

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-20150325134200-001

リリース日 : 2021/09/24 (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	8
2	設定の準備	12
2.1	設定の準備作業	12
2.2	PC 設定	12
2.3	本製品のログイン	16
3	デバイスの状態	18
3.1	デバイス情報	18
3.2	ネットワークインターフェイス情報	18
3.2.1	WAN 接続情報	18
3.2.2	PON 情報	19
3.3	ユーザインターフェイス情報	19
3.3.1	イーサネットインターフェイス情報	20
3.3.2	無線 LAN RF2.4G インターフェイス情報	21
3.3.3	無線 LAN RF5G インターフェイス情報	21
3.3.4	USB インターフェイス情報	22
4	ネットワークの設定	23
4.1	無線 LAN RF2.4G の設定	23
4.1.1	無線 LAN RF2.4G 基本パラメータの設定	23
4.1.2	SSID の設定	25
4.1.3	無線 LAN RF2.4G セキュリティ属性の設定	26
4.1.4	アクセス制御リストの設定	27
4.1.5	接続中の機器の確認	28
4.1.6	WPS 機能の設定	28
4.2	無線 LAN RF5G の設定	29
4.2.1	無線 LAN RF5G 基本パラメータの設定	29
4.2.2	SSID の設定	31
4.2.3	無線 LAN RF5G セキュリティ属性の設定	32
4.2.4	アクセス制御リストの設定	33
4.2.5	接続中の機器の確認	34
4.2.6	WPS 機能の設定	35
4.3	LAN の設定	36
4.3.1	静的アドレスの設定	36
4.3.2	動的 IPv4 アドレスの設定	37
4.3.3	動的 IPv6 アドレスの設定	39
4.3.4	スタティックプレフィックスの設定	40
4.3.5	プレフィックスデリゲーション方式の設定	40
4.3.6	RA サービスの設定	41
5	セキュリティの設定	43
5.1	ファイアウォールの設定	43
5.2	IPv4 フィルタの設定	44
5.3	IPv6 フィルタの設定	45
5.4	MAC フィルタの設定	47
5.5	URL フィルタの設定	49
5.6	アクセス制御の設定	49
5.7	ALG スイッチの設定	51

6	アプリケーションの設定	52
6.1	DMZ の設定	52
6.2	UPnP の設定	53
6.3	UPnP ポートマッピングの確認	54
6.4	仮想ホストの設定	54
6.5	DNS サービスの設定	56
6.5.1	ドメイン名の設定	56
6.5.2	ホスト名の設定	57
6.5.3	DNS サーバの設定	58
6.6	SNTP (時刻同期) の設定	59
6.7	USB ストレージの容量確認	60
6.8	DMS の設定	61
6.9	FTP の設定	62
6.9.1	FTP サーバ設定	62
6.9.2	FTP クライアントの設定	63
6.10	ポートトリガーの設定	64
6.11	ウェブホスティングの設定 (アプリケーションリスト)	65
6.12	アプリケーションリストの設定	66
6.13	ホーム共有 (samba) の設定	68
7	管理の設定	70
7.1	ユーザ管理の設定	70
7.2	システム管理	71
7.2.1	リモートアップデートの設定	71
7.2.2	リセット	72
7.3	ログ管理の設定	72
7.4	診断メンテナンス	73
7.4.1	Ping 診断の設定	73
7.4.2	Trace Route 診断の設定	74
	Q&A 76	
	略語リスト	77

1 製品概要

1.1 安全注意事項

注意事項

- ・ 同梱される電源アダプタ（ACアダプタ、電源コード）とLANケーブルをお使いください。
- ・ ACアダプタとその電源コードに傷を付れたり、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、すぐに本製品の電源コード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

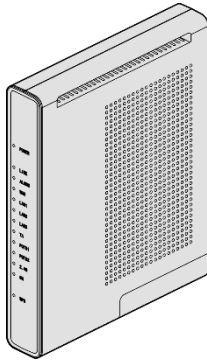
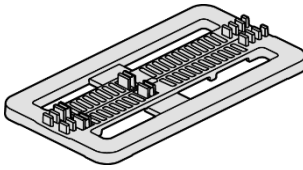
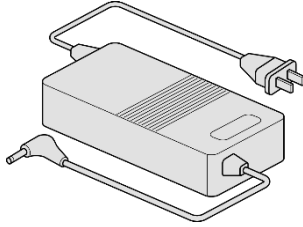
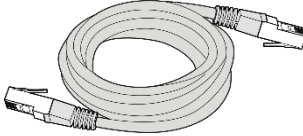

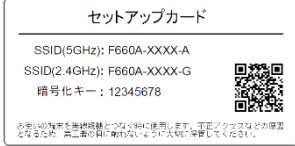
- ・ 直射日光を避け、本製品を通気性の良い場所に設置してください。
- ・ 本製品を乾燥している場所に設置し、熱源、水回りの近くへの設置は避けてください。
- ・ 本製品の上にはものを置かないでください。圧力による破損の恐れがあります。
- ・ 熱源、水周りの近くに設置しないでください。
- ・ 本製品設置時は電気製品・AV・OA機器などの磁気を帯びている場所や電磁波が発生している場所（電子レンジ、スピーカ、テレビ、ラジオ、蛍光灯、電気こたつ、インバータエアコン、電磁調理器など）を避けてください。

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個	
簡易ユーザガイド	1冊	
SSIDシール	1冊	 <p>セットアップカード</p> <p>SSID(5GHz): F660A-XXXX-A SSID(2.4GHz): F660A-XXXX-G 暗号化キー: 12345678</p> <p><small>お買い上げの保証書に無線LANの保証書が同梱されています。保証書のダウンロードは保証書の裏面に記載されているURLからダウンロードしてください。</small></p>

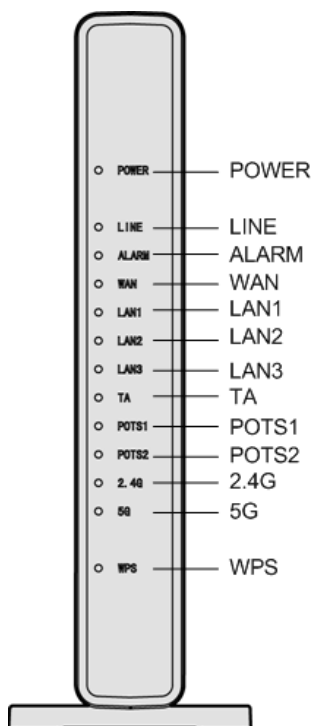


※設置を始める前に、構成品がすべてそろっていることを確認してください。

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

下図のように表示。



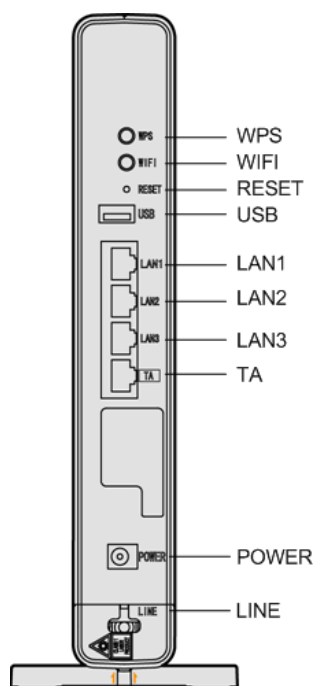
正面LED 表示説明は以下となります。

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、 TA	緑	消灯：LANポートに設備が接続されていません。 点灯：LANポートに設備が接続されていま

LED表示	色	説明
		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

ZXHN F660A背面ポートとボタン。



裏面ポートとボタンの説明は以下の表のように表示。

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機能の有効/無効を行います。
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設定情報は失われません。5秒以上長押しした場合、工場出荷設定に戻したのちに、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

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

ポート数	TA × 1
規格	IEEE802.3 (10BASE-T)、IEEE802.3u (100BASE-TX)、IEEE802.3ab (1000BASE-T)
全二重/半二重	自動検出
MDI/MDI-X	自動検出
物理インターフェイス	RJ-45
無線LANインターフェイス	
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(5.15-5.725 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アドレスフィルタリング。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 5.6G 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 [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アドレスフィルタリング。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

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%

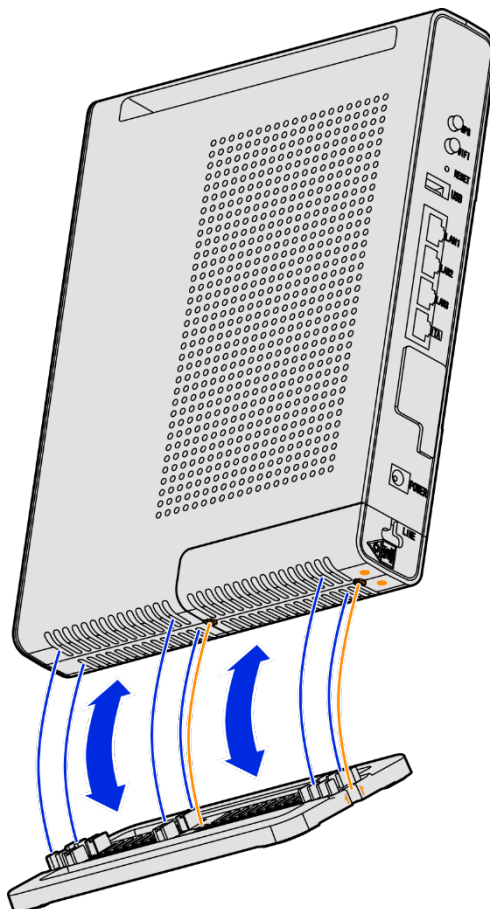
1.7 スタンドとファイバーカバーの取り付け

スタンドの取り付け

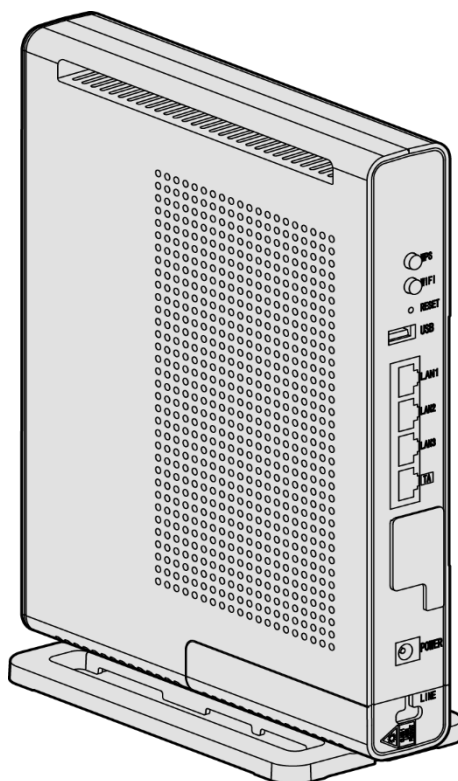
本製品はスタンドが付属しています。ご使用前にスタンドを取り付けて縦置きにしてください。

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。



2. 取り付けが正常に完了した場合、下図のようになります。

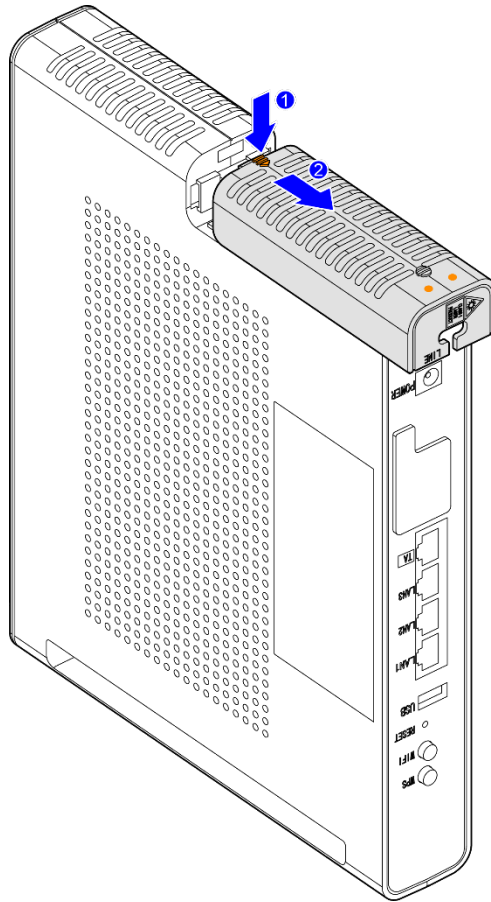


ファイバーカバーの取り付け

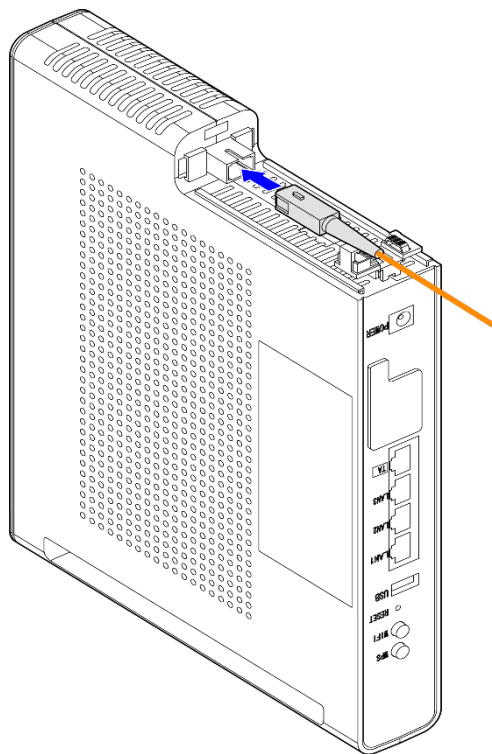
本製品はファイバー保護のため、ファイバーカバーを用意しています。

下記手順通りにファイバーカバーの開閉ができます。

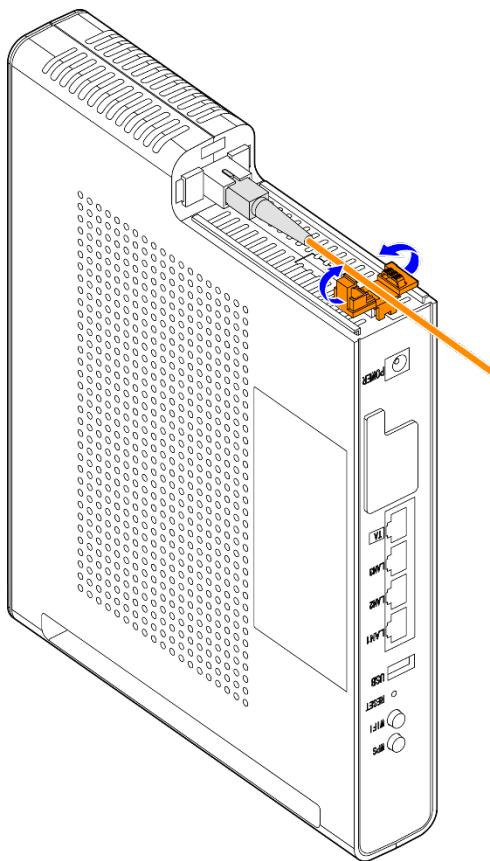
1. 下図のように下に押しながら外側にファイバーカバーをスライドさせます。



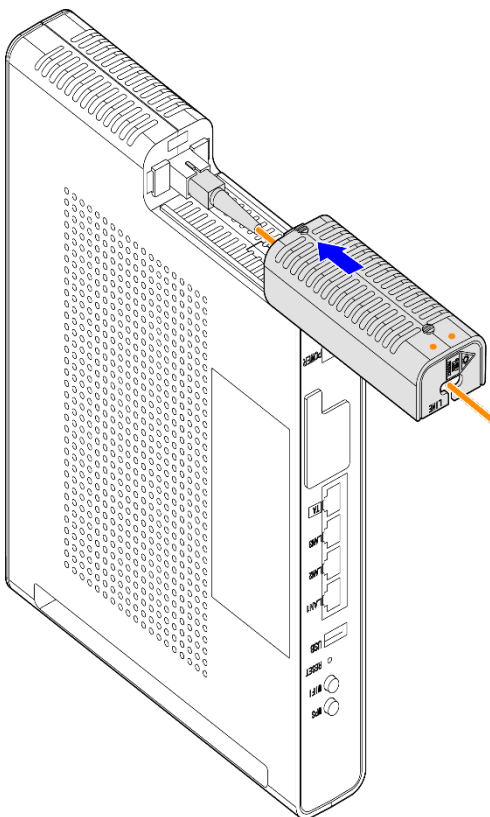
2. 下図のようファイバー末端部分をコネクタ端子に差し込みます。



3. 下図のようファイバーを固定します。



4. 下図のようファイバーカバーを閉めます。



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 PC 設定

設定されたメンテナンスPCのTCP/ IPプロトコル、メンテナンスPCがZXHN F660A機器にpingを実行できること。

Windows 10 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
- ・ サブネットマスク長さ：24

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 10 システムで、スタートボタン> 設定を選択し、「Windowsの設定」を開きます。



2. 「Windowsの設定」で、「ネットワークとインターネット」をクリックして、「ネットワークとインターネット」を開きます。



3. 「ネットワークとインターネット」で、サイトメニューの「イーサネット」をクリックし、右側の設定画面がイーサネットの設定画面に変わります。



4. 「イーサネット」をクリックし、イーサネットの詳細設定画面に変わります。



5. IP設定の「編集」をクリックし、IP設定の編集が表示されています。「自動 (DHCP)」が選択されていることをご確認ください。



6. 本例は192.168.1.2、サブネットマスクは24、デフォルトゲートウェイは192.168.1.1、下図のとおりです。



NOTE

注：

最初のデバイスのためのWeb設定ページにアクセスすると、上記の設定に従ってください。コンフィギュレーションは、ユーザのネットワーク要件に応じて変更することができる。

7. 「保存」ボタンをクリックします。

結果

Windows では、「Windowsキー + R」をクリックし、ポップアップ表示されたダイアログボックスでcmdを入力して、OKボタンをクリックします。ポップアップ表示されたダイアログボックスでping 192.168.1.1を入力して、Enterキーを押します。

- ・ 正しく接続され、Ping が通れた情報は以下となります。

192.168.1.1 に ping を送信しています 32 バイトのデータ:

```
192.168.1.1 からの応答: バイト数 =32 時間 <1ms TTL=64
192.168.1.1 からの応答: バイト数 =32 時間 =1ms TTL=64
192.168.1.1 からの応答: バイト数 =32 時間 =1ms TTL=64
192.168.1.1 からの応答: バイト数 =32 時間 =1ms TTL=64
```

- ・ 接続エラー、ping が通れない情報は以下となります :

192.168.1.1 に ping を送信しています 32 バイトのデータ:

```
要求がタイムアウトしました。
要求がタイムアウトしました。
要求がタイムアウトしました。
要求がタイムアウトしました。
```

192.168.1.1 の ping 統計:

パケット数: 送信 = 4、受信 = 0、損失 = 4 (100% の損失)、

以下の項目をご確認ください。

- I. お使いのデバイスとユーザのコンピュータのイーサネットケーブルの間に正しく接続されているかどうか? LANポート対応するインジケータとユーザのコンピュータ上でNICリンクランプが点灯しているかどうか?
- II. ユーザのコンピュータ上のネットワークアダプタドライバは正しくインストールされているかどうか?
- III. ユーザのコンピュータTCP/IPは適切に設定されているかどうか?

デバイスのIPアドレスは192.168.1.1であれば、ユーザのコンピュータのIPアドレスは必ず192.168.1.2~192.168.1.254間になる; サブネットマスクは255.255.255.0; デフォルトゲートウェイは192.168.1.1。

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。

Please login to continue... [日本語](#)

Username

Password

2. ユーザ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。

F660A

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	<table border="1"> <tr> <td>デバイスモデル</td> <td>F660A</td> </tr> <tr> <td>デバイスのシリアル番号</td> <td>1212121266661208</td> </tr> <tr> <td>ハードウェアバージョン</td> <td>V1.0</td> </tr> <tr> <td>ソフトウェアのバージョン</td> <td>V1.0.10P12N4</td> </tr> <tr> <td>ブートルoaderのバージョン</td> <td>V1.0.0T3</td> </tr> <tr> <td>PONシステムのシリアル番号</td> <td>5A544547C1231208</td> </tr> <tr> <td>パスワード</td> <td>GC1231208</td> </tr> </table>		デバイスモデル	F660A	デバイスのシリアル番号	1212121266661208	ハードウェアバージョン	V1.0	ソフトウェアのバージョン	V1.0.10P12N4	ブートルoaderのバージョン	V1.0.0T3	PONシステムのシリアル番号	5A544547C1231208	パスワード	GC1231208
デバイスモデル	F660A															
デバイスのシリアル番号	1212121266661208															
ハードウェアバージョン	V1.0															
ソフトウェアのバージョン	V1.0.10P12N4															
ブートルoaderのバージョン	V1.0.0T3															
PONシステムのシリアル番号	5A544547C1231208															
パスワード	GC1231208															
ネットワークインターフェース情報																
ユーザインターフェース情報																
ネットワーク																
セキュリティ																
アプリケーション																
管理																

©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。

The screenshot shows a web interface for device management. At the top right, the device model 'F660A' is displayed. Below it is a navigation menu with 'ステータス' (Status) selected. The main content area is titled 'ステータス>>デバイス情報' (Status >> Device Information) and includes links for 'ENGLISH' and 'ログアウト' (Logout). A table displays the following device information:

デバイスモデル	F660A
デバイスのシリアル番号	1212121266661208
ハードウェアバージョン	V1.0
ソフトウェアのバージョン	V1.0.10P12N4
ブートローダのバージョン	V1.0.0T3
PONシステムのシリアル番号	5A544547C1231208
パスワード	GC1231208

At the bottom of the page, the copyright notice reads: ©2012-2020 ZTE Corporation. All rights reserved.

3.2 ネットワークインターフェイス情報

本製品のネットワークインターフェイ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ーフェイス>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。

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	22323
IPプロトコルのバージョン	IPv4/v6
NAT	有効
IPv4アドレス	0.0.0.0/0.0.0.0
IPv4 DNS	0.0.0.0/0.0.0.0/0.0.0.0
IPv4ゲートウェイ	0.0.0.0
IPv4接続ステータス	切断
IPv4のオンライン時間	0秒
IPv4 リース残存期間	0秒
IPv6 LLA	::
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 プレフィックスアドレス	::/0
IPv6接続ステータス	接続されていない
IPv6のオンライン時間	0秒
WAN MAC	00:19:10:85:23:15

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ーフェイス>PONの情報を選択すると、PON接続情報画面に進み、PON状態の情報が表示されます。

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 ユーザインターフェイス情報

本製品のユーザインターフェイ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ーフェイス情報
- ・ 無線 LAN RF2. 4G インターフェイス情報
- ・ 無線 LAN RF5G インターフェイス情報
- ・ USB インターフェイス情報

3.3.1 イーサネットインターフェイス情報

WEB画面の左側メニューでステータス>ユーザインターフェイ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ーフェイス情報画面に進み、イーサネットインターフェイスに送受信パケット情報が表示されます。

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)	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

3.3.2 無線 LAN RF2.4G インターフェイス情報

WEB画面の左側メニューでステータス>ユーザインターフェイス情報>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。

ステータス	ステータス>>ユーザ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	GGG-F660A-1217
認証方法	WPA/WPA2-PSK
暗号化	TKIP+AES
MACアドレス	00:19:10:85:23:15
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	47

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 インターフェイス情報

WEB画面の左側メニューでステータス>ユーザ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。

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	36

SSID5の状態	有効
SSID5名	GGG-F660A-1217-A
認証方法	WPA/WPA2-PSK
暗号化	AES
MACアドレス	00:19:10:85:23:16
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	123
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 インターフェイス情報

WEB画面の左側メニューでステータス>ユーザインタフェース情報>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が表示されます。

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	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 ネットワークの設定

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 RF2.4Gを選択すると、デフォルトでは基本設定の画面に進みます。

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	<input checked="" type="checkbox"/>
他SSIDとの分離を有効にする	<input type="checkbox"/>
動作モード	Mixed(802.11b+802.11g+802.11n)
チャンネル帯域幅	40Mhz
無線チャンネル	自動
ShortGIを有効にする	<input checked="" type="checkbox"/>
ビーコン間隔	100 ミリ秒
電波出力	100%
QoSタイプ	WMM
RTSしきい値	2347
DTIM	1

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機能の有効/無効を行います。 チェックを入れると有効になります。
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。 <input type="checkbox"/> IEEE 802.11b Only <input type="checkbox"/> IEEE 802.11g Only <input type="checkbox"/> IEEE 802.11n Only <input type="checkbox"/> Mixed (802.11b+802.11g) <input type="checkbox"/> Mixed (802.11g+802.11n) <input type="checkbox"/> 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	国コードに基づいて適切なチャンネルを選択することができます。自動（デフォルト）または1~13が選択できます。チャンネルを使用して無線アクセスポイントと無線通信サイト、チャンネルは環境のローカル管理によって決定される。
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。 <input type="checkbox"/> 100% <input type="checkbox"/> 80% <input type="checkbox"/> 60% <input type="checkbox"/> 40% <input type="checkbox"/> 20%
QoSタイプ	不使用、WMM、SSIDが選択できます。 <input type="checkbox"/> 不使用 QoSは有効になっていません。 <input type="checkbox"/> WMM WMM仕様のQoS制御方式に適応して、優先度がハイからローへ：音声サービス、IPTVサービス、インターネットサービス、その他のサービス。 <input type="checkbox"/> SSID SSIDの優先度に従ってQoS制御を行います。SSID方式を選択する時、SSIDの優先順位をそれぞれ設定する必要があります。
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）

パラメータ	説明
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名と有効/無効が設定できます。

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設定の画面に進みます。

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	選択したSSID機能の有効/無効を行います。 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	ステルス機能の有効/無効を行います。 チェックを入れると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のユーザとの相互接続がなくなります。
最大ユーザ数	SSIDに接続できる最大ユーザ数を設定します。 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。

パラメータ	説明
	設定値の範囲は0～32文字です。
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 RF2.4G 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、セキュリティ設定の画面に進みます。

2. セキュリティ設定に関するパラメータの設定は、設定ボタンをクリックします。

セキュリティ設定のパラメータの説明については以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を選択する。 SSID1～SSID4を選ぶ事ができます。
認証方法	選択項目はOpen System（開放システム）、Shared Key（共有鍵）、WPA-PSK、WPA2-PSK、WPA/WPA2-PSKを含む <input type="checkbox"/> Open System：認定されていないオープンシステム認証、すべての要求は、無線端末アクセス認証を通じて提供される。 <input type="checkbox"/> Shared Key：共有鍵認証は無線端末装置側と同じ共有鍵を持っている必要がある。キーが同じである場合にのみ、認定を渡します。 <input type="checkbox"/> WPA-PSK：WPA-PSK認証方式をサポートします。 <input type="checkbox"/> WPA2-PSK：WPA2-PSK認証方式をサポートします。 <input type="checkbox"/> WPA/WPA2-PSK：無線端末およびデバイスは、同じエンド事前共有鍵を使用して構成されている、キーが同じである場合、PSKアクセス認証が成功；キーが同じでな

パラメータ	説明
	い場合、PSKアクセス認証が失敗。
WPA事前共有鍵	認証パスワードは8～63文字です。
WPA暗号化アルゴリズム	選択項目はAES、TKIP及びAES+TKIP。

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画面の左側にて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の設定画面に進みます。

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パラメータ説明については以下の表を参考してください。

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。 ・「無効」：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。
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上に関連付けられたデバイス（そのSSIDを使用するデバイス）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。

ステータス ネットワーク>>無線LAN RF2.4G>>接続中の機器 [ENGLISH](#) [ログアウト](#)

SSIDを選択 | SSID1

IPアドレス	MACアドレス
データエントリがありません。	

更新


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Wi-Fi保護の設定 (Wi-Fi Protected Setup、) 機能に関するパラメータです。この機能を有効にすると、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の設定画面に進みます。

ステータス ネットワーク>>無線LAN RF2.4G>>WPS [ENGLISH](#) [ログアウト](#)

 WPSモードは変更後すぐに有効になります。

WPSモード | PBC

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考してください。

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。EnrolleePIN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

ZXHN F660AのWLAN設定には以下の内容が含まれます。

- ・ 無線 LAN RF5G 基本パラメータの設定
- ・ SSID の設定
- ・ 無線 LAN RF5G 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、基本設定の画面に進みます。

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
ネットワーク		
無線LAN RF2.4G		
無線LAN RF5G		
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		
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	<input checked="" type="checkbox"/>
他SSIDとの分離を有効にする	<input type="checkbox"/>
動作モード	Mixed(802.11a+802.11n+802.11n)
チャンネル帯域幅	80Mhz
無線チャンネル	36
ShortGIを有効にする	<input checked="" type="checkbox"/>
ビーコン間隔	100 ミリ秒
電波出力	100%
QoSタイプ	WMM
RTS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。

WLAN基本パラメータについては以下の表を参考してください。

パラメータ	説明
無線LANを有効にする	無線LAN機能の有効/無効を行います。チェックを入れると有効になります。
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。 <input type="checkbox"/> IEEE 802.11a Only <input type="checkbox"/> IEEE 802.11n Only <input type="checkbox"/> 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、デフォルトでは80MHz。
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	チェックを入れると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。 <input type="checkbox"/> 100% <input type="checkbox"/> 80% <input type="checkbox"/> 60% <input type="checkbox"/> 40% <input type="checkbox"/> 20%

パラメータ	説明
QoSタイプ	不使用、WMM、SSIDが選択できます。 <input type="checkbox"/> 不使用 QoSは有効になっていません。 <input type="checkbox"/> WMM WMM仕様のQoS制御方式に適応して、優先度がハイからローへ：音声サービス、IPTVサービス、インターネットサービス、その他のサービス。 <input type="checkbox"/> SSID SSIDの優先度に従ってQoS制御を行います。SSID方式を選択する時、SSIDの優先順位をそれぞれ設定する必要があります。
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名と有効/無効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設定の画面に進みます。

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。

パラメータ	説明
ステルス機能を有効にする	ステルス機能の有効/無効を行います。 チェックを入れるとその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のユーザとの相互接続がなくなります。
最大ユーザ数	SSIDに接続できる最大ユーザ数を設定します。 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。
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。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 RF5G 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、セキュリティ設定の画面に進みます。

ネットワーク>>無線LAN RF5G>>セキュリティ設定

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

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

LAN

セキュリティ

アプリケーション

管理

SSIDを選択

認証方法

WPA事前共有鍵 (8~63文字)

WPA暗号化アルゴリズム

設定 キャンセル

2. 認証方式を設定して、設定ボタンをクリックします。

セキュリティ設定のパラメータの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
SSIDを選択	設定するSSIDを選択して、SSID5～SSID8が選択できます。
認証方法	<p>選択可能な項目はOpen System（開放システム）、Shared Key（共有鍵）、WPA-PSK、WPA2-PSK、WPA/WPA2-PSKが含まれます。</p> <p><input type="checkbox"/> Open System：開放システム認証は認定されていないとなり、全て要求されたアクセスする無線端末は認定されます。</p> <p><input type="checkbox"/> Shared Key：共有鍵認証は無線端末装置側と同じ共有鍵を持っている必要がある。共有鍵同じである場合のみ認証に合格します。</p> <p><input type="checkbox"/> WPA-PSK：WPA-PSK認証方式をサポートします。</p> <p><input type="checkbox"/> WPA2-PSK：WPA2-PSK認証方式をサポートします。</p> <p><input type="checkbox"/> WPA/WPA2-PSK：無線端末とデバイス端末に同じ相同的事前共有鍵を設定します、キーが同じである場合、PSKアクセス認証成功；キーが同じではない場合、PSKアクセス認証失敗。</p>
WPA事前共有鍵	認証パスワードは8～63字です。
WPA暗号化アルゴリズム	選択項目はAES、TKIP及びAES+TKIP。

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 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の設定画面に進みます。

ステータス

ネットワーク

無線LAN RF2.4G

無線LAN RF5G

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

LAN

セキュリティ

アプリケーション

管理

ネットワーク>>無線LAN RF5G>>アクセス制御リスト ENGLISH ログアウト

動作モードは変更後すぐに有効になります。

SSIDを選択

モード

MACアドレス

SSID	MACアドレス	削除
データエントリーがありません。		

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。

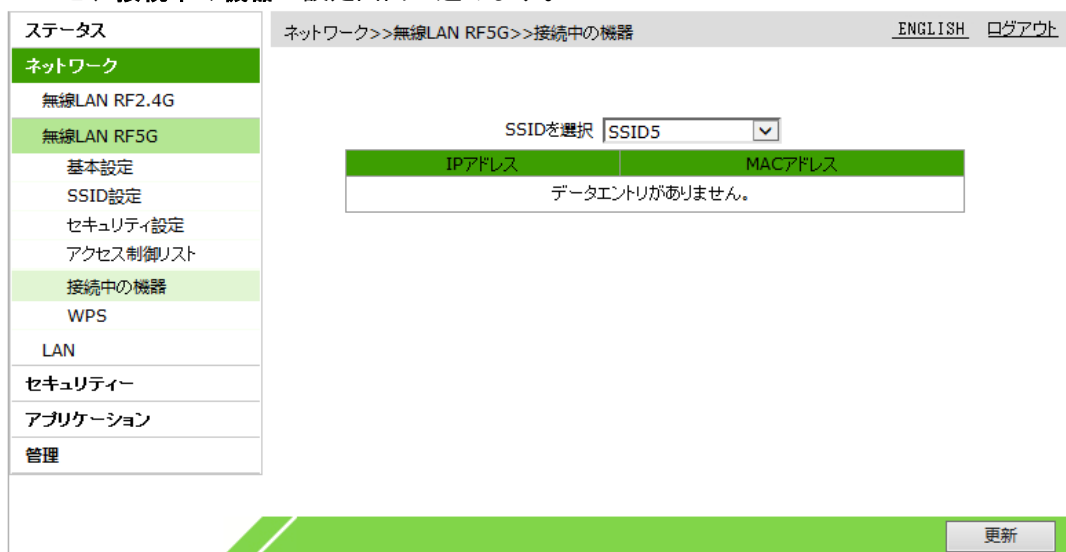
パラメータ	説明
SSIDを選択	設定するSSIDを選択します、SSID5～SSID8が選択できます。
モード	サポートするモードは以下の3種類です。 <ul style="list-style-type: none"> ・「無効」：SSIDのアクセス制御を行いません（デフォルトモード）。 ・「制限する」：登録するMACアドレスのデバイスからの接続を阻止するとき使用します。 ・「許可する」：登録するMACアドレスのデバイスからの接続を許可するとき使用します。
MACアドレス	無線LANにアクセスするデバイスのMACアドレスです。

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（該当SSIDのデバイスを使用する）。

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**の設定画面に進みます。

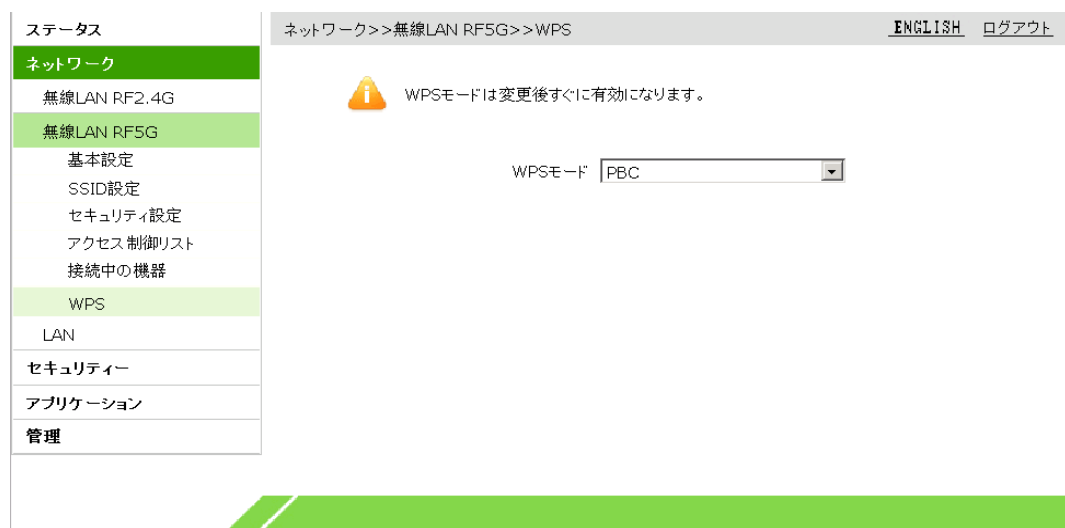


2. SSIDのドロップダウンリストボックスでSSID号を選択して、更新ボタンをクリックすると画面上でデバイスのIPアドレスと関連付けられたMACアドレスリストが表示されます。

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。この機能を有効にすると、端末 (パソコン、スマートフォン等) はONUと自動的に接続し、ユーザが都度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 RF5G>WPSを選択すると、WPSの設定画面に進みます。



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考してください。

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。EnrolleePIN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

ZXHN F660AのLAN設定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、ユーザインターフェイ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側デバイスのMACアドレスに固定し、不正なユーザ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固定アドレス割当を選択すると、DHCP固定割当の設定画面に進みます。


ステータス	ネットワーク>>LAN>>DHCP固定アドレス割当	ENGLISH	ログアウト								
ネットワーク	IPアドレス <input type="text"/>										
無線LAN RF2.4G	MACアドレス <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>										
無線LAN RF5G	<input type="button" value="追加"/>										
LAN	<table border="1"><thead><tr><th>IPアドレス</th><th>MACアドレス</th><th>変更</th><th>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。											
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											

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。



注：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。ユーザインターフェイ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) の設定画面に進みます。

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				
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	<input type="text" value="192.168.1.1"/>			
サブネットマスク	<input type="text" value="255.255.255.0"/>			
セカンダリIPアドレスを有効	<input type="checkbox"/>			
セカンダリIPアドレス	<input type="text"/>			
サブネットマスク	<input type="text"/>			
DHCPを有効	<input checked="" type="checkbox"/>			
DHCPプール開始IPアドレス	<input type="text" value="192.168.1.2"/>			
DHCPプール終了IPアドレス	<input type="text" value="192.168.1.254"/>			
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				
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	84396	A23329746	LAN1

設定	キャンセル
----	-------

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	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を有効	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IPアドレス/ DHCPプール終了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。

パラメータ	説明
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	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) の設定画面に進みます。

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。		

設定 キャンセル

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考ください。

パラメータ	説明
LLA	ZXHN F660AのIPv6アドレスです。
DHCPを有効	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サービスの設定を優先にする	チェックを入れるとDNSサービス機能が優先になります。
リース時間	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を選択すると、スタティックプレフィックス（IPv6）の設定画面に進みます。

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	プレフィックス <input type="text"/> / <input type="text"/> 望ましいライフタイム <input type="text"/> 秒 正式なライフタイム <input type="text"/> 秒 有効にする <input type="checkbox"/> RA <input type="checkbox"/> DHCPv6 <input type="button" value="追加"/>														
無線LAN RF2.4G	<table border="1"> <thead> <tr> <th>プレフィックス</th> <th>望ましいライフタイム</th> <th>正式なライフタイム</th> <th>有効にする</th> <th>修正</th> <th>削除</th> </tr> </thead> <tbody> <tr> <td colspan="6" style="text-align: center;">データエントリがありません。</td> </tr> </tbody> </table>			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。					
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。															
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															

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。
望ましいライフタイム	プレフィックスが有効となるまでにかかる時間です。
正式なライフタイム	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	チェックを入れると有効になります。 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) の設定画面に進みます。

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 <input type="text" value=""/>		
有効にする <input type="checkbox"/> RA		
<input type="checkbox"/> DHCPv6		

WAN接続	有効にする	修正
22323	RA/DHCPv6	
OMC1	RA/DHCPv6	

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。

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 <input type="text" value="OMC1"/>		
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
22323	RA/DHCPv6	
OMC1	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、RAサービスの設定画面に進みます。

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)	最小待ち時間 <input type="text" value="198"/> 秒(3 ~ 1350) 最大待ち時間 <input type="text" value="600"/> 秒(4 ~ 1800) Mフラグ <input checked="" type="checkbox"/> Oフラグ <input checked="" type="checkbox"/>	
セキュリティ		
アプリケーション		
管理		

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考してください。

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フラグ/Oフラグ	<p>M: 管理アドレス設定フラグ (Managed address configuration) 0: その他の状態設定フラグ (Other stateful configuration)</p> <p>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><input type="checkbox"/> M=0、O=0の時、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><input type="checkbox"/> 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><input type="checkbox"/> 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><input type="checkbox"/> M=1、O=0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 セキュリティの設定

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、ファイアウォールの設定画面に進みます。

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->>ファイアウォール ENGLISH ログアウト

ファイアウォール機能を有効

ファイアウォールレベル(IPv4) 低

SPI(IPv6)を有効

ファイアウォールレベル (IPv4) の解説:

高: 正当なWAN側からのアクセスを許可し、WAN側からのPINGを禁止。

中: 正当なWAN側からのアクセスを許可し、同時にインターネット上の危険なデータフローを制御し、WAN側からのPINGを許可。

低: 正当なWAN側からのアクセスを許可し、WAN側からのPINGを許可。

設定 キャンセル

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	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インターフェイスへの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インターフェイスへのPingパケットも許可します。
SPI (IPv6) を有効	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 IPV4 フィルタの設定

この操作ではIPv4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>Ipv4フィルタ**を選択すると、**Ipv4フィルタ**の設定画面に進みます。

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考してください。

パラメータ	説明
有効にする	IPフィルタの有効/無効を行います。 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。 <input type="checkbox"/> TCP (デフォルト) <input type="checkbox"/> UDP <input type="checkbox"/> TCP AND UDP <input type="checkbox"/> ICMP <input type="checkbox"/> ANY
名前	IPフィルタの名前を設定します。 文字数： 1 ～ 32文字です。
(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。

パラメータ	説明
(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。
着信インターフェイス 発信インターフェイス	データフローの方向です。着信インターフェイスと発信インターフェイスを同じにすることはできません。 着信インターフェイスがLAN、発信インターフェイ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。 着信インターフェイスがブロードバンド接続、発信インターフェイスがLANのときは下りデータフローになります。
モード	<ul style="list-style-type: none"> ・ 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 フィルタの設定

この操作ではIPV6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>Ipv6フィルタを選択すると、Ipv6フィルタの設定画面に進みます。

ステータス	セキュリティ>>IPフィルタ>>Ipv6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		
Ipv4フィルタ		
Ipv6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

名前

モード 拒否する 許可する

優先度

プロトコル

送信元ポート範囲 any

宛先ポート範囲 any

送信元IPv6アドレス / any

宛先IPv6アドレス / any

着信インターフェイス

発信インターフェイス



有効にする	名前	送信元IPv6アドレス	(開始)送信元ポート	(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	宛先IPv6アドレス	(終了)送信元ポート	(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		

データエントリがありません。

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	IPフィルタの有効/無効を行います。 チェックを入れるとIPフィルタ項目が有効になります。
名前	IPフィルタの名前を設定します。 文字数： 1 ～ 32文字です。
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	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。 TCP：TCPをフィルタリングします。 UDP：UDPをフィルタリングします。 TCPとUDP：TCPとUDPをフィルタリングします。 ICMPv6：ICMPv6をフィルタリングします。 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。 ICMPv6が選ばれた場合、次のパラメータもサポートします。 any：ICMPv6プロトコルがフィルタ対象を意味します。

パラメータ	説明
	コード指定： 「TYPE」と「CODE」にそれぞれ数値を入力します。
送信元ポート範囲 宛先ポート範囲	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。 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。 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。
送信元IPアドレス範囲 宛先IPアドレス範囲	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。 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。 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。
着信インターフェイス 発信インターフェイス	データトラフィックの方向性を指定します。対象インターフェイスのinとoutを同じにすることはできません。 ANY：WAN側/LAN側に適用します。 LAN：LAN側に適用します。

- （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側のLAN、つまり上りデータフローにのみ対応します。


- 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**の設定画面に進みます。

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	 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。 2. 動作モードは変更後すぐに有効になります。													
セキュリティ	有効にする <input type="checkbox"/>													
ファイアウォール	モード <input type="text" value="拒否"/>													
IPフィルタ	タイプ <input type="text" value="ブリッジ"/>													
MACフィルタ	プロトコル <input type="text" value="IPプロトコル"/>													
URLフィルタ	送信元MACアドレス <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/>													
アクセス制御	宛先MACアドレス <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/>													
ALGスイッチ	<input type="button" value="追加"/>													
アプリケーション	<table border="1"> <thead> <tr> <th>タイプ</th> <th>プロトコル</th> <th>送信元MACアドレス</th> <th>宛先MACアドレス</th> <th>変更</th> <th>削除</th> </tr> </thead> <tbody> <tr> <td colspan="6" style="text-align: center;">データエントリがありません。</td> </tr> </tbody> </table>		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。														
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	MACフィルタの有効/無効を行います。 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。 <ul style="list-style-type: none"> <input type="checkbox"/> ブリッジ (デフォルト) <input type="checkbox"/> ルータ <input type="checkbox"/> ブリッジ+ルータ
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。 <ul style="list-style-type: none"> <input type="checkbox"/> IP (デフォルト) <input type="checkbox"/> ARP <input type="checkbox"/> RARP <input type="checkbox"/> PPPoE <input type="checkbox"/> 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出来ません。
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、ユーザ側LANユーザから特定の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フィルタの設定画面に進みます。

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		
セキュリティ		
ファイアウォール	有効にする <input type="checkbox"/>	
IPフィルタ	モード <input type="text" value="ブラックリスト"/>	
MACフィルタ	URLアドレス <input type="text"/>	
URLフィルタ	<input type="button" value="追加"/>	
アクセス制御	 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。	
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	URLフィルタの有効/無効を行います。 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出来ません。

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の設定画面に進みます。

ステータス	セキュリティ>>アクセス制御	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	着信インターフェイス <input type="text"/>																		
ファイアウォール	(開始)送信元IPアドレス <input type="text"/>																		
IPフィルタ	(終了)送信元IPアドレス <input type="text"/>																		
MACフィルタ	モード <input type="text" value="拒否"/>																		
URLフィルタ	<input type="checkbox"/> HTTP																		
アクセス制御	<input type="checkbox"/> FTP																		
ALGスイッチ	<input type="checkbox"/> HTTPS																		
アプリケーション	<input type="button" value="追加"/>																		
管理	<table border="1"> <thead> <tr> <th>有効にする</th> <th>着信インターフェイス</th> <th>(開始)送信元IPアドレス</th> <th>(終了)送信元IPアドレス</th> <th>モード</th> <th>サービスのリスト</th> <th>変更</th> <th>削除</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	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										
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												
	データエントリがありません。																		
	注意：上記サービスがポートに遠隔アクセスするのを設定する場合は、このリンクをクリックしてください。 リモートアクセスポートを変更																		

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。

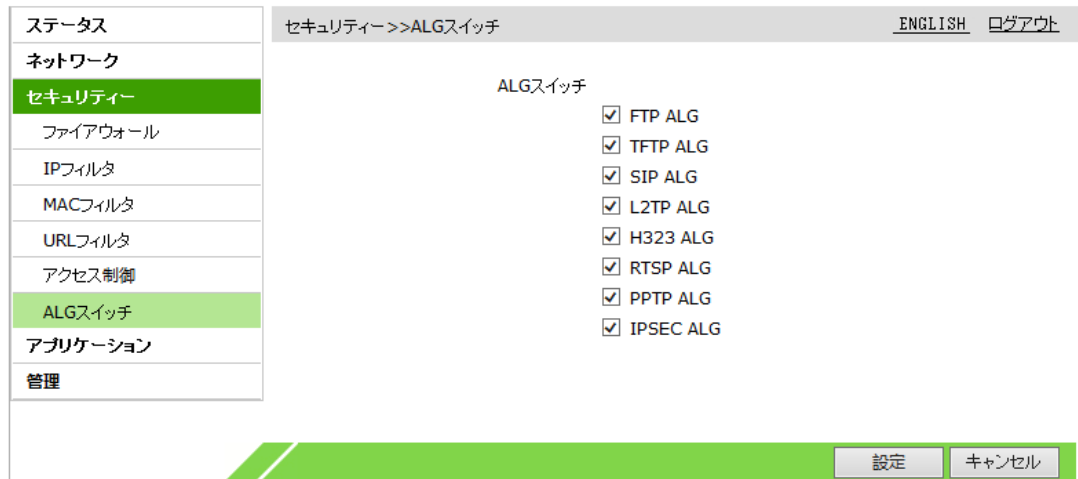
パラメータ	説明
有効にする	アクセス制御の有効/無効を行います。 チェックを入れるとサービス制御の当該項目が有効になります。
着信インターフェイス	サービスの送信元です。
(開始)送信元IPアドレス/(終了)送信元IPアドレス	サービス制御が必要なIPセクションです。
モード	<input type="checkbox"/> 拒否 <input type="checkbox"/> 許可
サービスのリスト	制御するサービスです。以下の種類から選択できます。 <input type="checkbox"/> HTTP <input type="checkbox"/> FTP <input type="checkbox"/> 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。

- (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。

5.7 ALG スイッチの設定

ALG設定スイッチの有効にすることで、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ません。これにより安全性を向上させます。

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**の設定画面に進みます。



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スイッチを有効にし、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の設定画面に進みます。

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	DMZ機能の有効/無効を行います。 チェックを入れるとDMZ機能が有効になります。
IPv4	
WAN接続	LAN側本台の対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。 <input type="checkbox"/> MACアドレスのマッピングを有効する時は、LANのMACアド

パラメータ	説明
	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IPアドレス	LAN側本台の对外サービス提供時にマッピングするIPアドレスです。
IPv6	
LANのIPv6アドレス	LAN側本台の对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時、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の設定画面に進みます。

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	UPnP機能の有効/無効を行います。 チェックを入れるとUPnP機能が有効になります。

パラメータ	説明
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。
有効期間（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。

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>>UPnPポートマッピング ENGLISH ログアウト

UPnPポートマッピングテーブル

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
✔	TCP	843	843	192.168.1.3	
✔	TCP	16000	4425	192.168.1.3	
✔	UDP	5041	31405	192.168.1.3	

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>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。

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	ポートフォワーディング機能の有効/無効を行います。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。 <input type="checkbox"/> TCP (デフォルト) <input type="checkbox"/> UDP <input type="checkbox"/> 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。

パラメータ	説明
MACアドレスのマッピングを有効にする	MACアドレスのマッピング機能の有効/無効を行います。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

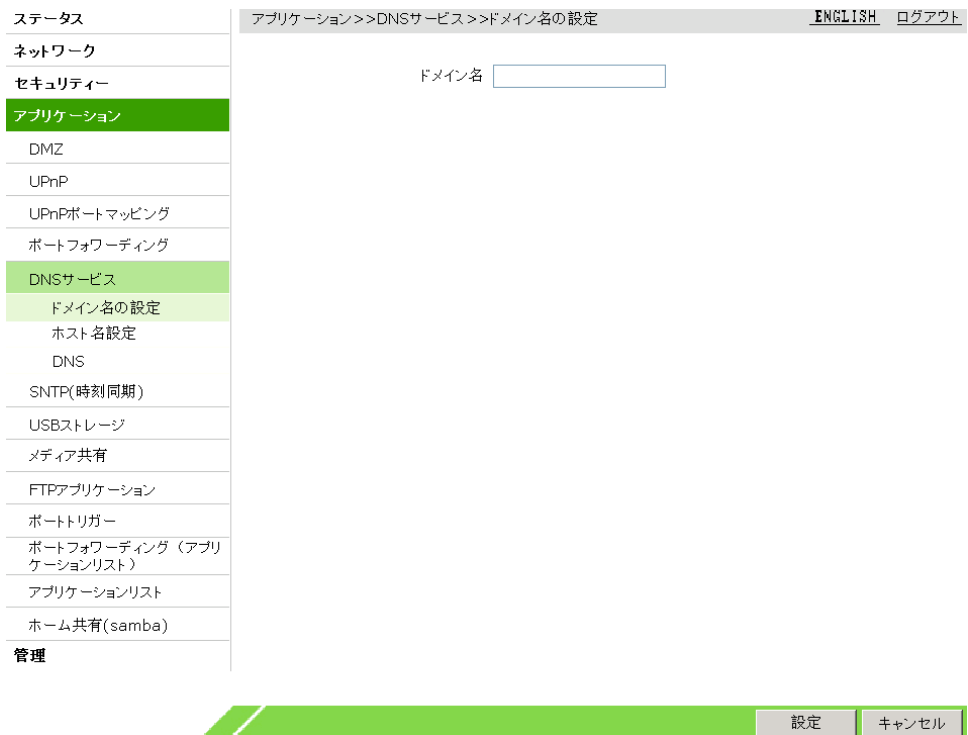
ZXHN F660AのDNSサービス設定には以下の内容が含まれます。

- ・ 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。



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>DNSサービス>ホスト名設定を選択すると、ホスト名設定の画面に進みます。

ステータス アプリケーション>>DNSサービス>>ホスト名設定 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

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

ホスト名



IPアドレス

追加

無効ボタンが表示されている項目は、DHCPサーバから動的に割り当てられているため操作ができません。

ホスト名	IPアドレス	変更	削除
データエントリがありません。			

設定 キャンセル

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>DNSを選択すると、DNSの画面に進みます。

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）の設定

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**SNTP（時刻同期）**の設定画面に進みます。

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		
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		

現在の日時 2000-01-01 01:01:49

タイムゾーン

プライマリSNTPサーバアドレス

セカンダリSNTPサーバアドレス

同期間隔 秒

DSCP値 (0 ~ 63)

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値	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インターフェイ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、USBストレージの確認画面に進みます。

アプリケーション>>USBストレージ ENGLISH ログアウト

ディスク名

パーティションの状態

パーティション情報

総容量

空き容量

インストールパス

2. 安全な取り外しボタンをクリックして、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して、画面を更新します。

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デバイスでの再生が可能です。

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の設定画面に進みます。

The screenshot shows the configuration page for DMS. On the left is a navigation menu with items 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', '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)', and '管理'. The 'メディア共有' item is highlighted. The main area is titled 'アプリケーション>>メディア共有' and includes a checkbox for '有効にする' (checked), a 'サーバー名' field containing 'Media Server', and four 'メディアソース' fields, each with a '参照' button. At the bottom right are '設定' and 'キャンセル' buttons.

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
有効にする	DMSの有効/無効を行います。 チェックを入れるとDMSが有効にします。
サーバ名	DMSサーバ名を入力します。
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します。

6.9 FTP の設定

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サーバの設定画面に進みます。

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

FTPサーバ

FTPクライアント

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

アプリケーション>>FTPアプリケーション>>FTPサーバ

ENGLISH ログアウト

FTPサーバを有効にする

FTPセキュリティ 有効

FTPのログインユーザ名 admin

FTPのログインパスワード ●●●●●●

設定 キャンセル

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。

FTPパラメータの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
FTPサーバを有効にする	FTPサーバの有効/無効を行います。 チェックを入れるとFTPサーバが有効になります。
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クライアントの設定

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クライアントの設定画面に進みます。

ステータス	アプリケーション>>FTPアプリケーション>>FTPクライアント	ENGLISH ログアウト
ネットワーク	サーバアドレス (ドメイン名またはIPアドレス) <input type="text"/>	
セキュリティ	ポート番号 <input type="text"/>	
アプリケーション	匿名ログイン <input type="checkbox"/>	
DMZ	ユーザ名 <input type="text"/>	
UPnP	パスワード <input type="text"/>	
UPnPポートマッピング	ファイルのダウンロードのパス <input type="text"/>	
ポートフォワーディング	ファイルパスを保存 <input type="text"/> <input type="button" value="参照"/>	
DNSサービス	ファイルのダウンロードステータス	
SNTP(時刻同期)	<input type="button" value="ダウンロードを開始"/> <input type="button" value="リフレッシュダウンロードステータス"/> <input type="button" value="ダウンロードをキャンセル"/>	
USBストレージ		
メディア共有		
FTPアプリケーション		
FTPサーバ		
FTPクライアント		
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		

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。
ファイルの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を入力します。
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を表示します。

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、トリガーが必要なおのみの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**の設定画面に進みます。

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	有効にする <input type="checkbox"/>																							
セキュリティ	アプリケーション名 <input type="text"/>																							
アプリケーション	トリガ側のIPアドレス <input type="text"/>																							
DMZ	サービスの種類 <input type="text" value="TCP"/>																							
UPnP	トリガポート <input type="text"/>																							
UPnPポートマッピング	接続 <input type="text" value="TCP"/>																							
ポートフォワーディング	(開始) WANポート <input type="text"/>																							
DNSサービス	(終了) WANポート <input type="text"/>																							
SNTP(時刻同期)	タイムアウト <input type="text" value="1200"/> (60~1800秒)																							
USBストレージ	<input type="button" value="追加"/>																							
メディア共有	<table border="1"> <thead> <tr> <th>アプリケーション名</th> <th>有効</th> <th>サービスの種類</th> <th>トリガ側のIPアドレス</th> <th>(開始) WANポート</th> <th>変更</th> <th>削除</th> </tr> <tr> <th></th> <th>タイムアウト</th> <th>接続</th> <th>トリガポート</th> <th>(終了) WANポート</th> <th></th> <th></th> </tr> </thead> <tbody> <tr> <td colspan="7" style="text-align: center;">データエントリがありません。</td> </tr> </tbody> </table>			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	(開始) WANポート	変更	削除		タイムアウト	接続	トリガポート	(終了) WANポート			データエントリがありません。						
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	(開始) WANポート	変更	削除																		
	タイムアウト	接続	トリガポート	(終了) WANポート																				
データエントリがありません。																								
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																								

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	ポートトリガーの有効/無効を行います。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。 <input type="checkbox"/> TCP (デフォルト)

パラメータ	説明
	<input type="checkbox"/> UDP <input type="checkbox"/> TCP AND UDP
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。
接続方式	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。 <input type="checkbox"/> TCP (デフォルト) <input type="checkbox"/> UDP <input type="checkbox"/> 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。

- (オプション) トリガー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) トリガー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 ウェブホスティングの設定 (アプリケーションリスト)

ウェブホステ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。

- WEB画面の左側メニューで **アプリケーション** > **ウェブホスティング** を選択すると **ウェブホスティング** の設定画面に進みます。

ステータス	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
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		

WAN接続


内部ホストのIPアドレス

アプリケーション

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、ウェブホステ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>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**の設定画面に進みます。

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	アプリケーションを追加するには、ここをクリックしてください。							
セキュリティー								
アプリケーション	<table border="1"> <thead> <tr> <th>アプリケーション</th> <th>変更</th> <th>削除</th> </tr> </thead> <tbody> <tr> <td colspan="3">データエントリがありません。</td> </tr> </tbody> </table>		アプリケーション	変更	削除	データエントリがありません。		
アプリケーション	変更	削除						
データエントリがありません。								
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)								
マルチキャストレート制限								
BPDU								
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								

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。

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	アプリケーションを追加するには、ここをクリックしてください。							
セキュリティー								
アプリケーション	<table border="1"> <thead> <tr> <th>アプリケーション</th> <th>変更</th> <th>削除</th> </tr> </thead> <tbody> <tr> <td colspan="3">データエントリがありません。</td> </tr> </tbody> </table>		アプリケーション	変更	削除	データエントリがありません。		
アプリケーション	変更	削除						
データエントリがありません。								
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								



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、アプリケーションリストの設定が追加されます。

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)	<input type="button" value="保存"/>
セキュリティー	プロトコル <input type="text" value="TCP"/>	
アプリケーション	(開始) WANポート <input type="text"/> (0 ~ 65535)	
DMZ	(終了) WANポート <input type="text"/> (0 ~ 65535)	
UPnP	(開始) マッピングポート <input type="text"/> (0 ~ 65535)	
UPnPポートマッピング	(終了) マッピングポート <input type="text"/> (0 ~ 65535)	
ポートフォワーディング	<input type="button" value="追加"/>	
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		

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
データエントリがありません。						

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。 <input type="checkbox"/> TCP (デフォルト) <input type="checkbox"/> UDP <input type="checkbox"/> 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) 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ことができる、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>ホーム共有 (Samba)** を選択すると、**ホーム共有 (Samba)** の設定画面に進みます。

ステータス	アプリケーション>>ホーム共有(samba) 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	

Sambaサーバを有効

自動的にSambaサーバを実行する

ホスト名 (1~15文字)

設定
キャンセル

2. 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。
自動的にSambaサーバを実行する	この項目をチェック入れてから、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。
ホスト名	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“smashed”。

7 管理の設定

7.1 ユーザ管理の設定

ZXHN F660Aは保守管理と保守管理機能をサポートします、Webユーザ管理者は、WEBメンテナンスページにログインする管理者アカウントのパスワード及び通常のユーザアカウントを修正することができます。

1. WEB画面の左側メニューで**管理>ユーザ管理**を選択すると、**ユーザ管理**の設定画面に進みます。

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"/>	
セキュリティー	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。



注：

ユーザ権限は**管理とメンテナンスアカウントと普通アカウントの2種類権限があります、管理員のユーザ名を修正することが出来ません、普通ユーザは普通アカウント情報しか設定出来ません。**

7.2 システム管理

ZXHN F660Aのシステム管理の説明は以下の内容となります。

- ・ リモートアップデートの設定
- ・ 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時は、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shutdown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。

前提条件

デバイスのバージョンアップデートファイルを取得済み。

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の設定画面に進みます。

The screenshot shows the 'Remote Update' settings page. On the left is a navigation menu with 'System Management' selected. The main content area shows the current and latest firmware versions, with buttons for 'Check Version' and 'Update'.

ステータス	管理>>システム管理>>リモートアップデート		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				
管理				
ユーザ管理				
システム管理				
リモートアップデート				
リセット				
ログ管理				
診断メンテナンス				

現在のファームウェアバージョン	V1.0.10P12N4
最新のファームウェアバージョン	-

バージョンチェック アップデート

2. サーバ上に新しいバージョンがある時有効となります。



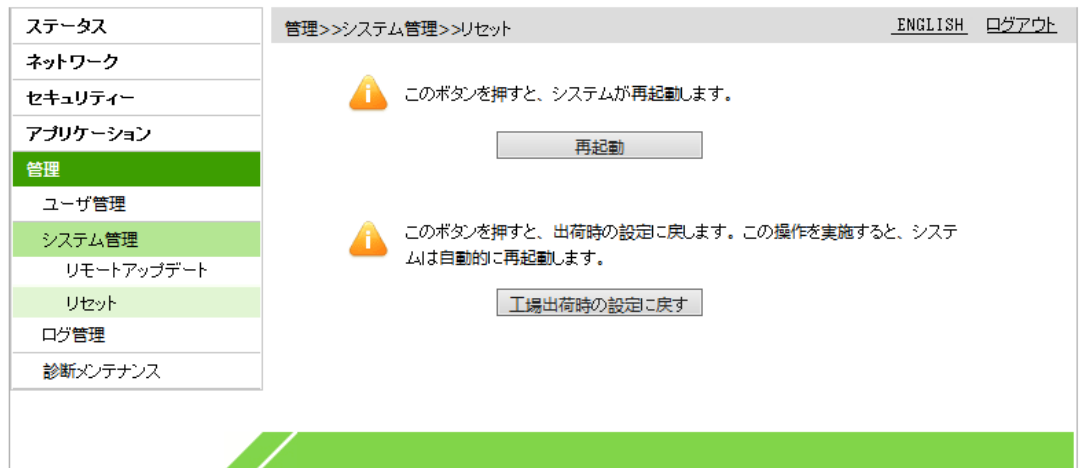
注：

バージョンアップパスは、表示されていない、または変更することはできません。

7.2.2 リセット

リセットでZXHNのF660Aの再起動または工場出荷時の設定に戻すことができます。

1. WEB画面の左側メニューで**管理>システム管理>リセット**を選択すると、**リセット**の画面に進みます。

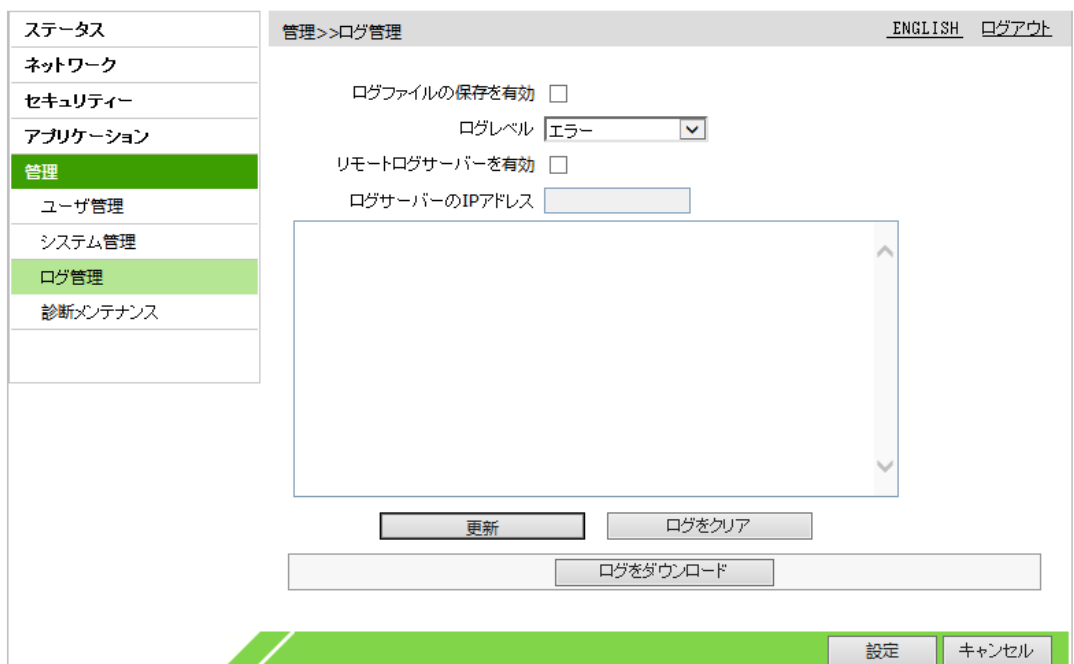


2. デバイス再起動ボタンをクリックして、デバイスは自動的に再起動します。
3. 工場出荷設定時を復元のボタンをクリックして、デバイスは工場出荷設定に復元し、再起動します。

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**の設定画面に進みます。



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	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を有効	チェックを入れるとリモートログサーバ機能が有効になり、ログが定期的にリモートログサーバへアップロードされます。
ログサーバのIPアドレス	リモートログサーバの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)ログの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>ping診断**を選択すると、**ping診断**の設定画面に進みます。

ステータス	管理>>診断メンテナンス>>ping診断	ENGLISH ログアウト
ネットワーク	IPアドレスまたはホスト名 <input type="text"/>	
セキュリティ	発信インターフェイス <input type="text"/>	
アプリケーション	<div style="border: 1px solid gray; height: 100px; width: 100%;"></div>	
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	<div style="text-align: right;"> <input type="button" value="設定"/> <input type="button" value="キャンセル"/> </div>	
ping診断		
traceroute診断		
©2012-2020 ZTE Corporation. All rights reserved.		

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。
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**の設定画面に進みます。

ステータス	管理>>診断メンテナンス>>traceroute診断	ENGLISH ログアウト
ネットワーク	IPアドレスまたはホスト名 <input type="text"/>	
セキュリティ	WAN接続 <input type="text" value="WAN接続"/>	
アプリケーション	最大ホップ数 <input type="text" value="30"/> (2~64)	
管理	タイムアウト <input type="text" value="5"/> (2~10秒)	
ユーザ管理	プロトコル <input type="text" value="UDP"/>	
システム管理	<div style="border: 1px solid gray; height: 100px; width: 100%;"></div>	
ログ管理		
診断メンテナンス		
ping診断	設定 キャンセル	
traceroute診断		

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/ICMPプロトコルを使います。

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。

略語リスト

ALG - Application Level Gateway、アプリケーションレベルゲートウェイ
BPDU - Bridge Protocol Data Unit、ブリッジプロトコルデータユニット
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、検疫ゾーン
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、構内通信ネットワーク
MAC - Medium Access Control、媒体アクセス制御
MTU - Maximum Transfer Unit、最大転送単位、Multi-Tenant Unit、テナント単位
NAT - Network Address Translation、ネットワークアドレス変換
NTP - Network Time Protocol、ネットワーク・タイム・プロトコル、Normal Transmitted Power、ノーマル送信された電力
OMCI - ONT Management Control Interface、ONT管理制御インターフェイス
PON - Passive Optical Network、受動光ネットワーク
PPP - Point to Point Protocol、ポイントツーポイントの議定書
PPPoE - Point to Point Protocol over Ethernet、イーサネットに基いてポイントツーポイントの議定書
RA - Routing Area、ルーティングエリア、Request Agent、要求エージェント、Reverse Activity、リバースアクティブ、Router Advertisement、ルータ通知、Recursion Available、利用可能な再帰、Route Analyser、ルートアナライザー、Route Accelerator、ルートアクセラレータ
RIP - Routing Information Protocol、ルーティング情報プロトコル、Request In Progress、要求中、Received Interference Power、受信干渉電力
RTS - Request To Send、 発送請求
SGI - Short Guard Interval、ショートガードインターバル
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
SMB - Server Message Block、サーバメッセージブロック、SubMiniature version B、超小型バージョンB
SSID - Service Set Identifier、サービスセット識別子
SNTP - Simple Network Time Protocol、簡易ネットワークタイムプロトコル
TCP - Transmission Control Protocol、伝送制御プロトコル
UDP - User Datagram Protocol、ユーザ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プロテクテッドセットアップ