J22389

TUF GAMING





J22389 初版 V1 2023年10月

Copyright © 2023 ASUSTeK COMPUTER INC. All Rights Reserved.

本書およびそれに付属する製品は著作権法により保護されており、その使用、複製、頒布および逆コンパイルを制限するライセンスのもとにおいて頒布されます。 購入者によるバックアップ目的の場合を除き、ASUSTeK Computer Inc. (以下、 ASUS)の書面による事前の許可なく、本製品および本書のいかなる部分も、い かなる方法によっても複製することが禁じられます。

以下に該当する場合は、製品保証サービスを受けることができません。

(1) 製品に対しASUSの書面により認定された以外の修理、改造、改変が行われた場合

(2) 製品のシリアル番号の確認ができない場合

本書は情報提供のみを目的としています。本書の情報の完全性および正確性については最善の努力が払われていますが、本書の内容は「現状のまま」で提供されるものであり、ASUSは明示または黙示を問わず、本書においていかなる保証も行ないません。ASUS、その提携会社、従業員、取締役、役員、代理店、ベンダーまたはサプライヤーは、本製品の使用または使用不能から生じた付随的な損害

(データの変化・消失、事業利益の損失、事業の中断など)に対して、たとえASUS がその損害の可能性について知らされていた場合も、一切責任を負いません。

本書に記載している会社名、製品名は、各社の商標または登録商標です。本書で は説明の便宜のためにその会社名、製品名などを記載する場合がありますが、 それらの商標権の侵害を行なう意思、目的はありません。

もくじ

1 製品の概要

1.1	はじめに	7
1.2	パッケージ内容	7
1.3	各部の名称	8
1.4	無線LANルーターの設置	
1.5	ご使用になる前に	11
2	セットアップ	
2.1		
	A. 有線接続	
	B. 無線接続	
2.2	クイックインターネットセットアップ (QIS)	16
2.3	ワイヤレスネットワークに接続する	19
3	一般設定と詳細設定の構成	
3.1	管理画面にログインする	
3.2	アダプティブ 〇へ	22
		···· ∠ ∠
3.3	*************************************	
3.3	アメアノアイン Q05<管理3.3.1 動作モード	
3.3	管理 3.3.1 動作モード 3.3.2 システム	23 23 23 24
3.3	管理 3.3.1 動作モード 3.3.2 システム 3.3.3 ファームウェア更新	
3.3	 管理 3.3.1 動作モード 3.3.2 システム 3.3.3 ファームウェア更新 3.3.4 リセット/保存/復元設定 	
3.3 3.4	管理 3.3.1 動作モード 3.3.2 システム 3.3.3 ファームウェア更新 3.3.4 リセット/保存/復元設定 AiCloud 2.0	
3.3 3.4	 管理	23 23 24 25 25 26 26 27
3.3 3.4	 管理	23 23 24 25 25 25 26 26 27 29
3.3 3.4	 管理	23 23 24 25 25 25 25 26 27 27 29 30
 3.3 3.4 3.5 	 管理	22 23 24 24 25 25 25 26 27 29 30 31
 3.3 3.4 3.5 	 管理	23 23 24 25 25 25 25 26 27 29 30 30 31 31

3.5.3 トラブルシューティング	
3.5.4 再配置	
3.5.5 AQ(よくあるご質問)	
AiProtection	
3.6.1 AiProtectionの設定	
3.6.2 悪質サイトブロック	40
3.6.3 脆弱性保護	
3.6.4 感染デバイス検出/ブロック	42
ファイアウォール	43
3.7.1 全般設定	43
3.7.2 URLフィルター	44
3.7.3 キーワードフィルター	45
3.7.4 パケットフィルター	46
Game	47
3.8.1 ゲームブースト	48
3.8.2 Open NAT	49
ゲストネットワークを構築する	50
IPv6	52
LAN	53
3.11.1 LAN IP	
3.11.2 DHCPサーバー	54
3.11.3 ルーティングテーブル	
3.11.4 IPTV	57
ネットワークマップを使用する	
3.12.1 セキュリティのセットアップ	
3.12.2 ネットワーククライアントの管理	60
3.12.3 USBデバイスの管理	61
	 3.5.3 トラブルシューティング

3.13	ペアレンタルコントロール	63
4.14	スマートコネクト	66
	4.14.1 スマートコネクトのセットアップ	66
3.15	システムログ	67
3.16	トラフィックアナライザー	68
3.17	USBアプリケーション	69
	3.17.1 AiDiskを使用する	70
	3.17.2 サーバーセンターを使用する	72
	3.17.3 3G/4G	77
3.18	VPN	79
	3.18.1 VPN サーバー	79
	3.18.2 VPN Fusion (VPN フュージョン)	80
	3.18.3 Instant Guard (インスタントガード)	82
3.19	WAN	83
	3.19.1 インターネット接続	
	3.19.2 デュアル WAN	86
	3.19.3 ポートトリガー	
	3.19.4 ポートフォワーディング	
	3.19.5 DMZ	92
	3.19.6 DDNS	92
	3.19.7 NATパススルー	94
3.20	ワイヤレス	95
	3.20.1 全般設定	95
	3.20.2 WPS	97
	3.20.3 ブリッジ	
	3.20.4 MACアドレスフィルタリング	101
	3.20.5 RADIUS	102
	3.20.6 ワイヤレス - 詳細	

4 ユーティリティ

4.1	Device Discovery	
4.2	Firmware Restoration (ファームウェアの復元)	
4.3	プリンターサーバーの設定	
	4.3.1 ASUS EZ Printer Sharing	
	4.3.2 LPRを共有プリンターに使用する	113
4.4	Download Master	118
	4.4.1 BitTorrent設定	119
	4.4.2 NZB設定	
-		
5	トフノルシューティンク	101
ור		1/1

J.1	本本的なレンフルン	
5.2	FAQ (よくある質問)	

付録

サービスとサポート	 142



1.1 はじめに

この度はASUS製品をお買い上げいただき、誠にありがとうございます。

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

1.2 パッケージ内容

- ☑ TUF Gaming Wireless Router 図 電源アダプター 本体
- ☑ LANケーブル

☑ かんたんセットアップガイド

ご注意:

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

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



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

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

ご注意:

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

・ 仕様:

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

1.4 無線LANルーターの設置

本製品を利用する際は、次のことに注意して設置してください。

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



1.5 ご使用になる前に

本製品をご使用になる前に、次のことをご確認ください。

回線契約とインターネットサービスプロバイダー (ISP) の加入

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

設定を行なうために必要なコンピューターの要件

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

ご注意:

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

重要!

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

connectivity-and-networking/broadband-Wi-Fi

Intel: <u>https://downloadcenter.intel.com/</u>

2 セットアップ

2.1 無線LANルーターのセットアップ

重要:

- セットアップ中の通信エラーなどによる問題を回避するために、有 線接続でセットアップを行なうことをお勧めします。
- ・ 無線LANルーターのセットアップを開始する前に、次の操作を行 なってください。
- 既存のルーターと交換を行なう場合は、現在実行されているすべての通信を停止します。
- モデム/回線終端装置とコンピューターに接続されたLANケーブ ルを取り外します。モデム/回線終端装置がバックアップ用バッテ リーを搭載している場合は、バッテリーを一旦取り外します。
- モデム/回線終端装置とコンピューターを再起動します。(推奨)

A. 有線接続

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

接続方法

 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。

Currently connected ASUS router Internet acce	ito: 47	* III
Wireless Network Co	onnection ^	
ARIES_RT-N66U	Connected	
ASUS Ariel 2G	line.	
ASUS_XX_2G	lite.	
	Connect	
Alen_Private	lite	
ASUSPM-Public	lite.	
ALIGU_87U_2G	Itee	
ASUS hm66 2G	at.	Ŧ
Open Network a	and Sharing Center	

Wi-Fi名(SSID): ASUS_XX

- * 「XX」は2.4GHz MACアドレスの最後の2桁になり ます。ルーター背面のラベルルに記載があります。
- * Wi-Fi接続にパスワードが必要になる場合がござい ます。パスワードは本体底面のラベルに記載があり ます。
- * ルーターの背面にあるQRコードをスキャンするこ とで、簡単にWi-Fi接続することができます。

ご注意:

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

2.2 クイックインターネットセットアップ (QIS)

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

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

クイックインターネットセットアップを使用する

 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 「<u>http://www.asusrouter.com</u>」または「192.168.50.1」を入力 してWebのセットアップ画面にアクセスします。



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

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

注記:

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





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

Assign a unique name or SSID (Ser identify your wireless network.	vice Set Identifier) to help	
2.4 GHz Network Name (SSID)		
2.4 GHz Wireless Security		ø
5 GHz Network Name (SSID)		
	Alle M	
5 GHz Wireless Security		Q
Separate 2.4 GHz and 5 GHz		
i illilli i illilli i	all aller all	

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

TUF GAMING		
LOGIN USERNAME / PASSHORD	Change the router password to proyour ASUS wireless router.	event unauthorized access to
SETTINGS	Router Login Name	
	New password	
	Retype Password	
	PREVIOUS	NEXT

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

2.3 ワイヤレスネットワークに接続する

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

コンピューターでワイヤレスネットワークに接続する

- 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。
- 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。
- 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 M が変わり 通信可能な状態になります。

ご注意:

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

3 一般設定と詳細設定の構成

3.1 管理画面にログインする

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

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

管理画面にログインする:

- Webブラウザーのアドレス欄に「<u>http://www.asusrouter.com</u>」 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。

LQGI) USERNAME / PASSHOR	Change the router password to provide your ASUS wireless router.	event unauthorized	d access to
	s Router Login Name		
	N		
	New password		8
	Retype Password		

3. ログインに成功すると管理画面が表示されます。



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

3.2 アダプティブ QoS

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



QoS機能を有効にする

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

注記: QoS タイプの定義については、QoS タブを参照してください。

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

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

5. 「適用」をクリックします。

3.3 管理

3.3.1 動作モード

動作モードでは、本製品の動作モードを簡単に切り替えることが できます。



動作モードのセットアップ

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

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

3.3.2 システム

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

手順

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

ご注意:動作モードを変更するには、無線LANルーターの再起動が必要です。

3.3.3 ファームウェア更新

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

ファイルからファームウェアを更新:

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

ご注意:

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

3.3.4 リセット/保存/復元設定

無線LANルーターの設定の保存とアップロード

- 1. 「管理」をクリックし、「リセット/保存/復元設定」 タブを選択します。
- 2. 実行するタスクを選択します:
 - 工場出荷時の状態にリセット 無線LANルーターのシステムを工場出荷時の状態に戻します。
 - ・設定をファイルに保存 現在の無線LANルーターの設定をファイルとして保存します。
 - 設定をファイルから復元

「設定をファイルに保存」で作成したファイルから、システム 設定を復元します。「参照」ボタンをクリックし、コンピュータ ーに保存した設定ファイルを指定します。

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

3.4 AiCloud 2.0

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

AiCloud 2.0	the filler of the second s			
ASUS AiCloud 2.0 keeps you conni links your home network and online app on your iOS or Android mobile can go where you go.	ected to your data wherever ar storage service and lets you a device or through a personaliz	id whenever you have an Internet connection iccess your data through the AiCloud mobile ed web link in a web browser. Now all your da	. It ata	
Enter AiCloud 2.0 <u>https://www.asusrouter.com</u>				
Find FAQs GO		Available on the Plane		
The wireless router is currently using This router may be in a multiple-NAT	a private WAN IP address. environment, and accessing AIC Enables USB-attached st streamed or shared throu or device.	loud from WAN does not work. orage devices to be accessed, gh an Internet-connected PC		
Smart Access	Enables Network Place (Samba) networked PCs and devices to be accessed remotely. Smart Access can also wake up a sleeping PC.			
KBCloud Sync	Enables synchronization cloud services like <u>ASUS</u> AiCloud 2.0-enabled netw	of USB-attached storage with <u>Webstorage</u> and other <u>GO</u> ovrks.		

AiCloudを使用する

- 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。
- ASUS AiCloudアプリをインストールしたスマートデバイスを本 機のワイヤレスネットワークに接続します。次にASUS AiCloud アプリを起動し、画面の指示に従ってセットアップを行います。

3.4.1 Cloud Disk

Cloud Diskを作成する

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



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



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

- 4. 本機のUSBポートに接続したUSBストレージデバイスにアクセス することができます。
 - ご注意: セキュリティ対策上、AiCloudではログイン情報を保存することはできません。



ご注意:本書で使用されているイラストや画面は実際とは異なる場合があります。

3.4.2 Smart Access

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



ご注意:

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

https://<ドメイン名>.asuscomm.com

3.4.3 AiCloud Sync

Cloud 2.0 Aid	Cloud Sync	Sync Server	Settings	Log	llfter Samer 12	•5) 		
USB¶'-(_	<u>ی</u>	Enables FAQ	AiCloud Syr	c functionality. Fo	r step-by-step ir	nstructions,	go to
Cloud List Provider	Usen	name	Rule	No data in ta	Folder Name	Conner	ction Status	Delete

AiCloud Syncを使用する

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

3.5 AiMesh

3.5.1 設定する前に

AiMesh Wi-Fi システムをセットアップする準備

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

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



3.5.2 AiMesh セットアップ手順

準備

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

AiMesh ノード

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



AiMesh ルーター

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



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

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



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

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



4) 同期化が完了すると、メッセージが表示されます。



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



3.5.3 トラブルシューティング

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

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



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



3.5.4 再配置

最適なパフォーマンス:

AiMesh ノードとルーターを最適な場所に設置します。

注記:

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



3.5.5 FAQ (よくあるご質問)

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

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

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

- 回答: はい。AiMesh システムは、AiMesh ルーターとノードの無線接続および有線接続の両方に対応して、スループットと安定性を最大化します。AiMesh は、使用できるそれぞれの周波数帯域の無線信号強度を分析し、無線接続または有線接続のどちらがルーター間接続バックボーンとして最も適しているかを自動的に決定します。
- 1) セットアップ手順に従って、まず、Wi-Fi 経由で AiMesh ルーター とノードの接続を確立します。
- 2) ノードを最適な場所に設置して、最良のカバレッジにしま す。 イーサネットケーブルを AiMesh ルーター の LAN ポー トから AiMesh ノードの WAN ノードに配線します。



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

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



3.6.1 AiProtectionの設定

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



AiProtectionを設定する

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

検索結果は、セキュリティ評価ページに表示されます。

	Network Protection with Trend Micro protects against network exploits to Souther Security Assessment cess.		
	Default router login username and password changed -	Yes	
	Wireless password strength check -	Very Weak	
	Wireless encryption enabled -	Strong	
	WPS disabled -	No	
	UPnP service disabled -		
	Web access from WAN disabled -	Yes	
	PING from WAN disabled -	Yes	
	DMZ disabled -	Yes	1
	Port trigger disabled -	Yes	
	Port forwarding disabled -	Yes	
	Anonymous login to FTP share disabled -	Yes	
	Disable guest login for Network Place Share -	Yes	
	Malicious Website Blocking enabled -	Yes	
	Vulnerability Protection enabled -	Yes	123/0
	Infected Device Prevention and Blocking -	Yes	
1	Two-Way IPS The Two-Way Intrusion Prevention S		

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

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

手順

- a. 項目をクリックすると、その項目の設定画面に移動します。
- b. 項目のセキュリティ設定画面から、設定して、必要な変更 を行い、完了したら「適用」をクリックします。
- c. 「**セキュリティ評価**」 画面に戻り、「**閉じる**」 をクリックして 画面を閉じます。
- 5. 確認メッセージで「OK」をクリックします。

3.6.2 悪質サイトブロック

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

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

悪質サイトブロックを有効にする

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

A	iProtection -	Malicious S	ites Bloc	king	S	e tas	"W//4					1
	Restrict acces hacking, and r	ss to known ma ransomware at Security E	licious web tacks. Event	sites to protec	t your net	work fro	om malw Thi	vare, ph reat Ac	ishing, tivities	spam,	adwa	re,
	#	O Protec Since 2023/05/7 Top Clie No Event Do	tion 24 17:07 ent etected	Q	Protect 1 5/18	5/19	5/20	5/21	5/22	5/23	5/2	4
	Details of Su	ccessfully Pr	otected E	vents						٦	Ō	Ľ
	Time		Threat	Source		I	Destinat	tion				

3.6.3 脆弱性保護

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

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

脆弱性保護を有効にする

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

AiProtection - Two-Way IPS The Two-Way Intrusion Prevention St attacks. It also blocks malicious incor as Shellshocked, Heartbleed, Bilcoin	ystem protects ar ning packets to p mining, and rans	ny device connector rotect your route comware. Additio	cted to the network In from network vul nally, Two-Way IPS	: from spam o nerability atta S detects sus	r DDoS cks, such picious
outgoing packets from infected device	es and avoids bo	tnet attacks.			
Security Event			Severity Le	evel	
C Protection Since 2023/05/24 17:07	9	Protection	🛑 High 🛛 🤒 Mediur	n 🔍 Low	
Top Client					
No Event Detected					
		0 • 5/18 5/19	5/20 5/21 5	5/22 5/23	5/24
Details of Successfully Protected	Events			C	ĐÔ
Time Level Type	Source	Destination	Threat		
	No dat	a in table.			

3.6.4 感染デバイス検出/ブロック

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

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

感染デバイス検出/ブロックを有効にする

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

アラートを設定する

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

- 「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。
- メールサービス、メールアドレス、パスワードを入力し「適用」を クリックします。



3.7 ファイアウォール

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

ご注意:ファイアウォール機能はデフォルト設定で有効に設定されています。

3.7.1 全般設定

基本的なファイアウォールのセットアップ

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

3.7.2 URLフィルター

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

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

URLフィルターのセットアップ

- 1. 「**ファイアウォール**」をクリックし、「**URLフィルター**」タブを選択 します。
- 2. 「URL フィルターを有効にする」の「有効」をチェックします。
- 4. 「適用」をクリックし、設定を保存します。

3.7.3 キーワードフィルター

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

e clients' access to webpages containing the s	specified keywords.
use HTTP compression technology cannot be f tered.	illered <u>See here for more details.</u>
Enabled ODisabled	
: 64)	
Keyword Filter List	Add / Delete
	•
	Crems access to verspages containing the s see HTTP compression technology cannot be s ered.

キーワードフィルターのセットアップ

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

ご注意:

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

3.7.4 パケットフィルター

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

Firewall - Network Services Filter	San III San	an a	
The Network Services filter blocks the LAN the For example, if you do not want the device to 30 will be blocked (but https can not be block Leave the source IP field blank to apply this	o WAN packet exchanges and restricts de o use the Internet service, key in 80 in the ked). rule to all LAN devices.	vices from using specific destination port. The traf	network services. fic that uses port
Deny List Duration : During the scheduled specified duration, all the clients in LAN can Allow List Duration : During the scheduled	duration, clients in the Deny List cannot us access the specified network services. duration, clients in the Allow List can ONL	e the specified network Y use the specified netw	services. After the ork
NOTE : If you set the subnet for the Allow Li Internet service.	st, IP addresses outside the subnet will no	t be able to access the Ir	iternet or any
Network Services Filter			
Enable Network Services Filter	• Yes • No		Manna I
Filter table type	Deny List 🗸		
Well-Known Applications	User Defined∨		
Date to Enable LAN to WAN Filter	🗹 Mon 🖉 Tue 🗹 Wed 🖉 Thu 🖉 Fri		
Time of Day to Enable LAN to WAN Filter	00 : 00 - 23 : 59		
Date to Enable LAN to WAN Filter	🗹 Sat 🗹 Sun		
Time of Day to Enable LAN to WAN Filter	00 : 00 - 23 : 59		
Filtered ICMP packet types			
Network Services Filter Table (Max Li	mit : 32)		
Source IP Port Range	Destination IP Port Range	Protocol	Add / Delete
		тср 🗸	Ð
	No data in table.		

ネットワークサービスフィルターのセットアップ

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

3.8 ゲームブースト

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



ゲームブーストを設定する:

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

3.8.1 ゲームブースト

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

Game		
Gear Accelerator	Game Device Prioritizing	
	Prioritizing your game devices for the best gaming experience.	
L'AS	Add	OFF

ゲームブーストを設定する:

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

注記: クライアントプロファイルを削除したい場合は、 をクリックします。

3.8.2 Open NAT

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

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



Open NAT (オープン NAT) を設定する:

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

3.9 ゲストネットワークを構築する

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

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

手順

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

The your	Guest Network provides Inte local network.	rnet connection for guests l	but restricts access to
Network Name (SSID)			
Authentication			
Method			
Network Key	Enable	Enable	Enable
Time Remaining			Default setting by Alexa
Access Intranet			
Network Name (SSID)			
Authentication			
Method			
Network Key	Enable	Enable	Enable
Time Remaining			Default setting by Alexa
Access Intranet			

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

3.10 IPv6

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

g of TUF GAMING AX6000.	
Disable 🗸	
Apply	
ng	ng of TUF GAMING AX6000. Disable v

IPv6のセットアップ

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

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

3.11 LAN

3.11.1 LAN IP

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

ご注意:

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

Configure the LAN setting of TUF GA	MING AX6000.	
Host Name	TUF-AX6000-CE54	
TUF GAMING AX6000's Domain Name		
IP Address	192.168.50.1	
Subnet Mask	255.255.255.0	

LAN IP設定を変更する

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

3.11.2 DHCPサーバー

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

LAN - DHCP Server				
DHCP (Dynamic Host Configuration Proto can assign each client an IP address and AX6000 supports up to 253 IP addresses Manually Assigned IP around the	icol) is a protocol for th informs the client of th for your local network e DHCP list FAQ	he automatic configuration i he of DNS server IP and de c	used on IP networks. The fault gateway IP: TUF GA	DHCP server
Basic Config				
Enable the DHCP Server	O Yes 🔍 No			
TUF GAMING AX6000's Domain Name				
IP Pool Starting Address	192.168.50.2			
IP Pool Ending Address	192.168.50.254			
Lease time (seconds)	86400			
Default Gateway				
DNS and WINS Server Setting				
DNS Server 1				
DNS Server 2				
Advertise router's IP in addition to user- specified DNS	🛛 Yes 🄍 No			
WINS Server				
Manual Assignment				
Enable Manual Assignment	• Yes • No			
Manually Assigned IP around the Di	HCP list (Max Limit	: 128)		
Client Name (MAC Address)	IP Address	DNS Server (Optional)	Host Name (Optional)	Add / Delete
ex: A0:36:BC:9E:CE:54				Ð
	No dat	a in table.		
	A	pply		

DHCPサーバー のセットアップ

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

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

ご注意:

- IPプール起点アドレスとIPプール終点アドレスは、次の範囲内で 設定されることをお勧めします。
 IPアドレス: 192.168.50.xxx「xxx」は 2~254の任意の数)
- IPプール起点アドレスの値はIPプール終点アドレスより小さい数 値である必要があります。
- 7. 設定が必要な場合は、「DNS と WINS サーバーの設定」で各サ ーバーのIPアドレスを入力します。
- 8. 本製品では、DHCPサーバー機能を使用しながら特定のMACアドレスに対してIPアドレスを手動で割り当てることもできます。
 - 「固定割り当てを有効にする」の「はい」をチェックし、下のリストで MACアドレスと割り当てるIPアドレスを入力し追加します。手動割 り当ては最大128個まで登録することができます。

3.11.3 ルーティングテーブル

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

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

LAN - Route					
This function allows you to GAMING AX6000 to share	add routing rules into TUF the same connection to the	GAMING AX6000. It is usefu e Internet.	ıl if you connect	several routers	behind TUF
Basic Config					
Enable static routes	• Yes	5 O No			
Static Route List (Max	Limit : 32)				
Network/Host IP	Netmask	Gateway	Metric	Interface	Add / Delete
				LAN 🗸	Ð
		No data in table.			
		Apply			

ルーティングテーブルのセットアップ

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

3.11.4 IPTV

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



3.12 ネットワークマップを使用する

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



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

	System	Status	
Wireless	Status	Aura RGB	
СРИ			
		Core 1	0%
		Core 2	0%
		Core 3	0%
		Core 4	0%
100%			
50%			
0%			



3.12.1 セキュリティのセットアップ

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

ワイヤレスネットワークのセキュリティを設定する

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

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

2.4GHz セキュリティ設定



5GHz セキュリティ設定



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

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

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

3.12.2 ネットワーククライアントの管理



ネットワーククライアントの状態を確認する

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



3.12.3 USBデバイスの管理

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



ご注意:

- この機能を使用するには、外付けHDDやUSBメモリー等のUSBストレージデバイスを無線LANルーターのUSBポートに接続する必要があります。本製品がサポートするUSBストレージデバイスのフォーマットタイプや容量については、次のWebサイトでご確認ください。<u>http://event.asus.com/networks/disksupport</u>
- USBポートは同時にUSBドライブ2台、またはUSBプリンター1台と USBドライブ1台を接続することが可能です。
- 重要:本機能を使用するには、ネットワーククライアントがFTPサ イト/サードパーティのFTPクライアントユーティリティ、Servers Center、Samba、AiCloud経由でUSBデバイスにアクセスできるよう、共有アカウントとアクセス権を作成する必要があります。詳し くは「3.17USBアプリケーションを使用する」と「3.4AlCloud 2.0を 使用する」をご覧ください。

USBデバイスの状態を確認する

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

ご注意:

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

USBディスクを安全に取り外す

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

手順

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

	Exteri USB DISK 3 Storage USB DISK 3	.0 Pro:
Internet status:	Informa	Scanner
WAN IP: 192.168.123.36	Model Name:	
DDNS: GO	USB DISK 3.0 Pro	
└¢¬J	Available space:	
	0.986 GB	
	Total space:	
	0.991 GB	
WPA2-	Media Server:	GO
	AiDisk Wizard:	GO
Blocked	Safely Remove disk:	Remove
Clients: 1 Use DISK 3.0 Pr V		

3.13 ペアレンタルコントロール

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

ペアレンタルコントロールを設定する:

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

Web&アプリケーションフィルター

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

Web&アプリケーションフィルターを設定する

- 1. 「ペアレンタルコントロール」画面右上の「Web&アプリケーションフィルター」をクリックします。
- 2. 「Web&アプリケーションフィルター」のスイッチをクリックし ONにします。
- 3. 「**クライアント名 (MAC アドレス)**」ドロップダウンリストから、制限を設定するクライアントを選択します。
- 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)
- 6. 設定を保存するには、「適用」をクリックします。

ご注意:

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

時間設定

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

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

Parental Controls	- Time Scheduling		
By enabling Block All [Devices, all of the connected devices will be b	locked from Internet access.	
Enable block all devices			
	This feature allows you to set up a sched	uled time for specific devices	Internet access.
	1. In [Client Name] column, select a c manually key in MAC address in th 2. In the [Add / Delete] column, click	levice you would like to mana is column. the plus(+) icon to add the cli	age. You can also ent
	3. In [Time Management] column, clid 4. Click [Apply] to save the configural	k the edit icon to set a scheo ions.	lule.
	Note: 1. Please disable <u>NAT Acceleration</u> for r	nore precise scheduling cont	
Enable Time Scheduling	ON ES		
System Time	Wed, May 24 17:23:48	2023	
Client List (Max Limi	it : 64)		
Select all∨	Client Name (MAC Address)	Time Management	Add / Delete
	ex: A0:36:BC:9E:CE:54		Ð
	No data in table.		
	Apply		

手順

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

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

- 5. 設定を保存するには、「適用」をクリックします。

4.14 スマートコネクト

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

4.14.1 スマートコネクトのセットアップ

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

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

et up the wireless related informatic	on below.
Enable Smart Connect	
Network Name (SSID)	Alex_TUF-AX6000_2.4G
Hide SSID	• Yes © No
Wireless Mode	Auto 🗸 🗹 Disable 11b
802.11ax / WiFi 6 mode	Enable V If compatibility issue occurs when enabling 802.11ax / WIFi 6 mode, please check: FAQ
WiFi Agile Multiband	Enable V
Target Wake Time	Disable v
Channel bandwidth	Auto 🗸
Control Channel	Auto v Current Control Channel: 3
Extension Channel	Auto 🗸
Authentication Method	WPA2-Personal v
WPA Encryption	
WPA Pre-Shared Key	1234567890 Danger
Protected Management Frames	Disable 🗸
Group Key Rotation Interval	3600

3.15 システムログ

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

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

システムログを参照する

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

This page shows the detailed syste	's activities.
System Time	Mon, May 29 10:19:45 2023
Uptime	4 days 18 hour(s) 51 minute(s) 48 seconds
Remote Log Server	
	514
Remote Log Server Port	* The default port is 514. If you reconfigured the port number, please make sure that
	remote log server or IoT devices' settings match your current configuration.
	Apply to plan, p
fay 29 03:46:52 kornal: 79866 fay 29 03:57:38 kornal: 79866 fay 29 10:03:04 kornal: _nurs fay 29 10:03:04 kornal: _nurs fay 29 10:03:07 kornal: _nurs fay 29 10:03:41 kornal: _nurs fay 29 10:03:41 rc_service: h fay 29 10:03:41 rc_service: h	<pre>Oilrack_mt7966 bm_suic_debug() 12517: BaritoFullCount = 50186, 014 Oilrack_mt786 bm_suic_debug() 12517: BaritoFullCount = 503900, 014 from : Sissingtop of the state of t</pre>
yy 20 76 75 karmaki. 7964 yy 20 60 63 karmaki. 7964 yy 20 60 64 managedi. 7974 yy 20 60 64 managedi. 7	<pre>ODlinesd, mt7986 bm_suic_debug() 12517: ExFifeFullCount = 50186, Oid Otlinesd, mt7986 bm_suic_debug() 12517: ExFifeFullCount = 503900, Oid free: 185110: Dorsen_140(7) / 21 free: 185110: Dorsen_140(7) / 21 free: 185310: Dorsen_140(7) / 21 free: 185310: Dorsen_140(7) / 21 free: 185310: Dorsen_140(7) / 21 free: 185310: Dorsen_140(7) / 21 free: 185110: Dorsen_</pre>
yy 21 20 74 5.5 karmaki. 7964 yy 20 60 6.7 karmaki. 7964 stranki. 7974 yy 20 60 6.7 karmaki. 7974 stranki. 7974 yy 21 60 6.7 karmaki. 7974 stranki. 7974 yy 21 60 6.7 karmaki.	<pre>ODlinesd, mr7966 bm_suto_debug() 12517: BařifoFullCount = 50186, Old Chirab, mr7966 bm_suto_debug() 12517: BařifoFullCount = 501900, Old Fræe: 18581httpd1 norma_145(1 / 2) Fræe: 15581httpd1 norma_1455(1 / 2) Fræe: 15581ht</pre>

3.16 トラフィックアナライザー

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



トラフィックアナライザーを使用する

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

3.17 USBアプリケーション

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

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



3.17.1 AiDiskを使用する

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

AiDisk を使用する:

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



3. ストレージの共有方法を選択します。

			3)		
My FTP serve	r is shared.: [Decide how to share your folders.			
admin rights					
Imited access	rights				
Irnitless accer	ss rights				
Acc	count	Password	Read	Write	
Ale	c_Hu		Z		

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。

$\textcircled{1} \longrightarrow \textcircled{2} \longrightarrow \textcircled{3}$	3
Create your domain name via the ASUS DDNS services.	
Previous Next	

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

3.17.2 サーバーセンターを使用する

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

メディアサーバーを使用する

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

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

etup the iTunes and UPnP media s	irver.		
iTunes Server			
Enable iTunes Server			
Media Server			
Enable UPnP Media Server			
Media Server Name			
Media Server Status	Idle		
Media Server Path Setting	🛛 All Disks Shared 🌑 Manual M	edia Server Path	

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

- iTunes サーバーを有効にする:
 iTunes サーバー機能の有効/無効を設定
- ・UPnPメディアサーバー: UPnPメディアサーバー機能の有効/無効を設定
- ・メディアサーバー名: メディアサーバーの表示名を設定
- ・メディアサーバーの状態: 現在のメディアサーバーの状態を表示
- メディアサーバーパス設定:
 メディアサーバー用ディレクトリパスの設定
ネットワークプレース (Samba) 共有サービスを使用する ネットワークプレース (Samba) を利用するためのアカウントとアク セス権限を設定することができます。

USB Application -	Network Place (Samba) Share / Cloud Disk	5
Set the account and per	mission of network place(samba) service.	-14/12; ~ 3
Enable Share	🔍 🚾 🗊 - 111 - 111 - 1111 - 1111 - 1111 - 111111	
Allow guest login	Usemame and password is necessary place(Samba)	to log in network
Device Name		
Work Group	WORKGROUP	
Maximum number of con	current connections 5	
	Apply	
()	0	A 🗈 🔊
Alex_Bu	TUF GAMING AX6000 R/W USB DISK 3.0 Pro USB DISK 3.0 Pro	R No
	Save	

手順

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

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

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

新しいアカウントを作成する

- a)

 <br
- 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。

	Add new account		
	New account has no read/wr	ite access rights.	
	Account:		
	Password:		
	Retype password:		
		Add	

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。

Add new folder in Public	
The default access rights for a new	folder is read/write.
Folder Name:	
	Add

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

FTP共有サービスを使用する

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

重要!

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

USB Application - F	TP Share		5
Set the account and perm	nission of FTP service.	1. 4. M.M.	Ť\$
Enable FTP			
Enable WAN access			
Allow anonymous login	0FF Username	and password is necessary to log in FTP servi	ice.
Enable TLS support	O Yes O No		
Maximum number of conc	urrent connections 5		
Character set on FTP Ser	Ver UTF-8 🗸		
	Apply		
$\oplus \ominus$	0		
Alex_Bu	TUF GAMING AX6000	R/W W R No	
		Save	

FTP共有サービスを使用する

- ご注意:本機能を使用する前に、AiDisk機能を設定しFTPサーバーを利用可能な状態にしてください。詳しくは「3.17.1 AiDiskを使用 する」をご覧ください。
- 1. 「USBアプリケーション」→「サーバーセンター」の順にクリック し、「FTP共有」タブを選択します。
- 2. 各項目を設定します。

・ 匿名アクセスを許可する

FTPリソースへの匿名アクセスの許可

・ 最大同時接続数

FTPサービスへの同時接続上限

・ 文字コード

FTPで使用する文字コード

- 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。
- FTPにアクセスするには、WebブラウザーまたはFTPクライアント に次のアドレスを入力します。 ftp://<LAN IP アドレス> ftp://<ドメイン名>asuscomm.com (DDNSが有効の場合)

3.17.3 3G/4G

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

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

(http://event.asus.com/networks/3gsupport/)

3G/4Gインターネットアクセスをセットアップする

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

ご注意: 設定を適用するためには、無線LANルーターの再起動が必要です。

重要:

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

3.18 VPN

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

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

VPN Server VPN Fusion Instant	Guard		
VPN Server			<u></u>
SERVER LIST		РРТР	
VPN Server PPTP	>	VPN Details	
		General	~
VPN Server OpenVPN		Network Place (Samba) Support	<u> </u>
VEN Samer		HOW TO SETUP	0
IPSec VPN			
VPN Server		⊶ VPN Client (Max Limit :16)	⊑∎ • ⊕
WireGuard VPN		No data in table.	
		Apply all setting	s

3.18.1 VPN サーバー

VPNサーバーのセットアップ

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

3.18.2 VPN Fusion (VPN フュージョン)

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



開始するには、次の手順に従います。

- 1. サーバーリストまたはプロファイルの

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



3.18.3 Instant Guard (インスタントガード)

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

	IT DIOCKED ITOITT ITTE			· · · ·
SSID: Alex_TUF-AX6000 Al	ex_TUF-AX6000_50	on: <u>3.0.0.4.388</u> 3		🍄 와 🇊 👸 🏟
	ALC: NOT THE OWNER			
PN Server VPN Fusion Instant	Guard			
Instant Guard				
Instant Guard allows you to create a to your VPN Server with Instant Gu	a VPN tunnel with ju ard app.	st one click via the A	SUS Router app. You can r	nonitor who's connected
Basic Config				
Instant Guard	ON			
Server IP Address				
System Log	Ch	eck log		
	Inter	net only O Internet a	nd local network	
Client will use VPN to access	The acce	ss setting will be applie	d to both IPSec VPN and Ins	tant Guard.
Connection Status				
Connection Status Remote IP Cli	ent status	Access time	Device	PSKRAUTHTIME

3.19 WAN

3.19.1 インターネット接続

インターネット接続では、WAN接続に関する各種設定をすることができます。



WAN接続のセットアップ

- 1. 「WAN」をクリックし、「インターネット接続」 タブを選択します。
- 2. プロバイダーやネットワーク管理者の指示に従って接続設定行 います。設定完了後は「適用」をクリックし、設定を保存します。
 - WAN接続タイプ: ISP (インターネットサービスプロバイダー)への 接続方法を選択します。ご契約プロバイダーの接続タイプにつ いては、ご契約時の書類またはご契約のプロバイダーへお問い 合わせください。

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

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

3.19.2 デュアル WAN

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

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

WAN - Dual WAN		
TUF GAMING AX6000 provides Dual N Select Load Balance mode to optimize both WAN connections. <u>Dual WAN FA</u> To enable WAN Aggregation go to the	WAN support. Select Failover mode to us e bandwidth, maximize throughput, minimi Q WAN-Internet Connection page.	e a secondary WAN for backup network access. ze response time, and prevent data overload for
Basic Config		
Enable Dual WAN	OFF OFF	
Primary WAN	2.5G WAN ~	
Auto USB Backup WAN	O Yes No	
Auto Network Detection Detailed explanations are available on th	e ASUS Support Site FAQ, which may help	you use this function effectively.
Detect Interval	Every 3 seconds	4779
Internet Connection Diagnosis	When the current WAN fails 2	continuous times, it is deemed a disconnection.
Network Monitoring	DNS Query Ping	
	Apply	

3.19.3 ポートトリガー

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

ポートトリガーは、次のような場合に使用することができます。

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

WAN - Port Trigger					
Port Trigger allows you to temporari two methods for opening incoming of the time and devices must use statili to the trigger port. Unlike port forwal multiple devices to share a single of <u>Port. Trigger FAQ</u>	ly open data ports whe data ports: port forward c IP addresses. Port tri rding, port trigger does pen port and port trigge	n LAN devices requ ing and port trigger. gger only opens the not require static IP r only allows one cl	ire unrestricted access Port forwarding opens incoming port when a l addresses for LAN de ient at a time to access	to the Internet. the specified da LAN device req vices. Port forw the open port.	There are ata ports all uests access arding allows
Basic Config					
Enable Port Trigger	• Yes • I	No			
Well-Known Applications	Please s	elect 🗸			
Trigger Port List (Max Limit : 32)(Ð				
Description	Trigger Port	Protocol	Incoming Port	Protocol	Delete
	N	o data in table.			
		Apply			

ポートトリガーのセットアップ

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

- ・ プロトコル: トリガーポートの通信プロトコルを選択します。
- 着信ポート: トリガーによって一時的に開放される着信ポートの 範囲を指定します。
- ・ プロトコル:着信ポートの通信プロトコルを選択します。
- 5. をクリックし、ポートトリガーに関する情報をリストに追加します。
 ボタンをクリックすることで、追加されたエントリーを 削除することができます。
- 6. 「適用」をクリックし、設定を保存します。

ご注意:

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

3.19.4 ポートフォワーディング

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

			0. V. T			
Virtual Server / Port forwarding allows re	emote computers to	o connect to a specific	computer or s	ervice within a pri	vate local	area
network (LAN). For a faster connection,	some P2P applica	tions (such as BitTorre	nt), may also i	require that you s	et the port	
forwarding setting. Please refer to the P	2P application's us	er manual for details.	You can open	the multiple port o	or a range	of port
in router and redirect data through those	e ports to a single o	lient on your network.				
If you want to specify a Port Range for o	clients on the same	network, enter the Se	rvice Name, tr	he Port Range (e.	g. 10200:1	0300),
the LAN IP address, and leave the Loca	il Port blank.					
 When your network's firewall is disab 	led and you set 80	as the HTTP server's	port range for	your WAN setup,	then your	http
server/web server would be in conflic	t with TUF GAMIN	G AX6000's web user i	interface.			
. When you set 20:21 as your ETP sen	ver's port range for	your WAN satup ther		ver would be in o		THE
GAMING AX6000's native FTP serve	vers portrange for	your waavesetup, men	your Phr Ser	ver would be in co	office with	101
Virtual Server / Port Forward	ing EAO					
				9		2
Basic Config						
Enable Port Forwarding	ON					
Port Forwarding List (Max Limit : (64)					
Service Name External Port	Internal Port	Internal IP Address	Protocol	Source IP	Edit	Delete
	N	lo data in table.				

ポートフォワーディングのセットアップ

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

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

ご注意:

- ネットワークファイアウォールを無効に設定し、WANセットアップ 用にHTTPサーバーにポート80を割り当てている場合、HTTPサー バー/Webサーバー/本製品の管理画面に競合が発生し使用する ことができません。
- ネットワークはデータ交換を行うためにポートを使用しますが、各ポートにはポートナンバーと特定のタスクが割り当てられています。 例えば、ポート80はHTTPに使用されます。特定のポートは1度に1つのアプリケーションまたはサービスのみを使用することができます。このため、2台のPCが同時に同じポートを経由してデータにアクセスすることはできません。例えば、2台のPCで同時にポート100にポートフォワーディングを設定することはできません。
- ローカルIP: ポートフォワーディングによって転送されたパケットを受信するクライアントのIPアドレスを設定します。
 - ご注意: ポートフォワーディング機能を使用するには、クライアントに 静的IPアドレスを割り当てる必要があります。詳細について は、「4.2 LAN」をご覧ください。
- ローカルポート:ポートフォワーディングによって転送されるパケットを特定のポートで受信させたい場合にポート番号を設定します。着信パケットを特定ポートではなくポート範囲内でリダイレクトするには、この項目を空欄にします。
- プロトコル: ポートフォワーディングの通信プロトコルを選択し ます。不明な場合は「BOTH」を選択することをお勧めします。

ポートフォワーディング機能が正しく設定されていることを確認する

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

ポートトリガーとポートフォワーディングの違い

- ポートトリガーは静的IPアドレスを設定せずに使用することができます。また、ポートトリガーではルーターを使用して動的な転送を可能とします。例えば、複数のクライアントが同じアプリケーションでポート開放を必要とする場合、ポートフォワーディングでは個別に設定する必要がありますが、ポートトリガーは発信ポート(トリガーポート)のアクセス要求を監視することで、ポートを開放します。
 - ポートトリガーは、一定時間が経過すると自動的に着信ポートを 閉じようとします。ポートフォワーディングのように指定したポ ートを常に開放せず、接続要求によってのみ一時的にポートを 開放するので安全に使用することができます。

3.19.5 DMZ

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

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

DMZのセットアップ

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

DMZの削除

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

3.19.6 DDNS

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

DDNS (Dynamic Domain Name Sy: dynamic public IP address, through and other DDNS services.	stern) is a service that allows network clients to connect to the wireless rout its registered domain name. The wireless router is embedded with the ASU	ter, even with a JS DDNS service
If you cannot use ASUS DDNS serv	rices, please go to <u>https://iplookup.asus.com/nslookup.php</u> to n	each your interne
IP address to use this service.		
The wireless router currently uses a	a private WAN IP address.	
This router may be in the multiple-N	IAT environment and DDNS service cannot work in this environment.	
Enable the DDNS Client	Var Q Na	

DDNSのセットアップ

- 1. 「WAN」をクリックし、「DDNS」タブを選択します。
- 2. ご利用環境に応じて以下の設定を行います。設定完了後は 「適用」をクリックし、設定を保存します。
 - ・ DDNSクライアントを有効にする: インターネット経由で外部から無線LAN/レ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/レーターにプライベートIPアドレスが割り当てられている場合。
 例: 192.168.x.x、172.16.x.x、10.x.x.x
 この場合、管理画面上に黄色のテキストで警告が表示されます。
- 複数のNATテーブルが存在するネットワーク上に無線LANル ーターがある場合。

3.19.7 NATパススルー

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

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

NATパススルーのセットアップ

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

Enable NAT Passthrough to allow	a Virtual Private Network (VPN) connection to pass through the router to the	network clients.
PPTP Passthrough	Enable 🗸	
L2TP Passthrough	Enable 🗸	
IPSec Passthrough	Enable 🗸	
RTSP Passthrough	Enable 🗸	
H.323 Passthrough	Enable 🗸	
SIP Passthrough	Enable 🗸	
PPPoE Relay	Disable 🗸	
FTP ALG port	2021	

3.20 ワイヤレス

3.20.1 全般設定

全般タブでは基本的なワイヤレス設定を行なうことができます。

et up the wireless related information	n below.
Enable Smart Connect	
Band	2.4 GHz ∨
Network Name (SSID)	Alex_TUF-AX6000_2.4G
Hide SSID	● Yes ◎ No
Wireless Mode	Auto 🗸 🖌 b/g Protection 🖉 Disable 11b
802.11ax / WiFi 6 mode	Enable V If compatibility issue occurs when enabling 802.11ax / WiFi 6 mode please check: FAQ
WiFi Agile Multiband	Enable 🗸
Target Wake Time	Disable 🗸
Channel bandwidth	20/40 MHz ✔
Control Channel	Auto Current Control Channel: 3 Auto select channel including channel 12, 13
Extension Channel	Auto 🗸
Authentication Method	WPA2-Personal 🗸 ⊘
WPA Encryption	AES 🗸
WPA Pre-Shared Key	1234567890 Danger
Protected Management Frames	Disable 🗸
Group Key Rotation Interval	3600

基本的なワイヤレス設定

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

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

ご注意:「b/g Protection」をチェックするとIEEE802.11bとIEEE802.11g が混在する環境でIEEE802.11gの通信を優先させることがで きます。

- 6. 通信チャンネルを選択します。
- 通信チャンネルを選択します。[自動]を選択した場合、無線LAN ルーターは電波干渉の少ないチャンネルを自動的に選択して使 用します。
- 8. より高速な通信を行う場合は、チャンネル帯域の設定を行います。
- 9. 認証方式を選択します。

ご注意: 暗号化方式でWEP (64/128 bit) またはTKIPを使用した場合、 最大転送速度は54Mbps (規格値) となります。

10. 「適用」をクリックし、設定を保存します。

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

3.20.2 WPS

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

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

VPS (WiFi Protected Setup) prov	es easy and secure establishment of a wireless network. You can configure WPS here via	the
PIN code or the WPS buttlon.		
Enable WPS		
Current Frequency	2.4 GHz / 5 GHz	
Connection Status	klie / klie	
Configured	Yes / Reset Yes / Pressing the reset button resets the network name (SSID) and WPA encryption key.	
AP PIN Code	15302137	
ou can easily connect a WPS cli	t to the network in either of these two ways:	
 Method1: Click the WPS be button on the client's WLAI 	on on this interface (or press the physical WPS button on the router), then press the WPS adapter and wait for about three minutes to make the connection.	
Method2: Start the client W	S process and get the client PIN code. Enter the client's PIN code on the Client PIN code	
field and click Start. Please	heck the user manual of your wireless client to see if it supports the WPS function. If your	
network Name (SSID) and	on the wirs function, you have to conligure the wireless client manually and set the same ecurity settings as this router	
	Push button Q Client PIN Code	

WPSを有効にする

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

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

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

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

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

ワイヤレスデバイスからの接続設定:

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

無線LANルーターからの接続設定:

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

3.20.3 ブリッジ

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

Wireless - Bridge		
Bridge (or named WDS - Wireless Di wirelessly. WDS may also be conside	stribution System) function allows your TUF GAMING AX60 red a repeater mode.	000 to connect to an access point
Note:		
The function only support [Open corresponding authentication me Click <u>Here</u> to modify. Please refe	System/NONE, Open System/WEP] security authentication thod, please select Legacy as your wireless mode first, to this <u>FAQ</u> for more details.	rmethod. To set up the
To enable WDS to extend the wireles	s signal, please follow these steps :	
Select (WDS Only) or (Hybrid) Ensure that this wireless route Key in the remote AP mac in to router's MAC address. To get the best performance, a bandwidth, control channel, ar You are currently using the Auto	mode and add MAC address of APs in Remote AP List. r and the AP you want to connect to use the same channel te remote AP list and open the remote AP's WDS manager bases go to Advanced Settings - Writeless - Seneral and a destension channel to every router in the network. channel bandwidth. Click <u>Hore</u> to modify.	nent interface, key in the this assign the same channel
You are currently using the Auto	channel. Click <u>Hene</u> to modify.	
Basic Config		
2.4 GHZ MAG	A0:36:BC:9E:CE:54	
5 GHz MAC	A2:36.BC:9E:CE:54	
Band	2.4 GHz ∨	
AP Mode	AP Only ✔	
Connect to APs in list	• Yes • No	
Remote AP List (Max Limit : 4)		
	Remote AP List	Add / Delete
	•	Ð
	No data in table,	
	Apply	

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。

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

3.20.4 MACアドレスフィルタリング

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



MACアドレスフィルタリングのセットアップ

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

3.20.5 RADIUS

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

This section allows you to set up	additional parameters	or authorizing wi	eless clients t	hrough RADIUS server	It is required while
you select "Authentication Methe	od" in "Wireless - Gener	al" as "WPA-Ente	rprise / WPA2	-Enterprise".	
Band	2.4 GH	z 🗸			
Server IP Address					
Server Port	1812				
Connection Secret					

RADIUS認証サーバーアクセスのセットアップ

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

ご注意:認証方式については、「4.2.1 全般設定」をご覧ください。

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

3.20.6 ワイヤレス - 詳細

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

ご注意:特に必要がなければ、設定を変更せずに使用することをお 勧めします。

Wireless - Professional	
Wireless Professional Setting allows you	u to set up additional parameters for wireless. But default values are recommended.
Band	2.4 GHz ∨
Enable Radio	© Yes ● No
Enable wireless scheduler	● Yes ◎ No
Set AP Isolated	● Yes ◎ No
Roaming assistant	Enable V Disconnect clients with RSSI lower than : -70 dBm
Enable IGMP Snooping	Disable v
Multicast Rate(Mbps)	Auto 🗸
Preamble Type	Long v
RTS Threshold	2347
DTIM Interval	
Beacon Interval	100
Enable TX Bursting	Enable 🗸
Enable Packet Aggregation	Enable 🗸
Enable WMM	Enable 🗸
Enable WMM No-Acknowledgement	Disable 🗸
Enable WMM APSD	Enable 🗸
256-QAM	Enable 🗸
Airtime Fairness	Disable 🗸
Multi-User MIMO	Enable 🗸
OFDMA/802.11ax MU-MIMO	DL OFDMA + MU-MIMO 🗸

「詳細」では、次の設定が可能です。

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

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

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

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

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

4 ユーティリティ

ご注意:

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

4.1 Device Discovery

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

Device Discovery ユーティリティを起動する:

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

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

4.2 FirmwareRestoration (ファームウェアの復元)

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

Firmware Restor	ation		×
<u>F</u> ilename:	I		<u>B</u> rowse
Status After locating th	ne firmware file, click Uplo	ad.	
[<u>U</u> pload	<u>C</u> lose	

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

- 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。
- 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。
- コンピューターのIP アドレスを次の値に設定します。
 IPアドレス: 192.168.50.x
 サブネットマスク: 255.255.255.0
- 「スタート」ボタン→「すべてのプログラム」→「ASUS Utility」→ 「Wireless Router」→「Firmware Restoration」の順にクリック します。
- 5. ファームウェアファイルを指定し、「アップロード」をクリックします。

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

4.3 プリンターサーバーの設定

4.3.1 ASUS EZ Printer Sharing

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



ご注意:

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

EZ Printer 共有モードのセットアップ

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



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

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



The conter	s Its of this package are be	ing extracted.		1
Please wait Printer Setu	while the InstallShield Wi p Utility on your compute	zard extracts the files r r. This may take a few	needed to install ASL moments.	IS
Extracting	JsbService64.exe			_
tallShield ———				

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。

ASLIS Printer Setup Utility
This utility will help you set up the USB printer. Connect your PC with the router through wired/wireless connection, then connect your printer to the router and power on it. Click "Next" to start printer installation.
Next Cancel

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

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



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



4.3.2 LPRを共有プリンターに使用する

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

LPRプリンターを共有する (Windows® OS)

手順

 「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。

Choose a printer port	
A printer port is a type of connection that allows your computer to exchange information with a printer.	
Use an existing port:	*
Create a new port:	ור
Type of port: Standard TCP/IP Port	-
	-
Next Cance	•

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。

🚱 🖶 Add Printer		×
Type a printer hostname or IP address		
Device type:	TCP/IP Device	Ŧ
Hostname or IP address:	192.168.1.1	
Port name:	192.168.1.1	
Query the printer and auto	matically select the driver to use	
	Next	Cancel

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。

😋 扁 Add Printer	
Additional port	information required
The device is not	found on the network. Be sure that:
 The device is 1 The network i The device is 1 The address o If you think the a address and performed before befo	urned on. i connected. ropedy configured. In the previous page is correct. ddress is not correct, click Back to return to the previous page. Then correct the min another search on the network. If you are sure the address is correct, select the
Device Type	
Standard	Generic Network Card 👻
Custom	Settings
	Next Cancel
_	

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。

ort Settings		
Port Name:	192.168.1.1	
Printer Name or IP Addres	192.168.1.1	
Protocol Raw	IPR	
Raw Settings		
Port Number:	9100	
I PR Settings		
Queue Name:	LPRServer	
LPR Byte Counting E	nabled	
SNMP Status Enable	d	
Community Name:	public	
SNMP Device Index:	1	

7. 「次へ」をクリックし、ドライバーの検出へ進みます。

Add Printer	t information required	×
The device is not 1. The device is 1 2. The network i	found on the network. Be sure that: turned on. s connected	
 The device is 4. The address o If you think the a address and perford device type below 	properly configured. In the previous page is correct. Iddess is not correct, click Back to return to the previous page. Then correct the orm another search on the network. If you are sure the address is correct, select the	2
Device Type Standard	Generic Network Card 👻	
Custom	Settings	
	Next	cel

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。

0	🚔 Add Printer				
	Install the printer driver Choose your printer from the list. Click Windows Update to see more models. To install the driver from an installation CD, click Have Disk.				
	Manufacturer Kyocera Lanier Lemark Microsoft Anc This driver is digitally signed Tell me why driver signing is	Printers Printers	•		
		Next Can	;el		

9. プリンター名を入力し、「次へ」をクリックします。

Mad Printer Type a printer name Printer name It commark 2544 PS (MS) This printer will be installed with the Lexmark X544 PS (MS) driver.			
Type a printer name Printer name: #corrunk X544 PS (MS) This printer will be installed with the Lexmark X544 PS (MS) driver.	G 🖶 Add Printer		_
Printer name: This printer will be installed with the Lexmark XS44 PS (MS) driver.	Type a printer nan	ne	
This printer will be installed with the Learnark XS44 PS (MS) driver.	Printer name:	Lexmark X544 PS (MS)	
	This printer will be insta	lled with the Lexmark X544 PS (MS) driver.	
Next Cancel			Next Cancel

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。

🕞 🖶 Add Printer
You've successfully added Lexmark X544 PS (MS)
To check if your printer is working properly, or to see troubleshooting information for the printer, print a test page Print a test page
Finish Cancel

4.4 Download Master

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

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

Download Master を使用する

- 「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。
- 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。FTR、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。

/ISUS	
Task	General Setting
Task	Refresh rate Seconds
Settings	Apply
General	
🔊 Bit Torrent	
💦 NZB	

4.4.1 BitTorrent設定

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

/1545	1000		
Alla			
Task	Bit Torrent Setting		
Task			
Settings	Use the default port Use the following port		
General	General Speed Limits:		
3.3	Maximum download speed:	KB/S	
Bit Torrent	Maximum upload speed:	KB/S	
	BitTorrent Network setting		
NZB	BitTorrent protocol encryption	Encryption disabled	
	Max peers allowed per torrent	100	
	DHT network	Enable DHT to activate trackiess tonent download.	
		Apply	

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

4.4.2 NZB設定

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

/15U5			
Task			
🧾 Task	NZB Setting		
	Setup USENET server to download NZB files:		
Settings	USENET Server		
No const	USENET Server Port	119	
General	Maximum download speed	KB/S	
💦 Bit Torrent	SSL/TLS connection only		
V.A.	User name		
NZB	Password		
	Confirm Password		
	Number of connections per NZB tasks	2	
		Apph	Y
			2011 ASUSTEK Computer Inc. All rights reserved.

5 トラブルシューティング

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

5.1 基本的なトラブルシューティング

ルーターに関する基本的なトラブルシューティングです。

ファームウェアを最新バージョンに更新します。

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

ネットワークを再起動します。

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

ネットワークケーブルが正しく接続されていることを確認します。

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

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

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

ルーターのネットワーク設定が正しいことを確認します。

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



5.2 FAQ (よくある質問)

管理画面にアクセスすることができません。

- 有線接続の場合は、コンピューターと無線LANルーターにネット ワークケーブルが正常に接続されLANLED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

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

	Internet Options ? ×
Ы	General Security Privacy Content Connections Programs Advanced
	Home page
	To create home page tabs, type each address on its own line.
	https://www.msn.com/?PC=UF01
	×
랔	Use current Use default Use new tab
2	Startup
/	O Start with tabs from the last session
-	Start with home page
	Change how webpages are displayed in take Tabs
2	
	Browsing history
-	form information.
5	Delete browsing history on exit
	Delete Settings
	Appearance
	Colors Languages Fonts Accessibility
	OK Cancel Analy
	OK Cancer Appry

ご注意:

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

無線LANルーターとコンピューターのワイヤレス接続が確立 できません。

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

- ・ 電波の有効範囲外:
 - ・ 無線LANルーターとコンピューターの距離を近づける。
 - 無線チャンネルを変更する。
 - ・ 無線LANルーターのアンテナの角度を調整する。
- DHCPサーバーを有効にする:
 - 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。
 - クライアントー覧にコンピューターが表示されていない場合 は、「LAN」をクリックし、「DHCPサーバー」タブで「DHCPサ ーバーを有効にする」の「はい」をチェックしまます。

LAN - DHCP Server				
DHCP (Dynamic Host Configuration Proto can assign each client an IP address and AX6000 supports up to 253 IP addresses Manually Assigned IP around the	col) is a protocol for informs the client of for your local netwo <u>DHCP list FAQ</u>	the automatic configuration the of DNS server IP and de rk.	used on IP networks. The efault gateway IP. TUF G/	DHCP server
Basic Config				
Enable the DHCP Server	O Yes O No			
TUF GAMING AX6000's Domain Name				
IP Pool Starting Address	192.168.50.2			
IP Pool Ending Address	192.168.50.25	4		
Lease time (seconds)	86400			
Default Gateway				
DNS and WINS Server Setting				
DNS Server 1				
DNS Server 2				
Advertise router's IP in addition to user- specified DNS	O Yes No			
WINS Server				
Manual Assignment				
Enable Manual Assignment	• Yes @ No			
Manually Assigned IP around the Di-	ICP list (Max Limi	it : 128)		
Client Name (MAC Address)	IP Address	DNS Server (Optional)	Host Name (Optional)	Add / Delete
ex: A0:36.BC:9E:CE:54				Ð
	No d	ata in table.		
	_	Annia		

• 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。

et up the wireless related information	on below.
Enable Smart Connect	N 🚾 🛯 🖉 🦾 🖓 🖉 🖉
Network Name (SSID)	Alex_TUF-AX6000_2.4G
Hide SSID	• Yes © No
Wireless Mode	Auto 🗸 🗹 Disable 11b
802.11ax / WiFi 6 mode	Enable v If compatibility issue occurs when enabling 802.11ax / WIFI 6 mode, please check: FAQ
WIFi Agile Multiband	Enable 🗸
Target Wake Time	Disable 🗸
Channel bandwidth	Auto 🗸
Control Channel	Auto Current Control Channel: 5 Auto select channel including channel 12, 13
Extension Channel	Auto 🗸
Authentication Method	WPA2-Personal v 🕐
WPA Encryption	
WPA Pre-Shared Key	1234567890 Danger
Protected Management Frames	Capable 🗸
Group Key Rotation Interval	3600

・ 通信チャンネルを確認する:

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

・ システムを工場出荷時の状態に戻す:

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



インターネットに接続できません。

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



• ネットワークを再起動する:

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

ペアレンタルコントロールが設定されている:

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

コンピューターを再起動する:
 コンピューターを一旦再起動し、「IPアドレス」と「デフォルトゲ

ートウェイ」が正常な値であることを確認します。

• 本機とモデム/回線終端装置を確認する:

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

ネットワーク名またはネットワークキーを忘れました。

ネットワーク名とネットワークキーを再設定する:

管理画面の「**ネットワークマップ**」、または「**ワイヤレス**」をクリ ックし、ネットワーク名 (SSID) とネットワークキーを再度設定し ます。 ・ システムを工場出荷時の状態に戻す:

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

システムを工場出荷時の状態に戻す方法を教えてください。

・ 管理画面からシステムを工場出荷時の状態に戻す:

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

工場出荷時のデフォルト設定は以下のとおりです。

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

ファームウェアを更新できません。

・ レスキューモードでファームウェアを修復する:

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

管理画面にアクセスできません。

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

A. プロキシサーバー設定を無効にする

Windows®

- 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。
- 「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。

To set up an Internet connection, dck Setup Setup. Setup and Virual Private Network settings Access RD Network Resources - Go to ypn.as Add Add VPN Add VPN Remove Choose Settings if you need to configure a proxy Settings Never dial a connection Never dial a connection Never a network connection is not present Add a connection Availy and with default connection Current None Set default				
Access RD Network Resources - Go to yon.as Add Add VPN Add VPN Remove Doose Settings If you need to configure a proxy Settings Never dial a connection Never a network connection is not present Nave add my default connection Current Nove Set default	Seti	et up an Interr 	net connection, dick	Setup
Add VPN Choose Settings if you need to configure a proxy Settings Where dia connection Dial wherever a network connection is not present News dala my default connection Current None Set default Set default Set default	Access	RD Network R	esources - Go to vpn	.as Add
m Remove Choose Settings if you need to configure a proxy Settings Settings Where dat a connection Dial whenever a network connection is not present Anays dal my default connection Current None Set default Set default				Add VPN
Choose Settings if you need to configure a proxy. Settings server for a connection. Never dal a connection Dal wherever a network connection is not present Aways dal my default connection Current None Set default out a lean Network (1 all) estimos		m		Remove
Current None Set default	 Never for a Never d Dial whe Always 	al a connection. al a connection never a netwo dial my default	rk connection is not p	resent
ocal Area Network (LAN) settings	Current	None		Set default
and the sector of the sector in the sector i	ocal Area N	etwork (LAN) s	ettings	
LAN Settings do not apply to dial-up connections. LAN settings Choose Settings above for dial-up settings.	LAN Setting Choose Set	s do not apply tings above for	to dial-up connection dial-up settings.	s. LAN settings

- 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。

utomatic configuration n se of manual settings, d 	nay override man isable automatic (ual setting configurat	gs. To ensure the ion.
Automatically detect s	ettings		
Use automatic configu	ration script		
Address			
oxy server			
		e settinas	will not apply to
Use a proxy server fo dial-up or VPN connect	r your LAN (Thes tions).		
Use a proxy server fo dial-up or VPN connect Address:	tions). Port:	80	Advanced
Use a proxy server fo dial-up or VPN connect Address:	r your LAN (Thesitions). Port:	80 Isses	Advanced
Use a proxy server fo dial-up or VPN connect Address: Bypass proxy serv	r your LAN (Thes tions). Port: er for local addre	80 Isses	Advanced

MAC OS

- 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。
- 「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。

Location: Automatic Show: Built-in Et	hernet
TCP/IP PPPoE Appl	eTalk Proxies Ethernet
Select a proxy server to configure:	FTP Proxy Server
V FTP Proxy Web Proxy (HTTP)	
Secure Web Proxy (HTTPS)	Set Password
SOCKS Proxy	Scerassword
Gopher Proxy	
Bypass proxy settings for these Hosts & Domains:	
du a i mau i airea	
Use Passive FTP Mode (PASV)	(

ご注意:設定方法についてはブラウザーのヘルプも併せてご覧ください。

B. IPアドレスの自動取得を設定する

Windows®

 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。

View your basic network information and set up connections			
View your active networks			
corpnet.asus Domain network	Access type: Internet Connections: Ethernet		
Change your networking settings			
Set up a new connection or ne Set up a broadband, dial-up, o	twork r VPN connection; or set up a router or access point.		
Troubleshoot problems Diagnose and repair network p	oroblems, or get troubleshooting information.		
	View your basic network inform View your active networks corpnet.asus Domain network Change your networking settings Change your networking settings Set up a new connection or ne Set up a broadband, dial-up, or Set up a broadband, dial-up, or Troubleshoot problems Diagnose and repair network p		

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。

Ethernet Status	;		Х
General			
Connection			-
IPv4 Connectiv	vity:	Internet	
IPv6 Connectiv	vity:	No network access	
Media State:		Enabled	
Duration:		03:29:31	
Speed:		1.0 Gbps	
Details]		
Activity			-
	Sent —	Received	
Bytes:	71,424,646	70,727,241	
Properties	Disable	Diagnose	

×

Ethernet Properties

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。

- 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。

Network	ing Authentica	ation				
Conne	ct using:					
1	Intel(R) Ethernet	Connection (2) 12	219-V			
			Г	Configure.		
This co	nnection uses t	he following items	c			
2	QoS Packet S	Scheduler col Version 4 (TC)	P/IPv4)		^	
	Microsoft Net	work Adapter Mul	tiplexor Prot	ocol		
	Microsoft LLD	P Protocol Driver				
	Internet Proto	col Version 6 (TC	P/IPv6)			
	 Link-Invertion 	pology Discovery	Responder			
	Link-Layer To Link-Layer To	pology Discovery pology Discovery	Responder Mapper I/C) Driver	~	
 	Link-Layer To Link-Layer To	pology Discovery pology Discovery	Responder Mapper I/C) Driver	*	
 	Link-Layer To Link-Layer To	pology Discovery pology Discovery Uninstall	Responder Mapper I/C	Driver	*	
< Desc	Link-Layer To Link-Layer To Install	pology Discovery pology Discovery Uninstall	Responder Mapper I/C	Properties	~	
Desc Trar wide acro	Link-Layer To Link-Layer To Install ription smission Contro area network p sss diverse interco	pology Discovery pology Discovery Uninstall I Protocol/Interne rotocol that provis connected networ	Responder Mapper I/C t Protocol. 1 des commun ks.	Properties The default		
Desc Trar wide acro	Link-Layer To Link-Layer To Install ription smission Contro e area network p sss diverse interco	pology Discovery pology Discovery Uninstall I Protocol/Interne rotocol that provis connected networ	Responder Mapper I/C t Protocol. ¹ des commun ks.	Properties The default nication		
Desc Trar wide acro	Ink-Layer To Install ription remission Contro e area network p ss diverse interco	pology Discovery pology Discovery Uninstall I Protocol/Interne rotocol that provi connected networ 4 (TCP/IPv4) Prop	Responder Mapper I/C t Protocol. ⁻ des commun ks.	Properties The default nication	~	×

nternet Prot	ocol Version 4 (TCP/IPv4)	Properti	es		×
General Alt	ternate Configuration				
You can ge this capabil for the app	t IP settings assigned autor ity. Otherwise, you need to ropriate IP settings.	natically if ask your	your net network	twork suppr administrat	orts tor
Obtair	n an IP address automatical	ly			
O Use th	e following IP address:				
IP addre	-551	1.1	1.1		
Subnet r	nask:		1.1	$(\mathbf{r}_{i})_{i \in \mathbb{N}}$	
Default (gateway:		1.1		
Obtair	n DNS server address autor	natically			
Use t	ne following DNS server add	resses:			_
Preferre	d DNS server:	1.1	1.1	4	
Alternati	e DNS server:			${\bf v}_{i} = {\bf v}_{i}$	
Valida	ate settings upon exit			Advance	ł
			ОК	G	ancel

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。
- : Show: Built-in Ethernet TCP/IP PPPoE AppleTalk Proxies Ethernet • Configure IPv4: Using DHCP 192,168,182,103 Renew DHCP Lease et Mask: 255,255,255,0 DHCP Client ID: (If requ Router: 192.168.182.250 DNS Servers: 192,168,128,10 (Ontional Search Domains: (Optional) IPv6 Address: fe80:0000:0000:0000:0211:24ff:fe32:b18e 4. 「**TCP/IP**」 タブをクリック Configure IPv6.... (?) し、「IPv4 の設定」ドロッ プダウンリストで「DHCP Click the lock to prevent further changes. Assist me... (Apply Now) サーバを参照」を選択します。

🔟 🔲 💩 🙆

Location: Automatic

-

5. 変更が終了したら、「今すぐ適用」をクリックして設定を適用し ます。

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

С. 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。

neral Security Privacy Conten	Connections Programs Advance
To set up an Internet conne Setup.	settings
Access RD Network Resources	s - Go to vpn.as Add
	Add VPN
٠ III .	Remove
 Never dial a connection Dial whenever a network conne Always dial my default connecti 	ection is not present ion
Current None	Set default
ocal Area Network (LAN) settings	

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



GNU General Public License

Licensing information

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

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

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

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

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

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

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

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations. Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

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

Terms & conditions for copying, distribution, & modification

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

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

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

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

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

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

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

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

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

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

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

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

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

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

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

- 4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
- 5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License.

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

- 6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
- 7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

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

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/ donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

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

- 8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
- 9. The Free Software Foundation may publish revised and/ or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

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

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

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

NO WARRANTY

- 11 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
- 12 IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

サービスとサポート

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

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



屋外での使用について

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

法律および規制遵守

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