J22389

TUF GAMING

USER MANUAL

TUF Gaming AX4200 Wireless Router

ASUS

J22389
初版 V1
2023年10月

もくじ

1　製品の概要

1.1　はじめに

この度はASUS製品をお買い上げいただき、誠にありがとうございます。

本マニュアルでは、本製品の設置方法、接続方法、各種機能の設定方法について説明をしています。お客様に本製品を末永くご愛用いただくためにも、ご使用前このユーザーマニュアルを必ずお読みください。

1.2　パッケージ内容

☑ TUF Gaming Wireless Router 本体

☑ 電源アダプター

☑ LANケーブル

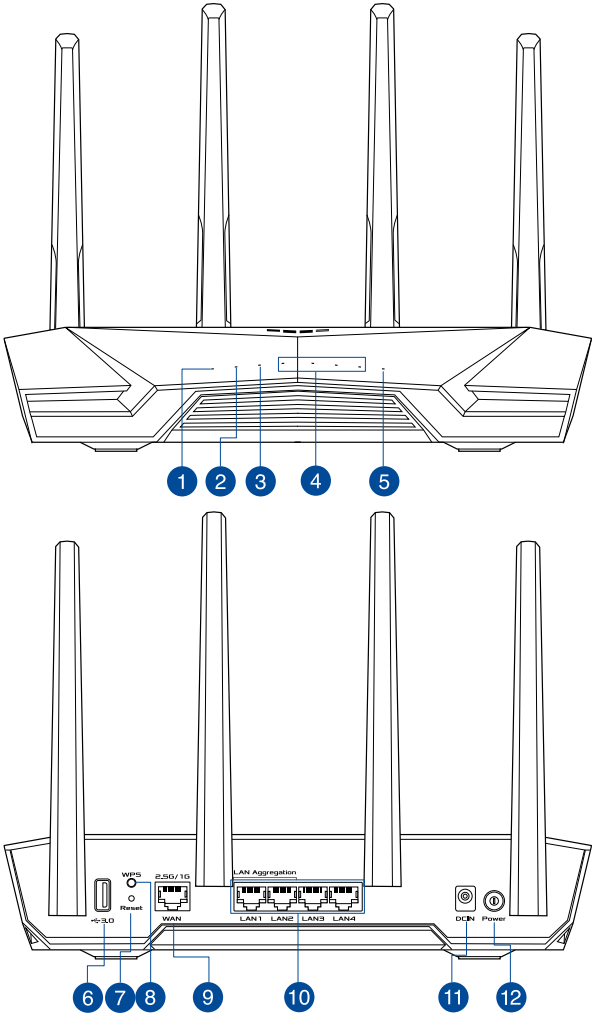
☑ かんたんセットアップガイド

ご注意:

- 万一、付属品が足りない場合や破損していた場合は、すぐにご購入元にお申し出ください 。
- 販売店舗独自の保証サービスや販売代理店の保証をお受けいただく場合、お買い上げ時の梱包箱、暖衝材、マニュアル、付属品がすべて揃っているなど、条件が設けられていることがあります。ご購入時の領収書やレシートと一緒に大切に保管してください。

ご注意: 本書で使用されているイラストや画面は実際とは異なる場合があります。各項目の名称、設定値、利用可能な機能は、ご利用のモデルやファームウェアのバージョンにより異なる場合があります。予めご了承ください。

1.3 各部の名称



1 **電源LED**
消灯: 電源が入っていません。
点灯: デバイスが利用可能な状態です。
低速点滅: レスキューモードで起動しています。

2 **2.4GHz LED**
消灯: 無線LANを使用していません。
点灯: 2.4GHzで通信可能な状態です。
点滅: 2.4GHzでデータ送受信をしています。

3	**5GHz LED** **消灯:** 無線LANを使用していません。 **点灯:** 5GHzで通信可能な状態です。 **点滅:** 5GHzでデータ送受信をしています。
4	**LAN 1~4 LED** **消灯:** ケーブルが接続されていない、または電源が入っていません。 **点灯:** LANのリンクが確立しています。
5	**2.5G/1G WAN (インターネット) LED** **消灯:** ケーブルが接続されていない、またはIPアドレスが取得できていません。 **点灯:** WANのリンクが確立しています。
6	**USB 3.2 Gen 1 ポート** 外付けHDDやUSBメモリー等のUSB 3.2 Gen 1デバイスを接続します。
7	**リセットボタン** システムを工場出荷時の状態に戻す際に使用します。
8	**WPSボタン** WPS機能をオンにします。
9	**2.5G/1G WAN (インターネット) ポート** ネットワークケーブルをこのポートに接続して、2.5G / 1G WAN 接続を確立します。
10	**LAN 1~4 ポート** コンピューターやゲーム機などと接続します。
11	**電源ポート (DCIN)** 付属の電源アダプターを接続します。
12	**電源ボタン** 本製品の電源のON/OFFの切り替えができます。

ご注意:

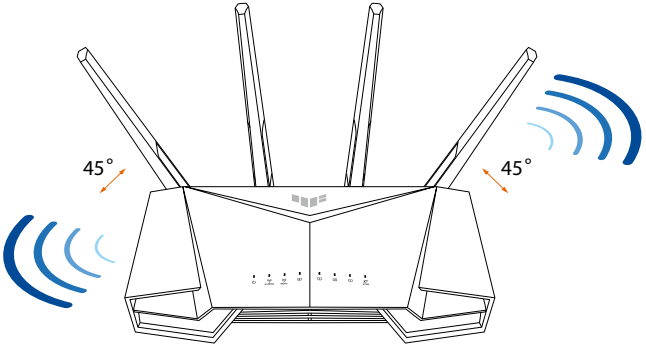
- 電源アダプターは、必ず本製品に付属のものをお使いください。また、本製品に付属の電源アダプターは他の製品に使用しないでください。火災、感電、故障の原因となります。
- **仕様:**

DC電源アダプター	DC出力 +12V、2.5A		
動作温度	0~40℃	保管時	0~70℃
動作湿度	50~90%	保管時	20~90%

1.4 無線LANルーターの設置

本製品を利用する際は、次のことに注意して設置してください。

- 複数のワイヤレスデバイスを接続する場合は、最適な通信環境のためにすべてのデバイスの中心位置に無線LANルーターを設置します。
- 無線LANルーターの周囲にパソコンや金属物などのものがない場所に設置します。
- 直射日光のあたる場所やストーブ、ヒーターなどの発熱機のそばなど、温度の高い所には設置しないでください。
- 同じ2.4GHz帯を使用する電子レンジ、コードレス電話機、医療機器、Bluetooth機器、レーザー式無線マウスなどの電波を放射する装置から離れた場所に設置します。設置距離が近すぎると、電波が干渉し通信速度が低下したりデータ通信が途切れる場合があります。
- パフォーマンスとセキュリティ向上のため、本機のファームウェアは常に最新のものをご使用ください。
- 無線LANルーター（親機）と無線LAN端末（子機）の距離が近すぎるとデータ通信でエラーが発生する場合があります。お互いを1m以上離してお使いください。
- 最適なパフォーマンスを得るために、次のイラストを参考にアンテナを調整して下さい。



1.5　ご使用になる前に

本製品をご使用になる前に、次のことをご確認ください。

回線契約とインターネットサービスプロバイダー (ISP) の加入

- 本製品をお使いの前に、予め回線の契約とインターネットサービスプロバイダー (ISP) の契約を行ない、ブロードバンド回線が開通していることをご確認ください。
- 本製品の設定に必要な情報 (接続ユーザー名、接続パスワードなど) については、ご契約時の書類またはご契約のプロバイダーへお問い合わせください。

設定を行なうために必要なコンピューターの要件

- 1000BASE-T / 100BASE-TX / 10BASE-T 対応LANポートまたはIEEE 802.11a/b/g/n/ac/ax 無線LAN機能を搭載するコンピューター
- TCP/IPサービスがインストール済み
- Webブラウザー
  (Internet Explorer、Firefox、Google Chrome、Safari)

ご注意:

- 本製品はIEEE 802. 11　a/b/g/n/ac/ax の無線LAN規格に対応した無線LANルーターです。Wi-Fi 接続を使用するには、IEEE 802. 11 a/b/g/n/ac/ax の無線LAN規格に準拠する機器が必要です。
- 本製品はデュアルバンドに対応しており、2.4GHz帯と5GHz帯、2つの周波数帯域による同時通信をサポートしています。テレビなどで動画のストリーミングを楽しむために電波干渉が少なく高速で安定した5GHz帯を使用し、スマートフォンなどでネットサーフィンを楽しみたい場合は2.4GHz帯を使用するなど、帯域を使い分けて効率的にデータ通信をすることが可能です。
- IEEE 802. 11n 対応製品の中には、5GHz帯に対応していない製品も存在します。ご利用機器の5GHz帯の対応については、製造メーカーへお問い合わせください。
- イーサネット規格IEEE802.3 により、1000BASE-T / 100BASE-TX / 10BASE-Tの最大ケーブル長は100m と規定されています。

重要!

- 無線アダプターによっては、802.11ax Wi-Fi AP に接続する際に問題が発生することがあります。
- 問題が発生する場合は、ドライバーを最新バージョンに更新してください。ソフトウェアドライバー、更新、その他の関係情報を取得できる製造元の公式サポートサイトを確認してください。
  - Realtek: https://www.realtek.com/en/downloads
  - Mediatek: https://www.mediatek.com/products/connectivity-and-networking/broadband-Wi-Fi
  - Intel: https://downloadcenter.intel.com/

2 セットアップ

2.1 無線LANルーターのセットアップ

重要:

- セットアップ中の通信エラーなどによる問題を回避するために、有線接続でセットアップを行なうことをお勧めします。
- 無線LANルーターのセットアップを開始する前に、次の操作を行なってください。

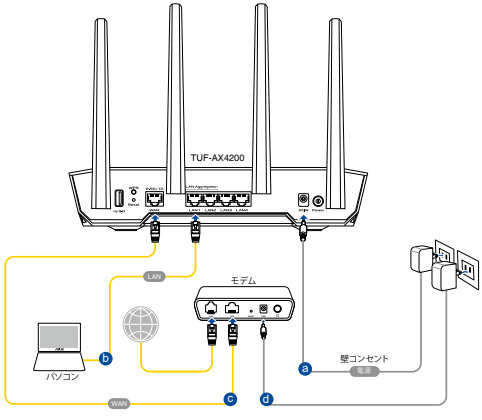
- 既存のルーターと交換を行なう場合は、現在実行されているすべての通信を停止します。
- モデム/回線終端装置とコンピューターに接続されたLANケーブルを取り外します。モデム/回線終端装置がバックアップ用バッテリーを搭載している場合は、バッテリーを一旦取り外します。
- モデム/回線終端装置とコンピューターを再起動します。(推奨)

A. 有線接続

ご注意: 本製品はオートネゴシエーション機能に対応しています。ネットワークケーブルがストレートケーブルかクロスケーブルかを自動的に判定し接続を行ないます。

接続方法

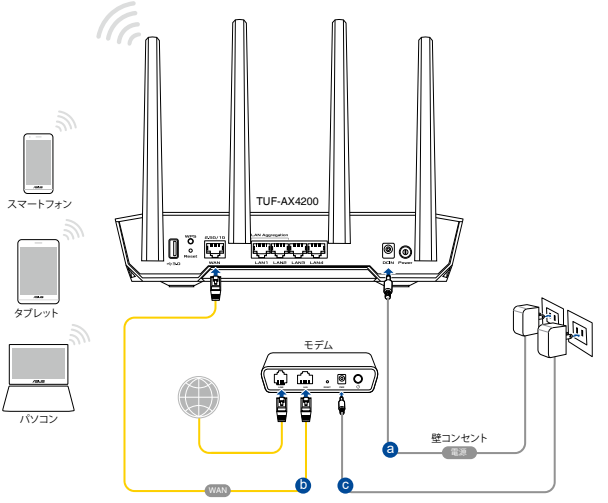
1. 無線LANルーターに電源ケーブルを接続し、電源を入れます。無線LANルーターのLANポートとコンピューターをLANケーブルで接続します。



B. 無線接続

接続方法

1. 無線LANルーターに電源ケーブルを接続し、電源を入れます。



2. 無線LANルーター背面の製品ラベルに記載されているネットワーク名（SSID）のネットワークに接続します。

Wi-Fi 名（SSID）：	ASUS_XX

* 「XX」は2.4GHz MACアドレスの最後の2桁になります。ルーター背面のラベルに記載があります。

* Wi-Fi接続にパスワードが必要になる場合がございます。パスワードは本体底面のラベルに記載があります。

* ルーターの背面にあるQRコードをスキャンすることで、簡単にWi-Fi接続することができます。

ご注意:

- ワイヤレスネットワークの接続方法については、ご利用のデバイスのユーザーマニュアルをご覧ください。
- ネットワークのセキュリティ設定については、本マニュアルに記載の「**セキュリティのセットアップ**」をご覧ください。

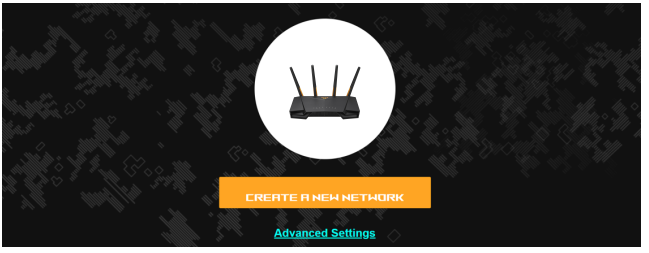
2.2 クイックインターネットセットアップ (QIS)

クイックインターネットセットアップ (QIS) では、簡単な操作でネットワーク環境を構築することができます。

注意: はじめから設定をやり直したい場合は、本体背面のリセットボタンを5秒以上押し、工場出荷時の状態にリセットしてください。

クイックインターネットセットアップを使用する

1. コンピューターと本製品をLANケーブルで接続し、コンピューターを起動します。ウェブブラウザーを起動して、アドレス欄に「**http://www.asusrouter.com**」または「**192.168.50.1**」を入力してWebのセットアップ画面にアクセスします。

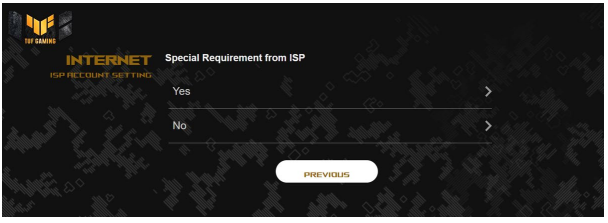


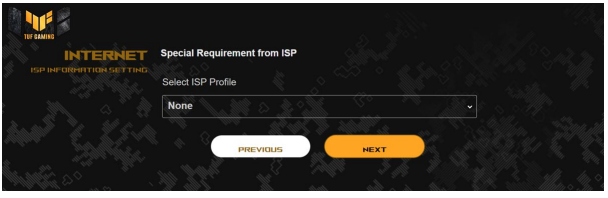
2. ISP (インターネットサービスプロバイダー) の接続に必要な情報を入力します。ISPの接続タイプが自動IP (動的IP) 、静的IP (スタティックIP) 、PPPoE、PPTP、L2TPである場合、無線LANルーターは自動的に接続タイプを検出します。

重要: インターネットの接続タイプや接続ユーザー名、接続パスワードなどについては、ご契約のプロバイダーへお問い合わせください。

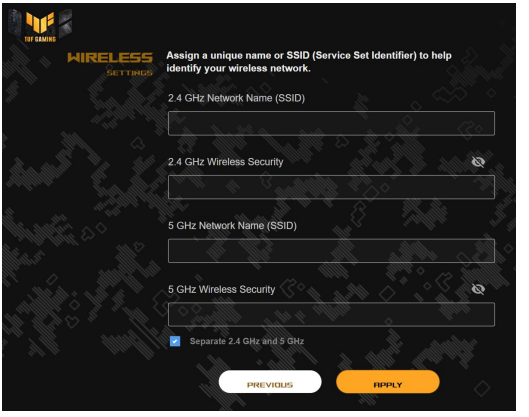
注記:

- 無線ルーターを初めて設定する場合、または、 無線ルーターが初期設定にリセットされた場合は、ISP 接続タイプの自動検出が行われます。
- クイックインターネットセットアップ（QIS）がインターネット接続タイプの検出に失敗した場合は、**詳細設定**をクリックして、手動で接続設定を行います。

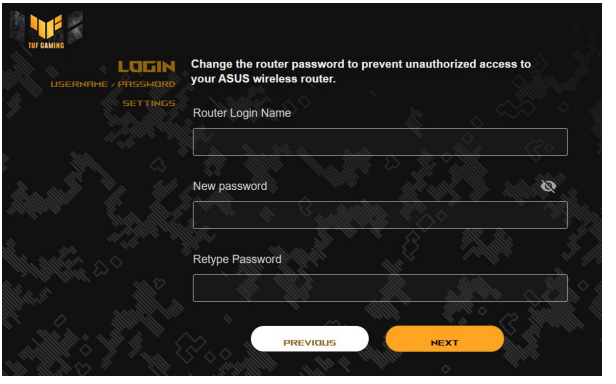




3. 2.4GHz帯と5GHz帯それぞれのワイヤレス接続用にネットワーク名(SSID)とセキュリティキーを設定し、「**適用**」をクリックして設定を保存します。



4. **ログイン情報設定**ページで、ルーターのログインパスワードを設定して、無線ルーターへの不正アクセスを防止します。



注記: 無線ルーターのログインユーザー名とパスワードは、2.4GHz/5GHz ネットワーク名 (SSID) とセキュリティキーとは異なります。 無線ルーターのログインユーザー名とパスワードで、無線ルーター管理画面 (Web GUI) にログインして、 無線ルーターの設定を行うことができます。 2.4GHz/5GHz ネットワーク名 (SSID) とセキュリティキーで、Wi-Fi デバイスがログインして、2.4GHz/5GHz ネットワークに接続できるようにします。

2.3 ワイヤレスネットワークに接続する

セットアップの完了後は、コンピューターやゲーム機、スマートフォンなどの無線LANデバイスをワイヤレスネットワークに接続することが可能になります。本製品では、次の方法で接続することができます。

コンピューターでワイヤレスネットワークに接続する

1. 通知領域（タスクトレイ）に表示されているワイヤレスネットワークアイコン をクリックします。
2. クイックインターネットセットアップで設定したネットワーク名(SSID) を選択し、「**接続**」をクリックします。
3. ネットワークキー (暗号化キー) を設定している場合は、キーを入力し「**OK**」をクリックします。
4. コンピューターがワイヤレスネットワークを構築するまでしばらく時間がかかります。コンピューターが正常にワイヤレスネットワークに接続されると、ワイヤレスネットワークアイコン が変わり通信可能な状態になります。

ご注意:

- ワイヤレスネットワークの詳細設定については、以降のページをご覧ください。
- ゲーム機やモバイル端末などのワイヤレスネットワークへの接続方法については、各デバイスの取扱説明書をご覧ください。
- お使いのOSのバージョンによって設定の方法が異なる場合がございます。予めご了承ください。

3 一般設定と詳細設定の構成

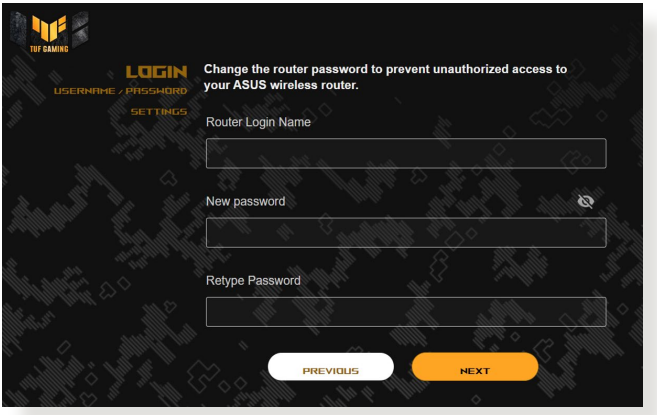
3.1 管理画面にログインする

本製品は誰にでも使いやすいインターフェースを採用しており、Webブラウザーでどなたでも簡単に設定をすることができます。

ご注意: ファームウェアのバージョンによって、利用できる機能や表示される画面、操作するボタンの名称が異なる場合があります。予めご了承ください。

管理画面にログインする:

1. Webブラウザーのアドレス欄に「**http://www.asusrouter.com**」と入力します。
2. ユーザー名とパスワードを入力し、管理画面にログインします。

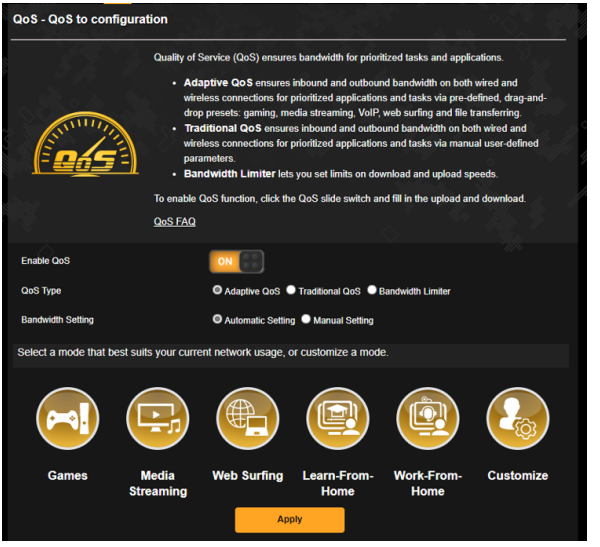


3. ログインに成功すると管理画面が表示されます。

ご注意: 本機をはじめて使用する場合、Webブラウザーを起動すると自動的にクイックインターネットセットアップが開始されます。

3.2 アダプティブ QoS

QoS (Quality of Service) とは、ネットワーク上でデータの種類に応じた優先順位に従ってデータを転送したり、ある特定の通信用にネットワーク帯域を予約し、一定の通信速度を保証する技術です。



QoS機能を有効にする

1. 「**アダプティブ QoS**」を選択し、画面上部の「QoS」をクリックします。
2. 「**QoS を有効にする**」のスイッチをクリックしONにします。
3. QoS タイプ (アダプティブ/ トラディショナル / 帯域リミッター) を選択します。

   注記: QoS タイプの定義については、QoS タブを参照してください。

4. **自動設定**をクリックして、自動的に最適な帯域幅にします。または、**手動設定**をクリックして、アップロード帯域幅とダウンロード帯域幅を手動で設定します。

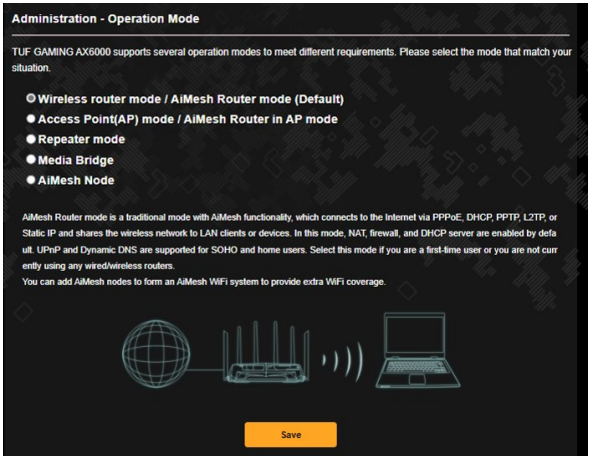
   ご注意: 帯域幅に関する情報はご契約のプロバイダーにご確認ください。次のWeb サイトで実測値を測定することができます。(http://speedtest.net)

5. 「**適用**」をクリックします。

3.3 管理

3.3.1 動作モード

動作モードでは、本製品の動作モードを簡単に切り替えることができます。



動作モードのセットアップ

1. 「**管理**」をクリックし、「**動作モード**」タブを選択します。
2. 動作モードを選択します。
   - **無線ルーターモード / AiMeshルーターモード (デフォルト):** 無線ルーターモードでは、無線ルーターを介してインターネットに接続し、ローカルネットワーク内のデバイスにインターネット接続を提供します。
   - **アクセスポイントモード / AiMesh アクセスポイントモード:** アクセスポイントモードでは、既存のネットワークに新たなワイヤレスネットワークを作成します。
   - **リピーターモード:** このモードでは、無線ルーターを中継器として設定し、無線信号の範囲を拡張します。
   - **メディアブリッジモード:** メディアブリッジモードを設定するには、2台の無線ルーターが必要です。2台目のルーターがメディアブリッジとして動作し、無線装置を持たないスマートTV、ゲーム機、BDレコーダー、メディアプレーヤーなどの各メディアデバイスのLANケーブルを介して無線接続を提供します。

- **AiMeshノード:** AiMeshを設定するには、2台以上のAiMesh対応ASUS無線ルーターが必要です。AiMeshノードを有効化し、親機のAiMeshルーターにログイン、管理画面からAiMeshノードを検索すれば近くの利用可能なAiMeshノードを自動的に発見し、AiMeshシステムに組み込みます。AiMeshは家全体にWi-Fiカバレッジとネットワークの中央管理を提供します。

3. **「保存」**をクリックし、設定を保存します。

ご注意: 動作モードを変更するには、無線LANルーターの再起動が必要です。

3.3.2 システム

システムでは、無線LANルーターのログイン名やパスワード、タイムゾーンなどのシステムに関連する設定を行うことができます。

手順

1. 「**管理**」をクリックし、「**システム**」タブを選択します。
2. ご利用の環境に応じて以下の設定を行います。
   - **ルーターのログイン名/ルーターログインパスワードの変更:** 本製品の管理画面にアクセスする際に使用する、管理者名 (ユーザー名) とパスワードを変更することができます。
   - **タイムゾーン:** 本製品内蔵時計のタイムゾーンを選択します。
   - **NTPサーバー:** 本製品の時間を同期するためのNTP (Network Time Protocol) サーバーを設定することができます。
   - **Telnet:** ネットワークに接続されたデバイスから遠隔操作をするためのTelnet通信の有効/無効を設定します。
   - **認証方式:** 本製品の管理画面へアクセスする際に使用する認証プロトコルを選択します。
   - **WANから接続を許可:** 外部ネットワーク上のクライアントによる管理画面アクセスの有効/無効を設定します。
   - **指定したIPアドレスからの接続を許可:** 外部ネットワーク上の特定のクライアントによる管理画面アクセスの有効/無効を設定します。アクセスを許可するクライアントはクライアントリストで指定することができます。
   - **指定したIPアドレス:** 管理画面アクセスを許可する外部ネットワーク上のクライアントIPアドレスで指定します。
3. 「**適用**」をクリックし、設定を保存します。

3.3.3 ファームウェア更新

ご注意: 最新のファームウェアはASUSのオフィシャルサイトからダウンロードいただけます。(https://www.asus.com/jp/)

ファイルからファームウェアを更新:

1. 「**管理**」をクリックし、「**ファームウェア更新**」タブを選択します。
2. 「**ファームウェア手動更新**」の「**アップロード**」ボタンをクリックし、コンピューターに保存したファームウェアファイルを指定します。
3. 「**アップロード**」をクリックし、ファームウェアの更新を開始します。ファームウェアの更新には約3分ほどかかります。

ご注意:

- ファームウェアの更新後は、無線LANルーターの再起動が必要です。
- ファームウェアの更新に失敗した場合、無線LANルーターは自動的にレスキューモードに移行し、電源LEDがゆっくりと点滅します。復旧方法ついては、「**4.2 Firmware Restoration (ファームウェアの復元)**」をご覧ください。

3.3.4 リセット/保存/復元設定

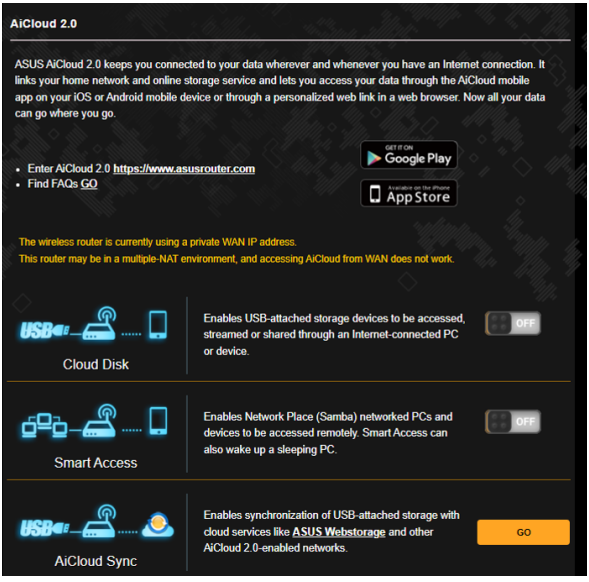
無線LANルーターの設定の保存とアップロード

1. 「**管理**」をクリックし、「**リセット/保存/復元設定**」タブを選択します。
2. 実行するタスクを選択します:
   - 工場出荷時の状態にリセット
     無線LANルーターのシステムを工場出荷時の状態に戻します。
   - 設定をファイルに保存
     現在の無線LANルーターの設定をファイルとして保存します。
   - 設定をファイルから復元
     「**設定をファイルに保存**」で作成したファイルから、システム設定を復元します。「**参照**」ボタンをクリックし、コンピューターに保存した設定ファイルを指定します。

設定の復元機能の使用によって問題が発生した場合は、お手数ですがファームウェアを最新バージョンに更新し再度手動にて設定を実施してください。

3.4 AiCloud 2.0

AiCloud 2.0 はホームネットワークとクラウドを結び、iOSやAndroidのアプリ、またはWeb ブラウザーで外出先から自宅のデータにアクセスすることができます。



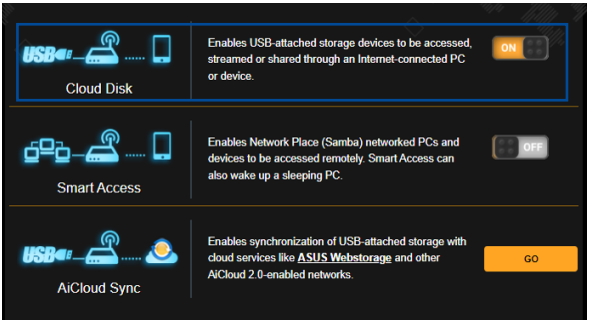
AiCloudを使用する

1. AndroidやiOSを搭載したスマートデバイスで、Google PlayまたはApp Storeから「**ASUS AiCloud**」アプリをダウンロードしてインストールします。
2. ASUS AiCloudアプリをインストールしたスマートデバイスを本機のワイヤレスネットワークに接続します。次にASUS AiCloudアプリを起動し、画面の指示に従ってセットアップを行います。

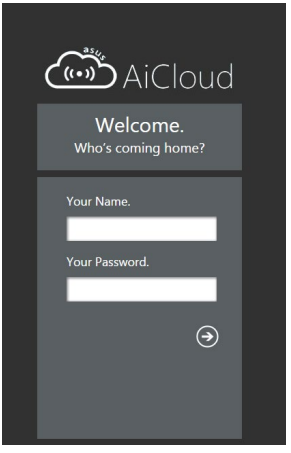
3.4.1 Cloud Disk

Cloud Diskを作成する

1. 本機のUSBポートにUSBストレージデバイスを接続します。
2. 「**AiCloud 2.0**」を選択し、「**Cloud Disk**」のスイッチをクリックしONにします。



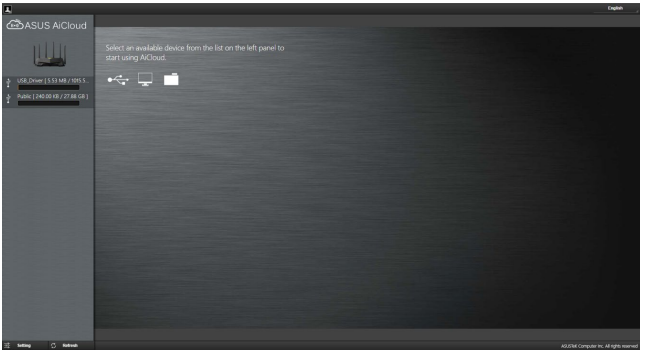
3. Webブラウザーのアドレス欄に「**http://www.asusrouter.com**」と入力してASUS AiCloudのログイン画面に移動し、ルーターのユーザー名とパスワードを入力してログインします。



快適にご利用いただくために、Google Chrome または Firefox ブラウザーをご使用頂くことをお勧めします。

4. 本機のUSBポートに接続したUSBストレージデバイスにアクセスすることができます。

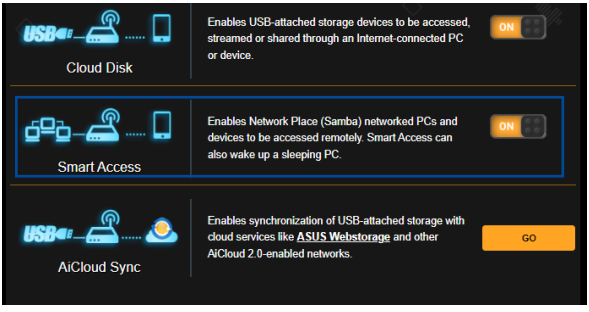
ご注意: セキュリティ対策上、AiCloudではログイン情報を保存することはできません。



ご注意: 本書で使用されているイラストや画面は実際とは異なる場合があります。

3.4.2 Smart Access

Smart Access は、利用環境に関わらずインターネット経由でLAN上のPCにアクセスすることができる機能です。WoL（Wake-on-LAN）に対応しているので、リモート操作でPCの電源を操作することが可能です。

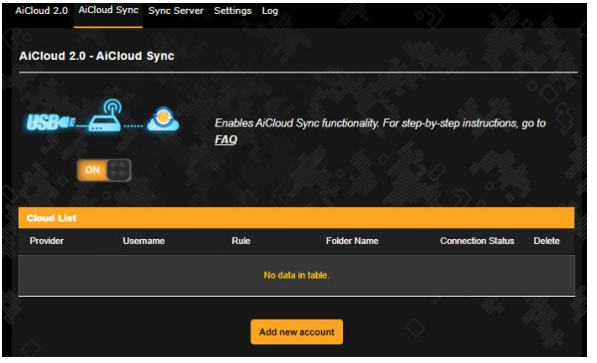


ご注意:

- 本製品は、ASUS DDNS Serviceを利用してドメイン名を作成することができます。詳しくは「**4.5.6 DDNS**」をご覧ください。
- AiCloudはセキュアな接続 (HTTPS) を利用することが可能です。次のURLでCloud DiskやSmart Accessを安全に使用することができます。

  https://<ドメイン名>.asuscomm.com

3.4.3 AiCloud Sync



AiCloud Syncを使用する

1. 「**AiCloud 2.0**」を選択し、「**AiCloud Sync**」の設定ボタンをクリックします。
2. スイッチをクリックしONにします。
3. 「**新しいアカウントの追加**」をクリックします。
4. ASUS WebStorageのアカウントとパスワードを入力し、同期を行うディレクトリを設定します。
5. ドロップダウンリストから同期ルールを選択します。
6. 「**適用**」をクリックし、設定を保存します。

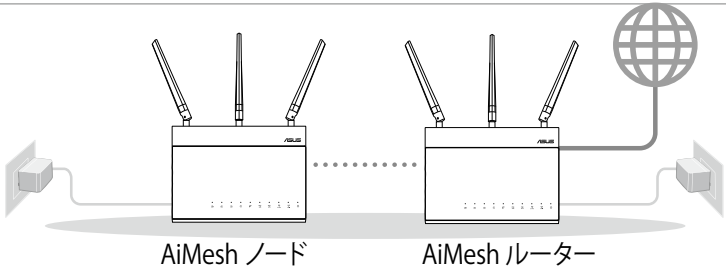
3.5 AiMesh

3.5.1 設定する前に

AiMesh Wi-Fi システムをセットアップする準備

1. 2 台の ASUS ルーター（AiMesh に対応するモデル: https://www.asus.com/AiMesh/）。
2. 1 台を AiMesh ルーターとして、もう 1 台を AiMesh ノードとして割り当てます。

注記: 複数の AiMesh ルーターがある場合は、最も高い仕様のルーターを AiMesh ルーターとして使用して、その他のルーターを AiMesh ノードとして使用することを推奨します。



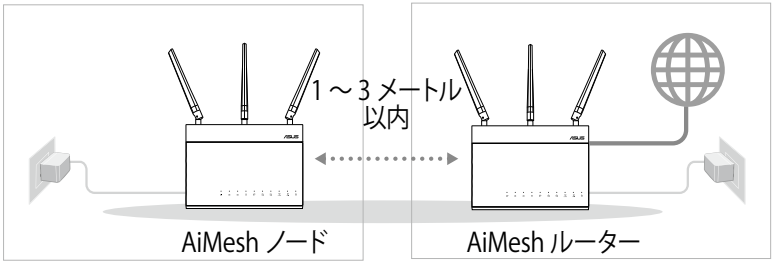
3.5.2 AiMesh セットアップ手順

準備

セットアップ中は、AiMesh ルーターとノードを 1 ～ 3 メートル以内の距離に設置します。

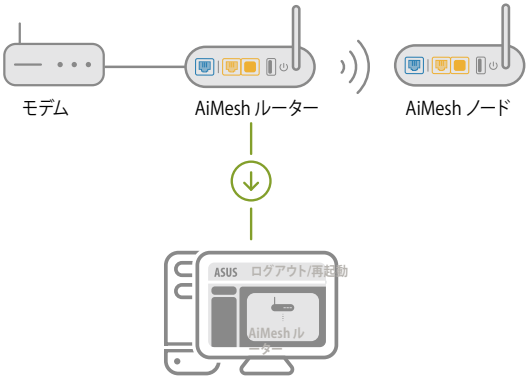
AiMesh ノード

工場出荷時の初期状態。 AiMesh システム設定のために、電源を入れてスタンバイ状態のままにします。



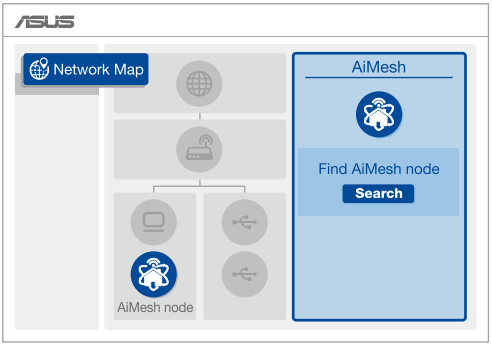
AiMesh ルーター

1) AiMesh ルーターを PC とモデムに接続し、次に、管理画面（Web GUI）にログインします。



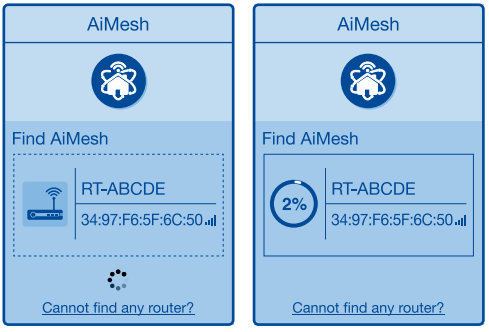
2) ネットワークマップページに進み、AiMeshアイコンをクリックし、次に、拡張 AiMesh ノードを検索します。

注記: ここで AiMesh アイコンが見つからない場合は、ファームウェアバージョンをクリックして、ファームウェアを更新します。

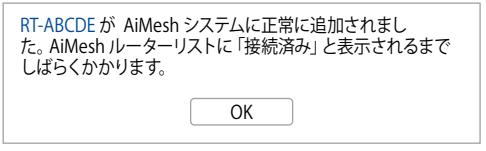


3) **検索**をクリックすると、AiMesh ノードを自動的に検索します。 このページに AiMesh ノードが表示される場合は、それをクリックして AiMesh システムに追加します。

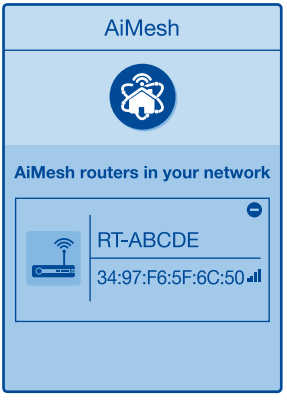
注記: AiMesh ノードが見つからない場合は、**トラブルシューティング**をご覧ください。



4) 同期化が完了すると、メッセージが表示されます。



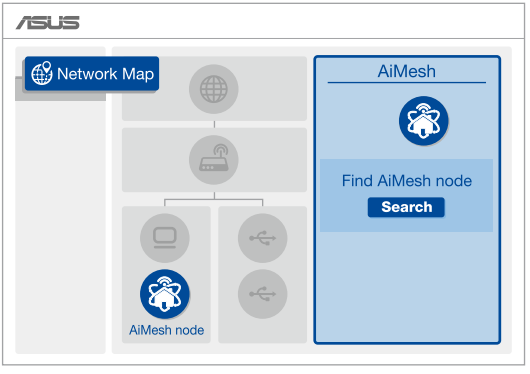
5) おめでとうございます! AiMesh ノードが AiMesh ネットワークに正常に追加されると、下のページが表示されます。



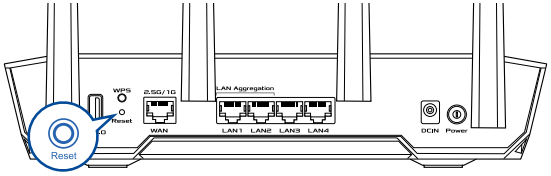
3.5.3 トラブルシューティング

AiMesh ルーターが近くにある AiMesh ノードを見つけることができない場合、または、同期化に失敗する場合は、次のことを確認して、もう一度お試しください。

1) AiMesh ノードを AiMesh ルーター に近づけて、最適な位置にします。1 ～ 3 メートル以内であることを確認します。
2) AiMesh ノードの電源がオンになっていることを確認します。
3) AiMesh ノードが AiMesh 対応ファームウェアにアップグレードされていることを確認します。
   i. 次から AiMesh 対応ファームウェアをダウンロードします: https://www.asus.com/AiMesh/
   ii. AiMesh ノードの電源をオンにして、ネットワークケーブル経由で PC に接続します。
   iii. 管理画面 (Web GUI) を起動します。 ASUS セットアップウィザードにリダイレクトされます。 リダイレクトされない場合は、http://www.asusrouter.com
   iv. **管理 >ファームウェア更新**の順に進みます。**アップロード**をクリックして、AiMesh 対応ファームウェアをアップロードします。
   v. ファームウェアがアップロードされた後で、Network Map (ネットワークマップ) ページに進み、AiMesh アイコンが表示されるかどうかを確認します。



   vi. AiMesh ノードの上のリセットボタンを少なくとも 5 秒間押します。 電源 LED がゆっくりと点滅したら、リセットボタンを放します。



3.5.4 再配置

最適なパフォーマンス:

AiMesh ノードとルーターを最適な場所に設置します。

注記:

- 干渉を最小限に抑えるために、コードレス電話、Bluetooth デバイス、電子レンジなどから離れた場所にルーターを設置してください。
- 障害物のない場所、または、広々とした場所にルーターを設置することを推奨します。

3.5.5 FAQ（よくあるご質問）

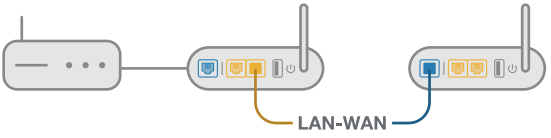
ご質問 1: AiMesh ルーターはアクセスポイントモードに対応しますか?

回答: はい。 AiMesh ルーターをルーターモードまたはアクセスポイントモードとして設定することを選択できます。 管理画面（Web GUI）（http://www.asusrouter.com）で、**管理 > 動作モード**のページを開きます。

ご質問 2: AiMesh ルーター間の有線接続（イーサネットバックホール）をセットアップできますか?

回答: はい。 AiMesh システムは、AiMesh ルーターとノードの無線接続および有線接続の両方に対応して、スループットと安定性を最大化します。 AiMesh は、使用できるそれぞれの周波数帯域の無線信号強度を分析し、無線接続または有線接続のどちらがルーター間接続バックボーンとして最も適しているかを自動的に決定します。

1) セットアップ手順に従って、まず、Wi-Fi 経由で AiMesh ルーターとノードの接続を確立します。
2) ノードを最適な場所に設置して、最良のカバレッジにします。 イーサネットケーブルを AiMesh ルーター の LAN ポートから AiMesh ノードの WAN ノードに配線します。



3) AiMesh システムは、有線でも無線でも、データ転送向けの最良の径路を自動選択します。

3.6 AiProtection

AiProtection では、マルウェア、不正アクセス、ランサムウェアをブロックし、ネットワークを強固に守ります。また、ペアレンタルコントロール機能では、1日あたりの利用時間を制限や有害なウェブサイトへのアクセスをブロックすることができます。

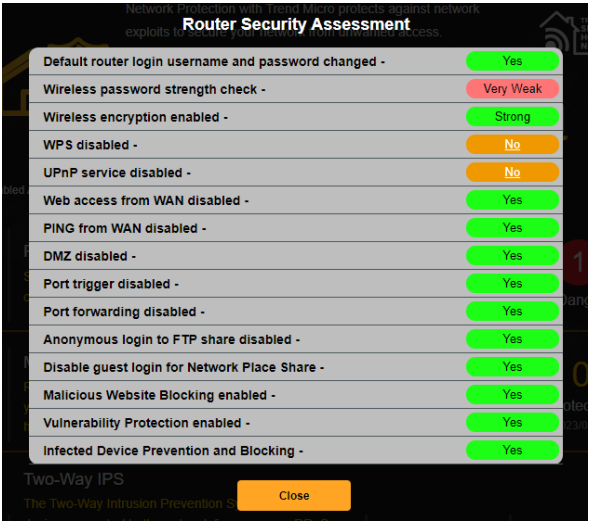
3.6.1 AiProtectionの設定

AiProtectionでは、悪質なWebサイトへのアクセスや不正な通信を防ぎ、ネットワークを保護します。

AiProtectionを設定する

1. Web GUIナビゲーションパネル全般の「**AiProtection**」を開きます。
2. AiProtectionのメイン画面で、「**有効 AiProtection**」のスイッチをクリックし、ONにします。
3. Network Protectionタブで、「**スキャン**」をクリックします。スキャンが完了すると、「**セキュリティ評価**」が表示されます。

検索結果は、**セキュリティ評価**ページに表示されます。



重要：「**セキュリティ評価**」画面で「**はい**」でマークされている項目は、 安全な状態です。（新規）

4. 必要に応じ、「**セキュリティ評価**」画面で「**脆弱**」、「**良好**」、「**強力**」の項目に対し手動設定を行います。

   手順

   a. 項目をクリックすると、その項目の設定画面に移動します。

   b. 項目のセキュリティ設定画面から、設定して、必要な変更を行い、完了したら「**適用**」をクリックします。

   c. 「**セキュリティ評価**」画面に戻り、「**閉じる**」をクリックして画面を閉じます。

5. 確認メッセージで「**OK**」をクリックします。

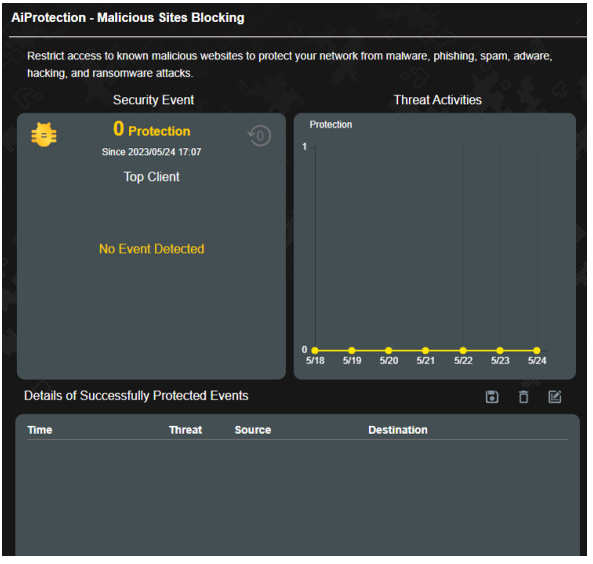
3.6.2 悪質サイトブロック

トレンドマイクロが提供するデータベースを参照し、悪質サイトへのアクセスを制限します。

注意: 「**有効 AiProtection**」を実行すると、この機能は自動的に有効になります。

悪質サイトブロックを有効にする

1. Web GUIナビゲーションパネル全般の「**AiProtection**」を開きます。
2. AiProtectionのメイン画面で、「**悪質サイトブロック**」をクリックします。



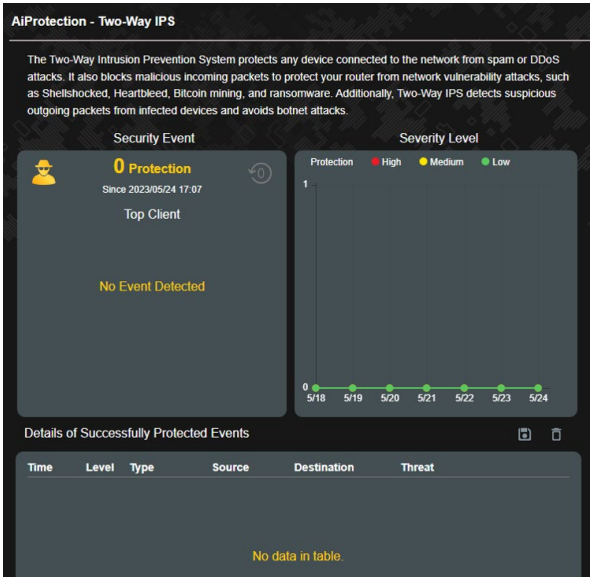
3.6.3 脆弱性保護

疑わしい通信や脆弱性を悪用する攻撃があった場合は即座に通信を遮断し、自宅のネットワーク内の機器やデータを守ります。

注意:「**有効 AiProtection**」を実行すると、この機能は自動的に有効になります。

脆弱性保護を有効にする

1. Web GUIナビゲーションパネル全般の「**AiProtection**」を開きます。
2. AiProtectionのメイン画面で、「**脆弱性保護**」をクリックします。



3.6.4 感染デバイス検出/ブロック

ウイルスやマルウェアに感染したデバイスが不正サーバーへの接続を試みる際にトレンドマイクロが提供するデータベースを参照させることで、不正サーバーへの接続をブロックします。

ご注意: **「有効 AiProtection」**を実行した場合、**「感染デバイス検出/ブロック」**は自動的にONになります。

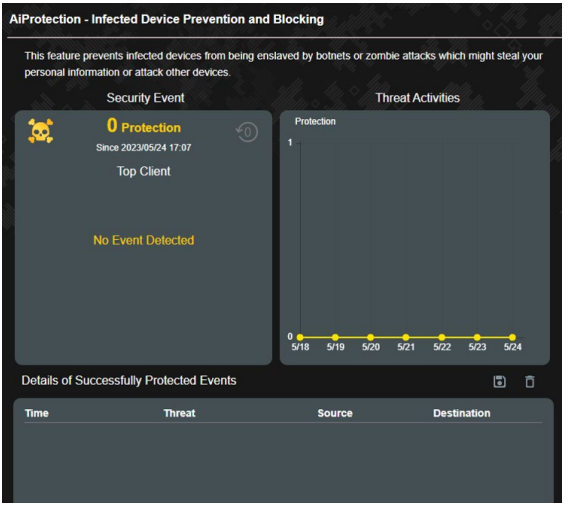
感染デバイス検出/ブロックを有効にする

1. Web GUIナビゲーションパネル全般の「**AiProtection**」を開きます。
2. AiProtectionのメイン画面で、「**感染デバイス検出/ブロック**」をクリックします。

アラートを設定する

不正な通信が検出され通信の遮断が発生した場合に登録したメールアドレスに通知メールを送信することができます。

1. 「**感染デバイス検出/ブロック**」の「**アラート設定**」をクリックします。
2. メールサービス、メールアドレス、パスワードを入力し「**適用**」をクリックします。



3.7 ファイアウォール

本製品はハードウェアファイアウォールをサポートし、より安全な接続を提供します。

ご注意: ファイアウォール機能はデフォルト設定で有効に設定されています。

3.7.1 全般設定

基本的なファイアウォールのセットアップ

1. 「**ファイアウォール**」をクリックし、「**全般**」タブを選択します。
2. 「**ファイアウォールを有効にする**」の「**はい**」をチェックします。
3. 「**DoS保護を有効にする**」でDoS (Denial of Service) 攻撃からネットワークを保護する機能の有効/無効を設定します。通常使用される場合は、この項目を「**はい**」にチェックすることをお勧めします。
4. LAN接続とWAN接続間のパケットを監視してログを取得する場合は、パケットタイプを選択します。
5. 「**適用**」をクリックし、設定を保存します。

3.7.2 URLフィルター

URLフィルターでは、任意のURLを設定し、一致したWebサイトへのアクセスを制限することができます。

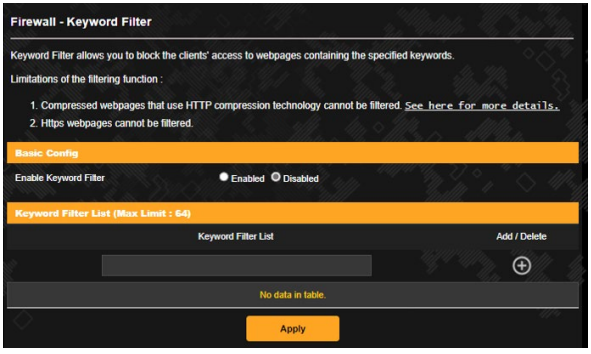
ご注意: URLフィルター機能はDNSクエリに基づいて行われます。システムストアの閲覧履歴はDNSキャッシュに格納されており、ネットワーククライアントが閲覧した履歴のあるWeb サイトはブロックすることができません。この問題を解決するには、URLフィルター機能を設定する前にDNSキャッシュをクリアする必要があります。

URLフィルターのセットアップ

1. 「**ファイアウォール**」をクリックし、「**URLフィルター**」タブを選択します。
2. 「**URL フィルターを有効にする**」の「**有効**」をチェックします。
3. アクセス制限を行いたいWebサイトのURLを入力し、 ボタンをクリックします。
4. 「**適用**」をクリックし、設定を保存します。

3.7.3 キーワードフィルター

キーワードフィルターでは、任意のキーワードを設定し、一致した文字列を含むWebサイトへのアクセスを制限することができます。



キーワードフィルターのセットアップ

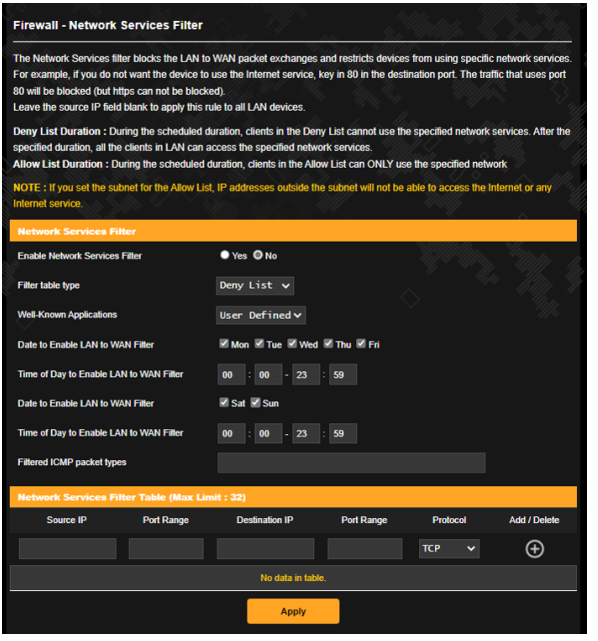
1. 「**ファイアウォール**」をクリックし、「**キーワードフィルター**」タブを選択します。
2. 「**キーワードフィルターを有効にする**」の「**有効**」をチェックします。
3. 単語またはフレーズを入力し、⊕ ボタンをクリックします。
4. 「**適用**」をクリックし、設定を保存します。

ご注意:

- キーワードフィルター機能はDNSクエリに基づいておこなわれます。システムストアの閲覧履歴はDNSキャッシュに格納されており、ネットワーククライアントが閲覧した履歴のあるWeb サイトはブロックすることができません。この問題を解決するには、キーワードフィルター機能を設定する前にDNSキャッシュをクリアする必要があります。
- HTTP圧縮を使用しているWebページをフィルタリングすることはできません。また、HTTPSセキュア接続のWebページはキーワードフィルター機能でフィルタリングすることができません。

3.7.4 パケットフィルター

パケットフィルターでは、LAN側からWAN側へのパケット交換、およびTelnetやFTPといった特定のWebサービスに対してのアクセスを制限することができます。

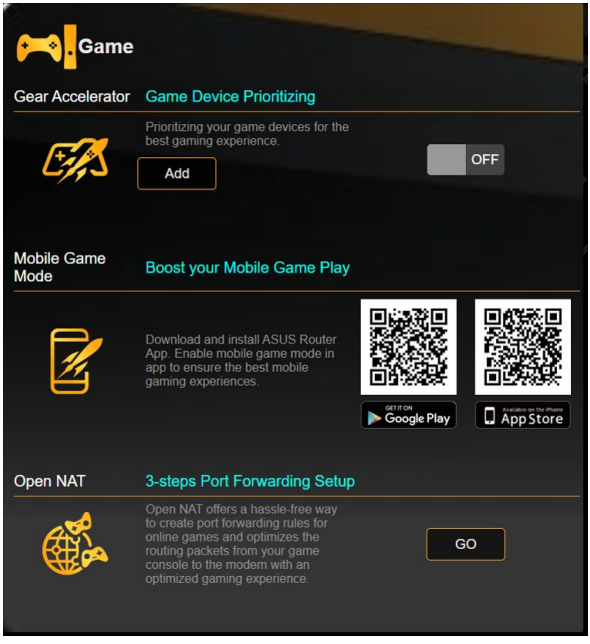


ネットワークサービスフィルターのセットアップ

1. 「**ファイアウォール**」をクリックし、「**パケットフィルター**」タブを選択します。
2. 「**パケットフィルターを有効にする**」の「**はい**」をチェックします。
3. フィルターリストのタイプを選択します。「**ブラックリスト**」は特定のネットワークサービスをブロックします。「**ホワイトリスト**」は指定したネットワークサービスのみアクセスを許可します。
4. ネットワークサービスフィルターを実施する日時を指定します。
5. フィルタリングを行うネットワークサービスを指定するには、ソースIP、宛先IP、ポートレンジ、プロトコルを入力し、⊕ボタンをクリックしリストに追加します。
6. 「**適用**」をクリックし、設定を保存します。

3.8 ゲームブースト

この機能では、ワンクリックでゲームブーストを有効にすることができます。ゲームブーストを有効にすることでゲームパケットが優先して転送されるため、より快適な環境でゲームをお楽しみ頂けます。

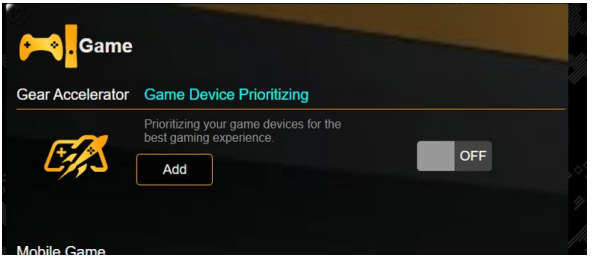


ゲームブーストを設定する:

1. Web GUIナビゲーションパネル全般の「**ゲームブースト**」を開きます。

3.8.1 ゲームブースト

ゲームブーストを使用して、オンラインコントロール パネル経由でゲームデバイスを優先化し、最高のゲーミング体験を実現します。



ゲームブーストを設定する:

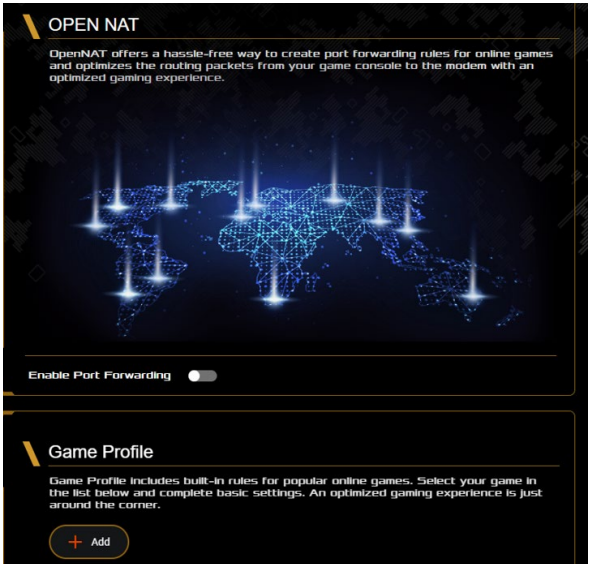
1. ナビゲーションパネルで、**全般 > ゲームブースト**の順に進みます。
2. ゲームブーストタブで、**ON (オン)** をクリックします。
3. 設定を適用した後で、追加をクリックしてクライアント名を選択します。
4. をクリックして、クライアントのプロファイルを追加します。
5. 適用をクリックして設定を保存します。

注記: クライアントプロファイルを削除したい場合は、 をクリックします。

3.8.2 Open NAT

Open NAT（オープン NAT）を使用すれば、オンラインゲームのポートフォファーディングルールを容易に作成し、ゲームコンソールからモデムへのルーティングパケットを最適化して、理想的なゲーミング体験を実現します。

PC ゲームまたはコンソールゲームをプレイする場合は、NAT ブロックやポートブロックなど、ISP 設定またはルーター設定のために接続の問題が発生することがあります。 Game Profile（ゲームプロファイル）は、ルーターがゲーム接続をブロックしないことを確かにする際に役立ちます。



Open NAT（オープン NAT）を設定する:

1. ナビゲーションパネルで、**全般→OpenNAT**の順に進みます。
2. **ポートフォワーディングを有効にする**をオンにします。
3. **ゲームタイトル**で、ゲームを選択して、基本設定を完了します。
4. **OK** をクリックします。

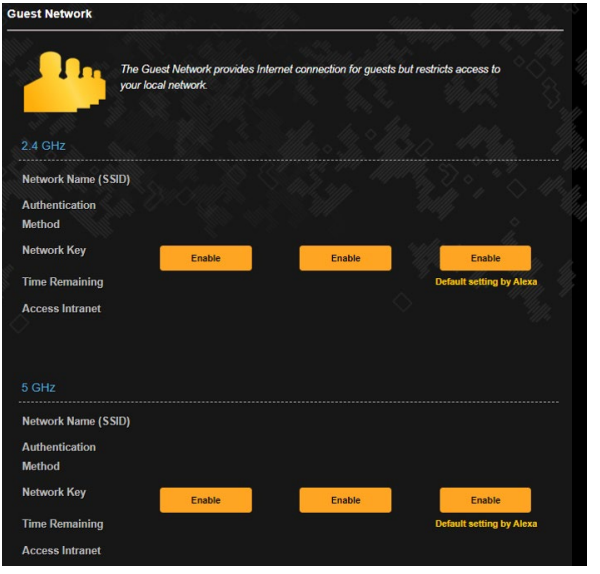
3.9　ゲストネットワークを構築する

ゲストネットワークは、普段利用しているネットワークとは別の隔離されたネットワークをゲスト用に設定することで、安全にインターネットを共有することができます。

ご注意: 本製品では、各周波数帯で3つずつ、合計6つのゲストネットワーク設定を行なうことができます。

手順

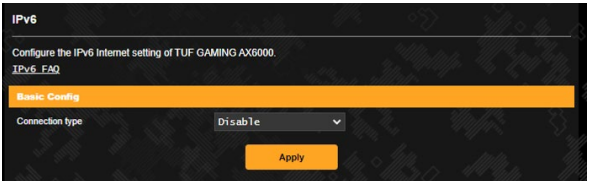
1. 「**ゲストネットワーク**」をクリックします。
2. 新たにゲストネットワークを作成する周波数帯を選択し、「**有効**」をクリックします。
3. ゲストの設定を変更するには、変更したいゲストの設定をクリックします。ゲストの設定を削除するには、「**削除**」をクリックします。



4. 「**ネットワーク名 (SSID)**」の欄にゲストネットワーク用のネットワーク名を入力します。
5. 「**認証方式**」ドロップダウンリストから利用する認証方式を選択します。
6. WPA認証方法を選択した場合は、WPA暗号化を選択してください。
7. 「**アクセス時間**」にゲストがネットワークに接続可能な合計時間を入力します。制限を設けない場合は、「**無制限**」をチェックします。
8. イントラネットのアクセスの項目で「**無効**」または「**有効**」を選択します。
9. すべての設定が完了したら「**適用**」をクリックしゲストネットワークの設定を適用します。

3.10 IPv6

本製品はIPv6をサポートしています。IPv6とは、従来のIPv4をベースに開発されたインターネットの新しい通信プロトコルです。



IPv6のセットアップ

1. 「**IPv6**」をクリックします。
2. 「**接続タイプ**」のドロップダウンリストから、ご契約のプロバイダーが提供するサービスに合わせて接続タイプを選択し、基本設定を行います。
3. 必要に応じて、LAN設定とDNS設定を入力します。
4. 「**適用**」をクリックし、設定を保存します。

ご注意: IPv6サービスの対応と詳しい設定方法については、ご契約のプロバイダーへお問い合わせください。

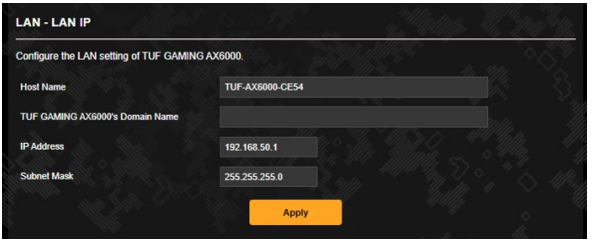
3.11 LAN

3.11.1 LAN IP

LAN IP では、本機に割り当てられているのIPアドレス設定を変更することができます。

ご注意:

- LAN IP の変更に伴い、DHCPサーバーの設定が変更されます。
- LAN IP を変更した場合、管理画面にログインするには、変更後のIPアドレスを使用する必要があります。

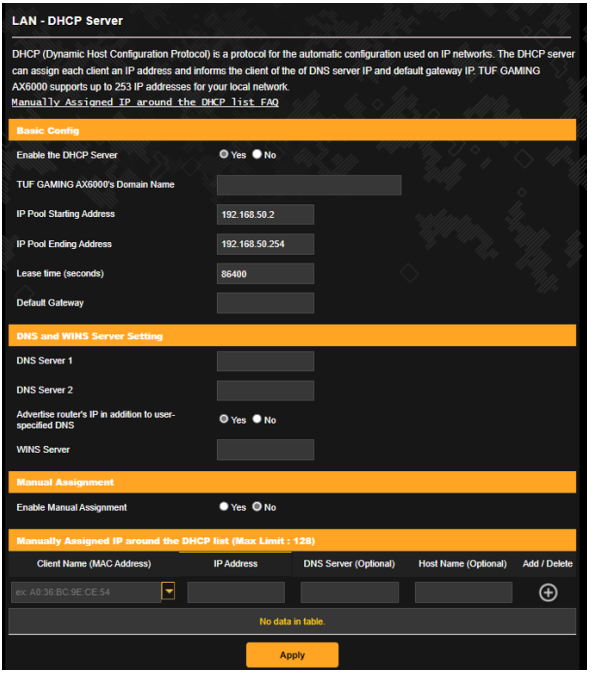


LAN IP設定を変更する

1. 「**LAN**」をクリックし、「**LAN IP**」タブを選択します。
2. 「**IPアドレス**」と「**サブネットマスク**」に新たなアドレスを入力します。
3. 「**適用**」をクリックし、設定を保存します。

3.11.2 DHCPサーバー

本製品は、DHCPサーバー機能 (IPアドレス自動割り当て) をサポートしています。この設定では、DHCPサーバーが自動で割り当てるIPアドレスの範囲やリースタイムなどの詳細設定を行うことができます。



DHCPサーバー のセットアップ

1. 「**LAN**」をクリックし、「**DHCP サーバー**」タブを選択します。
2. 「**DHCP サーバーを有効にする**」の「**はい**」をチェックします。
3. 「**TUF GAMING AX4200 のドメイン名**」にDHCPサーバー機能で割り当てるドメイン名を入力します。プロバイダーからドメイン名が指定されている場合や、独自のドメイン名を使用する場合に入力してください。指定がない場合は、空欄のままで使用します。
4. 「**IP アドレスプール開始IPアドレス**」に起点となるIPアドレスを入力します。

5. 「**IP アドレスプール終了IPアドレス**」に終点となるIPアドレスを入力します。
6. 「**リース時間**」のフィールドに、現在割り当てられているIP アドレスを破棄し、DHCPサーバーによるIPアドレスの再割り当てを要求する時間を入力します。

ご注意:

- IPプール起点アドレスとIPプール終点アドレスは、次の範囲内で設定されることをお勧めします。
  IPアドレス: **192.168.50.xxx**「xxx」は 2～254の任意の数)
- IPプール起点アドレスの値はIPプール終点アドレスより小さい数値である必要があります。

---

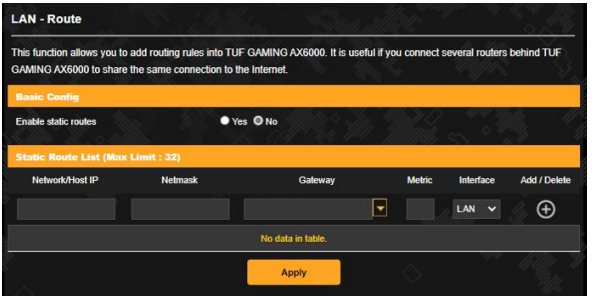
7. 設定が必要な場合は、「**DNS と WINS サーバーの設定**」で各サーバーのIPアドレスを入力します。
8. 本製品では、DHCPサーバー機能を使用しながら特定のMACアドレスに対してIPアドレスを手動で割り当てることもできます。

「固定割り当てを有効にする」の「はい」をチェックし、下のリストでMACアドレスと割り当てるIPアドレスを入力し追加します。手動割り当ては最大128個まで登録することができます。

3.11.3 ルーティングテーブル

ネットワーク上に複数の無線LANルーターが存在する場合など、すべての経路で同じインターネットサービスを使用するためにルーティング (経路制御) を設定する必要があります。この項目では、ルーティングテーブルに関する詳細設定を行うことができます。

ご注意: ルーティングテーブル (経路表) の設定を間違った場合、ネットワークがループする、またはネットワークに繋がらなくなる等の問題が生じる可能性があります。これらの設定を適切に行うには、高度な専門知識が必要です。通常はデフォルト (初期値) のままでご使用になることを推奨いたします。

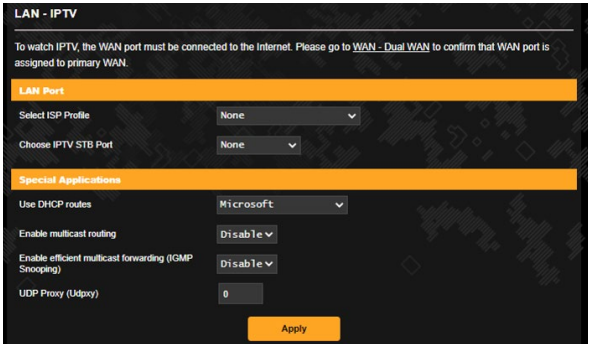


ルーティングテーブルのセットアップ

1. 「**LAN**」をクリックし、「**ルーティングテーブル**」タブを選択します。
2. 「**静的経路を有効にする**」の「**はい**」をチェックします。
3. 「**静的経路リスト**」にアクセスポイントまたは中継ノードの情報を入力し、リストに追加します。
4. 「**適用**」をクリックし、設定を保存します。

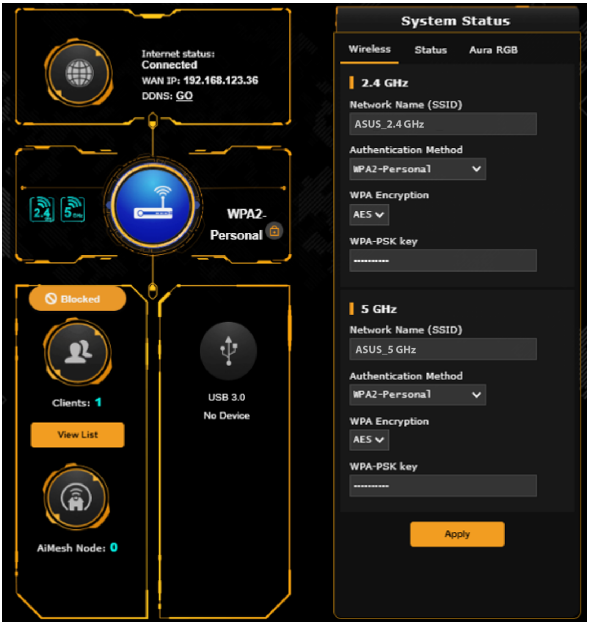
3.11.4 IPTV

本製品は、IPSまたはLANを介したIPTVサービスをサポートしています。この項目ではIPTV、VoIP、マルチキャスト、UDPに関する詳細設定を行うことができます。IPTVサービスに関する情報や適切な設定方法については、ご利用のサービスプロバイダーにお問い合わせください。

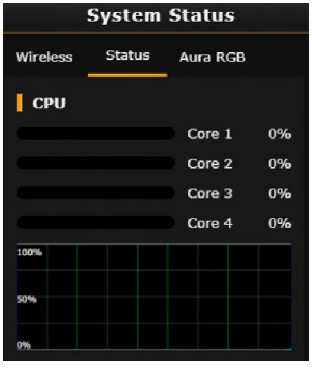


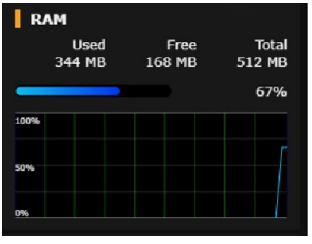
3.12 ネットワークマップを使用する

ネットワークマップでは、ネットワークのセキュリティ設定、ネットワーククライアントの確認、管理を行うことが出来ます。



各コアのCPUステータス、RAM使用状況ステータス、およびイーサネットポートステータスを監視できます。





3.12.1 セキュリティのセットアップ

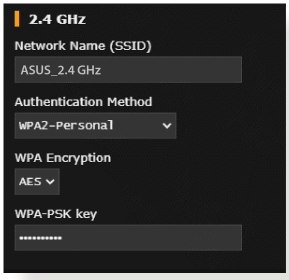
ワイヤレスネットワークを不正なアクセスから保護するには、セキュリティの設定を行なってください。

ワイヤレスネットワークのセキュリティを設定する

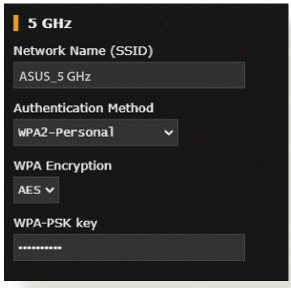
1. 「**ネットワークマップ**」をクリックします。
2. 「**セキュリティレベル**」(中央のルーターマークのアイコン)をクリックしてステータスパネルにシステムの状態を表示します。

ご注意: Smart Connect機能がOFFの場合、2.4GHz、5GHzの各周波数帯域で異なるセキュリティ設定を使用することができます。

2.4GHz セキュリティ設定



5GHz セキュリティ設定

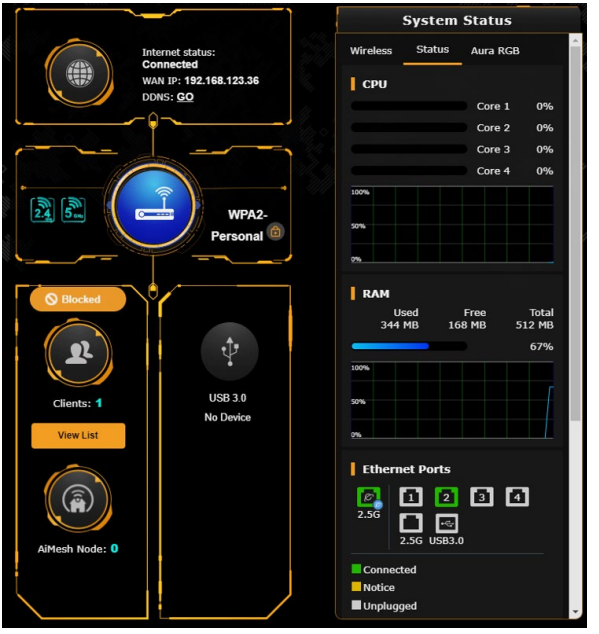


3. 「**ワイヤレス名 (SSID)**」に、他のワイヤレスネットワークと重複しないネットワーク名を入力します。
4. 「**認証方式**」ドロップダウンリストから利用する認証方式を選択します。

重要: IEEE 802.11n/ac 規格では、ユニキャスト暗号として WEPまたはTKIPで高スループットを使用することを禁じています。このような暗号化メソッド (WEP、WPA-TKIP) を使用している場合、データ転送レートは54Mbps 以下に低下します。

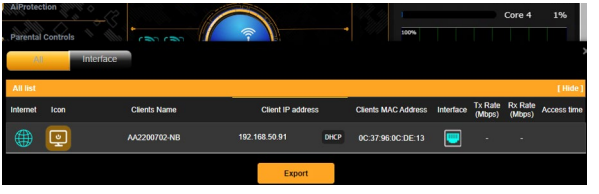
5. 認証方式にPersonalを設定した場合は、ネットワークキー (WPA-PSKキー) を設定します。
6. 「**適用**」をクリックし設定を完了します。

3.12.2 ネットワーククライアントの管理



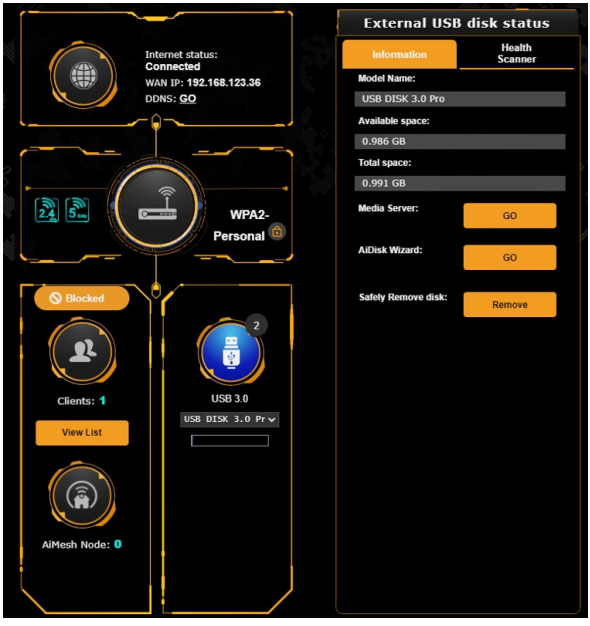
ネットワーククライアントの状態を確認する

1. 「**ネットワークマップ**」をクリックします。
2. 「**クライアント**」をクリックすることで現在無線LANルーターに接続されているクライアントの状態を確認することができます。
3. **クライアント**アイコンの下にある**リストを見る**をクリックして、すべてのクライアントを表示します。



3.12.3 USBデバイスの管理

本製品に搭載されているUSBポートでは、USB デバイスを接続することで本製品に接続した複数のコンピューターとファイルやプリンターを共有することができます。



ご注意:

- この機能を使用するには、外付けHDDやUSBメモリー等のUSBストレージデバイスを無線LANルーターのUSBポートに接続する必要があります。本製品がサポートするUSB ストレージデバイスのフォーマットタイプや容量については、次のWeb サイトでご確認ください。http://event.asus.com/networks/disksupport
- USBポートは同時にUSBドライブ2台、またはUSBプリンター1台とUSBドライブ1台を接続することが可能です。

重要: 本機能を使用するには、ネットワーククライアントがFTPサイト/サードパーティのFTPクライアントユーティリティ、Servers Center、Samba、AiCloud経由でUSBデバイスにアクセスできるよう、共有アカウントとアクセス権を作成する必要があります。詳しくは「**3.17 USBアプリケーションを使用する**」と「**3.4 AiCloud 2.0を使用する**」をご覧ください。

USBデバイスの状態を確認する

1. 「**ネットワークマップ**」をクリックします。
2. USBデバイスのアイコンをクリックすることで無線LANルーターに接続されたUSBデバイスの状態を確認することができます。
3. 「**USBアプリケーション**」の「**AiDisk**」から、USBストレージデバイス共有機能の設定を行なうことができます。

ご注意:

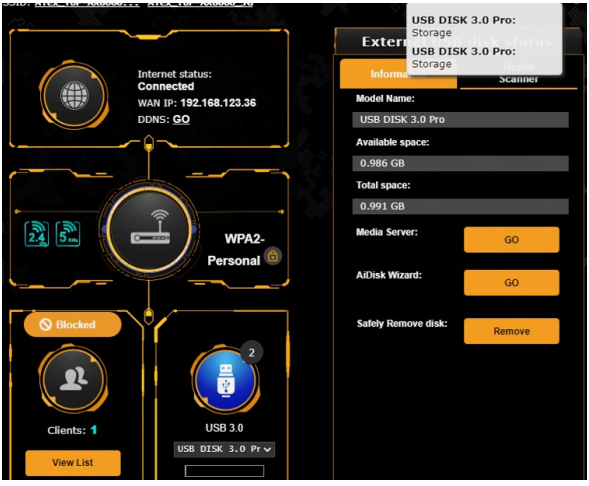
- 詳しくは「**3.17.2 サーバーセンターを使用する**」をご参考ください。
- 本製品は、最大4TBまでの容量のUSBストレージデバイスに対応しています。(対応フォーマット: FAT16、FAT32、NTFS、HFS+)
  本製品がサポートするUSB ストレージデバイスのフォーマットタイプや容量については、次のWeb サイトでご確認ください。
  http://event.asus.com/networks/disksupport

USBディスクを安全に取り外す

重要! USBストレージデバイスを取り外す際は、必ず安全な取り外しを行なってから取り外してください。適切な取り外し操作を行わずにデバイスを切断すると、デバイス上のデータが破損する可能性があります。

手順

1. 「**ネットワークマップ**」画面で取り外したいUSB デバイスをクリックします。
2. 次に「**ディスクを安全に取り外します**」の「**無効**」をクリックし、デバイスを停止させてからUSB ストレージを取り外します。または、情報バナーの  > をクリックし、対象のUSBデバイスを選択します。



3.13 ペアレンタルコントロール

ペアレンタルコントロール機能では、1日あたりの利用時間を制限したり、有害なウェブサイトの表示をブロックするなど、子供の成長に合わせて制限設定をすることができます。

ペアレンタルコントロールを設定する:

ナビゲーションパネルで、**全般 > ペアレンタルコントロール**の順に進みます。

Web&アプリケーションフィルター

有害なウェブサイトの表示をブロックしたり、不要なアプリケーションへのアクセスをクライアントごとに制限することができます。

Web&アプリケーションフィルターを設定する

1. 「**ペアレンタルコントロール**」画面右上の「**Web&アプリケーションフィルター**」をクリックします。
2. 「**Web&アプリケーションフィルター**」のスイッチをクリックしONにします。
3. 「**クライアント名 (MAC アドレス)**」ドロップダウンリストから、制限を設定するクライアントを選択します。
4. フィルターを実行するカテゴリーをクリックしてチェックします。（**成人向け、インスタントメッセンジャー/コミュニケーションツール、P2P/ファイル転送サービス、ストリーミング/エンターテインメント**）
5. ⊕ をクリックしクライアントのプロファイルを追加します。
6. 設定を保存するには、「**適用**」をクリックします。

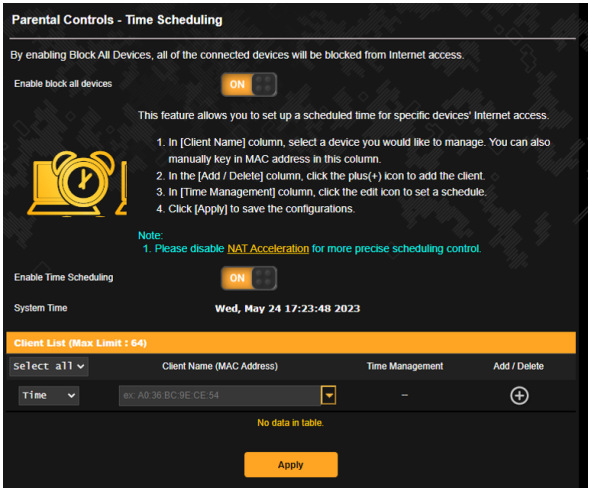
ご注意:

- 本機能はすべての通信を制御するものではありません。
- インスタントメッセンジャーなどの暗号化された通信は制御することができない場合があります。予めご了承ください。

時間設定

クライアントごとにインターネットを使用することができる時間を制限することができます。

ご注意: 時間設定機能を使用するには、本機のタイムゾーンとNTPサーバーが正しく設定されている必要があります。



手順

1. 「**ペアレンタルコントロール**」画面右上の「**時間設定**」をクリックします。
2. 「**タイムスケジュール**」のスイッチをクリックしONにします。
3. 「**クライアント名**」ドロップダウンリストから、制限を設定するクライアントを選択します。

ご注意: 「**クライアント名**」と「**クライアントのMACアドレス**」を手動で入力することでも設定することができます。クライアント名は半角英数字文字のみで入力してください。記号、スペース、特殊文字を使用した場合、正常に機能しない場合があります。

4. ⊕ をクリックし、クライアントのプロファイルを追加します。
5. 設定を保存するには、「**適用**」をクリックします。

4.14 スマートコネクト

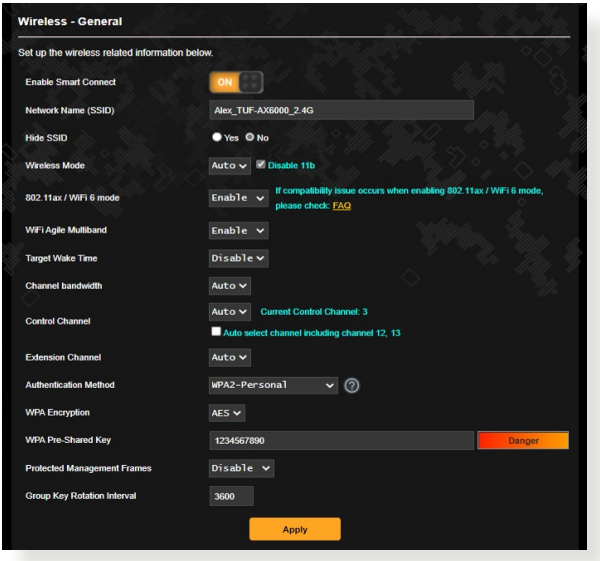
スマートコネクトでは、クライアントを2つの無線（2.4 GHz、5 GHz）のいずれかに自動的に切り替えます。

4.14.1 スマートコネクトのセットアップ

次の2つの方法で、Web GUIからスマートコネクトを有効にすることができます。

- **ワイヤレス画面から**

1. ウェブブラウザーのアドレス欄に「**http://www.asusrouter.com**」と入力します。
2. ログイン画面でユーザー名とパスワードを入力し、「**OK**」をクリックします。管理画面が表示されます。
3. ナビゲーションパネルから「**詳細設定**」→「**ワイヤレス**」→「**全般**」の順に開きます。
4. スマートコネクト機能を使用する場合は、「**スマートコネクト**」のスライダーを「**ON**」に移動します。（新規） この機能により、自動的に適切な周波数帯（2.4GHz、5GHz）でネットワーク内のクライアントを接続し、最適な速度を提供します。



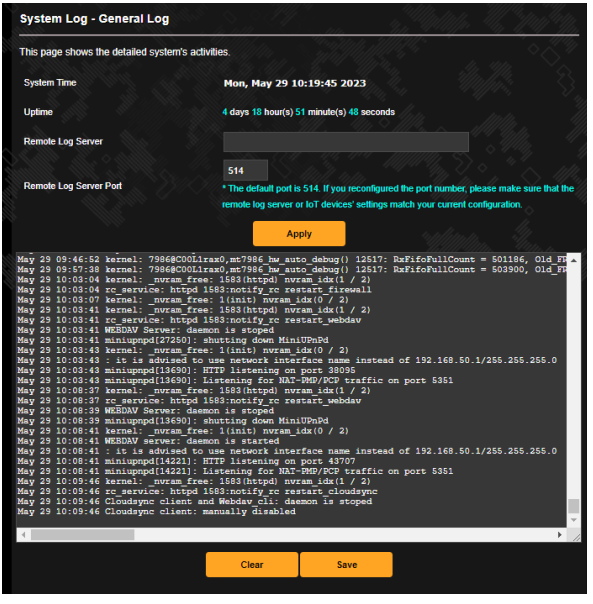
3.15 システムログ

システムログでは、本製品で行われた通信に関する履歴(ログ)をカテゴリーごとに確認することができます。

ご注意: 本製品を再起動または電電をオフにすると、システムログは自動的に消去されます。

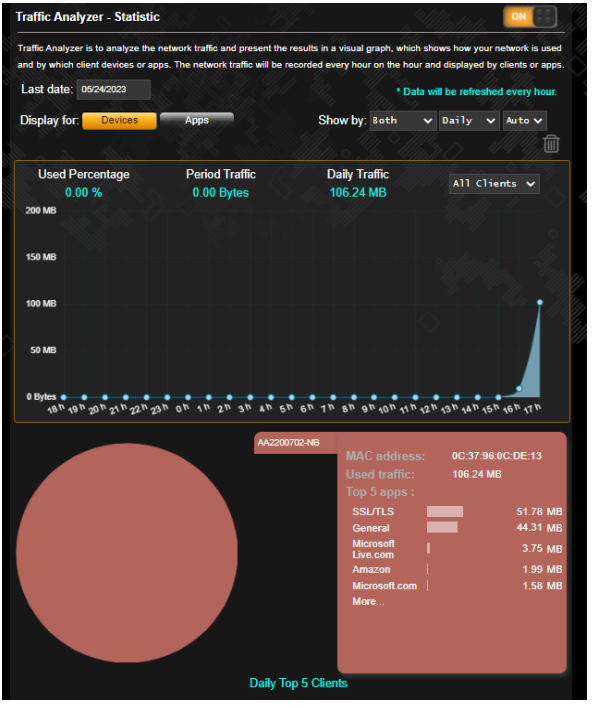
システムログを参照する

1. 「**システムログ**」をクリックします。
2. システムログは次のカテゴリーで分類されています。
   - 全般ログ
   - ワイヤレスログ
   - DHCPリース
   - IPv6
   - 経路表 (ルーティングテーブル)
   - ポートフォワーディング
   - 接続ログ



3.16 トラフィックアナライザー

トラフィックアナライザーでは、ネットワークのトラフィック状況を日、週、月ごとに統計を確認することができます。各ユーザーの帯域幅の使用状況や、使用デバイス、使用アプリを簡単に確認できるので、インターネット接続のボトルネックの軽減に役に立ちます。また、ユーザーのインターネット使用状況や利用コンテンツの監視も可能です。



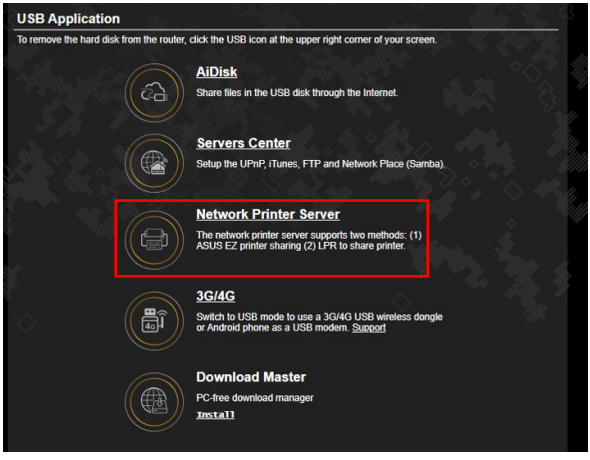
トラフィックアナライザーを使用する

1. Web GUIナビゲーションパネル全般の「**トラフィックアナライザー**」を開きます。
2. 「**トラフィックアナライザー**」メイン画面で、統計機能をオンにします。
3. グラフを表示したい日付を選択します。
4. 「**表示種別**」の欄で、情報を表示したいルーターまたはアプリを選択します。
5. 「**表示形式**」の欄で、情報を表示したい時間を選択します。

3.17 USBアプリケーション

無線LANルーターに接続したUSBストレージデバイスやプリンターなどを使用するためには、各アプリケーションで設定を行なう必要があります。

重要: 各種サーバー機能を使用するには、本体の外付けHDDやUSBメモリーなどの対応デバイスを接続する必要があります。本製品がサポートするUSBストレージデバイスのフォーマットタイプや容量については、次のWeb サイトでご確認ください。
(http://event.asus.com/networks/disksupport)
本製品がサポートするプリンターついては、次のWeb サイトでご確認ください。
(http://event.asus.com/networks/printersupport/)

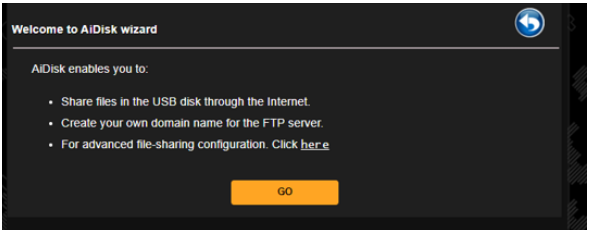


3.17.1 AiDiskを使用する

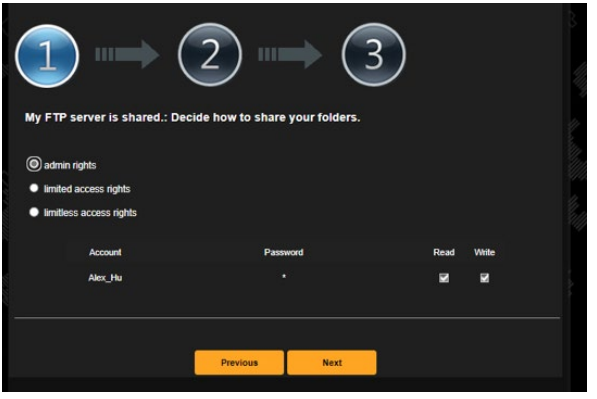
AiDisk は、無線LANルーターのUSBポートに接続したUSB ストレージデバイスをクラウドストレージのように使用することができる機能です。

AiDisk を使用する:

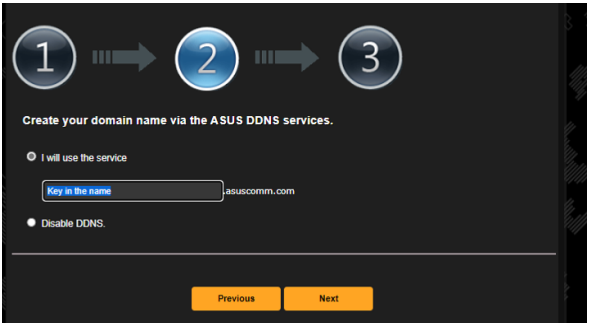
1. 「**USBアプリケーション**」→「**AiDisk**」の順にクリックします。
2. 「**設定**」をクリックし、AiDisk ウィザードを開始します。



3. ストレージの共有方法を選択します。



4. 外部ネットワークからのアクセスを可能にする場合は、asuscomm.comのドメインを作成します。



5. 「**次へ**」をクリックし設定を完了します。
6. AiDiskにアクセスするには、WebブラウザーまたはFTPクライアントに次のアドレスを入力します。
   ftp://<LAN IP アドレス>
   ftp://<ドメイン名>asuscomm.com (DDNSが有効の場合)

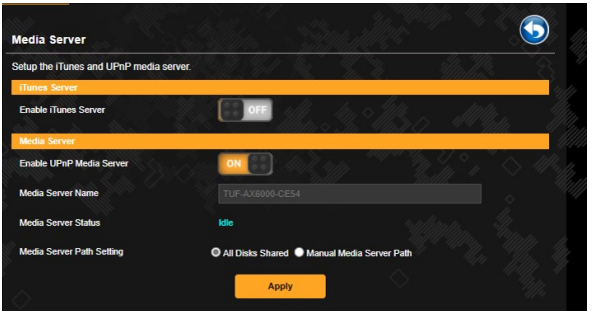
3.17.2 サーバーセンターを使用する

サーバーセンターでは、メディアサーバー、Sambaネットワーク共有、FTP共有によってUSBストレージデバイスに保存されたメディアファイルを共有することができます。

メディアサーバーを使用する

本製品では、UPnP対応デバイスからUSBストレージデバイスのメディアファイルにアクセスすることができます。

ご注意: UPnPメディアサーバー機能を使用する前に、DLNA対応デバイスを本機のネットワークに接続してください。

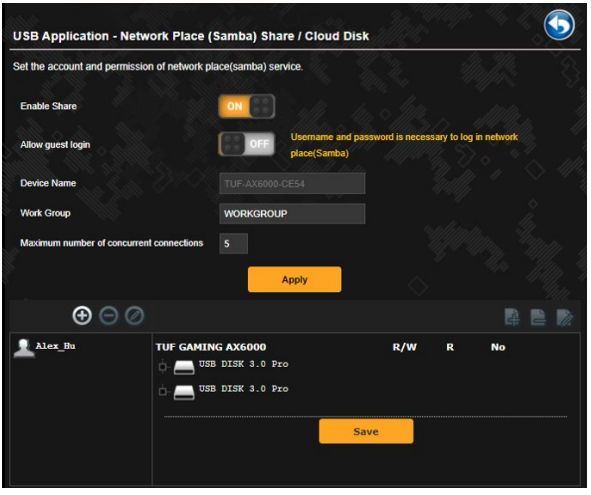


「**USBアプリケーション**」→「**サーバーセンター**」の順にクリックします。各項目については、次の説明をご覧ください。

- **iTunes サーバーを有効にする:**
  iTunesサーバー機能の有効/無効を設定
- **UPnPメディアサーバー:**
  UPnPメディアサーバー機能の有効/無効を設定
- **メディアサーバー名:**
  メディアサーバーの表示名を設定
- **メディアサーバーの状態:**
  現在のメディアサーバーの状態を表示
- **メディアサーバーパス設定**:
  メディアサーバー用ディレクトリパスの設定

ネットワークプレース (Samba) 共有サービスを使用する

ネットワークプレース (Samba) を利用するためのアカウントとアクセス権限を設定することができます。



手順

1. 「**USBアプリケーション**」→「**サーバーセンター**」の順にクリックします。

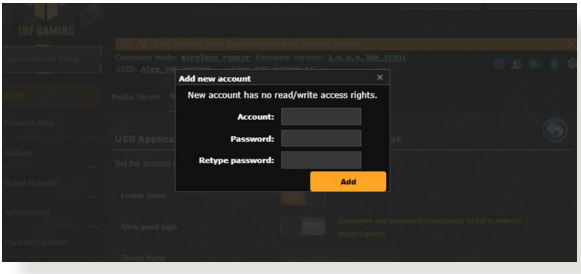
   ご注意: ネットワークプレース (Samba) はデフォルトで有効に設定されています。

2. 「**Samba 共有 / Cloud Disk**」タブをクリックし、次の手順でアカウントの管理を行います。

新しいアカウントを作成する

a) をクリックし、新しいアカウントを追加します。

b) 「**アカウント**」「**パスワード**」「**パスワードの再入力**」を入力し、「**追加**」をクリックしアカウントを作成します。



アカウントを削除する

a) アカウント一覧から削除したいアカウントを選択します。

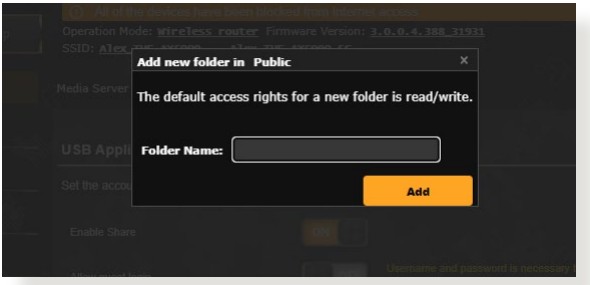
b) ⊖をクリックします。

c) アカウント削除の確認メッセージが表示されます。「**削除**」をクリックし、アカウントを削除します。

ストレージのルートディレクトリにフォルダーを追加する

a) USBストレージデバイスをクリックし、次に📁+をクリックします。

b) 新しいフォルダー名を入力し、「**追加**」をクリックします。作成されたフォルダーがフォルダーリストに追加されます。



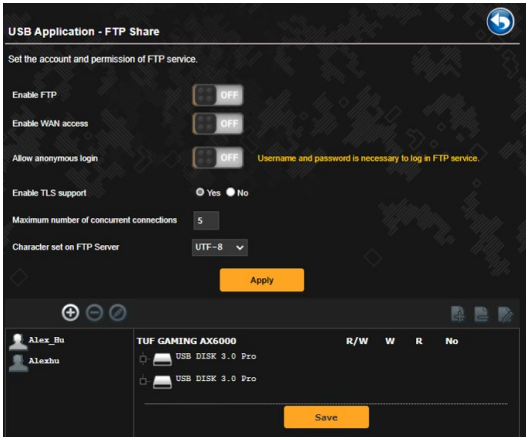
3. フォルダーリストから、フォルダーに割り当てるアクセス権限を選択します。ゲストアクセスがONの場合、この設定は不要です。
   - **R/W:** 読み取りアクセス許可 / 書き込みアクセス許可。
   - **R:** 読み取りアクセスのみ許可。
   - **No:** アクセスを許可しない (共有しない) 。
4. 「**権限を保存**」をクリックし、変更を適用します。

FTP共有サービスを使用する

本製品はFTPサーバーとして使うことができ、接続されたUSBストレージデバイスを共有することができます。

重要!

- USBストレージデバイスを取り外す際は、必ず安全な取り外しを行ってから取り外してください。適切な取り外し操作を行わずにデバイスを切断すると、デバイス上のデータが破損する可能性があります。
- USBディスクを安全に取り外す方法は、「**3.12.3 USBデバイスの管理**」の「**USBディスクを安全に取り外す**」をご覧ください。



FTP共有サービスを使用する

ご注意: 本機能を使用する前に、AiDisk機能を設定しFTPサーバーを利用可能な状態にしてください。詳しくは「**3.17.1 AiDiskを使用する**」をご覧ください。

1. 「**USBアプリケーション**」→「**サーバーセンター**」の順にクリックし、「**FTP共有**」タブを選択します。
2. 各項目を設定します。

    • **匿名アクセスを許可する**

    FTPリソースへの匿名アクセスの許可

    • **最大同時接続数**

    FTPサービスへの同時接続上限

- **文字コード**

  FTPで使用する文字コード

3. フォルダーリストから、フォルダーに割り当てるアクセス権限を選択します。 匿名アクセスの許可がONの場合、この設定は不要です。
   - **R/W**: 読み取りアクセス許可 / 書き込みアクセス許可。
   - **W**: 書き込みアクセスのみ許可。
   - **R**: 読み取りアクセスのみ許可。
   - **No**: アクセスを許可しない (共有しない) 。
4. 「**権限の保存**」をクリックし、変更を適用します。
5. FTPにアクセスするには、Webブラウザーまたは FTPクライアントに次のアドレスを入力します。

   ftp://<LAN IP アドレス>

   ftp://<ドメイン名>asuscomm.com (DDNSが有効の場合)

3.17.3 3G/4G

本製品のUSBポートに3G/4G USBモデムを接続することで、モバイルネットワークを使用してインターネットアクセスをすることができます。

ご注意: 本製品がサポートする3G/4Gモデムついては、次のWebサイトでご確認ください。
(http://event.asus.com/networks/3gsupport/)

3G/4Gインターネットアクセスをセットアップする

1. 「**USBアプリケーション**」→「**3G/4G**」の順にクリックします。
2. 「**USBモード**」を「**ON**」にします。
3. 各項目を設定します。
   - **場所:** 回線事業者（プロバイダー）の地域（国）をドロップダウンリストから選択します。
   - **通信方式**: 回線事業者、またはマニュアルの場合は回線方式を選択します。
   - **APNサービス(オプション):** 回線事業者が指定する接続先をご使用ください。
   - **ダイヤル番号、PINコード:** 詳細についてはご契約の回線事業者にお問い合わせください。
   - **ユーザー名/パスワード:** 詳細についてはご契約の回線事業者にお問い合わせください。
   - **USBアダプター:** USBポートに接続されている3G/4G USBモデムのタイプを選択します。3G/4G USBモデムのタイプが不明、またはリストに存在しない場合は「**自動**」を選択します。
4. 「**適用**」をクリックし、設定を保存します。

ご注意: 設定を適用するためには、無線LANルーターの再起動が必要です。

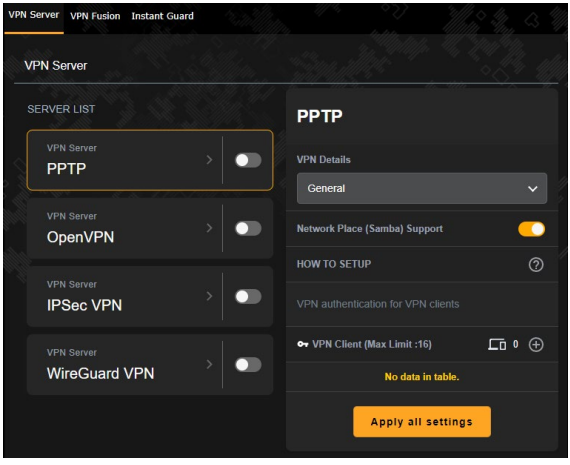
重要:

- 3G/4G インターネットアクセスの設定に必要な情報については、ご契約の回線事業者にご確認ください。
- ISPを選択した際に自動入力される値は最新でない可能性があります。設定を適用する前に、必ずご契約の回線事業者が指定する設定であることをご確認ください。
- ご契約の回線事業者によっては、3G/4G USBモデムによるネットワーク接続を使用した場合に別途通信料が発生する場合があります。本機能を利用するために必要となる通信機器、動作環境の整備及び通信料等は、ユーザーの責任で準備・負担するものとし、当社は一切責任を負いません。

3.18 VPN

VPN (Virtual Private Network) とは、インターネット上に仮想的な専用回線を構築する技術です。VPNを使用することで、外部ネットワークに接続されたコンピューターからインターネット経由でLAN側にアクセスすることができます。

ご注意: VPN接続を設定するには、VPNサーバーのIPアドレスまたはドメイン名が必要となります。



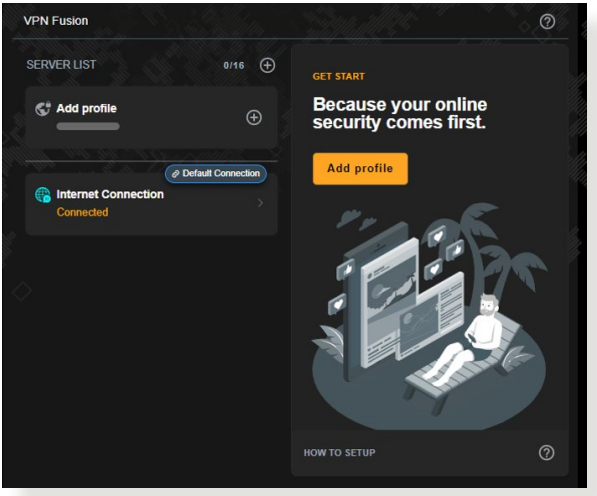
3.18.1 VPN サーバー

VPNサーバーのセットアップ

1. 「**VPN**」をクリックし、「**VPN サーバー**」タブを選択します。
2. 「**PPTP**」の「**はい**」をチェックします。
3. PPTPとOpenVPNは画面右上のボタンで切り替えることができます。
4. 「**ネットワークプレース (Samba) サポート**」の「**はい**」をチェックします。
5. VPNサーバー用のユーザー名とパスワードを入力し、⊕ ボタンをクリックします。
6. 「**適用**」をクリックし、設定を保存します。

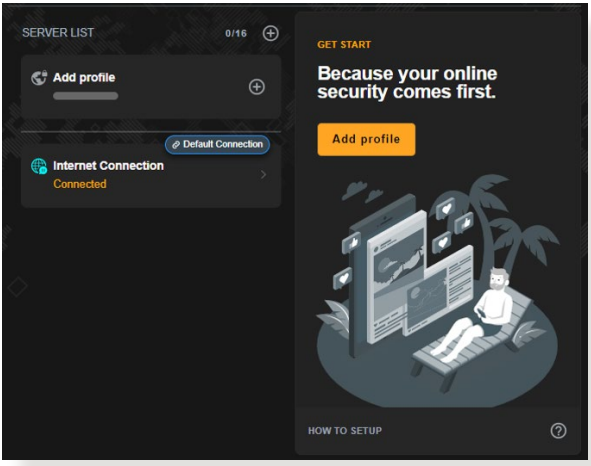
3.18.2 VPN Fusion（VPN フュージョン）

VPN Fusion（VPN フュージョン）を使用すれば、複数の VPN サーバーに同時に接続し、異なる VPN トンネルに接続するようにクライアントデバイスを割り当てることができます。 セットトップボックス、スマートテレビ、Blu-ray プレイヤーなどの一部の機器は VPN ソフトウェアに対応しません。 この機能は、ホームネットワーク内のそのようなデバイスに VPN アクセスを提供します。VPN ソフトウェアをインストールする必要はありません。スマートフォンは、VPN ではなく、インターネットに接続されたままになります。 ゲーマー向けには、VPN 接続は DDoS 攻撃を防いで、PC ゲームやストリームがゲームサーバーから切断されることを防止します。 VPN 接続を確立すれば、IP アドレスをゲームサーバーがあるリージョンに変更して、ゲームサーバーへの Ping 時間を改善することもできます。



開始するには、次の手順に従います。

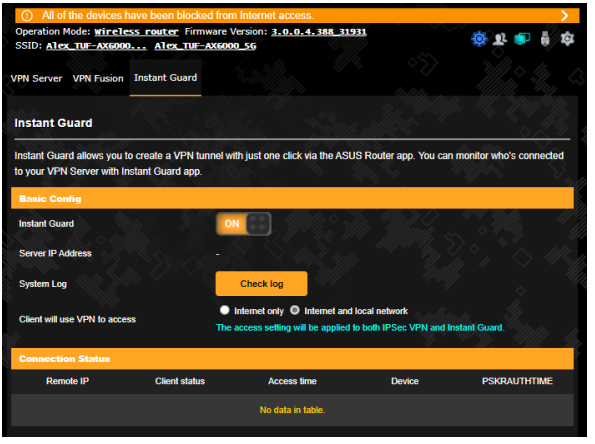
1. サーバーリストまたはプロファイルの 追加の横にあるをクリックして、新しいVPNトンネルを追加します。
2. サーバーリストで作成したVPN接続をアクティブにします。



3.18.3 Instant Guard（インスタントガード）

Instant Guard（インスタントガード）は、ルーター上でプライベートVPN サーバーを構築し、どこからでもホームネットワークへの安全な仮想プライベートネットワーク（VPN）アクセスを提供します。Instant Guard（インスタントガード） VPNトンネルを使用した場合は、すべてのデータがVPNサーバーを通過します。公共のフリーWiFi 使用時に自宅とデバイスの間に安全な VPN を構築し、お客様のデータ、プライバシーの保護を可能にする機能です。

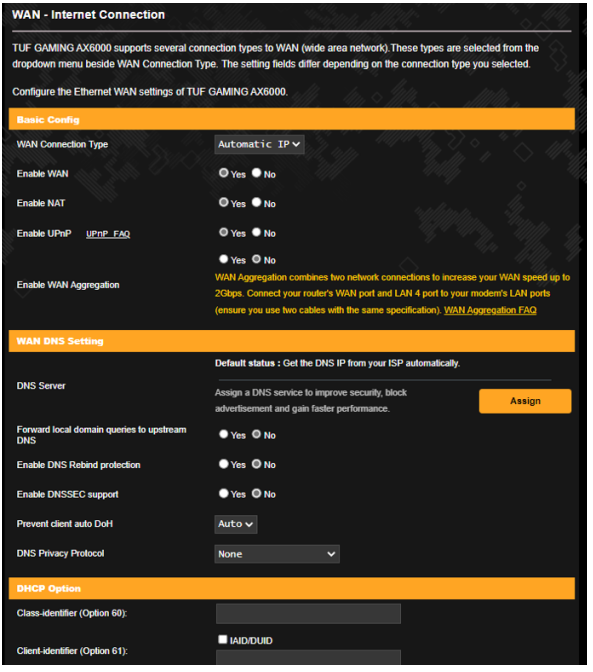
※利用するにはASUS Instant Guardアプリが必要です。



3.19 WAN

3.19.1 インターネット接続

インターネット接続では、WAN接続に関する各種設定をすることができます。



WAN接続のセットアップ

1. 「**WAN**」をクリックし、「**インターネット接続**」タブを選択します。
2. プロバイダーやネットワーク管理者の指示に従って接続設定行います。設定完了後は「**適用**」をクリックし、設定を保存します。

- **WAN接続タイプ**:ISP(インターネットサービスプロバイダー)への接続方法を選択します。ご契約プロバイダーの接続タイプについては、ご契約時の書類またはご契約のプロバイダーへお問い合わせください。

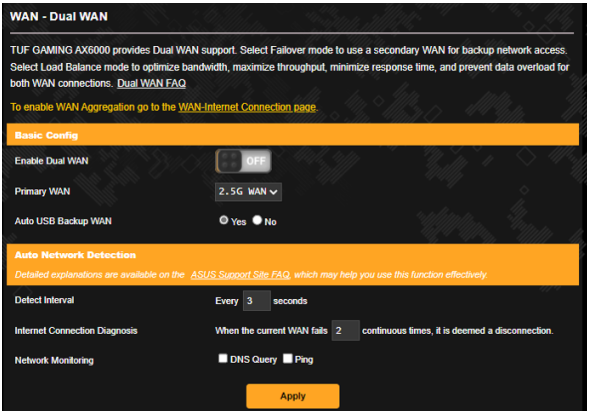
- **WAN を有効にする**: WAN (Wide Area Network) 接続の有効/無効を設定します。「**いいえ**」に設定した場合、WAN によるインターネット接続は無効になります。
- **NAT を有効にする**: NAT (Network Address Translation) は、プライベートIPアドレスを、インターネットで使用できるようグローバルIPアドレスに変換する機能です。これにより、1つのグローバルIPアドレス環境でプライベートIPアドレスを割り当てられた複数のコンピューターが、同時にインターネットへアクセスできるようになります。「**いいえ**」に設定した場合、インターネットは1台のみで利用可能です。
- **UPnPを有効にする**: UPnP (Universal Plug and Play) 機能の有効/無効を設定します。UPnPは、コンピューターやその周辺機器をはじめとして、AV機器、電話、家電製品、情報機器などのあらゆる機器をネットワーク経由で相互接続するための技術です。この機能を有効にすることで、UPnPによるデバイス検出、LAN内機器からのポートマッピング要求、LAN内機器へのWAN側IPアドレス通知、ポートフォワーディングの動的設定などを行なうことができます。
- **DNSサーバー:** DNSサーバーを設定します。ASUSルーターがインターネットに接続されると、デフォルトでインターネットサービスプロバイダー (ISP) からDNSサーバーのIPを自動的に取得します。
- **認証:** IEEE 802.1x (MD5) による認証を使用する際に設定します。この設定はプロバイダーから指定された場合にのみ設定します。認証方法やユーザー名、パスワードなどについては、ご契約時の書類またはご契約のプロバイダーへお問い合わせください。
- **ホスト名:** ご契約のプロバイダーによっては、このホスト名の設定が必要な場合があります。ホスト名については、ご契約時の書類またはご契約のプロバイダーへお問い合わせください。

- **MACアドレス**: MAC (Media Access Control) アドレスは、ネットワーク上で各ノードを識別するために、LANカードやネットワークデバイスに割り当てられている物理アドレスです。プロバイダーによっては、登録されたMACアドレスのデバイスでのみ通信を許可するなどの監視を行っている場合があります。未登録MACアドレスによる接続問題が発生した場合、次の手段で問題を回避することができます。
  - ご契約のプロバイダーへ新しいMACアドレスを通知し登録を更新する。
  - 「**MACクローン**」機能を使用し、ご契約のプロバイダーに登録されているMACアドレスを無線LANルーターのMACアドレスとしてクローン設定する。
- **DHCPクエリの頻度:** DHCPサーバー検出頻度を設定し、DHCPサーバーへの負荷を軽減することができます。

3.19.2 デュアル WAN

本製品はデュアルWANをサポートしており、次の2つのモードから設定することができます。

- **フェイルオーバー:** プライマリWANに障害が発生した場合、自動的にセカンダリWANに切り替えて使用します。
- **負荷分散:** プライマリWANとセカンダリWANの2つの回線を利用して負荷を分散させると共に障害が発生した際のバックアップ回線として機能します。

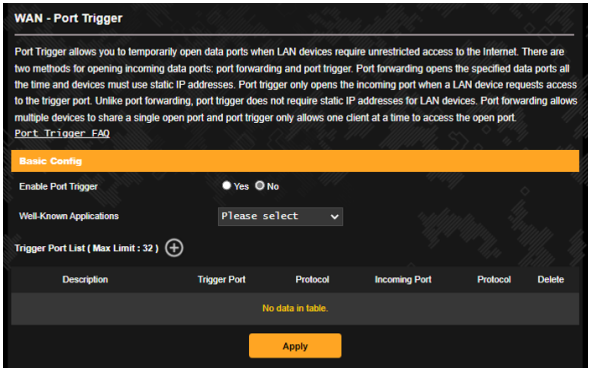


3.19.3 ポートトリガー

ポートトリガーは、LAN デバイスからのトリガーポートの要求に応じて外部ポートを一時的に開くことができます。

ポートトリガーは、次のような場合に使用することができます。

- 複数のクライアントが、同じアプリケーションで異なる時間にポート開放 (仮想サーバーまたはポートフォワーディング) を必要とする場合
- アプリケーションが発信ポートとは異なる特定の着信ポートを必要とする場合



ポートトリガーのセットアップ

1. 「**WAN**」をクリックし、「**ポートトリガー**」タブを選択します。
2. 「**ポートトリガーを有効にする**」を「**はい**」にチェックを入れます。
3. 「**アプリケーション**」を選択することで、一般的に使用されるアプリケーションを簡単にセットすることができます。
4. トリガーポートリストの各項目に必要事項を入力することで、手動でアイテムを追加することもできます。
   - **設定内容:** トリガーポートリストに登録する際の識別名を入力します。
   - **トリガーポート:**監視するトリガーポート (発信ポート) 範囲を指定します。

- **プロトコル:** トリガーポートの通信プロトコルを選択します。
- **着信ポート:** トリガーによって一時的に開放される着信ポートの範囲を指定します。
- **プロトコル:** 着信ポートの通信プロトコルを選択します。

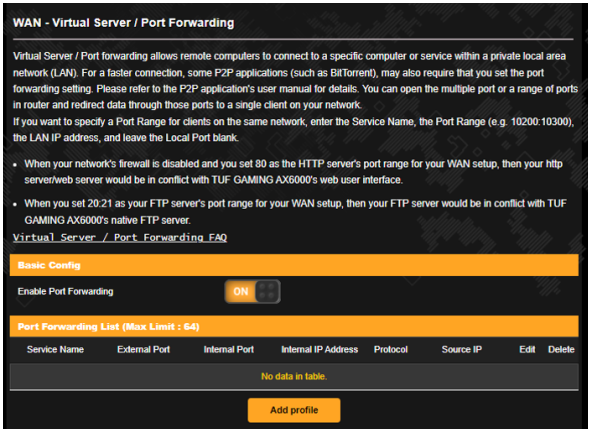
5. をクリックし、ポートトリガーに関する情報をリストに追加します。 ボタンをクリックすることで、追加されたエントリーを削除することができます。
6. 「**適用**」をクリックし、設定を保存します。

ご注意:

- IRCサーバーに接続する場合、クライアントはトリガーポート範囲「**66660-7000**」を使用して接続要求を行います。IRCサーバーはユーザー名を確認し、着信ポートを使用してクライアントへの新しい接続を確立することによって、要求に応答します。
- ポートトリガー機能が無効に設定されている場合、IRCサーバーへの接続要求を行っているクライアントを特定することができないため、ルーターの接続は強制的に切断されます。ポートトリガー機能が有効に設定されている場合、ルーターはデータを受信するために着信ポートを割り当てます。ルーターはアプリケーションが終了したかどうかを判断できないため、一定時間が経過すると自動的に着信ポートを閉じようとします。
- ポートトリガーは1度にネットワーク上の1つのクライアントのみに特定のサービスと特定の着信ポートを使用することを許可します。
- 同じアプリケーションを使用して1度に複数のクライアントでポートトリガーを行なうことはできません。ルーターは最後に送信されたクライアントの接続要求に対してのみ応答します。

3.19.4 ポートフォワーディング

ポートフォワーディングは、インターネットから特定のポート番号宛にパケットが届いた場合に、あらかじめ設定しておいた LAN 側のコンピューターにパケットを転送する機能です。ポートフォワーディング機能を有効にすることで、LANの外側からLAN内部のコンピューターが提供するサービスにアクセスすることが可能になります。



ポートフォワーディングのセットアップ

1. 「**WAN**」をクリックし、「**ポートフォワーディング**」タブを選択します。
2. 「**ポートフォワーディングを有効にする**」を「**On**」にします。
3. 「**サーバーリスト**」を選択することで、一般的に使用されるサーバーを簡単にセットすることができます。
4. 「**ゲームリスト**」を選択することで、一般的にプレイされるゲームを簡単にセットすることができます。
5. ポートフォワーディングリストの各項目に必要事項を入力することで、手動でアイテムを追加することもできます。

- **サービス名:** ポートフォワーディングリストに登録する際の識別名を入力します。

- **ポートレンジ:** ポートフォワーディングによって転送されたパケットを受信するクライアントのポートを設定します。同じネットワーク上にあるクライアントのポート範囲を指定したい場合は、サービス名、ポートレンジ (例 10200**:**10300)、ローカル IP を入力します。ローカルポートの項目は空欄にします。ポートレンジは複数の形式で指定することが可能です。
例: ポート範囲 (300**:**500)、個別ポート (566,789)、ポート範囲と個別 (1015**:**1024,3021)

ご注意:

- ネットワークファイアウォールを無効に設定し、WANセットアップ用にHTTPサーバーにポート80を割り当てている場合、HTTPサーバー/Webサーバー/本製品の管理画面に競合が発生し使用することができません。
- ネットワークはデータ交換を行うためにポートを使用しますが、各ポートにはポートナンバーと特定のタスクが割り当てられています。例えば、ポート80はHTTPに使用されます。特定のポートは1度に1つのアプリケーションまたはサービスのみを使用することができます。このため、2台のPCが同時に同じポートを経由してデータにアクセスすることはできません。例えば、2台のPCで同時にポート100にポートフォワーディングを設定することはできません。

- **ローカルIP:** ポートフォワーディングによって転送されたパケットを受信するクライアントのIPアドレスを設定します。

ご注意: ポートフォワーディング機能を使用するには、クライアントに静的IPアドレスを割り当てる必要があります。詳細については、「**4.2 LAN**」をご覧ください。

- **ローカルポート:** ポートフォワーディングによって転送されるパケットを特定のポートで受信させたい場合にポート番号を設定します。着信パケットを特定ポートではなくポート範囲内でリダイレクトするには、この項目を空欄にします。
- **プロトコル:** ポートフォワーディングの通信プロトコルを選択します。不明な場合は「**BOTH**」を選択することをお勧めします。

ポートフォワーディング機能が正しく設定されていることを確認する

- サーバーまたはアプリケーションが正しくセットアップされ動作していることを確認します。
- LANの外側へアクセス可能なクライアント (以下、インターネットクライアントと表記) を準備します。インターネットクライアントは、本製品のネットワークグループに接続しません。
- 本製品のWAN IPアドレスを使用してインターネットクライアントからサーバーにアクセスします。ポートフォワーディングが正常に機能している場合は、ファイルやアプリケーションにアクセスすることができます。

ポートトリガーとポートフォワーディングの違い

- ポートトリガーは静的IPアドレスを設定せずに使用することができます。また、ポートトリガーではルーターを使用して動的な転送を可能とします。例えば、複数のクライアントが同じアプリケーションでポート開放を必要とする場合、ポートフォワーディングでは個別に設定する必要がありますが、ポートトリガーは発信ポート (トリガーポート) のアクセス要求を監視することで、ポートを開放します。

  ポートトリガーは、一定時間が経過すると自動的に着信ポートを閉じようとします。ポートフォワーディングのように指定したポートを常に開放せず、接続要求によってのみ一時的にポートを開放するので安全に使用することができます。

3.19.5 DMZ

DMZ (DeMilitarized Zone) とは、ネットワーク上でファイアウォールによって包囲された、外部ネットワークからも内部ネットワークからも隔離された領域のことです。外部からアクセスされるDNSサーバー、メールサーバー、Webサーバーなどのホストコンピューターを仮想DMZ領域に配置することで、既存のLANに対してセキュリティを確保することができます。

警告: DMZを設定した場合、登録したIPアドレスに対してすべてのポートを開放した状態になります。セキュリティが低下しますのでご注意ください。セキュリティには十分ご注意ください。

DMZのセットアップ

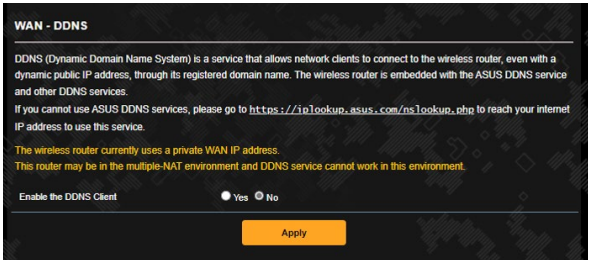
1. 「**WAN**」をクリックし、「**DMZ**」タブを選択します。
2. 「**DMZ を有効にする**」の「**はい**」を選択します。
3. **公開ステーションのIPアドレス:** DMZ指定するクライアントのIPアドレスを入力します。サーバークライアントは静的IPアドレスが割り当てられている必要があります。
4. 「**適用**」をクリックし、設定を保存します。

DMZの削除

1. 「**公開ステーションのIPアドレス**」に入力したIPアドレスを削除します。
2. 「**適用**」をクリックし、設定を保存します。

3.19.6 DDNS

DDNS (Dynamic Domain Name System) は、固定のIPアドレスが割り当てられていない場合でも、特定のドメイン名を利用できるサービスです。本製品では、ASUS DDNS Serviceまたはその他のDDNSサービスを介することにより外部ネットワークからのアクセスを可能にします。



DDNSのセットアップ

1. 「**WAN**」をクリックし、「**DDNS**」タブを選択します。
2. ご利用環境に応じて以下の設定を行います。設定完了後は「**適用**」をクリックし、設定を保存します。

- **DDNSクライアントを有効にする:** インターネット経由で外部から無線LANルーターにアクセスを可能にするDDNS機能の有効/無効を設定します。
- **サーバー/ホスト名:** DDNSサービスを利用するサーバーをドロップダウンリストから選択します。ASUS DDNS Service を利用する場合は、希望ホスト名 (ドメイン名) を入力します。
- ASUS DDNS Service (WWW.ASUS.COM) 以外のサーバーを利用したい場合は、まずはじめに「**無料お試し**」をクリックしオンライン登録を行ってください。
- **ワイルドカードを有効にしますか:** ご利用のDDNSサービスがワイルドカードをサポートしている場合のワイルドカードサポートの有効/無効を設定します。

ご注意:

DDNSサービスは次の条件下で動作しません。

- 無線LANルーターにプライベートIPアドレスが割り当てられている場合。
  例: 192.168.x.x、172.16.x.x、10.x.x.x
  この場合、管理画面上に黄色のテキストで警告が表示されます。
- 複数のNATテーブルが存在するネットワーク上に無線LANルーターがある場合。

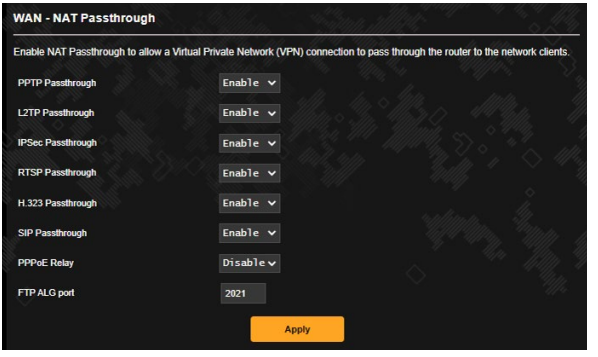
3.19.7 NATパススルー

NATパススルーでは、クライアントからの各VPNの接続要求に対してパケットをWAN (インターネット) 側に通過させるかどうかの設定が可能です。

PPTP、L2TP、IPsec、RTSP、H.323、SIP パススルーはデフォルトで有効に設定されています。

NATパススルーのセットアップ

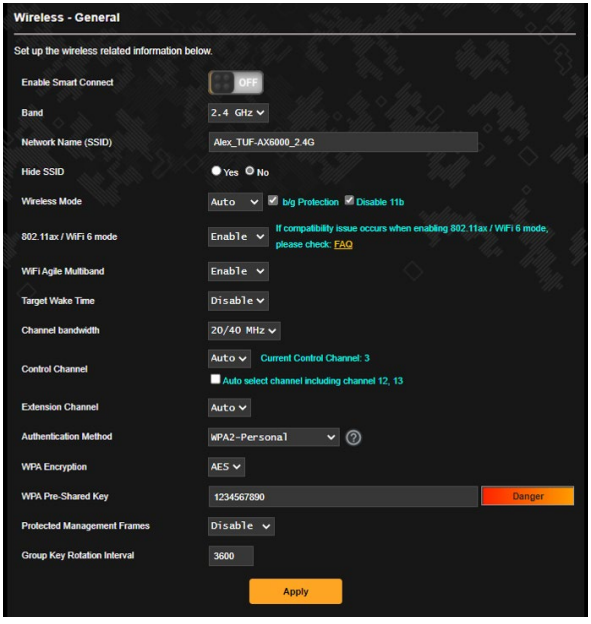
1. 「**WAN**」をクリックし、「**NAT パススルー**」タブを選択します。
2. 各パススルー機能の有効/無効を設定します。設定完了後「**適用**」をクリックし、設定を保存します。



3.20 ワイヤレス

3.20.1 全般設定

全般タブでは基本的なワイヤレス設定を行なうことができます。



基本的なワイヤレス設定

1. 「**ワイヤレス**」をクリックし、「**全般**」タブを選択します。
2. Smart Connect のON / OFF を設定します。
3. ネットワークを識別するためのネットワーク名 (SSID) を設定します。ネットワーク名は半角英数字、- (ハイフン) 、_ (アンダースコア) を使用して32文字以内で入力します。

4. 「**SSIDを非表示**」の項目で「**はい**」を選択すると、無線LANルーターは他のパソコンからのアクセスに対しネットワークの参照に応答しないため、ネットワーク名を検出することができなくなります。この機能を有効にした場合、ワイヤレスデバイスがワイヤレスネットワークにアクセスするにはネットワーク名をワイヤレスデバイス上で手動で入力する必要があります。
5. 通信に使用するワイヤレスモードを選択します。
   - **自動:** IEEE802.11 a/b/g/n/acで通信します。
   - **Legacy:** IEEE802.11 b/g/nで通信します。ただし IEEE802.11nをネイティブサポートするハードウェアの最大通信速度は54Mbpsとなります。
   - **N only(2.4GHz), N/AC mixed:** IEEE802.11nのみ、またはIEEE802.11n/acでのみ通信します。IEEE802.11a/b/gでの通信は行えません。

   ご注意: 「**b/g Protection**」をチェックするとIEEE802.11bとIEEE802.11gが混在する環境でIEEE802.11g の通信を優先させることができます。
6. 通信チャンネルを選択します。
7. 通信チャンネルを選択します。[**自動**]を選択した場合、無線LANルーターは電波干渉の少ないチャンネルを自動的に選択して使用します。
8. より高速な通信を行う場合は、チャンネル帯域の設定を行います。
9. 認証方式を選択します。

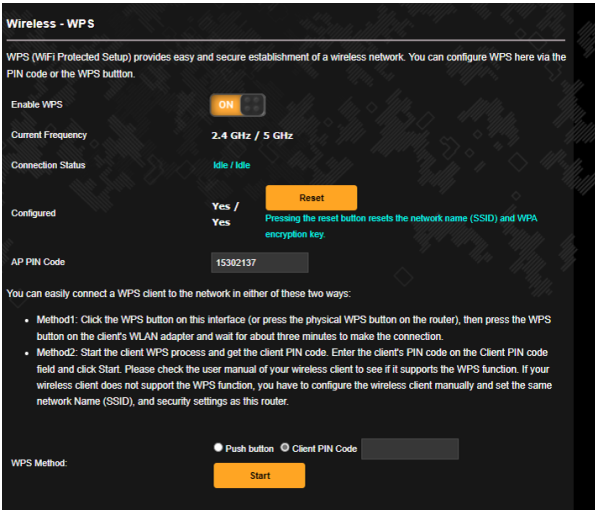
   ご注意: 暗号化方式でWEP (64/128 bit) またはTKIPを使用した場合、最大転送速度は54Mbps (規格値) となります。
10. 「**適用**」をクリックし、設定を保存します。

    ご注意: WEPによる暗号化通信、および一部の認証方式はワイヤレスモード「**Legacy**」のみで利用することができます。

3.20.2 WPS

WPS (Wi-Fi Protected Setup) は、Wi-Fi Allianceが策定したワイヤレスネットワーク接続・セキュリティの設定を簡単に行なうための規格です。WPS に対応したワイヤレスデバイスをプッシュボタン方式またはPIN方式で簡単に接続することができます。

ご注意: WPS機能を使用する前に、ご利用のデバイスがWPSに対応していることをご確認ください。



WPSを有効にする

1. 「**ワイヤレス**」をクリックし、「**WPS**」タブを選択します。
2. 「**WPSを有効にする**」のスイッチをクリックして、WPS機能をONにします。
3. WPSで接続設定を行なう周波数帯はデフォルト設定で「**2.4GHz**」に設定されています。周波数帯を変更する場合は、WPS機能を一旦OFFにし「**現在の周波数**」ドロップダウンリストから、使用する周波数帯を選択します。

ご注意: WPS機能は次の認証方式でのみ利用することができます。**Open System, WPA/WPA2/WPA3-Personal**。また、SSID非表示設定が有効の場合、WPS機能は使用できません。

4. 「**WPS方式**」で接続方法を選択します。WPS ボタン方式で接続する場合は**手順5**へ、PINコード方式で接続する場合は**手順6**へ進みます。
5. プッシュボタン接続方式を使用して接続する場合は、次の手順に従って操作します。
   a. コンピューターの場合は、WPSで接続設定を行なう周波数帯のネットワーク名 (SSID) を選択し、ネットワークキーの入力画面にします。その他のデバイスの場合は、デバイス上のWPSボタンを押し、接続待機状態にします。
   b. 管理画面でWPS方式の「**WPS ボタン**」をチェックし「**開始**」ボタンをクリックするか、または本体背面のWPSボタンを押します。

ご注意: WPSボタンの位置については、ご使用のデバイスの取扱説明書をご覧ください。

   c. しばらくすると、ネットワークに接続され通知領域 (タスクトレイ) のワイヤレスネットワークアイコンが接続状態となります。接続デバイスが検出されない場合、WPSは自動的にアイドル状態に切り替わります。
6. PINコード接続方式を使用して接続する場合は、次の手順に従って操作します。

   ワイヤレスデバイスからの接続設定:

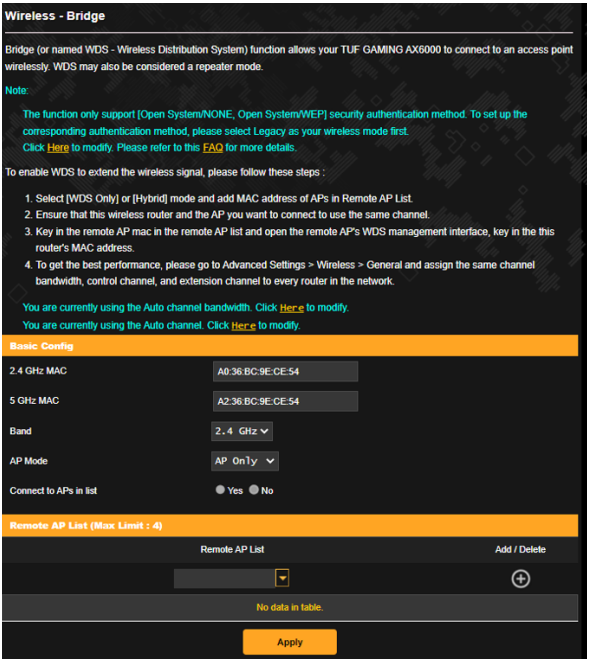
   a. 無線LANルーターのPINコードを確認します。PINコードは管理画面上の「**AP PIN コード**」に表記されています。
   b. ワイヤレスデバイスにPINコードを入力しWPS機能を有効にします。接続設定中は電源LEDが3回点滅します。

   無線LANルーターからの接続設定:

   a. ワイヤレスデバイスのPINコードを確認します。PINコードは、デバイス上または取扱説明書などをご確認ください。
   b. 「**クライアント PIN コード**」をチェックし、にワイヤレスデバイスのPINコードを入力して「**開始**」ボタンをクリックします。
   c. ワイヤレスデバイスのWPS機能を有効にしWPS接続を開始します。接続設定中は電源LEDが3回点滅します。

3.20.3 ブリッジ

ブリッジとは、別々のネットワークを1つのネットワークとして結合することです。本製品は、物理的に離れたネットワークをワイヤレス接続で結合するWDS (Wireless Distribution System) をサポートしています。WDSは「**ワイヤレスブリッジ**」、「**リピーター機能**」、「**アクセスポイント間通信**」とも呼ばれており、通信範囲を広げたり、電波の届きづらい場所への中継を可能にします。



ワイヤレスブリッジのセットアップ

1. 「**ワイヤレス**」をクリックし、「**WDS**」タブを選択します。
2. 「**バンド**」ドロップダウンリストでワイヤレスブリッジで使用する周波数帯を選択します。

3. 「**APモード**」ドロップダウンリストから動作モードを選択します。
   - **AP Only:** ワイヤレスブリッジ機能を使用しません。
   - **WDS Only:** ワイヤレスブリッジとしてのみ動作します。アクセスポイントとして動作しないため、ワイヤレスデバイスを接続することはできません。
   - **Hybrid:** ワイヤレスブリッジとして動作し、ワイヤレスデバイスを接続することもできます。

   ご注意:「**Hybrid**」モードに設定した場合、本製品のアクセスポイントの通信速度は通常の半分の速度となります。

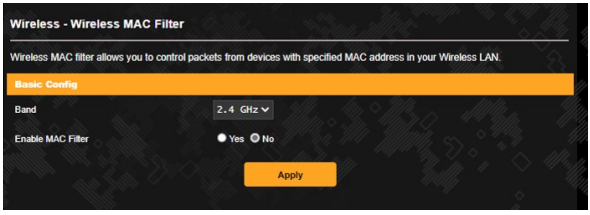
4. リモートブリッジリストに登録したアクセスポイントに接続する場合は、「**リスト内のAPに接続しますか**」の「**はい**」をチェックします。
5. リモートブリッジリストに新たなアクセスポイントを追加するには、プルダウンリストから選択するか、MACアドレスを入力し  ボタンをクリックします。

   ご注意: リモートブリッジリストに追加されたアクセスポイントを使用するには、無線LANルーターとアクセスポイントが同じチャンネル上にある必要があります。

6. 「**適用**」をクリックし、設定を保存します。
7. デフォルト設定では、ワイヤレスブリッジ用のチャンネルは「**自動**」に設定されており、ルーターは自動的に干渉が最も少ないチャンネルを選択します。チャンネルは「**ワイヤレス**」の「**全般**」タブ内で変更することができます。スマートコネクト機能が有効の場合、手動でチャンネル設定をすることはできません。

3.20.4 MACアドレスフィルタリング

MACアドレスフィルタリングでは、MACアドレスによる接続制限(MACアドレスフィルタリング) を設定することができます。

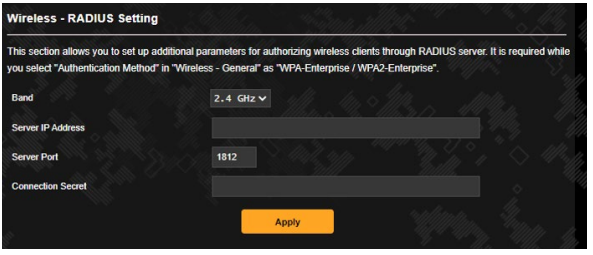


MACアドレスフィルタリングのセットアップ

1. 「**ワイヤレス**」をクリックし、「**ワイヤレスMACフィルタリング**」タブを選択します。
2. 周波数帯域を選択します。
3. 「**MAC アドレスフィルタリング**」の「**はい**」を選択します。
4. MACフィルターモードでフィルター動作を選択します。
   - **許可:** MACフィルターリストに登録されているデバイスのみ接続を許可します。
   - **拒否:** MACフィルターリストに登録されているデバイスの接続を拒否します。
5. MACフィルターリストに接続制限を行なうデバイスを追加するには、MACアドレスを入力し⊕ボタンをクリックします。
6. 「**適用**」をクリックし、設定を保存します。

3.20.5 RADIUS

RADIUS (Remote Authentication Dial In User Service) の設定では、RADIUS認証サーバーへの接続設定をすることができます。この設定は、ワイヤレスネットワークの認証方式をWPA/WPA2 Enterprise、またはRadius IEEE802.1xに設定した場合に必要となります。



RADIUS認証サーバーアクセスのセットアップ

1. ワイヤレス全般設定で認証方式をWPA/WPA2 Enterprise、またはRadius with 802.1xに設定したネットワークを構築します。

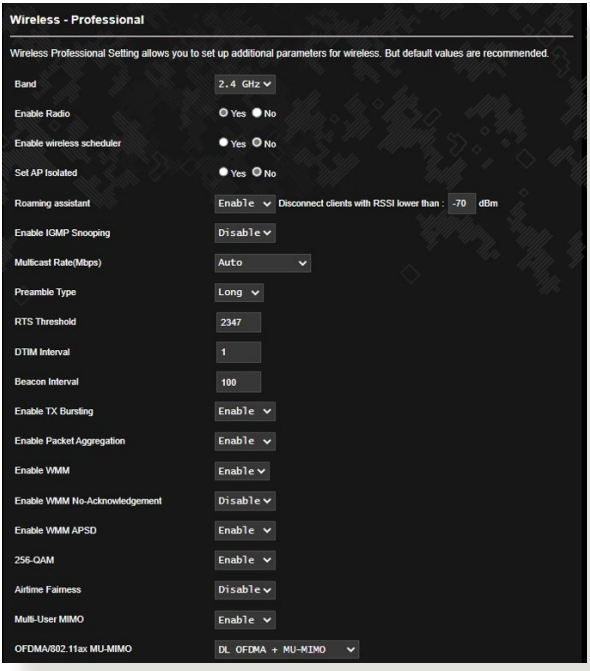
   ご注意: 認証方式については、「**4.2.1 全般設定**」をご覧ください。

2. 「**ワイヤレス**」をクリックし、「**RADIUS**」タブを選択します。
3. 「**バンド**」ドロップダウンリストで設定する周波数帯を選択します。
4. 「**サーバーIPアドレス**」に、RADIUS認証サーバーのIPアドレスを入力します。
5. 「**サーバーポート**」に、サーバーのポート番号を入力します。
6. 「**接続シークレット**」に、RADIUS認証サーバーにアクセスするためのパスワードを入力します。
7. 「**適用**」をクリックし、設定を保存します。

3.20.6 ワイヤレス - 詳細

「**詳細**」ではワイヤレスネットワークに関するより詳細な設定をすることができます。

ご注意: 特に必要がなければ、設定を変更せずに使用することをお勧めします。



「**詳細**」では、次の設定が可能です。

- **バンド:** 設定をする周波数帯を選択します。
- **ワイヤレス機能を有効にする:** ワイヤレスネットワークの有効/無効を設定します。
- **無線スケジューラを有効にする:** はいを選択して無線スケジューラを有効にして設定します。 いいえを選択して、ワイヤレススケジューラを無効にします。

- **時間設定:**「+」ボタンをクリックし、ワイヤレス機能を有効にする曜日や時間帯を設定します。「適用」をクリックし、設定を反映させます。
- **AP を隔離しますか:** ネットワーク上の各ワイヤレスデバイスが相互通信をできないようにします。この機能は多くのゲストユーザーが頻繁にネットワークに接続する場合などのセキュリティ強化として効果を発揮します。
- **ローミングアシスタント:** 複数のアクセスポイント、またはワイヤレスリピーターを含むネットワーク構成では、ワイヤレスクライアントがメインのワイヤレスルーターに接続されているため、ワイヤレスクライアントが利用可能なAPに自動的に接続できないことがあります。 この設定を有効にすると、信号強度が特定のしきい値を下回っている場合にクライアントがメインのワイヤレスルーターから切断され、より強い信号に接続されます。
- **IGMP スヌーピング:** この機能を有効にすると、デバイス間でIGMP（Internet Group Management Protocol）を監視し、無線マルチキャストトラフィックを最適化できます。
- **マルチキャスト速度 (Mbps) :** マルチキャストフレームの伝送レートを指定します。これは、アクセスポイントがワイヤレスネットワークにブロードキャストパケット及びマルチキャストパケットを伝送する速度です。
- **プリアンブルタイプ:** ワイヤレス通信の同期をとるプリアンブル信号の長さを選択します。「**ショートプリアンブル**」では通信速度が速くなる可能性がありますが、通信距離や互換性は低下します。「**ロングプリアンブル**」では通信距離と高い互換性を得ることができます。
- **AMPDU RTS:** この機能を有効にすると、複数のフレームを送信する前にグループ化し通信速度を高速化します。802.11gおよび802.11bデバイス間の通信では、すべてのAMPDUにRTS（request to send：送信要求)が使用されます。

- **RTSしきい値:** RTS (送信要求) 信号を送信するパケットサイズを設定します。しきい値を小さく設定することで、複数のデバイスを接続している場合などの通信の安定性を向上させることができます。
- **DTIM間隔:** DTIM (Delivery Traffic Indication Message) とは、省電力モードのワイヤレスデバイスに対してパケットの送信待ちであることを伝えるメッセージのことです。DTIM間隔では、ビーコンに対してDTIMを挿入する間隔を設定します。
- **ビーコン間隔:** ワイヤレスネットワークを同期させるためにアクセスポイントから送信するパケット (ビーコン) の間隔を設定します。ビーコン間隔を小さくすることでワイヤレスデバイスとの接続効率は向上しますが、通信効率は低下します。
- **Txバースト:** IEEE802.11g通信におけるバースト転送およびデータ圧縮により通信速度を向上させるTxバースト機能の有効/無効を設定します。
- **WMM APSDを有効にする:** WMM (Wi-Fi Multimedia) APSD (Automatic Power Save Delivery)、ワイヤレスデバイス間における電源管理機能の有効/無効を設定します。
- **256 QAM:** この機能を有効にすると、2.4GHz帯で256-QAM (MCS 8/9) をサポートし、この機能を有効にすると、2.4GHz帯で256-QAM(MCS 8/9)が有効となり、通信範囲とスループットを向上することができます。
- **エアタイムフェアネス:** この機能により、ネットワークの速度は、最も遅いトラフィックによる制限を回避できます。クライアント間で時間を均等に分配することにより、Airtime Fairnessは送信時に最高速度で転送が可能です。
- **エクスプリシットビームフォーミング:** クライアントのワイヤレスアダプターがビームフォーミングに対応している場合、本機器とのビームフォーミングをサポートします。この技術により、これら

のデバイス間で、チャンネル推定およびステアリングの方向を互いに通信して、ダウンロード速度およびアップリンク速度を向上させることができます。

- **インプリシットビームフォーミング:**ネットワークアダプターがビームフォーミングをサポートしない場合、「**インプリシットビームフォーミング**」を有効にすることで、チャンネルおよび、送信方向を推測し、ダウンリンク速度を向上させることができます。

4 ユーティリティ

ご注意:

- 無線LANルーター用ユーティリティは、次のURLからダウンロードいただけます。
- Device Discovery: http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Discovery.zip
- Firmware Restoration: http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Rescue.zip
- Windows Printer Utility: http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Printer.zip
- 無線LANルーター用ユーティリティはWindows® OS 環境でのみご利用いただけます。

4.1 Device Discovery

Device DiscoveryはASUS無線LANルーター専用のユーティリティで、コンピューターから接続可能なASUS無線LANルーターを検出し、設定を行うことができます。

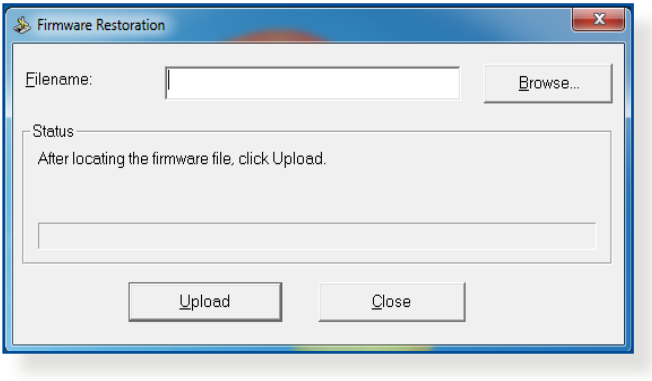
Device Discovery ユーティリティを起動する:

- 「**スタート**」ボタン→「**すべてのプログラム**」→「**ASUS Utility**」→「**ASUS Wireless Router**」→「**Device Discovery**」の順にクリックします。

ご注意: アクセスポイントモード、メディアブリッジモードをご使用の場合、ルーターのIPアドレスを確認するには本ユーティリティをご使用ください。

4.2 FirmwareRestoration（ファームウェアの復元）

本製品は、ファームウェアの更新に失敗した際に復旧を行うためのレスキューモードを備えています。レスキューモードでは、Firemware Restorationユーティリティを使用して指定したファームウェアファイルからファームウェアを復旧することができます。



重要! Firmware Restoration ユーティリティは、本機がレスキューモードで動作している場合にのみご使用ください。

ご注意: 本ユーティリティは、Windows® OS 環境でのみご利用いただけます。

Firmware Restorationユーティリティを使用する

1. 無線LANルーターの電源アダプターをコンセントから取り外します。
2. 無線LANルーター背面の「**リセットボタン**」を押したままの状態で、電源アダプターをコンセントに接続します。電源LEDが低速で点滅し、レスキューモードで起動したことを確認したらリセットボタンを放します。

3. コンピューターのIP アドレスを次の値に設定します。

   IPアドレス: 192.168.50.x

   サブネットマスク: 255.255.255.0

4. 「**スタート**」ボタン→「**すべてのプログラム**」→「**ASUS Utility**」→「**Wireless Router**」→「**Firmware Restoration**」の順にクリックします。

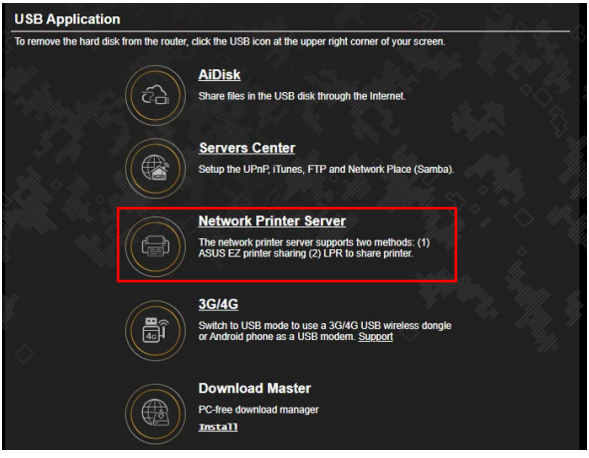
5. ファームウェアファイルを指定し、「**アップロード**」をクリックします。

ご注意: Firmware Restorationユーティリティはファームウェア更新用のユーティリティではありません。ファームウェアの更新を行う場合は、管理画面から実行してください。詳細については本マニュアルに記載の「**4.7.3 ファームウェアの更新**」をご覧ください。

4.3 プリンターサーバーの設定

4.3.1 ASUS EZ Printer Sharing

本製品では、専用のPrinter Setup Utility を使用するだけで、簡単に無線LANルーターのUSB ポートに接続したプリンターを共有することが可能です。

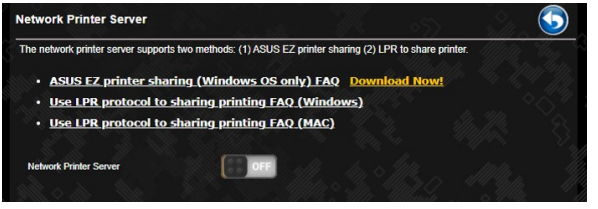


ご注意:

- 本製品がサポートするプリンターついては、次のWeb サイトでご確認ください。
  (http://event.asus.com/networks/printersupport)
- ご利用のOS環境により使用できる機能は異なります。

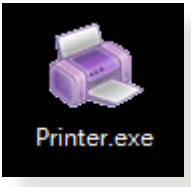
EZ Printer 共有モードのセットアップ

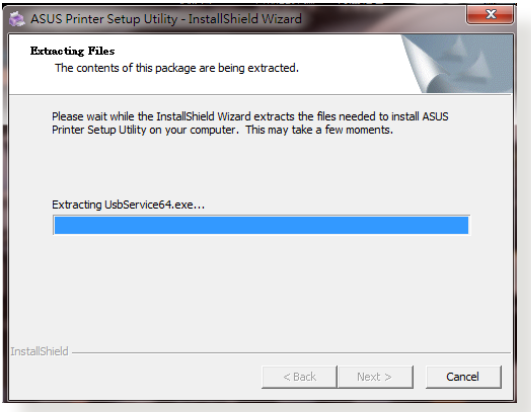
1. 管理画面で「**USBアプリケーション**」→「**ネットワークプリンターサーバー**」の順にクリックします。
2. 「**Download Now!**」をクリックし、Printer Setup Utility をダウンロードします。



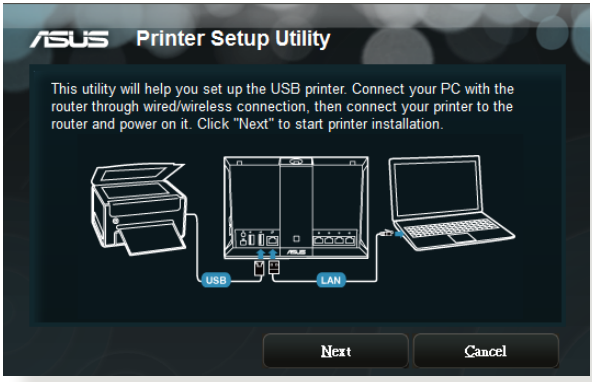
ご注意: LPRプロトコルでプリンターに接続する場合は、手動で設定を行う必要があります。

3. ダウンロードしたファイルを解凍し、実行ファイル「**Printer.exe**」を起動します。





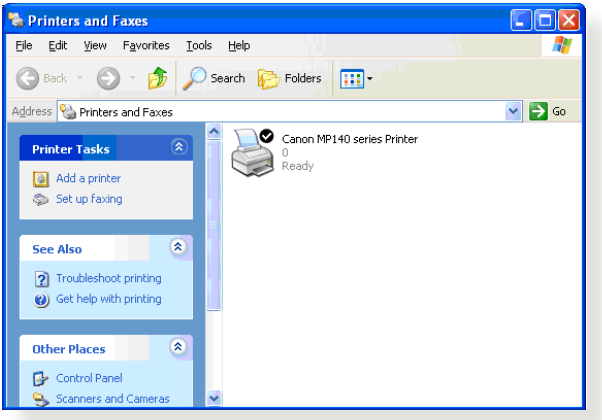
4. Printer Setup Utility によるセットアップウィザードが表示されます。画面に表示される指示に従ってセットアップを行います。



5. 初期セットアップが完了したら「**次へ**」をクリックします。初期セットアップには数分かかる場合があります。
6. 「**終了**」をクリックしセットアップを完了します。

7. Windows® OSの指示に従い、プリンタードライバーをインストールします。

8. プリンタードライバーのインストール後、ネットワークプリンターが利用可能となります。



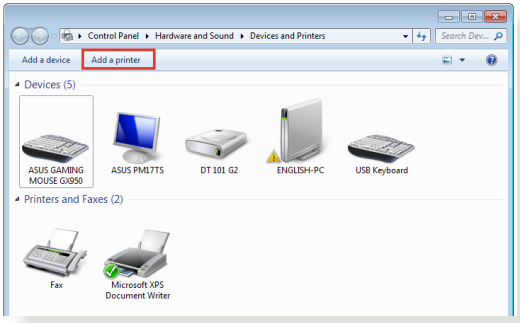
4.3.2 LPRを共有プリンターに使用する

LPR/LPD (Line Printer Remote/Line Printer Daemon) プロトコルを使用することで、ネットワーク上にあるWindows® OSやMac OSなど複数の環境でプリンターを共有することができます。

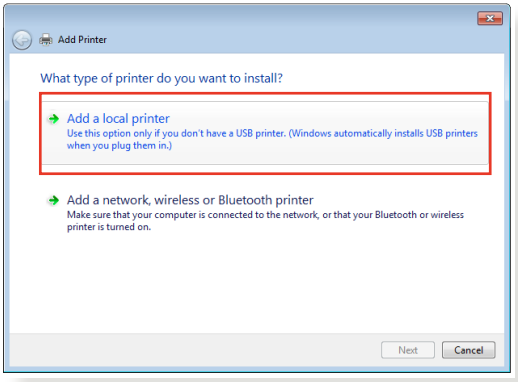
LPRプリンターを共有する （Windows® OS）

手順

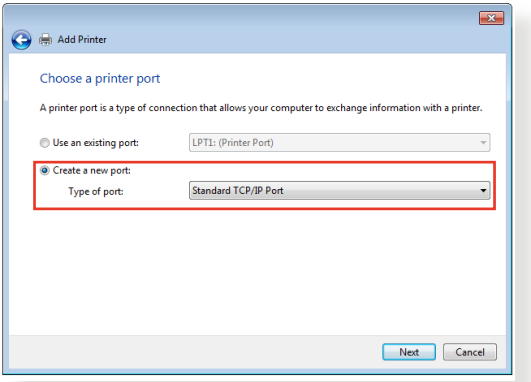
1. 「**スタート**」ボタン→「**コントロールパネル**」→「**ハードウェアとサウンド**」→「**デバイスとプリンター**」の順にクリックし、画面上部の「**プリンターの追加**」をクリックしてウィザードを起動します。



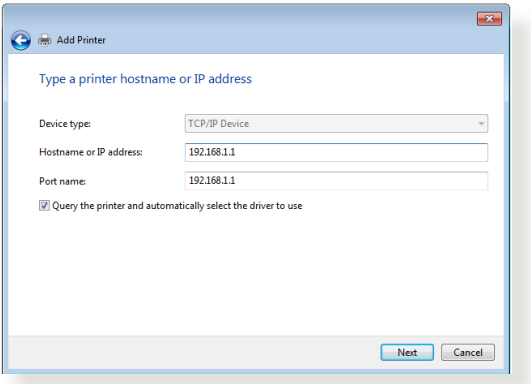
2. 「**ローカルプリンターの追加します**」をクリックします。



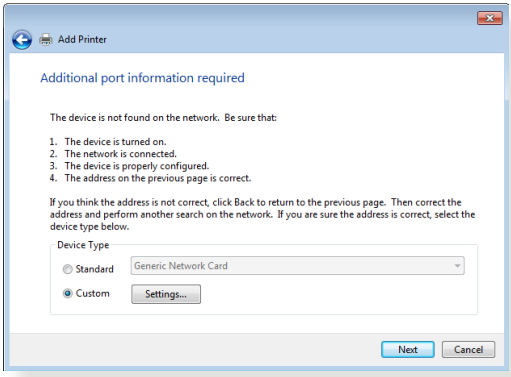
3. 「**新しいポートの作成**」をチェックし、ポートの種類を「**標準のTCP/IP ポート**」に設定し「**次へ**」をクリックします。



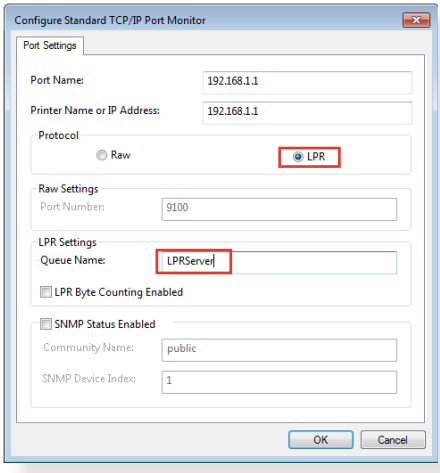
4. 「**ホスト名またはIPアドレス**」に無線LANルーターのIPアドレスを入力し「**次へ**」をクリックします。



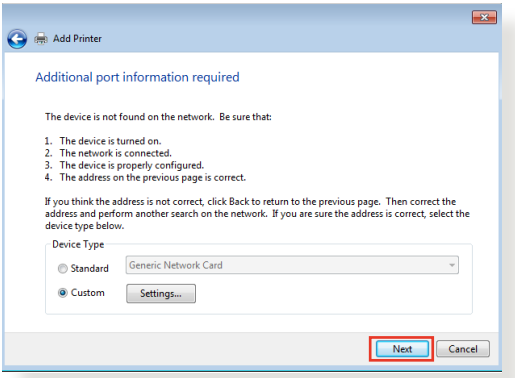
5. デバイスの種類の「**カスタム**」をチェックし、「**設定**」をクリックします。



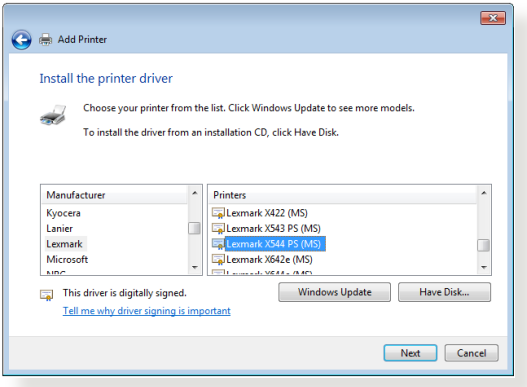
6. プロトコルを「**LPR**」に設定し、LPR設定のキュー名に「**LPRServer**」と入力し「**OK**」をクリックします。



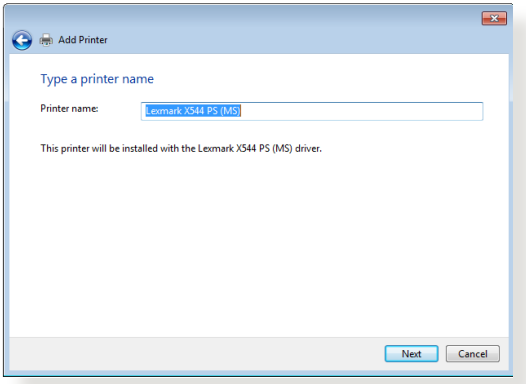
7. 「**次へ**」をクリックし、ドライバーの検出へ進みます。



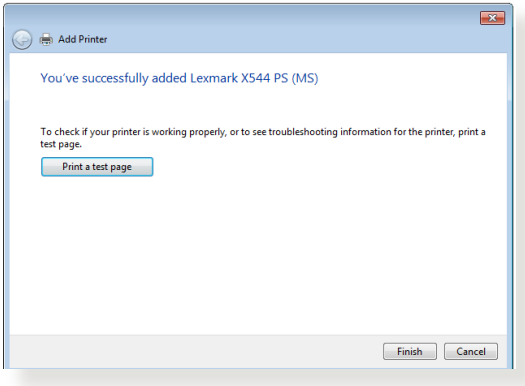
8. 製造元とプリンターを選択して「**次へ**」をクリックし、プリンタードライバーをインストールします。ご使用のプリンターが一覧に表示されない場合は、「**ディスク使用**」または「**Windows Update**」で適切なドライバーを読み込みます。



9. プリンター名を入力し、「**次へ**」をクリックします。



10. 「**完了**」をクリックして、プリンターの追加ウィザードを閉じます。



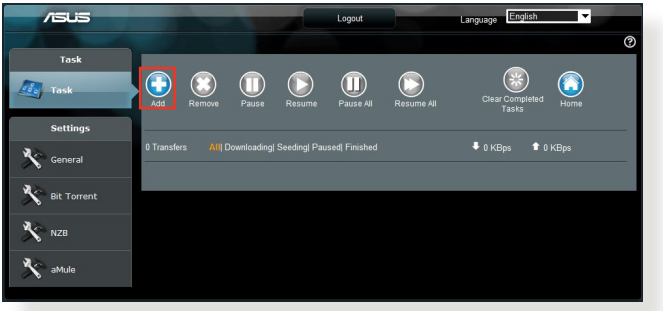
4.4 Download Master

Download Masterは、コンピューターや他のデバイスの電源がオフの状態でも無線LANルーターだけでファイルのダウンロードを行うことができる画期的な機能です。

ご注意: この機能を使用するには、外付けHDDやUSBメモリー等のUSBストレージデバイスを無線LANルーターのUSBポートに接続する必要があります。本製品がサポートするUSB ストレージデバイスのフォーマットタイプや容量については、次のWeb サイトでご確認ください。(http://event.asus.com/networks/disksupport)

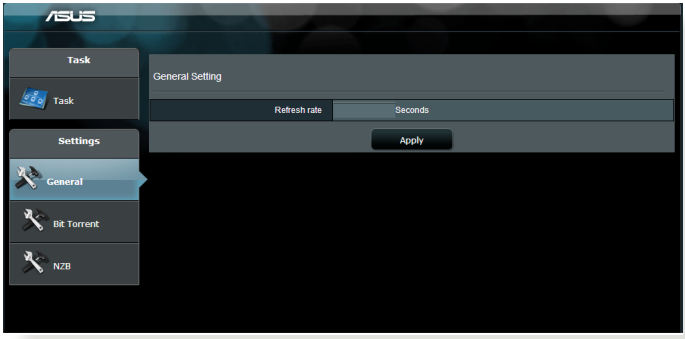
Download Master を使用する

1. 「**USBアプリケーション**」を選択し、「**Download Master**」のInstall をクリックします。接続されているUSBストレージドライブを選択するとDownload Masterユーティリティがインストールされます。
2. Download Master ユーティリティのインストール後は、USBアプリケーションの「**Download Master**」アイコンをクリックすることで起動することができます。
3. 「**追加**」ボタンをクリックしダウンロードタスクを追加します。



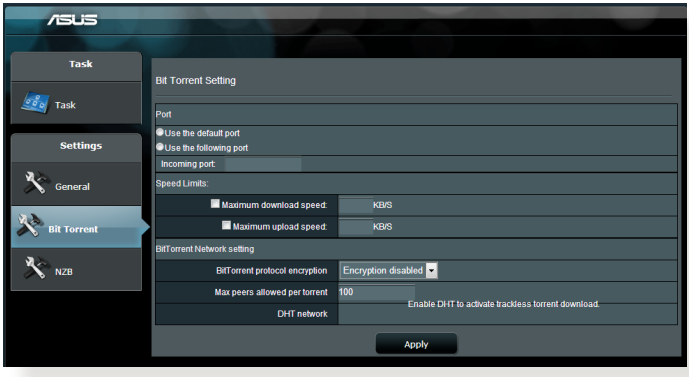
4. 「**ファイルを選択**」をクリックして、「.torrent」ファイル、または「.nzb」ファイルを選択しアップロードします。FTP、HTTP、Magnet Link からダウンロードを行う場合は、URLをコピーし下部入力欄に貼り付けます。

5. 各種設定の変更を行なうには、ナビゲーションパネルの設定から設定変更を行います。



4.4.1 BitTorrent設定

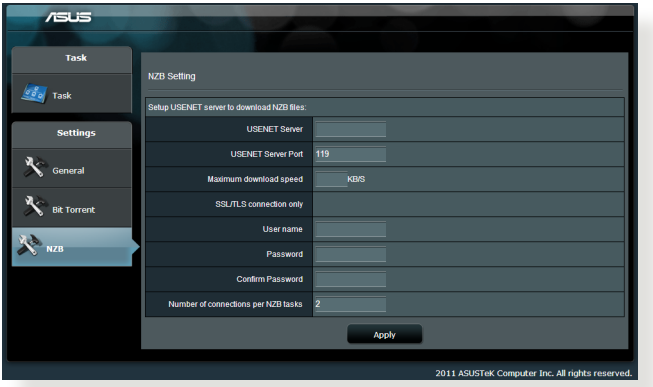
この設定では、BitTorrentを使用したダウンロードとアップロードに使用するポート、最大通信速度、ネットワーク接続設定などを変更することができます。



- **ポート:** 着信接続用ポートを指定することができます。
- **速度制限:** ネットワーク輻輳を回避するために、最大ダウンロード速度と最大アップロード速度を指定することができます。
- **ネットワーク設定:** 安全でスムーズなダウンロードを行うために、プロトコル暗号化、Torrent毎の最大ピア数、最大接続数、DHTネットワーク、PEXネットワークの設定を変更することができます。

4.4.2 NZB設定

NZBファイルを介してUsenetサーバーからファイルをダウンロードを行うには、Usenetの接続設定をする必要があります。



5 トラブルシューティング

本製品の使用中に問題が発生した場合は、まずトラブルシューティングをご覧ください。ここに記載されているトラブルシューティングを行っても問題を解決できない場合は、コールセンターに電話またはメールでお問い合わせください。

5.1 基本的なトラブルシューティング

ルーターに関する基本的なトラブルシューティングです。

ファームウェアを最新バージョンに更新します。

1. 管理画面で「**管理**」をクリックし、「**ファームウェア更新**」タブを選択します。ファームウェアバージョンの「**チェック**」ボタンをクリックし、利用可能なファームウェアをチェックします。
2. または、ASUSオフィシャルサイトから最新のファームウェアをダウンロードします。
   https://www.asus.com/jp/networking-iot-servers/wifi-routers/asus-gaming-routers/tuf-gaming-ax4200/helpdesk_download/
3. 「**ファームウェア手動更新**」の「**アプロード**」ボタンをクリックし、コンピューターに保存したファームウェアファイルを指定します。
4. 「**アップロード**」をクリックし、ファームウェアの更新を開始します。

ネットワークを再起動します。

1. 本製品 (ルーター) 、モデム/回線終端装置、コンピューターの電源を切ります。
2. 本製品とモデム/回線終端装置からすべてのケーブルを取り外します。
3. しばらく待ち、本製品の電源アダプターをコンセントに接続します。
4. 本製品の電源を入れ、2分程度待機します。
5. 本製品とコンピューターをネットワークケーブルで接続します。
6. 本製品とモデム/回線終端装置をネットワークケーブルで接続します。
7. モデム/回線終端装置の電源アダプターをコンセントに接続します。
8. モデム/回線終端装置の電源を入れ、2分程度待機します。
9. コンピューターの電源を入れ、ネットワークの接続状態を確認します。

ネットワークケーブルが正しく接続されていることを確認します。

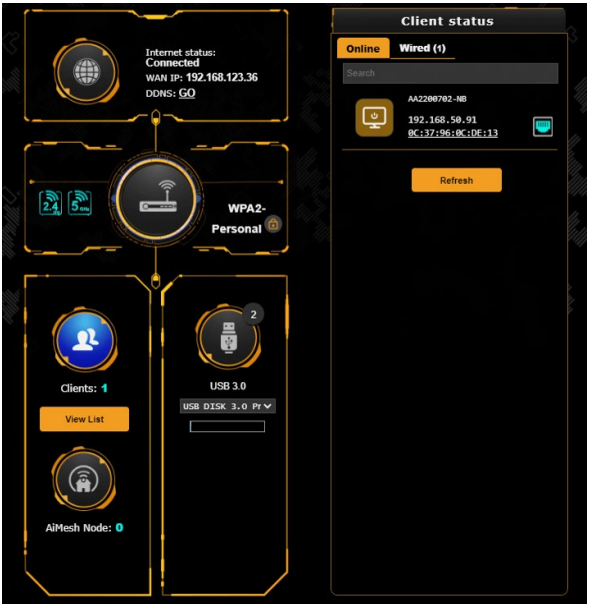
- 本製品とモデム/回線終端装置が正しく接続されている場合、本製品のWAN LEDが点灯します。
- 本製品とコンピューターが正しく接続されている場合、コンピューターの電源が入っている状態で本製品のLAN LEDが点灯します。

お使いのコンピューターのワイヤレスネットワーク接続設定が正しいことを確認します。

- コンピューターをワイヤレスネットワークで接続する場合は、ネットワーク名(SSID)、認証方式、ネットワークキー、通信チャンネルなどが正しく設定されていることを確認します。

ルーターのネットワーク設定が正しいことを確認します。

- ネットワーク上のクライアントが通信を行なうには、各クライアントすべてに個別のIPアドレスが割り当てられている必要があります。本製品ではDHCPサーバー機能を有しており、この機能を使用することで個別のIPアドレスを自動的に割り当てることが可能です。



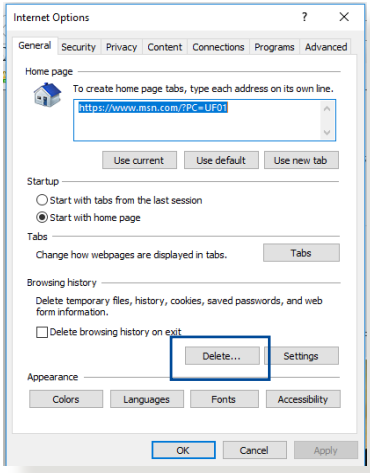
5.2 FAQ (よくある質問)

管理画面 にアクセスすることができません。

- 有線接続の場合は、コンピューターと無線LANルーターにネットワークケーブルが正常に接続されLAN LEDが点灯していることを確認する。
- 管理画面にアクセスする際に使用する、管理者名 (ユーザー名) とパスワードが正しいことを確認する。大文字/小文字の入力を間違わないようご注意ください。
- Web ブラウザーのCookie や一時ファイルを削除する。

例: Internet Explorer

1. メニューバー、またはツールから「**インターネットオプション**」を起動します。
2. 「**全般**」タブの閲覧の履歴にある「**削除**」ボタンをクリックし、「**インターネット一時ファイル**」と「**Cookie**」をチェックして「**削除**」をクリックします。



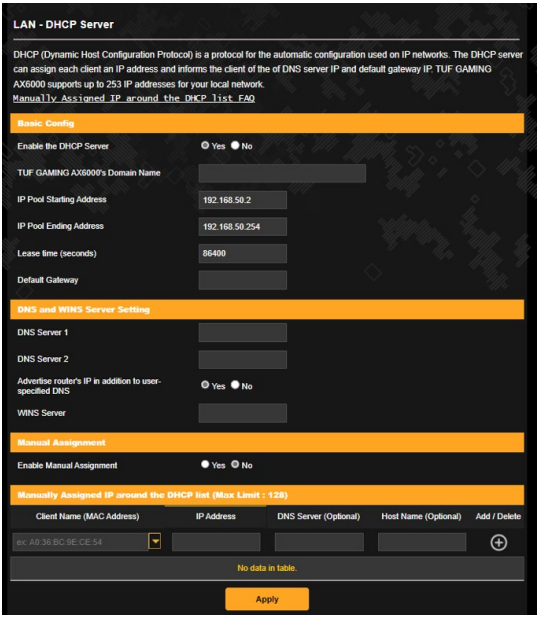
ご注意:

- ご利用のWeb ブラウザーにより操作方法は異なります。
- プロキシサーバーの無効、ダイヤルアップ接続の無効、IPアドレス自動取得の有効を確認します。詳細については本マニュアルに記載の「**セットアップを行う前に**」をご覧ください。
- カテゴリー5e (CAT5e) または6 (CAT6) のネットワークケーブルをご使用ください。

無線LANルーターとコンピューターのワイヤレス接続が確立できません。

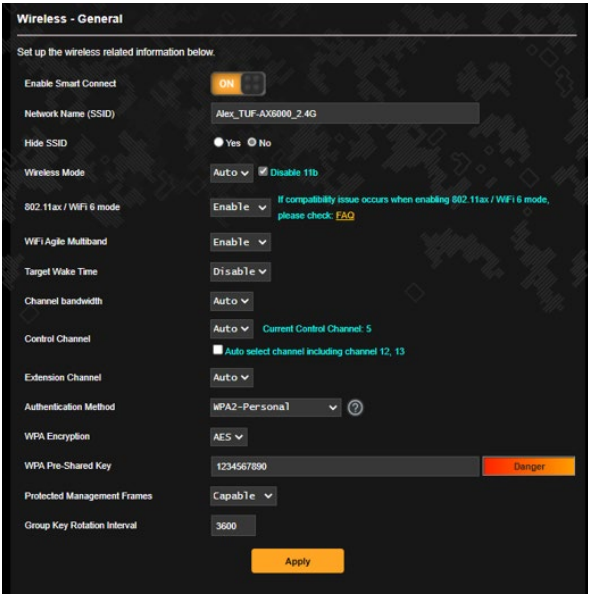
ご注意: 5GHz帯ネットワークに接続できない場合は、ワイヤレスデバイスが5GHzに対応していること、またはデュアルバンド対応であることをご確認ください。

- **電波の有効範囲外:**
  - 無線LANルーターとコンピューターの距離を近づける。
  - 無線チャンネルを変更する。
  - 無線LANルーターのアンテナの角度を調整する。
- **DHCPサーバーを有効にする:**
  1. 管理画面で「**ネットワークマップ**」をクリックし、クライアントに該当のコンピューターが表示されていることを確認します。
  2. クライアント一覧にコンピューターが表示されていない場合は、「**LAN**」をクリックし、「**DHCPサーバー**」タブで「**DHCPサーバーを有効にする**」の「**はい**」をチェックしまます。



- **SSIDの非表示設定を解除する:**

  管理画面で「**ワイヤレス**」をクリックし、「**SSIDを非表示**」の「**いいえ**」をチェックします。次に、「**チャンネル**」を「**自動**」に設定します。

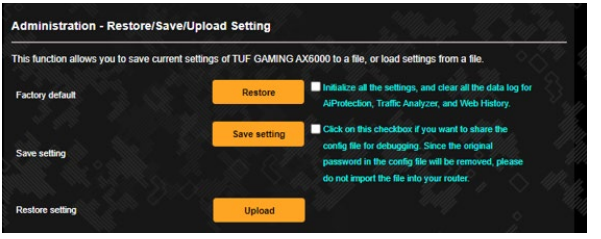


- **通信チャンネルを確認する:**

  無線LANアダプターをお使いの場合、現在設定しているチャンネルがご使用の地域で利用可能であることを確認します。許可されていない通信チャンネルに設定されている場合、ネットワークを構築することができません。

- **システムを工場出荷時の状態に戻す:**

  無線LANルーターの設定を工場出荷時の状態に戻し、再度ネットワークの設定を行います。システムを工場出荷時の状態に戻すには、管理画面で「**管理**」をクリックし、「**リセット/保存/復元**」タブを選択します。「**工場出荷時の状態にリセット**」の「**リストア**」をクリックします。



インターネットに接続できません。

- **ルーターがプロバイダーに接続可能でことを確認する:** 管理画面で「**ネットワークマップ**」をクリックしインターネットの接続状態が「**接続済み**」と表示され、「**WAN IP**」が割り当てられていることを確認します。

- **ネットワークを再起動する:**

  ルーターがWAN IPを取得していない場合は、「**6.1 基本的なトラブルシューティング**」の「**ネットワークを再起動する**」を参考にネットワークの再起動を実施します。

- **ペアレンタルコントロールが設定されている:**

  ご使用のコンピューターがペアレンタルコントロールによる利用制限に登録されている場合、ペアレンタルコントロールで指定されている時間インターネットを使用することはできません。設定状況は、管理画面の「**ペアレンタルコントロール**」で確認することができます。

- **コンピューターを再起動する:**

  コンピューターを一旦再起動し、「**IPアドレス**」と「**デフォルトゲートウェイ**」が正常な値であることを確認します。

- **本機とモデム/回線終端装置を確認する:**

  本機およびモデム/回線終端装置のLEDインジケーターが正常に点灯・点滅していることを確認します。本機のWAN LEDが消灯している場合、ネットワークケーブルが正しく接続されていないか、または破損しています。

ネットワーク名またはネットワークキーを忘れました。

- **ネットワーク名とネットワークキーを再設定する:**

  管理画面の「**ネットワークマップ**」、または「**ワイヤレス**」をクリックし、ネットワーク名 (SSID) とネットワークキーを再度設定します。

- **システムを工場出荷時の状態に戻す:**

  無線LANルーターの設定を工場出荷時の状態に戻し、再度ネットワークの設定を行います。システムを工場出荷時の状態に戻すには、管理画面で「**管理**」をクリックし、「**リセット/保存/復元**」タブを選択します。「**工場出荷時の状態にリセット**」の「**リストア**」をクリックします。

システムを工場出荷時の状態に戻す方法を教えてください。

- **管理画面からシステムを工場出荷時の状態に戻す:**

  管理画面で「**管理**」をクリックし、「**リセット/保存/復元**」タブを選択します。「**工場出荷時状態にリセット**」の「**リストア**」をクリックします。

  工場出荷時のデフォルト設定は以下のとおりです。

ユーザー名:	admin
パスワード:	admin、又は製品底面のラベルに記載されています。
DHCP:	有効（WANポート接続時）
IPアドレス:	http://www.asusrouter.com(または192.168.50.1)
ドメイン名:	（空白）
サブネットマスク:	255.255.255.0
DNSサーバー1:	192.168.50.1
DNSサーバー2:	（空白）
SSID :	ASUS_XX
Wi-Fiパスワード:	任意のパスワードを設定する、又は製品底面のラベルに記載されています。

ファームウェアを更新できません。

- **レスキューモードでファームウェアを修復する:**

  Firemware Restorationユーティリティを使用して指定したファームウェアファイルからファームウェアを復旧します。詳細については、「**5.2 Firmware Restoration（ファームウェアの復元）**」をご覧ください。

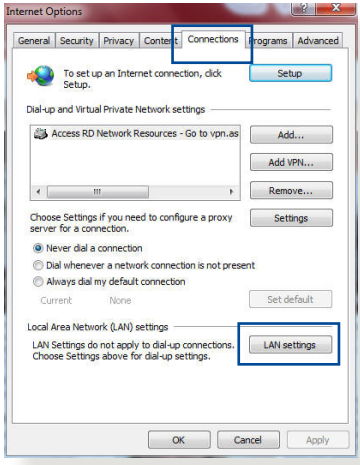
管理画面にアクセスできません。

本製品のセットアップを行う前に、お使いのコンピューターが次の環境であることをご確認ください。

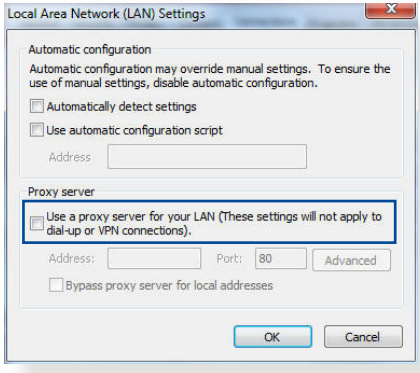
A. プロキシサーバー設定を無効にする

Windows®

1. Internet Explorerを開くには、「**スタート**」ボタンをクリックし、検索ボックスに「**Internet Explorer**」と入力して、結果の一覧の「**Internet Explorer**」 をクリックします。
2. 「**ツール**」ボタン→「**インターネットオプション**」→「**接続**」タブ→「**LANの設定**」の順にクリックします。

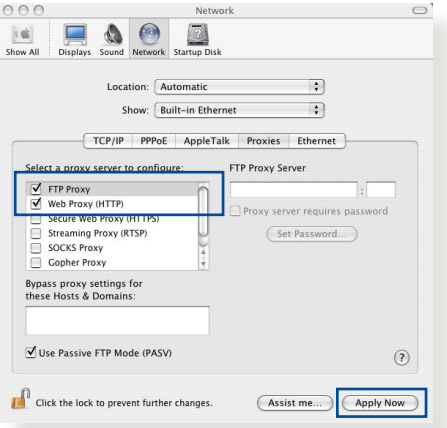


3. 「**LANにプロキシサーバーを使用する**」チェックボックスをオフにします。
4. 変更が終了したら、「**OK**」をクリックして Internet Explorerに戻ります。



MAC OS

1. Safari を起動し、「**Safari**」→「**環境設定**」→「**詳細**」タブ→プロキシ項目「**設定を変更**」の順にクリックします。
2. 「**設定するプロキシサーバーを選択**」で「**FTP プロキシ**」と「**Web プロキシ**」のチェックボックスをオフにします。
3. 変更が終了したら、「**今すぐ適用**」をクリックして設定を適用します。



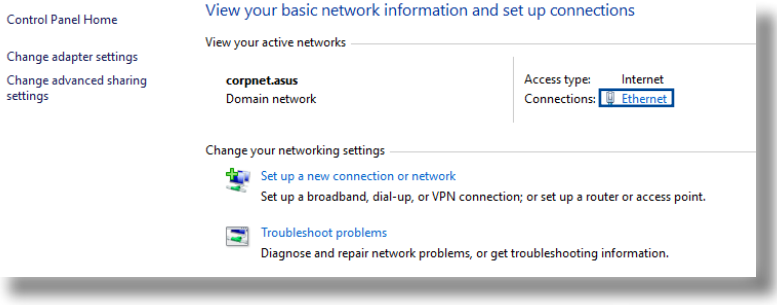
ご注意: 設定方法についてはブラウザーのヘルプも併せてご覧ください。

B. IPアドレスの自動取得を設定する

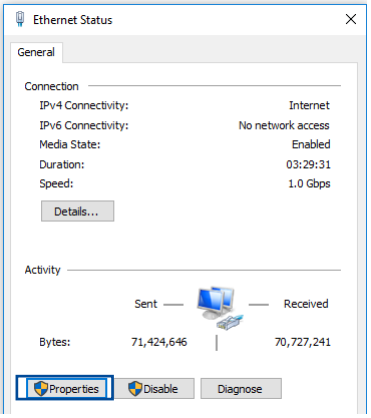
Windows®

1. ネットワーク接続を開くには、**「スタート」**ボタン→**「コントロールパネル」**の順にクリックします。ネットワークと共有センターの**「ネットワーク接続の表示」**をクリックします。

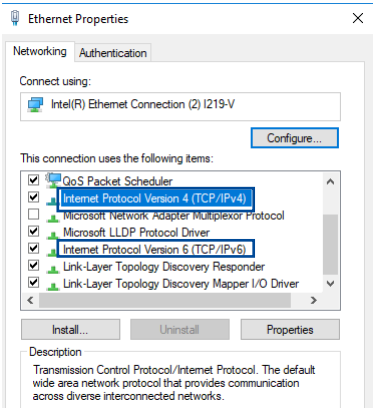
   次に、network connection（ネットワーク接続）をクリックして、ステータスウィンドウを表示します。



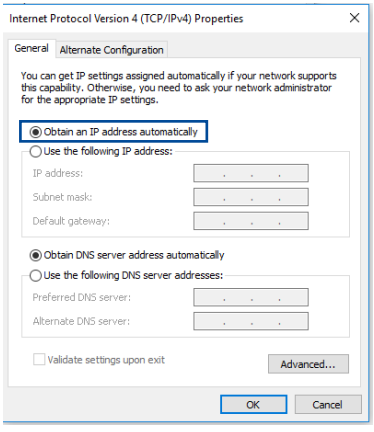
2. **Properties (プロパティ)** をクリックして、Ethernet Properties (イーサネットのプロパティ) 画面を表示します。



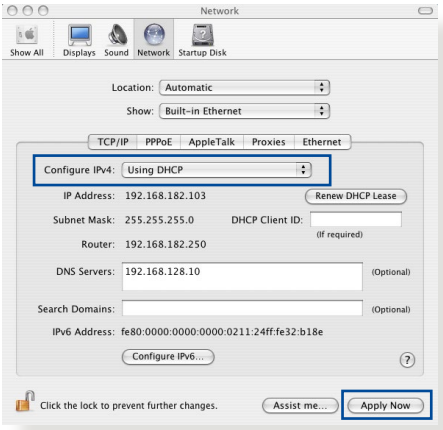
3. 「**ネットワーク**」タブをクリックします。「**この接続は次の項目を使用します**」で「**インターネット プロトコル バージョン 4 (TCP/IPv4)**」または「**インターネット プロトコル バージョン 6 (TCP/IPv6)**」のどちらかをクリックし、「**プロパティ**」をクリックします。



4. DHCP を使用してIP 設定を自動的に取得するには、「**IPアドレスを自動的に取得する**」をクリックします。
5. 変更が終了したら、「**OK**」をクリックして設定を適用します。



MAC OS

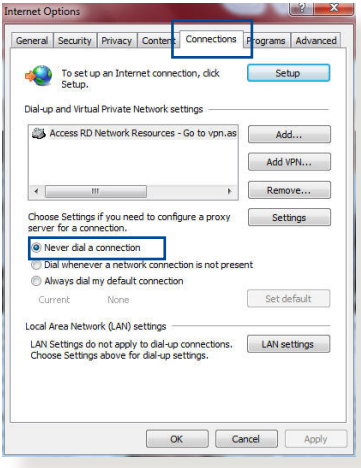


1. をクリックし、アップルメニューを開きます。
2. 「**システム環境設定**」を選択し、インターネットとネットワークの「**ネットワーク**」をクリックします。
3. 現在使用しているネットワークを選択し、「**設定**」をクリックします。
4. 「**TCP/IP**」タブをクリックし、「**IPv4 の設定**」ドロップダウンリストで「**DHCP サーバを参照**」を選択します。
5. 変更が終了したら、「**今すぐ適用**」をクリックして設定を適用します。

ご注意: TCP/IP の設定に関しては、オペレーティングシステムのヘルプファイルも併せてご覧ください。

C. ダイヤルアップ接続を無効する

Windows®



1. Internet Explorerを開くには、「**スタート**」ボタンをクリックし、検索ボックスに「**Internet Explorer**」と入力して、結果の一覧の「**Internet Explorer**」をクリックします。
2. 「**ツール**」ボタン→「**インターネットオプション**」→「**接続**」タブの順にクリックします。
3. 「**ダイヤルしない**」をクリックします。
4. 変更が終了したら、「**OK**」をクリックして Internet Explorer に戻ります。

ご注意: 自動ダイヤルアップ接続の設定方法についてはブラウザーのヘルプも併せてご覧ください。

付録

GNU General Public License

Licensing information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please see The GNU General Public License for the exact terms and conditions of this license. All future firmware updates will also be accompanied with their respective source code. Please visit our web site for updated information. Note that we do not offer direct support for the distribution.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

Terms & conditions for copying, distribution, & modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License.

Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide

range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission.

    For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12 IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

サービスとサポート

ASUSでは、製品に関する最新のサポート情報をサポートサイトで公開しております。お問い合わせの前に、まずは「サポートサイト」をご覧ください。

https://www.asus.com/jp/support

屋外での使用について

本製品は、5GHz 帯域での通信に対応しています。電波法の定めにより5.2GHz、5.3GHz 帯域の電波は屋外で使用が禁じられています。

法律および規制遵守

本製品は電波法及びこれに基づく命令の定めるところに従い使用してください。日本国外では、その国の法律または規制により、本製品を使用ができないことがあります。このような国では、本製品を運用した結果、罰せられることがありますが、当社は一切責任を負いかねますのでご了承ください。