

R55 クイックガイド

本端末との接続方法



Wi-Fi 初期設定

SSID(2.4GHz帯): R55-2.4GHz-000000

SSID(5GHz帯): R55-5GHz-000000

Password: 00000000

2.4GHz帯



5GHz帯



設定ツール

設定ツールURL: <http://192.168.169.1>



◆ QRでの接続

- ① 端末に電源アダプタを接続すると電源が入る
- ② 端末ランプが下記になると起動完了

POWER: 緑

Wi-Fi: 緑

5G: 青 ※5G利用可能な場合

4G/3G: 青

シール記載のQRコードを読み取り接続

◆ 手動での接続

手動の場合シール記載のSSIDを接続したいデバイスから選択しPasswordを入力することで接続可能

WEB管理画面へのログイン方法

◆管理用画面について

本製品の設定(プライバシーセパレーター等)は管理画面から行います。
管理画面は本製品に接続したパソコンやスマートフォンから
Webブラウザを使って表示します。

◆手順

1. 本製品とデバイスをWi-Fi接続する。
2. Webブラウザを起動してアドレス欄に「192.168.169.1」と入力して検索。
3. WEB 管理画面のログインページでユーザー名とパスワードを入力する。

ログイン情報

ユーザー名：admin

パスワード：admin

※ユーザー名、パスワードは本体底面の「User/Key」に記載しています。

端末の初期化方法

端末底面のRESET ボタンを電源がついた状態で10秒長押しすることで
端末の初期化が行われます。

※WEB管理画面で設定した項目が初期値に戻るため
不具合時以外はお控えください。

各部の名称

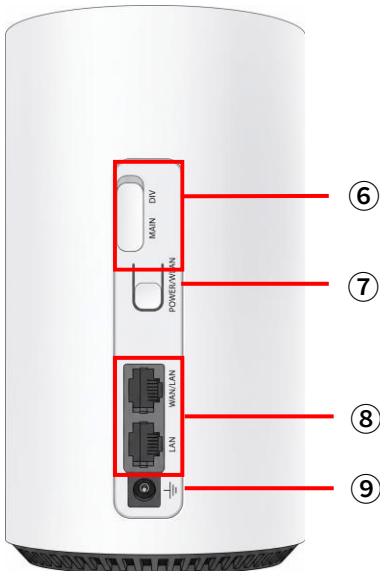
【正面】



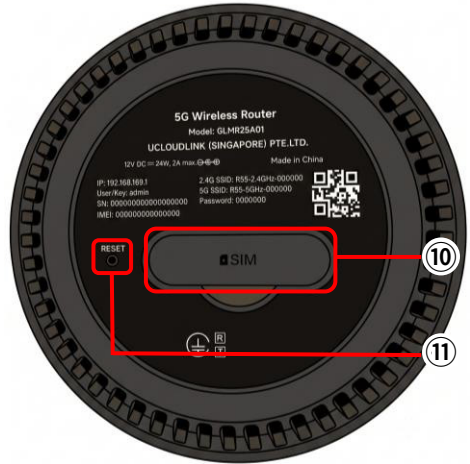
No	名称
①	MESH/WPSボタン
②	POWERランプ
③	Wi-Fi ランプ
④	5Gランプ
⑤	4G/ 3G ランプ

各部の名称

【背面】



【底面】



No	名称
⑥	アンテナ差し込み口 (使用しません)
⑦	POWER/WLANボタン (単押しでWi-FiをOFF 長押しで再起動)
⑧	LANポート
⑨	電源端子

No	名称
⑩	SIMカードスロット (使用しません)
⑪	RESETボタン

5G Wireless RouterR55

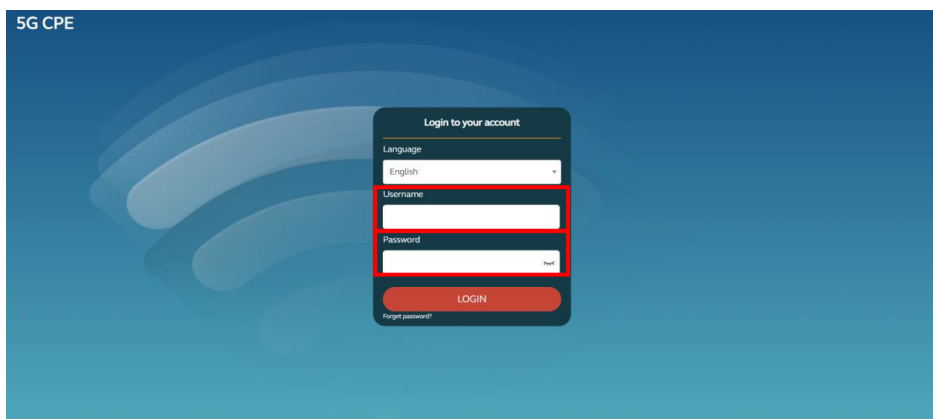
CPE ガイド

目次

1	<u>CPEへのログイン方法</u>	7P
2	<u>ホーム画面</u>	8P
3	<u>モバイルネットワーク</u>	9P
	-統計	9P
	-RFパラメータ	11P
4	<u>インターネット</u>	12P
	-イーサネット	12P
	-DHCP	13P
	-静的DHCP	14P
	-VPN	15P
	-IPSec設定	17P
5	<u>Wi-Fi</u>	20P
	-基本設定	20P
	-詳細設定	21P
	-ゲストWi-Fi	23P
	-WPS	23P
	-Wi-Fi Macアドレスフィルタリング	25P
6	<u>セキュリティ</u>	28P
	-ポート転送	28P
	-NAT設定	29P
	-プライバシーセパレーター機能	30P
7	<u>管理</u>	32P
	-SNTP	32P
	-デバイス情報	35P
	-アップデート	36P
	-再起動とリセット	38P
8	<u>その他の設定</u>	40P
	-ログアウト	40P
	-言語を切り替える	41P

1 CPEへのログイン方法

1. CPEがWi-Fiまたはイーサネットケーブルで接続されていることを確認してください。
2. ブラウザを開き、アドレスバーに「http://192.168.169.1」と入力します。
3. 管理者アカウントとして、ユーザー名に「admin」
デフォルトパスワードに「admin」を入力し、「LOGIN」をクリックします。
※ 初回ログイン時は、デバイスのラベルに記載されているデフォルトの
ユーザー名とパスワードを使用してください。



Web UIに初めてログインする際は、ウィザードの操作を完了する必要があります。
あり、デフォルトのログインパスワードの変更が必須となります。

WebUIには、10分間のタイムアウトによるログアウト機能が備わっています。
そのため、設定作業は事前に計画的に進め、設定を保存するために
「Apply(適用)」ボタンを忘れずに速やかにクリックしてください。

2 ホーム画面

◆ステータス

ホームページ上の「ホーム」ボタンをクリックすると、CPEの基本情報を確認できます。

これには、インターネット情報(インターネットモード、ネットワーク状態、接続タイプ、接続継続時間、IPアドレスなど)、

Wi-Fi情報(Wi-Fi 2.4GHz [状態、名前(SSID)、パスワード]、Wi-Fi 2.4GHz ゲスト [状態、名前(SSID)]、

Wi-Fi 5GHz [状態、名前(SSID)、パスワード])、

およびクライアント情報(ホスト名、MACアドレス、IPアドレスなど)が含まれます。

手順

1. [Home] > [Status] を選択します。
2. CPEのデバイス情報を確認します。

The screenshot shows the '5G CPE' interface with a sidebar on the left and a main content area. The sidebar has a red box around the 'Home' and 'Status' buttons. The main content area is divided into two columns: 'Internet Info' and 'Wi-Fi Status'. Below these is a 'Clients' table.

Internet Info

Internet Mode:	Mobile Data
Network Status:	Connected
Connection Type:	5G
Connection Uptime:	14 Hrs
IP Address:	11.151.26.125
Subnet Mask:	255.255.255.252
Default Gateway:	11.151.26.116
Primary DNS Server:	221.131.1.67
Secondary DNS Server:	221.131.1.68
IPv6 Address:	2408:6A71:622:80C6:8823:431F:D434:360C
IPv6 Primary DNS Server:	2408:688B:8
IPv6 Secondary DNS Server:	2408:688B:8

Wi-Fi Status

Wi-Fi 2.4GHz	Status: Enable
Name(SSID):	R55-2.4GHz-554BC5
Password:	K75HPR79
Wi-Fi 2.4GHz Guest	Status: Disable
Name(SSID):	R55-Guest-554BC5
Wi-Fi 5GHz	Status: Enable
Name(SSID):	R55-5GHz-554BC5
Password:	K75HPR79

Clients

Index	Hostname	Mac	IP	Type	Connection Uptime	Options
1	ZG-03-0184-23	00:ED:4C:6B:D1:AC	192.168.169.141	LAN	00:14:56	...

Copyright © 2026 | Open Source Notice | Privacy Statement

3 モバイルネットワーク

◆統計

このセクションでは、データ使用量と制限を管理できます。

5G CPE Mobile Network Statistics

1 Data Usage Total: 15.80 MB Clear History

2 Data Usage 1Month: 15.80 MB

3 Data Usage 1Day: 15.80 MB

4 Max Data Usage: 0 MB

5 Traffic Limit Notification Switch: ☐ Enable ☒ Disable

6 Percentage setting of traffic limit: 80 %

7 Traffic Overrun Action Settings: Unlimited

8 Flow Automatic Reset Switch: ☐ Enable ☒ Disable

Apply

COPYRIGHT © 2026 | Open Source Notice | Privacy Statement

① データ使用量合計:

デバイスが記録を開始してからの累積データ使用量を表示します。

「履歴を消去」をクリックすると、履歴がリセットされます。

② 1ヶ月のデータ使用量:

過去1ヶ月間のデータ使用量を表示します。

③ データ使用量(1日):

過去1日間のデータ使用量を表示します。

④ 最大データ使用量:

デバイスのデータ使用量の上限を設定します(単位はMB/GB/TBから選択可能)。制限を設けない場合は「0」に設定してください。

⑤ 通信量制限通知スイッチ:

有効にすると、データ使用量が設定した閾値(パーセンテージ)に達した際に通知アラートが送信されます。

⑥ トラフィック制限の割合設定:

通知をトリガーする割合のしきい値を設定します。デフォルトは80%です。

⑦ 通信量超過時の動作設定:

データ使用量が上限を超えた際の動作を設定します。デフォルトは「無制限」(速度制限なしで継続利用)です。

⑧ フロー自動リセットスイッチ:

有効にすると、データ使用量の統計が定期的に自動リセットされ、月次や日次の使用量管理が容易になります。

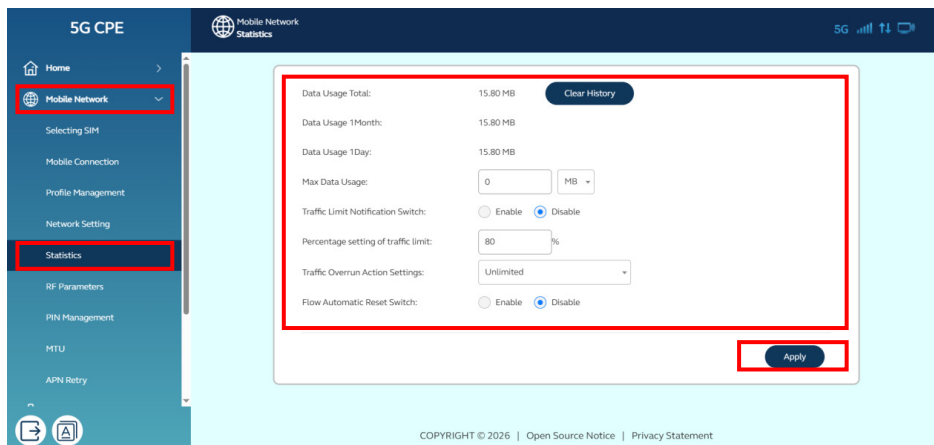
手順

1. [モバイルネットワーク]>[統計]を選択します。

2. 必要な設定パラメータに従い下記操作を行う。

- ・ ページ上部にある「データ使用量 (合計 / 1ヶ月 / 1日)」を確認すると、現在のデバイスのデータ使用量が表示されます。履歴を消去するには、「履歴を消去」ボタンをクリックしてください。
- ・ 「Max Data Usage (最大データ使用量)」の入力欄にデータ使用量の上限値を入力し、右側のドロップダウンリストから単位 (MB、GB、またはTB) を選択します。上限を設定しない場合は、デフォルト値の「0」のままにしてください。
- ・ データ使用量に関する通知を有効にするには、「通信量制限通知」のスイッチで「有効」を選択してください。通知が不要な場合は、「無効」を選択してください。
- ・ 「トラフィック制限」入力欄の「パーセンテージ」設定に、アラートをトリガーする割合を入力します (デフォルトは80%)。これは、データ使用量が最大制限のこの割合に達した際に通知が送信されることを意味します。
- ・ 「通信量超過時の動作設定」のドロップダウンリストから、データ使用量が上限を超えた際の動作を選択します (例:「無制限」は、上限を超えても切断されずに通信を継続することを意味します)。
データ使用量統計の自動リセット機能を有効にするには、「Flow Automatic Reset Switch」で「Enable」を選択します。リセットが不要な場合は、「Disable」を選択してください。

3. 「適用」をタップして設定を保存します。

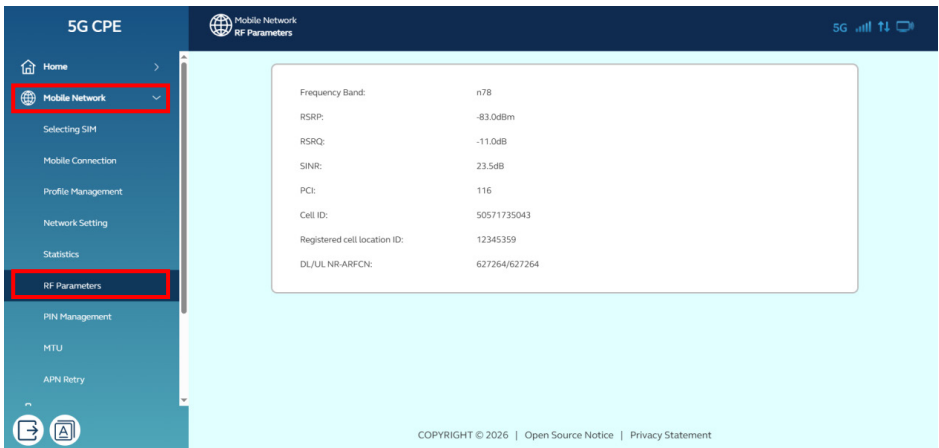


◆RFパラメータ

「RFパラメータ」ページでは、CPEの周波数帯域、RSRP、RSRQ、SINR、PCI、セルID、およびその他の情報を確認できます。

手順

1. [モバイルネットワーク] > [RFパラメータ] を選択します。
2. CPEのRFパラメータ情報を表示します。



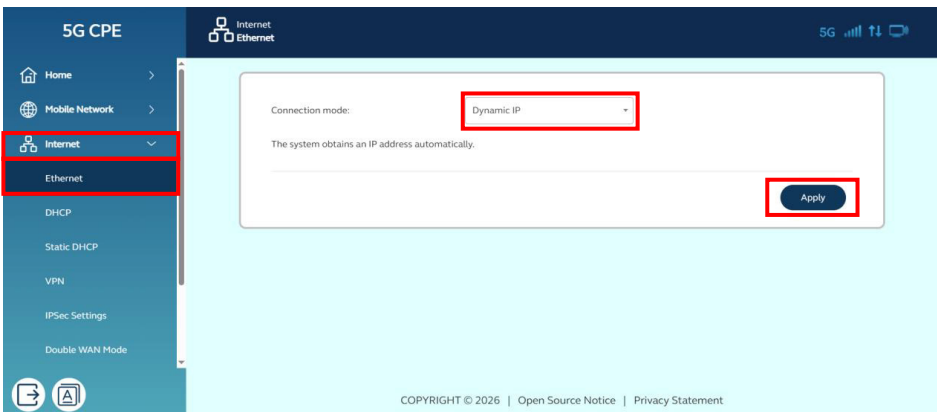
◆イーサネット

このページは、デバイスのWAN側イーサネットアクセスモードを設定するために使用します。

- Auto - システムが適切な接続方法を自動的に検出して選択します。
- 動的IP - システムが上位ネットワーク(DHCPサーバー)から自動的にIPアドレスを取得します。手動設定は不要です。ほとんどのブロードバンド接続環境に適しています。
- 静的IP - 固定IPアドレス、サブネットマスク、およびゲートウェイを手動で指定します。静的IPを必要とするネットワーク環境に適しています。
- PPPoE - ダイアルアップ認証にユーザー名とパスワードを使用します。ADSLやその他の通信事業者によるブロードバンド接続に適しています。
- LANのみ - WAN側でのダイアルアップやIPアドレスの取得を行わず、LANデバイスとしてのみ動作します。

手順

1. [インターネット] > [イーサネット] を選択します。
2. [接続モード] のドロップダウンリストから、接続モード (Auto、Dynamic IP、Static IP、PPPoE、LAN only) を選択します (デフォルトは Dynamic IP です)。
3. [適用] をタップして設定を保存します。



◆DHCP

このインターフェースでは、IPv4およびIPv6 DHCPサーバー設定の包括的な構成が可能であり、ネットワーク上のデバイスへのIPアドレスの自動割り当てを実現します。

DHCP v4設定

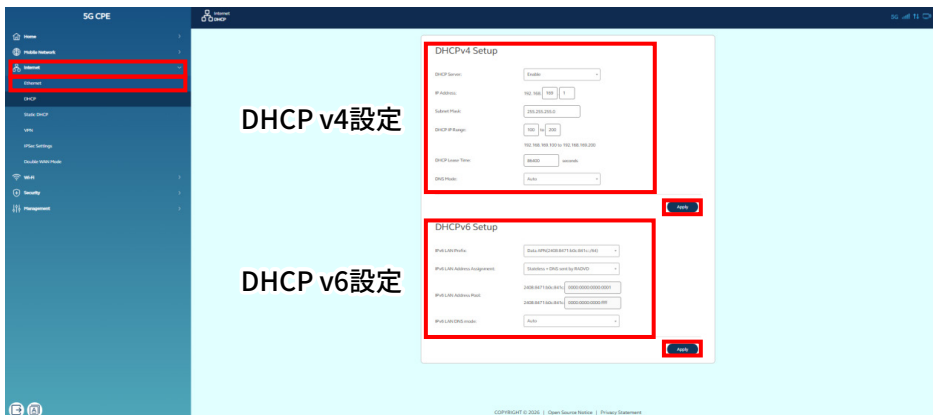
- DHCPサーバーはデフォルトで有効になっていますが、無効にすることも可能です。
- IPアドレス:192.168.169.1
- サブネットマスク:255.255.255.0
- DHCP IP範囲:100～200 (192.168.169.100～192.168.169.200)
- DHCPリース時間:86400秒。
- DNSモードのデフォルトは「自動」ですが、「手動」を選択することも可能です。
- 「適用」をタップして設定を保存します。

DHCP v6設定

- IPv6 LANプレフィックス:自動検出されたプレフィックスを確認します
(例:Data APN (2408:8471:b0c:841c::/64))
※ 通常、ISPまたはネットワーク管理者によってあらかじめ入力されています。
- IPv6 LANアドレス割り当て:Stateless + RADVDによるDNS送信、
Stateless + DHCPv6によるDNS送信、Stateful + DHCPv6サーバーの3つのオプションから1つを選択します。
- IPv6 LANアドレスプール:割り当て範囲の開始アドレス
(例:2408:8471:b0c:841c:(0000:0000:0000:0001))と終了アドレス
(例:2408:8471:b0c:841c:(0000:0000:0000:ffff))を指定します。
- IPv6 LAN DNSモードのデフォルトは「Auto」ですが、「Manual」を選択することも可能です。
- 「適用」をタップして設定を保存します。

手順

1. [インターネット]>[イーサネット] を選択します。
2. [接続モード] のドロップダウンリストから、接続モード (Auto、Dynamic IP、Static IP、PPPoE、LAN only) を選択します
(デフォルトは Dynamic IP です)。
3. 「適用」をタップして設定を保存します。



DHCP v4設定

DHCP v6設定

◆静的DHCP

このセクションでは、静的DHCPの設定を行うことができます。

1. 端末のMACアドレスに基づいてIPアドレスを設定してください(IPアドレスとMACアドレスの紐付け)。
2. 現在はIPv4のみをサポートしています。
3. 例: "XX:XX:XX:XX:XX:XX"

手順

1. [インターネット] > [静的DHCP]を選択します。
2. [追加] をクリックして、ホスト名、LAN IPアドレス、MACアドレス、およびステータスを設定します。
3. [保存]をタップして、設定を保存します。



◆VPN

GLMR25A01デバイスは、L2TPv3 VPNクライアントやL2TP VPNクライアントなど、複数のVPN機能オプションを提供します。

主な機能は以下の通りです。

1. VPN機能とIPSec機能は排他的です。一方を有効にする場合は、必ずもう一方を無効にしてください。
2. L2TPv3を使用する場合、ローカル側とリモート側の両方を同一サブネット上に設定する必要があります。
3. Session IDとCookieは、L2TPv3のネゴシエーションパラメータです。ここで設定するローカル値は、対向デバイス上のリモート値と一致している必要があります、その逆も同様です。

手順

1. [インターネット] > [VPN]を選択します。
2. [IPSec機能]が無効になっていることを確認してください。
現在この機能が有効になっている場合は、まず無効にしてください。
3. [VPNの有効化 (Enable VPN)]セクションで、VPN機能を有効にします。
[アクセスタイプ (Access Type)]では、L2TPv3 VPNクライアントまたはL2TP VPNクライアントのいずれかを設定できます。

■ L2TPv3 VPNクライアントの場合

【必須パラメータ】

• ピアIPアドレス:

サーバーまたはピアデバイスのパブリックネットワークIPアドレスを入力します。

• ローカルセッションID:

ローカルセッションIDを入力します(対向デバイスの「リモートセッションID」と一致

• している必要があります)。

リモートセッションID:

リモートセッションIDを入力します(対向デバイスの「ローカルセッションID」と一致している必要があります)。

■ Cookie設定

- ・ ローカルクッキー長：
ローカルクッキーの長さを設定します (通常は4または8バイト)。
- ・ リモートクッキー長：
リモートクッキーの長さを設定します
(対向機器と合意し、一致させる必要があります)。

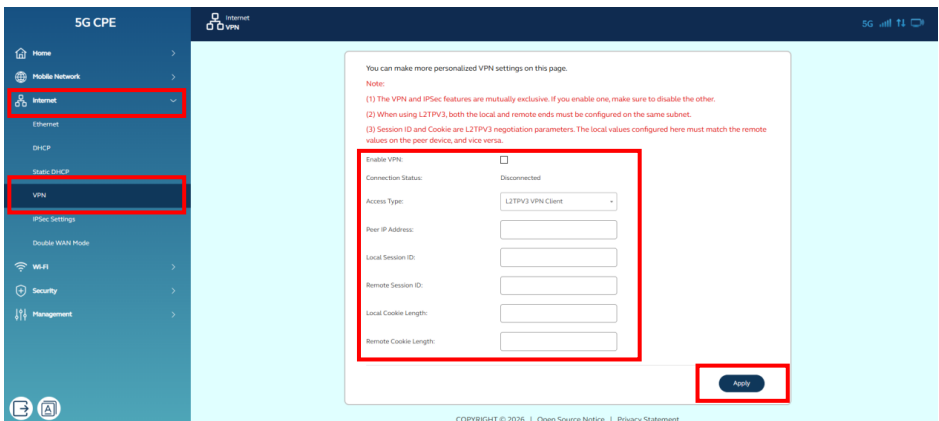
■ L2TP VPNクライアントの場合

- ・ LNSアドレス:VPNサーバーのIPアドレスを入力します。
- ・ ホスト名:(任意) デバイスを識別する名前を入力します。
- ・ トンネルパスワード:事前共有トンネルキーを入力します。
- ・ キープアライブ間隔 (秒) :キープアライブ時間を設定します (通常は30〜60秒)。

■ PPP認証 (必要な場合)

- ・ PPPユーザー名：
ISPまたはVPNサーバーから提供されたユーザー名を入力してください。
- ・ PPPパスワード：
該当するパスワードを入力してください。
- ・ 認証：
適切な方法 (例:PAP、CHAP) を選択してください。

4. [適用]をタップして設定を保存します。



◆IPSec設定

当該インターフェースは、ネットワーク間の暗号化接続を提供するIPSec VPNクライアントとして構成されています。本システムは、適切なトンネルを確立するために、VPNサーバーとのセキュリティパラメータの厳密な整合を強制します。

1. VPN機能とIPSec機能は排他的です。一方を有効にする場合は、必ずもう一方を無効にしてください。
2. IPSec SAのライフタイムは4時間に設定されています。Dead Peer Detection (DPD) の間隔は30秒に設定されています。DPDによってピアがオフラインであると検出された場合、ローカルゲートウェイはトンネルの再起動を開始します。鍵ネゴシエーションの再試行回数の上限は3回に設定されています。

手順

1. [インターネット] > [IPSec設定] を選択します。
2. IPSec VPNクライアントのパラメータ設定、IPSec VPNクライアントの有効化/無効化
IPSec VPNクライアントのトンネリングを有効にするには、[有効] を選択してください。
無効にするには「Disable」を選択します(デフォルト)。
3. 接続状態:「Disconnected (未接続)」と表示されている場合は、VPNトンネルが確立されていないことを示します。接続に成功すると、「Connected (接続済み)」と表示されます。
現在のネットワークの種類: デバイスが現在接続しているネットワークの種類
(例:パブリックネットワーク、プライベートネットワーク)を表示します。
4. 詳細な接続ログを確認するには、[IPSec ログ] チェックボックスをオンにします。これらのログは、接続失敗(認証失敗、パラメータの不一致など)のトラブルシューティングに役立ちます。
5. 基本パラメータを設定する
IPSec Select: IPSec1、IPSec2、IPSec3から選択します(デフォルト:IPSec1)。
・アクセスタイプ:
デフォルトはトンネルモードです。

IPSec Select:IPSec1、IPSec2、IPSec3から選択します(デフォルト:IPSec1)。

- アクセスタイプ:
デフォルトはトンネルモードです。
- IPタイプ:
デフォルトはIPv4です。
- ピアIPアドレス:
VPNサーバーのパブリックIPアドレスまたはドメイン名を入力します。
- 送信元ネットワークアドレス:
ローカルサブネット(例:192.168.169.0)を指定します。
- 送信元サブネットマスク:
該当するマスクを入力します(例:255.255.255.0)。
- 宛先ネットワークアドレス:
リモートの内部サブネット(例:10.0.0.0)を指定します。
- 宛先サブネットマスク:
対応するマスクを入力します(例:255.255.255.0)。
- IKEプロトコル:
デフォルトはIKEv2です。
- IKEライフタイム(分):
セキュリティアソシエーション(SA)のライフタイムを設定します(例:600~3600分)。
- DPDタイムアウト(秒):
Dead Peer Detection (DPD) の確認間隔を設定します(例:10~60秒)。

6. 高度な設定

IPSec VPNクライアントのパラメータ設定、IPSec VPNクライアントの有効化/無効化

- リモートローカルDNSサーバー:
VPNサーバーから提供されたDNS(例:8.8.8.8)を入力します。(任意)
- プロトコル:
AHおよびESPが選択可能で、デフォルトはESPです。
- IKEフェーズ1の暗号化:
利用可能なオプションは aes128、aes192、aes256、aes128gcm16、aes256gcm16
です。デフォルトは aes256 です。
- IKEフェーズ1認証:
SHA-1、SHA-256、SHA-384、SHA-512などのオプションがあります。デフォルトは
SHA-256です。
- フェーズ1 DHグループ:
選択肢には、1024bit(Group2)、1536bit(Group5)、2048bit(Group14)、4096bit

4096bit (Group16) があります。デフォルトは2048bit (Group14) です。

- IKEフェーズ2の暗号化:

オプションには、null_enc、aes128、aes192、aes256、

- aes128gcm16xaes256gcm16 があります。デフォルトはaes256です。

IKEフェーズ2認証:

- オプションにはSHA-1、SHA-256、SHA-384、SHA-512 があります。デフォルトはSHA-256です。

- PFS:

オプションには、None、1024bit (Group2)、1536bit (Group5)、2048bit (Group14)、4096bit (Group16) があります。デフォルトは None です。

- 認証モード:

デフォルトは事前共有鍵です。

- 事前共有鍵:

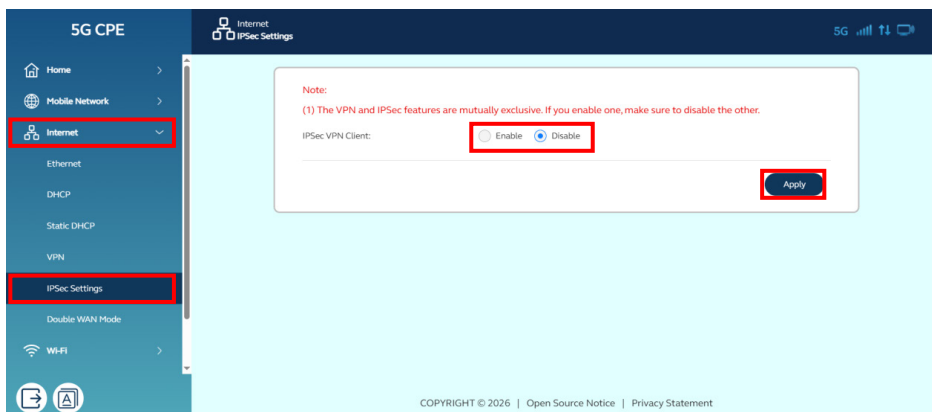
VPNサーバーの設定と一致する鍵を入力してください。(機密情報ですので、取り扱いには十分ご注意ください)

- セキュリティ警告:

IKEフェーズ1およびフェーズ2の認証に脆弱なSHA-1アルゴリズムを使用するように設定すると、重大なセキュリティリスクが生じます。適切な保護を確保するため、SHA-256またはそれより強力なアルゴリズムへアップグレードしてください。サービスの中断を避けるため、接続の両端で同一のセキュリティ設定が使用されていることを確認してください。

6. [適用]をタップして設定を保存します。

IPSec設定ページでの設定完了後、IPSec機能を有効にするために、SIMカード管理ページにて対応するSIMカード情報を設定してください。



◆Wi-Fi基本設定

このページでは、マルチリンク動作 (MLO)、バンドステアリング、および2.4GHz/5GHzのデュアル帯域それぞれの個別設定を含む、デバイスの基本的なWi-Fiパラメータを設定します。

■ Wi-Fiバンドアグリゲーション(MLO) -

Wi-Fiマルチリンクオペレーション(MLO)。複数の周波数帯域で同時にデータを送信することで、スループットと信頼性を向上させます。

現在の設定: 無効。

■ バンドステアリング -

デュアルバンド対応クライアントを最適な周波数帯へ自動的に誘導します。

現在の設定: 無効。

バンドステアリングが無効になっている場合、または2.4GHz帯と5GHz帯の802.11モードのいずれかが使用されていない場合、MLO機能は利用できません。

手順

1. [Wi-Fi] > [Wi-Fi基本設定]を選択します。
2. 必要に応じて、以下の機能を有効にしてください。
MLO (Multi-Link Operation) を有効にするには → 「Wi-Fi Band Aggregation(MLO)」を「有効」に設定します (「Band Steering」が有効であり、かつ両方の帯域がオンになっていることを確認してください)。
自動バンド切り替えを有効にするには → Band Steeringを「有効」に設定します。
3. 2.4GHzまたは5GHzのセクションでは、ステータスを「有効」または「無効」に設定できます。デフォルトは「有効」です。
4. 名前 (SSID)に、任意のWi-Fi名を入力します (範囲: 1~32文字。英数字、アンダースコア、その他の特殊文字を組み合わせで使用できます)。
5. 「セキュリティモード」で、暗号化方式 (None (Open)、WPA2-PSK、WPA/WPA2-PSK、WPA3-SAE、または WPA2-PSK/WPA3-SAE) を選択します。互換性とセキュリティのバランスを考慮し、デフォルト設定である「WPA2-PSK/WPA3-SAE」のままにすることをお勧めします。
6. 「パスワード」に接続用パスワードを入力します。パスワードの長さは、選択した暗号化モードの要件を満たす必要があります (デフォルトの

パスワードは、ランダムな8文字の文字列です。

パスワードには以下の文字を使用できます：

- ① 数字は計9種類で、「0」は含まれません。
- ② 大文字は計24種類で、「I」および「O」は含まれません。

7. 必要に応じて設定してください

- SSIDのブロードキャスト：
ネットワーク名を非表示にするには、「無効 (Disable)」に変更してください。
デフォルトは「有効 (Enabled)」です。
- Max Client:
実際のアクセス要件に応じて、クライアント接続の最大数を調整します。
デフォルトは32です。

8. [適用]をタップして設定を保存します。



◆Wi-Fi詳細設定

このページは、国/地域、802.11動作モード、チャンネル、チャンネル幅など、2.4GHz帯および5GHz帯の高度な無線設定を行うために使用します。

手順

1. [Wi-Fi] > [Wi-Fi 詳細設定]を選択します。
2. 2.4GHzまたは5GHzのセクションで、以下のパラメータを確認または変更してください。

- 国/地域：

デバイスが設置されている正しい地域が選択されていることを確認してください（例：中国の場合は「CN」を選択）。正しく選択されていない場合、チャンネルの使用が制限されたり、規制に適合しなくなったりする可能性があります。

- 802.11モード：

デフォルトの「802.11b/g/n/ax/be」は、すべてのクライアントと互換性があります。レガシープロトコル（802.11b、802.11b/g、802.11b/g/n、802.11b/g/n/ax）を制限する必要がある場合は、設定を変更できます。

※ MLO機能を有効にする場合、2.4GHz帯および5GHz帯の802.11モードを適切に設定する必要があります。そうしないと、MLO機能は無効になります。

- Wi-Fiチャンネル：

通常は「自動（Auto）」に設定しておくことが推奨されます。こ

れにより、システムが自動的に電波干渉を回避します。周囲で著しい同一チャンネル干渉が発生している場合は、手動で特定のチャンネルを指定することも可能です（2.4GHz：1～13、5GHz：36、40、44、48、149、153、157、161）。

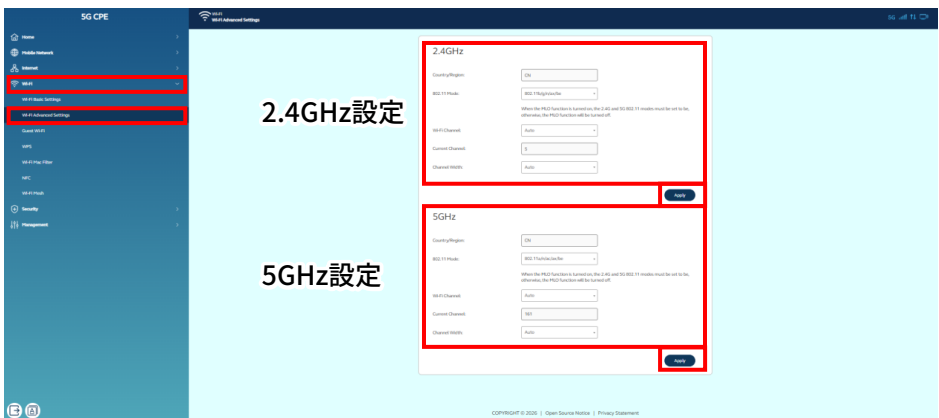
- 現在のチャンネル：

現在使用中のチャンネル番号を表示します。

- チャンネル幅：

通常は「Auto（自動）」に設定することをお勧めします。システムが自動的に最適な幅を選択します。また、必要に応じて、2.4GHz帯では20MHzまたは40MHzを、5GHz帯では20MHz、40MHz、または80MHzを手動で選択することも可能です。

3. [適用]をタップして設定を保存します。

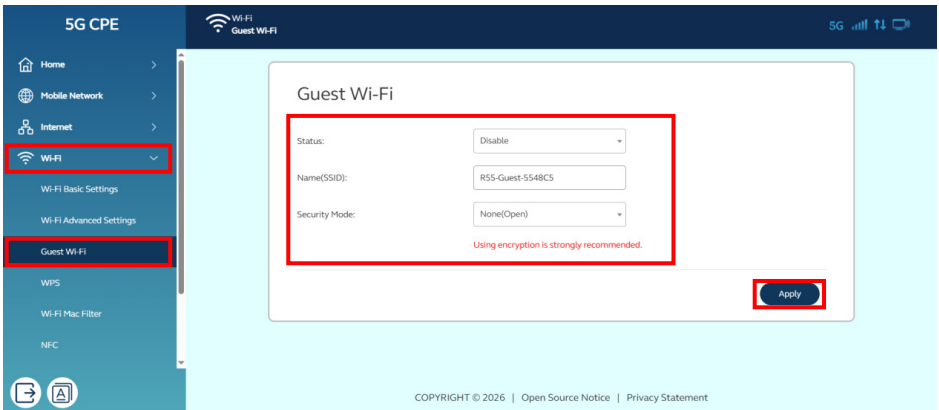


◆ゲスト用Wi-Fi

「ゲストWi-Fi」ページで、ステータス、名前 (SSID)、セキュリティモード、パスワードなどのゲストWi-Fi設定を行います。

手順

1. [Wi-Fi] > [ゲスト Wi-Fi]を選択します。
2. ゲストWi-Fiの「有効」または「無効」を選択してください。
デフォルトは「無効」です。
3. ゲストWi-Fiのパラメータ(名前 (SSID)、セキュリティモード、パスワード)を設定します。※ 暗号化の使用を強く推奨します。
4. 「適用」をタップして設定を保存します。



WPS (Wi-Fi Protected Setup) を使用すると、パスワードを手動で入力することなく、ボタン操作やPINコードによって、クライアントデバイスをWi-Fiに素早く接続できます。

- 設定を行う前に、Wi-Fiがオンになっていることを確認してください。
- 設定を行う前に、Wi-Fiが認識できる状態であることを確認してください。
- 設定を行う前に、暗号化方式がWPA3ではないことを確認してください。

手順

1. [Wi-Fi] > [WPS] を選択します。
2. WPSが「有効」に設定されていることを確認してください。
3. WPSモードのドロップダウンメニューで、接続方法を選択します。

- PBC: プッシュボタン設定モード
- PIN: PINコード・ペアリング・モード

選択したモードに基づいて、対応する操作を実行してください。

■ PBCモードが選択されている場合

- 接続するクライアントデバイスで、WPS接続オプションを選択してください。
- このページに戻り、[接続] ボタンをクリックしてください。
- クライアントは自動的にペアリングを完了し、Wi-Fiに接続します。

■ PINモードが選択されている場合

- クライアントデバイスのクライアントPIN (通常、デバイスのWi-Fiまたはネットワーク設定で確認できる8桁の番号) を入手します。
- クライアントPIN入力欄に、このPINコードを入力してください。
- [接続]ボタンをクリックします。すると、デバイスがクライアントとペアリングされます。
- 接続成功のメッセージが表示されるまでお待ちください。

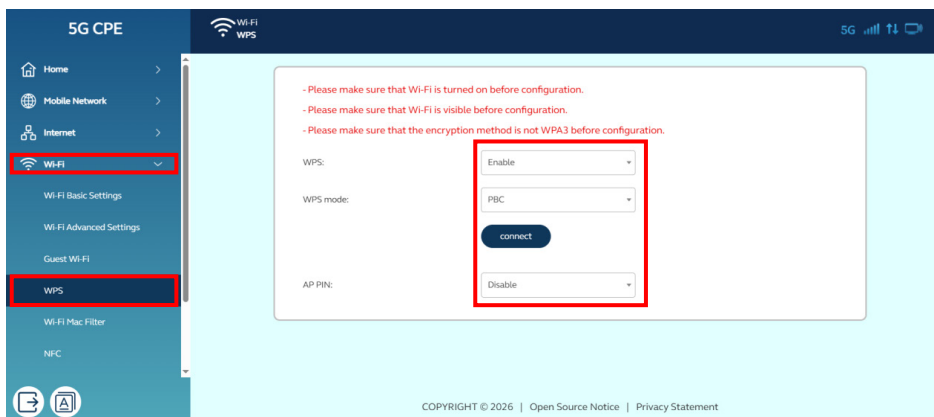
4. AP PIN方式

AP PINを「無効」から「有効」に切り替えます。デフォルトは「無効」です。デバイスに表示されるAP PINコード (通常は8桁の数字) を確認します。クライアントデバイスのWi-Fi設定でAP PINコードを入力し、ペアリングを完了します。

PINコードを変更するには

- [PINを生成]をクリックして、新しいPINコードをランダムに生成します。
- [PINをリセット]をクリックして、PINコードを工場出荷時の初期値に戻します。

ペアリング完了後は、PIN入力機能を無効にしてセキュリティを強化するため、AP PINの設定を「無効 (Disable)」に戻すことを推奨します。



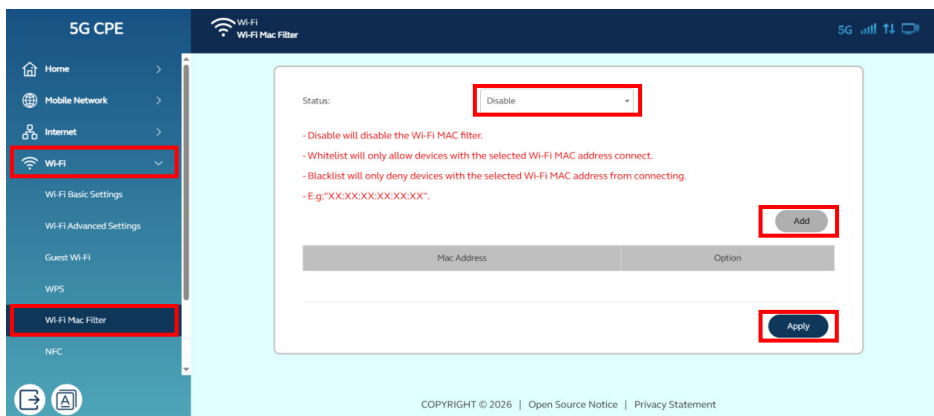
◆Wi-Fi MACアドレスフィルタリング

Wi-Fi MACフィルタのページで、無効、ブラックリスト、またはホワイトリストを選択できます。

- 「無効 (Disable)」にすると、Wi-Fi MACフィルタが無効になります。
- ホワイトリストは、選択されたWi-Fi MACアドレスを持つデバイスのみの接続を許可します。
- ブラックリストは、選択されたWi-Fi MACアドレスを持つデバイスの接続のみを拒否します。
- 例: 「XX:XX:XX:XX:XX:XX」

手順

1. [Wi-Fi] > [Wi-Fi MACフィルター]を選択します。
2. Wi-Fi MACフィルタの設定として、「無効」、「ブラックリスト」、
3. または「ホワイトリスト」を選択してください。デフォルトは「無効」です。
「MACアドレスの入力を追加」をクリックします。
4. [適用]をタップして設定を保存します。



◆Wi-Fi メッシュ

Wi-Fiメッシュは、複数のデバイスで統合された無線ネットワークを構築し、有線または無線のバックホールで相互接続することで、家全体をシームレスにカバーします。現在のデバイスの役割は「コントローラー」であり、2台のスレーブデバイスが接続されています。

手順

1. [Wi-Fi] > [Wi-Fi Mesh]を選択します。
2. Wi-Fiメッシュスイッチを「有効」に設定してください。
3. 「デバイスの役割 (Device Role)」メニューにおけるデフォルトの役割は「コントローラー (Controller)」です。コントローラーはメッシュのマスターデバイス(メインルーター)として機能し、統合管理や設定の配信を担います。
4. 接続済みデバイスの表示と管理
 - ・「接続機器リスト」で、現在メッシュに参加しているすべてのスレーブデバイスを確認します。
 - ・リストを使用して、各デバイスのオンライン状態、IP/MACアドレス、および接続方法を確認してください。
 - ・Wiredは、ノードが有線バックホールで接続されていることを示します。
 - ・ワイヤレスバックホールについては、受信電力やその他の情報が表示されます。

5G CPE

Wi-Fi

Wi-Fi Mesh

5G

Wi-Fi

Wi-Fi Basic Settings

Wi-Fi Advanced Settings

Guest Wi-Fi

WPS

Wi-Fi Mac Filter

NFC

Wi-Fi Mesh

Security

Management

Wi-Fi Mesh Switch:

Enable

Disable

Device Role:

Controller

Connected Equipment List

NO.	Equipment Name	IP Address	Received Power
		MAC Address	Type/Destination
1	GLMR25A01	192.168.169.1	-
		30:89:D3:55:48:C4	-
		192.168.169.141	-
2	ZG-03-0184-23	00:E0:4C:68:01:AC	Wired/1

COPYRIGHT © 2026

Open Source Notice

Privacy Statement

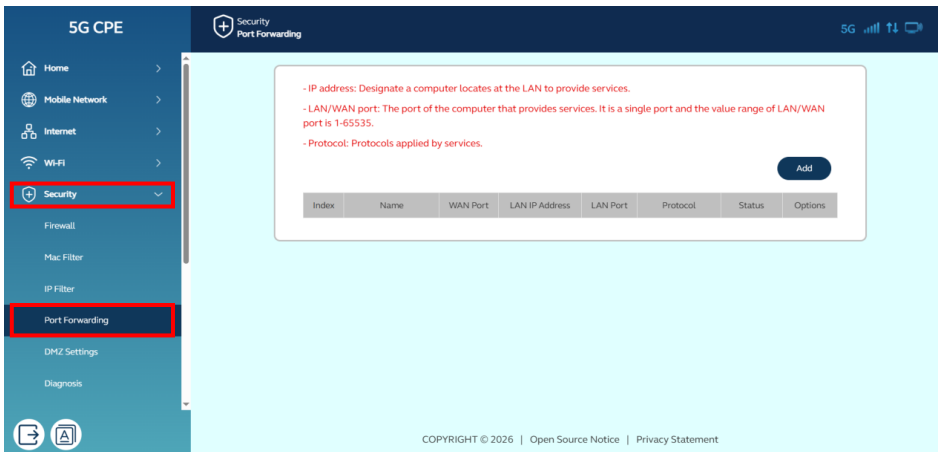
◆ポート転送

このセクションでは、外部のコンピュータから、LAN上で提供されているFTPやその他のサービスにアクセスできるように設定できます。

- IPアドレス - サービスを提供するLAN上のコンピュータを指定します。
- LAN/WANポート - サービスを提供するコンピュータ上のポートです。
- 単一のポートであり、その値の範囲は1～65535です。
プロトコル - サービスによって適用されるプロトコル。

手順

1. [セキュリティ] > [ポート転送] を選択します。
2. 「追加」をクリックして、名前、WANポート、LAN IPアドレス、LANポート、プロトコル、およびステータスを設定します。
3. 「保存」をタップして、設定を保存します。
4. 該当するルール「オプション」メニューから、「編集」または「削除」の操作を選択できます。



◆NAT設定

NAT (Network Address Translation) は、内部ネットワーク機器のプライベートIPアドレスをパブリックIPアドレスに変換 (マッピング) し、それらの機器がインターネットにアクセスできるようにする技術です。NATモードの選択は、内部機器によるアウトバウンド接続の確立方法や、NATトラバーサル (NAT越え) のパフォーマンスに影響を及ぼします。

■ 対称型 (Symmetric) -

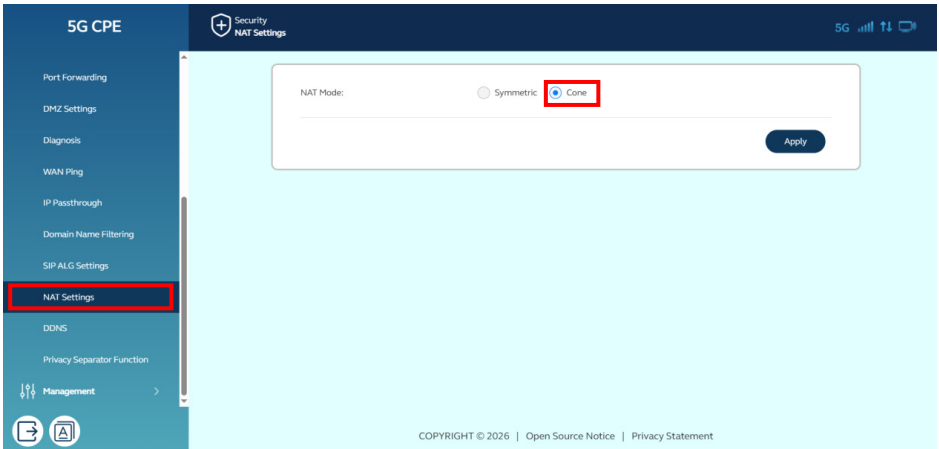
異なる宛先への接続ごとに異なるポートマッピングを使用します。セキュリティは高いもののNAT越え (NATトラバーサル) の能力は低いため、特定のP2Pアプリケーション (ビデオ通話やオンラインゲームなど) の利用が制限される場合があります。

コーン (Cone) -

- 同じ内部IPアドレスおよびポートからの送信接続に対し、固定のポートマッピングを使用します。強力なNATトラバーサル機能と優れた互換性を備えており、P2Pアプリケーションやリアルタイム通信のシナリオに適しています。(デフォルト、推奨)。

手順

1. [セキュリティ] > [プライバシーセパレーター機能] を選択します。
2. 「プライバシーセパレーター機能」のドロップダウンメニューをクリックし、希望する状態を選択してください。
 - 「有効」を選択:
アイソレーションを有効にします。これにより、無線クライアント同士が隔離されます。
 - 「無効」を選択:
アイソレーションを無効にします。ワイヤレスクライアント同士が通常通り通信できるようになります。
3. [適用]をタップして設定を保存します。



◆ プライバシーセパレーター機能

アイソレーション機能は、同一のWi-Fiネットワークに接続された無線クライアントデバイス同士を隔離し、直接通信できないようにするものです。隔離されたデバイスはアップストリームネットワーク（インターネット）へのアクセスのみが可能となるため、ユーザーのプライバシーとネットワークのセキュリティが効果的に保護されます。

■ 無効 -

アイソレーションを無効にします。同じWi-Fiネットワーク上のデバイス同士が互いを検出通信できるようになります。（デフォルト）

■ 有効 -

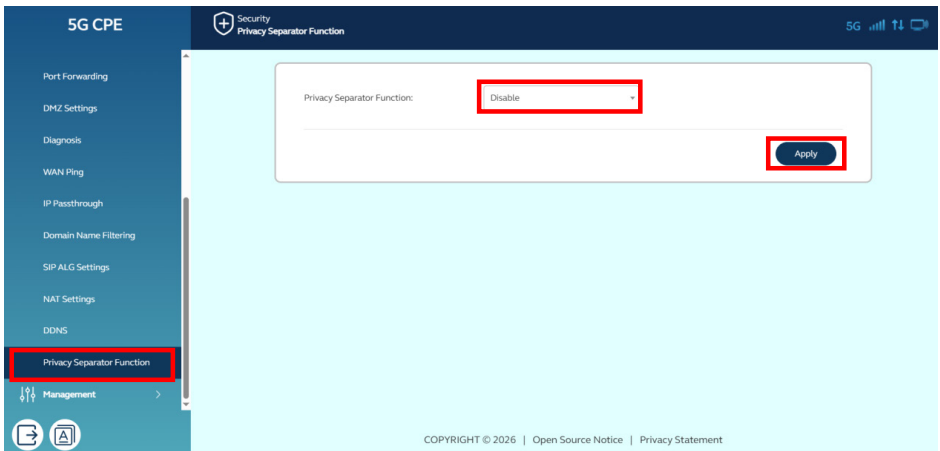
アイソレーション（隔離）機能を有効にします。同じWi-Fiネットワーク上の無線デバイス同士が隔離され、互いに直接アクセスできなくなります。公共の場所や、複数のユーザーでネットワークを共有する環境に適しています。

手順

1. [セキュリティ] > [プライバシーセパレーター機能] を選択します。
2. 「プライバシーセパレーター機能」のドロップダウンメニューをクリックし、希望する状態を選択してください。

- 「有効」を選択：
アイソレーションを有効にします。これにより、無線クライアント同士が隔離されます。
- 「無効」を選択：
アイソレーションを無効にします。ワイヤレスクライアント同士が通常通り通信できるようになります。

3. [適用]をタップして設定を保存します。



◆SNTP

SNTP設定インターフェース - デバイスの時刻を正確に保つための時刻同期機能を設定する際に使用します。

- 現在時刻 -
デバイスの現在時刻。
- ステータス -
時刻同期の状態。デフォルト:同期成功。
- 最終同期 -
最後の同期日時。
- タイムゾーン -
タイムゾーン設定、デフォルト:Asia/Tokyo。
- 時刻形式 -
時刻の表示形式(12時間制 / 24時間制)、
デフォルト:24時間制。
- ネットワーク時刻との自動同期を有効にする -
チェックを入れると、デバイスは定期的にNTPサーバーと時刻を自動同期します(デフォルトで有効)。
- Time Server 1～5 -
NTPタイムサーバーのアドレス(最大5つ)、デフォルト:pool.ntp.org。

手順

1. [Management] > [SNTP] を選択します。

2. 自動時刻同期を有効にする

- ① 「ネットワーク時刻との自動同期を有効にする」のチェックボックスにチェックを入れます。
- ② 「Time Server 1」のドロップダウンメニューから、使用するNTPサーバーのアドレスを選択または入力します(デフォルト:pool.ntp.org)。
- ③ (任意)「Time Server 2」から「Time Server 5」のフィールドに、プライマリサーバーが利用できない場合に使用するバックアップNTPサーバーのアドレスを入力します。

「Time Server 2」から「Time Server 5」については、以下のNTPサーバーから任意のものを選んで入力できます(「Time Server 1」に既に選択されているものに加え)。

- clock.fmt.he.net
- clock.nyc.he.net
- clock.sjc.he.net
- clock.via.net
- ntp1.tummy.com
- time.cachenetworks.com
- time.nist.gov
- time.windows.com
- pool.ntp.org
- europe.pool.ntp.org

- ④ [Time Format] (時刻形式) のドロップダウンメニューで、時刻の表示形式を確認または変更します (24時間形式が推奨されます)。
 - 24時間制: 24時間表記 (例: 18:30)
 - 12時間制: 12時間方式 (例: 午後6時30分)
- ⑤ [適用] をタップして設定を保存します。
- ⑥ 本機は、設定された間隔でNTPサーバーへの時刻同期を自動的に要求します。同期の状態は、「Status (ステータス)」および「Last Synchronize (最終同期)」で確認できます。

3. デバイスの時刻を手動で変更する

- ① SNTPページで「Current Time (現在時刻)」の項目を探し、右側にある「Change Time (時刻の変更)」リンクをクリックします。
 - ② ポップアップウィンドウで、デバイスの日時を手動で調整します。
 - ③ 確認して保存します。現在時刻が手動で設定した値に更新されます。
- ※ 時刻を手動で変更した後に自動同期を有効にすると、次の同期サイクルで、デバイス上の時刻はNTPサーバーの時刻で上書きされます。

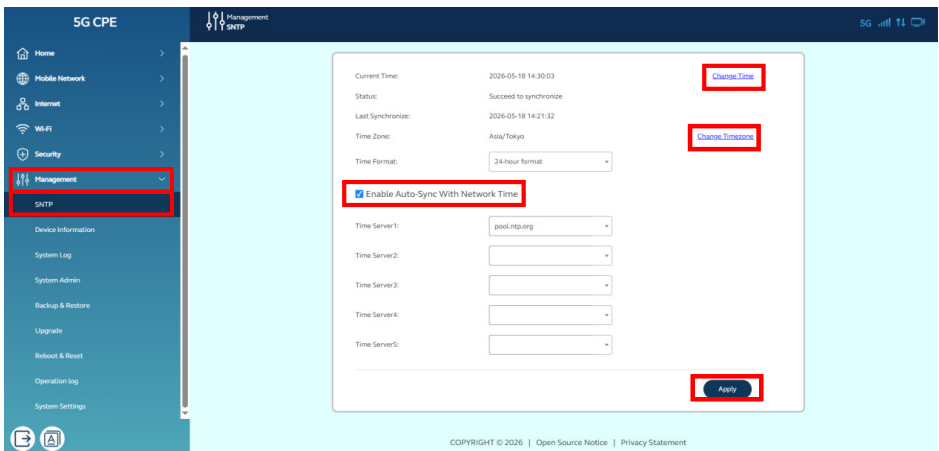
4. タイムゾーンを変更する

- ① 「現在時刻」の右側にある「時刻の変更」リンクをクリックします。
- ② ポップアップ表示される時刻設定画面で、日付と時刻を手動で入力します。
- ③ 保存後、デバイスは手動で設定した時刻を使用します (自動同期は無効にする必要があります)。

4. タイムゾーンの変更

- ① SNTPページで「Time Zone (タイムゾーン)」の項目を探し、右側にある「Change Timezone (タイムゾーンの変更)」リンクをクリックします。
- ② デバイスの設置場所に適したタイムゾーンを選択します (例: Asia/Tokyo)。

- ③ 設定を保存します。新しいタイムゾーンに基づいて、デバイスの時刻が自動的に調整されます。



◆デバイス情報

アイソレーション機能は、同一のWi-Fiネットワークに接続された無線クライアントデバイス同士を隔離し、直接通信できないようにするものです。隔離されたデバイスはアップストリームネットワーク(インターネット)へのアクセスのみが可能となるため、ユーザーのプライバシーとネットワークのセキュリティが効果的に保護されます。

■ デバイス名 -

デバイスの表示名(例:5Gワイヤレスルーター)。

■ モデル名 -

デバイスのモデル識別子(例:GLMR25A01)。

■ ソフトウェアバージョン - 現在のファームウェア／ソフトウェアのバージョン番号(例: R55_8.418.13_EQ100)。

■ ハードウェアバージョン -

デバイスのハードウェアバージョン識別子(例:R55_V1.03_PCB)。製造バッチやPCBバージョンの違いを区別するために使用されます。

■ IMEI -

International Mobile Equipment Identity(国際移動体装置識別番号):デバイスのセルラーモジュールを識別する固有の番号(15桁)。

◆デバイス情報

アイソレーション機能は、同一のWi-Fiネットワークに接続された無線クライアントデバイス同士を隔離し、直接通信できないようにするものです。隔離されたデバイスはアップストリームネットワーク(インターネット)へのアクセスのみが可能となるため、ユーザーのプライバシーとネットワークのセキュリティが効果的に保護されます。

■ MACアドレス -

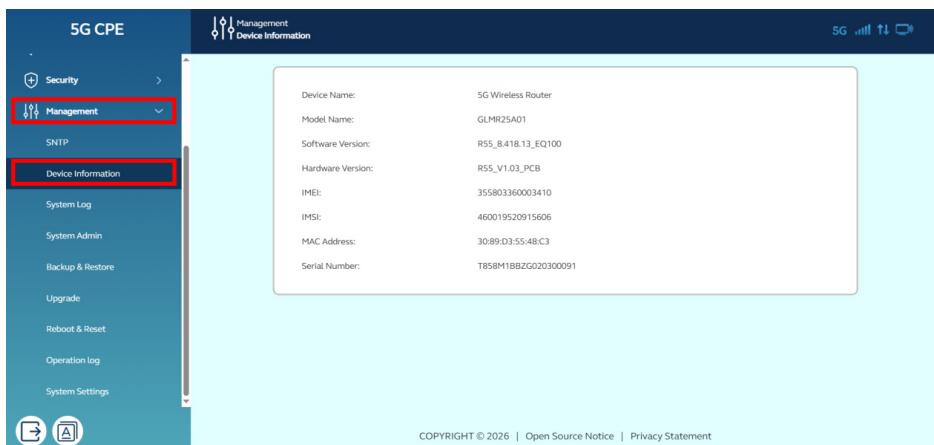
デバイスの物理アドレス(例:30:89:D3:55:48:C3)。ローカルネットワーク上でのデバイスの固有識別やアドレッシングに使用されます。

■ シリアル番号 -

製品の追跡やアフターサポートに使用される、デバイスの工場出荷時のシリアル番号(例:T858M1BBZG020300091)。

手順

1. [管理] > [デバイス情報] を選択します。
2. ページが自動的に読み込まれ、上記の基本的なデバイス情報がすべて表示されます。
3. トラブルシューティング、ファームウェアのアップグレード確認、またはアフターサービスへの問い合わせの際にデバイス情報を参照するには、以下の使用ガイドラインをご確認ください。
 - IMEI / シリアル番号:
特定のデバイスを特定するために、テクニカルサポート担当者に提示してください。
 - ソフトウェアバージョン / ハードウェアバージョン:
 - ファームウェアのアップグレードを依頼する際は、現在のバージョン番号を提示してください。
 - IMSI:
SIMカードが適切に有効化されているか、およびどの通信事業者に属しているかを確認します。
 - MACアドレス:
ルーターのMACフィルタリング、IPバインディング、その他の設定に使用されます。



◆ アップデート

設定更新インターフェース - デバイスのソフトウェア／ファームウェアのバージョンを更新するために使用され、オンライン更新と手動によるローカル更新の両方に対応しています。

■ オンラインアップデート -

インターネット経由でのアップグレードです。デバイスがサーバーから最新のファームウェアを自動的にダウンロードします。デバイスが正常にインターネットに接続されており、公式の最新バージョンが必要な場合に適しています。

■ 手動アップデート -

手動でアップグレードを行います。ユーザーがローカルのファームウェアファイルをアップロードしてアップグレードを実行します。オフライン環境、特定のバージョン要件がある場合、または障害からの復旧に適しています。

手順

1. [管理] > [更新] を選択します。

2. 手動での更新

① 公式サイトから、デバイスのモデルに対応するファームウェアファイル（例：.bin形式）をダウンロードします。

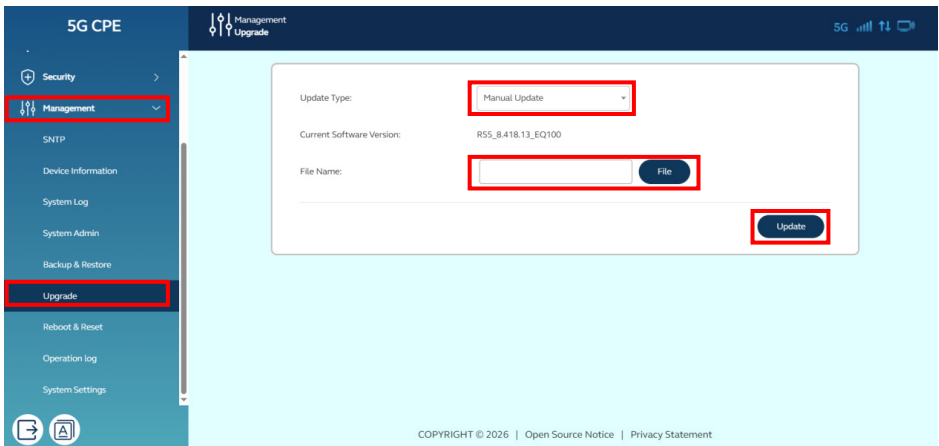
② [Update Type] (更新タイプ) のドロップダウンをクリックし、[Manual Update]

(手動更新)を選択します。デフォルト値は [Manual Update] です。

- ③ 「現在のソフトウェアバージョン」欄には、参考情報として、現在インストールされているファームウェアのバージョンが表示されます。
- ④ [File] ボタンをクリックし、ダウンロードしたファームウェアファイルを参照して選択します。
- ⑤ ファイルを選択すると、「ファイル名」に選択したファイルのパスが表示されます。
- ⑥ 右下の「更新」ボタンをクリックして、アップグレードを開始します。
- ⑦ アップグレードの完了を待ちます。デバイスは自動的に再起動します。

3. オンラインでの更新

- ① 「Update Type」のドロップダウンをクリックし、「Online Update」を選択します。
- ② 本機は、サーバー上で新しいファームウェアのバージョンが利用可能かどうかを自動的に確認します。
- ③ 新しいバージョンが見つかった場合、バージョン情報と更新内容が表示されます。
- ④ [更新の確認] ボタンをクリックして、ダウンロードと自動アップグレードを開始します。
- ⑤ アップグレードが完了するのを待ちます。デバイスは自動的に再起動します。



◆再起動とリセット

このページには、「再起動 (Reboot)」と「リセット (Reset)」の2つのモジュールが含まれています。これらは、デバイスのソフトリブート (再起動) や、工場出荷時の設定への復元を行うために使用します。

■ 再起動 -

デバイスを再起動します。システムのみが再起動し、すべての接続が約60秒間一時的に切断されます。すべての設定は保持されます。

■ リセット -

工場出荷時の設定に戻します。すべての設定を消去してデバイスをデフォルトの状態に戻します。これには約60秒かかります。すべての設定が完全に消去されます。

手順

1. [管理] > [再起動とリセット] を選択します。

2. 再起動モジュール

- ① 左側の「Reboot」モジュールで、「Reboot」ボタンをクリックします。
- ② 確認ダイアログが表示されますので、[OK] をクリックしてください。
- ③ デバイスが再起動を開始し、管理インターフェースが切断されます。
- ④ デバイスの再起動が完了するまで、約60秒間待ちます。
- ⑤ 管理インターフェースに再度ログインして、引き続き使用してください。

3. リセット - 工場出荷時設定へのリセットモジュール

- ① 右側の「Reset」モジュールで、「Reset」ボタンをクリックします。
- ② 確認ダイアログが表示されます。警告メッセージをよくお読みください。
※ 工場出荷時の設定に復元すると、管理者パスワード、Wi-Fi設定、ネットワーク設定など、すべての設定が消去されます。
- ③ 確認後、[OK] をクリックしてリセットを開始します。
- ④ デバイスは自動的に再起動し、工場出荷時の設定に復元されます。
- ⑤ デバイスがデフォルト設定で起動するまで、約60秒間待ちます。
- ⑥ デフォルトのユーザー名とパスワードを使用して再度ログインし、デバイスを再設定してください。

5G CPE

Management
Reboot & Reset

5G

Security

Management

SNTP

Device Information

System Log

System Admin

Backup & Restore

Upgrade

Reboot & Reset

Operation log

System Settings

Rebooting the device will takes about 60 seconds.
Click the button below to reboot.

Reboot

Click the button below to reset the device to its
factory settings.

Reset

再起動モジュール リセットモジュール

COPYRIGHT © 2026 | Open Source Notice | Privacy Statement

8 その他の設定

◆ログアウト

どのページからでも をクリックすると、ルーターからログアウトできます。

■ 機能：

不正アクセスを防ぐため、現在のログインセッションから安全にログアウトします。

■ 適用される場面：

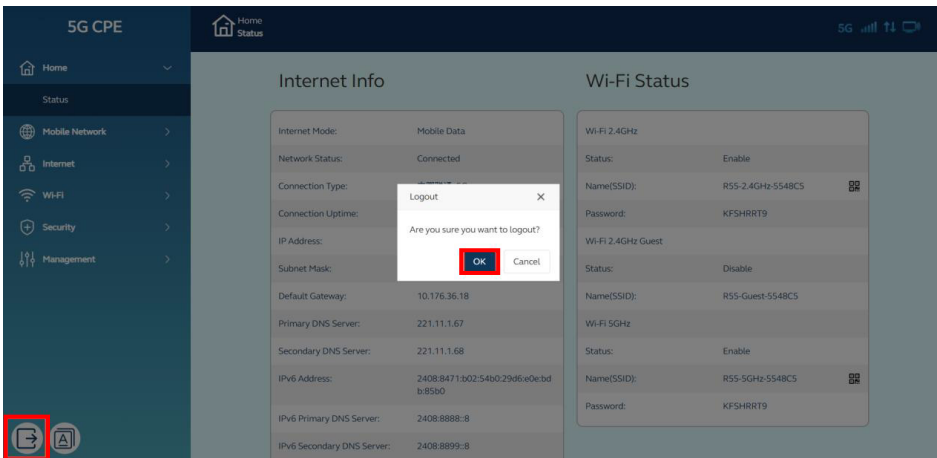
設定完了後、デバイスから離れる際、またはアカウントを切り替える際。

■ セキュリティに関する推奨事項：

管理操作の完了後は、明示的にログアウトすることをお勧めします。

手順

1. デバイス管理インターフェースのどのページでも、左下隅にあるボタンをクリックしてください。
2. ログアウト確認のダイアログが表示され、次のメッセージが表示されます。
「本当にログアウトしますか？」
3. [OK] ボタンをクリックして、ログアウトを確定してください。
4. システムは現在のログインセッションを終了し、ログインページに戻ります。



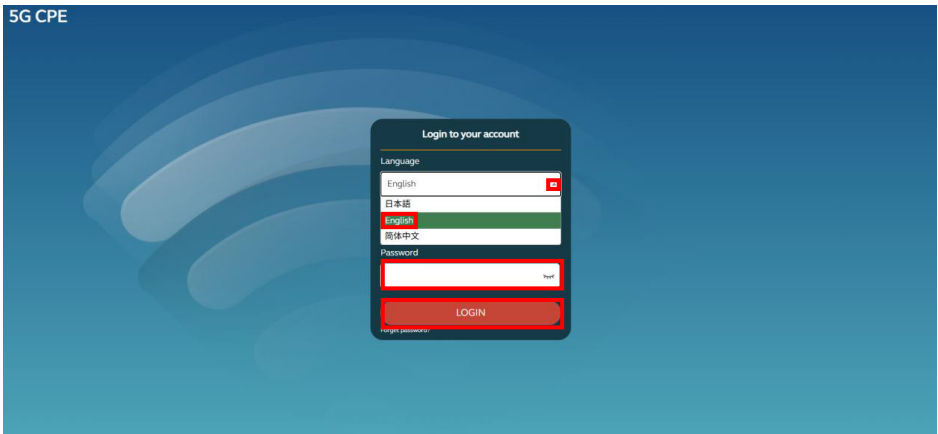
◆言語を切り替える

このページでは、デバイス管理インターフェースの表示言語を英語、日本語、簡体字中国語の間で切り替えられる「言語切り替え」機能を表示しています。

【ログインページで言語を切り替える】

手順

1. ログインページで、「言語 (Language)」のドロップダウンボックスを見つけてください。
2. ドロップダウンボックスをクリックして、利用可能な言語を表示します。
 - ①日本語 (デフォルト言語)
 - ②英語
 - ③簡体中文
3. 希望する言語 (例: 英語) をクリックしてください。
4. ログインページは、選択した言語に即座に切り替わります。
5. パスワードを入力し、「ログイン / LOGIN」をクリックしてログインします。



【ログイン後に言語を切り替える】

手順

1. デバイス管理インターフェースのどのページでも、左下隅にある（現在は英語と表示されている）アイコンをクリックしてください。
2. ドロップダウンメニューには、利用可能な言語が表示されます。
 - ①日本語（デフォルト言語）
 - ②英語
 - ③簡体中文
3. 希望する言語（例：英語）をクリックしてください。
4. ページが自動的に更新され、インターフェースの言語が選択した言語に切り替わります。

