HYBRID Wi-Fi 5G NC03

取扱説明書

Version 1.03

目次

目次 2
第 1 章：はじめに 4
端末の紹介 4
機能および仕様の紹介 4
モバイルネットワーク 4
LAN 4
Wi-Fi 5
セキュリティ 5
管理 5
ハードウェア仕様および物理インターフェース 5
SIM カードの取り付け 6
SIM カードの取り外し 7
バッテリーの充電 7
第 2 章：製品概要 8
外観 8
第 3 章：デバイス設定 9
端末へのログイン 9
ホーム 9
ステータス 9
モバイルネットワーク 10
SIM の選択 10
クラウド SIM 自動切替 11
eSIM アクティベーション 12
モバイル接続 13
プロファイル管理 14
ネットワーク設定 15
PIN コードマネージャ 16
LAN 17
DHCP 17
静的 DHCP 19
クライアント 20
USBで接続する 21
クレードル 22
動作モード 23
Wi-Fi 24
Wi-Fi 情報 24
Wi-Fi 基本設定 25
Wi-Fi 詳細設定 26
WPS 28
Wi-Fi MAC フィルタ 29
セキュリティ保護機能 30
セキュリティ 31
MAC フィルタ 31
IP フィルタ 32
ポートマッピング 33

DMZ 設定 34
IPv4 パケットフィルター設定 35
IPv6 パケットフィルター設定 36
管理 37
SNTP 37
デバイス情報 39
ログインアカウント 40
画面 ロック 40
バックアップ＆復元 41
SWアップデート 42
再起動＆初期化 43
電源・バッテリー 44
高速起動 46
データ使用量 47
1ヶ月 47
3 日 48
クラウド SIM 49
基準時間 49
ログアウト 50
言語の切り替え 51
第 4 章：トラブルシューティング 51
Q&A 52
Q：SSID が表示されるのに接続できない場合は？ 52
Q：サービスがない場合は？ 52
Q：Wi-Fi パスワードを忘れた場合は？ 52
Q：SIM カードがロックされた場合は？ 52
Q：データ接続が失敗する 52

第1章：はじめに

製品の紹介

HYBRID Wi-Fi 5G NC03は、モデム・ルーター・アクセスポイントの3つの機能を一体化した、携帯型のブロードバンド無線ルーターです。
1台の5Gネットワークへ接続し、内部のルーター機能により複数のユーザーや無線デバイス間でインターネット接続を共有できます。
デジタルカメラ、ノートパソコン、ゲーム機、マルチメディアプレーヤーなど、さまざまなWi-Fi対応機器を同時に利用可能です。
HYBRID Wi-Fi 5G NC03は、モバイル通信を利用して独自のWi-Fiネットワークを構築し、外出先でも手軽にインターネット共有を実現します。
5G対応SIMカードを挿入すると、5G信号を高速Wi-Fiに変換し、非5Gデバイスでも5Gの高速通信を快適に利用できます。

機能および仕様の紹介

・5G／4Gによる高速モバイルブロードバンド接続
・Wi-Fi 7（2x2 MIMO）対応
・USB Type-Cポート ×1
・2.4GHz & 5GHz、または 2.4GHz & 6GHz の同時動作に対応
・IPv6対応（IPv4/IPv6デュアルスタック）
・IEEE 802.11b/g/n/ax、802.11a/n/ac/ax/be、802.11ax/be 準拠の無線アクセスポイント
（WPS：Wi-Fi Protected Setup対応）
・Wi-Fi保護アクセス方式：
Open, WPA2-PSK(AES), WPA-PSK/WPA2-PSK(TKIP/AES), WPA3-SAE(AES), WPA2-PSK/WPA3-SAE(AES)
・ファイアウォールセキュリティ搭載
・SOHO、オフィス、家庭用に最適

モバイルネットワーク

・SIMの選択
・クラウドSIM自動切替
・eSIMアクティベーション
・モバイル接続
・プロファイル管理（IPv4、IPv6、またはIPv4/IPv6デュアルスタック）
・ネットワーク設定
・PINコード管理

LAN

・DHCP
・静的DHCP
・接続クライアント一覧
・USBモード設定
・クレードル設定
・動作モード設定（ルーターモード／ブリッジモード）

Wi-Fi

・Wi-Fiステータス
・Wi-Fi基本設定
・Wi-Fi詳細設定
・WPS設定（Wi-Fi Protected Setup）
・Wi-Fi MACフィルター
・セキュリティ保護機能

セキュリティ

・MACフィルター
・IPフィルター
・ポートフォワーディング
・DMZ設定
・IPv4パケットフィルター
・IPv6パケットフィルター

管理

・SNTP設定（時刻同期設定）
・デバイス情報表示
・ログインアカウント設定
・LCDロック設定（画面ロック）
・バックアップと復元
・デバイスソフトウェア更新
・再起動と初期化
・電源・バッテリー
・高速起動設定

データ使用量

・1か月間のデータ使用量
・3日間のデータ使用量
・クラウドSIMデータ使用量
・基準時刻設定

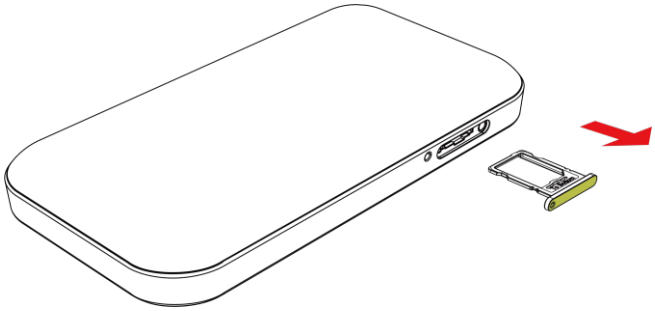
ハードウェア仕様および物理インターフェース

・SIMカードスロット：4FF（nanoSIMカード対応）
・USBポート：USB Type-C ×1
・電源ボタン
・リセットボタン（ピンホールタイプ）

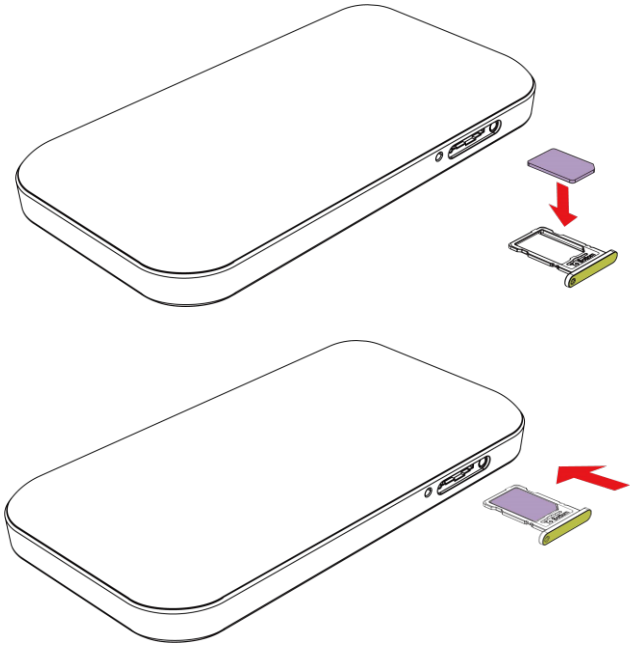
SIMカードの取り付け

1.SIMカードを外側のカードホルダーから慎重に取り外します。
　　このとき、金属端子部分には触れないようにしてください。

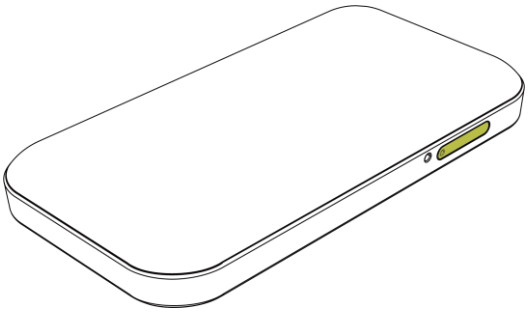
2.SIMカードを正しい向きでスロットに挿入します。



SIMカードスロットを開けます。



SIMカードをスロットに差し込みます。



スロットを閉じます。

注意: SIMカードを曲げたり傷つけたりしないでください。また、静電気、水、ほこりなどにさらさないように注意してください。

SIMカードを取り付けた後に再起動や電源オフを行う必要はありません。

SIMカードの取り外し

1.SIMカード取り出しピンを用意します。もし持っていない場合は、クリップなど先の細い金属製のもので代用することも可能です。

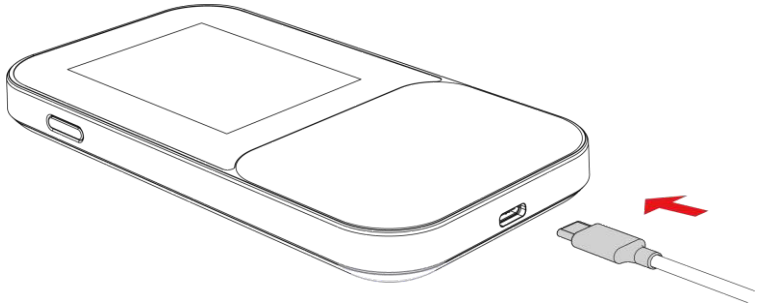
2.本体側面にあるSIMカードスロットを確認します。スロットの近くには、小さな穴が目印としてあります。

3.取り出しピンをスロット横の小さな穴にまっすぐ差し込み、軽く押し込みます。

4.スロットが少し押し出されるので、指でゆっくり引き出してください。

バッテリーの充電

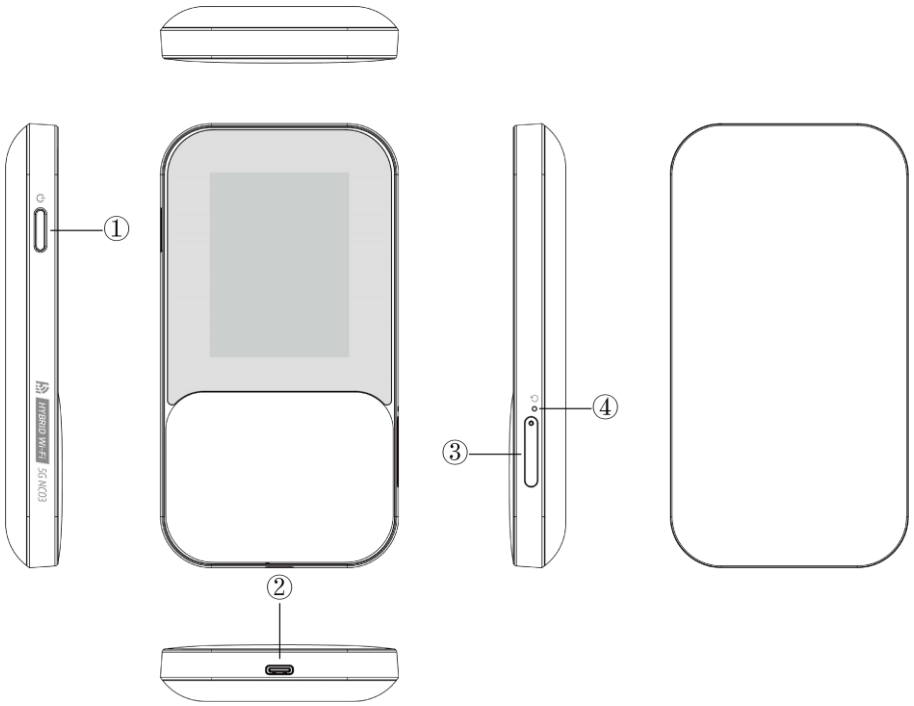
充電するには、充電器の一方の端をコンセントに接続し、もう一方の端を本体の USB Type-Cポート に差し込みます。



注意：バッテリーは取り外しできません。そのため、バッテリーを取り付ける作業は不要です。

第2章：製品概要

外観



①電源ボタン
②USBポート（Type-C™）
③SIMトレイ
④RESETボタン

注意: バッテリーは内蔵式のため、取り外すことはできません。

第3章：デバイス設定

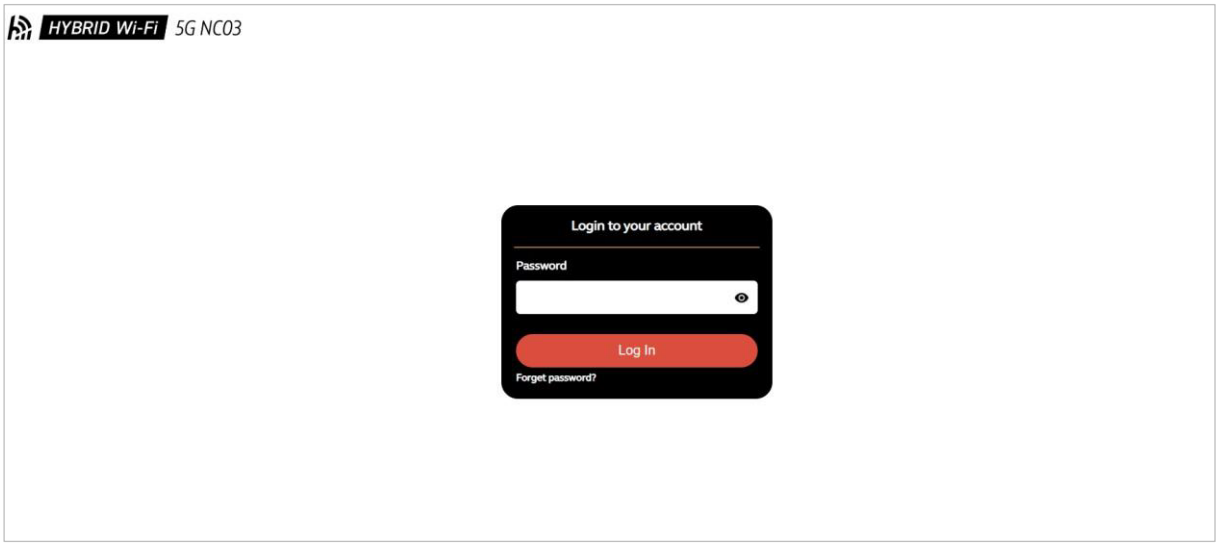
端末へのログイン

1.Wi-FiまたはUSB Type-Cケーブルで接続されていることを確認します。

2.ブラウザを開き、アドレスバーに http://192.168.0.1 を入力します。

3.パスワードを入力して「ログイン」をクリックします。

※初期ログインパスワードは8文字のランダムな値です。
端末画面の システム> Web設定 で初期ログインパスワードを確認してください。



ログイン後、ホーム画面が表示されます。

詳細な操作方法は、本マニュアル内の各項目を参照してください。

ホーム

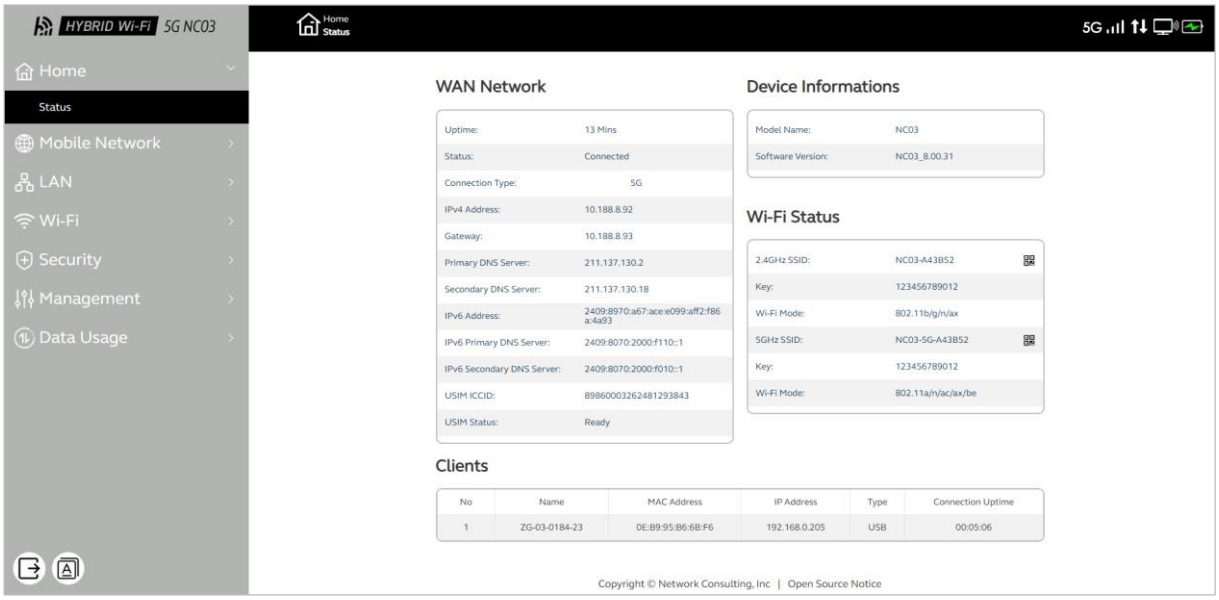
ステータス

ホームページでステータスボタンをクリックすると、端末の基本情報を取得することができます。

これには、WAN ネットワーク（動作時間、ステータス、接続タイプ、IPv4 アドレス など）、デバイス情報（モデル名、ソフトウェアバージョン）、Wi-Fi 状態（2.4GHz SSID、キー、Wi-Fi モード、5GHz SSID、キー、Wi-Fi モード）、接続端末一覧（端末名、MAC アドレス、IP アドレス、タイプ、接続タイムアップ）が含まれます。

手順

1. ホーム > ステータス を選択します。
2. 端末のデバイス情報を確認します。



モバイルネットワーク

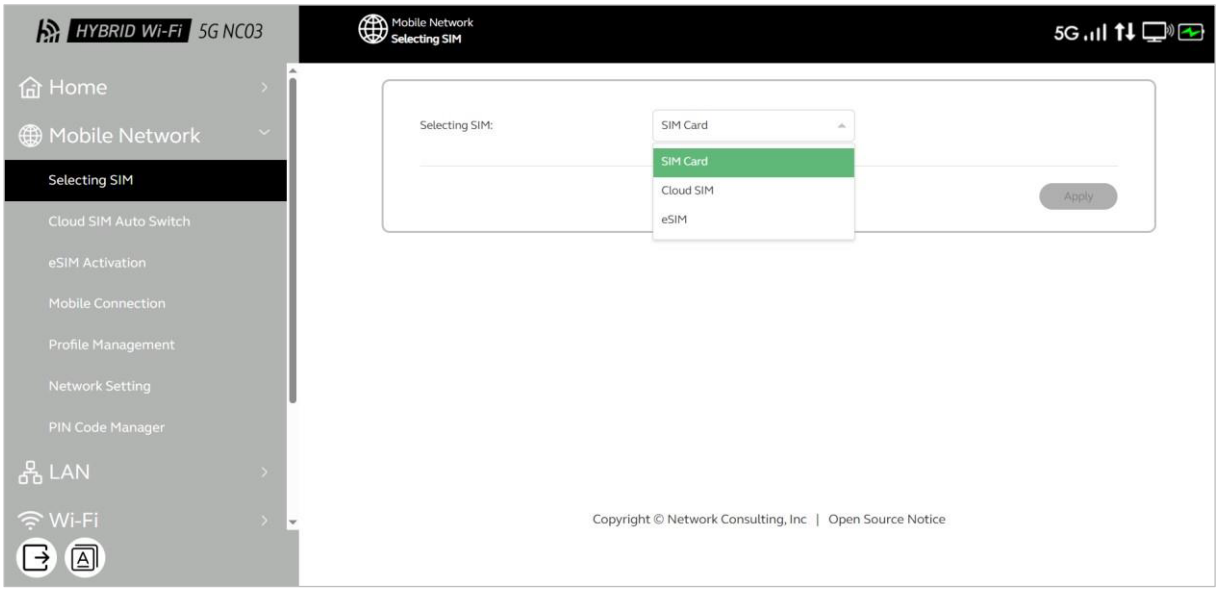
SIM の選択

この機能では、使用するSIM カードを選択できます。
複数のSIM または仮想SIM（クラウドSIM・eSIM）に対応している場合、希望のSIM を指定できます。
選択可能なSIM 種別
・SIM カード（4FF）： 通常の物理SIM カード。
・クラウド SIM： クラウド上の仮想SIM で、物理カードなしで通信可能。
・eSIM： 内蔵型SIM で、デジタルでアクティベーション可能。
これにより、旅行・バックアップ通信・コスト最適化などの用途に応じて柔軟に接続を切り替えられます。
「適用」ボタンを押すと選択内容が有効になります。

注意：使用できるSIM オプションは、機種および通信事業者によって異なります。

手順

1. 「モバイルネットワーク」>「SIM の選択」を開きます。
2. 使用したいSIM 種別（SIM カード／クラウド SIM／eSIM）を選択します。
3. 「適用」を押して設定を保存します。



クラウド SIM 自動切り替え

クラウドSIM 自動切替機能を有効にすると、あらかじめ定義された条件（例：信号強度・回線安定性・設定時間）に基づいて、クラウド SIM と物理SIM／eSIM の間を自動で切り替えます。
これにより、利用環境に応じて常に最適なネットワークへ自動接続します。

設定項目

・設定　　：クラウドSIM自動切り替え機能のオン／オフを切り替えます。
・測定時間：ネットワーク状況をチェックする頻度を設定します。
・SIM カード／sSIM切り替え時間：クラウドSIMのセッション継続時間を設定します。

手順

1.モバイルネットワーク > クラウドSIM 自動切り替え を選択します。
2.「設定」で自動切り替えの 有効にする／無効にする を切り替えます。
3.「測定時間」でネットワーク状況をチェックする頻度を設定します。（1 分、5 分、10 分、30 分、60 分）。
4.「SIM カード／sSIM切り替え時間」でクラウドSIMのセッション継続時間を設定します。（5分、10分、30分、60分、120分、180分）
5.各設定変更は即時に反映されます。「成功」と表示されます

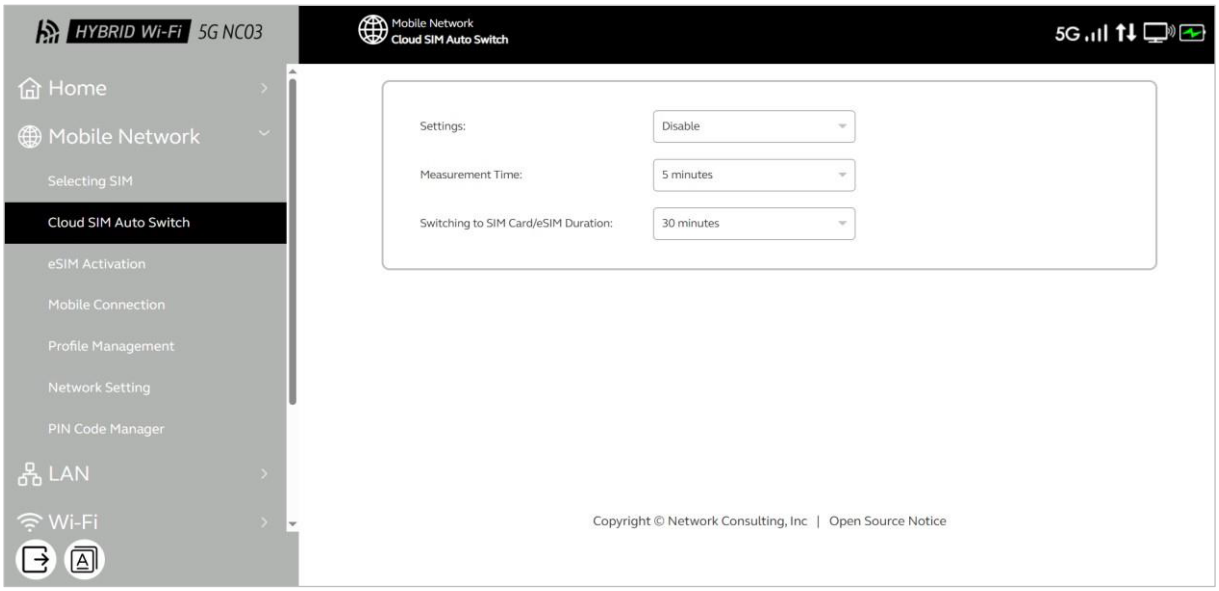
問題が発生した場合は、端末を再起動するか設定画面を再度確認してください。

設定の保存および確認方法

1.保存ボタンを押す必要はありません。変更は自動的に反映されます。
2.最適なパフォーマンスを得るために、設定後は端末を再起動してください。

トラブルシューティング ：切り替えが行われない場合は、以下を確認してください
1.両方のSIMタイプ（SIMカード／eSIMとクラウドSIM）が正しく有効化されていること。
2.「モバイルデータ」が有効になっていること。
3.ネットワーク圏内にいること。

問題が解決しない場合は、通信事業者にお問い合わせください。

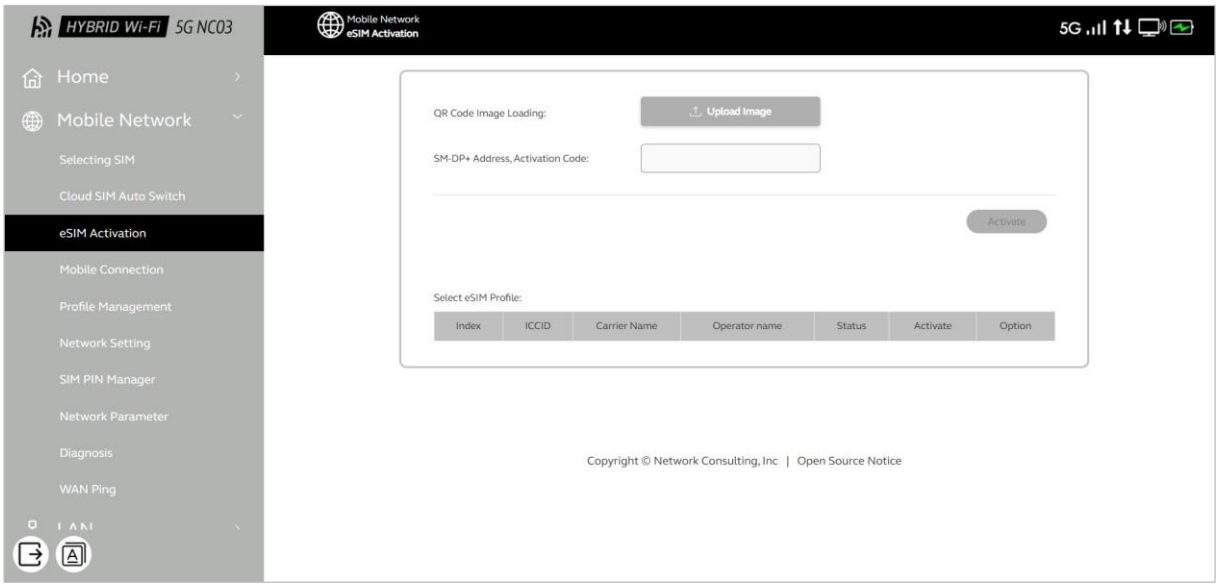


eSIM有効化

この機能では、eSIM の登録・アクティベーション・管理を行います。
QR コードのスキャンまたは手動入力によってeSIM を有効化します。

手順

1.「モバイルネットワーク」>「SIM の選択」でeSIM を選択します。
2.「モバイルネットワーク」>「eSIM有効化」を開きます。
3.以下のいずれかの方法でeSIM を有効化します。（※）
　① または ② の手順で必要な情報を登録したあと、③ を押して有効化を実行します。
4.QR コード画像をアップロード：「イメージアップロード」ボタンをクリックしてQR コード画像を選択します。
5.手動入力：「SM-DP+アドレス」「アクティベーションコード」欄に情報を入力します。
6.「有効にする」をクリックします。
4.「Wi-Fi クライアント構成」ウィンドウが表示されたら、利用可能なWi-Fiネットワークを選び、パスワードを入力して接続する。
5.「eSIM プロファイル一覧」で登録済みeSIM を確認できます。
　表示内容：番号／ICCID／プロファイル名／通信事業者／ステータス／有効化／オプション（削）
6.「有効化」にチェックを入れると そのeSIM が有効になります。不要なプロファイルを削除する場合は、「削除」ボタンをクリックします。
※登録可能なeSIMプロファイル数：最大8プロファイル



モバイル接続

この項目では、端末のモバイルデータ接続およびローミング設定を管理します。

主な機能

・モバイルデータ：すべてのモバイルデータ通信を有効／無効にします。

・ローミング設定：キャリア圏外でのネットワーク接続を管理します。

- 有効：提携ネットワークへ接続（※追加料金が発生する場合があります）
- 無効：ローミングをブロックし、追加料金を防ぎます。

・通信モード（UQ SIM専用）:「スタンダード」モードと「+A（プラスエリア）」モードを選択できます。

補足：通信モード（UQ SIM専用）は、UQ SIMを使用する場合にのみ表示されます。
UQ SIM以外のSIMカードまたはeSIM を使用している場合、この項目は表示されません。

手順

1.「モバイルネットワーク」>「モバイル接続」を選択します。

2.「モバイルデータ」を切り替えます

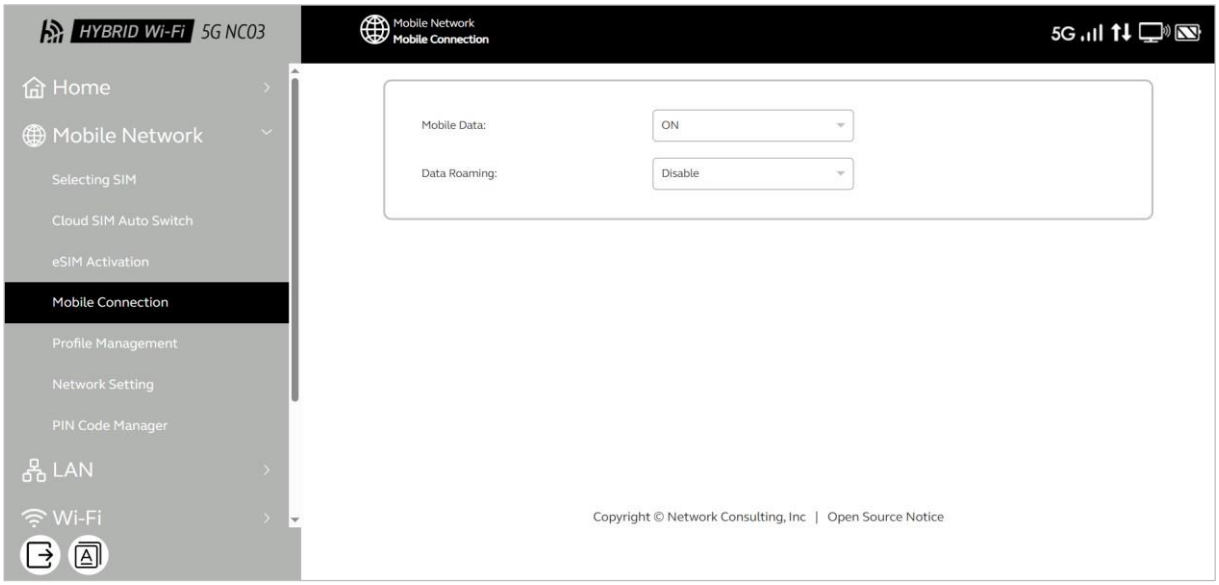
- オン：すべてのモバイルデータ通信を有効にします。
- オフ：すべてのモバイルデータ通信を無効にします。

3.「ローミング設定」を切り替えます。

- 有効にする：通信事業者のサービスエリア外でも提携ネットワークに接続できます。（※追加料金が発生する場合があります）
- 無効にする：ローミング接続をブロックし、追加料金の発生を防ぎます。

4.ステータスバーのアイコンで接続状況を確認します。

- 4G／5G アイコン：モバイルデータ通信が有効であることを示します。
- Rm アイコン：ローミング接続中であることを示します。



プロファイル管理

この機能では、通信事業者のAPN 設定（プロファイル）を確認・編集・追加できます。

1.既存のキャリアプロファイル（APN）の表示と編集
2.新しいプロファイルの作成
3.各通信パラメータの設定

設定項目

・プロファイル名：通信事業者の識別名
・認証タイプ：自動／PAP／CHAP／なし
・APN ：データ通信に使用するAPN名
・認証情報：ユーザー名／パスワード（キャリアにより異なる）
・IP タイプ：IPv4、IPv6、IPv4v6

補足：一部のSIMカードでは、APN情報が自動で判定・設定されます。
自動判定に対応していないSIMカードをご使用の場合は、APN情報を手動で入力してください。

プロファイル作成手順

1.「モバイルネットワーク」>「プロファイル管理」を開きます。
2.「新プロファイル」をクリックします。
3.表示されたダイアログで以下を設定します：
プロファイル名／認証タイプ／APN／ユーザー名／パスワード／IP タイプ
4.「保存」をクリックして完了。

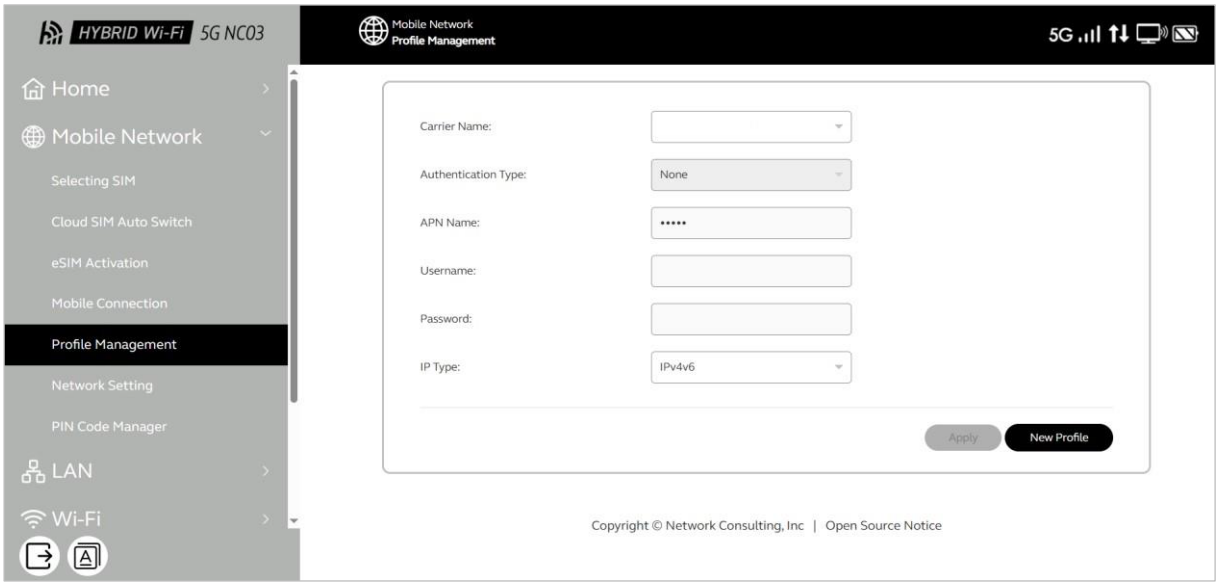
補足：作成したプロファイルは、保存後に自動的に適用されます。

プロファイル切り替え手順

1.「モバイルネットワーク」>「プロファイル管理」を開きます。
2.「プロファイル名」のドロップダウンリストから、使用したいプロファイルを選択します。
3.「適用」ボタンをクリックします。

プロファイル削除手順

1.「モバイルネットワーク」>「プロファイル管理」を開きます。
2.「プロファイル名」のドロップダウンリストから、削除したいプロファイルを選択します。
3.「削除」ボタンをクリックします。



ネットワーク設定

この項目では、端末のモバイルネットワーク動作を詳細に制御できます。

主な設定項目

・ネットワークモード：5G／4G 自動切替、または4G 固定を選択可能。

・ネットワーク検索：

- 自動：最適なネットワークを自動で選択。
- マニュアル：利用可能なネットワークを検索し、任意のキャリアを選択可能。

・5G SA モード：

- オン：スタンドアローン方式（純粋な5Gネットワーク接続、通信事業者の対応必要）
- オフ：ノンスタンドアローン方式（4Gネットワークをアンカーとして利用）

手順

1.「モバイルネットワーク」>「ネットワーク設定」を開きます。

2.「ネットワークモード」で5G／4G を自動または固定で選択します。

3.「ネットワーク検索」を自動または手動で設定します。

4.「5G SA モード」をオンまたはオフに設定します。

5.「適用」をクリックして設定を保存します。

重要事項

・手動設定時はネットワークの通信範囲が制限される場合があります。

・5G SA は通信事業者が対応している必要があります。

・誤った設定を行うと通信が不安定になることがあります。

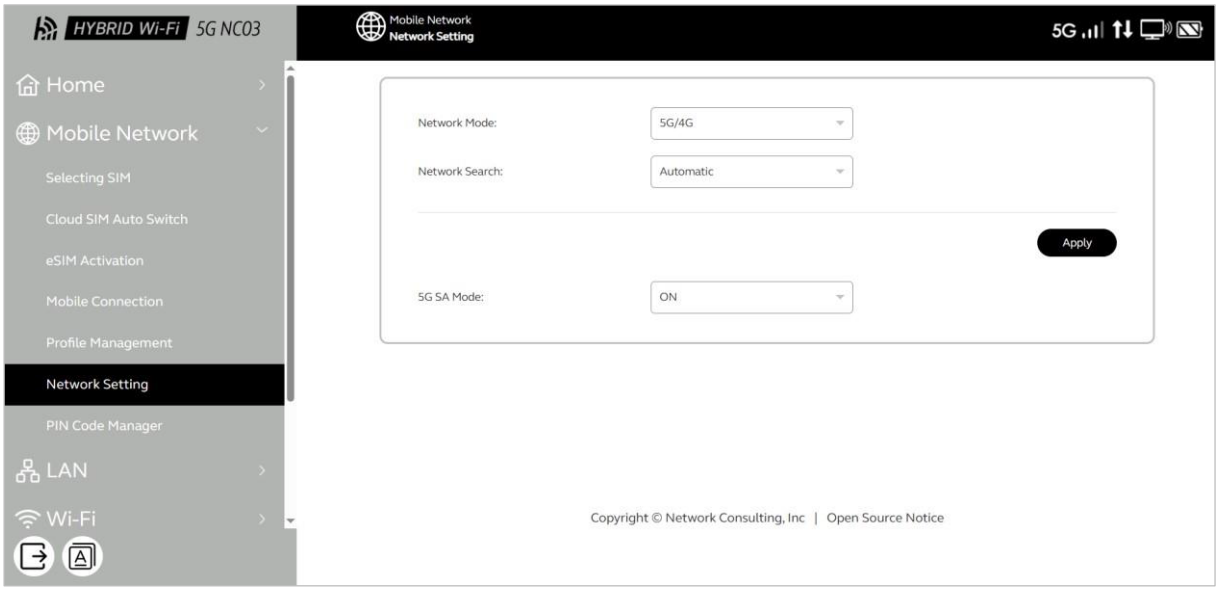
・特別な設定を行わない場合は、「自動モード」が推奨されます。

トラブル時の対処

・通信ができない場合はネットワーク設定を初期化してください。

・SIM カードの状態を確認してください。

・通信事業者にネットワーク対応状況をお問い合わせください。



PINコード管理

この機能は、SIM カードへのアクセスをPIN コードで保護します。

主な機能

1.PIN コード管理

- PIN 認証のオン／オフ切替
- 不正なSIMカード利用を防止

2.PIN コード

- 4～8桁のセキュリティコードを設定または変更

3.残り試行回数

- 残り入力回数を表示（通常3 回）
- 3 回間違えるとSIM がロックされ、PUK コードが必要になります。

手順

1.「モバイルネットワーク」>「PINコード管理」を開きます。

2.「PINコード管理」のプルダウンから以下を選択します。

- オン：PIN 認証を有効化
- オフ：PIN 認証を無効化（初期設定）

3.有効化した場合、「PIN コード」欄に正しいPIN を入力します。

4.「適用」をクリックして保存します。

PINコード管理がオンになっている場合、PINコードを変更することができます。

手順

1.「モバイルネットワーク」>「PINコード管理」を開きます。

2.「PINコード管理」のプルダウンから「PIN コード変更」を選択します。

3.現在のPIN コードを入力します。

4.新しいPIN コードを入力し、確認欄に再入力します。

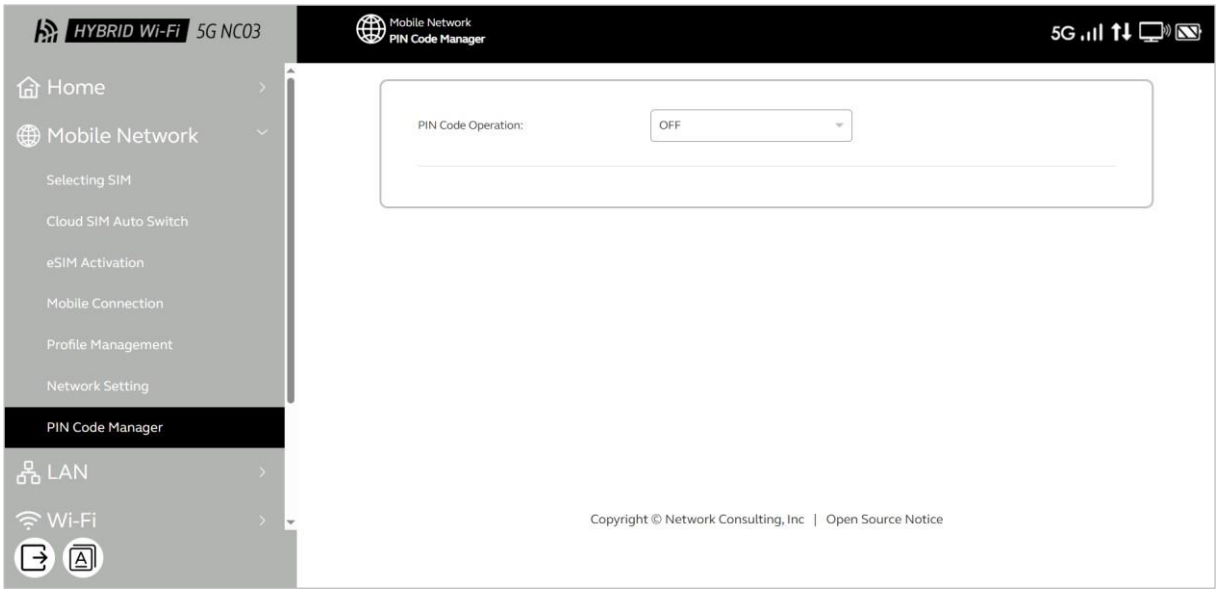
5.「適用」をクリックして保存します。

セキュリティ上の注意

トラブルシューティング

・「正しくないか有効ではないSIM PINです。」と表示される場合：

- Caps Lock／Num Lock の状態を確認してください。
- 通信事業者が提供する初期PINコードを使用してください。
- SIMがロックされた場合は、通信事業者に連絡してPUKコードを取得してください。



LAN 設定

DHCP

DHCP サーバー機能は、ローカルエリアネットワーク（LAN）上のデバイスに自動でIP アドレスを割り当てる機能です。

主な項目

・DHCP サーバ：自動でIPアドレスを割り当てるための機能
・IP アドレス：DHCP サーバのアドレス（通常はルーターのアドレス）
・サブネットマスク：LAN内で使用するネットワーク範囲を定義
・IP アドレス範囲：デバイスに割り当てることができるIPアドレスの範囲
・リース期間：割り当てられたIPアドレスが有効となる時間（秒単位）
・DNS モード：自動的にDNSサーバーを取得するか手動で指定するかを選択

手順

1.「LAN」>「DHCP」を開きます。

2.DHCP サーバを有効または無効に設定します。

- 有効にする：IPアドレスを自動的に割り当てます
- 無効にする：手動でIP設定を行う必要があります

3.IPアドレスとサブネットマスクを設定します。

- 例：IP アドレス：192.168.0.1
- 例：サブネットマスク：255.255.255.0

4.IP 範囲を設定します（必要に応じて変更）

- 開始アドレス：192.168.0.2（推奨最小値）
- 終了アドレス：192.168.0.254（推奨最大値）

※固定IP機器と重複しない範囲を設定してください

5.リース時間を設定します

- 3600 秒（1時間）：ゲストネットワーク向け
- 86400 秒（24時間）：標準設定
- 604800 秒（1週間）：安定したネットワーク向け

6.DNS モードを設定します。

- 自動：ISPからDNSサーバーを自動取得します
- 手動：任意のDNSサーバーを指定します
  - プライマリDNS サーバー：主要DNSサーバーのIPアドレスを入力
  - セカンダリDNS サーバー：補助DNSサーバーのIPアドレスを入力

7.「適用」をクリックして保存します。

※サービスの再起動に30秒以上かかる場合があります。

推奨設定

・下位のIPアドレス（例：192.168.0.2～192.168.0.50）は、固定IPを使用する機器に割り当てておくことを推奨します。

・大規模なネットワーク環境では、必要に応じてIPアドレス範囲を拡張してください。

・一時的に接続する機器が多い環境では、リース期間を短めに設定することで効率的な運用が可能です。

トラブルシューティング：デバイスが接続できない場合

・DHCPが有効になっているか確認してください

・割り当て可能なIPアドレスが残っているか確認してください

・IPアドレスの重複がないか確認してください

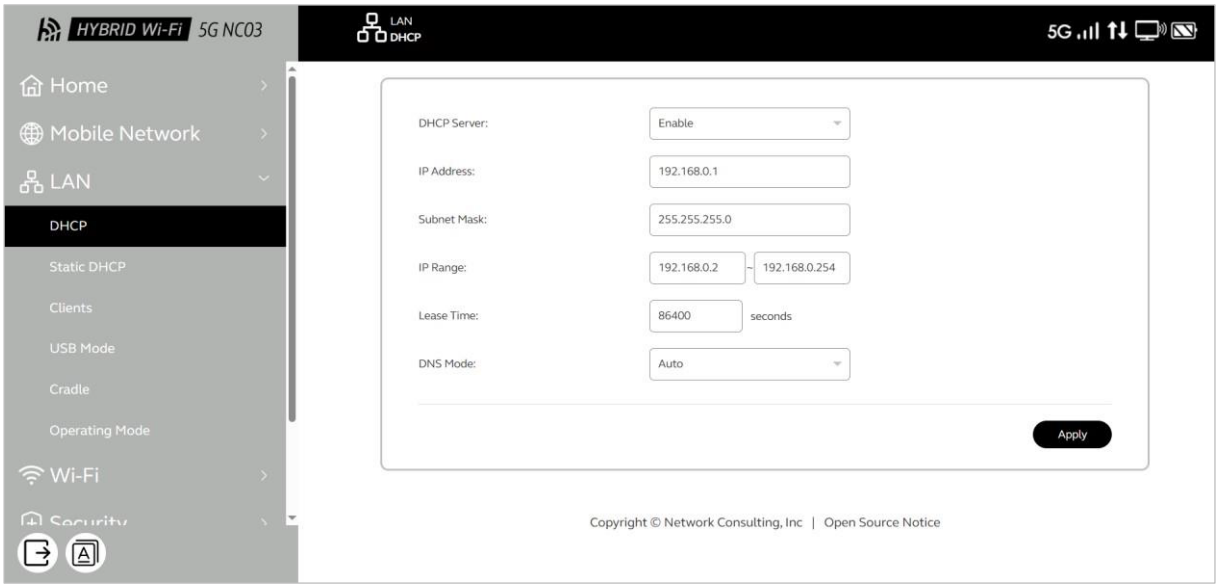
・DHCPサービスを再起動してください

セキュリティ上の注意

・既定のIP範囲を変更すると、セキュリティが向上します

・接続中のクライアントを定期的に監視してください

・公共Wi-Fiなどでは、リース期間を短く設定することを推奨します



DHCP手動割当

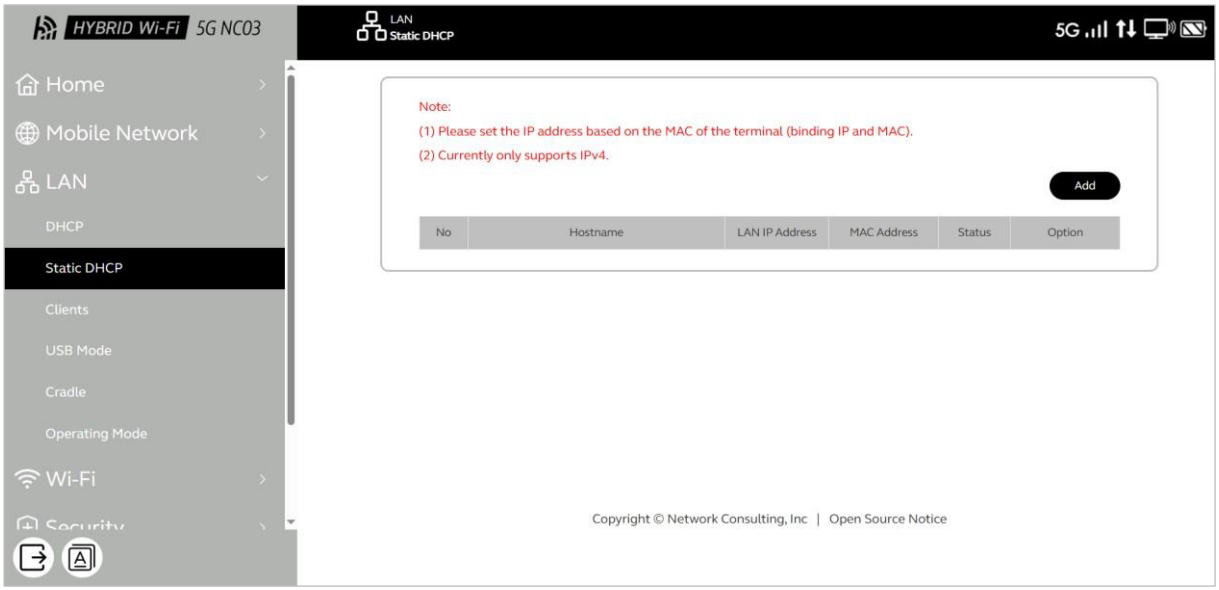
DHCP手動割当は、MACアドレスと固定IPアドレスを紐づけて、特定の端末へ常に同じIPアドレスを割り当てる機能です。

注意事項

1.割り当てIPは必ずデバイスのMACアドレスに基づいて設定してください。
2.IPv4のみ対応しています。

手順

1.「LAN」>「DHCP手動割当」を開きます。
2.「追加」をクリックします。
　各項目（ホスト名／LAN IPアドレス／MACアドレス／ステータス）を入力します。
3.「保存」をクリックして設定完了です。



接続端末一覧

DHCPクライアントリストでは、ネットワークに接続中の全デバイスをリアルタイムで監視・管理できます。

機能概要

1.ネットワーク可視化

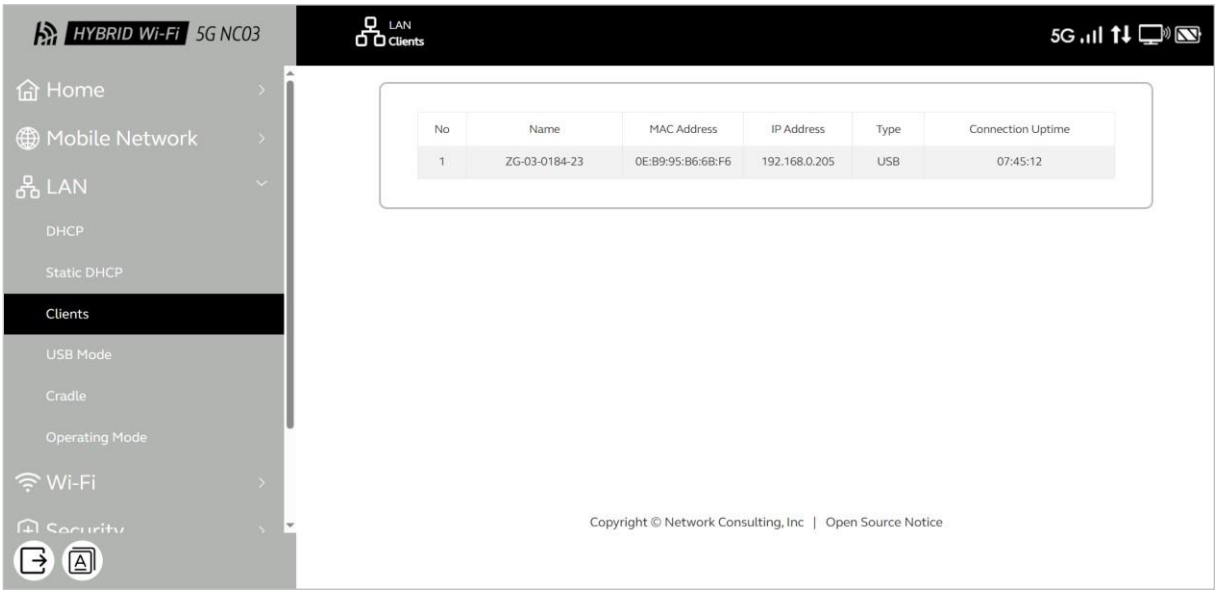
- 現在接続中の端末を一覧表示。
- 有線（USB）および無線（Wi-Fi）接続を区別。
- 接続時間（稼働時間）を表示。

2.デバイス識別情報

- ホスト名または端末識別名を表示。
- MACアドレスによる個別識別が可能。
- 割り当て済みIPアドレスを表示。

3.接続監視

- 接続種別（USB／Wi-Fi／LAN）を表示。
- セッション時間を監視。
- 不正デバイス検出に利用可能。



USBで接続する（USBモード）

USBモードでは、HYBRID Wi-Fi 5G NC03をUSB経由で柔軟に利用できます。

主な特徴

1. デュアル用途USBポート

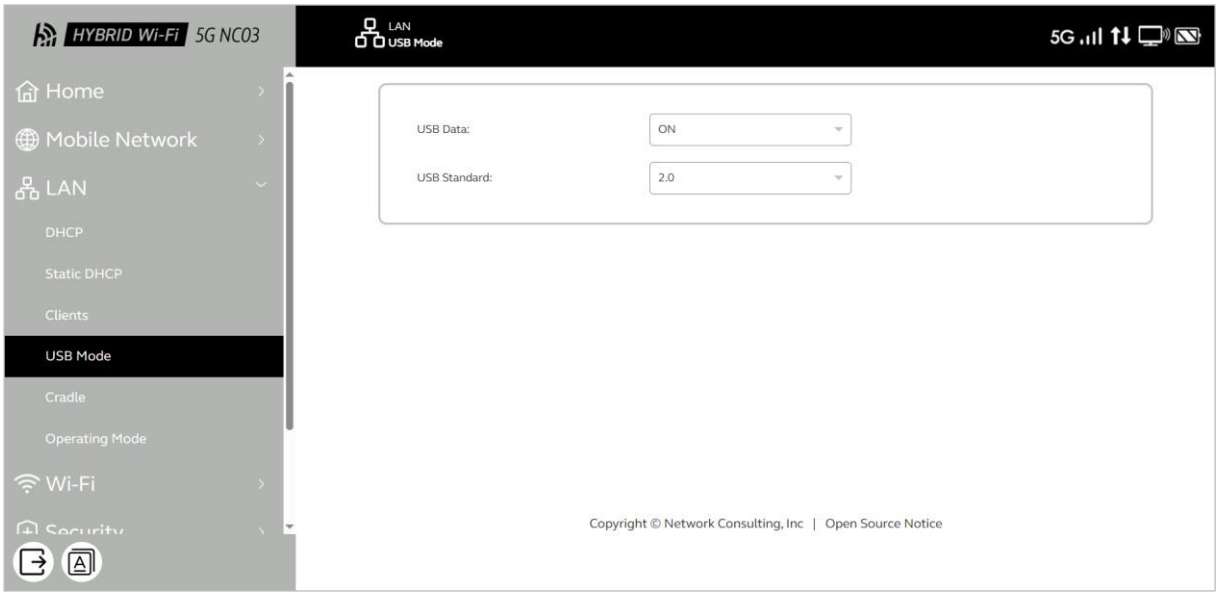
- ネットワーク共有とデバイス充電を両立。
- USBテザリングに対応。
- 各種USBクラスデバイスに互換。

2.動作

- データ通信と電源供給を同時に行います。

手順

1.「LAN」>「USBモード」を開きます。
2.「USBテザリング」スイッチをオンまたはオフに設定します。
- オン：データ転送機能を有効化。
- オフ：充電専用モード。
3.「USB規格」を選択します（2.0 または 3.1）。



クレードル

本機がWi-Fi AP モード（無線アクセスポイントモード） で動作している場合、クレードル上での スクリーンセーバー表示 は自動的に無効化されます。「ディスプレイ」設定が「オン」にであっても、LCD 画面はスクリーンセーバーモードに入りません。

備考

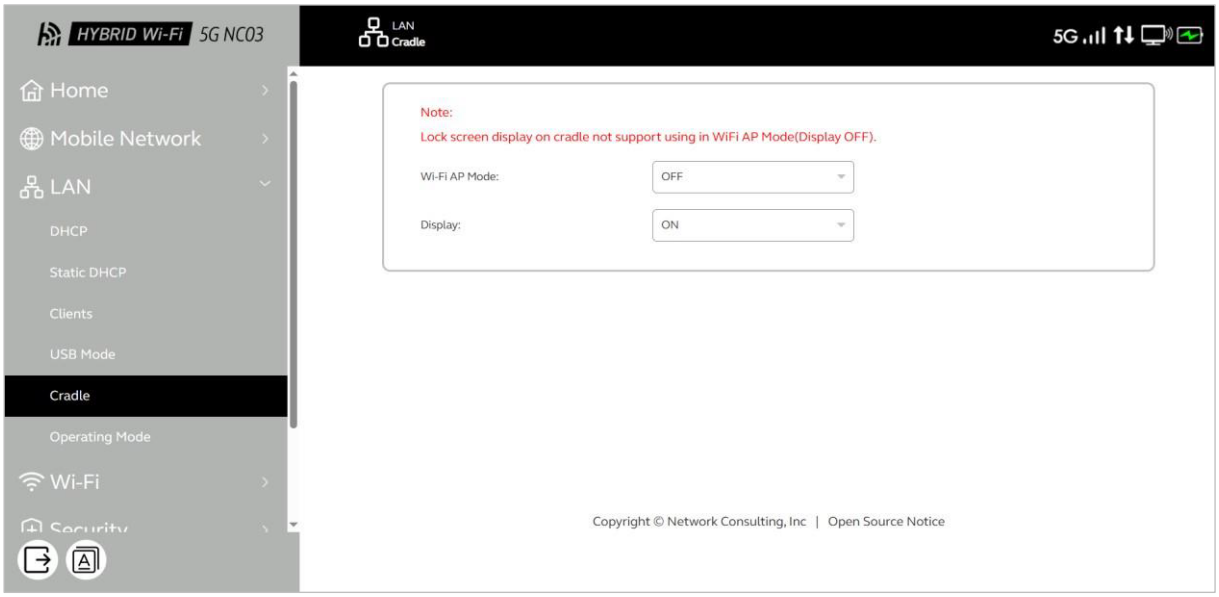
・スクリーンセーバー表示」とは、本機をクレードルに設置した際に自動的に表示される待機画面（時刻やネットワーク状態など）を指します。
・スクリーンセーバー表示は、Wi-Fi AP モード がオンの場合には使用できません。

状態例

Wi-Fi APモード：オフ
ディスプレイ：オン
この状態でクレードルに設置した際に、スクリーンセーバーの内容が通常どおり表示されます。

手順

1.「LAN」>「クレードル」を開きます。
2.クレードル設置時にスクリーンセーバーを表示したい場合：
- Wi-Fi APモードをOFFのままにします。
- クレードル設置時に画面が表示されます。
- ディスプレイ：ON → 画面が現在アクティブな状態で動作します
- ディスプレイ：OFF → 画面は自動画面オフ時間の経過後に自動的に消灯します。
3.Wi-Fi APモードを有効化する場合：
- Wi-Fi APモードをオンにします。
- システムが自動的にクレードルの画面表示を無効化します。
※ディスプレイ設定がオンのままであっても、クレードルの画面は点灯しません。
これはシステムの正常な動作であり、デバイスの故障を意味するものではありません。



動作モード

この設定では、MiFiのネットワーク動作モードを選択できます。
主に以下の2つのモードがあります。

1.ルーターモード（デフォルト）

- 通常のルーターとして動作します。
- NAT、DHCP、ファイアウォール機能をすべて提供。
- 家庭・オフィス環境に最適。

2.ブリッジモード（IPパススルー）

- モバイルデータをLANへ直接ブリッジ接続。
- ルーター機能（NATなど）をバイパスします。
- 管理用IPは手動で静的設定が必要です。
- WAN直結などの高度な用途向け。

注意事項

1.ブリッジモードでは、モバイルデータ通信のみでインターネットにアクセスできます。
2.ブリッジモードを有効にすると、管理画面からログアウトされます。
　再ログインするには、コンピューターに手動で静的 IP を割り当てる必要があります。

手順

1.「LAN」>「動作モード」を開きます。
2.使用したいモードを選択します。
- ルーターモード：標準的なルーター動作
- ブリッジモード：モバイルデータを直接LANに接続
3.「適用」をクリックします。

ブリッジモードの設定方法

ブリッジモードを選択した場合は、ブリッジ機能を有効にするための設定を行います。

1.ブリッジモードを選択します

2.「ブリッジモード」の設定項目で接続方法を選択します。

- USB/Cradle：USB テザリングによる直接接続、またはクレードルを介した 有線 LAN 接続
- Wi-Fi：Wi-Fi 経由でのインターネット共有

補足：ブリッジモードをオン にすると、IP パススルー機能が自動的に有効になります。

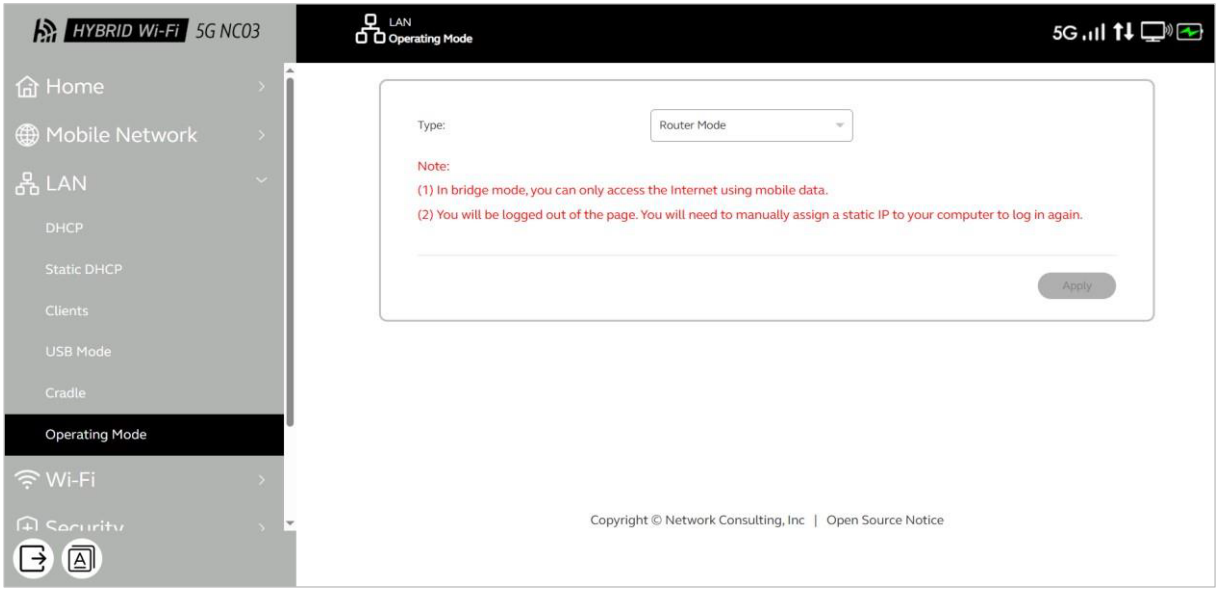
3.「適用」をクリックします。

注意

・ブリッジモードは、ネットワーク検証や企業用途など、上級者向けの構成です。

・一般的な利用（複数端末でのWi-Fi共有など）の場合は、ルーターモードでの使用をおすすめします。

・モードを切り替えると一時的に通信が切断されます。設定完了後、数十秒ほど待ってから再接続してください。



Wi-Fi

Wi-Fi情報

本製品はデュアルバンド対応の無線ルーター（またはアクセスポイント）として動作し、

2.4GHz／5GHz／6GHz、またはそれらの組み合わせ（2.4GHz+5GHz、2.4GHz+6GHz）に対応します。

現在の Wi-Fi ステータス例

・SSID：NC03-A43B52、NC03-5G-A43B52、NC03-6G-A43B52

・SSID 非表示設定：無効（ブロードキャスト有効）

・セキュリティモード：WPA2-PSK／WPA3-SAE ハイブリッド（AES 暗号化）

・チャネル：自動設定、屋内モード（W52、W53 帯域対応）

・接続ユーザー数：0（未接続）

・Wi-Fi モード：IEEE 802.11b/g/n/ax、802.11a/n/ac/ax/be、802.11ax/be

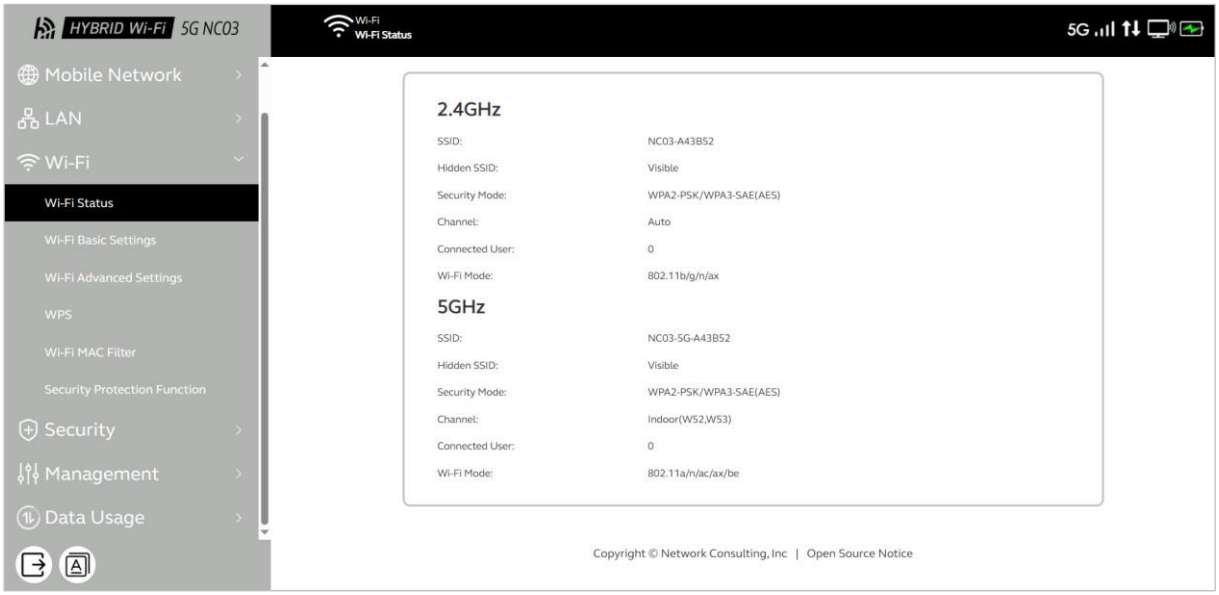
設定可能項目

1.SSID カスタマイズ
- ネットワーク名を変更
- SSID の表示／非表示を設定

2.セキュリティオプション
- 2.4GHz／5GHz：Open、WPA2-PSK(AES)、WPA-PSK/WPA2-PSK(TKIP/AES)、WPA3-SAE(AES)、WPA2-PSK/WPA3-SAE(AES)
- 6GHz：Open、WPA3-SAE(AES)

3.チャネル管理
- 自動選択（推奨）
- 手動設定も可能

4.モード選択
- 旧規格対応（802.11b/g/n/ax など）
- 通信速度と通信範囲をバランス設定可能



Wi-Fi 基本設定

この項目では、各バンド（2.4GHz／5GHz／6GHz／2.4GHz+5GHz／2.4GHz+6GHz）の基本設定を行います。

主要設定項目

・ネットワーク識別
- SSID（例：NC03-A43B52）
- 表示設定（SSID をブロードキャストするかどうか）

・セキュリティ設定
- ハイブリッド方式（WPA2-PSK／WPA3-SAE）
- AES 暗号化対応
- パスワード保護（非表示入力）

・パフォーマンス設定
- Wi-Fi モード：802.11b/g/n/ax／802.11a/n/ac/ax/be／802.11ax/be
- チャネル選択：自動最適化
- クライアント数制限：最大 32 台

・バンド管理
- 2.4GHz、5GHz、6GHz、または複合バンドを選択可能
- 各バンドを有効／無効に設定可能

手順

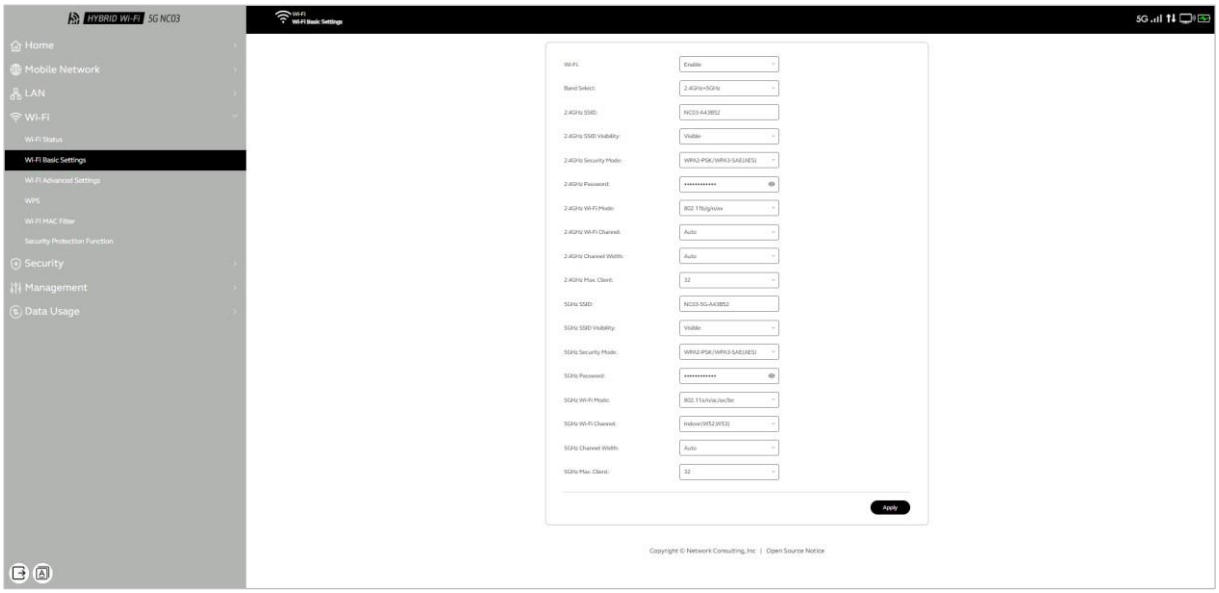
1.「Wi-Fi」>「Wi-Fi 基本設定」を開きます。

2.「バンド選択」ドロップダウンから希望のバンドを選びます。

3.各項目（SSID、可視性、セキュリティ、パスワード、Wi-Fi モード、チャネル、チャネル幅、最大クライアント数）を設定します。

4.「適用」をクリックして保存します。

注意：「適用」をクリックするとホットスポットが自動的に再起動します。



Wi-Fi 詳細設定

この設定では、Wi-Fi 通信の出力やセキュリティレベルを細かく制御できます。
業務・高密度環境での運用に適した高度な設定が可能です。

主な設定項目

1. 送信出力
- 調整可能値：12.5%、25%、50%、100%
- 既定値：100%（最大カバレッジ）
- 出力を下げると干渉を減らせますが、範囲が狭くなります。

2. PMF
- 高度なセキュリティプロトコル。

- 無線盗聴攻撃を防止。
- WPA3 準拠時は必須。

3. プライバシーセパレーター機能
- 同一 Wi-Fi 内のデバイス同士の通信を制御。
- 既定値：無効（Disable）。
- 「ネットワーク分離」設定：LAN 全体を分離（主にゲスト Wi-Fi 用途）。
- 「Wi-Fi 端末分離」設定：Wi-Fi 機器同士の通信を遮断。

手順

1.「Wi-Fi」>「Wi-Fi 詳細設定」を開きます。
2.「Tx Power」を設定（既定 100%、必要に応じて 25～50%などに変更）。
3.「PMF」スイッチをオン／オフに設定。
4.「プライバシーセパレーター機能」のドロップダウンから
「無効」「ネットワーク分離」「Wi-Fi 端末分離」を選択。

技術上の注意事項

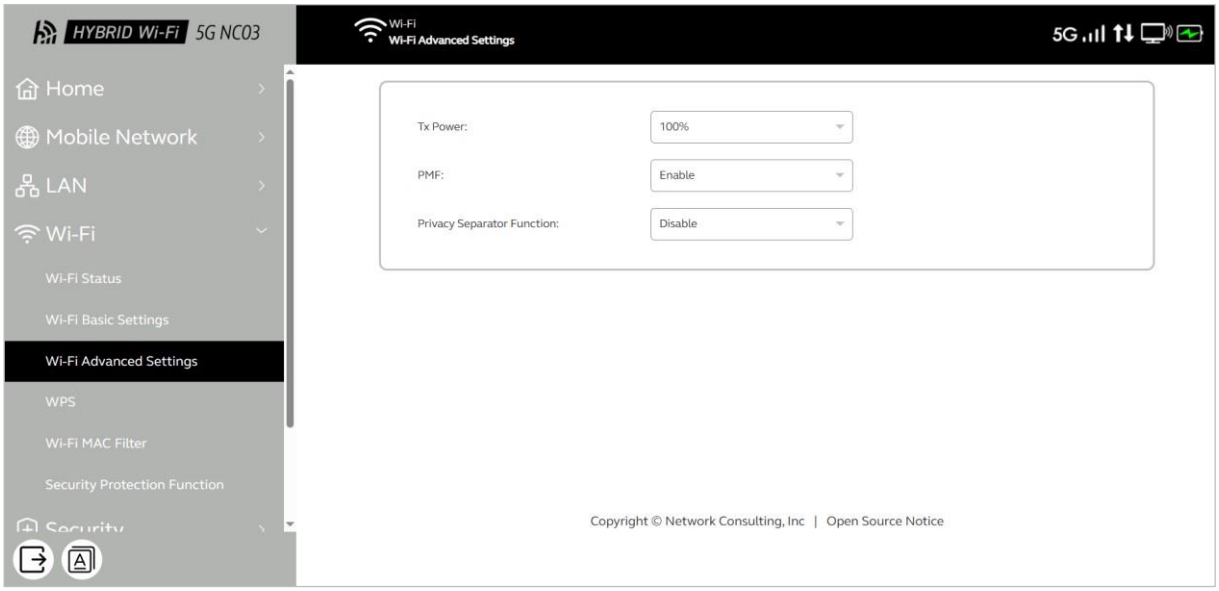
1.送信出力：
- 100%：広範囲・大型空間（倉庫など）
- 50%以下：小規模エリア、省電力運用

2.PMF の推奨設定：
- 企業ネットワーク：必須モード
- 混在環境：任意モード
- 旧機種互換が必要な場合のみ無効化可。

3.トラブル発生時：
- 送信出力を 100%に戻す。
- 一時的に PMF を無効化して確認。
- 特定端末で問題がある場合は分離機能を見直す。

セキュリティ警告

送信出力を 30%以下にすると、通信の死角が生じ、
外部から不正アクセスを受けやすくなる可能性があります。



WPS（Wi-Fi Protected Setup）

WPS 機能を使用すると、複雑なパスワードを入力せずに安全な Wi-Fi 接続を簡単に行うことができます。

主な機能

1. 接続モード
   - PBC（プッシュボタン接続）：Web UI 上で操作します。
   - PIN コード方式：接続する端末の PIN を入力します。
   - AP-PIN 方式：アクセスポイント側で生成される PIN を使用します。
2. セキュリティ規格
   - WPA2 セキュリティ標準に準拠。
   - 暗号化された認証情報を自動生成。
   - 接続受付時間は 2 分間の制限付き。
3. 互換性
   - すべての WPS 対応デバイスと互換。
   - 2.4GHz／5GHz 帯で同時動作可能。
   - 旧 WPS デバイスとの後方互換性あり。

PBC（プッシュボタン接続）

手順

1. 「Wi-Fi」>「WPS」を開きます。
2. 「接続」ボタンをクリックします。
3. 対応デバイス側で WPS ボタンを押すと、自動的に接続が確立されます。

ステーション PIN 方式

手順

1. 「Wi-Fi」>「WPS」を開きます。
2. 「接続モード」ドロップダウンから「PIN」を選択します。
3. 「クライアント PIN」欄に接続デバイスの PIN コードを入力します。
4. 「接続」をクリックします。

AP PIN 方式

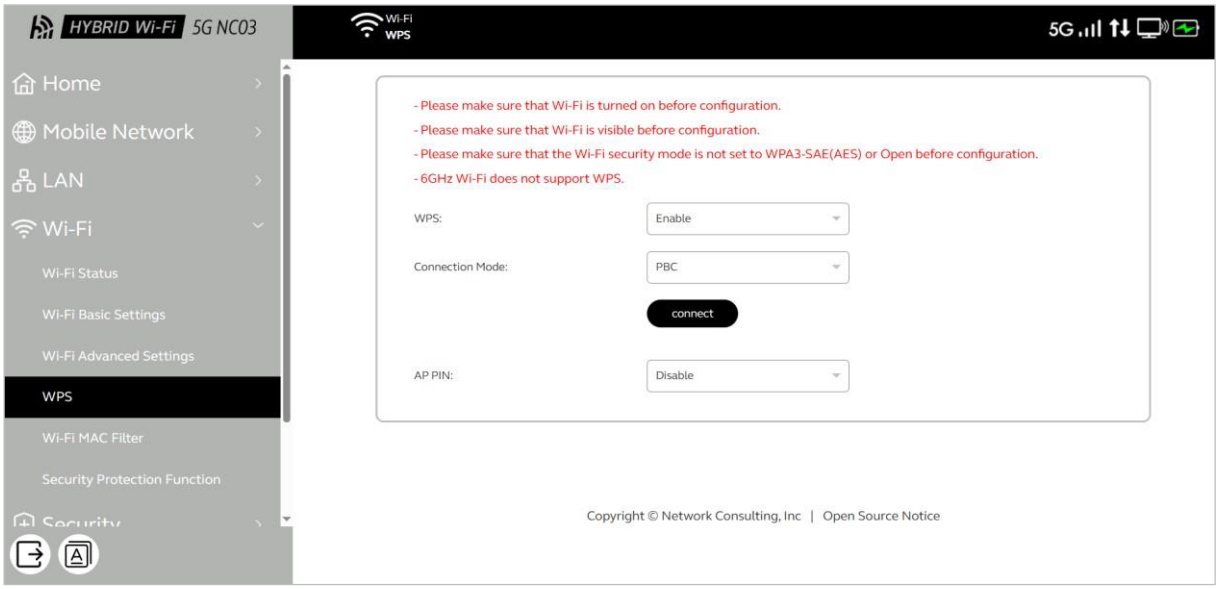
手順

1. 「Wi-Fi」>「WPS」を開きます。
2. 「AP PIN」ドロップダウンリストから「有効」を選択します。
3. 接続する端末に Web UI 上の PIN コードを入力します。

備考

・PIN リセット：初期 PIN コードに戻します。

・PIN 生成：新しい PIN コードを発行します。



Wi-Fi MAC フィルター

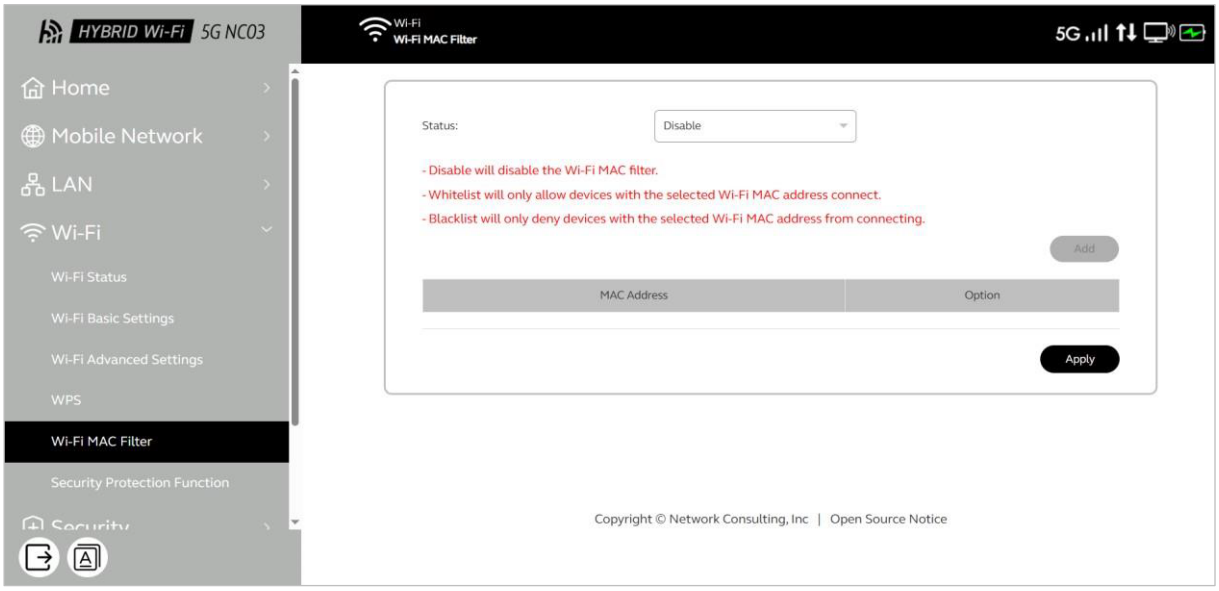
Wi-Fi MACフィルターは、NC03のWi-Fiに接続できるデバイスをMACアドレスで制限する機能です。

主な設定項目

1. フィルターモード
   - 無効：MAC フィルター機能をオフにします。
   - ホワイトリスト：指定した MAC アドレスのデバイスのみ接続を許可します。
   - ブラックリスト：指定した MAC アドレスのデバイスのみ接続を拒否します。
2. セキュリティ効果
   - 不正端末の接続を防止。
   - 他のセキュリティプロトコル（例：WPA3）と併用可能。
   - 暗号化と組み合わせることで MAC 偽装にも強くなります。
3. 管理機能
   - MACアドレス最大登録数：ホワイトリスト／ブラックリスト各16件。
   - すぐに有効／無効を切り替え可能。
   - すべての Wi-Fi 帯域（2.4GHz／5GHz／6GHz）に対応。

手順

1. 「Wi-Fi」>「Wi-Fi MAC フィルター」を開きます。
2. モードを「無効／ブラックリスト／ホワイトリスト」から選択します。
3. 「追加」ボタンをクリックし、対象デバイスの MAC アドレスを入力します。
4. 「適用」をクリックして設定を保存します。



セキュリティ保護機能

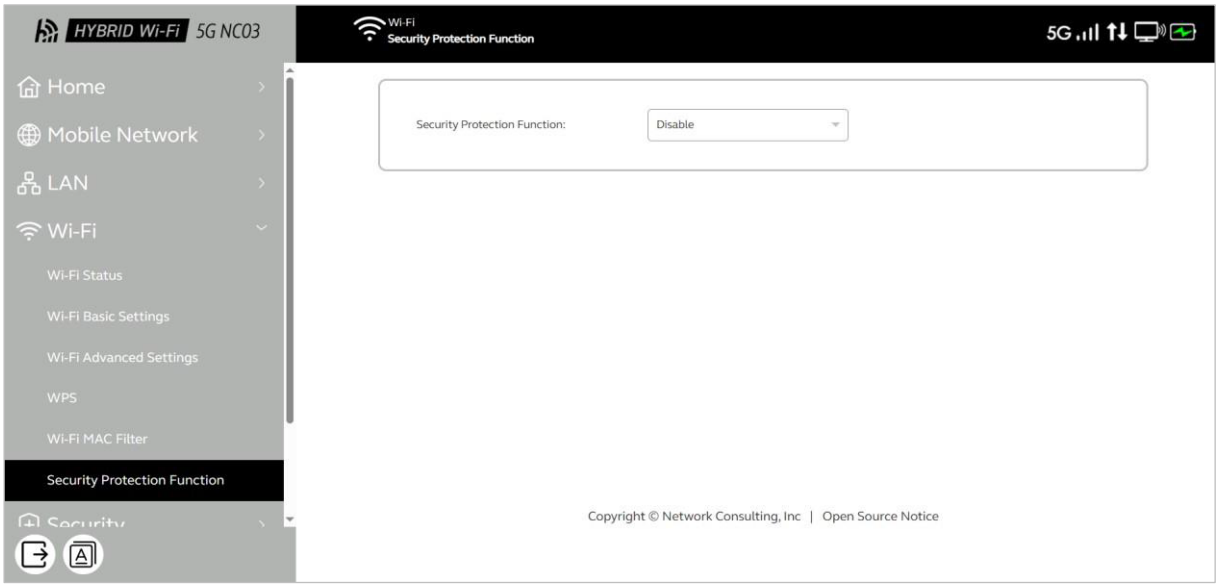
この機能は、ルーター全体のセキュリティ機能を一括で有効化するマスタースイッチです。
有効化すると、以下のような統合型セキュリティ保護が適用されます。

主な機能内容

・侵入検知・防止システム（IDS／IPS）
　ネットワークトラフィックを監視し、不正アクセスや DoS 攻撃などを自動的に検出・遮断。
・悪意あるサイトのブロック
　フィッシングサイトやマルウェア配布サイトへのアクセスを自動的に遮断。
・ウイルス・マルウェアフィルタリング
　通信データをスキャンし、ウイルス感染リスクを低減。
・攻撃ログの記録
　検知・防御イベントをログとして保存し、管理者が確認可能。

手順

1. 「Wi-Fi」>「セキュリティ保護機能」を開きます。
2. 「セキュリティ保護機能」の右側にあるドロップダウンからモードを選択します。
   - 有効：推奨。包括的なセキュリティ保護を有効化。
   - 無効：トラブルシューティングなど一時的に使用。



セキュリティ

MAC フィルタ

MAC アドレスフィルタリングは、IPv4 アドレスで動作するセキュリティ機能で、各デバイスの MAC アドレスに基づいて接続を許可または拒否します。Wi-Fi　MACフィルターが「NC03へのWi-Fi接続」を制限するのに対し、本機能は「Wi-Fi接続後のインターネット通信」を許可／拒否します。

MAC アドレスについて

各ネットワーク機器には固有の MAC（Media Access Control）アドレスが割り当てられています。これは 6 組の 16 進数で構成され、例として XX:XX:XX:XX:XX:XX の形式をとります。

動作モード

・無効：MAC フィルタ機能を停止。

・ホワイトリスト：登録された MAC のみ通信を許可。

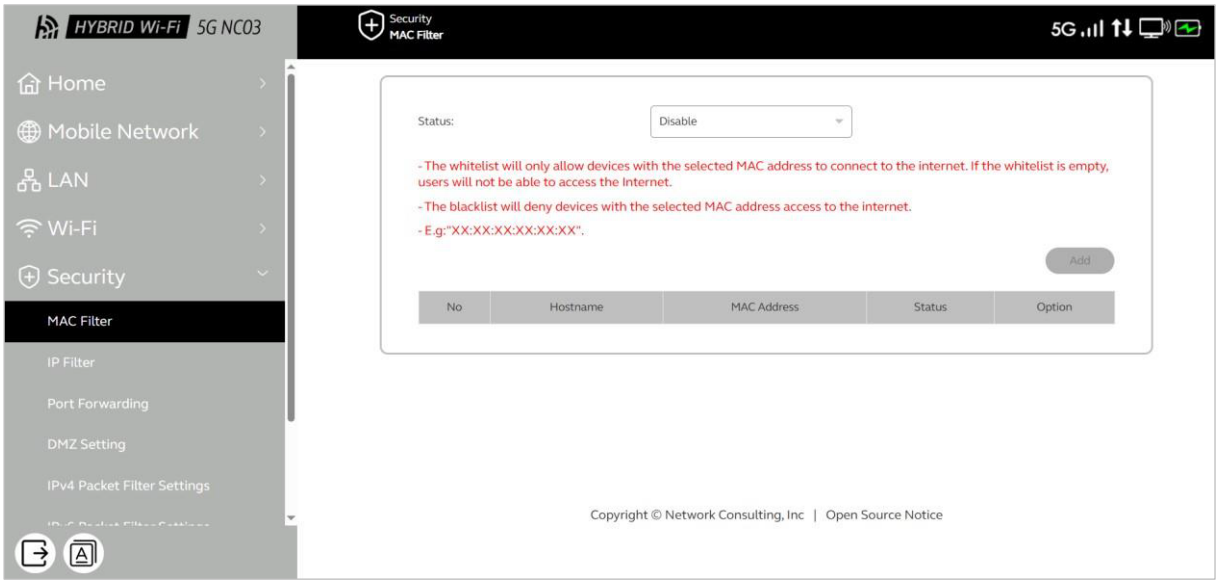
・ブラックリスト：登録された MAC を通信から除外。

※最大登録数：各32件

※ホワイトリストが空の場合、全てのデバイスが通信不可となります。

手順

1. 「セキュリティ」>「MAC フィルター」を開きます。
2. フィルタリングモードを選択します。
   - ブラックリスト：指定したアドレスからの通信を拒否。
   - ホワイトリスト：指定したアドレスのみ通信を許可。
3. 「追加」をクリックし、ホスト名・MAC アドレス・状態を設定します。
4. 「保存」をクリックして完了です。



IP フィルター

IP フィルター機能を使用すると、IP アドレス・プロトコル・ポート番号を基準に通信を制御できます。
これにより、特定の通信の許可／拒否を柔軟に設定できます。

設定項目

・インデックス：設定ルールの番号。
・LAN IP アドレス：LAN 側の送信元または宛先アドレス。
・LAN ポート：LAN 側で利用するポート番号。
・WAN IP アドレス：インターネット側の送信元または宛先アドレス。
・WAN ポート：外部通信で使用するポート番号。
・プロトコル：通信方式（TCP／UDP など）。
・ステータス：ルールの有効・無効。
・オプション：ルールの編集・削除操作。

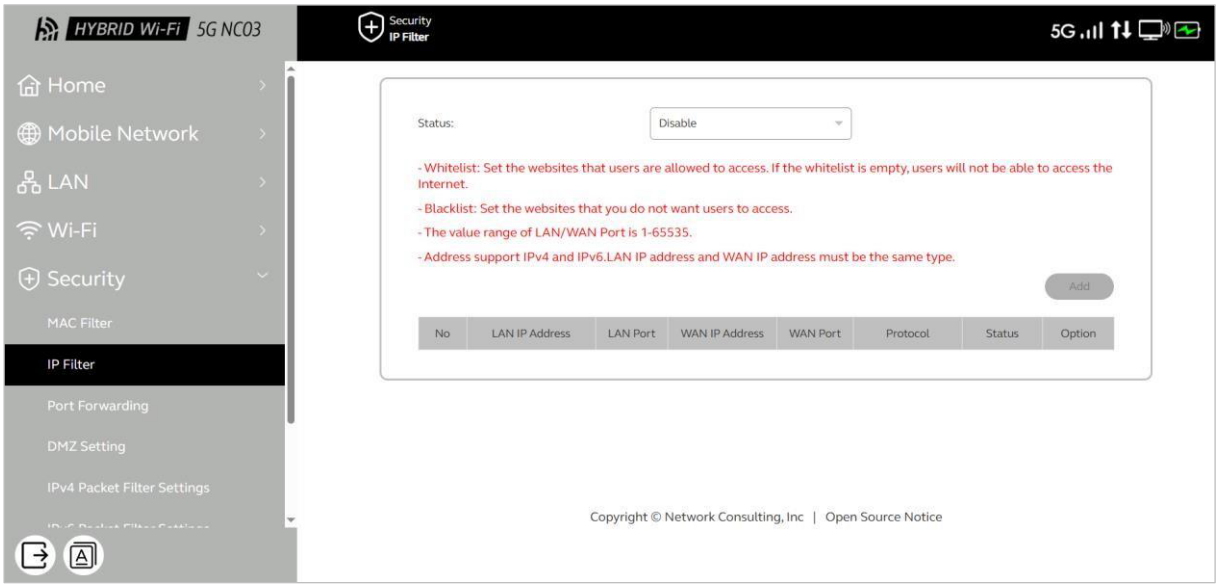
フィルターモード
・ホワイトリスト：指定サイトへのアクセスのみ許可。（空の場合、すべての通信が遮断されます）
・ブラックリスト：指定サイトへのアクセスを禁止。

補足

・ポート番号の範囲は 1～65535。
・IPv4 および IPv6 両方に対応。
・LAN／WAN の IP アドレスは同一タイプ（IPv4 同士または IPv6 同士）である必要があります。

手順

1.「セキュリティ」>「IP フィルター」を開きます。
2.モードを選択：無効／ブラックリスト／ホワイトリスト。
3.「追加」をクリックし、以下を入力します：LAN IP アドレス、LAN ポート、WAN IP アドレス、WAN ポート、プロトコル状態。
4.「保存」をクリックして設定を完了します。



ポートマッピング

ポート転送機能を使用すると、インターネットからの通信を LAN 内の特定デバイスへ転送できます。
通常、ルーターのファイアウォールは外部からの通信を遮断しますが、この機能により特定のサービスを外部へ公開可能です。

主な用途

・Web サーバー（HTTP／HTTPS）
・FTP サーバー
・メールサーバー
・オンラインゲームの通信

注意

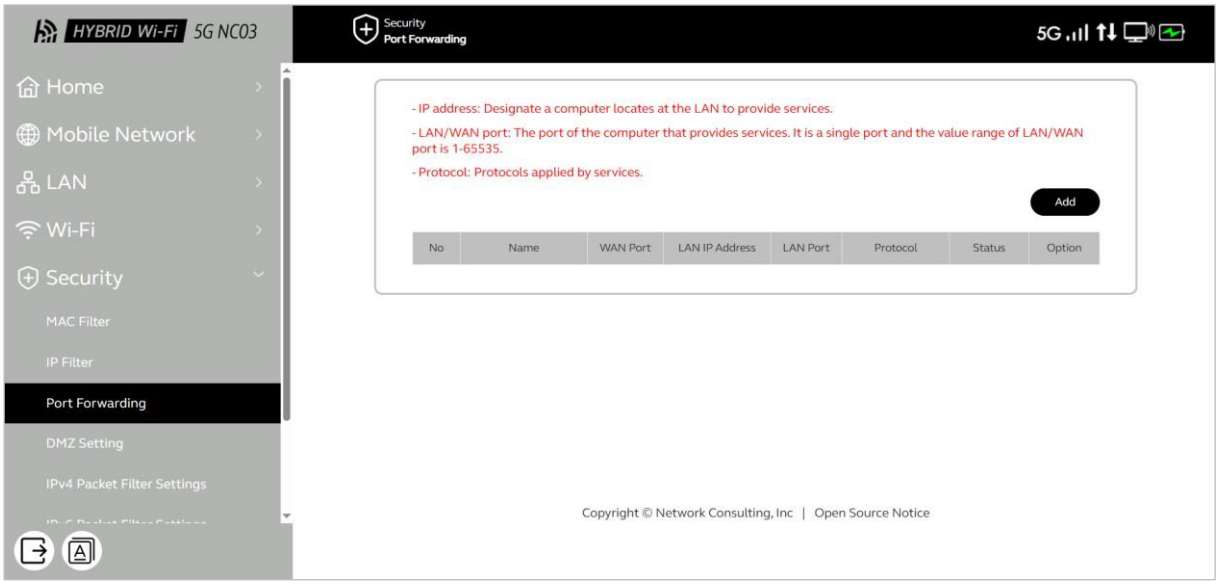
ポート転送はセキュリティリスクを伴うため、必要な場合にのみ有効化してください。
また、モバイルキャリアによってはプライベート IP を割り当てる場合があり、
その場合はインターネット側からのアクセスができません。

設定項目

・IP アドレス：サービスを提供する LAN 内のデバイスのアドレス。
・LAN／WAN ポート：通信に使用するポート番号（1～65535）
・プロトコル：利用する通信方式（TCP／UDP など）

手順

1.「セキュリティ」>「ポート転送」を開きます。
2.「追加」をクリックします。
3.項目（名称、WAN ポート、LAN IP、LAN ポート、プロトコル、状態）を入力します。
4.「保存」をクリックして完了です。



DMZ 設定

DMZ（非武装地帯）機能は、外部ネットワーク（インターネット）からの通信を LAN 内部の特定機器へ転送する機能です。
通常のファイアウォールや NAT 処理を経由したうえで、残りの全ポート通信を指定デバイスに転送します。

設定項目

・DMZ IP アドレス：DMZ ホストとして指定する端末の静的 IP。
・ステータス：機能の有効／無効。

動作概要

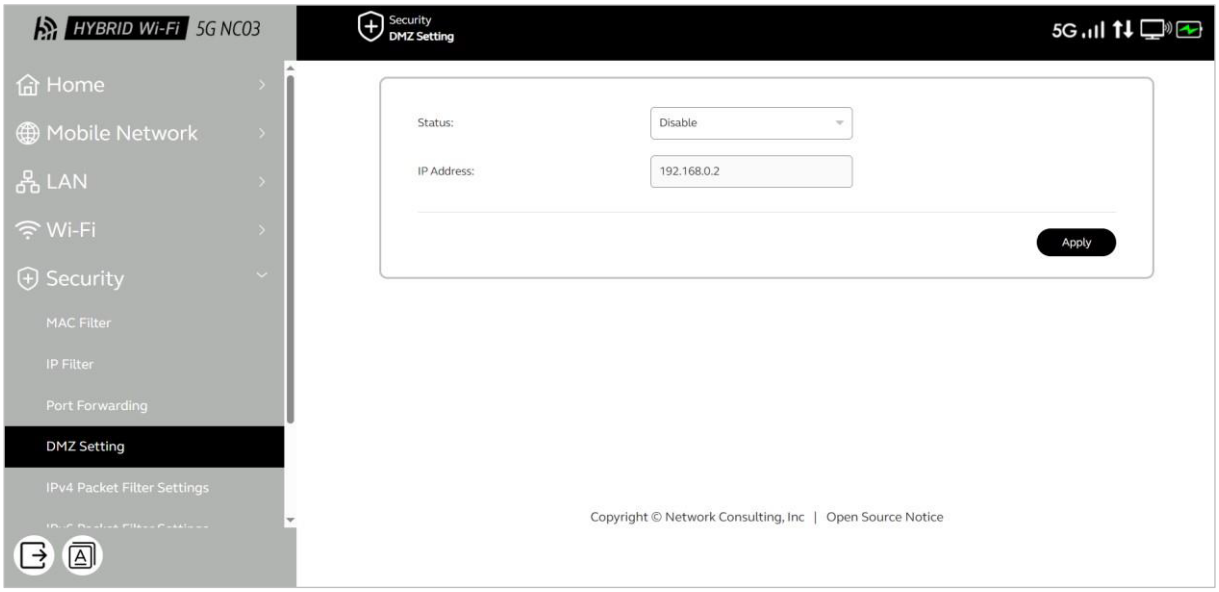
DMZ を有効にすると、未使用ポートへの通信がすべて指定のデバイスに転送されます。
外部から直接アクセスされるため、DMZ ホスト側には独自のファイアウォールを設けることを推奨します。

手順

1.「セキュリティ」>「DMZ 設定」を開きます。
2.「ステータス」列から「有効」を選択します。
3.「IP アドレス」欄に DMZ 対象デバイスの IP アドレスを入力します。（※接続デバイスの一覧から確認可能）
4.「適用」をクリックして設定します。

注意事項

・DMZ ホストの IP アドレスは外部へ公開されます。
・不要な場合は必ず「無効」に戻してください。
・DMZ は一部の通信アプリや VPN で問題解消に役立つ場合があります。



IPv4 パケットフィルター設定

IPv4 パケットフィルター機能は、ルーターを通過するデータパケットを制御する「ファイアウォールルール」です。
特定条件を満たす通信を許可または拒否するルールを作成できます。

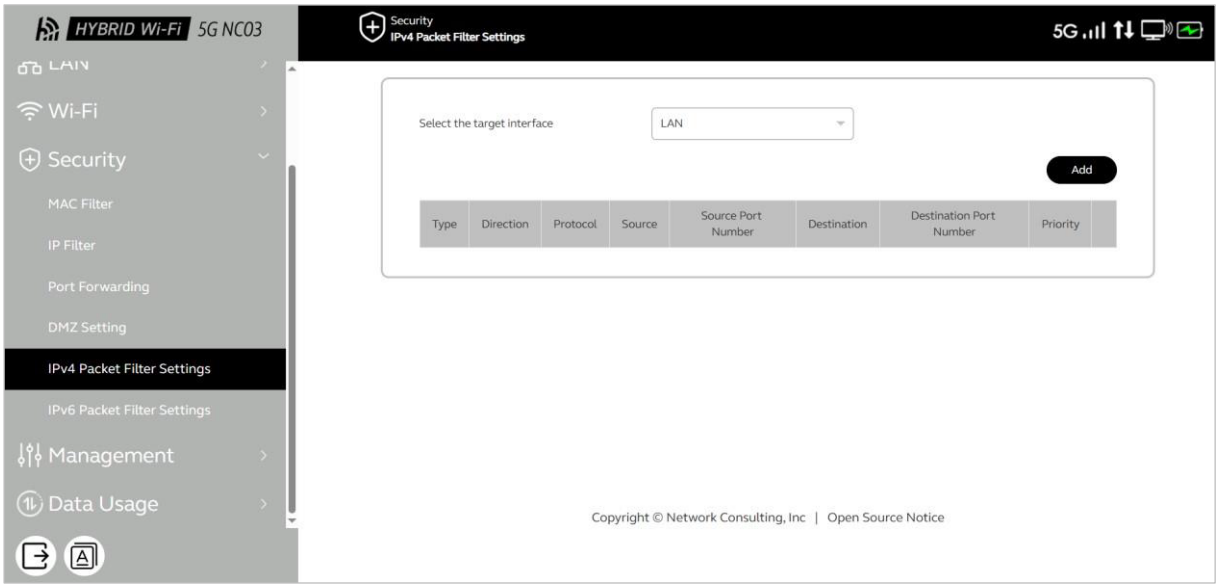
設定項目

・**タイプ**：許可または拒否。
・**方向**：通信の方向（入力／出力）。
・**プロトコル**：対象となる通信方式（ALL IP、ICMP、TCP、UDP など）。
・**送信元／宛先アドレス**：対象 IP アドレス。
・**送信元／宛先ポート番号**：TCP／UDP の特定ポート指定。
・**優先度**：複数ルールの処理順序を決定。
・**追加**：新しいルールを作成。

手順

1.「セキュリティ」>「IPv4 パケットフィルター設定」を開きます。
2.「対象インターフェースの選択」から適用先（WAN または LAN）を選びます。既定値は LAN です。
3.「追加」をクリックし、設定ウィンドウを開きます。
4.以下の項目を設定します：
- タイプ：許可または拒否（既定は許可）
- 方向：入力または出力（既定は入力）
- プロトコル：ALL IP／ICMP／TCP／UDP／その他（既定は ALL IP）
- 送信元／宛先：任意・ローカルホスト・指定 IP
- 送信元／宛先ポート番号：任意、または範囲指定可
- 優先度：ルールの優先順序を指定

5.「保存」をクリックして完了します。



IPv6 パケットフィルター設定

この機能では、IPv6 通信に対して許可・拒否のルールを設定できます。
IPv4 フィルターと同様に、ネットワークインターフェースごとに通信を制御し、セキュリティを強化します。

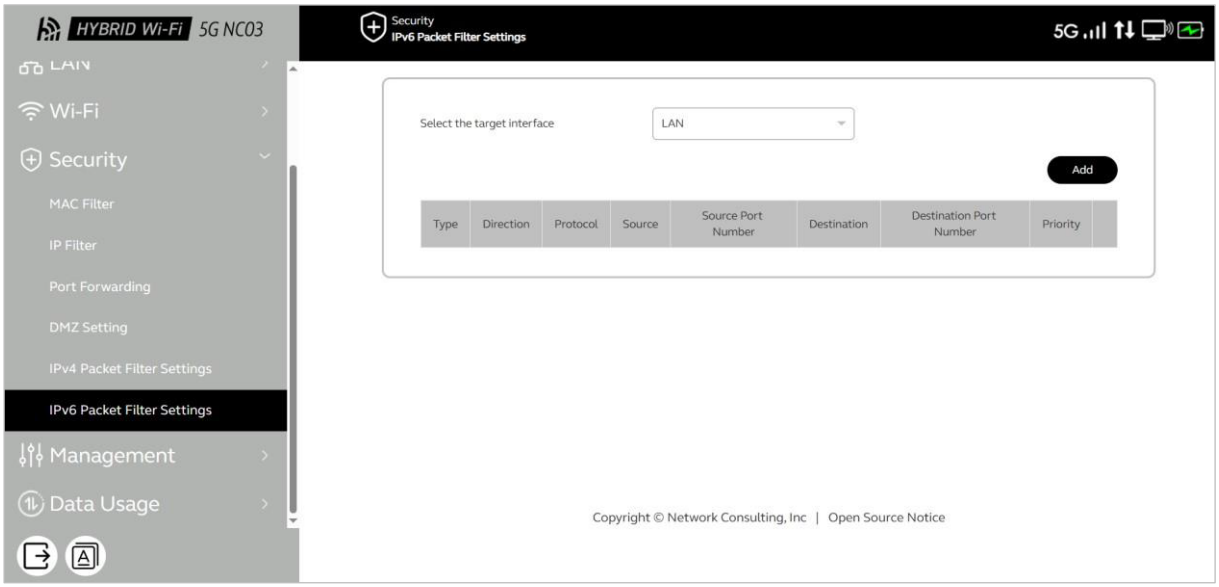
設定項目

・**タイプ**：許可または拒否を選択。
・**方向**：通信方向（入力／出力）。
・**プロトコル**：対象となる通信方式（ALL IPv6、ICMPv6、TCP、UDP など）。
・**送信元／宛先アドレス**：IPv6 の送信元および宛先アドレス。
・**送信元／宛先ポート番号**：TCP／UDP におけるポート指定。
・**優先度**：複数ルールがある場合の適用順。
・**追加**：新しいルールを作成。

手順

1.「セキュリティ」>「IPv6 パケットフィルター設定」を開きます。
2.「対象インターフェースの選択」ドロップダウンから適用先（WAN または LAN）を選択。（初期値は LAN）
3.「追加」をクリックし、詳細設定ウィンドウを開きます。
4.必要なルールを入力します。
- タイプ：許可／拒否（既定は許可）
- 方向：入力／出力（既定は入力）
- プロトコル：ALL IPv6／ICMPv6／TCP／UDP／その他（既定は ALL IPv6）
- 送信元・宛先：任意、ローカルホスト、または指定 IPv6 アドレス
- ポート番号：任意または範囲指定
- 優先度：数値を入力して処理順を指定

5.「保存」をクリックして完了です。



管理

SNTP

SNTP 機能は、外部の時刻サーバーと自動的に同期し、正確なシステム時間を維持します。

これにより、ログ記録やセキュリティ認証が正確な時刻に基づいて行われます。

主な機能

・時刻同期：指定した NTP サーバー（例：time.windows.com）と自動的に同期。

・タイムゾーン設定：地域に合わせた時刻を表示（例：アジア／東京）。

・サマータイム（DST）対応：必要に応じて自動調整。

・ステータス表示：同期状態、前回同期時刻、現在時刻などを表示。

手順

1.「管理」>「SNTP」を開きます。

2.現在の時刻設定を確認します：

- **現在時刻**：例）2025-06-04 10:07:09
- **ステータス**：同期成功など
- **最終同期時刻**：例）2025-06-04 04:05:43
- **タイムゾーン**：例）アジア／東京
- **時刻表示形式**：24 時間制（既定）

3.手動で時刻を変更する場合

- 「時刻変更」ボタンをクリック。
- 新しい日付と時刻を入力。
- 「OK」をクリックして確定。

※自動同期が有効な場合、手動設定は上書きされます。

4.タイムゾーンを変更する場合

- 「タイムゾーン変更」をクリック。

- 地域一覧から選択（例：アジア／東京）。
- 「OK」で確定。

5.時刻表示形式の変更

- 現在：24 時間制（例：14:30）。
- 12 時間制へ変更する場合：

「時刻形式」メニューから 12H を選択。

→ 表示が自動的に更新されます。

6.ネットワーク時刻との自動同期を有効化する場合

- 「ネットワーク時刻と自動同期」にチェックを入れます。
- **時刻サーバーの設定**：
- プライマリサーバー：ntp.nict.jp（既定）
- 変更可能（例：clock.fmt.he.net、clocksjc.he.net など）
- バックアップサーバー（2～5）：time.nist.gov、asia.pool.ntp.org など

7.サマータイム（DST）の設定

- 「サマータイムを有効にする」にチェックを入れます。
- 開始・終了ルールを設定：
- 開始：月、週、曜日、時刻（例：3 月第 1 日曜日 2:00AM）
- 終了：月、週、曜日、時刻（例：11 月第 1 日曜日 2:00AM）
- 時間差：通常 1 時間（地域により変更可）

8.「適用」をクリックして保存します。

トラブルシューティング

同期に失敗する場合

1. インターネット接続を確認。
2. NTP サーバーアドレスを再確認（例：time.windows.com）。
3. MiFi を再起動して再同期を試行。

恒久的に同期ができない場合

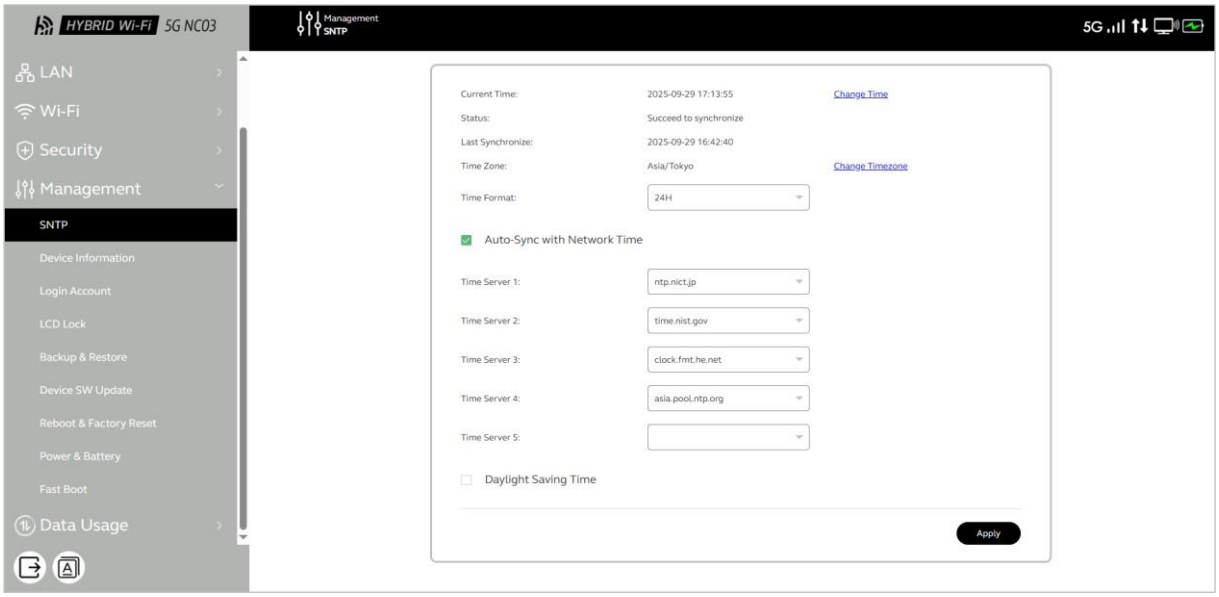
→ 自動同期をオフにして手動時刻設定を使用。

ヒント

「時刻変更」で手動修正可能。

「タイムゾーン変更」で地域に合わせた時間を表示可能。

「同期状態」を確認してサーバー接続を確認。

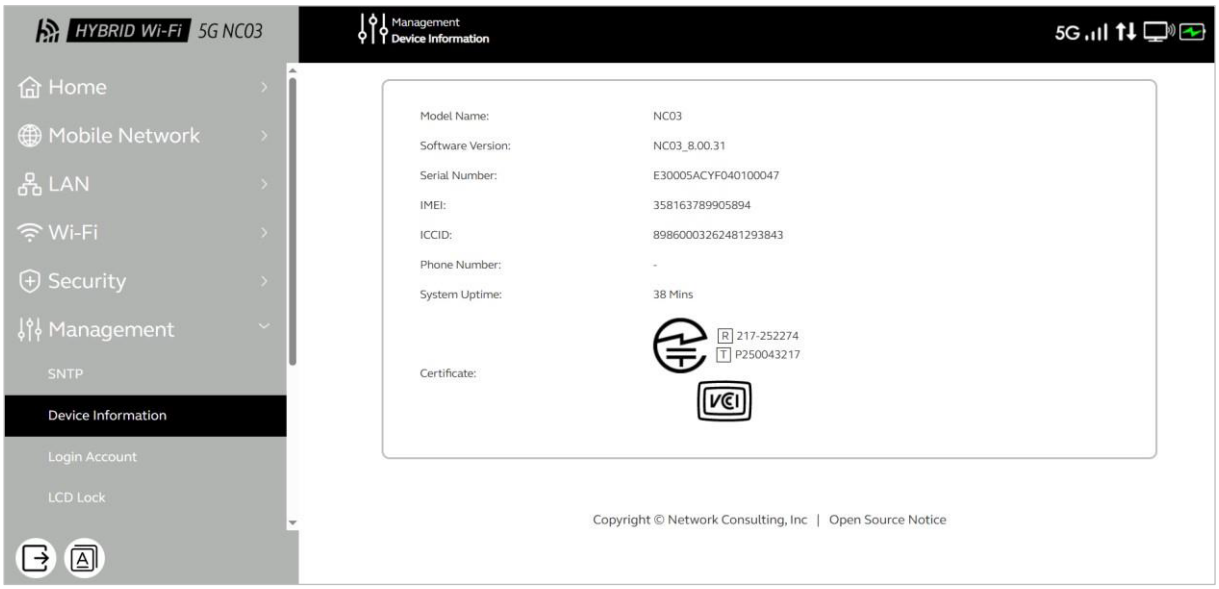


デバイス情報

この画面では、デバイスの基本情報と稼働状態を確認できます。

表示項目

・**モデル名**：MiFi のモデル番号。
・**ソフトウェアバージョン**：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。
・**シリアル番号**：製品固有の識別番号。ライセンス管理・保証対応などに使用されます。
・**IMEI 番号**：国際携帯端末識別番号。SIM を入れ替えても変わりません。
・**ICCID 番号**：SIM カードの識別番号。
・**電話番号**：SIM に紐づく電話番号。
・**システム稼働時間**：最後の再起動からの稼働時間。
・**認証番号**：例）R 217-252274、T P250043217
※技術基準適合や規制承認の証明番号であり、サポート時にも使用します。

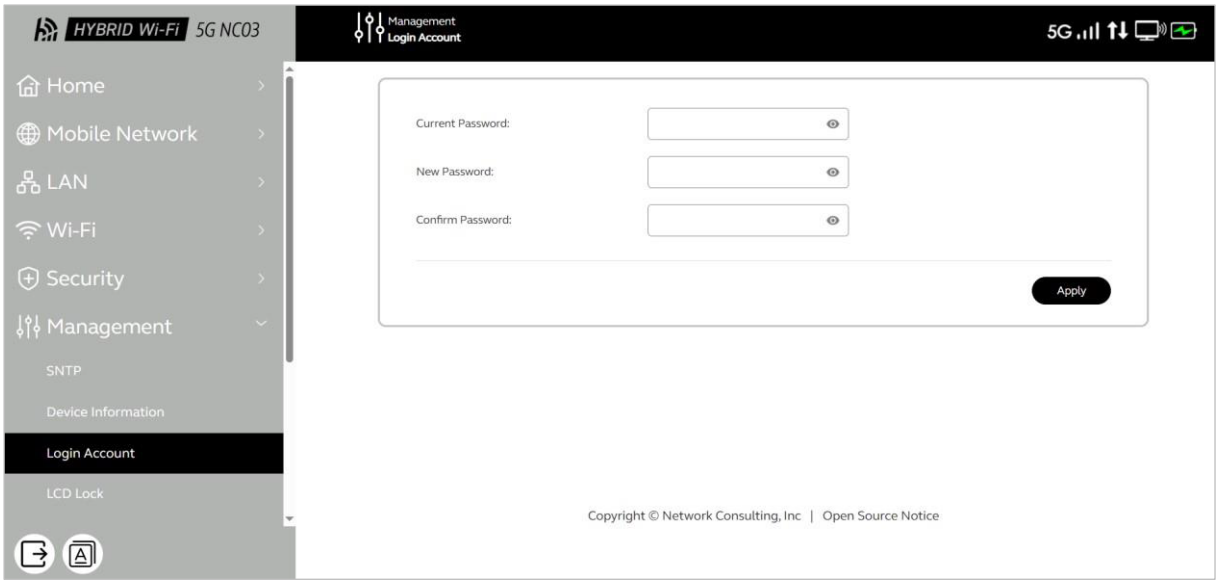


ログインアカウント

この設定では、MiFi の Web 管理画面にアクセスするためのパスワードを変更できます。
不正アクセス防止のため、定期的な更新を推奨します。

手順

1.「管理」>「ログインアカウント」を開きます。
2.「現在のパスワード」欄に現在のパスワードを入力します。
3.「新しいパスワード」欄に希望するパスワードを入力します。
4.「確認パスワード」欄に同じパスワードを再入力します。
5.「適用」をクリックして変更を保存します。
6.設定後、再度ログイン画面が表示されるため、新しいパスワードで再ログインします。

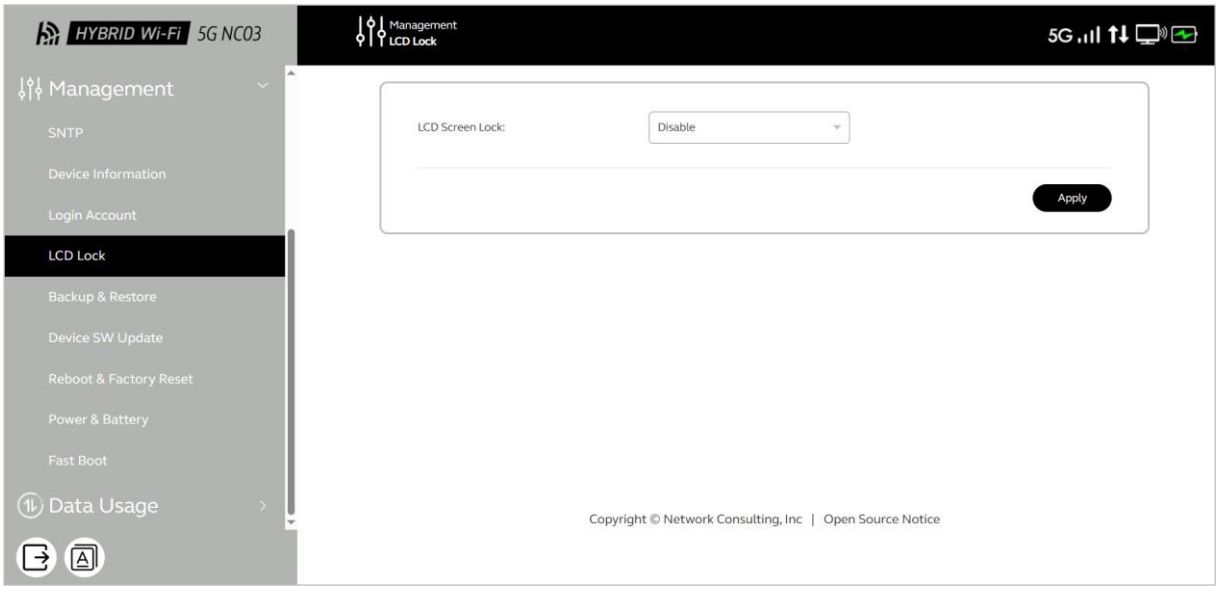


画面ロック

画面ロック機能は、本体ディスプレイに直接アクセスして設定を変更する際のセキュリティを強化します。
パスワードを設定すると、ロック解除時に入力が必要になります。

手順

1.「管理」>「画面 ロック」を開きます。
2.ドロップダウンメニュー から「有効」を選択します。
3.「新しいパスワード」欄にパスワードを入力します。
4.「確認パスワード」欄に再入力します。
5.「適用」をクリックして保存します。
6.次回 画面 操作時、ロック解除に設定したパスワードが必要になります。



バックアップ＆復元

この機能では、現在の 端末 設定（Wi-Fi 情報、ネットワーク構成、管理者情報など）をバックアップし、
トラブル発生時や新しい端末への移行時に復元できます。

用途

・設定の移行（別の同機種への設定コピー）
・設定ミスからの復旧
・初期化前のバックアップ保管

手順：バックアップ

1.「管理」>「バックアップ＆復元」を開きます。
2.「バックアップ」ボタンをクリックします。
3.システムが自動的に .bin ファイルを生成します。
4.表示された保存ダイアログで、安全な場所にファイルを保存します。

手順：リストア（復元）

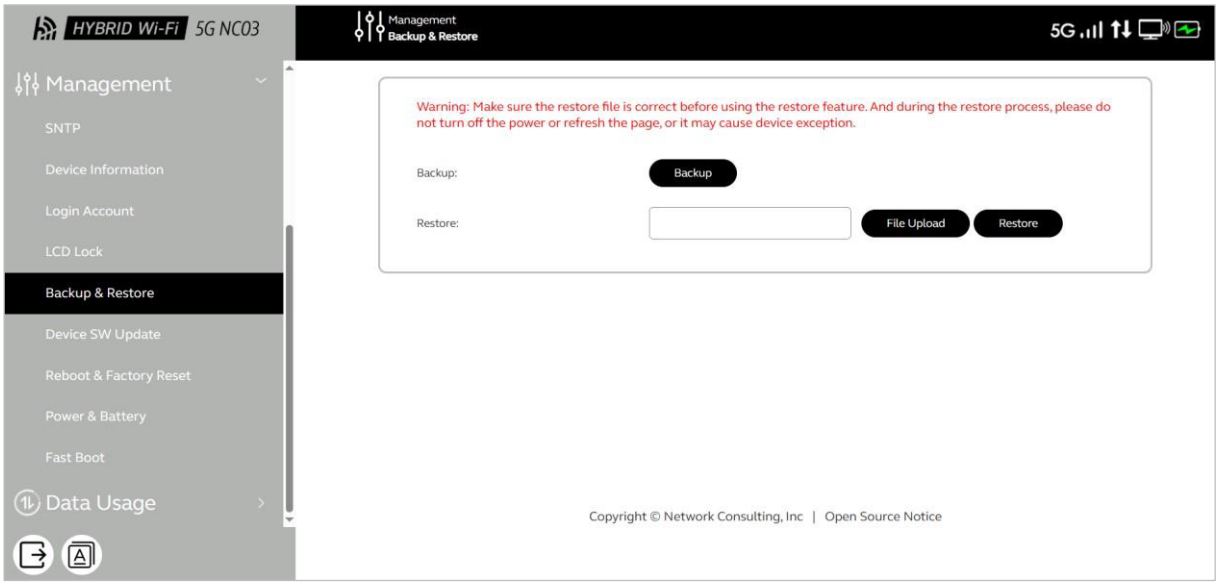
1.「ファイルを選択」をクリックします。
2.復元したいバックアップファイル（.bin）を選択します。
3.「復元 」をクリックします。
4.処理が完了するまで電源を切ったり、画面をリロードしないでください。

注意事項

・**互換性**：同一モデル・同一ファームウェアバージョンでのみ使用可能。
・**セキュリティ**：バックアップファイルにはパスワード情報が含まれる場合があります。安全な場所に保管してください。
・**電源安定性**：復元中の電源遮断は故障の原因になります。
・**復元失敗時**：工場出荷時リセット後、再度手動で設定を行ってください。

トラブル対処

・「復元に失敗しました」と表示された場合：
→ ファイルの破損やバージョン違いの可能性があります。
・デバイスが反応しない場合：
→「再起動と工場出荷時リセット」から初期化を実行してください。



SWアップデート

この機能は、端末 のファームウェアを最新バージョンに更新するためのものです。
セキュリティの改善、動作安定性の向上、新機能追加を目的としています。

自動更新

手順

1.「管理」>「SWアップデート」を開きます。
2.「ステータス」欄のチェックボックスをオンにして自動更新を有効化します。
3.更新実行時間（例：午前 2:00～午前 4:00）を指定します。
4.「適用」をクリックします。

注意

・指定時間帯にデバイスが使用されていない場合、自動的に更新が行われます。
・更新中は電源を切らないでください。

手動更新

手順

1.「管理」>「SWアップデート」を開きます。
2.「更新タイプ」ドロップダウンから「手動更新」を選択します。
3.「ファイルアップロード」ボタンをクリックし、更新ファイルを選択します。
4.「更新」をクリックしてファームウェア更新を実行します。

オンライン更新

手順

1.「管理」>「SWアップデート」を開きます。
2.「更新タイプ」ドロップダウンから「オンライン更新」を選択します。
3.「更新を確認」をクリックします。
4.新しいソフトウェアがある場合、自動的にダウンロードが開始されます。

注意

・更新中は電源およびインターネット接続を維持してください。
・更新時にバッテリー駆動の場合は、AC アダプターを接続してください。

重要事項

・**電源の安定**：更新中に電源を切らないでください。

・**ファイルの整合性**：必ず同一モデル（NC03）専用のファームウェアを使用してください。

・**バックアップ**：更新前に必ず「バックアップ＆リストア」で設定を保存してください。

トラブル対処

・**更新に失敗した場合**：

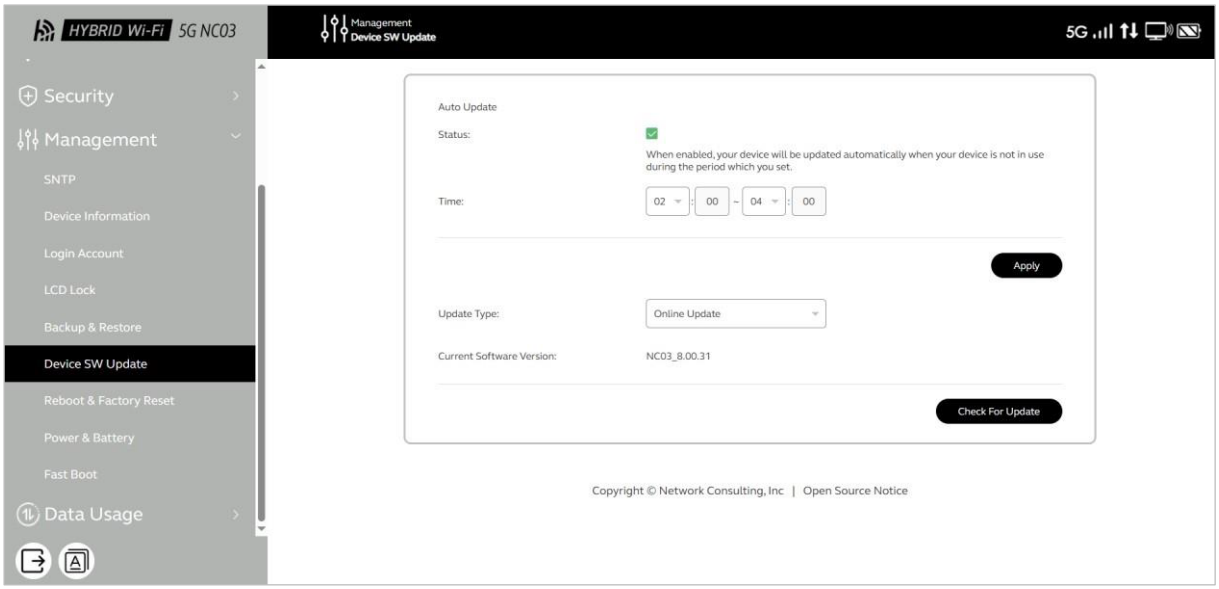
→ ファイル破損または接続不良の可能性があります。

・**自動更新が動作しない場合**：

→ インターネット接続を確認。

・**更新後に動作しない場合**：

→「工場出荷時リセット」で初期状態に戻してください。



再起動＆初期化

この機能では、デバイスの再起動および工場出荷時設定へのリセットを行えます。

設定不具合や動作異常の際に使用します。

機能内容

・**再起動**：システムを再起動します（所要時間：約 60 秒）。

・**工場出荷時リセット**：すべてのユーザー設定を削除し、出荷時状態に戻します。

手順

1.「管理」>「再起動＆初期化」を開きます。

2.再起動する場合：

- 「再起動」ボタンをクリックします。
- 「OK」を選択し、約 60 秒待ちます。
- 処理中は電源を切らないでください。

3.工場出荷時リセットを行う場合：

- 「工場出荷時リセット」ボタンをクリックします。

- 「OK」を選択し、1～2 分ほど待ちます。
- 全設定が初期化され、デバイスが自動再起動します。

注意事項

・リセットを行うと、すべての設定（Wi-Fi 名・パスワードなど）が削除されます。

・初期化前に「バックアップ＆リストア」で設定を保存してください。

・初期化後は、デフォルトログイン情報に戻ります（本体ラベルを参照）。

・リセット中に電源を切らないでください。

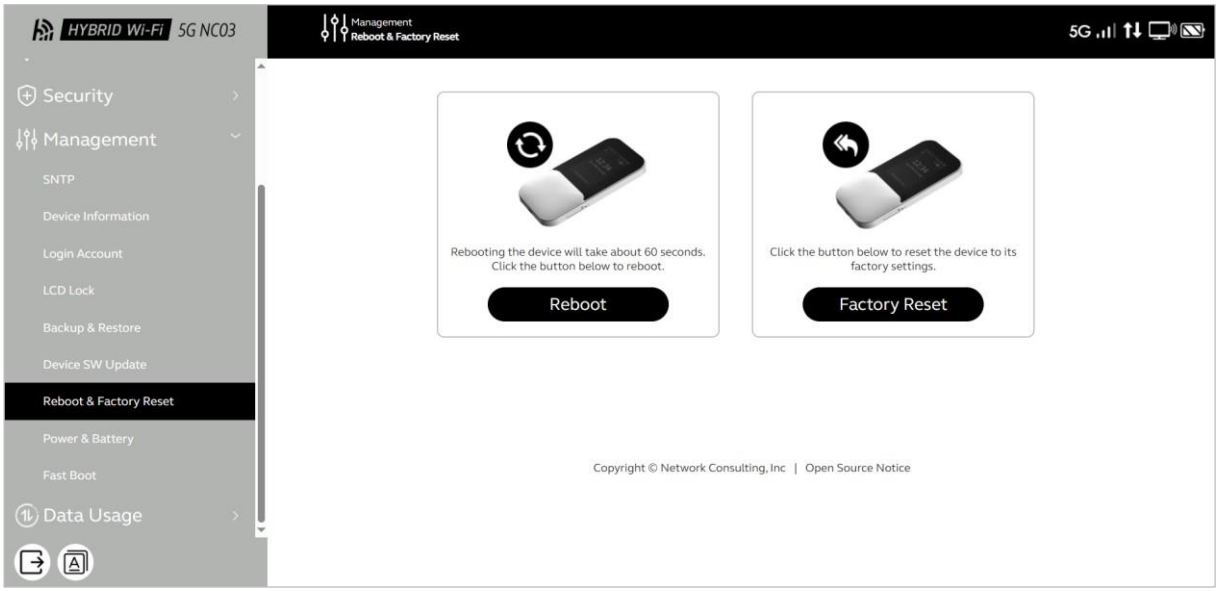
トラブル対処

・再起動後に反応がない場合：

→ 5 分程度待機してください。

→ バッテリー残量を確認し、接触不良がないか確認。

→ 最終手段として再度リセットを実行します。



電源・バッテリー

この設定では、バッテリーの消耗を抑え、電源動作を最適化することができます。

主な目的

・バッテリー寿命を延ばす

・省電力運用の管理

・画面のスリープや自動起動設定の制御

手順

1.「管理」>「電源・バッテリー」を開きます。

2.**長寿命充電モード**を設定します。

- 「有効」：バッテリーを最適な電圧で維持。
- 「無効」：通常充電。

3.**省電力モード**を選択します。

- 「ノーマル」または「ECO」。

4.**スリープ設定**を選択します。
- 「0（無効）」／「5 分」／「10 分」／「30 分」／「60 分」
- 既定値：10 分。

5.**自動画面オフ時間**を設定します。
- 「15 秒」／「30 秒」／「60 秒」／「120 秒」
- 既定値：30 秒。

6.**自動起動設定**を切り替えます。
- 「有効」：電源接続時に自動起動。
- 「無効」：手動起動（初期設定）。

注意事項

・一部の機能はバッテリー搭載モデル専用です。

・ECO モードを使用すると、パフォーマンスが低下することがあります。

トラブル対処

・バッテリー消耗が早い場合：

→ 省電力モードを確認。

→「動作ログ」をチェック。

→ 初期設定にリセットして再確認。

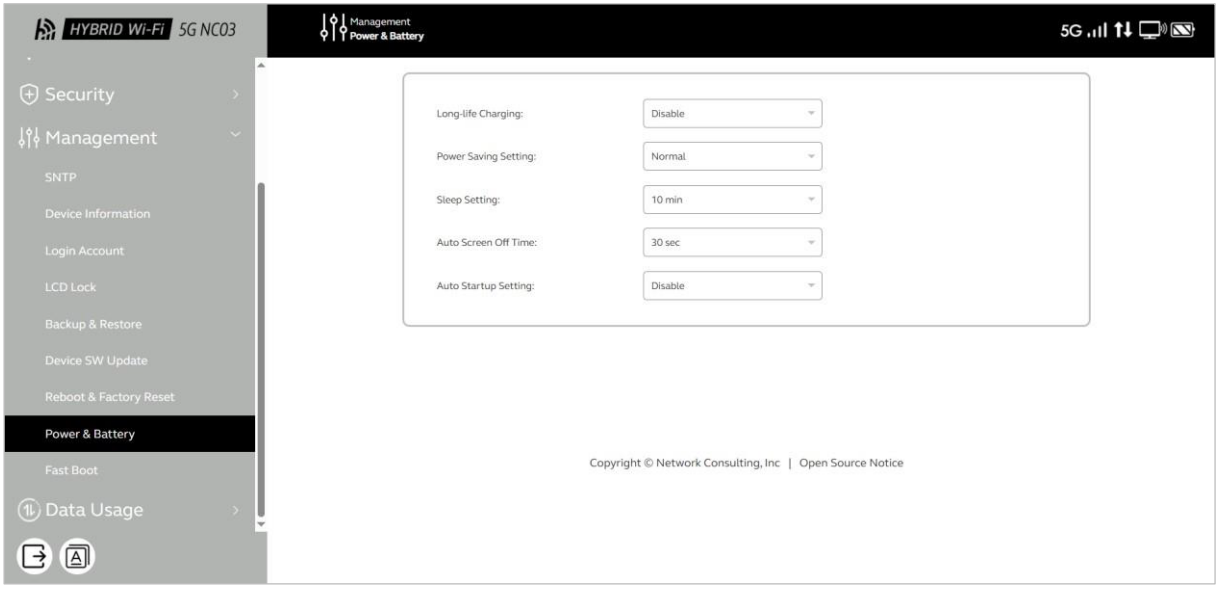
・画面が点灯しない場合：

→「自動画面オフ時間」の設定を確認。

→ 電源ボタン長押しで再起動を試行。

備考

機能はモデルによって異なる場合があります。詳細は仕様書を参照してください。



高速起動

高速起動を有効にすると、デバイスの電源投入時の起動時間を短縮できます。
これはハードウェアチェックの一部をスキップし、システム状態を保持することで実現されます。

注意

起動時間は短縮されますが、若干の電力消費増加やバッテリー寿命への影響が生じる可能性があります。

手順

1.「管理」>「高速起動」を開きます。
2.「高速起動」スイッチを設定します。
- 有効：起動時間を短縮（推奨）。
- 無効：フルハードウェア初期化を実行。

3.「適用」をクリックして保存します。
4.再起動後に設定が反映されます。

確認方法

・再起動後、起動時間の短縮を確認。
・「動作ログ」で起動イベントを確認可能。

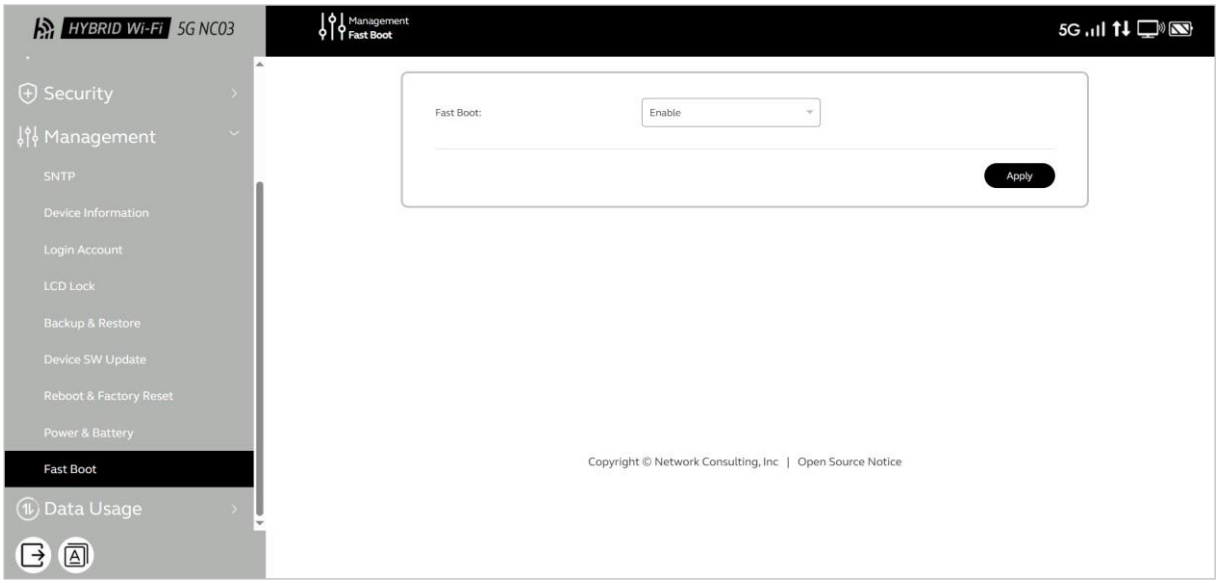
注意事項

・標準では高速起動が有効になっています。
・ハードウェア不具合が疑われる場合は無効化して起動してください。
・ファームウェア更新やバックアップ時も対応しています。

トラブル対処

・起動しない場合：
→ 電源ボタンを 10 秒長押ししてハードリセット。
→ 高速起動を無効化して再起動。

・ネットワーク設定が読み込まれない場合：
→「動作ログ」を確認し、必要に応じて「バックアップ＆リストア」で復元。



データ使用量

データ使用量画面では、モバイルデータ通信の消費量を監視・管理できます。

機能概要

・リアルタイムの通信量表示

・過去の使用履歴確認

・使用量アラート設定

・データ上限の指定

補足事項

・表示されるのはモバイルデータ通信量のみです（Wi-Fi／LAN は対象外）。

・表示に若干の遅延が生じる場合があります。

・通信量は SIM の契約内容に依存します。

トラブル対処

・データが記録されない場合：

→ モバイルネットワーク接続を確認。

→ SIM カードの有効状態を確認。

→ MiFi を再起動してください。

ヒント

「1 か月」ビュー：請求サイクルに合わせて月単位で確認。

「3 日」ビュー：短期間の使用状況を把握するのに便利。

1 ヶ月のデータ使用量設定

手順

1.【データ使用量】>【1 ヶ月】を選択します。

上限値（例：30.00GB）を入力します。変更したい場合は「上限値」欄に新しい値を入力してください。

【データ使用量制限の通知】を切り替えます：

有効にすると、上限に近づいたときにアラートを受け取ります。

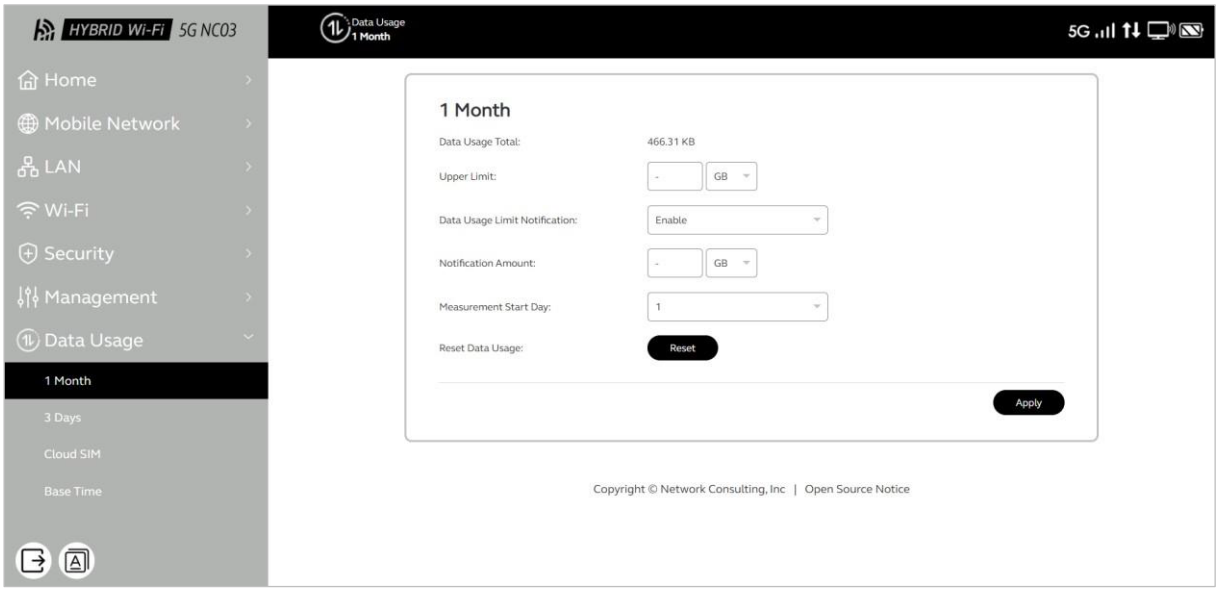
無効にすると、通知はありません。

通知量：通知を受け取る残りデータ量を必要に応じて設定してください（例：29.00GB）。

計測開始日：現在は自動で毎月リセットされる設定になっています。リセット日を変更する場合は、ドロップダウンから希望の日付を選択してください。

2.【適用】をタップして設定を保存します。

3.手動リセット：リセットボタンをクリックし、表示される確認ダイアログで【OK】をクリックします。これにより、現在の使用統計が即座にクリアされ、計測サイクルが再開されます。



3 日間のデータ使用量設定

手順

1.【データ使用量】>【3 日間】を選択します。

「上限値」欄に希望する値（例：「1GB」）を入力します。

【データ使用量制限の通知】のトグルを切り替えます：

有効の場合：上限に近づくとアラートを受け取ります。

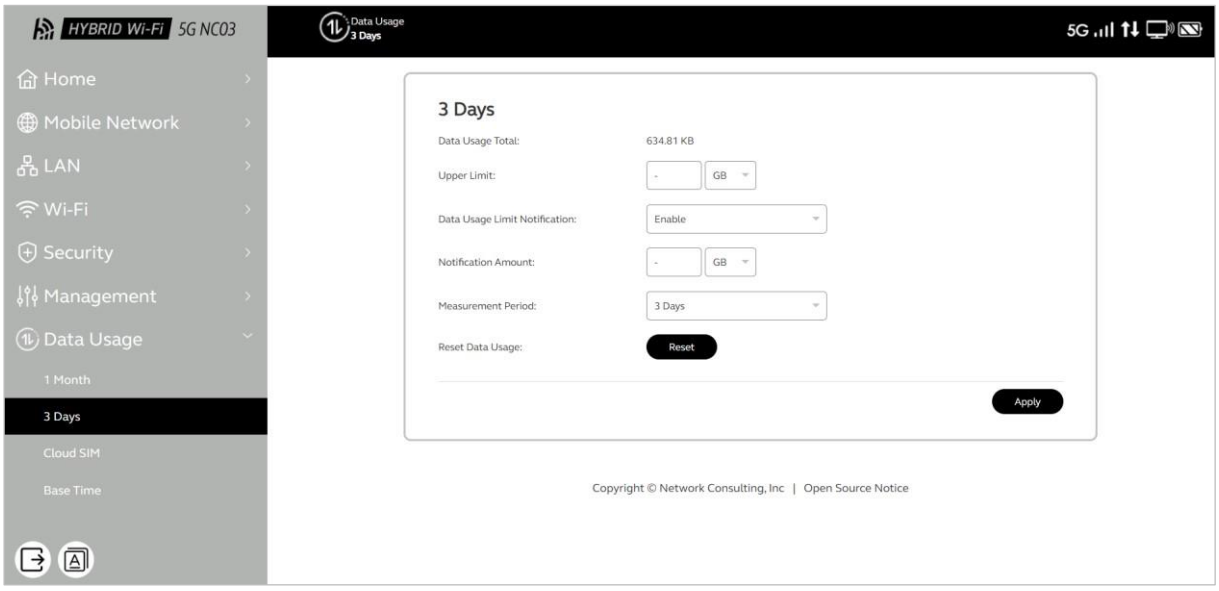
無効の場合：通知はありません。

通知量：通知を受け取る残りデータ量の閾値を「通知量」欄に設定します（例：「0.5GB」と入力すると、残り 500MB でアラートが表示されます）。

計測期間：現在のサイクルは 3 日間（72 時間ごとに自動リセットされます）。期間を変更したい場合は「3 日間」のドロップダウンをクリックし、他の選択肢（例：1 日、2 日）があれば選択してください。

2.【適用】をタップして設定を保存します。

3.手動リセット：リセットボタンをクリックし、表示される確認ダイアログで「OK」をクリックすると、現在の使用統計が即座にクリアされ、計測サイクルが再開されます。



クラウド SIM

この画面では、クラウド SIM によるモバイルデータ使用量を確認できます。

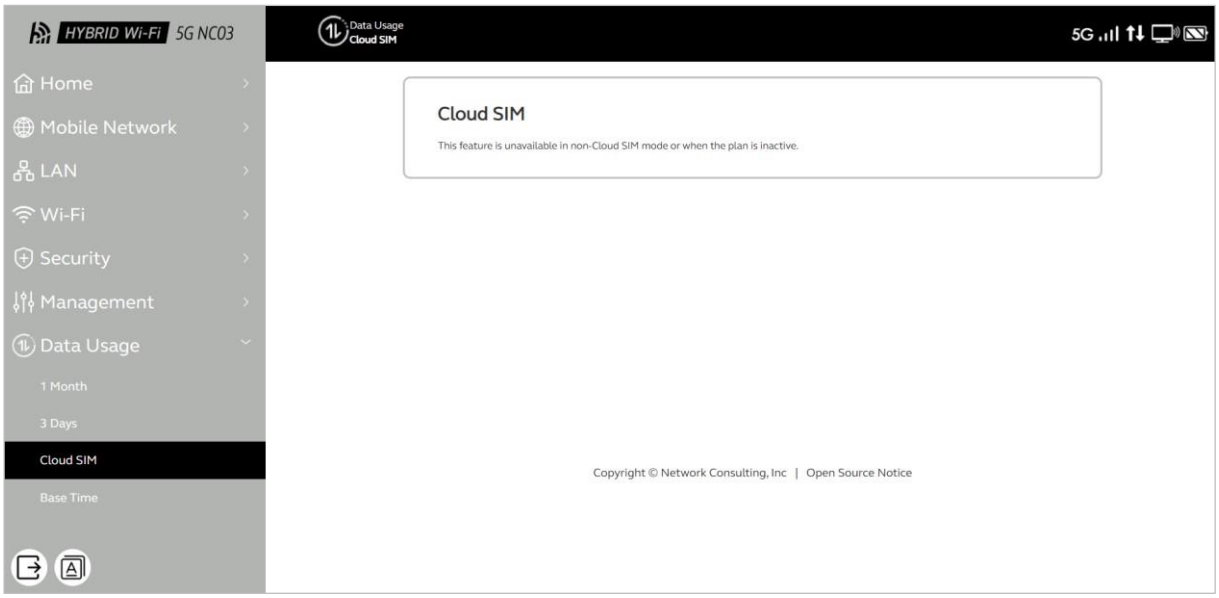
クラウド SIM とは、物理 SIM を使用せずにクラウド経由で通信を行うサービスです。

手順

1.クラウド SIM の使用状況を確認する前に、「モバイルネットワーク」>「SIM の選択」でクラウド SIM を選択しておきます。

2.「データ使用量」>「クラウド SIM」を開きます。

3.累計モバイルデータ使用量およびクラウド SIM プランの詳細を確認できます。



基準時間

この設定では、データ使用量の計測基準となる時刻を指定します。

異なるタイムゾーンでの利用や海外ローミング時に役立ちます。

利用目的

・国際旅行時のデータ計測誤差を防ぐ

・日次／月次リセットの基準を明確に設定

・各地域時間に合わせた正確な通信管理

設定項目

・**日本時間**：固定で日本標準時を基準に使用。

・**現地時間**：渡航先の現地時間を自動で適用。

・**グリニッジ標準時**：世界共通の基準時間を使用。

手順

1.「データ使用量」>「基準時刻」を開きます。

2.「基準時刻」ドロップダウンから以下のいずれかを選択：

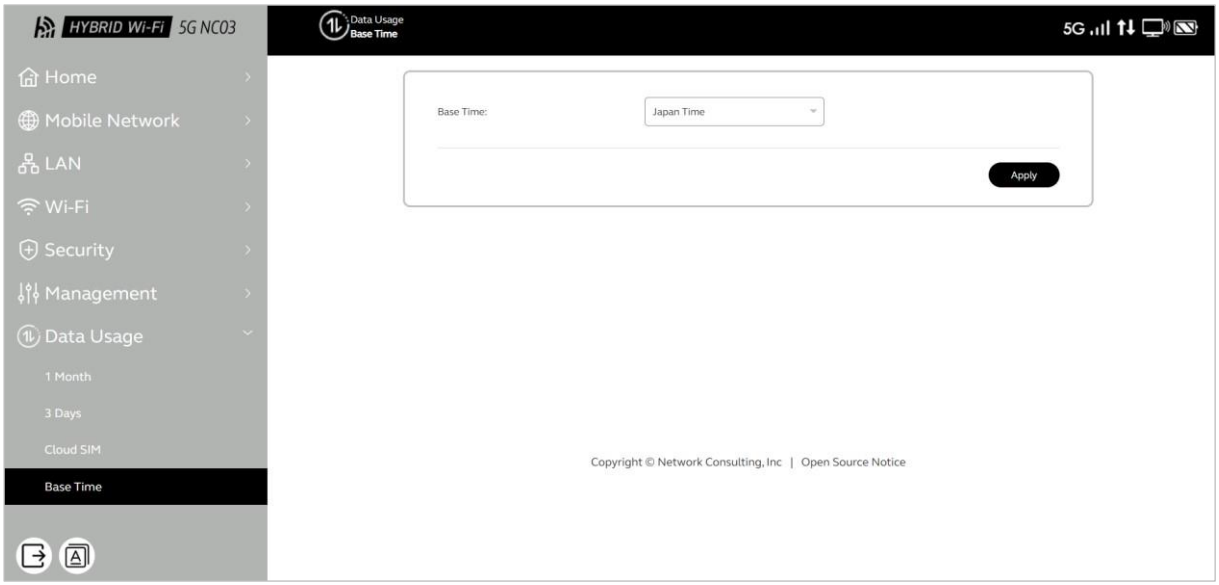
- 日本時間
- 現地時間
- グリニッジ標準時

3.「適用」をクリックして保存します。

補足

・初期設定は「日本時間」です。

・ローミング中に自動的に現地時間へ切り替えることも可能です。



ログアウト

MiFi の Web 管理画面から安全にログアウトするための操作です。

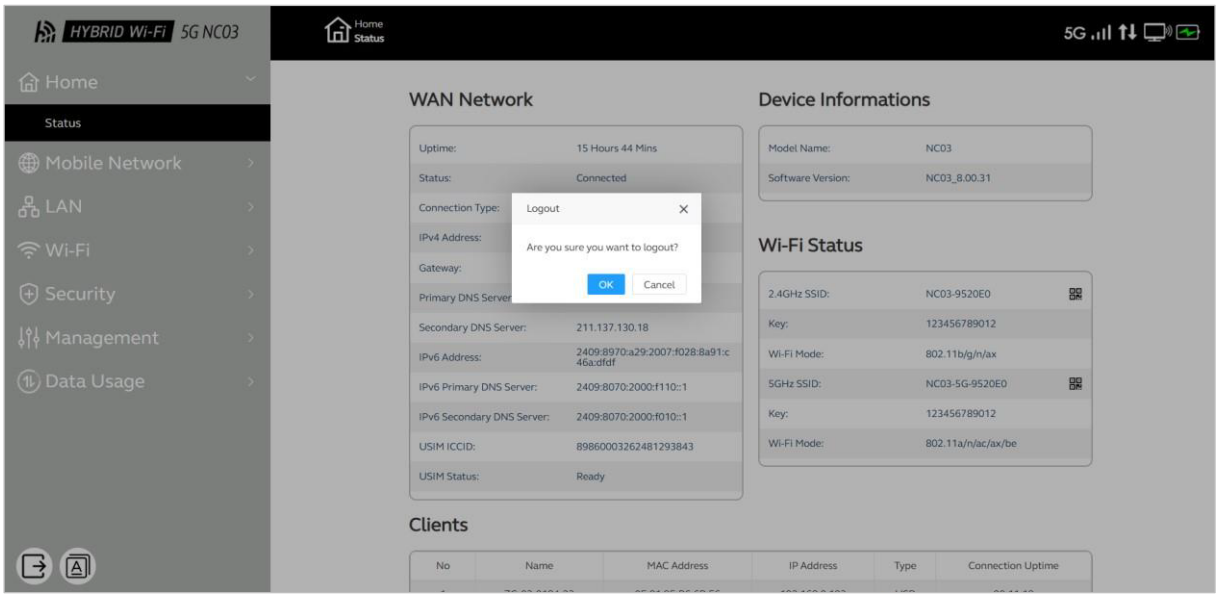
セキュリティ保護のため、作業終了後は必ずログアウトしてください。

手順

1.画面右上または任意ページ上部の「ログアウト」  アイコンをクリックします。

2.確認ダイアログで「OK」を選択します。

3.ログイン画面に戻り、セッションが終了します。



言語切り替え

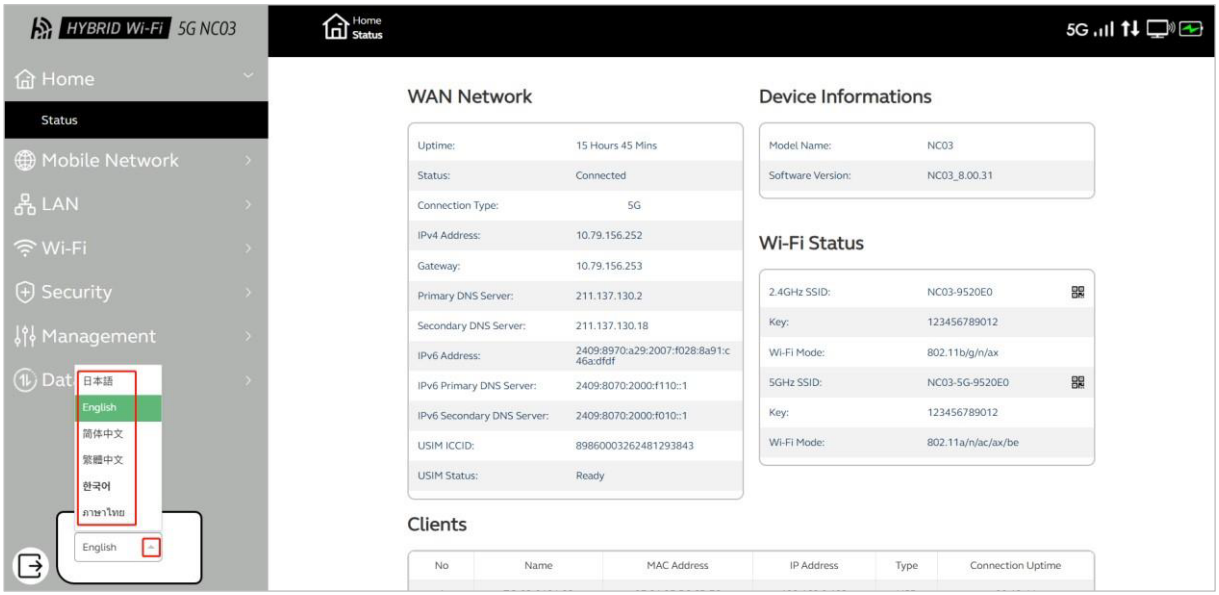
Web 管理画面の表示言語を変更できます。
複数言語に対応しており、日本語・英語・中国語などを選択可能です。

手順

1.任意のページで「言語」 アイコンをクリックします。
2.ドロップダウンリストから希望する言語を選択します。
3.ページが自動的にリロードされ、選択した言語で表示されます。

補足

・言語設定はブラウザごとに保存されます。
・再起動後も選択言語は維持されます。



第 4 章：トラブルシューティング

MiFi が正常に動作しない場合、以下の手順に従って問題を解決してください。

基本的な対処方法

1.デバイスが応答しない場合：
→ 電源ボタンを約 3 秒間長押しして電源をオフにします。
→ もう一度 3 秒間長押しして再度電源を入れます。

2.再起動しても改善しない場合：
→ 工場出荷時設定へのリセットを試してください（設定メニューまたはリセットピンホールから実行）。

Q&A

Q：SSID が表示されているのに接続できません。

A：1.入力したパスワードが正しいか確認してください。

2.接続先の PC やスマートフォンで「WPS セキュリティ」が有効な場合、WiFi側で WPS 操作が要求されていないか確認してください。

Q: サービスが利用できません。

A：原因として、ネットワーク信号の不安定さ、またはハードウェアの問題が考えられます。

以下の対処を試してください。

1.建物内や遮蔽物の多い場所にいる場合は、窓際など電波の届きやすい場所へ移動してください。

2.本体に破損や接触不良がないか確認してください。

Q: Wi-Fi パスワードを忘れてしまいました。

A：1.ディスプレイの「接続情報 → パスワード」メニューで確認できます。

2.どうしても確認できない場合は、デバイスを工場出荷時設定にリセットしてください。

初期設定のパスワードは、LCD 画面の「接続情報 > パスワード」に表示されます。

Q: SIM カードがロックされました。

A：SIM がロックされた場合は、Web 管理画面（http://192.168.0.1）にログインし、

通信事業者から提供された PIN コード または PUK コード を入力してください。

補足：

・PIN コードを 3 回誤入力すると、PUK コードが必要になります。

・PUK コードを 10 回誤ると、SIM カードが永久ロックされ、再利用できなくなります。

Q: データ通信ができません。

A：通信可能エリア外にいる可能性があります。以下を確認してください。

1.電波が届く場所へ移動します。

2.モバイルデータ通信が有効になっているか確認します。

3.必要に応じて再起動してください。