

ZXHN F660T

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 © 2020 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-20121225134200-003

リリース日: 2020/12/22 (R1.2)

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	10
2.1	設定の準備作業	10
2.2	TCP/IP 設定	10
2.3	本製品のログイン	12
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	14
3.3	ユーザーインタフェース情報	15
4	ネットワーク設定	19
4.1	無線 LAN RF2.4G の設定	19
4.2	無線 LAN RF5G の設定	25
4.3	LAN の設定	31
5	セキュリティ設定	37
5.1	ファイアウォールの設定	37
5.2	IPV4 フィルターの設定	39
5.3	IPV6 フィルターの設定	40
5.4	MAC フィルタの設定	42
5.5	URL フィルタの設定	43
5.6	アクセス制御の設定	44
5.7	ALG スイッチの設定	45
6	アプリケーションの設定	46
6.1	DMZ の設定	46
6.2	UPnP の設定	47
6.3	UPnP ポートマッピングの確認	48
6.4	仮想ホストの設定	49
6.5	DNS サービスの設定	50
6.6	SNTP(時刻同期)設定	52
6.7	USB ストレージの容量確認	53
6.8	DMS の設定	53
6.9	FTP 設定	54
6.10	ポートトリガーの設定	56
6.11	ポートフォワーディングの設定(アプリケーションリスト)	58
6.12	ポートフォワーディングリストの設定	59
6.13	ホーム共有(samba)の設定	61
7	管理の設定	63
7.1	ユーザー管理の設定	63
7.2	システム管理	63

7.3 ログ管理の設定	64
7.4 診断メンテナンス.....	66
8 Q&A	69
8.1 Q&A	69
9 略語リスト.....	70

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

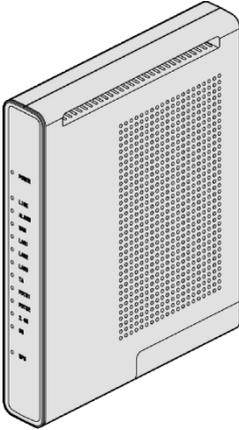
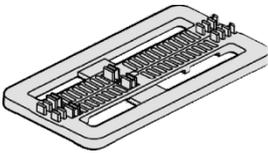
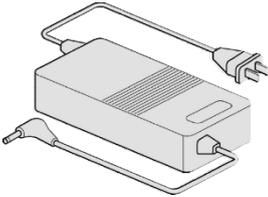
- ・直射日光を避け、本製品を通気性の良い場所に設置してください。
- ・本製品を乾燥している場所に設置し、熱源、水回りの近くへの設置は避けてください。
- ・本製品の上にはものを置かないでください。圧力による破損の恐れがあります。
- ・熱源、水周りの近くに設置しないでください。
- ・本製品設置時は電気製品・AV・OA 機器などの磁気を帯びている場所や電磁波が発生している場所(電子レンジ、スピーカ、テレビ、ラジオ、蛍光灯、電気こたつ、インバータエアコン、電磁調理器など)を避けてください。

本製品についてのお願い

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

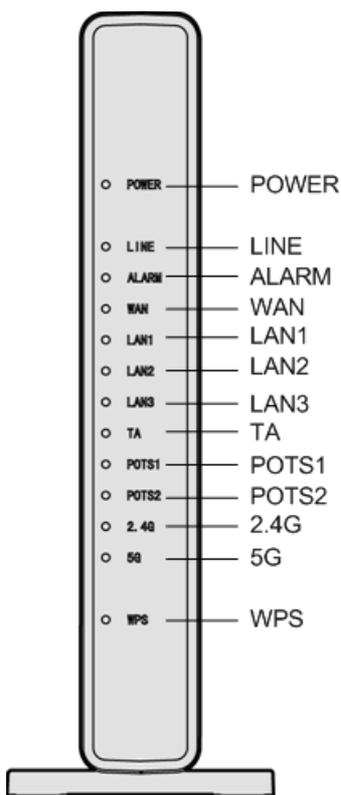
下記の部品が同梱されていることをご確認ください。

名前	数量	図
ZXHN F660T 本体	1 台	
ZXHN F660T 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 F660T 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 F660T 背面ポートとボタン

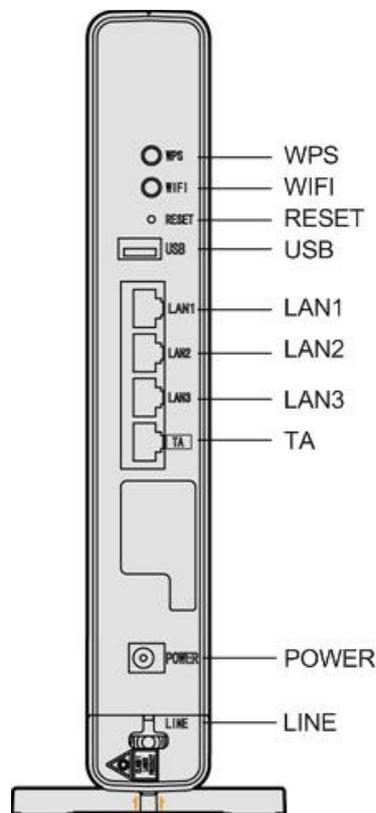


表 1-2 裏面ポートとボタンの説明

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)

※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%

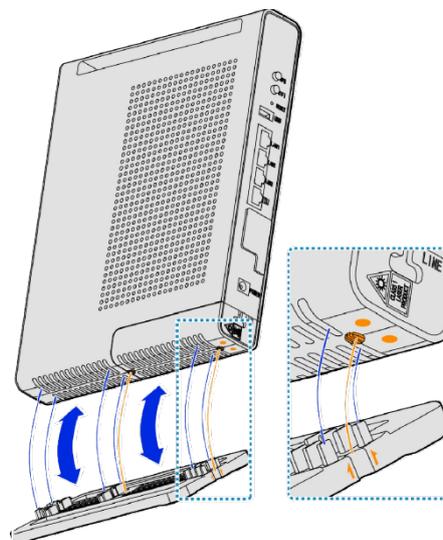
1.7 スタンドとファイバーカバーの取り付け

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：

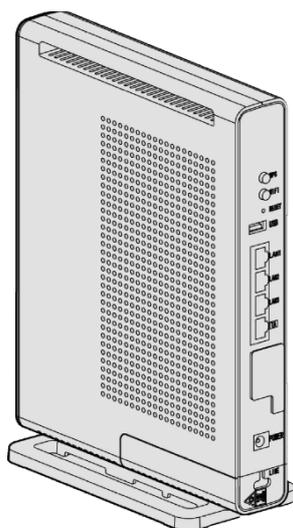
1. スタンドの矢印側を裏面(各ポートが入っている方向)に合わせ、散熱口に差し込みます。(図 1-3)

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

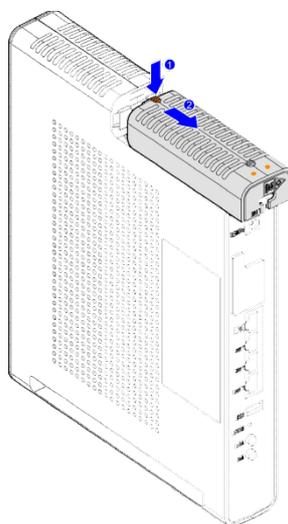


ファイバーカバーの取り付け

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。

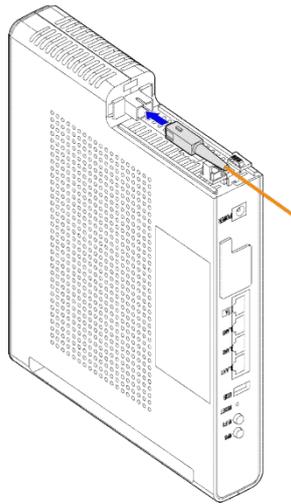
1.外に押しながら外側にファイバーカバーをスライドさせます。(図 1-

5) 図 1-5 ファイバーカバーの取り外し



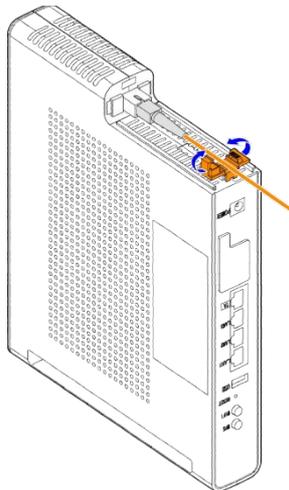
2.ファイバー末端部分をコネクタ端子に差し込みます。(図 1-6)

図 1-6 ファイバー端子の差し込み



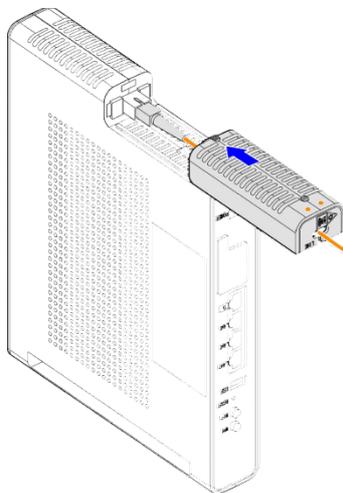
3.ファイバーを固定します。(図 1-7)

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

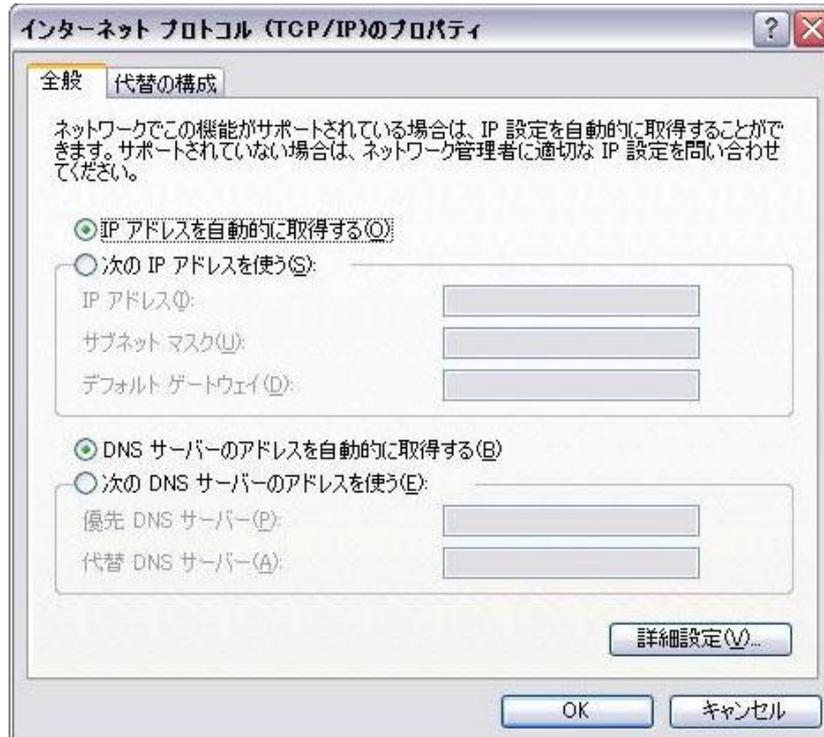
本製品のデフォルトネットワーク設定は以下の通りです。

- ・ 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:

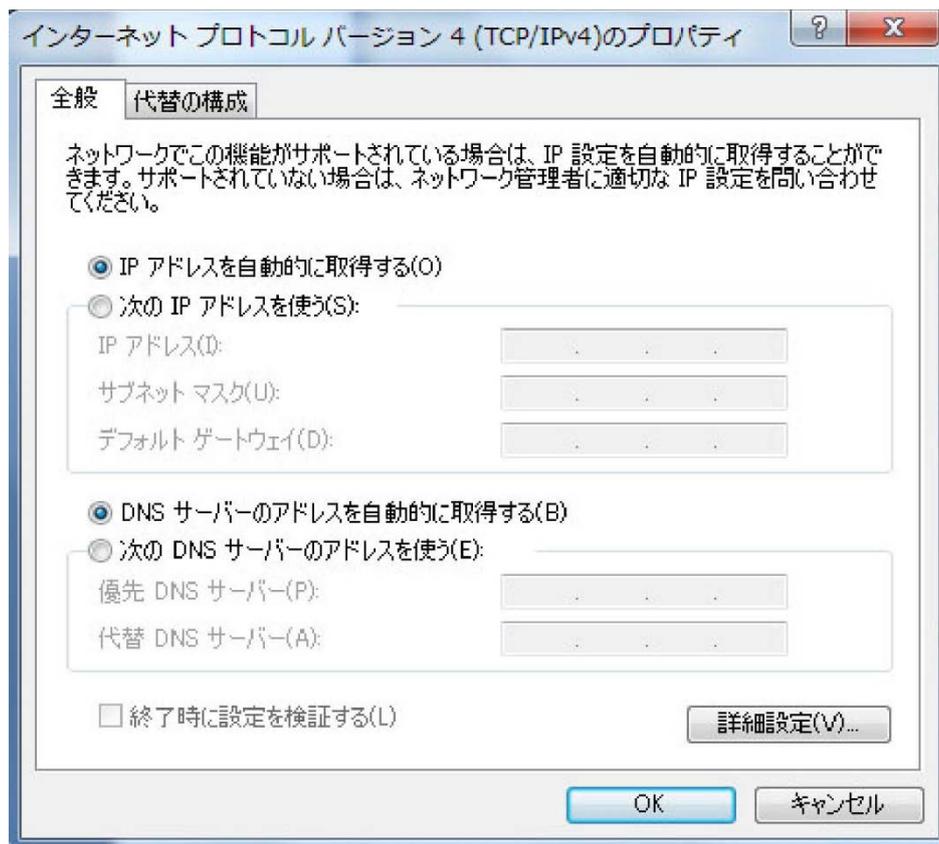
本製品のデフォルトネットワーク設定は以下の通りです。

- ・ 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

ステータス	ステータス>>デバイス情報	ENGLISH ログアウト
デバイス情報	デバイスモデル	F660T
ネットワークインタフェース情報	デバイスのシリアル番号	11190001
ユーザインタフェース情報	ハードウェアバージョン	V1.0
ネットワーク	ソフトウェアのバージョン	V1.0.0P16N4
セキュリティ	ブートルoaderのバージョン	V1.2.0T2
アプリケーション	PONシステムのシリアル番号	5A54454711190001
管理		

©2012-2020 ZTE Corporation. All rights reserved.

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

ステータス	ステータス>>デバイス情報	ENGLISH ログアウト
デバイス情報	デバイスモデル	F660T
ネットワークインタフェース情報	デバイスのシリアル番号	11190001
ユーザインタフェース情報	ハードウェアバージョン	V1.0
ネットワーク	ソフトウェアのバージョン	V1.0.0P16N4
セキュリティ	ブートルoaderのバージョン	V1.2.0T2
アプリケーション	PONシステムのシリアル番号	5A54454711190001
管理		

©2012-2020 ZTE Corporation. All rights reserved.

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	モード	IP		
ネットワークインタフェース情報	接続名	omci1_dhcp		
WAN接続情報	IPプロトコルのバージョン	IPv4/v6		
PON接続情報	NAT	有効		
ユーザインタフェース情報	IPv4アドレス	198.51.100.100/255.255.255.0		
ネットワーク	IPv4 DNS	203.0.113.33/203.0.113.49/0.0.0.0		
セキュリティ	IPv4ゲートウェイ	198.51.100.1		
アプリケーション	IPv4接続ステータス	接続中		
管理	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

PONの状態		認証完了
光モジュールの入力電力(dBm)	-15.62	
光モジュールの出力パワー(dBm)	3.32	
光モジュールの電源電圧(V)	3.293	
光送信バイアス電流(A)	0.011716	
光モジュールの動作温度(°C)	35.835	

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		
セキュリティー		
アプリケーション		
管理		

ポート名	LAN1
受信したデータ量(byte)	398534
受信したパケットの総数	4192
マルチキャストパケットの受信数	315
ブロードキャストパケットの受信数	95
送信したデータ量(byte)	1904842
送信されたパケットの総数	4282
マルチキャストパケットの送信数	4
ブロードキャストパケットの送信数	19

ポート名	LAN2
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	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>>ユーザーインタフェース情報>>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フェース情報			
ユーザー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			

無線の状態	有効
チャンネル	11

SSID1の状態	有効
SSID1名	F660T-SSID1
認証方法	WPA/WPA2-PSK
暗号化	TKIP+AES
MACアドレス	12:cc:bb:dd:00:01
受信パケット/バイト数	0/0
送信パケット/バイト数	0/0
受信エラー/パケット数	0
送信エラー/パケット数	0
受信パケットの廃棄数	0
送信パケットの廃棄数	55

SSID2の状態	無効
----------	----

SSID3の状態	無効
----------	----

SSID4の状態	無効
----------	----

更新

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>ユーザーインタフェース情報>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>>ユーザインタフェース情報>>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			

無線の状態	有効
チャンネル	N/A

SSID5の状態	有効
SSID5名	F660T-SSID5
認証方法	WPA/WPA2-PSK
暗号化	TKIP+AES
MACアドレス	00:00:00:00:00:00
受信パケット/バイト数	0/0
送信パケット/バイト数	0/0
受信エラーパケット数	0
送信エラーパケット数	0
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
----------	----

更新

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>ユーザーインタフェース情報>USB インタフェース情報を選択すると、USB インタフェース情報画面に進み、USB インタフェー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>>ユーザインタフェース情報>>USB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			

ポート番号	1
装置名	TransMemory
デバイスの種類	USB Mass Storage
デバイスID	0930_6544
デバイス速度	高速
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

更新

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

ステータス	ネットワーク>>無線LAN RF2.4G>>基本設定	ENGLISH ログアウト
ネットワーク		
無線LAN RF2.4G		
基本設定		
SSID設定		
セキュリティ設定		
アクセス制御リスト		
接続中の機器		
WPS		
無線LAN RF5G		
LAN		
セキュリティ		
アプリケーション		
管理		

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
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。
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)
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。
無線チャンネル	国コードから適当な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 を有効にする	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

ステータス	ネットワーク>>無線LAN RF2.4G>>セキュリティ設定	ENGLISH ログアウト
ネットワーク		
無線LAN RF2.4G		
基本設定		
SSID設定		
セキュリティ設定	SSIDを選択 <input type="text" value="SSID1"/>	
アクセス制御リスト	認証方法 <input type="text" value="WPA/WPA2-PSK"/>	
接続中の機器	WPA事前共有鍵 <input type="text" value="....."/> <input type="checkbox"/> (8~63文字)	
WPS	WPA暗号化アルゴリズム <input type="text" value="TKIP+AES"/>	
無線LAN RF5G		
LAN		
セキュリティー		
アプリケーション		
管理		

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
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。

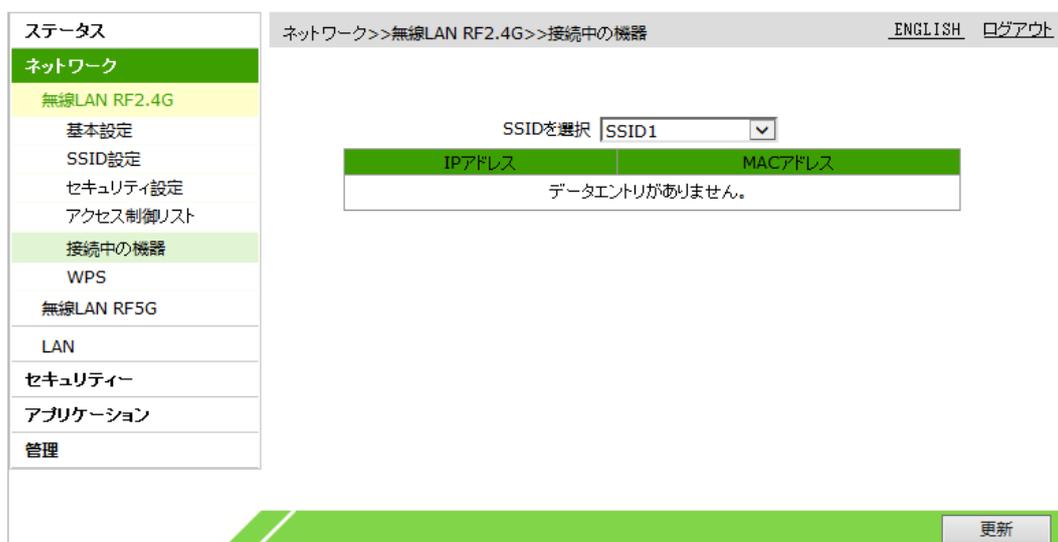
3.(オプション)SSID の後に表示される  アイコンをクリックすると設定データを削除できます。

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。
	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。

4.2 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

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
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)
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。
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。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 を有効にする	ショートガードインターバル (Short Guard Interval) を有効にします。
ビーコン間隔	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

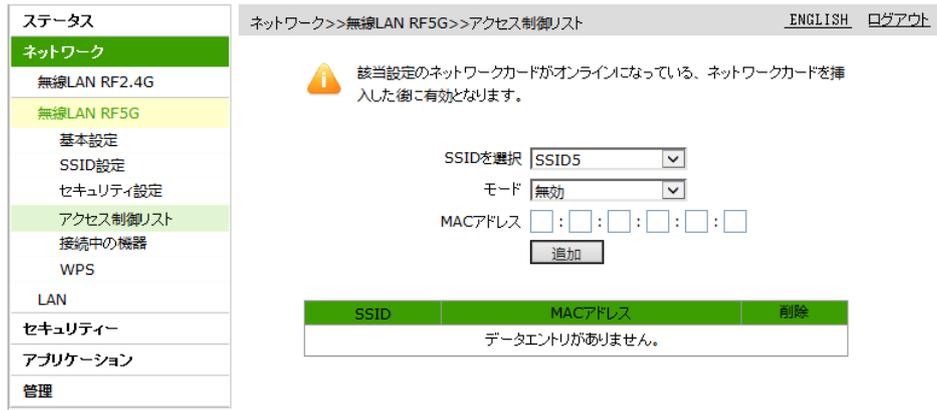
2.認証方式を設定して、設定ボタンをクリックします。
SSID がサポートしている認証方式は Open System(オープンシステム)、Shared Key(共有鍵方式)、WPA-PSK、WPA2-PSK、WPA/WPA2-PSK の 5 種類です。

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
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。

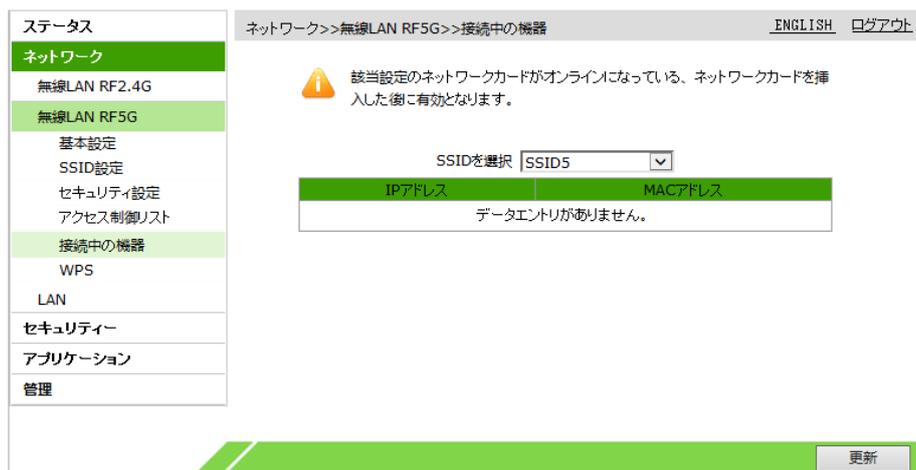
3.(オプション)SSID の後に表示される  アイコンをクリックすると設定データを削除できます。

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。

	<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。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>
--	--

4.3 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

<p>ステータス</p> <p>ネットワーク</p> <p>無線LAN RF2.4G</p> <p>無線LAN RF5G</p> <p>LAN</p> <p>DHCP固定アドレス割当</p> <p>ダイナミックアドレス管理 (IPv4)</p> <p>ダイナミックアドレス管理 (IPv6)</p> <p>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)</p> <p>ルータ広告(IPv6)</p> <p>セキュリティ</p> <p>アプリケーション</p> <p>管理</p>	<p>ネットワーク>>LAN>>DHCP固定アドレス割当 ENGLISH ログアウト</p> <p>IPアドレス <input type="text"/></p> <p>MACアドレス <input type="text"/> : <input type="text"/></p> <p style="text-align: center;"><input type="button" value="追加"/></p> <table border="1" style="width: 100%; text-align: center;"> <thead> <tr style="background-color: #4CAF50; color: white;"> <th style="width: 25%;">IPアドレス</th> <th style="width: 25%;">MACアドレス</th> <th style="width: 25%;">変更</th> <th style="width: 25%;">削除</th> </tr> </thead> <tbody> <tr> <td colspan="4">データエントリがありません。</td> </tr> </tbody> </table>	IPアドレス	MACアドレス	変更	削除	データエントリがありません。			
IPアドレス	MACアドレス	変更	削除						
データエントリがありません。									

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。

※当面は 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。

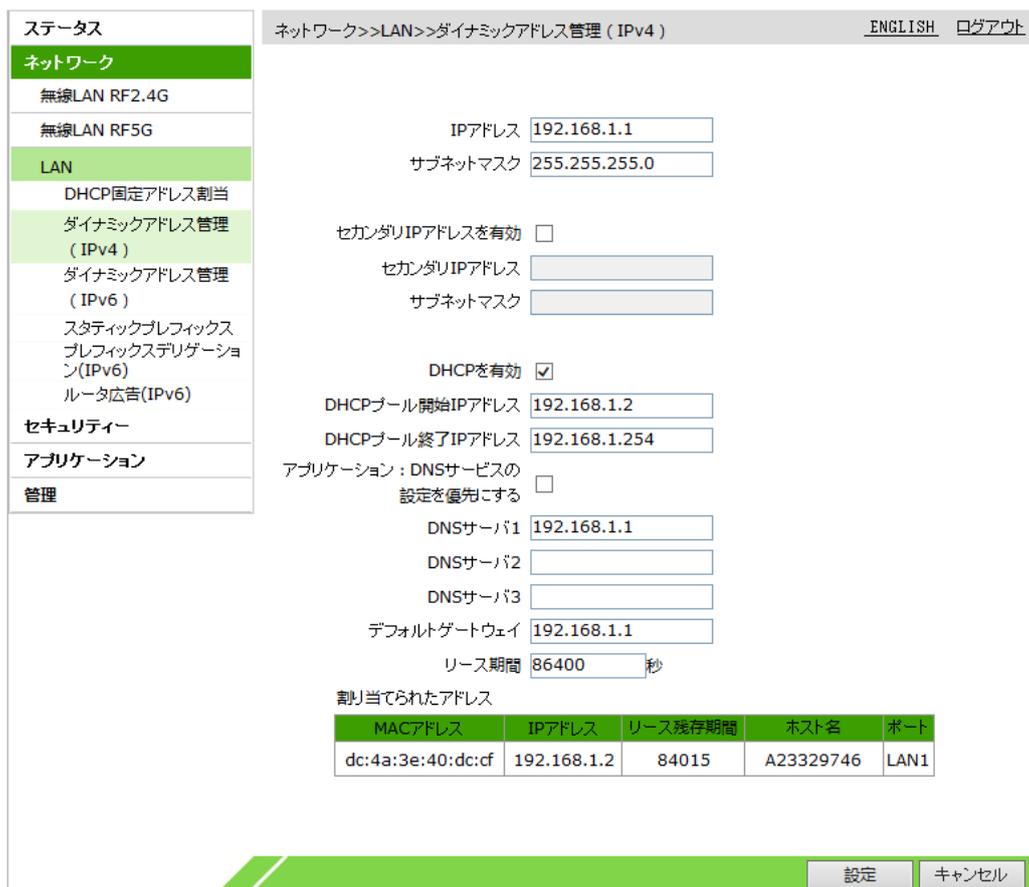
4.(オプション)アドレス内容の後に表示される  アイコンをクリックすると設定データを削除できます。

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。(図 4-14)

図 4-14 ダイナミックアドレス管理(IPv4)画面



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)	
ルータ広告(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ブール開始IPアドレス

DHCPブール終了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サーバ1

DNSサーバ2

DNSサーバ3

デフォルトゲートウェイ

リース期間 秒

割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
dc:4a:3e:40:dc:cf	192.168.1.2	84015	A23329746	LAN1

3. 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。
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。(図 4-15)

図 4-15 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。		

- 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 4-16 スタティックプレフィックス (IPv6) 画面

ネットワーク>>LAN>>スタティックプレフィックス

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。

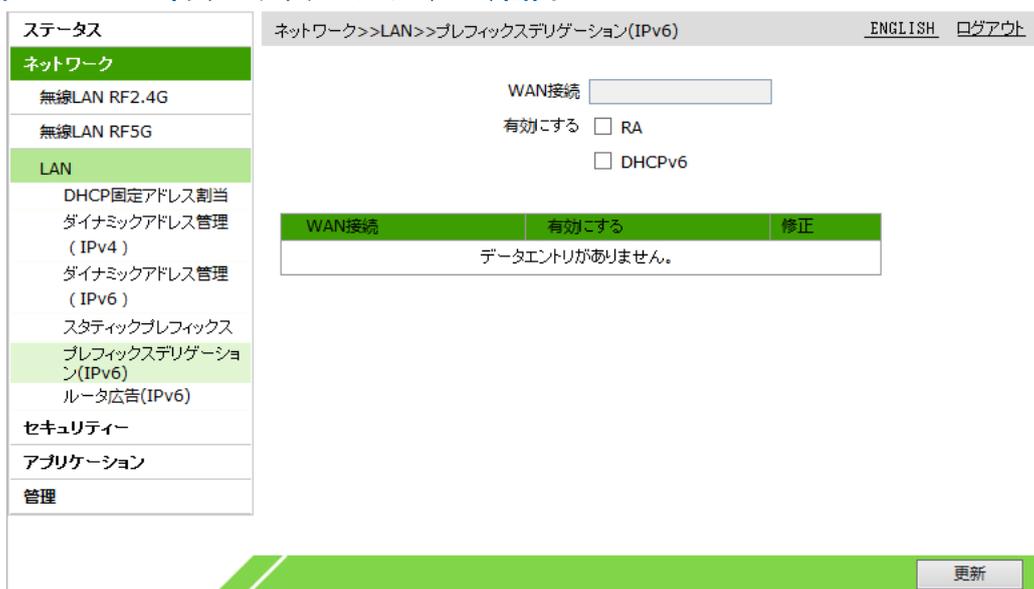
4.(オプション)アドレス内容の後に表示される  アイコンをクリックすると設定データを削除できます。

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 4-17 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 4-18 プレフィックスデリゲーション(IPv6)修正画面

ステータス	ネットワーク>>LAN>>プレフィックスデリゲーション(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			

WAN接続	omci1_dhcp		
有効にする	<input checked="" type="checkbox"/> RA		
	<input checked="" type="checkbox"/> DHCPv6		
	<input type="button" value="変更"/> <input type="button" value="キャンセル"/>		

WAN接続	有効にする	修正
omci1_dhcp	RA/DHCPv6	

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 パケットを返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 4-19 ルータ広告(IPv6)画面

ステータス	ネットワーク>>LAN>>ルータ広告(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			

最小待ち時間	198	秒(3 ~ 1350)
最大待ち時間	600	秒(4 ~ 1800)
Mフラグ	<input type="checkbox"/>	
Oフラグ	<input checked="" type="checkbox"/>	

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>

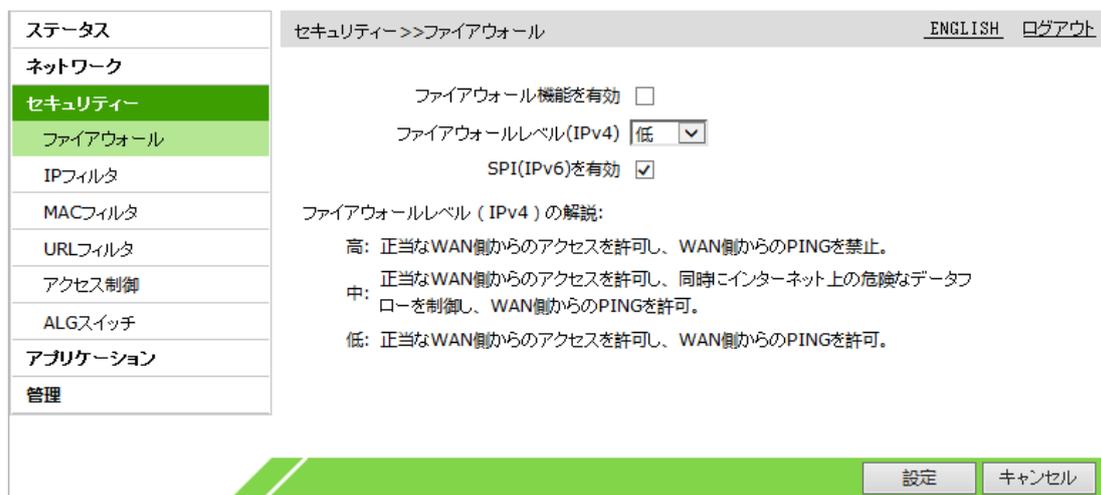
5 セキュリティ設定

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パフア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。

<p>ファイアウォールレベル (IPv4)</p>	<p>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。</p>
<p>SPI(IPv6)を有効にする</p>	<p>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。</p>

5.2 IPV4 フィルターの設定

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、IPV4 フィルタ画面に進みます。

(図 5-2)

図 5-2 IPV4 フィルタの設定画面

2. IPV4 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。IPV4 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。 TCP(デフォルト) UDP TCP AND UDP ICMP ANY
名前	該当 IP フィルターする項目の名称。

パラメータ	説明
(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。着信インタフェースが LAN、発信インタ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。着信インタフェースがブロードバンド接続、発信インタフェースが 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 IPV6 フィルターの設定

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 P 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 > Ipv6 フィルタと、**IPV6 フィルタ**画面に進みます。(図 5-3)

図 5-3 IPV6 フィルタの設定画面

2. IPV6 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。

IPV6 フィルタのパラメータについては下の表を参考してください。

パラメータ	説明
有効にする	オン：IPフィルタを有効にします。 オフ：IPフィルタを無効にします。
名前	IPフィルタの名前を設定します。 文字数 1 ～ 32
モード	許可する：フィルタエントリに合致したIPv6パケットを通信させます。 拒否する：フィルタエントリに合致したIPv6パケットを廃棄します。
優先度	フィルタの優先度を設定します。1 ～ 20まで選択可能。 ※フィルタエントリはマックス20個設定できます。 ※エントリが複数ある場合、優先度の数字の小さいエントリから優先します。 ※優先度が重なった場合、新しく設定したルールが適用され、以前設定されていたルールの優先度数字が1つ大きくなります。

プロトコル	<p>パケットをフィルタリングする対象のプロトコルを選択します。</p> <p>TCP : TCPをフィルタリングします。</p> <p>UDP : UDPをフィルタリングします。</p> <p>TCPとUDP : TCPとUDPをフィルタリングします。</p> <p>ICMPv6 : ICMPv6をフィルタリングします。</p> <p>any : IPv6パケットすべてを処理します。IPv6パケットであれば、TCP、UDP、ICMPv6も対象とします。</p> <p>ICMPv6が選ばれた場合、次のパラメータもサポートします。</p> <p>any : ICMPv6プロトコルがフィルタ対象を意味します。</p> <p>コード指定 : 「TYPE」と「CODE」にそれぞれ数値を入力します。</p>
送信元ポート範囲 宛先ポート範囲	<p>送信元ポート範囲 : フィルタ対象とするIPv6パケットの送信元ポート番号を設定します。</p> <p>宛先ポート範囲 : フィルタ対象とするIPv6パケットの宛先ポート番号を設定します。</p> <p>anyをチェック入れると、すべてのポートがフィルタ対象を意味します。</p>
送信元IPアドレス範囲 宛先IPアドレス範囲	<p>送信元IPアドレス範囲 : フィルタ対象とするIPv6パケットの送信元IPアドレスを設定します。</p> <p>宛先IPアドレス範囲 : フィルタ対象とするIPv6パケットの宛先IPアドレスを設定します。</p> <p>anyをチェック入れると、すべてのアドレスがフィルタ対象を意味します。</p>
着信インタフェース 発信インタフェース	<p>データトラフィックの方向性を指定します。対象インターフェースのinとoutを同じにすることはできません。</p> <p>ANY : WAN側/LAN側に適用します。</p> <p>LAN : LAN側に適用します。</p>

- (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。
- (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 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 5-4)

図 5-4 MAC フィルタの設定画面

ステータス	セキュリティ>>MACフィルタ	ENGLISH ログアウト												
ネットワーク	<div style="text-align: center;">  <p>1. 許可モードを選択した場合、最初に許可するMACアドレスを追加してください。</p> <p>2. 動作モードは変更後すぐに有効になります。</p> </div> <div style="margin-top: 20px;"> 有効にする <input type="checkbox"/> </div> <div style="margin-top: 5px;"> モード <input type="text" value="拒否"/> </div> <div style="margin-top: 10px;"> タイプ <input type="text" value="ブリッジ"/> </div> <div style="margin-top: 5px;"> プロトコル <input type="text" value="IPプロトコル"/> </div> <div style="margin-top: 5px;"> 送信元MACアドレス <input type="text" value=": : : : :"/> </div> <div style="margin-top: 5px;"> 宛先MACアドレス <input type="text" value=": : : : :"/> </div> <div style="margin-top: 5px; text-align: center;"> <input type="button" value="追加"/> </div> <div style="margin-top: 10px;"> <table border="1" style="width: 100%; text-align: center;"> <tr> <td style="background-color: #008000; color: white;">タイプ</td> <td style="background-color: #008000; color: white;">プロトコル</td> <td style="background-color: #008000; color: white;">送信元MACアドレス</td> <td style="background-color: #008000; color: white;">宛先MACアドレス</td> <td style="background-color: #008000; color: white;">変更</td> <td style="background-color: #008000; color: white;">削除</td> </tr> <tr> <td colspan="6">データエントリがありません。</td> </tr> </table> </div>		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。					
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。														
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														

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	以下 3 つのタイプをサポートしています。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	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。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。

5.5 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せん。(図 5-5)

図 5-5 URL フィルタの設定画面

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	<ul style="list-style-type: none"> 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。

5.6 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 5-6)

図 5-6 アクセス制御の設定画面

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 IP アドレス/(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 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。

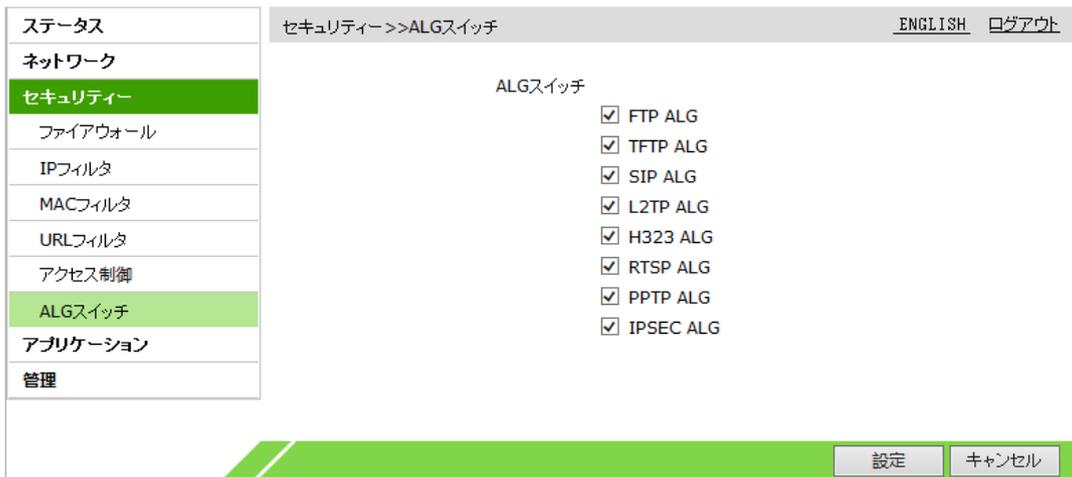
4.(オプション)フィルタ内容の後に表示される  アイコンをクリックすると設定データを削除できます。

5.7 ALG スイッチの設定

ALG 設定スイッチのオンで、ZXHN F660A は 4 つの情報パケット中のプライベートネットワークアドレスをパブリックアドレスに変更することができます。外部ネットワークはプライベート IP アドレスを知ることができない。これにより安全性を向上させる。

1. WEB 画面の左側メニューでセキュリティ > ALG スイッチを選択すると、ALG スイッチ設定画面に進みます。

図 5-7 ALG スイッチ設定画面



2. 起動するプロトコル ALG スイッチをチェック入れて、プロトコルの ALG スイッチをオンにて、設定をクリックします。

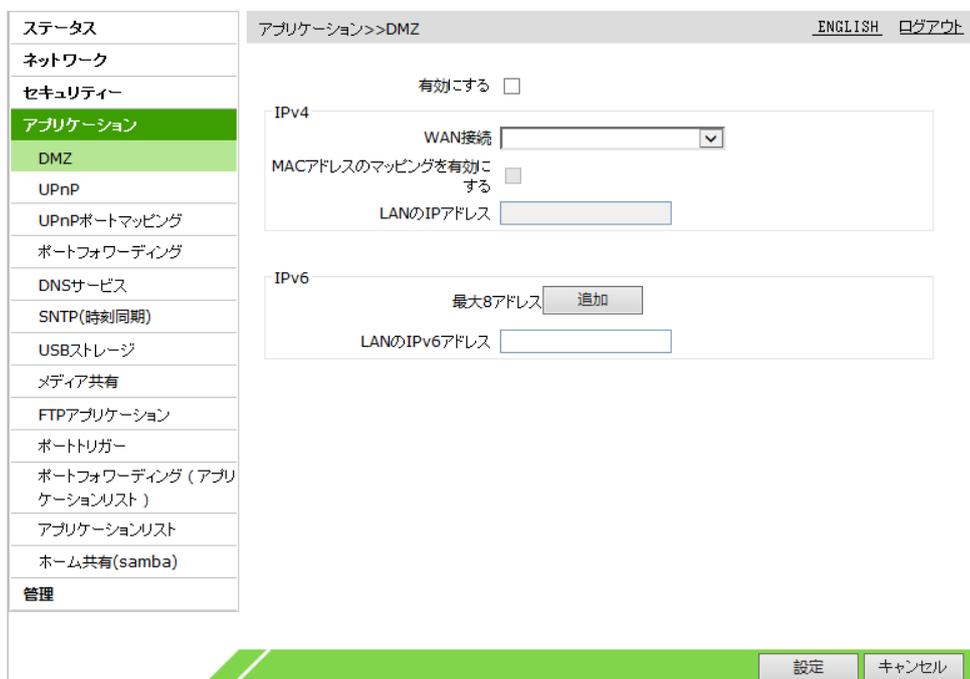
6 アプリケーションの設定

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



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

ステータス	アプリケーション>>UPnP	ENGLISH ログアウト
ネットワーク	UPnPを有効 <input checked="" type="checkbox"/>	
セキュリティ	WAN接続 <input type="text"/>	
アプリケーション	広報の周期(分) <input type="text" value="30"/>	
DMZ	有効期間 (ホップ数) <input type="text" value="4"/>	
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		
		設定 キャンセル

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

ステータス	アプリケーション>>UPnPポートマッピング					ENGLISH	ログアウト
ネットワーク	UPnPポートマッピングテーブル						
セキュリティ	アクティベーション	プロトコル	入力ポート	出力ポート	IPアドレス	削除	
アプリケーション	✓	TCP	6360	6360	10.37.66.197		
DMZ	✓	UDP	6360	6360	10.37.66.197		
UPnP							
UPnPポートマッピング							
仮想ホスト							
DNSサービス							
SNTP(時刻同期)							
USBストレージ							
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							
ポートフォワーディングリスト							
管理							
							更新

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。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。

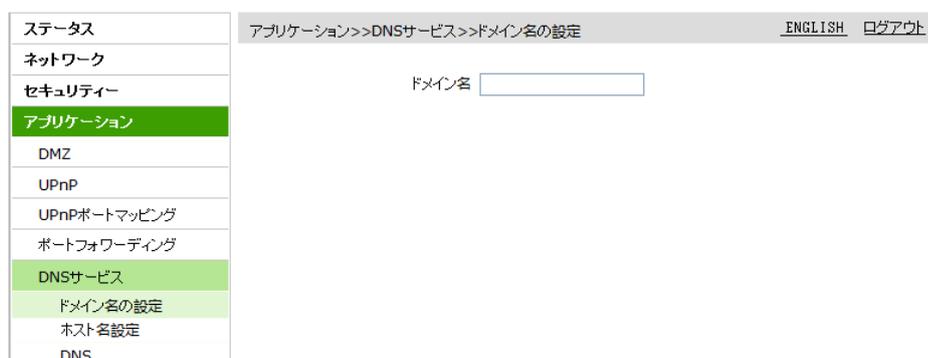
- ・ドメイン名の設定
- ・ホスト名の設定
- ・DNS サーバの設定

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

ホスト名	IPアドレス	変更	削除
A23329746	192.168.1.2		

- 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	IPv4 DNSサーバー 1 <input type="text"/>		
セキュリティ	IPv4 DNSサーバー 2 <input type="text"/>		
アプリケーション	IPv6 DNSサーバー 1 <input type="text"/>		
DMZ	IPv6 DNSサーバー 2 <input type="text"/>		
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			
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

ステータス	アプリケーション>>SNTP(時刻同期)	ENGLISH	ログアウト
ネットワーク	現在の日時 2000-01-01 01:20:24		
セキュリティ	タイムゾーン [(UTC+09:00) 大阪、札幌、東京]		
アプリケーション	プライマリSNTPサーバアドレス <input type="text"/>		
DMZ	セカンダリSNTPサーバアドレス <input type="text"/>		
UPnP	同期間隔 86400 秒		
UPnPポートマッピング	DSCP値 <input type="text"/> (0 ~ 63)		
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			
		設定	キャンセル

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。

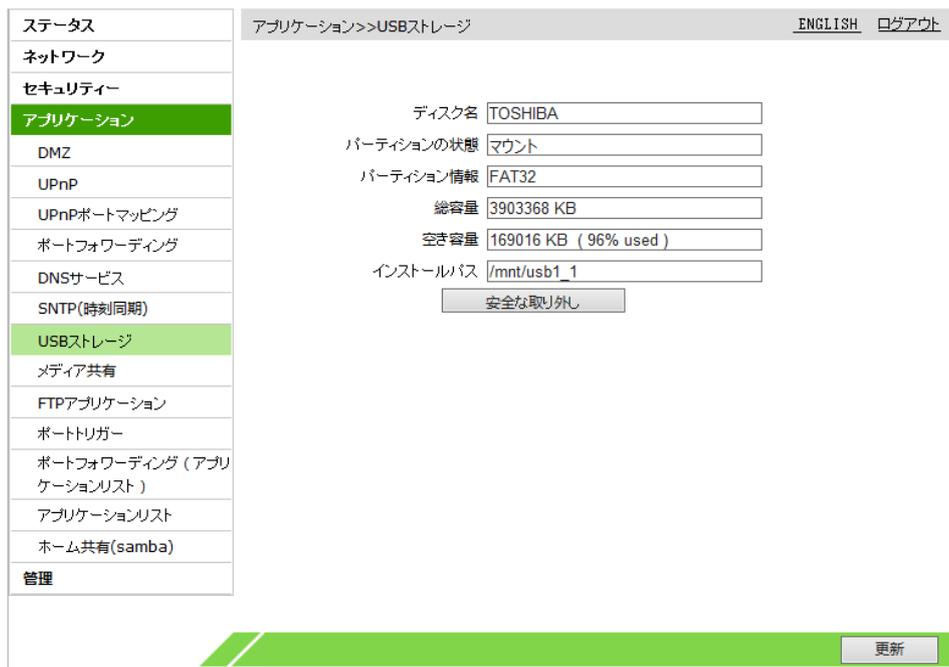
パラメータ	説明
タイムゾーン	本製品所在の場所
プライマリ SNTP サーバアドレス	プライマリ SNTP サーバのアドレス
セカンダリ SNTP サーバアドレス	セカンダリ SNTP サーバのアドレス
同期間隔	本製品が NTP サーバにリクエストを送信する間隔。設定範囲： 3600～86400 秒。デフォルトは 86400 秒。
DSCP	リクエストメッセージの DSCP 優先順位設定

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。

1. 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 DMS の設定

DMS の設定で ZXHN F660A の DMS サービスをカスタマイズ可能です。DMS とは DLNA の仕様に沿ったメディアサーバーです。USB 外部デバイスに保存されているビデオ、音楽、写真をホームネットワークの他の UPnP AV デバイスの再生するに提供します。

1. WEB 画面の左側メニューで**アプリケーション > メディア共有** , を選択すると DMS 設定画面に進みます。

図 6-10 USB ストレージ画面

2. DMS 関連パラメータを設定し、設定ボタンをクリックします。

DMS のパラメータ説明については下の表を参照してください。

パラメータ	説明
DMSを有効にします	チェックボックスを選択してDMSを有効にします。
サーバ名	DMSサーバ名。
メディアソース 1/2/3/4	[参照]ボタンをクリックしてメディアソースへのパスを設定する。

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。

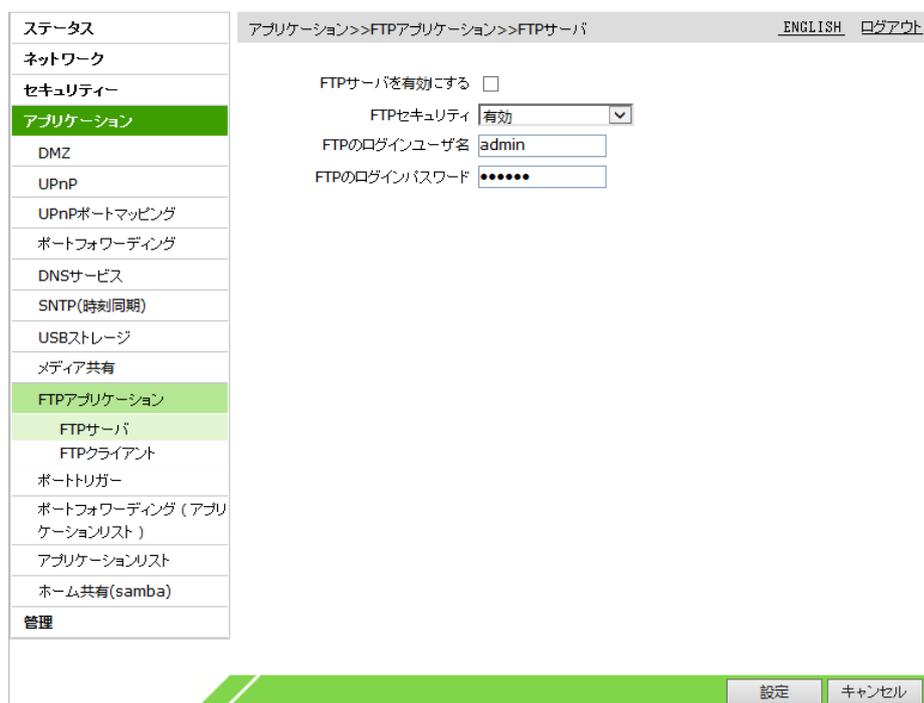
- FTP サーバ設定
- FTP クライアント設定

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 のログインユーザ名/FTP のログインパスワード	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、トリガーが必要なと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

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時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の設定(アプリケーションリスト)

ポートフォワーディングを設定すると、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出来ます。

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。

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**を選択すると、**ポートフォワーディング**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の設定画面



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。

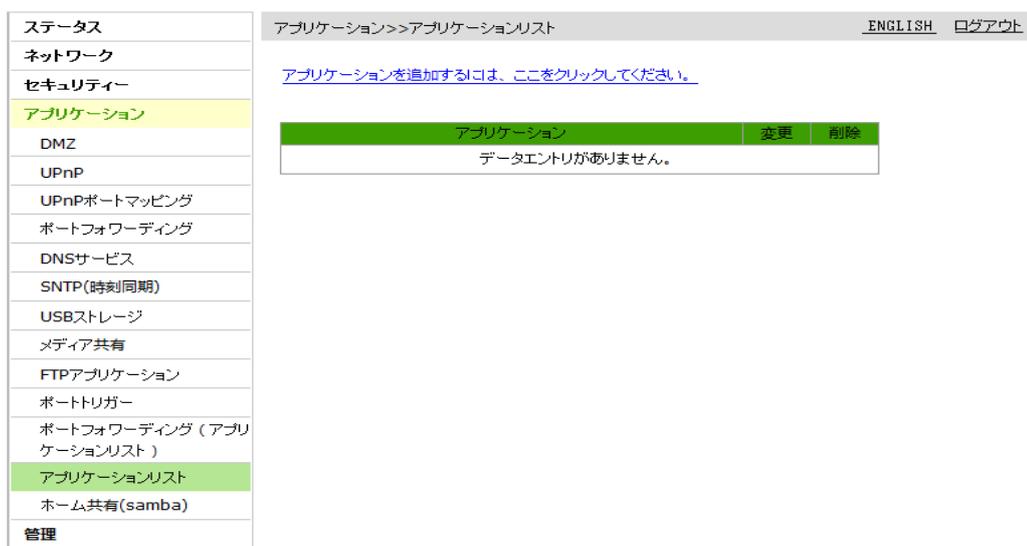
3.(オプション)アプリケーション内容の後に表示される  アイコンをクリックすると設定データを削除できます。

6.12 ポートフォワーディングリストの設定

ポートフォワーディング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認し、ポートフォワーディング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>ポートフォワーディングリスト**を選択すると、**ポートフォワーディングリスト設定画面**に進みます。(図 6-15)

図 6-15 ポートフォワーディングリストの設定画面



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 ポートフォワーディングリストの追加画面

ステータス	アプリケーション>>アプリケーションリスト	ENGLISH	ログアウト
ネットワーク	アプリケーション名 <input type="text" value="App1"/> (1 ~ 256)		
セキュリティ	<input type="button" value="保存"/>		
アプリケーション	プロトコル <input type="text" value="TCP"/>		
DMZ	(開始) WANポート <input type="text"/> (0 ~ 65535)		
UPnP	(終了) WANポート <input type="text"/> (0 ~ 65535)		
UPnPポートマッピング	(開始) マッピングポート <input type="text"/> (0 ~ 65535)		
ポートフォワーディング	(終了) マッピングポート <input type="text"/> (0 ~ 65535)		
DNSサービス	<input type="button" value="追加"/>		
SNTP(時刻同期)	プロトコル	(開始) WANポート	(終了) WANポート
USBストレージ	(開始) マッピングポート	(終了) マッピングポート	変更
メディア共有	データエントリがありません。		
FTPアプリケーション	削除		
ポートトリガー	<input type="button" value="戻る"/>		
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			

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 ポートフォワーディングリストの追加完了画面

ステータス	アプリケーション>>アプリケーションリスト	ENGLISH	ログアウト
ネットワーク	アプリケーション名 <input type="text" value="App1"/> (1 ~ 256)		
セキュリティ	<input type="button" value="変更"/>		
アプリケーション	プロトコル <input type="text" value="TCP"/>		
DMZ	(開始) WANポート <input type="text"/> (0 ~ 65535)		
UPnP	(終了) WANポート <input type="text"/> (0 ~ 65535)		
UPnPポートマッピング	(開始) マッピングポート <input type="text"/> (0 ~ 65535)		
ポートフォワーディング	(終了) マッピングポート <input type="text"/> (0 ~ 65535)		
DNSサービス	<input type="button" value="追加"/>		
SNTP(時刻同期)	プロトコル	(開始) WANポート	(終了) WANポート
USBストレージ	(開始) マッピングポート	(終了) マッピングポート	変更
メディア共有	データエントリがありません。		
FTPアプリケーション	削除		
ポートトリガー	<input type="button" value="戻る"/>		
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。

4.(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。

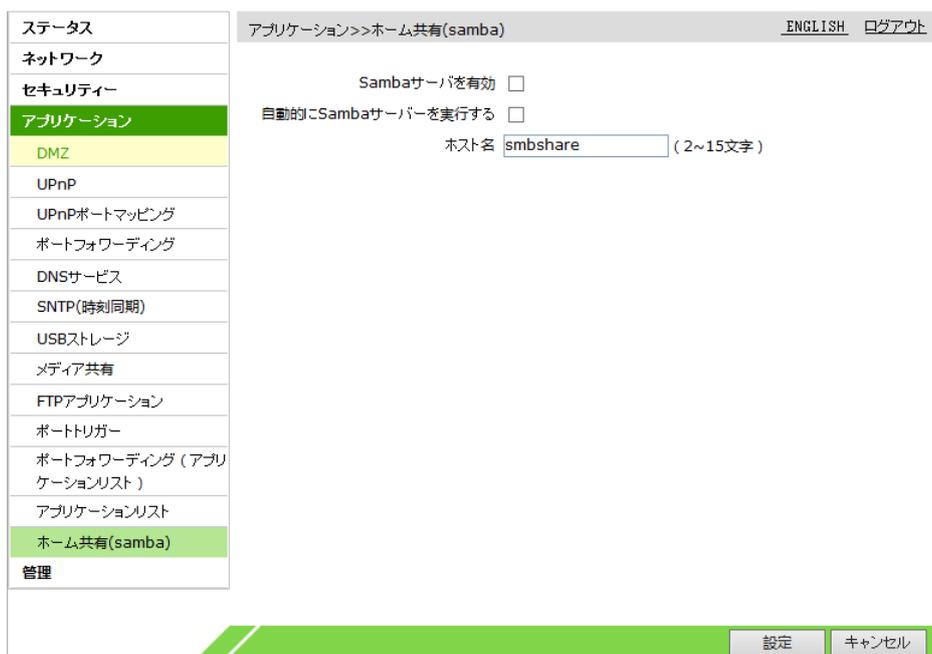
5.(オプション)アプリケーション内容の後に表示される  アイコンをクリックすると設定データを削除できます。

6.13 ホーム共有(samba)の設定

Samba は SMB を実装するために使用するソフトウェアです。ZXHN F660A の Samba サーバを有効にすると、Linux と Windows 情報の相互転送ができます。SMB プロトコルはローカルエリアネットワークで共有ファイル/プリンタのプロトコルとして見る事ができる、ネットワーク内部の他の Windows と Linux 機器にシステムファイル、印刷サービス、またはその他の情報を提供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 > Samba サービス**を選択すると、Samba サービス設定画面に進みます。

図 6-18 ホーム共有(samba)画面



2. 配置 Samba サーバの関連パラメータを設定して、設定をクリックします。

Samba サーバパラメータの説明は下の表を参照してください。

パラメータ	説明
Sambaサーバを有効にする	チェックを入れてSambaサーバ機能を有効にします, それ以外の場合は、Sambaサーバを停止します。この項目は、デフォルトで有効になっていません、そして「自動実行Sambaサーバ」オプションを使用して相互に排他的です。
Sambaサーバを自動実行する	この項目をチェック入れてから、在ONUのUSBポートにUSBストレージデバイス挿入する時、自動実行Sambaサーバ; USBストレージデバイスを抜いた後、Sambaサーバが自動停止します。デフォルトで有効になっていません、そして「Sambaサーバの有効」オプションを使用して相互に排他的です。
ホストネーム	Sambaサーバネーム

3. Samba サーバを有効にすると、LAN 側にて PC が“Samba サーバネーム”方式で Samba サーバにアクセスができます、例えば“smbshare”。

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

The screenshot shows a web interface for user management. On the left is a vertical menu with items: 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, 管理 (highlighted), ユーザ管理 (highlighted), システム管理, ログ管理, 診断メンテナンス. The main area is titled '管理>>ユーザ管理' and contains a form with the following fields: 'ユーザ名' (Username) with the value 'admin', '古いパスワード' (Old Password), '新しいパスワード' (New Password), and '新しいパスワードの確認' (Confirm New Password). At the bottom right of the form are two buttons: '設定' (Settings) and 'キャンセル' (Cancel). The top right of the interface has links for 'ENGLISH' and 'ログアウト'.

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。

- ・リモートアップグレード
- ・リセット

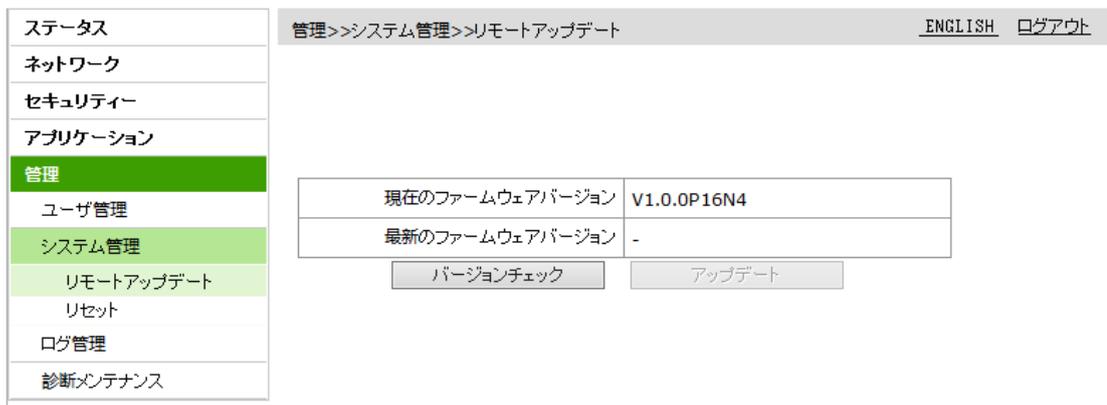
7.2.1 リモートアップグレードの設定

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、リモートアップグレードが利用できます。リモートアップグレードの完了後、ONU は再起動します。リモートアップグレード中は 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>リモートアップグレード**を選択すると、**リモートアップグレード**設定画面に進みます。(図 7-2)

図 7-2 システム管理の設定画面



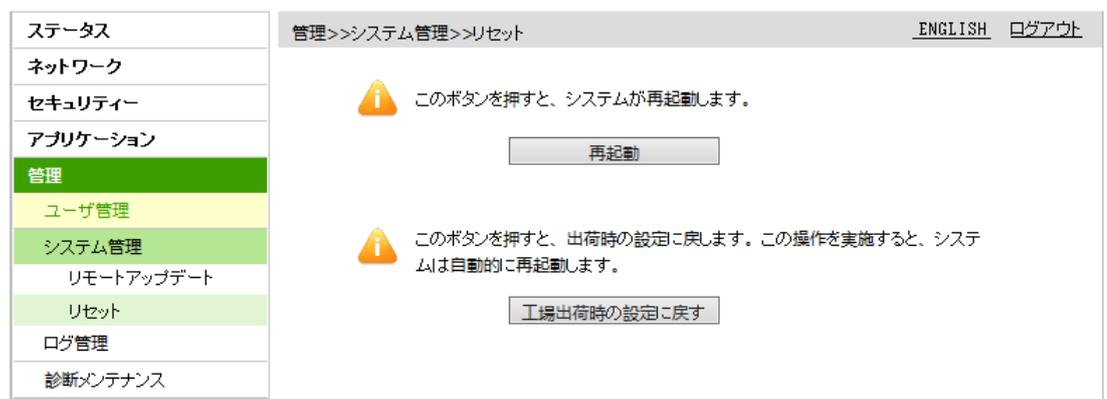
2.サーバー上に新しいバージョンがあるとき有効となります。

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。

1.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 リモートアップグレード画面



2.「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。

3.「工場出荷時の設定に戻す」ボタンをクリックすると、本製品が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。

1. 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、ログが定期的には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)ログをクリアする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>Ping 診断**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

The screenshot shows a web interface for configuring Ping diagnosis. On the left is a navigation menu with categories like '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', '管理', 'ユーザ管理', 'システム管理', 'ログ管理', '診断メンテナンス', 'ping診断', and 'traceroute診断'. The 'ping診断' option is selected. The main area displays the breadcrumb '管理>>診断メンテナンス>>ping診断' and 'ENGLISH ログアウト' links. Below the breadcrumb are two input fields: 'IPアドレスまたはホスト名' and '発信インターフェイス'. A large empty rectangular area is positioned below these fields. At the bottom right of the main area are two buttons: '設定' (Settings) and 'キャンセル' (Cancel).

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。
発信インターフェイス	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。
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 packets 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