J16201

USER MANUAL

GT-AC2900

ROG Rapture Dual-band Gaming Router

J16201
改訂版 V2
2020年1月

もくじ

5 ユーティリティ

6 トラブルシューティング

付録

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

- ☑ GT-AC2900 本体
- ☑ AC アダプター
- ☑ スタンド/ ウォールマウント
- ☑ クイックスタートガイド (本書)
- ☑ ワイヤレスアンテナ×3
- ☑ LANケーブル (RJ-45)
- ☑ ドライバー×1

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、緩衝材、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。

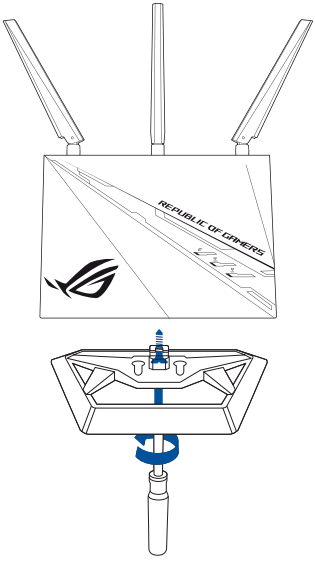
1.3 ルーターを組み立てる

GT-AC2900のスタンドは、壁掛け用のウォールマウントとして、設置用のスタビライザーとして柔軟にご利用いただくことができます。

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。

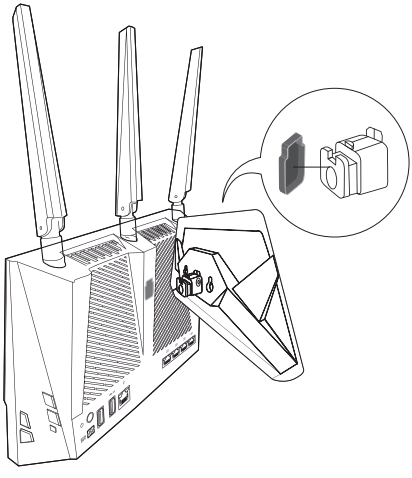
立てる:

スタンドをルーターの下に置き、凸面と凹面を揃えてねじを締めます。

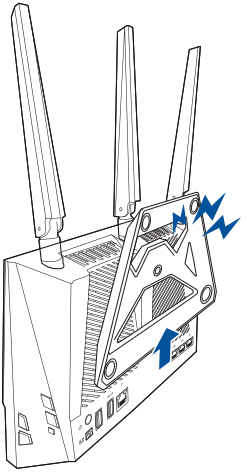


掛ける:

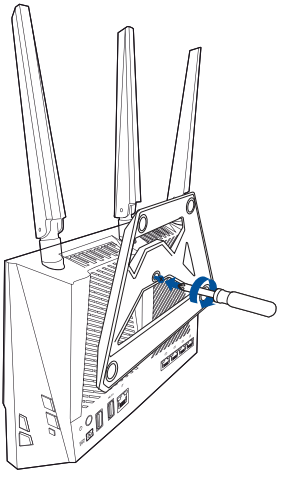
1. スタンドをルーターの後ろに置き、凸面と凹面を揃えます。



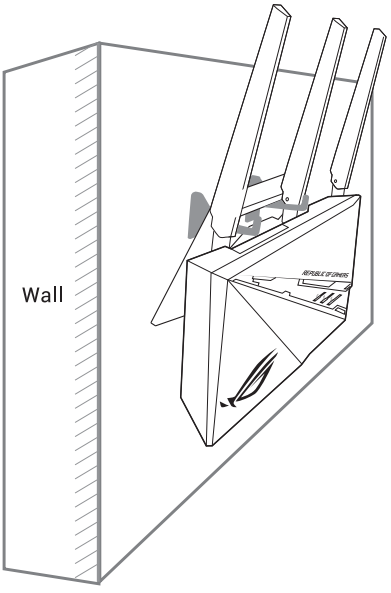
2. カチッという音が聞こえるまでスタンドを押し上げます。



3. ねじを締めます。

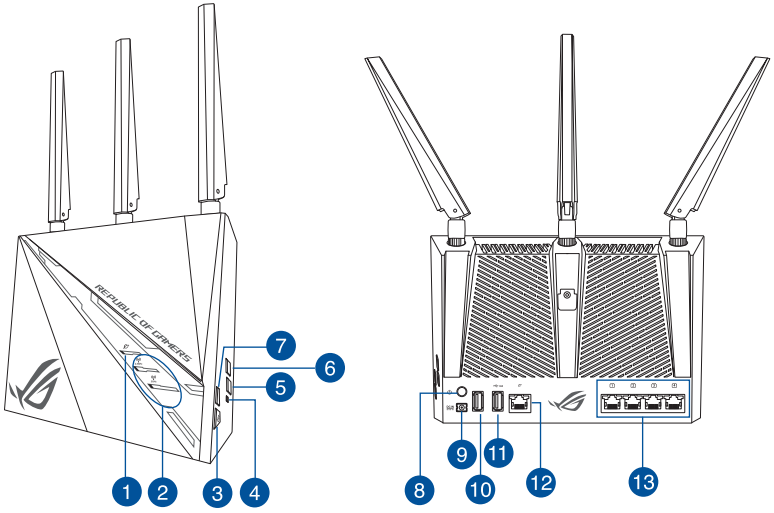


4. フックとねじを使ってルーターを壁に掛けます。



ご参考: フックの耐荷重は2kg以上であること、また、しっかりとネジで固定されていることをご確認ください。フックは同梱されておりません。

1.4 各部の名称



1	**WAN 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。
2	**2.4GHz / 5 GHz Wi-Fi LED** **消灯:** 無線LANを使用していません。 **点灯:** 通信可能な状態です。
3	**ROGブーストボタン** Auraライティングの効果の切り替え、ゲームブースト、DFS チャンネル、GeForce Now QoS をオン/オフにします。
4	**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。
5	**Wi-Fi オン/オフボタン** このボタンを押すと、Wi-Fi 接続のON/OFFができます。
6	**WPSボタン** WPS機能をオンにできます。
7	**LED ボタン** Auraライティングのオン/オフができます。

8	**電源ボタン** 本製品の電源のON/OFFができます。
9	**電源ポート (DC-IN)** 付属の電源アダプターを接続します。
10	**USB 2.0ポート** 外付けHDDやUSBメモリー等のUSB 2.0 対応デバイスを接続します。
11	**USB 3.0ポート** 外付けHDDやUSBメモリー等のUSB 3.0デバイスを接続します。
12	**WAN ポート** モデム/回線終端装置と接続します。
13	**LANポート** 有線デバイスを接続します。

ご注意:

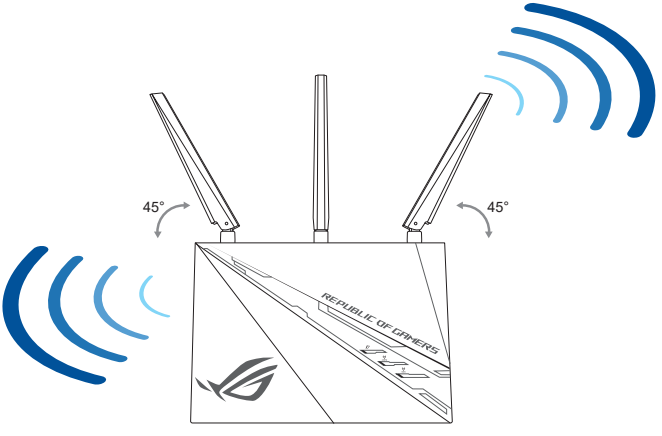
- 電源アダプターは、必ず本製品に付属のものをお使いください。また、本製品に付属の電源アダプターは他の製品に使用しないでください。火災、感電、故障の原因となります。
- ルーターを室内温度で室内に置きます。屋外で使用したり、著しい高温環境では危険につながることがあります。
- **仕様:**

DC電源アダプター	DC出力 +19V、1.75A		
動作温度	0～40℃	保管時	0～70℃
動作湿度	50～90%	保管時	20～90%

1.5　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。
- 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取り付けてください。
- 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。
- 本機は水平に設置してください。



1.6　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-TX / 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ブラザー
  (Internet Explorer、Firefox、Google Chrome、Safari)

ご参考:

- 本製品はIEEE802.11 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、IEEE802.11 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-TX / 100BASE-TX / 10BASE-Tの最大ケーブル長は100m と規定されています。

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。

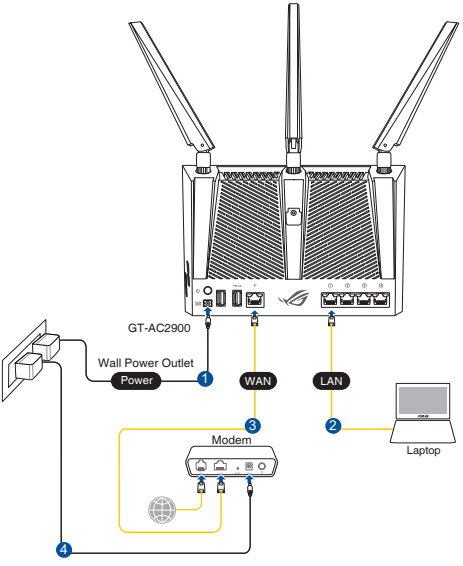
- 既存のルーターと交換を行なう場合は、現在実行されているすべての通信を停止します。
- モデム/回線終端装置とコンピューターに接続されたLANケーブルを取り外します。モデム/回線終端装置がバックアップ用バッテリーを搭載している場合は、バッテリーを一旦取り外します。
- モデム/回線終端装置とコンピューターを再起動します。(推奨)

A. 有線接続

ご参考: 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

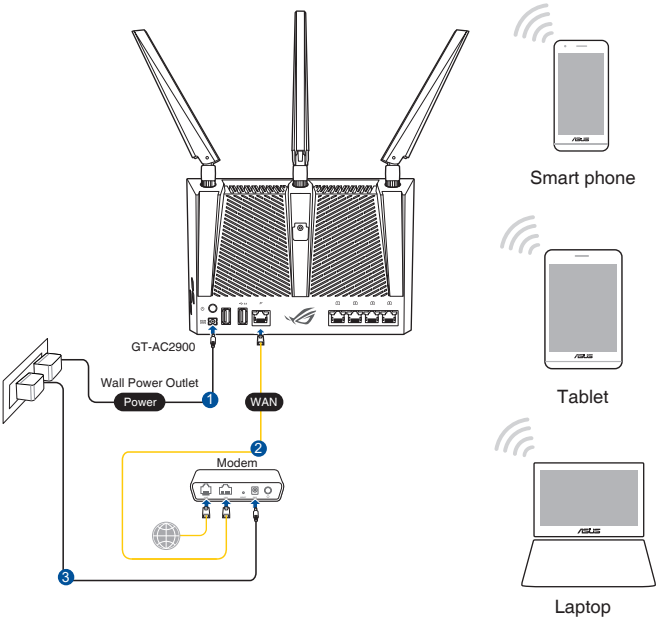
1. 無線LANルーターに電源ケーブルを接続し、電源を入れます。無線LANルーターのLANポートとコンピューターをLANケーブルで接続します。



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。

デフォルトの SSID:	ASUS_XX

* 「**XX**」はMACアドレスの最後の2桁を意味します。ROG 無線LANルーター背面のラベルに記載があります。

ご参考:

- 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。

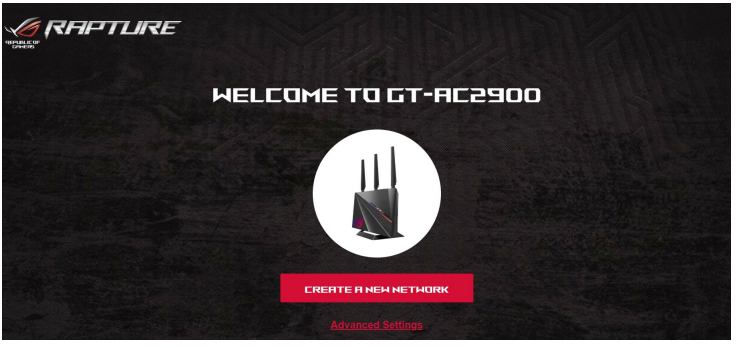
2.2　クイックインターネットセットアップ (QIS)

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://router.asus.com**」または「**http://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接続タイプに関する必要な情報を入力します。ISPの接続タイプがダイナミックIP (動的)、スタティックIP (静的IP)、PPPoE、L2TP、 PPTP 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。

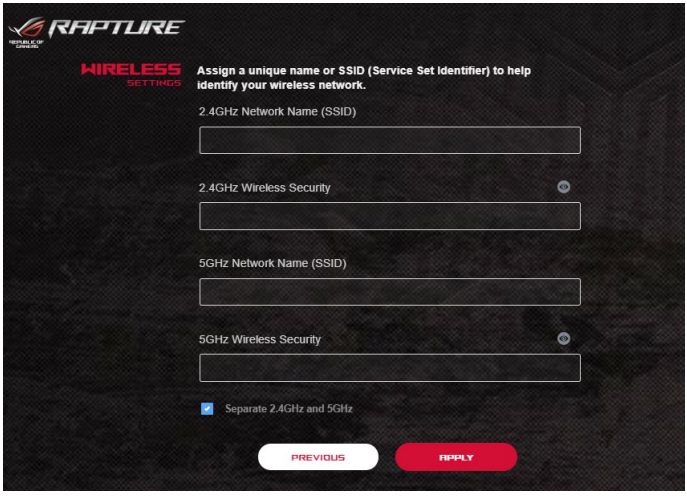
重要: インターネットの接続タイプや接続ユーザー名、接続パスワードなどについては、ご契約のプロバイダーへお問い合わせください。

ご注意:

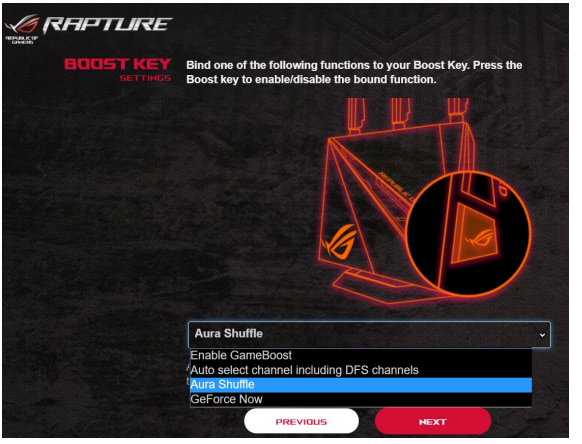
- ISP接続タイプの自動検出は、ルーターを初めて設定したとき、またはルーターがデフォルト設定にリセットされたときに行われます。
- QISでインターネット接続の種類を検出できなかった場合は、「**手動設定**」をクリックし手動で接続設定を行なってください。

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。

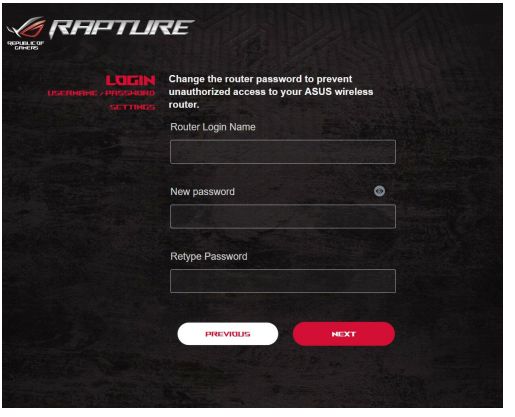
重要: ワイヤレスネットワークを2.4GHzと5GHzに分ける場合は、「2.4GHzと5GHzを個別に設定する」にチェックを入れてください。



4. ブーストキーの希望する機能を選択します。
   - **Aura シャッフル**: ブーストキーを押して Aura ライティング効果を切り替えることができます。
   - 5GHzのDFSチャンネルの使用を有効することでチャンネルの干渉を低減することができます。
   - **GeForce NOW オン/オフ**: GeForce Now ゲーミングデバイスを優先します。
   - **ゲームブースト 有効/無効**: ゲームパケットを優先するゲームブーストの設定ができます。



5. ルーターへの不正アクセスを防ぐため、「**ログイン設定**」画面でルーターのログインパスワードを変更します。



注意: 無線LANルーターのログイン名とパスワードは、2.4GHz/5GHzネットワーク名 (SSID)、セキュリティキーとは異なります。無線LANルーターのログインユーザー名とパスワードは無線LANルーターのWeb GUIにアクセスする際に使用するものです。2.4GHz/5GHzネットワーク名 (SSID) とセキュリティキーは、Wi-Fi デバイスで2.4GHz/5GHzネットワークにログインし接続する際に使用します。

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。

ご参考:

- 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 全般設定

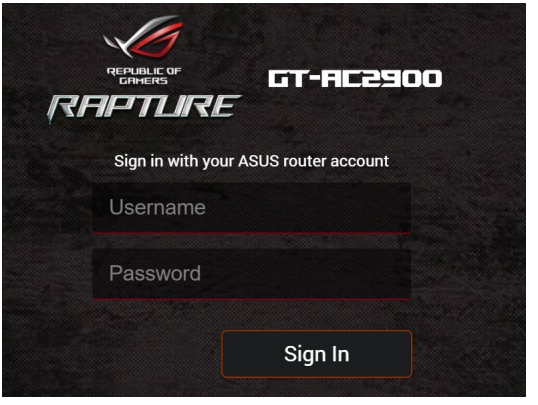
3.1 管理画面にログインする

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://router.asus.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。

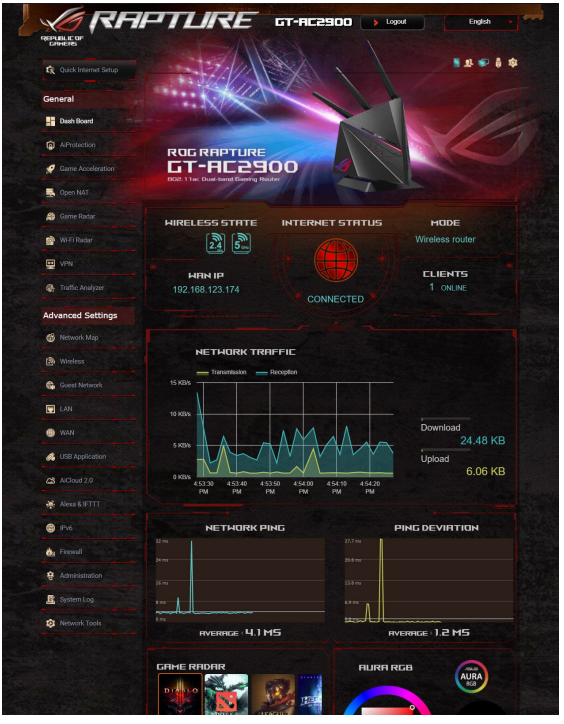


3. ログインに成功すると管理画面が表示されます。

ご参考: 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 Dash Board

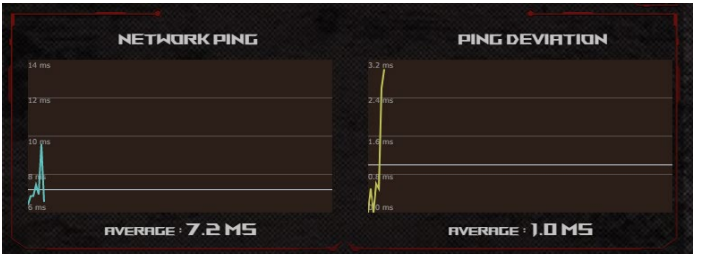
Dash Boardでは、ネットワーク環境のトラフィックをリアルタイムで監視し、またネットワークpingとpingの偏差をリアルタイムで分析することができます。



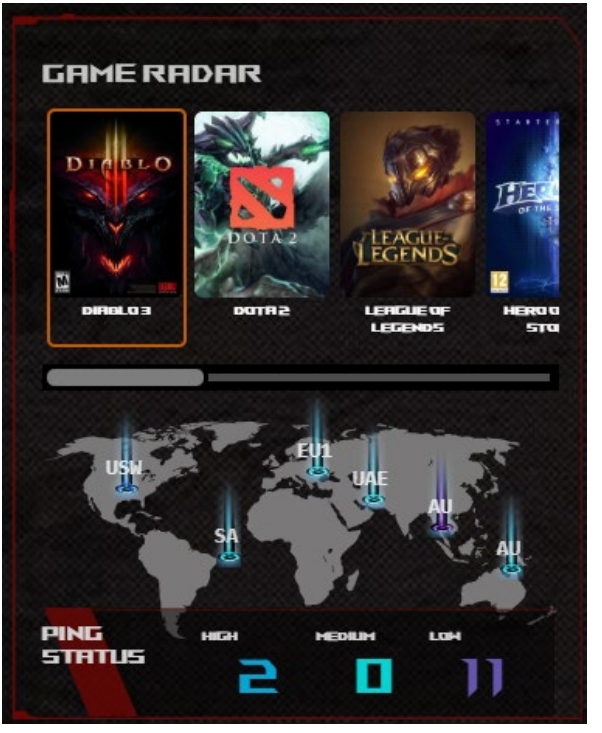
ネットワークpingは、オンラインゲームでの快適度を測ります。

pingが高いほど、リアルタイムゲームでの遅延が大きいことを意味します。多くのオンラインゲームでは、ネットワークpingが99ミリ秒未満であれば、良好であるとされています。ネットワークpingが150ミリ秒未満であれば、許容範囲であると言えます。通常、ネットワークpingが150ミリ秒を超えると、スムーズにゲームを行うことが難しくなります。

Pingの偏差も、オンラインゲームの快適さに大きく関連しています。Pingの偏差が高いと、オンラインゲームをプレイするときにラグが発生しやすくなります。pingの偏差には基準値はありません。ただし、pingの偏差が小さい方が好ましいとされています。



- **Game Radar:** DashboardのGame Radarを使うと、特定のゲームサーバーのpingの応答時間について調べることができます。。



- **Aura RGB:** DashboardからAura RGBを設定する、またはオン/オフにすることができます。お好みの色を設定し、11種類のライティングパターンから1つを選択できます。

- **イベントトリガー**

  イベントトリガーライトモードを選択すると、システムが次のイベントを検出して、LED が異なるライティング効果になるようにトリガーして通知します。

  - **ゲームブースト**

    ゲームブーストをオンにすると、LED が赤色に点滅します。ゲームブーストの詳細については、**3.4 ゲームアクセラレーション**を参照してください。

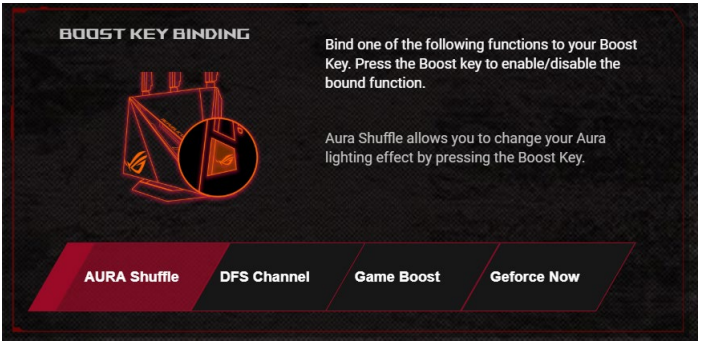
  - **トラフィックメーター**

    レインボー LED がリアルタイムのトラフィックを示します。インターネット速度に従って色の組み合わせが変わります。

- **ログイン失敗**
  ASUSWRT へのログインに失敗すると、LED バー上のコメットが赤色になります。
- **アタックブロック**
  システムが外部からの攻撃対して正常に、LED のコメットが赤色になります。

ご参考: イベントトリガーモードを選択すると、システムは現在検出されているイベントに基づいて異なるライティング効果を示します。この機能を選択すると、ライティング効果は制御できません。

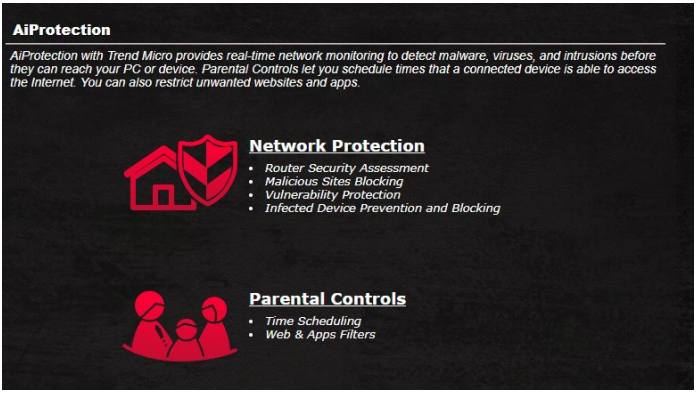
- **ブーストボタン:** ROG Rapture ゲーミングルーターは物理的な製品上のブーストキーに対応します。ユーザーはダッシュボードからブーストキーの機能を定義できます。



- **Aura シャッフル**: ブーストキーを押して Aura ライティング効果を切り替えることができます。
- **DFS チャンネル オン/オフ**: 5GHzのDFSチャンネルの使用を有効することでチャンネルの干渉を低減することができます。
- **GeForce NOW オン/オフ**: GeForce Now ゲーミングデバイスを優先します。
- **ゲームブースト 有効/無効**: ゲームパケットを優先するゲームブーストの設定ができます。

3.3 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。

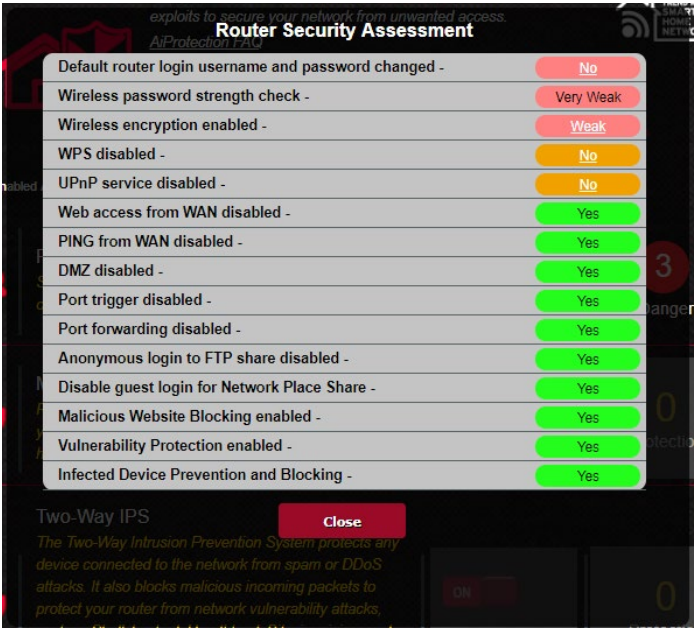


3.3.1 AiProtection の設定

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、「**ネットワーク保護**」をクリックします。
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。



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。

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。

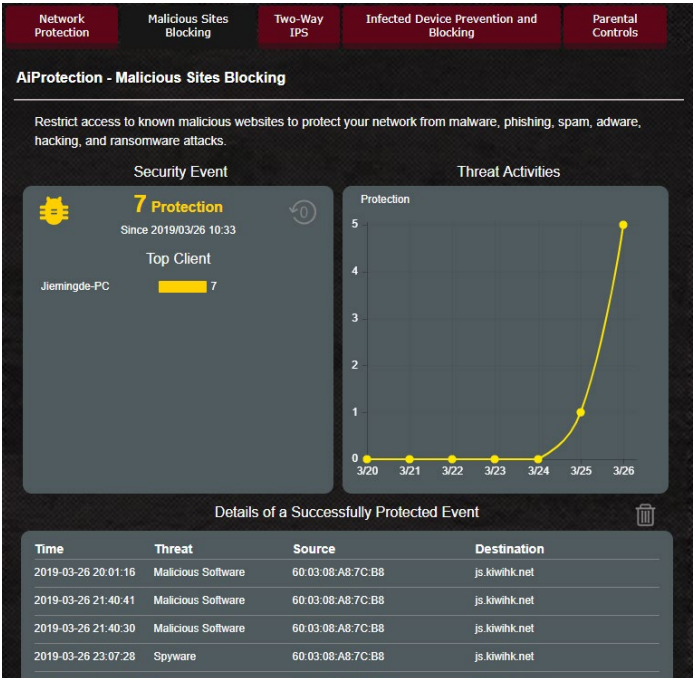
3.3.2 悪質サイトブロック

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:「**ルーターの保護**」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、「**ネットワーク保護**」をクリックします。
3. 「**悪質サイトブロック**」を「ON」にします。



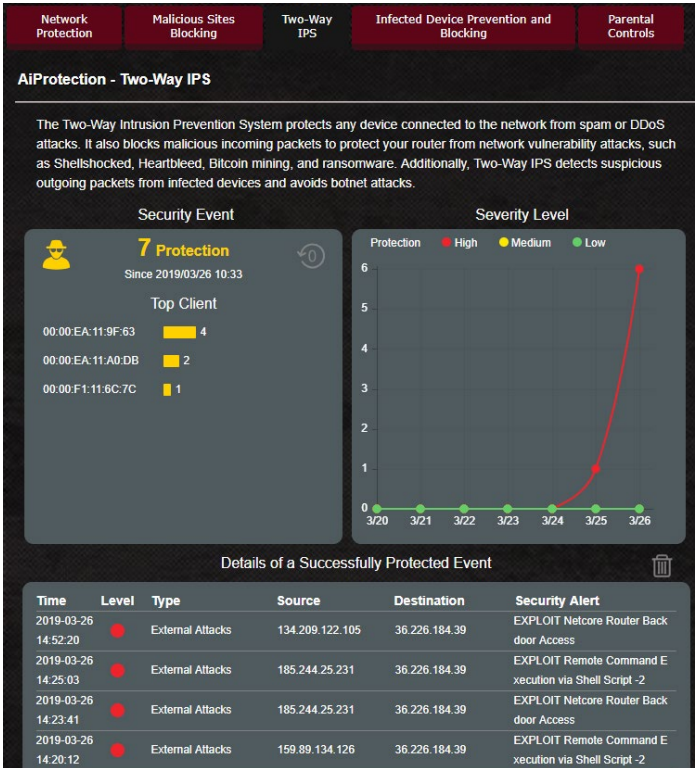
3.3.3 脆弱性保護

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:「**ルーターの保護**」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、「**ネットワーク保護**」をクリックします。
3. 「**脆弱性保護**」の欄を「**ON**」にします。



3.3.4 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。

> **ご参考:** セキュリティスキャンの結果画面で「**ルーターの保護**」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。

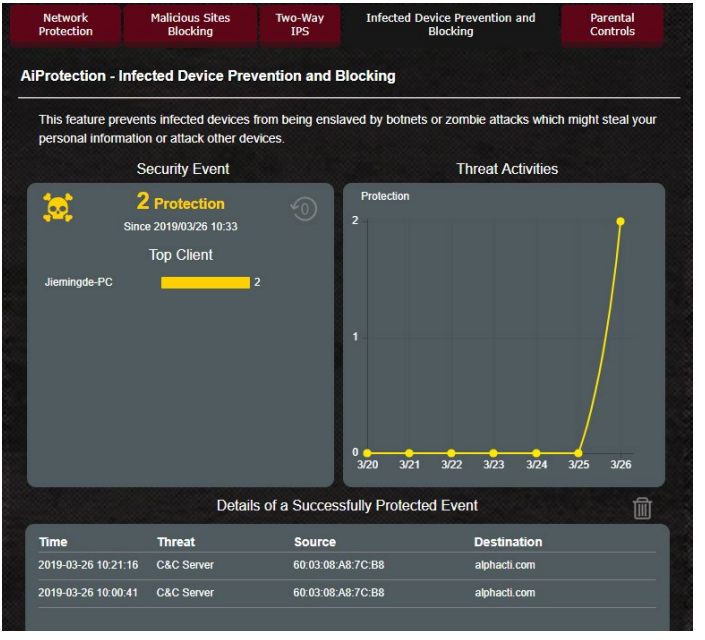
感染デバイス検出/ブロックを有効にする

1. 「**AiProtection**」をクリックします。
2. 「**感染デバイス検出/ブロック**」のスイッチをONにします。

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。

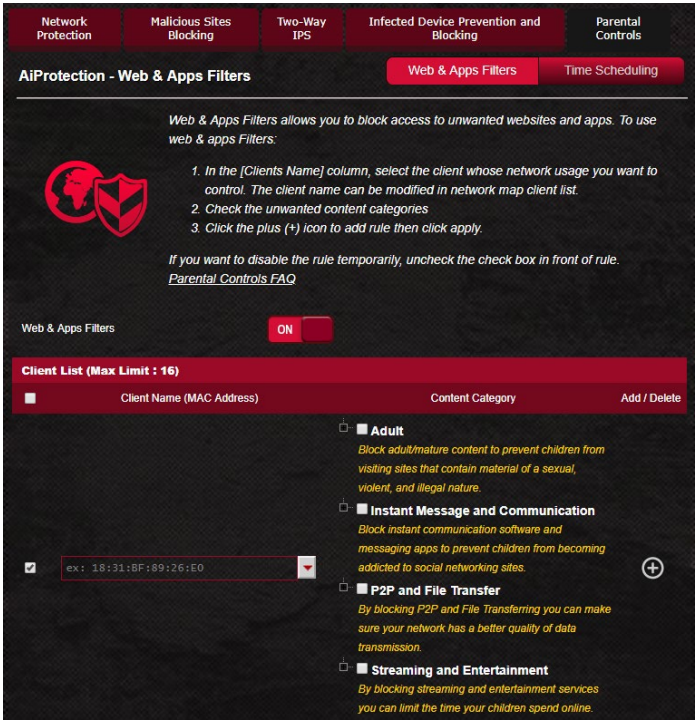
1. 「**感染デバイス検出/ブロック**」の「**アラート設定**」をクリックします。
2. メールサービス、メールアドレス、パスワードを入力し「**適用**」をクリックします。



3.3.5 ペアレンタルコントロールの設定

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。

1. 「**AiProtection**」をクリックします。
2. 「**ペアレンタルコントロール**」をクリックします。



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**」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。

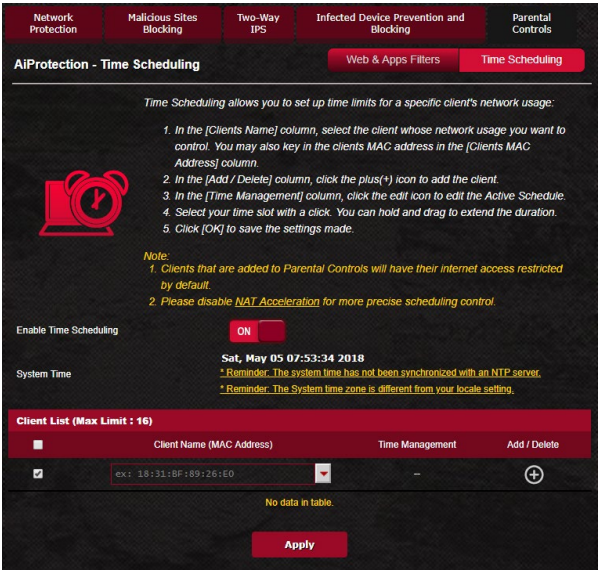
ご注意:

- 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。

タイムスケジュール

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: タイムスケジュール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「**タイムスケジュール**」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。

「**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。

3.4 ゲームアクセラレーション

3.4.1 段階のゲームアクセラレーション

GT-AC2900 は 3 段階のゲームアクセラレーションによってより快適なゲームをお楽しみいただけます。

- **ゲーミングポートを優先化**

  ゲーミングデバイスをゲーミングポート (LAN1) にによってより快適なゲームをお楽しみいただけます。

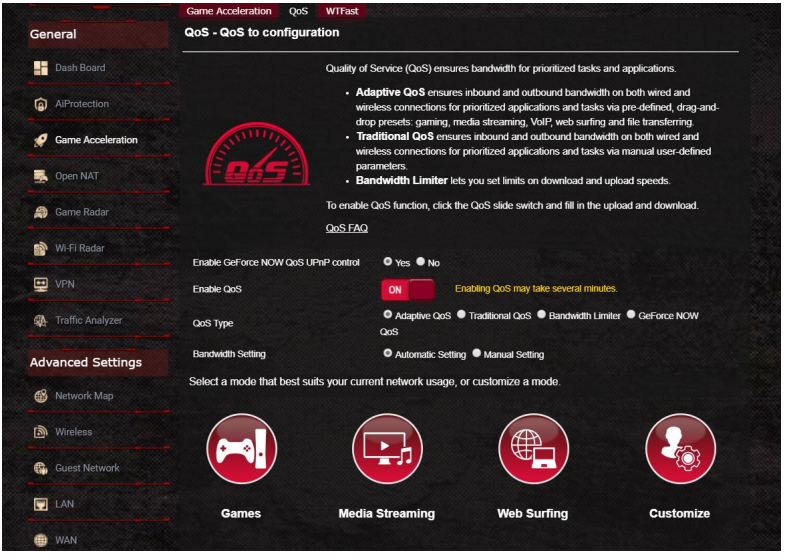
  ROG First は **GameFirst V** 内の ASUS ROG マザーボード用ユーティリティです。ASUS ROG ゲーミングルーターで使用できます。
- **ゲームのパケットを優先化**

  この機能を使用すれば、ワンクリックでゲームブーストを有効にできます。ゲームブーストを有効にすると、ゲーミングパケットを最優先処理し、より快適なゲーミングをお楽しみいただけます。
- **ゲームサーバーアクセラレーション**

  WTFast のゲーマーズプライベートネットワークによって、ゲームの遅延、パケットロスを低減します。詳細情報については、**3.4.3 ゲーマーズプライベートネットワーク**を参照してください。

3.4.2 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. 「**ゲームブースト**」を選択し、画面上部の「**ゲームアクセラレーション**」>「**QoS**」タブをクリックします。
2. 「**QoS 機能を有効**」のスイッチをクリックしONにします。
3. アップロードおよびダウンロードの帯域幅を入力します。

   ご参考: 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)

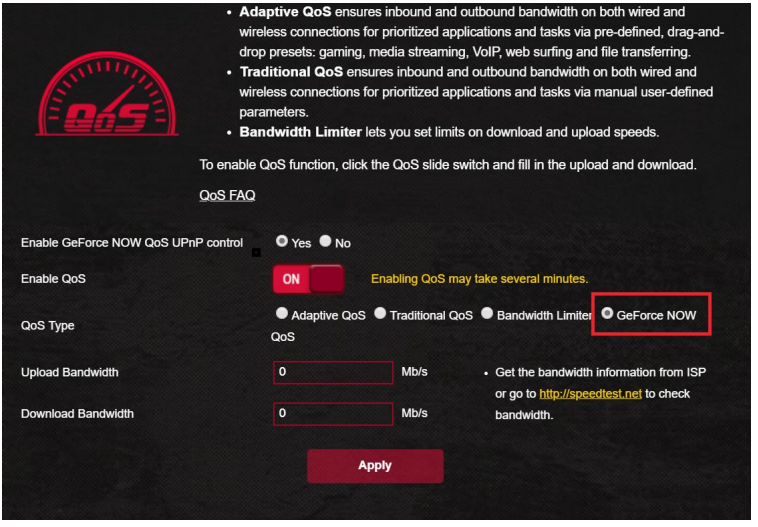
4. QoS Type (Ataptive / Traditional / 帯域リミッター) を選択します。
5. 「**適用**」をクリックします。
6. 画面の指示に従って、QoSの設定を完了します。

GeForce NOW QoS

GeForce NOW QoS モードは、NVIDIA クラウドゲーミングサービス向けの独自の QoS モードです。GeForce NOW QoS モードを有効にすると、ルーターは、Nvidia が定義する GeForce NOW 対応デバイス向けの必要な帯域幅、ワイヤレスモード、 QoS 優先度を確保します。

GeForce NOW QoS を有効にする:

1. **Game Acceleration（ゲームアクセラレーション）** > **QoS** と進み、Enable QoS（Qos を有効にする）ボタンにチェックを入れて、QoS type **GeForce NOW（QoS タイプ GeForce NOW）**を選択します。



2. Geforce NOW QoS を有効にします。

   「**Yes（はい）**」を選択します。

3. 希望するアップロード/ダウンロードの帯域幅を設定します。ISP から帯域幅情報を取得するか、または、オンラインサービスを使用して、帯域幅を確認します。

4. **Apply（適用）**をクリックして設定を保存します。

3.4.3 ゲーマープライベートネットワーク

wtfast は独自に開発されたゲーマー・プライベート・ネットワーク (GPN) を利用します。オンラインゲーム使用時に最適なトラフィックルートを選択することで、パケット損失を改善し、快適なゲーム環境を提供します。

ファームウェアの更新：

1. Webブラウザーを起動し、アドレス欄に次のURLを入力しルーターのログイン名とパスワードを入力してASUSWRT GUIを開きます。 (http://router.asus.com)
2. 「**管理者**」→「**ファームウェア更新**」で「**チェック**」をクリックし、画面の指示に従いファームウェアを更新します。

   手動で更新する場合は、最新のファームウェアを次のURLからダウンロードしてください。
   （http://support.asus.com/ServiceHome.aspx）

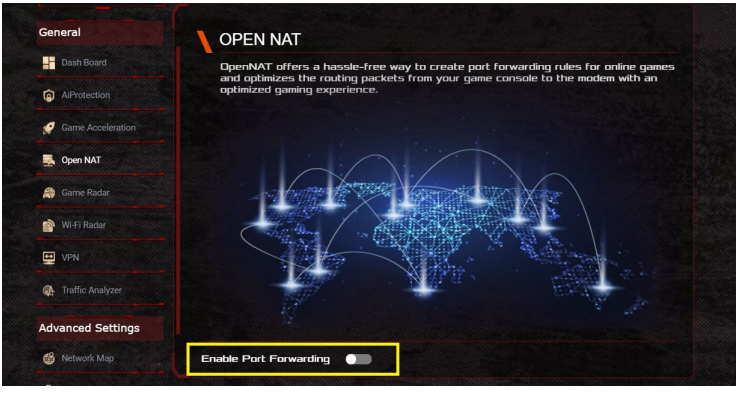
wtfastを使用する

1. Web GUIナビゲーションパネル全般の「**Gamer Private Network**」を開きます。
2. wtfast の無料アカウントを次のURLで作成します。（https://www.wtfast.com/）
3. wtfast アカウントでログインします。
4. ゲームブーストリストから、wtfast GPNを使用するデバイスのプロファイルを作成します。
5. お住まいの地域に応じたGPNサーバーを選択するか、「**Auto**」を選択し、「**適用**」を選択して設定を適用します。
6. ゲームを起動する前にGPNプロファイルを有効にします。

注意: 無料アカウントで対応可能なデバイスは1台です。複数のデバイスで使用する場合は、wtfastのホームページより追加する必要があります。

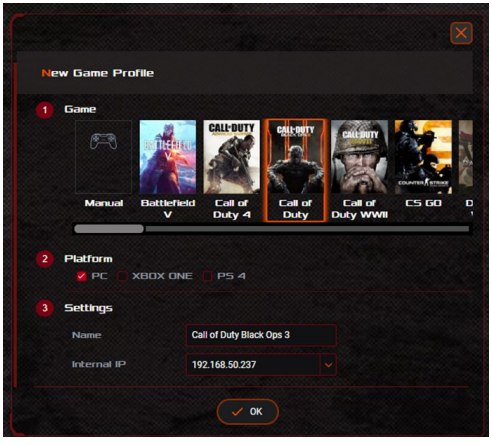
3.5 オープン NAT

PC またはコンソールゲームをプレイする際には、ISP または環境内のルーター設定が理由で、NAT やポートブロックなどの接続の問題が発生することがあります。Open NATでは、事前設定されたゲームプロファイルに応じてポートを開放し、アクセス制限による問題を解決することができます。

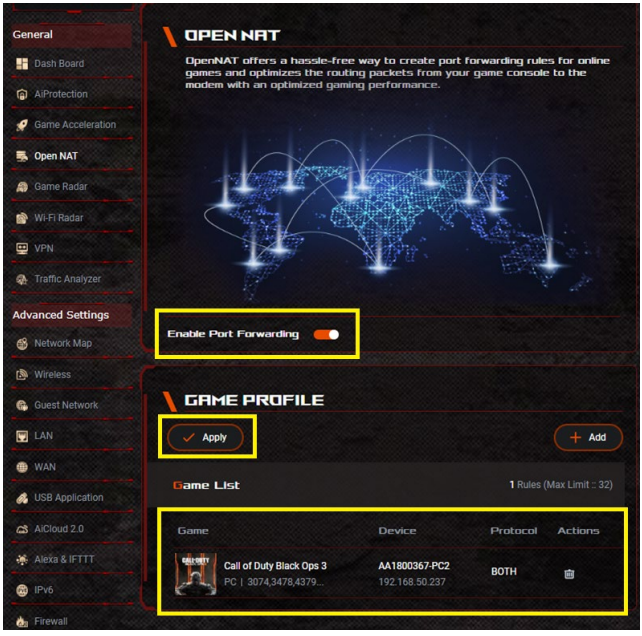


Open NAT (オープン NAT) を使用する:

1. ナビゲーションパネルから、**General (一般)** > **Open NAT (オープン NAT)** の順にアクセスし、**ポートフォワーディングを有効にします**。
2. ゲームリストからゲームを選択します。ゲームリストは随時更新されます。

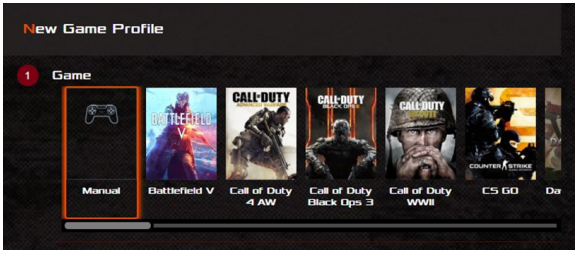


3. 使用したいプラットフォームにチェックを入れます。
4. Internal IP（内部 IP）フィールドにデバイスの IP アドレスを入力します。
5. **OK** をクリックし、次に、**Apply（適用）**をクリックします。



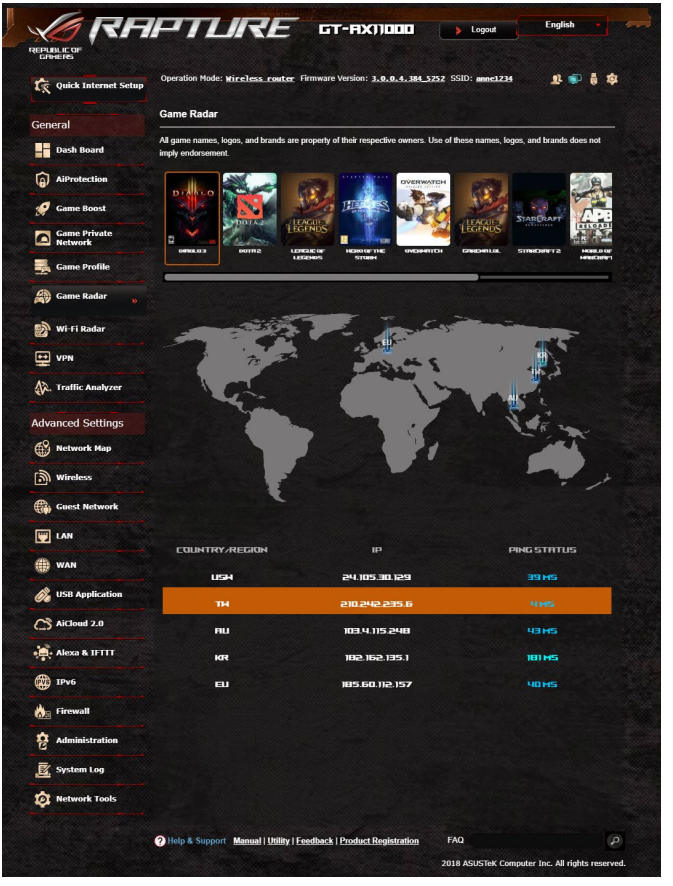
ご参考:

- FTP サーバーまたはその他のデバイス向けのポートフォワーディングルールをセットアップしたい場合は、WAN > Virtual server（仮想サーバー）/Port Forwarding（ポートフォワーディング）の順に進んでください（セクション 4.5.4 を参照してください）。
- プレイしたいゲームがゲームプロファイルに含まれていない場合は、 Add **Manual**（マニュアル）を選択し、ルールを作成します。



3.6 Game Radar

Game Radarは特定のゲームサーバーの接続状況を確認することができます。



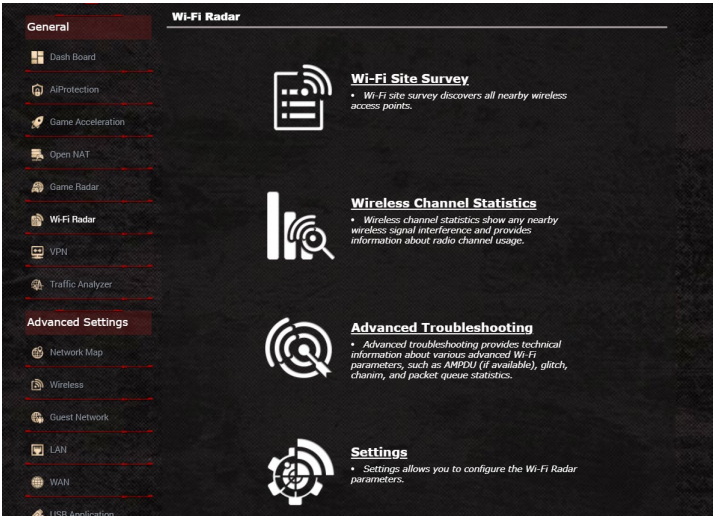
Game Radar を使用する

1. ナビゲーションパネルの「**全般**」→「**Game Radar**」の順に進み、ゲームリストからゲームを選択します。
2. 各サーバーの「**PINGの状態**」をチェックします。
3. pingステータスの低いゲームサーバーを選択すると、スムーズなオンラインゲームをお楽しみいただけます。

3.7 Wi-Fi レーダー

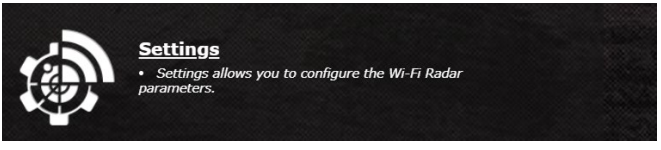
Wi-Fi レーダーは、ワイヤレスのトラブルシューティング時にチャンネル状況やパケットデータを詳細に分析可能なネットワークツールです。

注意: Wi-Fi レーダーを有効にすると、ワイヤレスパフォーマンスが低下する場合があります。必要なときのみ、Wi-Fi レーダーを有効にしてください。

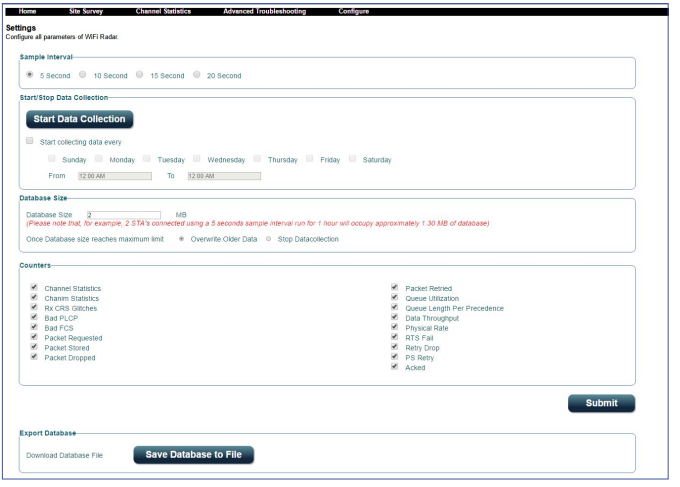


Wi-Fi レーダーを使用する

1. ナビゲーションパネルの「**全般**」→「**Wi-Fi レーダー**」に移動し、Wi-Fi レーダーの設定を行います。



2. 「**Start Data Collection**」をクリックします。
3. 全てのパラメータを設定したら、「**適用**」をクリックします。

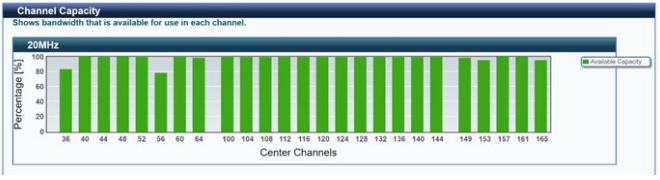


3.7.1 ワイヤレス検出

ワイヤレス検出 (WiFi Site Survey) では、ご使用の環境内のワイヤレスネットワークを検索することができます。

3.7.2 ワイヤレスチャンネル統計

この機能では、ご使用の環境内の全ての帯域のチャンネル使用状況とチャンネルごとの統計を表示します。



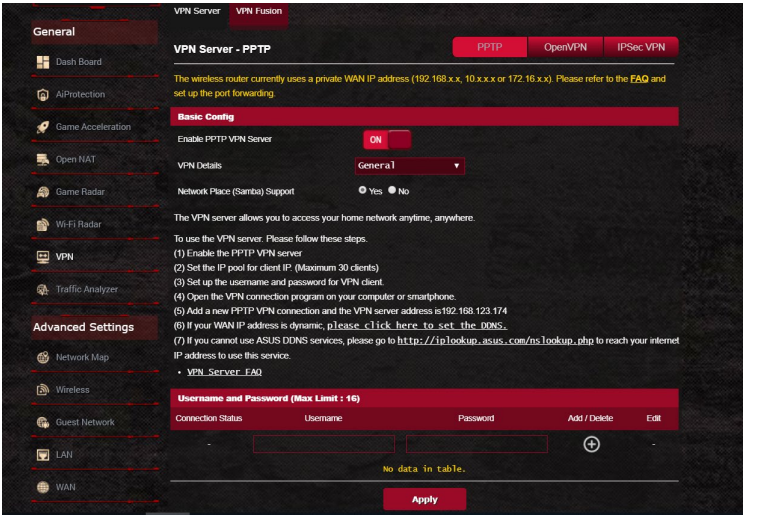
3.7.3 アドバンスドトラブルシューティング

この機能では、ご使用環境でのWi-Fi障害の統計情報を表示します。

3.8 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。

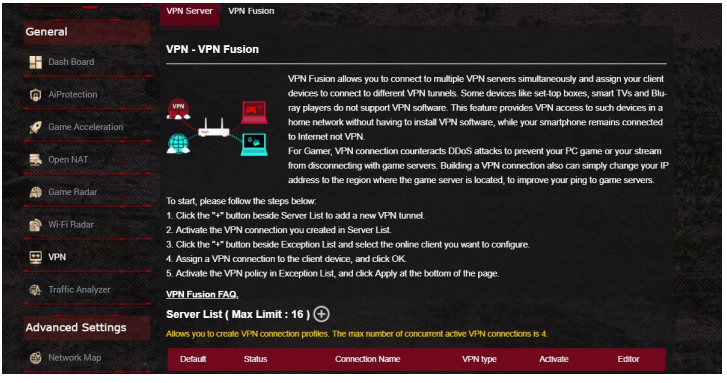


VPNサーバーのセットアップ

1. 「**VPN**」をクリックし、「**VPNサーバー**」タブを選択します。
2. 「**PPTP VPNサーバーを有効にしますか**」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。

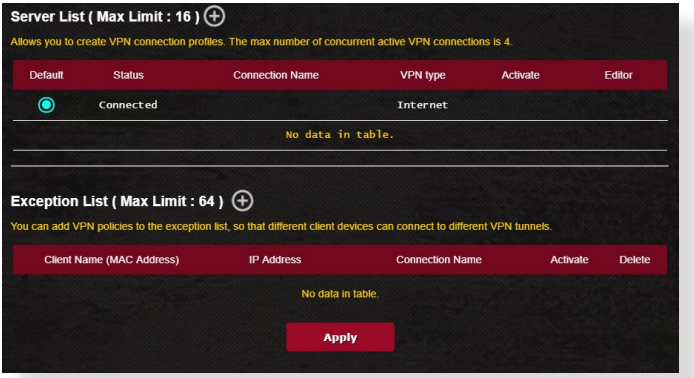
3.8.1 VPNフュージョン

VPNフュージョンを使用すると、複数のVPNサーバーに同時に接続し、クライアントデバイスを異なるVPNトンネルに接続するように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プレーヤーなどの一部のデバイスでは、VPNソフトウェアをサポートしていない場合があります。この機能は、スマートフォンをVPNではなくインターネットに接続したまま、VPNソフトウェアをインストールすることなく、ホームネットワーク内のデバイスへのVPNアクセスを可能にします。VPN接続はDDoS攻撃を防ぎ、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のを防ぎます。VPN接続を構築することでIPアドレスをゲームサーバーが配置されている地域に変更することができるため、ゲームサーバーへのpingを向上させることが可能です。



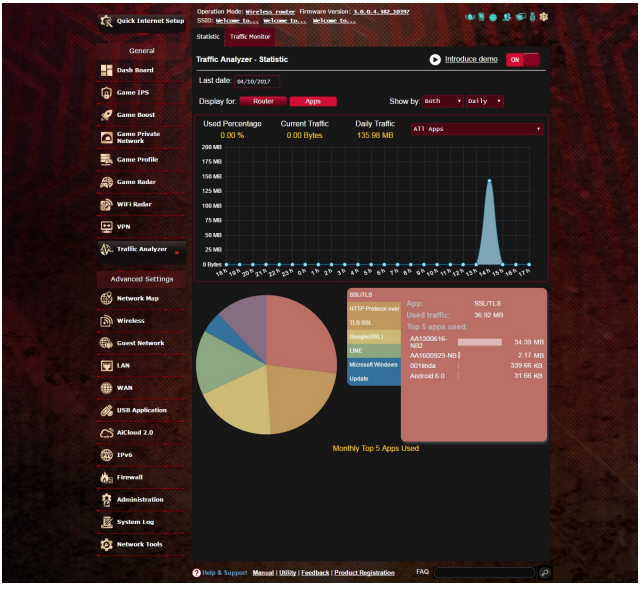
次の手順で設定を行ないます。

1. サーバーリストの横にある「+」ボタンをクリックして、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接続を有効にします。
3. 例外リストの横にある「+」ボタンをクリックし、設定するオンラインクライアントを選択します。
4. VPN接続をクライアントデバイスに割り当て、「OK」をクリックします。
5. 例外リストのVPNポリシーを有効にして、ページの下部にある「適用」をクリックします。


Server List (Max Limit : 16)
Allows you to create VPN connection profiles. The max number of concurrent active VPN connections is 4.
Default
Status
Connection Name
VPN type
Activate
Editor
Connected
Internet
No data in table.
Exception List (Max Limit : 64)
You can add VPN policies to the exception list, so that different client devices can connect to different VPN tunnels.
Client Name (MAC Address)
IP Address
Connection Name
Activate
Delete
No data in table.
Apply

3.9 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。



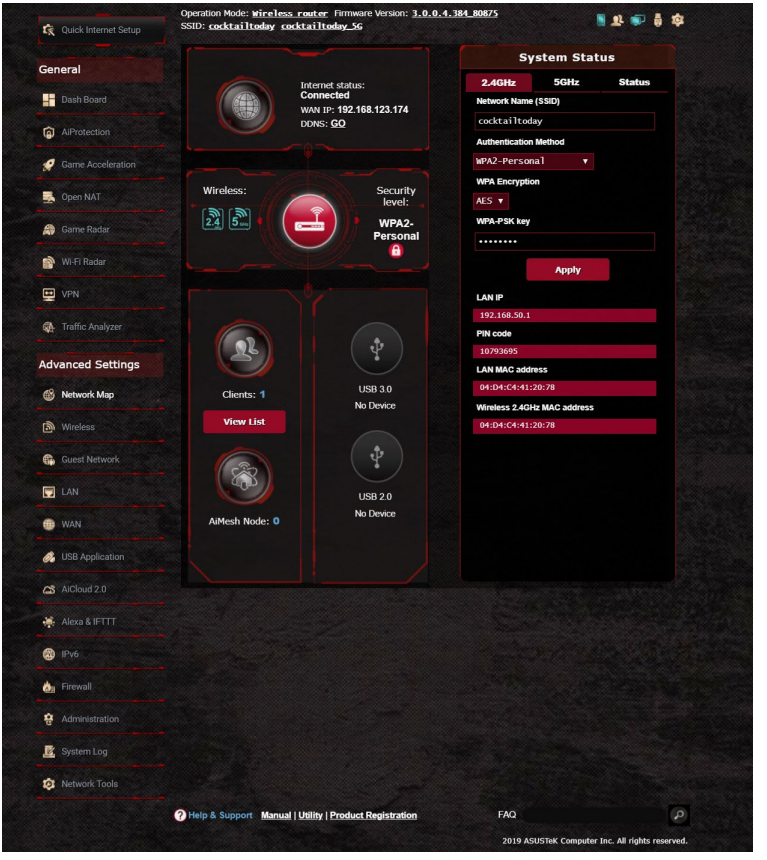
トラフィックアナライザーを使用する

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**」の欄で、情報を表示したい時間を選択します。

4 詳細設定

4.1 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管理、USBデバイスの管理を行なうことができます。



4.1.1 セキュリティのセットアップ

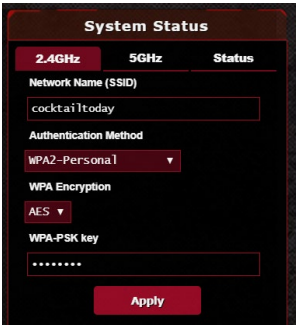
利用状況に応じてワイヤレスのセキュリティー設定を変更することができます。

ワイヤレスネットワークのセキュリティを設定する

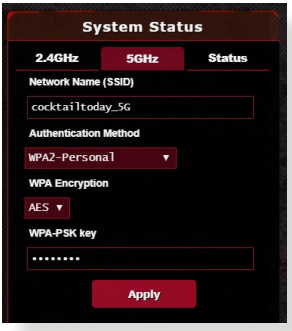
1. 「**ネットワークマップ**」をクリックします。
2. 「**セキュリティレベル**」をクリックしてステータスパネルにシステムの状態を表示します。

ご参考: 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

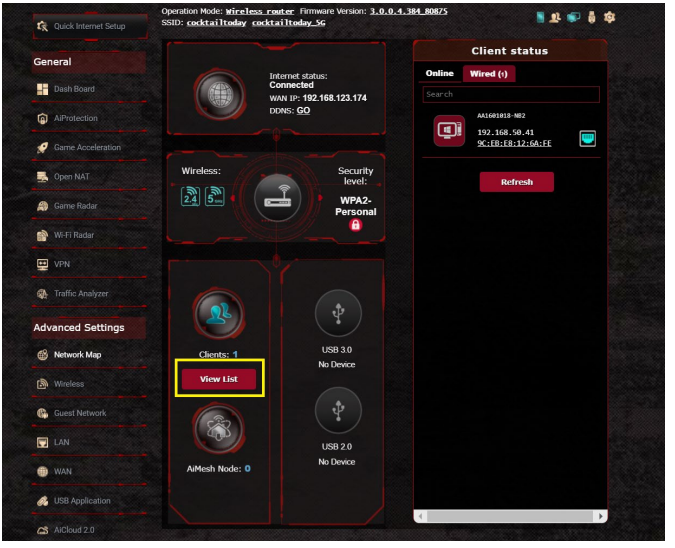


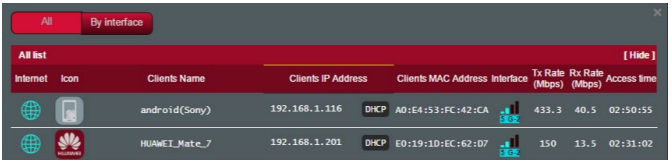
3. 「**ワイヤレス名 (SSID)**」に、他のワイヤレスネットワークと重複しないネットワーク名を入力します。
4. 「**認証方式**」ドロップダウンリストから利用する認証方式を選択します。

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。

4.1.2 ネットワーククライアントの管理



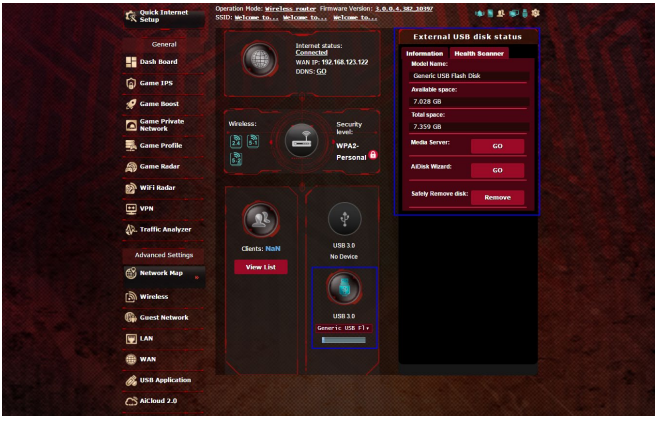


ネットワーククライアントの状態を確認する

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。

4.1.3 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。



ご参考:

- 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「**4.6 USBアプリケーションを使用する**」と「**4.7 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。

ご参考:

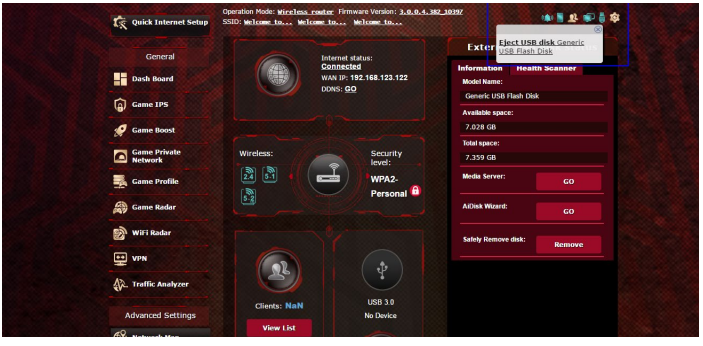
- 詳しくは「**4.6.2 Servers Center を使用する**」をご参考ください。
- 本製品は、最大4TBまでの容量のUSBストレージデバイスに対応しています。(対応フォーマット:FAT16、FAT32、NTFS、HFS+)
  本製品がサポートするUSB ストレージデバイスのフォーマットタイプや容量については、次のWeb サイトでご確認ください。
  http://event.asus.com/networks/disksupport

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「**取り外す**」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。



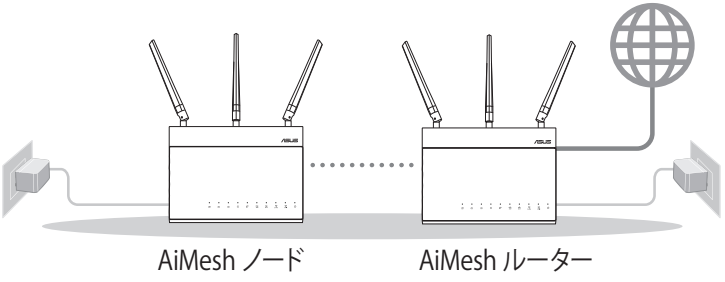
4.1.4 ASUS AiMesh

4.1.4.1 セットアップ準備

AiMesh Wi-Fi システムのセットアップ準備

1. 2台のASUSルーター（AiMeshをサポートするモデル: https://www.asus.com/AiMesh/）
2. 1台はAiMeshルーターとして、もう1台はAiMeshノードとして割り当てます。

ご参考: 複数台のAiMeshルーターがある場合は、スペックが最も高いルーターをAiMeshルーターとして使用し、他はAiMeshノードとして使用することをお勧めします。



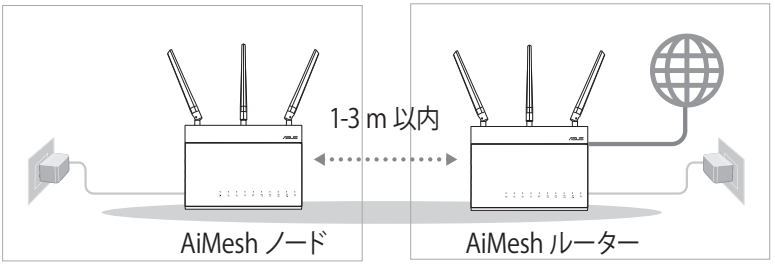
4.1.4.2 AiMesh のセットアップ手順

セットアップの前に

セットアップ中は、AiMeshルーターとノードの距離が1～3メートル以内になるように配置します。

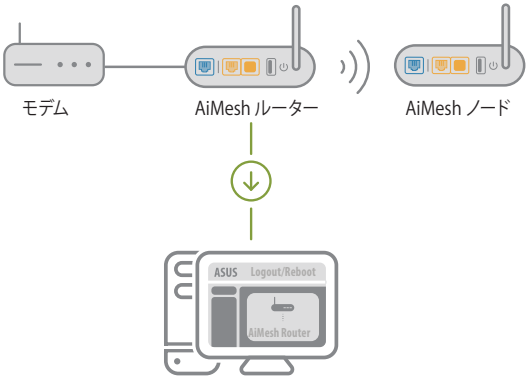
AiMesh ノード

工場出荷時の状態です。AiMeshシステム設定を行ないます。設定中は電源をオフにしないでください。



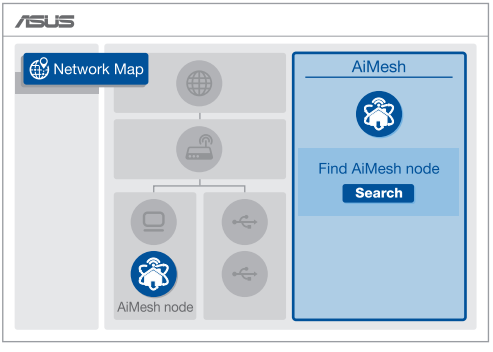
AiMesh ルーター

1) 他のルーターのクイックスターとガイドを参照し、AiMeshルーターをPCとモデムに接続し、Web GUIにログインします。



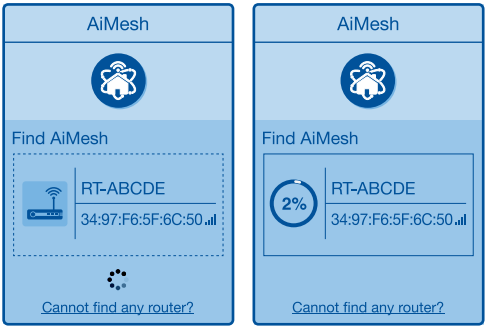
2) 「**ネットワークマップ**」ページを開き、AiMesh アイコンをクリックし、拡張するAiMeshノードを検索します。

ご参考: AiMeshアイコンが表示されない場合は、ファームウェアのバージョンをクリックし、ファームウェアを更新してください。

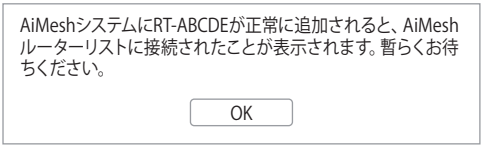


3) 「**Search (検索)**」をクリックすると、AiMeshノードが自動検索されます。AiMeshノードがこの画面に表示されたら、クリックしてAiMeshシステムに追加します。

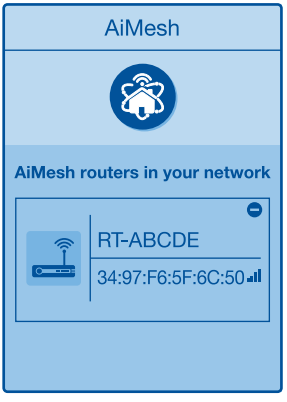
ご参考: AiMesh ノードが見つからない場合は、トラブルシューティングをご参照ください。



4) 同期が完了すると、メッセージが表示されます。



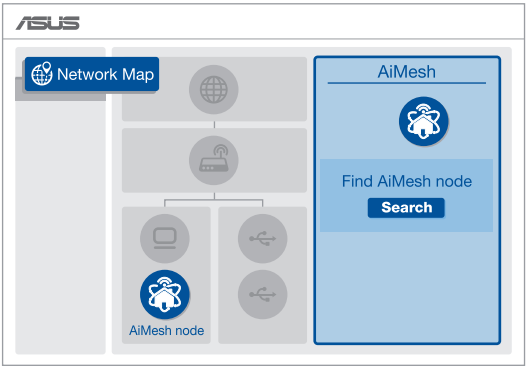
5) AiMeshノードがAiMeshネットワークに正常に追加されると、次のような画面が表示されます。



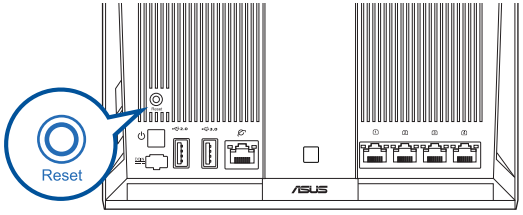
4.1.4.3 トラブルシューティング

AiMeshルーターで近くにあるAiMeshノードが検索できない場合や、同期に失敗する場合は、以下をご確認ください。問題が解決する場合があります。

1) AiMeshノードをAiMeshルーターの近くに移動します。1-3 m以内に設置されていることを確認します。
2) AiMeshノードの電源が入っていることを確認します。
3) AiMeshノードのファームウェアがAiMesh対応のバージョンであることを確認します。
   i. 次のURLからAiMeshがサポートするファームウェアをダウンロードしてください。(https://www.asus.com/AiMesh/)
   ii. AiMeshノードの電源をオンにし、ネットワークケーブルでPCに接続してください。
   iii. Web GUIを起動します。続いて、ASUS Setup Wizardにリダイレクトされます。リダイレクトされない場合は、次のURLにアクセスしてください。(http://router.asus.com)
   iv. 「**管理者**」→「**ファームウェア更新**」の順に開きます。「**Choose File**」をクリックし、AiMeshでサポートされているファームウェアをアップロードします。
   v. ファームウェアをアップロードしたら、ネットワークマップ画面を開き、AiMeshアイコンが表示されているかどうかを確認します。



   vi. AiMeshノードのリセットボタンを5秒以上押します。電源LEDがゆっくりと点滅したら、リセットボタンから手を離してください。



4.1.4.4 配置しなおす

最適な場所にAiMeshルーターとノードを配置します。

注意:

- 干渉を最小限に抑えるため、コードレス電話、Bluetoothデバイス、電子レンジなどの近くにルーターを設置しないでください。
- ルーターは可能な限り、信号を遮るものがないオープンスペースに設置することをお勧めします。

4.1.4.5 FAQ (よくある質問)

Q1: AiMeshルーターはアクセスポイントモードをサポートしていますか?

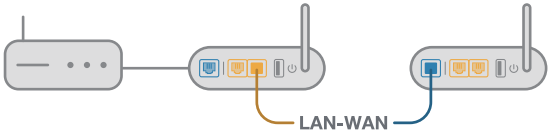
A: はい。AiMeshルーターをルーターモードまたはアクセスポイントモードに設定することができます。Web GUI (http://router.asus.com) にアクセスし、「**管理者**」→「**動作モード**」画面で設定します。

Q2: AiMesh ルーター間で有線接続を構築できますか (イーサネットバックホール) ?

A: はい。AiMeshシステムは、スループットと安定性を最大化するため、AiMeshルーターとノード間の無線接続と有線接続の両方をサポートしています。AiMeshは利用可能な各周波数帯の無線信号の強度を分析し、任意の無線接続または有線接続をルーター間接続バックボーンとして機能させるのことが適切であるかを自動的に判断します。

1) Wi-Fi 経由でAiMeshルーターとノード間の接続を確立するには、設定手順に従ってください。

2) 通信範囲が最大になるよう、ノードを適切な位置に配置します。イーサネットケーブルで、AiMeshルーターのLANポートとAiMeshノードのWANポートを接続します。

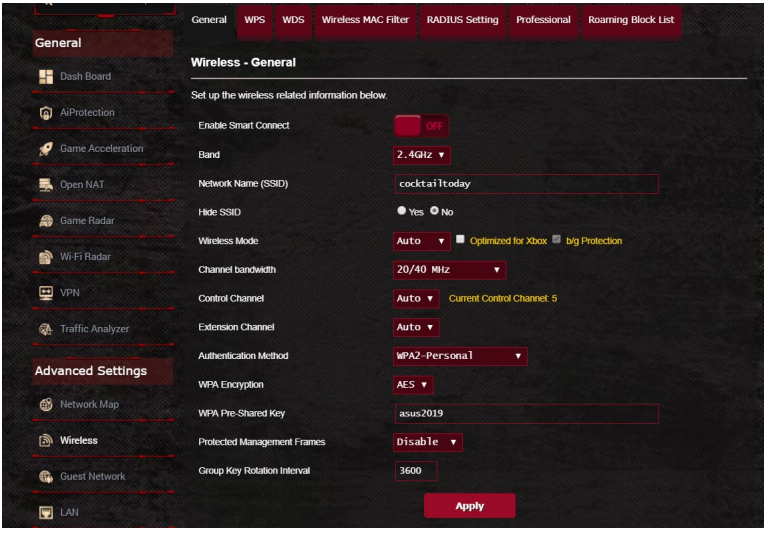


3) AiMeshシステムは、有線/無線のいずれの接続でも、データ伝送に最適な経路を自動的に選択します。

4.2 ワイヤレス

4.2.1 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**」をクリックします。
2. スマートコネクトの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/ax で通信します。
   - **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。
   - **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。

   ご参考:「**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。

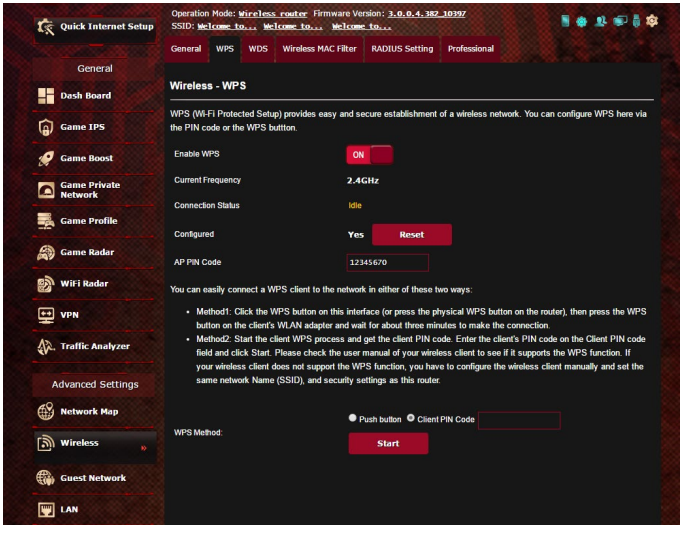
   ご参考:暗号化方式でWEP (64/128 bit) またはTKIPを使用した場合、最大転送速度は54Mbps (規格値) となります。
10. 「**適用**」をクリックし、設定を保存します。

    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。

4.2.2 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。

ご参考: 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。

ご参考: 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-Personal、WPA2-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。プッシュ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。

ご参考: 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:

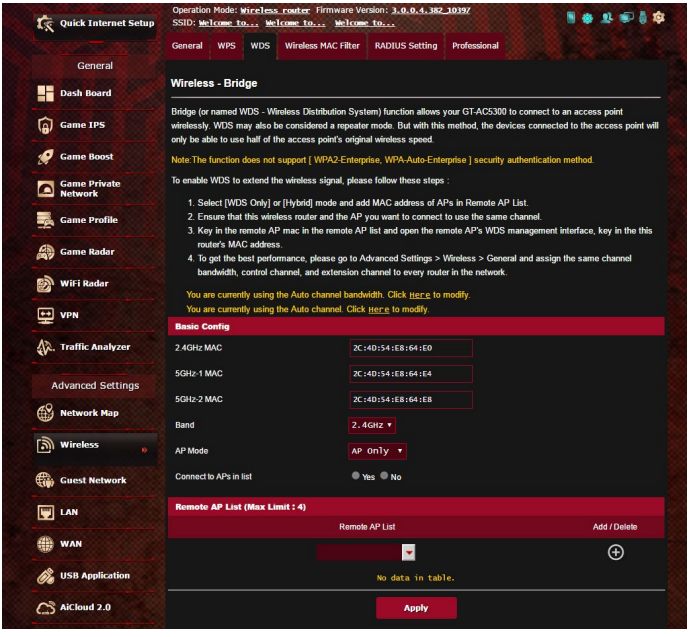
   a. 無線LANルーターのPINコードを確認します。PINコードは管理画面上の「**AP PIN コード**」に表記されています。
   b. ワイヤレスデバイスにPINコードを入力しWPS機能を有効にします。接続設定中は電源LEDが3回点滅します。

   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。

4.2.3 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。

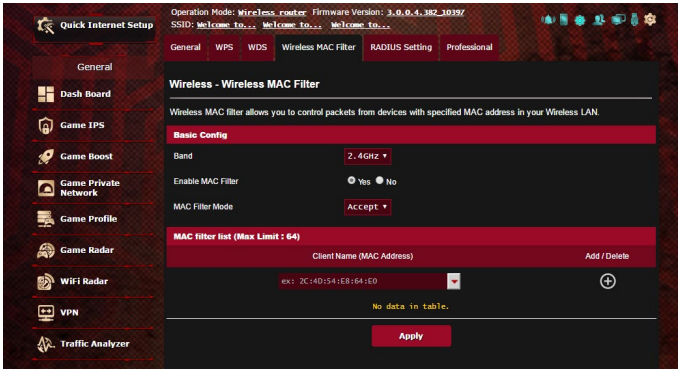
4. リモートブリッジリストに登録したアクセスポイントに接続する場合は、「**リスト内のAPに接続しますか**」の「**はい**」をチェックします。
5. リモートブリッジリストに新たなアクセスポイントを追加するには、プルダウンリストから選択するか、MACアドレスを入力し ⊕ ボタンをクリックします。

   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。

4.2.4 ワイヤレスMACフィルター

ワイヤレスMACフィルターでは、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。

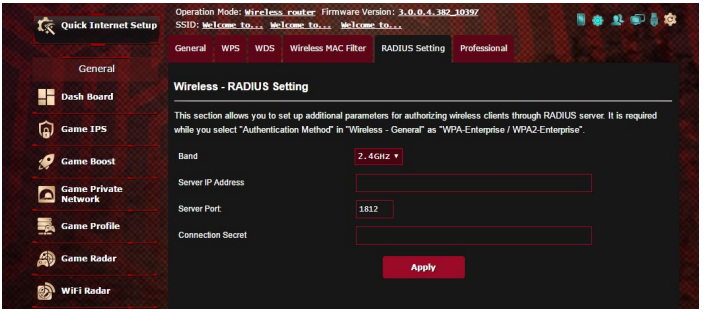


ワイヤレスMACフィルターのセットアップ

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. 「**MACフィルター**」の「**はい**」を選択します。
3. 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。
4. 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。
5. 「**適用**」をクリックし、設定を保存します。

4.2.5 RADIUSの設定

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。

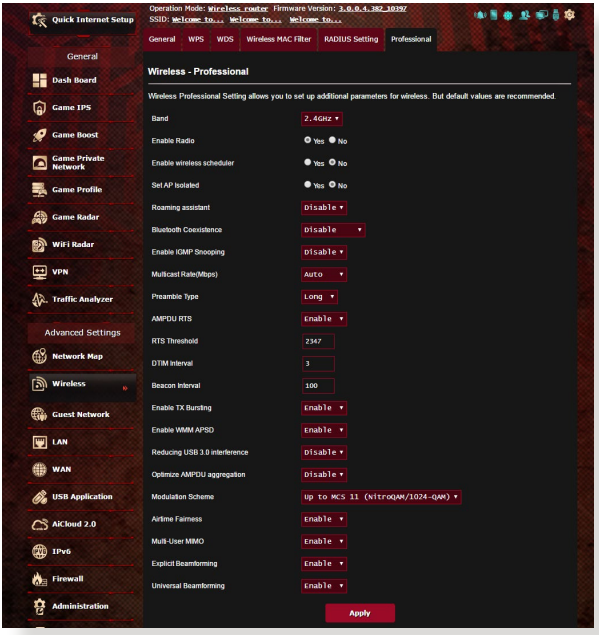
   ご参考: 認証方式については、「**4.2.1 全般設定**」をご覧ください。

2. 「**ワイヤレス**」をクリックし、「**RADIUSの設定**」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。

4.2.6 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。

ご参考: 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。
- **ワイヤレス機能を有効にする日 (平日) :** ワイヤレス機能を有効にする日を曜日単位で設定します。
- **ワイヤレス機能を有効にする時間:** 「**ワイヤレス機能を有効にする日 (平日)**」で設定した日のワイヤレス機能を有効にする時間帯を設定します。

- **ワイヤレス機能を有効にする日 (週末) :** ワイヤレス機能を有効にする日を曜日単位で設定します。
- **ワイヤレス機能を有効にする時間:** 「**ワイヤレス機能を有効にする日 (週末)**」で設定した日のワイヤレス機能を有効にする時間帯を設定します。
- **APを隔離:** 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スヌーピングを有効にする :** 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。「**Short**」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。「**Long**」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。
- **Beacon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:** 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。
- **USB 3.0干渉を低減する：**この機能を有効にすると、2.4 GHz帯で最高の無線性能が保証されます。この機能を無効にすると、USB 3.0ポートの伝送速度が向上し、2.4 GHz無線範囲に影響する可能性があります。
- **Optimize AMPDU aggregation:** AMPDUのMPDUの最大数を最適化し、エラーが発生しやすいワイヤレスチャンネルにおける送信中のパケットの損失を防ぎます。
- **Optimize ack suppression (act 抑制の最適化):** ackの最大数を連続で抑止するように最適化します。

- **Turbo 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。
- **エアタイムの公平性：**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。
- **Explicit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。
- **Implicit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、「**Implicit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。

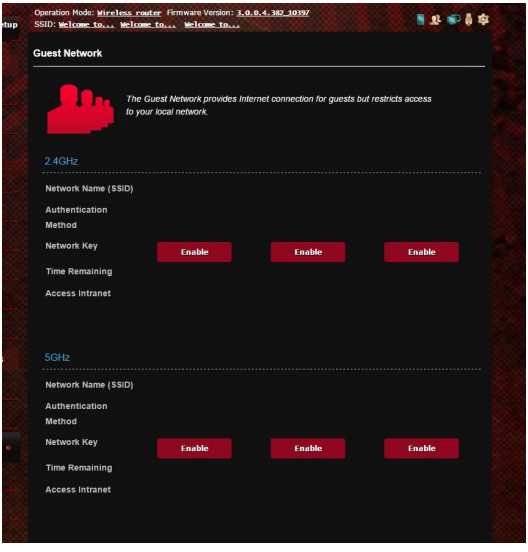
4.3　ゲストネットワークを構築する

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。

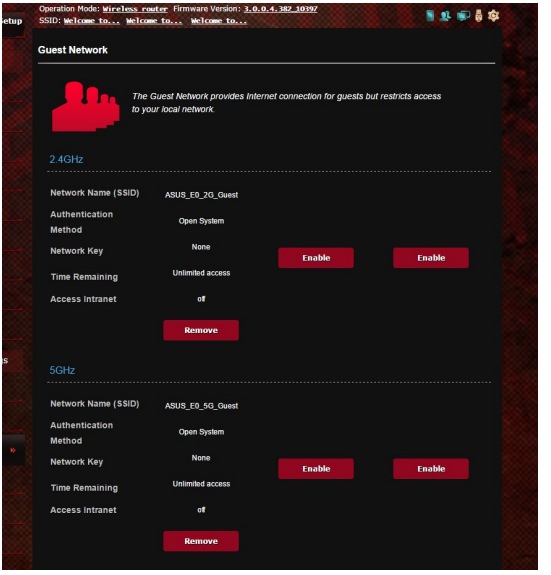
> **ご参考:** 本製品では、各周波数帯で3つずつ、合計6つのゲストネットワーク設定を行なうことができます。

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。

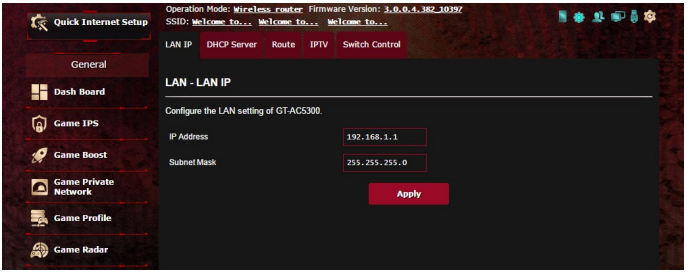
4.4 LAN

4.4.1 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。

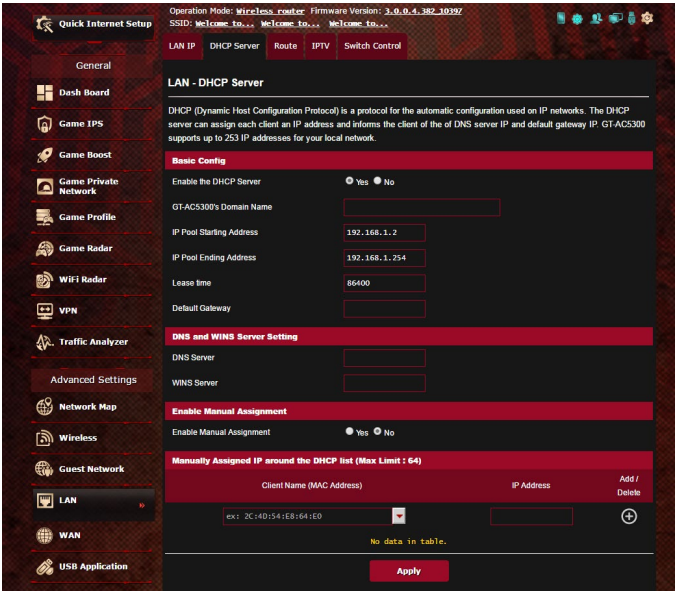


LAN IP設定を変更する

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。

4.4.2 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 サーバーを有効にしますか**」の「**はい**」をチェックします。
3. 「**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 プール起点アドレス**」に起点となるIPアドレスを入力します。

5. 「**IP プール終点アドレス**」に終点となるIPアドレスを入力します。
6. 「**リースタイム**」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: **192.168.1.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。

---

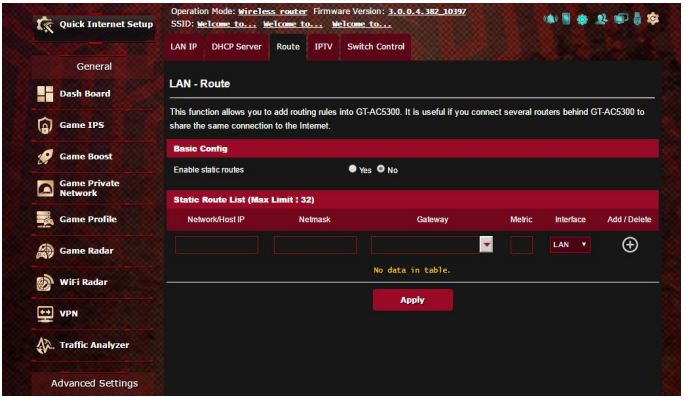
7. 設定が必要な場合は、「**DNS と WINS サーバーの設定**」で各サーバーのIPアドレスを入力します。

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。「**手動割り当てを有効にしますか**」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32個まで登録することができます。

4.4.3 経路

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。

> **ご参考:** 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。

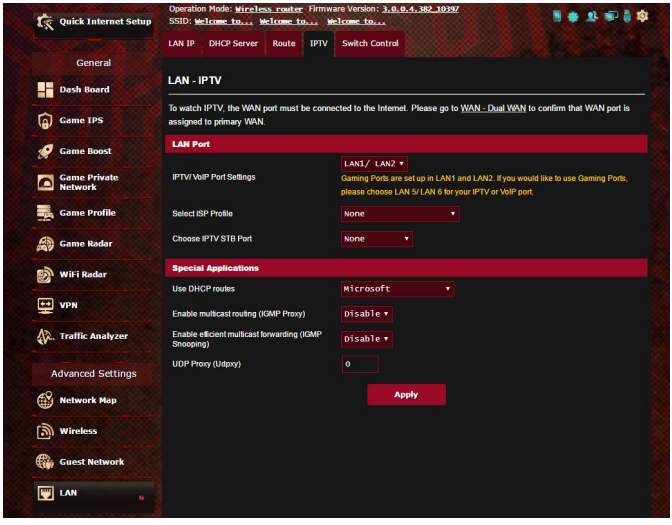


ルーティングテーブルのセットアップ

1. 「**LAN**」をクリックし、「**経路**」タブを選択します。
2. 「**静的経路を有効にしますか**」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。

4.4.4 IPTV

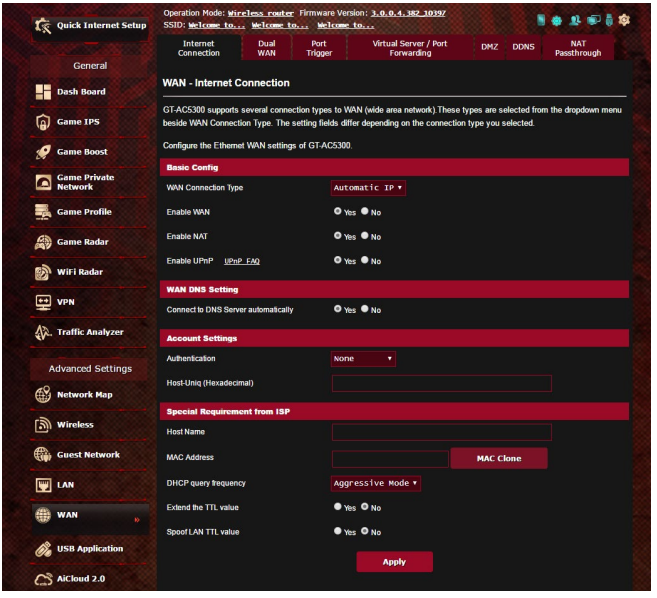
本製品は、IPSまたはLANを介したIPTVサービスをサポートしています。この項目ではIPTV、VoIP、マルチキャスト、UDPに関する詳細設定を行うことができます。IPTVサービスに関する情報や適切な設定方法については、ご利用のサービスプロバイダーにお問い合わせください。



4.5 WAN

4.5.1 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**: 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。

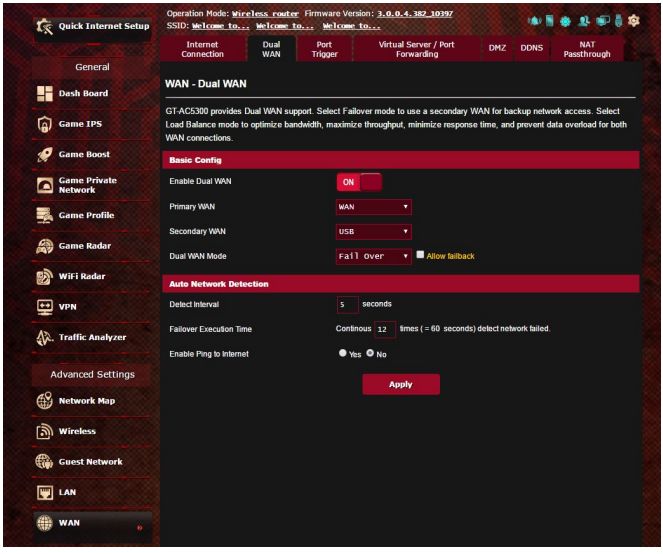
- **NATを有効**: NAT (Network Address Translation) は、プライベートIPアドレスを、インターネットで使用できるようグローバルIPアドレスに変換する機能です。これにより、1つのグローバルIPアドレス環境でプライベートIPアドレスを割り当てられた複数のコンピューターが、同時にインターネットへアクセスできるようになります。「**いいえ**」に設定した場合、インターネットは1台のみで利用可能です。
- **UPnPを有効にしますか**: UPnP (Universal Plug and Play) 機能の有効/無効を設定します。UPnPは、コンピューターやそ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 サーバーに自動接続しますか:** DNSサーバーアドレス自動取得の有効/無効を設定します。「**いいえ**」に設定した場合は、手動で固定アドレスを設定することができます。
- **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。

4.5.2 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。

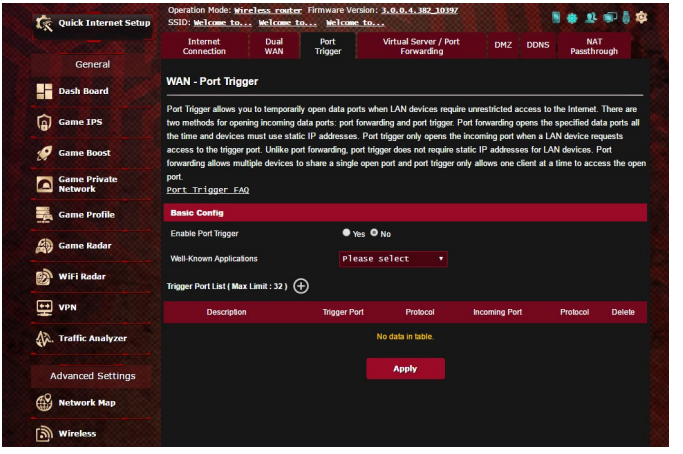


4.5.3 ポートトリガー

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. 「**よく使用されるアプリケーション**」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。

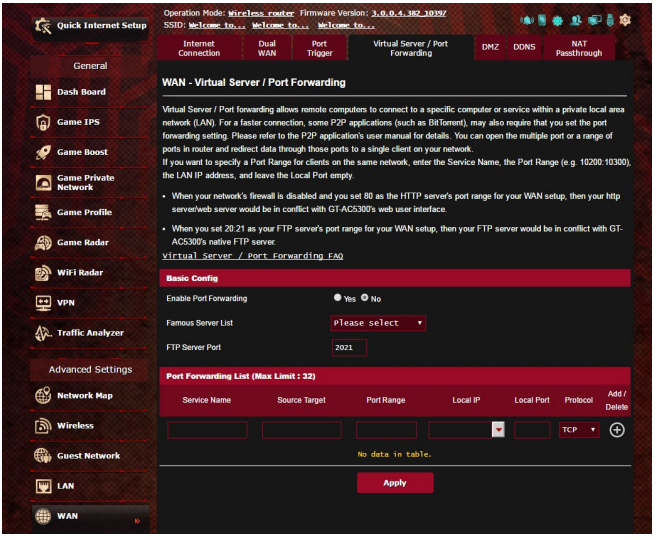
4. トリガーポートリストの各項目に必要事項を入力することで、手動でアイテムを追加することもできます。
   - **説明:** トリガーポートリストに登録する際の識別名を入力します。
   - **トリガーポート:**監視するトリガーポート (発信ポート) 範囲を指定します。
   - **プロトコル:** トリガーポートの通信プロトコルを選択します。
   - **着信ポート:**トリガーによって一時的に開放される着信ポートの範囲を指定します。
   - **プロトコル:** 着信ポートの通信プロトコルを選択します。
5. をクリックし、ポートトリガーに関する情報をリストに追加します。 ボ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。

ご参考:

- 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。

4.5.4 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しますか**」 を「**はい**」にチェックを入れます。

3. 「**よく知られたサーバーリスト**」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. 「**よく知られたゲームリスト**」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。

6. **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。
7. **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。

4.5.5 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

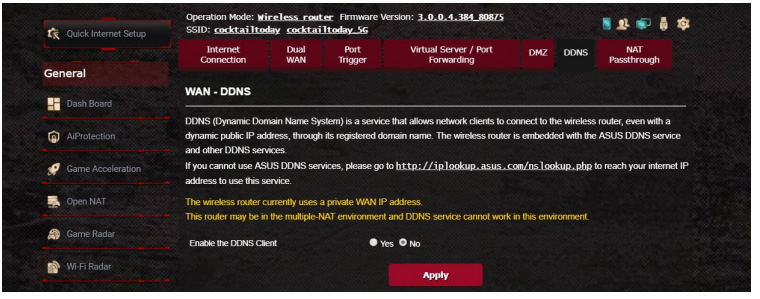
1. 「**WAN**」をクリックし、「**DMZ**」タブを選択します。
2. 「**DMZを有効**」の「**はい**」を選択します。
3. **公開ステーションのIPアドレス:** DMZ指定するクライアントのIPアドレスを入力します。サーバークライアントは静的IPアドレスが割り当てられている必要があります。
4. 「**適用**」をクリックし、設定を保存します。

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。

4.5.6 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しますか:** 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。

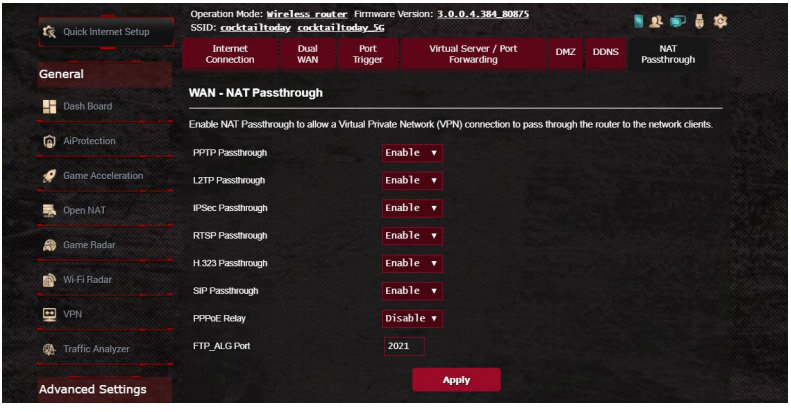
4.5.7 NATパススルー

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

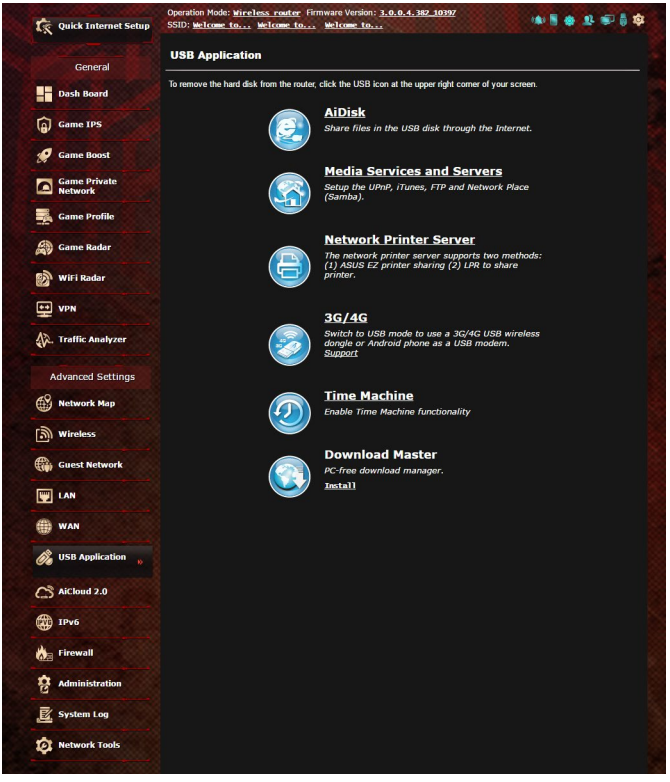
1. 「**WAN**」をクリックし、「**NAT パススルー**」タブを選択します。
2. 各パススルー機能の有効/無効を設定します。設定完了後「**適用**」をクリックし、設定を保存します。



4.6 USBアプリケーションを使用する

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/)

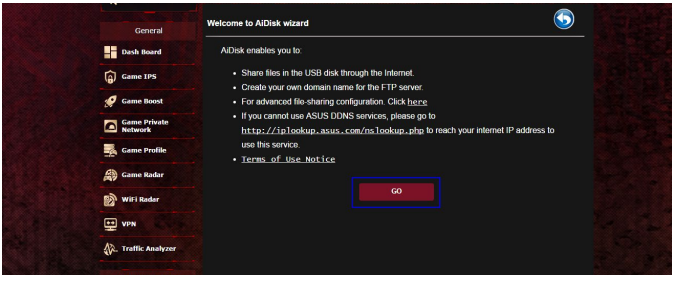


4.6.1 AiDiskを使用する

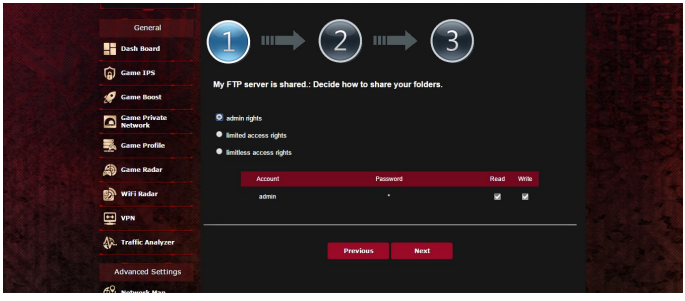
AiDisk は、無線LANルーターのUSBポートに接続したUSB ストレージデバイスをクラウドストレージのように使用することができる機能です。

AiDisk を使用する:

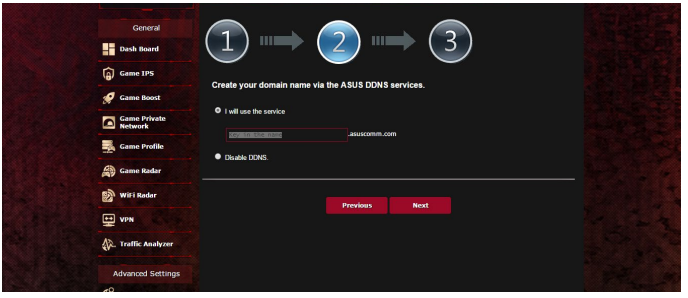
1. 「**USBアプリケーション**」→「**AiDisk**」の順にクリックします。
2. 「**GO**」をクリックし、AiDisk ウィザードを開始します。



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)

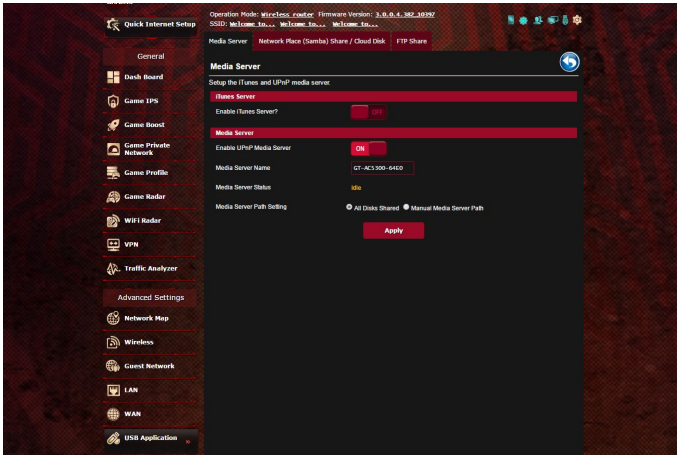
4.6.2 Servers Center を使用する

Servers Center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、DLNA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:** DLNA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。



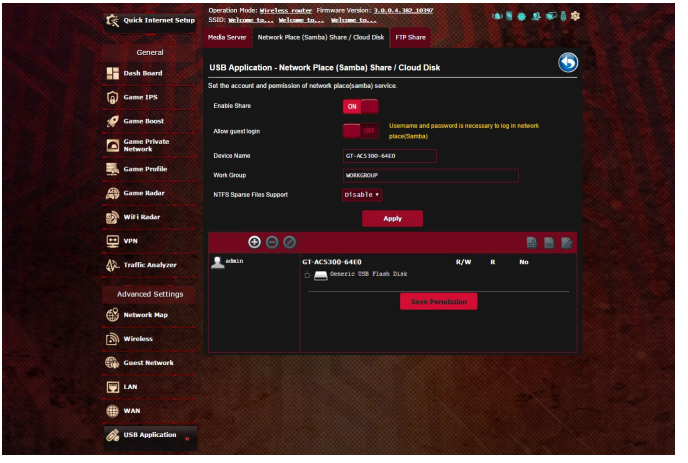
「**USBアプリケーション**」→「**サーバーセンター**」の順にクリックします。各項目については、次の説明をご覧ください。

- **iTunes Server を有効にしますか?:**
  iTunesサーバー機能の有効/無効を設定
- **Enable DLNA Media Server:**
  DLANメディアサーバー機能の有効/無効を設定

- **Media Server Name**
  メディアサーバーの表示名を設定
- **Media Server Status:**
  現在のメディアサーバーの状態を表示
- **Media Server Path Setting**:
  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。

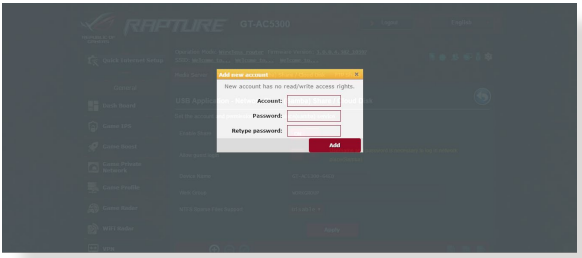
ご参考: ネットワークプレース (Samba) はデフォルトで有効に設定されています。

2. 「**Network Neighborhood 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。

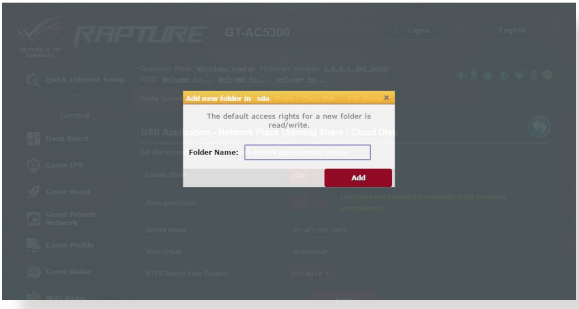
b) をクリックします。

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。



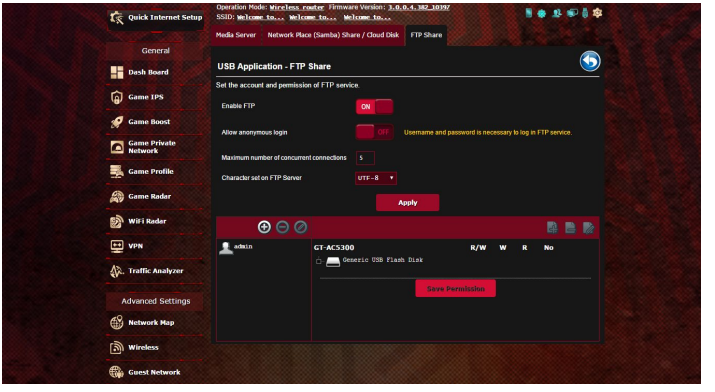
3. フォルダーリストから、フォルダーに割り当てるアクセス権限を選択します。ゲストアクセスがONの場合、この設定は不要です。
   - **R/W:** 読み取りアクセス許可 / 書き込みアクセス許可。
   - **R:** 読み取りアクセスのみ許可。
   - **No:** アクセスを許可しない (共有しない) 。
4. 「**権限を保存**」をクリックし、変更を適用します。

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、「**4.1.3 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

ご参考: 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「**4.6.1 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
   - **文字はFTPサーバーで設定**

     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)

4.6.3 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。

ご参考: 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モデムを有効にしますか**」の「**はい**」をチェックします。
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。
   - **ISP / USBモデム**: 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。

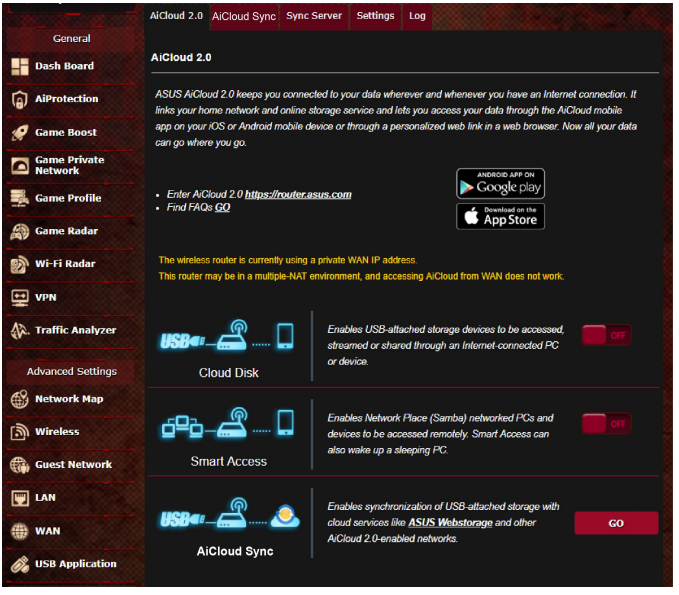
ご注意: 設定を適用するためには、無線LANルーターの再起動が必要です。

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。

4.7 AiCloud 2.0を使用する

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 2.0を使用する

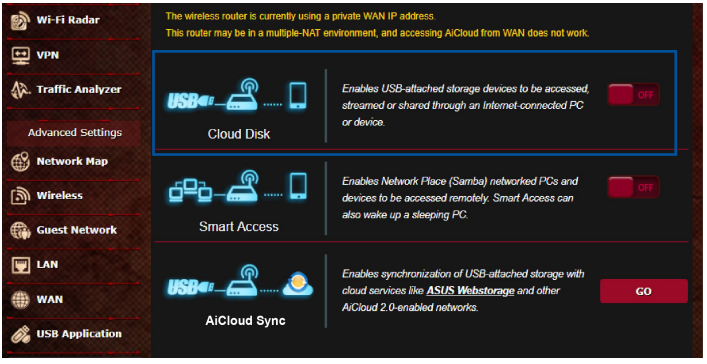
1. AndroidやiOSを搭載したスマートデバイスで、Google PlayまたはApp Storeから「**ASUS AiCloud**」アプリをダウンロードしてインストールします。
2. ASUS AiCloudアプリをインストールしたスマートデバイスを本機のワイヤレスネットワークに接続します。次にASUS AiCloudアプリを起動し、画面の指示に従ってセットアップを行います。

4.7.1 Cloud Disk

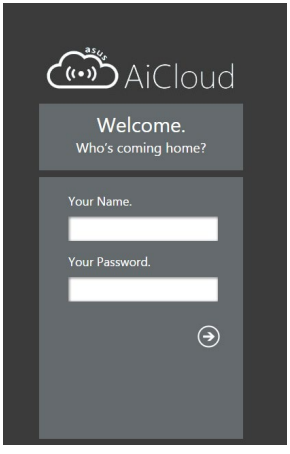
Cloud Disk は専用アプリ、またはWebブラウザーでルーターのUSBポートに接続したUSBストレージデバイスにアクセスすることができる機能です。

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。



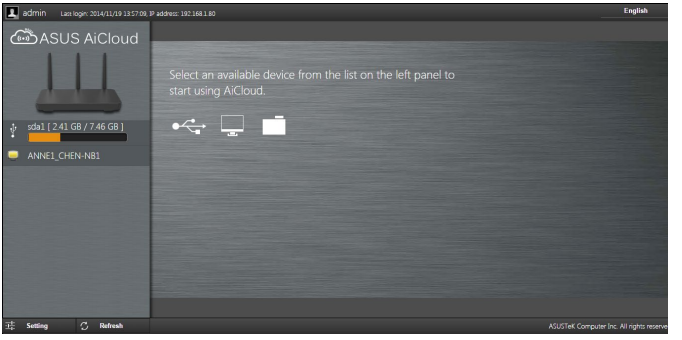
3. Webブラウザーのアドレス欄に「**https://router.asus.com**」と入力してASUS AiCloudのログイン画面に移動し、ルーターのユーザー名とパスワードを入力してログインします。



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。

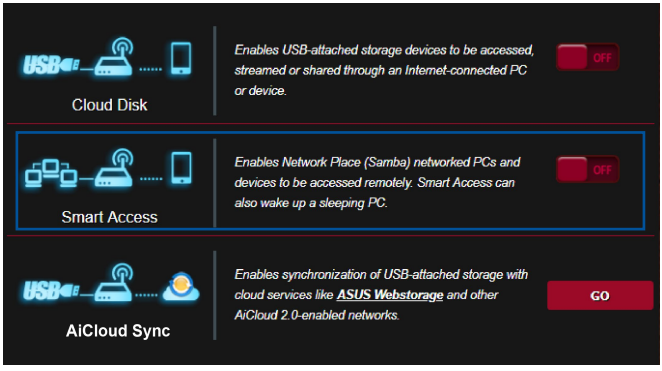
ご注意: セキュリティ対策上、AiCloudではログイン情報を保存することはできません。



ご参考: 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。

4.7.2 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。



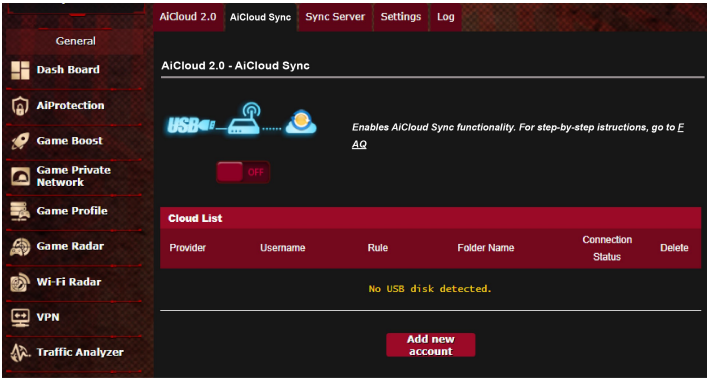
ご参考:

- 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

4.7.3 AiCloud Sync

AiCloud Syncは、無線LANルーターに接続されたUSBストレージデバイスのデータをオンラインストレージサービスASUS Webstorageと同期することができる機能です。リアルタイムに同期するので、アクセスするデータを常に最新の状態に保つことができます。

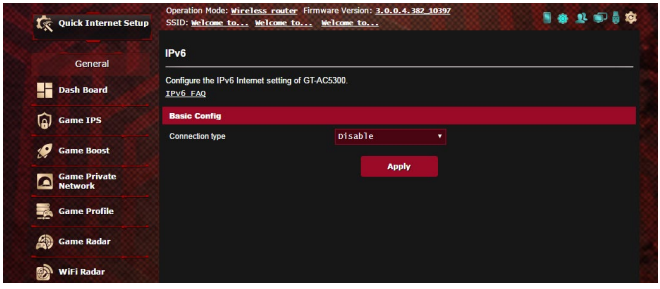


AiCloud Syncを使用する

1. 「**AiCloud 2.0**」を選択し、「**AiCloud Sync**」のGO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。

4.8 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。

ご参考: 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。

4.9 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。

ご参考: 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。

4.9.1 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しますか**」の「**はい**」をチェックします。
3. 「**DoS保護を有効にしますか**」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。

4.9.2 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。

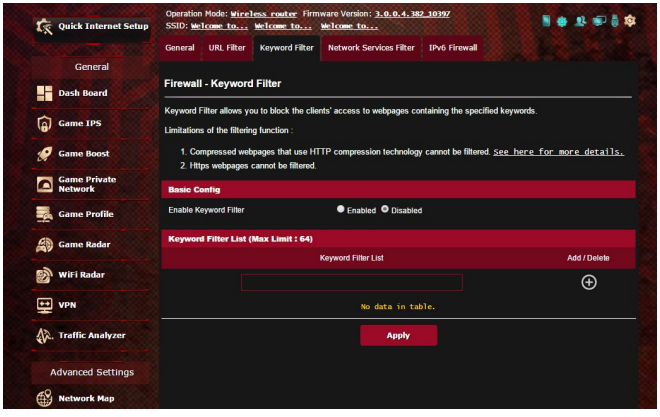
ご参考:URLフィルター機能はDNSクエリに基づいて行われます。システムストアの閲覧履歴はDNSキャッシュに格納されており、ネットワークのクライアントが閲覧した履歴のあるWeb サイトはブロックすることができません。この問題を解決するには、URLフィルター機能を設定する前にDNSキャッシュをクリアする必要があります。

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。

4.9.3 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します**」の「**有効**」をチェックします。

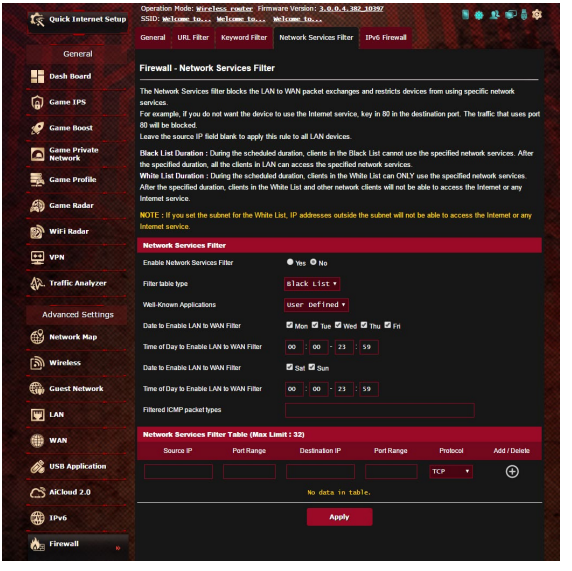
3. 単語またはフレーズを入力し、 ボタンをクリックします。
4. 「**適用**」をクリックし、設定を保存します。

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。

4.9.4 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。

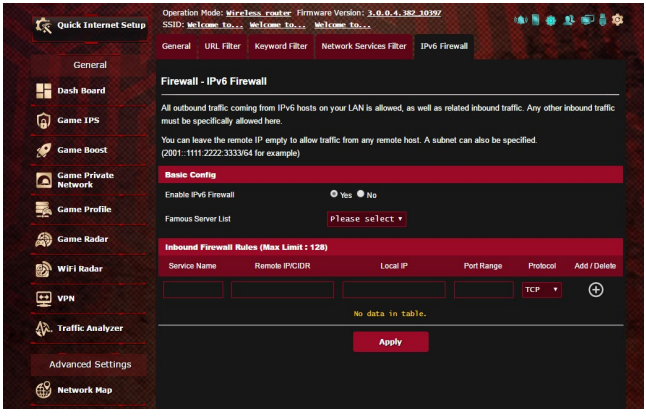


パケットフィルターのセットアップ

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しますか**」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. パケット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。

4.9.5 IPv6 ファイアウォール

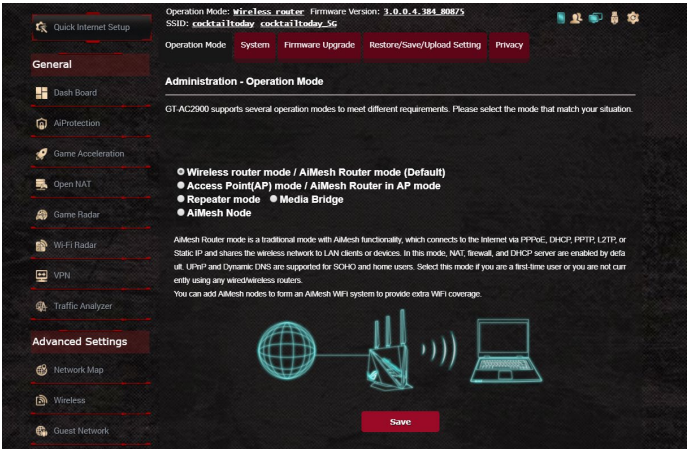
デフォルト設定では、本機はすべての迷惑な着信トラフィックをブロックします。IPv6ファイアウォール機能は、ネットワークを経由する指定されたサービスからの着信トラフィックを許可します。



4.10 管理者

4.10.1 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. 「**管理者**」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）：** AiMesh ルーターモードは既存のルーターモードとして動作します。PPPoE、DHCP、PPTP、L2TP、スタティック IP を通じてインターネットに接続し、デバイスにワイヤレスネットワークを提供します。このモードでは NAT、ファイアーウォール、DHCP サーバーはデフォルトで有効となります。また、UPnP、DDNS をサポートします。初めてワイヤレスや有線でルーターをお使いになる場合はこのモード選択してください。
     AiMesh システムに AiMesh ノードを追加することで広範囲のワイヤレス通信を提供することができます。
   - **アクセスポイント (AP)モード / AiMesh アクセスポイントモード：** AiMesh アクセスポイントモードではモデムまたはルーター親機と本機をイーサネットケーブルを接続することでワイヤレスの通信範囲を拡張することができます。このモードでは、ファイアウォール、IP 共有、NAT はデフォルトで無効となりま

す。AiMesh システムに AiMesh ノードを追加することで広範囲のワイヤレス通信を提供することができます。)

- **メディアブリッジモード:** メディアブリッジモードでは、同時に複数のデバイスと通信するために最適な IEEE 802.11ac で接続を行います。設定を行うには、メディアブリッジに対応したルーターが 2 台必要となります。1 台はルーターとして、もう 1 台はメディアブリッジモードの受信機として使用します。
- **リピーターモード:** リピーターモードでは、既存のアクセスポイントと無線LANアダプターとの電波を中継し、直接電波が届かない場所でも無線によるアクセスを可能にします。このモードでは、ファイアウォール、IP共有、およびNAT機能は無効になります。
- **AiMesh ノード:** 既存の AiMesh ルーターに AiMesh ノードを追加して通信範囲の拡張ができます。
  1. AiMesh ネットワークに追加するには工場出荷時の状態にリセットします。
  2. AiMesh ノードを追加するには AiMesh ルーターの設定ページから行います。

3. 「**適用**」をクリックし、設定を保存します。

ご参考: 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。

4.10.2 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. 「**管理者**」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。
   - **ログイン名/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を有効:** 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からのウェブアクセスを有効にしますか:** 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。
   - **特定IPの許可:** 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。
   - **クライアントリスト:** 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。

4.10.3 ファームウェア更新

ご参考: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。(http: //www.asus.co.jp/)

ファイルからファームウェアを更新:

1. 「**管理者**」をクリックし、「**ファームウェア更新**」タブを選択します。
2. 「**新しいファームウェアファイル**」の「**参照**」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。

ご参考:

- 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、「**5.2 Firmware Restoration (ファームウェアの復元)**」をご覧ください。

4.10.4 復旧/保存/アップロード設定

無線LANルーターの設定の保存とアップロード

1. 「**管理者**」をクリックし、「**復元/保存/アップロード設定**」タブを選択します。
2. 実行するタスクを選択します:
   - 工場出荷時のデフォルト
     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。
   - 設定の保存
     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。
   - 設定の復元
     「**設定の保存**」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。

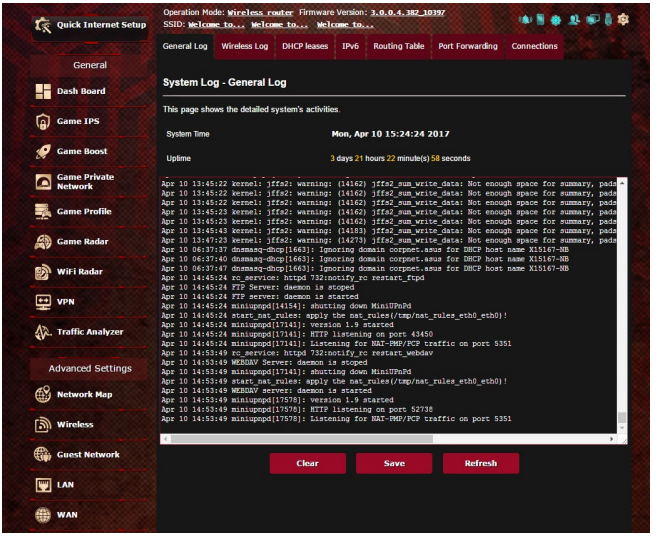
4.11 システムログ

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。

ご参考: 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
   - DHCPリース
   - ワイヤレスログ
   - ポートフォワーディング
   - 経路表 (ルーティングテーブル)
   - IPv6
   - 接続



4.12 スマートコネクト

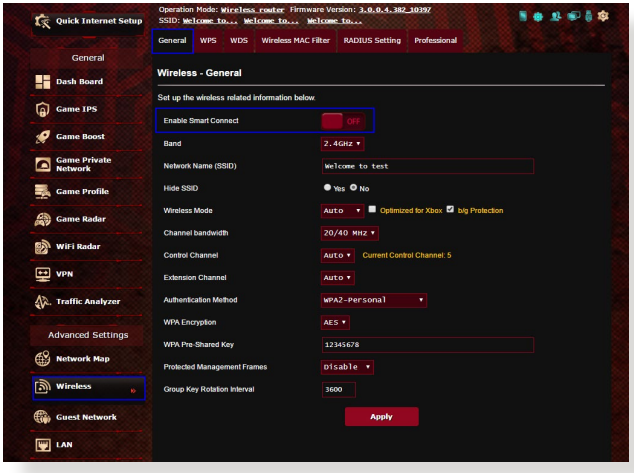
スマートコネクトでは、クライアントを3つの無線（2.4 GHz、低帯域5 GHz、高帯域5 GHz）のいずれかに自動的に切り替えます。

4.12.1 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。

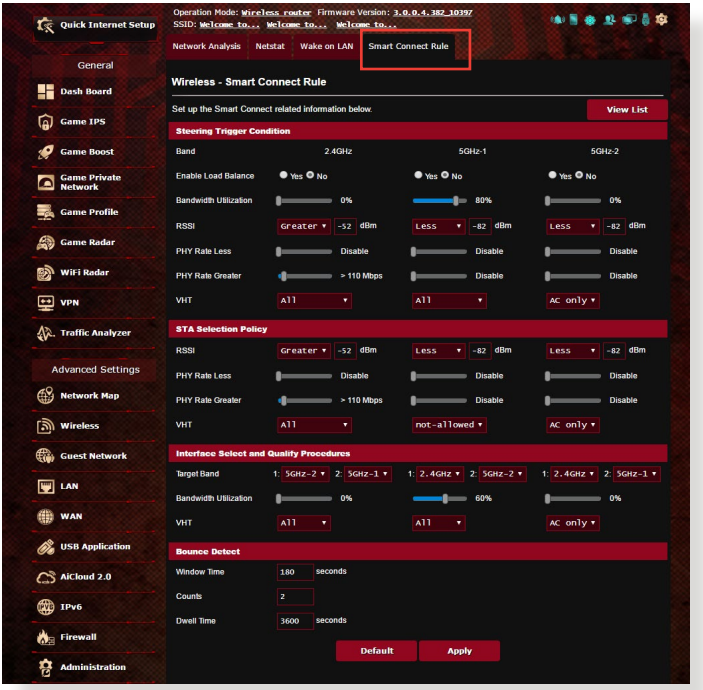
- **ワイヤレス画面から**

1. ウェブブラウザーのアドレス欄に「**http://router.asus.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**」→「**一般タブ**」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。この機能により、自動的に適切な周波数帯（2.4GHz、5GHz-1、5GHz-2）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。



4.12.2 スマートコネクト詳細設定

ASUSWRTでは、ネットワーク環境に応じて帯域切替の条件を設定することができます。設定を変更するにはネットワークツール画面の「**スマートコネクト詳細設定**」のタブを開きます。

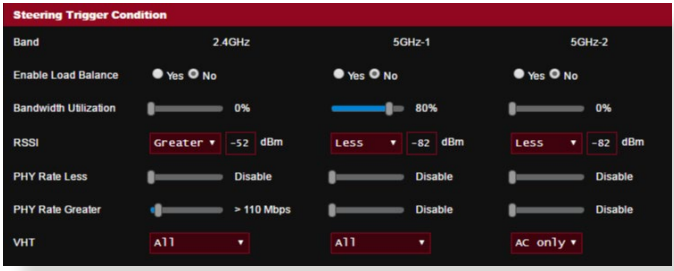


スマートコネクトの制御は、4つのセクションに分けられます。

- 帯域切替条件
- STA選択ポリシー
- インターフェースの選択と品質
- バウンス検出

帯域切替条件

こちらの設定項目では、バンドステアリングを作動させる基準を設定します。



- **帯域の最適化**

  帯域幅使用率がこのパーセンテージを超えると、ステアリングが作動します。
- **ロードバランス**

  負荷分散を制御します。
- **信号強度 (RSSI)**

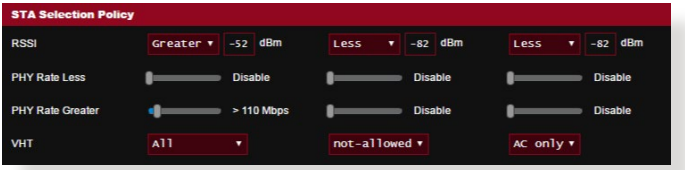
  接続クライアントの受信信号レベルがこの基準を満たすと、ステアリングが作動します。
- **PHY 減衰率 / RHY 増幅率**

  これらの制御項目により、バンドステアリング (帯域切換) を作動させる無線レート(The Physical Layer Rate)を決定します。
- **VHT**

  この制御項目により、802.11acクライアントと非ACクライアントの処理方法を決定します。
  - **ALL** (デフォルト) では、あらゆるタイプのクライアントがステアリングを作動させることができます。
  - **AC only**では、802.11ac 対応のクライアントのみが、ステアリングを作動させることができます。
  - **Not-allowed**では、非802.11aクライアント (例: 802.11a/b/g/n) のみが、ステアリングを動作させることができます。

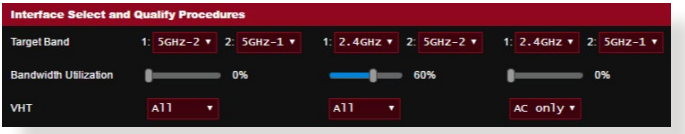
STA選択ポリシー

ステアリングが作動すると、ASUSWRTはSTA選択ポリシーに従い、クライアント（STA）は最も適切な帯域に切り替えられます。



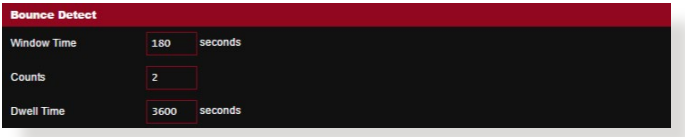
インターフェースの選択と品質

これらの制御項目では、ステアリングされたクライアントの切替条件を設定します。Target Band の制御項目では、ステアリングする第1・第2候補の帯域を選択します。無線のSTA選択ポリシー基準を満たすクライアントは、第1候補にステアリングされます。ただし、その無線の帯域幅使用率が設定値未満である場合に限られます。設定値を超過している場合は、クライアントは第2候の帯域にステアリングされます。



バウンス検出

これらの制御項目では、クライアントがステアリングされる頻度を設定します。これはクライアントが頻繁にステアリングされるのを防ぐためです。ただし、クライアント自身による切断や、バウンス発生時のカウントは防ぐことはできません。各クライアントは、**猶予時間**の範囲内であれは、無制限にステアリングされます。カウント回数の上限に達すると、**滞留時間**の間は、クライアントステアリングは停止します。



5 ユーティリティ

ご参考:

- 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。

5.1 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。

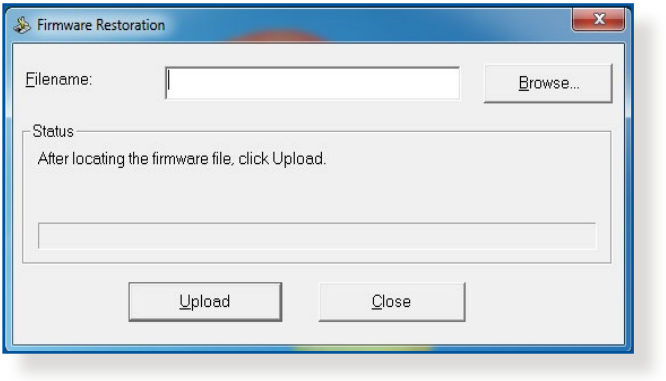
Device Discovery ユーティリティを起動する:

- 「**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。

ご参考: 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。

5.2 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: 192.168.1.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。

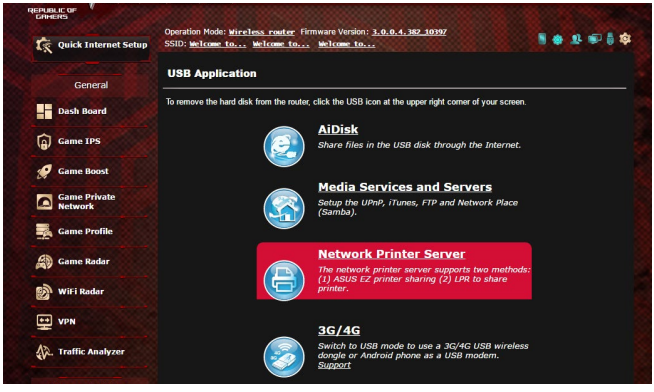
5. ファームウェアファイルを指定し、「**アップロード**」をクリックします。

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。

5.3 プリンターサーバーの設定

5.3.1 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。

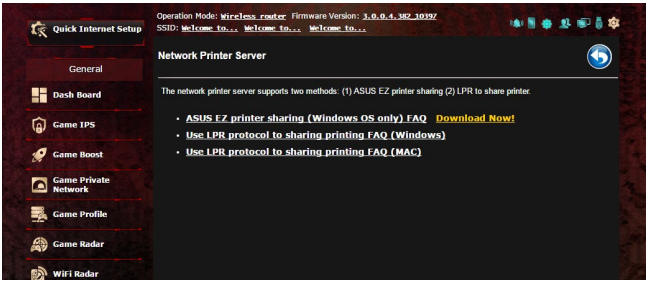


ご参考:

- 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。

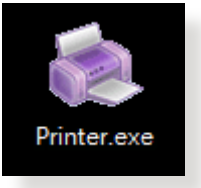
EZ Printer 共有モードのセットアップ

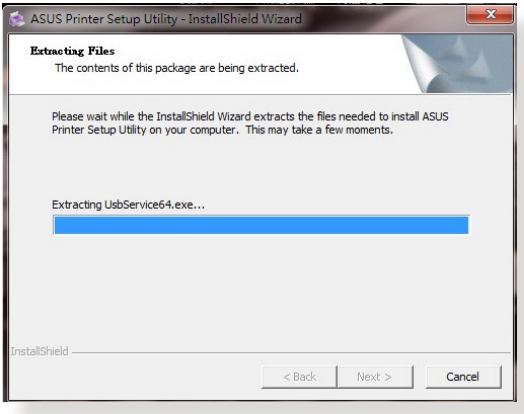
1. 管理画面で「**USBアプリケーション**」→「**ネットワークプリンターサーバー**」の順にクリックします。
2. 「**Download Now!**」をクリックし、Printer Setup Utility をダウンロードします。



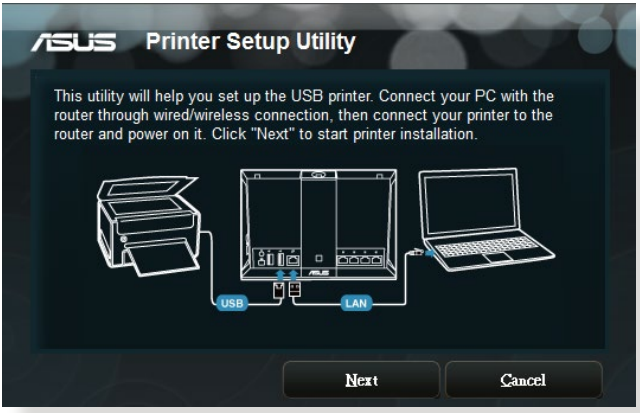
ご参考: LPRプロトコルでプリンターに接続する場合は、手動で設定を行う必要があります。

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。





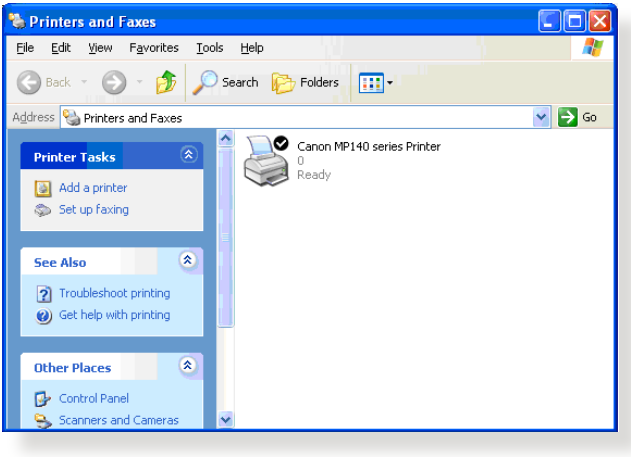
4. Printer Setup Utility によるセットアップウィザードが表示されます。画面に表示される指示に従ってセットアップを行います。



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。



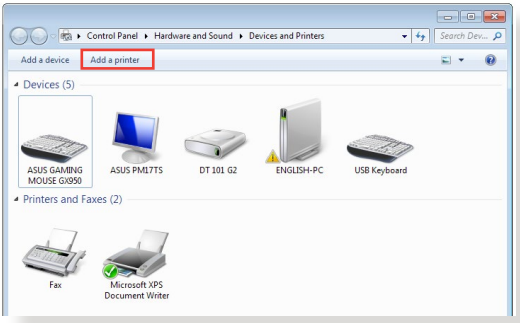
5.3.2 LPRを共有プリンターに使用する

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。

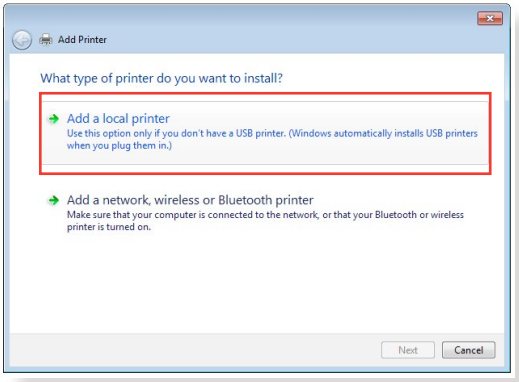
LPRプリンターを共有する （Windows® OS）

手順

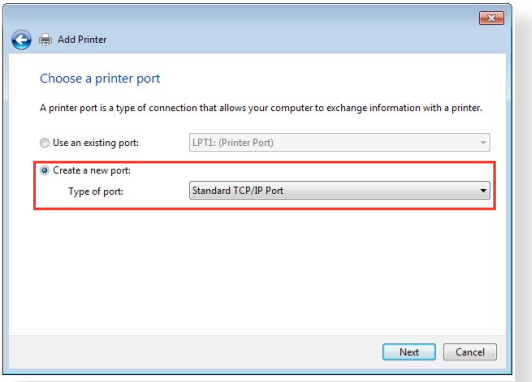
1. 「**スタート**」ボタン→「**コントロールパネル**」→「**ハードウェアとサウンド**」→「**デバイスとプリンター**」の順にクリックし、画面上部の「**プリンターの追加**」をクリックしてウィザードを起動します。



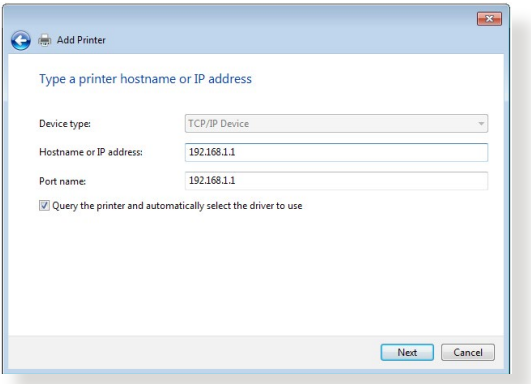
2. 「**ローカルプリンターの追加します**」をクリックします。



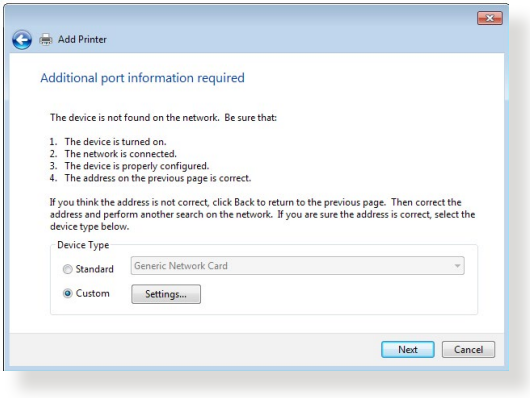
3. 「**新しいポートの作成**」をチェックし、ポートの種類を「**標準の TCP/IP ポート**」に設定し「**次へ**」をクリックします。



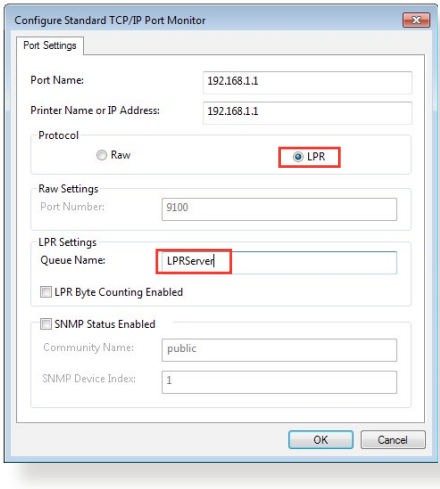
4. 「**ホスト名またはIPアドレス**」に無線LANルーターのIPアドレスを入力し「**次へ**」をクリックします。



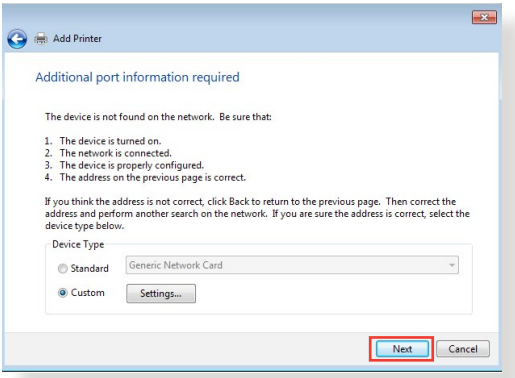
5. デバイスの種類の「**カスタム**」をチェックし、「**設定**」をクリックします。



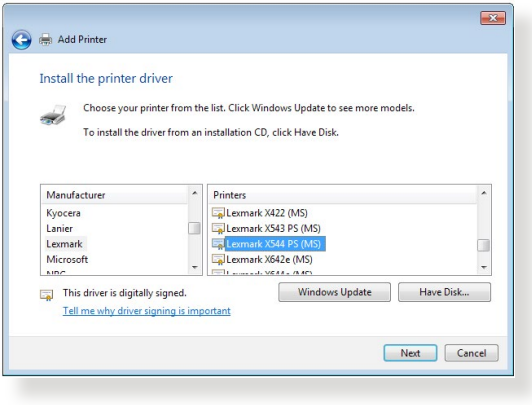
6. プロトコルを「**LPR**」に設定し、LPR設定のキュー名に「**LPRServer**」と入力し「**OK**」をクリックします。



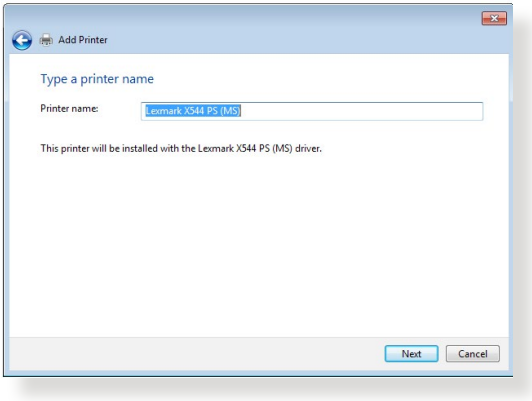
7. 「**次へ**」をクリックし、ドライバーの検出へ進みます。



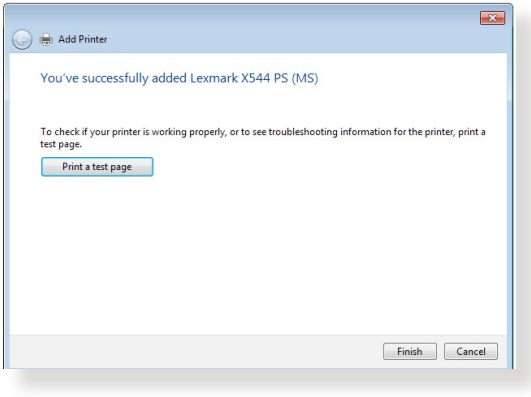
8. 製造元とプリンターを選択して「**次へ**」をクリックし、プリンタードライバーをインストールします。ご使用のプリンターが一覧に表示されない場合は、「**ディスク使用**」または「**Windows Update**」で適切なドライバーを読み込みます。



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。



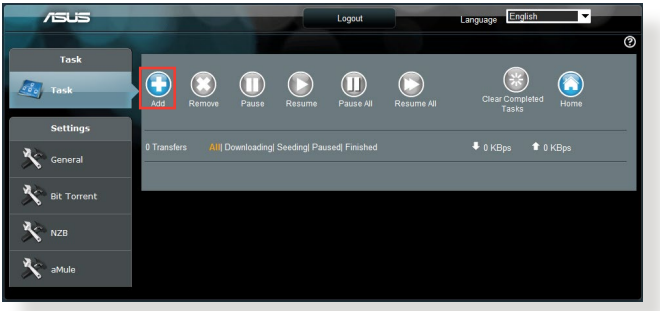
5.4 Download Master

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。

> **ご参考:** 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)

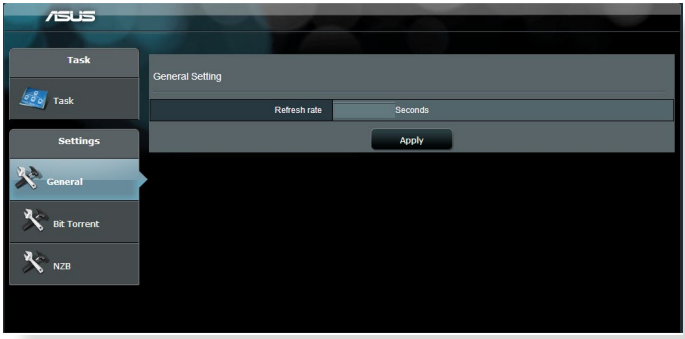
Download Master を使用する

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。



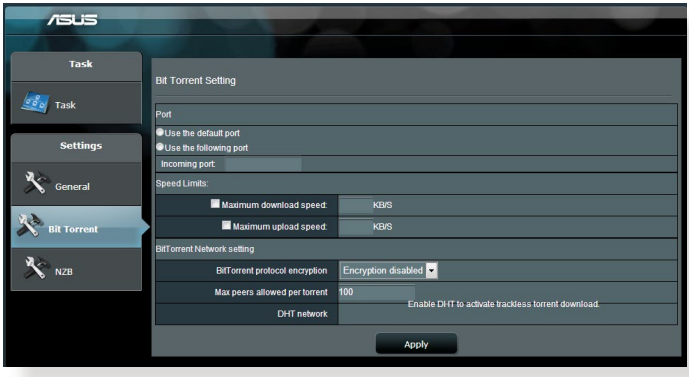
4. 「**ファイルを選択**」をクリックして、「.torrent」ファイル、または「.nzb」ファイルを選択しアップロードします。FTP、HTTP、Magnet Link からダウンロードを行う場合は、URLをコピーし下部入力欄に貼り付けます。

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。



5.4.1 BitTorrent設定

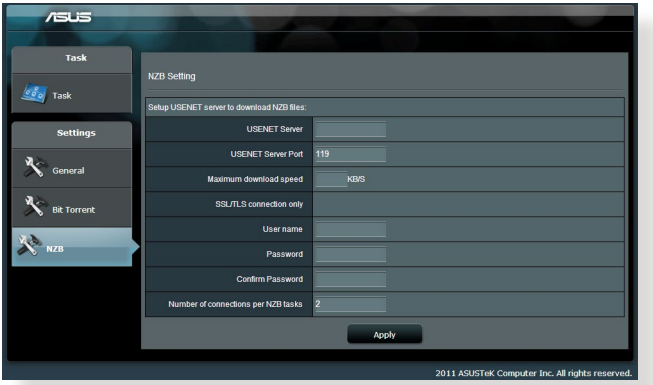
この設定では、BitTorrentを使用したダウンロードとアップロードに使用するポート、最大通信速度、ネットワーク接続設定などを変更することができます。



- **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。

5.4.2 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。



6　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。

6.1　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「**管理者**」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/Networking/ROG-Rapture-GT-AC2900/HelpDesk_BIOS/
3. 「**新しいファームウェアファイル**」の「**参照**」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。

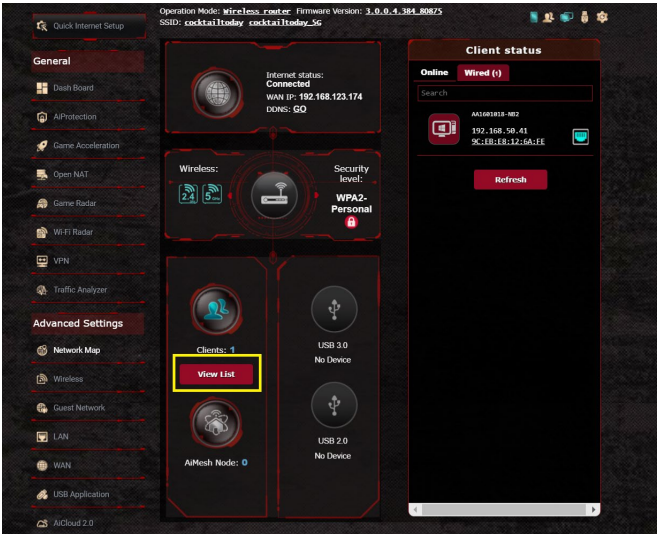
- 本製品とモデム/回線終端装置が正しく接続されている場合、本製品のWAN LEDが点灯します。
- 本製品とコンピューターが正しく接続されている場合、コンピューターの電源が入っている状態で本製品のLAN LEDが点灯します。

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。



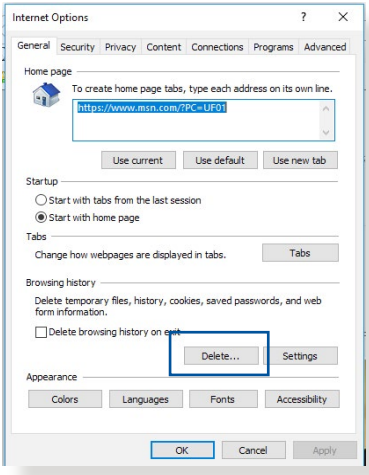
6.2 FAQ (よくある質問)

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、**Temporary Internet files and website files (インターネット一時ファイルおよび Web サイトのファイル)**、および、**Cookies and website data (クッキーと Web サイトのデータ)** を選択して、 次に、**Delete (削除)** をクリックします。



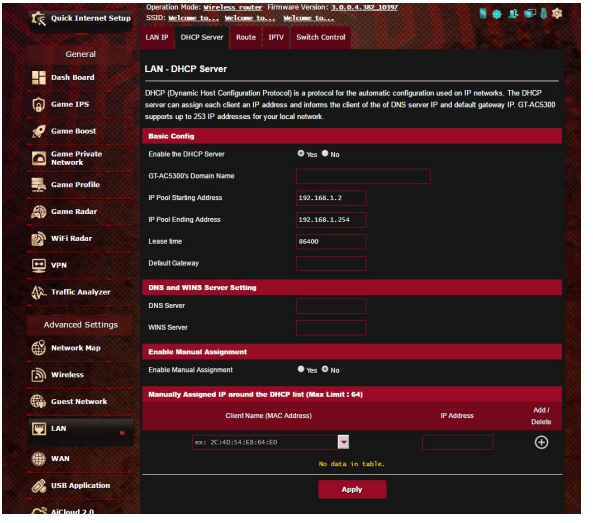
ご参考:

- 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。

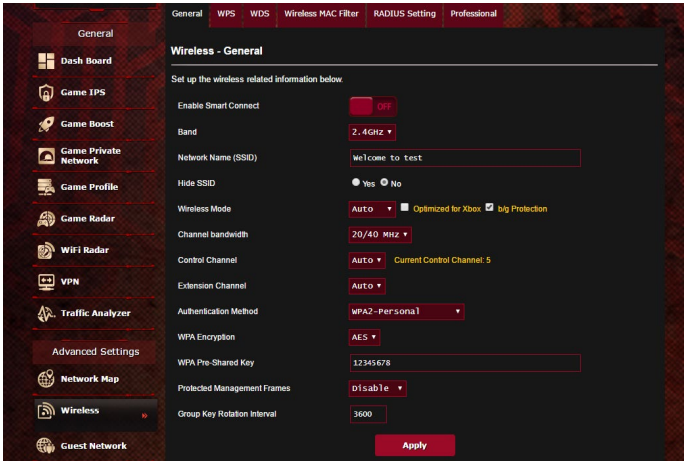
ご注意: 5GHz帯ネットワークに接続できない場合は、ワイヤレスデバイスが5GHzに対応していること、またはデュアルバンド対応であることをご確認ください。

- **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サーバーを有効にしますか**」の「**はい**」をチェックします。



- **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。

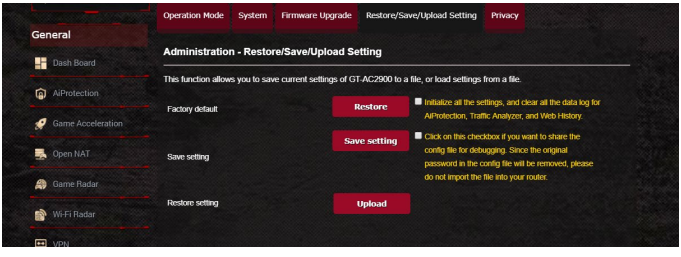


- **通信チャンネルを確認する:**

  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できません。

- **システムを工場出荷時の状態に戻す:**

  本機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「**管理者**」をクリックし、「**復元/保存/アップロード設定**」タブを選択します。「**工場出荷時のデフォルト**」の「**復元**」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「**管理者**」をクリックし、「**復元/保存/アップロード設定**」タブを選択します。「**工場出荷時のデフォルト**」の「**復元**」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「**管理者**」をクリックし、「**復元/保存/アップロード設定**」タブを選択します。「**工場出荷時のデフォルト**」の「**復元**」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
DHCP:	有効 (WANポート接続時)
IPアドレス:	http://router.asus.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:	192.168.1.1
DNSサーバー2:	(空白)
SSID (2.4GHz):	ASUS
SSID (5GHz):	ASUS_5G

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。

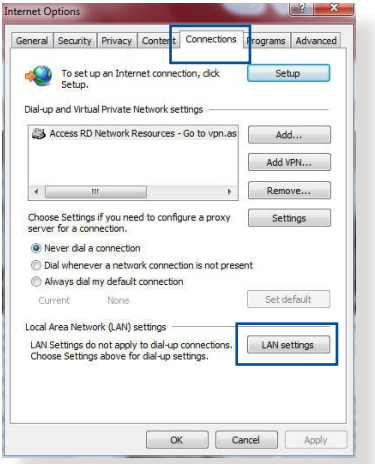
管理画面にアクセスできません。

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。

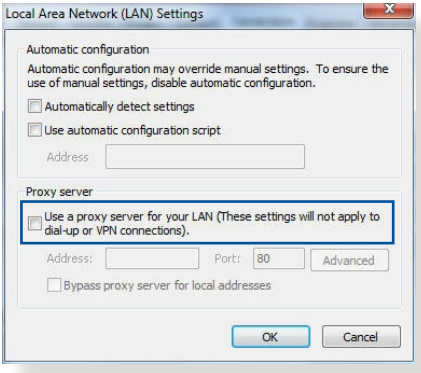
A. プロキシサーバー設定を無効にする

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。

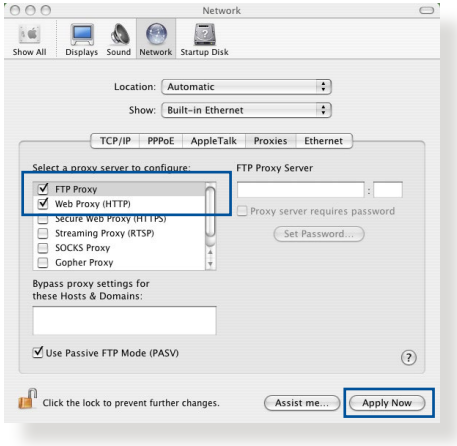


3. 「**LANにプロキシサーバーを使用する**」チェックボックスをオフにします。
4. 変更が終了したら、「**OK**」をクリックしてInternet Explorerに戻ります。



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。



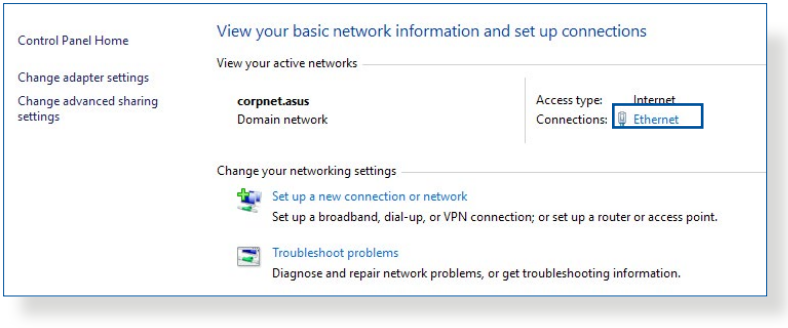
ご参考: 設定方法についてはブラウザーのヘルプも併せてご覧ください。

B. IP アドレスの自動取得を設定する

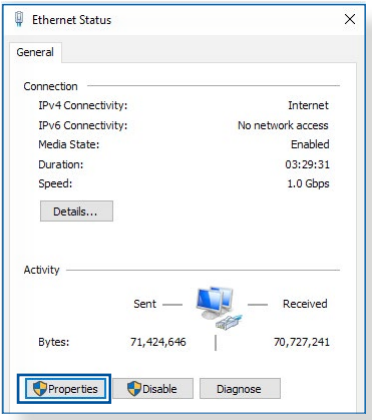
Windows®

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。

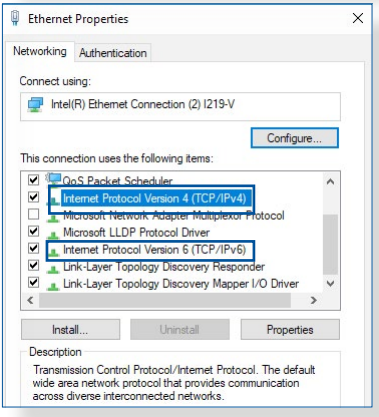
   次に、network connection（ネットワーク接続）をクリックして、ステータスウィンドウを表示します。



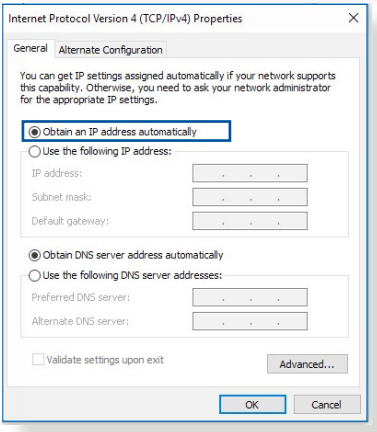
2. **Properties（プロパティ）**をクリックして、Ethernet Properties（イーサネットのプロパティ）画面を表示します。



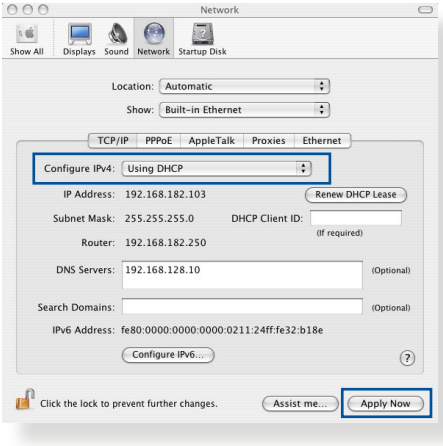
3. 「**ネットワーク**」タブをクリックします。「**この接続は次の項目を使用します**」で「**インターネット プロトコル バージョン 4 (TCP/IPv4)**」または「**インターネット プロトコル バージョン 6 (TCP/IPv6)**」のどちらかをクリックし、「**プロパティ**」をクリックします。



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

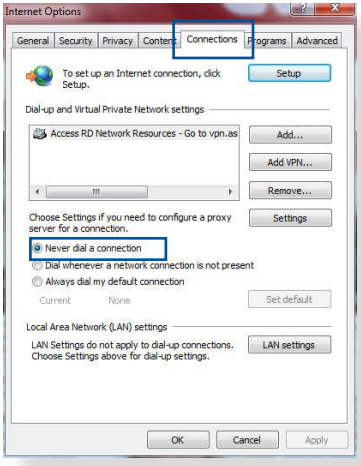


1. をクリックし、アップルメニューを開きます。
2. 「**システム環境設定**」を選択し、インターネットとネットワークの「**ネットワーク**」をクリックします。
3. 現在使用しているネットワークを選択し、「**設定**」をクリックします。
4. 「**TCP/IP**」タブをクリックし、「**IPv4 の設定**」ドロップダウンリストで「**DHCPサーバを参照**」を選択します。
5. 変更が終了したら、「**今すぐ適用**」をクリックして設定を適用します。

ご参考: 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。

ご参考: 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

Notices

回収とリサイクルについて

使用済みのコンピューター、ノートPC等の電子機器には、環境に悪影響を与える有害物質が含まれており、通常のゴミとして廃棄することはできません。リサイクルによって、使用済みの製品に使用されている金属部品、プラスチック部品、各コンポーネントは粉砕され新しい製品に再使用されます。また、その他のコンポーネントや部品、物質も正しく処分・処理されることで、有害物質の拡散の防止となり、環境を保護することに繋がります。

REACH

Complying with the REACH (Registration, Evaluation, Authorisation, and Restriction of Chemicals) regulatory framework, we published the chemical substances in our products at ASUS REACH website at http://csr.asus.com/english/REACH.htm

Federal Communications Commission Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

WARNING! Any changes or modifications not expressly approved by the party responsible for compliance could void the user' s authority to operate the equipment.

Prohibition of Co-location

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

IMPORTANT NOTE:

Radiation Exposure Statement: This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. To maintain compliance with FCC exposure compliance requirement, please follow operation instruction as documented in this manual.

WARNING! This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

Safety Notices

- Use this product in environments with ambient temperatures between 0° C(32° F) and 40° C(104° F).
- Refer to the rating label on the bottom of your product and ensure your power adapter complies with this rating.
- DO NOT place on uneven or unstable work surfaces. Seek servicing if the casing has been damaged.
- DO NOT place or drop objects on top and do not shove any foreign objects into the product.
- DO NOT expose to or use near liquids, rain, or moisture. DO NOT use the modem during electrical storms.
- DO NOT cover the vents on the product to prevent the system from getting overheated.
- DO NOT use damaged power cords, accessories, or other peripherals.
- If the Adapter is broken, do not try to fix it by yourself. Contact a qualified service technician or your retailer.
- To prevent electrical shock hazard, disconnect the power cable from the electrical outlet before relocating the system.

Safety Notices

- Utilisez ce produit dans un environnement dont la température ambiante est comprise entre 0˚C (32° F) et 40˚C (104° F).
- Référez-vous à l'étiquette située au dessous du produit pour vérifier que l'adaptateur secteur répond aux exigences de tension.
- NE PAS placer sur une surface irrégulière ou instable. Contactez le service après-vente si le châssis a été endommagé.
- NE PAS placer, faire tomber ou insérer d'objets sur/dans le produit.
- NE PAS exposer l'appareil à la pluie ou à l'humidité, tenez-le à distance des liquides. NE PAS utiliser le modem lors d'un orage.

- NE PAS bloquer les ouvertures destinées à la ventilation du système pour éviter que celui-ci ne surchauffe.
- NE PAS utiliser de cordons d'alimentation, d'accessoires ou autres périphériques endommagés.
- Si l'adaptateur est endommagé, n'essayez pas de le réparer vous-même. Contactez un technicien électrique qualifié ou votre revendeur.
- Pour éviter tout risque de choc électrique, débranchez le câble d'alimentation de la prise électrique avant de toucher au système.

Radiation Exposure Statement
Déclaration d'exposition aux radiations

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 31cm between the radiator & your body.

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 31cm de distance entre la source de rayonnement et votre corps.

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

(1) This device may not cause interference.

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil contient des émetteurs / récepteurs exempts de licence qui sont conformes au (x) RSS (s) exemptés de licence d'Innovation, Sciences et Développement économique Canada. L'opération est soumise aux deux conditions suivantes:

(1) Cet appareil ne doit pas provoquer d'interférences.

(2) Cet appareil doit accepter toute interférence, y compris les interférences susceptibles de provoquer un fonctionnement indésirable de l'appareil.

This radio transmitter [IC: 3568A-RTHR00] has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Le présent émetteur radio (IC: 3568A-RTHR00) a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal d'antenne. Les types d'antennes non inclus dans cette liste qui ont un gain supérieur au gain maximal indiqué pour tout type listé sont strictement interdits pour une utilisation avec cet appareil.

Set	Ant.	Port				Brand	P/N	Type	Connector	Gain (dBi)			
		2.4 GHz	5GHz B1/B2	5GHz B3	5GHz B4					2.4 GHz	5GHz B1/B2	5GHz B3	5GHz B4
1	1	1	-	4	4	WHA YU	C660-510413-A	Dipole	Reverse SMA Plug	1.9	-	2.3	1.9
	2	2	-	3	3	WHA YU	C660-510413-A	Dipole	Reverse SMA Plug	1.9	-	2.3	1.9
	3	3	-	2	2	WHA YU	C660-510413-A	Dipole	Reverse SMA Plug	1.9	-	2.3	1.9
	4	4	-	1	1	WHA YU	C660-510413-A	Dipole	Reverse SMA Plug	1.9	-	2.3	1.9
	5	-	1	-	-	WHA YU	C660-510413-A	Dipole	Reverse SMA Plug	-	2.3	-	-
	6	-	2	-	-	WHA YU	C660-510413-A	Dipole	Reverse SMA Plug	-	2.3	-	-
	7	-	3	-	-	WHA YU	C660-510413-A	Dipole	Reverse SMA Plug	-	2.3	-	-
	8	-	4	-	-	WHA YU	C660-510413-A	Dipole	Reverse SMA Plug	-	2.3	-	-
2	1	1	-	4	4	WHA YU	C660-510431-A	Dipole	Reverse SMA Plug	1.9	-	2.3	1.9
	2	2	-	3	3	WHA YU	C660-510431-A	Dipole	Reverse SMA Plug	1.9	-	2.3	1.9
	3	3	-	2	2	WHA YU	C660-510431-A	Dipole	Reverse SMA Plug	1.9	-	2.3	1.9
	4	4	-	1	1	WHA YU	C660-510431-A	Dipole	Reverse SMA Plug	1.9	-	2.3	1.9
	5	-	1	-	-	WHA YU	C660-510431-A	Dipole	Reverse SMA Plug	-	2.3	-	-
	6	-	2	-	-	WHA YU	C660-510431-A	Dipole	Reverse SMA Plug	-	2.3	-	-
	7	-	3	-	-	WHA YU	C660-510431-A	Dipole	Reverse SMA Plug	-	2.3	-	-
	8	-	4	-	-	WHA YU	C660-510431-A	Dipole	Reverse SMA Plug	-	2.3	-	-
3	1	1	-	4	4	PSA	RFDPA161000 SBLB801	Dipole	Reverse SMA Plug	1.9	-	2.3	1.9
	2	2	-		3	PSA	RFDPA161000 SBLB801	Dipole	Reverse SMA Plug	1.9	-	2.3	1.9
	3	3	-	2	2	PSA	RFDPA161000 SBLB801	Dipole	Reverse SMA Plug	1.9	-	2.3	1.9
	4	4	-	1	1	PSA	RFDPA161000 SBLB801	Dipole	Reverse SMA Plug	1.9	-	2.3	1.9
	5	-	1	-	-	PSA	RFDPA161000 SBLB801	Dipole	Reverse SMA Plug	-	2.3	-	-
	6	-	2	-	-	PSA	RFDPA161000 SBLB801	Dipole	Reverse SMA Plug	-	2.3	-	-
	7	-	3	-	-	PSA	RFDPA161000 SBLB801	Dipole	Reverse SMA Plug	-	2.3	-	-
	8	-	4	-	-	PSA	RFDPA161000 SBLB801	Dipole	Reverse SMA Plug	-	2.3	-	-

Dynamic Frequency Selection (DFS) for devices operating in the bands 5250- 5350 MHz, 5470-5600 MHz and 5650-5725 MHz.

Sélection dynamique de fréquences (DFS) pour les dispositifs fonctionnant dans les bandes 5250-5350 MHz, 5470-5600 MHz et 5650-5725 MHz.

The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

The maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit.

le gain maximal d'antenne permis pour les dispositifs utilisant les bandes 5250-5350 MHz et 5470-5725 MHz doit se conformer à la limite de p.i.r.e.

The maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate.

le gain maximal d'antenne permis (pour les dispositifs utilisant la bande 5725-5850 MHz) doit se conformer à la limite de p.i.r.e. spécifiée pour l'exploitation point à point et non point à point, selon le cas.

For indoor use only.

Pour une utilisation en intérieur uniquement.

IMPORTANT NOTE:

IC Radiation Exposure Statement:

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 31cm between the radiator & your body.

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 31 cm de distance entre la source de rayonnement et votre corps.

VCCI: Japan Compliance Statement

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラス B 情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、ラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱をして下さい。

5.3GHz 帯 *W53 (5,250-5,350MHz) は屋内利用に限定されています。

KC: Korea Warning Statement

B급 기기 (가정용 방송통신기자재)	이 기기는 가정용(B급)으로 전자파적합등록을 한 기기로서 주로 가정에서 사용하는 것을 목적으로 하며, 모든 지역에서 사용할 수 있습니다.
Class B equipment **(For Home Use Broadcasting & Communication Equipment)**	This equipment is home use (Class B) electromagnetic wave suitability and to be used mainly at home and it can be used in all areas.

NCC 警語

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電通信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

「產品之限用物質含有情況」之相關資訊，請參考下表：

單元	限用物質及其化學符號					
	鉛 (Pb)	汞 (Hg)	鎘 (Cd)	六價鉻 (Cr^{+6})	多溴聯苯 (PBB)	多溴二苯醚 (PBDE)
印刷電路板及電子組件	-	○	○	○	○	○
結構組件（金屬 / 塑膠）	○	○	○	○	○	○
其他組件（如天線/ 指示燈/連接線）	○	○	○	○	○	○
其他及其配件（如電源供應器）	-	○	○	○	○	○
備考1.“○”係指該項限用物質之百分比含量未超出百分比含量基準值。 備考2.“-”係指該項限用物質為排除項目。						

DFS 警語

操作在5.15~5.35/5.47~5.85GHz之無線資訊傳輸設備(802.11a/ac產品)，應避免影響附近雷達系統之操作。

MPE

本產品電磁波曝露量(MPE)標準值1mW/cm^2，送測產品實測值為XXXmW/cm^2，建議使用時至少距離人體XXcm。

安全說明：

- 請在溫度為 0° C (32° F) 至 40° C (104° F) 之間的環境中使用本產品。
- 請依照產品上的電源功率貼紙說明使用正確的電源變壓器，如果使用錯誤規格的電源變壓器有可能會造成內部零件的損毀。
- 請勿將產品放置於不平坦或不穩定的表面，若產品的機殼毀損，請聯絡維修服務人員。
- 請勿在產品上放置其他物品，請勿將任何物品塞入產品內，以避免引起元件短路或電路損毀。
- 請保持機器在乾燥的環境下使用，雨水、溼氣、液體等含有礦物質將會腐蝕電子線路，請勿在雷電天氣下使用數據機。
- 請勿堵塞產品的通風孔，以避免因散熱不良而導致系統過熱。
- 請勿使用破損的電源線、附件或其他周邊產品。
- 如果電源已毀損，請不要嘗試自行修復，請將其交給專業技術服務人員或經銷商來處理。
- 為了防止電擊風險，在搬動主機之前，請先將電源線插頭暫時從電源插座上拔除。

电子电气产品有害物质限制使用标识要求：图中之数字为产品之环保使用期限。仅指电子电气产品中含有的有害物质不致发生外泄或突变从而对环境造成污染或对人身、财产造成严重损害的期限。

产品中有害物质的名称及含量

部件名称	有害物质					
	铅 (Pb)	汞(Hg)	镉(Cd)	六价铬 (Cr(VI))	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
印刷电路板及其电子组件	×	○	○	○	○	○
外壳	○	○	○	○	○	○
电源适配器	×	○	○	○	○	○
外部信号连接头及线材	×	○	○	○	○	○
中央处理器与内存	×	○	○	○	○	○

本表格依据 SJ/T 11364 的规定编制。

○：表示该有害物质在该部件所有均质材料中的含量均在 GB/T 26572 规定的限量要求以下。

×：表示该有害物质至少在该部件的某一均质材料中的含量超出 GB/T 26572 规定的限量要求，然该部件仍符合欧盟指令 2011/65/EU 的规范。

备注：此产品所标示之环保使用期限，系指在一般正常使用状况下。

安全说明：

- 请在温度为 0° C (32° F) 至 40° C (104° F)之间的环境中使用本产品。
- 请依照产品上的电源功率贴纸说明使用正确的电源适配器，如果试用错误规格的电源适配器可能会造成内部零件的损坏。
- 请勿将产品放置于不平坦或不稳定的表面，若产品的外壳损坏，请联系维修服务人员。
- 请勿在产品上放置其他物品，请勿将任何物品塞入产品内，以避免引起组件短路或电路损坏。
- 请保持机器在干燥的环境下使用，雨水、湿气、液体等含有矿物质会腐蚀电子线路，请勿在雷电天气下使用调制解调器。
- 请勿堵塞产品的通风孔，以避免因散热不良而导致系统过热。
- 请勿使用破损的电源线、附件或其他周边产品。
- 如果电源已损坏，请不要尝试自行修复，请将其交给专业技术服务人员或经销商来处理。
- 为了防止电击风险，在搬动主机前，请先将电源线插头暂时从电源插座上拔除。

UA.TR.028

Precautions for the use of the device

a. Pay particular attention to the personal safety when use this device in airports, hospitals, gas stations and professional garages.

b. Medical device interference: Maintain a minimum distance of at least 15 cm (6 inches) between implanted medical devices and ASUS products in order to reduce the risk of interference.

c. Kindly use ASUS products in good reception conditions in order to minimize the radiation's level.

d. Keep the device away from pregnant women and the lower abdomen of the teenager.

Précautions d'emploi de l'appareil

a. Soyez particulièrement vigilant quant à votre sécurité lors de l'utilisation de cet appareil dans certains lieux (les avions, les aéroports, les hôpitaux, les stations-service et les garages professionnels).

b. Évitez d'utiliser cet appareil à proximité de dispositifs médicaux implantés. Si vous portez un implant électronique (stimulateurs cardiaques, pompes à insuline, neurostimulateurs…),veuillez impérativement respecter une distance minimale de 15 centimètres entre cet appareil et votre corps pour réduire les risques d'interférence.

c. Utilisez cet appareil dans de bonnes conditions de réception pour minimiser le niveau de rayonnement. Ce n'est pas toujours le cas dans certaines zones ou situations, notamment dans les parkings souterrains, dans les ascenseurs, en train ou en voiture ou tout simplement dans un secteur mal couvert par le réseau.

d. Tenez cet appareil à distance des femmes enceintes et du bas-ventre des adolescents.

Условия эксплуатации:

- Температура эксплуатации устройства: 0-40 °C. Не используйте устройство в условиях экстремально высоких или низких температур.
- Не размещайте устройство вблизи источников тепла, например, рядом с микроволновой печью, духовым шкафом или радиатором.
- Использование несовместимого или несертифицированного адаптера питания может привести к возгоранию, взрыву и прочим опасным последствиям.
- При подключении к сети электропитания устройство следует располагать близко к розетке, к ней должен осуществляться беспрепятственный доступ.
- Утилизация устройства осуществляется в соответствии с местными законами и положениями. Устройство по окончании срока службы должны быть переданы в сертифицированный пункт сбора для вторичной переработки или правильной утилизации.
- Данное устройство не предназначено для детей. Дети могут пользоваться устройством только в присутствии взрослых.
- Не выбрасывайте устройство и его комплектующие вместе с обычными бытовыми отходами.

EAC

India RoHS

This product complies with the "India E-Waste (Management) Rules, 2016" and prohibits use of lead, mercury, hexavalent chromium, polybrominated biphenyls(PBBs) and polybrominated diphenyl ethers (PBDEs) in concentrations exceeding 0.1 % by weight in homogenous materials and 0.01 % by weight in homogenous materials for cadmium, except for the exemptions listed in Schedule II of the Rule.

הוראות בטיחות לשימוש במוצר

יש לפעול ע"פ כללי הבטיחות הבאים בעת שימוש במוצר:

- ודא שלמות ותקינות התקע ו/או כבל החשמל.
- אין להכניס או להוציא את התקע מרשת החשמל בידיים רטובות.
- באם המוצר מופעל ע"י מטען חיצוני, אין לפתוח את המטען, במקרה של בעיה כלשהי, יש לפנות למעבדת השירות הקרובה.
- יש להרחיק את המוצר והמטען מנוזלים.
- במקרה של ריח מוזר, רעשים שמקורם במוצר ו/או במטען/ספק כוח, יש לנתקו מיידית מרשת החשמל ולפנות למעבדת שירות.
- המוצר והמטען/ספק כוח מיועד לשימוש בתוך המבנה בלבד, לא לשימוש חיצוני ולא לשימוש בסביבה לחה.
- אין לחתוך, לשבור, ולעקם את כבל החשמל.
- אין להניח חפצים על כבל החשמל או להניח לו להתחמם יתר על המידה, שכן הדבר עלול לגרום לנזק, דליקה או התחשמלות.
- לפני ניקוי המוצר ו/או המטען יש לנתקו מרשת החשמל.
- יש לאפשר גישה נוחה לחיבור וניתוק פתיל הזינה מרשת החשמל
- יש להקפיד ולתחזק את התקן הניתוק במצב תפעולי מוכן לשימוש

אזהרה:

- אין להחליף את כבל הזינה בתחליפים לא מקוריים, חיבור לקוי עלול לגרום להתחשמלות המשתמש.
- בשימוש על כבל מאריך יש לוודא תקינות מוליך הארקה שבכבל.

AEEE Yönetmeliğine Uygundur. IEEE Yönetmeliğine Uygundur.

- Bu Cihaz Türkiye analog şebekelerde çalışabilecek şekilde tasarlanmıştır.
- Cihazın ayrıntılı kurulum rehberi kutu içeriğinden çıkan CD içerisindedir. Cihazın kullanıcı arayüzü Türkçe'dir.
- Cihazın kullanılması planlanan ülkelerde herhangi bir kısıtlaması yoktur. Ülkeler simgeler halinde kutu üzerinde belirtilmiştir.

Manufacturer	ASUSTeK Computer Inc. Tel: +886-2-2894-3447 Address: 4F, No. 150, LI-TE RD., PEITOU, TAIPEI 112, TAIWAN
Authorised representative in Europe	ASUS Computer GmbH Address: HARKORT STR. 21-23, 40880 RATINGEN, GERMANY
Authorised distributors in Turkey	BOGAZICI BILGISAYAR TICARET VE SANAYI A.S. Tel./FAX No.: +90 212 331 10 00 / +90 212 332 28 90 Address: ESENTEPE MAH. BUYUKDERE CAD. ERCAN HAN B BLOK NO.121 SISLI, ISTANBUL 34394
	CIZGI Elektronik San. Tic. Ltd. Sti. Tel./FAX No.: +90 212 356 70 70 / +90 212 356 70 69 Address: GURSEL MAH. AKMAN SK.47B 1 KAGITHANE/ ISTANBUL
	KOYUNCU ELEKTRONiK BiLGi iSLEM SiST. SAN. VE DIS TIC. A.S. Tel. No.: +90 216 5288888 Address: EMEK MAH.ORDU CAD. NO:18, SARIGAZi, SANCAKTEPE ISTANBUL
	ENDEKS BİLİŞİM SAN VE DIŞ TİC LTD ŞTİ Tel./FAX No.: +90 216 523 35 70 / +90 216 523 35 71 Address: NECIP FAZIL BULVARI, KEYAP CARSI SITESI, G1 BLOK, NO:115 Y.DUDULLU, UMRANIYE, ISTANBUL
	PENTA TEKNOLOJI URUNLERI DAGITIM TICARET A.S Tel./FAX No.: +90 216 528 0000 Address: ORGANIZE SANAYI BOLGESI NATO YOLU 4.CADDE NO:1 UMRANIYE, ISTANBUL 34775

ASUSコンタクトインフォメーション

ASUSTeK COMPUTER INC. (アジア太平洋)

住所	15 Li-Te Road, Peitou, Taipei, Taiwan 11259
Web サイト	http://www.asus.com/tw/

テクニカルサポート

電話	+886228943447
サポートファックス	+886228907698
オンラインサポート	https://www.asus.com/support

ASUSコールセンター (日本)

電話	0800-123-2787 (通話料無料)
受付時間	年中無休/ 9:00～19:00 (年末年始は受付時間が変更となります。詳細は弊社Webサイトでご確認ください)
Web サイト	https://www.asus.com/jp/support

※ 携帯電話、PHS、公衆電話からは0570-783-886 (通話料はお客様負担)

ご参考: グローバールサービスセンターの所在地等につきましては、弊社サポートサイトをご確認ください。
(http://www.asus.com/support)

Ma nufacturer:	ASUSTeK Computer Inc.	
	Tel:	+886-2-2894-3447
	Address:	4F, No. 150, LI-TE RD., PEITOU, TAIPEI 112, TAIWAN
Authorised representative in Europe:	ASUS Computer GmbH	
	Address:	HARKORT STR. 21-23, 40880 RATINGEN, GERMANY

English

CE statement

Simplified EU Declaration of Conformity

ASUSTek Computer Inc. hereby declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU. Full text of EU declaration of conformity is available at https://www.asus.com/Networking/ROG-Rapture-GT-AC2900/HelpDesk_Declaration/.

Declaration of Conformity for Ecodesign directive 2009/125/EC

Testing for eco-design requirements according to (EC) No 1275/2008 and (EU) No 801/2013 has been conducted. When the device is in Networked Standby Mode, its I/O and network interface are in sleep mode and may not work properly. To wake up the device, press the Wi-Fi on/off, LED on/off, reset, or WPS button.

This equipment complies with EU radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

All operational modes:

2.4GHz: 802.11b, 802.11g, 802.11n (HT20), 802.11n (HT40), 802.11ac (VHT20), 802.11ac (VHT40)

5GHz: 802.11a, 802.11n (HT20), 802.11n (HT40), 802.11ac (VHT20), 802.11ac (VHT40), 802.11ac (VHT80)

The frequency, mode and the maximum transmitted power in EU are listed below:

2412-2472MHz (802.11g 6Mbps): 19.81 dBm

5180-5240MHz (802.11ac VHT20 MCSO): 20.1 dBm

5260-5320MHz (802.11ac VHT40 MCSO): 21.31 dBm

5500-5700MHz (802.11ac VHT80 MCSO): 27.48 dBm

The device is restricted to indoor use only when operating in the 5150 to 5350 MHz frequency range.

The adapter shall be installed near the equipment and shall be easily accessible.

	AT	BE	BG	CZ	DK	EE	FR
	DE	IS	IE	IT	EL	ES	CY
	LV	LI	LT	LU	HU	MT	NL
	NO	PL	PT	RO	SI	SK	TR
	FI	SE	CH	UK	HR		

Safety Notices

- Use this product in environments with ambient temperatures between 0° C(32° F) and 40° C(104° F).
- Refer to the rating label on the bottom of your product and ensure your power adapter complies with this rating.
- DO NOT place on uneven or unstable work surfaces. Seek servicing if the casing has been damaged.
- DO NOT place or drop objects on top and do not shove any foreign objects into the product.
- DO NOT expose to or use near liquids, rain, or moisture. DO NOT use the modem during electrical storms.
- DO NOT cover the vents on the product to prevent the system from getting overheated.
- DO NOT use damaged power cords, accessories, or other peripherals.
- If the Adapter is broken, do not try to fix it by yourself. Contact a qualified service technician or your retailer.
- To prevent electrical shock hazard, disconnect the power cable from the electrical outlet before relocating the system.
- DO NOT mount this equipment higher than 2 meters.