

**ZXHN F260A**

**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 © 2016 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-20160119091801-004

リリース日: 2017/08/25 (R1.0)

# 目次

1	製品概要	1
1.1	安全注意事項	1
1.2	包装明細書	1
1.3	LED 表示	2
1.4	ポート	3
1.5	製品仕様	4
1.6	技術仕様	6
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	11
3	デバイス状態	12
3.1	デバイス情報	12
3.2	ネットワークインターフェイス情報	12
3.2.1	ネットワーク接続情報	12
3.2.2	PON 情報	13
3.3	ユーザインターフェイス情報	14
3.3.1	WLAN RF2.4G のインターフェイス情報	14
3.3.2	WLAN RF5G のインターフェイス情報	14
3.3.3	イーサネットインターフェイス情報	15
3.3.4	USB インターフェイス情報	16
4	ネットワーク設定	17
4.1	WLAN RF2.4G 設定	17
4.1.1	WLAN RF2.4G の基本設定	17
4.1.2	SSID 設定	19
4.1.3	WLAN RF2.4G セキュリティ属性の設定	20
4.1.4	VLAN 設定パラメータ	21
4.1.5	アクセス制御リストの設定	22
4.1.6	接続中の機器情報	23
4.1.7	WPS 機能の設定	23
4.2	WLAN RF5G 設定	24
4.2.1	WLAN RF5G 基本パラメータ設定	24
4.2.2	SSID 設定	26
4.2.3	WLAN RF5G セキュリティ属性の設定	27
4.2.4	VLAN パラメータ設定	29
4.2.5	アクセス制御リストの設定	30
4.2.6	接続中の機器情報	31
4.2.7	WPS 機能の設定	31
4.3	LAN 設定	32
4.3.1	動的 IPv4 アドレスの設定	32
4.3.2	動的 IPv6 アドレスの設定	34
4.3.3	静的アドレスの設定	35

4.3.4 RA サービスの設定 .....	35
5 セキュリティー設定 .....	37
5.1 ファイアウォールの設定 .....	37
5.2 IP フィルタの設定 .....	37
5.3 MAC フィルタの設定 .....	39
5.4 URL フィルタの設定 .....	40
5.5 アクセス制御の設定 .....	41
5.6 ALG スイッチの設定 .....	42
6 アプリケーション設定 .....	43
6.1 DMZ の設定 .....	43
6.2 UPnP の設定 .....	44
6.3 UPnP ポートマッピングの確認 .....	45
6.4 仮想ホストの設定 .....	45
6.5 DNS サービスの設定 .....	47
6.5.1 ドメイン名の設定 .....	48
6.5.2 ホスト名の設定 .....	48
6.5.3 DNS サーバの設定 .....	49
6.6 SNTP(時刻同期)の設定 .....	50
6.7 USB ストレージの容量確認 .....	51
6.8 FTP サーバの設定 .....	52
6.9 ポートトリガーの設定 .....	53
6.10 ポートフォワーディング(アプリケーションリスト)の設定 .....	55
6.11 アプリケーションリストの設定 .....	56
6.12 Samba サービスの設定 .....	58
7 管理設定 .....	61
7.1 ユーザ管理設定 .....	61
7.2 デバイス管理 .....	61
7.2.1 システム管理 .....	61
7.2.2 リモートアップデート設定 .....	62
7.3 ログ管理の設定 .....	63
7.4 診断メンテナンス .....	64
7.4.1 Ping 診断設定 .....	64
7.4.2 Trace Route 診断の設定 .....	64
7.5 ループバック検出 .....	65
7.5.1 基本パラメータの設定 .....	65
7.5.2 ポート機能の設定 .....	66
7.5.3 VLAN 設定 .....	67
略語リスト .....	69

# 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。

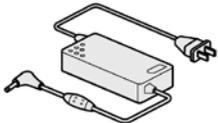
### 本製品についてのお願

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 F260A 本体	1台	

名前	数量	図
ZXHN F260A スタンド	1個	
電源アダプタ	1個	
RJ-45ケーブル	1本	
簡易ユーザガイド	1冊	

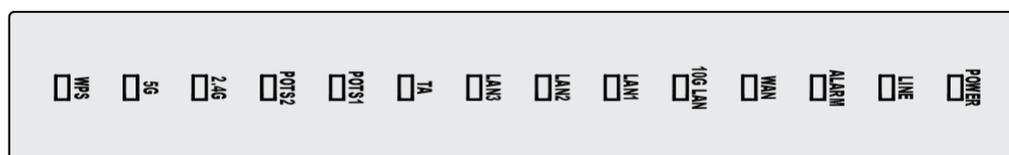
同時に、デバイスに《ZXHN F260A (V1.0) XG-PON ONT 簡易ユーザガイド》一冊を付属しています。



※設置を始める前に、構成部品がすべてそろっていることを確認してください。

不足しているものがある場合はサービス提供元が指定するお問い合わせ先にご連絡ください。

## 1.3 LED 表示



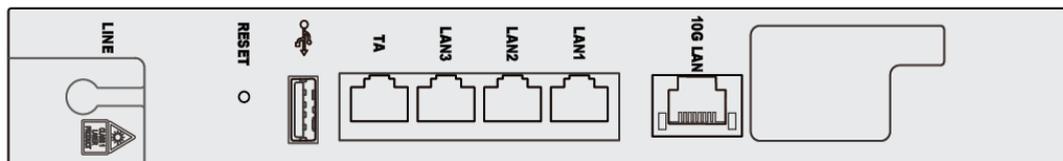
正面LED 表示説明は下表のとおり。

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 ※この状態の時は電源を抜かないでください
ALARM	赤	消灯: ONUが受信した光信号の出力が正常

LED表示	色	説明
		<p>です</p> <p>点灯: ONU PONポート光出力が電源オフになっています</p> <p>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</p>
WAN	緑	<p>消灯: インターネット接続がありません</p> <p>点灯: 接続が確立され、IPアドレスを取得しました</p> <p>点滅: データ受送信中です</p>
10G LAN、LAN1、LAN2、LAN3、TA	緑	<p>消灯: LANポートに設備が接続されていません</p> <p>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</p> <p>点滅: データ受送信中です</p>
2.4G/5G	緑	<p>消灯: WIFI機能オフ</p> <p>点灯: WIFI機能オン</p> <p>点滅: データ受送信中です</p>
WPS	黄、緑、赤	<p>消灯: WPSのオートネゴシエーションがされていません</p> <p>黄色点灯: オートネゴシエーション中</p> <p>緑色点灯: オートネゴシエーションが成功しました</p> <p>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</p>

## 1.4 ポート

ZXHN F260A背面ポートとボタン。



裏面ポートとボタンの説明は下表のとおり。

ポート、ボタン	説明
10G LAN	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。
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。
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。

ポート、ボタン	説明
	標準USB3.0ポート、USB 2.0互換設備に接続できます。
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秒以上長押しすれば、工場出荷設定に戻してリセットします。
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。
2.4G/5G	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。

NOTE またUSBインターフェイス、2.4G/5GとWPSボタンはLEDパネルのサイド側にあります。

## 1.5 製品仕様

### ■ WAN インターフェイス

ポート数	XG-GPONポート × 1
通信方式	ITU-TG.987.x/G.988標準
物理インターフェイス	SC/UPC

### ■ LAN インターフェイス

ポート数	10G LAN × 1、LAN × 3
規格	10G LAN:IEEE802.3u(100BASE-TX)、IEEE802.3ab(1000BASE-T) IEEE802.3an(10GBASE-T) LAN: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(5.150-5.725 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600 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(5.150-5.725 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)
IEEE802.11ac	
周波数帯域/ チャンネル	5GHz帯(5.150-5.725 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/[VHT160]484 MU-MIMO
伝送速度	5GHz帯(最大1.7Gbps)
アンテナ/セキュリティ	
アンテナ	送信4×受信4(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

ZXHN F260Aの技術仕様は下表とおりです。

項目	仕様
外観寸法	206 mm × 222 mm × 32 mm(H×W×D)
定格電流	3 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

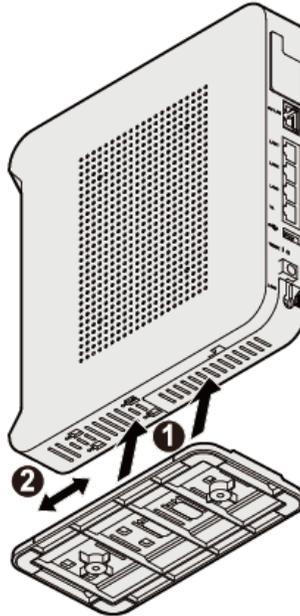
### スタンドの取り付け

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：

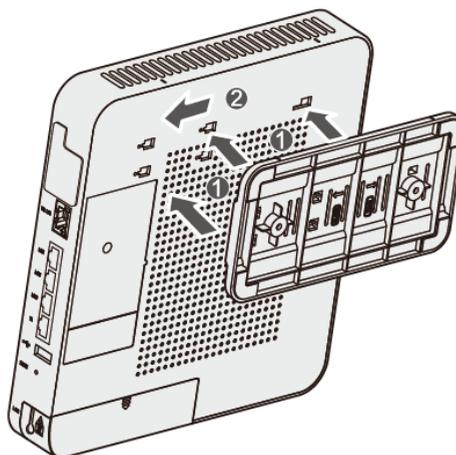
1. 図1-1に示すように、スタンドを本体の挿入ボード側に差し込んでから①、底板を固定させるために、矢印②の方向に従って左右にスライドします。

図1-1 縦設置



2. 図1-2に示すように、スタンドを本体側面側のスロットに差し込めてから①、底板を固定させるために、矢印②の方向に従って左右にスライドします。

図1-2 壁付け型設置



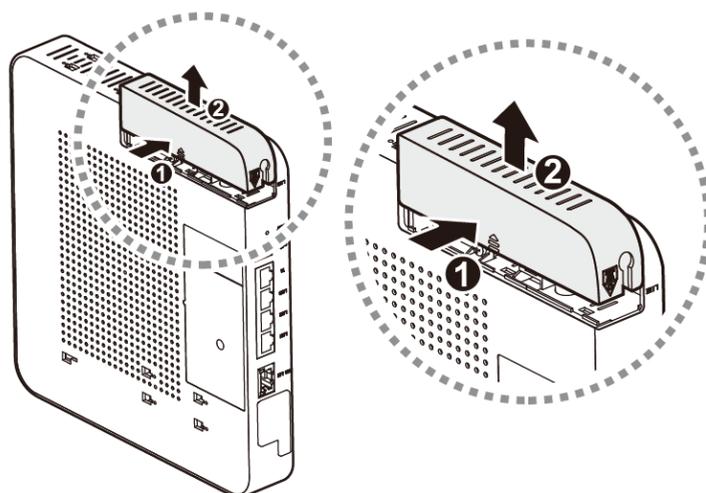
### ファイバーカバーの取り付け

ZXHN F260A 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。

下記手順とおりにファイバーカバーの開け閉めができます。

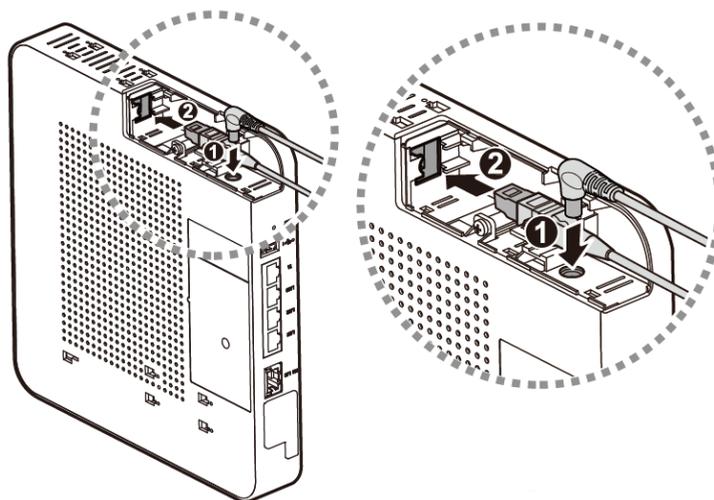
1. 図1-3のようにファイバーカバーを押しながら外側にスライドさせます。

図1-3 ファイバーカバーを外します

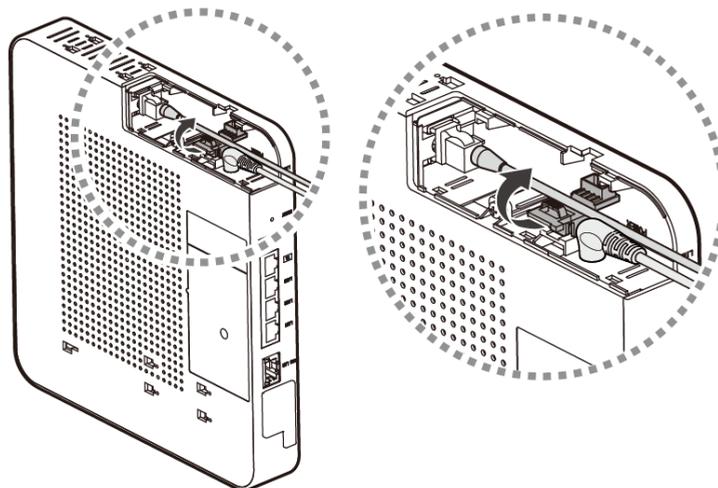


2. 図1-4に示すように、電源コネクタを挿入してから(①)、光ファイバーをコネクタ端子に差し込みます(②)。

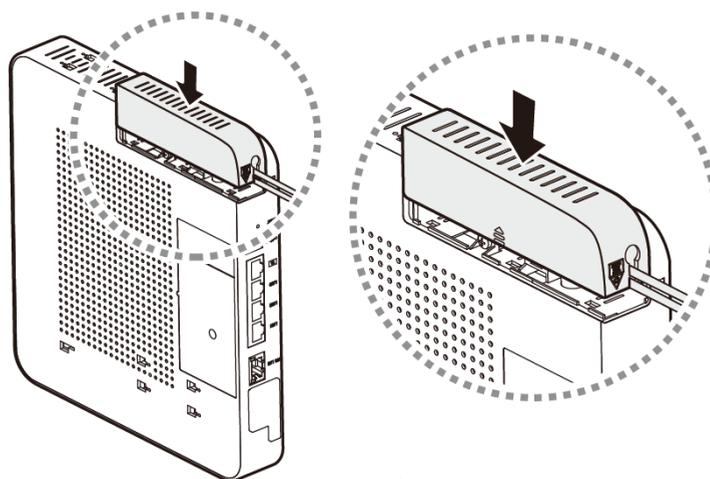
図1-4 電源コネクタと光ファイバーを差し込みます



3. 図1-5のようにファイバーを固定します。  
図1-5 ファイバーの固定



4. 図1-6のようにファイバーカバーを閉めます。  
図1-6 ファイバーカバーの取り付け



**NOTE** 蓋を取り付け/取り外す際や、電源と光ファイバーを差込/取り外す際には、電源をオフにしてください。光ファイバーを差込/取り外す際に、電源コネクタに触れないようにご注意ください。

## 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。

本製品のインターネットポートのいずれかにパソコンが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

#### Windows7環境下での設定

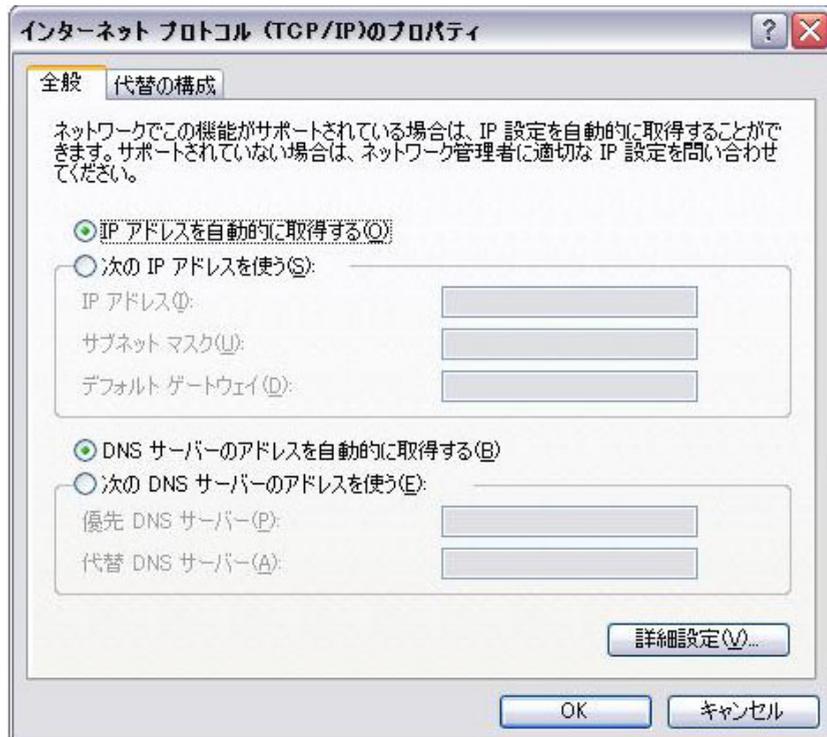
本製品のデフォルトのネットワーク設定は以下の通りです。

- ・ 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**ネットワークと共有センター**をクリックして、**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、**ローカル接続**をクリックし、**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. IPアドレスを自動的に取得する。DNSサーバ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

## 2.3 本製品のログイン

本製品ではWEBブラウザを通じて設定・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.WEB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2-2)

図2-2 ログイン画面

2. デフォルトでは、ユーザ名「admin」とパスワード「admin」を入力してログインボタンをクリックするとログイン完了後の画面に進みます。

## 3 デバイス状態

### 3.1 デバイス情報

WEB画面の左側メニューでステータスを選択すると、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			
+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			
+ネットワーク			
+セキュリティ			
+アプリケーション			
+管理			

デバイスモデル	F260A
デバイスのシリアル番号	07A80401
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	V1.0.0T6
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	5A54454707A80401

©2008-2016 ZTE Corporation. All rights reserved.

### 3.2 ネットワークインターフェイス情報

#### 3.2.1 ネットワーク接続情報

WEB画面の左側メニューでステータス> ネットワークインターフェイス情報> ネットワーク接続情報を選択すると、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 ネットワーク接続情報画面

-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>>ネットワーク接続情報	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			
ネットワーク接続情報			
PON情報			
+ユーザインタフェース情報			
+ネットワーク			
+セキュリティ			
+アプリケーション			
+管理			

モード	IP
接続名	omci_ipv4_dhcp_1
IPプロトコルのバージョン	IPv4/v6
NAT	有効
IP	10.46.43.89/255.255.255.128
DNS	10.30.1.9/10.30.1.10/0.0.0.0
IPv4ゲートウェイ	10.46.43.1
IPv4接続ステータス	接続中
IPv4 Disconnect Reason	無し
IPv4のオンライン時間	139秒
リース残存期間	761秒
LLA	fe80::fec8:97ff:fe04:18b
DNS	:::/:/::
IPv6ゲートウェイ	::
IPv6 プレフィックスアドレス	::
IPv6接続ステータス	接続中
IPv6のオンライン時間	150秒
WAN MAC	fc:c8:97:04:01:8b

モード	IP
接続名	omci_ipv4_dhcp_2

## 3.2.2 PON 情報

本ページではZXHN F260Aが正常に登録されたかどうかをご確認いただけます。

WEB画面の左側メニューで**ステータス> ネットワークインタフェース情報> PON情報**を選択すると、**PON状態**に関する情報が表示されます。(図3-3)

図3-3 PON情報画面

-ステータス	ステータス>>ネットワークインタフェース情報>>PON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			
ネットワーク接続情報			
PON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			

GPON状態	認証完了
--------	------

更新

## 3.3 ユーザーインターフェイス情報

### 3.3.1 WLAN RF2.4G の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> ユーザーインターフェイス情報> WLAN RF2.4Gを選択すると、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3-4)

図3-4 WLAN RF2.4G インターフェイス情報画面

-ステータス		ステータス>>ユーザーインターフェイス情報>>WLAN RF2.4G(オンライン)	English	ログアウト
デバイス情報				
+ネットワークインターフェイス情報				
-ユーザーインターフェイス情報				
WLAN RF2.4G(オンライン)		無線状態	有効	
WLAN RF5G(オンライン)		チャンネル	1	
イーサネットインターフェイス情報		WDSモード	制限しない	
USBインターフェイス情報		SSID1 有効にする	有効	
+ネットワーク		SSID1名	F260A-0401-G	
+セキュリティ		認証方法	WPA/WPA2-PSK	
+アプリケーション		暗号化	TKIP+AES	
+管理		MACアドレス	fc:c8:97:04:01:8b	
		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	420	
		SSID2 有効にする	制限しない	
		SSID3 有効にする	制限しない	
		SSID4 有効にする	制限しない	

更新

### 3.3.2 WLAN RF5G の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> ユーザーインターフェイス情報> WLAN RF5Gを選択すると、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 WLAN RF5G インターフェイス情報画面

-ステータス	ステータス>>ユーザインターフェイス情報>>WLAN RF5G(オンライン)	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			
WLAN RF2.4G(オンライン)			
WLAN RF5G(オンライン)			
イーサネットインターフェイス情報			
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			

無線状態	有効
チャンネル	116
WDSモード	制限しない
SSID5 有効にする	有効
SSID5名	F260A-0401-A
認証方法	WPA/WPA2-PSK
暗号化	TKIP+AES
MACアドレス	fc:c8:97:04:01:8c
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 有効にする	制限しない
SSID7 有効にする	制限しない
SSID8 有効にする	制限しない

更新

### 3.3.3 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、イーサネットインターフェイスの送受信パケット情報が表示されます。(図3-6)

図3-6 イーサネットインターフェイス情報画面

-ステータス		ステータス>>ユーザインタフェース情報>>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					
WLAN RF2.4G(オンライン)					
WLAN RF5G(オンライン)					
イーサネットインタフェース情報					
USBインタフェース情報					
+ネットワーク					
+セキュリティ					
+アプリケーション					
+管理					

ポート名	LAN1
受信/パケット/バイト数	0/0
送信/パケット/バイト数	815/79198
エラーフレーム	0

ポート名	LAN2
受信/パケット/バイト数	1122/118306
送信/パケット/バイト数	517/384018
エラーフレーム	0

ポート名	LAN3
受信/パケット/バイト数	0/0
送信/パケット/バイト数	815/79198
エラーフレーム	0

ポート名	LAN4
受信/パケット/バイト数	0/0
送信/パケット/バイト数	54/3888
エラーフレーム	0

ポート名	LAN5
受信/パケット/バイト数	0/0
送信/パケット/バイト数	814/79096
エラーフレーム	0

### 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が表示されます。(図3-7)

図3-7 USBインターフェイス情報画面

-ステータス		ステータス>>ユーザインタフェース情報>>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					
WLAN RF2.4G(オンライン)					
WLAN RF5G(オンライン)					
イーサネットインタフェース情報					
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	USB DISK
デバイスの種類	USB Mass Storage
デバイスID	090c_1000
デバイス速度	不明
接続ステータス	接続されている
アクセスアドレス	ftp://192.168.1.1

## 4 ネットワーク設定

### 4.1 WLAN RF2.4G 設定

#### 4.1.1 WLAN RF2.4G の基本設定

WLAN RF2.4Gの基本設定により、無線LANの動作条件及び動作状態を変更できます。

1. WEB画面の左側メニューでネットワーク> WLAN RF2.4G(オンライン)を選択すると、下図のとおり、基本設定画面に進みます。

ネットワーク>>WLAN RF2.4G(オンライン)>>基本設定 English ログアウト

無線LANを有効にする

他SSIDとの分離を有効にする

動作モード Mixed(802.11b+802.11g+802.11n)

地域/国 日本

チャンネル帯域幅 20MHz

無線チャンネル 自動

ShortGIを有効にする

ビーコン間隔 100 ミリ秒

電波出力 100%

QoSタイプ WMM

RTS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た上で、設定ボタンをクリックします。WLAN Raido2.4Gの基本パラメータについては下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	WLAN RF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との分離機能を有効にし、各SSIDのユーザ間の相互接続ができなくなります。
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)

パラメータ	説明
	<input type="checkbox"/> Mixed (802.11b+802.11g+802.11n)
地域/国	デフォルトでは日本とします
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、20MHzとなります。
無線チャンネル	国コードに応じて適切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チャンネルは地元の規制環境により決めます。
ShortGIを有効にする	SPIショートガードインターバルを有効にします。
ビーコン間隔	ビーコンの送信間隔時間です。システムのデフォルトでは100msです。
電波出力	送信電力のレベルは以下の設定できます。 <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を使用しません。 <input type="checkbox"/> WMM WMM基準のQoS制御方式に準じて、優先順位レベルは以下のとおりとなります。 (高→低): 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の優先順位に従ってQoS制御を行います。このモードを選択する場合は、SSIDの優先順位を設定しておくこと。
RTSしきい値	リクエスト送信RTSしきい値を設定します。(リクエスト送信回数の上限)
DTIM	DTIM(Delivery Traffic Indication Message)の配信トラフィック表示の時間間隔です。

## 4.1.2 SSID 設定

1台のZXHN F260Aにおいて四つのSSIDの設定が可能です。各SSIDに異なるSSID名、優先順位と最大接続可能数などが設定できます。

1. WEB画面の左側でネットワーク> WLAN RF2.4G(オンライン) >SSID設定を選択すると、下図のとおり、SSID設定画面に進みます。

2. SSIDに関するパラメータを設定してから、**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表を参照してください。

パラメータ	説明
SSIDを選択	対象SSIDを選択します。SSID1～SSID4が選択できます。
非表示	チェックを入れるとSSIDを非表示となります。この場合では、無線端末デバイス(モバイル等)はこのSSIDを検知することができなくなります。非表示のSSIDを通じてネットワークに接続には、無線デバイスから申請を送信しておくこと。デフォルトでは無効となっています。
有効にする	チェックを入れるとSSIDが有効になります。
SSID内の端末間での通信を無効	チェックを入れると他のSSIDとの分離機能が有効になり、各SSIDのユーザ間に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1～32です。
SSID名	対象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です。

パラメータ	説明
	デフォルトでは0となり、プライオリティが設定されていないを意味します。値が大きいほどプライオリティが高くなります。

### 4.1.3 WLAN RF2.4G セキュリティー属性の設定

WLANセキュリティ属性を設定することにより、各SSIDに異なる認証方式と認証パスワードの設定ができます。

1. WEB画面の左側メニューでネットワーク> WLAN RF2.4G(オンライン)>セキュリティ設定を選択すると、下図のとおり、セキュリティ設定画面に進みます。

2. セキュリティー設定に関するパラメータを設定してから、設定ボタンをクリックします。  
セキュリティ設定パラメータについては下表を参照してください。

パラメータ	説明
SSIDを選択	対象SSIDを選択します。SSID1～SSID4が選択できます。
認証方法	以下の方式は選択可能です: Open System、Shared Key(共有キー)、WPA-PSK、WPA2-PSK、WPA/WPA2-PSK、WPA-EAP、WPA2-EAP、WPA/WPA2-EAP。 WPAは各ユーザに異なる暗号鍵を送信する802.1X認証サーバと組み合わせて使うことができます。それはWPA-EAPまたはWPA2-EAP(エンタープライズ)です。 また、WPAは事前共有鍵(PSK)モードでユーザ毎に同じパスワードを送信します。その方式WPA-PSKあるいはWPA-PSK(個人)となります。 WPA2のセキュリティ性能はWPAより優れています。

パラメータ	説明
	<p>しかしながら、一部のワイヤレスカードは、この暗号化モードをサポートしていませんので、セキュリティと互換性の面ではWPAを推奨します。</p> <p><input type="checkbox"/> Open System: 認証しないシステムであり、すべてのアクセスをリクエストする無線端末が認証されます。</p> <p><input type="checkbox"/> Shared Key: 共有鍵の認証には無線端末とデバイス側は同じ共有鍵であること。共有鍵が同じである場合のみ、認証されます。</p> <p><input type="checkbox"/> WPA/WPA2-PSK: WPA-PSK認証方式とWPA2-PSK認証方式との交換性を備えています。</p> <p><input type="checkbox"/> WPA/WPA2-EAP: WPA-EAP認証方式とWPA2-EAP認証方式との交換性を備えています。</p>
WPA事前共有鍵	認証パスワードは半角8～63文字となります。
WPA暗号化アルゴリズム	オプションはAES、TKIP及びAES+TKIPです。

#### 4.1.4 VLAN 設定パラメータ

SSIDのVLANパラメータを設定することにより、各SSIDに異なるVLANパラメータを設定することができます。

1. WEB画面左側でネットワーク> WLAN RF2.4G(オンライン) >VLAN設定を選択すると、下図のとおり、VLAN設定画面に進みます。

ネットワーク>>WLAN RF2.4G(オンライン)>>VLAN設定 English ログアウト

SSIDを選択

ダウンTAGストリップ有効

アップTAG有効

VLAN  (0 ~ 4095)

優先順位

2. 必要に応じてVLANに関するパラメータを設定してから、設定ボタンをクリックします。

VLANのパラメータについては下表を参照してください。

パラメータ	説明
SSIDを選択	設定対象のSSIDを選択します。SSID1～SSID4が選択できます。
ダウンTAGストリップ有効	チェックを入れると、ダウンリンクのメッセージにタグ機能がなくなります。
アップTAG有効	チェックを入れると、アップリンクのメッセージはタグ付きとなります。
VLAN	SSIDが属するVLAN IDを設定します。値の範囲は0～4095です。
優先順位	SSIDのVLANのプライオリティを設定します。選択可能範囲は0～7です。デフォルトでは0となり、プライオリティが設定されていないのを意味します。値がたかいほどプライオリティが高くなります。

#### 4.1.5 アクセス制御リストの設定

WLANアクセス制御機能を有効にしてMACアドレスリストを通じて、WLANアクセスのブロック/ホワイトリストを設定することにより、WLANから端末へのアクセス制御を実現できます。モードを「制限する」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「許可する」に設定すると、リスト上の無線端末のみが当該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> WLAN RF2.4G(オンライン) >アクセス制御リストを選択すると、下図のとおり、アクセス制御リスト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、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表を参照してください。

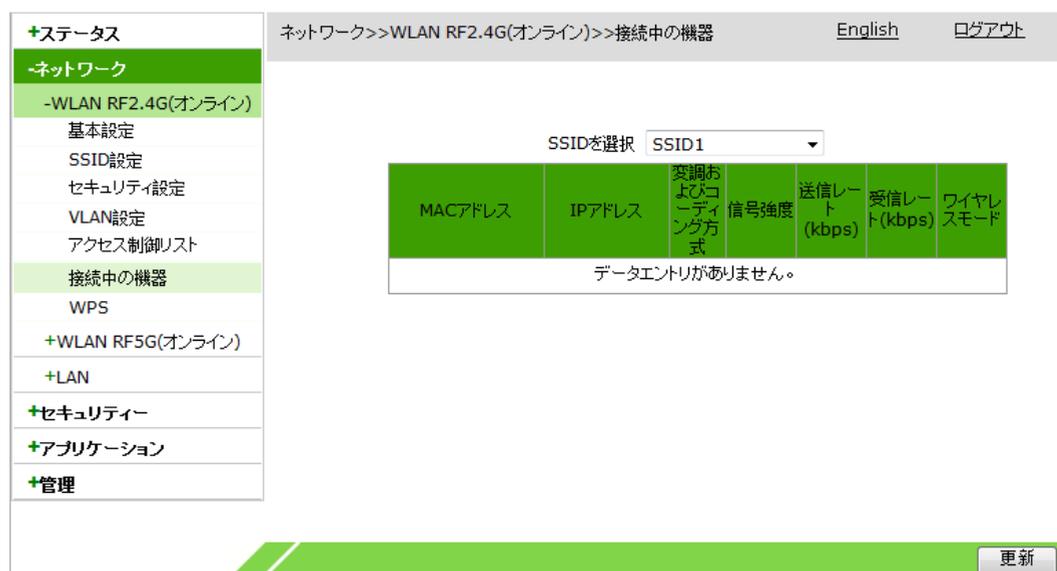
パラメータ	説明
SSIDを選択	設定対象のSSIDを選択します。SSID1～SSID4が選択可能です。
モード	以下の3つのモードをサポートしています。 <input type="checkbox"/> 制限にしない: SSIDのアクセス制御を行いません(デフォルトモード)。 <input type="checkbox"/> 制限する: 登録するMACアドレスのデバイスからWLANへの接続を制限します。 <input type="checkbox"/> 許可する: 登録するMACアドレスのデバイスからWLANへの接続を許可します。
MACアドレス	WLAN無線端末にアクセスするMACアドレス

3. (オプション) SSID後ろの  アイコンをクリックすると設定データを削除できます。

#### 4.1.6 接続中の機器情報

本操作により、WLANに接続しているIPアドレスとMACアドレス情報を確認できます。

1. WEB画面の左側メニューでネットワーク> WLAN RF2.4G(オンライン)>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。



2. SSIDを選択ドロップダウンリストから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アドレスリストが表示されます。

#### 4.1.7 WPS 機能の設定

本操作はWPS(Wi-Fi Protected Setup, Wi-Fi保護設定)機能に関するパラメータを設定します。通常では、変更する必要はありません。このWPS機能をオンにすると、端末デバイスはWPSを通じてWLANに自動的に接続し、ユーザ側によりSSIDの検索及びパスワード

ドの入力は要りません。

1. WEB画面の左側メニューでネットワーク> WLAN RF2.4G(オンライン) >WPSを選択すると、WPS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: キーモードです。ZXHN F260AパネルのWPSボタンを押すと、WPS機能をオンにします。 無効にする: WPS機能をオフにします。

## 4.2 WLAN RF5G 設定

### 4.2.1 WLAN RF5G 基本パラメータ設定

本設定作業はWLANの作動条件と作動状態などを含め、WLAN Radio5Gの基本パラメータを設定します。

1. WEB画面の左側メニューでネットワーク> WLAN RF5G(オンライン)を選択すると、下図のとおり、基本設定画面に進みます。

+ステータス	ネットワーク>>WLAN RF5G(オンライン)>>基本設定	English	ログアウト
-ネットワーク			
+WLAN RF2.4G(オンライン)			
-WLAN RF5G(オンライン)			
基本設定			
SSID設定			
セキュリティ設定			
VLAN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+802.11ac)
地域/国	日本
チャンネル帯域幅	80MHz
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WLAN Radio5Gの基本パラメータを設定した上で、設定ボタンをクリックします。WLAN基本パラメータは下表をご参照ください。

パラメータ	説明
無線LANを有効にする	WLAN RF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との分離機能を有効にし、各SSIDのユーザ間の相互接続ができなくなります。
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) <input type="checkbox"/> Mixed(802.11a+802.11n+802.11ac)
地域/国	デフォルトでは日本とします。
チャンネル帯域幅	無線ブロードバンドの帯域を設定します。デフォルトでは、80MHzとなります。
無線チャンネル	5G帯無線LANのチャンネル設定は、ONUにより無線信号状態に応じて自動的、または手動的にチャンネル方式を指定します。チャンネル選定はローカルの無線管理機関に定められる基準に準ずること。
ShortGIを有効にする	SIGI(Short Guard Interval、ショートガードインターバル)を有効にします。

パラメータ	説明
ビーコン間隔	ビーコンの送信間隔時間です。システムのデフォルトでは100msです。
電波出力	送信電力のレベルは以下の設定できます。 <input type="checkbox"/> 100% <input type="checkbox"/> 80% <input type="checkbox"/> 60% <input type="checkbox"/> 40% <input type="checkbox"/> 20%
QoSタイプ	<input type="checkbox"/> 不使用 QoSを使用しません。 <input type="checkbox"/> WMM WMM基準のQoS制御方式に準じて、優先順位レベルは以下の通りになります。 (高→低): 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の優先順位に従ってQoS制御を行います。このモードを選択する場合は、SSIDの優先順位を設定しておくこと。
RTSしきい値	リクエスト送信RTSしきい値 (Request To Send)を設定します。(リクエスト送信回数の上限)
DTIM	DTIM (Delivery Traffic Indication Message) の配信トラフィック表示の時間間隔です。

## 4.2.2 SSID 設定

1台のZXHN F260Aにおいて四つのSSIDの設定が可能です。各SSIDに異なるSSID名、優先順位と最大接続可能数などが設定できます。

1. WEB画面の左側でネットワーク> WLAN RF5G(オンライン) >SSID設定を選択すると、下図のとおり、SSID設定画面に進みます。

ネットワーク>>WLAN RF5G(オンライン)>>SSID設定 English ログアウト

+ステータス

**-ネットワーク**

+WLAN RF2.4G(オンライン)

**-WLAN RF5G(オンライン)**

基本設定

**SSID設定**

セキュリティ設定

VLAN設定

アクセス制御リスト

接続中の機器

WPS

+LAN

+セキュリティー

+アプリケーション

+管理

SSIDを選択

非表示

有効にする

SSID内の端末間での通信を無効

最大ユーザ数  (1~32)

SSID名  (1~32文字)

プライオリティ

2. SSIDに関するパラメータを設定してから、**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表を参照してください。

パラメータ	説明
SSIDを選択	対象SSIDを選択します。SSID5～SSID8が選択できます。
非表示	チェックを入れるとSSIDを非表示となります。この場合では、無線端末デバイス(モバイル等)はこのSSIDを検知することができなくなります。非表示のSSIDを通じてネットワークに接続には、無線デバイスから申請を送信しておくこと。デフォルトでは無効となっています。
有効にする	チェックを入れるとSSIDが有効になります。
SSID内の端末間での通信を無効	チェックを入れると他のSSIDとの分離機能が有効になり、各SSIDのユーザ間に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1～32です。
SSID名	対象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です。 デフォルトでは0となり、プライオリティが設定されていないのを意味します。値が大きいほどプライオリティが高くなります

### 4.2.3 WLAN RF5G セキュリティー属性の設定

WLANセキュリティー属性を設定することにより、各SSIDに異なる認証方式と認証パスワード

ードの設定ができます。

1. WEB画面の左側メニューでネットワーク> WLAN RF5G(オンライン) >セキュリティー設定を選択すると、下図のとおり、セキュリティー設定画面に進みます。

2. セキュリティー設定に関するパラメータを設定してから、設定ボタンをクリックします。

セキュリティー設定パラメータについては下表を参照してください。

パラメータ	説明
SSIDを選択	対象SSIDを選択します。SSID5～SSID8が選択できます。
認証方法	<p>以下の方式は選択可能です：Open System、Shared Key(共有鍵)、WPA-PSK、WPA2-PSK、WPA/WPA2-PSK、WPA-EAP、WPA2-EAP、WPA/WPA2-EAP。</p> <p>WPAは各ユーザに異なる暗号鍵を送信する802.1X認証サーバと組み合わせて使うことができます。それはWPA-EAPまたはWPA2-EAP(エンタープライズ)です。</p> <p>また、WPAは事前共有鍵(PSK)モードでユーザ毎に同じパスワードを送信します。その方式WPA-PSKあるいはWPA-PSK(個人)となります。</p> <p>WPA2のセキュリティー性能はWPAより優れています。しかしながら、一部のワイヤレスカードは、この暗号化モードをサポートしていませんので、セキュリティーと互換性の面ではWPAを推奨します。</p> <p><input type="checkbox"/> Open System: 認証しないシステムであり、すべてのアクセスをリクエストする無線端末が認証されます。</p> <p><input type="checkbox"/> Shared Key: 共有鍵の認証には無線端末とデバイス側は同じ共有鍵であること。共有鍵が同じである場合のみ、認証されます。</p>

パラメータ	説明
	<input type="checkbox"/> WPA/WPA2-PSK: WPA-PSK認証方式とWPA2-PSK認証方式との交換性を備えています。 <input type="checkbox"/> WPA/WPA2-EAP: WPA-EAP認証方式とWPA2-EAP認証方式との交換性を備えています。
WPA事前共有鍵	認証パスワードは8～63文字となります。
WPA暗号化アルゴリズム	オプションはAES、TKIP及びAES+TKIPです。

## 4.2.4 VLAN パラメータ設定

本操作はSSIDのVLANパラメータを設定します。各SSIDに異なるVLANパラメータを設定することができます。

1. WEB画面左側でネットワーク> WLAN RF5G(オンライン) >VLAN設定を選択すると、下図のとおり、VLAN設定画面に進みます。

2. 必要に応じてVLANIに関するパラメータを設定してから、**設定**ボタンをクリックします。  
VLANのパラメータについては下表を参照してください。

パラメータ	説明
SSIDを選択	設定対象のSSIDを選択します。SSID5～SSID8が選択できます。
ダウンTAGストリップ有効	チェックを入れると、ダウンリンクのメッセージにタグ機能がなくなります。

パラメータ	説明
アップTAG有効	チェックを入れると、アップリンクのメッセージはタグ付きとなります。
VLAN	SSIDが属するVLAN IDを設定します。値の範囲は0～4095です。
優先順位	SSIDのVLANのプライオリティを設定します。選択可能範囲は0～7です。デフォルトでは0となり、プライオリティが設定されていないのを意味します。値がたかいほどプライオリティが高くなります。

## 4.2.5 アクセス制御リストの設定

WLANアクセス制御機能を有効にしてMACアドレスリストを通じて、WLANアクセスのブロック/ホワイトリストを設定することにより、WLANから端末へのアクセス制御を実現できます。モードを「制限する」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「許可する」に設定すると、リスト上の無線端末のみが当該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> WLAN RF5G(オンライン) >アクセス制御リストを選択すると、下図のとおり、アクセス制御リスト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、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表を参照してください。

パラメータ	説明
SSIDを選択	設定対象のSSIDを選択します。SSID5～SSID8が選択可能です。
モード	以下の3つのモードをサポートしています。 <input type="checkbox"/> 制限しない:SSIDのアクセス制御を行いません(デフォルト)

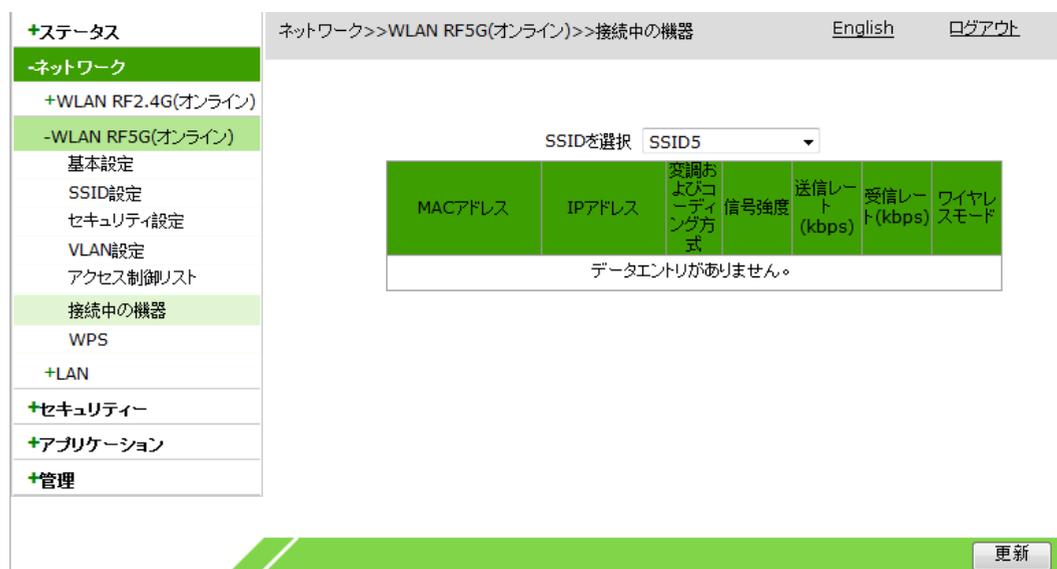
パラメータ	説明
	トモード)。 <input type="checkbox"/> 制限する: 登録するMACアドレスのデバイスからWLANへの接続を制限します。 <input type="checkbox"/> 許可する: 登録するMACアドレスのデバイスからWLANへの接続を許可します。
MACアドレス	WLAN無線端末にアクセスするMACアドレス

3. (オプション) SSID後ろの  アイコンをクリックすると設定データを削除できます。

## 4.2.6 接続中の機器情報

本操作により、WLANに接続しているIPアドレスとMACアドレス情報を確認できます。

1. WEB画面の左側メニューでネットワーク > WLAN RF5G(オンライン) > 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。



2. SSIDを選択ドロップダウンリストから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アドレスリストが表示されます。

## 4.2.7 WPS 機能の設定

本操作はWPS(Wi-Fi Protected Setup, Wi-Fi保護設定)機能に関するパラメータを設定します。通常では、変更する必要はありません。このWPS機能をオンにすると、端末デバイスはWPSを通じてWLANに自動的に接続し、ユーザ側によりSSIDの検索及びパスワードの入力は要りません。

1. WEB画面の左側メニューでネットワーク > WLAN RF5G(オンライン) > WPSを選択すると、WPS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: キーモードです。ZXHN F260AパネルのWPSボタンを押すと、WPS機能をオンにします。 無効にする: WPS機能をオフにします。

## 4.3 LAN 設定

### 4.3.1 動的 IPv4 アドレスの設定

本作業はZXHN F260A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。また、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アドレスを配ります。

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。

+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	<p>ヒント:</p> <p>DHCPの開始IPアドレスとDHCPの終了IPアドレスはLANのIPサブネット内にある必要があります。</p> <p>IPアドレス <input type="text" value="192.168.1.1"/></p> <p>サブネットマスク <input type="text" value="255.255.255.0"/></p> <p>DHCPを有効 <input checked="" type="checkbox"/></p> <p>DHCPプール開始IPアドレス <input type="text" value="192.168.1.2"/></p> <p>DHCPプール終了IPアドレス <input type="text" value="192.168.1.254"/></p> <p>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"/></p> <p>DNSサーバ1 <input type="text" value="192.168.1.1"/></p> <p>DNSサーバ2 <input type="text"/></p> <p>DNSサーバ3 <input type="text"/></p> <p>デフォルトゲートウェイ <input type="text" value="192.168.1.1"/></p> <p>リース期間 <input type="text" value="86400"/> 秒</p> <p>割り当てられたアドレス</p> <table border="1"> <thead> <tr> <th>MACアドレス</th> <th>IPアドレス</th> <th>リース残存期間</th> <th>ポート</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>			MACアドレス	IPアドレス	リース残存期間	ポート	データエントリがありません。			
MACアドレス	IPアドレス	リース残存期間	ポート								
データエントリがありません。											
+WLAN RF2.4G(オンライン)											
+WLAN RF5G(オンライン)											
-LAN											
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)											
DHCP固定アドレス割当											
ルータ広告(IPv6)											
+セキュリティー											
+アプリケーション											
+管理											

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	ZXHN F260Aのアドレス/サブネットマスクです。
DHCPを有効	チェックを入れるとDHCPサーバを起動します。
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。ZXHN F260AのIPアドレスとは同じセグメント内であること。
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提供元から提供されるDNSサーバを起動します。
DNSサーバ1	デフォルトのDNSサーバ(ZXHN F260A)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	ZXHN F260AのIPアドレスとなります。

パラメータ	説明
ゲートウェイ	
リース期間	IPアドレスのリース期間です。値の範囲は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(秒)と設定されています。-1とは「無期限」を意味します。

### 4.3.2 動的 IPv6 アドレスの設定

本操作はZXHN F260Aの動的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適用します。

- 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(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。

- 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表をご参照ください。

パラメータ	説明
IPアドレス	ZXHN F260AのIPv6アドレスです。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適用します。
DHCPを有効	チェックを入れるとDHCPサーバを起動します。
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提供元から提供されるDNSサーバを起動します。
リース期間	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。

### 4.3.3 静的アドレスの設定

静的アドレスの管理により、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のデバイスのMACアドレスと固定し、不正なユーザからのアクセスを防ぎます。

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

ネットワーク>>LAN>>DHCP固定アドレス割当 English ログアウト

IPアドレス

MACアドレス  :  :  :  :  :

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。

■ **注意:**

**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。

### 4.3.4 RA サービスの設定

この操作により、RAサービスのパラメータを設定します。SLAAC方式で、IPv6のクライアント/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。

+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			
+WLAN RF2.4G(オンライン)		最小待ち時間 198 (3 ~ 1350)秒	
+WLAN RF5G(オンライン)		最大待ち時間 600 (4 ~ 1800)秒	
-LAN		M <input type="checkbox"/>	
ダイナミックアドレス管理 (IPv4)		O <input checked="" type="checkbox"/>	
ダイナミックアドレス管理 (IPv6)			
DHCP固定アドレス割当			
ルータ広告(IPv6)			
+セキュリティ			
+アプリケーション			
+管理			

設定    キャンセル

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になり、チェックを外すと0になります。設定値については以下のとおりです。</p> <p><input type="checkbox"/> M=0、O=0の場合、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の場合、DHCPv6方式でアドレス及びその他の設定情報を取得します。</p> <p><input type="checkbox"/> M=0、O=1の場合、ステートレスモードでアドレスの設定情報を取得します。DHCPv6はIPv6アドレス設定に使用せず、IPアドレスを除いたネットワークパラメータ設定のみに使用します。</p> <p><input type="checkbox"/> M=1、O=0の場合、DHCPv6方式でアドレスを取得しますが、その他の設定には使いません。</p>

## 5 セキュリティー設定

### 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ー性能が向上し、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ー > 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。

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

オフ  
 低  
 中  
 高

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Pingflood/Ping to death/Syn floodなどです。
ファイアウォールレベル	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。

### 5.2 IPフィルタの設定

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

**※設定ミスにより、アクセスができなくなる恐れがあります。**

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

セキュリティ>>IPフィルタ
English [ログアウト](#)

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

有効にする	名前	(開始)送信元IPアドレス	(終了)送信元IPアドレス	(開始)宛先IPアドレス	(終了)宛先IPアドレス	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	(開始)送信元IPアドレス	(終了)送信元IPアドレス	(開始)宛先IPアドレス	(終了)宛先IPアドレス	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. IPフィルタに関するパラメータを設定し、追加ボタンをクリックします。  
 IPフィルタのパラメータについては下表を参考してください。

パラメータ	説明
有効にする	チェックを入れると IPフィルタ項目が有効になります。
プロトコル	パケットフィルタのプロトコルを設定です。次のプロトコルをサポートしています。 <ul style="list-style-type: none"> <li><input type="checkbox"/> TCP (デフォルト)</li> <li><input type="checkbox"/> UDP</li> <li><input type="checkbox"/> TCP AND UDP</li> <li><input type="checkbox"/> ICMP</li> <li><input type="checkbox"/> ANY</li> </ul>
名前	該当IPフィルタする項目の名称。
(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。

パラメータ	説明
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	<input type="checkbox"/> 拒否 <input type="checkbox"/> 許可

- (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。

## 5.3 MAC フィルタの設定

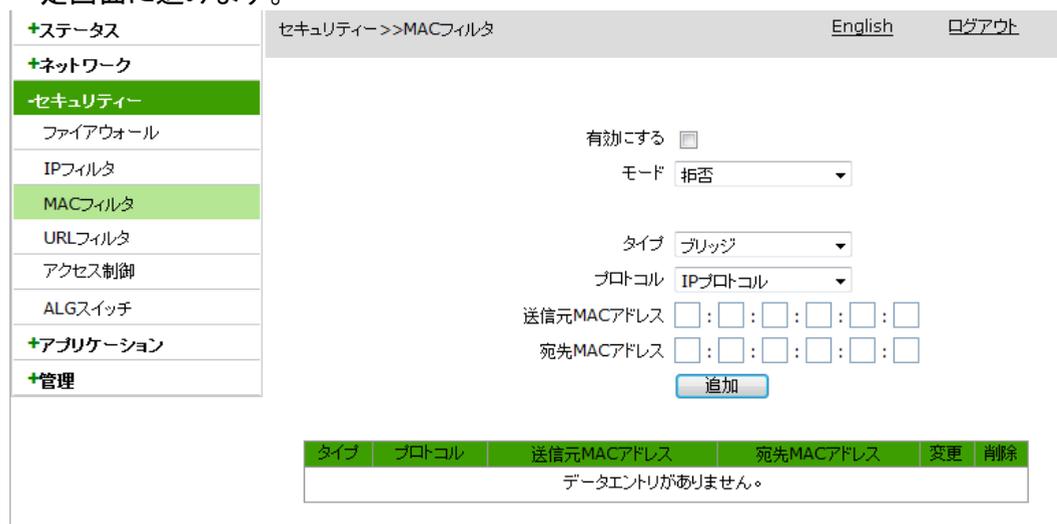
MACアドレスのフィルタ項目を設定することで、特定のMACアドレスから本製品へのアクセスを許可または拒否できます。

※設定ミスにより、アクセスができなくなる恐れがあります。

### 関連情報

MACアドレスのフィルタはユーザ側の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フィルタ設定画面に進みます。



- 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	<input type="checkbox"/> 拒否 <input type="checkbox"/> 許可

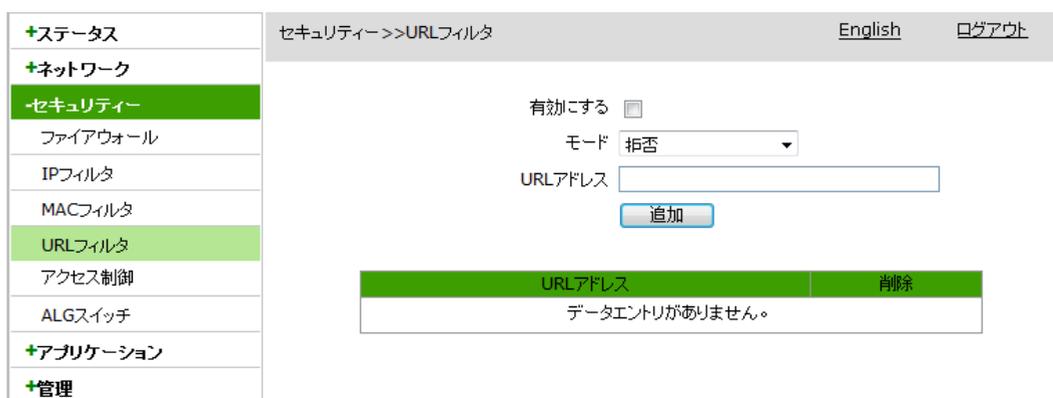
パラメータ	説明
タイプ	以下の3つのタイプをサポートしています。 <input type="checkbox"/> ブリッジ(デフォルト) <input type="checkbox"/> ルータ <input type="checkbox"/> ブリッジ+ルータ
プロトコル	データフローのプロトコルタイプです。以下のプロトコルをサポートしています。 <input type="checkbox"/> IP(デフォルト) <input type="checkbox"/> ARP <input type="checkbox"/> RARP <input type="checkbox"/> PPPoE <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。

- (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 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。

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



セキュリティ->>URLフィルタ English ログアウト

有効にする

モード 拒否

URLアドレス

追加

URLアドレス	削除
データエントリがありません。	

- 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。

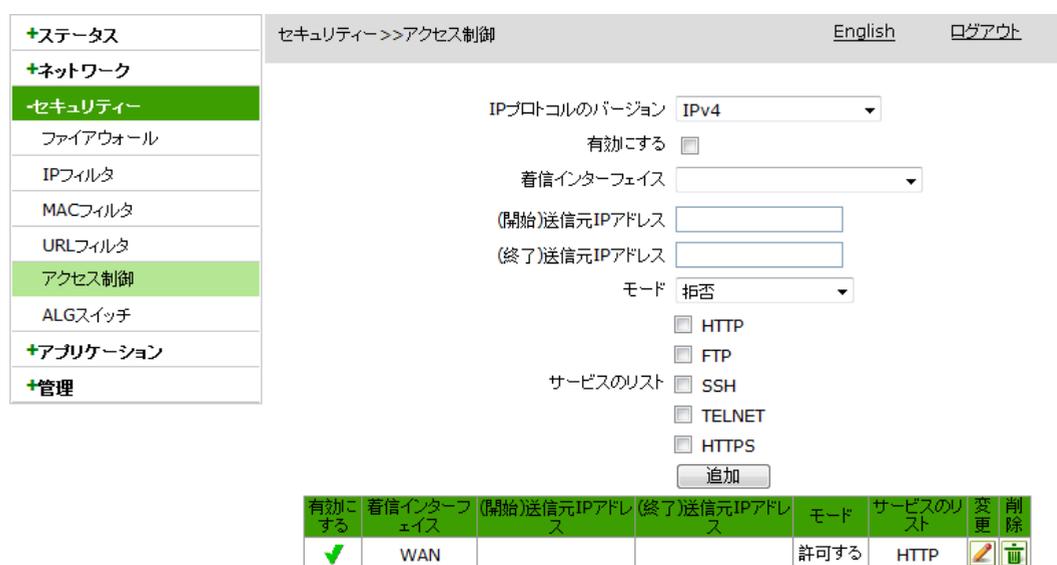
パラメータ	説明
有効にする	チェックを入れるとURLフィルタが有効になります。
モード	<input type="checkbox"/> 拒否 <input type="checkbox"/> 許可
URLアドレス	フィルタリングが必要なURLアドレスです。このパラメータは空欄にすることが出来ません。

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。

## 5.5 アクセス制御の設定

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

1. WEB画面の左側メニューでセキュリティ > アクセス制御を選択すると、アクセス制御画面に進みます。



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

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。
着信インターフェイス	サービスの送信元です。
(開始)送信元/ (終了)送信元	サービス制御が必要なIPセクションです。

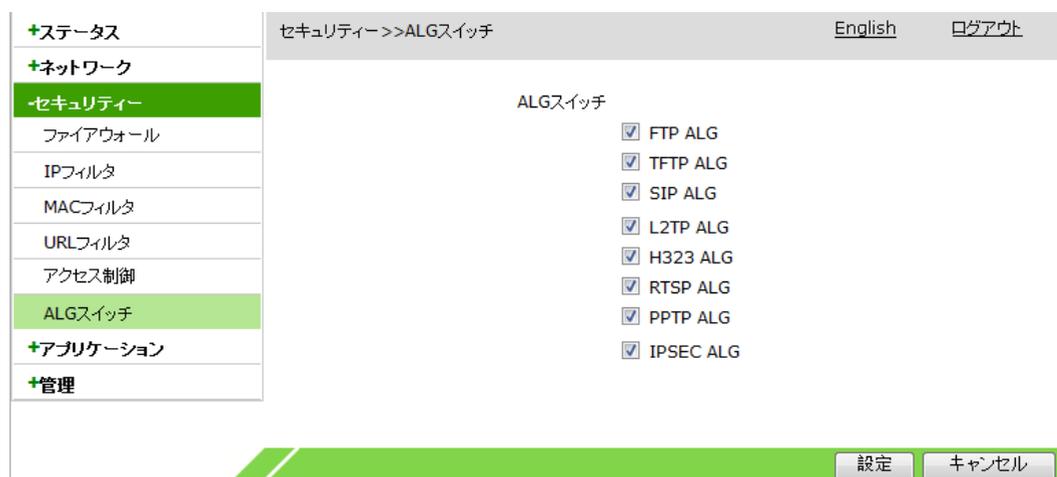
パラメータ	説明
IPアドレス	
モード	<input type="checkbox"/> 拒否 <input type="checkbox"/> 許可
サービスのリスト	制御するサービスです。以下の種類から選択できます。 <input type="checkbox"/> HTTP <input type="checkbox"/> FTP <input type="checkbox"/> SSH <input type="checkbox"/> TELNET <input type="checkbox"/> HTTPS
リモートアクセスポートを変更	リンクをクリックしてサービスのアクセスポートを変更します。

- (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。

## 5.6 ALG スイッチの設定

本操作でALGスイッチをオンにすることにより、ZXHN F260Aがメッセージのプライベートネットワークアドレスをパブリックネットワークアドレスに変更し、外部ネットワークからプライベートネットワークアドレスを分からなくなり、セキュリティ性を向上させます。

- WEB画面の左側メニューでパスセキュリティ > 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。



- オンする対象のALGスイッチにチェックを入れると、該当プロトコルのALGスイッチをオンにし、**設定ボタン**をクリックします。

## 6 アプリケーション設定

### 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。

アプリケーション>>DMZ English ログアウト

有効にする

IPv4

WAN接続

MACアドレスのマッピングを有効にする

LANのIPアドレス

IPv6

最大8アドレス

LANのIPv6アドレス

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アドレス設定が必要です。 <input type="checkbox"/> MACアドレスのマッピングを有効にしている場合、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 MACアドレス	LAN側本体の対外サービス提供時にマッピングするMACアドレスです。

パラメータ	説明
LANのIPアドレス	LAN側本体の対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側本体の対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表を参照してください。

パラメータ	説明
UPnPを有効	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。
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

パラメータ	説明
	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すすみます。

The screenshot displays the web interface for UPnP Port Mapping. On the left, a navigation menu is visible with 'アプリケーション' expanded and 'UPnPポートマッピング' selected. The main content area shows the title 'アプリケーション>>UPnPポートマッピング' and a table titled 'UPnPポートマッピングテーブル'. The table has six columns: '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', and '削除'. The table is currently empty, displaying the message 'データエントリがありません。' (No data entries). A '更新' (Refresh) button is located at the bottom right of the page.

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側をクライアントがLAN側にアクセスするサーバと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。

アプリケーション>>仮想ホスト

English ログアウト

+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

仮想ホスト

+DNSサービス

SNTP(時刻同期)

USBストレージ

メディア共有

FTPアプリケーション

ポートトリガー

ポートフォワーディング(アプリケーションリスト)

アプリケーションリスト

ホーム共有(samba)

+管理

有効にする

名前

プロトコル TCP

(開始)外部ホストIPアドレス

(終了)外部ホストIPアドレス

WAN接続 omci ipv4 dhcp 1

(開始)外部ポート番号  (1 ~ 65535)

(終了)外部ポート番号  (1 ~ 65535)

MACアドレスのマッピングを有効にする

内部ホストのIPアドレス

(開始)内部ポート番号  (1 ~ 65535)

(終了)内部ポート番号  (1 ~ 65535)

追加

有効にする	名前	(開始)外部ホストIPアドレス	(開始)外部ポート番号	(開始)内部ポート番号	WAN接続	変更	削除
	プロトコル	(終了)外部ホストIPアドレス	(終了)外部ポート番号	(終了)内部ポート番号	仮想ホストのアドレス		

データエントリがありません。

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下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	必要な設定項目です。ここに仮想ホストの名前を入力してください。
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側のホストの開始IPアドレスと及WAN側のホストの終了IPアドレスです。
(終了)外部ホストIPアドレス	IPアドレスの設定により、FTPサーバへアクセスする外部設備を制限できます。 この項目を設定しない場合は、全ての外部設備がFTPサーバへアクセスすることができるようになります。
WAN接続	必要な設定項目です。該当仮想ホストの関連WAN接続です。デフォルトモードとなります。
(開始)外部ポート番号	

パラメータ	説明
(終了)外部ポート番号	<p>必要な設定項目です。</p> <p>開始ポート番号と終了ポート番号の設定により、FTPサーバへ外部設備がアクセスするポート番号を制限できます。</p> <p>ポート番号の制限を行わない場合は、開始ポート番号を1、終了ポート番号を65535と設定してください。</p> <p>例: 開始ポート番号と終了ポート番号両方とも2121と設定した場合、外部設備からFTPサーバへアクセスポートは2121のみとなります。</p>
MACアドレスのマッピングを有効にする	<p>【仮想ホストIPアドレス】オプションとは何れかを選択してください。</p> <p>【MACマッピングを有効にする】を選択する場合、FTPサーバのMACアドレスを設定する必要があります。</p> <p>MACマッピング機能とは、ZXHN F260Aではこの項目で設定されたFTPサーバのMACアドレスとFTPサーバに接続したままにする機能です。</p> <p>例: ここにFTPサーバのMACアドレスをこのように入力します: 00-1B-FC-F7-DA-01。</p>
仮想ホストのMACアドレス	
内部ホストのIPアドレス	<p>【MACマッピングを有効にする】を選択しない場合は、ここでFTPサーバのIPアドレスを設定する必要があります。ZXHN F260Aではここで設定されたFTPサーバのIPアドレスとFTPサーバとの接続状態を維持します。</p>
(開始)内部ポート番号	<p>必要な設定項目です。設定情報はFTPサーバ上のポート設定と一致していること。</p> <p>FTPサーバ上のFTPサービスポート番号は21と設定された場合、こちらを21と設定すること。</p>
(終了)内部ポート番号	

- (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。
- (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

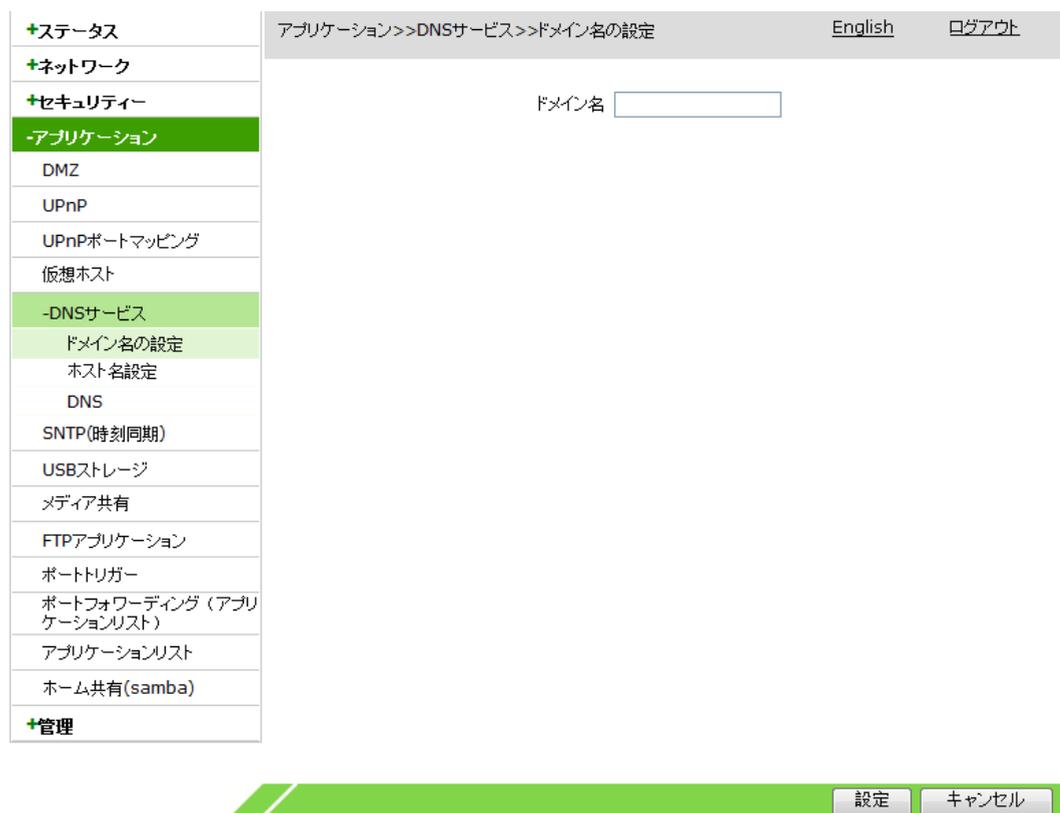
ZXHN F260AのDNSサービスの設定は以下の内容が含まれます。

- ・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、ZXHN F260Aを関連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>ドメイン名の設定を選択すると、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、ホスト名設定画面に進みます。

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

ホスト名

IPアドレス

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。			

+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

仮想ホスト

-DNSサービス

ドメイン名の設定

**ホスト名設定**

DNS

SNTP(時刻同期)

USBストレージ

メディア共有

FTPアプリケーション

ポートリガー

ポートフォワーディング(アプリケーションリスト)

アプリケーションリスト

ホーム共有(samba)

+管理

アプリケーション>>DNSサービス>>ホスト名設定

ホスト名

IPアドレス

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。			

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

グローバル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の機能をグローバル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設定画面に進みます。

+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			
-アプリケーション			
DMZ			
UPnP			
UPnPポートマッピング			
仮想ホスト			
-DNSサービス			
ドメイン名の設定			
ホスト名設定			
DNS			
SNTP(時刻同期)			
USBストレージ			
メディア共有			
FTPアプリケーション			
ポートリガー			
ポートフォワーディング(アプリケーションリスト)			
アプリケーションリスト			
ホーム共有(samba)			
+管理			

IPv4 DNSサーバー1

IPv4 DNSサーバー2

IPv6 DNSサーバー1

IPv6 DNSサーバー2

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)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			
仮想ホスト			
+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	1970-01-01 02:06:42
タイムゾーン	(GMT+09:00) 大阪、札幌、東京、ソウル
プライマリSNTPサーバアドレス	<input type="text"/>
セカンダリSNTPサーバアドレス	<input type="text"/>
同期間隔	86400 秒

設定	キャンセル
----	-------

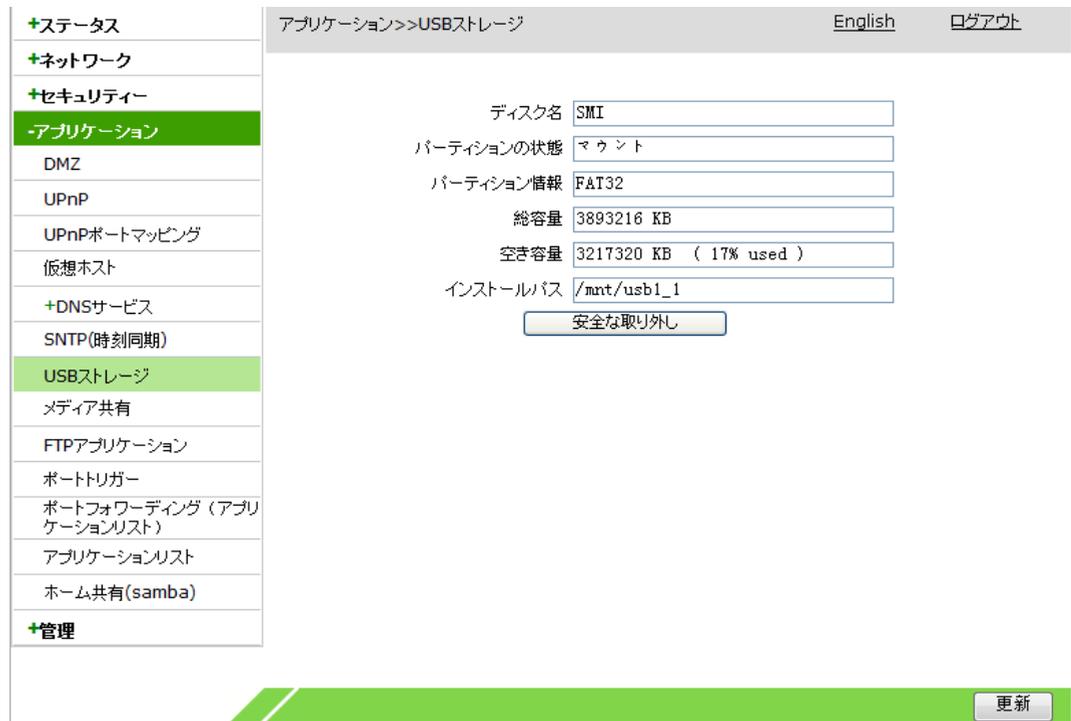
2. SNTPパラメータを設定し、設定ボタンをクリックします。SNTPのパラメータは下表を参照ください。

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。

## 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設備のストレージ容量を確認します。

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、下図のとおり、USBストレージ画面に進みます。



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 FTP サーバの設定

本操作ではFTPパラメータを設定し、ZXHN F260Aの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アプリケーション>FTPアプリケーションを選択すると、FTPアプリケーション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	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			
仮想ホスト			
+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			

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のパラメータについての説明は下表をご参照ください。

パラメータ	説明
FTPサーバを有効にする	チェックを入れると、FTPサーバを有効にします。
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セキュリティ機能が有効である場合にのみ設定できます。

## 6.9 ポートトリガーの設定

本操作では指定されてポートをポートトリガーに設定することにより、システム上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する際に、デバイスに接続されている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

ポートトリガーは保護が必要なポートに用います。システムから直接にポートを開放する必要がなく、トリガーが必要とされた場合のみに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
- +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
- 仮想ホスト
- +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

アプリケーション>>ポートトリガー
English
ログアウト

有効にする

アプリケーション名

トリガー側のIPアドレス

サービスの種類 TCP

トリガーポート

接続 TCP

(開始) WANポート

(終了) WANポート

タイムアウト  (60~1800秒)

アプリケーション名	有効にする	サービスの種類	トリガー側のIPアドレス	(開始) WANポート	(終了) WANポート	変更	削除
データエントリがありません。							

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

ポートトリガーのパラメータについては下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を有効にします。
アプリケーション名	このポートトリガーの名前です。
トリガー側の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タイプです。 <input type="checkbox"/> TCP(デフォルト値) <input type="checkbox"/> UDP <input type="checkbox"/> TCP AND UDP
トリガーポート	アクセスするトリガーポートです。このパラメータは空欄にしないこと。
接続	外部ルータとの接続プロトコルです。以下のプロトコルをサポートしています。 <input type="checkbox"/> TCP(デフォルト値) <input type="checkbox"/> UDP <input type="checkbox"/> TCP AND UDP
(開始)WANポート (終了)WANポート	トリガー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。デバイスがトリガー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

パラメータ	説明
	は有効になります。このパラメータは空欄にしないこと。また、開始ポートと終了ポート間の差は1から9の間にするこ と。
タイムアウト	一定時間内にデータフローがない場合、タイムアウトとなり 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。

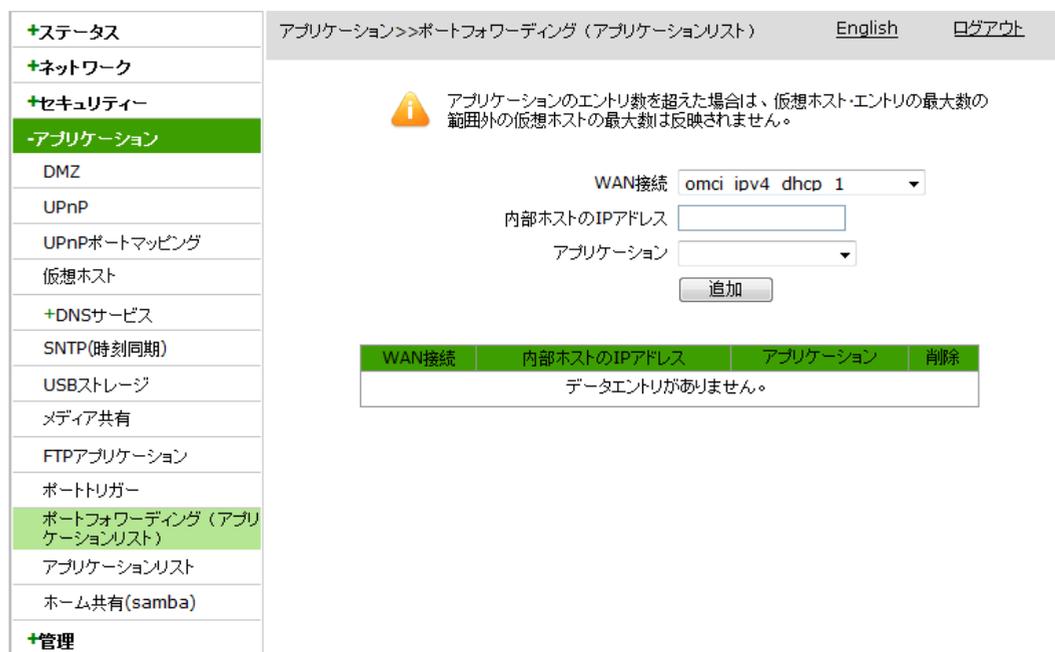
## 6.10 ポートフォワーディング(アプリケーションリスト)の設定

本操作では仮想ホストを設定することにより、WAN側をクライアントがLAN側へアクセスするサーバとします。

### 事前確認事項

アプリケーションリストの設定が完了され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>ポートフォワーディング(アプリケーションリスト)を選択すると、ポートフォワーディング(アプリケーションリスト)の設定画面に進みます。



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

 アプリケーションのエントリ数を超えた場合は、仮想ホスト・エントリの最大数の範囲外の仮想ホストの最大数は反映されません。

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。			

- 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際のWAN接続です。
内部ホストのIPアドレス	LAN側設定されたホストのIPアドレスです。
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。

## 6.11 アプリケーションリストの設定

本操作はアプリケーションリストを設定することにより、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(アプリケーションリスト)など他の機能から呼び出せるようになります。

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



The screenshot shows the web interface for configuring application lists. On the left, a sidebar menu is visible with the following 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 (highlighted), DMZ, 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, 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 (highlighted), ホーム共有(samba), +管理. The main content area is titled 'アプリケーション>>アプリケーションリスト' and includes a link: [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。](#) Below the link is a table with the following structure:

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。		

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**」というリンクをクリックして、アプリケーションの追加画面に進みます。

<b>+ステータス</b>	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														
<b>+ネットワーク</b>	アプリケーション名 <input type="text" value="App1"/> (1~256文字)																
<b>+セキュリティ</b>	<input type="button" value="保存"/>																
<b>-アプリケーション</b>	プロトコル <input type="text" value="TCP"/>																
DMZ	(開始) WANポート <input type="text"/>	(1 ~ 65535)															
UPnP	(終了) WANポート <input type="text"/>	(1 ~ 65535)															
UPnPポートマッピング	(開始) マッピングポート <input type="text"/>	(1 ~ 65535)															
仮想ホスト	(終了) マッピングポート <input type="text"/>	(1 ~ 65535)															
<b>+DNSサービス</b>	<input type="button" value="追加"/>																
SNTP(時刻同期)	<table border="1"> <thead> <tr> <th>プロトコル</th> <th>(開始) WANポート</th> <th>(終了) WANポート</th> <th>(開始) マッピングポート</th> <th>(終了) マッピングポート</th> <th>変更</th> <th>削除</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>			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。						
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。																	
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)																	
<b>アプリケーションリスト</b>																	
ホーム共有(samba)																	
<b>+管理</b>																	

3. アプリケーションリストに関するパラメータを設定し、**保存ボタン**をクリックし、ポートフォワーディングリスト(アプリケーションリスト)の名前が保存され、**追加ボタン**をクリックして設定を完了します。

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														
アプリケーション名 <input type="text" value="App1"/> (1 ~ 256)																
<input type="button" value="変更"/>																
プロトコル <input type="text" value="TCP"/>																
(開始) WANポート <input type="text"/>	(0 ~ 65535)															
(終了) WANポート <input type="text"/>	(0 ~ 65535)															
(開始) マッピングポート <input type="text"/>	(0 ~ 65535)															
(終了) マッピングポート <input type="text"/>	(0 ~ 65535)															
<input type="button" value="追加"/>																
<table border="1"> <thead> <tr> <th>プロトコル</th> <th>(開始) WANポート</th> <th>(終了) WANポート</th> <th>(開始) マッピングポート</th> <th>(終了) マッピングポート</th> <th>変更</th> <th>削除</th> </tr> </thead> <tbody> <tr> <td>TCP</td> <td>10</td> <td>20</td> <td>30</td> <td>40</td> <td></td> <td></td> </tr> </tbody> </table>			プロトコル	(開始) WANポート	(終了) WANポート	(開始) マッピングポート	(終了) マッピングポート	変更	削除	TCP	10	20	30	40		
プロトコル	(開始) WANポート	(終了) WANポート	(開始) マッピングポート	(終了) マッピングポート	変更	削除										
TCP	10	20	30	40												

アプリケーションリストパラメータについての説明は下表をご参照ください。

パラメータ	説明
アプリケーション名	アプリケーションの名前です。

パラメータ	説明
プロトコル	プロトコル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(デフォルト値) <input type="checkbox"/> UDP <input type="checkbox"/> TCP AND UDP
WAN開始ポート/ WAN終了ポート	下りにおいてパケットの初期プロトコルポート番号の範囲です。
開始ポート/ 終了ポート	下りにおいて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。

## 6.12 Samba サービスの設定

SambaはSMBプロトコルを実現する一種のSWです。ZXHN F260AのSambaサーバを再起動することにより、LinuxとWindows間にファイル交換を可能にします。SMBプロトコルはローカルエリアネットワーク上の共有ファイル/プリンターについてのプロトコルの一種とも言えます。ネットワーク内部においてその他のWindowsとLinux機器にファイルシステム、プリンターサービスや他の情報を提供します。

- 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)**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			
仮想ホスト			
+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			

Sambaサーバを有効

自動的にSambaサーバを実行する

ホスト名  (2~15文字)

匿名アクセス

Sambaログインユーザ名  (1 ~ 32文字)

Sambaログインパスワード  (0 ~ 32文字)

2. Sambaサーバパラメータを設定して、「設定」ボタンをクリックします。

Sambaサーバパラメータについての説明は下表をご参照ください。

パラメータ	説明
Sambaサーバを有効	チェックを入れるとSambaサーバ機能を有効にします。チェックを入れない場合はSambaサーバ機能を無効にします。この項目を空欄にする場合、該当機能は無効となり、「Sambaサーバ自動稼動」とは相互に排他的な項目です。
自動的にSambaサーバを実行する	チェックを入れて、ONUのUSB挿入ポートにUSBストレージデバイスを差し込んだ後、Sambaサーバは自動稼動モードとなります。USBストレージを取り外すと、Sambaサーバは稼動停止となります。この項目を空欄にする場合、該当機能は無効となり、「Sambaサーバを有効にする」とは相互に排他的な項目です。
ホスト名	Sambaサーバの名前です。値の範囲は2~15文字です。
匿名アクセス	チェックを入れると匿名アクセス機能を有効にします。この場合では、Sambaログインユーザ名を入力する必要はありません。
Sambaログインユーザ名	Sambaサーバのログインユーザ名です。Sambaサーバ上の設定データと一致していること。
Sambaログインパスワード	Sambaサーバのログインパスワードです。Sambaサーバ上の設定データと一致していること。

3. Sambaサーバを起動後、PC はLAN側から「¥¥Sambaサーバ名」でSambaサーバへのアクセスができるようになります。



## 7 管理設定

### 7.1 ユーザ管理設定

ZXHN F260Aではアカウントの管理/運用保守ができます。WEBユーザはWEBユーザ管理画面でアカウントやパスワード等のユーザ管理を行うことが可能です。

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

管理>>ユーザ管理>>WEBユーザ管理 English ログアウト

ユーザ名

古いパスワード

新しいパスワード

新しいパスワードの確認

設定 キャンセル

2. ユーザアカウントパラメータを設定して、**設定ボタン**をクリックします。

ユーザアカウントパラメータについての説明は下表を参照してください。

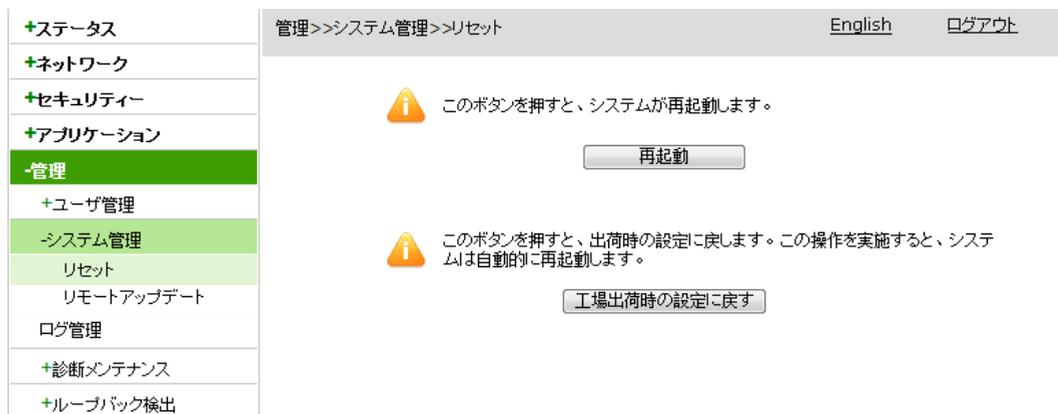
パラメータ	説明
ユーザ名	システムアドミンユーザ名/一般ユーザ名となります。
旧パスワード	システムのデフォルトアドミンアカウントのパスワードです。
新パスワード	ユーザによりパスワードを設定します。
新パスワード確認	入力内容が新しいパスワードと一致しているかご確認ください。

### 7.2 デバイス管理

#### 7.2.1 システム管理

システム管理により、ZXHN F260Aを再起動し、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、**リセット設定画面**に進みます。

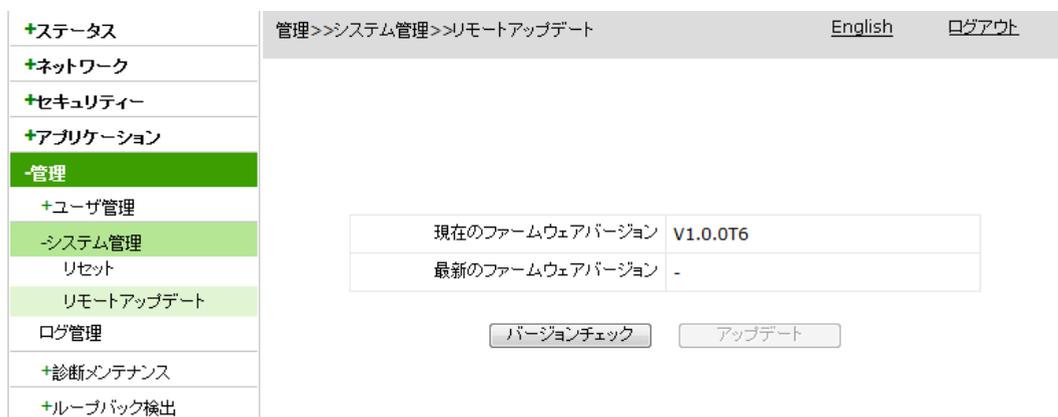


2. 「再起動」ボタンをクリックすると、本製品が自動で再起動します。
3. 「工場出荷時の設定に戻す」ボタンをクリックすると、本工場出荷時設定に復元して再起動します。

## 7.2.2 リモートアップデート設定

サービス提供元から新しいファームウェアが提供される場合、リモートアップグレード機能を利用してONUをアップデートすることができます。リモートアップデートが完了するとONUは自動的に再起動されます。リモートアップデート中はONUの電源を切らないよう注意してください。もし、リモートアップデート中に電源を切った場合は、ONUが正常に動作できなくなる恐れがあります。

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



2. バージョンチェックボタンをクリックすると、現在利用しているバージョンとサーバ上の最新バージョンが表示されます。サーバ上に最新バージョンがある場合、アップデートボタンが有効になります。

## 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ことや、ログをリモートサーバ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。

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の説明は下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デバッグ、情報、通知、注意、エラー、クリティカル、警告、緊急となります。ログレベルの設定が完了後、選択されたレベルまたはそれ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にする	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)ログをクリアボタンをクリックすると、テキストボックスに表示中のログがクリアされます。
5. (オプション)ログをダウンロードするボタンをクリックすると、ログをローカルにダウンロードできます。

## 7.4 診断メンテナンス

### 7.4.1 Ping 診断設定

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。

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診断パラメータについての説明は下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の送信先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接続されているのを検知され場合は、関連する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、(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 > traceroute診断**を選択すると、Trace Route診断画面に進みます。

- 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診断が始まります。

Trace Route診断のパラメータについての説明は下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の宛先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接続されているのを検知され場合は、関連するWAN接続も選択する必要があります。
最大ホップ数	Trace Route診断のパケットが目的地までに経る最大ホップ数です。
タイムアウト	応答パケットの待機時間です。この時間を超えて応答パケットが受信されない場合、星印が表示されます。星印の表示が続いている場合、該当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プロトコルです。

## 7.5 ループバック検出

### 7.5.1 基本パラメータの設定

本操作は、ポートやケーブルの問題を検出と解析するためのループバック検出用の全局パラメータを設定します。

- WEB画面の左側メニューで**管理>ループバック検出>基本構成**を選択すると、**基本構成画面**に進みます。

管理 >> ループバック検出 >> 基本構成 English [ログアウト](#)

宛先MAC:  ブロードキャストアドレス  BPDUマルチキャストアドレス

イーサネットタイプ  (16進数 0000 - ffff)

パケット間隔を検出  (100 - 1000)ミリ秒

ポートの閉鎖時間  (60 - 300)秒

ループ回復時間  (5 - 300)秒

2. ループバック検出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。

ループバック検出のパラメータについての説明は下表を参照してください。

パラメータ	説明
宛先MAC	ブロードキャストアドレスまたはBPDUマルチキャストアドレス。
イーサネットタイプ	検出対象ポートがループバックにより送信されたイーサネットタイプであることを確認用です。
パケット間隔を検出	ループバック診断による検出パケット送信時間の間隔です。
ポートの閉鎖時間	ループバックポートが検出された際に、そのポートの閉鎖時間です。
ループ回復時間	ループバックが消えたのかの確認用の時間です。該時間内、検出パケットが受信されていない場合は、ループが消えたと確認できます。

## 7.5.2 ポート機能の設定

本操作は、ポートのループバック検出機能を有効にし、アラームの発報機能を有効に、ポート自動閉鎖機能を無効にします。

1. WEB画面の左側メニューで**管理>ループバック検出>設定の有効化**を選択すると、**設定の有効化画面**に進みます。

<ul style="list-style-type: none"> <li>+ステータス</li> <li>+ネットワーク</li> <li>+セキュリティ</li> <li>+アプリケーション</li> <li>-管理</li> <li>+ユーザ管理</li> <li>+システム管理</li> <li>ログ管理</li> <li>+診断メンテナンス</li> <li>-ループバック検出 <ul style="list-style-type: none"> <li>基本構成</li> <li>設定の有効化</li> <li>VLAN設定</li> </ul> </li> </ul>	管理 >> ループバック検出 >> 設定の有効化			English	ログアウト	
	ポート	ループバック検出が有効になっている	アラームが有効	ポート自動シャットダウン有効		
	LAN1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
	LAN2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
	LAN3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
	LAN4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
	LAN5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
						<input type="button" value="設定"/> <input type="button" value="キャンセル"/>

2. 検出対象のポートのチェックを入れて、設定ボタンをクリックします。

**注意:**

ZXHN F260Aはデフォルトではアラームのポート自動シャットダウン機能は有効になっています。

「アラームが有効」機能は、ループバックが検出された際に、アラームが報告されるかどうかの制御をする機能です。

「ポート自動シャットダウン」機能は、ループバックが検出された際に、ポートがポート自動シャットダウンにするための機能です。

## 7.5.3 VLAN 設定

本操作は、ポートのVLANループバック検出機能を有効にします。

1. WEB画面の左側メニューで管理>ループバック検出>VLAN設定を選択すると、VLAN設定画面に進みます。

<ul style="list-style-type: none"> <li>+ステータス</li> <li>+ネットワーク</li> <li>+セキュリティ</li> <li>+アプリケーション</li> <li>-管理</li> <li>+ユーザ管理</li> <li>+システム管理</li> <li>ログ管理</li> <li>+診断メンテナンス</li> <li>-ループバック検出 <ul style="list-style-type: none"> <li>基本構成</li> <li>設定の有効化</li> <li>VLAN設定</li> </ul> </li> </ul>	管理 >> ループバック検出 >> VLAN設定			English	ログアウト	
	ポート	LAN1	VLAN	<input type="text" value=""/>	(1 - 4094)	
	<input type="button" value="追加"/>					
	ポート	VLAN	修正	削除		
	データエントリがありません。					

2. ループバック検出対象ポートを選択してVLAN IDを設定し、「追加」ボタンをクリックします。

3. (オプション)ポート項目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)ポート項目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。

## 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  
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, 隔離ゾーン  
DNAT – Destination Network Address Translation, 宛先ネットワークアドレス変換  
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, ローカルエリアネットワーク  
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  
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プロトコル  
PPPoE – Point to Point Protocol over Ethernet, イーサネットフレーム上にポイントツー  
ポイントプロトコル  
RA – Routing Area, ルーティングエリア  
RIP – Routing Information Protocol, ルーティング情報プロトコル  
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  
SMB – Server Message Block, サーバメッセージブロック  
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 プロテクトドセットアップ