各SSIDのユーザーとの相互接続がなくなります。
最大ユーザー数	SSIDに接続できる最大ユーザー数を設定します。設定値の範囲は1～10です。
SSID名	選択中のSSIDの名称を設定します。設定できる範囲は0～32文字です。 ※選択中のSSIDの名称を設定します。設定できる範囲は0～32文字で、次の文字が使えます:A-Z,a-z,0-9,`~!@#%&*()_+ =¥□◇;:” ,./<>?
プライオリティ	SSIDのプライオリティを設定します。設定値の範囲は0～7です。デフォルトでは0(プライオリティ未設定)となっています。この値が大きいほどプライオリティが高くなります。

4.2.3 無線 LAN セキュリティ属性の設定

無線LANセキュリティ属性を設定すると、SSIDごとに異なる暗号化方式が設定できます。

1.WEB画面の左側メニューで**ネットワーク>無線LAN RF5G>セキュリティ設定**を選択すると、**セキュリティ設定画面**に進みます。(図4-9)

図 4-9 セキュリティ設定画面

2. 認証方式を設定して、**設定**ボタンをクリックします。

SSIDがサポートしている認証方式はOpen System(オープンシステム)、Shared Key(共有鍵方式)、WPA-PSK、WPA2-PSK、WPA/WPA2-PSKの5種類です。

4.2.4 アクセス制御リストの設定

無線LANアクセス制御機能を有効にして無線LANアクセスのブラック/ホワイトリストを設定すると、無線LANアクセスの制御を実現できます。モードを「阻止」に設定すると、リスト外の無線端末が当該SSIDにアクセスできません。モードを「許可」に設定すると、リスト内の無線端末だけが当該SSIDにアクセスできるようになります。

1. WEB画面の左側メニューで**ネットワーク>無線LAN RF5G>アクセス制御リスト**を選択すると、**アクセス制御リスト設定画面**に進みます。(図4-10)


図 4-10 アクセス制御リストの設定画面

2. アクセス制御リストに関するパラメータを設定して、**追加**ボタンをクリックします。

アクセス制御リストの設定パラメータについては下の表を参照してください。

パラメータ	説明
-------	----

パラメータ	説明
SSIDを選択	設定するSSIDを選択します。SSID5～SSID8が選択できます。
モード	サポートするモードは以下の3種類です。 ・「制限しない」: SSIDのアクセス制御を行いません(デフォルトモード)。 ・「制限する」: 対応するMACアドレスのデバイスからの接続を阻止するとき使用します。 ・「許可する」: 対応するMACアドレスのデバイスからの接続を許可するとき使用します。
MACアドレス	無線LANにアクセスするデバイスのMACアドレスです。

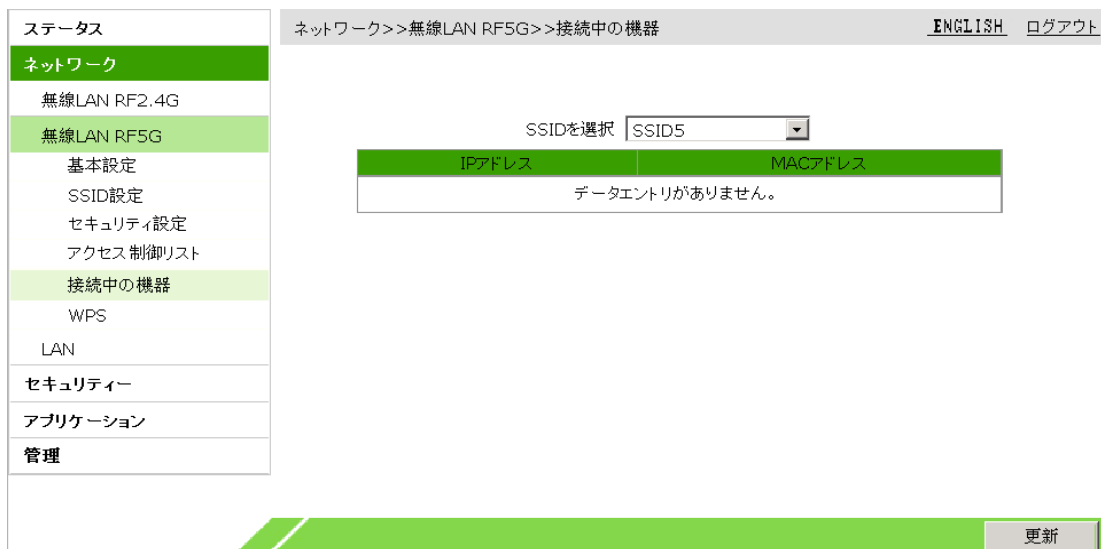
3.(オプション)SSIDの後に表示される  アイコンをクリックすると設定データを削除できます。

4.2.5 接続中の機器の確認

WEB画面で各SSID上に関連付けられたデバイス(そのSSIDを使用しているデバイス)のIPアドレスとMACアドレスを確認できます。

1.WEB画面の左側メニューでネットワーク>無線LAN RF5G>接続中の機器を選択すると、接続中の機器画面に進みます。(図4-11)

図 4-11 接続中の機器画面



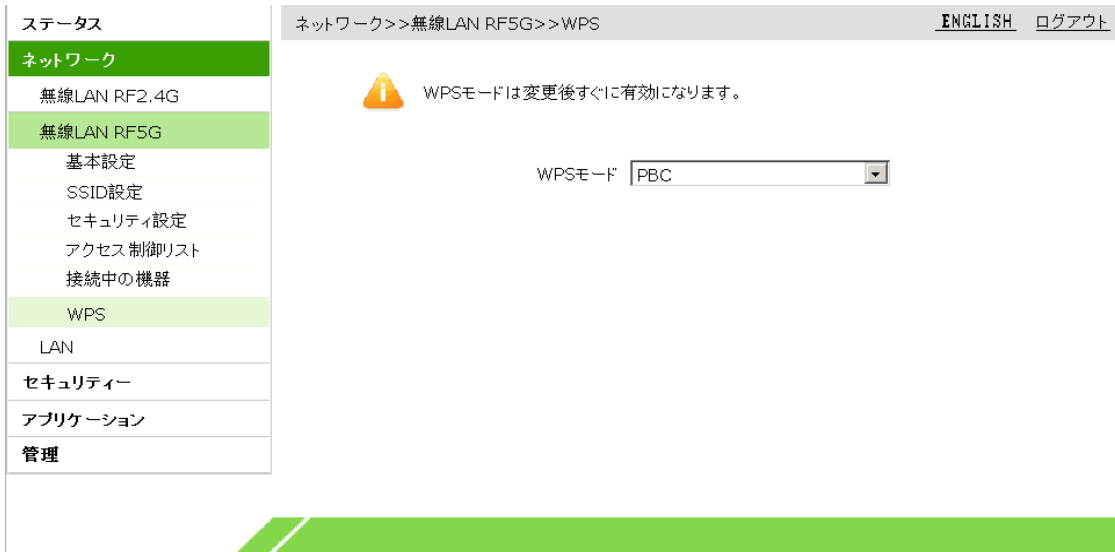
2.SSIDを選択プルダウンリストからSSID番号を選択して更新ボタンをクリックすると、接続中の機器のIPアドレスとMACアドレスが表示されます。

4.2.6 WPS 機能の設定

5G 無線LANモードの保護設定(Wi-Fi Protected Setup)機能に関するパラメータです。この機能をオンにすると、端末(パソコン、スマートフォン等)はONUと自動的に接続し、ユーザーがいちいちSSIDを検索しパスワードを入力する必要がなくなります。通常、変更する必要はありません。

1. WEB画面の左側メニューでネットワーク>無線LAN RF5G>WPSを選択すると、WPS設定画面に進みます。(図4-12)

図 4-12 WPS 設定画面



2.必要に応じてWPSモードを設定します。設定は完了後すぐ有効になります。

WPSの設定パラメータについては下の表を参照してください。

パラメータ	説明
WPSモード	PBCモード: プッシュボタンモードです。本製品パネル上のWPSボタンをクリックするとWPS機能が有効になります。
	PINモード: PIN番号の使い方によってDevice PINとEnrollee PINに分けられます。 Device PIN: デバイスが自動で生成する8ビットのPIN番号です。無線ネットワークカード管理ソフトウェア上でデバイスの生成したPIN番号を入力することで関連付けを行います。生成ボタンをクリックすると、デバイスは新たに8ビットのPIN番号を取得します。
	Enrollee PIN: 無線ネットワークカードが生成する8ビットのPIN番号です。Enrollee PIN入力枠にPIN番号を入力すると無線ネットワークカードとデバイスとの関連付けが有効になります。

4.3 LAN の設定

本製品のLAN設定には以下の内容が含まれます。

- ・静的アドレスの設定
- ・動的IPv4アドレスの設定
- ・動的IPv6アドレスの設定
- ・スタティックプレフィックスの設定
- ・プレフィックスデリゲーション方式の設定
- ・RAサービスの設定

4.3.1 静的アドレスの設定



静的アドレス管理により、ユーザーインターフェースに接続されているデバイスへ静的IPアドレスを配分してユーザー側デバイスのMACアドレスに固定し、不正なユーザーのアクセスを防止できます。

- 1.WEB画面の左側メニューでネットワーク>LAN>DHCP固定割当設定を選択すると、DHCP固定割当設定画面に進みます。(図4-13)

図 4-13 DHCP 固定割当設定画面

- 2.IPアドレステキストボックスにIPアドレスを入力し、MACアドレステキストボックスにMACアドレスを入力して、追加ボタンをクリックします。

※当方は IPv4 アドレスのみサポートしています。

- 3.(オプション)アドレス内容の後に表示される  アイコンをクリックすると設定データを修正できます。
- 4.(オプション)アドレス内容の後に表示される  アイコンをクリックすると設定データを削除できます。

4.3.2 動的 IPv4 アドレスの設定

本製品のIPアドレスとサブネットマスクを設定し、DHCPサービス機能を起動します。ユーザーインターフェースに接続されているデバイスへ動的にIPアドレスを配分します。

- 1.WEB画面の左側メニューでネットワーク>LAN>ダイナミックアドレス管理(IPv4)を選択すると、ダイナミックアドレス管理(IPv4)画面に進みます。ここでDHCP有効化の設定、及びDNSサービス優先化の設定ができます。(図4-14-1、図4-14-2)

図 4-14-1 ダイナミックアドレス管理(IPv4)画面

ステータス ネットワーク>>LAN>>ダイナミックアドレス管理 (IPv4) ENGLISH ログアウト

ネットワーク																
無線LAN RF2.4G																
無線LAN RF5G	IPアドレス <input type="text" value="192.168.1.1"/>															
LAN	サブネットマスク <input type="text" value="255.255.255.0"/>															
DHCP固定アドレス割当																
ダイナミックアドレス管理 (IPv4)	セカンダリIPアドレスを有効 <input type="checkbox"/>															
ダイナミックアドレス管理 (IPv6)	セカンダリIPアドレス <input type="text"/>															
スタティックプレフィックス プレフィックスデリゲーション (IPv6)	サブネットマスク <input type="text"/>															
ルータ広告(IPv6)	DHCPを有効 <input checked="" type="checkbox"/>															
セキュリティ	DHCPプール開始IPアドレス <input type="text" value="192.168.1.2"/>															
アプリケーション	DHCPプール終了IPアドレス <input type="text" value="192.168.1.254"/>															
管理	アプリケーション: DNSサービスの 設定を優先にする <input type="checkbox"/>															
	DNSサーバ1 <input type="text" value="192.168.1.1"/>															
	DNSサーバ2 <input type="text"/>															
	DNSサーバ3 <input type="text"/>															
	デフォルトゲートウェイ <input type="text" value="192.168.1.1"/>															
	リース期間 <input type="text" value="86400"/> 秒															
	割り当てられたアドレス															
	<table border="1"> <thead> <tr> <th>MACアドレス</th> <th>IPアドレス</th> <th>リース残存期間</th> <th>ホスト名</th> <th>ポート</th> </tr> </thead> <tbody> <tr> <td>e8:8d:28:b4:c9:63</td> <td>192.168.1.2</td> <td>74128</td> <td>AdminiskiiPhon</td> <td>SSID5</td> </tr> <tr> <td>7c:dd:90:86:90:a8</td> <td>192.168.1.3</td> <td>66924</td> <td>A23102142</td> <td>SSID5</td> </tr> </tbody> </table>	MACアドレス	IPアドレス	リース残存期間	ホスト名	ポート	e8:8d:28:b4:c9:63	192.168.1.2	74128	AdminiskiiPhon	SSID5	7c:dd:90:86:90:a8	192.168.1.3	66924	A23102142	SSID5
MACアドレス	IPアドレス	リース残存期間	ホスト名	ポート												
e8:8d:28:b4:c9:63	192.168.1.2	74128	AdminiskiiPhon	SSID5												
7c:dd:90:86:90:a8	192.168.1.3	66924	A23102142	SSID5												

図 4-15-2 ダイナミックアドレス管理(IPv4)画面

ステータス ネットワーク >> LAN >> ダイナミックアドレス管理 (IPv4) ENGLISH ログアウト

ステータス

ネットワーク

無線LAN RF2.4G

無線LAN RF5G

LAN

DHCP固定アドレス割当

ダイナミックアドレス管理 (IPv4)

ダイナミックアドレス管理 (IPv6)

スタティックプレフィックス
プレフィックスデリゲーション (IPv6)

ルータ応答 (IPv6)

セキュリティー

アプリケーション

管理

IPアドレス

サブネットマスク

セカンダリIPアドレスを有効

セカンダリIPアドレス

サブネットマスク

DHCPを有効

DHCPプール開始IPアドレス

DHCPプール終了IPアドレス

アプリケーション: DNSサービスの設定を優先にする

DNSパススルー

デフォルトゲートウェイ

リース期間 秒

割り当てられたアドレス

MACアドレス	IPアドレス	リース残存期間	ホスト名	ポート
b8:70:f4:1e:df:6f	192.168.1.2	85103	MTC-PC	Unknown
30:10:e4:b2:ec:e8	192.168.1.3	84912	wqgde-iPa	Unknown

※「アプリケーション:DNS サービスの設定を優先にする」のチェックを入れると、「DNS パススルー」と「DNS アドレス指定」の選択肢をプルダウンメニューから選択できます。

2.関連するパラメータを設定して、設定ボタンをクリックします。

動的アドレス管理のパラメータについては下の表をご参照ください。

パラメータ	説明
IPアドレス/サブネットマスク	IPアドレス/サブネットマスクです。
セカンダリIPアドレスを有効にする	チェックを入れるとセカンダリIPアドレス機能が有効になります。
セカンダリIPアドレス/ サブネットマスク	セカンダリIPアドレス/サブネットマスクです。
DHCPサービスを有効にする	チェックを入れるとDHCPサービス機能が有効になります。
DHCPプール開始/終了IPアドレス	DHCPサーバのアドレスプールの開始/終了IPアドレスです。本製品のIPアドレスと同一のセグメント内である必要があります。
アプリケーション:DNSサービスの設定を優先にする	チェックを入れると「アプリケーション:DNSサービス」で設定したDNSが有効になります。
DNSサーバ1	デフォルトのDNSサーバ(本製品)のIPアドレスです。

パラメータ	説明
DNSサーバ2	DNSサーバのIPアドレスです。サービス提供元から提供されます。
DNSサーバ3	DNSサーバのIPアドレスです。サービス提供元から提供されます。
デフォルトゲートウェイ	本製品のIPアドレスです。
リース期間	IPアドレスのリース期間です。60～157,680,000秒または、-1(無期限)の範囲内で設定できます。デフォルトでは86400と設定されています。

4.3.3 動的IPv6アドレスの設定

本製品のIPv6アドレスを設定してDHCPサービス機能を起動します。ホームゲートウェイ機器の場合、このIPアドレスはLAN側サブネットのゲートウェイアドレスも兼用しています。

1. WEB画面の左側メニューでネットワーク>LAN>ダイナミックアドレス管理(IPv6)を選択すると、ダイナミックアドレス管理(IPv6)画面に進みます。ここでDHCP有効化の設定、及びDNSサービス優先化の設定ができます。

(図4-15-1、図4-15-2)

図 4-16-1 ダイナミックアドレス管理(IPv6)画面

ネットワーク>>LAN>>ダイナミックアドレス管理 (IPv6) ENGLISH ログアウト

LLA /

現在利用中のLLA fe80::1

DHCPを有効

アプリケーション: DNSサービスの設定を優先にする

リース期間 秒

割り当てられたアドレス

DUID	IPアドレス	リース残存期間
データエントリがありません。		

図 4-17-2 ダイナミックアドレス管理(IPv6)画面

ステータス	ネットワーク>>LAN>>ダイナミックアドレス管理 (IPv6)	ENGLISH ログアウト
ネットワーク		
無線LAN RF2.4G		
無線LAN RF5G		
LAN		
DHCP固定アドレス割当		
ダイナミックアドレス管理 (IPv4)		
ダイナミックアドレス管理 (IPv6)		
スタティックプレフィックス		
プレフィックスデリゲーション (IPv6)		
ルータ広告 (IPv6)		
セキュリティ		
アプリケーション		
管理		

LLA	fe80::1	/ 64
現在利用中のLLA	fe80::1	
DHCPを有効	<input checked="" type="checkbox"/>	
アプリケーション: DNSサービスの設定を優先にする	<input checked="" type="checkbox"/>	
	DNSパススルー	
リース期間	86400	秒

割り当てられたアドレス		
DUID	IPアドレス	リース残存期間
データエントリがありません。		

設定 キャンセル

※「アプリケーション:DNS サービスの設定を優先にする」のチェックを入れると、「DNS パススルー」と「DNS アドレス指定」の選択肢をプルダウンメニューから選択できます。

2.動的アドレスに関するパラメータを設定し、設定ボタンをクリックします。

動的アドレスのパラメータについては下の表をご参照ください。

パラメータ	説明
IPアドレス	本製品のIPv6アドレスです。
DHCPサービスを有効にする	チェックを入れるとDHCPサービス機能が有効になります。
DNSの更新時間	DNSの更新時間です。60～864000秒の範囲内で設定できます。初期値では86400と設定されています。

4.3.4 スタティックプレフィックスの設定

スタティックプレフィックスを設定し、RAまたはDHCPv6サーバがLAN設備に配分するIPv6プレフィックスを選択します。

1. WEB画面の左側メニューでネットワーク>LAN>スタティックプレフィックス (IPv6)を選択すると、スタティックプレフィックス (IPv6)画面に進みます。(図4-16)

図 4-18 スタティックプレフィックス (IPv6) 画面

ステータス ネットワーク >> LAN >> スタティックプレフィックス ENGLISH ログアウト

ネットワーク

無線LAN RF2.4G

無線LAN RF5G

LAN

DHCP固定アドレス割当
ダイナミックアドレス管理 (IPv4)
ダイナミックアドレス管理 (IPv6)

スタティックプレフィックス
プレフィックスデリゲーション (IPv6)

ルータ広告(IPv6)

セキュリティ

アプリケーション

管理

プレフィックス /

望ましいライフタイム 秒

正式なライフタイム 秒

有効にする RA
 DHCPv6


追加


プレフィックス	望ましいライフタイム	正式なライフタイム	有効にする	修正	削除
データエントリがありません。					

2.スタティックプレフィックスのパラメータを設定し、**追加**ボタンをクリックします。

スタティックプレフィックスのパラメータについては下の表をご参照ください。

パラメータ	説明
プレフィックス	IPv6アドレス/プレフィックス長は、GUAタイプのプレフィックスのみサポートしています。プレフィックス長の設定値の範囲は48～64です。
必要時間	プレフィックスが有効となるまでにかかる時間です。
有効時間	プレフィックスが有効である時間です。有効時間は必要時間より大きく設定する必要があります。
デリゲーション方式	RA: RA方式でこの設定を発信します。 DHCPv6: DHCPv6方式でこの設定を発信します。

3.(オプション)アドレス内容の後に表示される  アイコンをクリックすると設定データを修正できます。

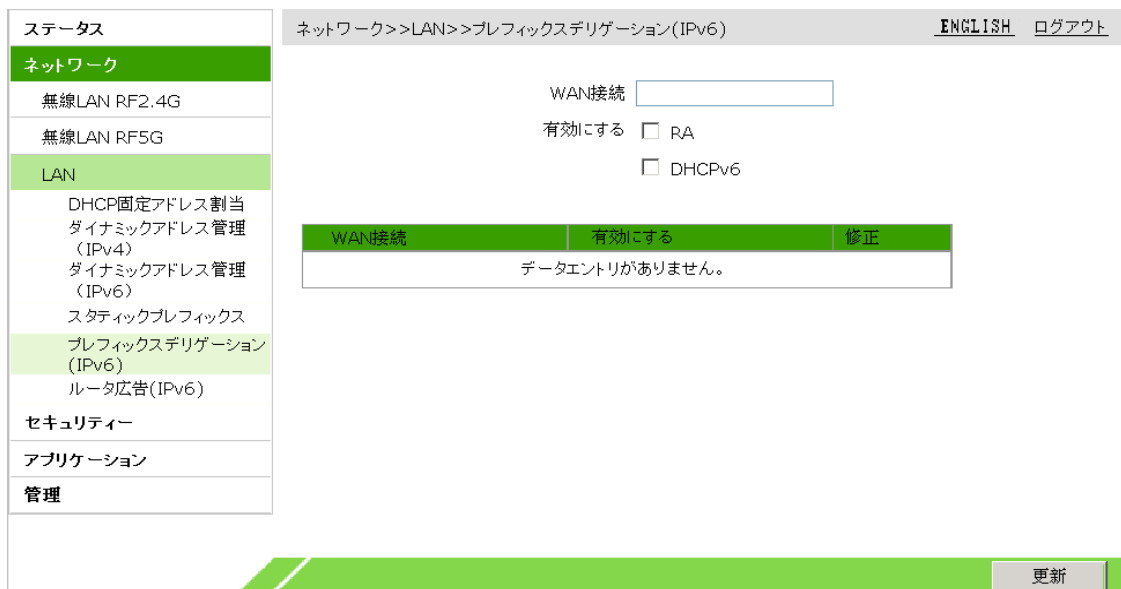
4.(オプション)アドレス内容の後に表示される  アイコンをクリックすると設定データを削除できます。

4.3.5プレフィックスデリゲーション方式の設定

本製品がサポートしているIPv6アドレスのプレフィックスデリゲーション方式はRAとDHCPv6の2種類です。この操作ではWAN接続のIPv6アドレスのプレフィックスデリゲーション方式を修正できます。

1. WEB画面の左側メニューでネットワーク>LAN>プレフィックスデリゲーション (IPv6)を選択すると、プレフィックスデリゲーション (IPv6)画面に進みます。(図4-17)

図 4-19 プレフィックスデリゲーション (IPv6)画面




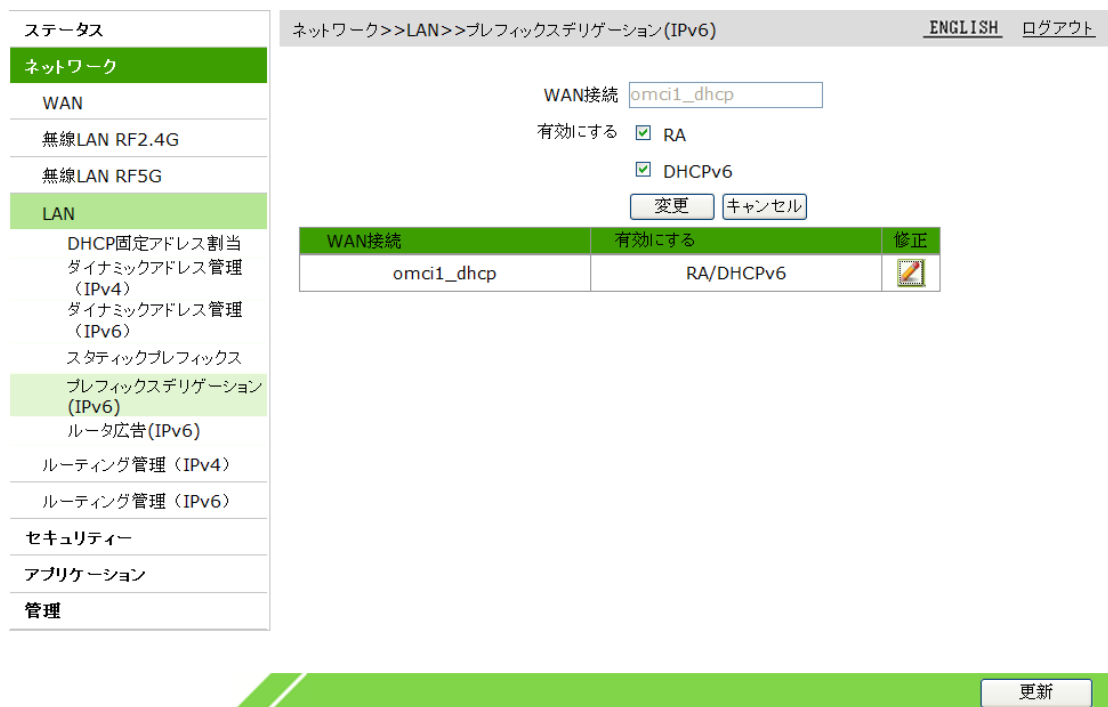
2. WAN接続の後に表示される  アイコンをクリックして、プレフィックスデリゲーションの方式を選択し、更新ボタンをクリックします。(図4-18)

図 4-20 プレフィックスデリゲーション (IPv6) 修正画面

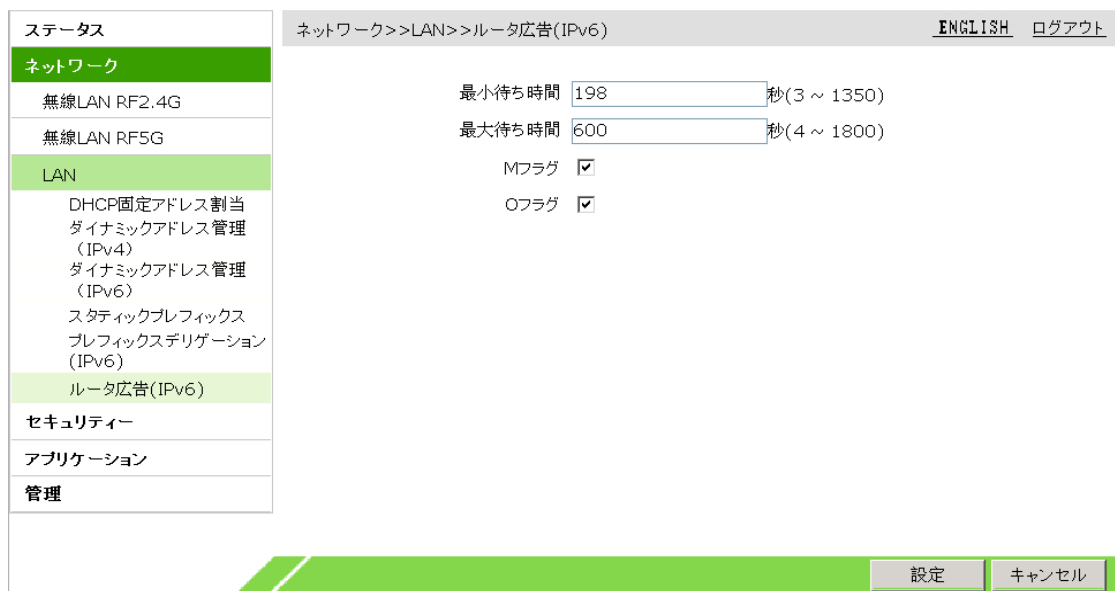


4.3.6 RA サービスの設定

この操作ではRAサービスのパラメータを設定します。SLAAC方式では、IPv6クライアント/サーバがRSメッセージを通じてIPv6アドレスのグローバルルーティングプレフィックスを取得します。ルータはクライアントからのRSメッセージを受信後、RA/RA-NACKメッセージを送信してグローバルルーティングプレフィックスを提供します。

1. WEB画面の左側メニューでネットワーク>LAN>ルータ広告(IPv6)を選択すると、ルータ広告(IPv6)画面に進みます。(図4-19)

図 4-21 ルータ広告(IPv6)画面



2.RAサービスのパラメータを設定して、**設定ボタン**をクリックします。

RAサービスのパラメータについては下の表を参照してください。

パラメータ	説明
最小待ち時間	RA待機の最小時間です。設定値の範囲は3～1350秒です。
最大待ち時間	RA待機の最大時間です。設定値の範囲は4～1800秒です。
M,O	<p>M: 管理アドレス設定フラグ (Managed address configuration) O: その他の状態設定フラグ (Other stateful configuration) チェックを入れると1、外すと0になります。設定値については以下をご参照ください。</p> <p>M=0、O=0のとき、SLAAC方式で情報を取得します。DHCPv6インフラストラクチャを備えていないネットワークに対応します。</p> <p>M=1、O=1のとき、DHCPv6方式でアドレスその他の設定を取得します。</p> <p>M=0、O=1のとき、ステートレス方式でアドレスの設定を取得します。DHCPv6はIPv6アドレス設定に使用せず、IPアドレスを除くネットワークパラメータ設定にのみ用います。</p> <p>M=1、O=1のとき、DHCPv6方式でアドレスを取得しますが、その他の設定には用いません。</p>

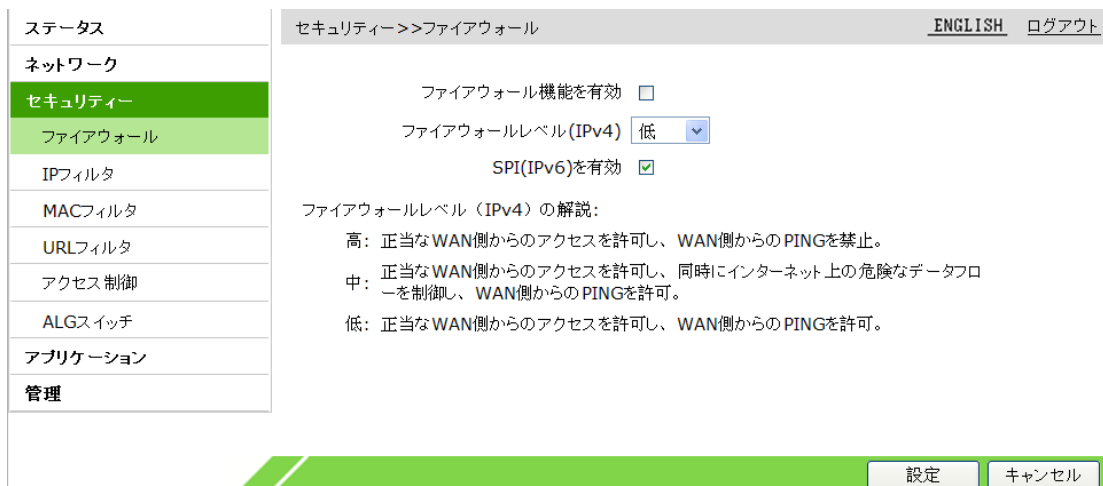
5 セキュリティ設定

5.1 ファイアウォールの設定

ファイアウォールを設定するとデバイスのセキュリティ性能が向上し、外部ネットワークからの悪意あるアクセスを防ぐことができます。

1.WEB画面の左側メニューで**セキュリティ>ファイアウォール**を選択すると、**ファイアウォール**設定画面に進みます。(図5-1)

図 5-1 ファイアウォールの設定画面



2.ファイアウォールに関するパラメータを設定し、設定ボタンをクリックします。

ファイアウォールのパラメータについては下の表を参照してください。

パラメータ	説明
ファイアウォール機能を有効にする	チェックを入れるとファイアウォール機能が有効になり、インターネットからのバッファオーバーフロー攻撃を防止できます。主に防止できる攻撃の種類はPing flood/Ping to death/Syn floodなどです。
ファイアウォールレベル (IPv4)	高: 明示的に定義したWANからアクセスするデバイスを許可しますが、インターネット上のデバイスから本製品WANインタフェースへのPingパケットを禁止します。 中: 明示的に定義したWANからアクセスするデバイスを許可し、インターネット上の危険なデータフローを一部ブロックします。 低: 明示的に定義したWANからアクセスするデバイスを許可し、インターネット上のデバイスから本製品WANインタフェースへのPingパケットも許可します。
SPI (IPv6) を有効にする	チェックを入れるとSPI (Stateful Packet Inspection、ステートフルパケットインスペクション型) ファイアウォール機能が有効になります。

5.2 IP フィルタの設定

この操作ではIPアドレスのフィルタ項目を設定することで、特定のIPアドレスから本製品へのアクセスを許可または拒否できます。

※設定ミスにより、アクセスができなくなる恐れがあります。

1.WEB画面の左側メニューでセキュリティ>IPフィルタを選択すると、IPフィルタ画面に進みます。

(図5-2)

図 5-2 IP フィルタの設定画面

ステータス セキュリティ>>IPフィルタ [ENGLISH](#) [ログアウト](#)

ネットワーク

セキュリティ

ファイアウォール

IPフィルタ

MACフィルタ

URLフィルタ

アクセス制御

ALGスイッチ

アプリケーション

管理

有効にする

プロトコル TCP

名前

(開始)送信元IPアドレス

(終了)送信元IPアドレス

(開始)宛先IPアドレス

(終了)宛先IPアドレス

(開始)送信元ポート

(終了)送信元ポート

(開始)宛先ポート

(終了)宛先ポート

着信インターフェイス

発信インターフェイス

モード 拒否

追加

有効にする	名前	(開始)送信元IP アドレス	(開始)送信元 ポート	(開始)宛先IP アドレス	(開始)宛先 ポート	着信インター フェイス	発信インター フェイス	変更	削除
プロトコル	モード	(終了)送信元IP アドレス	(終了)送信元 ポート	(終了)宛先IP アドレス	(終了)宛先 ポート				

データエントリがありません。

2. IPフィルタに関するパラメータを設定し、**追加**ボタンをクリックします。

IPフィルタのパラメータについては下の表を参照してください。

パラメータ	説明
有効にする	チェックを入れるとIPフィルタ項目が有効になります。
プロトコル	パケットフィルタのプロトコルを設定です。次のプロトコルをサポートしています。 <ul style="list-style-type: none"> • TCP(デフォルト) • UDP • TCP AND UDP • ICMP • ANY
(開始)送信元IPアドレス (終了)送信元IPアドレス	フィルタ条件を実際の状況に応じて設定します。オプションのパラメータですので、空欄にしておくこともできます。
(開始)宛先IPアドレス (終了)宛先IPアドレス	フィルタ条件を実際の状況に応じて設定します。オプションのパラメータですので、空欄にしておくこともできます。
(開始)送信元ポート (終了)送信元ポート	フィルタ条件を実際の状況に応じて設定します。オプションのパラメータですので、空欄にしておくこともできます。
(開始)宛先ポート (終了)宛先ポート	フィルタ条件を実際の状況に応じて設定します。オプションのパラメータですので、空欄にしておくこともできます。
着信インタフェース 発信インタフェース	データフローの方向です。着信インタフェースと発信インタフェースを同じにすることはできません。

パラメータ	説明
	着信インターフェースがLAN、発信インターフェースがブロードバンド接続のときは上りデータフローになります。 着信インターフェースがブロードバンド接続、発信インターフェースがLANのときは下りデータフローになります。
モード	拒否 許可

3.(オプション)フィルタ内容の後に表示される アイコンをクリックすると設定データを修正できます。

4.(オプション)フィルタ内容の後に表示される アイコンをクリックすると設定データを削除できます。

5.3 MAC フィルタの設定

MACアドレスのフィルタ項目を設定することで、特定のMACアドレスから本製品へのアクセスを許可または拒否できます。

※設定ミスにより、アクセスができなくなる恐れがあります。

関連情報

MACアドレスのフィルタはユーザー側のLAN、つまり上りデータフローにのみ対応します。

- 1.WEB画面の左側メニューで**セキュリティ**>**MACフィルタ**を選択すると、**MACフィルタ設定**画面に進みます。(図5-3)

図 5-3 MAC フィルタの設定画面

ステータス

ネットワーク

セキュリティ

ファイアウォール

IPフィルタ

MACフィルタ

URLフィルタ

アクセス制御

ALGスイッチ

アプリケーション

管理

ENGLISH ログアウト

セキュリティ>>MACフィルタ

1. 許可モードを選択した場合、始めに許可するMACアドレスを追加してください。

2. 動作モードは変更後すぐに有効になります。

有効にする

モード 拒否

タイプ ブリッジ

プロトコル IPプロトコル

送信元MACアドレス : : : : :

宛先MACアドレス : : : : :

追加

タイプ	プロトコル	送信元MACアドレス	宛先MACアドレス	変更	削除
データエントリがありません。					

2.MACフィルタに関するパラメータを設定し、追加ボタンをクリックします。

MACフィルタのパラメータについては下の表を参照してください。

パラメータ	説明
有効にする	チェックを入れるとMACフィルタが有効になります。
モード	<ul style="list-style-type: none"> ・ 拒否 ・ 許可
タイプ	<p>以下3つのタイプをサポートしています。</p> <ul style="list-style-type: none"> ・ ブリッジ(デフォルト) ・ ルーター ・ ブリッジ+ルーター
プロトコル	<p>データフローのプロトコルタイプです。以下のプロトコルをサポートしています。</p> <ul style="list-style-type: none"> ・ IP(デフォルト) ・ ARP ・ RARP ・ PPPoE ・ ALL
送信元MACアドレス	フィルタリングが必要なMACアドレスです。このパラメータは空欄にすることができません。
宛先MACアドレス	フィルタリングが必要なMACアドレスです。このパラメータは空欄にしておくこともできます。

3.(オプション)フィルタ内容の後に表示される アイコンをクリックすると設定データを修正できます。

4.(オプション)フィルタ内容の後に表示される アイコンをクリックすると設定データを削除できます。

5.4 URLフィルタの設定

URLフィルタ項目を設定することで、ユーザー側LANユーザーから特定のURLアドレスへのアクセスを許可または拒否できます。

- 1.WEB画面の左側メニューで**セキュリティ**>**URLフィルタ**を選択すると、URLフィルタ画面に進みます。
(図5-4)

図 5-4 URLフィルタの設定画面

ステータス	セキュリティ>>URLフィルタ	ENGLISH ログアウト
ネットワーク	有効にする <input type="checkbox"/>	
セキュリティ	モード ブラックリスト	
ファイアウォール	URLアドレス <input type="text"/>	
IPフィルタ	<input type="button" value="追加"/>	
MACフィルタ	ブラックリスト: 下記URLへのアクセスが遮断されます。 ホワイトリスト: 下記URLへのアクセスのみ許可されます。	
URLフィルタ		
アクセス制御		
ALGスイッチ		
アプリケーション		
管理		

URLアドレス	削除
データエントリがありません。	

- 2.URLフィルタに関するパラメータを設定し、**追加ボタン**をクリックします。

URLフィルタのパラメータについては下の表を参照してください。

パラメータ	説明
有効にする	チェックを入れるとURLフィルタが有効になります。
モード	・ 拒否 ・ 許可
URLアドレス	フィルタリングが必要なURLアドレスです。このパラメータは空欄にすることができません。

- 3.フィルタ内容の後に表示される アイコンをクリックすると設定データを削除できます。

5.5 アクセス制御の設定

アクセス制御のフィルタを設定することで、特定のサービスから本製品へのアクセスを許可または拒否できます。

- 1.WEB画面の左側メニューで**セキュリティ**>**アクセス制御**を選択すると、**アクセス制御設定画面**に進みます。(図5-5)

図 5-5 アクセス制御の設定画面

ステータス
ネットワーク
セキュリティ
ファイアウォール
IPフィルタ
MACフィルタ
URLフィルタ
アクセス制御
ALGスイッチ
アプリケーション
管理

セキュリティ>>アクセス制御 ENGLISH ログアウト

有効にする

着信インターフェイス

(開始)送信元IPアドレス

(終了)送信元IPアドレス

モード

HTTP
 FTP
 TELNET
 HTTPS

サービスのリスト [リモートアクセスポートを変更](#)

有効にする	着信インターフェイス	(開始)送信元IPアドレス	(終了)送信元IPアドレス	モード	サービスのリスト	変更	削除
<input checked="" type="checkbox"/>	omci_1_			許可する	HTTP		

2.サービス制御に関するパラメータを設定し、**追加**ボタンをクリックします。

サービス制御のパラメータ詳細は下の表を参照してください。

パラメータ	説明
有効にする	チェックを入れるとサービス制御の当該項目が有効になります。
着信インタフェース	サービスの送信元です。以下3種類の送信元から選択できます。 「LAN」: ユーザー側からのアクセスです。 ・「omci1_dhcp」: OMCi管理チャンネルからのアクセスです。 ・「WAN」: ネットワーク側からのアクセスです。
(開始)送信元/(終了)送信元IPアドレス	サービス制御が必要なIPセクションです。
モード	・ 拒否 ・ 許可
サービスのリスト	制御するサービスです。以下の4種類から選択出来ます。 ・ HTTP ・ FTP ・ TELNET ・ HTTPS
リモートアクセスポートを変更	リンクをクリックしてサービスのアクセスポートを変更します。

3.(オプション)フィルタ内容の後に表示される アイコンをクリックすると設定データを修正できます。

4.(オプション)フィルタ内容の後に表示される アイコンをクリックすると設定データを削除できます。

5.6 ALG スイッチの設定

ALG(Application Layer Gateway)スイッチは、特定の Application の IP パケットのペイロードに含まれる IP アドレスの変換を有効にします。

チェックを入れると当該プロトコルの項目の ALG が有効になります。

FTP(File Transfer Protocol)
TFTP(Trivial File Transfer Protocol)
SIP(Session Initiation Protocol)
L2TP(Layer 2 Tunneling Protocol)
H323(H.323 Protocol)
RTSP(Real Time Streaming Protocol)
PPTP(Point-to-Point Tunneling Protocol)
IPSEC(IPsec – Security Architecture for Internet Protocol)

以下画面で ALG スイッチの設定ができます。

図 5-6 ALG スイッチの設定画面



6 アプリケーションの設定

6.1 DMZ の設定

DMZの設定によりDMZの全ポートマッピング機能が有効になり、宛先アドレスのDNAT変換でLAN側本体の対外サービスを実現します。この設定を省略すると、システムは全ポートを開放します。

- 1.WEB画面の左側メニューで**アプリケーション>DMZ**を選択すると、**DMZ**設定画面に進みます。(図6-1)

図 6-1 DMZ の設定画面

ステータス	アプリケーション>>DMZ	ENGLISH ログアウト
ネットワーク		
セキュリティ		
アプリケーション		
DMZ		
UPnP		
UPnPポートマッピング		
ポートフォワーディング		
DNSサービス		
SNTP(時刻同期)		
USBストレージ		
メディア共有		
FTPアプリケーション		
ポートトリガー		
ポートフォワーディング (アプリケーションリスト)		
アプリケーションリスト		
ホーム共有(samba)		
管理		

有効にする

IPv4

WAN接続 ▼

MACアドレスのマッピングを有効にする

LANのIPアドレス

IPv6

最大8アドレス 追加

LANのIPv6アドレス

設定
キャンセル

2.DMZに関するパラメータを設定して、設定ボタンをクリックします。

DMZのパラメータについては下の表を参照してください。

パラメータ	説明
有効にする	チェックを入れるとDMZ機能が有効になります。
WAN接続	LAN側本体の對外サービスで採用するWAN接続です。
MACアドレスのマッピングを有効にする	チェックを入れるとMACアドレスのマッピングが有効になります。 MACアドレスのマッピングを有効にするときは、LANのMACアドレス設定が必要です。 ・MACアドレスのマッピングを有効にしていない場合、システムはIPアドレスのマッピング使用を省略します。
LANのMACアドレス	LAN側本体の對外サービス提供時にマッピングするMACアドレスです。
LANのIPアドレス	LAN側本体の對外サービス提供時にマッピングするIPアドレスです。
LANのIPv6アドレス	LAN側本体の對外サービス提供時にマッピングするIPv6アドレスです。最大8つのIPv6アドレスをサポートします。追加ボタンをクリックしてIPv6アドレスを追加します。

6.2 UPnP の設定

UPnP機能を設定すると、デバイスが何らかのネットワークに接続したとき、そのIPアドレスを取得し、その機能を知らせると同時に、その他のデバイス機能を知ることができます。

- 1.WEB画面の左側メニューでアプリケーション>UPnPを選択すると、UPnP設定画面に進みます。(図 6-2)

図 6-2 UPnP 設定画面



2.UPnPに関するパラメータを設定し、**設定ボタン**をクリックします。

UPnPのパラメータについては下の表を参照してください。

パラメータ	説明
UPnPを有効にする	チェックを入れるとUPnP機能が有効になります。
WAN接続	WAN側のブロードバンド接続です。
広報の周期(分)	UPnPデバイスの広報の周期、(広報パケットを送信する時間間隔)です。周期内に広報パケットが送信されないときは、UPnPデバイスが失効していると判断できます。デフォルトでは30分間と設定されています。
生存時間(ホップ数)	UPnPデバイスの広報関連パケットのTTL値、(ルータが廃棄するまでの最大転送回数)です。初期値4の使用をおすすめします。

6.3 UPnP ポートマッピングの確認


WEB画面でUPnPデバイスの状態、プロトコル、入力/出力ポート番号、IPアドレスを含むポートマッピング情報を表示できます。

- 1.WEB画面の左側メニューで**アプリケーション>UPnPポートマッピング**を選択すると、UPnPポートマッピング画面に進みます。(図6-3)

図 6-3 UPnP ポートマッピング画面



2.更新ボタンをクリックするとUPnPポートマッピング情報を更新できます。

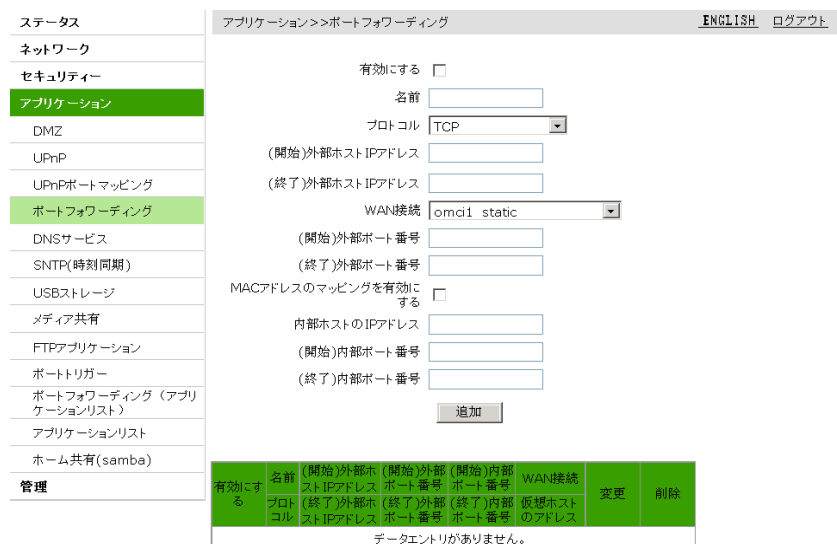
3.(オプション)ポートマッピング内容の後に表示される  アイコンをクリックすると設定データを削除できます。

6.4 仮想ホストの設定

仮想ホストを設定すると、WAN側をクライアントのLAN側にアクセスするサーバにすることができます。

1. WEB画面の左側メニューでアプリケーション>仮想ホストを選択すると、仮想ホストの設定画面に進みます。(図6-4)

図 6-4 仮想ホストの設定画面





2.仮想ホストに関するパラメータを設定して、追加ボタンをクリックします。

仮想ホストのパラメータについては次の表を参照してください。

パラメータ	説明
有効にする	チェックを入れると仮想ホスト機能が有効になります。
名前	仮想ホストの名前です。
プロトコル	プロトコルのタイプを選択します。以下のプロトコルをサポートしています。

パラメータ	説明
	<ul style="list-style-type: none"> ・ TCP(デフォルト) ・ UDP ・ TCP AND UDP
(開始)外部ホストIPアドレス	WAN側ホストの開始IPアドレスです。
(終了)外部ホストIPアドレス	WAN側ホストの終了IPアドレスです。
WAN接続	ユーザー側の仮想ホストにアクセスするWAN接続です。
(開始)外部ポート番号	WAN側ターゲットの開始ポート番号です。
(終了)外部ポート番号	WAN側ターゲットの終了ポート番号です。
MACアドレスのマッピングを有効にする	チェックを入れるとMACアドレスのマッピング機能が有効になります。
内部ホストのMACアドレス	LAN側ホストのMACアドレスです(MACアドレスのマッピング機能が有効のときのみ有効)。
内部ホストのIPアドレス	LAN側ホストのIPアドレスです。
(開始)内部ポート番号	LAN側ホストの開始ポート番号です。
(終了)内部ポート番号	LAN側ホストの終了ポート番号です。

- 3.(オプション)仮想ホスト内容の後に表示される  アイコンをクリックすると設定データを修正できます。
- 4.(オプション)仮想ホスト内容の後に表示される  アイコンをクリックすると設定データを削除できます。

6.5 DNS サービスの設定

本製品のDNSサービス設定には以下の内容が含まれます。

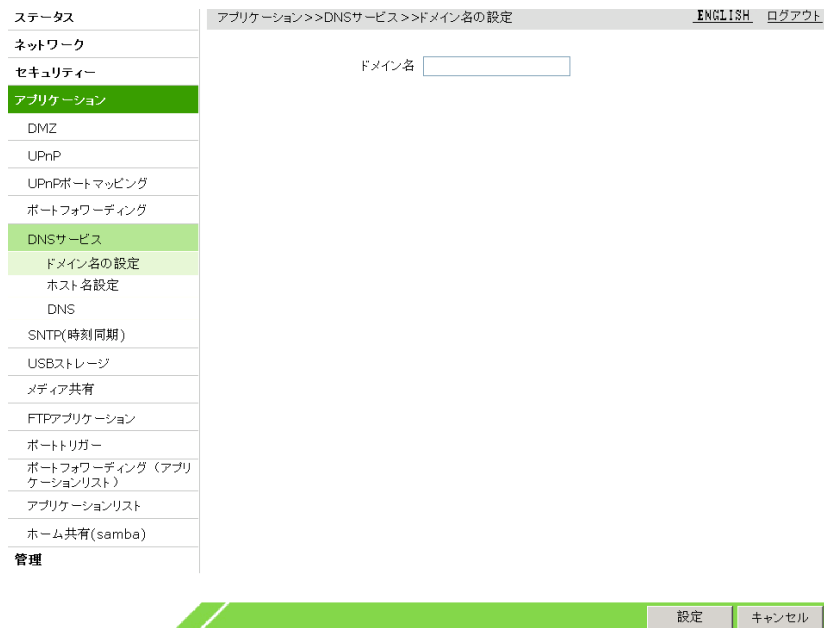
- ・ドメイン名の設定
- ・ホスト名の設定
- ・DNSサーバの設定

6.5.1ドメイン名の設定

ドメイン名の設定により、本製品を対応するネットワークドメインに加えます。

- 1.WEB画面の左側メニューでネットワーク>DNSサービスを選択すると、ドメイン名の設定画面に進みます。(図6-5)

図 6-5 ドメイン名の設定画面



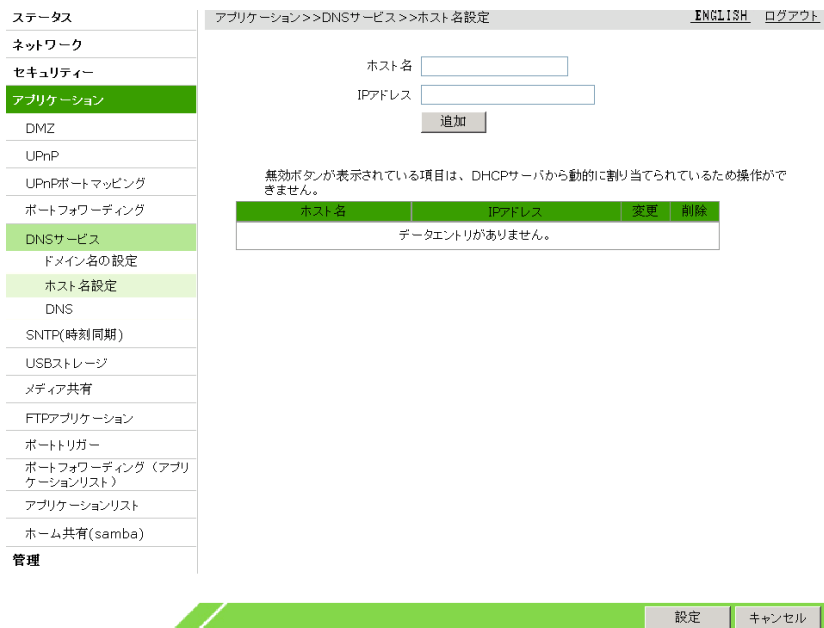
2.ドメイン名テキストボックスに本製品のドメイン名を入力し、設定ボタンをクリックします。

6.5.2ホスト名の設定


ホスト名の設定により、ユーザー側ネットワークのホスト名とIPアドレスのマッピング関係を管理します。


1. WEB画面の左側メニューでアプリケーション>ホスト名設定を選択すると、ホスト名設定画面に進みます。(図6-6)

図 6-6 ホスト名の設定画面



2.ホスト名とIPアドレスを設定し、追加ボタンをクリックします。

3.(オプション)ホスト名の後に表示される  アイコンをクリックすると設定データを修正できます。

4.(オプション)ホスト名の後に表示される  アイコンをクリックすると設定データを削除できます。

6.5.3 DNS サーバの設定

全局DNSサーバの設定により、具体的なWAN接続を指定しない一部機能を全局DNSサーバで中継できます。

1. WEB画面の左側メニューで**アプリケーション>DNSサービス**を選択すると、DNS設定画面に進みます。(図6-7)

図 6-7 DNS の設定画面

ステータス	アプリケーション>>DNSサービス>>DNS	ENGLISH	ログアウト
ネットワーク			
セキュリティ	IPv4 DNSサーバー1	<input type="text"/>	
アプリケーション	IPv4 DNSサーバー2	<input type="text"/>	
DMZ	IPv6 DNSサーバー1	<input type="text"/>	
UPnP	IPv6 DNSサーバー2	<input type="text"/>	
UPnPポートマッピング			
ポートフォワーディング			
DNSサービス			
ドメイン名の設定			
ホスト名設定			
DNS			
SNTP(時刻同期)			
USBストレージ			
メディア共有			
FTPアプリケーション			
ポートリガー			
ポートフォワーディング (アプリケーションリスト)			
アプリケーションリスト			
ホーム共有(samba)			
管理			

設定 キャンセル

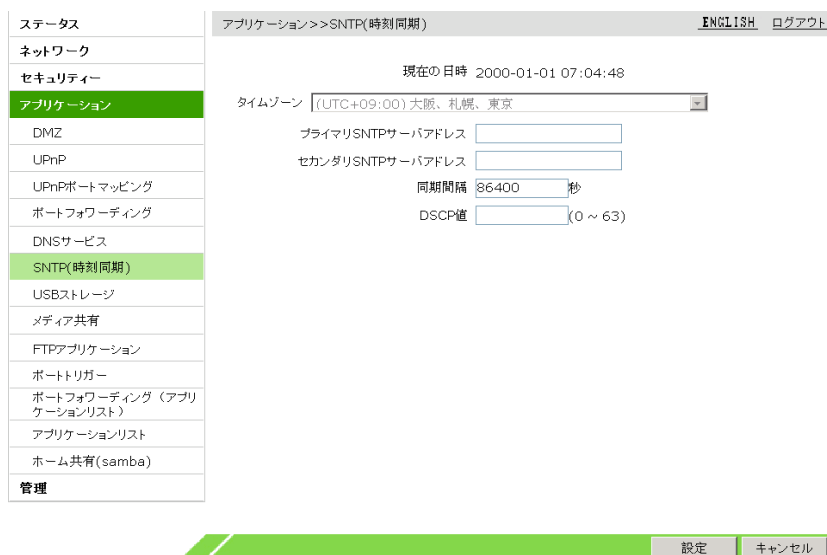
2. DNSサーバのIPアドレスを設定して、**設定ボタン**をクリックします。

6.6 SNTP(時刻同期)設定

SNTP設定後、本製品はNTPクライアントとして定期的にNTPサーバーと時刻を同期できます。

1. WEB画面の左側メニューで**アプリケーション>SNTP(時刻同期)**を選択すると、下の図のようなSNTP(時刻同期)画面に進みます。(図6-8)

図 6-8 SNTP(時刻同期)画面



2. SNTPパラメータを設定し、**設定ボタン**をクリックします。SNTPのパラメータは下記表をご参照ください。

3.

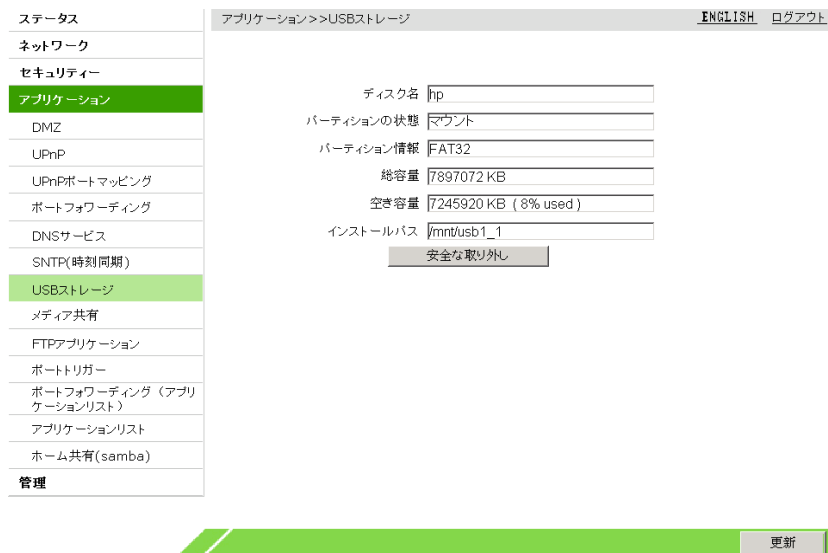
パラメータ	説明
タイムゾーン	本製品所在の場所
プライマリSNTPサーバアドレス	プライマリSNTPサーバのアドレス
セカンダリSNTPサーバアドレス	セカンダリSNTPサーバのアドレス
同期間隔	本製品がNTPサーバにリクエストを送信する間隔。 設定範囲： 3600～86400秒。デフォルトは86400秒。
DSCP	リクエストメッセージのDSCP優先順位設定

6.7 USBストレージの容量確認

この操作ではUSBインタフェースに接続されているストレージの容量を確認します。

4.WEB画面の左側メニューで**アプリケーション>USBストレージ**を選択すると、下の図のような**USBストレージ画面**に進みます。(図6-9)

図 6-9 USBストレージ画面



2.安全な取り外しボタンをクリックすると、USBデバイスを安全に取り外すことができます。

3.(オプション)更新ボタンをクリックすると画面が更新できます。

6.8 メディア共有

デジタルメディアサーバー機能になります。共有ディレクトリが4つまで選択できます。WEB画面の左側メニューでFTPアプリケーション>メディア共有を選択すると、メディア共有設定画面に進みます。(図6-10)

図 6-10 メディア共有設定画面



6.9 FTP 設定

本製品のFTP設定には以下の内容が含まれます。

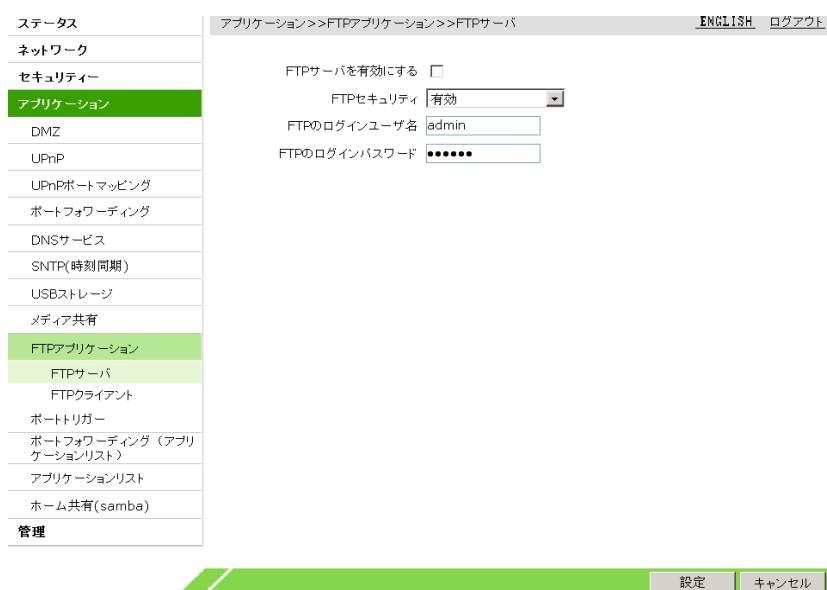
- FTPサーバ設定
- FTPクライアント設定

6.9.1 FTP サーバ設定

FTPサーバ機能を有効にし、ユーザー名とパスワードを指定します。

1.WEB画面の左側メニューでFTPアプリケーション>FTPサーバを選択すると、FTPサーバ設定画面に進みます。(図6-11)

図 6-11 FTP サーバ設定画面



2.FTPサーバのパラメータを設定し、設定をクリックします。

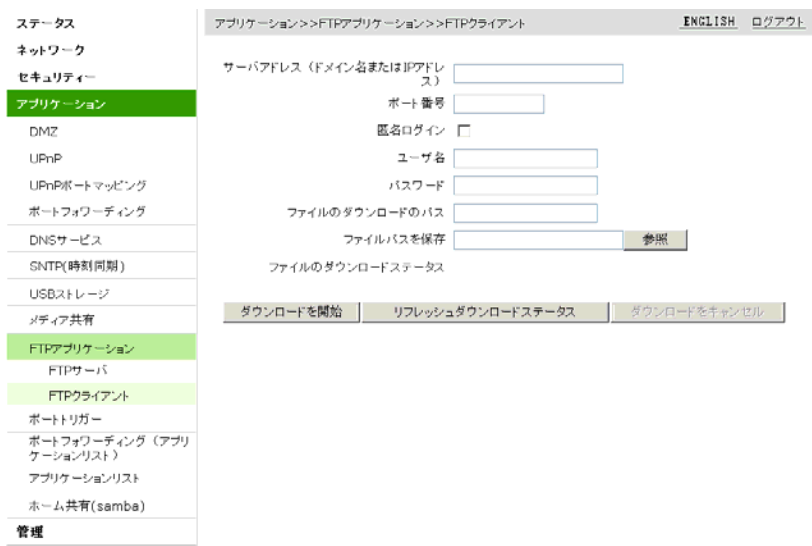
パラメータ	説明
FTPサーバを有効にする	FTPサーバを有効にする
FTPセキュリティ	FTPセキュリティ機能の有効/無効を設定します
FTPユーザ名/パスワード	FTPセキュリティ機能を有効に設定したときに設定できます

6.9.2 FTP クライアント設定

本製品はFTPクライアントとして、外部FTPサーバよりファイルをダウンロードできます。

1.WEB画面の左側メニューでFTPアプリケーション>FTPクライアントを選択すると、FTPクライアント設定画面に進みます。(図6-12)

図 6-12 FTPクライアント設定画面



2.FTPクライアントパラメータを設定し、「ダウンロードを開始」ボタンをクリックします。

FTPクライアントのパラメータは下記をご参考ください。

パラメータ	説明
サーバアドレス(ドメイン名またはIPアドレス)	FTPサーバのドメイン名またはIPアドレスを設定します
ポート番号	FTPポート番号を設定します
匿名ログイン	匿名でFTPサーバにアクセスします
ユーザ名/パスワード	非匿名でサーバにアクセスする際のユーザ名とパスワード
ファイルダウンロードのパス	FTPサーバ上にあるダウンロード予定のファイルパスとファイル名
ファイルパスを保存	ファイルを保存するパス
ファイルのダウンロードステータス	ファイルダウンロードのステータス表示

3.(オプション)「リフレッシュダウンロードステータス」ボタンをクリックして、最新のダウンロード状況を確認できます。「ダウンロードをキャンセル」ボタンをクリックして、ダウンロードをキャンセルできます。

6.10 ポートトリガーの設定

ポートをポートトリガーに設定すると、システムのなんらかのアプリケーションがポートトリガーを使用して外部と接続を確立するとき、デバイスに接続されたルータが外部接続を内部の中継ポートへ転送します。

関連情報

ポートトリガーのアプリケーションは保護が必要なポートに用います。システムが直接ポートを開放する必要がなく、トリガーが必要となきのみ対象ポートが開放されます。

1. WEB画面の左側メニューで**アプリケーション>ポートトリガー**を選択すると、**ポートトリガー設定画面**に進みます。(図6-13)

図 6-13 ポートトリガー設定画面

ステータス アプリケーション>>ポートトリガー ENGLISH ログアウト

ネットワーク

セキュリティ

アプリケーション

DMZ

UPnP

UPnPポートマッピング

ポートフォワーディング

DNSサービス

SNTP(時刻同期)

USBストレージ

メディア共有

FTPアプリケーション

ポートトリガー

ポートフォワーディング(アプリケーションリスト)

アプリケーションリスト

ホーム共有(samba)

管理

有効にする

アプリケーション名

トリガ側のIPアドレス

サービスの種類

トリガポート

接続

〈開始〉WANポート

〈終了〉WANポート

タイムアウト (60~1800秒)


アプリケーション名	有効	サービスの種類	トリガ側のIPアドレス	トリガポート	〈開始〉WANポート	〈終了〉WANポート	変更	削除
データエントリがありません。								

2.ポートトリガーに関するパラメータを設定して、追加ボタンをクリックします。

ポートトリガーのパラメータについては下の表を参照してください。

パラメータ	説明
有効にする	チェックを入れるとポートトリガー項目が有効になります。
アプリケーション名	このポートトリガー項目の名前です。
トリガ側のIPアドレス	デバイスがアクセスするIPアドレスです。
サービスの種類	アプリケーションのアクセスサービスの種類です。TCP、UDP、TCP AND UDPから選択できます。デフォルトではTCPとなっています。
トリガポート	デバイスがアクセスするプロトコルのポートです。このパラメータは空欄にすることができません。
接続	外部ルータとの接続に使用するプロトコルです。以下のプロトコルをサポートしています。 ・ TCP(デフォルト) ・ UDP ・ TCP AND UDP
〈開始〉WANポート 〈終了〉WANポート	トリガポートマッピングのデバイスプロトコルポートの範囲(パケット内レイヤ4のポート番号)です。デバイスがトリガポートにアクセスすると、開始ポート/終了ポートのサービスが有効になります。このパラメータは空欄にすることができません。また、開始ポートと終了ポートの差は1から9の間にする必要があります。
タイムアウト	一定時間内にデータフローがない場合、タイムアウトします。

3.(オプション)トリガ内容の後に表示される  アイコンをクリックすると設定データを修正できます。

4.(オプション)トリガ内容の後に表示される  アイコンをクリックすると設定データを削除できます。

6.11 ポートフォワーディング(アプリケーションリスト)の設定

ポートフォワーディング(アプリケーションリスト)を設定すると、WAN側をクライアントのLAN側にアクセスするサーバにすることができます。

事前確認事項

アプリケーションリストの設定が完了していることをご確認ください(6.14参照)。

- 1.WEB画面の左側メニューで**アプリケーション>ポートフォワーディング(アプリケーションリスト)**を選択すると、**ポートフォワーディング(アプリケーションリスト)**の設定画面に進みます。(図6-14)

図 6-14 ポートフォワーディング(アプリケーションリスト)の設定画面

ステータス
ネットワーク
セキュリティ
アプリケーション
DMZ
UPnP
UPnPポートマッピング
ポートフォワーディング
DNSサービス
SNTP(時刻同期)
USBストレージ
メディア共有
FTPアプリケーション
ポートリガー
ポートフォワーディング(アプリケーションリスト)
アプリケーションリスト
ホーム共有(samba)
管理

アプリケーション>>ポートフォワーディング(アプリケーションリスト) ENGLISH ログアウト


WAN接続 omci1 static
内部ホストのIPアドレス
アプリケーション
追加

WAN接続	内部ホストのIPアドレス	アプリケーション	削除
データエントリがありません。			

- 2.関連するパラメータを設定し、**追加**ボタンをクリックします。

パラメータについては下の表を参照してください。

パラメータ	説明
WAN接続	ユーザー側の仮想ホストにアクセスするWAN接続です。
内部ホストのIPアドレス	LAN側をホストのIPアドレスに設定します。
アプリケーション	アプリケーションの呼び出しにより、パケットの外部プロトコルポート番号と内部プロトコルポート番号のマッピングを行います。

- 3.(オプション)アプリケーション内容の後に表示される  アイコンをクリックすると設定データを削除できます。

6.12 アプリケーションリストの設定

アプリケーションリストを設定すると、下りパケットのプロトコルポート番号のマッピング関係を確立し、ポートフォワーディング(アプリケーションリスト)など他の具体的な機能から呼び出せるようになります。

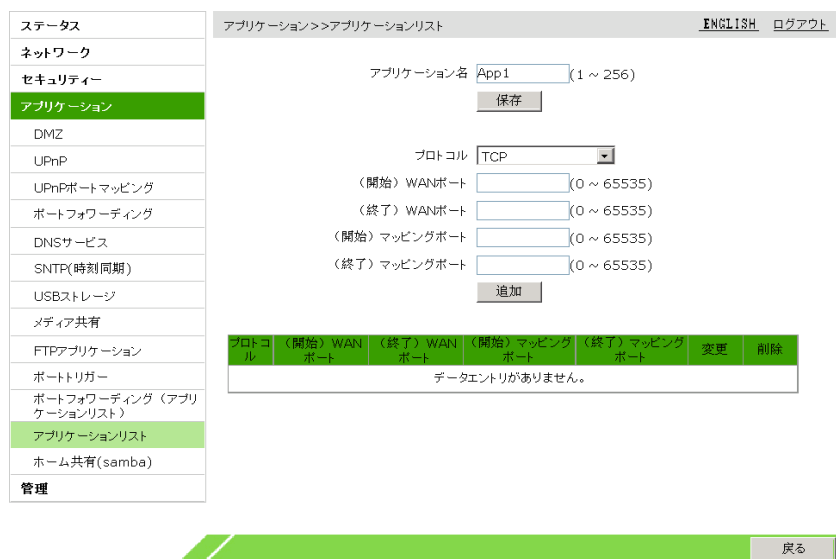
- 1.WEB画面の左側メニューで**アプリケーション>アプリケーションリスト**を選択すると、**アプリケーションリスト**設定画面に進みます。(図6-15)

図 6-15 アプリケーションリストの設定画面



2. 「アプリケーションを追加するには、ここをクリックしてください」のリンクをクリックするとアプリケーションの追加画面に進みます。

図 6-16 アプリケーションリストの追加画面



3. プロトコル等パラメータを設定し、追加ボタンをクリックすると、ポートフォワーディングリストの設定が追加されます。図6-17)

図 6-17 アプリケーションリストの追加完了画面

プロトコル	(開始)WANポート	(終了)WANポート	(開始)マッピングポート	(終了)マッピングポート	変更	削除
TCP	10	20	10	20		

アプリケーションリストの各パラメータに詳細については下の表を参照してください。

パラメータ	説明
アプリケーション名	アプリケーションプログラムの名前です。名前入力後 変更 ボタンをクリックすると変更されます。
プロトコル	プロトコル選択プルダウンリストです。以下のプロトコルをサポートしています。 ・ TCP(デフォルト) ・ UDP ・ TCP AND UDP
(開始)WANポート (終了)WANポート	下りパケットの初期プロトコルポート番号範囲です。
(開始)マッピングポート (終了)マッピングポート	下りパケットのマッピングされたプロトコルポート番号範囲です。

- (オプション)アプリケーション内容の後に表示される アイコンをクリックすると設定データを修正できます。
- (オプション)アプリケーション内容の後に表示される アイコンをクリックすると設定データを削除できます。

6.13 ホーム共有(samba)

Samba アプリケーションリストを設定すると、下りパケットのプロトコルポート番号のマッピング関係を確立し、ポートフォワーディング(アプリケーションリスト)など他の具体的な機能から呼び出せるようになります。

電源を入れると smbд を自動的に有効されたい場合、「samba サーバ機能を有効」のチェックを入れてください。USB 機器を検知でき次第 smbд を有効にされたい場合、「自動的に Samba サーバを実行する」のチェックを入れてください。

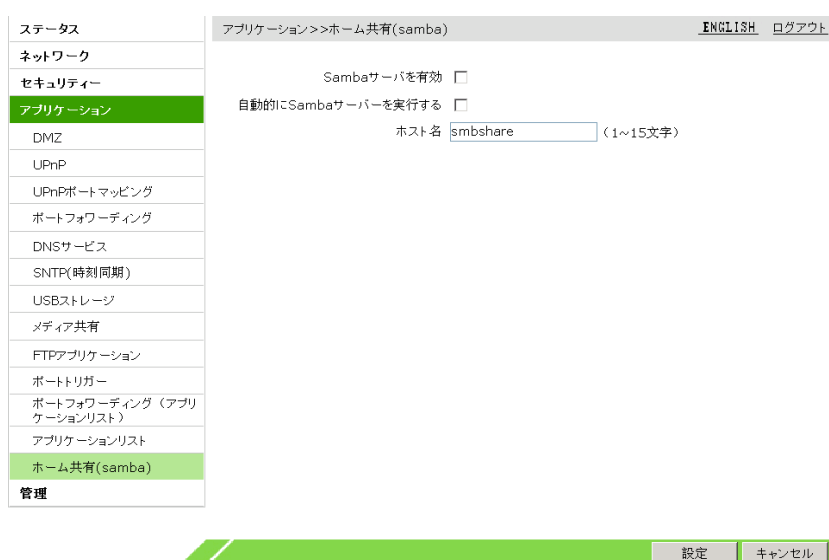
ホスト名について

- 空欄不可

- 2、2桁-15桁半角英数字・記号(_)(.)の乱数(大文字・小文字混在)
- 3、最初と最後は数字か英字
- 4、数字のみのドメイン名(NDN)が登録不可
- 5、ドメイン名「.」の後に全部数字が登録不可

WEB画面の左側メニューでFTPアプリケーション>ホーム共有(samba)を選択すると、ホーム共有(samba)設定画面に進みます。(図6-18)

図 6-18 メディア共有設定画面



7 管理の設定

7.1 ユーザー管理の設定

ユーザーはここでアカウントのパスワードを変更することができます。

- 1.WEB 画面の左側メニューで管理>システム管理を選択すると、システム管理設定画面に進みます。

図 7-1 ユーザー管理画面

ステータス	管理>>ユーザ管理	ENGLISH ログアウト
ネットワーク	ユーザ名 <input type="text" value="admin"/>	
セキュリティ	古いパスワード <input type="text"/>	
アプリケーション	新しいパスワード <input type="text"/>	
管理	新しいパスワードの確認 <input type="text"/>	
ユーザ管理		
システム管理		
ログ管理		
診断メンテナンス		

設定 キャンセル

2.ユーザーアカウントのパラメータを設定して、**設定**ボタンをクリックします。

ユーザーアカウントのパラメータについては下の表を参照してください。

パラメータ	説明
ユーザー名	このパラメータは設定できません。システムのデフォルト管理者アカウントはadminとなっています。
古いパスワード	システムのデフォルト管理者アカウントのパスワードです。
新しいパスワード	ユーザー自身がパスワードを定義します。
新しいパスワードの確認	入力が 新しいパスワード と一致しているかご確認ください。

7.2 システム管理

本製品のシステム管理では以下の内容について説明します。

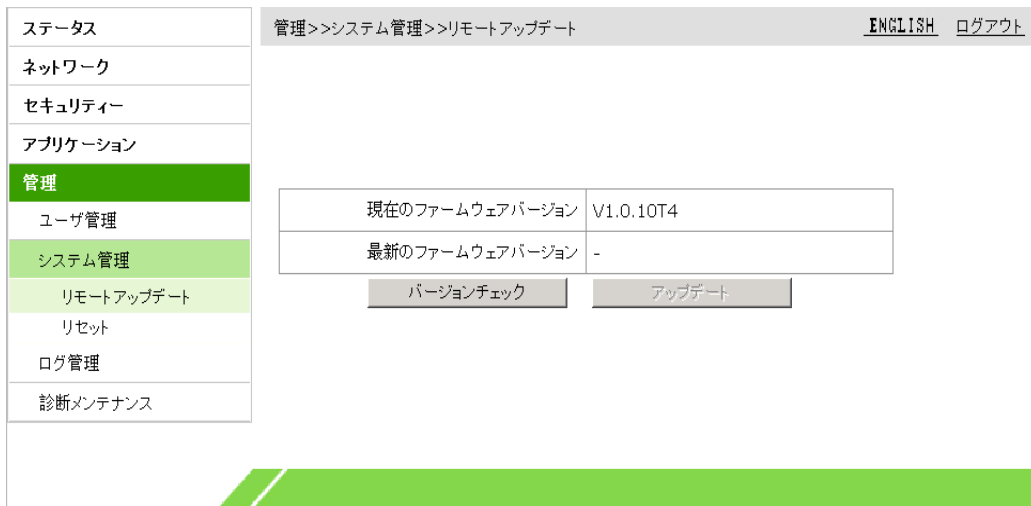
- ・リモートアップデート
- ・リセット

7.2.1 リモートアップデートの設定

サービス提供元がお客様側にある本製品のバージョンまたは設定ファイルを一括してアップグレードする必要があるときは、リモートアップデートが利用できます。リモートアップデートの完了後、ONUは再起動します。リモートアップデート中はONUのシャットダウンや再起動を行わないでください。ONUが正常に使用できなくなる恐れがあります。

1.WEB画面の左側メニューで**管理>システム管理>リモートアップデート**を選択すると、**リモートアップデート**設定画面に進みます。(図7-2)

図 7-2 リモートアップデートの設定画面



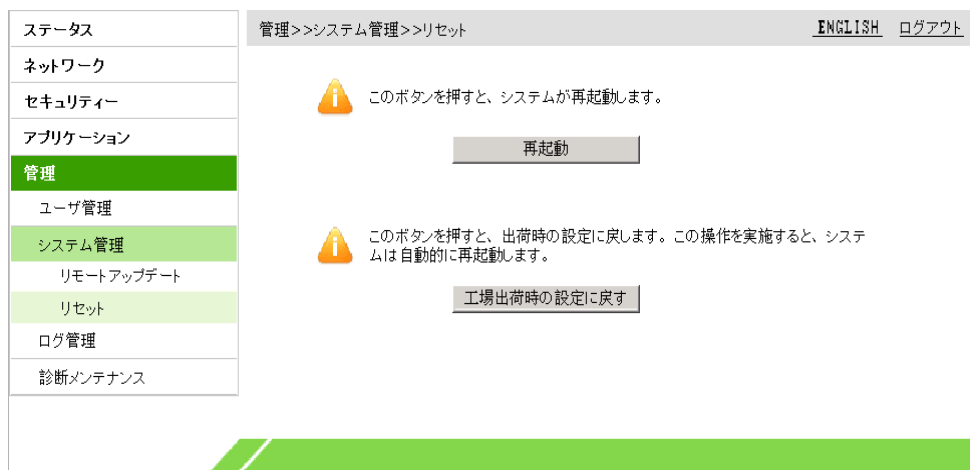
- バージョンチェックボタンをクリックすると、現在利用しているバージョンとサーバー上にある最新バージョンが表示されます。
- サーバー上により新しいバージョンがある場合、アップデートボタンが有効になります。アップデートボタンをクリックしてアップデートしてください。

7.2.2 リセット

管理メニューで、本製品の再起動や工場出荷設定への復元ができます。

- WEB画面の左側メニューで**管理 > システム管理 > リセット**を選択すると、リセット設定画面に進みます。(図7-3)

図 7-3 リセット設定画面



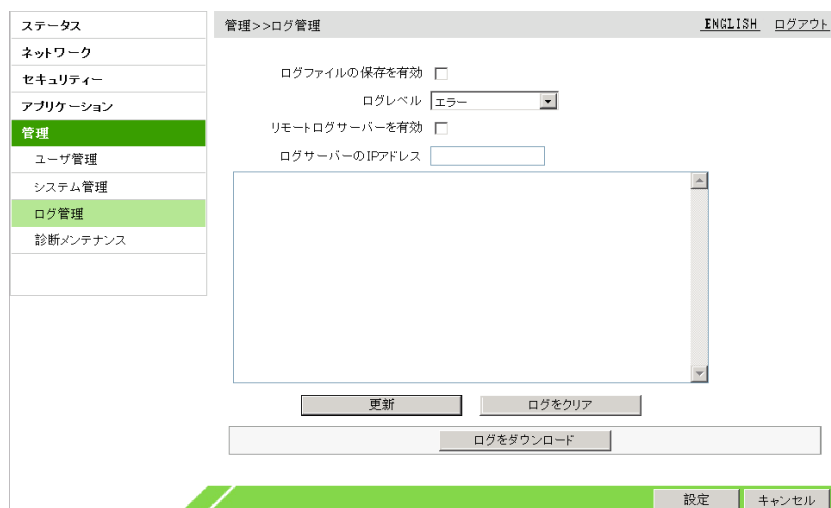
- 「再起動」ボタンをクリックすると、本製品が自動で再起動します。
- 「工場出荷時の設定に戻す」ボタンをクリックすると、本工場出荷時設定に復元して再起動します。

7.3 ログ管理の設定

ログ管理メニューでログのプリント機能を有効にするや、ログをリモートサーバ上にエクスポートすることができます。また、クラス別にデバイスの警告、通知、デバッグ情報も出力できます。

- WEB画面の左側メニューで**管理 > ログ管理**を選択すると、ログ管理設定画面に進みます。(図7-4)

図 7-4 ログ管理画面



2.ログ管理に関するパラメータを設定し、**設定ボタン**をクリックします。

ログ管理のパラメータについては下の表をご参照ください。

パラメータ	説明
ログファイルの保存を有効にする	チェックを入れるとログファイルのローカル保存機能が有効になります。
ログレベル	ログのレベルは低い順に Debug、Informational、Notice、Warning、Error、Critical、Alert、Emergencyです。ログレベルの設定が完了すると、そのレベル以上のログのみ記録するようになります。
リモートログサーバーを有効	チェックを入れるとリモートログサーバー機能が有効になり、ログが定期的リモートログサーバーへアップロードされます。
ログサーバーのIPアドレス	リモートログサーバーのIPアドレスです。

3.(オプション)**更新**ボタンをクリックすると、最新20件のログがテキストボックスに表示されます。

4.(オプション)**ログをクリア**ボタンをクリックすると、テキストボックスに表示中のログがクリアされます。

5.(オプション)**ログをダウンロード**するボタンをクリックすると、ログをローカルにダウンロードできます。

7.4 診断メンテナンス

本製品の診断メンテナンスでは以下の内容について説明します。

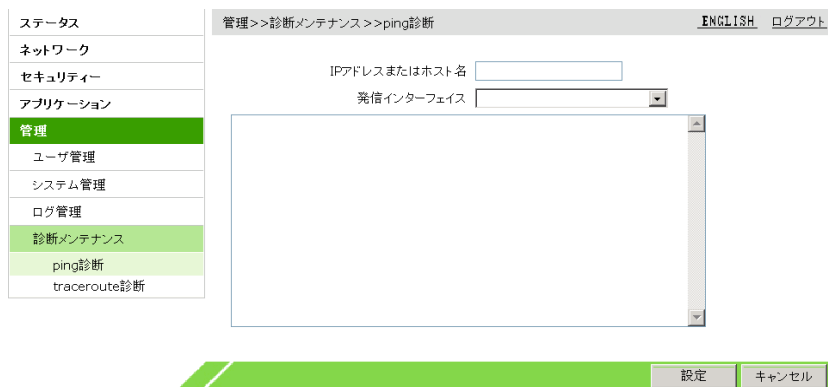
- Ping診断の設定
- Trace Route診断の設定

7.4.1 Ping 診断の設定

Ping診断メニューで、本製品のネットワークのリンク状況を確認できます。

- 1.WEB画面の左側メニューで**管理>診断メンテナンス**を選択すると、**Ping診断**設定画面に進みます。
(図7-5)

図 7-5 Ping 診断の設定画面



2. Ping診断に関するパラメータを設定し、**設定**ボタンをクリックします。

Ping診断のパラメータについては下の表を参照してください。

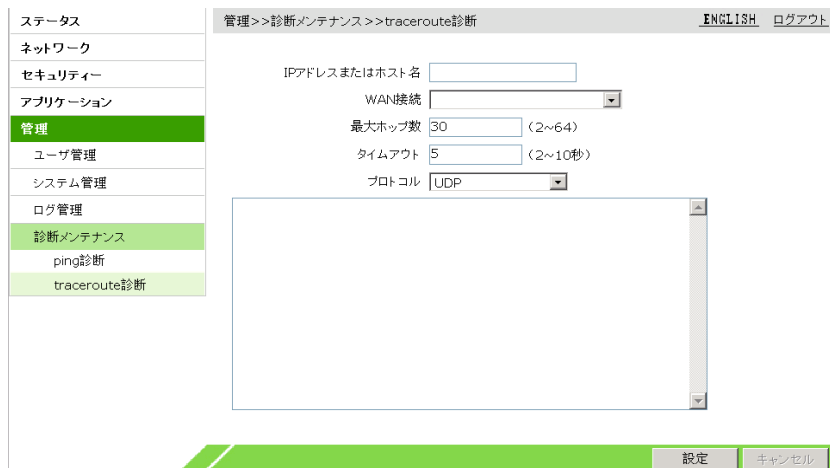
パラメータ	説明
IPアドレスまたはホスト名	PingのターゲットIPアドレスまたはホスト名です。
発信インタフェース	外部ネットワークとの接続状況を試験する場合、対応するWAN接続も選択する必要があります。

7.4.2 Trace Route 診断の設定

Trace Routeは宛先アドレスまでにパケットが通ったノード、(ある発信元から宛先までのパス)を確認できます。リンクのpingが通らないとき、Trace Routeで問題のあるノードを検出することができます。

1. WEB画面の左側メニューで**管理>診断メンテナンス>Trace Route診断**を選択すると、**Trace Route診断**画面に進みます。(図7-6)

図 7-6 Trace Route 診断の設定画面



2. Trace Route診断に関するパラメータを設定して、**設定**ボタンをクリックし、Trace Route診断を起動します。

Trace Route診断のパラメータについては下の表を参照してください。

パラメータ	説明
IPアドレスまたはホスト名	Trace RouteのターゲットIPアドレスまたはホスト名です。

パラメータ	説明
WAN接続	外部ネットワークとの接続状況を試験する場合、対応するWAN接続も選択する必要があります。
最大ホップ数	Trace Route診断のパケットが目的地までに経る最大ホップ数です。
タイムアウト	応答パケットの待機時間です。この時間を超えても応答パケットが受信されない場合、星印が表示されます。星印の表示が続く場合、その対応するノードに問題があることを示します。
プロトコル	UDPまたはICMPプロトコルを使います。

8 Q&A

8.1 Q&A

POWER LEDが点灯しません。

電源がオフになっています。付属品の電源アダプタが正常に接続しているかご確認ください。

通電後ALARM LEDが赤色で点灯しています。

ONU本体が故障しています。ONUをリセットしLED状態を確認してください。同じ状況が続く場合、サービス提供元が指定するお問い合わせ先に連絡しONUを交換してください。

通電後、LINE LEDが点灯しません。

PONが接続されていません。POWER LEDが緑色で点灯しているかご確認ください。POWER LEDが点灯している状態でLINE LEDが点灯しない場合、サービス提供元が指定するお問い合わせ先に連絡し、接続を確認してください。回線認証が成功した場合、LINE LEDは常に点灯します。

通電後、LAN LEDが点灯しません。

該当のLANポートにインターネットが接続されていません。このポートに接続されているデバイスが通電しているか、インターネットケーブルが繋がっているかご確認ください。

9 略語リスト

- DHCP – Dynamic Host Configuration Protocol, ダイナミックホストコンフィギュレーションプロトコル
- DMZ – Demilitarized Zone, 隔離区
- DNAT – Destination Network Address Translation, 宛先ネットワークアドレス変換
- DNS – DNS – Domain Name System, ドメインネームシステム
- DTIM – Delivery Traffic Indication Message, 配信トラフィック表示メッセージ
- ICMP – Internet Control Message Protocol, インターネット制御通知プロトコル
- IP – Internet Protocol, インターネットプロトコル
- LAN – Local Area Network, 構内通信網
- MAC – Medium Access Control, 媒体アクセス制御
- OMCI – ONT Management Control Interface, ONT管理制御インタフェース
- PON – Passive Optical Network, 受動光ネットワーク
- RTS – Request To Send, 発送請求
- ShortGI – Short Guard Interval, ショートガードインターバル
- SLAAC – Stateless Address Autoconfiguration, ステートレスアドレス自動設定
- SSID – Service Set Identifier, サービスセット識別子
- TCP – Transmission Control Protocol, 伝送制御プロトコル
- UDP – User Datagram Protocol, ユーザーデータグラムプロトコル
- UPnP – Universal Plug and Play, ユニバーサルプラグアンドプレイ
- VLAN – Virtual Local Area Network, 仮想ローカルエリアネットワーク
- WAN – Wide Area Network, ワイドエリアネットワーク
- WLAN – Wireless Local Area Network, 無線ローカルエリアネットワーク
- WMM – Wi-Fi MultiMedia, Wi-Fi マルチメディア
- WPS – Wi-Fi Protected Setup, Wi-Fiプロテクトドセットアップ