NETGEAR®

ユーザーマニュアル

Insight Managed WiFi 6 AX6000

トライバンド・マルチギガ・アクセスポイント

WAX630

2023年1月
202-12194-06

NETGEAR, Inc.
350 E. Plumeria Drive
San Jose, CA 95134, USA

サポートとコミュニティ

netgear.com/supportから、最新のファームウェアをダウンロードしてください。

また、community.netgear.comのNETGEARコミュニティでも役立つアドバイスを提供しています。

規制と法律

本製品がカナダで販売されている場合、https://www.netgear.com/support/download/から、カナダ語のフランセ ンス文書にアクセスできます。

(本製品がカナダで販売されている場合、カナダ・フランス語の本書には https://www.netgear.com/support/download/ からアクセスできます)。

EU適合宣言を含む規制適合情報については、
https://www.netgear.com/about/regulatory/。

電源装置を接続する前に、規制順守に関する文書を参照してください。NETGEAR

のプライバシーポリシーについては、https://www.netgear.com/about/privacy-

policy。

本デバイスを使用することにより、お客様はNETGEARの利用規約（https://www.netgear.com/about/terms-and-conditions）に同意したものとみなされます。同意いただけない場合は、返品期間内にデバイスを購入先に返品してください。

このデバイスを屋外で使用しないでください。PoE ソースは建物内接続専用です。

6 GHzの機器にのみ適用されます：本装置は屋内でのみ使用してください。石油プラットフォーム、自動車、列車、船舶、航空機での 6GHz 機器の使用は禁止されています。ただし、10,000 フィート上空を飛行中の大型航空機ではこの機器の使用が許可されています。
5.925～7.125GHz帯の送信機の運用は、無人航空機システムの制御または無人航空機システムとの通信のために禁止されている。

商標

NETGEAR, Inc.、NETGEAR、NETGEARロゴはNETGEAR, Inc.の商標です。NETGEAR以外の商標は、参照目的でのみ使用されています。

改訂履歴

出版物品番	発行日	コメント
202-12194-06	2023年1月	マルチキャストDNSゲートウェイの管理（150ページ）とそのサブセクションを追加しました。 NETGEAR Insight Instant Mesh WiFi ネットワークのアクセスポイントでは、*ルートとノードという*用語を使用するようになりました。以前は、*ルートアクセスポイントとエクステンダーアクセスポイントという*用語を使用していました。
202-12194-05	2022年9月	以下のセクションを追加した： 79 ページの WiFi ネットワークのマルチ PSK の設定 133 ページの L2 セキュリティの有効化 180ページのエネルギー効率モードの管理
202-12194-04	2022年7月	以下の項目を改訂した： ローカル ブラウザ ユーザー インターフェイスと NETGEAR Insight について 11 ページ 初期設定のためにアクセス ポイントに接続する 23 ページ NETGEAR Insight クラウド ポータルを使用してインターネット経由で接続する 24 ページ NETGEAR Insight アプリを使って WiFi 経由で接続する (26 ページ) WiFi経由でローカルブラウザUIに接続し、初期設定を行う（28ページ その他、複数のセクションでマイナーな変更と改善を行いました。取り付けオプションとしてサポートされていない 9/16 インチ（15 mm）の T バーに関する情報を削除しました（「アクセス・ポイントを壁または天井に取り付ける（266 ページ）」を参照）。
202-12194-03	2022年5月	アクセスポイントに新しいファームウェアをチェックさせるオプションを文書化するために、以下のセクションを改訂しました： WiFi経由でローカルブラウザUIに接続し、初期設定を行う（28ページ LAN経由でローカルのブラウザーUIに接続し、初期設定を行う（33ページ 38 ページの「直接接続されたコンピュータを使用したオフラインでのアクセ スポイントの設定 55ページの「Insightアプリを使用して、アクセスポイントをノードとしてルートに接続する」を改訂し、51ページの「クラウドポータルを使用して、アクセスポイントをノードとしてルートに接続する」を追加しました。

続き

出版物品番	発行日	コメント
202-12194-02	2022年4月	アクセスポイントのFacebook Wi-Fiの登録と設定（106ページ）を参照。 MAC ACLでサポートできるMACアドレスの数を256から512に変更しました（ローカルのMACアクセス制御リストの管理（118ページ）参照）。 RADIUSサーバーのセットアップ (131 ページ)を参照。 アドレスとトラフィックにNATモードまたはブリッジモードを設定するを追加しました。 240ページにWiFiとイーサネットパケットのキャプチャを追加しました。 米国およびカナダで使用する5GHz無線のDFS動作周波数範囲を追加するため、264ページの技術仕様を改訂しました。 268 ページの「アクセスポイントを壁に取り付ける」を修正。その他、細かな変更を加えました。
202-12194-01	2021年6月	初出版。

内容

第 11 章 アクセス・ポイントとネットワークの監視

第12章 WiFiネットワークの高度なWiFi機能を管理する

第13章 WiFiブリッジのセットアップ

第14章 高度な無線能の管理

第15章 診断とトラブルシューティング

付録A 工場出荷時の初期設定と技術仕様

付録 B 壁または天井へのアクセスポイントの取り付け

1

はじめに

このマニュアルは、NETGEAR Insight Managed WiFi 6 AX6000 Tri-band Multi-Gig Access Point モデル WAX630 用です。モデルWAX630（本マニュアルではアクセスポイントと呼ぶ）は、IEEE 802.11ax、12（4+4+4）ストリームのWiFi 6、および2.4GHz、5GHzローバンド、5GHzハイバンドの3バンド同時動作をサポートします。合計スループットは6000Mbps：2.4 GHzで1200 Mbps、5 GHzローバンドで2400 Mbps、5 GHzハイバンドで2400 Mbps。

このアクセスポイントは、802.3bt電源（アクセスポイントに接続されたポートに60W PoE++電源）を供給するPoE++スイッチに接続された既存のネットワークにおいて、パワー・オーバー・イーサネット・プラス（PoE++）電源デバイス（PD）として機能します。アクセスポイントは、通常のスイッチに接続するための電源アダプターもサポートしています。モデル WAX630 は電源アダプタなしで出荷され、モデル WAX630PA は電源アダプタ*付き*で出荷されます。モデルWAX630を注文したが、PoE++接続なしでアクセスポイントを使用したい場合は、電源アダプタを別途注文することができます。

PoE++イーサネットポートは、最大2.5Gbpsの高速通信をサポートします。もう1つのイーサネットLANポートは、リンクアグリゲーション（LAG）接続用に1Gbpsの速度をサポートします。

この章には以下のセクションがある：

- 追加資料
- ローカルブラウザのユーザーインターフェイスとNETGEAR Insightについて

注：本マニュアルに記載されているトピックの詳細**については、**netgear.com/support/ のサポートウェブサイトをご覧ください。

注：新機能やバグフィックスを含むファームウェアアップデートは、netgear.com/support/download/ で随時提供されています。新しいファームウェアを手動で確認し、ダウンロードすることができます。お使いの製品の機能や動作が本マニュアルに記載されているものと異なる場合は、ファームウェアのアップデートが必要な場合があります。

注：このマニュアルでは、***WiFi**ネットワーク*はSSID（サービスセット識別子またはWiFiネットワーク名）またはVAP（仮想アクセスポイント）と同じ意味です。つまり、WiFiネットワークとは、個々のSSIDまたはVAPを意味します。

追加資料

以下の文書は netgear.com/support/download/ で入手できます：

- インストレーションガイド
- データシート

NETGEAR Insight Cloud PortalとInsightアプリについては、以下をご覧ください。netgear.com/business/services/insight/subscriptionをご覧ください。および netgear.com/support/product/insight.aspxのNETGEARナレッジベースを参照してください。

ローカルブラウザのユーザーインターフェイスとNETGEAR Insightについて

このユーザーマニュアルでは、アクセスポイントがスタンドアロンのアクセスポイントとして機能する場合に使用する、ローカルブラウザのユーザーインターフェイス（UI）について説明します。

NETGEAR Insight リモート管理は、スタンドアロンモードでは利用できない追加機能とアドオンサービスを提供します。NETGEAR Insight PremiumとInsight Proの契約者向けに、アクセスポイントはNETGEAR Insight Cloud PortalとInsightアプリをサポートしています：

- **Insight クラウドポータル**：クラウドベースの管理プラットフォームInsightのポータルから、アクセスポイントをリモートで設定・管理できます。
- **Insightアプリ**：iOSまたはAndroidモバイルデバイスからアクセスポイントをリモートで設定・管理し、Insightクラウドベースの管理プラットフォームに接続できます。

NETGEAR Insight Cloud PortalとInsightアプリについては、以下のページをご覧ください：

- netgear.com/business/services/insight/subscription
- netgear.com/support/product/insight.aspx
- kb.netgear.com/000061848

アクセスポイントを NETGEAR Insight 管理デバイスとしてインストールした場合、Insight クラウドポータルと Insight アプリで管理できる機能の設定は、ローカルブラウザ UI ではマスクされます。ただし、ローカルブラウザ UI を使用して、Insight でまだサポートされていない特定の機能の設定を管理できます。

2

ハードウェアの概要

NETGEAR Insight Managed WiFi 6 AX6000 Tri-band Multi-Gig Access Point モデル WAX630 は屋内用アクセスポイントです。

この章には以下のセクションがある：

アクセスポイントの開梱

パッケージには以下のものが含まれている：

- NETGEAR WAX630 アクセスポイント
- マウンティングプレート
- メタル・ブラケット、Tバー・ロック、ロック・スクリュー、ショート・スクリュー4本付き
- 背の高いネジ3本と壁取り付け用アンカー
- インストレーションガイド

注：モデルWAX630は電源アダプターなしで出荷されます。モデル WAX630PA *には*電源アダプターが付属しています（電源アダプターのタイプは地域によって異なります）。モデルWAX630を注文したが、PoE++接続なしでアクセスポイントを使用したい場合は、電源アダプターを別途注文することができます。

取り付けオプションについては、「壁または天井へのアクセスポイントの取り付け（266 ペー ジ）」を参照してください。

LED付きトップパネル

アクセス ポイントのステータスを示す LED は、アクセス ポイントのトップ パネルにあります。

図1.トップパネルとLED

表 1.LEDの説明

LEDアイコン	カラー	説明
電源/クラウドLED		**最初はオレンジで点灯し、その後ゆっくりとオレンジで点滅します**：アクセスポイントは、IP アドレスの取得を開始しているか、または取得中です。
		緑色の点灯：アクセスポイントは起動し、スタンドアロンのアクセスポイントとして、または Insight クラウドベースの管理プラットフォームに接続されていない Insight 検出アクセスポイントとして機能します。
		青色の点灯：アクセスポイントは Insight モードで機能し、Insight クラウドベースの管理プラットフォームに接続されています。
		オレンジの高速点滅：アクセスポイントは、ファームウェアを更新中、または工場出荷時設定にリセット中です。
		マルチカラー点滅：アクセスポイントは、Insight Instant Mesh WiFi ネットワークのノードとして機能しており、メッシュのセットアップが進行中です。
		オレンジに点灯：アクセスポイントが受信した PoE 電力は、802.3bt（PoE++）レベルではありません。
		オフ：アクセスポイントに電源が供給されていません。
LAN 1 LED		**緑の点灯**：LAN 1ポートで2.5Gbpsイーサネットリンクが検出されています。
		緑点滅：LAN 1ポートで2.5Gbpsのトラフィックアクティビティを検出。
		オレンジ点灯：LAN 1 ポートで 2.5 Gbps 未満のイーサネットリンクが検出されました。
		オレンジ点滅：LAN 1 ポートで 2.5 Gbps 未満のトラフィックが検出されています。
		オフ：LAN 1ポートにイーサネットデバイスが接続されていないか、イーサネットリンクが検出されていません。
LAN 2 LED		**緑色に点灯**：LAN 2 ポートで 1 Gbps イーサネットリンクが検出されます。
		緑点滅：LAN 2 ポートで 1 Gbps のトラフィックが検出されています。
		オレンジ点灯：LAN 2 ポートで 1 Gbps 未満のイーサネットリンクが検出されています。
		オレンジの点滅：LAN 2 ポートで 1 Gbps 未満のトラフィックが検出されています。
		オフ：LAN 1ポートにイーサネットデバイスが接続されていないか、イーサネットリンクが検出されていません。

表 1.LEDの説明（続き）

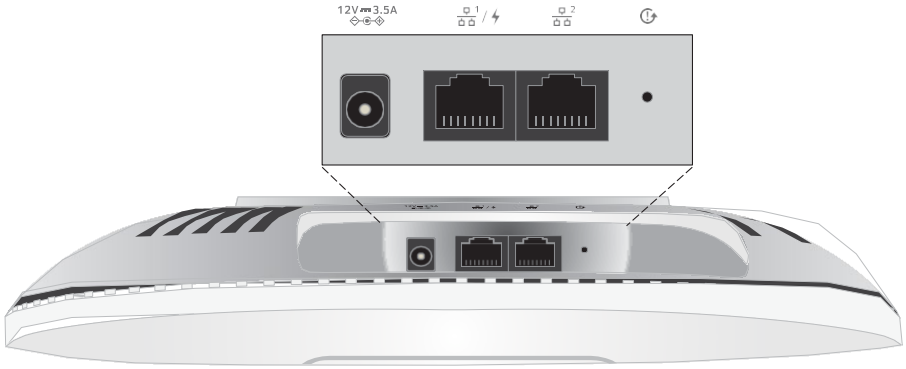
LEDアイコン	カラー	説明
2.4G WLAN LED 2.4GHz	●	**緑の点灯**：2.4 GHz WiFi 無線がオンになっていますが、クライアントは接続されていません。
	●	**青色の点灯**：1 台以上の WLAN クライアントが 2.4 GHz WiFi 無線に接続されています。
	✳	**青色の点滅**：2.4 GHz WiFi 無線でトラフィックが検出されています。
		オフ：2.4GHz WiFi無線はオフです。
5G H WLAN LED 5GHz H	●	**緑の点灯**：5GHzハイバンドWiFi無線がオンになっていますが、クライアントは接続されていません。
	●	**青色の点灯**：1 台以上の WLAN クライアントが 5 GHz ハイバンド WiFi 無線に接続されています。
	✳	**青色の点滅**：5GHzハイバンドWiFi無線でトラフィックが検出されています。
		オフ：5GHzハイバンドWiFi無線はオフです。
5G L WLAN LED 5GHz L	●	**緑色に点灯**：5GHz帯ローバンドWiFi無線がオンになっていますが、クライアントは接続されていません。
	●	**青色の点灯**：1台以上のWLANクライアントが5GHz帯ローバンドWiFi無線に接続されています。
	✳	**青色の点滅**：5 GHz ローバンド WiFi 無線でトラフィックが検出されています。
		オフ：5GHzローバンドWiFi無線はオフです。

注：LEDによるトラブルシューティングについては、245ページのLEDによるトラブルシューティングを参照してください。

ハードウェア・インターフェース

アクセス・ポイントの底部パネルには、オプションの電源アダプタ用の DC 電源コネクタ、LAN 1/PoE++ ポート、LAN 2 ポート、および**リセット**・ボタンがあります。

図2.ハードウェア・インターフェース



ボトムパネルには以下のコンポーネントが含まれる：

- **DC 電源コネクタ**：アクセスポイントに電力を供給するために PoE++ スイッチを使用しない場合は、オプションの電源アダプタを DC 電源コネクタに接続します。
- **LAN 1/PoE++ ポート**：LAN 1/PoE++ ギガビット イーサネット RJ-45 LAN ポートを使用して、アクセス ポイントを PoE++ スイッチに接続するか、 オプションの電源アダプタを使用する場合は、非 PoE スイッチに接続します。アクセスポイントのネットワーク接続には、 LAN 1/PoE++ ポートを使用する必要があります。(LAN 2 ポートはネットワーク接続に使用しないでください。）

  2.5Gbps機器に接続した場合、LAN 1/PoE++ポートはLAN内で最大2.5Gbpsのイーサネット速度をサポートします。インターネット接続、モデム、ルーター、スイッチが2.5Gbpsの速度をサポートしている場合、アクセスポイントのインターネット接続も2.5Gbpsで機能します。それ以外の場合、インターネット接続は一般的な速度である1Gbpsで機能します。

  LAN 1/PoE++ ポートの接続の詳細については、22 ページの「アクセスポイントのセットアップとネットワークへの接続」を参照してください。
- **LAN 2 ポート**：LAN 2 ポートはギガビットイーサネット RJ-45 ポートで、アクセスポイントを LAN 1 ポートと同じスイッチに接続してリンクアグリゲーション（LAG）接続するために使用できます。スイッチは LAG 接続をサポートする必要があり、スイッチで設定する必要があります。アクセスポイントでの LAG の設定と有効化の詳細については、147 ページの「リンクアグリゲーション機能の管理」を参照してください。
- **リセット ボタン**：アクセス ポイントを再起動したり、工場出荷時の設定にリセットするには、**リセット ボタンを**使用します。アクセス ポイントを再起動するには、**リセット** ボタンを約 2 秒間押します。アクセス ポイントを工場出荷時の設定にリセットするには、**リセット ボタンを** 10 秒以上押します。

注: アクセス ポイントを NETGEAR Insight ネットワーク ロケーションに追加した**場合、[リセット]** ボタンの工場出荷時デフォルト設定機能が使用できるようになる前に、まず Insight クラウド ポータルまたは Insight アプリを使用して、Insight ネットワーク ロケーションからアクセス ポイントを削除する必要があります。詳細については、175 ページの「リセットボタンを使用してアクセス ポイントをリセットする」を参照してください。

アクセスポイントラベル

底面のアクセスポイントラベルには、アクセスポイントのQRコード、シリアル番号、MACアドレス、セットアップWiFiネットワーク名（SSID）、ネットワークキー（パスワード）が表示されます。

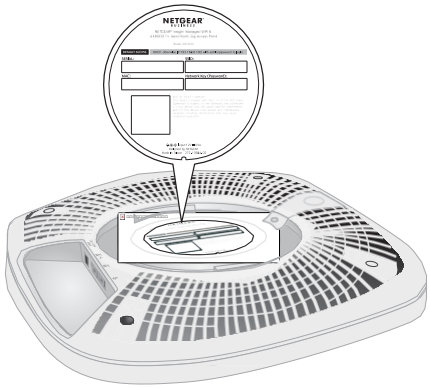


図3.アクセスポイントラベルの位置

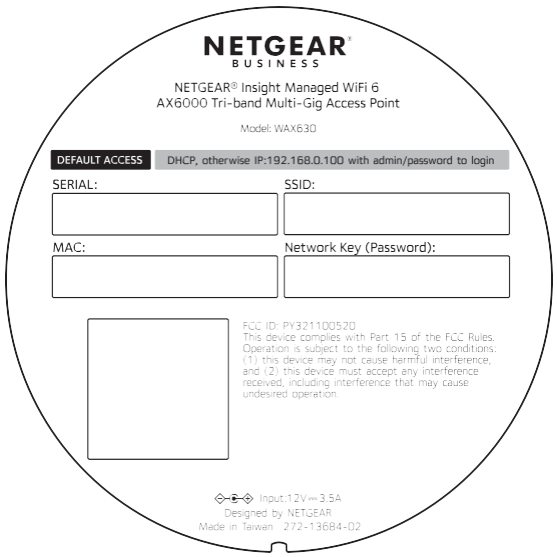


図4.アクセスポイントのラベル

屋内アクセスポイントの安全に関する指示と警告

以下の安全ガイドラインを使用して、個人の安全を確保し、潜在的な損傷からシステムを保護してください。

身体への傷害、感電、火災、装置への損傷を避けるため、以下の注意事項を守ってください：

- 本製品は、温度と湿度が管理された環境での屋内使用専用に設計されています。以下の点にご注意ください：
  - 本製品が動作しなければならない環境の詳細については、付録の環境仕様またはデータシートを参照してください。
  - 本製品をイーサネットケーブルで屋外の機器に接続する場合は、屋外の機器が適切に接地され、サージ保護されている必要があり、屋内製品と屋外の機器の間にイーサネットサージプロテクターをインラインで設置する必要があります。これを怠ると、製品が損傷することがあります。
  - 製品を屋外ケーブルまたは有線屋外機器に接続する前に、https://kb.netgear.com/000057103 で安全および保証に関する追加情報をご確認ください。

  これらのガイドラインに従わない場合、NETGEAR 製品が損傷し、適用される法律で許容される範囲内で NETGEAR の保証が適用されない場合があります。
- 製品マニュアルに記載されている以外の方法で製品を修理しないでください。機器によっては、絶対に開けないでください。
- 次のような状況が発生した場合は、製品の電源プラグを抜いてから、部品を交換するか、トレーニングを受けたサービス担当者にご連絡ください：
  - お使いの製品によっては、電源アダプタ、電源アダプタケーブル、電源アダプタプラグ、またはPoEイーサネットケーブルが損傷しています。
  - 製品に物が落ちた。
  - 製品は水にさらされた。
  - 製品が落下または破損した。
  - 取扱説明書に従って操作しても、製品は正しく動作しません。

- 製品をラジエーターや熱源から遠ざけてください。また、冷却用の通気口を塞がないようにしてください。

- 本製品の部品に食べ物や液体をこぼしたり、濡れた環境で本製品を操作したりしないでください。製品が濡れた場合は、トラブルシューティングガイドの該当セクションを参照するか、トレーニングを受けたサービス担当者に連絡してください。
- 製品の開口部に物を押し込まないでください。内部の部品がショートし、火災や感電の原因となります。
- 本製品は、認可された装置でのみ使用してください。
- ご使用の製品に該当する場合は、カバーを外したり内部部品に触れたりする前に、製品が冷めてから行ってください。
- イーサネットケーブルで接続する機器は、その場所で使用可能な電力で動作する電気定格であることを確認してください。
- お使いの製品によっては、付属の電源アダプターまたはPoE対応のイーサネットケーブルのみを使用してください。

  お使いの製品が電源アダプターを使用している場合：
  - 電源アダプタが提供されていない場合は、最寄りの NETGEAR 販売店にお問い合わせください。
  - 電源アダプターの定格は、本製品および本製品の電気定格ラベルに記載されている電圧と電流に適合している必要があります。

- 感電を防ぐため、システムおよび周辺機器の電源ケーブルはすべて、適切に接地された電源コンセントに接続してください。
- ご使用の製品に該当する場合、周辺電源ケーブルには、適切な接地を確保するための3極プラグが装備されています。アダプタプラグを使用したり、ケーブルから接地プロングを取り外したりしないでください。延長ケーブルを使用する必要がある場合は、適切に接地されたプラグ付きの3線ケーブルを使用してください。
- 延長ケーブルおよび電源タップの定格を守る。延長ケーブルや電源タップに接続されているすべての製品の定格電流の合計が、延長ケーブルや電源タップの定格電流の80%を超えないようにしてください。
- 急激で過渡的な電力の増減からシステムを保護するには、サージサプレッサ、ラインコンディショナ、無停電電源装置（UPS）を使用してください。
- システムケーブル、電源アダプタケーブル、PoEイーサネットケーブルは、慎重に配置してください。ケーブルを踏んだり、つまずいたりしないように配線してください。ケーブルの上には何も乗らないようにしてください。
- 電源アダプター、電源アダプターケーブル、プラグは改造しないでください。電気工事士または電力会社にご相談ください。
- 必ずお住まいの地域や国の配線規則に従ってください。

3

アクセス・ポイントをネットワークに設置し、アクセス・ポイントにアクセスして初期設定を行います。

本章では、アクセスポイントをネットワークにインストールし、アクセスする方法について説明します。この章には、次のセクションがあります：

- 最高のパフォーマンスを得るためのアクセスポイントの位置
- アクセスポイントの設定とネットワークへの接続
- アクセスポイントに接続して初期設定を行う
- 初期設定後、アクセスポイントにログインする
- ブラウザのセキュリティ警告が表示された場合の対処法

注意：本機は専門家による設置が必要です。合法的な周波数チャネル内での操作、出力電力、および DFS 要件を含め、各国の規制に従うことは設置者の責任です。ベンダー、再販業者、または販売業者は、違法な無線操作について責任を負いません。詳細については、デバイスの利用規約を参照してください。

注：このマニュアルでは、*WiFiネットワークは*SSID（サービスセット識別子またはWiFiネットワーク名）またはVAP（仮想アクセスポイント）と同じ意味です。つまり、WiFiネットワークとは、個々のSSIDまたはVAPを意味します。

アクセスポイントを最適な位置に設置する

本マニュアルのインストレーションガイドまたは付録の説明に従ってアクセスポイントを設置およびマウントする前に、最高のパフォーマンスを得るためにアクセスポイントをどのように配置するかを検討してください。

アクセスポイントのWiFi範囲内にあるWiFiクライアントは、WiFiネットワークに接続できます。ただし、WiFi範囲はアクセスポイントの物理的な配置によって大きく異なります。例えば、WiFi 信号が通過する壁の厚さ、密度、数によって範囲が制限されることがあります。

さらに、オフィス、自宅、庭、キャンパス内やその周辺にある他のWiFiデバイスが、アクセスポイントの信号に影響を与える可能性もあります。WiFiデバイスには、他のアクセスポイント、ルーター、リピーター、WiFiレンジエクステンダー、その他WiFi信号を発信してネットワークアクセスを提供するデバイスがあります。

アクセスポイントの位置に関するヒント

- アクセスポイントは、WiFi クライアントが動作するエリアの中央付近に設置します。アクセスポイントと WiFi クライアントの間に見通しの良いラインは必要ありません。
- 電源アダプタを使用する場合は、アクセスポイントがAC電源コンセントの届く範囲にあることを確認してください。
- アクセスポイントを高い場所に設置し、アクセスポイントとWiFiクライアントの間の壁や天井を最小限にします。
- アクセスポイントは、次のような電気機器から離して設置してください：
  - シーリングファン
  - ホーム・セキュリティ・システム
  - 電子レンジ
  - コンピュータ
  - コードレス電話のベース
  - 2.4 GHzおよび5.8 GHzコードレス電話機
- アクセスポイントは、大きな金属面、大きなガラス面、断熱された壁、およびこれらのようなものから離して設置してください：
  - ソリッド・メタル・ドア
  - アルミスタッド
  - 水槽

- 鏡
- レンガ
- コンクリート

隣接するスタンドアロン型アクセスポイントを使用する場合は、干渉を低減するために異なる無線周波数チャネルを使用します。詳しくは、96 ページの無線のチャンネルを変更するを参照してください。

アクセスポイントの設定とネットワークへの接続

アクセスポイントは、ネットワーク内のPower over Ethernet plus（PoE++、802.3bt）スイッチに接続できます。このスイッチは、インターネットに接続されているネットワークルータに接続されている必要があります。PoE++接続を使用する場合、アクセスポイントに電源アダプタは必要ありません。

注：ご注文の製品によっては、電源アダプターが同梱されていない場合があります。アクセスポイントの電源は、PoE++スイッチに接続して供給します。電源アダプターなしのパッケージを注文したが、PoE++接続を使用したくない場合でも、オプションとして電源アダプターを注文できます。

2.5Gbps機器に接続する場合、アクセスポイントLAN 1/PoE++ポートはLAN内で最大2.5Gbpsのイーサネット速度をサポートします。下図はNETGEAR MS510TXUPスイッチを示しており、2.5Gbps以上の速度とPoE++をサポートしています。インターネット接続、モデム、ルーター、スイッチが 2.5 Gbps の速度をサポートしている場合、アクセスポイントのインターネット接続も 2.5 Gbps で機能します。それ以外の場合、インターネット接続は一般的な速度である1Gbpsで機能します。

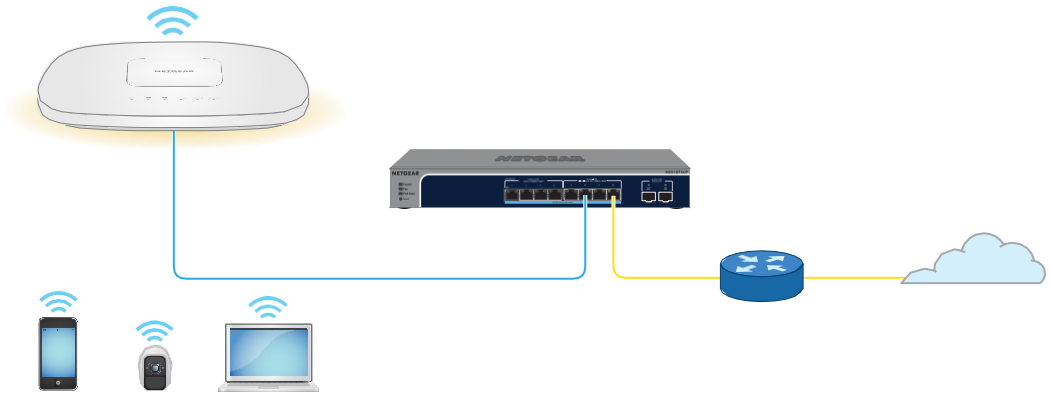


図 5.アクセス・ポイントをネットワークにPoE++接続します。

アクセスポイントをネットワークにイーサネット接続でセットアップするには、次の手順に従います：

1. イーサネットケーブルをアクセスポイントの LAN 1/PoE++ ポートに接続します。
2. イーサネットケーブルのもう一方の端を、ネットワークとインターネットに接続されているスイッチのポートに接続します。

   PoE++スイッチを使用する場合は、アクセスポイントに接続するスイッチポートが 60W PoE++電力を供給できる必要があります。アクセスポイントには、802.3bt（PoE++）入力が必要です。

   注：最適な機能を実現するには、802.3at（PoE+）または 802.3af（PoE）スイッチではなく、802.3bt（PoE++）スイッチを使用していることを確認してください。アクセス ポイントが起動しても電源 LED がオレンジに点灯したままの場合は、アクセス ポイントの PoE 給電が不足している可能性があります。詳細については、247 ページの「アクセス ポイントが PoE PD として機能し、電源 / クラウド LED がオレンジ点灯のままになっている」を参照してください。

   アクセス ポイントが起動中、 またはネットワーク内の DHCP サーバー （または DHCP サーバーとして機能するルーター） から IP アドレスを取得中、 電源 / クラウド LED は最初、 オレンジ （オレンジ） の点灯 （ベタ点灯） になり、 その後、 オレンジ （オレンジ） の点滅 （緩やか） になります。約 2 分後、電源 / クラウド LED が緑色または青色 の点灯に変わり、アクセスポイントは初期設定を実行できるようになります。

初期設定のためのアクセス ポイントへのアクセスについては、23 ページの「初期設定の ためのアクセス ポイントへの接続」を参照してください。

アクセスポイントに接続して初期設定を行う

アクセスポイントを設定した後、初期設定のためにいくつかの方法でアクセスポイントに接続することができます。

アクセス ポイント（および複数のデバイスとネットワーク）のリモート管理には、コンピュータまたはタブレットの NETGEAR Insight クラウド ポータル、または iOS または Android モバイル デバイスの NETGEAR Insight アプリを使用できます。アクセス ポイントをスタンドアロン構成で使用する場合は、コンピューターまたはタブレットでローカル ブラウザー UI を使用できます。詳細については、11 ページの「ローカル ブラウザ ユーザー インターフェイスと NETGEAR Insight について」を参照してください。

Insight Cloud Portal または Insight アプリの使用については、次のいずれかのセクションを参照してください：

- NETGEAR Insight クラウドポータルを使用したインターネット経由での接続 (24 ページ)
- NETGEAR Insight アプリを使って WiFi 経由で接続する (26 ページ)

ローカルブラウザのUIの使用については、以下のセクションのいずれかを参照してください：

- WiFi経由でローカルブラウザUIに接続し、初期設定を行う（28ページ
- LAN経由でローカルのブラウザーUIに接続し、初期設定を行う（33ページ
- 38 ページの「直接接続されたコンピュータを使用したオフラインでのアクセ スポイントの設定

注：ネットワークに DHCP サーバー（または DHCP サーバーとして機能するルーター）がなく、これらのセクションのいずれかに記載されているアクセス ポイントの初期設定を実行しない**場合**、アクセス ポイントには 5 台のクライアントしか接続できず、アクセス ポイントは 5 台のクライアントにしか IP アドレスを提供できません。この 状況を防ぐには、アクセス ポイントの初期設定を必ず実行してください。

NETGEAR Insight Cloud Portalを使用してインターネット経由で接続します。

Insight Cloud Portal は、Insight Premium または Insight Pro 加入者が利用できます。NETGEAR Insight Cloud Portal を使用してアクセス ポイントを設定および管理するには、アクセス ポイントがすでにインターネットに接続されている必要があります。

Insight Cloud Portalの詳細については、以下のページをご覧ください：

- netgear.com/business/services/insight/subscription
- netgear.com/support/product/insight.aspx
- kb.netgear.com/000061848

NETGEAR アカウントは Insight アカウントでもあります。NETGEAR アカウントの認証情報により、Insight Premium ユーザーとして、または Insight Pro アカウントにアップグレードした場合は Insight Pro ユーザーとしてログインできます。

Insight Cloud Portal を介してインターネット経由でアクセスポイントに接続する：

1. アクセスポイントがインターネットに接続されていることを確認します。
2. コンピュータまたはタブレットで、insight.netgear.comにアクセスします。

   NETGEAR アカウント ログイン ページが表示されます。
3. まだインサイトのアカウントをお持ちでない方は、今すぐアカウントを作成してください。

   Insight Premiumアカウントの作成またはInsight Proアカウントへのアップグレードについては、kb.netgear.com/000044343をご覧ください。
4. NETGEAR アカウントの電子メールアドレスとパスワードを入力し、[NETGEAR **Sign In]** ボタンをクリックします。
5. Insight Pro ユーザーの場合のみ、アクセスポイントを追加する組織を選択します。

6. アクセスポイントを追加する新しいネットワークの場所を追加するか、 既存のネットワークの場所を選択します。
7. **+ (Add Device)**ボタンをクリックします。

   注：Insight Proユーザーの場合、デバイスを1台追加するか、デバイスリストをCSVファイルとしてアップロードして、複数のInsight管理デバイスを追加できます。

8. Add New Device] ポップアップページで、アクセスポイントのシリアル番号とMAC アドレスを入力し、[**Go]** をクリックします。

   シリアル番号とMACアドレスは、アクセスポイントのラベルに記載されています。
9. Insight がアクセス ポイントが有効な製品であることを確認したら、オプションでアクセ ス ポイントのデバイス名を変更し、[**Next]** をクリックします。

   アクセス ポイントがポータルに正常に追加されると、セットアップが進行中であることを確認するページが表示されます。

   注：アクセスポイントがオンラインなのにInsightがアクセスポイントを検出しない場合、アクセスポイントがある物理的な場所のファイアウォールがInsightクラウドとの通信を妨げている可能性があります。その場合は、ファイアウォールにアウトバウンドアクセス用のポートと DNS エントリーを追加します。詳しくは、kb.netgear.com/000062467 を参照してください。

   アクセスポイントは、自動的に最新の Insight ファームウェアと Insight ロケーション設定に更新されます。これには最大10分かかる場合があり、その間にアクセスポイントは再起動します。

   アクセスポイントは、Insight クラウドベースの管理プラットフォームに接続された Insight 管理対象デバイスになりました。電源/クラウド LED が緑色の点灯だった場合は、青色の点灯になります。

   アクセスポイントの設定と管理には、Insight Cloud Portal または Insight アプリを使用できます。

注: アクセス ポイントを NETGEAR Insight ネットワーク ロケーションに追加し、Insight クラウド ポータルまたは Insight アプリでアクセス ポイントを管理すると、アクセス ポイントの管理者パスワードが変更されます。つまり、アクセスポイントを Insight ネットワークロケーションに追加すると、そのロケーションの Insight ネットワークパスワードが管理者パスワードに置き換わります。ローカルブラウザーUIにアクセスするには、管理者パスワードではなく、Insightネットワークパスワードを入力する必要があります。後でアクセス ポイントを Insight ネットワークの場所から削除したり、管理モードを Web ブラウザー モードに変更したりする場合（「管理モードを NETGEAR Insight または Web ブラウザーに変更する（155 ページ）」を参照）、アクセス ポイントの管理パスワードを手動で変更するまで、ローカル ブラウザー UI にアクセスするには、引き続き Insight ネットワーク パスワードを使用する必要があります。

NETGEAR Insightアプリを使用してWiFi経由で接続します。

NETGEAR Insightアプリは、Insight PremiumおよびInsight Proの契約者が利用できます。

iOSまたはAndroidモバイルデバイスにNETGEAR Insightアプリをインストールし、アクセスポイントを設定することができます（他の多くのタスクも実行できます）。

インサイトアプリの詳細については、以下のページをご覧ください：

- netgear.com/business/services/insight/subscription
- netgear.com/support/product/insight.aspx
- kb.netgear.com/000061848

NETGEAR アカウントは Insight アカウントでもあります。NETGEAR アカウントの認証情報により、Insight Premium ユーザーとして、または Insight Pro アカウントにアップグレードした場合は Insight Pro ユーザーとしてログインできます。

iOSまたはAndroidのモバイルデバイスを使用してWiFi経由でアクセスポイントに接続します：

1. モバイルデバイスで、アプリストアにアクセスし、NETGEAR Insightを検索し、Insightアプリをダウンロードします。

2. モバイルデバイスで、以下のいずれかの方法を使用して、アクセスポイントのセットアップWiFiネットワークにWiFi経由で接続します：
   - **QRコードをスキャン**：アクセスポイントの底面にあるアクセスポイントラベルのQRコードをスキャンして、セットアップWiFiネットワークに接続します。
   - **手動で接続**：この場合、xxxxxxはアクセスポイントのMACアドレスの下6桁の16進数です。デフォルトのパスワードは**sharedsecret**です。

3. インサイトアプリを起動する。
4. まだインサイトのアカウントをお持ちでない方は、今すぐアカウントを作成してください。

   Insight Premiumアカウントの作成またはInsight Proアカウントへのアップグレードについては、kb.netgear.com/000044343をご覧ください。
5. NETGEARアカウントのメールアドレスとパスワードを入力し、**ログインを**タップします。

6. 次へ] ボタンをタップし、[OK] をタップして、アクセスポイントを追加する新しいネットワークの場所を追加します。

   既存のネットワークの場所を選択することもできます。

   新しいネットワークロケーションに入力したデバイス管理パスワードは、ネットワークロケーションに追加したすべてのデバイスの既存の管理パスワードに置き換わります。

   ほとんどの場合、Insightはアクセスポイントを自動的に検出しますが、これには数分かかります。

7. アクセス ポイントをネットワークの場所に追加するには、次のいずれかを実行します：

   - アクセスポイントが自動的に検出され、[Insight Manageable Devices] セクションに表示されている場合は、アクセスポイントのアイコンをタップし、[**ADD DEVICE]** ボタンをタップします。
   - アクセスポイントが自動的に検出されない場合、または別の方法でアクセスポイントを追加したい場合は、上部バーの「**+**」アイコンをタップし、次のいずれかを実行します：
     - **SCAN BARCODE OR QR CODE**」ボタンをタップし、アクセスポイントのラベルに記載されているアクセスポイントのコードをスキャンします。
     - **Enter Serial Number and MAC Address]**リンクをタップし、アクセス ポイントのラベルに記載されているアクセス ポイントのシリアル番号と MAC アドレスを手動で入力します。

8. プロンプトが表示されたら、アクセスポイントに名前を付け、**[Next]** ボタンをタップします。

   アクセスポイントは、自動的に最新の Insight ファームウェアと Insight ロケーション設定に更新されます。これには最大10分かかる場合があり、その間にアクセスポイントは再起動します。

   アクセスポイントは、Insight クラウドベースの管理プラットフォームに接続された Insight 管理対象デバイスになりました。Power/Cloud LED が緑色の点灯だった場合は、青色の点灯になります。

   アクセスポイントの設定と管理には、Insight Cloud Portal または Insight アプリを使用できます。

注: アクセス ポイントを NETGEAR Insight ネットワークの場所に追加し、Insight クラウドポータルまたは Insight アプリでアクセス ポイントを管理すると、アクセス ポイントの管理者パスワードが変更されます。つまり、その場所の Insight ネットワークパスワードが管理者パスワードに置き換わります。ローカルブラウザー UI にアクセスするには、管理者パスワードではなく、Insight ネットワークパスワードを入力する必要があります。後でアクセス ポイントを Insight ネットワークの場所から削除したり、管理モードを Web ブラウザー モードに変更したりする場合は（「管理モードを NETGEAR Insight または Web ブラウザーに変更する（155 ページ）」を参照）、アクセス ポイントの管理者パスワードを手動で変更するまで、ローカル ブラウザー UI にアクセスするには、引き続き Insight ネットワーク パスワードを使用する必要があります。

WiFi経由でローカルブラウザUIに接続し、初期設定を行う。

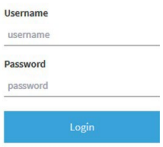
このセクションでは、WiFi 対応のコンピュータまたはモバイルデバイスを使用して（NETGEAR Insight アプリを使用せずに）、WiFi 経由でアクセスポイントに初回接続し、初期設定を完了する方法を説明します。

WiFi経由でローカルブラウザUIに接続し、初期設定を行う：

1. コンピュータまたはモバイルデバイスから、次のいずれかの方法を使用して、アクセスポイントのセットアップWiFiネットワークにWiFi経由で接続します：
   - **QRコードをスキャンします**：アクセスポイントの底面にあるアクセスポイントラベルのQRコードをスキャンして、セットアップWiFiネットワークに接続します。
   - **手動で接続します**：この場合、xxxxxxはアクセスポイントのMACアドレスの下6桁の16進数です。デフォルトのパスワードは**sharedsecret**です。

2. コンピューターまたはモバイルデバイスでウェブブラウザーを起動し、アドレスバーに「**http://aplogin.net**」と入力する。

   注：http://aplogin.net は、アクセスポイントの初期セットアップ中にのみ使用できます。



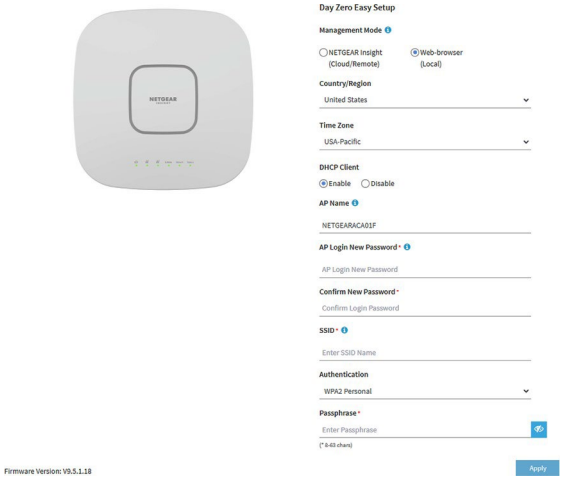
   アクセスポイントの自己署名証明書が原因で、ブラウザがセキュリティ警告を表示するかもしれませんが、これは予期された動作です。

続行するか、セキュリティ警告の例外を追加できます。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。

3. アクセスポイントのユーザー名とデフォルトのパスワードを入力します。

   ユーザー名は**admin**。デフォルトのパスワードは**password**である。ユーザー名とパスワードは大文字と小文字を区別する。

4. **ウェブブラウザの**ラジオボタンを選択します。



   注：ページに表示されている基本設定を保存すると、ログイン時にDay Zero Easy Setupページは表示されなくなります。代わりに、ログインページが表示されます。ログイン後、ダッシュボードページが表示されます。

5. アクセスポイントに最新のファームウェアを確認させるには、**[Check for Upgrade]** をクリックします。

   ボタンをクリックします（このボタンは前の図には表示されていません）。

   アクセスポイントに新しいファームウェアが提供されている場合は、ファームウェアのアップグレードをお勧めします。ファームウェアのアップグレードが完了すると、アクセス ポイントが再起動します。アクセス ポイントの準備ができたら、この手順のステップ 1 に戻ります。

6. 以下の表に記載されている設定を入力してください。

設定	説明
Country /Region	メニューから、アクセスポイントが動作している国と地域を選択します。**注**：デバイスが動作している場所に国が設定されていることを確認してください。チャネル、電力レベル、および周波数範囲に設定されている地域、地方、お よび国の規制を順守する責任があります。 **注**：メニューに記載されている地域以外では、アクセスポイントを操作することが法律で禁止されている場合があります。お住まいの国または地域が一覧にない場合は、お住まいの地域の行政機関にご確認ください。
Time Zone	メニューから、アクセスポイントが動作している国と地域のタイムゾーンを選択します。
DHCP Client	アクセスポイントの DHCP クライアントは、デフォルトでは、アクセスポイントがネットワーク内の DHCP サーバー（または DHCP サーバーとして機能するルーター）から IP アドレスを受信できるようにします。アクセスポイントを静的（固定）IP アドレスで設定するには、次の手順に従います： a. **Disable** ラジオボタンを選択します。追加フィールドが表示されます。 b. IPアドレス、IPサブネットマスク、デフォルトゲートウェイのIPアドレス、DNSサーバーのIPアドレスを指定します。
AP Name	オプションとして、アクセス ポイントの新しい名前を入力します。名前には英数字を含める必要があり、少なくとも 1 文字のアルファベットを含める必要があり、15 文字より長くすることはできず、ハイフンを含めることはできますが、ハイフンで開始または終了することはできません。 デフォルトでは、アクセスポイント名は Netgearxxxxxx で、 xxxxxx はアクセスポイントの MAC アドレスの下 6 桁の 16 進数を表します。
AP Login New Password	新しい管理者パスワードを入力します。これは、アクセスポイントのローカルブラウザ UI にログインする際に使用するパスワードです。(WiFiアクセスに使用するパスワードではありません）。 パスワードの長さは8～63文字で、少なくとも1つの大文字、1つの小文字、1つの数字を含んでいなければなりません。以下の特殊文字が使用できます： !@ # $ % ^ & * ( ) 将来使用するためにパスワードを保存してください。

設定	説明
Confirm New Password	**AP Login New Password]**フィールドに入力したものとまったく同じパスワードを入力します。
SSID	セットアップSSIDは通常の運用では使用できません。セットアップ SSID は初期セットアップ専用です。新しい名前を最大 32 文字で入力します。引用符 (") とバックスラッシュ (\) を除き、英数字と特殊文字を組み合わせて使用できます。

7. **Authentication**メニューから、WiFiネットワークの認証タイプを1つ選択し、該当する場合は、WiFiネットワークの新しいパスフレーズ（ネットワークキーまたはWiFiパスワード）を設定します：
   - **Open**：クライアントは認証されず、トラフィックは暗号化されず、802.11w (PMF)は自動的に無効になります。この設定はセキュリティを提供せず、ほとんどの状況には適していません。メニューから［**Open**］を選択すると、［**Enhanced Open**］チェックボックスが表示され、［**Allow Devices to Connect with Open**］チェックボックスが表示されます：
     - **Enhanced Open**：「**Enhanced Open**」チェックボックスを選択すると、WiFi enhanced open 機能が有効になります。この機能は、opportunistic wireless encryption（OWE）に基づいています。暗号化はCCMモードプロトコル（CCMP）に設定され、802.11w（PMF）は自動的に必須設定になります。
     - **Allow Clients to Authenticate using Legacy Open (OWE Transition Mode)]**：**Enhanced Open** チェックボックスを選択すると、**Allow Clients to Authenticate using Legacy Open (OWE Transition Mode)** チェックボックスが表示されます。このチェックボックスを選択すると、WiFi ネットワークは、WiFi 拡張オープン機能をサポートするクライアントとそうでないクライアントの両方を受け入れることができます。WiFi open enhanced 機能をサポートしていないクライアントの場合、トラフィックは暗号化されません。このチェックボックスを選択しない場合、WiFi ネットワークは、WiFi enhanced open 機能をサポートするクライアントのみを受け入れることができます。
   - **WPA2 Personal**：WPA2をサポートするWiFiクライアントのみがSSIDに接続できるようにします。すべてのWiFiクライアントがWPA2をサポートできる場合は、このオプションを選択します。このオプションは、AES 暗号化を使用します。［**Passphrase**］フィールドに、WiFi ネットワークの新しいパスフレーズを入力します。
   - **WPA2/WPA Personal**：このオプションは、WPAとWPA2の両方のWiFiクライアントがSSIDに接続することを可能にします。このオプションは、TKIPとAESの暗号化を使用します。ブロードキャストパケットでは、TKIPを使用します。ユニキャスト（つまりポイントツーポイント）通信では、WPAクライアントはTKIPを使用し、WPA2クライアントはAESを使用します。［**Passphrase**］フィールドに、WiFiネットワークの新しいパスフレーズを入力します。

- **WPA3 Personal**：このオプションは、WPA3をサポートするWiFiクライアントのみがSSIDに接続できるようにします。すべてのWiFiクライアントがWPA3をサポートできる場合は、このオプションを選択します。このオプションは、SAE暗号化を使用します。**Passphrase**］フィールドに、WiFi ネットワークの新しいパスフレーズを入力します。
- **WPA3/WPA2 Personal**：このオプションは、WPA2およびWPA3の両方のWiFiクライアントがSSIDに接続できるようにします。このオプションは、AESとSAEの暗号化を使用します。WPA2クライアントはAESを使用し、WPA3クライアントはSAEを使用します。**Passphrase**］フィールドに、WiFiネットワークの新しいパスフレーズを入力します。

注: セットアッププロセスを完了した後、RADIUS サーバーを使用して WPA2 Enterprise または WPA3 Enterprise セキュリティを設定できます。詳細については、WiFi ネットワークの認証と暗号化の変更 (73 ページ) を参照してください。

8. **Apply** ボタンをクリックする。

   設定が保存されます。ポップアップウィンドウにIPアドレスと新しいWiFiネットワークとパスワード（パスフレーズ）が表示されます。

   静的IPアドレスを指定した場合は、再ログイン時にIPアドレスを入力する必要があるため、IPアドレス情報を保存してください。

   アクセスポイントから切断されます。デフォルトの国を変更した場合は、アクセスポイントが再起動します。

9. Day Zero Easy Setupページで定義した新しいSSIDとパスフレーズを使用して、アクセスポイントのWiFiネットワークにWiFi経由で再接続します。
10. ブラウザのアドレスバーにアクセスポイントのIPアドレスを入力します。

    IPアドレスを変更した場合は、ステップ6で指定したIPアドレスを入力します。

    アクセスポイントの自己署名証明書が原因で、ブラウザがセキュリティ警告を表示するかもしれませんが、これは予期された動作です。続行するか、セキュリティ警告の例外を追加できます。詳細については、45 ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。

    ログイン画面が表示されます。

11. アクセスポイントのユーザー名とパスワードを入力します。

    ユーザー名は**admin**です。パスワードはDay Zero Easy Setupページで定義したものです。ユーザー名とパスワードは大文字と小文字を区別します。
    Dashboard］ページが表示されます。これで、ネットワーク環境に応じてアクセスポイントの設定をカスタマイズすることができます。

LAN経由でローカルのブラウザーUIに接続し、初期設定を行う。

この手順では、ネットワークに DHCP サーバー （または DHCP サーバーとして機能するルーター） があり、 アクセスポイントとコンピュータが同じ LAN 上にあることを前提に説明します。デフォルトでは、アクセスポイントは DHCP クライアントとして機能します。

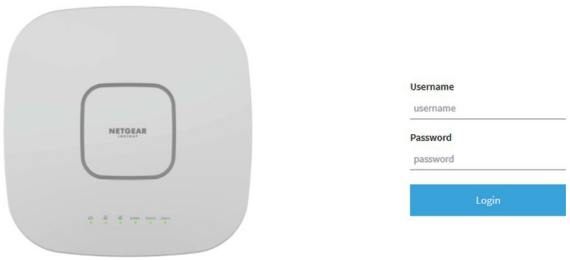
LAN経由でローカルブラウザUIに接続し、初期設定を行う：

1. DHCP サーバーがアクセスポイントに割り当てた IP アドレスを確認するには、DHCP サーバーにアクセスするか、IP ネットワークスキャナーを使用します。

   Windows ベースのコンピュータを使用している場合は、ファイルエクスプローラ（または Windows エクスプローラ）を起動し、ナビゲーションペインから**ネットワークを**選択して、アクセスポイントのデバイスアイコンを右クリックし、 **プロパティを選択して** IP アドレスを表示します。

   注: NETGEAR Insight アプリを使用して、アクセス ポイントに割り当てられている IP アドレスを検出することもできます。詳細については NETGEAR Insight アプリ 26 ページ）を参照してください。

2. コンピュータでウェブブラウザを起動し、アドレスバーにアクセスポイントに割り当てられているIPアドレスを入力します。

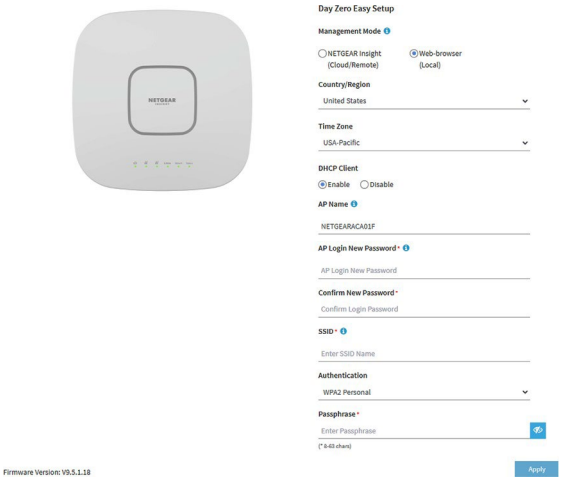
   

   アクセスポイントの自己署名証明書 のために、ブラウザがセキュリティ警告を表示するかもしれません。続行するか、セキュリティ警告の例外を追加できます。詳 しくは、 45 ページの 「ブラウザのセキュリティ警告が表示された場合の対処方法」 を参照してください。

3. アクセスポイントのユーザー名とデフォルトのパスワードを入力します。

ユーザー名は**admin**。デフォルトのパスワードは**password**です。ユーザー名とパスワードは大文字と小文字を区別する。

4. **ウェブブラウザの**ラジオボタンを選択します。



注：ページに表示されている基本設定を保存すると、ログイン時にDay Zero Easy Setupページは表示されなくなります。代わりに、ログインウィンドウが表示されます。ログイン後、ダッシュボードページが表示されます。

5. アクセスポイントに最新のファームウェアを確認させるには、[**Check for Upgrade]**をクリックします。
   ボタンをクリックします（このボタンは前の図には表示されていません）。
   アクセスポイントに新しいファームウェアが提供されている場合は、ファームウェアをアップグレードすることをお勧めします。ファームウェアのアップグレードが完了すると、アクセス ポイントが再起動します。アクセス ポイントの準備ができたら、状況に応じて、この手順のステップ 2 またはステップ 3 に戻ります。

6. 以下の表に記載されている設定を入力してください。

設定	説明
Country/Region	メニューから、アクセスポイントが動作している国と地域を選択します。**注**：デバイスが動作している場所に国が設定されていることを確認してください。チャネル、電力レベル、および周波数範囲に設定されている地域、地方、お よび国の規制を順守する責任があります。 **注**：メニューに記載されている地域以外では、アクセスポイントを操作することが法律で禁止されている場合があります。お住まいの国または地域が一覧にない場合は、お住まいの地域の行政機関にご確認ください。
Time Zone	メニューから、アクセスポイントが動作している国と地域のタイムゾーンを選択します。
DHCP Client	アクセスポイントの DHCP クライアントは、デフォルトでは、アクセスポイントがネットワーク内の DHCP サーバー（または DHCP サーバーとして機能するルーター）から IP アドレスを受信できるようにします。アクセスポイントを静的（固定）IP アドレスで設定するには、次の手順に従います： a. **Disable** ラジオボタンを選択します。追加フィールドが表示されます。 b. IPアドレス、IPサブネットマスク、デフォルトゲートウェイのIPアドレス、DNSサーバーのIPアドレスを指定します。
AP Name	オプションとして、アクセス ポイントの新しい名前を入力します。名前には英数字を含める必要があり、少なくとも 1 文字のアルファベットを含める必要があり、15 文字より長くすることはできず、ハイフンを含めることはできますが、ハイフンで開始または終了することはできません。 デフォルトでは、アクセスポイント名は Netgearxxxxxx で、 xxxxxx はアクセスポイントの MAC アドレスの下 6 桁の 16 進数を表します。
AP login New Password	新しい管理者パスワードを入力します。これは、アクセスポイントのローカルブラウザ UI にログインする際に使用するパスワードです。(WiFiアクセスに使用するパスワードではありません）。 パスワードの長さは8～63文字で、少なくとも1つの大文字、1つの小文字、1つの数字を含んでいなければなりません。以下の特殊文字が使用できます： !@ # $ % ^ & * ( ) 将来使用するためにパスワードを保存してください。

設定	説明
Confirm New Password	**AP Login New Password]**フィールドに入力したものとまったく同じパスワードを入力します。
SSID	セットアップSSIDは通常の運用では使用できません。セットアップ SSID は初期セットアップ専用です。新しい名前を最大 32 文字で入力します。引用符 (") とバックスラッシュ (\) を除き、英数字と特殊文字を組み合わせて使用できます。

7. **Authentication**]メニューから、WiFiネットワークの認証タイプを1つ選択し、該当する場合は、WiFiネットワークの新しいパスフレーズ（ネットワークキーまたはWiFiパスワード）を設定します：

   Open：クライアントは認証されず、トラフィックは暗号化されず、802.11w (PMF) は自動的に無効になります。この設定は、セキュリティを提供しないので、ほとんどの状況には適していません。メニューから［Open］を選択すると、［Enhanced Open］チェックボックスが表示され、［**Allow Devices to Connect with Open**］チェックボックスが表示 *できる：*

   - **Enhanced Open**：「**Enhanced Open**」チェックボックスを選択すると、WiFi enhanced open 機能が有効になります。この機能は、opportunistic wireless encryption（OWE）に基づいています。暗号化はCCMモードプロトコル（CCMP）に設定され、802.11w（PMF）は自動的に必須設定になります。
   - **Allow Clients to Authenticate using Legacy Open (OWE Transition Mode)**：**Enhanced Open** チェックボックスを選択すると、**Allow Clients to Authenticate using Legacy Open (OWE Transition Mode)** チェックボックスが表示されます。このチェックボックスを選択すると、WiFi ネットワークは、WiFi 拡張オープン機能をサポートするクライアントとそうでないクライアントの両方を受け入れることができます。WiFi open enhanced 機能をサポートしていないクライアントの場合、トラフィックは暗号化されません。このチェックボックスを選択しない場合、WiFi ネットワークは、WiFi enhanced open 機能をサポートするクライアントのみを受け入れることができます。

- **WPA2 Personal**：このオプションは、WPA2をサポートするWiFiクライアントのみがSSIDに接続できるようにします。すべてのWiFiクライアントがWPA2をサポートできる場合は、このオプションを選択します。このオプションは、AES暗号化を使用します。**Passphrase**］フィールドに、WiFi ネットワークの新しいパスフレーズを入力します。
- **WPA2/WPA Personal**：このオプションは、WPAとWPA2の両方のWiFiクライアントがSSIDに接続することを可能にします。このオプションは、TKIPとAESの暗号化を使用します。ブロードキャストパケットでは、TKIPを使用します。ユニキャスト（つまりポイントツーポイント）送信では、WPAクライアントはTKIPを使用し、WPA2クライアントはAESを使用します。**Passphrase**］フィールドに、WiFiネットワークの新しいパスフレーズを入力します。

- **WPA3 Personal**：このオプションは、WPA3をサポートするWiFiクライアントのみがSSIDに接続できるようにします。すべてのWiFiクライアントがWPA3をサポートできる場合は、このオプションを選択します。このオプションは、SAE暗号化を使用します。**Passphrase**］フィールドに、WiFi ネットワークの新しいパスフレーズを入力します。
- **WPA3/WPA2 Personal**：このオプションは、WPA2およびWPA3の両方のWiFiクライアントがSSIDに接続できるようにします。このオプションは、AESとSAEの暗号化を使用します。WPA2クライアントはAESを使用し、WPA3クライアントはSAEを使用します。**Passphrase**］フィールドに、WiFiネットワークの新しいパスフレーズを入力します。

注: セットアッププロセスを完了した後、RADIUS サーバーを使用して WPA2 Enterprise または WPA3 Enterprise セキュリティを設定できます。詳細については、WiFi ネットワークの認証と暗号化の変更 (73 ページ) を参照してください。

8. **Apply** ボタンをクリックする。

   設定が保存されます。ポップアップウィンドウにIPアドレスと新しいWiFiネットワークとパスワード（パスフレーズ）が表示されます。

   静的IPアドレスを指定した場合は、再ログイン時にIPアドレスを入力する必要があるため、IPアドレス情報を保存してください。

   デフォルトの国を変更した場合、アクセスポイントは再起動します。

   注：ページを閉じないでください！

   しばらくすると、ダッシュボード・ページが自動的に表示されます。固定IPアドレスを割り当てたなどの理由でダッシュボード・ページが表示されない場合は、次のステップを参照してください。

   これで、ネットワーク環境に合わせてアクセスポイントの設定をカスタマイズできます。

9. ダッシュボードが自動的に表示されない場合は、以下を実行してください：
   a. 以下のいずれかのアクションを取る：
      - アクセス ポイントに固定 IP アドレスを割り当てた場合は、手順 6 で指定した IP アドレスを Web ブラウザのアドレス バーに入力します。
      - 固定IPアドレスを割り当てていない場合は、ウェブブラウザのアドレスバーに表示されているIPアドレスを再入力してください。それでもうまくいかない場合は、IPアドレスをメモし、ウェブブラウザを閉じてから、再度ウェブブラウザを起動し、ウェブブラウザのアドレスバーにIPアドレスを再入力してください。
      - このオプションを使用すると、アクセス ポイントの IP アドレスが表示されます。

        注: NETGEAR Insight アプリを使用して、アクセス ポイントに割り当てられている IP アドレスを検出することもできます。詳細については、26 ページの 「NETGEAR Insight アプリを使って WiFi で接続する」 を参照してください。

        次に、ブラウザを起動し、ウェブブラウザのアドレスバーにIPアドレスを入力する。

      アクセスポイントの自己署名証明書が原因で、ブラウザがセキュリティ警告を表示するかもしれませんが、これは予期された動作です。続行するか、セキュリティ警告の例外を追加できます。詳細については、45 ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。

      ログイン画面が表示されます。
   b. アクセスポイントのユーザー名とパスワードを入力します。

      ユーザー名は**admin**です。パスワードは Day Zero Easy Setup ページで定義したものです。ユーザー名とパスワードは大文字と小文字を区別します。

      ダッシュボード] ページが表示されます。これで、ネットワーク環境に合わせてアクセスポイントの設定をカスタマイズできます。

直接接続されたコンピュータを使用してオフラインでアクセスポイントを設定する

アクセス ポイントをオフラインにし（つまり、ネットワークから切断し）、イーサネット ケーブルでコンピュータをアクセス ポイントの LAN 2 ポートに接続し、デフォルトの IP アドレスでアクセス ポイントに接続すると、オフラインでアクセス ポイントを設定できます。この設定を完了したら、アクセス ポイントをオンラインにすることができます。

注： オフライン設定を完了し、アクセス ポイントをネットワークに設置したら、ネットワーク接続に LAN 1/PoE++ ポートを使用していることを確認してください。電源アダプタを使用するためアクセスポイントへの PoE++ 接続が不要な場合でも、ネットワーク接続には LAN 1/PoE++ ポートを使用する必要があります。

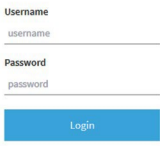
アクセスポイントのLAN 2ポートに接続したパソコンを使ってアクセスポイントに接続する場合：

1. コンピュータのIPアドレスとサブネットマスクを記録し、後でこれらのIPアドレス設定を元に戻せるようにします。
2. コンピュータのIPアドレスを一時的に192.168.0.210、サブネットマスクを255.255.255.0に変更します。

   (アクセスポイントのデフォルトIPアドレスであるIPアドレス192.168.0.100を除き、実際には192.168.0.2～192.168.0.254の範囲内のどのIPアドレスでも使用できます)。

   コンピュータのIPアドレスの変更についての詳細は、コンピュータのヘルプまたはマニュアルを参照してください。
3. イーサネットケーブルを使用して、コンピュータをアクセスポイントの LAN 2 ポートに接続します。
4. コンピュータでウェブブラウザを起動し、アドレスバーに**192.168.0.100**と入力する。

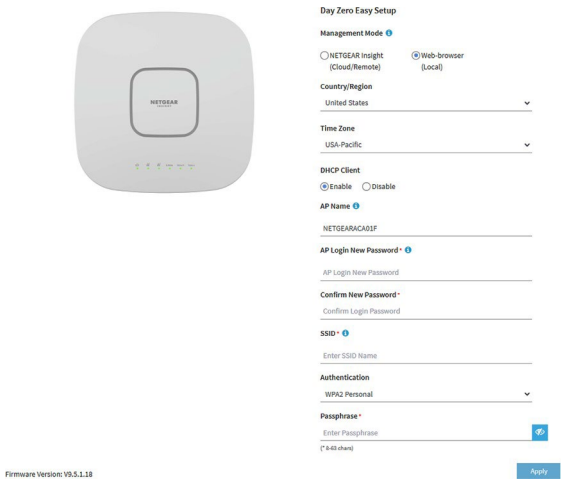
   

   アクセスポイントの自己署名証明書が原因で、ブラウザがセキュリティ警告を表示するかもしれませんが、これは予期された動作です。続行するか、セキュリティ警告の例外を追加できます。詳細については、45 ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
5. アクセスポイントのユーザー名とデフォルトのパスワードを入力します。

ユーザー名は**admin**。デフォルトのパスワードは**passwordです**。ユーザー名とパスワードは大文字と小文字を区別する。

6. **ウェブブラウザの**ラジオボタンを選択します。



注：ページに表示されている基本設定を保存すると、ログイン時にDay Zero Easy Setupページは表示されなくなります。代わりに、ログインウィンドウが表示されます。ログイン後、ダッシュボードページが表示されます。

7. アクセスポイントに最新のファームウェアを確認させるには、**[アップグレードの確認]**をクリックします。
   ボタンをクリックします（このボタンは前の図には表示されていません）。
   アクセスポイントに新しいファームウェアが提供されている場合は、ファームウェアをアップグレードすることをお勧めします。ファームウェアのアップグレードが完了すると、アクセス ポイントが再起動します。アクセス ポイントの準備ができたら、状況に応じて、この手順のステップ 4 またはステップ 5 に戻ります。

8. 以下の表に記載されている設定を入力してください。

設定	説明
Country/Region	メニューから、アクセスポイントが動作している国と地域を選択します。**注**：デバイスが動作している場所に国が設定されていることを確認してください。チャネル、電力レベル、および周波数範囲に設定されている地域、地方、お よび国の規制を順守する責任があります。 **注**：メニューに記載されている地域以外では、アクセスポイントを操作することが法律で禁止されている場合があります。お住まいの国または地域が表示されていない場合は、最寄りの行政機関にご確認ください。
Time Zone	メニューから、アクセスポイントが動作している国と地域のタイムゾーンを選択します。
DHCP Client	アクセスポイントの DHCP クライアントは、デフォルトでは、アクセスポイントがネットワーク内の DHCP サーバー（または DHCP サーバーとして機能するルーター）から IP アドレスを受信できるようにします。アクセスポイントを静的（固定）IP アドレスで設定するには、次の手順に従います： a. **Disable** ラジオボタンを選択します。追加フィールドが表示されます。 b. IPアドレス、IPサブネットマスク、デフォルトゲートウェイのIPアドレス、DNSサーバーのIPアドレスを指定します。
AP Name	オプションとして、アクセス ポイントの新しい名前を入力します。名前には英数字を含める必要があり、少なくとも 1 つのアルファベット文字を含める必要があります。 デフォルトでは、アクセスポイント名は Netgearxxxxxx で、 xxxxxx はアクセスポイントの MAC アドレスの下 6 桁の 16 進数を表します。
AP Login New Password	新しい管理者パスワードを入力します。これは、アクセスポイントのローカルブラウザ UI にログインするために使用するパスワードです。(WiFiアクセスに使用するパスワードではありません）。 パスワードの長さは8～63文字で、少なくとも1つの大文字、1つの小文字、1つの数字を含んでいなければなりません。以下の特殊文字が使用できます： !@ # $ % ^ & * ( ) 将来使用するためにパスワードを保存してください。

設定	説明
Confirm New Password	**AP Login New Password]**フィールドに入力したものとまったく同じパスワードを入力します。
SSID	セットアップSSIDは通常の運用では使用できません。セットアップ SSID は初期セットアップ専用です。新しい名前を最大 32 文字で入力します。引用符 (") とバックスラッシュ (\) を除き、英数字と特殊文字を組み合わせて使用できます。

9. **Authentication**メニューから、WiFiネットワークの認証タイプを1つ選択し、該当する場合は、WiFiネットワークの新しいパスフレーズ（ネットワークキーまたはWiFiパスワード）を設定します：
   - **Open**：クライアントは認証されず、トラフィックは暗号化されず、802.11w (PMF) は自動的に無効になります。この設定は、セキュリティを提供しないので、ほとんどの状況には適していません。メニューから［**Open**］を選択すると、［**Enhanced Open**］チェックボックスが表示され、［**Allow Devices to Connect with Open**］チェックボックスが表示 できる：
     - **Enhanced Open**：「**Enhanced Open**」チェックボックスを選択すると、WiFi enhanced open 機能が有効になります。この機能は、opportunistic wireless encryption（OWE）に基づいています。暗号化はCCMモードプロトコル（CCMP）に設定され、802.11w（PMF）は自動的に必須設定になります。
     - **Allow Clients to Authenticate using Legacy Open (OWE Transition Mode)**：**Enhanced Open** チェックボックスを選択すると、**Allow Clients to Authenticate using Legacy Open (OWE Transition Mode)** チェックボックスが表示されます。このチェックボックスを選択すると、WiFi ネットワークは、WiFi 拡張オープン機能をサポートするクライアントとそうでないクライアントの両方を受け入れることができます。WiFi open enhanced 機能をサポートしていないクライアントの場合、トラフィックは暗号化されません。このチェックボックスを選択しない場合、WiFi ネットワークは、WiFi enhanced open 機能をサポートするクライアントのみを受け入れることができます。
   - **WPA2 Personal**：このオプションは、WPA2をサポートするWiFiクライアントのみがSSIDに接続できるようにします。すべてのWiFiクライアントがWPA2をサポートできる場合は、このオプションを選択します。このオプションは、AES暗号化を使用します。**Passphrase**］フィールドに、WiFi ネットワークの新しいパスフレーズを入力します。
   - **WPA2/WPA Personal**：このオプションは、WPAとWPA2の両方のWiFiクライアントがSSIDに接続することを可能にします。このオプションは、TKIPとAESの暗号化を使用します。ブロードキャストパケットでは、TKIPを使用します。ユニキャスト（つまりポイントツーポイント）通信では、WPAクライアントはTKIPを使用し、WPA2クライアントはAESを使用します。**Passphrase**］フィールドに、WiFiネットワークの新しいパスフレーズを入力します。

- **WPA3 Personal**：このオプションは、WPA3をサポートするWiFiクライアントのみがSSIDに接続できるようにします。すべてのWiFiクライアントがWPA3をサポートできる場合は、このオプションを選択します。このオプションは、SAE暗号化を使用します。**Passphrase**］フィールドに、WiFi ネットワークの新しいパスフレーズを入力します。
- **WPA3/WPA2 Personal**：このオプションは、WPA2およびWPA3の両方のWiFiクライアントがSSIDに接続できるようにします。このオプションは、AESとSAEの暗号化を使用します。WPA2クライアントはAESを使用し、WPA3クライアントはSAEを使用します。**Passphrase**］フィールドに、WiFiネットワークの新しいパスフレーズを入力します。

注: セットアッププロセスを完了した後、RADIUS サーバーを使用して WPA2 Enterprise または WPA3 Enterprise セキュリティを設定できます。詳細については、WiFi ネットワークの認証と暗号化の変更 (73 ページ) を参照してください。

10. **Apply** ボタンをクリックする。

    設定が保存されます。ポップアップウィンドウにIPアドレスと新しいWiFiネットワークとパスワード（パスフレーズ）が表示されます。

    静的IPアドレスを指定した場合は、再ログイン時にIPアドレスを入力する必要があるため、IPアドレス情報を保存してください。

    アクセスポイントから切断されます。デフォルトの国を変更した場合は、アクセスポイントが再起動します。

11. 数分後、ログイン・ウィンドウが自動的に表示されない場合は、次のように入力します。

    ブラウザのアドレスバーに**192.168.0.100を入力して**ください。

    IPアドレスを変更した場合は、ステップ8で指定したIPアドレスを入力します。

    アクセスポイントの自己署名証明書が原因で、ブラウザがセキュリティ警告を表示するかもしれませんが、これは予期された動作です。続行するか、セキュリティ警告の例外を追加できます。詳細については、45 ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。

    ログイン画面が表示されます。

12. アクセスポイントのユーザー名とパスワードを入力します。

    ユーザー名は**admin**です。パスワードはDay Zero Easy Setupページで定義したものです。ユーザー名とパスワードは大文字と小文字を区別します。

    ダッシュボード] ページが表示されます。これで、ネットワーク環境に合わせてアクセスポイントの設定をカスタマイズできます。

13. セットアッププロセス、またはセットアップとカスタマイズの両方のプロセスが完了したら、コンピュータを元のIPアドレス設定に戻すことができます。

初期設定後、アクセスポイントにログインする

初期設定後、アクセスポイントは使用可能な状態になり、設定の変更やトラフィックの監視ができるようになります。

アクセスポイントのローカルブラウザ UI にログインする：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

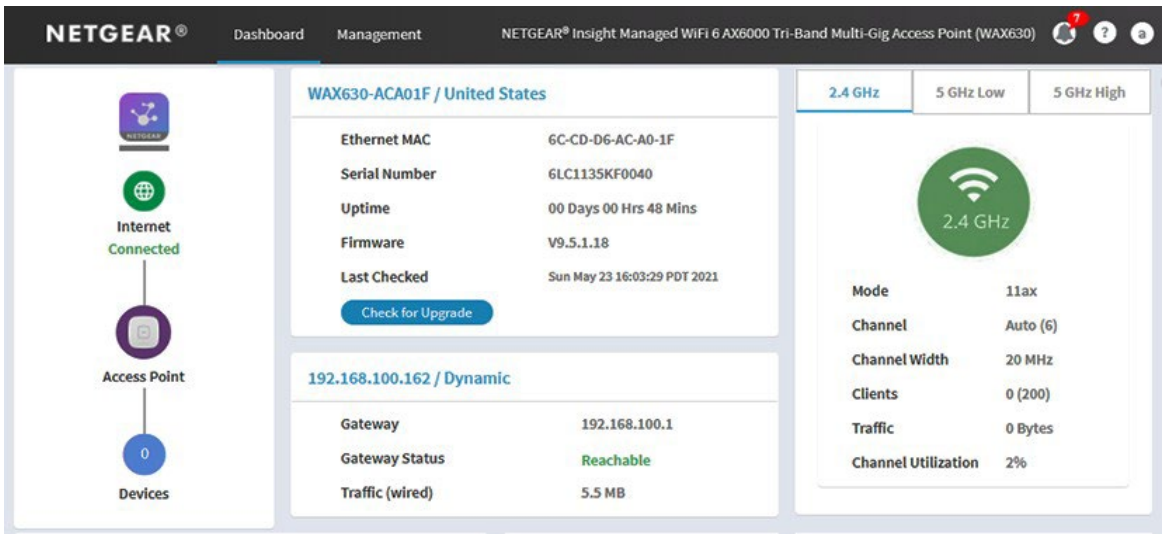
   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。

次の図は、ダッシュボード・ページの上部を示している。



ダッシュボード]ページには、アクセスポイントの状態を一目で確認できるさまざまなペインが表示されます。ダッシュボード]ページとその各種ペインの詳細については、182 ページの「アクセスポイントとネットワークの監視」を参照してください。

ブラウザのセキュリティ警告が表示された場合の対処法

ブラウザのアドレス欄にアクセスポイントに割り当てられているIPアドレスを入力すると、デバイスの自己署名証明書のためにセキュリティ警告が表示されることがあります。これは予期された動作です。続行するか、セキュリティ警告の例外を追加できます。

セキュリティ警告を続行するか、セキュリティ警告の例外を追加する：

- **Google Chromeの場合：ADVANCED]** リンクをクリックします。このとき、x.x.x.xはデバイスのドメイン名またはIPアドレスを表します）次に、「**Proceed to x.x.x.x (unsafe)** 」リンクをクリックします。
- **Apple Safariを使用します：詳細を表示**」ボタンをクリックします。次に、「**このWebサイトを訪問する**」リンクをクリックします。警告のポップアップウィンドウが表示された場合は、「**Webサイトにアクセス**」ボタンをクリックします。証明書の信頼設定の変更を確認するための別のポップアップウィンドウが表示された場合は、Macのユーザー名とパスワードを入力し、「**設定を更新**」ボタンをクリックします。
- **Mozilla Firefox**：**ADVANCED**ボタンをクリックします。次に、**[例外の追加]ボタン**をクリックします。表示されたポップアップウィンドウで、［**セキュリティ例外の確認**］ボタンをクリックします。
- **Microsoft Edge**: [**Details] > [Go on the webpage]** を選択します。
- **Microsoft Internet Explorer**：**このウェブサイトに進む（推奨されません）**リンクをクリックします。

4

Insight Instant Mesh WiFiネットワークにアクセスポイントを設置する

アクセスポイントは、通常のスタンドアロンアクセスポイントとして機能するだけでなく、Insight Instant Mesh WiFiネットワークにおいて、ルートアクセスポイント（*ルートと呼ぶ*）またはノードアクセスポイント（*ノードと呼ぶ*）として機能することができます。この章では、NETGEAR Insight クラウドポータルまたは Insight アプリを使用してアクセスポイントをルートに接続し、アクセスポイントを Insight Instant Mesh WiFi ネットワークのノードとして機能させる方法について説明します。NETGEAR Insight クラウドポータルと Insight アプリは、Insight Premium と Insight Pro の契約者が利用できます。

注記: ルートへの接続で NETGEAR Insight Instant Mesh WiFi ネットワークのノードを設定するには、NETGEAR Insight クラウドポータルまたは Insight アプリのいずれかを使用する必要があります。ローカルブラウザ UI を使用してルートへのメッシュ WiFi 接続を設定することはできません。

Insight Cloud Portal および Insight アプリでノードを管理および監視する方法については、netgear.com/insight を参照してください。Insight Cloud Portal と Insight アプリにはヘルプが組み込まれており、netgear.com/support にアクセスしてアクセスできる複数のナレッジベース記事に文書化されています。

この章には以下のセクションがある：

- ルートとノードとは何ですか？
- インサイト・インスタント・メッシュWiFiネットワークとは何ですか？
- メッシュWiFiネットワークにノードを配置するための要件
- NETGEAR Insight Cloud Portal にアクセスして、Insight Instant Mesh WiFi ネットワークを設定または管理します。
- クラウド・ポータルを使用して、アクセス・ポイントをノードとしてルートに接続する。
- NETGEAR InsightアプリをインストールしてInsight Instant Mesh WiFiネットワークを管理する
- Insightアプリを使用して、アクセスポイントをノードとしてルートに接続する

注：このマニュアルでは、***WiFiネットワークは***SSID（サービスセット識別子またはWiFiネットワーク名）またはVAP（仮想アクセスポイント）と同じ意味です。つまり、WiFiネットワークとは、個々のSSIDまたはVAPを意味します。

ルートとノードとは何ですか？

アクセスポイントは、インサイトインスタントメッシュWiFiネットワークのルートまたはノードとして機能します：

- **ルート**：ネットワークへの有線接続を設定して、ノードとして機能する1つまたは複数のメッシュ対応アクセスポイントへのゲートウェイを作成するメッシュ対応アクセスポイント。ルートでは、ネットワークへの接続にイーサネットポートを使用します。ルートは、複数のノードに同時にサービスを提供できます。
- **ノード**：インターネット接続を提供するルートへのWiFiバックホール接続を持つメッシュ対応アクセスポイント。ノードは有線接続ではなく、WiFi接続でネットワークに接続される。

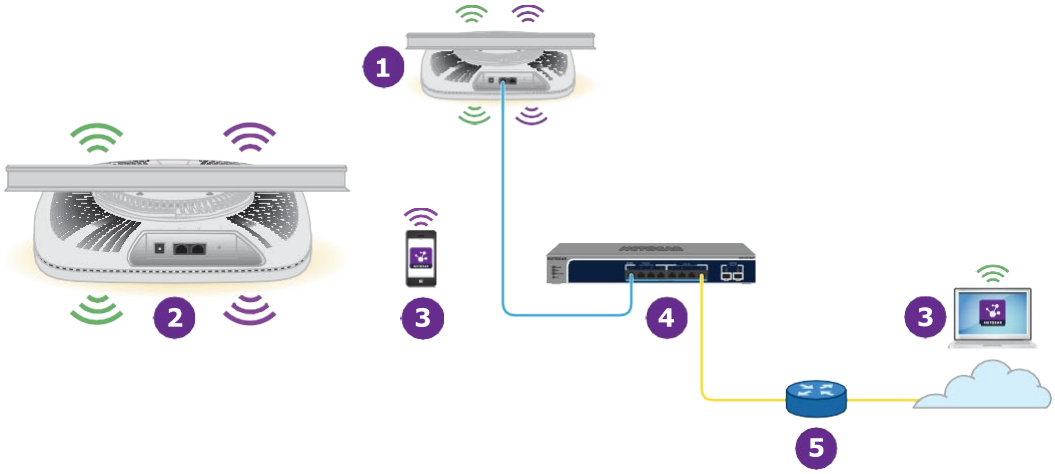


図6.ノードとワイヤード・ルートを持つメッシュ・ネットワーク

番号またはアイコンと説明
1 ネットワーク・スイッチにイーサネットで接続されているルート。
2 5GHzのバックホールWiFi接続でルートに接続されているノード。
3 Insightアプリをインストールした携帯電話、またはInsightクラウドポータルにアクセスできるコンピューターまたはタブレット。Insight Cloud PortalまたはInsightアプリで、Insight Instant Mesh WiFiネットワークのノードを設定・管理できます。
4 ネットワーク・スイッチ。
5 インターネットに接続されているネットワーク・ルーター。

続き

番号またはアイコンと説明
2.4GHz帯の電波。
5GHz帯のhighまたはLowの電波。

インサイト・インスタント・メッシュWiFiネットワークとは何ですか？

メッシュWiFiネットワークは、少なくとも1つのメッシュ対応ルートと、WiFi経由でルートに接続する1つ以上のノードで構成されます（47ページの「ルートとノードとは」を参照）。ルートは、ルータまたはインターネットゲートウェイにイーサネットで接続され、ノードにインターネットアクセスを提供します。ルートとノードは、メッシュネットワークであるWiFiネットワークで広範なエリアをカバーするために協働します。

メッシュネットワークは、以下のような環境にWiFiを導入したい場合に有効なソリューションとなる：

- ケーブルが利用できない近くの部屋（見通しで、現在のWiFi受信範囲内）
- 近隣のオフィスビル（見通しが良く、現在のWiFi受信範囲内）
- ケーブルが通せない環境

メッシュWiFiネットワークでは、ノードはWiFi接続を介してルートに接続し、WiFiクライアントにWiFiネットワークをブロードキャスト（拡張）する：

- **バックホール接続**：ルートとノード間のWiFi接続はバックホール接続と呼ばれる。
- **フロントホール接続**：ノードとそのWiFiクライアント間のWiFi接続は、フロントホール接続と呼ばれる。

NETGEAR Insight Instant Mesh WiFi ネットワークでは、ルートとノード間のメッシュ WiFi 接続を設定するには、Insight Cloud Portal または Insight アプリを使用する必要があります。つまり、ルートまたはノードのローカルブラウザ UI からはできません。複数のルートがあるネットワークでは、NETGEAR Insight は最も強い WiFi 信号を持つルートにノードを自動的に接続します。

ノードはルートと同じWiFiネットワークまたはネットワークをブロードキャストしますが、ノードにWiFiネットワークを設定し、ルートやメッシュネットワーク内の他のノードからブロードキャストすることもできます。

アクセスポイントは、5GHzのハイバンドとローバンド（バックホール接続に適したバンド）、および2.4GHzバンドでブロードキャストできます。WiFiクライアントのWiFi機能（）に応じて、どのバンドでもフロントホール接続を提供できます。

メッシュWiFiネットワークにノードを配置するための要件

以下は、Insight Instant Mesh WiFiネットワークにノードを配置するための要件です：

- 既存のWiFiネットワークには、最新のファームウェアバージョンが動作するメッシュ対応アクセスポイントが少なくとも1つ含まれている必要があります。ルートでは、ネットワークへの接続にイーサネットポートを1つ使用します。
- ノードは工場出荷時のデフォルト状態でなければなりません。ノードを以前ネットワークで使用していた場合は、アクセスポイントを工場出荷時のデフォルト設定にリセットしてください。
- ノードは、ルートと同期できるように、ルートのWiFi信号の範囲内にある必要があります。セットアップの際、信頼性の高いWiFi接続を実現するために、ノードは最も近いルートから7.5m以内で、障害物の少ない見通しの良い場所に設置してください。
- 既存の WiFi ネットワークにノードをインストールするには、NETGEAR Insight Cloud Portal または Insight アプリを使用する必要があります。

以下の NETGEAR アクセス ポイント モデルは、ルートまたはノードとして機能します：

- WAX610
- WAX610Y(ノードとして機能しますが、電源はPoEのみとなります。)
- WAX615
- WAX618
- WAX620
- WAX625
- WAX628
- WAX630
- WAX630E
- WAX638E

- WAC564
- WAC540

注：WAX610、WAX610Y、WAX615、WAX618、WAX620、WAX625、WAX628、WAX630、WAX630E、またはWAX638Eモデルと*WAC540*または*WAC564*を使用したメッシュWiFiネットワークの場合。

モデル、WAC540およびWAC564モデルは、ファームウェアバージョン9.5またはそれ以降のバージョンを実行する必要があります。

近い将来、NETGEARのモデルがさらに追加されるかもしれない。

NETGEAR Insight Cloud Portal にアクセスして、Insight Instant Mesh WiFi ネットワークを設定または管理します。

NETGEAR Insight Cloud Portalは、Insight PremiumとInsight Proの契約者が利用できます。

Insight Instant Mesh WiFi ネットワークにアクセスポイントを設置したら、Insight Cloud Portal を使用してメッシュ WiFi 接続を設定し、アクセスポイントを設定、管理、監視できます。

NETGEAR Insight Cloud Portalの詳細については、以下のページをご覧ください：

- netgear.com/business/services/insight/subscription
- netgear.com/support/product/insight.aspx
- kb.netgear.com/000061848

Insight Cloud Portal を介してインターネット経由でアクセスポイントに接続する：

1. コンピュータまたはタブレットで、insight.netgear.comにアクセスします。
   NETGEAR アカウント ログイン ページが表示されます。
2. まだインサイトのアカウントをお持ちでない方は、今すぐアカウントを作成してください。
   Insight Premiumアカウントの作成またはInsight Proアカウントへのアップグレードについては、kb.netgear.com/000044343をご覧ください。
3. NETGEAR アカウントの電子メールアドレスとパスワードを入力し、[NETGEAR **Sign In]** ボタンをクリックします。

これで、アクセスポイントのメッシュWiFi接続を設定できます。詳細については、kb.netgear.com/000061304を参照してください。

クラウド・ポータルを使用して、アクセス・ポイントをノードとしてルートに接続する。

NETGEAR Insight Cloud Portalは、Insight PremiumとInsight Proの契約者が利用できます。

Insight Cloud Portal を使用して、アクセスポイントをノードとしてルートに接続できます。ルートがノードにインターネット接続を提供できるように、ルーターまたはインターネットゲートウェイへの有線接続を設定する必要があります。

Insight Cloud Portal、および Insight Cloud Portal で利用可能な設定と管理オプションの詳細については、netgear.com/insight をご覧ください。Insight Cloud Portal にはヘルプが組み込まれており、netgear.com/support からアクセスできる複数のナレッジベース記事に文書化されています。

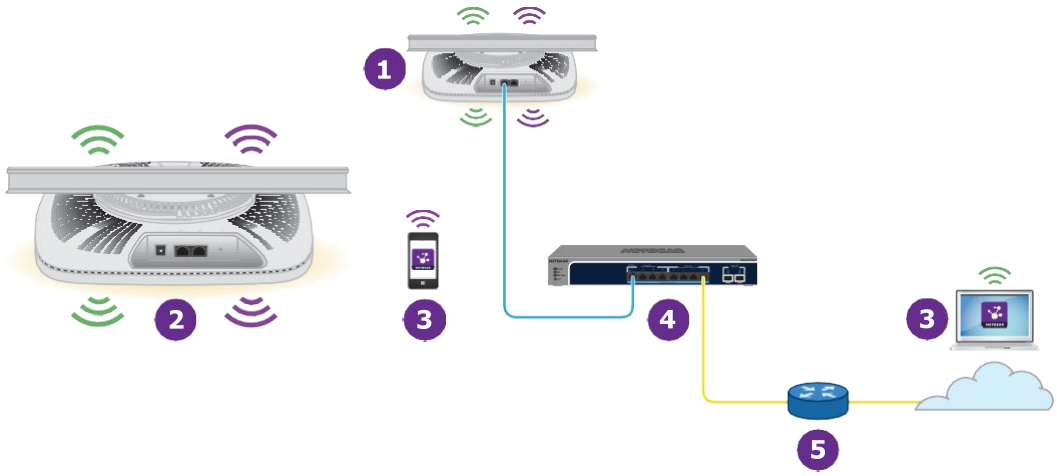


図7.ノードを有線ルートに接続する

番号またはアイコンと説明
1 ネットワーク・スイッチにイーサネットで接続されているルート。
2 5GHzのバックホールWiFi接続でルートに接続されているノード。
3 Insightアプリを搭載した携帯電話、またはInsightクラウドポータルにアクセスできるコンピューターまたはタブレット。Insight Cloud PortalまたはInsightアプリで、Insight Instant Mesh WiFiネットワークのノードを設定・管理できます。
4 ネットワーク・スイッチ。

番号またはアイコンと説明
5 インターネットに接続されているネットワーク・ルーター。
2.4GHz帯の電波。
5GHz帯のHighまたはLowの電波。

ノードは、ルートへのバックホール接続とWiFiクライアントへのフロントホール接続を確立するために、どのバンドを使用することもできます。ただし、バックホール接続が確立された後、ルートとノードの両方が5 GHzバンドをサポートできる場合、ノードはバックホール接続の優先バンドとして5 GHzバンドに自動的に切り替わります。Insight Cloud Portal を使用して、バックホール設定を変更できます。

Insight Cloud Portal を使用して、ノードを既存の WiFi ネットワークのルートに接続するには：

1. Insight ネットワークの場所のメッシュモードが Auto に設定されていることを確認します。詳細については、kb.netgear.com/000064932 を参照してください。
2. ルートのメッシュモードがAutoに設定されていることを確認してください。詳細については、kb.netgear.com/000064931をご覧ください。
3. ノードが工場出荷時の状態になっていることを確認する。
   アクセスポイントを以前ネットワークで使用していた場合は、アクセスポイントを工場出荷時の設定にリセットします。
4. 信頼性の高いWiFi接続を行うには、ノードを最も近いルートから7.5m（25フィート）以内で、障害物の少ない見通しの良い場所に設置してください。
5. ノードを電源に接続する。
   ノードの電源/クラウドLEDがオレンジに点灯した後、緑色に点灯します。

   注：ネットワークのループを防ぐには、ノードをルートと同じネットワークやインターネットに接続されていないPoE++スイッチに接続します。オプションの電源アダプタを使用することもできます。
6. insight.netgear.com にアクセスして Insight Cloud Portal にアクセスし、NETGEAR の電子メールアドレスとパスワードを入力し、**NETGEAR Sign In** ボタンをクリックします。
7. Insight Pro ユーザーの場合のみ、ノードを追加する組織を選択します。

8. ノードを追加する場所を選択します。
9. **+ (Add Device)**ボタンをクリックします。
10. Add New Device（新しいデバイスの追加）ポップアップ・ページで、ノードのシリアル番号とMACアドレスを入力し、**Go**をクリックします。

    インサイトはノードを自動的に検出します。このプロセスには数分かかる場合があります。

    ノードは、Insight Instant Mesh WiFiネットワークで最も強いWiFi信号を提供するルートを検出し、接続を試みます。

    注：初期接続と設定プロセスには最大10分かかる場合があります。設定プロセス中にノードが再起動することがあります。

11. ノードが初期接続と設定プロセスを経て、電源/クラウドLEDがオレンジ、緑色、青色の点滅を止め、青色で点灯するのを待ちます。

    注：初期接続と設定プロセスには最大10分かかる場合があります。設定プロセス中にノードが再起動することがあります。

    電源/クラウドLEDは、最初の接続と設定プロセス中に以下のように点灯します：

    - **緑色に点滅**：ノードはルートを検出しようとしている。
    - **緑色に点灯**：ノードは、最も強いWiFi信号を提供するルートと最初の接続を行っています。
    - **オレンジでゆっくり点滅**：ノードがネットワークルーターまたはDHCPサーバーに連絡してIPアドレスを受信している。
      電源 / クラウド LED のオレンジの点滅が止まらない場合は、247 ページの「電源 / クラウド LED がオレンジでゆっくりと点滅し続けている」を参照してください。
    - **オレンジ、グリーン、ブルーの点滅**：ノードは、Insight Instant Mesh WiFi ネットワークの管理対象デバイスとして設定されています。
      電源/クラウドLEDがオレンジ、緑色、青色の点滅を停止しない場合は、電源/クラウドLEDがオレンジ、緑色、青色の点滅を停止しない（249ページ） を参照してください。

    設定が完了すると、Power/Cloud LEDが以下のように点灯します：

    - **青色で点灯**：設定が完了し、ノードを操作できる状態。ノードはInsight Instant Mesh WiFiネットワークで機能し、Insightクラウドに接続されています。

ノードは自動的にルートのWiFiネットワークをブロードキャスト（拡張）するように設定される。

ノードとルートの接続が困難な場合は、「ノードとルートが接続できません（250ページ）」を参照してください。

NETGEAR Insight Cloud Portal および Insight アプリによるノードへのアクセス、管理、監視については、netgear.com/insight をご覧ください。Insight Cloud Portal と Insight アプリにはヘルプが組み込まれており、netgear.com/support にアクセスしてアクセスできる複数のナレッジベース 記事で文書化されています。

NETGEAR Insightアプリをインストールして Insight Instant Mesh WiFiネットワークを管理する

NETGEAR Insightアプリは、Insight PremiumおよびInsight Proの契約者が利用できます。

NETGEAR Insightアプリを使用してInsight Instant Mesh WiFiネットワークにアクセスポイントを追加する前に、iOSまたはAndroidモバイルデバイスにアプリをインストールする必要があります。

NETGEAR Insightアプリの詳細については、以下のページをご覧ください：

- netgear.com/business/services/insight/subscription
- netgear.com/support/product/insight.aspx
- kb.netgear.com/000061848

Insight Instant Mesh WiFiネットワークを管理するためにInsightアプリをインストールするには：

1. モバイルデバイスで、アプリストアにアクセスし、NETGEAR Insightを検索し、Insightアプリをダウンロードします。

2. インサイトアプリを起動する。
3. まだインサイトのアカウントをお持ちでない方は、今すぐアカウントを作成してください。

   Insight Premiumアカウントの作成またはInsight Proアカウントへのアップグレードについては、kb.netgear.com/000044343をご覧ください。
4. NETGEARアカウントのメールアドレスとパスワードを入力し、**ログインを**タップします。

これで、アクセスポイントのメッシュ WiFi 接続を設定できます（Insight アプリ を使用して、アクセスポイントをノードとしてルートに接続（55 ページ）参照）。

Insightアプリを使用して、アクセスポイントをノードとしてルートに接続する

NETGEAR Insight アプリを使用して、アクセス ポイントをノードとしてルートに接続できます。ルートがノードにインターネット接続を提供できるように、ルーターまたはインターネット ゲートウェイへの有線接続を設定する必要があります。

Insight アプリと Insight アプリで利用できる設定および管理オプションの詳細については、netgear.com/insight をご覧ください。Insight アプリにはヘルプが組み込まれており、netgear.com/support からアクセスできる複数のナレッジベース記事で説明されています。

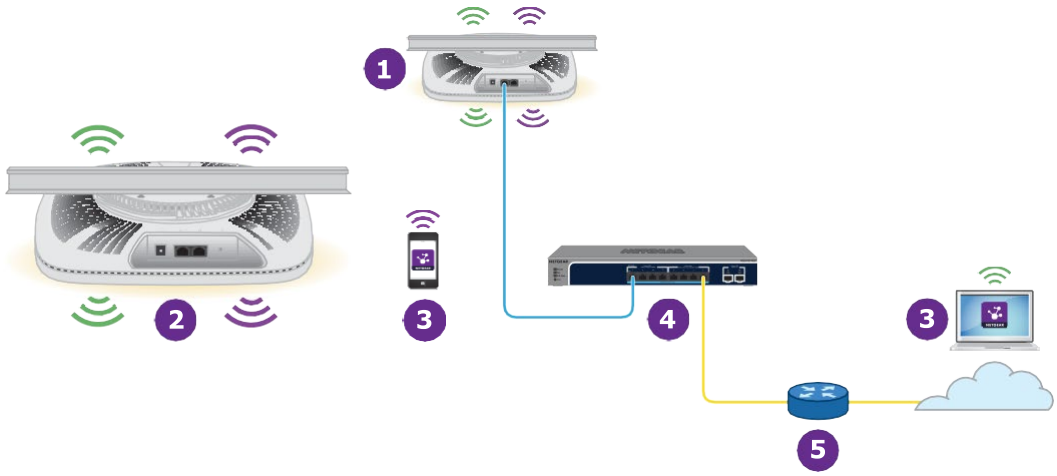


図8.ノードを有線ルートに接続する

番号またはアイコンと説明
1 ネットワーク・スイッチにイーサネットで接続されているルート。
2 5GHzのバックホールWiFi接続でルートに接続されているノード。
3 Insightアプリを搭載した携帯電話、またはInsightクラウドポータルにアクセスできるコンピューターまたはタブレット。Insight Cloud PortalまたはInsightアプリで、Insight Instant Mesh WiFiネットワークのノードを設定・管理できます。
4 ネットワーク・スイッチ。
5 インターネットに接続されているネットワーク・ルーター。

番号またはアイコンと説明
2.4GHz帯の電波。
5GHz帯のHightまたはLowの電波。

ノードは、ルートへのバックホール接続とWiFiクライアントへのフロントホール接続を確立するために、どのバンドを使用することもできます。ただし、バックホール接続が確立された後、ルートとノードの両方が5 GHzバンドをサポートできる場合、ノードはバックホール接続の優先バンドとして5 GHzバンドに自動的に切り替わります。Insight Cloud Portal を使用して、バックホール設定を変更できます。

NETGEAR Insight アプリを使用して、ノードを既存の WiFi ネットワークのルートに接続するには：

1. Insight ネットワークの場所のメッシュモードが Auto に設定されていることを確認します。詳細については、kb.netgear.com/000064932 を参照してください。

   Insight アプリを使って、Insight ネットワークロケーションのメッシュモードを変更することはできません。クラウドポータルを使用する必要があります。この手順の他のすべての手順では、Insight アプリを使用 できます。

2. ルートのメッシュモードがAutoに設定されていることを確認してください。詳細については、kb.netgear.com/000064929をご覧ください。
3. ノードが工場出荷時の状態になっていることを確認する。

   アクセスポイントを以前ネットワークで使用していた場合は、アクセスポイントを工場出荷時の設定にリセットします。
4. 信頼性の高いWiFi接続を行うには、ノードを最も近いルートから7.5m（25フィート）以内で、障害物の少ない見通しの良い場所に設置してください。
5. ノードを電源に接続する。

   ノードの電源/クラウドLEDがオレンジに点灯した後、緑色に点灯します。

   注：ネットワークのループを防ぐには、ノードをルートと同じネットワークやインターネットに接続されていないPoE++スイッチに接続します。オプションの電源アダプタを使用することもできます。

6. 1つ以上のルーツを含む既存のWiFiネットワークにモバイルデバイスを接続します。
7. インサイトアプリを起動し、アカウントにサインインします。

8. インサイトのネットワークの場所をルートで選択する。

   ほとんどの場合、Insight アプリがノードを自動的に検出します。このプロセスには数分かかる場合があります。

9. 以下のいずれかの操作を行って、ノードをインサイトのネットワークロケーションに追加します：

   - **自動的に検出される**：ノードが自動的に検出され、[Insight Manageable Devices]セクションに表示されている場合は、ノードのアイコンをタップし、[**ADD DEVICE]**ボタンをタップします。
   - **自動的に検出されない**：ノードが自動的に検出されない場合は、以下の操作を行ってください：
     a. 上部バーの＋アイコンをタップします。
     b. 以下のいずれかを行う：
        - **SCAN BARCODE OR QR CODE**ボタンをタップし、ノードのコードをスキャンします。
        - **Enter Serial Number and MAC address**リンクをタップし、ノードのシリアル番号とMACアドレスを手動で入力します。
     c. プロンプトが表示されたら、ノードに名前を付けて「**Next**」ボタンをタップします。

   ノードは、Insight Instant Mesh WiFiネットワークで最も強いWiFi信号を提供するルートを検出し、接続を試みます。

   注：初期接続と設定プロセスには最大10分かかる場合があります。設定プロセス中にノードが再起動することがあります。

10. ノードが初期接続と設定プロセスを経て、電源/クラウドLEDがオレンジ、緑色、青色の点滅を止め、青色で点灯するのを待ちます。

    注：初期接続と設定プロセスには最大10分かかる場合があります。設定プロセス中にノードが再起動することがあります。

    電源/クラウドLEDは、最初の接続と設定プロセス中に以下のように点灯します：

    - **緑色に点滅**：ノードはルートを検出しようとしている。
    - **緑色の点灯**：ノードは、最も強いWiFi信号を提供するルートと最初の接続を行っています。
    - **オレンジでゆっくり点滅**：ノードがネットワークルーターまたはDHCPサーバーに連絡してIPアドレスを受信している。

電源 / クラウド LED のオレンジの点滅が止まらない場合は、247 ページの「電源 / クラウド LED がオレンジでゆっくりと点滅し続けている」を参照してください。

- **オレンジ、グリーン、ブルーの点滅**：ノードは、Insight Instant Mesh WiFi ネットワークの管理対象デバイスとして設定されています。
  電源/クラウドLEDがオレンジ、緑色、青色の点滅を停止しない場合は、電源/クラウドLEDがオレンジ、緑色、青色の点滅を停止しない（249ページ） を参照してください。

設定が完了すると、Power/Cloud LEDが以下のように点灯します：

- **青色で点灯**：設定が完了し、ノードを操作できる状態。ノードはInsight Instant Mesh WiFiネットワークで機能し、Insightクラウドに接続されています。

ノードは自動的にルートのWiFiネットワークをブロードキャスト（拡張）するように設定される。

ノードとルートの接続が困難な場合は、「ノードとルートが接続できません（250ページ）」を参照してください。

NETGEAR Insight Cloud Portal および Insight アプリによるノードへのアクセス、管理、監視については、netgear.com/insight をご覧ください。Insight Cloud Portal と Insight アプリにはヘルプが組み込まれており、netgear.com/support にアクセスしてアクセスできる複数のナレッジベース記事に文書化されています。

5

WiFiネットワークの基本的なWiFi機能を管理する

アクセスポイントは 8 つの WiFi ネットワークをサポートすることができ、各ネットワークは WiFi セキュリティを含む独自の WiFi 設定を持ちます。この章では、WiFi ネットワークの基本的な WiFi 機能を管理する方法について説明します。

WiFi ネットワークの高度な WiFi 機能については、WiFi ネットワークの高度な WiFi 機能の管理 (204 ページ) を参照してください。

この章には以下のセクションがある：

- オープンまたはセキュアなWiFiネットワークを設定する
- WiFiネットワークの設定を表示または変更する
- WiFiネットワークを削除する
- WiFiネットワークのSSIDを隠す、またはブロードキャストする
- WiFiネットワークのVLAN IDを変更する
- WiFiネットワークの認証と暗号化を変更する
- WiFiネットワークのPMFを有効または無効にする
- WiFiネットワークにマルチPSKを設定する
- WiFiネットワークの無効化または有効化、WiFiアクティビティスケジュールの設定
- 802.11k RRMおよび802.11v WiFiネットワーク管理によるバンドステアリングの有効化または無効化

注：アクセスポイントのWiFiネットワークの設定を変更する**場合は、**新しいWiFi設定が有効になったときに切断されないように、有線接続を使用してください。

注：このマニュアルでは、***WiFi****ネットワークは*SSID（サービスセット識別子またはWiFiネットワーク名）またはVAP（仮想アクセスポイント）と同じ意味です。つまり、WiFiネットワークとは、個々のSSIDまたはVAPを意味します。

オープンまたはセキュアなWiFiネットワークを設定する

アクセスポイントは、デフォルトで有効になっており、2.4 GHz 帯、5 GHz ハイバンド、および 5 GHz ローバンドでブロードキャストする 1 つのセットアップ SSID を提供します。これは、アクセスポイントに最初に接続したときに名前を変更し、新しいパスフレーズを設定した SSID です。また、この SSID をデフォルト WiFi ネットワークと呼び、ローカルブラウザ UI では SSID1 と表示されます。さらに SSID を追加できます：アクセスポイントは合計 8 つの SSID をサポートできます。このアクセスポイントは、802.11b/g/n/ax WiFiデバイス用の2.4GHz帯と、802.11a/na/ac/ax WiFiデバイス用の5GHz帯のハイバンドとローバンドを同時にサポートすることができます。

SSIDはservice set identifierの略で、WiFiネットワーク名です。新しいSSIDを作成すると、仮想アクセスポイント（VAP）とも呼ばれる新しいWiFiネットワークの設定を定義することになります。つまり、アクセスポイントは最大8つのWiFiネットワークまたはVAPをサポートします。

WPA2 エンタープライズセキュリティまたは WPA3 エンタープライズセキュリティを WiFi ネットワークに使用する場合は、まず RADIUS サーバーを設定します (「RADIUS サーバーの設定 (131 ページ)」を参照)。WPA2 Enterprise セキュリティと WPA3 Enterprise セキュリティは、マルチキャスト DNS (mDNS) ゲートウェイには対応していないことに注意してください (「マルチキャスト DNS ゲートウェイの管理 (150 ページ)」を参照)。

WiFiネットワークをセットアップする：

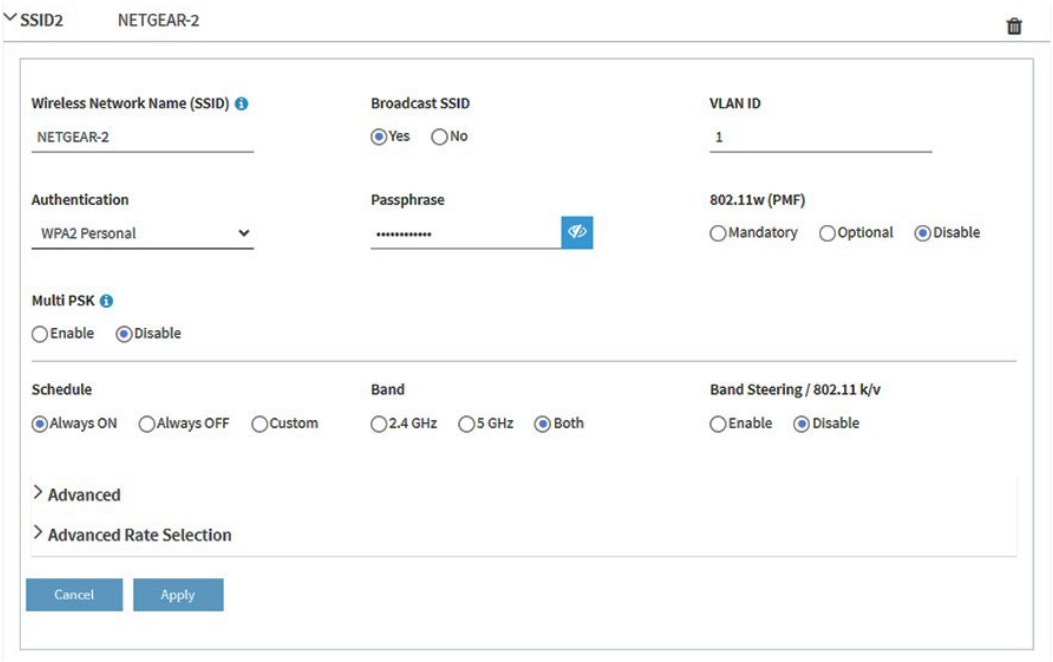
1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。ログインウィンドウが表示されます。ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Wireless > Basic** を選択します。

   表示されるページで、SSID を選択して追加できます。

5. Add SSIDの左にある**+**ボタンをクリックします。



先ほどの図はSSID2を例として示しています。

6. WiFiネットワーク名（SSID）を指定し、SSIDをブロードキャストするかどうかを選択し、次の表に示すようにVLAN IDを指定します。

設定	説明
Wireless Network Name (SSID)	SSID は VAP の WiFi ネットワーク名です。SSID の名前を最大 32 文字で入力します。引用符(")とバックスラッシュ(\)を除き、英数字と特殊文字を組み合わせて使用できます。 WiFiデバイスがVAPに接続するには、WiFiデバイスのSSIDがVAPのSSIDと一致する必要があります。
Broadcast SSID	デフォルトでは、WiFiクライアントがスキャンしたネットワークリストでSSIDを検出できるように、VAPはSSIDをブロードキャストします。SSID ブロードキャストをオフにするには、**[No]** ラジオボタンを選択します。 SSIDブロードキャストをオフにすると、WiFiセキュリティがさらに強化されますが、ユーザーはVAPに参加するためにSSIDを知る必要があります。
VLAN ID	VAP に関連付けなければならない VLAN ID を入力できます。デフォルトでは、VLAN ID は 1 です。 この VLAN ID は、有線ネットワークで使用される 802.1Q VLAN ID とは異なります（802.1Q VLAN と管理 VLAN の設定（139 ページ）参照）。

7. **Authentication**」メニューからオプションを選択し、該当する場合は「**Passphrase**」フィールドにパスフレーズを指定するか、「**Encryption**」メニューからオプションを選択して、WiFiセキュリティを指定します：

- **Open**：レガシーオープンWiFiネットワークは、セキュリティを提供しません。どんなWiFiデバイスでもネットワークに参加することができます。レガシーオープンWiFiネットワークは使用せず、WiFiセキュリティを設定することをお勧めします。ただし、レガシーオープンネットワークは、WiFiホットスポットに適している場合があります。

  Authentication」メニューから「**Open**」を選択すると、「**Enhanced Open**」チェックボックスが表示されます。

  - **Enhanced Openチェックボックスがオフ**：WiFiネットワークは、セキュリティのないレガシーなオープンネットワークです。これはオープンネットワークのデフォルトオプションです。クライアントは認証されず、トラフィックは暗号化されず、802.11w（PMF）は自動的に無効になります（ステップ8を参照）。
  - **Enhanced Openのチェックボックスが選択されている**：WiFi enhanced open 機能が有効になります。この機能は、OWEに基づいています。暗号化はCCMPに設定され、802.11w（PMF）は自動的に必須に設定されます（ステップ8参照）。**Enhanced Open**］チェックボックスを選択すると、

    ［**Allow Devices to Connect with Open**］チェックボックスが表示されます。**チェックボックスを**選択すると、WiFiネットワークは、WiFi拡張オープン機能をサポートするクライアントとそうでないクライアントの両方を受け入れることができます。WiFi open enhanced 機能をサポートしていないクライアントの場合、トラフィックは暗号化されません。

    チェックボックスをオフにすると、WiFiネットワークはWiFi拡張オープン機能をサポートするクライアントのみを受け入れることができます。

- **WPA2 Personal**：このオプションはWPA2-PSKと同じで、デフォルト設定であり、AES暗号化を使用します。このタイプのセキュリティでは、WPA2をサポートするWiFiデバイスのみがVAPに参加できます。

  WPA2は安全な接続を提供しますが、一部のレガシーWiFiデバイスはWPA2を検出せず、WPA のみをサポートしています。ネットワークにそのような古いデバイスが含まれている場合は、**WPA2/WPA Personal** 認証を選択します。

  Passphraseフィールドに、8～63文字のフレーズを入力します。VAPに参加するには、ユーザーはこのパスフレーズを入力する必要があります。パスフレーズをクリアテキストで表示するには、目のアイコンをクリックします。

- **WPA2/WPA Personal**：このオプションは、WPA2-PSK/WPA-PSKと同じで、WPA2またはWPAをサポートするWiFiデバイスがVAPに参加することを可能にします。このオプションは、AES および TKIP 暗号化を使用します。

WPA-PSK（TKIPを使用）はWPA2-PSK（AESを使用）より安全性が低く、WiFi機器の速度を54Mbpsに制限しています。

Passphraseフィールドに、8～63文字のフレーズを入力します。VAPに参加するには、ユーザーはこのパスフレーズを入力する必要があります。パスフレーズをクリアテキストで表示するには、目のアイコンをクリックします。

- **WPA2 Enterprise**：このエンタープライズレベルのセキュリティは、RADIUSを使用して認証、認可、および会計（AAA）管理を集中的に行います。WPA2 Enterprise セキュリティを機能させるには、RADIUS サーバーを設定する必要があります（「RADIUS サーバの設定 (131 ページ)」を参照）。

  暗号化メニューから、データ暗号化モードを選択します：

  - **TKIP+AES**。このタイプのデータ暗号化は、WPAまたはWPA2をサポートするWiFiデバイスがアクセスポイントのWiFiネットワークに参加できるようにします。これがデフォルトのモードです。
  - **AES**。このタイプのデータ暗号化は安全な接続を提供しますが、一部の古いWiFiデバイスはWPA2を検出せず、WPAのみをサポートします。そのため、ネットワークにそのような古いデバイスが含まれている場合は、**TKIP + AES** 暗号化を選択してください。

  WPA2 Enterprise 認証を選択すると、**Dynamic VLAN** ラジオボタンが表示されます：

  - **Enable**：RADIUSサーバーはクライアントにに VLAN IDを割り当てることができます。RADIUSサーバーが割り当てない場合、クライアントにはSSIDに設定したVLAN IDが自動的に割り当てられます。
  - **Disable**：クライアントには、SSID に設定した VLAN ID が割り当てられます。これはデフォルト設定です。

- **WPA3 Personal**：このオプションは、最も安全な個人認証オプションです。WPA3はSAE暗号を使用し、WPA3をサポートするWiFiデバイスのみがVAPに参加できるようにします。このオプションを選択すると、802.11w（PMF）は自動的に必須に設定されます（ステップ8を参照）。

  WPA3は安全な接続を提供しますが、一部のレガシーWiFiデバイスはWPA3を検出せず、WPA2のみをサポートしています。ネットワークにWPA2機器も含まれている場合は、「**WPA3/WPA2 Personal** 認証」を選択します。

  Passphraseフィールドに、8～63文字のフレーズを入力します。VAPに参加するには、ユーザーはこのパスフレーズを入力する必要があります。パスフレーズをクリアテキストで表示するには、目のアイコンをクリックしますす。

- **WPA3/WPA2 Personal**：このオプションは、WPA3/WPA2-PSKと同じで、WPA3またはWPA2をサポートするWiFiデバイスがVAPに参加できるようにします。このオプションは、SAEとAESの暗号化を使用します。

  WPA2-PSK（AESを使用）は、WPA3（SAEを使用）よりも安全性が低い。

  Passphraseフィールドに、8～63文字のフレーズを入力します。VAP に参加する

には、ユーザーはこのパスフレーズを入力する必要があります。パスフレーズをクリアテキストで表示するには、目のアイコンをクリックします。

- **WPA3 Enterprise**：このエンタープライズレベルのセキュリティは、RADIUS を使用して認証、認可、およびアカウンティング（AAA）を集中管理します。WPA3 Enterprise セキュリティを機能させるには、RADIUS サーバをセットアップする必要があります（「RADIUS のセットアップ」を参照）。サーバー（131 ページ）。このオプションを選択すると、802.11w（PMF）は自動的に必須に設定されます（ステップ8参照）。

  WPA3 Enterprise セキュリティを選択すると、暗号化は自動的に 256 ビット暗号化プロトコルの GCMP256 に設定されます。

  WPA3 Enterprise 認証を選択すると、**Dynamic VLAN** ラジオボタンが表示されます：

  - **Enable**：RADIUSサーバーはクライアントにVLAN IDを割り当てることができます。RADIUSサーバーが割り当てない場合、クライアントにはSSIDに設定したVLAN IDが自動的に割り当てられます。
  - **Disable**：クライアントには、SSID に設定した VLAN ID が割り当てられます。これはデフォルト設定です。

8. オプションで、802.11w Protected Management Frames (PMF) を有効にします。

   保護された管理フレーム（PMF）は、802.11w 標準に従って、ユニキャストおよびマルチキャスト管理フレームが傍受され、悪意ある目的のために変更されるのを防ぐセキュリティ機能です。選択する認証のタイプによって、この機能が必須、オプション、または無効になるかが決まります。手動で設定することもできます。

   - **Mandatory（必須）**：このオプションは、デバイスがPMFを使用することを要求します。PMF をサポートしていないデバイスは、WiFi ネットワークに接続できません。Enhanced Open認証、WPA3個人認証、WPA3企業認証を選択した場合、PMFのラジオボタンは「**必須**」に設定されており、変更することはできません。
   - **Optional（オプション）**：このオプションは、デバイスが PMF をサポートできるかどうかに基づいて、アクセスポイントが自動的に PMF を有効にするようにします。WPA3/WPA2 Personal authentication を選択した場合、PMF のラジオボタンは **Optional** に設定されていますが、変更することができます。
   - **Disable:**このオプションは、PMFを無効にします。Open認証、WPA2 Personal認証、WPA2/WPA Personal認証、WPA2 Enterprise認証を選択した場合、PMFのラジオボタンは「**無効**」に設定されていますが、変更することができます（Open認証を除く）。

9. オプションで、マルチプリシェアードキー（PSK）を有効にすると、WiFiネットワークを異なるVLANに分離し、それぞれ固有のパスフレーズでアクセスできるようになります。マルチPSKは、WiFiセキュリティがWPA2 PersonalまたはWPA2/WPA Personalの場合のみサポートされます。ある意味、マルチPSKを使えば、設定中のWiFiネットワーク上に異なるサブWiFiネットワークを作ることができる。WiFi ネットワークのセットアップ中にこの機能を設定することもできますが、この機能はより複雑であるため、

10. 別途説明します。詳細については、WiFi ネットワークのマルチ PSK のセットアップ (79 ページ) を参照してください。
11. オプションとして、以下のラジオボタンのいずれかを選択して、WiFiブロードキャストを無効にするか、またはWiFiアクティビティスケジュールを設定します：
    - **Always ON**：SSID を設定すると、新しい VAP が作成されます。デフォルトでは、新しい VAP は有効になっており、「**Always ON**」ラジオボタンが選択されています。
    - **Always OFF**：このラジオボタンを選択すると、SSIDは設定されますが、VAPは一時的に無効になります。
    - **Custom**：スケジュールを設定するには、このラジオボタンを選択します。ラジオボタンの右側にアイコンが表示されます。以下を実行します：
        a. ラジオボタンの横にあるアイコンをクリックします。
        ポップアップ・ウィンドウが表示されます。
        b. プリセットメニューから定義済みの時間を選択するか、タイムブロックをクリックしてカスタムタイムブロックを選択します。
        タイムブロックの青色は、VAPが有効（オン）であることを示す。タイムブロックの色がグレーである場合は、VAPが無効（オフ）であることを示す。
        c. **Done**ボタンをクリックする。ポップアップウィンドウが閉じる。

    各SSIDについて、カスタムスケジュールを1つ作成できます。このスケジュールでは、午前12時から午後11時59分までの各日について、VAPを無効にする時間帯を指定します。
12. オプションで、単一の無線バンドのみを選択します。

    ラジオボタンは、単一のバンド（**2.4 GHz** または **5 GHz**）を選択するか、デフォルトのままにしておきます。デフォルトでは、［**Both**］ラジオボタンが選択されており、アクセスポイントは、2.4 GHz バンドと 5 GHz バンド（ハイバンドとローバンド）の両方で SSID をブロードキャストします。
13. オプションとして、802.11k無線リソース管理（RRM）と802.11v WiFiネットワーク管理でバンドステアリングを有効にします。

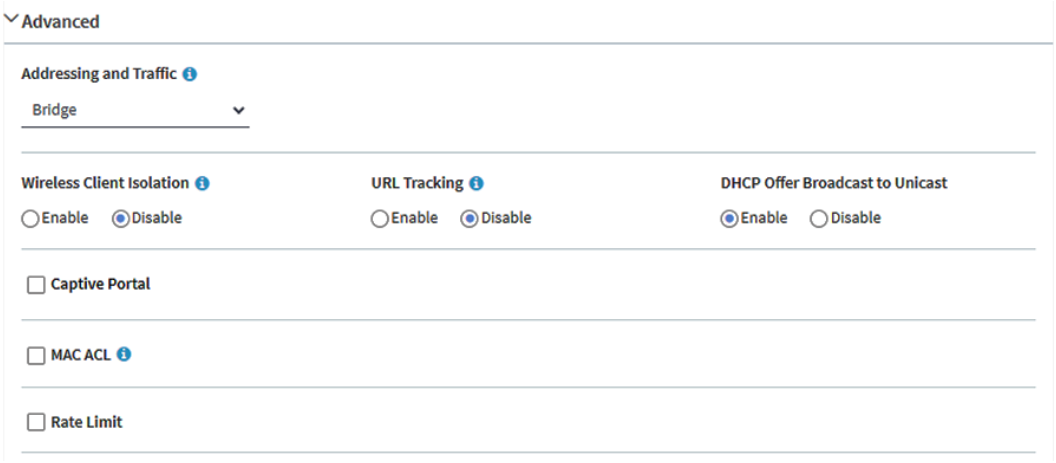
    デフォルトでは、802.11k RRM および 802.11v WiFi ネットワーク管理によるバンドステアリングは、VAP では無効になっています。

    802.11k RRMおよび802.11v WiFiネットワーク管理でバンドステアリングを有効にするには、[**Enable]**ラジオボタンを選択します。これにより、アクセスポイントは、特定のチャンネル条件下で、デュアルバンド対応のWiFiデバイスをVAPの2.4GHzバンドまたは5GHzバンドにステアすることができます。2.4GHz帯に比べ、5GHz帯では一般的に多くのチャンネルと帯域幅が利用できるため、干渉が少なく、より快適なユーザーエクスペリエンスが得られます。

    802.11k RRM および 802.11v WiFi ネットワーク管理は、以下の方法でネットワークに影響を与えます：

- **802.11k RRM**： この機能により、アクセスポイントと 802.11k 対応クライアントは、利用可能な無線リ ソースを動的に測定することができます。802.11k対応ネットワークでは、アクセスポイントとクライアントは互いにネイバーレポート、ビーコンレポート、リンク測定レポートを送信することができ、802.11k対応クライアントは初期接続やローミングに最適なアクセスポイントを自動的に選択することができます。
- **802.11v WiFiネットワーク管理**：この機能により、アクセスポイントは、アクセスポイントのチャネル負荷に基づいて、WiFiクライアントを2.4GHz帯または5GHz帯に誘導することができます。

アクセスポイントは受信信号強度インジケータ（RSSI）のしきい値を自動的に設定します。(つまり、RSSI しきい値を手動で設定することはできません）。



14. アドレスとトラフィックモードの設定、クライアント分離の設定、URLトラッキングの設定、DHCP Offerメッセージがユニキャストかブロードキャストかの設定、またはこれらすべてを行うには、下にスクロールして「**> Advanced**」タブをクリックします。
15. オプションで、アドレスとトラフィックのNATモードまたはブリッジモードを設定する。

    デフォルトでは、アクセスポイントのアドレス設定とトラフィックモードはブリッジモードで、WiFiクライアントはネットワーク内のDHCPサーバー（またはDHCPサーバーとして機能するルーター）からIPアドレスを受け取ります。これは通常、アクセスポイント自体にIPアドレスを割り当てるのと同じDHCPサーバーです。

    アクセスポイントの DHCP サーバーを WiFi クライアントに有効にする NAT モードも設定できます。アクセスポイントの DHCP サーバーは、異なる範囲のIPアドレスを割り当てます。

    アクセスポイント自体のIPアドレスから。NATモードとマルチPSK（ステップ9参照）は相互に互換性がありません。

    Addressing and Trafficメニューから、アドレッシングとトラフィックのモードを選択します：

- **Bridge**：WiFiクライアントは、アクセスポイントと同じネットワーク内のDHCPサーバーからIPアドレスを受け取ります。これはデフォルトのモードです。
- **NAT**：WiFi クライアントは、アクセスポイントのプライベート DHCP アドレスプールから IP アドレスを受け取ります。このモードを選択すると、デフォルトで WLAN ネットワークアドレスは 172.31.0.0 になります。これは、WiFi クライアントに 172.31.0.2 ～ 172.31.3.254 の範囲の IP アドレスが割り当てられることを意味します。WLANのデフォルトDNSサーバーのIPアドレスは8.8.8.8です。DHCPアドレスプール、デフォルトDNSサーバー、またはその両方のデフォルト範囲を変更するには、次の手順に従います。

  a. **Network Address**］フィールドに、アクセス ポイントのネットワーク アドレスとは異なるネットワーク アドレスを入力します。たとえば、アクセスポイントの IP アドレスが 192.168.0.1 ～ 192.168.0.254 の範囲 （一般的な IP アドレスの範囲） の場合、192.168.0.0 とは異なるネットワーク アドレスを入力します。

  b. **DNS**フィールドに、使用するDNSサーバーのIPアドレスを入力します。このIPアドレスは、前の手順で設定したWLANネットワークアドレスとは異なる必要があります。

16. オプションで、WiFiクライアントの分離を設定します。

    デフォルトではクライアント分離はVAPに対して無効になっており、「**Disable**」ラジオボタンが選択されています。クライアント分離とマルチPSK（ステップ9参照）は相互に互換性がありません。

    アクセスポイントの同じ SSID または異なる SSID に関連付けられた WiFi クライアント間の通信をブロックするには、**[Enable]** ラジオボタンを選択します。

    Enableラジオボタンを選択すると、以下のチェックボックスが表示されます：

    - **Allow Access to AP UI（APのUIへのアクセスを許可する）**：管理VLANとWiFiネットワークVLANが同一で（デフォルトではどちらもVLAN1）、クライアント分離を有効にすると、「**Allow Access to AP UI**」チェックボックスが表示されます。デフォルトでは、このチェックボックスが選択されており、管理ユーザーがWiFiネットワーク経由でローカルブラウザUIにアクセスできるようになっています。**Allow Access to AP UI**］**チェックボックスを**オフにすると、管理者ユーザーはWiFiネットワーク経由でローカルブラウザーUIにアクセスできなくなります。管理VLANとWiFiネットワークVLANが同一であれば（デフォルトでは同一）、管理ユーザーは常に有線ネットワーク接続でローカルブラウザUIにアクセスすることができます。
    - **Allow access to devices listed below**：静的 IP アドレスまたはドメイン (静的 IP アドレスに解決する) を指定し、クライアントのアクセスを許可することができます。詳細については、WiFi ネットワークのクライアント分離の有効化または無効化 (206 ページ) を参照してください。

17. オプションでURLトラッキングを有効にする。

デフォルトでは、URL トラッキングは無効になっており、[**Disable]** ラジオボタンが選択されています。SSID に接続している WiFi クライアントから要求されるすべての URL に対して URL トラッキングを有効にするには、[**Enable]** ラジオボタンを選択します。

SSID または WiFi クライアントごとに追跡された URL を表示する方法については、追跡された URL の表示またはダウンロード（197 ページ）を参照してください。

18. オプションで、DHCPオファー・メッセージの設定を変更します。

    デバイスがWiFiネットワークにアソシエーションしようとしてIPアドレスをネゴシエートするとき、アクセスポイントはDHCPサーバーから受信したブロードキャストDHCPオファーメッセージをユニキャストメッセージに変換し、デバイスに転送します。これはデフォルトのオプションです（すなわち、**[Enable]**ラジオボタンが選択されている）。このオプションを無効にして、アクセスポイントがブロードキャストDHCPオファーメッセージをユニキャストメッセージに変換*しないようにするには*、***[Disable]***ラジオボタンを選択します。

19. キャプティブポータル、MAC ACL、および帯域幅レート制限を設定するには、以下のセクションの情報を参照してください：

    - 99ページのキャプティブポータルの設定と管理

      キャプティブ・ポータルとマルチPSK（ステップ9参照）は相互に互換性がない。
    - ローカルの MAC アクセス制御リストの管理（118 ページ）および WiFi ネットワークの MAC ACL の選択（211 ページ
    - 213ページのWiFiネットワークの帯域幅レート制限の設定

    WiFiネットワークのセットアップ中にこれらの機能を設定することもできますが、これらの機能はより複雑であるため、別途説明します。

20. 高度なレート選択を設定するには、WiFi ネットワークの高度なレート選択を設定する（214 ページ） を参照してください。

21. **Apply** ボタンをクリックします。

    設定が保存されます。

22. 新しいWiFiネットワークに接続できることを確認します。

    新しいWiFiネットワークに接続できない場合は、以下を確認してください：

    - WiFi対応のコンピューターやモバイル機器が、すでにお住まいの地域の別のWiFiネットワークに接続されている場合は、そのWiFiネットワークから切断し、正しいWiFiネットワークに接続してください。一部のWiFiデバイスは、WiFiセキュリティのない最初のオープンネットワークに自動的に接続します。
    - WiFi対応コンピューターまたはモバイル機器が古い設定（設定を変更する前）のままネットワークに接続しようとしている場合は、WiFi対応コンピューターまたはモバイル機器のWiFiネットワーク選択を更新して、ネットワークの現在の設定と一致させてください。

- WiFi デバイスは接続クライアントとして表示されますか？(クライアント分布、接続クライアント、クライアントの傾向の表示 (191 ページ)を参照)。表示されていれば、ネットワークに接続されています。
- 正しいWiFiネットワーク名（SSID）とパスワードを使用していますか？

  WiFi認証と暗号化がWPA3 Personalに設定されている場合は、コンピューターたはモバイル機器のWiFiのデバイスドライバーが最新バージョンにアップデートされていることを確認してください。

WiFiネットワークの設定を表示または変更する

デフォルトの WiFi ネットワーク（SSID または VAP）またはカスタム WiFi ネットワークの設定を表示または変更できます。デフォルトの WiFi ネットワークは、アクセスポイントに最初に接続したときに名前を変更し、新しいパスフレーズを設定した SSID です。この SSID は、ローカルブラウザ UI では SSID1 として表示されます。

WiFiネットワークの設定を表示または変更する：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Wireless > Basic**を選択します。

   表示されたページでSSIDを選択できます。
5. SSIDの左にある>ボタンをクリックします。

選択したSSIDの設定が表示されます。

6. 必要に応じてWiFiネットワークの設定を変更してください。

   設定の詳細については、オープンまたはセキュアなWiFiネットワークのセットアップ（60ページ）を参照してください。

7. 変更した場合は、**[Apply]** ボタンをクリックします。
   設定が保存されます。

8. 変更した場合は、新しい設定のネットワークにWiFiで再接続できることを確認してください。

   WiFiで接続できない場合は、以下を確認してください：

   - WiFi対応のコンピューターやモバイル機器が、すでにお住まいの地域の別のWiFiネットワークに接続されている場合は、そのWiFiネットワークから切断し、正しいWiFiネットワークに接続してください。一部のWiFiデバイスは、WiFiセキュリティのない最初のオープンネットワークに自動的に接続します。
   - WiFi対応コンピューターやモバイル機器が古い設定（設定を変更する前）のままネットワークに接続しようとしている場合は、WiFi対応コンピューターやモバイル機器のWiFiネットワーク選択を更新し、現在のネットワーク設定に合わせます。
   - WiFi デバイスは接続クライアントとして表示されますか？(クライアント分布、接続クライアント、およびクライアントの傾向の表示 (191 ページ)を参照してください)。表示されている場合は、 ネットワークに接続されています。
   - 正しいWiFiネットワーク名（SSID）とパスワードを使用していますか？

WiFiネットワークを削除する

不要になったカスタムWiFiネットワーク（SSIDまたはVAP）を削除できます。デフォルトの WiFi ネットワークは削除できません。デフォルトの WiFi ネットワークは、アクセスポイントに最初に接続したときに名前を変更し、新しいパスフレーズを設定した SSID です。この SSID は、ローカルブラウザ UI では SSID1 として表示されます。

WiFiネットワークを削除するには

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。
   ログインウィンドウが表示されます。

ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。

3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。

4. **Management > Configuration > Wireless > Basic**を選択します。

   表示されたページでSSIDを選択できます。

5. SSIDの右にあるゴミ箱アイコンをクリックします。

   警告ポップアップウィンドウが表示されます。

6. **Delete]**ボタンをクリックする。

   ポップウィンドウが閉じ、WiFiネットワークが削除されます。

WiFiネットワークのSSIDを隠す、またはブロードキャストする

デフォルトでは、WiFiネットワーク（SSIDまたはVAP）は、WiFiクライアントがスキャンされたネットワークリストでSSIDを検出できるように、そのネットワーク名（SSIDとも呼ばれる）をブロードキャストします。セキュリティを強化するために、SSIDブロードキャストをオフにしてSSIDを隠し、ユーザーがWiFiネットワークに参加できるようにSSIDを知る必要があります。

注：ワイヤレスディストリビューションシステム（WDS; 219 ページの「WiFi ブリッジのセットアップ」を参照）をセットアップする**場合、** SSID ブロードを有効にしておく必要があります。

WiFiネットワークのネットワーク名を非表示またはブロードキャストする：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。

3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。

4. **Management > Configuration > Wireless > Basic]** を選択します。
   表示されたページでSSIDを選択できます。
5. SSID の左側にある **>** ボタンをクリックします。
   選択したSSIDの設定が表示されます。
6. ブロードキャストSSID］で、次のラジオボタンのいずれかを選択します：
   - **No**：WiFiネットワークのSSIDは非表示です。
   - **Yes**：SSIDはWiFiネットワーク用にブロードキャストされます。
7. **Apply** ボタンをクリックします。
   設定が保存されます。

WiFiネットワークのVLAN IDを変更する

WiFi ネットワークの VLAN ID は、有線ネットワークに使用される 802.1Q VLAN ID とは異なります（802.1Q VLAN と管理 VLAN の設定 (139 ページ)を参照）。

注意：VLAN ID を変更する前に、ネットワークスイッチと DHCP サーバーで VLAN が設定され、アクセスポイントとそのクライアントが新しい VLAN で IP アドレスを取得できることを確認してください。

WiFiネットワークのVLAN IDを変更するには：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。
   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Wireless > Basic]** を選択します。
   表示されたページでSSIDを選択できます。
5. SSID の左側にある **>** ボタンをクリックします。
   選択したSSIDの設定が表示されます。
6. **VLAN ID**フィールドにID（つまり数字）を入力します。
   デフォルトでは、WiFiネットワークのVLAN IDは1です。
7. **Apply** ボタンをクリックします。
   設定が保存されます。

WiFiネットワークの認証と暗号化を変更する

デフォルトの WiFi ネットワーク（SSID または VAP）または任意のカスタム WiFi ネットワークの認証と暗号化を変更できます。デフォルトの WiFi ネットワークは、アクセスポイントに最初に接続したときに名前を変更し、新しいパスフレーズを設定した SSID です。この SSID は、ローカルブラウザ UI では SSID1 として表示されます。

認証と暗号化を変更する前に、WiFiネットワークに接続できなければならないクライアントの種類を検討してください。WPA3 は WPA2 よりも安全な接続を提供しますが、多くの WiFi デバイスはまだ WPA3 を検出せず、WPA2 のみをサポートしている場合があります。同様に、WPA2 は WPA よりも安全な接続を提供しますが、一部のレガシー WiFi デバイスは WPA2 を検出せず、WPA のみをサポートしています。

WPA2 エンタープライズセキュリティまたは WPA3 エンタープライズセキュリティを WiFi ネットワークに使用する場合は、まず RADIUS サーバーを設定します（RADIUS サーバーの設定 (131 ページ)を参照）。

WiFiネットワークの認証と暗号化を変更するには：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。ログインウィンドウが表示されます。ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Wireless > Basic]** を選択します。

   表示されるページで、SSID を選択して追加できます。
5. Add SSIDの左にある**+ボタンを**クリックします。

   選択したSSIDの設定が表示されます。
6. **Authentication**メニューから、WiFiネットワークの認証タイプを1つ選択し、該当する場合は、**Passphrase**フィールドに新しいパスフレーズ（ネットワークキーまたはWiFiパスワード）を設定するか、**Encryption**メニューからオプションを選択します：

   - **Open**：レガシーオープンWiFiネットワークは、セキュリティを提供しません。どんなWiFiデバイスでもネットワークに参加することができます。レガシーオープンWiFiネットワークは使用せず、WiFiセキュリティを設定することをお勧めします。ただし、レガシーオープンネットワークは、WiFiホットスポットに適している場合があります。

Authentication」メニューから「**Open**」を選択すると、「**Enhanced Open**」チェックボックスが表示されます：

- **Enhanced Openチェックボックスがオフ**：WiFiネットワークは、セキュリティのないレガシーなオープンネットワークです。これはオープンネットワークのデフォルトオプションです。クライアントは認証されず、トラフィックは暗号化されず、802.11w(PMF)は自動的に無効になります（WiFiネットワークのPMFの有効化または無効化(77ページ)を参照）。
- **Enhanced Openチェックボックスがオン**：WiFi Enhanced Open機能が有効になります。この機能は(OWE)に基づいています。暗号化はCCMモードプロトコル（CCMP）に設定され、802.11w（PMF）は自動的に必須に設定されます（WiFiネットワークのPMFの有効化または無効化（77ページ）参照）。**Enhanced Open**］チェックボックスを選択すると、［**Allow Devices to Connect with Open**］チェックボックスが表示されます。**Allow Devices to Connect with Open]**チェックボックスを選択すると、WiFiネットワークは、WiFi拡張オープン機能をサポートするクライアントとサポートしないクライアントの両方を受け入れることができます。WiFiオープン拡張機能をサポートしていないクライアントの場合、トラフィックは暗号化されません。**Allow Devices to Connect with Open**］チェックボックスをオフにすると、WiFiネットワークはWiFi拡張オープン機能をサポートするクライアントのみを受け入れることができます。

- **WPA2Personal**：このオプションはWPA2-PSKと同じで、デフォルト設定であり、AES暗号化を使用します。このタイプのセキュリティでは、WPA2をサポートするWiFiデバイスのみがVAPに参加できます。WPA2はWPAよりも安全な接続を提供しますが、一部のレガシーWiFiデバイスはWPA2を検出せず、WPAのみをサポートしています。ネットワークにそのような古いデバイスが含まれている場合は、**WPA2/WPAPersonal**認証を選択します。

  Passphraseフィールドに、8～63文字のフレーズを入力します。VAPに参加するには、ユーザーはこのパスフレーズを入力する必要があります。パスフレーズをクリアテキストで表示するには、目のアイコンをクリックします。

- **WPA2/WPAPersonal**：このオプションは、WPA2-PSK/WPA-PSKと同じで、WPA2またはWPAをサポートするWiFiデバイスがVAPに参加することを可能にします。このオプションは、AESおよびTKIP暗号化を使用します。

  WPA-PSK（TKIPを使用）はWPA2-PSK（AESを使用）より安全性が低く、WiFi機器の速度を54Mbpsに制限しています。

  Passphraseフィールドに、8～63文字のフレーズを入力します。VAPに参加するには、ユーザーはこのパスフレーズを入力する必要があります。パスフレーズをクリアテキストで表示するには、目のアイコンをクリックします。

- **WPA2エンタープライズ**：このエンタープルレベルのセキュリティは、RADIUSを使用して認証、認可、およびアカウンティング(AAA)を集中管理します。WPA2Enterpriseセキュリティを機能させるには、RADIUSサーバを設定する必要があります（「RADIUSサーバの設定(131ページ)」を参照）。

暗号化メニューから、データ暗号化モードを選択します：

- **TKIP + AES**：このタイプのデータ暗号化は、WPA または WPA2 をサポートする WiFi デバイスがアクセスポイントの WiFi ネットワークに参加できるようにします。これはデフォルトのモードです。
- **AES**：このタイプのデータ暗号化は安全な接続を提供しますが、一部の古いWiFiデバイスはWPA2を検出せず、WPAのみをサポートします。そのため、ネットワークにそのような古いデバイスが含まれている場合は、**TKIP + AES** 暗号化を選択してください。

WPA2 Enterprise認証を選択すると、**Dynamic VLAN**ラジオボタンが表示されます：

- **Enable**：RADIUSサーバーはクライアントにVLAN IDを割り当てることができます。RADIUSサーバーが割り当てない場合、クライアントにはSSIDに設定したVLAN IDが自動的に割り当てられます。
- **Disable**：クライアントには、SSID に設定した VLAN ID が割り当てられます。これはデフォルト設定です。

- **WPA3 Personal**：このオプションは最も安全な個人認証オプションです。WPA3 は SAE 暗号化を使用し、WPA3 をサポートする WiFi デバイスのみが VAP に参加できるようにします。このオプションを選択すると、802.11w（PMF）は自動的に必須に設定されます（WiFi ネットワークの PMF の有効化または無効化（77 ページ）を参照）。WPA3はWPA2よりも安全な接続を提供しますが、多くのWiFiデバイスはまだWPA3を検出せず、WPA2のみをサポートしている可能性があります。ネットワークに WPA2 デバイスも含まれている場合は、**WPA3/WPA2 Personal**認証を選択します。**Passphrase**フィールドに、8～63文字のフレーズを入力します。VAP に参加するには、ユーザーはこのパスフレーズを入力する必要があります。パスフレーズをクリアテキストで表示するには、目のアイコンをクリックします。
- **WPA3/WPA2 Personal**：このオプションは WPA3/WPA2-PSK と同じで、WPA3 または WPA2 をサポートする WiFi デバイスが VAP に参加できるようにします。このオプションは SAE および AES 暗号化を使用します。

  WPA2-PSK（AESを使用）はWPA3（SAEを使用）よりも安全性が低い。

  Passphraseフィールドに、8～63文字のフレーズを入力します。VAP に参加するには、ユーザーはこのパスフレーズを入力する必要があります。パスフレーズをクリアテキストで表示するには、目のアイコンをクリックします。
- **WPA3 エンタープライズ**：このエンタープルレベルのセキュリティは、RADIUS を使用して認証、認可、およびアカウンティング（AAA）を集中管理します。WPA3Enterpriseセキュリティを機能させるには、RADIUSサーバーを設定する必要があります（「RADIUSサーバーの設定(131ページ)」を参照）。このオプションを選択すると、802.11w(PMF)は自動的に必須に設定されます（WiFiネットワークのPMFの有効化または無効化（77ページ）参照）。WPA3Enterpriseセキュリティを選択すると、暗号化は自動的に256ビット暗号化プロトコルのGCMP256に設定されます。

WPA3 Enterprise 認証を選択すると、**Dynamic VLAN** ラジオボタンが表示されます：

- **Enable**：RADIUSサーバーはクライアントにVLAN IDを割り当てることができます。RADIUSサーバーが割り当てない場合、クライアントにはSSIDに設定したVLAN IDが自動的に割り当てられます。
- **Disable**：クライアントには、SSID に設定した VLAN ID が割り当てられます。これはデフォルト設定です。

7. **Apply** ボタンをクリックします。設定が保存されます。
8. 新しいWiFiネットワークに接続できることを確認します。
   新しいWiFiネットワークに接続できない場合は、以下を確認してください：
   - WiFi対応のコンピューターやモバイル機器が、すでにお住まいの地域の別のWiFiネットワークに接続されている場合は、そのWiFiネットワークから切断し、正しいWiFiネットワークに接続してください。一部のWiFiデバイスは、WiFiセキュリティのない最初のオープンネットワークに自動的に接続します。
   - WiFi対応コンピューターやモバイル機器が古い設定（設定を変更する前）のままネットワークに接続しようとしている場合は、WiFi対応コンピューターやモバイル機器のWiFiネットワーク選択を更新し、現在のネットワーク設定に合わせます。
   - WiFi デバイスは接続クライアントとして表示されますか？(クライアント分布、接続クライアント、クライアントの傾向の表示 (191 ページ)を参照)。表示されていれば、ネットワークに接続されています。
   - 正しいWiFiネットワーク名（SSID）とパスワードを使用していますか？
   - WiFi認証と暗号化をWPA3 Personalに変更した場合は、WiFiアダプタのデバイスドライバがWiFi対応コンピュータまたはモバイルデバイス上で最新バージョンに更新されていることを確認してください。

WiFiネットワークのPMFを有効または無効にする

保護された管理フレーム（PMF）は、802.11w 標準に従って、ユニキャストおよびマルチキャスト管理フレームが傍受され、悪意ある目的のために変更されるのを防ぐセキュリティ機能です。選択する認証のタイプによって、この機能が必須、オプション、または無効になるかが決まります。手動で設定することもできます。

WiFiネットワークのPMFを有効または無効にする：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。
   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。
   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Wireless > Basic]** を選択します。
   表示されるページでSSIDを選択できます。
5. SSID の左側にある **>** ボタンをクリックします。
   選択したSSIDの設定が表示されます。
6. 802.11w（PMF）で、以下のラジオボタンのいずれかを選択します：
   - **Mandatory**：デバイスが PMF を使用する必要があります。PMF をサポートしないデバイスは、WiFi ネットワークに接続できません。拡張オープン認証、WPA3 個人認証、または WPA3 エンタープライズ認証を選択した場合、PMF のラジオボタンは [**Mandatory]** に設定され、変更できません。
   - **Optional**：WPA3/WPA2 Personal authentication を選択した場合、 PMF のラジオボタンは Optional に設定されていますが、変更することができます。WPA3/WPA2 Personal authentication を選択した場合、PMF のラジオボタンは **Optional** に設定されていますが、変更することができます。
   - **Disable**：PMF は WiFi ネットワークに対して無効です。Open、WPA2 Personal、WPA2/WPA Personal、または WPA2 Enterprise 認証を選択した場合、PMF のラジオボタンは **[Disable]** に設定されますが、変更できます（Open 認証を除く）。
7. **Apply** ボタンをクリックします。
   設定が保存されます。

WiFiネットワークにマルチPSKを設定する

Multi Pre-Shared Key（PSK）を使用すると、単一のWiFiネットワークを異なるVLANに分離し、それぞれが一意のパスフレーズでアクセスできるようになります。ある意味、マルチPSKは、単一のWiFiネットワーク上に異なるサブWiFiネットワークを作成することができます。WiFiネットワークに接続する際、ユーザーが入力するパスフレーズによって、WiFiクライアントが置かれるVLANが決まります。

VLAN とパスフレーズに加えて、キー識別子を VLAN とパスフレーズのマッピングに関連付けることができます。キー識別子を使用すると、ネットワーク監視の目的でWiFi ネットワークの VLAN を識別できます。たとえば、WiFi クライアントを表示するとき、キー識別子も表示できます（クライアントの分布、接続クライアント、およびクライアントの傾向を表示（191 ページ）参照）。

キー識別子の例として、corporatenetwork_22、corporatenetwork_23、corporatenetwork_24のような用語を使うことができます。これらのキー識別子（または関連するVLAN ID）はWiFiネットワークに接続しようとするユーザーには見えません：ユーザーはSSIDを見てパスフレーズを入力します。

Multi PSK を有効にすると、WiFi ネットワークのパスフレーズと VLAN は、Multi PSK 設定の一部であるパスフレーズと VLAN に置き換えられます。

注: マルチ PSK は、WiFi セキュリティが WPA2 Personal または WPA2/WPA Personal の場合のみサポートされます。アクセスポイントに最初に接続したときに定義したデフォルトの WiFi ネットワーク（ローカルの Bowser UI では SSID1 と表示されます）にマルチ PSK を設定するには、まず、WiFi セキュリティを WPA2 Personal または WPA2/WPA Personal に変更する必要があります。

また、マルチPSKには以下の制限が適用される：

- 最大 4 つの WiFi ネットワークで Multi PSK を設定できます。
- マルチ PSK を設定する各 WiFi ネットワークは、最大 8 つの VLAN 対パスフレーズのマッピングをサポートできます。(各 WiFi ネットワーク内で、各パスフレーズとキー識別子は一意である必要があります）。アクセスポイントは、最大 32 のマルチ PSK VLAN 間マッピングをサポートできます。たとえば、4 つの WiFi ネットワークがそれぞれ 8 つのマルチ PSK VLAN 間マッピングをサポートできます。
- 1つのWiFiネットワーク上のマルチPSK内で、同じVLAN IDを異なるパスフレーズにマッピングできます。また、異なる WiFi ネットワークで Multi PSK に同じ VLAN ID を使用することもできます。

- アクセスポイントが接続されているネットワークでVLAN間ルーティングが無効になっている場合は、次のようになります：
  - 同じWiFiネットワーク上の異なるVLANに接続されているWiFiクライアント（つまり、WiFiクライアントが同じWiFiネットワークに接続するために異なるパスフレーズを使用している）は、互いに通信できず、隔離されたままです。

    異なるWiFiネットワークで*同じ*VLANに接続されているWiFiクライアントは、お互いにコミュニケーションを取ることが可能です。
- マルチPSKと以下の機能は相互に排他的である：
  - キャプティブポータル（「キャプティブポータルの設定と管理（99ページ）」を参照
  - mDNS ゲートウェイ（「マルチキャスト DNS ゲートウェイの管理 (150 ページ)」を参照
  - NATモード（「アドレスとトラフィックにNATモードまたはブリッジモードを設定する（205ページ）」を参照
  - クライアント分離（WiFi ネットワークのクライアント分離の有効化または無効化 (206 ページ)を参照

WiFiネットワークにマルチPSKを設定するには：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

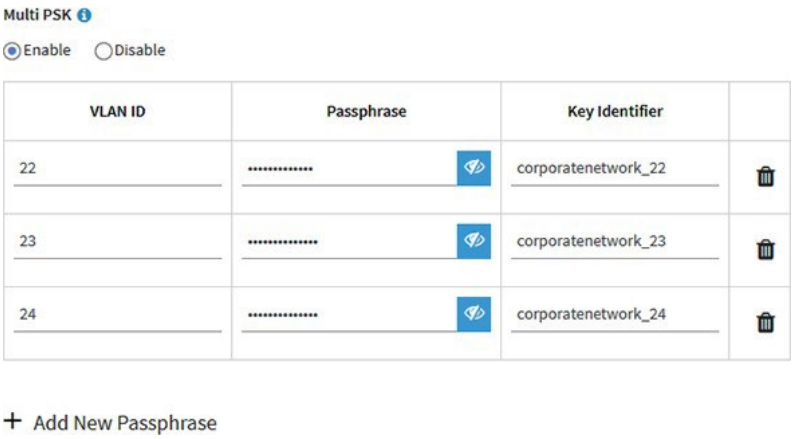
   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Wireless > Basic]** を選択します。

   表示されたページでSSIDを選択できます。
5. SSIDの左にある>ボタンをクリックします。

選択したSSIDの設定が表示されます。

アクセスポイントに最初に接続したときに定義したWiFiネットワークであるデフォルトのWiFiネットワーク（ローカルバウザーUIではSSID1と表示）では、マルチPSKを設定できません。

6. Multi PSK **Enable** ラジオボタンを選択します。下図はその例です。



7. Add New Passphraseの左にある**+**ボタンをクリックします。
   ページが調整されます。
8. マルチPSKの設定を行う：
   - **VLAN ID**：WiFiクライアントが所属するVLANであるVLAN ID。
   - **Passphrase**：WiFiクライアントがWiFiネットワークの関連VLANに接続するためにユーザーが入力しなければならない固有のパスフレーズ（WiFiパスワード）。
   - **Key Identifier**：WiFiネットワーク内のVLANを識別するためのフレーズまたは用語。ハイフン (-) とアンダースコア (_) の特殊文字を含め、最大 30 文字の英数字です。
9. 別のMulti PSKエントリーを追加するには、Add New Passphraseの左側にある**+**ボタンをクリックし、前のステップを繰り返します。
   マルチPSKエントリを削除するには、エントリの右側にあるゴミ箱アイコンをクリックします。
10. **Apply** ボタンをクリックします。
    設定が保存されます。

WiFiネットワークの無効化または有効化、WiFiアクティビティスケジュールの設定

WiFiネットワーク（SSIDまたはVAP）を一時的に無効にしたり、WiFiネットワークを再び有効にしたり、WiFiネットワークがアクティブになるタイミングを指定するスケジュールを設定したりできます。

WiFiネットワークのスケジューリングは、予定された休暇、オフィスのシャットダウン、夜間、週末にWiFiネットワークをオフにすることができる緑色の機能です。

各WiFiネットワークに対して、1つのカスタムスケジュールを作成できます。このスケジュールでは、午前12:00から午後11:59までの各日について、VAPを無効にする時間帯を指定します。

WiFiネットワークを無効または有効にしたり、WiFiアクティビティスケジュールを設定するには：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Wireless > Basic]** を選択します。

   表示されたページでSSIDを選択できます。
5. SSID の左側にある **>** ボタンをクリックします。

   選択したSSIDの設定が表示されます。
6. Schedule（スケジュール）」で、以下のラジオボタンのいずれかを選択する：
   - **Always ON**：WiFiネットワークが有効になっています。
   - **Always OFF**：WiFiネットワークは無効です。

- **Custom**：WiFiネットワークは、設定したスケジュールに従って有効または無効になります。

  ラジオボタンの右側にアイコンが表示されます。

7. 前のステップで「Custom」を選択した場合は、次のようにします：
   a. ラジオボタンの横にあるアイコンをクリックします。
   ポップアップ・ウィンドウが表示されます。
   b. プリセットメニューから定義済みの時間を選択するか、タイムブロックをクリックしてカスタムタイムブロックを選択します。

   タイムブロックの青色は、WiFiネットワークが有効（オン）になることを示します。タイムブロックの色がグレーの場合は、WiFiネットワークが無効（オフ）であることを示します。
   c. **Apply**ボタンをクリックします。ポップアップウィンドウが閉じる。
8. **Apply** ボタンをクリックします。設定が保存されます。

802.11k RRMおよび802.11v WiFiネットワーク管理によるバンドステアリングの有効化または無効化

バンドステアリングにより、アクセスポイントはデュアルバンド対応のWiFiデバイスを識別し、それらのデバイスをWiFiネットワーク（SSIDまたはVAP）の2.4GHz帯または5GHz帯に誘導します。一般的に、2.4 GHz 帯域と比較して、5 GHz 帯域ではより多くのチャネルと帯域幅が利用可能であるため、干渉が少なく、より良いユーザーエクスペリエンスが得られます。バンドステアリングには、802.11k 無線リソース管理（RRM）と 802.11v WiFi ネットワーク管理が含まれます。デフォルトでは、バンドステアリングは無効になっています。

802.11k RRM および 802.11v WiFi ネットワーク管理は、以下の方法でネットワークに影響を与えます。

- **802.11k RRM**： この機能により、アクセスポイントと 802.11k 対応クライアントは、利用可能な無線リ ソースを動的に測定することができます。802.11k対応ネットワークでは、アクセスポイントとクライアントは互いにネイバーレポート、ビーコンレポート、リンク測定レポートを送信することができ、802.11k対応クライアントは初期接続やローミングに最適なアクセスポイントを自動的に選択することができます。
- **802.11v WiFiネットワーク管理**：この機能により、アクセスポイントは、アクセスポイントのチャネル負荷に基づいて、WiFiクライアントを2.4GHz帯または5GHz帯に誘導することができます。複数のアクセスポイントがある環境では、802.11v WiFiネットワーク管理は、ローミングしているWiFiクライアントが最適なアクセスポイントを選択するのに役立ちます。

アクセスポイントは受信信号強度インジケータ（RSSI）のしきい値を自動的に設定します。(つまり、RSSI しきい値を手動で設定することはできません）。

802.11k RRM および 802.11v WiFi ネットワーク管理で、WiFi ネットワークのバンドステアリングを有効または無効にします：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Wireless > Basic]** を選択します。

   表示されたページでSSIDを選択できます。
5. SSID の左側にある **>** ボタンをクリックします。

   選択したSSIDの設定が表示されます。
6. Band Steering / 802.11 k/v で、以下のラジオボタンのいずれかを選択します：
   - **Disable**：VAP のバンドステアリングが無効。これはデフォルト設定です。
   - **Enabled**：特定のチャネル条件下で、アクセスポイントはデュアルバンド対応のWiFiデバイスをVAPの2.4GHz帯または5GHz帯に誘導します。
7. **Apply** ボタンをクリックします。

   設定が保存されます。

6

無線の基本機能の管理

この章では、アクセス ポイントの基本的な無線能を管理する方法について説明します。高度な無線能については、224 ページの「高度な無線機能の管理」を参照してください。

注意：2.4 GHz無線の無線能を変更した場合、その変更は2.4 GHz無線でブロードキャストするすべてのWiFiネットワークに影響します。同様に、5 GHz 無線（5 GHz ハイバンドと 5 GHz ローバンドを別々に設定できます）の無線能を変更した場合、その変更は 5 GHz ハイバンドまたはローバンド無線でブロードキャストするすべての WiFi ネットワークに影響します。変更が 1 つの無線に固有でない場合、変更はアクセスポイント上のすべての WiFi ネットワークに影響します。

この章には以下のセクションがある：

- 無線の基本的なWiFi設定を管理する
- 無線のオン／オフ
- 無線のWiFiモードを変更する
- 無線のチャンネル幅を変更する
- 無線のガードインターバルを変更する
- 無線の出力を変更する
- 無線のチャンネルを変更する
- WiFiのサービス品質管理

注：無線設定を変更する場合は、新しい無線設定が有効になったときに切断されないように、有線接続を使用してください。

注：このマニュアルでは、*WiFiネットワークは*SSID（サービスセット識別子またはWiFiネットワーク名）またはVAP（仮想アクセスポイント）と同じ意味です。つまり、WiFiネットワークとは、個々のSSIDまたはVAPを意味します。

無線の基本的なWiFi設定を管理する

各無線の基本 WiFi 設定は、無線で設定されているすべての WiFi ネットワーク（VAP または SSID）に適用されます。2.4 GHz、5 GHz ハイバンド、および 5 GHz ローバンド無線の無線設定を個別に指定できます。

無線の基本的なWiFi設定を管理する：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

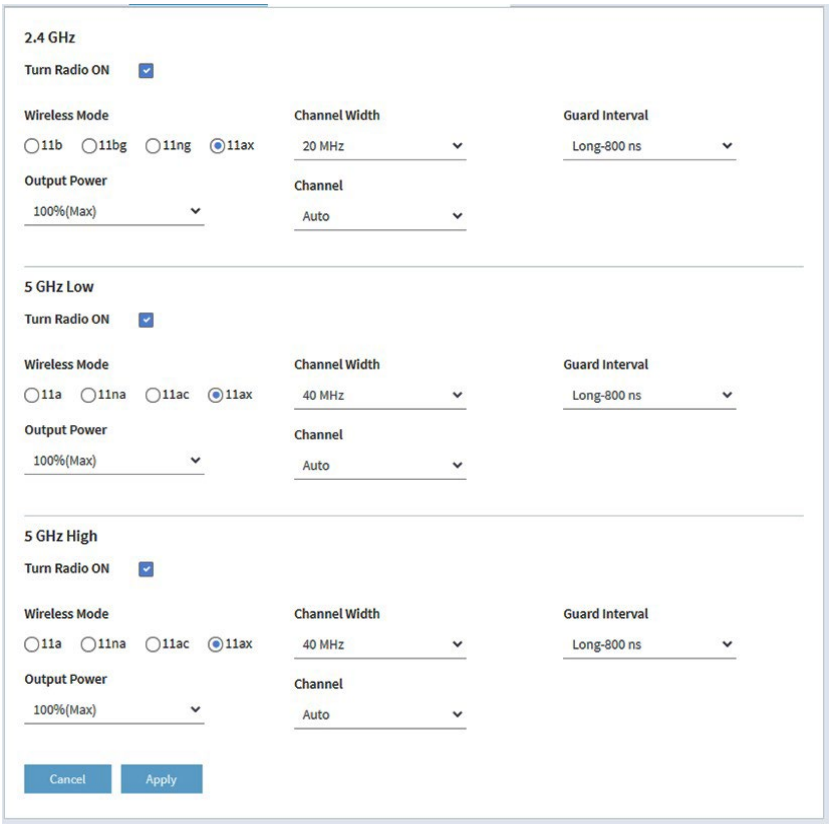
   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。

4. **Management > Configuration > Wireless > Basic > Wireless Settings]** を選択します。



以下の説明はすべての無線に適用されますが、2.4 GHz、5 GHz ハイバンド、および 5 GHz ローバンド無線の無線設定を個別に指定できます。

5. 以下の設定を行う：

- **Turn Radio ON**：デフォルトでは、**[Turn Radio ON]** チェックボックスが選択され、無線がブロードキャストされます。無線をオフにすると、そのバンドのWiFiアクセスが無効になり、設定、ネットワークチューニング、トラブルシューティングの際に役立ちます。
- **Wireless Mode**：

  2.4GHz無線のワイヤレスモード（WiFiモード）は、以下のいずれかを選択します：

  - **11ax**：802.11ax、802.11ng、802.11bg、802.11b WiFi クライアントがアクセスポイントに接続できます。これはデフォルト設定です。
  - **11ng**：802.11ax、802.11ng、802.11bg、802.11b WiFi クライアントはアクセスポイントに接続できます。ただし、802.11axクライアントの速度は、802.11ngがサポートする最大速度（約400Mbps）に制限されます。
  - **11bg**：802.11ax、802.11ng、802.11bg、802.11b WiFi クライアントはアクセスポイントに接続できます。ただし、802.11axと802.11ngクライアントの速度は、802.11bgがサポートする最大速度（約54Mbps）に制限されます。

- **11b**：802.11ax、802.11ng、802.11bg、802.11b WiFi クライアントはアクセスポイントに接続できます。ただし、802.11ax、802.11n、802.11bgクライアントの速度は、802.11bがサポートする最大速度（約11Mbps）に制限されます。

5GHz無線では、以下の無線モード（WiFiモード）のいずれかを選択します：

- **11ax**：802.11ax、802.11ac、802.11na、802.11a WiFi クライアントがアクセスポイントに接続できます。これはデフォルト設定です。
- **11ac**：802.11ax、802.11ac、802.11na、802.11a WiFiクライアントがアクセスポイントに接続できます。ただし、802.11axクライアントの速度は、802.11acがサポートする最大速度（約867Mbps）に制限されます。
- **11na**：802.11ax、802.11ac、802.11na、802.11a WiFiクライアントがアクセスポイントに接続できます。ただし、802.11axと802.11acクライアントの速度は、802.11naがサポートする最大速度（約450Mbps）に制限されます。
- **11a**：802.11ax、802.11ac、802.11na、802.11a WiFiクライアントがアクセスポイントに接続できます。ただし、802.11ax、802.11ac、802.11naクライアントの速度は、802.11aがサポートする最大速度（最大約54Mbps）に制限されます。

- **Channel Width**：メニューから無線のチャンネル幅を選択します。ワイヤレスモードメニューからの選択により、チャンネル幅を設定できるかどうか、設定できる場合はどのチャンネル幅が利用できるかが決まります。

  以下のガイドラインに従ってください：

  - より広いチャンネルは、パフォーマンスを向上させる（干渉がない、または最小限に抑えられ、データレートが向上する）。
  - 802.11n仕様では、他のモードで使用可能な従来の20MHzチャンネルに加え、40MHz幅のチャンネルが使用可能です。
  - 802.11ac仕様では、他のモードで使用可能な20MHzと40MHzのチャンネルに加え、80MHz幅のチャンネルが使用可能です。
  - 40MHzと80MHzのチャンネルは、より高いデータレートを可能にするが、使用可能なチャンネル数は少なくなる。

  詳しくは、無線のチャンネル幅の変更（92ページ）をご覧ください。

- **Guard Interval**：メニューから無線の送信電力を選択します。**100%(Max)**、**50**%、**25**%、**12.5**%、**4%(Min)**から選択できます。デフォルトは 100%(Max) です。

注：2 つ以上のアクセスポイントが同じエリアで同じチャネルで動作している**場合、**干渉が発生する可能性があります。このような場合、アクセスポイントの出力を下げるとよいでしょう。この場合、アクセスポイントの出力電力を下げることをお勧めします。

- **チャンネル**メニューから、無線の WiFi チャンネルを選択します。利用可能な WiFi チャンネルと周波数は、アクセスポイントで選択した国と無線によって異なります。デフォルトは Auto で、無線が自動的に最適なチャンネルを選択します。

  注意：WiFiチャンネルを変更する必要は**ありません。**

  注：複数のアクセスポイントを使用する場合は、隣接するアクセスポイントに異なるチャネルを選択することで、干渉を低減します。隣接するアクセスポイント間のチャネル間隔は4チャネルを推奨します（例えば、2.4GHz帯では、チャネル1と5、またはチャネル6と10を使用します）。

6. **Apply** ボタンをクリックする。
   警告ポップアップウィンドウが表示されます。

7. **OK**ボタンをクリックする。
   ポップアップウィンドウが閉じ、設定が保存されます。無線が再起動し、WiFiクライアントが再接続する必要がある場合があります。

無線のオン／オフ

デフォルトでは、2.4 GHz、5 GHz ハイバンド、および 5 GHz ローバンド無線がブロードキャストします。無線をオフにすると、関連するバンドのWiFiアクセスが無効になり、そのバンドのすべてのWiFiネットワーク（VAPまたはSSID）に影響します。無線をオフにすると、設定、ネットワークチューニング、トラブルシューティングの際に役立ちます。

無線のオン／オフ

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。
   ログインウィンドウが表示されます。

ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。

3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。

4. **Management > Configuration > Wireless > Basic > Wireless Settings]** を選択します。Wireless Settings page] ページが表示されます。
5. 以下のいずれかのアクションを取る：
   - **Turn a radio on：**［Turn Radio ON］チェックボックスを選択します。
   - **Turn a radio off:**［Turn Radio ON］チェックボックスをオフにします。
6. **Apply** ボタンをクリックする。

   警告ポップアップウィンドウが表示されます。
7. **OK**ボタンをクリックする。

   ポップアップウィンドウが閉じ、設定が保存されます。無線が再起動し、WiFiクライアントが再接続する必要がある場合があります。

無線のWiFiモードを変更する

つまり、アクセスポイントの WiFi モードは、802.11ax、802.11ac、802.11na、802.11ng、802.11bg、802.11b、802.11a クライアントをサポートします。WiFiモードを変更して、特定のタイプのクライアントへのアクセスを制限することができます。

無線のWiFiモードを変更する：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。

3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。

4. **Management > Configuration > Wireless > Basic > Wireless Settings]** を選択します。Wireless Settings page] ページが表示されます。

5. 無線のWiFiモードを選択します：

   - **2.4 GHz無線**：2.4GHz無線のWiFiモードは、以下のいずれかを選択します：
     - **11ax**：802.11ax、802.11ng、802.11bg、802.11b WiFi クライアントがアクセスポイントに接続できます。これはデフォルト設定です。
     - **11ng**：802.11ax、802.11ng、802.11bg、802.11b WiFi クライアントはアクセスポイントに接続できます。ただし、802.11axクライアントの速度は、802.11ngがサポートする最大速度（約400Mbps）に制限されます。
     - **11bg**：802.11ax、802.11ng、802.11bg、802.11b WiFi クライアントはアクセスポイントに接続できます。ただし、802.11axと802.11ngクライアントの速度は、802.11bgがサポートする最大速度（約54Mbps）に制限されます。
     - **11b**：802.11ax、802.11ng、802.11bg、802.11b WiFi クライアントはアクセスポイントに接続できます。ただし、802.11ax、802.11n、802.11bgクライアントの速度は、802.11bがサポートする最大速度（約11Mbps）に制限されます。
   - **5 GHz無線**：5GHz 無線の WiFi モードとして、以下のいずれかを選択します：
     - **11ax**：802.11ax、802.11ac、802.11na、802.11a WiFi クライアントがアクセスポイントに接続できます。これはデフォルト設定です。
     - **11ac**：802.11ax、802.11ac、802.11na、802.11a WiFiクライアントがアクセスポイントに接続できます。ただし、802.11axクライアントの速度は、802.11acがサポートする最大速度（約867Mbps）に制限されます。
     - **11na**：802.11ax、802.11ac、802.11na、802.11a WiFiクライアントがアクセスポイントに接続できます。ただし、802.11axおよび802.11acクライアントの速度は、以下のとおりです。

802.11naでサポートされている最大速度（約450Mbps）に制限されています。

- **11a**：802.11ax、802.11ac、802.11na、802.11a WiFiクライアントがアクセスポイントに接続できます。ただし、802.11ax、802.11ac、802.11naクライアントの速度は、802.11aがサポートする最大速度（最大約54Mbps）に制限されます。

6. **Apply** ボタンをクリックする。

   警告ポップアップウィンドウが表示されます。

7. **OK**ボタンをクリックする。

   ポップアップウィンドウが閉じ、設定が保存されます。無線が再起動し、 WiFi クライアントは再接続が必要になる場合があります。

無線のチャンネル幅を変更する

無線のチャンネル幅を決める際には、以下のガイドラインを参考にしてください：

- より広いチャンネルは、一般的にパフォーマンスを向上させる（干渉がない、または最小限に抑えられ、データレートが向上する）。
- 一般的に、狭いチャンネルはスループットが低くなりますが、アクセスポイントとWiFiクライアント間の距離が長く、通常よりも干渉が多い環境など、要求の厳しい状況では、より安定した接続を提供できる可能性があります。
- 802.11n仕様では、他のWiFiモードで利用可能な従来の20MHzチャンネルに加え、40MHz幅のチャンネルが利用できる。
- 5GHz帯の802.11ac仕様と802.11ax仕様では、他のWiFiモードで利用可能な20MHzと40MHzのチャンネルに加えて、80MHz幅のチャンネルが利用可能です。
- 40MHzと80MHzのチャンネルは、より高いデータ・レートを可能にするが、使用可能なチャンネル数は少なくなる。

注：デフォルトのオプション（2.4GHz無線は20MHz、5GHz無線は40MHz）のままにしておくことをお勧めします。

WiFi モード（無線の WiFi モードの変更（90 ページ）参照）は、チャネル幅を設定できるかどうか、設定できる場合はどのチャネル幅が利用可能かを決定します。

無線のチャンネル幅を変更する

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Wireless > Basic > Wireless Settings]** を選択します。Wireless Settings] ページが表示されます。
5. 無線の**Channel Width**メニューから、以下の設定のいずれかを選択します。
   - **20 MHz**：これは2.4GHz無線のデフォルト設定です。
   - **40 MHz**：これは5GHz無線のデフォルト設定です。
   - **80 MHz**：この選択は5GHz無線でのみ有効です。
   - **Dynamic 20 / 40 MHz**：この選択は2.4GHz無線でのみ有効です。
   - **Dynamic 20 / 40 / 80 MHz**：この選択は5 GHz無線でのみ有効です。
6. **Apply** ボタンをクリックする。

   警告ポップアップウィンドウが表示されます。
7. **OK**ボタンをクリックする。

   ポップアップウィンドウが閉じ、設定が保存されます。無線が再起動し、WiFiクライアントが再接続する必要がある場合があります。

無線のガードインターバルを変更する

メニューから、無線送信を干渉から保護するガード間隔を選択します。WiFi モード (無線の WiFi モードの変更 (90 ページ) を参照) によって、ガ ード間隔を設定できるかどうか、設定できる場合はどのガ ード間隔が利用可能かが決まります。11a、11b、および 11bg WiFi モードでは、ガード間隔をまったく設定できません。

以下のガイドラインに従ってください :

- より短いガードインターバルは、WiFiデバイスがアクセスポイントからより短い距離で動作する環境において、より多くのスループットをサポートする。
- ガードインターバルを長くすると、複数のSSIDやアクセスポイントから長い距離で動作するWiFiデバイスがある環境で効果的です。
- レガシー・デバイスの中には、-800nsという長いガードインターバルだけで動作するものもある。

無線のガードインターバルを変更するには

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Wireless > Basic > Wireless Settings]** を選択します。Wireless Settings page] ページが表示されます。
5. 無線の**Guard Interval**メニューから、以下の設定のいずれかを選択します :
   - **Auto**: Guard Intervalはアクセスポイントによって自動的に設定されます。このオプションは、11ax WiFi モードでは使用できません。

- **Long-800 ns**：このオプションは、11ax、11ac、11na、および 11ng モードで使用できます。11ax WiFi モードでは、このオプションがデフォルト設定です。
- **ダブルロング-1600 ns**：このオプションは11ax WiFiモードでのみ利用可能です。
- **クアドラプルロング-3200 ns**：このオプションは11ax WiFiモードでのみ利用可能です。

6. **Apply** ボタンをクリックする。

   警告ポップアップウィンドウが表示されます。

7. **OK**ボタンをクリックする。

   ポップアップウィンドウが閉じ、設定が保存されます。無線が再起動し、 WiFi クライアントは再接続が必要になる場合があります。

無線の出力を変更する

デフォルトでは、アクセスポイントの出力電力は最大に設定されています。同じエリアと同じチャネルで複数のアクセスポイントが動作している場合、干渉が発生する可能性があります。このような状況では、アクセスポイントの出力電力を下げるとよいでしょう。お住まいの国の無線周波数（RF）合計出力電力に関する規制要件に準拠していることを確認 してください。

無線の出力を変更する：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。

3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。

4. **Management > Configuration > Wireless > Basic > Wireless Settings]** を選択します。Wireless Settings] ページが表示されます。
5. **Wireless Mode**の**Output Power**メニューから、**100%(Max)**、**50**%、**25**%、**12.5**%、または**4%(Min)**を選択します。

   デフォルトは100%(Max)。
6. **Apply** ボタンをクリックする。

   警告ポップアップウィンドウが表示されます。
7. **OK**ボタンをクリックする。

   ポップアップウィンドウが閉じ、設定が保存されます。無線が再起動し、WiFi クライアントは再接続が必要になる場合があります。

無線のチャンネルを変更する

利用可能なWiFiチャンネルと周波数は、アクセスポイントと無線に選択した国によって異なります。デフォルトは Auto で、無線が自動的に最適なチャンネルを選択します。

注意：WiFiチャンネルを変更する必要はありません。

注：複数のアクセスポイントを使用する**場合は、**隣接するアクセスポイントに異なるチャネルを選択することで、干渉を低減します。隣接するアクセスポイント間のチャンネル間隔は4チャンネルを推奨します（例えば、2.4GHz帯では、チャンネル1と5、またはチャンネル6と10を使用します）。

無線のチャンネルを変更する

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

ダッシュボード・ページが表示されます。

4. **Management > Configuration > Wireless > Basic > Wireless Settings]** を選択します。Wireless Settings] ページが表示されます。
5. 無線の**Channel**メニューから、チャンネルを選択します。

   デフォルトはAuto。特定のチャンネルを選択すると、チャンネル選択は固定されます。
6. **Apply** ボタンをクリックする。

   警告ポップアップウィンドウが表示されます。
7. **OK**ボタンをクリックする。

   ポップアップウィンドウが閉じ、設定が保存されます。無線が再起動し、WiFiクライアントが再接続する必要がある場合があります。

WiFi無線のサービス品質管理

サービス品質（QoS）設定は、2.4 GHz 無線と 5 GHz 無線で別々に指定できます。これらの設定は、各無線に対してデフォルトで有効になっています。無線の QoS を無効にすると、アクセスポイントの WiFi トラフィックのスループットと速度に影響する場合があります。

WiFi 無線の QoS 設定を管理するには：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前に NETGEAR Insight ネットワークの場所にアクセスポイントを追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、次のように入力します。

その場所の Insight ネットワークパスワード。詳細については、26 ページの「NETGEAR Insight アプリを使って WiFi で接続する」を参照してください。

ダッシュボード・ページが表示されます。

4. **Management > Configuration > Wireless > Basic > QoS Settings]** を選択します。QoS Settings] ページが表示されます。
5. 無線の以下の機能を有効または無効にするには、該当する項目を選択します。

   ラジオボタンを**有効**または**無効にする：**

   - **Wi-Fiマルチメディア（WMM）**：WiFiマルチメディア（WMM）は802.11e規格のサブセットです。ビデオやオーディオのような時間に依存する情報は、通常のトラフィックよりも高い優先順位が与えられます。WMM が正しく機能するには、WiFi クライアントも WMM をサポートしている必要があります。WMM を有効にすると、WiFi デバイスからアクセスポイントに流れるアップストリームトラフィックと、アクセスポイントから WiFi デバイスに流れるダウンストリームトラフィックを WMM が制御できるようになります。WMM は、優先度の低い順に次の 4 つのキューを定義しています：
     - **Voice**：遅延を最小限に抑えた最優先のキューで、VoIPやストリーミング・メディアなどのアプリケーションに最適。
     - **Video**：遅延の少ない2番目に優先度の高いキュー。ビデオアプリケーションはこのキューにルーティングされます。
     - **Best effort**：中程度の遅延を持つ中程度の優先度のキュー。ほとんどの標準的な IP アプリケーションは、このキューを使用します。
     - **Backgroupd：**高いスループットを持つ低優先度キュー。FTP のような、時間に敏感ではないが高いスループットを必要とするアプリケーションは、 このキューを使用することができます。
   - **WMM Powersave**：WMMパワーセーブ機能を有効にすると、バッテリー駆動デバイスの電力を節約し、消費電力を微調整できます。
6. **Apply** ボタンをクリックする。

   警告ポップアップウィンドウが表示されます。
7. **OK**ボタンをクリックする。

   ポップアップウィンドウが閉じ、設定が保存されます。無線が再起動し、WiFiクライアントが再接続する必要がある場合があります。

7

キャプティブ・ポータルの設定と管理

この章では、アクセス ポイントでキャプティブ ポータルを設定および管理する方法について説明します。

キャプティブポータルとは、ユーザーがWiFiネットワークに接続しようとしたときに表示されるウェブページのことです。キャプティブポータルにはスプラッシュページが含まれ、通常はユーザーに何らかの認証が必要です。アクセスポイントは、3 種類のキャプティブポータルをサポートしています：

- **Click-through captive portal**：スプラッシュページがアクセスポイントに保存される基本的なポータル。WiFi ネットワークごとに、固有のクリックスルー キャプティブ ポータルを設定できます。
- **External captive portal**：外部のキャプティブポータルベンダによってホストされているポータル。複数の WiFi ネットワークに外部キャプティブポータルを適用したり、各 WiFi ネットワークに固有の外部キャプティブポータルを適用したりできます。
- **Facebook Wi-Fi captive portal**：ポータルとして機能するFacebookのビジネスページ。アクセスポイントに設定できるFacebook Wi-Fiキャプティブポータルは1つですが、複数のWiFiネットワークに適用できます。

この章には以下のセクションがある：

注：キャプティブポータルはマルチ PSK と互換性がありません。キャプティブポータルを有効にするには、まずマルチ PSK を無効にします（WiFi ネットワークのマルチ PSK の設定 (79 ページ)を参照）。

注：このマニュアルでは、*WiFiネットワークは*SSID（サービスセット識別子またはWiFiネットワーク名）またはVAP（仮想アクセスポイント）と同じ意味です。つまり、WiFiネットワークとは、個々のSSIDまたはVAPを意味します。

WiFiネットワーク用のクリックスルー・キャプティブ・ポータルの設定

クリックスルー型キャプティブポータルは、スプラッシュページがアクセスポイントに保存される基本的なポータルです。クリックスルー キャプティブ ポータルを使用して、WiFi ユーザーを歓迎または指示し、セッションを制限します。エンドユーザー使用許諾契約書（EULA）に同意するようユーザーに要求し、特定の Web サイトにリダイレクトできます。クリックスルー・キャプティブ・ポータルは、設定したWiFiネットワーク（SSID）に固有のものです。

WiFiネットワークにクリックスルーのキャプティブポータルを設定するには：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

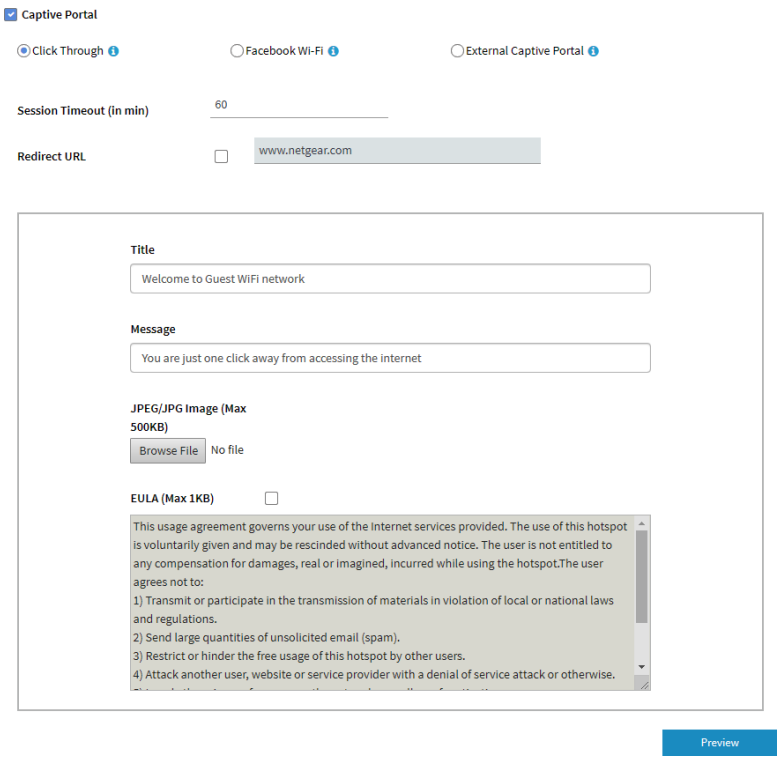
   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Wireless > Basic]** を選択します。

   表示されるページでSSIDを選択できます。
5. SSID の左側にある **>** ボタンをクリックします。

   選択したSSIDの設定が表示されます。
6. 下にスクロールし、**> Advanced**タブをクリックします。

   ページが展開します。
7. **Captive Portal**チェックボックスを選択します。

   ページが調整されます。デフォルトでは**Click Through**ラジオボタンが選択されています。



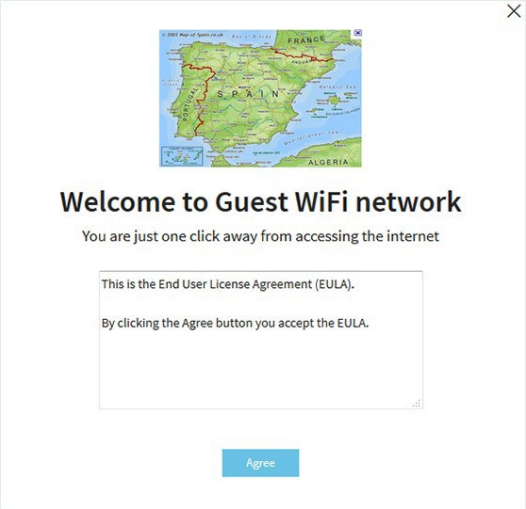
8. クリックスルーの設定を以下の表のように指定する。

設定	説明
Session Timeout (in min)	WiFiセッションが終了し、ユーザーが再度ログインする必要があるまでの分数を1から1440の間で入力します。デフォルトは60分です。
Redirect URL	ログイン後にユーザーを特定の Web サイトにリダイレクトするには、［**Redirect URL**］チェックボックスを選択し、URLを入力します。**Redirect URL**］チェックボックスがオフの場合、ユーザーはデフォルトのWebページに誘導されます。
Title	キャプティブポータルのログインページに表示されるタイトルを入力します。タイトルをカスタマイズしない場合、デフォルトのタイトルがキャプティブポータルのログインページに表示されます。
Message	ユーザーへのメッセージを入力します。このメッセージは、キャプティブポータルのログインページに表示されます。メッセージをカスタマイズしない場合、デフォルトのメッセージがキャプティブポータルのログインページに表示されます。

続き

設定	説明
JPEG/JPG画像（最大500KB）	キャプティブポータルのログインページに表示される画像をカスタマイズするには、［**Browse**］ボタンをクリックし、画像に移動して選択します。画像をカスタマイズしない場合、デフォルトの画像がキャプティブポータルのログインページに表示されます。
EULA (最大1 KB)	このフィールドには、デフォルトのエンドユーザーライセンス契約（EULA）が含まれています。フィールドにカスタムテキストを入力またはコピーできます。キャプティブポータルのログインページに EULA を表示するには、**EULA** チェックボックスを選択します。

9. キャプティブポータルのログインページをプレビューするには、**Preview**ボタンをクリックします。
   次の図はその例である（つまり、この図はデフォルトのキャプティブ・ポータルではなく、カスタマイズしたものを示している）。



10. **Apply** ボタンをクリックする。
    設定が保存されます。WiFiクライアントがSSIDに接続しようとすると、キャプティブポータルのログインページが表示されます。

    注：HTTPSセッションは、キャプティブ・ポータル認証が行われるまでブロックされる。

WiFiネットワークの外部キャプティブポータルを設定する

外部キャプティブポータルとは、外部のキャプティブポータルベンダーがホストするポータルのことです。つまり、このタイプのポータルはアクセスポイントに保存されません。外部キャプティブ ポータルの場合、通常、デバイスをベンダーに登録し、ベンダーからライセンスを購入する必要があります。

複数のWiFiネットワークに外部キャプティブポータルを適用することも、各WiFiネットワークに固有の外部キャプティブポータルを適用することもできます。

WiFiネットワークの外部キャプティブポータルを設定するには

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Wireless > Basic]** を選択します。

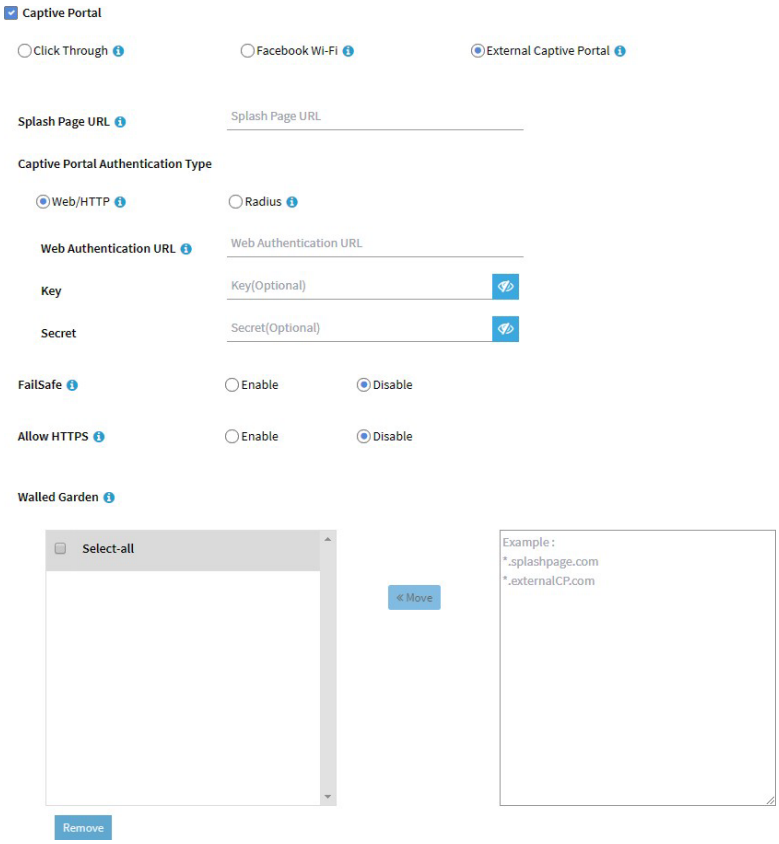
   表示されるページでSSIDを選択できます。
5. SSID の左側にある **>** ボタンをクリックします。

   選択したSSIDの設定が表示されます。
6. 下にスクロールし、**> Advanced**タブをクリックします。

   ページが展開します。
7. **Captive Portal**チェックボックスを選択します。

   ページが調整されます。デフォルトでは**Click-Through**ラジオボタンが選択されています。

8. **External Captive Portal**］ラジオボタンをクリックします。



9. **Splash Page URL**フィールドには、ベンダーから提供されたURLを入力します。

   このURLは、キャプティブポータルをホストするウェブサイトのスプラッシュページにユーザーをリダイレクトします。

10. 次の **Captive Portal Authentication Type**のラジオボタンのいずれかを選択します：

- **Web/HTTP**: スプラッシュ ページへのアクセスの認証は、HTTPS プロトコルを使用してアクセス ポイントで行われます。以下の設定を行います：
  - **Web Authentication URL**：ベンダーが提供する Web 認証 URL を入力します。
  - **Key**：ベンダーから提供されるキー・クレデンシャルを入力する。このフィールドはオプションであり、ベンダーの認証要件に依存する。
  - **Secret**：ベンダーが提供する秘密のクレデンシャルを入力する。このフィールドはオプションであり、ベンダーの認証要件に依存する。
- **Radius**：スプラッシュページにアクセスするための認証は、外部のRADIUS認証サーバーで行われる。ベンダーはまた、アカウンティングRADIUSも要求するかもしれない。

サーバを指定します。*各* RADIUS サーバーについて、ベンダーの指示に従い、以下の設定を行う：

- **IPv4 Address**：サーバーのIPアドレスを入力します。IPアドレスはベンダーから提供されます。
- **Port**：サーバーが使用するポート番号を入力します。IP ポート番号は、ベンダによって提供される。既定では、認証サーバはポート番号 1812 を使用し、アカウンティング・サーバはポート番号 1813 を使用します。
- **Password**：サーバーとやりとりするためのパスワード（共有秘密）を入力します。

  パスワードはベンダーが提供する。

11. 以下の**FailSafe**ボタンのいずれかを選択し、認証が不可能な場合に、ユーザーがスプラッシュページに到達し、インターネットにアクセスすることを許可するかどうかを指定します：
    - **Enable**：認証ができない場合（キャプティブ・ポータル・サーバーが応答しないなど）、ユーザーは30分間インターネットにアクセスできる。
    - **Disable**：これはデフォルトの設定です。認証ができない場合、ユーザーはスプラッシュ・ページに到達できず、インターネットにアクセスできません。代わりに「*Oops.何か問題が発生しました。しばらくしてから試してください。*
12. 以下の［**Allow HTTPS**］ボタンのいずれかを選択して、セキュアなHTTP（HTTPS）トラフィックの通過を許可するタイミングを指定します：
    - **Enable**：認証が行われる前に、HTTPSトラフィックの通過が許可される。
    - **Disable**：これはデフォルト設定である。HTTPSトラフィックは認証が行われる。
13. **Walled Garden**の設定を行う。

    ウォールド・ガーデンは、ユーザーがキャプティブ・ポータルからアクセスできる外部のアプリケーションやサイトを指定する。一般に、ベンダーがアプリケーションとサイトに関する情報を提供する。ベンダーのスプラッシュ・ページ、ドメイン名、および認証サーバもウォール・ ガーデンに含める必要があります。ベンダーの指示に従う。

    ウォールド・ガーデンを設定するには次のようにする：
    - **Add a single URL**：右側のフィールドにURLを入力し、**Enter**キーを押した後、**Move**をクリックします。
    - **複数のURLを追加します**：右側のフィールドにURLのリストを貼り付け、「**Move**」をクリックする。
    - **Remove one or more URLs**：URLのチェックボックスを選択し「**Remove**」ボタンをクリックします。

- **Remove all URLs**：**Select All]**チェックボックスを選択し、[**Remove]**ボタンをクリックします。

14. **Apply** ボタンをクリックする。

    設定が保存されます。WiFiクライアントがSSIDに接続しようとすると、キャプティブポータルのログインページが表示されます。

アクセスポイントのFacebook Wi-Fiの登録と設定

アクセスポイントに Facebook Wi-Fi を設定して、既存の Facebook ビジネスページにチェックインさせることで、顧客に WiFi アクセスを提供できるようにする前に（WiFi ネットワークに Facebook Wi-Fi キャプティブポータルを設定する（108 ページ）参照）、アクセスポイントを Facebook に登録し、Facebook 設定を構成する必要があります。デフォルトでは、登録機能は無効になっています。

アクセスポイントにFacebook Wi-Fiを登録・設定する：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

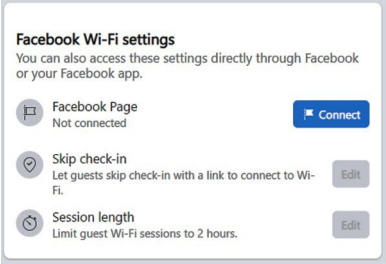
   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Wireless > Basic > Facebook Wi-Fi**を選択します。Facebook Wi-Fi ページが表示されます。
5. Facebook Wi-Fi に登録する」ラジオボタンで「**Yes**」を選択します。

   登録機能を有効にする。デフォルトでは、この機能は無効になっている。

6. **Apply** ボタンをクリックする。
   設定が保存され、**Add Page**ボタンが表示されます。
7. **Add Page**ボタンをクリックします。
   ポップアップ・ウィンドウが表示されます。
8. **OK**ボタンをクリックする。
   ポップアップウィンドウが閉じる。
   ブラウザのページが立ち上がり、フェイスブックのページが表示される。



9. FacebookのWi-Fi設定を行う：
   a. **Connect**ボタンをクリックして、Facebookのビジネスページが関連付けられているアカウントにログインし、ページを選択します。
      ページを選択すると、そのページがアクセスポイントに関連付けられます。
   b. Facebook Wi-Fiの設定ページで、「**Save**」ボタンをクリックします。
      設定が保存されます。
   c. クライアントにチェックインをスキップさせるには、[Skip check in Edit**]**ボタンをクリックし、設定を行います。
   d. セッションの長さを制限するには、「Skip check in Edit」ボタンをクリックし、設定を行う。
      セッションの長さを超えると、クライアントは自動的にログアウトする。
10. ローカルブラウザのUIでページを更新する。
11. Facebookキャプティブポータルに接続しているクライアントが、キャプティブポータル認証が発生する*前に*セキュアなHTTP(HTTPS)セッションを確立できるようにするには、［HTTPSを許可**する**］ラジオボタンを選択します。
    デフォルトでは、[Allow HTTPS **Disable]**ラジオボタンが選択されており、Facebookキャプティブポータルに接続しているクライアントは、キャプティブポータル認証が発生するまでHTTPSセッションを確立できません。
12. **Apply** ボタンをクリックします。
    設定が保存されます。

WiFiネットワークにFacebook Wi-Fiキャプティブポータルを設定する

Facebook のビジネスページにチェックインさせることで、顧客に WiFi アクセスを提供できます。その前に、アクセスポイントを Facebook Wi-Fi に登録する必要があります（アクセスポイントの Facebook Wi-Fi の登録と設定（106 ページ）を参照）。

WiFiネットワークにFacebook Wi-Fiキャプティブポータルを設定するには：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Wireless > Basic]** を選択します。

   表示されたページでSSIDを選択できます。
5. SSID の左側にある **>** ボタンをクリックします。

   選択したSSIDの設定が表示されます。
6. 下にスクロールし、**>Advanced**タブをクリックします。

   ページが展開します。
7. **Captive Portal**チェックボックスを選択します。

   ページが調整されます。デフォルトでは、**クリックスルーの**ラジオボタンが選択されています。
8. **Facebook Wi-Fi** ラジオボタンを選択します。

ページ上でこれ以上の設定を指定する必要がないため、ページは再び調整される。

Facebook のビジネスページにチェックインすることで、WiFi アクセスが可能になります。このオプションを使用するには、まずアクセスポイントをFacebook Wi-Fiに登録し、Facebook設定を構成します（アクセスポイントのFacebook Wi-Fiの登録と構成（106ページ）を参照）。

9. **Apply** ボタンをクリックする。

   設定が保存されます。WiFiクライアントがSSIDに接続しようとすると、Facebookのビジネスページが表示されます。

   注意：Facebook Wi-Fiでキャプティブポータルを設定する場合、キャプティブポータルの認証が行われる*前に*、Facebookキャプティブポータルに接続しているクライアントがセキュアなHTTP（HTTPS）セッションを確立できるようにオプションを設定できます（参照）。 アクセスポイントの Facebook Wi-Fi の登録と設定を参照してください）。

Facebook Wi-Fiからアクセスポイントの登録を解除する

アクセスポイントがFacebook Wi-Fiに登録されているが、キャプティブポータルにそのオプションを使用しなくなった場合、または別のFacebookアカウントを使用したい場合は、Facebook Wi-Fiからアクセスポイントの登録を解除し、アクセスポイントのエントリを削除することができます。

Facebook Wi-Fiからアクセスポイントの登録を解除し、アクセスポイントのエントリーを削除します：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前に NETGEAR Insight ネットワークの場所にアクセスポイントを追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、次のように入力します。

その場所の Insight ネットワークパスワード。詳細については、26 ページの「NETGEAR Insight アプリを使って WiFi で接続する」を参照してください。

ダッシュボード・ページが表示されます。

4. **Management > Configuration > Wireless > Basic > Facebook Wi-Fi** を選択します。Facebook Wi-Fi ページが表示されます。
5. **No**」のラジオボタンを選択します。

   登録機能は無効になっています。ただし、フェイスブックのビジネスページにあるアクセスポイントの項目はまだ削除されていない。
6. **Apply** ボタンをクリックします。

   設定が保存されます。
7. Facebookのビジネスページにアクセスし、アカウントにログインする。
8. アクセスポイントのエントリーのチェックボックスを選択します。
9. **Delete**ボタンをクリックする。

   アクセスポイントのエントリーは削除される。

8

アクセスとセキュリティの管理

この章では、アクセスおよびセキュリティ機能とユーザーアカウントを管理する方法について説明します。

この章には以下のセクションがある：

- インターネットアクセスの特定のURLやキーワードをブロックする
- ユーザーアカウントの管理
- ローカルMACアクセス制御リストの管理
- 近隣AP検出の管理
- RADIUSサーバーの設定
- L2セキュリティを有効にする

注記：不可欠なWiFiセキュリティ（ネットワーク認証と暗号化）については、60ページのオープンまたはセキュアWiFiネットワークのセットアップを参照してください。

注：このマニュアルでは、*WiFiネットワーク*はSSID（サービスセット識別子またはWiFiネットワーク名）またはVAP（仮想アクセスポイント）と同じ意味です。つまり、WiFiネットワークとは、個々のSSIDまたはVAPを意味します。

インターネットアクセスの特定のURLやキーワードをブロックする

ブラックリストは、インターネット アクセスをブロックする必要がある URL （ウェブアドレス）を指定して設定できます。また、キーワードを指定して、そのキーワードを含む URL をアクセスポイントに拒否させることもできます。

インターネットアクセスをブロックしなければならないURLとキーワードでブラックリストを設定する：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

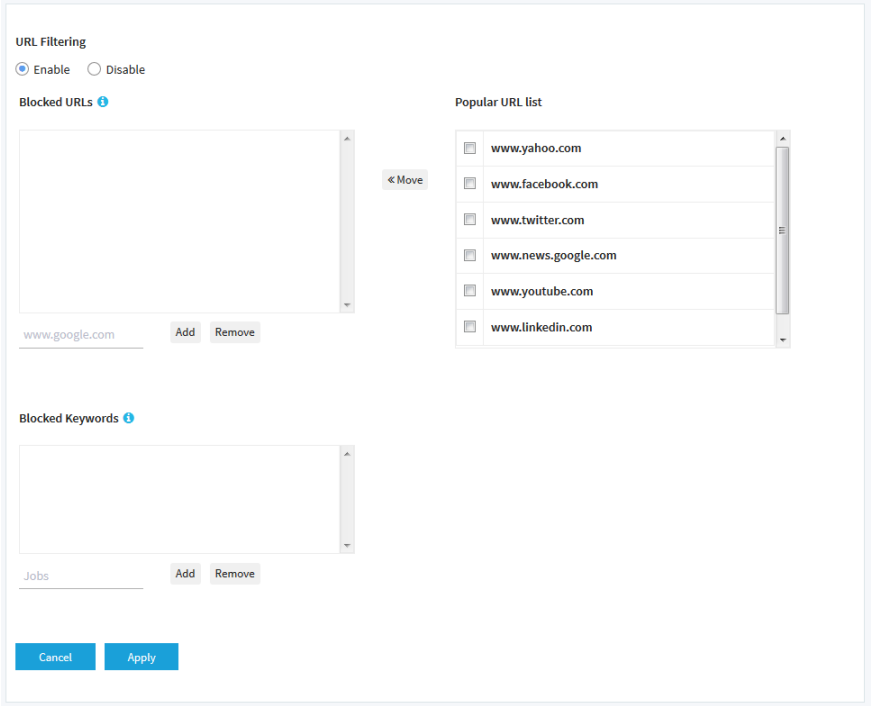
   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Security > URL Filtering**を選択します。

   URL Filteringページが表示されます。

5. **Enable** ラジオボタンを選択します。



6. 以下の方法でブラックリストを作成する：
   - **Blocked URLs**：ブラックリストにURLを追加するには、上部フィールド（上部**追加ボタンの**左側）にURLを入力またはコピーし、上部**Addボタンを**クリックします。また、URLのチェックボックスを選択し、**<<Move**ボタンをクリックすることにより、人気URLリストから1つまたは複数のURLを選択することができます。

     ブラックリストからURLを削除するには、そのURLのチェックボックスを選択し、左上の**Remove**ボタンをクリックします。

     URLをブロックすると、ドメインとドメイン内のすべてのURLがブロックされます。たとえば、www.google.com を追加すると、www.google.com/finance など、www.google.com ドメイン内のすべてのウェブページがブロックされます。
   - **Blocked Keywords**：キーワードエントリをブラックリストに追加するには、下側のフィールド（下側の**Add**ボタンの左側）にキーワードを入力し、下側の**Add ボタンを**クリックします。

     ブラックリストからキーワードエントリを削除するには、そのエントリのチェックボックスを選択し、下部の**Remove**ボタンをクリックします。

     キーワードを含むすべてのURLがブロックされます。例えば、Jobsを追加すると、Jobs（またはjobs）を含むすべてのURLがブロックされます。
7. **Apply** ボタンをクリックします。
   設定が保存されます。

ユーザーアカウントの管理

ユーザー アカウントは、アクセス ポイントのローカル ブラウザ UI への読み取り/書き込みまたは読み取り専用アクセスを提供します。管理者ユーザーアカウントの削除やユーザー名の変更はできませんが、パスワードは変更できます。他のユーザーのアカウントを追加したり、これらのアカウントを変更または削除することができます。

以下のセクションでは、ユーザーアカウントの管理方法について説明します：

- ユーザーアカウントの追加
- ユーザー・セッションのタイムアウト時間を変更する
- ユーザーアカウントの設定を変更する
- ユーザーアカウントを削除する

デフォルトのadminユーザーアカウントのパスワードの変更については、adminユーザーアカウントのパスワードの変更（ページ158）を参照してください。

ユーザーアカウントの追加

ユーザーアカウントを追加するには

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > System > Advanced > User Accounts]**を選択します。

5. ユーザーアカウント追加アイコンをクリックします。
   追加フィールドとメニューが表示されます。
6. 新しいユーザーアカウントの設定を指定します：
   - **User Name**：ユーザー名を入力します。
   - **Password**：8文字以上64文字以下のパスワードを入力します。パスワードには、少なくとも1つの大文字、1つの小文字、1つの数字を含める必要があります。以下の特殊文字が使用できます：
     !@ # $ % ^ & * ( )
   - **Privilege**：メニューから**Read-Write**または**Read-Only**を選択する。
   - **Session Timeout**：**Hours（時間）**」および「**Minutes（分）**」フィールドを使用して、セッションが自動的に終了し、ユーザーが再ログインしなければならない期間を指定します。
     デフォルトでは、セッションの有効期限は45分である。
7. **Apply** ボタンをクリックします。
   設定が保存されます。

ユーザー・セッションのタイムアウト時間を変更する

ユーザーがローカルブラウザUIにログインすると、45分後にセッションが自動的にタイムアウトします。このタイムアウト時間は、管理ユーザーを含むすべてのユーザーに適用されます。

ユーザーセッションのタイムアウト時間を変更するには：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。
   ログインウィンドウが表示されます。

ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。

3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。

4. **Management > Configuration > System > Advanced > User Accounts]**を選択します。

5. Session Timeout（セッションタイムアウト）］の［**Hours（時間）**］フィールドと［**Minutes（分）**］フィールドを使用して、セッションが自動的に終了し、ユーザーが再ログインしなければならない期間を指定します。

   デフォルトでは、セッションの有効期限は45分である。

6. **Apply** ボタンをクリックする。

   設定が保存されます。セッションは終了し、再度ログインする必要があります。

ユーザーアカウントの設定を変更する

デフォルトのadminユーザーアカウントのアクセス権限を変更することはできません。

ユーザー名、パスワード、またはユーザーアカウントのアクセス権を変更する場合：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。

3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。

4. **Management > Configuration > System > Advanced > User Accounts]** を選択します。既存のユーザーアカウントが表示されます。
5. ユーザーアカウントの右側で、必要に応じて既存の設定を変更する：
   - **User Name**：別のユーザー名を入力します。
   - **Password**：8文字以上64文字以下のパスワードを入力してください。パスワードには、少なくとも1つの大文字、1つの小文字、1つの数字を含める必要があります。以下の特殊文字が使用できます：

     !@ # $ % ^ & * ( )
   - **Privilege**：メニューから**Read-Write**または**Read-Only**を選択する。
6. **Apply** ボタンをクリックします。

   設定が保存されます。

ユーザーアカウントを削除する

不要になったユーザーアカウントを削除することができます。デフォルトのadminユーザーアカウントは削除できません。

ユーザーアカウントを削除するには

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。

3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。

4. **Management > Configuration > System > Advanced > User Accounts]** を選択します。既存のユーザーアカウントが表示されます。
5. ユーザーアカウントの右にある**X**をクリックします。

   警告ポップアップウィンドウが表示されます。

6. **Delete**ボタンをクリックする。

   ポップアップウィンドウが閉じ、ユーザーアカウントが削除されます。

ローカルMACアクセス制御リストの管理

アクセス・ポイントは、MAC アドレスに基づく 8 つのローカル・アクセス・ コントロール・リスト（ACL）をサポートしています。各ローカル MAC ACL には、合計 512 個の MAC アドレスを含めることができます。

アクセスを許可するポリシーでACLを設定し、そのACLをWiFiネットワーク（つまりSSID）に適用すると、ACLは以下のように機能する：

- ACLにMACアドレスを配置したWiFiデバイスは、WiFiネットワークへのアクセスを許可されます。
- 他のすべてのWiFiデバイスは、WiFiネットワークへのアクセスを拒否されます。

アクセスを拒否するポリシーでACLを設定し、そのACLをWiFiネットワーク（つまりSSID）に適用すると、ACLは次のように機能する：

- ACLにMACアドレスを配置したWiFiデバイスは、WiFiネットワークへのアクセスを拒否されます。
- 他のすべてのWiFiデバイスは、WiFiネットワークへのアクセスを許可されます。

ACL は、WiFi ネットワークに適用してから有効になります。WiFi ネットワークへの ACL の適用については、WiFi ネットワークの MAC ACL の選択 (36 ページ) を参照してください。

211.MAC ACL は複数の WiFi ネットワークに適用できます。次のセクションでは、

MAC ACL を管理する方法について説明します：

- MACアクセス制御リストの手動設定
- 既存のMACアクセス制御リストをインポートする

MACアクセス制御リストの手動設定

アクセス制御リスト（ACL）は、それぞれ最大 512 の MAC アドレスに基づいて、最大 8 つまで構成できます。アクセスポイントには、次のデフォルトグループ名と設定の MAC ACL が含まれています：

- **Management**：有効にすると、デフォルトで信頼されたステーションへのアクセスを許可する。
- **Guest**：有効の場合、デフォルトで信頼されたステーションへのアクセスを許可する。
- **Guest1**：有効の場合、デフォルトで信頼されていないステーションへのアクセスを拒否する。
- **Custom**：有効の場合、デフォルトで信頼されていないステーションへのアクセスを拒否する。
- **Custom 1**：有効の場合、デフォルトで信頼済みステーションへのアクセスを許可する。
- **Custom 2**：有効の場合、デフォルトで信頼済みステーションへのアクセスを許可する。
- **Custom 3**：有効の場合、デフォルトで信頼済みステーションへのアクセスを許可する。
- **Custom 4**：有効の場合、デフォルトで信頼済みステーションへのアクセスを許可する。

デフォルトでは、これらの MAC ACL は無効になっており、ステーションは含まれていません。手動でデバイスを追加するか、デバイスをインポートするか（既存の MAC アクセス制御リストのインポート（127 ページ）参照）、またはその両方を実行できます。

MAC ACL を使用して、WiFi ネットワークにアクセスできる WiFi デバイス（ステーション）を制御できます。1 つの MAC ACL を複数の WiFi ネットワークに適用できます。

手動でMAC ACLを設定するには

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

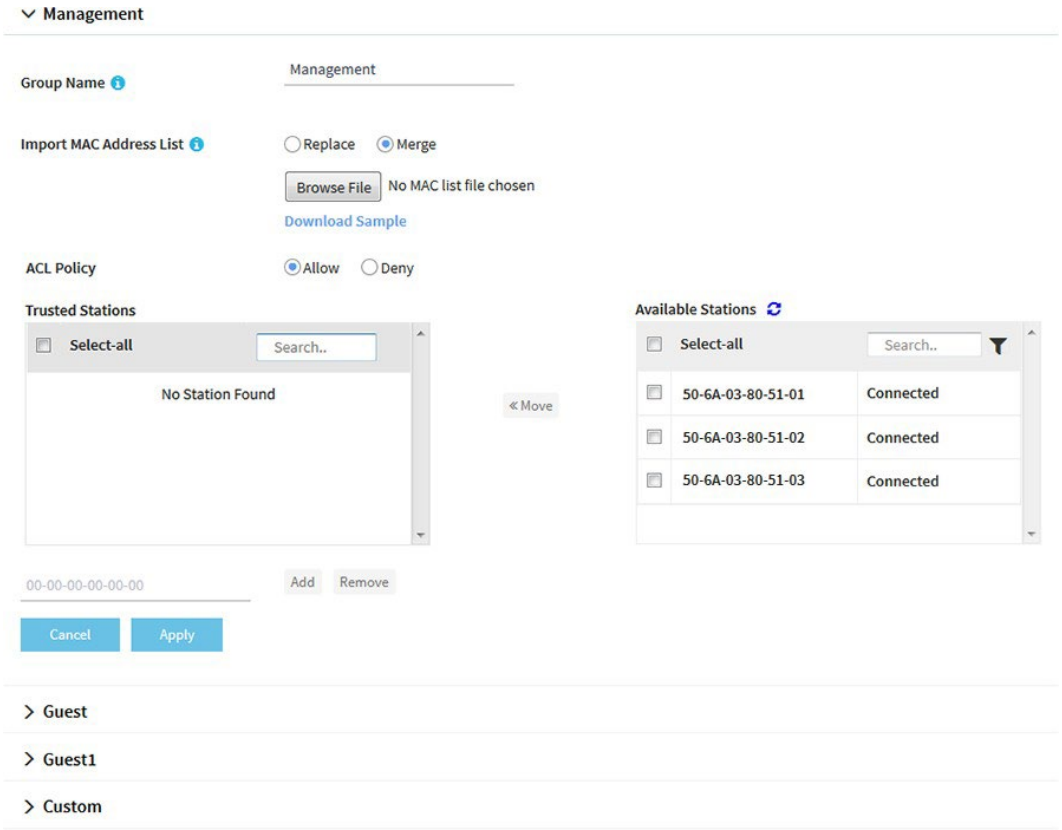
   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

ダッシュボード・ページが表示されます。

4. **Management > Configuration > Security > MAC ACL** を選択します。
5. 設定したいMAC ACLのグループ名をクリックする。



前の図はいくつかの例を示しています。利用可能なステーション]テーブル内のデバイスは、アクセスポイントによって自動的に検出され、すべての MAC ACL に共通であるため、複数の MAC ACL にデバイスを追加できます。隣接しているステーションは に Neighbor と表示され、接続されているステーションは Connected と表示されます。

6. グループ名を変更するには、**Group Name**フィールドに新しい名前を入力します。

   8つのMAC ACLのデフォルトのグループ名は、Management、Guest、Guest1、Custom、Custom 1、Custom 2、Custom 3、Custom 4である。
7. ACL Policy **Allow** または **Deny** ラジオボタンを選択する。

Allowラジオボタンを選択すると、ACLにMACアドレスを配置したWiFiデバイスはWiFiネットワークへのアクセスが許可されますが、それ以外のWiFiデバイスはWiFiネットワークへのアクセスが拒否されます。

Deny] ラジオボタンを選択すると、ACL に MAC アドレスを配置した WiFi デバイスは WiFi ネットワークへのアクセスを拒否されますが、他のすべての WiFi デバイスは WiFi ネットワークへのアクセスを許可されます。

8. ACLは次のように構成する：
   - ステップ7で**Allow**ラジオボタンを選択したACLについて、以下を実行する：
     - 手動でデバイスをTrusted Stationsテーブルに追加するには、Trusted Stationsテーブルの下のフィールドに00-00-00-00-00-00の形式でMACアドレスを入力し、**Add**ボタンをクリックします。

       デバイスがTrusted Stationテーブルに追加される。
     - デバイスをAvailable StationsテーブルからTrusted Stationsテーブルに移動するには、デバイスのチェックボックスを選択し、**「<<Move」ボタンを**クリックします。利用可能局テーブルを検索することができます。また、フィルタアイコンをクリックすることで、Available Stationsテーブルのデバイスをフィルタリングすることができます。
     - Trusted Stationsテーブルからデバイスを削除するには、デバイスのチェックボックスを選択し、[**Remove]**ボタンをクリックします。

       Trusted Stationsテーブルを検索できます。デバイスをTrusted Stationsテーブルから削除すると、アクセスポイントがデバイスを再検出した後、デバイスは再びAvailable Stationsテーブルに配置されます。
   - ステップ7で**[Deny]**ラジオボタンを選択したACLについて、以下を実行する：
     - デバイスをUntrusted Stationsテーブルに手動で追加するには、Untrusted Stationsテーブルの下のフィールドに、00-00-00-00-00-00 の形式で MAC アドレスを 入力し、「**Add**」ボタンをクリックします。

       デバイスは「Untrusted Stations」テーブルに追加される。
     - デバイスをAvailable StationsテーブルからUntrusted Stationsテーブルに移動するには、そのデバイスのチェックボックスを選択し、**「<< Move**」ボタンをクリックします。Available Stationsテーブルを検索することができます。また、フィルタアイコンをクリックすることで、Available Stationsテーブルのデバイスをフィルタリングすることができます。
     - Untrusted Stationsテーブルからデバイスを削除するには、デバイスのチェック・ボックスを選択し、"**Remove "**ボタンをクリックする。

       Untrusted Stationsテーブルを検索できます。

       Untrusted Stationsテーブルからデバイスを削除すると、アクセス ポイントがデバイスを再検出した後、デバイスは再びAvailable Stationsテーブルに配置されます。

9. **Apply** ボタンをクリックします。
   設定が保存されます。

   WiFi ネットワークに ACL を適用する方法の詳細については、WiFi ネットワークの MAC ACL の選択（211 ページ）を参照してください。

   Trusted Stations テーブルの WiFi デバイスは、ACL を適用した WiFi ネットワークにアクセスできます。Untrusted Stations テーブルの WiFi デバイスは、ACL を適用する WiFi ネットワークにアクセスできません。

既存のMACアクセス制御リストをインポートする

最大 512 個の MAC アドレスに基づく既存のアクセス制御リスト（ACL）をインポートできます。リストはどのMAC ACLにもインポートできますが、リスト上のMACアドレスは、リストをインポートしたMAC ACLでのみ使用できます。つまり、同じリストを別のMAC ACLで使用する場合は、そのMAC ACLにもリストをインポートする必要があります。

MACアドレスのファイルは以下の形式でなければならない：

- ファイル内の項目はMACアドレスのみで、各オクテットをハイフンで区切った16進数形式でなければならない（例：00-11-22-33-44-55）。
- コンマで区切ってください。
- ファイルはテキスト形式（拡張子が.txtまたは.cfg）でなければなりません。

MAC ACL を使用して、WiFi ネットワークにアクセスできる WiFi デバイスを制御できます。MAC ACL は複数の WiFi ネットワークに適用できます。

既存のMAC ACLをインポートするには

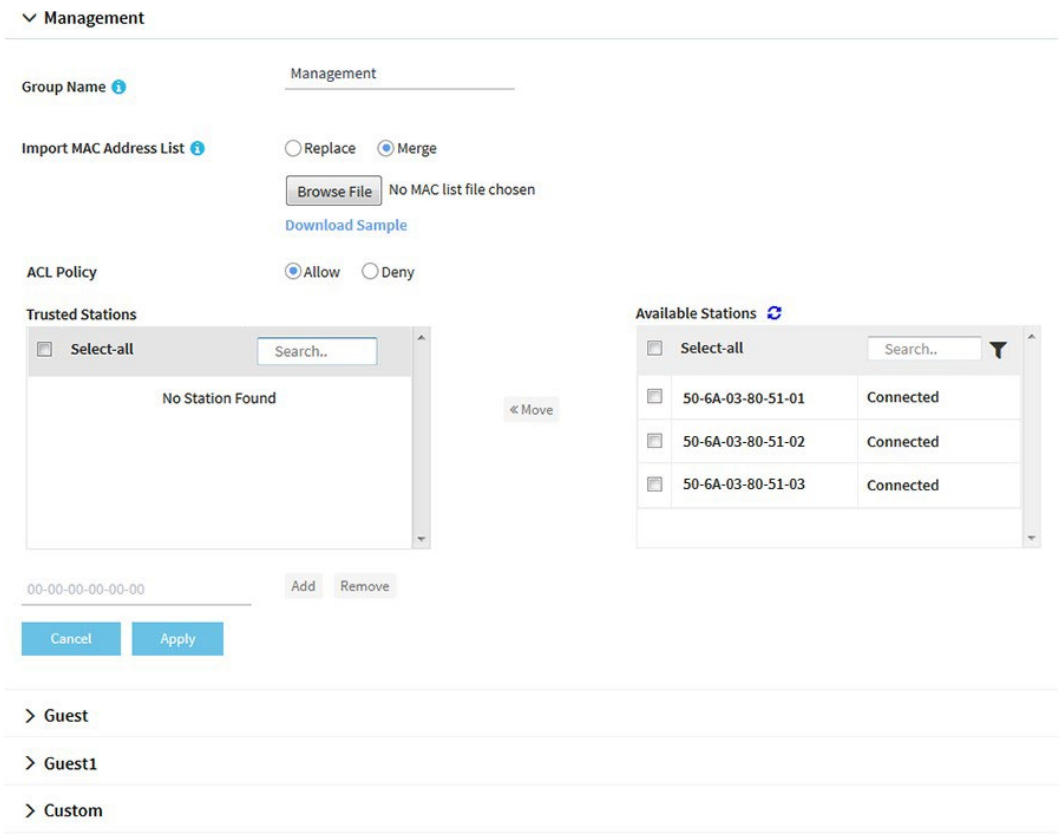
1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。
   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。
   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

ダッシュボード・ページが表示されます。

4. **Management > Configuration > Security > MAC ACL** を選択します。
5. 設定したいMAC ACLのグループ名をクリックする。



前の図はいくつかの例を示しています。利用可能局テーブルのデバイスはアクセスポイントによって自動的に検出され、すべての MAC ACL に共通です。このため、複数の MAC ACL にデバイスを追加することができます。

6. グループ名を変更するには、**Group Name**フィールドに新しい名前を入力します。

   8つのMAC ACLのデフォルトのグループ名は、Management、Guest、Guest1、Custom、Custom 1、Custom 2、Custom 3、Custom 4である。

7. ACL Policy **Allow** または **Deny** ラジオボタンを選択する。

   Allowラジオボタンを選択すると、ACLにMACアドレスをインポートしたWiFiデバイスはWiFiネットワークへのアクセスが許可されますが、それ以外のWiFiデバイスはWiFiネットワークへのアクセスが拒否されます。

Deny] ラジオボタンを選択すると、MAC アドレスを ACL にインポートした WiFi デバイスは WiFi ネットワークへのアクセスを拒否されますが、他のすべての WiFi デバイスは WiFi ネットワークへのアクセスを許可されます。

8. インポートに必要な形式のMAC ACLのサンプルをダウンロードするには、**Download Sample**リンクをクリックする。
9. 以下の方法でACLをインポートし、構成する：
   - ステップ7で**Allow**ラジオボタンを選択したACLについて、以下を実行する：
     a. 以下のラジオボタンのいずれかを選択して、インポートリストのMACアドレスをTrusted Stationsテーブルの MACアドレスに置き換える、またはマージする（すでにテーブル内にある場合）：
        - **Replace**：Trusted StationsテーブルのMACアドレスは、インポートリストのものと置き換えられる。
        - **Merge**：Trusted StationsテーブルのMACアドレスは、インポートリストのものとマージされる。

     b. **Browse**ボタンをクリックし、インポートファイルに移動して選択します。
        インポートリスト上のMACアドレスは、Trusted Stationsテーブルに置かれる。
     c. Trusted Stationsテーブルから MACアドレスを削除するには、MACアドレスを選択し、**Remove**ボタンをクリックします。
        Trusted Stationsテーブルを検索できます。
        デバイスをTrusted Stationsテーブルから削除すると、アクセスポイントがデバイスを再検出した後、デバイスは再びAvailable Stationsテーブルに配置されます。
   - ステップ7で**[Deny]**ラジオボタンを選択したACLについて、以下を実行する：
     a. 以下のラジオボタンのいずれかを選択して、インポート・リストのMACアドレスをUntrusted Stationsテーブルの MACアドレス（すでにテーブル内にある場合）に置換またはマ ージする：
        - **Replace**：Untrusted StationsテーブルのMACアドレスは、インポートリストのものと置き換えられる。
        - **Merge**：Untrusted StationsテーブルのMACアドレスは、インポートリストのものとマージされる。

     b. **Browse**ボタンをクリックし、インポートファイルに移動して選択します。
        インポートリスト上のMACアドレスは、Untrusted Stationsテーブルに置かれる。

c. Untrusted StationsテーブルからMACアドレスを削除するには、MACアドレスを選択し、「**Remove**」ボタンをクリックします。

Untrusted Stationsテーブルを検索できます。

Untrusted Stationsテーブルからデバイスを削除すると、アクセス ポイントがデバイスを再検出した後、デバイスは再び Available Stationsテーブルに配置されます。

10. **Apply** ボタンをクリックする。

設定が保存されます。MACアドレスをTrusted Stationsテーブルまたは「Untrusted Stationsテーブル に手動で追加する方法については、「MACアクセス制御リストの手動設定（119ページ）」を参照してください。

WiFi ネットワークに ACL を適用する方法の詳細については、WiFi ネットワークの MAC ACL の選択（211 ページ）を参照してください。

Trusted Stations テーブルの WiFi デバイスは、 が ACL を適用する WiFi ネットワークにアクセスできます。Untrusted Stations テーブルの WiFi デバイスは、ACL を適用した WiFi ネットワークにアクセスできません。

近隣AP検出の管理

アクセスポイントは、無線帯域内の近隣のアクセスポイント（AP）を検出することができ、それらを既知のAPとして分類することができます。

無線帯域の近隣 AP 検出を有効にすると、アクセスポイントは定期的に WiFi ネットワークをスキャンし、チャネル上のすべてのアクセスポイントに関する情報を収集し、そのエリアで検出したアクセスポイントのリストを維持します。初期状態では、検出されたすべてのアクセスポイントが不明 AP リストに表示されます。使い慣れたアクセスポイントを [Known AP List] に追加できます。既知の AP リストに既知のアクセスポイントのリストをインポートすることもできます。

注意：不明 AP リストにあるアクセス・ポイントは、さらに調査が必要です。これらのアクセスポイントは、正規のネットワークの SSID を使用する不正なアクセスポイントである可能性があります。この種のアクセス・ポイントは、深刻なセキュリティ上の脅威となる可能性があります。

次のセクションでは、近隣 AP 検出を管理し、近隣アクセスポイントを Known AP リストに追加する方法について説明します：

- 近隣アクセスポイントの検出を有効にし、アクセスポイントをKnown APリストに移動する
- Known AP Listで既存の近隣アクセスポイントリストをインポートする

注：エネルギー効率モードを有効にすると、アクセスポイントは 5 GHz 無線帯域で近隣 AP を検出できません。5 GHz 無線帯域で近隣 AP 検出を使用するには、まずエネルギー効率モードを無効にします。詳細については、「エネルギー効率モードの管理 (180 ページ)」を参照してください。

近隣アクセスポイントの検出を有効にし、アクセスポイントをKnown APリストに移動する

アクセスポイントは、近隣のアクセスポイント（AP）を検出し、既知の AP として分類できます。近隣 AP 検出を有効にした後、アクセス ポイントはエリア内で検出したアクセス ポイントのリストを維持します。初期状態では、検出されたすべてのアクセス ポイントが不明 AP リストに表示されます。手動でアクセス ポイントを不明 AP リストから既知 AP リストに移動できます。

デフォルトでは、近隣アクセスポイント検出は無効になっています。

近隣のアクセスポイントの検出を有効にし、検出されたアクセスポイントを Known AP リストに移動する：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

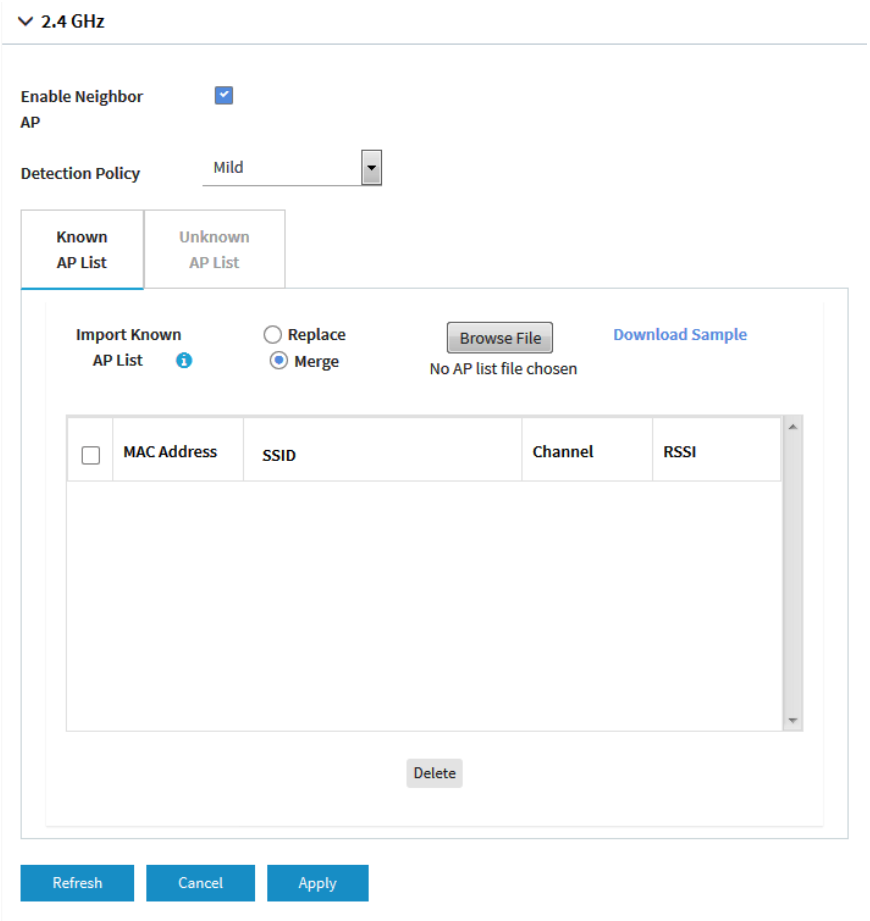
   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Security > Neighbor AP** を選択します。

   表示されるページで、無線バンド（2.4 GHz、5 GHz Low、または 5 GHz High）を選択できます。
5. ラジオバンドの左にある **>** ボタンをクリックします。

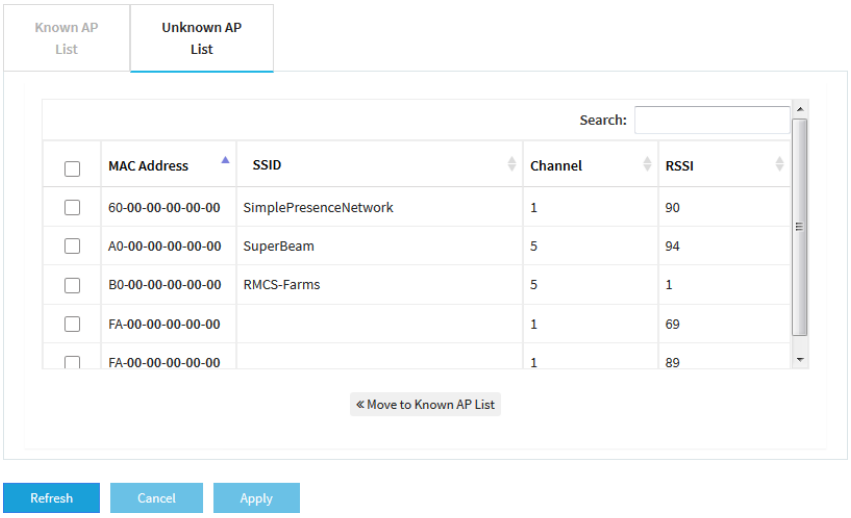
   選択した無線バンドの Neighbor AP ページが表示されます。

6. **Enable Neighbor AP**チェックボックスを選択します。
7. **Apply** ボタンをクリックする。
   設定が保存されます。近隣AP検出が有効になりました。



8. **Detection Policy]**メニューから、スキャン方法を選択します：
   - **Mild**：アクセスポイントは1時間ごとに近隣のアクセスポイントをスキャンします。これはデフォルト設定です。
   - **Moderate**：アクセスポイントは30分ごとに近隣のアクセスポイントをスキャンします。
   - **Aggressive**：アクセス ポイントは、15 分ごとに近隣のアクセス ポイントをスキャンします。検出された近隣アクセスポイントは、不明 AP リストに表示されます。

9. 検出された近隣のアクセス ポイントを表示し、不明な AP リストから既知の AP リストに移動するには、次の手順を実行します：
   a. **Unknown AP List** タブをクリックします。



   b. アクセス ポイントが表示されない場合は、[**Refresh]** ボタンをクリックします。
   c. 使い慣れていて信頼できるアクセスポイントのチェックボックスを選択します。
   d. **Move to Known AP List**」ボタンをクリックする。
   e. **Known AP List** タブをクリックします。
   選択したアクセスポイントは Known AP List に表示されます。

   注: Known AP リストからアクセス ポイントを削除できます。検出された後、これらのアクセス ポイントは再び [Unknown AP List] に表示されます。

10. **Apply** ボタンをクリックします。
    設定が保存されます。

Known AP Listで既存の近隣アクセスポイントリストをインポートする

既知の近隣アクセスポイントの MAC アドレスを含むリストを Known AP List にインポートできます。

MACアドレスのファイルは以下の形式でなければならない：

- ファイル内の項目はMACアドレスのみで、各オクテットをハイフンで区切った16進数形式でなければならない（例：00-11-22-33-44-55）。

- コンマで区切ってください。
- ファイルはテキスト形式（拡張子が.txtまたは.cfg）でなければなりません。

近隣 AP 検出の有効化については、「近隣アクセスポイント検出の有効化と既知 AP リストへのアクセスポイントの移動（126 ページ）」を参照してください。

既知の近隣アクセスポイントの MAC アドレスを含むリストを Known AP List にインポートするには、次の手順に従います：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

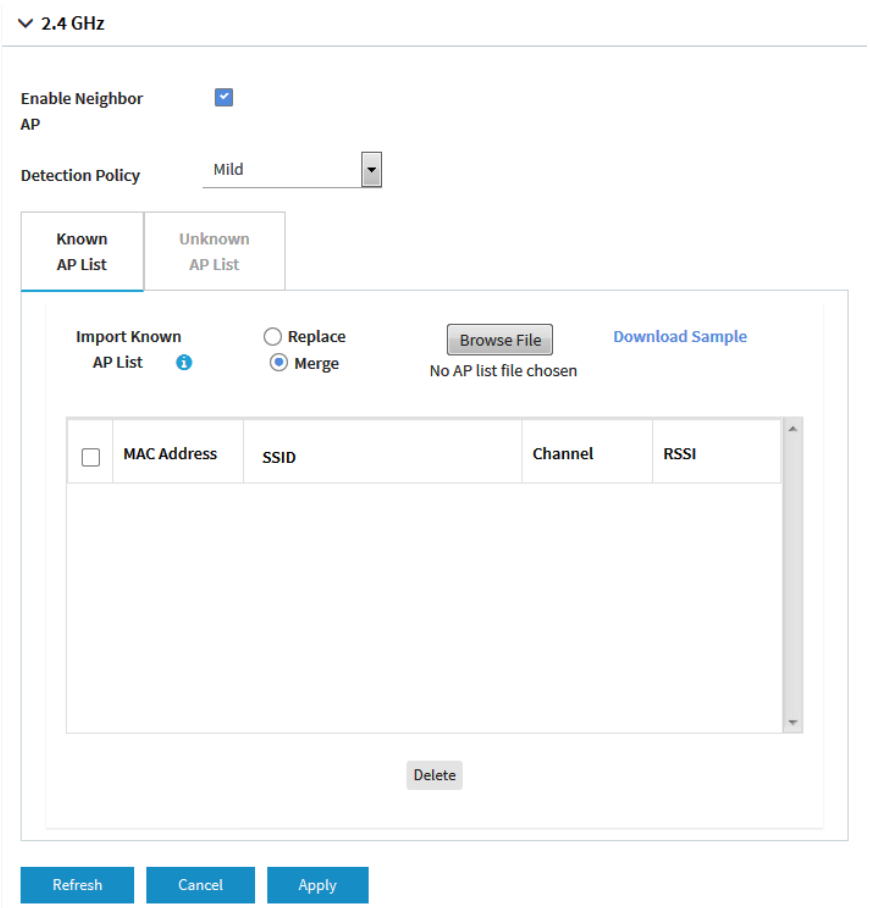
   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Security > Neighbor AP** を選択します。

   表示されるページで、無線バンド（2.4 GHz、5 GHz Low、または 5 GHz High）を選択できます。

5. ラジオバンドの左にある **>** ボタンをクリックします。



6. Known AP Listでインポートするために必要な形式のAPリストのサンプルをダウンロードするには、**Download Sample**リンクをクリックしてください。
7. 以下の方法でKnown AP Listをインポートし、構成する：
   a. 以下のラジオボタンのいずれかを選択して、インポートリストのMACアドレスをKnown APリストのMACアドレスに置換またはマージします：
      - **置き換える**：Known APリストのMACアドレスは、インポートリストのものに置き換えられる。
      - **マージ**：Known APリストのMACアドレスは、インポートリストのものとマージされる。
   b. **Browse** ボタンをクリックし、インポートファイルに移動して選択します。インポートリストのMACアドレスがKnown AP Listに配置されます。
   c. Known AP ListからMACアドレスを削除するには、MACアドレスを選択し、**Delete**ボタンをクリックします。

      Known AP リストからデバイスを削除すると、アクセスポイントがデバイスを再検出した後、デバイスは再び Known AP リストに登録されます。

8. **Apply** ボタンをクリックします。
   設定が保存されます。

RADIUSサーバーの設定

WPA2 Enterpriseセキュリティ、WPA3 Enterpriseセキュリティ、またはRADIUS MAC ACLを使用する場合は、認証用のRADIUSサーバー、またはRADIUSを使用した認証とアカウンティングの両方を設定する必要があります。プライマリ IPv4 サーバーを設定する必要があり、セカンダリ IPv4 サーバーを設定できます。これらの RADIUS サーバー設定は、WPA2 エンタープライズセキュリティまたは WPA3 エンタープライズセキュリティを使用するすべての WiFi ネットワーク（「オープンまたはセキュアな WiFi ネットワークのセットアップ (60 ページ)」を参照）、または RADIUS MAC ACL を使用するすべての WiFi ネットワークに適用されます。

注：WPA2 Enterprise セキュリティまたは WPA3 Enterprise セキュリティと RADIUS MAC ACL は、 相互に排他的です。WiFi ネットワークに RADIUS MAC ACL を使用する場合は、別のタイプの WiFi セキュリティを選択します（オープンまたはセキュアな WiFi ネットワークのセットアップ (60 ページ) を参照）。WiFi ネットワークに WPA2 エンタープライズセキュリティまたは WPA3 エンタープライズセキュリティを使用する場合は、ローカル MAC ACL を使用します（ローカル MAC アクセス制御リストの管理 (118 ページ) を参照）。

RADIUS MAC ACLを使用する場合は、RADIUSサーバーでクライアントのMACアドレスに次の例の形式を使用して、ACLを定義する必要があります：クライアントMACアドレスが00:0a:95:9d:68:16の場合、RADIUSサーバーで000a959d6816と指定します。

RADIUSサーバーを設定する：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。
   ログインウィンドウが表示されます。

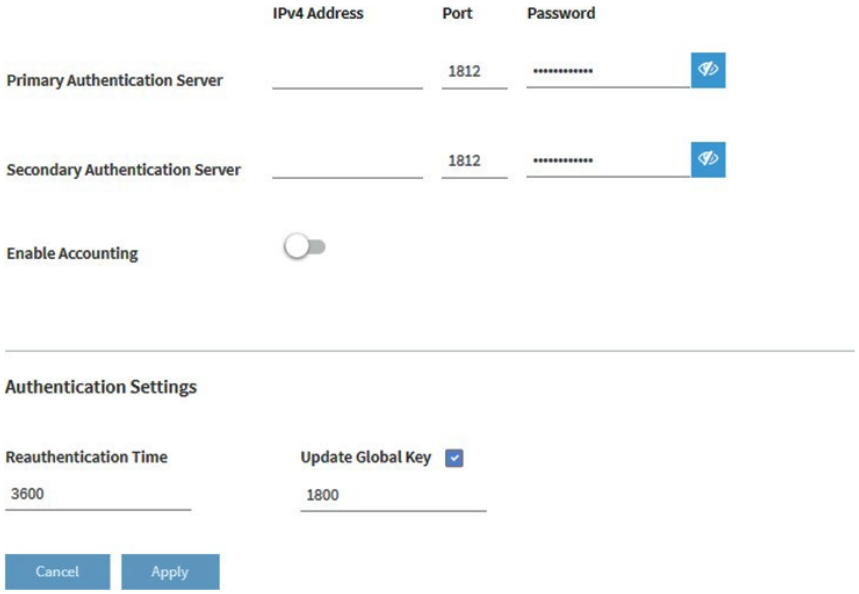
   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。
   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前に NETGEAR Insight ネットワークの場所にアクセスポイントを追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、次のように入力します。

その場所の Insight ネットワークパスワード。詳細については、26 ページの「NETGEAR Insight アプリを使って WiFi で接続する」を参照してください。

ダッシュボード・ページが表示されます。

4. **Management > Configuration > Security > RADIUS Settings**を選択します。



5. 設定したいRADIUSサーバーごとに、以下の設定を行う：
   - **IPv4 Address**：RADIUS サーバーの IPv4 アドレスを入力します。アクセスポイントはこの IP アドレスに到達できる必要があります。
   - **Port**：RADIUSサーバーへのアクセスに使用するアクセスポイントのUDPポートの番号を入力します。デフォルトのポート番号は 1812 です。
   - **Password**：認証またはアカウンティングプロセス中にアクセスポイントと RADIUS サーバー間で使用されるパスワード（共有キー）を入力します。デフォルトでは、パスワードは sharedsecret です。
6. 認証サーバでアカウンティングを有効にするには、「**Enable Accounting**」ボタンが青く表示されるようにする。
7. 以下の認証設定を構成します（設定したすべての RADIUS サーバーに適用されます）：
   - **Reauthentication time**：サプリカント（WiFi クライアント）が RADIUS サーバーで再認証されるまでの間隔を秒単位で入力します。デフォルトの間隔は 3600 秒（1 時間）です。再認証を無効にするには、**0** を入力します。

- **Update Global Key**：グローバル・キーの更新を許可するチェック・ボックスを選択し、間隔を秒単位で入力する。チェック・ボックスはデフォルトで選択されており、デフォルトの間隔は1800秒（30分）です。チェックボックスをオフにすると、グローバル・キーの更新は行われなくなります。

8. **Apply** ボタンをクリックします。
   設定が保存されます。

L2セキュリティを有効にする

L2 セキュリティは、WiFi インターフェイス上の VLAN タグ付きパケットをブロックすることで、VLAN スタッキングによる攻撃を防ぐことができます。L2 セキュリティを有効にすると、アクセスポイントは、ARP、IPv4、IPv6 トラフィックなど、特定のタイプのクライアント トラフィックのみを任意の WiFi ネットワークで許可します。L2 セキュリティはデフォルトで無効になっています。

L2セキュリティを有効にする：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。
   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。
   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management] > [Configuration] > [Security] > [L2 Security]** を選択します。
   L2 Security] ページが表示されます。
5. **Yes**」ラジオボタンを選択します。
   デフォルトでは、[No]ラジオボタンが選択されており、L2セキュリティは無効になっている。

6. **Apply** ボタンをクリックします。
   設定が保存されます。

9

ローカルエリアネットワークとIP設定の管理

この章では、アクセス ポイントのローカル エリア ネットワーク (LAN) と IP 設定を管理する方法について説明します。

この章には以下のセクションがある：

- DHCPクライアントを無効にし、固定IPアドレスを指定する。
- DHCPクライアントを有効にする
- 802.1Q VLANと管理VLANの設定
- 既存のドメイン名を設定する
- スパニングツリープロトコルの有効化または無効化
- ネットワーク整合性チェック機能の有効化または無効化
- IGMPスヌーピングの有効化または無効化
- イーサネットLLDPの有効化または無効化
- UPnPを有効または無効にする
- リンクアグリゲーション機能の管理
- マルチキャストDNSゲートウェイの管理

注：このマニュアルでは、*WiFiネットワークは*SSID（サービスセット識別子またはWiFiネットワーク名）またはVAP（仮想アクセスポイント）と同じ意味です。つまり、WiFiネットワークとは、個々のSSIDまたはVAPを意味します。

DHCPクライアントを無効にし、固定IPアドレスを指定する。

デフォルトでは、アクセス ポイントの DHCP クライアントは有効になっており、アクセス ポイントはネットワーク内の DHCP サーバー（または DHCP サーバーとして機能するルーター）から IP アドレスを受信します。ネットワークに DHCP サーバーがない場合、または固定（静的） IP アドレスを指定したい場合は、アクセス ポイントの DHCP クライアントを無効にします。

DHCPクライアントを無効にし、固定IPアドレスを指定する：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

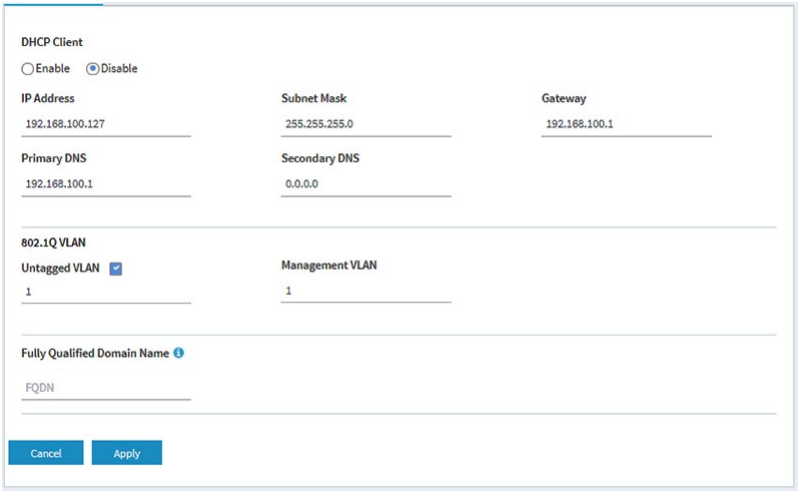
   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > IP > LAN**を選択します。

   表示されたページでLAN設定を指定できますが、DHCPクライアントが有効になっているため、フィールドはマスクされています。

5. **Disable**」ラジオボタンを選択します。



これでフィールドはマスクされなくなった。

6. 以下の表で説明されている設定を指定します。

設定	説明
IP Address	LANで使用されている範囲のIPアドレス（通常は255.255.255.0）。
Subnet Mask	サブネットマスクはLANに対応したものでなければなりません。
Gateway	LAN上のゲートウェイのIPアドレス。
Primary DNS	LAN上のプライマリドメインネームシステム（DNS）サーバーのIPアドレス
Secondary DNS	LAN上のセカンダリDNSサーバーのIPアドレス、またはこのフィールドを空白にする

7. **Apply** ボタンをクリックする。
設定が保存されます。アクセス ポイントは、新しい IP 設定で再起動します。

DHCPクライアントを有効にする

デフォルトでは、アクセスポイントの DHCP クライアントは有効になっており、アクセスポイントはネットワーク内の DHCP サーバー（または DHCP サーバーとして機能するルーター）から IP アドレスを受信します。

DHCPクライアントを無効にした場合は、再度有効にしてください。

DHCPクライアントを有効にするには

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

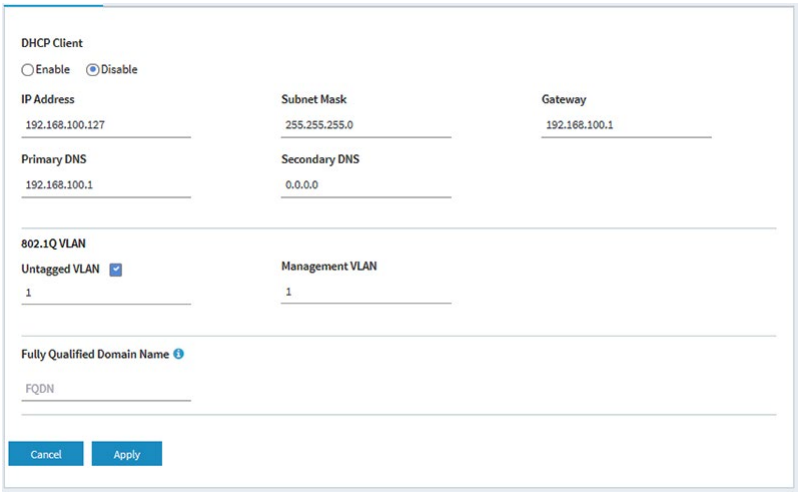
   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > IP > LAN**を選択します。



5. **Enable** ラジオボタンを選択します。

   フィールドがマスクされます。
6. **Apply** ボタンをクリックする。

   設定が保存されます。アクセスポイントは、新しい IP 設定で再起動します。アクセスポイントが DHCP サーバーから IP アドレス設定を受信するまで、しばらく時間がかかる場合があります。

802.1Q VLANと管理VLANの設定

アクセスポイント上の 802.1Q VLAN プロトコルは、同じ物理（有線）ネットワーク上のトラフィックを論理的に分離します。このプロトコルは、次のようにタグ付きおよびタグなし VLAN で動作できます：

- **Untagged VLAN**：アクセスポイントは、イーサネットインターフェイスからタグなしフレームを送信します。着信タグなしフレームはタグなし VLAN に割り当てられます。デフォルトでは、タグなし VLAN は VLAN 1 です。デフォルトでは、アクセス ポイントはタグなし VLAN で機能します。
- **Tagged VLAN**：アクセスポイントは、イーサネットインターフェイスから送信するすべてのフレームにタグを付けます。既知の VLAN ID でタグ付けされた受信フレームだけが受け入れられます。

管理 VLAN は、アクセスポイントに送受信される Telnet、SNMP、HTTP、HTTPS などのトラフィックを管理するために使用されます。管理 VLAN に属し、トランクを介して送信されるフレームは、802.1Q ヘッダーを受け取りません。ポートが 1 つの VLAN のメンバである場合、そのトラフィックはタグなしにすることができます。

管理VLANと以下の機能は相互に排他的です：

- mDNS ゲートウェイ（「マルチキャスト DNS ゲートウェイの管理 (150 ページ)」を参照
- NATモード（「アドレスとトラフィックのNATモードまたはブリッジモードの設定（205ページ）」参照

802.1Q VLAN と管理 VLAN を設定します：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

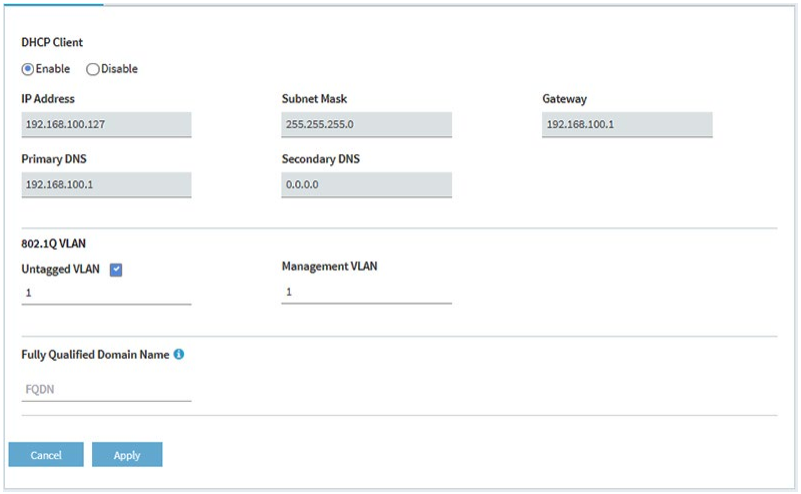
   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

ダッシュボード・ページが表示されます。

4. **Management > Configuration > IP > LAN**を選択します。



5. 802.1Q VLAN を変更するには、**Untagged VLAN** チェックボックスをクリアするか選択します：
   - **Untagged VLAN**：デフォルトでは、**Untagged VLAN** チェックボックスが選択されています。アクセスポイントは、イーサネットインターフェイスからタグなしフレームを送信します。受信したタグなしフレームは、タグなし VLAN に割り当てられます。デフォルトでは、タグなし VLAN は VLAN 1 ですが、その VLAN ID がネットワークでサポートされている場合は、フィールドに別の VLAN ID を入力できます。
   - **Tagged VLAN**：LAN上のハブやスイッチが 802.1Q VLAN プロトコルをサポートしている場合のみ、［**Untagged VLAN**］チェックボックスをオフにします。アクセスポイントは、イーサネットインターフェイスから送信するすべてのフレームにタグを付けます。既知の VLAN ID でタグ付けされた受信フレームだけが受け入れられます。同様に、タグなし VLAN の ID を変更するのは、LAN 上のハブとスイッチが 802.1Q VLAN プロトコルをサポートしており、新しい VLAN ID がネットワークでサポートされている場合のみです。
6. 管理VLANのVLAN IDを変更するには、［Management VLAN］フィールドに別の VLAN IDを入力します。

   デフォルトでは、管理 VLAN は VLAN 1 です。VLAN IDを変更する場合は、その VLAN IDがネットワークでサポートされていることを確認してください。
7. **Apply** ボタンをクリックする。

   設定が保存されます。アクセス ポイントは、新しい VLAN 設定で再起動します。

既存のドメイン名を設定する

アクセス ポイントの既存の完全修飾ドメイン名（FQDN）を指定すると、IP アドレスの代わりにドメイン名を使用してアクセス ポイントにアクセスできます。

FQDNは、ドメインネームシステム（DNS）プロバイダーに登録されているドメイン名でなければならない。

以下はFQDNの要件である：

- 長さは1文字から64文字まで。
- 英数字可（a-zおよび1-9）
- ドット(.)とハイフン(-)は使用できますが、どちらか一方から始まる名前は使

用できません。例としては、*myap01-firstfloor-myorganization.comがあります*。

既存の**FQDN**を設定するには

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

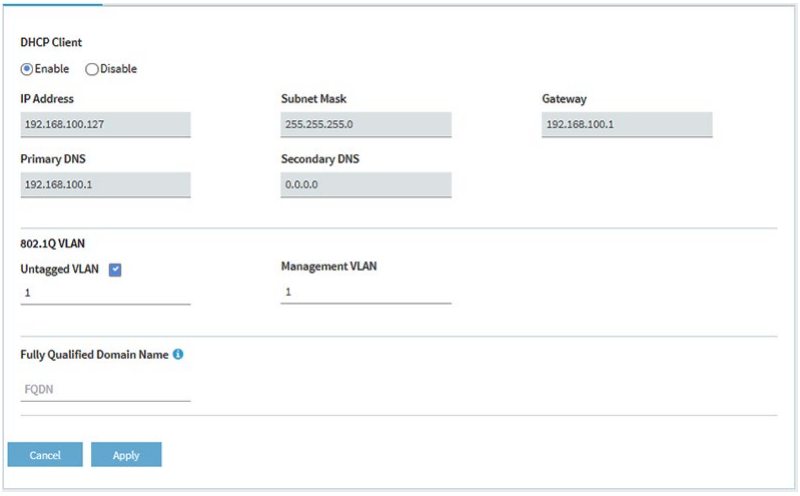
   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。

4. **Management > Configuration > IP > LAN**を選択します。



5. **Fully Qualified Domain Name**（完全修飾ドメイン名）フィールドで、FQDNを指定します。
6. **Apply** ボタンをクリックする。

   設定が保存されます。アクセスポイントは、FDQN を IP アドレスに解決しようとします。

スパニングツリープロトコルの有効化または無効化

複数のアクセスポイントがアクティブで、冗長ネットワークパスが存在する可能性がある場所では、スパニングツリープロトコル（STP）を使用すると、ネットワークループを防 ぐことができます。冗長ネットワークパスが存在する可能性がある場所では、STP を有効にすることをお勧めします。

スパニングツリープロトコルを有効または無効にします：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

ダッシュボード・ページが表示されます。

4. **Management > Configuration > System > Advanced > General** を選択します。
   General] ページが表示されます。
5. スパニングツリープロトコルのラジオボタンを選択します：
   - **Enable**：STP が有効。
   - **Disable**：STPを無効にする。これはデフォルト設定である。
6. **Apply** ボタンをクリックします。
   設定が保存されます。

ネットワーク整合性チェック機能の有効化または無効化

ネットワーク整合性チェック機能により、アクセスポイントは、WiFi 関連付けを許可する前に、上流リンクがアクティブであるかどうかを検証できます。デフォルトゲートウェイが正しく設定されていることを確認してください。デフォルトでは、ネットワーク整合性チェック機能は無効になっています。

ネットワーク整合性チェック機能を有効または無効にする：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。
   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。
   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前に NETGEAR Insight ネットワークの場所にアクセスポイントを追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。

詳細については、26 ページの「NETGEAR Insight アプリを使って WiFi で接続する」を参照してください。

ダッシュボード・ページが表示されます。

4. **Management > Configuration > System > Advanced > General**を選択します。

   General] ページが表示されます。

5. Network Integrity Checkラジオボタンを選択します：
   - **Enable**：ネットワーク整合性チェック機能が有効。
   - **Disable**：ネットワーク整合性チェック機能は無効です。これはデフォルト設定です。
6. **Apply** ボタンをクリックします。

   設定が保存されます。

IGMPスヌーピングの有効化または無効化

IGMPスヌーピングは、IPマルチキャストパケットを対応するマルチキャストグループのメンバーだけに送信できるようにします。IGMP スヌーピングを有効にすると、ブロードキャストドメイン内のすべてのポートへのマルチキャストトラフィックのフラッディングを防ぐことができます。デフォルトでは、アクセスポイントの IGMP スヌーピングは無効になっています。

IGMP スヌーピングを有効または無効にする：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入

   力します。ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

ダッシュボード・ページが表示されます。

4. **Management > Configuration > System > Advanced > General**を選択します。
   General] ページが表示されます。
5. IGMP Snooping ラジオボタンを選択します：
   - **Enable**：IGMP スヌーピングが有効。
   - **Disable**：IGMPスヌーピングを無効にする。デフォルト設定。
6. **Apply** ボタンをクリックします。
   設定が保存されます。

イーサネットLLDPの有効化または無効化

IEEE 802.1AB で規定されている LLDP （Link Layer Discovery Protocol） は、 隣接するネ ットワーク機器にリンク層のメッセージを提供します。たとえば、 LLDP を使用すると、 スイッチや管理デバイスなどのネットワーク デバイスが、 ネットワーク内のアクセス ポイントを検出できます。

LLDP は、 アクセス・ポイントが PoE で電力を得ているかどうかも検出できます。デフォルトでは、 LLDP は有効になっています。

LLDP を有効または無効にします：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。
   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。
   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。

4. **Management > Configuration > System > Advanced > Ethernet LLDP]** を選択します。Ethernet LLDP] ページが表示されます。
5. ラジオボタンを選択します：
   - **有効にする**：LLDP が有効。これはデフォルト設定です。
   - **無効にする**：LLDP が無効。

   注意: アクセス ポイントが PoE スイッチから電力供給を受けている場合に LLDP を無効にすると、**[Apply]** ボタンをクリックした後にアクセス ポイントの電源がオフになることがあります。その場合は、アクセス ポイントを再起動します。
6. **Apply** ボタンをクリックします。
   設定が保存されます。

UPnPを有効または無効にする

ユニバーサルプラグアンドプレイ（UPnP）を使用すると、UPnP をサポートするネットワーク内の他のデバイスによってアクセスポイントが検出されるようになります。UPnP はデフォルトで有効になっています。

UPnPを有効または無効にする：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。
   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > System > Advanced > UPnP**を選択します。

UPnPページが表示されます。

5. ラジオボタンを選択します：
   - **Enable**：UPnPが有効です。これはデフォルト設定です。
   - **Disable**：UPnPは無効です。
6. **Apply** ボタンをクリックします。
   設定が保存されます。

リンクアグリゲーション機能の管理

リンクアグリゲーション（LAG）接続には、リンクアグリゲーションをサポートするスイッチを使用する必要があります。アクセスポイントとスタティックリンクアグリゲーションをサポートするスイッチの間で LAG 接続を行うことができます。このような LAG 接続では、スループットを向上させる単一の 2 Gbps 接続、または 1 Gbps の冗長接続が可能です。

注：LAN 1ポートは最大2.5Gbps、LAN 2ポートは最大1Gbpsをサポートします。LAG接続の場合、両方のポートが同じ速度で機能する必要があります。

したがって、LAG接続の場合、LAN 1ポートの速度は1Gbpsに制限されます。ただし、スループットを向上させるためにLAG接続を使用する場合、LAG接続の速度は2 Gbps（1 Gbps + 1 Gbps）になります。

デフォルトでは、アクセスポイントでは LAN 1 ポートと LAN 2 ポートの両方が有効になっており、どちらのポートもデフォルト VLAN（VLAN ID 1）のメンバーになっています。LAN 2 ポートは LAG 接続ポートとして使用できます。また、デフォルトでは、アクセスポイントのリンクアグリゲーション機能は無効になっていますが、有効にすることができます。また、LAG 接続を確立するスイッチでリンクアグリゲーションを設定する必要があります。

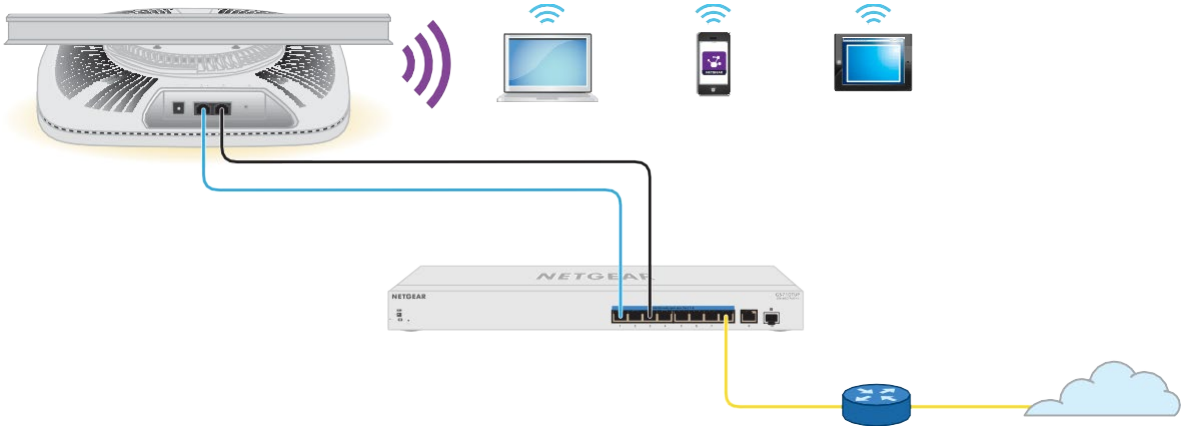


図9.リンクアグリゲーション接続

LAN 2 ポートのリンクアグリゲーションを有効にします。

アクセスポイントとスイッチ間のスタティックリンクアグリゲーション接続は、以下の方法で設定できます：

1. スイッチで、アクセスポイントへのLAG接続に使用する2つのイーサネットポートに静的リンクアグリゲーションを設定します。

   注意：ネットワークのループを防ぐため、スイッチポートをアクセスポイントポートに接続する*前に*構成してください。

2. スイッチの2つのイーサネットポートを、アクセスポイントのLAN 1ポートとLAN 2ポートに接続します。

アクセスポイントのリンクアグリゲーション機能を有効にする：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management] > [Configuration] > [System] > [Advanced] > [LAG]** を選択します。

   LAG ページが表示されます。
5. **Enable** ラジオボタンを選択します。
6. **Apply** ボタンをクリックする。

   ポップアップ警告ウィンドウが開きます。
7. **OK**ボタンをクリックする。

ポップアップ・ウィンドウが閉じ、設定が保存されます。リンクアグリゲーション機能が有効になります。

LAN 2ポートのリンクアグリゲーションを無効にする

リンクアグリゲーションを有効にしたが、その必要がなくなった場合、アクセスポイントのリンクアグリゲーションを無効にし、LAN 2 ポートをアクセスモードに戻すことができます。

注： アクセス ポイントのリンク アグリゲーションを無効にする前に、アクセス ポイントの LAN 2 ポートを、リンク アグリゲーションに使用したスイッチのイーサネット ポートから切断してください。

アクセスポイントのリンクアグリゲーション機能を無効にするには、次の手順に従います：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management] > [Configuration] > [System] > [Advanced] > [LAG]** を選択します。

   LAG ページが表示されます。
5. **Disable**」ラジオボタンを選択します。

   注意： ネットワークのループを防ぐため、アクセスポイントが LAN 1 ポートのみを経由してスイッチに接続されていることを確認してください。
6. **Apply** ボタンをクリックする。

   ポップアップ警告ウィンドウが開きます。

7. **OK**ボタンをクリックする。

   ポップアップ・ウィンドウが閉じ、設定が保存されます。リンクアグリゲーション機能が無効になります。

マルチキャストDNSゲートウェイの管理

mDNSは、アクセスポイントが接続されているネットワークでVLAN間ルーティングが無効になっている場合でも機能します。

共有デバイスには、プリンター、スキャナー、ストレージデバイス、その他のハードウェアデバイスが含まれる。サービスには、あらかじめ定義された複数の電話、音楽、ビデオストリーミングサービス、ファイル共有サービス、その他のサービスやアプリケーションが含まれる。

たとえば、WiFiクライアントのグループがVLAN 20にあり、プリンタがVLAN 1にある場合、mDNSゲートウェイポリシーによって、WiFiクライアントがプリンタを利用できるようにすることができます。また、会議参加者がVLAN 20上のWiFiネットワークに接続された電話を使用して、VLAN 30上のWiFiネットワークに接続された大画面デバイスにプレゼンテーションをキャストしたい場合、別のmDNSゲートウェイポリシーでこれを可能にすることができます。

サービスは有線デバイスでもWiFiデバイスでも実行できますが、WiFiクライアントがサービスにアクセスするには、mDNSゲートウェイ機能が有効になっているアクセスポイント上のWiFiネットワークにWiFiクライアントが接続されている必要があります。

mDNS ゲートウェイ機能をサポートする複数のアクセスポイントを持つネットワークでは、1 つのアクセスポイントを mDNS リフレクターアクセスポイントとして設定できます。

mDNSゲートウェイと以下の機能は相互に排他的である：

- 動的 VLAN を使用する WPA2 エンタープライズセキュリティおよび WPA3 エンタープライズセキュリティ（オープンまたはセキュア WiFi ネットワークのセットアップ（60 ページ）参照
- マルチ PSK（WiFi ネットワークのマルチ PSK の設定（79 ページ）参照
- 管理 VLAN (「802.1Q VLAN と管理 VLAN の設定 (139 ページ)」を参照)
- NATモード（「アドレスとトラフィックのNATモードまたはブリッジモードの設定（205ページ）」参照
- クライアントの分離（WiFi ネットワークのクライアント分離の有効化または無効化 (206 ページ)を参照

マルチキャストDNSゲートウェイを有効にし、ポリシーを追加する

マルチキャスト DNS (mDNS) ゲートウェイを有効にし、ポリシーを追加すると、アクセス ポイントは共有可能なデバイスとサービスを自動的に検出できます。ポリシーは、次の 2 つの VLAN 間のブリッジを形成します：

- **Service VLAN**：共有デバイスまたはサービスをメンバーとして含むVLAN。たとえば、共有デバイスの種類は*プリンター*で、*この場合*、サービスVLANはプリンターがメンバーであるVLANとなります。また、共有サービスの種類を***Googlecast***とすることもでき、この場合、サービスVLANはGooglecastデバイスがメンバーであるVLANとなる。
- **VLANs on allowed WiFi networks**：サービスVLAN上の共有デバイスまたはサービスを使用できるWiFiデバイスをメンバーとして含むVLAN。

ポリシーは最大8つまで追加できる。ポリシーは、共有デバイスまたはサービスへのアクセスを有効にします。クライアントが接続されているアクセスポイントに、共有デバイスや共有サービス用のポリシーが設定されている場合、WiFiクライアントは共有デバイスや共有サービスにアクセスできます。

マルチキャストDNSゲートウェイを有効にし、ポリシーを追加する：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。ダッシュボード・ページが表示されます。
4. **管理 > 設定 > mDNSゲートウェイを**選択します。

   mDNS Gatewayページが表示されます。
5. mDNS Gateway **Enable**ラジオボタンを選択します。

   デフォルトでは、mDNSゲートウェイは無効になっており、[Disable]ラジオボタンが選択されています。

6. ネットワークに、mDNS ゲートウェイ機能をサポートする複数のアクセス ポイントがあり、このアクセス ポイントがネットワーク内の mDNS リフレクター アクセス ポイントとして機能する必要がある場合は、**[Yes]** ラジオ ボタンを選択します。

   デフォルトでは、「No」ラジオボタンが選択されています。
7. Add Policy **+** ボタンをクリックします。

   mDNSゲートウェイポリシーのテーブルに行が追加されます。(複数のポリシーに対して複数の行を追加できます)。
8. 以下を指定して、mDNSゲートウェイポリシーを定義する：
   - **Policy Name**：ポリシーを識別するための名前です。二重引用符 ("") とバックスラッシュ (\) を除いて、最大 32 文字の英数字と特殊文字を使用できます。
   - **Shared Services**：**Shared Services**メニューから、共有する必要があるデバイス（プリンターなど）またはサービス（Googlecastなど）のタイプを選択します。
   - **Service VLAN**：「**Service VLAN**」フィールドに、「**Shared Services**」メニューから選択した共有デバイスまたはサービスのタイプをメンバーとして含むVLAN IDを入力します。
   - **Service IP**：Shared Servicesメニューから選択した共有デバイスまたはサービスのIPアドレスを入力します。
   - **Allowed Wireless Network**：**Allowed Wireless Network**メニューから、［**Shared Services**］メニューから選択したタイプの共有デバイスまたはサービスを使用できるWiFiデバイスをメンバーとして含む、関連するVLANを持つWiFiネットワークを選択します。
9. 別のmDNSポリシーを追加するには、Add Policy **+**ボタンをクリックし、前の手順を繰り返します。
10. **Apply** ボタンをクリックします。

    設定が保存されます。

マルチキャストDNSポリシーの変更または削除

マルチキャストDNS（mDNS）ポリシーを変更または削除できます。

mDNSポリシーを変更または削除する：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。

3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。

4. **Management > Configuration > mDNS Gateway**を選択します。

   mDNS Gatewayページが表示されます。

5. ポリシーを変更するには
   a. ポリシーの右側にある**鉛筆とノートブック**のアイコンをクリックします。
   b. 設定を変更する。

      設定の詳細については、「マルチキャストDNSゲートウェイの有効化とポリシーの追加（151ページ）」を参照してください。

   c. **Apply** ボタンをクリックします。
      設定が保存されます。
6. ポリシーを削除するには
   a. ポリシーの右側にある**ゴミ箱**アイコンをクリックします。
   b. 削除を確認する。

10

アクセス・ポイントの管理と維持

この章では、アクセス ポイントを管理および保守する方法について説明します。

この章には、次のセクションがあります：

- 管理モードを NETGEAR Insight または Web ブラウザに変更します。
- 国または地域の変更
- 管理ユーザーアカウントのパスワードを変更する
- システム名の変更
- カスタムNTPサーバーの指定
- タイムゾーンの設定
- シスログ設定の管理
- アクセスポイントのファームウェアを管理する
- アクセスポイントの設定ファイルを管理する
- ローカルブラウザのUIからアクセスポイントを再起動する
- アクセスポイントの再起動をスケジュールする
- アクセスポイントを工場出荷時のデフォルト設定に戻す
- SNMPの有効化とSNMP設定の管理
- LEDの管理
- エネルギー効率モードの管理

注：このマニュアルでは、*WiFiネットワークは*SSID（サービスセット識別子またはWiFiネットワーク名）またはVAP（仮想アクセスポイント）と同じ意味です。つまり、WiFiネットワークとは、個々のSSIDまたはVAPを意味します。

管理モードを NETGEAR Insight または Web ブラウザに変更します。

アクセスポイントは、次のいずれかの管理モードで機能します：

- **NETGEAR Insight モード**：NETGEAR Insight Premium および Insight Pro 加入者は、Insight Cloud Portal または NETGEAR Insight アプリがインストールされたモバイルデバイスからアクセスポイントをリモート管理できます。

  NETGEAR Insight モードがデフォルト設定です。このモードでは、ローカル ブラウザー UI 経由でアクセス ポイントに接続できますが、利用できるのは基本的かつ限定的なローカル ブラウザー UI のみです。NETGEAR Insight Cloud Portal と Insight アプリについては、 insight.netgear.com を参照し、netgear.com/support/product/insight.aspx の NETGEAR ナレッジベースを参照してください。

  注意: 管理モードを Web ブラウザ モードから NETGEAR Insight モードに変更すると、IP アドレス、アクセス ポイント名、ローカル ブラウザ UI のパスワードを除いて、アクセス ポイントの構成がリセット（クリア）されます。アクセス ポイントは再起動し、SSID Netgearxxxxxx をブロードキャストします。MAC アドレスは製品ラベルに記載されています。デフォルトの WiFi パスフレーズは **sharedsecret** です。

- **ウェブブラウザモード**：ローカルブラウザ UI を使用して、WiFi または有線デバイスからアクセスポイントをローカルに管理できます。このモードでは、アクセスポイントはスタンドアロンデバイスとして機能し、Insight クラウドベースの管理プラットフォームには接続されません。

  注: 最初にアクセス ポイントを NETGEAR Insight ネットワーク ロケーションに追加し、Insight クラウド ポータルまたは Insight アプリでアクセス ポイントを管理した後、管理モードを Web ブラウザー モードに変更した**場合**、アクセス ポイントの管理者パスワードを手動で変更するまで、ローカル ブラウザー UI にアクセスするには、引き続き Insight ネットワーク パスワードを使用する必要があります。

管理モードを NETGEAR Insight モードまたはウェブブラウザモードに変更するには：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。

3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。

4. **Management > Configuration > System > Basic > Management Mode]** を選択します。Management Mode（管理モード）ページが表示されます。
5. 以下のラジオボタンのいずれかを選択します：
   - **NETGEAR Insight**：アクセスポイントは、NETGEAR Insight 管理モードで機能します。
   - **Web-browser**：アクセスポイントは、Web ブラウザ管理モードで機能します。

   注意: 管理モードを Web ブラウザ モードから NETGEAR Insight モードに変更すると、IP アドレス、アクセス ポイント名、ローカル ブラウザ UI のパスワードを除いて、アクセス ポイントの構成がリセット（クリア）されます。アクセス ポイントは再起動し、SSID Netgearxxxxxx をブロードキャストします。MAC アドレスは製品ラベルに記載されています。デフォルトの WiFi パスフレーズは **sharedsecret** です。
6. **Apply** ボタンをクリックする。

   警告ポップアップウィンドウが表示されます。
7. **OK**ボタンをクリックする。

   ポップアップ ウィンドウが閉じ、設定が保存されます。アクセスポイントは新しい管理モードで再起動します。

国または地域の変更

アクセスポイントが動作する国または地域を変更できます。次の点に注意してください：

- 国がデバイスが動作する場所に設定されていることを確認します。チャンネル、電力レベル、周波数範囲について設定されている地域、地方、国の規制を遵守する責任があります。
- メニューに記載されている国または地域以外では、アクセスポイントを操作することが法律で禁止されている場合があります。メニューに記載されていない国や地域でアクセスポイントを使用する場合は、お住まいの地域の行政機関に問い合わせるか、NETGEAR の Web サイトで使用できるチャンネルを確認してください。
- 国によっては、アクセスポイントの国または地域の設定があらかじめ設定された状態で販売されており、変更できない場合があります。

国または地域を変更するには

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > System > Basic]** を選択します。

   General（全般）ページには、基本的なシステム設定が表示されます。
5. **Country / Region**メニューから国または地域を選択します。
6. **Apply** ボタンをクリックする。

   警告ポップアップウィンドウが表示されます。

7. **OK**ボタンをクリックする。

   ポップアップウィンドウが閉じ、設定が保存されます。アクセスポイントは、選択した国または地域に固有のデフォルトの WiFi および無線設定で再起動します。

管理ユーザーアカウントのパスワードを変更する

このadminユーザーアカウントのパスワードは、adminというユーザー名でアクセスポイントのローカルブラウザUIにログインする際に使用するパスワードです（WiFiアクセスに使用するパスフレーズではありません）。

パスワードの長さは8～63文字で、少なくとも1つの大文字、1つの小文字、1つの数字を含んでいなければなりません。以下の特殊文字が使用できます：

!@ # $ % ^ & * ( )

ユーザー名adminのパスワードを変更する：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > System > Advanced > User Accounts]** を選択します。表示されるページで、ユーザーアカウントを変更できます。
5. adminの隣の**Password**フィールドに新しいパスワードを入力する。
6. **Confirm Password**フィールドに、同じ新しいパスワードを入力します。

注：ユーザー名は変更できません。ユーザー名はadminのままにしてください。

7. **Apply** ボタンをクリックする。

   設定が保存されます。次にアクセス ポイントにログインするときは、新しいパスワードを使用する必要があります。新しいパスワードを忘れた場合は、アクセス ポイントを工場出荷時の設定にリセットする必要があります。そうすることで、パスワードがデフォルトの パスワードに復元されます。

システム名の変更

システム名（アクセス ポイント名、AP 名とも呼ばれる）は、アクセス ポイントの一意の NetBIOS 名です。デフォルトのシステム名は、アクセスポイントのラベルに記載されています。デフォルトのシステム名は Netgearxxxxxx で、 xxxxxx はアクセスポイントの MAC アドレスの下 6 桁の 16 進数を表します。

システム名を変更するには

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使って WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > System > Basic]** を選択します。

   General（全般）ページには、基本的なシステム設定が表示されます。
5. **System Name**フィールドに新しい名前を入力する。

以下のガイドラインに従ってください：

- 名前は英数字でなければならず、ハイフンを含むことができ、15文字より長くすることはできない。
- 名前はハイフンで始めることも、ハイフンで終わることもできない。
- 名前には少なくともアルファベットを1文字含まなければならない。

6. **Apply** ボタンをクリックします。
   設定が保存されます。

カスタムNTPサーバーの指定

デフォルトでは、アクセス ポイントはデフォルトの NETGEAR Network Time Protocol (NTP) サーバーから時刻を受信しますが、カスタム NTP サーバーを指定することもできます。

カスタムNTPサーバーを指定するには

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。
   ログインウィンドウが表示されます。

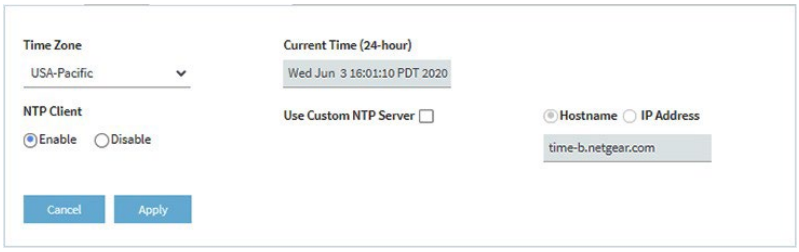
   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。

4. **Management > Configuration > System > Basic > Time**を選択します。



デフォルトでは、**[Enable]** ラジオ ボタンが選択され、アクセス ポイントはデフォルトの NETGEAR NTP サーバーから時刻を受信します。

5. **Use Custom NTP Server**チェックボックスを選択します。
6. 以下のいずれかのアクションを取る：
   - NTPサーバーのホスト名を入力します。
     デフォルトでは、「**Hostname**」ラジオボタンが選択されています。
   - **IP address**ラジオボタンを選択し、NTPサーバーのIPアドレスを入力します。
7. **Apply** ボタンをクリックする。
   設定が保存されます。アクセスポイントがインターネット経由で新しい NTP サーバーに接続すると、 ページに表示される日付と時刻は の設定に従って調整されます。
   タイムゾーンの設定については、161ページの「タイムゾーンの設定」を参照してください。

タイムゾーンの設定

アクセス ポイントの時計がネットワーク タイム プロトコル （NTP）サーバーと同期すると、ページに日付と時刻が表示されます。ページが正しい日付と時刻を表示しない場合は、タイムゾーンを設定し、サマータイム設定を調整する必要がある可能性があります。

タイムゾーンを設定し、サマータイム設定を調整する：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられているIPアドレスを入力します。
   ログインウィンドウが表示されます。
   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。

3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。

4. **Management > Configuration > System > Basic > Time**を選択します。

   表示されるページで時間設定を変更できます。

5. **Time Zone]** メニューから、アクセス ポイントが動作する地域のタイム ゾーンを選択します。

6. **Apply** ボタンをクリックする。

   設定が保存されます。アクセスポイントがインターネット経由でNTPサーバーに接続すると、ページに表示される日付と時刻が設定に従って調整されます。

   その他の時間設定については、カスタムNTPサーバーの指定（160ページ）を参照してください。

シスログ設定の管理

ネットワーク上に syslog サーバーが存在する場合、そのシステムログを syslog サーバーに送信するようにアクセスポイントを設定できます。

syslog 設定を管理し、syslog 機能を有効にする：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。

3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

ダッシュボード・ページが表示されます。

4. **Management > Configuration > System > Advanced > Syslog**を選択します。

5. syslogサーバーのIPアドレスとポート番号を指定します：
   - **Syslog Server IP Address**：ネットワーク上のsyslogサーバーのIPアドレスを入力します。
   - **Port Number**：syslogにアクセスできるポート番号を入力する。デフォルトでは、ポート番号は514です。
6. syslogサーバー機能を有効にするには、「**Enable Syslog**」チェックボックスを選択します。
7. **Apply** ボタンをクリックします。設定が保存されます。

アクセスポイントのファームウェアを管理する

アクセスポイントのファームウェアはフラッシュメモリーに保存されています。

新しいファームウェアが利用可能かどうかを確認し、アクセス ポイントを新しいファームウェアに更新できます。また、NETGEAR サポート Web サイトにアクセスして、ファームウェアをローカル コンピュータに手動でダウンロードし、アクセス ポイントを新しいファームウェアに更新することもできます。誰かが （通常、ネットワーク管理者が） ネットワーク内の安全な FTP （SFTP） サーバーに新しいファームウェアを置くと、サーバーからファームウェアを読み込んで、アクセスポイントのファームウェアをアップデートできます。

アクセスポイントへの接続方法に応じて、以下のファームウェアアップデート方法をお勧めします：

- **WiFi接続**：アクセスポイントに WiFi 接続している場合は、アクセスポイントにインターネットをチェックさせ、新しいファームウェアが利用可能かどうかを確認します。164 ページの「アクセスポイントに新しいファームウェアを確認させ、ファームウェアを更新する」を参照してください。

  この方法では、新しいファームウェアが利用可能な場合、アクセスポイントに直接ダウンロードされる。

- **LAN 接続**：アクセスポイントに LAN 接続している場合は、コンピュータまたは SFTP サーバーから手動でファームウェアを更新します。ファームウェアを手動でダウンロードしてアクセス ポイントを更新する (165 ページ)、または SFTP サーバーを使用してアクセス ポイントを更新する (168 ページ)を参照してください。

  このモードでは、新しいファームウェアが利用可能な場合、コンピュータにダウンロードしてからアクセスポイントにアップロードするか、SFTPサーバーからアクセスポイントにアップロードする必要があります。

以下のセクションでは、ファームウェアの管理方法について説明する：

- アクセスポイントに新しいファームウェアをチェックさせ、ファームウェアを更新させる
- 手動でファームウェアをダウンロードし、アクセスポイントを更新する
- バックアップファームウェアに戻す
- SFTPサーバーを使用してアクセスポイントを更新する

アクセスポイントに新しいファームウェアをチェックさせ、ファームウェアを更新させる

アクセスポイントに新しいファームウェアをチェックさせるには、アクセスポイントがインターネットに接続されている必要があります。

アクセスポイントに新しいファームウェアをチェックさせ、アクセスポイントを更新させます：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Check for Upgrade]**ボタンをクリックします。

アクセスポイントは、新しいファームウェアがあればそれを検出し、利用可能な最新バージョンを表示します。

5. リリースノートがある場合は、**Release Notes**のリンクをクリックしてください。ウェブページにリリースノートが表示されます。
6. 新しいファームウェアをダウンロードしてインストールするには、「**Upgrade Now**」ボタンをクリックし、プロンプトとダイアログボックスに従ってください。

   アクセスポイントはファームウェアを探し、ダウンロードし、アップデートを開始します。

   警告：ファームウェアが破損する危険を避けるため、アップデートを中断しないでください。たとえば、ブラウザを閉じたり、リンクをクリックしたり、新しいページを読み込んだりしないでください。アクセス ポイントの電源を切らないでください。アクセス ポイントの再起動が終了し、電源 / クラウド LED が緑色または青色で点灯したままになるまで待ちます。

   ファームウェアの更新プロセスには数分かかります。アップデートが完了すると、アクセスポイントは再起動します。

7. アクセス ポイントにログインし直して、アクセス ポイントが新しいファームウェアバージョンを実行していることを確認します。

   ファームウェアのバージョンはダッシュボードページに表示されます。
8. 新しいファームウェアのリリースノートを読んで、更新後にアクセスポイントを再設定する必要があるかどうかを判断します。

手動でファームウェアをダウンロードし、アクセスポイントを更新する

ファームウェアをローカル コンピュータにダウンロードすることと、アクセス ポイントを更新す ることは、2 つの別々の作業ですが、次の手順では組み合わせて行います。アクセスポイントを新しいファームウェアに更新した後、古いファームウェアはバックアップファームウェアとして保存され、元に戻すことができます（167ページの「バックアップファームウェアに戻す」を参照）。

注意: 古いファームウェア バージョン（またはバックアップ ファームウェア バージョン）をインス トールした場合、つまりファームウェアを更新せずにダウングレードした場合、IP アドレス、 アクセス ポイント名、ローカル ブラウザ UI のパスワードを除いて、アクセス ポイントの設定はリセット（クリア）されます。アクセスポイントは再起動し、SSID Netgearxxxxxx をブロードキャストします。MAC アドレスは製品ラベルに記載されています。デフォルトの WiFi パスフレーズは **sharedsecret** です。

ファームウェアを手動でダウンロードし、アクセスポイントを更新するには、次の手順に従います：

1. netgear.com/support/download/にアクセスし、お使いの製品のサポートページを探し、新しいファームウェアをダウンロードしてください。
2. 新しいファームウェアのリリースノートを読んで、アップグレード後にアクセスポイントを再設定する必要があるかどうかを判断します。
3. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
4. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
5. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
6. **Management > Maintenance > Upgrade > Firmware Upgrade** を選択します。

   Firmware Upgrade] ページが表示されます。
7. **Upgrade Options**メニューで「**Local**」が選択されていることを確認してください。

   ローカルがデフォルトで選択されています。
8. 以下の手順で、コンピューター上のファームウェアファイルを探し、選択します：
   a. **Browse**ボタンをクリックする。
   b. ファームウェアファイルに移動する。

      ファイル名は.tarで終わる。
   c. ファームウェアファイルを選択します。
9. **Upgrade**ボタンをクリックします。

警告：ファームウェアが破損する危険を避けるため、アップデートを中断しないでください。たとえば、ブラウザを閉じたり、リンクをクリックしたり、新しいページを読み込んだりしないでください。アクセス ポイントの電源を切らないでください。アクセス ポイントの再起動が終了し、電源 / クラウド LED が緑色または青色で点灯したままになるまで待ちます。

ファームウェアの更新プロセスには数分かかります。更新が完了すると、アクセスポイントは再起動します。

10. アクセス ポイントにログインし直して、アクセス ポイントが新しいファームウェアバージョンを実行していることを確認します。

    ファームウェアのバージョンはダッシュボードページに表示されます。

バックアップファームウェアに戻す

アクセスポイントを新しいファームウェアにアップグレードした後、古いファームウェアはバックアップファームウェアとして保存され、元に戻すことができます。

注意: バックアップ ファームウェアに戻したとき、バックアップ ファームウェアがアクセ ス ポイントで動作しているファームウェア バージョンより古いバージョンの場合、IP アドレス、アクセ ス ポイント名、ローカル ブラウザ UI のパスワードを除いて、アクセス ポイントの構成はリセッ ト（クリア）されます。アクセス ポイントは再起動し、SSID Netgearxxxxxx をブロードキャストします。xxxxxx は、アクセス ポイントの MAC アドレスの下 6 桁の 16 進数を表します。MAC アドレスは製品ラベルに記載されています。デフォルトの WiFi パスフレーズは **sharedsecret** です。

アクセスポイントのバックアップファームウェアに戻す：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

ダッシュボード・ページが表示されます。

4. **Management > Maintenance > Upgrade > Firmware Upgrade**を選択します。

   ファームウェア・アップグレード・ページが表示されます。このページには、現在のファームウェア・バージョンとバックアップ・ファームウェア・バージョンの両方が表示されます。

5. **Boot up Backup Firmware**ボタンをクリックします。

   警告ポップアップウィンドウが表示されます。

   注意: バックアップ ファームウェアに戻すと、IP アドレス、アクセス ポイント名、ローカル ブラウザ UI のパスワードを除いて、アクセス ポイントの構成がリセット (クリア) されます。アクセス ポイントは再起動し、SSID Netgearxxxxxx をブロードキャストします。xxxxxx は、アクセス ポイントの MAC アドレスの下 6 桁の 16 進数を表します。MAC アドレスは製品ラベルに記載されています。デフォルトの WiFi パスフレーズは **sharedsecret** です。

6. **Swap**ボタンをクリックする。

   ポップアップウィンドウが閉じ、ファームウェアの復帰プロセスが開始し、アクセスポイントが再起動します。

   警告：ファームウェアが破損する危険を避けるため、復帰を中断しないでください。たとえば、ブラウザを閉じたり、リンクをクリックしたり、新しいページを読み込んだりしないでください。アクセス ポイントの電源を切らないでください。アクセス ポイントの再起動が終了し、電源 / クラウド LED が緑色または青色 の点灯のままになるまで待ちます。

7. アクセス ポイントにログインし直して、アクセス ポイントがバックアップ ファームウェア バージョンを実行していることを確認します。

   ファームウェアのバージョンはダッシュボードページに表示されます。

SFTPサーバーを使用してアクセスポイントを更新する

誰か（通常はネットワーク管理者）が新しいファームウェアをネットワーク内のセキュアFTP（SFTP）サーバーに置いた場合、SFTPサーバーからファームウェアをロードして、アクセスポイントのファームウェアを更新することができます。

SFTP サーバーからアクセスポイントのファームウェアを更新する場合：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。

3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使って WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。

4. **Management > Maintenance > Upgrade > Firmware Upgrade**を選択します。

   Firmware Upgrade] ページが表示されます。

5. **Upgrade Options**」メニューから、**SFTP**を選択します。
6. 以下のサーバー設定を指定する：
   - **Firmware File**： SFTP サーバー上のアクセスポイントのファームウェアファイル名。
   - **SFTP Server IP**：ネットワーク上のSFTPサーバーのIPアドレス。
   - **User Name**：SFTP サーバーへのアクセスに必要なユーザー名。
   - **Password**：SFTPサーバーにアクセスするために必要なパスワード。
7. **Upgrade**］ボタンをクリックします。

   警告：ファームウェアが破損する危険を避けるため、アップデートを中断しないでください。たとえば、ブラウザを閉じたり、リンクをクリックしたり、新しいページを読み込んだりしないでください。アクセス ポイントの電源を切らないでください。アクセス ポイントの再起動が終了し、電源 / クラウド LED が緑色または青色で点灯したままになるまで待ちます。

   ファームウェアの更新プロセスには数分かかります。更新が完了すると、アクセスポイントは再起動します。

8. アクセス ポイントにログインし直して、アクセス ポイントが新しいファームウェアバージョンを実行していることを確認します。

   ファームウェアのバージョンはダッシュボードページに表示されます。

アクセスポイントの設定ファイルを管理する

アクセス ポイントの構成設定は、アクセス ポイント内で 構成ファイルに保存されます。このファイルをコンピュータにバックアップ（保存）したり、復元することができます。

アクセスポイントの設定をバックアップする

現在の構成設定のコピーを保存できます。必要に応じて、後で構成設定を復元できます。

注意：バックアップファイルはバイナリ形式で保存されるため、保護され、通常のアプリケーションで開くことはできません。

アクセスポイントのコンフィグレーション設定をバックアップする：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Maintenance > Upgrade > Backup and Restore > Backup**を選択します。

   Backup Settings］ページが表示されます。
5. **Backup**］ボタンをクリックします。

   ポップアップウィンドウが表示されます。

6. バックアップファイルを保護するためのパスワードを入力し、「**Continue**」ボタンをクリックします。

   既存のパスワード（アクセスポイントにログインする際に使用するパスワード）を使用するか、独自のパスワードを入力します。

   パスワードの長さは8～63文字で、少なくとも大文字1文字、小文字1文字、数字1文字が含まれていなければなりません。特殊文字は使用できません。

   注：バックアップファイルから設定を復元する場合、パスワードを再度入力する必要があるため、パスワードを保存しておくことをお勧めします。

7. ファイルをコンピュータに保存する場所を選択します。

   バックアップファイルの名前は

   `WAX6XX-NETGEARYYYYYYYY-dd-mm-yy_hh-mm-ss-config.tar`または

   `WAX6XX-WAX6XX-YYYYYY-dd-mm-yy_hh-mm-ss-config.tar`。

   6XXはモデル番号、YYYYYYはアクセスポイントのMACアドレス（またはシステム名）の下6桁の16進数、ddは日付、mmは月、yyは年、hhは時間（24時間形式）、mmは分、ssは秒を表します。

   バックアップ・ファイル名の例

   `WAX6XX-NETGEAR1A2B3C-06-18-21_16-44-12-config.tar` and

   `WAX6XX-WAX6XX-1A2B3C-06-18-21_16-44-12-config.tar`.

8. ブラウザの指示に従ってファイルを保存してください。

アクセスポイントの設定を復元する

設定ファイルをバックアップした場合は、このファイルから設定を復元できます。

バックアップしたコンフィギュレーション設定をリストアする：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入

   力します。ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

ダッシュボード・ページが表示されます。

4. **Management > Maintenance > Upgrade > Backup and Restore > Restore Settings**を選択します。

   Restore Settingsページが表示されます。

5. **Browse（参照）**ボタンをクリックし、保存した設定ファイルに移動して選択します。バックアップファイルの名前は

   `WAX6XX-NETGEARYYYYYYYY-dd-mm-yy_hh-mm-ss-config.tar`または

   `WAX6XX-WAX6XX-YYYYYY-dd-mm-yy_hh-mm-ss-config.tar`。

   6XXはモデル番号、YYYYYYはアクセスポイントのMACアドレス（またはシステム名）の下6桁の16進数、ddは日付、mmは月、yyは年、hhは時間（24時間形式）、mmは分、ssは秒を表します。

   バックアップ・ファイル名の例

   `WAX6XX-NETGEAR1A2B3C-06-18-21_16-44-12-config.tar` and

   `WAX6XX-WAX6XX-1A2B3C-06-18-21_16-44-12-config.tar`.

6. **Restore** ボタンをクリックします。

   ポップアップウィンドウが表示されます。

1. バックアップファイルの保存時に指定したパスワードを入力し、[OK]をクリックします。

   Continue」ボタンを押します。

7. **Restore** ボタンをクリックします。

   ポップアップ ウィンドウが閉じ、構成がアクセス ポイントにアップロードされます。復元が完了すると、アクセス ポイントが再起動します。このプロセスには約 2 分かかります。

   警告：ファームウェアが破損する危険を避けるため、復元を中断しないでください。たとえば、ブラウザを閉じたり、リンクをクリックしたり、新しいページを読み込んだりしないでください。アクセス ポイントの電源を切らないでください。アクセス ポイントの再起動が終了し、電源 / クラウド LED が緑または青の点灯になるまで待ちます。

ローカルブラウザのUIからアクセスポイントを再起動する

アクセス ポイントを再起動するために物理的にアクセスできない場合（つまり、電源を切断して再接続する）、ローカル ブラウザ UI を使用してアクセス ポイントを再起動できます。

アクセスポイントを再起動するには

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセス ポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management** > **Maintenance** > **Reset** > **Reboot AP]**を選択します。

   Reboot AP] ページが表示されます。
5. **Reboot AP** ボタンをクリックします。

   警告ポップアップウィンドウが表示されます。
6. **Reboot**］ボタンをクリックする。

   ポップアップウィンドウが閉じ、アクセスポイントが再起動します。

アクセスポイントの再起動をスケジュールする

例えば、アクセスポイントに接続するWiFiクライアントが1台もない（または数台しかない）場合など、ネットワークにとって都合の良い時間にアクセスポイントを再起動するようスケジュールすることができます。設定したスケジュールは、定期的なスケジュールです。

アクセスポイントの再起動をスケジュールするには

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Maintenance > Reset > Reboot AP]**を選択します。

   Reboot AP] ページが表示されます。
5. **Enable Scheduled Reboot**］ボタンをクリックして、ボタンが青く表示されるようにする。スケジューリング・コントロールが表示されます。
6. アクセス ポイントを再起動する日のチェック ボックスをオンにします。複数の日を選択できます。
7. **Start Time]**メニューを使用して、アクセス ポイントが再起動する時刻の時 と分を指定します。

   時間を24時間形式で指定する。
8. **Apply** ボタンをクリックします。設定が保存されます。

アクセスポイントを工場出荷時のデフォルト設定に戻す

アクセス ポイントを工場出荷時の設定にリセットするには、次の手順に従います。

アクセス ポイントの現在の IP アドレスがわからない場合は、アクセス ポイントを工場出荷時の設定にリセットする前に、まず IP スキャナー アプリケーションを使用して IP アドレスを検出してみてください。

注: NETGEAR Insight アプリを使用して、アクセス ポイントに割り当てられている IP アドレスを検出することも**できます。** 詳細については、26 ページの 「NETGEAR Insight アプリを使って WiFi で接続する」 を参照してください。

アクセス ポイントを工場出荷時の設定にリセットするには、アクセス ポイントの**リセット** ボタンまたはローカル ブラウザ UI のリセット機能のいずれかを使用できます。ただし、IP アドレスが見つからない場合、またはアクセス ポイントにアクセスするためのパスワードを紛失した場合は、**リセット** ボタンを使用する必要があります。

アクセスポイントを工場出荷時の設定にリセットすると、管理ユーザー名のパスワードは**password**、アクセスポイントのDHCPクライアントは有効、セットアップSSIDはNETGEARxxxxxx-SETUPの形式で表示され、WiFiアクセス のデフォルトパスワードは**sharedsecretになります**。アクセス ポイントが DHCP サーバーから IP アドレスを受信しない場合、LAN IP アドレスは 192.168.0.100 に設定されます。

工場出荷時設定の一覧については、工場出荷時設定（259 ページ）を参照してください。

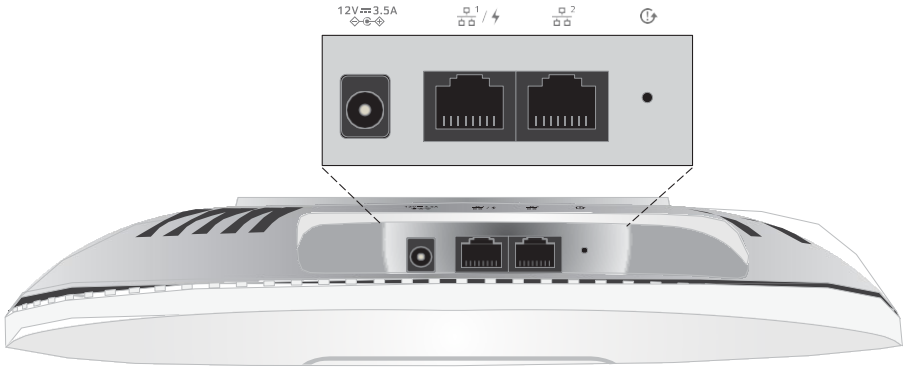
アクセス ポイントをリセットするには、[リセット] ボタンを使用します。

リセット ボタンを使用して、アクセス ポイントを工場出荷時のデフォルト設定に戻すことができます。ただし、アクセスポイントを NETGEAR Insight ネットワークロケーションに追加した場合は、[リセット**] ボタンの工場出荷時**デフォルト設定機能を使用する前に、まず Insight クラウドポータルまたは Insight アプリを使用して、Insight ネットワークロケーションからアクセスポイントを削除する必要があります。

注意：このプロセスを実行すると、アクセスポイントに設定したすべての設定が消去されます。

アクセスポイントを工場出荷時の設定にリセットするには、次の手順に従います：

1. アクセス ポイントの底部パネルで、凹型の**リセット** ボタンを見つけます。



2. まっすぐに伸ばしたペーパークリップを使い、**リセット**ボタンを少なくとも10秒間押し続けます。

   注: **[リセット]** ボタンを 10 秒未満押したまま放すと、アクセス ポイントは工場出荷時の設定に戻らず、再起動します。

3. **リセット**ボタンを離す。

   工場出荷時の設定にリセットされます。リセットが完了すると、アクセスポイントは再起動します。このプロセスには約 2 分かかります。

   警告：ファームウェアが破損する危険を避けるため、リセットを中断しないでください。アクセス ポイントの電源を切らないでください。アクセス ポイントの再起動が完了し、電源 / クラウド LED が緑色または青色 の点灯に変わるまで待ちます。

ローカルブラウザのUIを使用してアクセスポイントをリセットする

アクセス ポイントのローカル ブラウザ UI を使用して、アクセス ポイントを工場出荷時のデフォルト設定に戻すことができます。

注意：このプロセスを実行すると、アクセスポイントに設定したすべての設定が消去されます。

ローカルブラウザの UI を使用してアクセスポイントを工場出荷時の設定にリセットするには、次の手順に従います：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。

3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。

4. **Management > Maintenance > Reset > Restore Defaults]**を選択します。

   Restore Defaults（デフォルトに戻す）ページが表示されます。

5. **Restore Defaults**］ボタンをクリックします。

   警告ポップアップウィンドウが表示されます。

6. **Restore** ボタンをクリックします。

   ポップアップウィンドウが閉じ、設定が工場出荷時の設定にリセットされます。リセットが完了すると、アクセスポイントは再起動します。このプロセスには約 2 分かかります。

警告：ファームウェアが破損する危険を避けるため、リセットを中断しないでください。たとえば、ブラウザを閉じたり、リンクをクリックしたり、新しいページを読み込んだりしないでください。 アクセス ポイントの電源を切らないでください。アクセス ポイントの再起動が完了し、電源 / クラウド LED が緑色または青色 に点灯するまで待ちます。

SNMPの有効化とSNMP設定の管理

SNMPv1 または SNMPv2 プロトコルを使用して、HP OpenView などの SNMP ネットワーク管理ソフトウェアがアクセスポイントを管理できるようにします。デフォルトでは、SNMP は無効になっています。

SNMPを有効にし、SNMP設定を管理する：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Maintenance > Remote Management**］を選択します。

   リモート管理ページが表示されます。
5. SNMP **Enable**ラジオボタンを選択します。

   デフォルトでは、SNMPは無効になっています。

6. 以下の設定を行う：
   - **Read-Only Community Name**：SNMP マネージャーがアクセスポイントの MIB オブジェクトを読み取ることを許可するコミュニティ文字列。デフォルトは public です。

- **Read-Write Community Name**：SNMP マネージャーがアクセスポイントの MIB オブジェクトを読み書きできるようにするコミュニティ文字列。デフォルトは private です。
- **Trap Community Name**：トラップを受信する必要があるIPアドレスに関連付けられているコミュニティ名。デフォルトはtrap。
- **IP address (to receive traps)**：トラップを受信するSNMPマネージャーのIPアドレス。
- **Trap Port**：SNMPマネージャーがトラップを受信するポート番号。デフォルトは162。

7. **Apply** ボタンをクリックします。設定が保存されます。

LEDの管理

デフォルトでは、すべてのLEDが有効になっており、13ページの「LED付きトップパネル」の説明に従って機能します。LED が点灯するかどうかを管理できます。この機能は、アクセスポイントを暗い環境で機能させたい場合に便利です。

LEDを有効または無効にする：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > System > Advanced > LED Control**を選択します。LED Control ページが表示されます。

5. 以下のラジオボタンのいずれかを選択またはクリアします：
   - **すべてのLEDを有効にする**：すべてのLEDが有効になります。これはデフォルト設定です。
   - **すべてのLEDを無効にする**：すべてのLEDが無効になります。
   - **電源/クラウドLEDを有効にします**：電源/クラウドLEDを除くすべてのLEDが無効になります。
6. **Apply** ボタンをクリックします。設定が保存されます。

エネルギー効率モードの管理

アクセスポイントにWiFiクライアントが接続されていない場合、アクセスポイントは自動的にエネルギー効率モード（EEM）に入り、消費電力を削減してエネルギーを節約できます。1 つ以上の WiFi クライアントが接続されると、アクセス ポイントは自動的に EEM を解除して通常の動作を再開します。

EEM が有効で、WiFi クライアントがアクセス ポイントに接続されていない場合、アンテナ ストリームの動作は 1x1 に制限されます（通常の状況では、アクセス ポイントは複数のアンテナ ストリームをサポートできます）。WiFi クライアントがアクセス ポイントへの接続を開始すると、アンテナ ストリームは通常の動作を再開します。

以下の制限に注意：

- **Wireless distribution system**：EEM はワイヤレス分配システム（WDS、219 ページの WiFi ブリッジのセットアップを参照）とは相互排他的です。
- **Neighbor AP detection**：EEM は 5 GHz 無線に近隣 AP を検出させません（近隣 AP 検出の管理（125 ページ）参照）。
- **DFS channels**：WiFiクライアントがアクセスポイントに接続し、アクセスポイントが通常動作を再開すると、アクセスポイントがDFSチャネルで動作している場合、5GHz無線送信が一時的に中断されることがあります（DFSチャネルの場合は約1分間の中断、ウェザーDFSチャネルの場合は約10分間の中断）。

注記：EEMを使用する場合は、WiFiネットワークのバンドステアリングを有効にすることをお勧めします。バンドステアリングを使用すると、5GHz対応のWiFiクライアントを2.4 GHz 帯域を 5 GHz 帯域にステアリングしてパフォーマンスを向上させます。詳細については、802.11k RRM と 802.11v WiFi ネットワーク管理でバンドステアリングを有効または無効にする（83 ページ） を参照してください。

エネルギー効率モードを有効または無効にします：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > System > Advanced > Energy Efficiency Mode** を選択します。

   エネルギー効率モードページが表示されます。
5. ラジオボタンを選択します：
   - **Enable**：エネルギー効率モードが有効。
   - **Disable**：エネルギー効率モードは無効です。これはデフォルト設定です。
6. **Apply** ボタンをクリックします。

   設定が保存されます。

11

アクセス・ポイントとネットワークの監視

本章では、アクセスポイントとネットワークの監視方法について説明します。本章には、次のセクションがあります：

- アクセスポイントのインターネット、IP、およびシステム設定を表示します。
- WiFi無線設定を表示する
- 未知および既知の近隣アクセスポイントを表示
- 顧客分布、接続顧客、顧客動向を表示
- WiFiとイーサネットのトラフィック、トラフィックとARPの統計、チャネルの使用率を表示
- 追跡されたURLの表示またはダウンロード
- ログの閲覧、保存、ダウンロード、消去
- WiFiブリッジ接続の表示
- アラームと通知の表示

注：このマニュアルでは、*WiFiネットワークは*SSID（サービスセット識別子またはWiFiネットワーク名）またはVAP（仮想アクセスポイント）と同じ意味です。つまり、WiFiネットワークとは、個々のSSIDまたはVAPを意味します。

アクセスポイントのインターネット、IP、およびシステム設定を表示します。

アクセスポイント、インターネット、IP、およびシステム設定を表示します：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

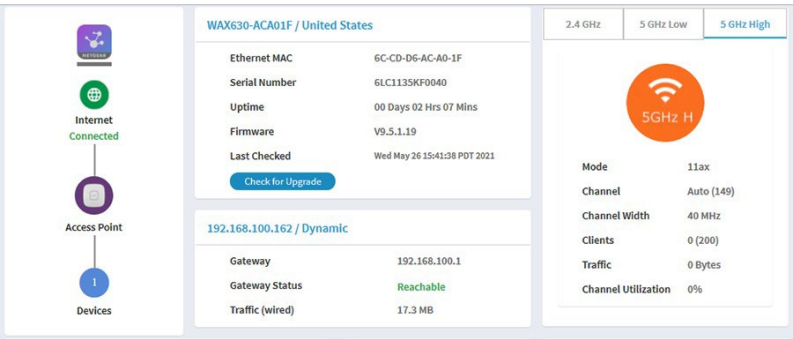
   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. 以下のダッシュボード図の左、中央上、中央下にそれぞれ表示されている「接続ステータス情報」ペイン、「システム情報」ペイン、「IP設定情報」ペインを探します。

   お使いのデバイスのページ幅が狭い場合、これらのペインはダッシュボードの別の場所に配置されることがあります。

無線設定については、WiFi 無線設定の表示（187 ページ）を参照してください。

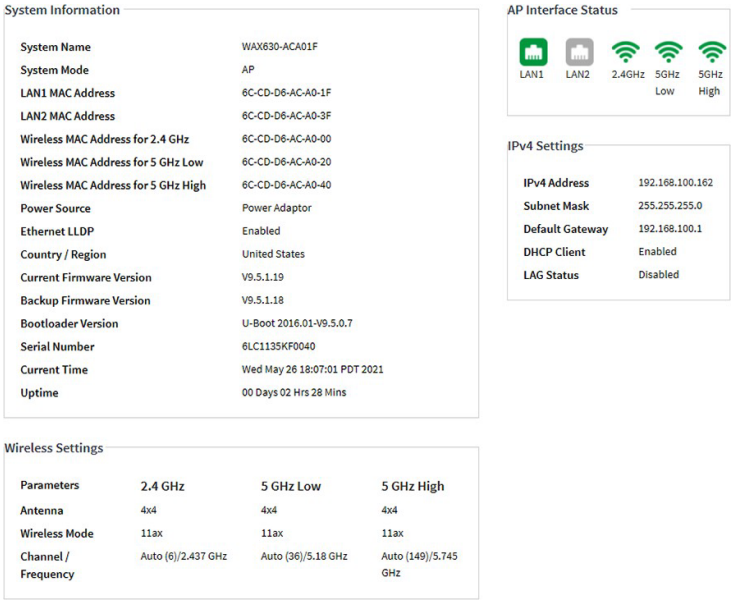


- **Connection Status Information pane**：このペインはダッシュボードの左上隅にあり（お使いのデバイスのページ幅が十分な場合：
  - NETGEAR Insight クラウドベース管理プラットフォームへの接続状態（ある場合）。
  - インターネット接続の状態。
  - アクセス・ポイントの機能モード。
  - アクセスポイントに接続されているクライアントの数。
- **System Information pane**：このペインは、ダッシュボードの上部の中央にあり（お使いのデバイスのページ幅が十分な場合、そうでない場合は他の場所にある可能性があります）、以下のように表示されます：
  - アクセス・ポイントのシステム名と運用されている国または地域。
  - イーサネットのMACアドレス。
  - シリアル番号。
  - デバイスの稼働時間。
  - ファームウェアのバージョン
  - 新しいファームウェアが利用可能かどうかをアクセスポイント自身または手動で最後に確認した日時。

  このペインには、アクセス ポイントのファームウェア アップデートを確認するためのボタンもあります。更新が利用可能な場合は、**[Update Available]** ボタンが表示されます。(ファームウェアの更新の詳細については、164 ページの「アクセス ポイントに新しいファーム ウェアを確認させ、ファームウェアを更新する」を参照してください)。

- **IP設定情報ペイン**：このペインはダッシュボード・ページの中央にあり（お使いのデバイスのページ幅が十分な場合：
  - アクセスポイントのIPアドレスとDHCPステータス。
  - ゲートウェイIPアドレス。
  - ゲートウェイの状態。
  - 有線のトラフィック量。

5. より詳細な情報を表示するには、**Management > Monitoring > System**を選択します。



ページには4つのセクションが表示される：

- **System Information section**：以下の設定が表示されます：
  - **System Name**：アクセスポイントのNetBIOS名。
  - **System Mode**：アクセスポイントのシステムモード（AP）。
  - **LAN1 MAC Address**：アクセスポイントの LAN 1 イーサネットポートの MAC アドレス。
  - **LAN2 MAC Address**：アクセスポイントの LAN 2 イーサネットポートの MAC アドレス。
  - **Wireless MAC Address for 2.4 GHz**：アクセスポイントの2.4GHz WiFi インターフェース（無線）のMACアドレス。
  - **Wireless MAC Address for 5 GHz Low**：アクセスポイントの5GHzローバンドWiFiインターフェース（無線）のMACアドレス。

- **Wireless MAC Address for 5 GHz High**：アクセスポイントの5GHz帯ハイバンドWiFiインターフェース（無線）のMACアドレス。
- **Power Source**：電源の種類（PoE 802.3bt、802.3at、または電源アダプタ）。

  PoE レベルの詳細については、247 ページの「アクセス ポイントが PoE PD として機能し、電源 / クラウド LED がオレンジに点灯したままになっている」を参照してください。
- **Ethernet LLDP**：Ethernet LLDP 機能の状態（Enabled または Disabled）。
- **Country / Region**：アクセスポイントが動作している、またはアクセスポイントがライセンスされている国または地域。
- **Current Firmware Version**：アクセスポイントで実行中のファームウェアのバージョン。
- **Backup Firmware Version**：アクセスポイントのバックアップファームウェアのバージョン。
- **Bootloader Version**：アクセスポイントにインストールされているプライマリブートローダ（U-Boot）のバージョン。
- **Serial Number**：アクセスポイントのシリアル番号。
- **Current Time**：アクセスポイントの現在のシステム時刻。
- **Uptime**：アクセスポイントが最後に再起動されてからの時間。

- **IPv4 Settings section**：緑色のアイコンは、インターフェイスが使用中であることを示します。グレーのアイコンは、インターフェイスが使用中でないことを示します。
- **IPv4 Settings section**：以下の設定が表示されます：
  - **IPv4 Address**：アクセスポイントの IPv4 アドレス。
  - **Subnet Mask**：アクセスポイントのサブネットマスク。
  - **Default Gateway**：アクセスポイントのデフォルトゲートウェイ。
  - **DHCP Client**：DHCP クライアントの状態（有効または無効）。
  - **LAG Status**：物理的な LAG 接続の有無に関係なく、LAG 機能のステータス（Enabled または Disabled）。
- **Wireless Settings section**：以下の設定が表示され、2.4 GHzと5 GHzの無線用に別々の列があります：
  - **Antenna**: アンテナの種類（デフォルトは4x4）。
  - **Wireless Mode**：無線の動作WiFiモード。
  - **Channel / Frequency**：無線が使用するチャンネルと周波数。

WiFi無線設定を表示する

アクセスポイントのWiFi無線設定を表示します：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

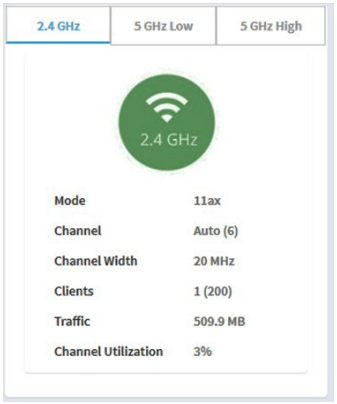
   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. ダッシュボード・ページの上部、右隅にあるラジオ情報ペインを探します（お使いのデバイスのページ幅が十分な場合。）



   以下の設定が表示されます：

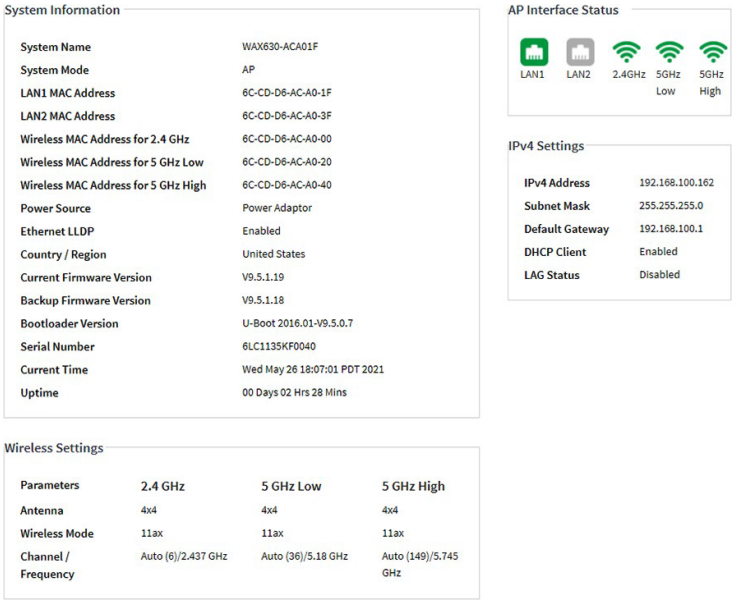
   - 無線の状態 (2.4 GHz、5 GHz Low、または 5 GHz High アイコンがグレーで表示されている場合、無線はオフになっています)
   - **Mode**：無線の動作WiFiモード
   - **Channel**：無線が使用しているチャンネル

- **Mode**：無線の動作WiFiモード
- **Channel**：無線が使用しているチャンネル
- **Channel Width**：使用しているチャンネルの帯域幅
- **Clients**：接続クライアント数、最大対応クライアント数
- **Traffic**：WiFiの通信量
- **Channel Utilization**：チャネル利用率

5. 別の無線の情報を表示するには、**2.4 GHz**、**5 GHz Low**、または **5 GHz High** タブをクリックします。

   ペインが調整される。

6. より詳細な情報を表示するには、**Management > Monitoring > System**を選択します。



ページには4つのセクションが表示される：

- **システム情報セクション**：以下の設定が表示されます：
  - **System Name**：アクセスポイントのNetBIOS名。
  - **System Mode**：アクセスポイントのシステムモード（AP）。
  - **LAN1 MAC Address**：アクセスポイントの LAN 1 イーサネットポートの MAC アドレス。
  - **LAN2 MAC Address**：アクセスポイントの LAN 2 イーサネットポートの MAC アドレス。
  - **Wireless MAC Address for 2.4 GHz**：アクセスポイントの2.4GHzの WiFiインターフェースのMACアドレス。
  - **Wireless MAC Address for 5 GHz Low**：アクセスポイントの5GHzローバンドWiFiインターフェース（無線）のMACアドレス。

- **Wireless MAC Address for 5 GHz High**：アクセスポイントの5GHz帯ハイバンドWiFiインターフェース（無線）のMACアドレス。
- **Power Source**：電源の種類（PoE 802.3bt、802.3at、または電源アダプタ）。PoE レベルの詳細については、247 ページの「アクセス ポイントが PoE PD として機能し、電源 / クラウド LED がオレンジに点灯したままになっている」を参照してください。
- **Ethernet LLDP**：Ethernet LLDP 機能の状態（Enabled または Disabled）。
- **Country / Region**：アクセスポイントが動作している、またはアクセスポイントがライセンスされている国または地域。
- **Current Firmware Version**：アクセスポイントで動作しているファームウェアのバージョン。
- **Backup Firmware Version**：アクセスポイントに搭載されているバックアップファームウェアのバージョン。
- **Bootloader Version**：アクセスポイントにインストールされているプライマリーブートローダ（U-Boot）のバージョン。
- **Serial Number**：アクセスポイントのシリアル番号。
- **Current Time**：アクセスポイントの現在のシステム時刻。
- **Uptime**：アクセスポイントが最後に再起動されてからの時間。

- **AP Interface Status**：緑色のアイコンは、インターフェイスが使用中であることを示します。グレーのアイコンは、インターフェイスが使用中でないことを示します。
- **IPv4 Settings section**：以下の設定が表示されます：
  - **IPv4 Address**：アクセスポイントの IPv4 アドレス。
  - **Subnet Mask**：アクセスポイントのサブネットマスク。
  - **Default Gateway**：アクセスポイントのデフォルトゲートウェイ。
  - **DHCP Client**：DHCP クライアントの状態（有効または無効）。
  - **LAG Status**：物理的な LAG 接続の有無に関係なく、LAG 機能のステータス（Enabled または Disabled）。

- **Wireless Settings section**：以下の設定が表示され、2.4 GHzと5 GHzの無線用に別々の列があります：
  - **Antenna**：アンテナの種類（デフォルトは4x4）。
  - **Wireless Mode**：無線の動作WiFiモード。
  - **Channel / Frequency**：無線が使用するチャンネルと周波数。

未知および既知の近隣アクセスポイントを表示

近隣のアクセスポイント (AP) 検出を有効にした場合 (「近隣 AP 検出の管理 (125 ページ)」を参照)、不明なアクセスポイントを [Unknown AP] リストに、既知のアクセスポイントを [Known AP] リストに表示できます。

検出された近隣アクセスポイントを表示するには

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

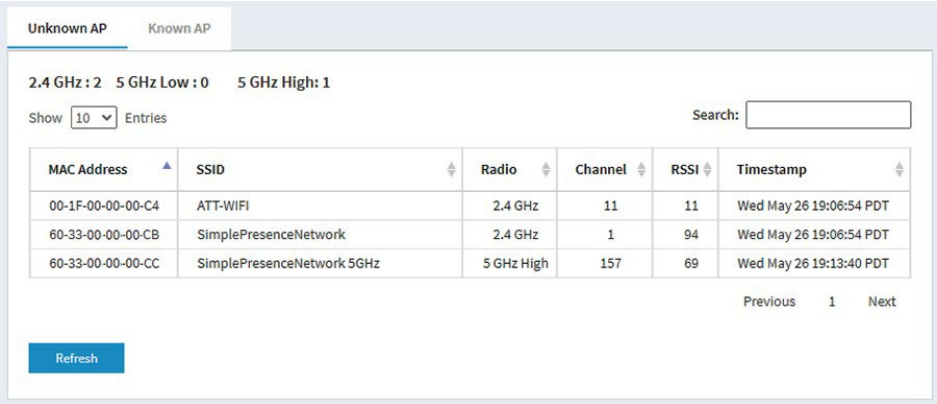
   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

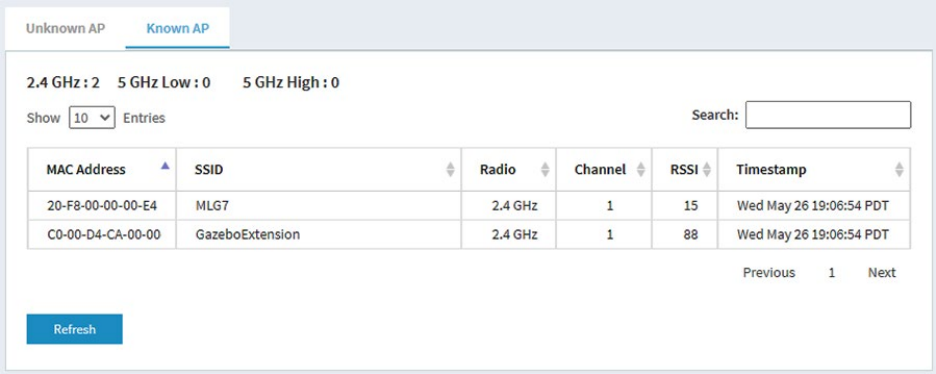
   ダッシュボード・ページが表示されます。
4. **Management > Monitoring > Neighbor AP** を選択します。



ページの上部には、各無線バンドについて、不明なアクセスポイントの総数が表示されます。

不明なアクセス ポイントを Known AP リストに移動する方法については、「近隣アクセス ポイントの検出を有効にし、アクセス ポイントを Known AP リストに移動する (126 ページ)」を参照してください。

5. 最新の不明なアクセスポイントを表示するには、[**Refresh**] ボタンをクリックします。
6. 既知の AP リストを表示するには、「**Known AP**」タブをクリックします。



ページの上部には、各無線バンドについて、 既知のアクセスポイントの総数が表示されます。

7. 最新の既知のアクセスポイントを表示するには、[**Refresh**] ボタンをクリックします。

顧客分布、接続顧客、顧客動向を表示

WiFi経由でアクセスポイントに接続しているクライアントを表示する：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

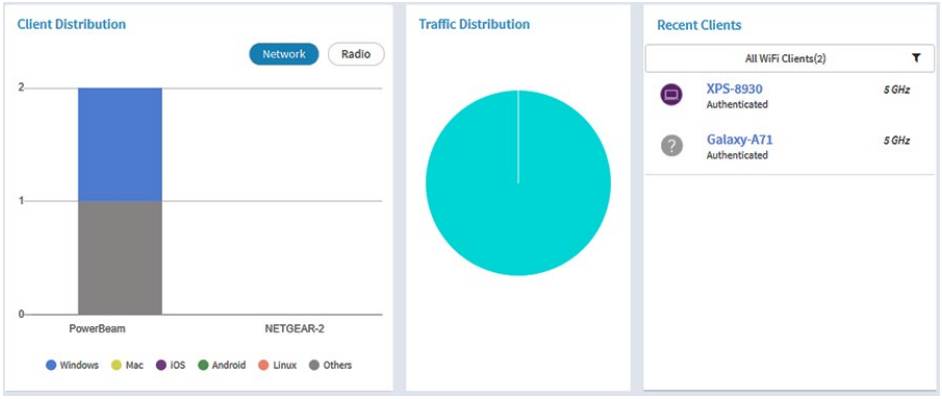
   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前に NETGEAR Insight ネットワークの場所にアクセスポイントを追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、次のように入力します。

その場所の Insight ネットワークパスワード。詳細については、26 ページの「NETGEAR Insight アプリを使って WiFi で接続する」を参照してください。

ダッシュボード・ページが表示されます。

4. **Client Distribution**ペイン（下図の左側）と最近使用した**Recent Clients**ペイン（下図の右側） を探します。



Client Distribution]ペインには、クライアントの種類（Windows、Mac、iOS、Android、Linux、その他のオペレーティングシステム）と、これらのクライアントがネットワーク上でどのように分布しているかが表示されます（デフォルトでは、[**Network**]ボタンが選択されています）。(デフォルトでは、［**Network**］ボタンが選択されています）。

Recent Clients] ペインには、最近接続したクライアントのトップ 5 が表示されます。

5. クライアントが無線にどのように分配されるかを表示するには、[Client Distribution] ペインの [**Radio]** ボタンをクリックします。

   このページは、各無線のクライアントのタイプを調整し、表示します。

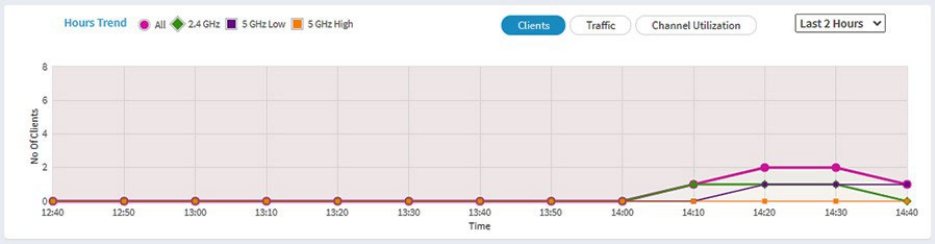
6. すべてのネットワークまたは単一のネットワークの最近のクライアントを表示するには、[Connected Clients]ペインで、[Recent Clients]の下にあるメニューのアイコンをクリックし、[**All WiFi Clients]**または特定のWiFiネットワーク（SSID）のクライアントを選択します。

   選択したクライアントの総接続数とデバイス名が表示されます。

7. 接続されているクライアントの情報を表示するには、デバイス名をクリックします。

   このページには、クライアントのMACアドレス、デバイス名、IPアドレス、SSIDが表示されます。また、非常に詳細な情報を含む、より多くの情報を表示することもできます（ステップ11とステップ12を参照）。

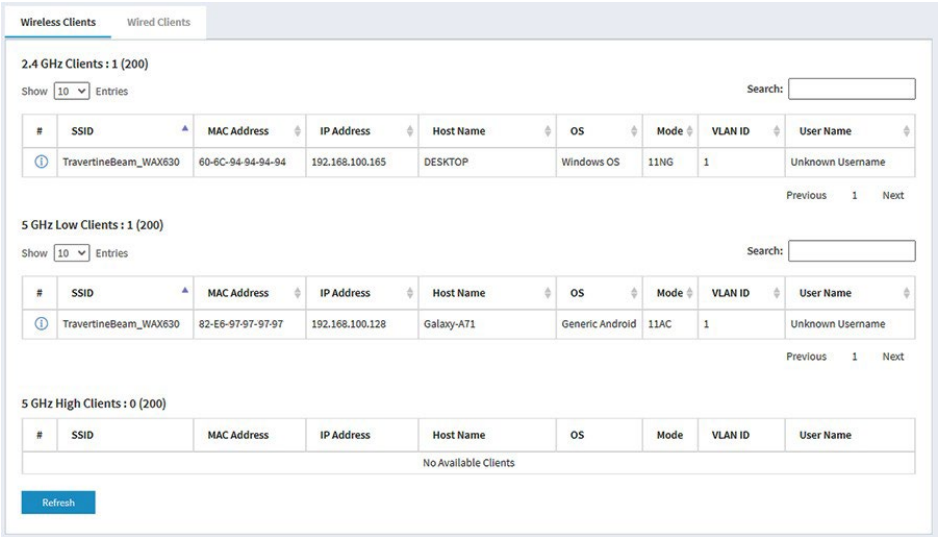
8. 顧客に関するトレンドを表示するには、「時間トレンド」ペインまでスクロールします。



Hours Trend] ペインには、クライアント数、MBps 単位のトラフィック、または選択した期間 のチャネル使用率のグラフが表示されます。(デフォルトでは、クライアント情報が選択されており（つまり、クライアントボタンが選択されている）、グラフには全無線の合計クライアント数と各無線（2.4 GHz、5 GHz Low、5 GHz High）のクライアント数が表示されます。）

Traffic] ボタンまたは **[Channel Utilization]**ボタンをクリックすることもできます。詳細については、WiFi とイーサネットのトラフィック、トラフィックと ARP の統計、およびチャネルの使用率の表示（195 ページ）を参照してください。

9. より詳細な情報を表示するには、グラフ上のいずれかの線上のノードをポイントする。
10. 情報をフィルタリングして表示する期間を変更するには、ボタンの右側にあるメニューから最近の時間数を選択します。
11. 現在接続されているクライアントに関する詳細情報を表示するには、「**Management > Monitoring > Connected Clients**」を選択します。



各無線について、ページには接続クライアント数とサポートされる最大クライアント数が表示されます。

各無線と各 WiFi クライアントについて、ページには SSID、MAC アドレス、IP アドレス、ホスト名、オペレーティングシステム（OS）、WiFi モード、VLAN ID、およびユーザー名またはキー識別子（マルチ PSK 構成の場合）が表示されます。

12. WiFiクライアントに関する非常に詳細な情報を表示するには、クライアントの左側にある情報（I）アイコンをクリックします。

    Detailed Client Information」ページが表示され、以下の情報が表示されます：

    - **MAC Address**：クライアントのMACアドレス。
    - **IP Address**：クライアントに関連するIPアドレス。
    - **Host Name**：クライアントのホスト名。
    - **OS**：クライアントで動作するオペレーティングシステム。
    - **BSSID**：クライアントが接続するBSSID。
    - **SSID**：クライアントが接続する無線のSSID。
    - **Channel**：クライアントが接続するチャンネル。
    - **Channel Width**：クライアントが接続するチャネルの幅。
    - **Tx Rate**：クライアントのトラフィック送信のレート。
    - **Rx Rate**：クライアントのトラフィック受信のレート。
    - **RSSI**： クライアントの RSSI の閾値。
    - **Tx Bytes**：クライアントが送信したバイト数。
    - **Rx Bytes**：クライアントが受信したバイト数。
    - **Type**：接続に使用されるWiFiセキュリティのタイプ。
    - **Device Type**：クライアントが持つデバイスのタイプ。
    - **Mode**：接続のWiFiモード。
    - **Status**：接続のセキュリティ状況。
    - **Idle Time**：クライアントがアイドル状態であった時間。
    - **Assoc Time Stamp**：Detailed Client Information」ページの情報に関連付けられた時間です。
    - **PMF Support**：アクセスポイントで PMF が有効な場合、クライアントが PMF をサポートしているかどうかを示します。

13. Detailed Client Informationページを開いた場合は、「**Close**」ボタンをクリックします。Detailed Client Informationページが閉じます。

14. 有線クライアントの情報を表示するには、[**Wired Clients**]タブをクリックします。

各有線クライアントについて、MACアドレス、ホスト名、IPアドレス、オペレーティングシステム（OS）が表示されます。

15. 最新の情報を表示するには、「**Refresh**」ボタンをクリックします。

WiFiとイーサネットのトラフィック、トラフィックとARPの統計、チャネルの使用率を表示

WiFiおよびイーサネット（有線LAN）のトラフィック、トラフィックおよびARP統計、チャネル利用率を表示します：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. ダッシュボードページの下部にある[Hours Trend]ペインまでスクロールダウンします。

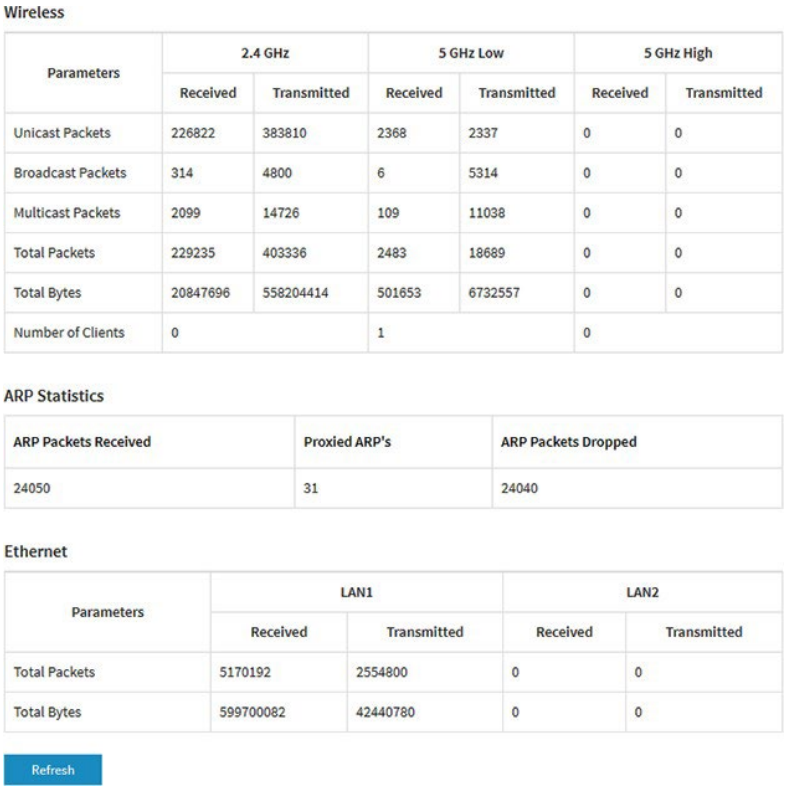
デフォルトでは「**Clients**」ボタンが選択されています。

5. トラフィック情報を見るには、次のようにする：
   a. **Traffic**］ボタンをクリックします。
      グラフは、イーサネット（有線LAN）トラフィック、WiFiトラフィックの合計、2.4GHz無線のWiFiトラフィック、および各5GHz無線のWiFiトラフィックの情報を示しています。
   b. より詳細な情報を見るには、グラフ上のいずれかの線上のノードをポイントする。

6. チャンネル使用率を表示するには、次のようにします：
   a. **Channel Utilization**］ボタンをクリックします。
      グラフは2.4GHz無線のチャンネル使用率を示しています。
   b. 5 GHz 無線のチャネル使用率を表示するには、**[5 GHz Low]** または **[5 GHz High]** ボタンをクリックします。
   c. 詳細情報を表示するには、バーをポイントする。

7. 情報をフィルタリングして表示する期間を変更するには、ボタンの右側にあるメニューから最近の時間数を選択します。

8. トラフィックの統計情報を表示するには、[**Management] > [Monitoring] > [Statistics]** を選択します。



Wireless

Parameters	2.4 GHz		5 GHz Low		5 GHz High	
	Received	Transmitted	Received	Transmitted	Received	Transmitted
Unicast Packets	226822	383810	2368	2337	0	0
Broadcast Packets	314	4800	6	5314	0	0
Multicast Packets	2099	14726	109	11038	0	0
Total Packets	229235	403336	2483	18689	0	0
Total Bytes	20847696	558204414	501653	6732557	0	0
Number of Clients	0		1		0	

ARP Statistics

ARP Packets Received	Proxied ARP's	ARP Packets Dropped
24050	31	24040

Ethernet

Parameters	LAN1		LAN2	
	Received	Transmitted	Received	Transmitted
Total Packets	5170192	2554800	0	0
Total Bytes	599700082	42440780	0	0

Refresh

このページには、アクセス ポイントが起動または再起動してから、アクセス ポイントの WiFi インターフェイスとイーサネット インターフェイスの両方のネットワークトラフィック統計が表示されます。このページには、各無線に関連付けられているクライアントの数も表示されます。

ARPプロキシが有効になっている場合(ARPプロキシの管理 (ページ235)を参照)、このページは 、プロキシされたパケット数とドロップされたパケット数を含むARP統計情報も表示します。

9. 最新の情報を表示するには、「**Refresh**」ボタンをクリックします。

トラッキングされたURLの表示またはダウンロード

WiFi ネットワークの URL トラッキングを有効にした場合 (WiFi ネットワークの URL トラッキングの有効化または無効化 (218 ページ) を参照)、URL、WiFi クライアント、SSID ごとにトラッキングされた URL を表示できます。URL トラッキングレポートを .csv ファイルとしてダウンロードすることもできます。

追跡されたURLを表示またはダウンロードするには

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

ログイン画面が表示されます。

ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。

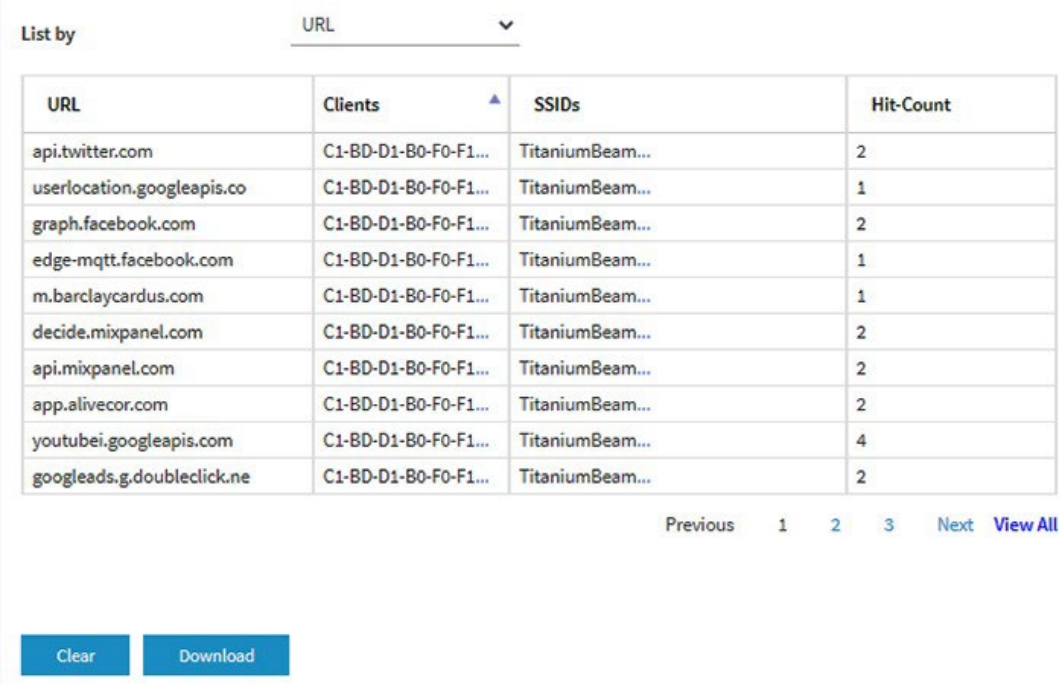
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。

4. **Management > Monitoring > URL Tracking**を選択します。



   デフォルトでは、テーブルにアクセスされたURLが表示され、それぞれURLにアクセスしたWiFiクライアントのMACアドレス、関連するSSID、およびWiFiクライアントがURLにアクセスした回数が表示されます。

5. 追加情報を表示するには、MACアドレスまたはSSIDの右にある **...** リンクをクリックします。

6. WiFiクライアント別のURLトラッキング情報を表示するには、以下のようにします：
   a. **List by** メニューから、**Client** を選択します。
      この表には、WiFiクライアントのMACアドレス、それぞれのクライアントホスト名、およびクライアントがアクセスしたURLリストの最初のURLが表示されます。
   b. WiFiクライアントがアクセスしたすべてのURLを表示するには、最初のURLの右にある **...** リンクをクリックします。
      ポップアップウィンドウには、WiFiクライアントがアクセスしたすべてのURLが表示されます。
   c. **Close**」ボタンをクリックします。
      ポップアップウィンドウが閉じる。
7. SSIDごとのURLトラッキング情報を見るには、以下のようにします：
   a. **List by**メニューから**SSID**を選択します。
      表はSSIDと、そのSSIDでアクセスされたURLのリストの最初のURLを示しています。
   b. SSIDにアクセスしたすべてのURLを表示するには、最初のURLの右にある **...** リンクをクリックします。
      ポップアップウィンドウは、SSIDでアクセスされたすべてのURLを表示します。
   c. **Close**」ボタンをクリックします。
      ポップアップウィンドウが閉じる。
8. URLトラッキングレポートを.csvファイルとしてダウンロードするには、**Download**ボタンをクリックし、ブラウザの指示に従ってください。
9. すべてのURLトラッキング情報を消去するには、以下のようにしてください：
   a. **Clear**］ボタンをクリックします。
      警告ポップアップウィンドウが表示されます。
   b. **OK**ボタンをクリックする。
      ポップアップウィンドウが閉じ、情報がクリアされます。

ログの閲覧、保存、ダウンロード、消去

アクセスポイントのアクティビティログを表示および管理できます。詳細なログファイルをダウンロードすることもできます。

注: アクセス ポイントが NETGEAR Insight 管理モードで機能する場合、クラウド アクティビティ ログも表示および管理できます。アクセス ポイントが NETGEAR Insight 管理モードで機能する場合、このオプションはダッシュボード ページから**Management > Monitoring > Cloud Logs**を選択して利用できます。

ログの表示、保存、ダウンロード、消去を行う：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセス ポイントに割り当てられている IP アドレスを入力します。

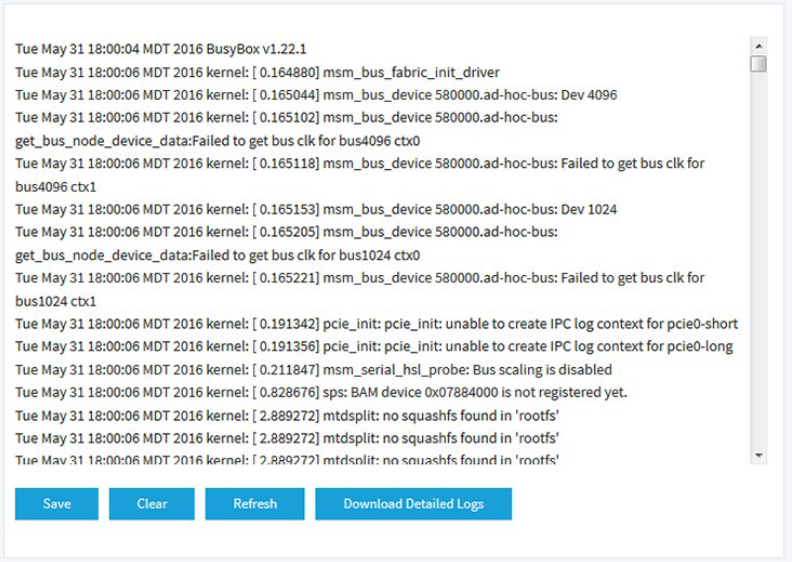
   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Monitoring > Logs**を選択します。



5. ログを保存するには、以下のようにする：
   a. **Save** ボタンをクリックします。
   b. ブラウザの指示に従ってファイルをコンピュータに保存してください。

6. 詳細なログエントリーをダウンロードするには、以下のようにする：
   a. **Download Detailed Logs**」ボタンをクリックします。
      ファイルのサイズにもよるが、詳細なログエントリーのダウンロードには数分かかる。
   b. ブラウザの指示に従ってファイルをコンピュータに保存してください。
7. 画面上のログエントリを更新するには、［**Refresh**］ボタンをクリックします。
   警告：ログ・エントリーを消去した後は、保存もダウンロードもできなくなります。
8. ログエントリをクリアするには、［**Clear**］ボタンをクリックします。

WiFiブリッジ接続の表示

2つのアクセスポイント間のポイントツーポイントWiFiブリッジ接続で構成されるワイヤレスディストリビューションシステム（WDS）を構成できます（WiFiブリッジのセットアップ（219ページ）参照）。これは、NETGEAR Insight Instant Mesh WiFi ネットワークとは異なります。

WiFiブリッジが確立されているかどうかを表示し、WiFiブリッジを形成するアクセスポイントの機能（ベースステーションまたはリピーター）、MACアドレス、およびIPアドレスを表示できます。

WiFiブリッジ接続を表示するには

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。
   ログインウィンドウが表示されます。

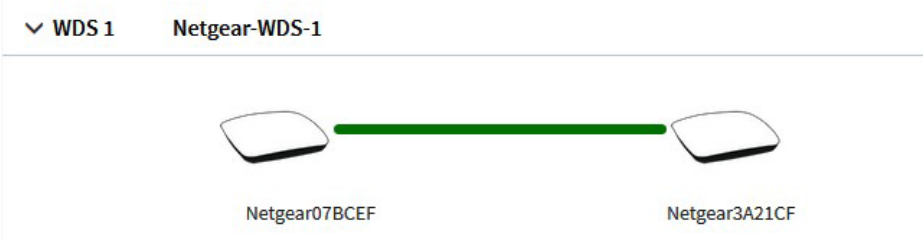
   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。
   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使って WiFi で接続する」を参照してください。

ダッシュボード・ページが表示されます。

4. **Management > Monitoring > Wireless Bridge**を選択します。

   表示されたページで WDS プロファイル（WDS 1、WDS 2、WDS 3、WDS 4）を選択できます。



5. WDS プロファイルの左にある **>** ボタンをクリックします。

6. アクセスポイントの機能、MAC アドレス、IP アドレスを表示するには、カーソルをアクセ スポイントに合わせます。

アラームと通知の表示

アラームと通知は、どのアクセス ポイント ページからでも表示できます。次の手順では、ダッシュボード ページから表示する方法を説明します。

アラームと通知を表示するには

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

ダッシュボード・ページが表示されます。

4. ページの右上にあるアラームベルのアイコンを探してください。

   アイコンには数字が表示され、前回アラームと通知を表示した時以降の新しいアラームと通知の合計数を示します。

5. アラームベルのアイコンをクリックします。

   ポップアップウィンドウには、アラーム（赤いベルで表示）と通知（青いベルで表示）が説明と時間と共に表示されます。

6. より多くのアラームと通知を表示するには、ポップアップウィンドウを下にスクロールします。

12

WiFiネットワークの高度なWiFi機能を管理する

この章では、WiFi ネットワークの高度な WiFi 機能を管理する方法について説明します。

WiFi ネットワークの基本的な WiFi 機能については、「WiFi ネットワークの基本的な WiFi 機能の管理 (59 ページ)」を参照してください。

この章には以下のセクションがある：

- アドレスとトラフィックのNATモードまたはブリッジモードの設定
- WiFiネットワークのクライアント分離を有効または無効にする
- WiFiネットワークのURLトラッキングを有効または無効にする
- WiFiネットワークのDHCPオファーメッセージのフォーマットを変更する
- WiFiネットワークのMAC ACLを選択する
- WiFiネットワークの帯域幅レート制限の設定
- WiFiネットワークの高度なレート選択を設定する

注：アクセスポイントのWiFiネットワークの設定を変更する**場合は、**新しいWiFi設定が有効になったときに切断されないように、有線接続を使用してください。

注：このマニュアルでは、***WiFiネットワークは***SSID（サービスセット識別子またはWiFiネットワーク名）またはVAP（仮想アクセスポイント）と同じ意味です。つまり、WiFiネットワークとは、個々のSSIDまたはVAPを意味します。

アドレスとトラフィックのNATモードまたはブリッジモードの設定

デフォルトでは、アクセスポイントのアドレス設定とトラフィックモードはブリッジモードで、WiFiクライアントはネットワーク内のDHCPサーバー（またはDHCPサーバーとして機能するルーター）からIPアドレスを受け取ります。これは通常、アクセスポイント自体にIPアドレスを割り当てるのと同じDHCPサーバーです。

アクセスポイントの DHCP サーバーを WiFi クライアントに有効にする NAT モードも設定できます。アクセスポイントの DHCP サーバーは、アクセスポイント自体の IP アドレスとは異なる範囲の IP アドレスを割り当てます。

NATモードと以下の機能は相互に排他的である：

- マルチ PSK（WiFi ネットワークのマルチ PSK の設定（79 ページ）参照
- 管理 VLAN (「802.1Q VLAN と管理 VLAN の設定 (139 ページ)」を参照)
- mDNS ゲートウェイ（「マルチキャスト DNS ゲートウェイの管理 (150 ページ)」を参照

アドレスとトラフィックのNATモードまたはブリッジモードを設定する：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management** > **Configuration** > **Wireless** > **Basic**を選択します。

   表示されるページでSSIDを選択できます。
5. SSIDの左にある>ボタンをクリックします。

選択したSSIDの設定が表示されます。

6. 下にスクロールし、**>Advanced**タブをクリックします。
   ページが展開します。
7. **Addressing and Traffic**メニューから、アドレッシングとトラフィックのモードを選択します：
   - **Bridge**：WiFiクライアントは、アクセスポイントと同じネットワーク内のDHCPサーバーからIPアドレスを受け取ります。これはデフォルトのモードです。
   - **NAT** ：WiFi クライアントは、アクセスポイントのプライベート DHCP アドレスプールから IP アドレスを受け取ります。このモードを選択すると、デフォルトで WLAN ネットワークアドレスは 172.31.0.0 になります。これは、WiFi クライアントに 172.31.0.2 ～ 172.31.3.254 の範囲の IP アドレスが割り当てられることを意味します。WLANのデフォルトDNSサーバーのIPアドレスは8.8.8.8です。DHCPアドレスプール、デフォルトDNSサーバー、またはその両方のデフォルト範囲を変更するには、次の手順に従います：
     a. **Network Addrerss**］フィールドに、アクセス ポイントのネットワーク アドレスとは異なるネットワーク アドレスを入力します。たとえば、アクセス ポイントの IP アドレスが 192.168.0.1 ～ 192.168.0.254 の範囲 （一般的な IP アドレスの範囲） の場合、 192.168.0.0 とは異なるネットワーク アドレスを入力します。
     b. **DNS**フィールドに、使用するDNSサーバーのIPアドレスを入力します。このIPアドレスは、前の手順で設定したWLANネットワークアドレスとは異なる必要があります。
8. **Apply** ボタンをクリックします。
   設定が保存されます。

WiFiネットワークのクライアント分離を有効または無効にする

デフォルトでは、クライアント分離はWiFiネットワーク（SSIDまたはVAP）に対して無効になっており、アクセスポイント上の同じまたは異なるWiFiネットワークに関連付けられているWiFiクライアント間の通信を許可します。セキュリティを強化するために、クライアントの分離を有効にして、同じまたは異なる WiFi ネットワークに関連付けられているクライアント同士が通信 *できないようにする*ことができます。

クライアント分離はマルチ PSK と互換性がありません。クライアント分離を有効にするには、まずマルチ PSK を無効にします（WiFi ネットワークのマルチ PSK のセットアップ（79 ページ）を参照）。

WiFiネットワークのクライアント分離を有効または無効にする：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。
   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。
   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Wireless > Basic** を選択します。
   表示されるページでSSIDを選択できます。
5. SSID の左側にある **>** ボタンをクリックします。
   選択したSSIDの設定が表示されます。
6. 下にスクロールし、**> Advanced**タブをクリックします。
   ページが展開します。
7. Wireless Client Isolation] で、次のラジオボタンのいずれかを選択します：
   - **Disable**：クライアント隔離は WiFi ネットワークでは無効です。これはデフォルト設定です。
   - **Enable**：クライアント分離が WiFi ネットワークで有効になっています。次のチェックボックスが表示されます：

   Enableラジオボタンを選択すると、2つのチェックボックスが表示されます（以下の手順を参照）。
8. **Allow Access to AP UI** チェックボックスが表示されている場合：管理者ユーザーがWiFiネットワーク経由でローカルブラウザUIにアクセスできないようにするには、［**Allow Access to AP UI**］チェックボックスをオフにします。

デフォルトでは、このチェックボックスが選択されており、管理者ユーザーがWiFiネットワーク経由でローカルブラウザUIにアクセスできるようになっています。

注：管理VLANとWiFiネットワークVLANが同一である場合（デフォルトでは同一）、WiFiネットワーク経由のアクセスを無効にしても、管理者ユーザーは常に有線ネットワーク接続経由でローカルブラウザUIにアクセスできます。

9. **Allow access to devices listed below]**チェックボックスが表示されている場合 は、以下の手順に従ってください：隔離の対象外となるネットワークデバイスを追加し、クライアントからのアクセスを許可するには、以下の手順に従います：
   a. **Allow access to devices listed below]**チェックボックスを選択します。
      デフォルトでは、このチェックボックスはオフになっています。
      許可リストが表示されます。
   b. 右側のフィールドに、クライアントがWiFiネットワーク経由で到達することを許可されるデバイスの静的IPアドレスとドメイン名を最大5つまで入力します。
      例えば、WiFiクライアントが利用できるようにしたいネットワークプリンタの静的IPアドレスやドメイン名を入力することができます。Allowlist上のドメイン名は、静的IPアドレスに解決する必要があります。
   c. **Move**］ボタンをクリックします。
      アドレスとドメイン名が許可リストに追加される。
   d. 1つ、複数、またはすべてのアドレスとドメイン名を削除するには、個々のチェックボックスまたは［**Select All**］チェックボックスを選択し、［**Remove**］ボタンをクリックします。
10. **Apply** ボタンをクリックします。
    設定が保存されます。

WiFiネットワークのURLトラッキングを有効または無効にする

アクセスポイントが、WiFi ネットワーク（SSID または VAP）に接続している WiFi クライアントから要求されたすべての URL を追跡できるようにすることができます。この機能はデフォルトでは無効になっていますが、有効にすることができます。

SSID または WiFi クライアントごとに追跡された URL を表示する方法については、追跡された URL の表示またはダウンロード（197 ページ）を参照してください。

WiFiネットワークのURLトラッキングを有効または無効にする：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。
   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。
   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management** > **Configuration** > **Wireless** > **Basic**を選択します。
   表示されるページでSSIDを選択できます。
5. SSID の左側にある **>** ボタンをクリックします。
   選択したSSIDの設定が表示されます。
6. 下にスクロールし、**>Advanced**タブをクリックします。
   ページが展開します。
7. URL Tracking」で、以下のラジオボタンのいずれかを選択します：
   - **Enable**：URL トラッキングが WiFi ネットワークで有効になっています。
   - **Disable**：WiFi ネットワークの URL トラッキングを無効にします。
8. **Apply** ボタンをクリックします。
   設定が保存されます。

WiFiネットワークのDHCPオファーメッセージのフォーマットを変更する

デバイスがWiFiネットワークにアソシエートしようとしてIPアドレスをネゴシエートすると、アクセスポイントはDHCPサーバーから受信したブロードキャストDHCPオファーメッセージをユニキャストメッセージに変換し、デバイスに転送します。これはデフォルトの設定です。DHCPメッセージの交換では、ユニキャストパケットの方が信頼性が高く、ネットワークのトラフィックを最小限に抑えることができます。

特定のWiFiネットワークでDHCPオファーメッセージをブロードキャストパケットとして配信する必要がある場合は、アクセスポイントがブロードキャストDHCPオファーメッセージをユニキャストメッセージに変換*しない*ように、そのWiFiネットワークのメッセージフォーマットを変更できます。

WiFiネットワークでDHCPオファーメッセージのフォーマットを変更するには：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Wireless > Basic**を選択します。

   表示されたページでSSIDを選択できます。
5. SSID の左側にある **>** ボタンをクリックします。

   選択したSSIDの設定が表示されます。
6. 下にスクロールし、**>Advanced**タブをクリックします。

   ページが展開します。

7. DHCP Offer Broadcast to Unicast］で、以下のラジオボタンのいずれかを選択します：
   - **Enable**：アクセスポイントは、WiFi ネットワーク内で DHCP オファーメッセージをユニキャストパケットとして転送します。これはデフォルトの選択です。
   - **Disable**：アクセスポイントは、DHCP オファーメッセージを WiFi ネットワーク内でブロードキャストパケットとして転送します。
8. **Apply** ボタンをクリックします。
   設定が保存されます。

WiFiネットワークのMAC ACLを選択する

1つまたは複数のローカルMACアクセス制御リスト（ACL、アクセスリストとも呼ばれる、118ページのローカルMACアクセス制御リストの管理を参照）を設定した後、SSIDで使用するACLを選択できます。

ACL に定義したポリシーに応じて、MAC アドレスが MAC ACL にある WiFi デバイスは、この SSID を介したアクセス ポイントへのアクセスを許可されるか、または SSID へのアクセスを拒否されます。SSID へのアクセスが拒否された場合、これらのデバイスは、その SSID に対して MAC ACL セキュリティを設定していなければ、別の SSID を介してアクセス ポイントに接続できる可能性があります。

RADIUS サーバーをセットアップして（「RADIUS サーバーのセットアップ（131ページ）」を参照）、RADIUS MAC ACL を選択することもできます。RADIUS サーバでクライアント MAC アドレスに次の形式を使用して、ACL を定義する必要があります：クライアントMACアドレスが00:0a:95:9d:68:16の場合、RADIUSサーバーで000a959d6816と指定します。

注：WiFi セキュリティが WPA2 Enterprise または WPA3 Enterprise の場合、RADIUS MAC ACL は機能しません。RADIUS MAC ACL を使用する場合は、WiFi ネットワークに別のタイプの WiFi セキュリティを選択します（WiFi ネットワークの認証と暗号化の変更 (73 ページ) を参照）。

WiFiネットワークのMAC ACLを選択する前に、ACLのポリシーを確認してください：

- **ACL policy that allows access**：ACL上のWiFiデバイスはSSIDへのアクセスを許可され、他のすべてのWiFiデバイスはSSIDへのアクセスを拒否されます。
- **ACL policy that denies access**：ACL上のWiFiデバイスはSSIDへのアクセスを拒否され、他のすべてのWiFiデバイスはSSIDへのアクセスを許可されます。

WiFiネットワークのMAC ACLを選択するには：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。
   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。
   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Wireless > Basic**を選択します。
   表示されたページでSSIDを選択できます。
5. SSID の左側にある **>** ボタンをクリックします。
   選択したSSIDの設定が表示されます。
6. 下にスクロールし、**>Advanced**タブをクリックします。
   ページが展開します。
7. **MAC ACL** チェックボックスを選択します。
8. 以下のいずれかを行う：
   - **Local MAC ACL**ラジオボタンを選択し、**Select Group**メニューから先ほど定義したMAC ACLを選択します。

     MAC ACLポリシー、ACL内のMACアドレス、またはその両方を変更するには、グループの横にあるリンクをクリックします。詳細については、ローカルのMACアクセス制御リストの管理（118ページ）を参照してください。
   - **Radius MAC ACL** ラジオボタンを選択します。
     このオプションは、RADIUSサーバーをセットアップした場合にのみ機能する（「RADIUSサーバーのセットアップ（131ページ）」を参照）。
9. **Apply** ボタンをクリックする。

設定が保存されます。

WiFiネットワークの帯域幅レート制限の設定

WiFiネットワークに接続されているデバイスのアップロードおよびダウンロード帯域幅のレート制限を設定できます。最小帯域幅レートは64 Kbpsで、最大帯域幅レートは1024 Mbpsです。アップロード帯域幅のレートとダウンロード帯域幅のレートを設定できます。

注: 帯域幅レートの制限を設定する前に、アクセスポイントのインターネット速度を確認することをお勧めします (「インターネット速度の確認 (243 ページ)」を参照)。

WiFiネットワークに接続しているデバイスの帯域幅レート制限を設定する：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Wireless > Basic**を選択します。

   表示されたページでSSIDを選択できます。
5. SSID の左側にある **>** ボタンをクリックします。

   選択したSSIDの設定が表示されます。
6. 下にスクロールし、**>Advanced**タブをクリックします。

   ページが展開します。

7. **Rate Limit**］チェックボックスを選択する。
8. 値を指定する：
   - **Upload**：アップロード帯域幅の制限には、64～1024の値を入力し、メニューから**Kbps**または**Mbps**を選択します。
   - **Download**：ダウンロード帯域幅の制限には、64～1024の値を入力し、メニューから**Kbps**または**Mbpsを選択します。**
9. **Apply** ボタンをクリックします。
   設定が保存されます。

WiFiネットワークの高度なレート選択を設定する

高度なレート選択により、*個々の*WiFiネットワーク（無線とは異なり、無線上の*すべて*のWiFiネットワークに影響する）の容量を向上させ、WiFiネットワーク内の以下のコンポーネント間の最適なバランスを達成することができます：

- トラフィックの種類（マルチキャスト、管理、制御、データトラフィック）
- 顧客の数と近さ（顧客密度）
- クライアントの種類（レガシーWiFiモードを含む、クライアントがサポートできるWiFiモード）
- クライアントのスループット速度
- WiFiネットワークがカバーしなければならないエリア

高度なレート選択をうまく設定するには、ネットワーク内のクライアントが要求できるもの（トラフィックの種類、サポートされているWiFiモード、予想されるスループット速度）、WiFiネットワークに同時に接続できる可能性のあるクライアントの数、およびクライアントの配置場所を決定することをお勧めします。

注：デフォルトでは、高度なレート選択は無効になっています。高度なレート選択を有効にすると、アクセスポイントはレートコントロール設定を通常のWiFiネットワーク内のWiFi接続に適用しますが、ワイヤレスディストリビューションシステム（WDS）またはインサイトインスタントメッシュWiFiネットワーク内の接続には適用しません。

高度なレート選択では、WiFiネットワークの2.4GHzおよび5GHz無線帯域に対して以下の設定を行うことができます：

- **Fixed multicast rate**：選択したマルチキャストトラフィックの送信レートが自動的に適用されます。選択できるレートは、無線帯域がサポートする基本的なマルチキャストレートです。
- **Rate control**：選択したレートは、ビーコンやその他の管理フレーム、および制御フレームとデータフレームに自動的に適用されます。レート制御を有効にすると、以下に説明する4つの要素からなるDensity Levelを設定できます。つまり、Density Levelには、クライアント密度（WiFi ネットワーク内のクライアントの数と近接性）以上のものが含まれます。

  WiFi ネットワークのDensity Levelの利用可能な設定は、無線が動作する WiFi モードによって異なります。WiFi モードの詳細については、無線の WiFi モードの変更 (90 ページ)を参照してください)。

  Density Levelは、0（実際には0～4の範囲、デフォルト設定）、1（1～4の範囲）、2（2～4の範囲）、3（3～4の範囲）、または4で設定できる。この設定は、次の*相互依存的な*構成要素に適用される。相互依存的な構成要素であるため、個別に正確に設定することはできない：

  - **Density**：WiFiネットワーク内のクライアントの密度（数と近さ）。(密度は、Density Level*の*4つのコンポーネントの1つです） 0の設定は、クライアント密度が非常に低いことを意味します。4 に設定すると、クライアント密度が非常に高くなります。
  - **Compatibility**：WiFiネットワーク内のレガシークライアントのWiFiモードとの互換性。0の設定は、802.11b/g/n/axクライアントとの互換性を意味します。4の設定は、802.11g/n/axクライアントとの互換性を意味しますが、802.11bレガシークライアントとの互換性はありません。
  - **Overall performance**：WiFiネットワーク内のクライアントのスループット速度。0 に設定するとパフォーマンスが低下します。4の設定は最適なパフォーマンスを意味します。例として、非常に広いカバレッジエリアが必要な場合は、意図的にパフォーマンスを低下させることができます。
  - **Coverage**：WiFiネットワークがカバーしなければならないエリア。0に設定すると非常に広い範囲をカバーします。4の設定は、非常に狭いカバーエリアを意味します。例として、最適なパフォーマンスが必要な場合は、意図的に非常に狭いエリアを選択することができます。

Density Levelを説明する別の方法は、選択されたレベルが、対応するクライアントのDensity Level、WiFiモード、最小レガシー・レート、ビーコン・レート、および最小MCS（Modulation Coding Scheme）レートにマッピングされることである。

WiFiネットワークの高度なレート選択を設定するには：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使って WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Wireless > Basic**を選択します。

   表示されるページで、SSID を選択して追加できます。
5. SSID の左側にある **>** ボタンをクリックします。

   選択したSSIDの設定が表示されます。

6. 下にスクロールし、「**Advanced Rate Selection**」タブをクリックします。

注：選択した SSID に対して、2.4 GHz、5 GHz Low、および 5 GHz High の無線帯域の無線設定を個別に指定できます。以下の手順の説明は、すべての無線に適用されます。

7. 基本的な固定マルチキャストレートを適用するには、「**Fixed Multicast Rate**」メニューから、無線帯域に応じて以下のレートのいずれかを選択します：
   - **2.4 GHz**：**1**、**2**、**5.5**、**11** Mbps、または**Auto**。(デフォルトでは、Autoは11 Mbpsです）。
   - **5 GHz Low**：**6**、**12**、**24** Mbps または **Auto**。(デフォルトではAutoが24 Mbps）。
   - **5 GHz High**：**6**、**12**、**24** MbpsまたはAuto。(デフォルトではAutoが24 Mbps）。

8. ビーコンとその他の管理フレーム、および制御フレームとデータフレームの自動最小レート制御を有効にするには、**Rate Control**チェックボックスを選択します。

   Rate Control］チェックボックスを選択すると、［**Density Level**］スライダが使用可能になります。

9. あなたの環境に合った**Density Level**を設定するには、**Density Level**スライダーを**0**、**1**、**2**、**3**、**4**に動かします。

   スライダーを動かすと、選択した**Density Level**が対応する WiFi モード、ビーコンレート、最小レガシーレート、および最小 MCS レートにマッピングされます。利用可能な設定は、無線に選択した WiFi モードによって異なります（無線の WiFi モードの変更 (90 ページ)を参照）。デフォルトでは、各無線の WiFi モードは 11ax です。

   WiFiネットワークのDensity Levelは、スライダーの位置によって設定が割り当てられ、*個別に設定することは*できない、以下の相互依存コンポーネントに基づいています：

   - **Density of the WiFi clients**：無線のデフォルト11ax WiFiモードでは、スライダーの位置に応じて、非常に低い、低い、中程度、高い、または非常に高いに設定できます。
   - **Compatibility with WiFi modes for legacy clients**：無線のデフォルト11ax WiFiモードでは、以下のように設定できます：
     - **2.4GHz**：802.11bクライアントをサポートする802.11b/g/n/ax、またはサポートしない802.11g/n/ax。
     - **5 GHz Low**：802.11a/n/ac/ax。スライダーのどの位置でも、5 GHz Low無線帯域のすべてのタイプのクライアントをサポートします。
     - **5 GHz High**：802.11a/n/ac/ax。スライダーのどの位置でも、5 GHz High無線帯域のすべてのタイプのクライアントをサポートします。
   - **Overall performance for the WiFi clients**：無線のデフォルトの11ax WiFiモードでは、スライダーの位置によって、低減、中程度、良好、非常に良好、または最適に設定できます。
   - **WiFi coverage**：線のデフォルト11ax WiFiモードでは、スライダーの位置によって、非常に狭い、狭い、平均的、広い、または非常に広い設定にすることができます。

   注：ローカルブラウザUIのヘルプテキストは、無線のWiFiモードがこれらのコンポーネントにどのように影響するか、また、これらのコンポーネントが互いにどのように依存するかについての詳細な情報を含む表を提供します。

10. **Apply** ボタンをクリックします。設定が保存されます。

13

WiFiブリッジのセットアップ

本章では、2つのアクセスポイント間でポイントツーポイントのWiFiブリッジ接続で構成されるワイヤレスディストリビューションシステム（WDS）を設定する方法を説明します。各WiFiブリッジ接続には、ブリッジを構成するアクセスポイントで設定が一致するWDSプロファイルが必要です。

WDSは、ルートが必要なNETGEAR Insight Instant Mesh WiFiネットワークとは*異なります*（「Insight Instant Mesh WiFiネットワークにアクセスポイントをインストールする（46ページ）」を参照）。

この章には以下のセクションがある：

注：エネルギー効率モードを有効にすると、WDSは使用できません。WDS を使用するには、まずエネルギー効率モードを無効にします。詳細については、「エネルギー効率モードの管理 (180 ページ)」を参照してください。

注：このマニュアルでは、***WiFi**ネットワークは*SSID（サービスセット識別子またはWiFiネットワーク名）またはVAP（仮想アクセスポイント）と同じ意味です。つまり、WiFiネットワークとは、個々のSSIDまたはVAPを意味します。

WiFiベースステーション、WiFiリピータ、WiFiブリッジの要件

アクセスポイントが有線接続でインターネットに接続されている場合、アクセスポイントはWiFiリピータとして機能する他のアクセスポイント最大4台のWiFiベースステーションとして機能することができます。また、WiFi ベースステーションとして機能する別のアクセスポイントに接続すれば、アクセスポイント自体も WiFi リピーターとして機能します。

WiFiベースステーションはインターネットに接続し、有線およびWiFiクライアントはベースステーションに接続でき、ベースステーションはWiFi信号をWiFiリピータとして機能する1つ以上のアクセスポイントに送信します。有線およびWiFiクライアントもWiFiリピーターに接続できますが、リピーターはWiFiベースステーションを介してインターネットに接続します。

次の図は、左側にWiFiベースステーション、右側にWiFiリピーターが1つあるWiFiリピーターセットアップの2つのアクセスポイントを示しています。

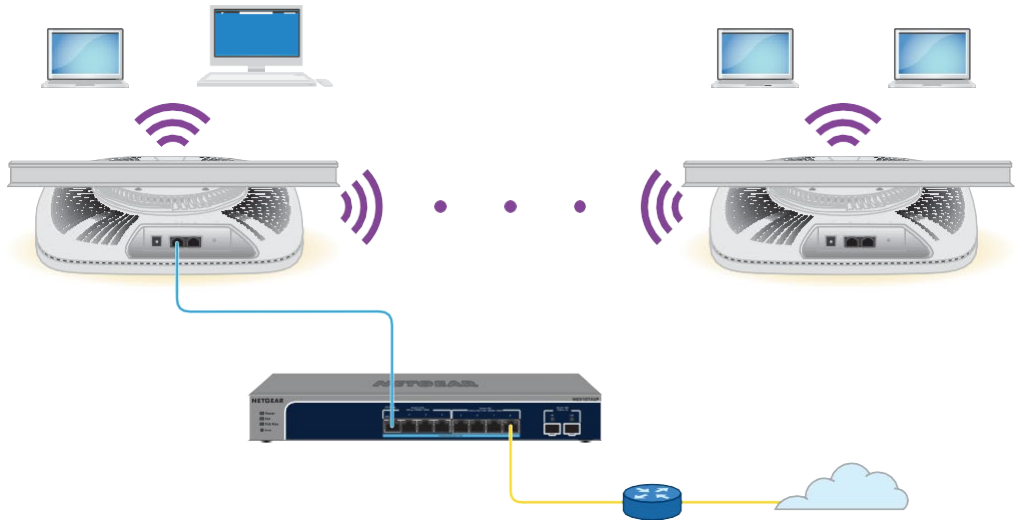


図10.5 GHz無線帯域における2つのアクセス・ポイント間のWiFiブリッジ構成

WiFiブリッジを使用するには、アクセスポイントの自動チャンネル機能を使用できず、SSIDブロードキャストを有効にする必要があります。

WiFiブリッジの場合、1つのアクセスポイントをWiFiベースステーションとして設定し、もう1つのアクセスポイントをWiFiリピーターとして設定する必要があります：

- **WiFi base station**：ベースステーションはイーサネットでネットワークスイッチ（通常はインターネット接続）に接続され、リピータとのトラフィックをブリッジします。ベースステーションはローカル WiFi と有線トラフィックも処理します。このモードを設定するには、リピータの 2.4 GHz または 5 GHz 無線の MAC アドレスを知っている必要があります。

- **WiFi repeater**：リピーターは、ローカル WiFi または有線デバイスからのすべてのトラフィックを WiFi ベースステーションに送信します。同様に、リピーターはローカル WiFi または有線コンピュータのすべてのトラフィックをベースステーションから受信します。リピーターはベースステーションへの WiFi 接続を介してネットワーク（およびインターネット）に接続されます。このモードを設定するには、ベースステーションの 2.4 GHz または 5 GHz 無線の MAC アドレスを知っている必要があります。

WDSでWiFiネットワークを設定する前に、設定が以下の条件を満たしている必要があります：

- 両方のアクセスポイントは、同じWiFiチャネルとWiFiセキュリティ設定を使用する必要があります。
- 両方のアクセスポイントが同じ LAN IP サブネット上にある必要があります。つまり、すべてのアクセスポイントのLAN IPアドレスが同じネットワーク内にあります。
- すべてのLANデバイス（有線およびWiFiコンピュータ）は、アクセスポイントと同じLANネットワークアドレス範囲で動作するように設定されています。

注: アクセスポイントをベースステーションとして使用し、NETGEAR 以外のアクセスポイントをリピーターとして使用する場合、より多くの構成設定を変更する必要がある場合があります。特に、リピーターであるNETGEAR以外のアクセスポイントのDHCPサーバー機能を無効にする必要があるかもしれません。

注意: 2 つのアクセスポイント間で WiFi ブリッジをセットアップする前に、アクセスポイントで STP を有効にし（スパニングツリープロトコルの有効化または 無効化 (142 ページ)を参照）、アクセスポイントが接続されているスイッチで STP を有効にします。スイッチが STP をサポートしていない場合、WiFi ブリッジが確立された後、ネットワークのループや接続の問題を防ぐために、アクセス ポイントの 1 つをそのスイッチから切断します。そのアクセスポイントに PoE++ スイッチを使用した場合は、電源アダプターを使用する必要があります。

アクセスポイント間にWiFiブリッジを設定する

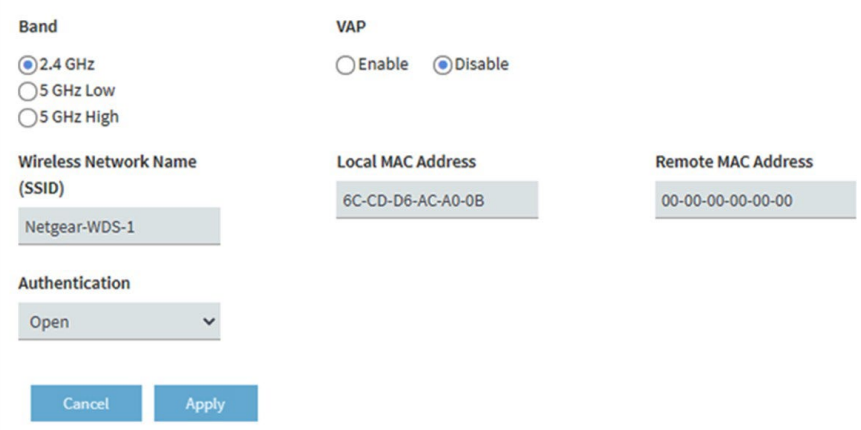
次の手順では、1 つのアクセスポイントで WiFi ブリッジ設定を行い、別のアクセスポイントでも同じ設定を行って、WiFi ブリッジを確立する方法について説明します。

2つのアクセスポイント間にWiFiブリッジをセットアップする：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。
   ログインウィンドウが表示されます。

ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。

3. アクセスポイントのユーザー名とパスワードを入力します。
   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。
   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。
   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Wireless Bridge**を選択します。
   表示されたページで WDS プロファイル（WDS 1、WDS 2、WDS 3、WDS 4）を選択できます。
5. WDSプロファイルの左にある>ボタンをクリックします。
   WDSプロファイルページが表示されます。
6. Band **2.4 GHz**、**5 GHz Low**、または **5 GHz High** ラジオボタンを選択します。
   この選択により、WDSが確立される無線バンドが決まります。デュアルバンドやトライバンドに対応していない国では、無線を選択することはできません。
7. VAP **Enable** ラジオボタンを選択します。デフォルトでは、
   WDS プロファイルは無効になっています。



8. 次の表に示すように、WDS プロファイル設定を構成します。

設定	説明
Wireless Network Name（SSID）	WDS が確立されているネットワークの WiFi ネットワーク名。デフォルト名はNetgear-WDS-xで、xはWDSの番号（1、2、3、4）です。 **注意**：WiFi ネットワーク名は、WiFi ベースステーションと WiFi リピーターで同一でなければなりません。
Local MAC Address	ローカルWDS無線インタフェースのMACアドレス、つまりWDSが確立されているローカル無線のMACアドレスです。このページでこの MAC アドレスを変更することはできません。MAC アドレスは参考のために表示されます。 WDS 接続のリモートアクセスポイントにこの MAC アドレスを入力します。
Remote MAC Address	リモートWDS無線インタフェースのMACアドレス、つまりWDSが確立されたリモート無線のMACアドレス。
Network Authentication, Data Encryption, and passphrase	デフォルトでは、メニューからの選択は「オープン」で、この場合、認証とデータの暗号化は適用されません。WDS接続を保護するために、**WPA2 Personalを選択**し、以下の設定を指定します： • **暗号化**：データの暗号化はAESで、この設定を変更することはできません。 • **Passphrase**: WDS 接続のパスフレーズ。WDS 接続を有効にするには、リモートアクセスポイントのパスフレーズがこのフィールドで定義したパスフレーズと一致する必要があります。

9. **Apply** ボタンをクリックします。
   設定が保存されます。

10. WiFiブリッジのもう一方の端にあるアクセスポイントでWiFiブリッジ設定を構成し、そのアクセスポイントを再起動します。

    注：WiFiブリッジのもう一方の端にあるデバイスがNETGEARアクセスポイントの場合、再起動する必要はないかもしれません。

    WiFiブリッジが確立される。

11. 両方のアクセスポイントの LAN 間で接続性を確認します。
    正しく設定されていれば、WiFiリピーターとして機能するアクセスポイントのWiFiまたは有線LANセグメント上のコンピュータは、インターネットに接続したり、WiFiベースステーションとして機能するアクセスポイントに接続された他のコンピュータやサーバーとファイルやプリンタを共有したりすることができます。

注：WiFiブリッジが確立された後、WiFiブリッジが確立された無線のWiFiチャンネルを変更することはできません。

14

高度な無線能の管理

この章では、アクセス ポイントの高度な無線能を管理する方法について説明します。基本無線能については、85 ページの「基本無線機能の管理」を参照してください。

注意：2.4 GHz無線の無線機能を変更した場合、その変更は2.4 GHz無線でブロードキャストするすべてのWiFiネットワークに影響します。同様に、5 GHz 無線（5 GHz ハイバンドと 5 GHz ローバンドを別々に設定できます）の無線機能を変更した場合、その変更は 5 GHz ハイバンドまたはローバンド無線でブロードキャストするすべての WiFi ネットワークに影響します。変更が 1 つの無線に固有でない場合、変更はアクセスポイント上の *すべての* WiFi ネットワークに影響します。

この章には以下のセクションがある：

- 無線の高度なWiFi設定を管理する
- 無線の最大クライアント数の管理
- 無線のブロードキャストおよびマルチキャスト設定の管理
- 無線の負荷分散を管理する
- スティッキークライアントの管理
- ARPプロキシの管理
- ブロードキャスト・トラフィック量の管理

注：無線設定を変更する場合は、新しい無線設定が有効になったときに切断されないように、有線接続を使用してください。

注：このマニュアルでは、***WiFi****ネットワーク*はSSID（サービスセット識別子またはWiFiネットワーク名）またはVAP（仮想アクセスポイント）と同じ意味です。つまり、WiFiネットワークとは、個々のSSIDまたはVAPを意味します。

無線の高度なWiFi設定を管理する

無線の高度なWiFi設定は、すべてのWiFiネットワーク（VAPまたはSSID）に適用されます。これらの設定は、ほとんどのネットワーク環境では問題なく機能し、変更する必要はほとんどありませんが、無線の設定を変更することができます。

2.4GHz、5GHzハイバンド、5GHzローバンド無線を個別に使用。

注意：これらの高度なWiFi設定は、その結果を十分に理解した上で変更することをお勧めします。設定を誤ると、アクセスポイントに接続しようとするデバイスに接続性の問題が発生する場合があります。

設定を変更するには、無線の電源が入っている必要があります。ラジオをオンにする方法については、89ページの無線のオン／オフを参照してください。

無線の高度な WiFi 設定を管理する：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

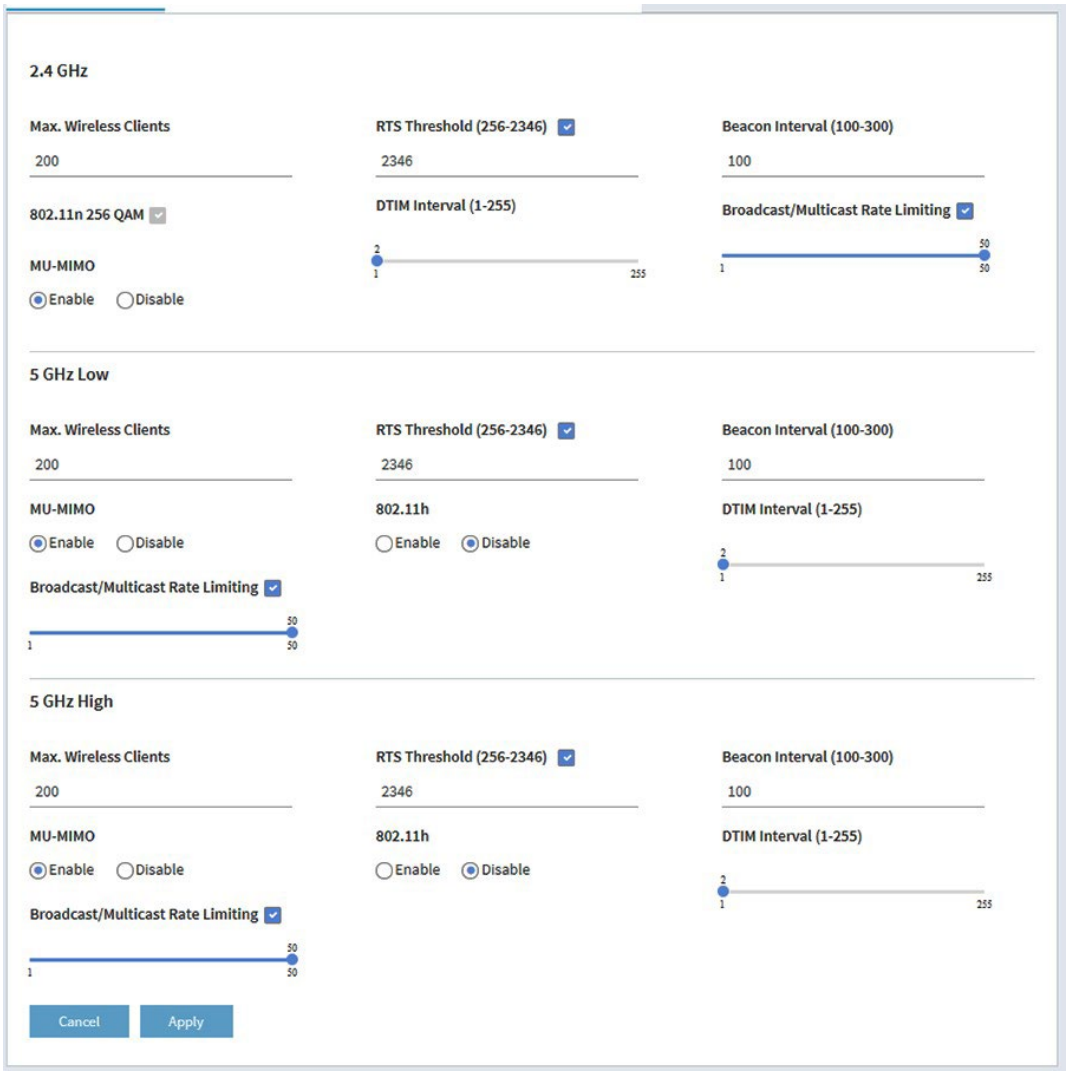
   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。

4. **Management > Configuration > Wireless > Advanced**を選択します。



5. 次の表のように設定する。

   表の説明は、すべての無線に適用されます。802.11n 256 QAM 機能のチェックボックスは、2.4 GHz 無線のみに適用されます （5 GHz 無線では、この機能は常に有効です）。802.11h 機能は、5 GHz 無線のみに適用されます。

設定	説明
Max. Wireless Clients	無線と同時にアソシエートできるWiFiクライアントの最大数を入力します。 WiFiクライアントの範囲は1～200で、デフォルトは200です。
RTS Threshold（256-2346）	送信要求（RTS）のしきい値を入力する。範囲は256から2346まで。デフォルトは2346である。 パケットサイズがRTS閾値と同じかそれ以下の場合、無線はCSMA/CD（Carrier Sense Multiple Access with Collision Detection）メカニズムを使用し、データフレームは無音期間の直後に送信されます。パケット・サイズがRTS閾値より大きい場合、システムはCSMA with Collision Avoidance（CSMA/CA）メカニズムを使用します。この状況では、送信デバイスは受信デバイスにRTSパケットを送信し、実際のパケット・データを送信する前に、受信デバイスがCTS（Clear to Send）パケットを返すのを待ちます。
Beacon Interval（100-300）	各ビーコン送信の間隔を 100 ms から 300 ms の間で入力し、無線が WiFi ネットワークを同期できるようにします。デフォルトは 100ms です。 **注**：4つ以上のWiFiネットワークを設定した場合、ビーコン間隔は自動的に300に変更されます。
802.11n 256 QAM	WiFi モードが 802.11n の場合、**802.11n 256 QAM** チェックボックスを選択すると、2.4 GHz 無線が 256-quadrature amplitude modulation (QAM) で機能するようになり、256 QAM をサポートする 802.11n クライアントの 2.4 GHz 無線スループットを向上させることができます。デフォルトでは、256 QAM は 2.4 GHz 無線では無効になっています。 デフォルトでは、256-QAMは5GHz無線で有効になっており、無効にすることはできません（このページには5GHz無線のチェックボックスはありません）。
DTIM Interval (1-255)	スライダーを動かして、配信トラフィック表示メッセージ（DTIM）間隔、またはビーコン配信トラフィック表示メッセージ期間をビーコン間隔の倍数で示すデータビーコンレートを指定します。この値は1から255の間でなければなりません。デフォルトは 2 です。
Broadcast/ Multicast Rate Limiting	マルチキャストとブロードキャストのレート制限はデフォルトで有効になっており、ネットワーク上で送信されるパケット数を制限することで、ネットワーク全体のパフォーマンスを向上させます。デフォルトでは、設定は50（可能な最大値）で、1秒間に50パケットの最大レート制限を指定します。設定を変更するには、スライダーを動かします。マルチキャストとブロードキャストのレート制限を無効にするには、小のチェックボックスをオフにします。

続き

設定	説明
MU-MIMO	デフォルトでは、「MU-MIMO **Enable**」ラジオボタンが選択され、マルチユーザーMIMO（MU-MIMO）が有効になっています。MU-MIMO を無効にするには、MU-MIMO **Disable** ラジオボタンを選択します。 MU-MIMOは、複数のユーザーが同じチャネルを使って同時にアクセスポイントからデータを受信することを可能にします。MU-MIMOでは、アクセスポイントは同じチャネルを使用して複数のクライアントに同時に送信できます。MU-MIMOはダウンストリーム方向に使用され、アクセスポイントとWiFiクライアントの両方が802.11ac Wave 2または802.11axに対応している必要があります。
802.11h	802.11h 対応の WiFi クライアントが、アクセスポイントから切り離さずに、またアクセスポイントが別のチャネルに変わるときにデータを失うことなく、自動的に新しいチャネルに切り替えることができるようにするには、802.11h **Enable** ラジオボタンを選択します。デフォルトでは、802.11h **Disable ラジオボタンが**選択され、802.11h は無効になっています。 802.11h は、5 GHz 無線では有効または無効にできますが、2.4 GHz 無線では無効です。

6. **Apply** ボタンをクリックする。
   警告ポップアップウィンドウが表示されます。

7. **OK**ボタンをクリックする。
   ポップアップウィンドウが閉じ、設定が保存されます。無線が再起動し、WiFiクライアントが再接続する必要がある場合があります。

無線の最大クライアント数の管理

無線との接続を許可するクライアントの数は、WiFi接続の信頼性とスループットに影響します。数が少なければ信頼性とスループットが向上し、多ければ信頼性とスループットが低下します。

デフォルトでは、1つの無線で最大200のクライアントの関連付けが可能です。これより少ない数のクライアントを指定することもできる。関連付けられたクライアントの数が指定した最大数を超えると、無線はその最大数を下回るまで新しいクライアントの関連付けを拒否します。

無線の最大クライアント数を管理する：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Wireless > Advanced**を選択します。

   ワイヤレス設定] ページが表示されます。
5. 無線の **Max.Wireless Clients** フィールドに、無線と同時にアソシエートできる WiFi クライアントの最大数を入力します。

   WiFiクライアントの範囲は1～200で、デフォルトは200。
6. **Apply** ボタンをクリックする。

   警告ポップアップウィンドウが表示されます。
7. **OK**ボタンをクリックする。

   ポップアップウィンドウが閉じ、設定が保存されます。無線が再起動し、WiFiクライアントが再接続する必要がある場合があります。

無線のブロードキャストおよびマルチキャスト設定の管理

マルチキャストとブロードキャスト・トラフィックはWiFiネットワークのスループットとレイテンシーに悪影響を与える可能性があるため、無線のマルチキャストとブロードキャストのレート制限設定を変更することができます。

デフォルトでは、マルチキャストとブロードキャストのレート制限が有効になっており、ネットワークを介して送信されるパケット数を制限することで、ネットワーク全体のパフォーマンスを向上させます。デフォルトでは、設定は50（可能な最大値）で、1秒間に50パケットの最大レート制限を指定します。この数値を下げることもできます。

無線のブロードキャストとマルチキャストの設定を管理する：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Wireless > Advanced > Wireless Settings**を選択します。ワイヤレス設定] ページが表示されます。
5. マルチキャストおよびブロードキャストレート制限の設定を変更するには、無線の Broadcast/Multicast Rate Limiting で、以下のいずれかの操作を行います：
   - レート制限の設定を変更するには、スライダーを動かします。デフォルトでは、設定は50（可能な最大値）であり、これは最大レート制限を毎秒50パケットに指定します。
   - マルチキャストとブロードキャストのレート制限を無効または有効にするには、小のチェックボックスをクリアまたは選択します。
6. **Apply** ボタンをクリックする。

   警告ポップアップウィンドウが表示されます。
7. **OK**ボタンをクリックする。

   ポップアップウィンドウが閉じ、設定が保存されます。無線が再起動し、WiFiクライアントが再接続する必要がある場合があります。

無線の負荷分散を管理する

無線利用率のしきい値を設定することで、クライアントがWiFiネットワークに接続したり、接続を解除したりする際に、各無線がWiFiネットワークの速度とパフォーマンスを維持できるようになります。

ロードバランシングを有効にすると、クライアントのアソシエーションは、無線ごとのクライアントの最大数、無線ごとのチャネル負荷、および各クライアントの受信信号強度インジケータ（RSSI）に依存します。無線の使用率が定義されたロードバランシング設定内にある場合、新しいクライアントのアソシエーションが許可されます。無線の使用率が定義された負荷分散設定を超えた場合、無線の使用率が定義された負荷分散設定内に収まるまで、新しいクライアントの関連付けは一時的に停止されます。

注：ダッシュボード・ページは、無線ごとのクライアントおよびトラフィック分布、ならびに無線ごとのクライアント、トラフィック、およびチャネル利用率に関する情報を表示できます（クライアント分布、接続クライアント、およびクライアント・トレンドの表示（191ページ）、およびWiFiおよびイーサネット・トラフィック、トラフィックおよびARP統計、およびチャネル利用率の表示（195ページ）を参照）。

デフォルトでは、以下のすべてのタイプのロードバランシングが、デフォルト設定で有効になっている：

- **Load balancing based on the maximum number of clients**：アクセスポイントは、指定された最大クライアント数までクライアントの関連付けを許可します。最大数を超えると、新しいクライアントは拒否されます。これはグローバル設定ですが、無線ごとに実装されます。
- **Load balancing based on the channel load**：アクセス・ポイントは、定義された最大チャネル利用率までクライアントの関連付けを許可します。最大チャネル使用率を超えると、新しいクライアントは拒否されます。これはグローバル設定ですが、無線ごとに実装されます。

  注：クライアントが拒否されてもしつこくアソシエーションしようとした場合、アクセスポイントはそのクライアントにアクセスを許可します。
- **Load balancing based on the RSSI of the client**：定義された最小値以上の RSSI を持つクライアントは、アクセスポイントとのアソシエーションを許可されます。定義された最小値以下の RSSI を持つクライアントは拒否されます。これはグローバル設定ですが、無線ごとに実装されます。

  注：クライアントが拒否されてもしつこくアソシエーションしようとした場合、アクセスポイントはそのクライアントにアクセスを許可します。

ロードバランシングの各タイプのデフォルト設定を変更したり、1つまたは複数のタイプのロードバランシングを完全に無効にすることができます。

無線のロードバランシングを管理する：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

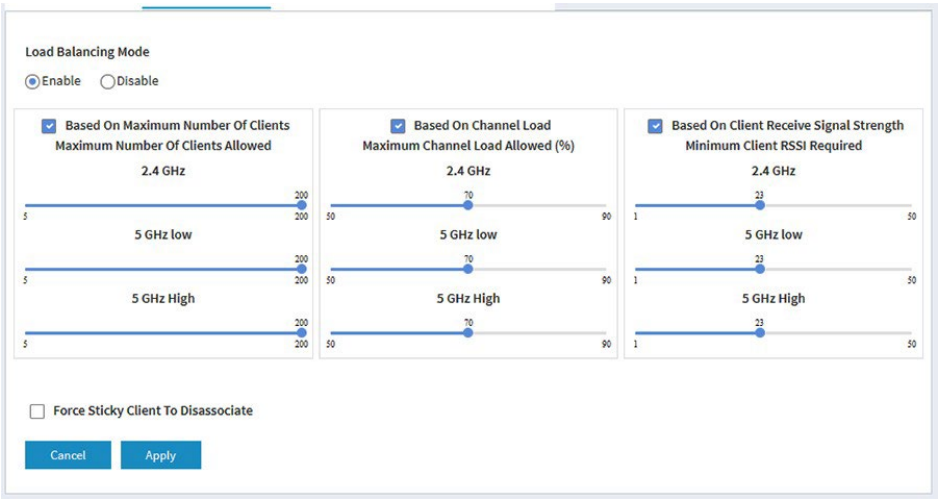
   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Wireless > Advanced > Load Balancing**を選択します。



5. 無線のロードバランシングをグローバルに有効にするには、Load Balancing Modeラジオボタンを**有効にする**。

   このページでは、ロードバランシングの各タイプと各無線のスライダーを調整し、表示します。

デフォルトでは、ロードバランシングは無効になっている。ロードバランシングを有効にすると、3種類すべてのロードバランシングが有効になります。1つまたは複数のタイプのロードバランシングを個別に無効にすることができます。

6. 1つまたは複数のタイプのロードバランシングを個別に有効または無効にするには、以下のようにする：
   - 特定のタイプのロードバランシングを無効にするには、*Based On*テキストの左にある小さな青いチェックボックスをオフにします。
   - 特定のタイプのロードバランシングを有効にするには、*Based On*テキストの左にある小さな青いチェックボックスを選択します。
7. ロードバランシング設定を変更するには、以下のようにする：
   - **Based On Maximum Number Of Clients**：各無線について、関連するスライダーを動かして、無線が新しいクライアントの関連付けを受け付けなくなるまでに許可されるクライアントの最大数を指定します。

     各無線について、クライアントの最小数は5、最大数は200であり、デフォルトは200である。
   - **Based On Channel Load**：各無線について、関連するスライダーを動かして、新しいクライアントのアソシエーションを受け付けなくなる前に、無線で許容されるチャネル負荷の最大割合を指定します。

     各無線について、チャンネル負荷の最小パーセンテージは50、最大パーセンテージは90、デフォルトのパーセンテージは70である。
   - **Based on Channel Receive Signal Strength**：各無線について、関連するスライダを動かして、個々のクライアントに必要な最小 RSSI 値を指定します。

     各無線について、RSSIの最小値は1、最大値は50、デフォルト値は23である。
8. **Apply** ボタンをクリックします。

   設定が保存されます。

スティッキークライアントの管理

ローミング中、スティッキー・クライアントは、より良い信号のアクセス・ポイントに変更せず、そのアクセス・ポイントへの接続品質が低下しているにもかかわらず、最初のアクセス・ポイントに関連付けられたまま（つまり、*スティッキー・クライアント*）である。このような状況は、そのアクセスポイントに関連付けられている他のクライアントに遅延を引き起こします。

注：アクセスポイントが1つのホームWiFiネットワークでは、ローミング中に他のアクセスポイントが利用できないため、スティッキークライアントは便利です。複数のアクセスポイントを持つビジネスまたは企業ネットワークでは、スティッキークライアントはWiFiリソースの消耗を引き起こす可能性があります。

この設定により、アクセスポイントの無線からスティッキークライアントを強制的に切り離すことができます。

クライアントのRSSIに基づくロードバランシングが有効になっている場合（「無線のロードバランシングを管理する（231ページ）」を参照）、クライアントが強制的に切断された後、クライアントは以下の状況で再び参加できます：

- クライアントは、RSSIが最低必要RSSI以上であれば、再度アソシエートすることができる。
- クライアントがしつこくアクセスポイントとのアソシエーションを試みる場合、アクセスポイントは、そのクライアントのRSSIが最低必要RSSIを下回っていても、そのクライアントへのアクセスを許可する。

スティッキークライアントを管理する：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。ダッシュボード・ページが表示されます。
4. **Management] > [Configuration] > [Wireless] > [Advanced] > [Load Balancing]** を選択します。Load Balancing] ページが表示されます。
5. **Force Sticky Clients To Disassociate]** チェックボックスをオンまたはオフにします。

   チェックボックスを選択すると、スティッキークライアントはラジオから強制的に解除されます。チェックボックスをオフにすると、スティッキークライアントは無線に関連付けられたままになります。
6. **Apply** ボタンをクリックする。

設定が保存されます。

ARPプロキシの管理

デフォルトでは、 ARP プロキシがアクセスポイントで有効になっているため、アクセスポイン トはクライアントのすべての ARP ブロードキャストパケットを検査できます。このようにすると、アクセスポイントはクライアントの ARP 要求に応答し、 無線の不必要なブロードキャストトラフィックを防ぐことができます。

プロキシされたパケット数およびドロップされたパケット数を含む ARP 統計については、WiFi およびイーサネットトラフィック、トラフィックおよび ARP 統計、およびチャネル利用率の表示（195 ページ）を参照してください。

ARPプロキシを管理する：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Configuration > Wireless > Advanced > ARP Proxy]**を選択します。ARP Proxy] ページが表示されます。
5. 以下のラジオボタンのいずれかを選択します。
   - **Enable**：ARPプロキシが有効になっている。これはデフォルト設定である。
   - **Disable**：ARP プロキシは無効です。無線のブロードキャストトラフィックが増加する可能性があります。
6. **Apply** ボタンをクリックします。

   設定が保存されます。

ブロードキャスト・トラフィック量の管理

アクセスポイントは、無線上のブロードキャストトラフィックを削減するブロードキャスト拡張機能をサポートしているため、アクセスポイントに設定するすべてのWiFiネットワークでブロードキャストトラフィックを削減できます。

ブロードキャスト機能拡張は、アクセスポイントが両方の 5 GHz 無線で合わせて 20 未満のクライアントをホストし、2.4 GHz 無線で 10 未満のクライアントをホストすると予想される場合にのみ有効にすることをお勧めします。デフォルトでは、ブロードキャスト機能は無効になっています。

ブロードキャスト機能拡張には以下の制限がある：

- 20台以上のクライアントがWiFiネットワークに接続されている場合、ブロードキャスト機能拡張はそのWiFiネットワークでは機能しません。
- アクセスポイントがワイヤレスディストリビューションシステム（WDS）またはInsight Instant Mesh WiFiネットワークで機能する場合、ブロードキャストエンハンスメントは機能しません。

ブロードキャスト管理を強化する：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。ダッシュボード・ページが表示されます。
4. **Management** ＞ **Configuration** ＞ **Wireless** ＞ **Advanced** ＞ **Broadcast Enhancements**を選択します。

   Broadcast Enhancements］ページが表示されます。
5. 以下のラジオボタンのいずれかを選択します。
   - **Enable**：ブロードキャスト機能拡張が有効。

- **Disable**：ブロードキャスト拡張機能を無効にする。これはデフォルトの設定です。

6. **Apply** ボタンをクリックします。
   設定が保存されます。

15

診断とトラブルシューティング

この章では、WiFi パケットをキャプチャして、アクセスポイントとネットワークのトラブルシューティングを行う方法について説明します。

この章には以下のセクションがある：

注：このマニュアルでは、*WiFiネットワークは*SSID（サービスセット識別子またはWiFiネットワーク名）またはVAP（仮想アクセスポイント）と同じ意味です。つまり、WiFiネットワークとは、個々のSSIDまたはVAPを意味します。

pingテストの実行

アクセスポイントからデバイスまたはネットワークの場所の IP アドレスを ping して、ping テストの結果を表示できます。

pingテストを行うには

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

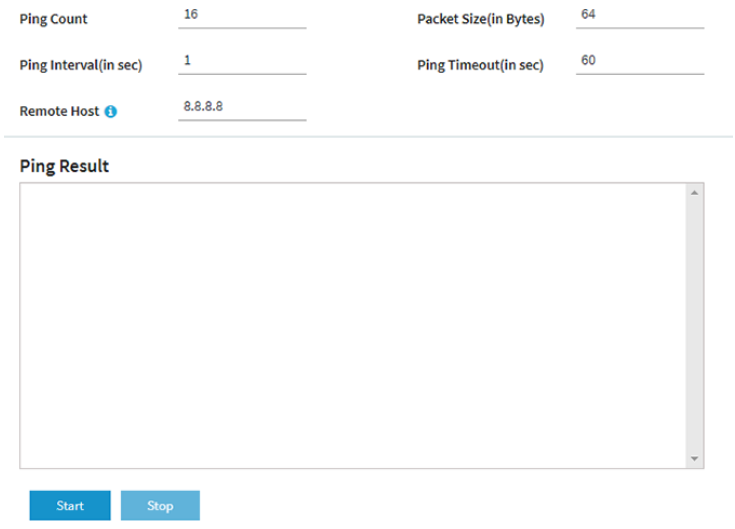
   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management > Diagnostics > Ping Test**を選択します。



5. 以下の表で説明されている設定を指定します。

設定	説明
Ping Count	アクセスポイントが送信しなければならない Ping の数。デフォルト 値は 16 。
Packet Size (in Bytes)	各pingパケットのサイズ。　デフォルトのサイズは64バイトです。
Ping Interval（in sec）	Pingの間隔。デフォルトの間隔は1秒です。
Ping Timeout (in sec)	Pingがタイムアウトする時間。デフォルトは60秒。
Remote Host	アクセスポイントが ping を送信するIP アドレス。

6. Pingテストを開始するには、[**Start]**ボタンをクリックします。
   Pingテストの結果がPing Resultフィールドに表示される。
7. pingカウントに達する前に、またはpingがタイムアウトする前にpingテストを停止するには、[**Stop]**ボタンをクリックします。

WiFiとイーサネットのパケットをキャプチャ

アクセスポイントが送受信するWiFiやイーサネットのパケットをキャプチャし、キャプチャしたパケットを含むファイルをパソコンに保存することができます。パケットキャプチャ中は、アクセスポイントの通常の機能に影響はありません。

パケットキャプチャ機能は、WiFi配備の分析、WiFiネットワークの監視、プロトコルのデバッグ、WiFiネットワークのボトルネックの決定、および一般的にWiFiネットワークのあらゆる不規則性のトラブルシューティングに役立ちます。

すべてのパケットをキャプチャするか、選択したパケットのみをキャプチャするかを選択できます。

注：キャプチャしたパケットを表示するには、.pcapを開くことができるアプリケーションが必要です。
ファイルである。

パケットをキャプチャする：

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。
   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。

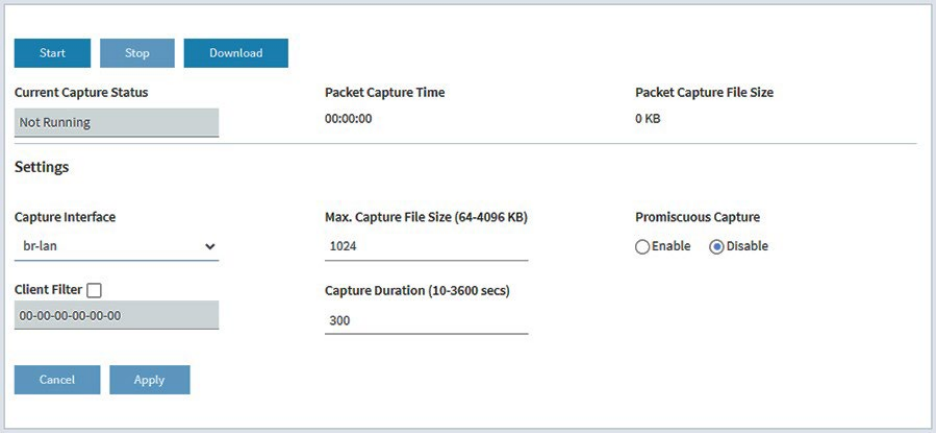
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。

4. **Management > Diagnostics > Packet Capture**を選択します。



5. 以下の表で説明されている設定を指定します。

設定	説明
Capture Interface	**Capture Interface**メニューから、パケットをキャプチャするインターフェイスを以下の中から1つ選択する： • **br-lan**。すべてのパケット、つまり、イーサネット・インターフェイス、2.4GHz無線、5GHzローバンド無線、5GHzハイバンド無線のパケットがキャプチャされる。これはデフォルトの設定です。 • **bond0**。両方のイーサネット・インターフェースがLAGでボンディングされている場合、両方のインターフェースのパケットがキャプチャされる。 • **Eth0**。LAN 1 イーサネットインターフェースのパケットのみがキャプチャされます。 • **radio1**.2.4GHz無線のパケットのみがキャプチャされる。 • **radio2**.5GHz帯ローバンド無線のパケットのみがキャプチャされる。 • **radio2**.5GHz帯ハイバンド無線のパケットのみがキャプチャされる。
Max. Capture File Size (64-4096 KB)	パケットをキャプチャしたファイルの最大サイズを入力します。64～4096KBの範囲で設定できます。デフォルトは1024 KBです。

続き

設定	説明
Promiscuous Capture	アクセスポイントがプロミスキャスモードでパケットをキャプチャできるようにするには チェックボックスを**Enable]にする。**デフォルトでは、プロミスキャス・モードは無効になっている。 プロミスキャスモードでは、無線は、アクセスポイント宛でないトラフィックも含め、チャネル上のすべてのトラフィックを受信する。無線がプロミスキャスモードで動作している間は、関連するクライアントにサービスを提供し続けます。アクセスポイント宛でないパケットは転送されません。キャプチャプロセスが停止すると、無線または無線は非プロミスキャスモードに戻ります。
Client Filter	特定のクライアントのパケットのみをキャプチャするには、[**Client Filter]** チェックボックスを選択し、[**Client Filter MAC Address]** フィールドにクライアントの MAC アドレスを入力します。
Client Filter MAC Address	**Client Filter**］チェックボックスを選択した場合は、クライアントの MAC アドレスを入力して、選択したインターフェイス上の特定のクライアントのパケットのみをキャプチャします。 MACアドレスは、各オクテットをハイフンで区切った16進数形式で入力する必要があります（例：00-11-22-33-44-55）。
Capture Duration（10～3600秒）	キャプチャプロセスの最大継続時間（つまり、[停止]ボタンをクリックしない場合）を入力します。 範囲は10秒から3600秒です。デフォルトでは最大時間は300秒です。

6. パケットキャプチャプロセスを開始するには、[**Start]**ボタンをクリックします。
   キャプチャされたパケットがすでにアクセスポイントに保存されている場合は、パケットキャプチャプロセスが古い情報を上書きすることを許可するよう促されます。
7. パケットキャプチャプロセスを停止するには、**Stop**ボタンをクリックします。
   手動でプロセスを停止しない場合、キャプチャ継続時間を超えるとプロセスは自動的に停止されます。
8. キャプチャしたパケットを含むファイルをダウンロードするには、以下のようにする：
   a. **Download**ボタンをクリックしてください。
   b. ブラウザの指示に従ってファイルをコンピュータに保存してください。
9. ページに最新の情報を表示するには、「**Refresh**」ボタンをクリックします。

インターネットの速度をチェックする

アクセスポイントのインターネット速度を確認できます。この結果は、帯域幅レートの制限を設定する場合 に役立ちます（「WiFiネットワークの帯域幅レート制限を設定する（213ペー ジ）」を参照）。

インターネットの速度をチェックするには

1. アクセスポイントと同じネットワークに接続されているコンピュータから、またはイーサネットケーブルまたはWiFi接続を介してアクセスポイントに直接接続されているコンピュータから、Webブラウザを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。

   ログインウィンドウが表示されます。

   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳細については、45ページの「ブラウザのセキュリティ警告が表示された場合の対処法」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**。パスワードは指定したもの。ユーザー名とパスワードは大文字と小文字を区別します。

   以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   ダッシュボード・ページが表示されます。
4. **Management** > **Diagnostics** > **Speed Check**を選択します。

   Internet Speed Check] ページが表示されます。
5. プライバシーポリシーを表示するには、「**Privacy Policy**」リンクをクリックします。

   Privacy Policy」ポップアップウィンドウが表示されます。
6. ポップアップ・ウィンドウを閉じるには、右上の**×**印をクリックします。
7. **Test Speed**ボタンをクリックします。

   しばらく待つと、測定された待ち時間（ms）、ダウンロード速度（Mbps）、アップロード速度（Mbps）が表示されます。
8. テストの履歴を表示するには、「**View History**」リンクをクリックします。

   以前のテスト結果が表に表示されます。

WiFiトラブルシューティングの簡単なヒント

1つまたは複数のWiFiネットワークが正常に機能しない場合は、アクセスポイントの電源を入れ直すことを検討してください：

1. アクセスポイントからネットワークスイッチへのイーサネットケーブルを抜きます。
2. 電源アダプタを使用している場合は、アクセスポイントからアダプタを取り外します。
3. アクセスポイントからネットワークスイッチにイーサネットケーブルを差し込みます。2分間待ちます。
4. 電源アダプタを使用する場合は、電源アダプタをアクセスポイントに接続します。2分間待ちます。WiFiクライアントデバイスがアクセスポイントに接続できない場合は、以下を確認してください：

- アクセスポイントの WLAN LED が消灯していないことを確認します。

  WLAN LED が消灯しており、LED を無効にしていない場合（LED の管理 (179 ページ)を参照）、関連する WiFi 無線も消灯している可能性があります。WiFi 無線の詳細については、89 ページの無線のオン／オフを参照してください。
- WiFiクライアントデバイスとアクセスポイントのWiFi設定が正確に一致していることを確認してください。アクセスポイントとWiFiクライアントデバイスのWiFiネットワーク名（SSID）とWiFiセキュリティ設定は正確に一致している必要があります。

  WiFi 接続でアクセス ポイントにアクセスして初期設定を行う方法については、23 ページの「アクセス ポイントに接続して初期設定を行う」を参照してください。
- WiFi クライアントデバイスが、WiFi ネットワークで使用している認証と暗号化をサポートしていることを確認します。詳細については、WiFi ネットワークの認証と暗号化の変更 (73 ページ) を参照してください。

  注：アクセスポイントのWiFi認証および暗号化がWPA3 Personalに設定されており、WiFiクライアントデバイスがWPA3をサポートしている場合は、WiFiクライアントデバイスでWiFiアダプタデバイスドライバが最新バージョンに更新されていることを確認してください。
- WiFiクライアントデバイスがアクセスポイントから遠すぎたり近すぎたりしていないことを確認します。信号強度が向上するかどうかを確認するには、WiFiクライアントデバイスをアクセスポイントの近くに移動しますが、少なくとも6フィート（1.8メートル）離します。
- アクセスポイントとWiFiクライアントデバイスの間に物体があり、WiFi信号がブロックされていないことを確認します。
- アクセスポイントのSSIDブロードキャストが無効になっていないことを確認してください。アクセスポイントのSSIDブロードキャストが無効になっている場合、WiFiネットワーク名は非表示になり、WiFiクライアントデバイスのスキャンリストに表示されません。非表示のネットワークに接続するには、ネットワーク名とWiFiパスワードを入力する必要があります。

SSID ブロードキャストについては、WiFi ネットワークの SSID を隠すまたはブロードキャストする（71 ページ）を参照してください。

- WiFiクライアントデバイスが静的IPアドレスを使用せず、DHCPで自動的にIPアドレスを受信するように設定されていることを確認します。(ほとんどのデバイスでは、DHCPは のデフォルト設定です）。

LEDによるトラブルシューティング

LEDとLEDアイコンに関する一般的な情報については、13ページのLED付きトップパネルを参照してください。

アクセス ポイントを電源に接続し、LED を無効にしなかった場合（179 ページの「LED の管理」を参照）、LED はここで説明するように点灯します：

1. 電源/クラウドLEDは、初めはオレンジの点灯で、その後ゆっくりとオレンジに点滅します。約2分後、電源/クラウドLEDが緑色の点灯または青色の点灯になり、起動手順が完了してアクセスポイントの準備が完了したことを示します：
   - **緑色の点灯**：アクセス ポイントは、スタンドアロンアクセスポイントとして、または Insight クラウドベース管理プラットフォームに接続されていない Insightで検出されたアクセスポイントとして機能します。
   - **青色の点灯**：アクセスポイントは Insight モードで機能し、Insight クラウドベースの管理プラットフォームに接続されています。
2. 起動手順が完了したら、以下を確認する：
   - LAN 1 LEDは、イーサネット・リンクの速度に応じて、緑色またはオレンジに点灯します。

     アクセスポイントがイーサネットトラフィックを処理する場合、LAN LED は緑または青に点滅します。
   - 2.4G WLAN LED と 5G WLAN LED が緑色に点灯します。

     クライアントが無線に接続されている場合、関連する WLAN LED は青色で点灯します。無線がトラフィックを処理している場合、関連する WLAN LED は青く点滅します。

LEDはトラブルシューティングに使用できます。詳細については、以下のセクションを参照してください：

- 電源/クラウドLEDは消灯したまま
- 電源/クラウドLEDがオレンジに点灯したまま
- 電源/クラウドLEDがオレンジでゆっくり点滅し続ける
- アクセスポイントは PoE PD として機能し、Power/Cloud LED はオレンジに点灯したままです。
- NETGEAR Insight 管理モードで電源/クラウド LED が青く点灯しない
- 電源/クラウドLEDのオレンジ、緑、青の点滅が止まらない

- 2.4G または 5G WLAN LED が消灯している

電源/クラウドLEDは消灯したまま

PoE++接続を使用していて、イーサネットケーブルがPoE++スイッチに接続されているときにPower/Cloud LEDと他のLEDが消灯している場合は、次のようにしてください：

- LEDが無効になっていないことを確認してください（LEDの管理（179ページ）を参照）。
- アクセスポイントと PoE++ スイッチ間のイーサネットケーブルの両端が正しく接続されていることを確認します。
- イーサネットケーブルのもう一方の端が、受電しているPoE++スイッチのPoE++ポートに差し込まれていることを確認してください。
- PoE++スイッチがアクセスポイントにPoE++（802.3bt）電力を供給できるように、PoE++スイッチのPoEパワーバジェットがオーバーサブスクライブしていないことを確認してください。

オプションの電源アダプタを使用していて、アクセス ポイントの電源を入れたときに電源 / クラウド LED およびその他の LED が消灯したままの場合は、次の手順を実行します：

- LEDが無効になっていないことを確認してください（LEDの管理(179ページ)を参照）。
- 電源アダプタがアクセスポイントに正しく接続されていること、および電源アダプタが機能する電源コンセントに正しく接続されていることを確認します。電源タップに接続されている場合は、電源タップの電源がオンになっていることを確認します。コンセントに直接接続されている場合は、コンセントの電源がオフになっていないことを確認します。
- 本製品用のNETGEAR電源アダプタを使用していることを確認してください。つまり、NETGEAR 電源アダプタを別の NETGEAR 製品またはサードパーティの電源アダプタに使用しないでください。

エラーが続く場合は、ハードウェアに問題がある可能性があります。復旧手順やハードウェアの問題については、netgear.com/support のテクニカルサポートにお問い合わせください。

電源/クラウドLEDがオレンジに点灯したまま

アクセス ポイントを電源に接続すると、電源 / クラウド LED が最初はオレンジに点灯し、次にオレンジにゆっく り点滅し、最後に緑色または青色に点灯します。

電源 / クラウド LED が 5 分経過してもオレンジに点灯している場合は、ブートエラーが発生したか、アクセ スポイントが故障しています。

以下を実行する：

1. アクセスポイントの電源を切断して再接続し、数分待って起動手順が正常に完了するかどうかを確認します。
2. 起動手順がまだ正常に完了せず、5 分経過しても電源 / クラウド LED がオレンジに点灯したままの場合は、**リセット** ボタンを使用してアクセス ポイントを工場出荷時のデフォルト設定に戻します。

   詳細については、175 ページの「アクセス ポイントをリセットするには、[リセット] ボタンを使用します」を参照してください。

エラーが続く場合は、ハードウェアに問題がある可能性があります。復旧手順やハードウェアの問題については、netgear.com/support のテクニカルサポートにお問い合わせください。

電源/クラウドLEDがオレンジでゆっくり点滅し続ける

アクセス ポイントを電源に接続すると、電源 / クラウド LED が一時的にオレンジの点灯にな り、その後緑色または青色の点灯に変わります。通常動作中、電源 / クラウド LED が一時的にオレンジに点滅するのは、ファームウェアをアップグレードしているときだけです。また、その場合、電源 / クラウド LED は、ゆっくりではなく、すばやくオレンジに点滅します。

電源 / クラウド LED がゆっくりと連続してオレンジに点滅している場合、アクセ ス ポイントは DHCP サーバーから IP アドレスを受信していません。

アクセス ポイントの DHCP クライアントが有効になっていること（「DHCP クライアントを有効にする（137 ページ）」を参照）、ネットワークに DHCP サーバー（または DHCP サーバーとして機能するルーター）が含まれていること、DHCP サーバーがアクセス ポイントに到達できること（両方が同じネットワーク上にある必要 があります）を確認します。

ネットワークに DHCP サーバーがない場合、アクセスポイントに固定 （静的） IP アドレスを設定する必要がある場合があります （「DHCP クライアントを無効にして固定 IP アドレスを指定する (136 ページ)」を参照）。

アクセスポイントは PoE PD として機能し、Power/Cloud LED はオレンジに点灯したままです。

アクセス ポイントを電源に接続すると、電源 / クラウド LED が最初はオレンジに点灯し、次にオレンジにゆっく り点滅し、最後に緑色または青色に点灯します。

アクセス ポイントが PoE PD として機能し、5 分経過しても電源 / クラウド LED がオレンジに点灯したままの場合、アクセス ポイントは必要な 802.3bt（PoE++）レベルの電力を受信していない可能性があります。たとえば、802.3bt（PoE++）ではなく 802.3at（PoE+）のみを提供するスイッチにアクセス ポイントが接続されている場合、このような状況が発生する可能性があります。

注： アクセス ポイントが 802.3at（PoE+）レベルで電力を受信する場合、アクセス ポイントは、2.4 GHz 無線と 5 GHz 低帯域無線の動作を 2x2 ストリームに制限し、その結果、これら 2 つの無線のピーク スループットが半分になります（5 GHz 高帯域無線は正常に機能します）。(アクセスポイントが 802.3af（PoE）レベルで電力を受信する場合、すべての無線はオフのままです。

以下を実行する：

1. アクセスポイントの LAN 1/PoE++ ポートと PoE++ スイッチの 802.3bt (PoE++) ポートでイーサネットケーブルを取り外し、再接続します。

   アクセスポイントは再起動する。
2. 電源 / クラウド LED が 5 分経過してもオレンジに点灯したままの場合は、PoE++ スイッチがアクセス ポイントに十分な PoE 電力を供給できない原因を確認してください。ほとんどの場合、PoE++スイッチのPoEパワーバジェットはオーバーサブスクライブしているため、アクセスポイントで十分なPoEパワーを利用できるようにするには、PoE++スイッチから別のPoEデバイスを切り離す必要があるかもしれません。

エラーが続く場合は、電源/クラウド LED がオレンジに点灯したまま（246 ページ） を参照してください。

NETGEAR Insight 管理モードで電源/クラウド LED が青く点灯しない

アクセス ポイントが Web ブラウザ管理モードで機能する場合、電源 / クラウド LED は緑色に点灯します。これは通常の LED の動作です。

ただし、アクセス ポイントが NETGEAR Insight 管理モードで機能し、電源 / クラウド LED が青色に点灯せず緑色のままである場合、アクセス ポイントは Insight クラウドベース管理プラットフォームに接続されていません。

アクセス ポイントが NETGEAR Insight 管理モードで機能し、電源 / クラウド LED が青く点灯しない場合は、問題が解決するまで次のトラブルシューティング手順をお試しください：

1. アクセス ポイントの管理モードが NETGEAR Insight であることを確認します。

   詳細については、「管理モードを NETGEAR Insight または Web ブラウザに変更する (155 ページ)」を参照してください。
2. アクセスポイントとネットワーク間のイーサネットケーブル接続が正常であることを確認します。
3. アクセスポイントがインターネットに接続され、インターネット接続が良好であることを確認します。
4. アクセスポイントが最新のファームウェアバージョンを実行していることを確認します。詳細については、163 ページの「アクセスポイントのファームウェアの管理」を参照してください。

5. LAN 1/PoE++ ポートでイーサネットケーブルを取り外し、再接続し、5分間待って、電源/クラウドLEDが青く点灯するかどうかを確認します。

   アクセス ポイントで電源アダプタを使用している場合は、電源アダプタの接続を解除して再接続し、5 分間待って、電源 / クラウド LED が青色で点灯するかどうかを確認します。
6. それでも問題が解決しない場合は、**リセット** ボタンを使用してアクセス ポイントを工場出荷時のデフォルト設定に戻し、アクセス ポイントを再設定します。

   詳細については、175 ページの「アクセス ポイントをリセットするには、[リセット] ボタンを使用します」を参照してください。

エラーが続く場合は、ハードウェアに問題がある可能性があります。復旧手順やハードウェアの問題については、netgear.com/support のテクニカルサポートにお問い合わせください。

電源/クラウドLEDのオレンジ、緑、青の点滅が止まらない

Insight Instant Mesh WiFi ネットワークの初期インストールと設定プロセス中、アクセスポイントをノードとして設定している間、電源 / クラウド LED がオレンジ、緑色、青色に点滅します。詳しくは、55 ページの「Insight アプリを使用して、アクセスポイントをノードとしてルートに接続する」を参照してください。

電源/クラウドLEDがオレンジ、緑色、青色の点滅を止めない場合、ノードは接続できません。

以下の項目をチェックするか、以下のトラブルシューティング手順を試してください：

- ノードが接続できるルートが少なくとも1つあることを確認する。
- すべてのルーツが最新のファームウェアバージョンであることを確認してください。
- 各ルートの各無線の出力電力が最大レベルであることを確認してください。デフォルトでは、無線の出力電力は最大レベルになっています。詳細については、無線の出力電力の変更（95ページ）を参照してください。
- ノードがルートから離れすぎていないことを確認してください。詳細については、250ページの「ノードとルートが接続できない」を参照してください。
- ノードを再起動する。
- Insight ネットワークの場所と Insight アカウントからノードを削除します。その後、Insight アカウントと Insight ネットワークの場所にノードを追加します。

2.4G または 5G WLAN LED が消灯している

2.4G WLAN LED、5G H WLAN LED、または 5G L WLAN LED が消灯している場合は、次の操作を行ってください：

- 無線が無効になっていないか確認します（無線のオン／オフ（89ページ）参照）。デフォルトでは、無線は有効になっており、WLAN LED は以下のように点灯します：
  - **緑の点灯**：無線はクライアントなしで動作しています。
  - **青色で点灯**：無線はクライアントで動作しています。
  - **青色の点滅**：無線はクライアントで動作しており、トラフィックを処理中です。
- PoE 接続を使用する場合は、PoE++ スイッチがアクセスポイントに十分な電力を供給していることを確認してください。アクセスポイントには、802.3bt（PoE++）レベルの電力が必要です。PoE++ より低いレベルの電力は、 無線に影響を与えます。詳細については、247 ページの「アクセス ポイントが PoE PD として機能し、電源 / クラウド LED がオレンジに点灯したままになっている」を参照してください。

エラーが続く場合は、ハードウェアに問題がある可能性があります。復旧手順やハードウェアの問題については、netgear.com/support のテクニカルサポートにお問い合わせください。

ノードとルートが接続できない

アクセスポイントを、1 つ以上のルートを含む Insight ネットワークの場所にノードとして追加する場合（「Insight アプリを使用して、アクセスポイントをルートにノ ードとして接続する (55 ページ)」を参照）、最初の同期の際に、ノードをルートと同 じ部屋に配置することをお勧めします。同期に成功したら、ノードを使用する場所に移動します。

信頼性の高いWiFi接続を行うには、ノードを最も近いルートから7.5m（25フィート）以内で、障害物の少ない見通しの良い場所に設置してください。

ノードを Insight ネットワークロケーションに追加した後に、ノードとルートを同期するには：

1. ノードをルートと同じ部屋に置く。

   このノードの位置は、同期プロセス中にのみ使用する。
2. ノードを電源に接続する。

   PoEスイッチにPoE接続しない場合は、DC電源コネクタに電源アダプタを接続してください。

   ノードのPower/Cloud LEDがオレンジに点灯します。

3. ノードが初期接続と設定プロセスを経て、電源/クラウドLEDがオレンジ、緑色、青色の点滅を止め、青色で点灯するのを待ちます。

   注：初期接続と設定プロセスには最大10分かかる場合があります。設定プロセス中にノードが再起動することがあります。

   電源/クラウドLEDは、最初の接続と設定プロセス中に以下のように点灯します：

   - **緑の点滅**：ノードはルートを検出しようとしている。
   - **緑の点灯**：ノードは、最も強いWiFi信号を提供するルートと最初の接続を行っています。
   - **オレンジでゆっくり点滅**：ノードがネットワークルーターまたはDHCPサーバーに連絡してIPアドレスを受信している。

     電源 / クラウド LED のオレンジの点滅が止まらない場合は、247 ページの「電源 / クラウド LED がオレンジでゆっくりと点滅し続けている」を参照してください。
   - **オレンジ、グリーン、ブルーの点滅**：ノードは、Insight Instant Mesh WiFi ネットワークの管理対象デバイスとして設定されています。

     電源/クラウドLEDがオレンジ、緑色、青色の点滅を停止しない場合は、電源/クラウドLEDがオレンジ、緑色、青色の点滅を停止しない（249ページ） を参照してください。

   設定が完了すると、Power/Cloud LEDが以下のように点灯します：

   - **青色で点灯**：設定が完了し、ノードを操作できる状態。ノードはInsight Instant Mesh WiFiネットワークで機能し、Insightクラウドに接続されています。

4. ノードの接続を外し、使用する場所に移動する。
5. 新しい場所で、ステップ2とステップ3を繰り返す。
6. ノードがルートと再同期するのを待つ。

   ノードのPower/Cloud LEDが青く点灯したら、ノードとルートは正常に同期したことになります。

   ノードとルートが同期しなかった場合は、ノードをルートに近づけて再試行してください。良好または公平なWiFi接続を確立するには、ノードがルートのWiFiカバレッジエリア内にある必要があります。

WiFiクライアントデバイスのWiFi接続のトラブルシューティング

WiFiクライアントデバイスがアクセスポイントに接続できない場合、またはWiFi接続が正常でない場合は、問題の切り分けを試みます：

- WiFiクライアントデバイスとアクセスポイントのWiFi設定が正確に一致していることを確認してください。

  アクセスポイントとWiFiデバイスのWiFiネットワーク名（SSID）とWiFiセキュリティ設定が正確に一致している必要があります。WiFiクライアントデバイスがWiFiネットワークの正しいパスフレーズを使用していることを確認してください。

  WiFi 接続でアクセス ポイントにアクセスして初期設定を行う方法については、23 ページの「アクセス ポイントに接続して初期設定を行う」を参照してください。
- WiFiクライアントデバイスは、WiFiネットワークに設定した認証と暗号化をサポートしていますか？

  詳細については、WiFi ネットワークの認証と暗号化の変更 (73 ページ) を参照してください。

  注：アクセスポイントのWiFi認証および暗号化がWPA3 Personalに設定されており、WiFiクライアントデバイスがWPA3をサポートしている場合は、WiFiクライアントデバイスでWiFiアダプタデバイスドライバが最新バージョンに更新されていることを確認してください。

- WiFiクライアントデバイスはWiFiネットワークを見つけられますか？

  消灯していない場合は、WLAN LED を確認します。WLAN LED が消灯している場合は、関連する WiFi 無線も消灯している可能性があります。WiFi 無線の詳細については、89 ページの無線のオン／オフを参照してください。
- アクセスポイントの SSID ブロードキャストを無効にすると、WiFi ネットワークは非表示になり、WiFi デバイスのネットワークスキャンリストに表示されません (デフォルトでは、SSID ブロードキャストは有効です)。(デフォルトでは、SSID ブロードキャストは有効です。) SSID ブロードキャストの詳細については、WiFi ネットワークの SSID を隠すまたはブロードキャストする (71 ページ) を参照してください。

注：アクセスポイント上のWiFiネットワークの設定を変更する場合は、新しいWiFi設定が有効になったときに切断されないように、有線LAN接続を使用してください。

WiFiクライアントデバイスがWiFiネットワークを見つけたが、信号強度が弱い場合は、以下の条件を確認してください：

- WiFiクライアントデバイスがアクセスポイントから遠すぎるか、近すぎるか？

  WiFiクライアントデバイスをアクセスポイントの近くに、少なくとも6フィート（1.8メートル）離して置き、信号強度が向上するかどうかを確認します。

- WiFiクライアントデバイスとアクセスポイントの間に、WiFi（）の信号を遮るものがありませんか？

インターネット閲覧のトラブルシューティング

WiFiデバイスがアクセスポイントに接続されているにもかかわらず、インターネットからウェブページを読み込むことができない場合、次のいずれかの理由が考えられます：

- WiFiデバイスがDNSサーバーアドレスを認識していない可能性があります。

  アクセス ポイントのセットアップ時に DNS アドレスを手動で入力した場合（つまり、アクセス ポイントが静的 IP アドレス設定を使用している場合）、WiFi デバイスを再起動して DNS アドレスを確認します。
- WiFiデバイスが正しいTCP/IP設定を使用していない可能性があります。

  WiFi デバイスが DHCP で情報を取得している場合は、WiFi デバイスを再起動し、アクセス ポイントが接続されているスイッチまたはインターネット モデムのアドレスを確認します。TCP/IP の問題については、255 ページの ping ユーティリティを使用したネットワークのトラブルシューティングを参照してください。

LAN接続でアクセスポイントにログインできない

LAN 上のコンピュータからアクセス ポイントにログインできず、アクセス ポイントのローカル ブラウザ UI を使用できない場合は、以下を確認してください：

- 正しいログイン情報を使用していることを確認してください。ユーザー名はadminで、パスワードは指定したものです。ユーザー名とパスワードは大文字と小文字を区別します。

  以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。
- コンピュータのIPアドレスがアクセスポイントと同じサブネット内にあることを確認してください。

  アクセス ポイントの DHCP クライアントを無効にし、アクセス ポイントをネットワークに接続したときに固定（静的） IP アドレスを設定した場合は （「DHCP クライアントを無効にし、固定 IP アドレスを指定する (136 ページ)」を参照）、コンピュータの IP アドレスとサブネット マスクを変更して、コンピュータとアクセス ポイントの IP アドレスが同じ IP サブネットになるようにします。
- ブラウザを終了して、もう一度起動してみてください。

- 古いタイプのブラウザを使用している場合は、Java、JavaScript、またはActiveXがブラウザで有効になっていることを確認してください。例えば、Internet Explorerを使用している場合は、**更新**ボタンをクリックしてJavaアプレットがロードされていることを確認してください。
- アクセスポイントのIPアドレスが変更され（たとえば、ネットワーク内のDHCPサーバーがアクセスポイントにIPアドレスを発行した）、現在のIPアドレスがわからない場合は、IPスキャナーアプリケーションを使用してIPアドレスを検出します。

  注: NETGEAR Insight アプリを使用して、アクセス ポイントに割り当てられている IP アドレスを検出することもできます。詳細については、26 ページの 「NETGEAR Insight アプリを使って WiFi で接続する」 を参照してください。

  この設定により、 アクセス ポイントの IP アドレスが 192.168.0.100 に設定され、DHCP クライアントが有効になります。この操作により、 アクセス ポイントの IP アドレスが 192.168.0.100 に設定され、 DHCP クライアントが有効になります。詳細については、175 ページの「リセットボタンを使用してアクセス ポイントをリセットする」を参照してください。

変更が保存されない

アクセス ポイントのローカル ブラウザ UI にログインしていて、アクセス ポイントがページで行った変更を保存しない場合は、次の手順を実行します：

- コンフィギュレーション設定を入力する際は、他のページやタブに移動する前に必ず「Apply」ボタンをクリックしてください。
- ウェブブラウザの「Refresh」または「Reload」ボタンをクリックします。変更が行われたにもかかわらず、古い設定がウェブブラウザのキャッシュに残っている可能性があります。

パスワードを間違えて入力し、アクセスポイントにログインできなくなった。

管理者パスワードを 3 回以上間違って入力すると、アクセス ポイントのローカル ブラウザ UI へのアクセスが一定時間ブロックされます。たとえば、間違ったパスワードを 3 回入力すると、アクセス ポイントへのアクセスは 5 分間ブロックされます。

閉塞期間は、ログインの失敗回数によって異なります。閉塞期間中は、正しいパスワードを入力しても、アクセスポイントへのログイン試行は無視されます。閉塞が解除されるまで待つ必要があり、その後、正しいパスワードを入力する*機会が 1 回*与えられます。再度間違ったパスワードを入力すると、次の表に示すように遮断期間が延長されます。

表2.ログインできない期間

失敗した回数	ブロック期間
3	5
4	10
5	20
6	40
などなど	

また、ログイン失敗回数には以下のルールが適用される：

- ログイン失敗回数が再試行可能回数より少ない場合、ログイン失敗回数のカウンタは30分後にリセットされる。例えば、間違ったパスワードを2回入力したが、3回目のログイン試行で正しいパスワードを入力した場合、30分後に2回のログイン試行失敗はメモリから消去される。
- ログイン失敗回数が再試行可能回数より多い場合、ログイン失敗回数のカウンタは24時間後にリセットされる。たとえば、間違ったパスワードを5回入力したが、6回目のログイン試行で正しいパスワードを入力した場合、ログインに失敗した5回は24時間後にメモリから消去される。
- 最後のアクセス試行によって、ログイン試行失敗のカウンタが増加するかどうかが決定される。
- アクセスポイントを再起動すると、ログイン試行失敗のカウンタはリセットされます。

pingユーティリティを使ったネットワークのトラブルシューティング

ほとんどのネットワーク・デバイスやルーターには、指定されたデバイスにエコー要求パケットを送信するpingユーティリティーが含まれています。デバイスは、エコー応答で応答します。コンピュータやワークステーションのpingユーティリティを使用すると、ネットワークのトラブルシューティングを簡単に行うことができます。

アクセスポイントまでのLAN経路をテストする

アクセスポイントへのLANパスが正しく設定されていることを確認するために、コンピュータからアクセスポイントにpingを送信することができます。

Windows ベースのコンピュータからアクセス ポイントに ping を送信するには、次の手順に従います：

1. Windowsのタスクバーから「**スタート**」ボタンをクリックし、「ファイル名を指定して**実行**」**を選択します**。
2. 提供されているフィールドに、この例のように、**ping** の後にアクセスポイントの IP アドレスを入力します：

   ping 192.168.0.100
3. **OK**ボタンをクリックする。

   次のようなメッセージが表示される：

   Pinging <IP address> with 32 bytes of data
   If the path is working, you see this message:
   Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
   If the path is not working, you see this message:
   Request timed out

パスが正しく機能していない場合、以下のいずれかの問題が発生している可能性がある：

- 誤った物理的接続

  ネットワーク デバイスの適切な LED が点灯していることを確認します。アクセス ポイントとコンピュータが別のイーサネット スイッチに接続されている場合は、コンピュータとアクセス ポイントに接続されているスイッチ ポートのリンク LED が点灯していることを確認します。
- 誤ったネットワーク設定

  コンピュータとアクセス ポイントの IP アドレスが正しく、同じサブネット内にあることを確認します。

コンピュータからリモートデバイスへのパスをテストする

LANパスが正しく動作することを確認したら、コンピュータからリモートデバイスへのパスをテストします。

コンピューターからリモートデバイスへのパスをテストするには：

1. Windowsのタスクバーから「**スタート**」ボタンをクリックし、「ファイル名を指定して**実行**」**を選択します**。
2. 提供されたフィールドに、**ping -n 10** ***IP****アドレス*と入力する。

   IPアドレスは、リモートDNSサーバーなどのリモートデバイスのIPアドレスである。

パスが正しく機能している場合、256 ページの「アクセスポイントへの LAN パスのテスト」で説明したようなリピーが表示されます。応答を受信しない場合は、次の操作を行います：

- アクセスポイントが接続されているルーターの IP アドレスが、コンピュータにデフォルトのルーターとして表示されていることを確認します。コンピュータのIP設定がDHCPによって割り当てられている場合、この情報はコンピュータのネットワークコントロールパネルには表示されません。
- お使いのコンピュータのネットワークアドレス（ネットマスクで指定されたIPアドレスの部分）が、リモートデバイスのネットワークアドレスと異なることを確認します。

A

工場出荷時の設定と技術仕様

この付録には以下のセクションが含まれる：

- 工場出荷時の設定
- 技術仕様

工場出荷時の設定

アクセスポイントは、次の表に示す工場出荷時のデフォルト設定にリセットできます。

アクセス ポイントを工場出荷時の設定にリセットする方法の詳細については、175 ページの「アクセス ポイントを工場出荷時の設定に戻す」を参照してください。

表 3.工場出荷時の設定

設定項目	初期設定
管理およびログイン設定	
管理モード	NETGEAR Insight（クラウド/リモート） **注**：ローカルブラウザUIにアクセスするには、管理モードとしてWebブラウザ（ローカル）を選択する必要があります。
ユーザーログインURL	ネットワークに接続されていない場合は、192.168.0.100。 **注**：ネットワークに接続されている場合、アクセスポイントはネットワーク内のDHCPサーバーまたはルーターからIPアドレスを受信します。
ユーザー名	**admin**、設定不可
APログインパスワード	**パスワード**、大文字小文字を区別、設定可能 **注**：ローカルブラウザ UI に初めてログインするときは、AP ログインパスワードを変更する必要があります。以前にアクセス ポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、そのロケーションの Insight ネットワークパスワードを入力します。詳細については、26 ページの「NETGEAR Insight アプリを使って WiFi で接続する」を参照してください。
初期設定とWiFiログインのためのWiFiネットワーク設定	
初期SSID名	初期セットアップ用の SSID は NETGEARxxxxxx-SETUP で、 xxxxxx はアクセスポイントの MAC アドレスの下 6 桁の 16 進数です。 **注**: ローカル ブラウザー UI に初めてログインするときは、SSID を変更する必要があります。以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、この要件が適用されない場合があります。
初期のWiFiセキュリティ	WPA2パーソナル（これはWPA2-PSKである） WiFiパスワード（ネットワークキー）：**sharedsecret** **注**：ローカルブラウザ UI に初めてログインするときは、WiFi パスワードを変更する必要があります。以前にアクセスポイントを NETGEAR Insight ネットワークロケーションに追加し、Insight クラウドポータルまたは Insight アプリでアクセスポイントを管理した場合は、この要件が適用されない場合があります。
RFチャンネル	すべての無線で自動選択（Auto）。 **注**：利用可能なチャンネルとサポートされているチャンネルは、アクセスポイントで選択した国と地域によって異なります。
一般的なシステム設定	
動作モード	APモード

表 3.工場出荷時のデフォルト設定（続き）

設定項目	初期設定
DHCPクライアント	アクセスポイントが ネットワーク内のDHCP サーバーまたはルーターから IP アドレスを受信するように有効にする。
NTPクライアント	有効
スパニングツリープロトコル	無効
ネットワーク整合性チェック	無効
IGMPスヌーピング	無効
802.1Q VLAN	VLAN ID 1のタグなしVLAN
管理VLAN	VLAN ID 1
シスログ	無効
イーサネットLLDP	有効
UPnP	有効
リンクアグリゲーション	無効
マルチキャストDNSゲートウェイ	無効
LED	すべて有効
エネルギー効率モード	無効
個々のWiFiネットワークのWLAN設定（SSIDまたはVAP）	
ブロードキャストSSID	有効
VLAN ID（WiFi クライアント用）	1
ネットワーク認証	WPA2パーソナル（これはWPA2-PSKである） WPA2 Personal の設定不可能なデータ暗号化は AES です。
802.11w (PMF)	無効
マルチPSK	無効
スケジュール	常時オン
無線バンド	すべて有効
バンドステアリング	無効 自動バンドステアリングには、自動802.11k RRMおよび自動802.11v WiFiネットワーク管理が含まれます。
WiFiクライアントの隔離	無効
URLトラッキング	無効

表 3.工場出荷時のデフォルト設定（続き）

設定項目	初期設定
DHCPオファーのユニキャスト化	有効
キャプティブ・ポータル	なし
MAC ACL	割り当てなし
レート制限	なし
高度なレート選択	マルチキャストレート固定：Auto レート制御：無効
すべてのWiFiネットワーク（SSIDまたはVAP）に適用される基本的な無線設定	
周波数帯	2.4GHz：有効 5GHz L：有効 5GHz H：有効
WiFiモード	2.4 GHz：11ax、11b、11bg、11na 5 GHz L：11ax、11a、11na、11ac 5 GHz H：11ax、11a、11na、11ac
チャンネル幅	2.4 GHz：20 MHz 5 GHz L：40 MHz 5 GHz H：40 MHz
ガードインターバル	2.4 GHz：Long-800 ns 5 GHz L：Long-800 ns 5 GHz H ：Long-800 ns
出力	2.4GHz：最大（100） 5 GHz L：最大（100） 5 GHz H：最大（100）
チャンネル	2.4 GHz：オート 5 GHz L：オート 5 GHz H：オート
Wi-Fiマルチメディア（WMM）	2.4 GHz：有効 5 GHz L：有効 5 GHz H：有効
WMMパワーセーブ	2.4 GHz：有効 5 GHz L：有効 5 GHz H：有効
すべてのWiFiネットワーク（SSIDまたはVAP）に適用される高度な無線設定	
WiFiクライアント数	2.4 GHz：デフォルト200（最大数も同じ） 5 GHz L：デフォルト200（最大数も同じ） 5 GHz H：デフォルト200（最大数も同じ）

表 3.工場出荷時のデフォルト設定（続き）

設定項目	初期設定
RTSしきい値	2.4 GHz：2346で有効 5 GHz L：2346 で有効 5 GHz H：2346で有効
ビーコン間隔	2.4GHz：100ミリ秒 5 GHz L：100ミリ秒 5 GHz H：100ミリ秒
802.11n 256 QAM	2.4 GHz：無効（11ng WiFi モードでのみ適用） 5 GHz L：設定不可 5 GHz H：設定不可
MU-MIMO	2.4 GHz：有効 5 GHz L：有効 5 GHz H：有効
DTIM間隔	2.4GHz：2 5 GHz L：2 5 GHz H：2
ブロードキャストとマルチキャストのレート制限	2.4 GHz：50ppsの制限付きで有効 5 GHz L：50ppsの制限付きで有効 5 GHz H：50ppsの制限付きで有効
802.11h	2.4 GHz ：非対応 5 GHz L：無効 5 GHz H：無効
無線間の負荷分散	無効
スティッキークライアントを強制的にディスアソシエイトする	無効
ARPプロキシ	無効
ブロードキャスト機能強化	有効
ワイヤレスブリッジ	設定なし
セキュリティ全般	
URLフィルタリング	無効
RADIUS	サーバー設定なし
近隣APの検出	2.4 GHz：無効 5 GHz L：無効 5 GHz H：無効
MAC ACL	8つのデフォルトACLがあるが、MACアドレスは設定されていない。
L2セキュリティ	無効

表 3.工場出荷時のデフォルト設定（続き）

設定	初期設定
リモート管理	
SNMP	無効

技術仕様

以下の表は技術仕様である。

表 4.技術仕様

機能	説明
WiFiモード	2.4 GHz無線：802.11ax、802.11ng、801.11bg、802.11b 5 GHz L無線：802.11ax、802.11ac、802.11na、802.11a 5 GHz H 無線：802.11ax、802.11ac、802.11na、802.11a このアクセスポイントは、2.4GHz、5GHzローバンド、5GHzハイバンドの同時動作をサポートしています。
理論上の最大スループット	同時スループット約6000Mbps（2.4GHz帯1200Mbps、5GHz帯ローバンド2400Mbps、5GHz帯ハイバンド2400Mbps）。 **注**：スループットは変動する可能性があります。ネットワークのトラフィック量、建物の材質や構造、ネットワークのオーバーヘッドなどのネットワーク条件や環境要因が、データ・スループット・レートに影響します。
最大サポートクライアント数	2.4GHz：200 5 GHz L：200 5 GHz H：200 アクセスポイントは、すべての無線を有効にして、最大600クライアントをサポートできます。
802.11セキュリティ	WPA3パーソナル、WPA3エンタープライズ、WPA3/WPA2パーソナル、WPA2パーソナル、WPA2エンタープライズ、WPA2/WPAパーソナル、オープン・エンハンスト、オープン
WiFi規格	IEEE 802.11ax (WiFi 6) WiFi マルチメディア優先制御（WMM） ワイヤレス・ディストリビューション・システム（WDS）
WiFiストリーム	12（4+4+4）ストリーム： 2.4GHz：4ストリーム 5 GHz L：4ストリーム 5 GHz H：4ストリーム
動作周波数範囲	2.4GHz帯： • 米国およびカナダ：2.412～2.462GHz • ヨーロッパ：2.412～2.472GHz 5GHzのローバンド： • 米国およびカナダ5.18-5.24 GHzおよびDFS 5.25-5.35 GHz • 欧州：5.18～5.24GHz、DFS 5.25～5.35GHz 5GHzのハイバンド： • 米国およびカナダ5.475-5.825 GHzおよびDFS 5.47-5.725 GHz • ヨーロッパDFS 5.50-5.70 GHz

特徴	説明
パワー・オーバー・イーサネット	電源アダプターを使用しない場合、LAN/PoE++ポートには802.3bt（PoE++）電源が必要ですが、802.3at（PoE+）電源でも機能する場合があります。802.3bt（PoE++）電源を使用することをお勧めします。詳細については、247 ページの「アクセスポイントが PoE PD として機能し、電源 / クラウド LED がオレンジに点灯したままになっている」を参照してください。 **注**：PoEは、IEC TR 62101によるネットワーク環境0とみなされる可能性があるため、相互接続されたITE回路は安全特別低電圧（SELV）とみなされる可能性がある。
PoE消費電力	30.1W
電源アダプター	12VDC、3.5A プラグは販売国にローカライズされている。 **注**：モデルWAX630PAには電源アダプターが付属しています。モデルWAX630の場合、電源アダプターは付属していませんが、オプションとして注文できます。
ハードウェア・インターフェース	2.5Gbps、1Gbps、100Mbps、10Mbpsに対応するRJ-45 LAN 1/PoE++ Ethernetポート×1。このポートはオートアップリンク（Auto MDI-X）にも対応しています。 1Gbps、100Mbps、10Mbps対応のRJ-45 LAN 2イーサネットポート×1。このポートはオートアップリンク（Auto MDI-X）にも対応しています。 **注：**電源アダプターがない場合、LAN 1/PoE++ ポートは 802.3bt（PoE++）電源を必要としますが、802.3at（PoE+）電源でも機能する場合があります。802.3bt（PoE++）電源の使用をお勧めします。詳細については、247 ページの「アクセスポイントが PoE PD として機能し、電源 / クラウド LED がオレンジに点灯したままになっている」を参照してください。
寸法（幅×奥行×高さ）	10.49×10.56×2.18インチ (266.6 x 268.3 x 55.5 mm)
重量2	.10ポンド（956g）
動作温度	32°～104°F（0°～40°C）
動作湿度	10～90% 最大相対湿度、結露しないこと
保管温度	-4°～158°F（-20°～70°C）
保存湿度	5～95% 最大相対湿度、結露しないこと
EMI認証	FCCパート15レポート（EMI）サブパートB CE EMC レポート、EN 55032/24/35 レポート EN 301 489-1/-17 EMC レポート
規制遵守 米国	FCCグラント、FCC認可 FCCスペクトラムレポート、パート15、サブパートC (15.247) FCCスペクトラムレポート、パート15、サブパートE (15.407) FCC標準吸収率報告書（SARまたはMPE）、FCC Part 2 SpJ
欧州規制コンプライアンス	EN 300 328、無線スペクトラムレポート EN 301 893 ラジオスペクトラムレポート EN 301 893 DFSレポート EN RF Exposure（SARまたはMPE）、EN 50385（APルータ用）、EN 50566（ボディSAR）
安全性とエネルギー・コンプライアンス	IEC 60950-1 CB Certificate and Test Report, CB IEC60950 / EN60950 CE LVD Report, EN60950 Report EC 278/2009、外部電源

B

アクセスポイントを壁または天井に取り付ける

アクセス ポイントは、24 mm (15/16 インチ) の T バーを使用して壁または天井に取 り付けることも、平らな面に自立させて設置することもできます。

イーサネットケーブルは、アクセスポイントと設置面との間の狭いスペースに収まるように、平らなケーブルを使用することをお勧めします。

アクセスポイントをマウントする前に、まずアクセスポイントをセットアップしてテストし、WiFiネットワークの接続性を確認します。

この付録には以下のセクションが含まれる：

取付部品

パッケージには以下の取り付け部品が含まれる：

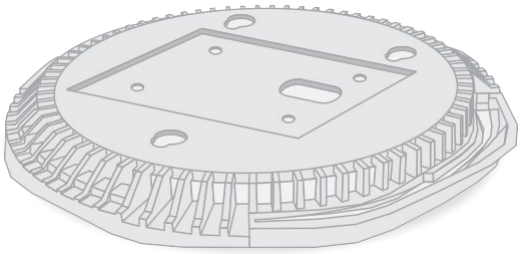


図 11.取り付けプレート

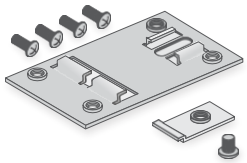


図12.メタルブラケット、Tバーロック、ロックネジ、短いネジ4本付き

図13.背の高いネジ3本と壁取り付け用アンカー

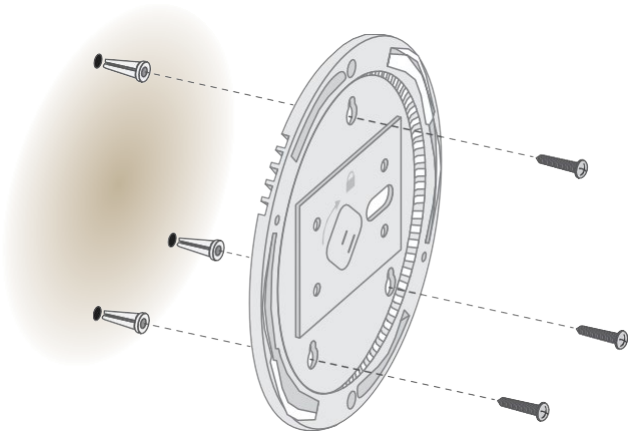
アクセスポイントを壁に取り付ける

注意：壁に損傷がないことを確認してください。例えば、水濡れは乾式壁を破壊する可能性があります。

アクセスポイントを壁に取り付けるには

1. マウンティングプレートを壁に設置します。
2. 取り付け穴のある壁に印をつける。
3. 3/16インチ（4.7mm）のドリルビットを使い、壁に穴を開ける。
4. アンカーが壁と面一になるまで、柔らかい木槌で各アンカーを壁に叩き込む。
5. ネジを使ってマウンティングプレートを壁に取り付けます。

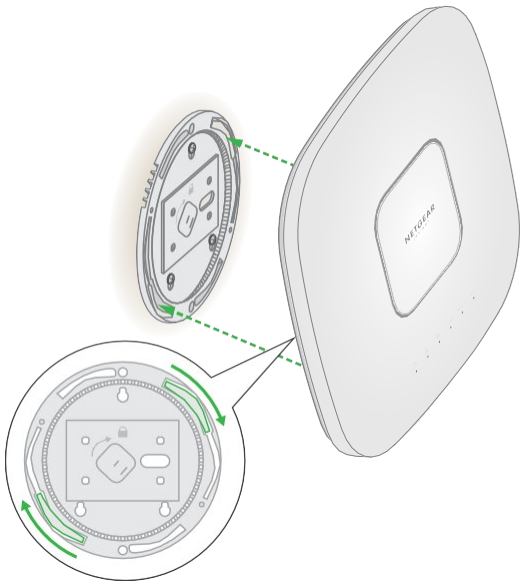
   注意：アンカーなしで壁にネジを差し込まないでください。



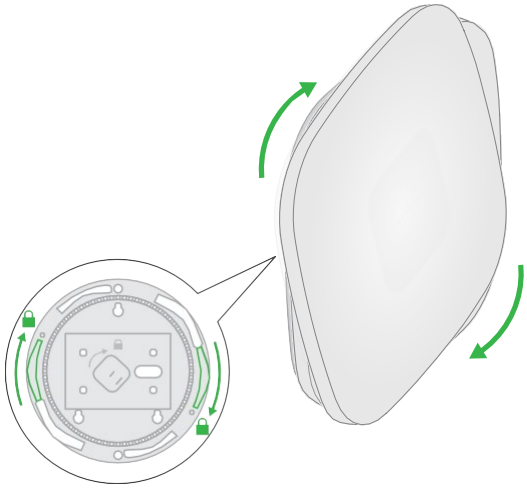
6. アクセス ポイントを取り付けプレートに取り付ける前に、イーサネット ケーブル（PoE++ スイッチを使用する場合）、または電源アダプタとイーサネット ケーブルの両方をアクセス ポイントに接続します。

   アクセスポイントを壁に取り付けると、平らになります。

7. アクセス ポイントを取り付けプレートに取り付けます。



8. アクセス ポイントを時計回りにねじって、取り付けプレートにロックします。

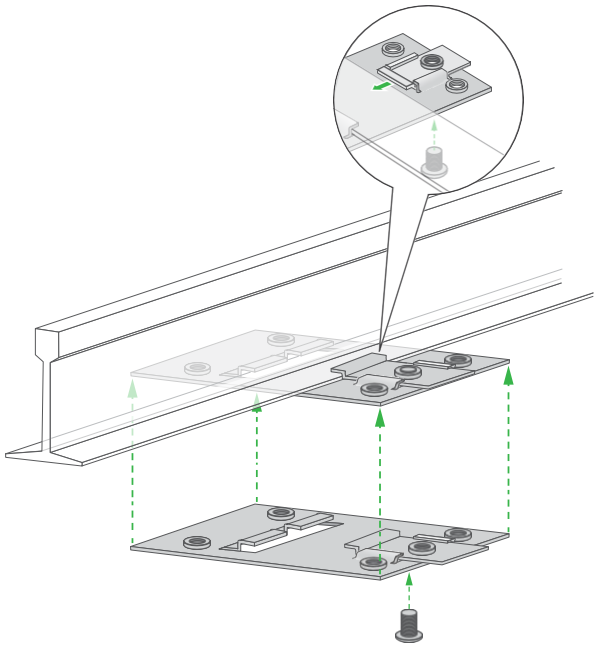


アクセスポイントをTバーに取り付ける

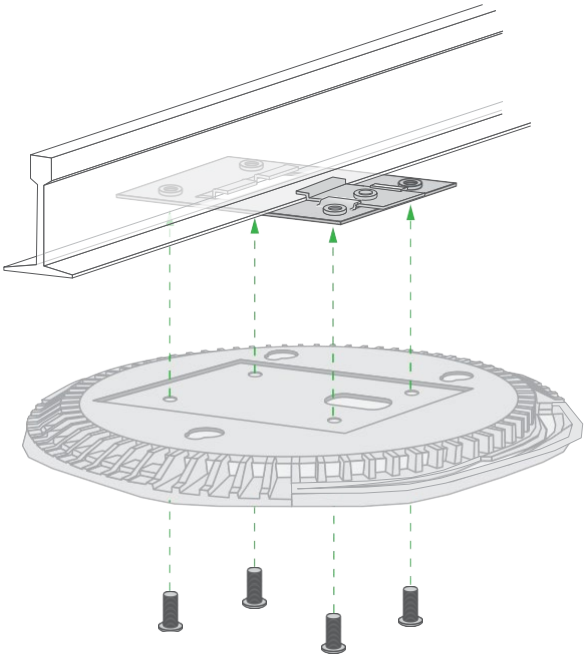
アクセスポイントを T バーに取り付けるには、次の手順に従います：

1. Tバー・ロックがまだメタル・ブラケットに取り付けられていない場合は、Tバー・ロックをメタル・ブラケットに部分的にスライドさせます。
2. メタルブラケットをTバーに取り付ける。
3. TバーロックをTバーの上に押します。

4. ロックスクリューを使用して、金属ブラケットを所定の位置にロックします。



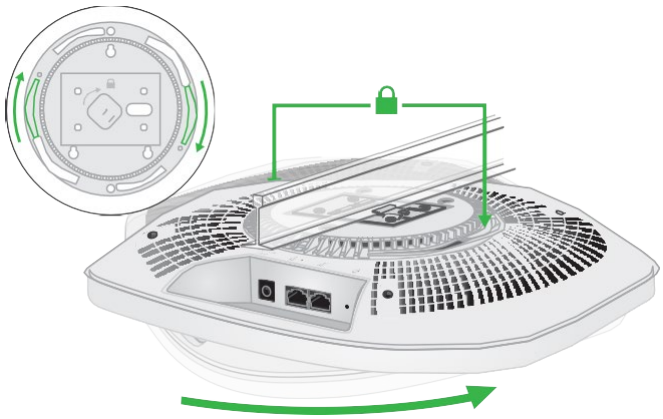
5. 4本の短いネジを使ってマウンティングプレートをTバーに取り付けます。



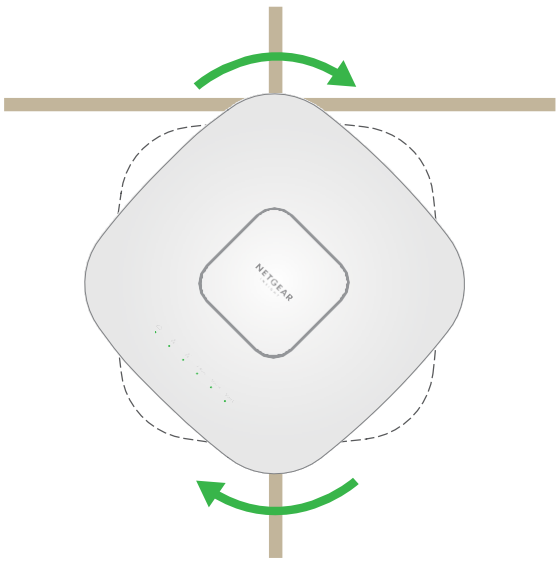
6. アクセス ポイントを取り付けプレートに取り付ける前に、イーサネット ケーブル（PoE++ スイッチを使用する場合）、または電源アダプタとイーサネット ケーブルの両方をアクセス ポイントに接続します。

   アクセスポイントを取り付けると、天井面に平らに設置されます。

7. アクセスポイントを逆さまに持ち、マウントプレートに取り付けます。



8. アクセス ポイントを、取り付けプレートにロックされるまで時計回りに回します。

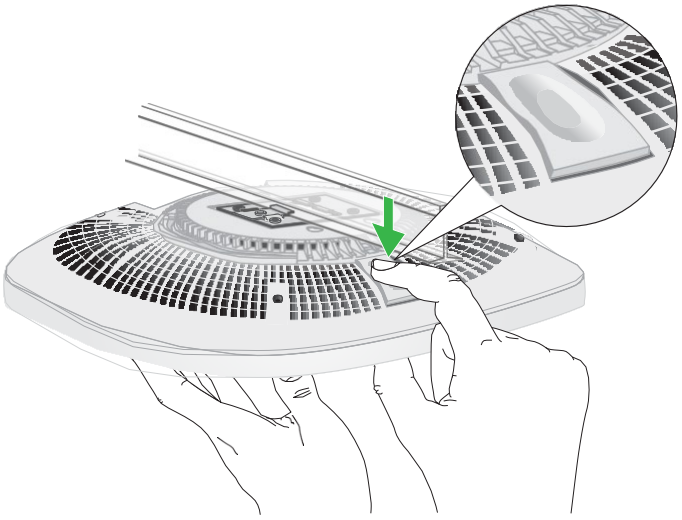

NETGEAR

アクセスポイントのアンマウント

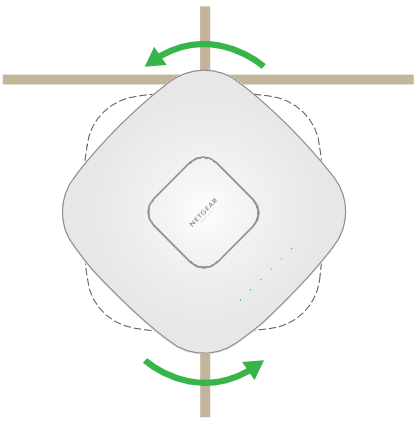
注意：アクセス ポイントを取り付けプレートから離すときに、落下しないように持 ってください。

アクセスポイントをアンマウントするには

1. 親指をLEDの中央に、指をアクセスポイントの反対側、親指と正反対に置いて、ロックラッチを見つけます。
2. ラッチを押し下げるとロックが解除され、ロックが開いたままになります。



3. アクセス ポイントが取り付け板から外れるまで、アクセス ポイントを反時計回りに回します。



4. アクセス ポイントを取り付けプレートから取り外します。
   取り付けプレートは天井や壁に取り付けたままです。