

H3701Q Wi-Fi7 取扱説明書

改版履歴

版数番号	改版日	改版内容	改版者
R1.0	2025-04-08	初版	First edition

シリアル番号: SJ-20240318144432-004

リリース日: 2025-04-08 (R1.0)

目次

1	はじめに.....	5
2	安全上の注意.....	6
3	エージェントモード.....	7
3.1	管理システムへのログイン.....	7
3.2	ローカルネットワークの設定.....	12
3.2.1	無線LANの状態の確認.....	12
3.2.2	無線LANの設定.....	14
3.2.3	LANの設定.....	17
3.3	管理と診断の設定.....	18
3.3.1	アカウント管理の設定.....	18
3.3.2	アイドルタイムアウトの設定.....	19
3.3.3	システム管理設定.....	20
3.3.4	ログ管理.....	23
3.3.5	診断.....	26
3.3.6	動作モード設定.....	30
4	コントローラー (ルーター)モード.....	31
4.1	管理システムへのログイン.....	31
4.2	トポロジー情報の参照.....	34
4.3	インターネット接続設定.....	35
4.3.1	インターネット接続確認.....	35
4.3.2	セキュリティ設定.....	36
4.3.3	時刻の設定.....	41
4.3.4	マルチキャスト設定.....	42
4.4	LAN接続の設定.....	43
4.4.1	ステータスの確認.....	43
4.4.2	無線LANの設定.....	45
4.4.3	LANの設定.....	57
4.4.4	ルーティングの設定.....	61
4.5	管理と診断の設定.....	66

4.5.1 アカウント管理の設定	66
4.5.2 アイドルタイムアウトの設定	67
4.5.3 システム管理設定	68
4.5.4 ログ管理	72
4.5.5 診断	75
4.5.6 動作モード設定	78
5 よくある質問	80
図	81
表	83
用語、略語	85

1 はじめに

H3701Qシリーズの機能、特徴、準備、手順について説明します。

内容

本取扱説明書の主な内容は以下のとおりです：

章名	概要
1 はじめに	本製品の環境要件、クリーニング要件、および注意事項について説明します。
2 安全上の注意	本製品の安全注意事項について説明します。
3 エージェントモード	エージェント モードで本製品のローカル ネットワーク、管理、および診断機能を構成する方法について説明します。
4 コントローラーモード	本製品のトポロジ、ローカルネットワーク構成、管理、および診断機能をコントローラー（ルータ）モードで実行する方法について説明します。
5 よくある質問	本製品の一般的な問題に対する対策と手順について説明します。

シンボル

このマニュアルで使用されているシンボルと意味は次のとおりです：

シンボル	シンボルの意味
	本文に関する補足説明やヒントです。

2 安全上の注意



注:

本製品を使用および操作する前に、本製品を安全にお使いいただくために、以下の安全上の注意事項をかならずお読みください。

- 本製品に添付している電源アダプタ（ACアダプタ、電源コード）をお使いください。
- アダプタの電源ケーブルを変更したり、延長したりしないでください。ショートや電源異常などの安全上のリスクが生じる可能性があります。
- 感電やその他の危険を避けるため、電源プラグを乾燥した清潔な状態に保ってください。
- 本製品を分解しないでください。本製品の損傷や電源を入れたときに感電の危険があります。
- 万が一、使用中に煙、異常な音、異常な匂いが発生した場合には、本製品の使用を中止し、すぐに電源プラグを抜いてください。

使用環境要件

- 本装置を風通しの良い場所に置き、直射日光を避けて保管してください。周囲の温度が高すぎると、装置に障害が発生したり、装置の耐用年数が短くなったりする可能性があります。
- 水濡れによるショートを防ぐため、デバイスを乾燥した状態に保ってください。
- 本製品の変形や損傷を防ぐため横置きや重ね置きをしないでください。
- 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（電磁レンジ、スピーカー、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）への設置はさけてください。

環境保護

- 本製品を使用しないときは、電源を切り、電源プラグを抜いてください。
- 本製品機器や付属の電源アダプタを不適切に廃棄しないでください。
- 機器の廃棄や処理に関しては使用される地域の規則を守ってください。

クリーニング手順

- お手入れの際は、本体の電源を切り、電源ケーブル、本体に接続されているすべてのケーブルを抜いてください。
- 清掃時には液体やスプレーを使用しないでください。柔らかい乾いた布で拭いてください。

3 エージェントモード

この章には次のトピックが含まれます。

- 管理システムへのログイン
- ローカルネットワークの構成
- 構成管理と診断

エージェントモード: AP（アクセスポイント）としてコントローラー機器とWi-Fiメッシュ接続を行い、Wi-Fi の範囲を拡張できます。

3.1 管理システムへのログイン

本製品は、Web ページに基づく構成および管理機能をサポートしています。一連の構成および管理操作を実行するには、ブラウザからデバイス管理システムにログインしてください。これらの操作には、機器のステータスの確認、ネットワーク設定の変更、ワイヤレス ネットワークの管理、ソフトウェア バージョンの更新、トラブルシューティング、ログの表示などが含まれますが、これらに限定されません。本製品はエージェント モードで動作し、管理アドレスはアップリンクのルーター(H8748Q など) のトポロジで表示されます。

前提条件

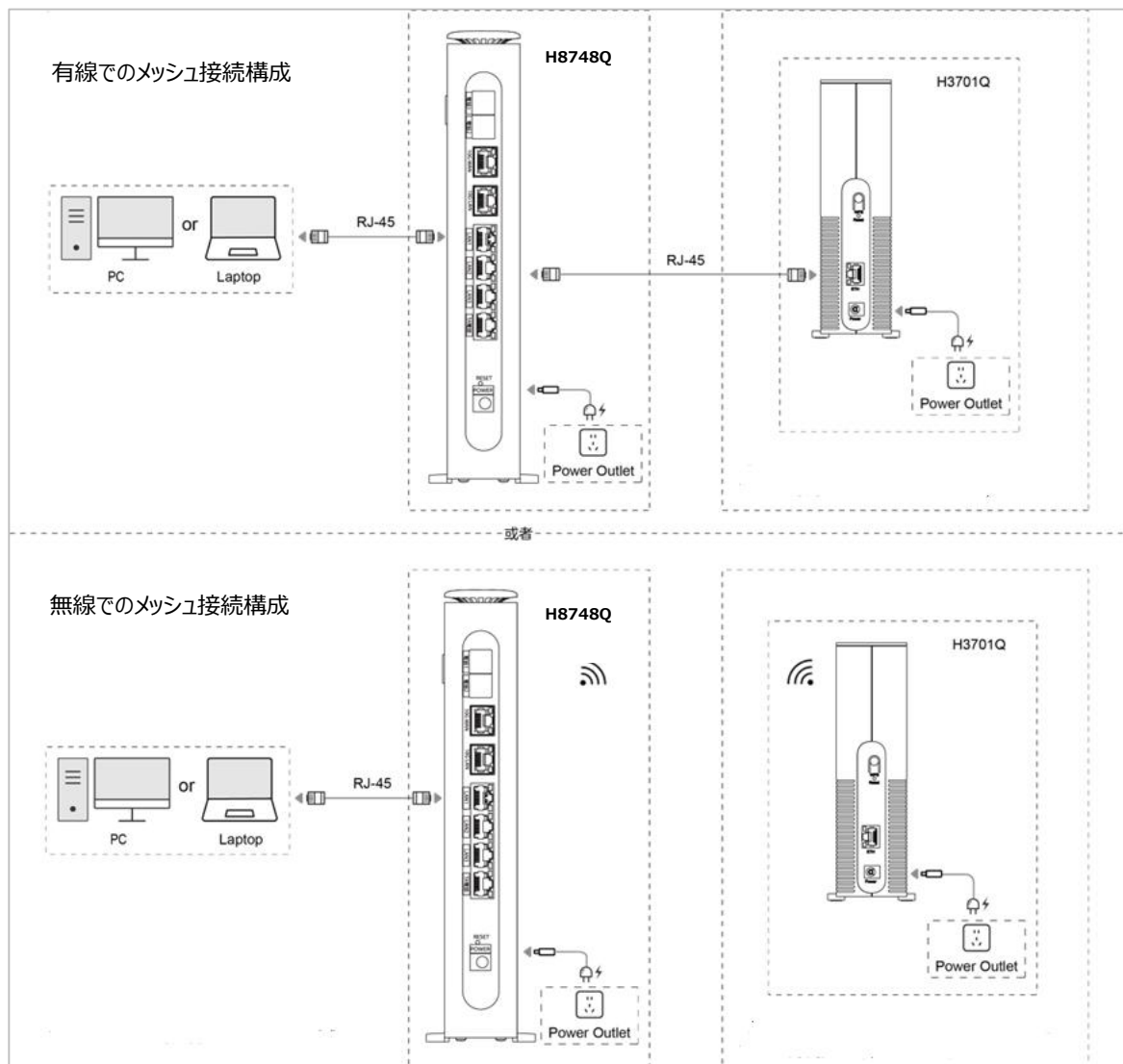
- 実行中のファイアウォールまたはセキュリティソフトウェアがすべてオフの状態
- ブラウザのプロキシサーバがオフの状態

手順

H3701Qハードウェア接続の構成

1. デスクトップ型パソコンやノートパソコンをH8748Qへ接続して本製品の管理システムに接続します。ハードウェア接続図を[図2-1](#)に示します。

図 3-1 H3701Q ハードウェア接続図 (エージェントモード)



H8748Q (メッシュ : コントローラー) の管理ページにログインします。

2. ブラウザのアドレスバーに <http://192.168.1.1> を入力してEnterを実行してください。(192.168.1.1 はデフォルトの管理アドレスになります。)接続するH8748Qのログイン画面を表示します。ログインページを 図3-2に示します。

図 3-2 H8748Qログインページ



H8748Qの初期パスワードは、H8748Q本体ラベルに記載されています。

3. ユーザー名（admin）とパスワードを入力後、「ログイン」ボタンをクリックするとH8748QのWeb管理画面を表示します。管理画面のトポロジーをクリックしてトポロジー画面を表示してください。図3-3を参照してください。

図 3-3 トポロジー画面 (本製品接続時)

MEGA EGG 現在時刻:1970-01-01T00:23 admin ログアウト 日本語 | English

ホーム トポロジー インターネット LAN 管理&診断

トポロジー画面 (本製品接続時)

ZTE:H8748Q V...
MAC: 00:19:c6:51:00:24
IP: 192.168.1.1

ZTE:H3701Q
MAC: 20:3a:eb:de:1f:20
IP: 192.168.1.3

▼ すべてのAP

AP名	IP	MAC	モード	バックホール	操作エリア
ZTE:H8748Q V2	192.168.1.1	00:19:c6:51:00:24	controller	/	修正
ZTE:H3701Q	192.168.1.3	20:3a:eb:de:1f:20	agent	ETH	修正

▼ すべてのクライアント

クライアント名	接続先デバイス	関連バンド	RSSI	操作エリア
A23866605	controller	ETH	/	修正

4. こちらの画面でエージェントモードの本製品のIPアドレスを参照できます。

H3701Q (エージェントモード)管理画面へのログイン

5. ブラウザのアドレスバーに、本製品の管理アドレス (図3-3の接続例ではH8748Qから192.168.1.3が割り当てられています) を入力し、Enterキーを押してください。本製品のログイン ページが表示されます。図3-4 を参照してください。

図 3-4 H3701Q (エージェントモード)ログインページ



6. ユーザー名 (admin) と初期パスワード (初期パスワードは本体ラベルに記載されています) を入力した後、「ログイン」ボタンをクリックしてください。初回接続では新パスワードの設定ページに入ります。図3-5を参照してください。

図 3-5 H3701Q (エージェントモード) パスワード変更画面



7. 新しいパスワードを設定し、「設定」ボタンをクリックして、ログインページに戻ります。
8. 再度ユーザー名、パスワードを入力してエージェントモードの本製品の管理ページにログインします。図3-6を参照してください。

図 3-6 H3701Q (エージェントモード) 管理画面



3.2 ローカルネットワークの設定

3.2.1 無線LANの状態の確認

無線LANのステータスを確認する方法について説明します。

- 無線LANの状態を確認することで、無線LANの状態情報を取得できます。
- 無線LANクライアントのステータスを表示することで、ユーザーは、デバイスの数、接続ステータス、信号強度など、無線ネットワークに接続されているクライアントデバイスに関する詳細情報を取得できます。

手順

無線LANの状態確認

1. Web管理メインページで、メニュー[LAN] > [ステータス] > [無線LANステータス]を選択して、無線LANステータスページに入ります。図3-7を参照してください。

図 3-7 無線LANステータスページ

▼ 無線LANステータス			
無線LAN基本ステータス			
無線LAN (2.4GHz)	オン	チャンネル (2.4GHz)	1
無線LAN (5GHz)	オン	チャンネル (5GHz)	100
無線LAN (6GHz)	オン	チャンネル (6GHz)	5
2.4GHz-Pri			
SSID名	egg-E1F20	MACアドレス	20:3a:eb:de:1f:21
SSIDスイッチ	オン	受信パケット数 / 送信パケット数	0/0
暗号化タイプ	WPA2-PSK/WPA3-SAE	受信バイト数/送信バイト数	0/0
2.4GHz-Sec			
SSID名	egg-2g-E1F20	MACアドレス	26:3a:eb:de:1f:21
SSIDスイッチ	オン	受信パケット数 / 送信パケット数	800/568
暗号化タイプ	WPA2-PSK-AES	受信バイト数/送信バイト数	63882/49911

2. 「更新」ボタンをクリックして最新の情報を取得します。

無線LANクライアントのステータスの確認

1. Web管理メインページで、メニュー[LAN] > [ステータス] > [無線LANクライアントステータス] を選択して、無線LANクライアントステータスページに入ります。図3-8を参照してください。

図 3-8 無線LANクライアントステータスページ

▼ 無線LANクライアントステータス			
クライアント-1			
SSID	SSID5	名前	DESKTOP-69HGB00
IPv4アドレス	192.168.0.2	MACアドレス	c8:09:a8:6d:24:dc
IPv6アドレス			
アクセスモード			
更新			

2. 「更新」ボタンをクリックして最新の情報を取得します。

3.2.2 無線LANの設定

3.2.2.1 アクセス制御ルールテーブルの参照

このセクションでは、アクセス制御ルールを含む詳細設定機能のパラメータについて説明します。アクセス制御ルールは、特定のSSIDに接続できるデバイスを制御するために使用されます。エージェントモードではH8748Qで設定されたアクセス制御ルールを引き継ぎます。

手順

1. Web管理メインページで、メニュー[LAN] > [無線LAN] > [無線LAN拡張]を選択し、無線LAN拡張ページを開きます。こちらのページでアクセス制御ルールテーブルを参照できます。図3-9を参照してください。

図 3-9 アクセス制御ルールテーブルページ

▼ アクセス制御ルールテーブル		
SSID名	MACアドレス	ACLポリシー
SSID1	f4:6d:3f:41:3e:8a	Allow
SSID5	f4:6d:3f:41:3e:8a	Allow
SSID9	f4:6d:3f:41:3e:8a	Allow

2. 「更新」ボタンをクリックして最新の情報を取得します。

3.2.2.2 MLOの設定

本製品はMLO機能をサポートし、ルーターが2.4GHz、5GHz、および6GHzの周波数帯を同時に使用してデータを伝送することを可能にします。これによりネットワークの速度と安定性が向上します。

手順

1. Web管理メインページで、メニュー[LAN] > [無線LAN] > [MLO]を選択し、図のようにMLO設定ページを開きます。図3-10を参照してください。

図 3-10 MLOページ

▼ MLO

MLO を有効にすると、プライマリの2.4GHz 2.4GHz-Priの構成が、SSID 名、暗号化タイプ、WPA パスフレーズを含め、プライマリの5GHz-Priおよび6GHz-Priの両方に同期されます。さらに、すべての無線がオンになり、各無線のプライマリのSSIDも有効になります。

MLO有効

☒ 自動 ☐ オフ

設定

キャンセル

2. パラメータを設定します。パラメータの説明については表3-1を参照してください。

表 3-1 MLOモードパラメータ

パラメータ名	パラメータの説明
MLO有効	● 自動: MLO機能を有効にする。 ● オフ: MLO機能を無効にする。

3. 設定後、「設定」ボタンをクリックして設定を終了します。

3.2.2.3 WPSの設定

WPS機能を有効にすると、デバイスはネットワーク名とワイヤレス暗号化キーを自動的に構成できるため、ワイヤレス ネットワーク暗号化の構成プロセスが簡素化されます。WPSは高速なネットワーク接続を提供しますが、セキュリティ上のリスクも伴う可能性があります。セキュリティ要件が高いシナリオでは、WPS機能を無効にすることをお勧めします。

手順

1. Web管理メインページで、メニュー [LAN] > [無線LAN] > [WPS] を選択して、WPS設定ページに入ります。図3-11を参照してください。

図 3-11 WPS設定ページ

3. パラメータを設定します。パラメータの説明は表3-2を参照してください。

表 3-2 WPSモードパラメータ

パラメータ名	パラメータの説明
WPSモード	● PBC (プッシュボタン接続): 本製品のWPSボタンで操作できるようになります。 ● 無効: WPSモードが「無効」に設定されている場合、WPS動作は完全に停止されます。ユーザーはWPSのクイック接続機能を使用して無線接続を確立することができず、SSIDやパスワードの入力などを含むネットワーク設定を手動で構成する必要があります。

3. 設定後、「設定」ボタンをクリックして設定を終了します。

3.2.2.4 WLAN検出の設定

WLAN検出機能は、デバイスの近くにある無線信号を検出します。

手順

1. Web管理メインページで、メニュー [LAN] > [無線LAN] > [WLAN検出] を選択して、WLAN検出ページに入ります。図3-12を参照してください。

図 3-12 WLAN検出ページ

▼ ワイヤレスリピーターの構成

接続されたワイヤレスネットワーク	ステータス	信号強度	選択
	接続なし		>

ワイヤレスネットワークをスキャン

SSID名	暗号化タイプ	バンド	チャンネル	信号強度	選択
その他(ネットワークを手動で追加) >					

2. (オプション操作) [スキャン] をクリックします。現在のネットワークで使用できるすべてのバックホールSSID情報が表示されます。対応するバックホールSSIDを手動で選択できます。

3.2.3 LANの設定



注:

エージェントモードではLANの設定、ステータス確認をH8748Qで行いますので、[LAN] > [LAN]の画面は使用しません。

3.3 管理と診断の設定

3.3.1 アカウント管理の設定

本製品のパスワードを変更することで、ネットワークを保護し、権限のない人がネットワークにアクセスするのを防ぐことができます。以下のルールでパスワードを強力にしてください。

- パスワードの長さは8文字以上
- パスワードは数字、アルファベット、および記号で構成

手順

1. Web管理メイン画面で、メニュー[管理&診断] > [アカウント管理]を選択し、管理者アカウント管理ページに入ります。図3-13を参照してください。

図 3-13 アカウント管理画面

▼ 管理者アカウント管理

ユーザー名

admin

旧パスワード

新パスワード

パスワードの確認

設定

キャンセル

2. パラメータを設定します。パラメータについての説明は表3-3を参照してください。

表 3-3 管理者アカウント管理パラメータ

パラメータ名	パラメータの説明
ユーザ名	ユーザ名はadmin固定（変更不可）
旧パスワード	変更前パスワード
新パスワード	新しいパスワード
パスワードの確認	新しいパスワードの再入力

3. 設定後、「設定」ボタンをクリックして設定を終了します。

3.3.2 アイドルタイムアウトの設定

アイドル タイムアウト時間を設定して、本製品のセキュリティを強化します。ユーザーが一定時間内に操作を行わない場合、自動的にユーザーをログアウトし、権限のない人物がユーザーのセッションを使用して不正な操作を行うことを防ぎます。

手順

1. Web管理メイン画面で、メニュー[管理&診断] > [アイドルタイムアウト]を選択して、アイドルタイムアウトページに入ります。図3-14を参照してください。

図 3-14 アイドルタイムアウトページ

2. パラメータを設定します。パラメータについての説明は表3-4を参照してください。

表 3-4 アイドルタイムアウトパラメータ

パラメータ名	パラメータの説明
タイムアウト	ユーザーが自動的にログアウトされるまでのアイドル時間（最大30分） 単位：分

3. 設定後、「設定」ボタンをクリックして設定を終了します。



注:

アイドルタイムアウト設定は、システムに再度ログインした後に有効になります。

3.3.3 システム管理設定

3.3.3.1 デバイス管理設定

Web管理ページで、デバイスを再起動できます。再起動後、構成パラメータはクリアされないため、H3701Qを再構成する必要はありません。工場出荷時の設定を復元すると、ネットワーク設定やパスワードなど、デバイスのすべての設定と構成がクリアされます。

- デバイスの再起動の主な機能には、キャッシュの解放、急速な劣化の防止、デバイスの耐用年数の延長などがあります。
- 工場出荷時設定の復元機能は、次のシナリオに適用されます：
- デバイスの故障：ホームゲートウェイにネットワーク接続の問題、パフォーマンスの低下、またはその他の障害が発生した場合、工場出荷時の設定に戻すことで、デバイスを正常な動作状態に戻すことができます。
- デバイスのパスワードや設定を忘れた場合：ホームゲートウェイの管理者パスワードやその他の重要な設定を忘れた場合、デバイスを工場出荷時のデフォルト設定に復元し、デバイスを再設定することができます。

手順

1. Web管理メイン画面で、メニュー[管理&診断] > [システム管理] > [デバイス管理]を選択して、デバイス管理ページへ入ります。図3-15を参照してください。

図 3-15 デバイスリブート、リセット画面

The screenshot displays a web interface for device management. It features two main sections: 'Report Function' (リブート機能) and 'Reset Function' (リセット機能). The 'Report Function' section includes a warning that the device will restart automatically after the operation, and a blue 'Report' button. The 'Reset Function' section includes a warning that all parameter settings will be restored to factory defaults and the device will restart automatically, and a blue 'Reset' button.

▼ リブート機能

この操作完了後、本装置は自動的に再起動します。
注：再起動操作は、現在のすべてのサービスを中断します。

リブート

▼ リセット機能

工場出荷時のリセット：すべてのパラメータ設定が工場出荷時の状態に戻ります。この操作が完了すると、デバイスは自動的に再起動します。
注：この操作が終了すると、すべての設定が初期化され、工場出荷時の状態に戻ります。

リセット

2. (再起動の場合)「リブート」ボタンをクリックしてください。
3. (工場出荷時設定への復元の場合)「リセット」ボタンをクリックしてください。

3.3.3.2 ソフトウェアアップグレード

ソフトウェアアップグレードの目的は、既知のセキュリティ脆弱性を修正し、新しい機能を追加し、システムパフォーマンスを向上させ、ネットワーク接続の安定性とセキュリティを確保します。

前提条件

アップグレード用のファイルが必要となります。

手順



注:

- 本製品では自動でソフトウェアアップグレードを行うため、通常使用時にはこの操作は使用しません。
- ソフトウェアアップグレード中は電源を切らないでください。
- アップグレード後、自動的に再起動を実行します。

1. Web管理メイン画面で、メニュー[管理&診断] > [システム管理] > [ソフトウェアのアップグレード]を選択して、ソフトウェアのアップグレード画面に入ります。図3-16を参照してください。

図 3-16 ソフトウェアのアップグレードページ

2. 「ファイルの選択」をクリックしてサービスプロバイダーから提供されたアップグレード用ファイルを指定してください。
3. 「アップグレード」ボタンをクリックすると、アップグレード確認のポップアップを表示します。「OK」ボタンをクリックするとソフトウェアのアップグレードを開始します。

3.3.3.3 自動アップグレード設定

本製品はソフトウェアを自動でアップグレードします。自動アップグレードの設定を行います。バージョンアップが完了すると、本製品は自動的に再起動を実施します。

手順

1. Web管理メイン画面で、メニュー[管理&診断] > [システム管理] > [自動アップグレード]を選択して、自動アップグレード画面に入ります。図3-17を参照してください。

図 3-17 自動アップグレード

▼ ソフトウェアのアップグレード

☒ 自動 ☐ 手動

アップグレード後にデバイスが再起動します。

ソフトウェアアップグレード用のURLを記入してください。

ソフトウェアアップグレードの時刻を設定してください。

時から

時まで

設定

キャンセル

2. パラメータを設定します。パラメータについての説明は表3-6を参照してください。

表 3-6 自動アップグレード設定パラメータ

パラメータ名	パラメータの説明
自動	このモードでは、自動的にアップグレードを検出し、指定された時刻の範囲内で自動的にソフトウェアをアップグレードします。
手動	このモードでは、自動的にアップグレードを検出し、検出された状態時にアップグレード用のポップアップ表示します。「アップグレード」ボタン をクリックするとアップグレードを開始します。図3-18を参照してください。
URL	サービスオペレータから提供されたURLを入力してください。
アップグレード時刻	アップグレードを開始する時刻を指定してください。自動設定でアップグレードを検出した場合には、指定された時間内でランダムにアップグレードを開始します。

図 3-18 手動設定時にアップグレードポップアップ



3. 設定後、「設定」ボタンをクリックして設定を終了します。

3.3.4 ログ管理

ネットワーク機器のログ管理は、家庭ネットワークの維持と障害トラブルシューティングにおいて重要な役割を果たします。システムログとリモートログの記録と分析を通じて、ユーザーは家庭ネットワークの動作状態をよりよく理解し、ネットワークのセキュリティを保護し、ネットワークの問題を迅速に解決することができます。

- システムログに記録されたエラーや警告情報を確認することで、ネットワーク障害の具体的な症状や可能性のある原因を把握することができます。
- リモートログ管理機能により、本製品がログ情報をリモートのログサーバーやストレージデバイスに送信することができます。この機能を有効にする主な目的は、管理者が本製品の動作状態をリモートで監視・分析し、潜在的な問題を迅速に発見し解決するためです。

手順

システムログの確認

1. Web管理メイン画面で、メニュー[管理&診断] > [ログ管理]を選択して、ログ管理画面に入ります。システムログ管理画面でシステムログを確認できます。図3-19を参照してください。

図 3-19 システムログ管理画面

▼ システムログ管理

ログの保存 ☒ オン ☐ オフ

設定 キャンセル

ログ出力

```

2025-01-06T08:10:12Z [Error] [wlan_hostapd0..] pid[298]asend EVENT[0XA92F] Len=[116] sendto
[multiapd.map.slave] ERROR,swLen=[-1] errno=[111:Connection refused]!!!
P0000-00-00T00:01:38 [Error] Web get fail. (objname: OBJ_WLAN_STAPROFILE_ID identity: DEV.WIFI.STAIF1 iRet: -3)
P0000-00-00T00:01:44 [Error] Web get fail. (objname: OBJ_WLAN_STAPROFILE_ID identity: DEV.WIFI.STAIF1 iRet: -3)
P0000-00-00T00:01:48 [Error] Web user is authenticated fail from the host(192.168.0.100).authCode == 201
P0000-00-00T00:01:48 [Error] Web user is authenticated fail from the host(192.168.0.100).authCode == 204[Appear
4 times]
P0000-00-00T00:03:57 [Error] Web set failed. (objname: OBJ_USERINFO_ID identity: IGD.AU1 iRet: -264)
P0000-00-00T00:04:02 [Error] Web set failed. (objname: OBJ_USERINFO_ID identity: IGD.AU1 iRet: -264)
P0000-00-00T00:04:03 [Error] Web set failed. (objname: OBJ_USERINFO_ID identity: IGD.AU1 iRet: -264)
P0000-00-00T00:07:32 [Error] Web user is authenticated fail from the host(192.168.0.1).authCode == 204
P0000-00-00T00:08:15 [Error] Web user is authenticated fail from the host(192.168.0.1).authCode == 204
  
```

更新 ログダウンロード

2. パラメータの設定、ログ表示を参照します。パラメータについての説明は表3-5を参照してください。

表 3-5 システムログ管理パラメータ

パラメータ名	パラメータの説明
ログの保存	オンの場合にはシステムログを取得し、ログを出力します。
ログ出力	システムログを表示します。

3. ログの保存設定後、「設定」ボタンをクリックして設定を完了します。
4. 「更新」ボタンをクリックすると最新のログをログ出力へ表示します。
5. 「ログダウンロード」ボタンをクリックすると、システムログをダウンロードすることができます。

セキュリティログ管理

1. セキュリティログ管理画面でセキュリティログを確認できます。図3-20を参照してください。

図 3-20 セキュリティログ管理画面

▼ セキュリティログ管理

ログの保存 ☒ オン ☐ オフ

設定 キャンセル

ログ出力

```
P0000-00-00T00:23:43 The device is restored to the factory settings.
P0000-00-00T00:23:43 reboot for module(DB) msg : reset(4)
P0000-00-00T00:00:41 System start!
P0000-00-00T00:00:46 Telnet: will start...
P0000-00-00T00:00:46 SSH: will start...
2024-11-02T22:34:27Z System start!
2024-11-02T22:34:33Z Telnet: will start...
2024-11-02T22:34:34Z SSH: will start...
2024-11-02T22:47:41Z Msntp synchronized localtime success!dwTimeOffset=-962058649
current time is Sat Nov 2 22:47:41 2024
2024-11-02T22:47:49Z WLAN: PSK password of [SSID1] has been changed!
```

更新 ログダウンロード

2. パラメータの設定、ログ表示を参照します。パラメータについての説明は表3-6を参照してください。

表 3-6 セキュリティログ管理パラメータ

パラメータ名	パラメータの説明
ログの保存	オンの場合にはシステムログを取得し、ログを出力します。
ログ出力	システムログを表示します。

3. ログの保存設定後、「設定」ボタンをクリックして設定を完了します。
4. 「更新」ボタンをクリックすると最新のログをログ出力へ表示します。
5. 「ログダウンロード」ボタンをクリックすると、システムログをダウンロードすることができます。

リモートログの管理

1. リモートログ管理画面でリモートログサーバへのログの転送を設定できます。図3-21を参照してください。

図 3-21 リモートログ管理画面

▼ リモートログ管理

リモートログ ☒ オン ☐ オフ

リモートログサーバ

設定 キャンセル

- パラメータを設定します。パラメータについての説明は表3-7を参照してください。

表 3-7 リモートログ管理画面

パラメータ名	パラメータの説明
リモートログ	オンの場合には、指定されたリモートログサーバにログメッセージの送信を開始します。 オフの場合には、リモートサーバへのログメッセージの送信を停止し、ログメッセージをローカルにのみ保存します。
リモートログサーバ	ログメッセージ送信先のリモートログサーバのIPアドレス

- 設定後、「設定」ボタンをクリックして設定を終了します。

3.3.5 診断

診断機能では、障害箇所の特定や日常メンテナンスのためのPing診断とトレースルート診断を提供します。

- **Ping診断:** ユーザのホストから別のホストへのネットワークが接続されているかどうかをテストするために使用されます。
- **トレースルート診断:** ユーザーのホストから別のホストへのネットワーク経路を表示します。

手順

Ping診断の実行

- Web管理メインページで、メニュー[管理と診断] > [ネットワーク診断] > [PING診断] を選択して、PING診断ページに入ります。図3-22を参照してください。

図 3-22 PING診断画面

▼ PING診断

IPアドレス/ホスト名

Egress

繰り返し回数

パケットサイズ bytes

タイムアウト ms

診断

診断結果

2. パラメータを設定します。パラメータについての説明は表3-7を参照してください。

表 3-8 PING診断パラメータ

パラメータ名	パラメータの説明
IPアドレス/ホスト名	Pingを実施する宛先のIPアドレス/ホスト名を設定します。
Egress	Pingテストを実施したいインターフェースを選択します。 ● オート：設定したアドレスによりLAN側/WAN側を自動判別し、PINGテストを実行します。 ● LAN：LAN側のテストを実行する場合に選択します。 ● DHCP：WAN側のテストを実行する場合に選択します。
繰り返し回数	Pingリクエストメッセージの送信回数
パケットサイズ	Pingリクエストメッセージのパケットサイズ
タイムアウト	各Pingからの応答を待機する最大時間。設定した時間内に応答が受信されない場合、Ping要求は失敗したとみなされます。

3. 「診断」ボタンをクリックすると、システムは指定されたアドレスへのPingを開始します。繰り返し回数で指定された回数のPing操作を実行し、結果が下の診断結果ボックスに表示されます。

トレースルート診断の実行

1. Web管理メインページで、メニュー[管理と診断] > [ネットワーク診断] > [トレースルート診断] を選択して、トレースルート診断ページに入ります。図3-23を参照してください。

図 3-23 トレースルート診断画面

トレースルート診断

IPアドレス/ホスト名

インターフェース

最大ホップ数

待ち時間 ms

プロトコル

診断結果

2. パラメータを設定します。パラメータについての説明は表3-8を参照してください。

表 3-9 トレースルート診断設定パラメータ

パラメータ名	パラメータの説明
IPアドレス/ホスト名	トレースルート診断を実施する宛先のIPアドレス/ホスト名を設定します。
Egress	トレースルート診断を実施したいインターフェースを選択します。 ● オート：設定したアドレスによりLAN側/WAN側を自動判別し、PINGテストを実行します。 ● LAN：LAN側のテストを実行する場合に選択します。 ● DHCP：WAN側のテストを実行する場合に選択します。
最大ホップ数	最大ホップ数を設定します。初期値：30、範囲は1から64までとなります。
待ち時間	応答パケットを待機する時間を設定します。単位：ミリ秒です。この期間内に応答パケットが受信されない場合は、アスタリスクが表示されます。
プロトコル	プロトコルを選択します ● UDP：UDPを設定します。 ● ICMP：ICMPを設定します。

3. 「診断」ボタンをクリックして上記の設定を完了すると、診断が開始され、下の診断結果ボックスに結果が表示されます。

3.3.6 動作モード設定

ネットワーク内の動作モードを切り替える方法について説明します。

- **コントローラー (ルーター):** Wi-Fi メッシュネットワーク内のコントローラーとして機能します。
- **エージェント:** Wi-Fi メッシュネットワーク内のエージェントとして機能します。

手順

1. Web管理メイン画面で、メニュー[管理&診断] > [動作モード]を選択して、動作モード画面に入ります。図3-24を参照してください。

図 3-24 動作モードページ

2. パラメータを設定します。パラメータについての説明は表3-10を参照してください。

表 3-10 動作モードパラメータ

パラメータ名	パラメータの説明
モード	● メッシュ自動 (DHCP): 接続する機器に応じて自動的にコントローラーモードまたはエージェントモードに切り替えます。 ● コントローラー (ルーター): コントローラーモードで動作します。 ● エージェント: エージェントモードで動作します。

3. 設定後、「設定」ボタンをクリックして設定を終了します。

4 コントローラー (ルーター)モード

この章には次のトピックが含まれます:

- 管理システムへのログイン
- トポロジー情報の参照
- インターネット接続設定
- ローカルネットワークの構成
- 構成管理と診断

コントローラー (ルーター) モード: コントローラーとして接続するアクセスポイントとWi-Fiメッシュネットワークを構築します。

4.1 管理システムへのログイン

前提条件

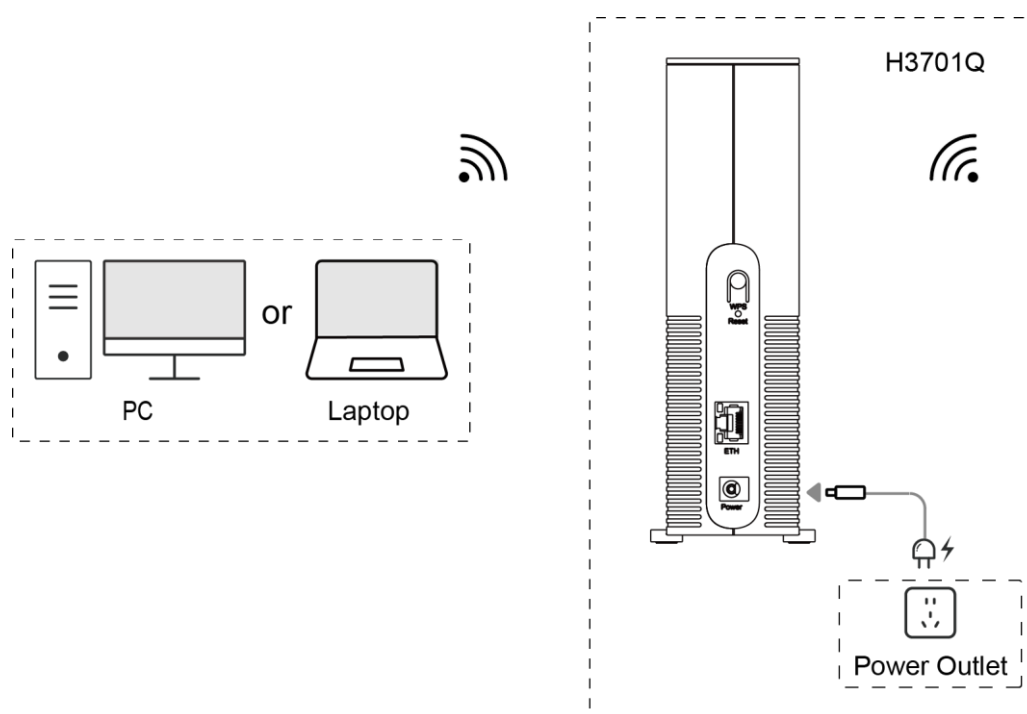
- 実行中のファイアウォールまたはセキュリティソフトウェアがすべてオフの状態
- ブラウザのプロキシサーバがオフの状態
- 接続するアップリンクのルータ (H8748Qなど) のメッシュ機能がオフの状態

手順

H3701Qハードウェア接続の構成

1. デスクトップ型パソコンやノートパソコンで無線LAN接続を行い、本製品の管理システムに接続します。ハードウェア接続図を[図4-1](#)に示します。

図 4-1 H3701Q ハードウェア接続図 (コントローラーモード)



H3701Q (コントローラーモード)管理画面へのログイン

2. 本製品へアクセスする機器の無線LAN設定で、本製品のSSIDを指定してアクセスしてください。SSID名と接続用のパスワードは本製品本体ラベルに記載されています。
3. ブラウザのアドレスバーに `http://192.168.0.254` を入力してEnterを実行してください。
(192.168.0.254はデフォルトの管理アドレスになります。)接続する本製品のログイン画面を表示します。ログインページを図4-2に示します。

図 4-2 H3701Qのログインページ

The login page for the H3701Q device. At the top left is a padlock icon. To its right, a header bar contains the text 'H3701Q へようこそ。ログインしてください。' (Welcome to H3701Q. Please log in.). Below this, there are two input fields: the first is labeled 'ユーザー名' (Username) and the second is labeled 'パスワード' (Password). At the bottom right, there is a blue button labeled 'ログイン' (Log in).

4. ユーザー名（admin）と初期パスワード（初期パスワードは本体ラベルに記載されています）を入力した後、「ログイン」ボタンをクリックしてください。初回接続では新パスワードの設定ページに入ります。図4-3を参照してください。

図 4-3 H3701Q (コントローラーモード) パスワード変更画面

ログイン画面 -パスワード変更-

パスワードは8文字以上で、半角英数字及び記号を含む必要があります。

ユーザー名 admin

新パスワード

パスワードの確認

設定 キャンセル

5. 新しいパスワードを設定し、「設定」ボタンをクリックして、ログインページに戻ります。
6. 再度ユーザー名、パスワードを入力してコントローラーモードの本製品の管理ページにログインします。図4-4を参照してください。

図 4-4 H3701Qコントローラー（ルーター）モード管理ページ

ZTE 現在時刻:1970-01-01T00:09 admin ログアウト 日本語 | English

ホーム トポロジー インターネット LAN 管理&診断

ステータス
アカウント管理
アイドルタイムアウト
システム管理
ログ管理
ネットワーク診断
動作モード

ページ情報
このページでは、デバイスの基本情報を表示します。

▼ デバイス情報

デバイスタイプ	H3701Q
デバイスのシリアル番号	ZTEMH9MQB400003
ハードウェアバージョン	V3.0.00
ソフトウェアバージョン	V3.0.0P2_JP
ブートバージョン	V1.0.0
動作モード	コントローラー(ルーター)

更新

4.2 トポロジー情報の参照

トポロジー画面では、すべてのAP情報と接続されている無線LANクライアントと有線LANクライアントの詳細を表示できます。

手順

1. Web管理メイン画面でトポロジーを選択すると、トポロジー情報を表示します。図4-5を参照してください。

図 4-5 トポロジー画面

The screenshot shows the ZTE web management interface. At the top, there is a header with the ZTE logo, the current time (1970-01-01T00:10), and user information (admin, ログアウト, 日本語 | English). Below the header is a navigation bar with tabs: ホーム, トポロジー (selected), インターネット, LAN, and 管理&診断. The main content area displays a router icon with a blue notification bubble containing the number 1. Below the icon, the text reads: ZTE:H3701Q, MAC:20:3a:eb:de:1f:20, IP: 192.168.0.254. There are two expandable sections: 'すべてのAP' (All APs) and 'すべてのクライアント' (All Clients). The 'すべてのAP' section contains a table with columns: AP名, IP, MAC, モード, バックホール, and 操作エリア. The table has one row for ZTE:H3701Q with IP 192.168.0.254, MAC 20:3a:eb:de:1f:20, mode controller, and backhaul /. The '操作エリア' column has a '修正' (Edit) button. The 'すべてのクライアント' section contains a table with columns: クライアント名, 接続先デバイス, 関連バンド, RSSI, and 操作エリア. The table has one row for DESKTOP-69HGB00 with connection device controller, band 5GHz, and RSSI -34dBm. The '操作エリア' column has a '修正' (Edit) button. At the bottom, there is a footer with the text H3701Q V3.0.0P2_JP.

AP名	IP	MAC	モード	バックホール	操作エリア
ZTE:H3701Q	192.168.0.254	20:3a:eb:de:1f:20	controller	/	修正

クライアント名	接続先デバイス	関連バンド	RSSI	操作エリア
DESKTOP-69HGB00	controller	5GHz	-34dBm	修正

2. 各AP、クライアントの操作エリアの「修正」ボタンをクリックすると、AP名、クライアント名を変更することができます。

4.3 インターネット接続設定

4.3.1 インターネット接続確認

インターネット接続確認では、IP アドレス、接続名など、インターネット接続のステータスを確認できます。インターネット接続のステータス情報は、インターネット接続が確立された場合にのみ表示されます。

手順

インターネットインターフェース情報

1. Web管理メイン画面で、メニュー[インターネット] > [ステータス] > [インターネット]を選択して、インターネットページに入ります。インターネットページではインターネットインターフェース情報を確認できます。図4-6を参照してください。

図 4-6 インターネットインターフェース情報

▼ インターネットインターフェース情報	
インターフェイス名	WAN
MACアドレス	20:3a:eb:de:1f:20
ステータス	アップ
モード	1000M 全二重
受信バケット数/受信バイト数	294/43847
送信バケット数/送信バイト数	159/33466
更新	

2. 「更新」ボタンをクリックすると最新情報を表示します。

インターネット接続ステータス

1. インターネットページではインターネット接続状態を確認できます。図4-7を参照してください。

図 4-7 インターネット接続ステータス

▼ インターネット接続ステータス	
接続名	DHCP
タイプ	DHCP
IPバージョン	IPv4
NAT	オン
IPアドレス	192.168.1.5/255.255.255.0
DNSアドレス	192.168.1.1/0.0.0.0/0.0.0.0
IPv4ゲートウェイ	192.168.1.1
リース残時間	23 時 14 分 54 秒
IPv4接続ステータス	接続済み 更新 リリース
IPv4オンライン期間	0 時 45 分 5 秒
切断理由	なし
WANMAC	20:3a:eb:de:1f:18

更新

2. 「更新」ボタンをクリックすると最新情報を表示します。

4.3.2 セキュリティ設定

4.3.2.1 フィルタ設定

このセクションでは、URL フィルター、IP フィルターのフィルター設定を構成する方法について説明します。

手順

フィルタスイッチとモード設定

1. Web管理メイン画面で、メニュー[インターネット] > [セキュリティ] > [フィルタ条件]を選択して、フィルタ条件ページに入ります。
2. URLフィルタの使用とモードをフィルタスイッチとモード設定画面で設定します。図4-8を参照してください。

図 4-8 フィルタスイッチとモード設定画面

▼ フィルタスイッチとモード設定

URLフィルタ

☐ オン ☒ オフ

モード

ブラックリスト ▼

設定

キャンセル

3. パラメータを設定します。パラメータについての説明は表4-1を参照してください。

表 4-1 フィルタースイッチ、モードパラメータ

パラメータ名	パラメータの説明
URLフィルタ	● オン: URLフィルタが有効. ● オフ: URLフィルタが無効.
モード	● ブラック リスト: URLフィルター リスト内で指定されたアドレスのデバイスはアクセスできません。 ● ホワイト リスト: URLフィルター リスト内で指定されたアドレスのデバイスのみがアクセスできます。

4. 設定後、「設定」ボタンをクリックして設定を終了します。

URLフィルタの設定

5. URLフィルタ画面を開いてURLを指定します。図4-9を参照してください。

図 4-9 URLフィルタ画面

▼ URLフィルタ

▼ 新しいアイテム

名前

URL

設定

キャンセル

+

 新しいアイテムを作成する

6. パラメータを設定します。パラメータについての説明は表4-2を参照してください。

表 4-2 URLフィルタパラメータ

パラメータ名	パラメータの説明
名前	URLフィルタの名前となります。
URL	フィルタで使用するURLを設定します。

7. 設定後、「設定」ボタンをクリックして設定を終了します。

8. 「新しいアイテムを作成する」をクリックするとフィルタ設定を追加できます。
9. 設定画面右上のゴミ箱イメージをクリックするとフィルタ設定を削除します。

IPフィルタの設定

10. IPフィルタ画面を開いてIPフィルタを設定します。図4-10を参照してください。

図 4-10 IPフィルタ画面

▼ IPフィルタ

ファイアウォールIPフィルタを構成する際に注意すべきことは何ですか?

▼ 新しいアイテム

○ オン ○ オフ

○ オン ○ オフ

名前

モード

● 許可 ○ 破棄

優先度

1

IPバージョン

任意

送信元IPアドレス

宛先IPアドレス

プロトコル

任意

対象インターフェース(in)

任意

対象インターフェース(out)

任意

DSCP

設定

キャンセル

+ 新しいアイテムを作成する

11. パラメータを設定します。パラメータについての説明は表4-3を参照してください。

表 4-3 IPフィルタパラメータ

パラメータ	パラメータの説明
オン/オフ	● オン: IPフィルタが有効 ● オフ: IPフィルタが無効
名前	URLフィルタの名前となります。
モード	● 許可: パケット受信を許可 ● 破棄: パケットを破棄
優先度	IPフィルタの優先度の値を指定します。優先度は1から20までです。
IPバージョン	IPアドレスのバージョンを任意、IPv4、IPv6から選択します。
送信元IPアドレス/宛先IPアドレス	送信元と宛先のIPアドレスとネットマスク
プロトコル	● ICMP ● TCP ● UDP ● 任意（プロトコル指定なし） ● TCPとUDP ● その他（その他を選択後、プロトコル番号を指定してください。）
対象インタフェース（IN）	● 任意: LAN、インターネット両方からのパケット ● LAN: LAN側からのパケット ● DHCP: インターネット側からのパケット
対象インタフェース（OUT）	● 任意: LAN、インターネット両方へのパケット ● LAN: LAN側へのパケット ● DHCP: インターネット側へのパケット
DSCP	IPヘッダのDSCP値（0から63まで）

12. 設定後、「設定」ボタンをクリックして設定を終了します。
13. 「新しいアイテムを作成する」をクリックするとフィルタ設定を追加できます。
14. 設定画面右上のゴミ箱イメージをクリックするとフィルタ設定を削除します。

4.3.2.2 DMZ設定

このセクションでは、DMZの設定方法について説明します。コントローラーモード設定では、宛先IPアドレスとポート番号を外部ネットワーク アドレス（ネットワーク側） から内部ネットワーク アドレス（ユーザー側） に変換し、内部ネットワークサーバーにアクセスできるようにします。

手順

1. Web管理メイン画面で、メニュー[インターネット] > [セキュリティ] > [DMZ]を選択して、DMZページに入ります。図4-11を参照してください。

図 4-11 DMZ画面

2. パラメータを設定します。パラメータについての説明は表4-4を参照してください。

表 4-4 DMZ設定パラメータ

パラメータ名	パラメータの説明
DMZ	● オン: DMZが有効 ● オフ: DMZが無効
DMZホストのIPアドレス	外部ネットワークから接続するクライアントデバイスのLAN用IPアドレスを指定します。

3. 設定後、「設定」ボタンをクリックして設定を終了します。

4.3.3 時刻の設定

手順

1. Web管理メイン画面で、メニュー[インターネット] > [時刻の設定]を選択して、SNTPページに入ります。図4-12を参照してください。

図 4-12 SNTP画面

▼ SNTP

現在の日付と時刻

1970-01-01T00:44:49

タイムゾーン

(GMT+09:00) Osaka,Sapporo,Tokyo ▼

NTPサーバー1

ntp.nict.jp

NTPサーバー2

NTPサーバー3

NTPサーバー4

NTPサーバー5

ポーリング間隔

86400

秒

設定

キャンセル

2. パラメータを設定します。パラメータについての説明は表4-5を参照してください。

表 4-5 SNTPパラメータ

パラメータ名	パラメータの説明
タイムゾーン	タイムゾーンはGMT+9:00固定です。
NTPサーバー1-5	接続するNTPサーバのIPアドレスまたはホスト名 NTPサーバー1の初期値はntp.nict.jp
ポーリング間隔	NTP サーバーへ同期用要求パケットを送信する間隔です。 範囲： は3600～86400、単位は秒です。

3. 設定後、「設定」ボタンをクリックして設定を終了します。

4.3.4 マルチキャスト設定

4.3.4.1 IGMPモード設定

手順

1. Web管理メイン画面で、メニュー[インターネット] > [マルチキャスト] > [IGMP]を選択して、IGMPページに入ります。図4-13を参照してください。

図 4-13 IGMPモード

▼ IGMPモード

IGMPプロキシ

☐ オン ☒ オフ

設定

キャンセル

2. パラメータを設定します。パラメータについての説明は表4-6を参照してください。

表 4-6 IGMPモードパラメータ

パラメータ	パラメータの説明
IGMPプロキシ	● オン: IGMPプロキシが有効 ● オフ: IGMPプロキシが無効

3. 設定後、「設定」ボタンをクリックして設定を終了します。

4.3.4.2 MLDモード設定

MLD は IGMP の IPv6 バージョンです。

手順

1. Web管理メイン画面で、メニュー[インターネット] > [マルチキャスト] > [MLD]を選択して、MLDページに入ります。図4-14を参照してください

図 4-14 MLDモード画面

2. パラメータを設定します。パラメータについての説明は[表4-7](#)を参照してください。

表 4-7 MLDモードパラメータ

パラメータ名	パラメータの説明
MLDプロキシ	● オン: MLDプロキシが有効 ● オフ: MLDプロキシが無効

3. 設定後、「設定」ボタンをクリックして設定を終了します。

4.4 LAN接続の設定

4.4.1 ステータスの確認

このセクションでは、無線LANステータスを確認する方法について説明します。

- 無線LANステータスを表示することで、無線LANステータス情報を取得し、ワイヤレスネットワークのパフォーマンスと安定性を判断することができます。
- 無線LANクライアントステータスを確認することで、デバイスの数、接続ステータス、信号強度など、ワイヤレス ネットワークに接続されているクライアント デバイスに関する詳細情報を取得できます。この情報は、潜在的なネットワークの問題を発見し、ネットワークパフォーマンスをタイムリーに最適化するのに役立ちます。

手順

無線LANステータスの確認

1. Web管理メイン画面で、メニュー[LAN] > [ステータス] > [無線LANステータス]を選択して、無線LANステータスを表示します。図[4-15](#)を参照してください。

図 4-15 無線LANステータス画面

▼ 無線LANステータス			
無線LAN基本ステータス			
無線LAN (2.4GHz)	オン	チャンネル (2.4GHz)	6
無線LAN (5GHz)	オン	チャンネル (5GHz)	100
無線LAN (6GHz)	オン	チャンネル (6GHz)	5
2.4GHz-Pri			
SSID名	egg-E1F20	MACアドレス	20:3a:eb:de:1f:21
SSIDスイッチ	オン	受信パケット数 / 送信パケット数	0/0
暗号化タイプ	WPA2-PSK/WPA3-SAE	受信バイト数/送信バイト数	0/0
2.4GHz-Sec			
SSID名	egg-2g-E1F20	MACアドレス	26:3a:eb:de:1f:21
SSIDスイッチ	オン	受信パケット数 / 送信パケット数	0/0
暗号化タイプ	WPA2-PSK-AES	受信バイト数/送信バイト数	0/0

2. 「更新」ボタンをクリックすると最新情報を表示します。

無線LANクライアントステータスの確認

1. Web管理メイン画面で、メニュー[LAN] > [ステータス] > [無線LANステータス]を選択して、無線LANステータスを表示します。図4-16を参照してください。

図 4-16 無線LANクライアントステータス画面

▼ 無線LANクライアントステータス			
クライアント-1			
SSID	SSID5	名前	DESKTOP-69HGB00
IPv4アドレス	192.168.0.2	MACアドレス	c8:09:a8:6d:24:dc
IPv6アドレス			
アクセスモード			
			更新

2. 「更新」ボタンをクリックすると最新の情報を表示します。

4.4.2 無線LANの設定

4.4.2.1 無線LAN基本パラメータの設定

手順

無線LANのオン/オフ設定.

1. Web管理メイン画面で、メニュー[LAN] > [ステータス] > [無線LAN] > [無線LAN基本]を選択して、無線LAN基本ページに入り、無線LANオン/オフ設定を表示します。図4-17を参照してください。

図 4-17 無線LANオン/オフ設定

▼ 無線LANオン/オフ設定

無線LAN (2.4GHz)

☒ オン ☐ オフ

無線LAN (5GHz)

☒ オン ☐ オフ

無線LAN (6GHz)

☒ オン ☐ オフ

設定

キャンセル

2. パラメータを設定します。パラメータについての説明は表4-8を参照してください。

表 4-8 無線LANオン/オフ設定パラメータ

パラメータ名	パラメータの説明
無線LAN (2.4GHz)	● オン: 2.4GHz帯が有効 ● オフ: 2.4GHz帯が無効
無線LAN (5GHz)	● オン: 5GHz帯が有効 ● オフ: 5GHz帯が無効
無線LAN (6GHz)	● オン: 6GHz帯が有効 ● オフ: 6GHz帯が無効

3. 設定後、「設定」ボタンをクリックして設定を終了します。

無線LAN詳細設定

4. 無線LAN詳細設定を表示して設定します。図4-18を参照してください。

図 4-18 無線LAN詳細設定画面

▼ 無線LAN詳細設定

▼ 2.4GHz

チャンネル

自動

モード

Mixed(802.11b/g/n/ax/be)

 Intelネットワークカードを使用しているラップトップなど、一部のWi-Fiデバイスのネットワークカードドライバは古い
です。ネットワークカードドライバをアップグレードするか、Wi-Fiモードをb/g/nに切り替えてください。

帯域幅

20MHz

SGI

☐ オン ☒ オフ

ピーコン間隔(ms)

100

ms

送信出力

100%

設定

キャンセル

▼ 5GHz

チャンネル

自動

モード

Mixed(802.11a/n/ac/ax/be)

 Intelネットワークカードを使用しているラップトップなど、一部のWi-Fiデバイスのネットワークカードドライバは古い
です。ネットワークカードドライバをアップグレードするか、Wi-Fiモードをa/n/acに切り替えてください。

帯域幅

80MHz

SGI

☐ オン ☒ オフ

ピーコン間隔(ms)

100

ms

送信出力

100%

設定

キャンセル

▼ 6GHz

チャンネル

自動

モード

Mixed(802.11ax/be)

帯域幅

320MHz

SGI

☐ オン ☒ オフ

ピーコン間隔(ms)

100

ms

送信出力

100%

PSC

☐

設定

キャンセル

5. パラメータを設定します。パラメータについての説明は表4-9を参照してください。

表 4-9 無線LAN詳細設定パラメータ

パラメータ名	パラメータの説明
チャンネル	無線LAN で使用される通信チャンネルを設定します。 ● 2.4GHz: Autoまたは 1~13 ● 5GHz: Autoまたは36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140,144, ● 6GHz: Autoまたは 1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93
モード	● 2.4GHz: IEEE 802.11b のみ IEEE 802.11g のみ IEEE 802.11n のみ (802.11b/g) (802.11g/n) (802.11b/g/n) (802.11b/g/n/ax) (802.11b/g/n/ax/be) ● 5GHz: IEEE 802.11a のみ IEEE 802.11n のみ IEEE 802.11ac のみ (802.11a/n) (802.11a/n/ac) (802.11a/n/ac/ax) (802.11a/n/ac/ax/be)

	● 6GHz: IEEE 802.11ax のみ (802.11ax/be)
帯域幅	帯域幅を設定します。 ● 2.4GHz: 自動、20MHz、40MHz 初期値 : 20MHz ● 5GHz: 自動、20MHz、40MHz、80MHz、160MHz 初期値 : 80MHz ● 6GHz: 自動、20MHz、40MHz、80MHz、160MHz、320MHz 初期値 : 320MHz
SGI	2.4GHz/5GHz/6GHz: 送信間隔を短くするには、このオプションをオンにします。 ● オン: オプションを有効にします。 ● オフ: オプションを無効にします。
ビーコン間隔	ビーコン間隔を設定します。 2.4GHz/5GHz/6GHz: 100 ~1000 初期値 : 100
送信出力	送信電力を選択します。 2.4GHz/5GHz/6GHz : 100%、80%、60%、40%、20% 初期値 : 100%
PSC	PSC は Power Save Class の略称で、6GHz 用のパラメータです。 ● オン: 省電力モードをオンにします。低消費電力状態になります。 ● オフ: 省電力モードをオフにします。

6. 各帯域の設定後、「設定」ボタンをクリックして設定を終了します。

無線LAN SSIDの設定

7. 無線LAN SSIDの設定を表示して設定します。図4-19を参照してください。

図 4-19 無線LAN SSID設定画面

▼ 無線LAN SSIDの設定

▼ 2.4GHz-Pri

☒ オン ☐ オフ

SSID名

egg-E1F20

SSIDステルス機能

☐ オン ☒ オフ

暗号化タイプ

WPA2-PSK/WPA3-SAE

WPAパスフレーズ

.....

☐ パスワードを表示

最大クライアント数

64

設定

キャンセル

8. パラメータを設定します。パラメータについての説明は表4-10を参照してください。

表 4-10 無線LAN SSID設定パラメータ

パラメータ名	パラメータの説明
2.4GHz-Pri 2.4GHz-Sec 5GHz-Pri 5GHz-Sec 6GHz-Pri 6GHz-Sec	● オン：選択した SSID の設定を有効にします。 ● オフ：選択した SSID の設定を無効にします。
SSID名	SSIDの名前を設定します。
SSIDステルス機能	ステルス機能を設定します。 ● オン：SSID ステルス機能を有効にします。 ● オフ：SSID ステルス機能を無効にします。 初期値：オフ

暗号化タイプ	暗号化のタイプを設定します。 セキュリティなし WPA2-PSK(AES)、 WPA/WPA2-PSK(AES)、 WPA3(SAE)、 WPA/WPA2-PSK(AES)/WPA3(SAE)、 WPA2-PSK(AES)/WPA3(SAE)
WPAパスフレーズ	暗号化キーを設定します。 文字数 8 – 63 英数記号を用いて入力します。
最大クライアント数	SSIDに接続できるクライアントの最大数を設定します。これによりネットワークの過負荷を防ぎ、安定した接続を確保できます。 クライアント数の範囲は 1から64です。

9. 各SSIDの設定後、「設定」ボタンをクリックして設定を終了します。

4.4.2.2 無線LAN拡張パラメータの設定

このセクションでは、アクセス制御モードやアクセス制御ルールなど、高度な構成機能のパラメータについて説明します。アクセス制御モードとルールは、ネットワーク セキュリティを強化し、許可されたデバイスまたはユーザーのみがネットワーク リソースにアクセスできるようにするために使用されます。

- アクセス制御モードは、ネットワーク リソースにアクセスできるデバイスまたはユーザーを制御するために使用されます。アクセス制御モードには、フィルタなし、ブラック リスト、ホワイト リストがあります。
- アクセス制御ルールは、特定のSSIDに接続できるデバイスを制御するために使用されます。これらのルールは、デバイス名、SSID、およびMACアドレスに従って設定されます。
- アクセス制御ルールテーブルは、データパケットの送信を制御し、ネットワークリソースへの順序付けられたアクセスを実現します。たとえば、どのパケットがネットワークデバイスを通過できるか、どのパケットが拒否されるかを制御することで、不正なデータアクセスや潜在的な攻撃を防ぐことができます。

手順

アクセス制御 モード設定

1. Web管理メイン画面で、メニュー[LAN] > [ステータス] > [無線LAN] > [無線LAN拡張]を選択して、無線LAN拡張ページに入り、アクセス制御-モード設定を表示します。図4-20を参照してください。

図 4-20 アクセス制御-モード設定画面

▼ アクセス制御-モード設定

2.4GHz-Pri	☒ フィルタなし	☐ ブラックリスト	☐ ホワイトリスト
2.4GHz-Sec	☒ フィルタなし	☐ ブラックリスト	☐ ホワイトリスト
5GHz-Pri	☒ フィルタなし	☐ ブラックリスト	☐ ホワイトリスト
5GHz-Sec	☒ フィルタなし	☐ ブラックリスト	☐ ホワイトリスト
6GHz-Pri	☒ フィルタなし	☐ ブラックリスト	☐ ホワイトリスト
6GHz-Sec	☒ フィルタなし	☐ ブラックリスト	☐ ホワイトリスト

2. パラメータを設定します。パラメータについての説明は表4-11を参照してください。

表 4-11 アクセス制御モード設定パラメータ

パラメータ名	パラメータの説明
フィルタなし	SSIDのアクセス制限を行いません。
ブラックリスト	登録されたSSIDからの接続を拒否する時に使用します。
ホワイトリスト	登録されたSSIDからの接続を許可する時に使用します。

3. 設定後、「設定」ボタンをクリックして設定を終了します。

アクセス制御 ルール設定

5. アクセス制御-ルール設定を表示して設定します。図4-21を参照してください。

図 4-21 アクセス制御-ルール設定画面

▼ アクセス制御-ルール設定

[アクセス制御ルールを設定する際の注意点](#)

▼ 新しいアイテム

名前

SSID

2.4GHz-Pri

MACアドレス

:

:

:

:

:

関連するデバイスから選択

設定

キャンセル

+

 新しいアイテムを作成する

6. パラメータを設定します。パラメータについての説明は表4-12を参照してください。

表 4-12 アクセス制御-ルール設定画面

パラメータ名	パラメータの説明
名前	アクセス制御の名前を設定します。
SSID	SSIDを選択してアクセスを制御するSSIDを設定します。
MACアドレス	無線デバイスのMACアドレスを設定します。 MACアドレス入力の下の「関連するデバイスから選択」をクリックすると接続中のデバイスのMACアドレスを指定できます。

7. 設定後、「設定」ボタンをクリックして設定を終了します。
8. 「新しいアイテムを作成する」をクリックするとアクセス制御ルールを追加できます。
9. 設定画面右上のゴミ箱イメージをクリックするとアクセス制御ルールを削除します。

アクセス制御ルールテーブルの参照

10. アクセス制御ルールテーブルを表示して設定中のアクセス制御ルールを参照できます。図4-22を参照してください。

図 4-22 アクセス制御ルールテーブル画面

▼ アクセス制御ルールテーブル		
SSID名	MACアドレス	ACLポリシー
SSID1	8e:15:88:88:74:b9	Ban
SSID5	8e:15:88:88:74:b9	Ban
SSID9	8e:15:88:88:74:b9	Ban

11. 「更新」ボタンをクリックすると最新の情報を表示します。

4.4.2.3 WLANバンドステアリング設定

このセクションでは、無線LANバンドステアリング機能を設定する方法について説明します。

WLANバンドステアリングは、ネットワーク負荷と信号強度に応じて、端末（携帯電話やラップトップなど）が2.4G、5G、または6G周波数帯域を介して本製品にアクセスするようにガイドするように設定され、端末のWi-Fi アクセスエクスペリエンスが向上します。

- クライアントデバイスが本製品に近い場合、バンドステアリング機能は端末を優先的に6G周波数帯域に接続するようにガイドします。これは6G周波数帯域は通常、より高速で干渉が少ないためです。（注：クライアントデバイスは6G Wi-Fiアクセスをサポートしている必要があります。）
- クライアントデバイスが本製品から遠く離れている場合、または 6GHz周波数帯域に多くのクライアントがある場合、バンドステアリングはクライアントデバイスに2.4Gまたは5GHz周波数帯域に切り替えるように指示し、ワイヤレスエクスペリエンスを向上させることができます。

手順

1. Web管理メイン画面で、メニュー[LAN] > [ステータス] > [無線LAN] > [WLANバンドステアリング]を選択して、WLANバンドステアリングページに入ります。図4-23を参照してください。

図 4-23 WLANバンドステアリング画面

▼ WLANバンドステアリング

[バンドステアリング機能を構成する際に注意すべきことは何ですか？](#)

バンドステアリング ☒ オン ☐ オフ

設定

キャンセル

2. パラメータを設定します。パラメータについての説明は表4-13を参照してください。

表 4-13 WLANバンドステアリング設定パラメータ

パラメータ名	パラメータの説明
バンドステアリング	● オン: バンドステアリング機能を有効にします。 ● オフ: バンドステアリング機能を無効にします。 バンドステアリング機能を無効にすると、5GHz周波数帯のSSID名とパスワードは、バンドステアリング機能を有効にする前の設定に復元されます。

3. 設定後、「設定」ボタンをクリックして設定を終了します。

4.4.2.4 MLOの設定

本製品はMLO機能をサポートし、ルーターが2.4GHz、5GHz、および6GHzの周波数帯を同時に使用してデータを伝送することを可能にします。これによりネットワークの速度と安定性が向上します。

手順

1. Web管理メインページで、メニュー[LAN] > [無線LAN] > [MLO]を選択し、MLO設定ページを開きます。図4-24を参照してください。

図 4-24 MLO設定画面

▼ MLO

MLO を有効にすると、プライマリの2.4GHz 2.4GHz-Priの構成が、SSID 名、暗号化タイプ、WPA パスフレーズを含め、プライマリの5GHz-Priおよび6GHz-Priの両方に同期されます。さらに、すべての無線がオンになり、各無線のプライマリのSSIDも有効になります。

MLO有効

☒ オン ☐ オフ

設定

キャンセル

2. パラメータを設定します。パラメータの説明については表4-14を参照してください。

表 4-14 MLOモードパラメータ

パラメータ名	パラメータの説明
MLO有効	● オン: MLO機能を有効にする。 ● オフ: MLO機能を無効にする。

3. 設定後、「設定」ボタンをクリックして設定を終了します。

4.4.2.5 WPSの設定

WPS機能を有効にすると、デバイスはネットワーク名とワイヤレス暗号化キーを自動的に構成できるため、ワイヤレス ネットワーク暗号化の構成プロセスが簡素化されます。WPSは高速なネットワーク接続を提供しますが、セキュリティ上のリスクも伴う可能性があります。セキュリティ要件が高いシナリオでは、WPS機能を無効にすることをお勧めします。

手順

1. Web管理メインページで、メニュー [LAN] > [無線LAN] > [WPS] を選択して、WPS設定ページに入ります。図4-25を参照してください。

図 4-25 WPS設定ページ

2. パラメータを設定します。パラメータについての説明は表4-15を参照してください。

表 4-15 WPSモードパラメータ

パラメータ名	パラメータの説明
WPSモード	● PBC (プッシュボタン接続): 本製品のWPSボタンで操作できるようになります。 ● 無効: WPSモードが「無効」に設定されている場合、WPS動作は完全に停止されます。ユーザーはWPSのクイック接続機能を使用して無線接続を確立することができず、SSIDやパスワードの入力などを含むネットワーク設定を手動で構成する必要があります。

3. 設定後、「設定」ボタンをクリックして設定を終了します。

4.4.3 LANの設定

このセクションでは、LAN (IPv4) を構成する方法について説明します。

インターネットステータスの関連情報には、割り当てられたアドレス (DHCP)、DHCP サーバー、DHCP バインディング、およびポート制御が含まれます。

手順

割り当てアドレス (DHCP)の確認

1. Web管理メインページで、メニュー [LAN] > [LAN] > [IPv4] を選択して、LAN設定ページに入り、割り当てアドレス (DHCP) を表示します。図4-26を参照してください。

図 4-26 割り当てアドレス (DHCP) の表示

▼ 割り当てアドレス (DHCP)				
ホスト名	MACアドレス	IPアドレス	ポート	リース残時間
A23866605	c8:09:a8:6d:25:b8	192.168.0.1	SSID6	23時 58分 44秒
				<button>更新</button>

2. 「更新」ボタンをクリックすると最新の情報を表示します。

DHCPサーバー機能の設定

3. DHCPサーバーを表示し、DHCPサーバー機能を設定します。図4-27を参照してください。

図 4-27 DHCPサーバー設定画面

▼ DHCPサーバー

DHCPサーバー

☒ オン
☐ オフ

LAN側IPアドレス

192
168
0
254

サブネットマスク

255
255
255
0

DHCP割当開始IPアドレス

192
168
0
1

DHCP割当終了IPアドレス

192
168
0
253

ISP DNSサーバー

☐ オン
☒ オフ

プライマリDNSサーバー

192
168
0
254

セカンダリDNSサーバー

0
0
0
0

リース期間モード

カスタム
▼

リース期間

86400
秒

設定

キャンセル

- パラメータを設定します。パラメータについての説明は表4-16を参照してください。

表 4-16 DHCPサーバー設定パラメータ

パラメータ名	パラメータの説明
DHCPサーバー	本製品を DHCP サーバーとして機能させ、IP アドレスをクライアント PC または無線デバイスに割り当てます。 ● オン：DHCP サーバー機能を有効にします。 ● オフ：DHCP サーバー機能を無効にします。
LAN側IPアドレス	LAN用のIPv4アドレス
サブネットマスク	LAN用のサブネットマスク
DHCP割当開始IPアドレス	DHCPアドレスプールの開始IPアドレス
DHCP割当終了IPアドレス	DHCPアドレスプールの終了IPアドレス
ISP DNSサーバー	● オン：DN サーバーを手動設定します。 ● オフ：手動設定のDNSサーバーを無効にします。
プライマリDNSサーバー	ISP から提供された DNS サーバーの IP アドレス
セカンダリDNSサーバー	ISP から提供された DNS サーバー2 の IP アドレス

リース期間モード	リースタイムのモードを選択します。 ● カスタム：リース期間（秒）で時間設定を可能にします。 ● 無限：リース期間は無制限にします。
リース期間	リース期間モードをカスタムに設定したときのみ、設定が可能です。 クライアント PC が DHCP サーバーによって割り当てられた IP アドレスを使用している時間を設定します。リース期限が切れると、プライベート IP アドレスは他のネットワークデバイスに割り当てられるようになります。 初期値：86400 範囲：60 ～ 157680000

5. 設定後、「設定」ボタンをクリックして設定を終了します。

DHCPバインディング設定

6. DHCPバインディングを表示し、DHCPバインディング機能を設定します。[図4-28](#)を参照してください。

図 4-28 DHCPバインディング設定画面

7. パラメータを設定します。パラメータについての説明は[表4-17](#)を参照してください。

表 4-17 DHCPバインディング設定パラメータ

パラメータ名	パラメータの説明
名前	DHCPバインディングの名前を設定します。
MACアドレス	DHCPバインディングのMACアドレスを設定します。
IPアドレス	DHCPバインディングのIPアドレスを設定します。

8. 設定後、「設定」ボタンをクリックして設定を終了します。
9. 「新しいアイテムを作成する」をクリックするとDHCPバインディングを追加できます。
10. 設定画面右上のゴミ箱イメージをクリックすると DHCP バインディングを削除します。

ポート制御の設定

11. ポート制御画面を表示し、DHCPポート制御機能を設定します。SSIDごとにDHCP制御のオン、オフを指定します。図4-29を参照してください。.

図 4-29 ポート制御機能画面

▼ ポート制御

SSID1	☒ オン ☐ オフ
SSID2	☒ オン ☐ オフ
SSID3	☒ オン ☐ オフ
SSID4	☒ オン ☐ オフ
SSID5	☒ オン ☐ オフ
SSID6	☒ オン ☐ オフ
SSID7	☒ オン ☐ オフ
SSID8	☒ オン ☐ オフ
SSID9	☒ オン ☐ オフ
SSID10	☒ オン ☐ オフ
SSID11	☒ オン ☐ オフ
SSID12	☒ オン ☐ オフ

すべてオン | すべてオフ

設定 キャンセル

12. 設定後、「設定」ボタンをクリックして設定を終了します。



注:

- 「すべてオン」をクリックするとすべてのSSIDがオンとなります。
- 「すべてオフ」をクリックするとすべてのSSIDがオフとなります。

4.4.4 ルーティングの設定

4.4.4.1 IPv4ルーティング設定

手順

ルーティングテーブルの確認

1. Web管理メインページで、メニュー [LAN] > [ルーティング] > [IPv4] を選択して、IPv4ページに入り、ルーティングテーブルを表示します。図4-30を参照してください。

図 4-30 ルーティングテーブルの表示

▼ ルーティングテーブル			
ネットワークアドレス	サブネットマスク	ゲートウェイ	インタフェース
192.168.0.0	255.255.255.0	0.0.0.0	LAN
			<button>更新</button>

2. 「更新」ボタンをクリックすると最新の情報を表示します。

静的ルーティングの設定

3. 静的ルーティング設定を表示します。図4-31を参照してください。

図 4-31 静的ルーティング(IPv4)設定画面

▼ 静的ルーティング

静的ルーティングを設定する際に注意すべき点は何ですか?

▼ 新しいアイテム

名前

Egress

選んでください ▼

ネットワークアドレス

サブネットマスク

ゲートウェイ

設定

キャンセル

+

 新しいアイテムを作成する

4. パラメータを設定します。パラメータについての説明は表4-18を参照してください。

表 4-18 静的ルーティング(IPv4)設定パラメータ

パラメータ名	パラメータの説明
名前	静的ルーティングエントリの名前
Egress	● LAN : LAN側ネットワーク ● DHCP : インターネット側ネットワーク
ネットワークアドレス	宛先ネットワークのネットワークアドレス、ネットワークアドレスとサブネットマスクの両方が0.0.0.0の場合、この構成は初期値のルーティングになり、どの宛先アドレスにも有効です。
サブネットマスク	宛先ネットワークのサブネットマスク
ゲートウェイ	ネットワークインターフェースが属するネットワークセグメントのゲートウェイ

5. 設定後、「設定」ボタンをクリックして設定を終了します。
6. 「新しいアイテムを作成する」をクリックすると静的ルーティングエントリを追加できます。
7. 設定画面右上のゴミ箱イメージをクリックすると静的ルーティングエントリを削除します。

ポリシールーティングの設定

ユーザーが独自に設定した特定の経路にデータを転送することができます。ポリシールーティングにより、通信経路の負荷を分散したり重要な帯域を保証したりすることができ、ネットワークの運用をより効率的に実現できます。

8. 図4-32を参照してください。

図 4-32 ポリシールーティング(IPv4)設定画面

9. パラメータを設定します。パラメータについての説明は表4-19を参照してください。

表 4-19 ポリシールーティング(IPv4)設定パラメータ

パラメータ名	パラメータの説明
名前	ポリシールーティングエントリの名前
Egress	● LAN：LAN側ネットワーク ● DHCP：インターネット側ネットワーク
送信元IPアドレス	合致するパケットの送信元IPアドレス
送信元マスク	合致するパケットの送信元ネットマスク
宛先IPアドレス	合致するパケットの宛先IPアドレス
宛先マスク	合致するパケットの宛先ネットマスク
プロトコル	● ICMP：ポリシーにICMPを設定 ● TCP：ポリシーにTCPを設定 ● UDP：ポリシーにUDPを設定 ● 任意：TCP、UDP、ICMPを設定
送信元MACアドレス	合致するパケットを送信する送信元デバイスのMACアドレス MACアドレス入力の下の「関連するデバイスから選択」をクリックすると接続中のデバイスのMACアドレスを指定できます。

10. 設定後、「設定」ボタンをクリックして設定を終了します。

11. 「新しいアイテムを作成する」をクリックするとポリシールーティングエントリを追加できます。

12. 設定画面右上のゴミ箱イメージをクリックするとポリシールーティングエントリを削除します。

4.4.4.2 IPv6ルーティング設定

手順

ルーティングテーブルの確認

1. Web管理メインページで、メニュー [LAN] > [ルーティング] > [IPv6] を選択して、IPv6ページに入り、ルーティングテーブルを表示します。図4-33を参照してください。

図 4-33 IPv6ルーティングテーブル

▼ ルーティングテーブル		
プレフィックス	ゲートウェイ	インタフェース
fe80::1/128	::	LAN
fe80::/64	::	LAN
		<button>更新</button>

2. 「更新」ボタンをクリックすると最新の情報を表示します。

静的ルーティング設定

3. 静的ルーティング設定を表示します。図4-34を参照してください。

図 4-34 静的ルーティング(IPv6)設定画面

▼ 静的ルーティング

静的ルーティングを設定する際に注意すべき点は何ですか?

▼ 新しいアイテム

名前

Egress

選んでください

プレフィックス

ゲートウェイ

設定

キャンセル

+

 新しいアイテムを作成する

4. パラメータを設定します。パラメータについての説明は表4-20を参照してください。

表 4-20 静的ルーティング(IPv6)設定パラメータ

パラメータ名	パラメータの説明
名前	静的ルーティングエントリの名前
Egress	LAN : LAN側ネットワーク
プレフィックス	IPv6 プレフィックスアドレス プレフィックスが:: / 0の場合、この構成は初期値のルーティングで、任意の宛先アドレスに有効です。
ゲートウェイ	ネットワークインターフェースが属するネットワークセグメントのゲートウェイ

5. 設定後、「設定」ボタンをクリックして設定を終了します。
6. 「新しいアイテムを作成する」をクリックすると静的ルーティングエントリを追加できます。
7. 設定画面右上のゴミ箱イメージをクリックすると静的ルーティングエントリを削除します。

ポリシールーティングの設定

8. ポリシールーティング設定を表示します。[図4-35](#)を参照してください。

図 4-35 ポリシールーティング(IPv6)設定画面

▼ ポリシールーティング

▼ 新しいアイテム 

名前

Egress ▼

送信元IPアドレス /

宛先IPアドレス /

プロトコル ▼

送信元MACアドレス : : : : :

[関連するデバイスから選択](#)

 新しいアイテムを作成する

9. パラメータを設定します。パラメータについての説明は[表4-21](#)を参照してください。

表 4-21 ポリシールーティング(IPv6)設定パラメータ

パラメータ名	パラメータの説明
名前	ポリシールーティングエントリの名前
Egress	LAN : LAN側ネットワーク
送信元IPアドレス	合致するパケットの送信元IPアドレス
宛先IPアドレス	合致するパケットの宛先IPアドレス
プロトコル	● ICMP : ポリシーにICMPを設定 ● TCP : ポリシーにTCPを設定 ● UDP : ポリシーにUDPを設定 ● 任意 : TCP、UDP、ICMPを設定
送信元MACアドレス	合致するパケットを送信する送信元デバイスのMACアドレス MACアドレス入力の下に「関連するデバイスから選択」をクリックすると接続中のデバイスのMACアドレスを指定できます。

10. 設定後、「設定」ボタンをクリックして設定を終了します。
11. 「新しいアイテムを作成する」をクリックするとポリシールーティングエントリを追加できます。
12. 設定画面右上のゴミ箱イメージをクリックするとポリシールーティングエントリを削除します。

4.5 管理と診断の設定

4.5.1 アカウント管理の設定

本製品のパスワードを変更することで、ネットワークを保護し、権限のない人がネットワークにアクセスするのを防ぐことができます。以下のルールでパスワードを強力にしてください:

- パスワードの長さは8文字以上
- パスワードは数字、アルファベット、および記号で構成

手順

1. Web管理メイン画面で、メニュー[管理&診断] > [アカウント管理]を選択し、管理者アカウント管理ページに入ります。図4-36を参照してください。

図 4-36 アカウント管理画面

2. パラメータを設定します。パラメータについての説明は表4-22を参照してください。

表 4-22 管理者アカウント管理パラメータ

パラメータ名	パラメータ説明
ユーザー名	ユーザー名はadmin固定（変更不可）
旧パスワード	変更前パスワード
新パスワード	新しいパスワード
パスワードの確認	新しいパスワードの再入力

3. 設定後、「設定」ボタンをクリックして設定を終了します。

4.5.2 アイドルタイムアウトの設定

アイドル タイムアウト時間を設定して、本製品のセキュリティを強化します。ユーザーが一定時間内に操作を行わない場合、自動的にユーザーをログアウトし、権限のない人物がユーザーのセッションを使用して不正な操作を行うことを防ぎます。

手順

1. Web管理メイン画面で、メニュー[管理&診断] > [アイドルタイムアウト]を選択して、アイドルタイムアウトページに入ります。図4-37を参照してください。

図 4-37 アイドルタイムアウトページ

▼ アイドルタイムアウト

タイムアウト

分

設定

キャンセル

2. パラメータを設定します。パラメータについての説明は表4-23を参照してください。

表 4-23 アイドルタイムアウトパラメータ

パラメータ名	パラメータ説明
タイムアウト	ユーザーが自動的にログアウトされるまでのアイドル時間（最大30分） 単位: 分

3. 設定後、「設定」ボタンをクリックして設定を終了します。



注:

アイドルタイムアウト設定は、システムに再度ログインした後に有効になります。

4.5.3 システム管理設定

4.5.3.1 デバイス管理設定.

システム管理ページで、デバイスを再起動できます。再起動後、構成パラメータはクリアされないため、H3701Qを再構成する必要はありません。工場出荷時の設定を復元すると、ネットワーク設定やパスワードなど、デバイスのすべての設定と構成がクリアされます。

- デバイスの再起動の主な機能には、キャッシュの解放、急速な劣化の防止、デバイスの耐用年数の延長などがあります。
- 工場出荷時設定の復元機能は、次のシナリオに適用されます:
- デバイスの故障：ホームゲートウェイにネットワーク接続の問題、パフォーマンスの低下、またはその他の障害が発生した場合、工場出荷時の設定に戻すことで、デバイスを正常な動作状態に戻すことができます。
- デバイスのパスワードや設定を忘れた場合：ホームゲートウェイの管理者パスワードやその他の重要な設定を忘れた場合、デバイスを工場出荷時のデフォルト設定に復元し、デバイスを再設定することができます。

手順

1. Web管理メイン画面で、メニュー[管理&診断] > [システム管理] > [デバイス管理]を選択して、デバイス管理ページへ入ります。図4-38を参照してください。

図 4-38 デバイスリブート、リセット画面

▼ リブート機能

この操作完了後、本装置は自動的に再起動します。

注：再起動操作は、現在のすべてのサービスを中断します。

リブート

▼ リセット機能

工場出荷時のリセット：すべてのパラメータ設定が工場出荷時の状態に戻ります。この操作が完了すると、デバイスは自動的に再起動します。

注：この操作が終了すると、すべての設定が初期化され、工場出荷時の状態に戻ります。

リセット

2. (再起動の場合)「リブート」ボタンをクリックしてください。
3. (工場出荷時設定への復元の場合)「リセット」ボタンをクリックしてください。

4.5.3.2 ソフトウェアアップグレード

ソフトウェアアップグレードの目的は、既知のセキュリティ脆弱性を修正し、新しい機能を追加し、システムパフォーマンスを向上させ、ネットワーク接続の安定性とセキュリティを確保します。

前提条件

アップグレード用のファイルが必要となります。

手順

 注：

- 本製品では自動でソフトウェアアップグレードを行うため、通常使用時にはこの操作は使用しません。
- ソフトウェアアップグレード中は電源を切らないでください。
- アップグレード後、自動的に再起動を実行します。

1. Web管理メイン画面で、メニュー[管理&診断] > [システム管理] > [ソフトウェアのアップグレード]を選択して、ソフトウェアのアップグレード画面に入ります。図4-39を参照してください。

図 4-39 ソフトウェアのアップグレードページ

▼ ソフトウェアのアップグレード

ⓘ アップグレード後にデバイスが再起動します。

ソフトウェアのバージョンファイルを選択してください:

ファイルの選択

ファイルが選択されていません

アップグレード

2. 「ファイルの選択」をクリックしてサービスプロバイダーから提供されたアップグレード用ファイルを指定してください。
3. 「アップグレード」ボタンをクリックすると、アップグレード確認のポップアップを表示します。「OK」ボタンをクリックするとソフトウェアのアップグレードを開始します。

70

4.5.3.3 自動アップグレード設定

本製品はソフトウェアを自動でアップグレードします。自動アップグレードの設定を行います。バージョンアップが完了すると、本製品は自動的に再起動を実施します。

手順

1. Web管理メイン画面で、メニュー[管理&診断] > [システム管理] > [自動アップグレード]を選択して、自動アップグレード画面に入ります。図4-40を参照してください。

図 4-40 自動アップグレード

▼ ソフトウェアのアップグレード

☒ 自動 ☐ 手動

アップグレード後にデバイスが再起動します。

ソフトウェアアップグレード用のURLを記入してください。

ソフトウェアアップグレードの時刻を設定してください。

時から

時まで

設定

キャンセル

2. パラメータを設定します。パラメータについての説明は表4-24を参照してください。

表 4-24 自動アップグレード設定パラメータ

パラメータ名	パラメータ説明
自動	このモードでは、自動的にアップグレードを検出し、指定された時刻の範囲内で自動的にソフトウェアをアップグレードします。
手動	このモードでは、自動的にアップグレードを検出し、検出された状態時にアップグレード用のポップアップ表示します。「アップグレード」ボタン をクリックするとアップグレードを開始します。図4-41を参照してください。
URL	サービスオペレータから提供されたURLを入力してください。
アップグレード時刻	アップグレードを開始する時刻を指定してください。自動設定でアップグレードを検出した場合には、指定された時間内でランダムにアップグレードを開始します。

図 4-41 手動設定時にアップグレードポップアップ



3. 設定後、「設定」ボタンをクリックして設定を終了します。

4.5.4 ログ管理

このセクションでは、本製品のログ管理機能について説明します。

- システムログに記録されたエラーや警告情報を確認することで、ネットワーク障害の具体的な症状や可能性のある原因を把握することができます。
- リモートログ管理機能により、本製品がログ情報をリモートのログサーバーやストレージデバイスに送信することができます。この機能を有効にする主な目的は、管理者が本製品の動作状態をリモートで監視・分析し、潜在的な問題を迅速に発見し解決するためです。

手順

システムログの確認

1. Web管理メイン画面で、メニュー[管理&診断] > [ログ管理]を選択して、ログ管理画面に入ります。システムログ管理画面でシステムログを確認できます。図4-42を参照してください。

図 4-42 システムログ管理画面

▼ システムログ管理

ログの保存 ☒ オン ☐ オフ

設定 キャンセル

ログ出力

```

2025-01-06T08:10:12Z [Error] [wlan_hostapd0..] pid[298]asend EVENT[0XA92F] Len=[116] sendto
[multiapd.map.slave] ERROR,swLen=[-1] errno=[111:Connection refused]!!!
P0000-00-00T00:01:38 [Error] Web get fail. (objname: OBJ_WLAN_STAPROFILE_ID identity: DEV.WIFI.STAIF1 iRet: -3)
P0000-00-00T00:01:44 [Error] Web get fail. (objname: OBJ_WLAN_STAPROFILE_ID identity: DEV.WIFI.STAIF1 iRet: -3)
P0000-00-00T00:01:48 [Error] Web user is authenticated fail from the host(192.168.0.100).authCode == 201
P0000-00-00T00:01:48 [Error] Web user is authenticated fail from the host(192.168.0.100).authCode == 204[Appear
4 times]
P0000-00-00T00:03:57 [Error] Web set failed. (objname: OBJ_USERINFO_ID identity: IGD.AU1 iRet: -264)
P0000-00-00T00:04:02 [Error] Web set failed. (objname: OBJ_USERINFO_ID identity: IGD.AU1 iRet: -264)
P0000-00-00T00:04:03 [Error] Web set failed. (objname: OBJ_USERINFO_ID identity: IGD.AU1 iRet: -264)
P0000-00-00T00:07:32 [Error] Web user is authenticated fail from the host(192.168.0.1).authCode == 204
P0000-00-00T00:08:15 [Error] Web user is authenticated fail from the host(192.168.0.1).authCode == 204
  
```

更新 ログダウンロード

2. パラメータの設定、ログ表示を参照します。パラメータについての説明は表4-25を参照してください。

表 4-25 システムログ管理パラメータ

パラメータ名	パラメータ説明
ログの保存	オンの場合にはシステムログを取得し、ログを出力します。
ログ出力	システムログを表示します。

3. ログの保存設定後、「設定」ボタンをクリックして設定を完了します。
4. 「更新」ボタンをクリックすると最新のログをログ出力へ表示します。
5. 「ログダウンロード」ボタンをクリックすると、システムログをダウンロードすることができます。

セキュリティログ管理

1. セキュリティログ管理画面でセキュリティログを確認できます。図4-43を参照してください。

図 4-43 セキュリティログ管理画面

▼ セキュリティログ管理

ログの保存 ☒ オン ☐ オフ

設定 キャンセル

ログ出力

```
P0000-00-00T00:23:43 The device is restored to the factory settings.
P0000-00-00T00:23:43 reboot for module(DB) msg : reset(4)
P0000-00-00T00:00:41 System start!
P0000-00-00T00:00:46 Telnet: will start...
P0000-00-00T00:00:46 SSH: will start...
2024-11-02T22:34:27Z System start!
2024-11-02T22:34:33Z Telnet: will start...
2024-11-02T22:34:34Z SSH: will start...
2024-11-02T22:47:41Z Msntp synchronized localtime success!dwTimeOffset=-962058649
current time is Sat Nov 2 22:47:41 2024
2024-11-02T22:47:49Z WLAN: PSK password of [SSID1] has been changed!
```

更新 ログダウンロード

2. パラメータの設定、ログ表示を参照します。パラメータについての説明は表4-26を参照してください。

表 4-26 セキュリティログ管理パラメータ

パラメータ名	パラメータ説明
ログの保存	オンの場合にはシステムログを取得し、ログを出力します。
ログ出力	システムログを表示します。

3. ログの保存設定後、「設定」ボタンをクリックして設定を完了します。
4. 「更新」ボタンをクリックすると最新のログをログ出力へ表示します。
5. 「ログダウンロード」ボタンをクリックすると、システムログをダウンロードすることができます。

リモートログの管理

1. リモートログ管理画面でリモートログサーバへのログの転送を設定できます。図4-44を参照してください。

図 4-44 リモートログ管理画面

▼ リモートログ管理

リモートログ ☒ オン ☐ オフ

リモートログサーバ

設定 キャンセル

- パラメータを設定します。パラメータについての説明は表4-27を参照してください。

表 4-27 リモートログ管理画面

パラメータ名	パラメータ説明
リモートログ	オンの場合には、指定されたリモートログサーバにログメッセージの送信を開始します。 オフの場合には、リモートサーバへのログメッセージの送信を停止し、ログメッセージをローカルにのみ保存します。
リモートログサーバ	ログメッセージ送信先のリモートログサーバのIPアドレス リモートログがオンの場合に表示します。

- 設定後、「設定」ボタンをクリックして設定を終了します。

4.5.5 診断

診断機能では、障害箇所の特定や日常メンテナンスのためのPing診断とトレースルート診断を提供します。

- **Ping診断**: ユーザのホストから別のホストへのネットワークが接続されているかどうかをテストするために使用されます。
- **トレースルート診断**: ユーザーのホストから別のホストへのネットワーク経路を表示します。

手順

Ping診断の実行

- Web管理メインページで、メニュー[管理と診断] > [ネットワーク診断] > [PING診断] を選択して、PING診断ページに入ります。図4-45を参照してください。

図 4-45 PING診断画面

▼ PING診断

IPアドレス/ホスト名

Egress ▼

繰り返し回数

パケットサイズ ▼ bytes

タイムアウト ms

診断結果

2. パラメータを設定します。パラメータについての説明は表4-28を参照してください。

表 4-28 PING診断パラメータ

パラメータ名	パラメータ説明
IPアドレス/ホスト名	Pingを実施する宛先のIPアドレス/ホスト名を設定します。
Egress	Pingテストを実施したいインターフェースを選択します。 ● オート：設定したアドレスによりLAN側/WAN側を自動判別し、PINGテストを実行します。 ● LAN：LAN側のテストを実行する場合に選択します。 ● DHCP：WAN側のテストを実行する場合に選択します。
繰り返し回数	Pingリクエストメッセージの送信回数
パケットサイズ	Pingリクエストメッセージのパケットサイズ
タイムアウト	各Pingからの応答を待機する最大時間。設定した時間内に応答が受信されない場合、Ping要求は失敗したとみなされます。

3. 「診断」ボタンをクリックすると、システムは指定されたアドレスへのPingを開始します。繰り返し回数で指定された回数のPing操作を実行し、結果が下の診断結果ボックスに表示されます。

トレースルート診断の実行

1. トレースルート診断画面を表示します。図4-46を参照してください。

図 4-46 トレースルート診断画面

▼ トレースルート診断

IPアドレス/ホスト名

インターフェース

オートセンス ▼

最大ホップ数

30

待ち時間

5000

ms

プロトコル

UDP ▼

診断

診断結果

2. パラメータを設定します。パラメータについての説明は表4-29を参照してください。

表 4-29 トレースルート診断設定パラメータ

パラメータ名	パラメータ説明
IPアドレス/ホスト名	トレースルート診断を実施する宛先のIPアドレス/ホスト名を設定します。
Egress	トレースルート診断を実施したいインターフェースを選択します。 ● オート：設定したアドレスによりLAN側/WAN側を自動判別し、PINGテストを実行します。 ● LAN：LAN側のテストを実行する場合に選択します。

	● DHCP：WAN側のテストを実行する場合に選択します。
最大ホップ数	最大ホップ数を設定します。初期値：30、範囲は1から64までとなります。
待ち時間	応答パケットを待機する時間を設定します。単位：ミリ秒です。この期間内に応答パケットが受信されない場合は、アスタリスクが表示されます。
プロトコル	プロトコルを選択します ● UDP：UDPを設定します。 ● ICMP：ICMPを設定します。

3. 「診断」ボタンをクリックして上記の設定を完了すると、診断が開始され、下の診断結果ボックスに結果が表示されます。

4.5.6 動作モード設定

ネットワーク内の動作モードを切り替える方法について説明します。

- **コントローラー (ルーター)**: Wi-Fi メッシュネットワーク内のコントローラとして機能します。
- **エージェント**: Wi-Fi メッシュネットワーク内のエージェントとして機能します。

手順

1. Web管理メイン画面で、メニュー[管理&診断] > [動作モード]を選択して、動作モード画面に入ります。図4-47を参照してください。

図 4-47 動作モードページ

▼ 動作モード

モード

2. パラメータを設定します。パラメータについての説明は表4-30を参照してください。

表 4-30 動作モードパラメータ

パラメータ名	パラメータの説明
モード	● メッシュ自動 (DHCP): 接続する機器に応じて自動的にコントローラーモードまたはエージェントモードに切り替えます。 ● コントローラー (ルーター): コントローラーモードで動作します。 ● エージェント: エージェントモードで動作します。

3. 設定後、「設定」ボタンをクリックして設定を終了します。

5 よくある質問

コンセントに電源プラグを入れても、フロントパネルの電源ランプが点灯しない

- 電源が未接続。
- 電源アダプタがデバイスに正しく接続されていません。デバイスに付属の電源アダプタを使用していることを確認してください。

工場出荷時のデフォルト設定を復元

本製品の電源がオンで動作しているときに、針などの細い棒を使用してRESETボタンを5秒以上押し続けると、工場出荷時の設定の復元が完了し、ルーターが自動的に再起動します。

工場出荷時の設定に復元した後、設定パラメータはクリアされるため、本製品を再設定する必要があります。



図 3-1 H3701Q ハードウェア接続図（エージェントモード）	8
図 3-2 H8748Qログインページ	9
図 3-3 トポロジー画面（本製品接続時）	10
図 3-4 H3701Q（エージェントモード）ログインページ	11
図 3-5 H3701Q（エージェントモード）パスワード変更画面	11
図 3-6 H3701Q（Agentモード）管理画面	12
図 3-7 無線LANステータスページ	13
図 3-8 無線LANクライアントステータスページ	13
図 3-9 アクセス制御ルールテーブルページ	14
図 3-10 MLOページ	15
図 3-11 WPS設定ページ	16
図 3-12 WLAN検出ページ	17
図 3-13 アカウント管理画面	18
図 3-14 アイドルタイムアウトページ	19
図 3-15 デバイスリブート、リセット画面	20
図 3-16 ソフトウェアのアップグレードページ	21
図 3-17 自動アップグレード	22
図 3-18 手動設定時にアップグレードポップアップ	23
図 3-19 システムログ管理画面	24
図 3-20 セキュリティログ管理画面	25
図 3-21 リモートログ管理画面	26
図 3-22 PING診断画面	27
図 3-23 トレースルート診断画面	28
図 3-24 動作モードページ	30
図 4-1 H3701Q ハードウェア接続図（コントローラーモード）	32
図 4-2 H3701Qのログインページ	32
図 4-3 H3701Q（コントローラーモード）パスワード変更画面	33
図 4-4 H3701Qコントローラー（ルーター）モード管理ページ	33
図 4-5 トポロジー画面	34
図 4-6 インターネットインターフェース情報	35
図 4-7 インターネット接続ステータス	36
図 4-8 フィルタスイッチとモード設定画面	36
図 4-9 URLフィルタ画面	37
図 4-10 IPフィルタ画面	38
図 4-11 DMZ画面	40
図 4-12 SNTP画面	41

図 4-13 IGMPモード.....	42
図 4-14 MLDモード画面	43
図 4-15 無線LANステータス画面	44
図 4-16 無線LANクライアントステータス画面.....	44
図 4-17 無線LANオン/オフ設定	45
図 4-18 無線LAN詳細設定画面.....	46
図 4-19 無線LAN SSID設定画面	49
図 4-20 アクセス制御-モード設定画面	51
図 4-21 アクセス制御-ルール設定画面	52
図 4-22 アクセス制御ルールテーブル画面	53
図 4-23 WLANバンドステアリング画面	54
図 4-24 MLO設定画面.....	55
図 4-25 WPS設定ページ.....	56
図 4-26 割り当てアドレス（DHCP）の表示	57
図 4-27 DHCPサーバー設定画面.....	58
図 4-28 DHCPバインディング設定画面	59
図 4-29 ポート制御機能画面	60
図 4-30 ルーティングテーブルの表示.....	61
図 4-31 静的ルーティング(IPv4)設定画面.....	61
図 4-32 ポリシールーティング(IPv4)設定画面	63
図 4-33 IPv6ルーティングテーブル	64
図 4-34 静的ルーティング(IPv6)設定画面.....	64
図 4-35 ポリシールーティング(IPv6)設定画面	65
図 4-36 アカウント管理画面	67
図 4-37 アイドルタイムアウトページ	68
図 4-38 デバイスリブート、リセット画面	69
図 4-39 ソフトウェアのアップグレードページ.....	70
図 4-40 自動アップグレード.....	71
図 4-41 手動設定時にアップグレードポップアップ	72
図 4-42 システムログ管理画面	73
図 4-43 セキュリティログ管理画面	74
図 4-44 リモートログ管理画面.....	75
図 4-45 PING診断画面	76
図 4-46 トレースルート診断画面	77
図 4-47 動作モードページ.....	78

表

表 3-1 MLOモードパラメータ	15
表 3-2 WPSモードパラメータ	16
表 3-3 管理者アカウント管理パラメータ	18
表 3-4 アイドルタイムアウトパラメータ	19
表 3-5 システムログ管理パラメータ	24
表 3-6 セキュリティログ管理パラメータ	25
表 3-7 リモートログ管理画面	26
表 3-8 PING診断パラメータ	27
表 3-9 トレースルート診断設定パラメータ	29
表 3-10 動作モードパラメータ	30
表 4-1 フィルタスイッチ、モードパラメータ	37
表 4-2 URLフィルタパラメータ	37
表 4-3 IPフィルタパラメータ	39
表 4-4 DMZ設定パラメータ	40
表 4-5 SNTPパラメータ	41
表 4-6 IGMPモードパラメータ	42
表 4-7 MLDモードパラメータ	43
表 4-8 無線LANオン/オフ設定パラメータ	45
表 4-9 無線LAN詳細設定パラメータ	47
表 4-10 無線LAN SSID設定パラメータ	49
表 4-11 アクセス制御モード設定パラメータ	52
表 4-12 アクセス制御-ルール設定画面	53
表 4-13 WLANバンドステアリング設定パラメータ	54
表 4-14 MLOモードパラメータ	55
表 4-15 WPSモードパラメータ	56
表 4-16 DHCPサーバー設定パラメータ	58
表 4-17 DHCPバインディング設定パラメータ	60
表 4-18 静的ルーティング(IPv4)設定パラメータ	62
表 4-19 ポリシールーティング(IPv4)設定パラメータ	63
表 4-20 静的ルーティング(IPv6)設定パラメータ	65
表 4-21 ポリシールーティング(IPv6)設定パラメータ	66
表 4-22 管理者アカウント管理パラメータ	67
表 4-23 アイドルタイムアウトパラメータ	68
表 4-24 自動アップグレード設定パラメータ	71
表 4-25 システムログ管理パラメータ	73
表 4-26 セキュリティログ管理パラメータ	74
表 4-27 リモートログ管理画面	75

表 4-28 PING診断パラメータ	76
表 4-29 トレースルート診断設定パラメータ	77
表 4-30 動作モードパラメータ	79

用語、略語

AP

- Access Point, Access Point

DHCP

- Dynamic Host Configuration Protocol

DMZ

- Demilitarized Zone, isolation area

DNS

- Domain Name System

DSCP

- Differentiated Services Code Point

ICMP

- Internet Control Message Protocol, Internet control packet protocol

IGMP

- Internet Group Management Protocol

IP

- Internet Protocol, Internet Protocol

IPoA

- IP over ATM, which is an IP packet carried on the ATM network.

IPv4

- Internet Protocol Version V4

IPv6

- Internet Protocol Version V6

ISP

- Internet Service Provider

LAN

- Local Area Network, LAN

MAC

- Media Access Control

MLD

- Multicast Listener Discovery, multicast listening and discovery

MLO

- Multi-Link Operation

NTP

- Network Time Protocol

ONU

- Optical Network Unit

PC

- Personal Computer

PPPoE

- Point to Point Protocol over Ethernet

SGI

- Short Guard Interval, short protection interval

SNTP

- Simple Network Time Protocol

SSID

- Service Set Identifier, service set ID

TCP

- Transmission Control Protocol

TOS

- Termination of Service, service termination

UDP

- User Datagram Protocol

URL

- Uniform Resource Locator

WAN

- Wide Area Network, WAN

WLAN

- Wireless Local Area Network

WPA

- Wi-Fi Protected Access, Wi-Fi Network Security Access

WPS

- Wi-Fi Protected Setup, Wi-Fi protection setting