NETGEAR®

ユーザーマニュアル

Insight Managed WiFi 6 AX1800 デュアルバンド アクセスポイント

WAX610、屋内用モデル
WAX610Y、屋外用モデル

2023年1月
202-12099-07

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では、ご質問への回答や最新ダウンロードへのアクセスを提供しています。

また、community.netgear.comのNETGEARコミュニティで役立つアドバイスを得ることができます。

規制・法律

本製品がカナダで販売されている場合、vous pouvez accéder à ce document en français canadien à https://www.netgear.com/support/download/.

(本製品がカナダで販売されている場合、このドキュメントにはカナダ・フランス語でアクセスできます。https://www.netgear.com/support/download/)。

EU Declaration of Conformityを含む規制対応情報については、https://www.netgear.com/about/regulatory/ をご覧ください。

電源を接続する前に、規制遵守のドキュメント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 を参照してください。

このデバイスを使用することで、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。同意できない場合は、返品期間内にデバイスを購入先に返送してください。

本機を屋外で使用しないでください。PoE源は建物内接続専用です。

6GHz 機器にのみ適用されます：本機器は屋内でのみ使用してください。6GHz機器の操作は、石油プラットフォーム、自動車、列車、ボート、航空機では禁止されています。ただし、10,000フィート以上飛行中の大型航空機では、この機器の操作が許可されています。
無人航空機システムの制御や通信のために、5.925～7.125GHz帯の送信機を操作することは禁止されています。

商標について

改訂の経緯

出版物の品番	発行日	コメント
202-12099-07	2023年1月	マルチキャスト DNS ゲートウェイを管理する（159 ページ）」および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について、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。
202-12099-06	2022年9月	以下の項目を追加しました： WiFi ネットワークの Multi PSK を設定する (90 ページ) L2 セキュリティを有効にする (145 ページ) エネルギー効率モードを管理する（P.190） 以下の項目を改訂しました： 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 10ページ 初期設定のためにアクセスポイントに接続する 33ページ NETGEAR Insight Cloud Portal を使用してインターネット経由で接続する（34 ページ NETGEAR Insightアプリを使用してWiFiで接続する（35ページ 初期設定のためのローカルブラウザーUIにWiFiで接続する（38ページ その他、複数のセクションでマイナーチェンジや改良を行いました。
202-12099-05	2022年6月	アクセスポイントに新しいファームウェアを確認させるオプションを文書化するため、以下の項目を改訂しました： 初期設定のためのローカルブラウザーUIにWiFiで接続する（38ページ LANで接続して、ローカルのブラウザーUIで初期設定を行う（43ページ 屋内型WAX610を直接接続したコンピューターでオフラインで設定する 48ページ 62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、66ページの「インサイト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」を改訂しました。
202-12099-04	2022年3月	118ページの「アクセスポイントのFacebook Wi-Fiの登録と設定」を修正しました。 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MACアクセス制御リストの管理（130ページ）」を参照）。 RADIUS サーバーのセットアップ（143 ページ）を改訂しました。 215ページの「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。 251ページにCapture WiFi and Ethernet packetsを追加しました。その他、細かな変更を行いました。

(続き)

出版物品番	発行日	コメント
202-12099-03	2021年7月	Day Zero Easy Setup ページで認証オプションとして Enhanced Open、WPA3 Personal、WPA3/WPA2 Personal WiFi セキュリティを追加しました。33 ページの「初期設定のためにアクセスポイントに接続する」の項を参照してください。 55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」を追加しました。拡張オープンWiFiセキュリティをサポートしていないデバイスについて、拡張オープンWiFiセキュリティが有効な場合に、それらのデバイスのアクセスを許可するオプションを追加しました。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（72 ページ）および WiFi ネットワークの認証と暗号化の変更（85 ページ）を参照してください。WPA3 Enterprise WiFi セキュリティオプションを追加しました。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 (72 ページ)、および WiFi ネットワークの認証と暗号化の変更 (85 ページ) を参照してください。 WiFiクライアント分離の対象外となるネットワークデバイスを指定するオプションを追加しました。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（216 ページ）を参照してください。 マニュアルを再編成し、高度なWiFi機能を別の章に配置し、224ページに WiFiネットワークの高度な料金選択を設定することを追加しました。 微修正を行いました。 複数のマイナーチェンジや改良を行いました。
202-12099-02	2020年10月	以下の項目を削除しました：Secure Shellを有効または無効にする。
202-12099-01	2020年8月	屋外用モデルである「WAX610Y」を追加しました。
202-12098-01	2020年7月	初出版です。

目次

第14章 WiFiブリッジをセットアップする

第15章 無線の高度な機能を管理する

第16章 診断とトラブルシューティング

1

はじめに

本書は、以下のNETGEAR Insight Managed WiFi 6 AX1800 Dual Band Access Pointのモデル用です：

- WAX610：NETGEAR Insight Managed WiFi 6 AX1800 Dual Band Access Point（屋内用）。
- WAX610Y：NETGEAR Insight Managed WiFi 6 AX1800 Dual Band Access Point（屋外用）。

WAX610およびWAX610Y（本書ではアクセスポイントと表記）は、IEEE 802.11ax、4ストリーム（2+2）のWiFi 6、およびデュアルバンド同時動作に対応し、以下の機能を備えています。
2.4GHzと5GHzを合わせて1800Mbps（2.4GHz：600Mbps、5GHz：1200Mbps）のスループットを実現しました。

このアクセスポイントは、PoE+スイッチに接続された既存のネットワークにおいて、Power over Ethernet plus（PoE+）のパワードデバイス（PD）として機能します。モデルWAX610は、通常のスイッチに接続するためのオプションの電源アダプターをサポートしています。PoE+イーサネットポートは、最大2.5Gbpsの高速通信に対応しています。

この章では、次の項目を説明します：

- 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
- 追加ドキュメント

注：このマニュアルで扱わ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参照してください。
注：新機能やバグフィックスを含むファームウェアのアップデートは、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は、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、このマニュアルに記載されているものと一致しない場合は、ファームウェアの更新が必要な場合があります。
注：本書において、***WiFi***ネットワークとは、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ネットワークという場合は、個々のSSIDまたはVAPを意味します。

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およびアドオンサービスを提供します。NETGEAR Insight PremiumとInsight Proの契約者の場合、アクセスポイントはNETGEAR Insight Cloud PortalとInsightアプリをサポートします：

- **インサイトクラウドポータル**：クラウドベースの管理プラットフォーム「Insight」のポータルサイトを通じて、アクセスポイントの設定や管理をリモートで行うことができます。
- **Insightアプリ**：iOSまたはAndroidの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・管理でき、クラウドベースの管理プラットフォーム「Insight」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 Cloud Portal 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 でマスクされます。ただし、ローカルブラウザー UI を使用して、Insight でまだサポートされていない可能性のある特定の機能の設定を管理することは可能です。

追加ドキュメント

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

- インストールガイド
- データシート

NETGEAR Insight Cloud PortalとInsightアプリについては、netgear.com/business/services/insight/subscriptionをご覧いただき、netgear.com/support/product/insight.aspxのNETGEAR knowledge baseをご覧下さい。

2

ハードウェアの概要 インドアモデル WAX610

NETGEAR Insight Managed WiFi 6 AX1800 Dual Band Access Point Model WAX610は、*屋内用*アクセスポイントです。

この章には、次の項目があります：

屋内用モデルWAX610を開梱

パッケージには以下のものが入っています：

- アクセスポイント「WAX610
- 天井または15/16インチ（23.8mm）Tバーに取り付けるためのネジ穴付きマウントブラケット
- 9/16インチ（14.3mm）Tバーに取り付けるためのネジ穴のないマウントブラケット
- 天井取り付け用または壁取り付け用のネジとアンカーを2本。
- ネジ穴配置ガイド
- インストールガイド

注：ご注文の製品によっては、パッケージに電源アダプターが含まれていない場合があります。アクセスポイントをPoE+スイッチに接続することで電源を供給します。電源アダプターのないパッケージを注文した場合でも、オプションとして電源アダプターを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、「屋内型WAX610を壁や天井に取り付ける」（277ページ）を参照してください。

LED付きトップパネル、屋内用モデルWAX610

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配置されています。

図1.トップパネルにLEDを配置した屋内用モデルWAX610

表1.LEDの説明 屋内モデル WAX610

LED アイコン	色	説明
電源/クラウドLED 		**最初はオレンジ色に点灯し、その後ゆっくりとオレンジ色に点滅**：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、またはその過程にあります。
		**緑色に点灯**：アクセスポイントは起動し、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検出アクセスポイントとして機能します。
		**青色の実線**：アクセスポイントはInsightモードで機能し、クラウドベースの管理プラットフォームInsightに接続されています。
		**オレンジ色が速く点滅**：アクセスポイントは、ファームウェアを更新中、または工場出荷時の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 Network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しています。
		**動作中、オレンジ色が点灯**：アクセスポイントが受信したPoE電力は、802.3at（PoE+）の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ない状態です。
LAN LED 		**緑色に点灯**：LANポートで2.5Gbpsのイーサネットリンクが検出されています。
		**緑点滅**：LANポートで2.5Gbpsのトラフィックアクティビティを検知しています。
		**オレンジ色で点灯**：LANポートで2.5Gbps以下のイーサネットリンクが検出されています。
		**オレンジ色に点滅**：LANポートで2.5Gbps以下のトラフィックが検出されました。
		オフ：LANポートにイーサネット機器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ない状態です。

表1.LEDの説明 屋内モデルWAX610（続き）

LED アイコン	色	説明
2.4G WLAN LED 2.4GHz		**緑色に点灯**：2.4GHzのWiFiは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。
		青色で点灯：2.4GHzのWiFiに1台以上のWLANクライアントが接続されています。
		青色に点滅：2.4GHzのWiFiでトラフィックを検知しています。
		オフ：2.4GHzのWiFiがオフになっています。
5G WLAN LED 5GHz		**緑色に点灯**：5GHz WiFiは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。
		青色で点灯：1つ以上のWLANクライアントが5GHzに接続されています。
		青色に点滅：5GHz帯のWiFiでトラフィックを検知しています。
		オフ：5GHzのWiFiがオフになっています。

注：LEDを使ったトラブルシューティングについては、「LEDを使ったトラブルシューティング（256ページ）」を参照してください。

ハードウェア・インターフェース 室内モデル WAX610

アクセスポイントの底面には、LAN/PoE+ポート、**リセット**ボタン、オプションの電源アダプター用DC電源コネクターがあります。

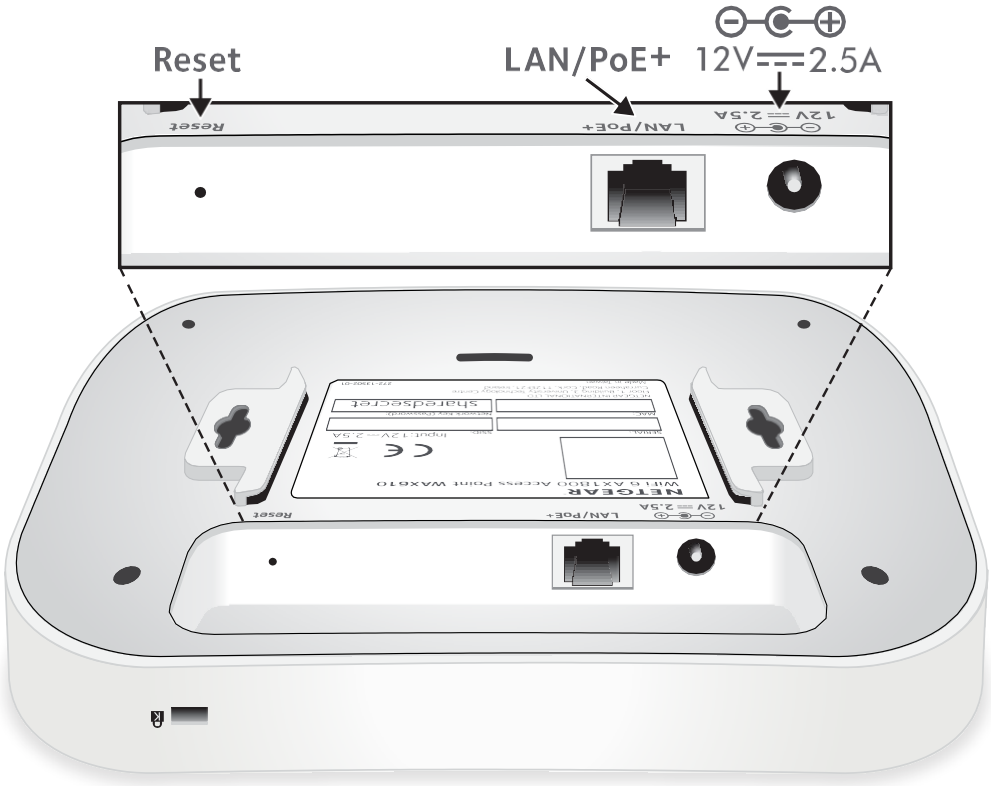


図2.屋内用モデル「WAX610」のハードウェア・インターフェース

パネルには、以下のコンポーネントがあります：

- **Reset（リセット）ボタン**：**リセットボタンを**使用すると、アクセスポイントを再起動したり、アクセスポイントを工場出荷時の設定に戻したりすることができます。アクセスポイントを再起動するには、**Reset** ボタンを約 2 秒間押してください。**リセットを** 10 秒以上押すと、アクセスポイントは工場出荷時の設定にリセットされます。

  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設定機能を利用する前に、まず Insight Cloud Portal 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、184 ページの「屋内モデル WAX610 をリセットするには、リセットボタンを使用する」を参照してください。

- **LAN/PoE+ポート**：LAN/PoE+ギガビットイーサネットRJ-45LANポートを使用して、アクセスポイントをPoE+スイッチに、またはオプションの電源アダプタを使用する場合は、非PoEスイッチに接続することができます。
  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に対応します。インターネット接続、モデム、ルーター、スイッチが2.5Gbpsの速度に対応している場合、アクセスポイントのインターネット接続も2.5Gbpsで動作します。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/PoE+ポートの接続については、30ページの「屋内型WAX610のセットアップとネットワークへの接続」をご覧ください。
- **DC電源コネクター**：アクセスポイントへの電力供給にPoE+スイッチを使用しない場合、オプションの電源アダプターをDC電源コネクターに接続します。

注：バックパネルには、オプションのセキュリティケーブル用のケンジントンロックスロットが用意されています。

製品ラベル 屋内型 WAX610

アクセスポイントの製品ラベルには、アクセスポイントのQRコード、シリアル番号、MACアドレス、設定用WiFiネットワーク名（SSID）、ネットワークキー（パスワード）が記載されています。

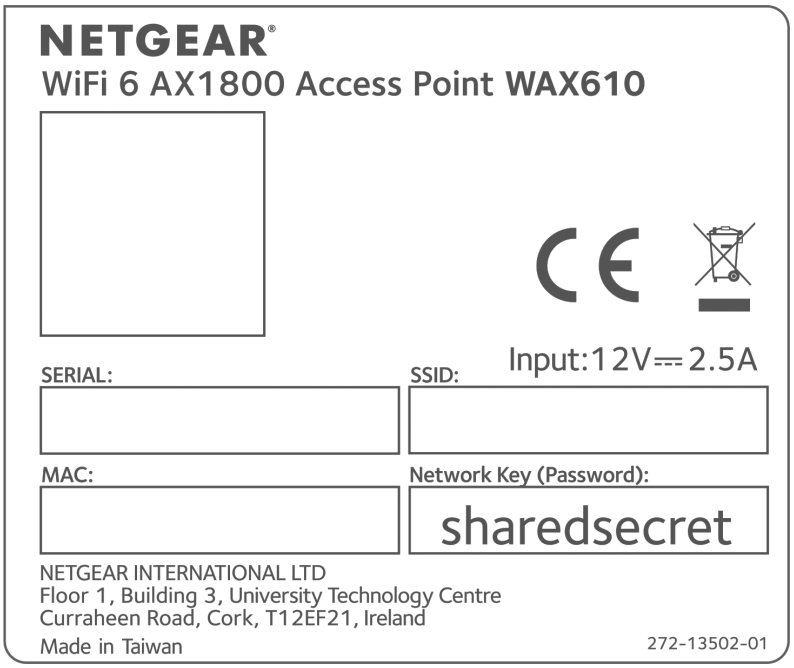


図 3.製品ラベル屋内型WAX610

屋内用アクセスポイントに関する安全上のご注意と注意事項

以下の安全ガイドラインを使用して、お客様自身の安全を確保し、潜在的な損害からシステムを保護するために役立ててください。

人身事故、感電事故、火災事故、装置破損のリスクを低減するため、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のみを想定しています。次のことに注意してください：
  - 本製品を使用しなければならない環境の詳細については、付録の環境仕様書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にある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、製品に損傷を与える可能性があります。
  - 製品を屋外ケーブルや有線屋外機器に接続する前に、https://kb.netgear.com/000057103、追加の安全性と保証に関する情報を参照してください。

  これらのガイドラインに従わない場合、NETGEAR 製品が損傷し、適用法の許す範囲で NETGEAR の保証が適用されない可能性があります。
- 製品マニュアルに説明されていること以外は、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。
- 次のような状態になった場合は、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提供者に連絡してください：
  - 電源アダプター、電源アダプターケーブル、電源アダプタープラグ、PoEイーサネットケーブルが破損している。
  - 製品に物体が落下した。
  - 製品が水にさらされた。
  - 製品を落下させたり、破損させたりした。
  - 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。
- 本製品をラジエーターや熱源から遠ざけてください。また、冷却用の通気孔をふさがないようにしてください。

- 製品のコンポーネントに食べ物や液体をこぼしたり、濡れた環境で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適切なセクションを参照するか、訓練を受けたサービスプロバイダー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て、火災や感電の原因になることがあります。
- 本製品は、認可された装置でのみ使用してください。
- お使いの製品が該当する場合は、カバーを外したり、内部の部品に触れたりする前に、製品が冷えていることを確認してください。
- イーサネットケーブルで接続される機器は、お住まいの地域で利用可能な電力で動作するように電気的な定格が設定されていることを確認してください。
- 製品によっては、付属の電源アダプターまたはPoEを提供する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対応した定格のものを使用してください。
- 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、適切にアースされた電源コンセントに接続してください。
- お使いの製品に適用される場合、周辺機器の電源ケーブルには、適切な接地を確保するための3つのプロング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、ケーブルからアース用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が付いた3線式のケーブルを使用してください。
- 延長ケーブルと電源タップの定格を守ってください。延長ケーブルや電源タップに接続されたすべての製品のアンペア定格の合計が、延長ケーブルや電源タップのアンペア定格の制限の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ために、サージサプレッサー、ラインコンディショナー、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、電源アダプターケーブル、PoEイーサネットケーブルは、慎重に配置してください。ケーブルは、踏んだりつまずいたりしないように配線してください。ケーブルの上に何も乗っていないことを確認してください。
- 電源アダプター、電源アダプターケーブル、プラグの改造はしないでください。改造する場合は、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

ハードウェアの概要 屋外用モデル WAX610Y

NETGEAR Insight Managed WiFi 6 AX1800 Dual Band Access Point Model WAX610Yは、*屋外用*アクセスポイントです。

使用上の注意：このデバイスは専門家が設置する必要があります。設置者の責任において、合法的な周波数チャンネル内での操作、出力電力、DFS要件など、各国の規制を遵守してください。ベンダー、リセラー、販売店は、違法な無線操作に責任を負いません。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。

この章には、次の項目があります：

開梱モデル 屋外モデル WAX610Y

パッケージには、以下のものが入っています：

- アクセスポイント「WAX610Y
- ポールマウントストラップ
- 壁掛け用ネジ・アンカー
- スクリュープレイスメントガイド
- インストールガイド

注：このモデルでは、電源アダプターはサポートされていません。アクセスポイントをPoE+スイッチに接続することで電源を供給します。

取り付けオプションについては、「屋外モデルWAX610Yを壁や柱に取り付ける」（285ページ）を参照してください。

LED付きサイドパネル、屋外用WAX610Y

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右サイドパネルに配置されています。

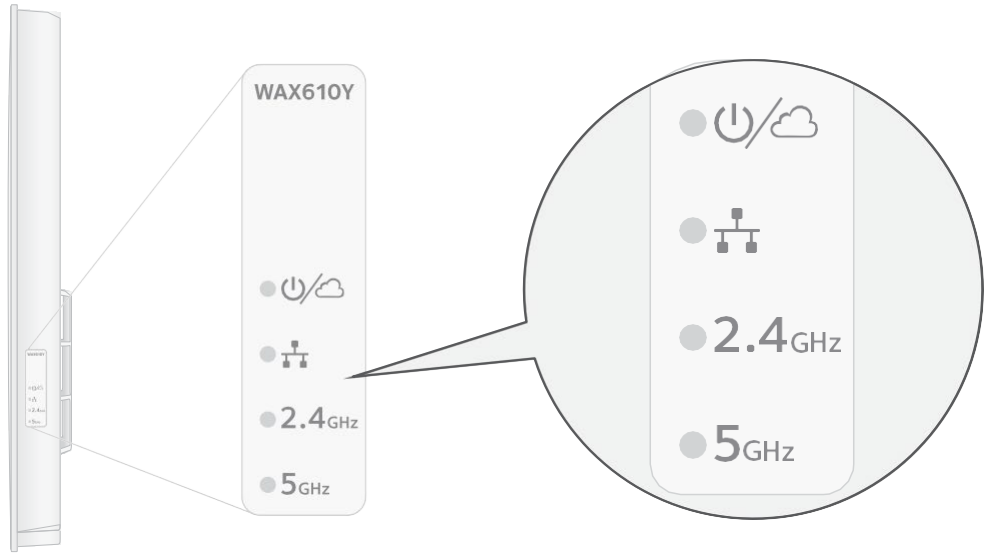


図4.LED付きサイドパネル、屋外用WAX610Y

表2.LEDの説明 屋外モデル WAX610Y

LED	色	説明
電源/クラウドLED 		**最初はオレンジ色に点灯し、その後ゆっくりとオレンジ色に点滅**：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、またはその過程にあります。
		緑色に点灯：アクセスポイントは起動し、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検出アクセスポイントとして機能します。
		青色に点灯：アクセスポイントはInsightモードで機能し、クラウドベースの管理プラットフォームInsightに接続されています。
		**オレンジ色が速く点滅**：アクセスポイントは、ファームウェアを更新中、または工場出荷時の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 Network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しています。
		動作中、オレンジ色に点灯：アクセスポイントが受信したPoE電力は、802.3at（PoE+）の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ない状態です。
LAN LED 		**緑色に点灯**：LANポートで2.5Gbpsのイーサネットリンクが検出されています。
		**緑点滅**：LANポートで2.5Gbpsのトラフィックアクティビティを検知しています。
		オレンジ色に点灯：LANポートで2.5Gbps以下のイーサネットリンクが検出されています。
		**オレンジ色に点滅**：LANポートで2.5Gbps以下のトラフィックが検出されました。
		オフ：LAN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ない状態です。
2.4G WLAN LED 		**緑色に点灯**：2.4GHzのWiFiラジオは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。
		青色に点灯：2.4GHzのWiFiに1台以上のWLANクライアントが接続されています。
		**青色に点滅**：2.4GHzのWiFiでトラフィックを検知しています。
		オフ：2.4GHzのWiFiがオフになっています。

表2.LEDの説明 屋外モデルWAX610Y（続き）

LED アイコン	カラ	商品説明
5G WLAN LED 5GHz	●	**緑色に点灯**：5GHz WiFiは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。
	●	**青色に点灯**：1つ以上のWLANクライアントが5GHz WiFiに接続されています。
	✳	**青色に点滅**：5GHz帯のWiFiでトラフィックを検知しています。
		オフ：5GHzのWiFiがオフになっています。

注：LEDを使ったトラブルシューティングについては、「LEDを使ったトラブルシューティング」（256ページ）を参照してください。

ハードウェア・インターフェース 屋外用モデル WAX610Y

アクセスポイントの前面にあるラッチを使用して、カバーを開きます。ラッチを注意深く手前に引き、カバーを下方向に引いて、筐体からスライドさせます。アクセス ポイントの底部パネルで、LAN/PoE+ ポートと**リセット** ボタンにアクセスできるようになりました。

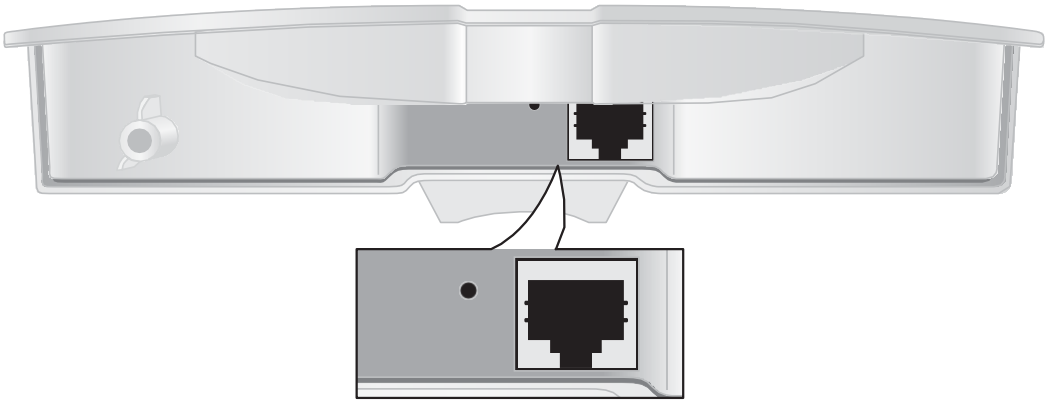


図 5.ハードウエア・インターフェース 屋外モデル WAX610Y

注：アクセスポイントには、電源コネクタはなく、電源アダプタも必要ありません。アクセスポイントの電源は、イーサネットケーブルをPoE+スイッチに接続することによってのみ供給されます。

パネルには、以下のコンポーネントがあります：

- **Reset（リセット）ボタン：リセットボタンを**使用すると、アクセスポイントを再起動したり、アクセスポイントを工場出荷時の設定に戻したりすることができます。アクセスポイントを再起動するには、**Reset** ボタンを約 2 秒間押してください。**リセットを** 10 秒以上押すと、アクセスポイントは工場出荷時の設定にリセットされます。
  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設定機能を利用する前に、まず Insight Cloud Portal 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、184 ページの「屋内モデル WAX610 をリセットするには、リセットボタンを使用する」を参照してください。

- **LAN/PoE+ポートを使用します**：アクセスポイントをPoE+スイッチに接続するには、LAN/PoE+ギガビットイーサネットRJ-45 LANポートを使用する必要があります。
  注意：屋内にあるPoE+スイッチを使用する場合、スイッチから屋外にあるアクセスポイントまでのケーブルにPoE+イーサネットサージプロテクター（非付属）を使用する必要があります。

  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に対応します。インターネット接続、モデム、ルーター、スイッチが2.5Gbpsの速度に対応している場合、アクセスポイントのインターネット接続も2.5Gbpsで動作します。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/PoE+ポートの接続については、30ページの「屋内型WAX610のセットアップとネットワークへの接続」をご覧ください。

製品ラベル 屋外用モデル WAX610Y

アクセスポイントの製品ラベルには、アクセスポイントのQRコード、シリアル番号、MACアドレス、設定用WiFiネットワーク名（SSID）、ネットワークキー（パスワード）が記載されています。

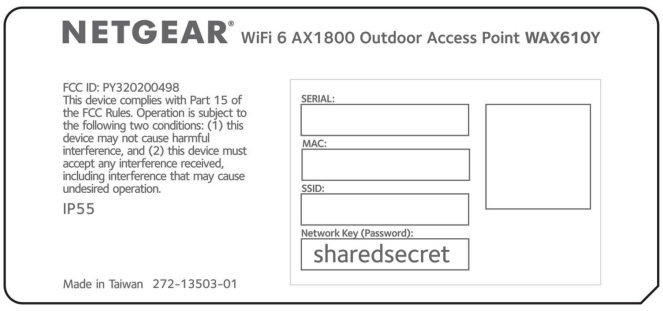


図 6.製品ラベル屋外用WAX610Y

屋外用アクセスポイントに関する安全上のご注意と注意事項

以下の安全ガイドラインを使用して、お客様自身の安全を確保し、潜在的な損害からシステムを保護するために役立ててください。

人身事故、感電事故、火災事故、装置破損のリスクを低減するため、以下の注意事項を守ってください：

- 本製品は屋外での使用を想定しています。以下のことに注意してください：
  - 本製品が動作しなければならない環境については、付録の環境仕様書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内の機器に接続する場合は、本製品と屋内の機器の間にイーサネットサージプロテクタをインラインで設置する必要があります。これを怠ると、製品にダメージを与える可能性があります。
  - 製品を屋内ケーブルまたは有線屋内機器に接続する前に、追加の安全および保証情報については、https://kb.netgear.com/000057103 を参照してください。

  これらのガイドラインに従わない場合、NETGEAR 製品が損傷し、適用法の許す範囲で NETGEAR の保証が適用されない可能性があります。
- 製品マニュアルに説明されていること以外は、製品を修理しないでください。機器によっては、絶対に開けてはいけないものがあります。
- 次のような状態になった場合は、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提供者に連絡してください：
  - 電源アダプター、電源アダプターケーブル、電源アダプタープラグ、PoEイーサネットケーブルが破損している。
  - 製品に物体が落下した。
  - 製品を落下させたり、破損させたりした。
  - 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。
- 湿気や虫が製品内部に入らないように、カバーを閉じた状態で操作してください。
- 本製品は、浸水する可能性のある場所や、ホースパイプなどから大量の水がかかるような場所に設置しないよう注意してください。
- 本製品を熱源から遠ざけてください。直射日光が当たり続ける場所には設置しないでください。また、冷却用の通気口をふさがないようにしてください。

- 本製品に塗装をしないでください。
- 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て、火災や感電の原因になることがあります。
- 本製品は、認可された装置でのみ使用してください。
- お使いの製品が該当する場合は、カバーを外したり、内部の部品に触れたりする前に、製品が冷えていることを確認してください。
- イーサネットケーブルで接続される機器は、お住まいの地域で利用可能な電力で動作するように電気的に定格されていることを確認してください。
- 製品によっては、付属の電源アダプター、またはPoEを使用する場合は、インラインEthernetサージプロテクターが装着されたEthernet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対応した定格のものを使用してください。
- 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、適切にアースされた電源コンセントに接続してください。
- お使いの製品に適用される場合、周辺機器の電源ケーブルには、適切な接地を確保するための3つのプロング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、ケーブルからアース用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が付いた3線式のケーブルを使用してください。
- 延長ケーブルと電源タップの定格を守ってください。延長ケーブルや電源タップに接続されたすべての製品のアンペア定格の合計が、延長ケーブルや電源タップのアンペア定格の制限の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ために、サージサプレッサー、ラインコンディショナー、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、電源アダプターケーブル、PoEイーサネットケーブルは、慎重に配置してください。ケーブルは、踏んだりつまずいたりしないように配線してください。ケーブルの上に何も乗っていないことを確認してください。
- 電源アダプター、電源アダプターケーブル、プラグの改造はしないでください。改造する場合は、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。

4

ネットワークにアクセスポイントを設置し、アクセスポイントにアクセスして初期設定を行う。

この章では、ネットワークにアクセスポイントを設置し、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：

- アクセスポイントを最適な位置に設置する
- アクセスポイントを設定し、ネットワークに接続する
- 初期設定のためにアクセスポイントに接続する
- 屋内用WAX610を、直接接続したパソコンでオフラインで設定する場合
- 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方法について

注意：このデバイスは専門家が設置する必要があります。合法的な周波数チャンネル内での操作、出力電力、DFS要件など、各国の規制を遵守する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、違法な無線操作に対し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：本書において、*WiFi*ネットワークとは、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ネットワークという場合は、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

本書のインストールガイドまたは付録に記載されているようにアクセスポイントを設置し、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範囲内にいるWiFiクライアントは、WiFiネットワークに接続することができます。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変化することがあります。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があります。WiFi機器とは、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機器を指します。

アクセスポイントの位置決めのコツ：

- 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てください。アクセスポイントとWiFiクライアントの間の見通し線は、良好なパフォーマンスのために必要ではありません。
- モデルWAX610のみ、電源アダプターを使用する場合は、アクセスポイントがAC電源コンセントから届く範囲にあることを確認してください。
- アクセスポイントとWiFiクライアントの間の壁や天井を極力なくし、高所にアクセスポイントを設置する。
- モデルWAX610のみ、アクセスポイントをこれら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
  - コンピュターズ
  - コードレス電話機のベース
  - 2.4GHzおよび5.8GHzのコードレス電話機
- 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：
  - 厚い金属製ドア
  - 金属の骨組

- 水槽（屋内型WAX610のみ）
- ミラー（屋内用WAX610のみ）
- 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、干渉を減らすために異なる無線周波数チャンネルを使用します。詳しくは、「無線のチャンネルを変更する（107ページ）」を参照してください。

アクセスポイントを設定し、ネットワークに接続する

アクセスポイントの設定やネットワークへの接続は、機種によって手順が異なります。

屋内型WAX610の設定とネットワークへの接続

本項は、屋内型WAX610のみに適用されます。

アクセスポイントは、ネットワーク内のPower over Ethernet plus（PoE+、802.3at）スイッチに接続することができます。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ー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ーは必要ありません。

注：ご注文の製品によっては、パッケージに電源アダプターが含ま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+スイッチに接続することで供給します。電源アダプターのないパッケージを注文したが、PoE+接続を使用しない場合は、オプションとして電源アダプターを注文することができます。

2.5Gbpsの機器に接続した場合、アクセスポイントのLAN PoE+ポートは、LAN内で最大2.5Gbpsのイーサネット速度に対応します。下図は、2.5Gbps以上の速度とPoE+をサポートするNETGEAR MS510TXUPスイッチを示しています。インターネット接続、モデム、ルーター、スイッチが2.5Gbpsに対応している場合、アクセスポイントのインターネット接続も2.5Gbpsで動作します。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。

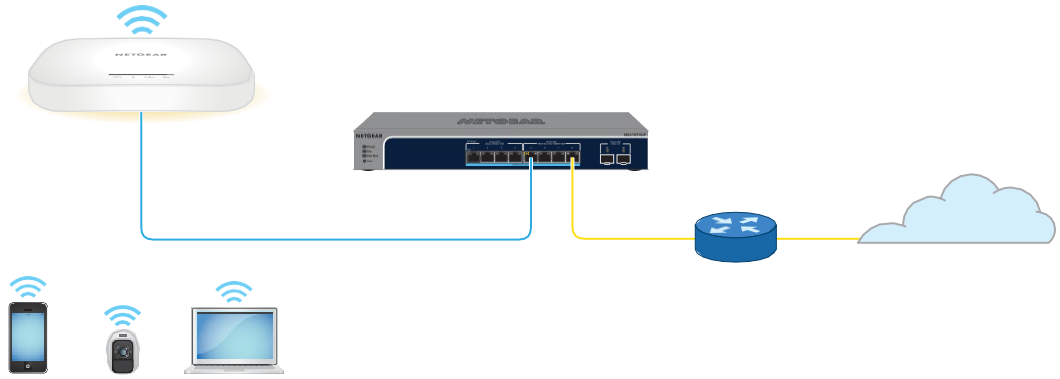


図 7.モデルWAX610をPoE+接続でネットワークにセットアップする

ネットワークにイーサネット接続したアクセスポイントを設定する場合：

1. アクセスポイントのLAN/PoE+ポートに、イーサネットケーブルを接続します。
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。
   アクセスポイントには802.3at（PoE+）入力が必要です。

   注：最適な機能を実現するには、802.3af（PoE）スイッチではなく、802.3at（PoE+）スイッチを使用することを確認してください。アクセスポイントの起動後、電源LEDがオレンジ色に点灯したままの場合は、アクセスポイントのPoE給電が不十分な可能性があります。詳しくは、「アクセスポイントが PoE PD として機能し、Power/Cloud LED がオレンジ色で点灯したままになっている（258 ページ）」を参照してください。

   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 アドレスを取得するために開始または処理中、電源/クラウド LED は最初オレンジ色の点灯で、その後オレンジ色をゆっくり点滅します。約 2 分後、電源/クラウド LED が緑色または青色で点灯し、アクセスポイントは、初期設定を実行する準備が整った状態になります。

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、「初期設定のためのアクセスポイントへの接続（33ページ）」を参照してください。

屋外用WAX610Yのセットアップとネットワークへの接続

本項は、屋外用モデル WAX610Y にのみ適用されます。

注：アクセスポイントを屋外の定位置に設置する前に、ネットワーク環境に応じてアクセスポイントを設定し、セットアップをテストすることをお勧めします。

アクセスポイントをネットワーク内のPower over Ethernet plus (PoE+, 802.3at) スイッチに接続します。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ーに接続する必要があります。屋内にある PoE+ スイッチを使用する場合は、スイッチから屋外にあるアクセスポイントへのケーブルに PoE+ イーサネットサージプロテクターを設置する必要があります。

注：モデルWAX610Yは、電源コネクタを提供せず、電源アダプタも必要としません。このモデルの電源は、PoE+スイッチにイーサネットケーブルを接続することによってのみ供給されます。

2.5Gbpsの機器に接続した場合、アクセスポイントのLAN PoE+ポートは、LAN内で最大2.5Gbpsのイーサネット速度に対応します。下図は、2.5Gbps以上の速度とPoE+をサポートするNETGEAR MS510TXUPスイッチを示しています。インターネット接続、モデム、ルーター、スイッチが2.5Gbpsに対応している場合、アクセスポイントのインターネット接続も2.5Gbpsで動作します。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。

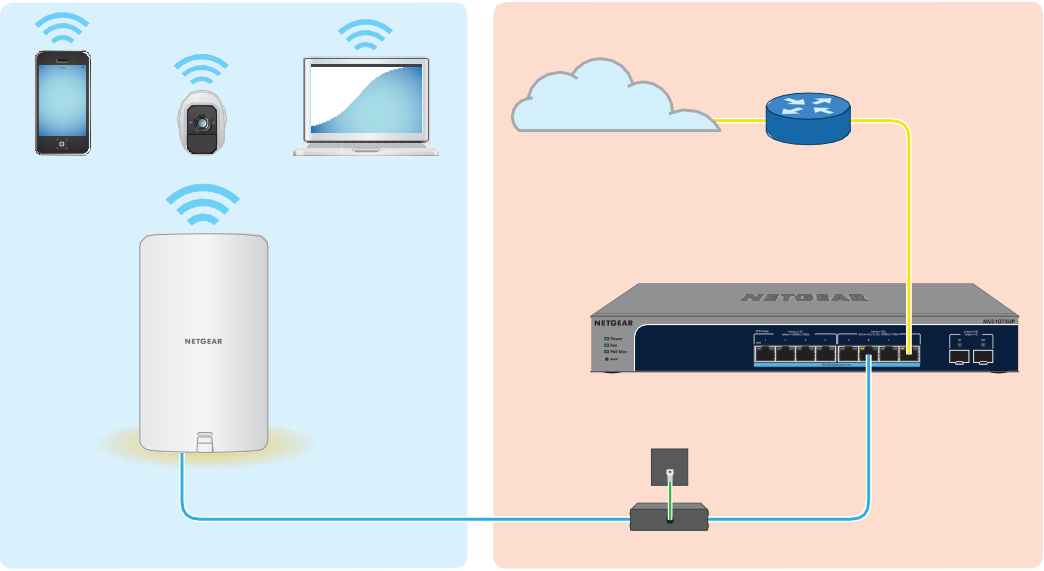


図 8.モデルWAX610YをPoE+接続でネットワークにセットアップする

ネットワークにイーサネット接続したアクセスポイントを設定する場合：

1. アクセスポイント前面のラッチを使って、カバーを開けます。
   ラッチを注意深く手前に引き、カバーを下方向に引いて、筐体からスライドさせるようにします。これで、LAN/PoE+ポートにアクセスできるようになりました。
2. アクセスポイントのLAN/PoE+ポートにイーサネットケーブルを接続します。
3. 屋内にあるPoE+スイッチを使用する場合、スイッチから屋外にあるアクセスポイントまでのケーブルにPoE+イーサネットサージプロテクター（別売）を設置します。前の図は、そのような設定を示しています。

4. 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PoE+スイッチのポートに接続します。

   アクセスポイントには802.3at（PoE+）入力が必要です。
   注：最適な機能を実現するには、802.3af（PoE）スイッチではなく、802.3at（PoE+）スイッチを使用することを確認してください。アクセスポイントの起動後、Power LEDがオレンジ色に点灯したままの場合は、アクセスポイントのPoE電源が不足している可能性があります。詳しくは、「アクセスポイントが PoE PD として機能し、Power/Cloud LED がオレンジ色で点灯したままになっている（258 ページ）」を参照してください。

   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アドレスを取得するために開始または処理中に、電源/クラウドLEDは最初オレンジ色の点灯で、その後オレンジ色がゆっくり点滅します。約 2 分後、電源/クラウド LED が緑色または青色で点灯し、アクセスポイントが初期設定を実行できる状態になります。

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、「初期設定のためのアクセスポイントへの接続（33ページ）」を参照してください。

初期設定のためにアクセスポイントに接続する

アクセスポイントを設定した後、いくつかの方法でアクセスポイントに接続して初期設定を行います。

アクセスポイント（および複数のデバイスやネットワーク）のリモート管理には、コンピューターやタブレット上のNETGEAR Insight Cloud PortalまたはiOSまたはAndroidモバイルデバイス上の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、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、12 ページの「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」を参照してください。

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

- NETGEAR Insight Cloud Portal を使用してインターネット経由で接続する (34 ページ)
- NETGEAR Insightアプリを使用してWiFiで接続する（35ページ

ローカルブラウザーUIの使用方法については、以下のいずれかのセクションを参照してください：

- 初期設定のためのローカルブラウザーUIにWiFiで接続する（38ページ
- LANで接続して、ローカルのブラウザーUIで初期設定を行う（43ページ

- 屋内型WAX610を直接接続したコンピューターでオフラインで設定する 48ページ

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行わない場合、アクセス ポイントに接続できるクライアントは 5 台のみ、アクセス ポイントが提供できる IP アドレスは 5 クライアントのみとなります。この の状況を防ぐには、アクセスポイントの初期設定を必ず行ってください。

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 の契約者が利用できます。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、Insight Pro ユーザーとしてログインできます。

Insight Cloud Portalを経由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場合：

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する。
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 Account Login ページが表示されます。
3. インサイトアカウントをまだお持ちでない方は、今すぐアカウントを作成することができます。
   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、「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ロケーションを追加するか、既存のネットワークロケーションを選択します。
7. 右上の＋（Add Device）ボタンをクリックします。

注：Insight Proユーザーの場合、単一のデバイスを追加するか、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することができます。

8. 新しいデバイスの追加」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、「**進む**」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. インサイト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後、オプションでアクセスポイントのデバイス名を変更し、**[次へ]**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、設定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および DNS エントリーを追加します。詳細については、kb.netgear.com/000062467 を参照してください。

   アクセスポイントは、最新のInsightファームウェアとInsightロケーション設定に自動的に更新されます。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 クラウドベース管理プラットフォームに接続されたInsight マネージドデバイスになりました。Power/Cloud LED が緑色の点灯だった場合、青色の点灯になります。

   Insight Cloud Portal または Insight アプリを使って、アクセスポイントの設定と管理を行うことができます。

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 Cloud Portal または Insight アプリでアクセスポイントを管理する場合、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した後、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、インサイト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 ブラウザに変更する（164 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、Insight ネットワークパスワードを使用してローカルブラウザ UI にアクセスし続ける必要があります。

NETGEAR Insightアプリを使ってWiFiで接続する

NETGEAR Insightアプリは、Insight PremiumおよびInsight Proの契約者向けに提供されています。

iOSまたはAndroidの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（その他にも多くのタスクを実行することができます）。

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、Insight Pro ユーザーとしてログインできます。

iOSまたはAndroidのモバイル端末を使用して、WiFiでアクセスポイントに接続する場合：

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

2. モバイル端末で、以下のいずれかの方法でアクセスポイントの設定したWiFiネットワークにWiFiで接続します：
   - **QRコードを読み取る**：アクセスポイント底面のラベルに記載されているQRコードを読み取ると、設定したWiFiネットワークに接続することができます。
   - **手動で接続**：設定されたWiFiネットワークはアクセスポイントのラベルに記載されており、NETGEARxxxxxx-SETUPという形式で表示されます（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します。
4. インサイトアカウントをまだお持ちでない方は、今すぐアカウントを作成することができます。

   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、「**LOG IN**」をタップします。
6. 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ロケーションを追加します。
   次へ」ボタンを押し、「**OK**」をタップします。
   また、既存のネットワークロケーションを選択することも可能です。

新しいネットワークロケーションに入力したデバイスの管理者パスワードは、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者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、それには数分かかることがあります。

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た場合は、アクセスポイントのアイコンをタップし、「デバイスの追加」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、トップバーの＋アイコンをタップし、次のいずれかを行ってください：

     - **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。
     - **シリアル番号の入力**」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て、「**次へ**」ボタンをタップします。

   アクセスポイントは、最新のInsightファームウェアとInsightロケーション設定に自動的に更新されます。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 管理対象デバイスとなりました。Power/Cloud LED が緑色の点灯だった場合、青色の点灯になります。

   Insight Cloud Portal または Insight アプリを使って、アクセスポイントの設定と管理を行うことができます。

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 Cloud Portal または Insight アプリでアクセスポイントを管理する場合、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 ブラウザに変更する（164 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 UI にアクセスするには Insight ネットワークパスワードを使用し続ける必要があります。

WiFiで接続し、ローカルブラウザのUIで初期設定を行う。

このセクションでは、WiFi 対応のコンピューターまたはモバイル デバイスを使用して（NETGEAR Insight アプリを使用せずに）WiFi で初めてアクセス ポイントに接続し、初期設定を完了する方法について説明します。

注）本項の図は、モデル WAX610 を示しています。モデルWAX610Yを使用する場合、ローカルブラウザのUIはモデルWAX610Yを表示します。

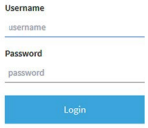
WiFiで接続し、ローカルのブラウザUIで初期設定を行うため：

1. パソコンやモバイル機器から、次のいずれかの方法で、アクセスポイントの設定したWiFiネットワークにWiFiで接続します：

   - **QRコードを読み取る**：アクセスポイント底面のラベルに記載されているQRコードを読み取ると、設定したWiFiネットワークに接続することができます。
   - **手動で接続する**：設定されたWiFiネットワークはアクセスポイントのラベルに記載されており、NETGEARxxxxxx-SETUPという形式で表示されます（xxxxxxはアクセスポイントのMACアドレスの下6桁の16進数です）。デフォルトのパスワードは**sharedsecret**です。

2. パソコンまたはモバイル端末でウェブブラウザを起動し、アドレスバーに「**http://aplogin.net**」と入力してください。

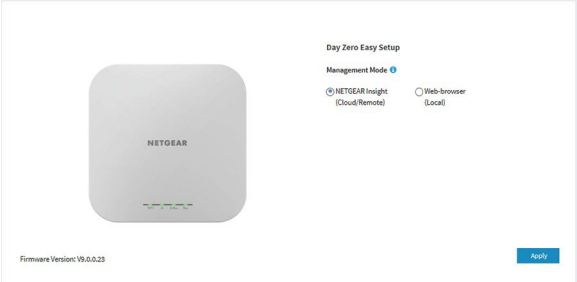
   注： **http://aplogin.net** は、アクセスポイントの初期設定時のみ使用できます。



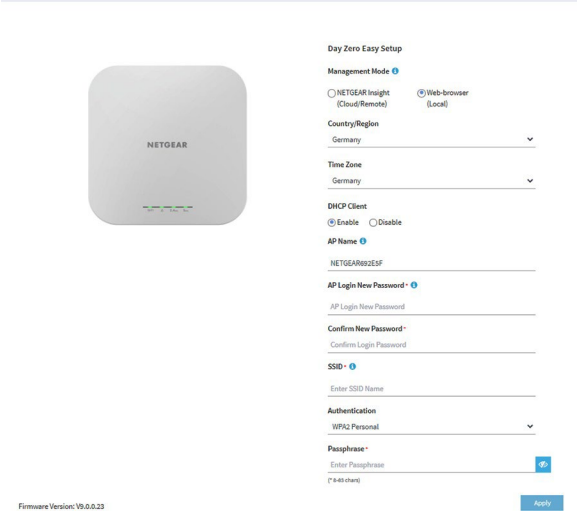
   アクセスポイントの自己署名証明書が原因で、ブラウザにセキュリティ警告が表示されることがありますが、これは予想された動作です。続行するか、セキュリティ警告の例外を追加することができます。詳しくは、「ブラウザのセキュリティ警告が表示された場合の対処法（55ページ）」を参照してください。

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**です。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、大文字と小文字が区別されます。



4. **Web-browser**」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。ログインすると、「Dashboard」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場合は、［**Check for Upgrade**］をクリックします。
   ボタンをクリックします（前図ではボタン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、アクセスポイントは再起動します。アクセスポイントの準備ができたら、本手順のステップ1へ戻ります。

6. 次の表に記載されている設定を入力します。

設定項目	概要
Country /Region	メニューから、アクセスポイントが動作している国や地域を選択します。**注**：国がデバイスが動作している場所に設定されていることを確認してください。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。**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。お住まいの国や地域が記載されていない場合は、お住まいの国の政府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や地域のタイムゾーンを選択します。
DHCP Client	デフォルトでは、アクセスポイントのDHCPクライアントは、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アドレスを受信することを許可します。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、次のようにします： 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。名前は、英数字を含むこと、少なくとも1つのアルファベット文字を含むこと、15文字より長くできないこと、ハイフンを含むことができるが、ハイフンで開始または終了することはできないことです。デフォルトでは、アクセスポイント名はNetgearxxxxx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。このパスワードは、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必要があるパスワードです。(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文字を含む必要があります。以下の特殊文字が使用可能です： !@ # $ % ^ & * ( ) パスワードは今後のために保存しておきましょう。

設定項目	概要
Confirm New Password	**AP Login New Password**」フィールドに入力したパスワードとまったく同じものを入力します。
SSID	セットアップ用SSIDは、通常の運用では使用できません。セットアップ用SSIDは、初期設定専用です。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（\）を除く、英数字と特殊文字の組み合わせが可能です。

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することができます。詳細については、「WiFiネットワークの認証と暗号化を変更する（85ページ）」を参照してください。

8. **Apply**］ボタンをクリックします。

   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、アクセスポイントは再起動します。

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、WiFi経由でアクセスポイントのWiFiネットワークに再接続します。
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、手順6で指定したIPアドレスを入力してください。

    アクセスポイントの自己署名証明書が原因で、ブラウザにセキュリティ警告が表示されることがありますが、これは予想された動作です。続行するか、セキュリティ警告の例外を追加することができます。詳しくは、「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（55ページ）」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ページで定義したばかりのものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

    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で接続し、ローカルのブラウザUIで初期設定を行う。

以下の手順は、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上にあることを想定しています。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。

注）本項の図は、モデル WAX610 を示しています。モデルWAX610Yを使用する場合、ローカルブラウザのUIはモデルWAX610Yを表示します。

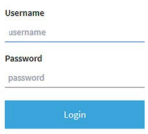
LAN経由でローカルのブラウザUIに接続して初期設定を行う：

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を使用します。

   Windowsをお使いの場合は、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、アクセスポイント機器の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 割り当てられた 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 アプリを使用して WiFi で接続する（35 ページ）」を参照してください。

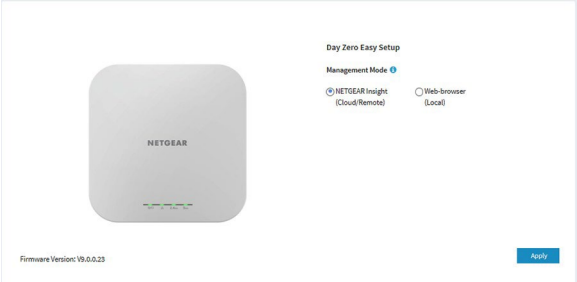
2. パソコンでWebブラウザを起動し、アドレスバーにアクセスポイントに割り当てられているIPアドレスを入力します。



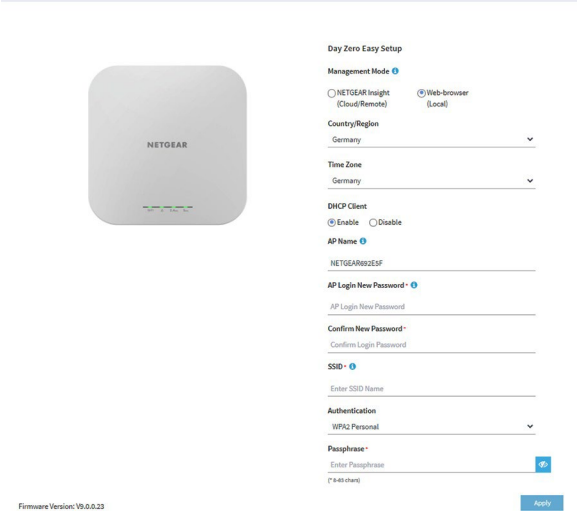
   アクセスポイントの自己署名証明書が原因で、ブラウザにセキュリティ警告が表示されることがありますが、これは予想された動作です。続行するか、セキュリティ警告の例外を追加することができます。詳しくは、「ブラウザのセキュリティ警告が表示された場合の対処法（55ページ）」を参照してください。

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**です。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、大文字と小文字が区別されます。



4. **Web-browser**」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。ログインすると、「Dashboard」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場合は、［**Check for Upgrade**］をクリックします。
   ボタンをクリックします（前図ではボタン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、アクセスポイントは再起動します。アクセスポイントの準備ができたら、状況に応じて、本手順のステップ2またはステップ3に戻ってください。

6. 次の表に記載されている設定を入力します。

設定項目	概要
Country/Region	メニューから、アクセスポイントが動作している国や地域を選択します。**注**：国がデバイスが動作している場所に設定されていることを確認してください。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。**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。お住まいの国や地域が記載されていない場合は、お住まいの国の政府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や地域のタイムゾーンを選択します。
DHCP Client	デフォルトでは、アクセスポイントのDHCPクライアントは、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アドレスを受信することを許可します。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、次のようにします： 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。名前は、英数字を含むこと、少なくとも1つのアルファベット文字を含むこと、15文字より長くできないこと、ハイフンを含むことができるが、ハイフンで開始または終了することはできないことです。デフォルトでは、アクセスポイント名はNetgearxxxxx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。このパスワードは、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必要があるパスワードです。(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文字を含む必要があります。以下の特殊文字が使用可能です： !@ # $ % ^ & * ( ) パスワードは今後のために保存しておきます。

設定項目	概要
Confirm New Password	**AP Login New Password**」フィールドに入力したパスワードとまったく同じものを入力します。
SSID	セットアップ用SSIDは、通常の運用では使用できません。セットアップ用SSIDは、初期設定専用です。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（\）を除く、英数字と特殊文字の組み合わせが可能です。

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することができます。詳細については、「WiFiネットワークの認証と暗号化を変更する（85ページ）」を参照してください。

8. **Apply**］ボタンをクリックします。
   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。

   注意：ページを閉じないでください！

   しばらくすると、Dashboard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、Dashboard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。

9. ダッシュボードが自動的に表示されない場合は、以下の操作を行ってください：
   a. 以下のいずれかのアクションを行います：
      - 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、Webブラウザーのアドレスバーに手順6で指定したIPアドレスを入力してください。
      - 固定IPアドレスを割り当てていない場合は、Webブラウザー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アドレスをメモしてWebブラウザーを終了し、再度Webブラウザーを起動してから、WebブラウザーのアドレスバーにIPアドレスを再入力してください。
      - 静的IPアドレスを割り当てず、ページを閉じてアクセスポイントのIPアドレスを確認できないようにした場合は、IPスキャナツールを使用するか、ネットワーク発見ツールを使用するか、DHCPサーバーにアクセスしてネットワーク内のアクセスポイントのIPアドレスを発見してください。
        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、35 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。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、ブラウザにセキュリティ警告が表示されることがありますが、これは予想された動作です。続行するか、セキュリティ警告の例外を追加することができます。詳しくは、「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（55ページ）」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 ページで定義したばかりのものです。ユーザー名とパスワードは、大文字と小文字が区別されます。
      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。

屋内用WAX610を、直接接続したパソコンでオフラインで設定する場合

注：屋外用WAX610Yは、PoE+スイッチへのPoE+接続が必要なため、本手順は適用されません。(直接接続したパソコンでは、アクセスポイントにPoE+を供給することはできません)。

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/PoE+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、オフラインで設定することができます。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：アクセスポイントはPoE+スイッチに接続されていないため、この設定方法は、アクセスポイント用の電源アダプターがある場合にのみ使用できます。

アクセスポイントのLAN/PoE+ポートに接続されたパソコンを使って、アクセスポイントに接続する場合：

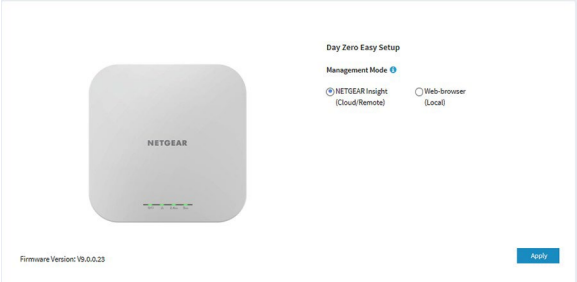
1. コンピュータのIPアドレスとサブネットマスクを記録しておくと、後でこれらのIPアドレス設定を復活させることができます。
2. コンピュータのIPアドレスを192.168.0.210、サブネットマスクを255.255.255.0に一時的に変更します。

   (実際には、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、192.168.0.2～192.168.0.254の範囲のどのIPアドレスも使用できます)。

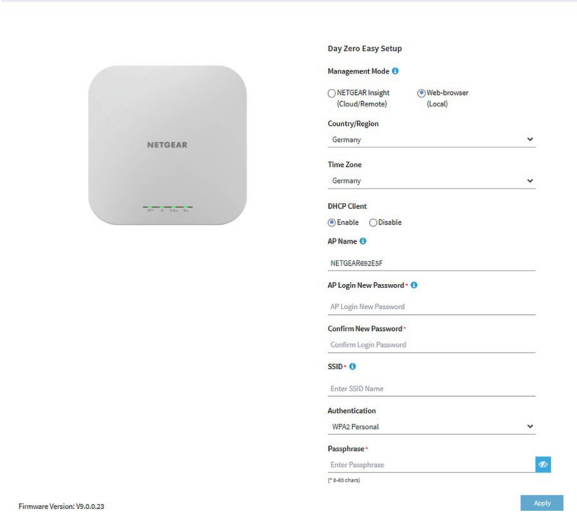
   パソコンのIPアドレスの変更については、パソコンのヘルプやマニュアルを参照してください。
3. イーサネットケーブルを使って、パソコンとアクセスポイントのLAN/PoE+ポートを接続します。
4. パソコンでWebブラウザを起動し、アドレスバーに「**192.168.0.100**」と入力する。

   アクセスポイントの自己署名証明書が原因で、ブラウザにセキュリティ警告が表示されることがありますが、これは予想された動作です。続行するか、セキュリティ警告の例外を追加することができます。詳しくは、「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（55ページ）」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**です。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、大文字と小文字が区別されます。



6. **Web-browser**」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。ログインすると、「Dashboard」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場合は、［Check for Upgrade］をクリックします。
ボタンをクリックします（前図ではボタン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、アクセスポイントは再起動します。アクセスポイントの準備ができたら、状況に応じて、本手順のステップ4またはステップ5に戻ってください。

8. 次の表に記載されている設定を入力します。

設定項目	概要
Country/Region	メニューから、アクセスポイントが動作している国や地域を選択します。**注**：国がデバイスが動作している場所に設定されていることを確認してください。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。 **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。お住まいの国や地域が記載されていない場合は、お住まいの国の政府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や地域のタイムゾーンを選択します。
DHCP Client	デフォルトでは、アクセスポイントのDHCPクライアントは、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アドレスを受信することを許可します。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、次のようにします： 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。名前は、英数字を含むこと、少なくとも1つのアルファベット文字を含むこと、15文字より長くできないこと、ハイフンを含むことができるが、ハイフンで開始または終了することはできないことです。デフォルトでは、アクセスポイント名はNetgearxxxxx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。このパスワードは、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必要があるパスワードです。(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文字を含む必要があります。以下の特殊文字が使用可能です： !@ # $ % ^ & * ( ) パスワードは今後のために保存しておきましょう。

設定項目	概要
Confirm New Password	**AP Login New Password**」フィールドに入力したパスワードとまったく同じものを入力します。
SSID	セットアップ用SSIDは、通常の運用では使用できません。セットアップ用SSIDは、初期設定専用です。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（\）を除く、英数字と特殊文字の組み合わせが可能です。

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。**パスフレーズ**］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 セキュリティをセットアップすることができます。詳細については、「変更 WiFiネットワークの認証と暗号化」（85ページ）を参照してください。

10. **Apply**］ボタンをクリックします。

    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、アクセスポイントは再起動します。

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**」と入力してください。

    IPアドレスを変更した場合は、手順10で保存したIPアドレスを入力してください。

    アクセスポイントの自己署名証明書が原因で、ブラウザにセキュリティ警告が表示されることがありますが、これは予想された動作です。続行するか、セキュリティ警告の例外を追加することができます。詳しくは、「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（55ページ）」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ページで定義したばかりのものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

    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。

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後、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ーUIにログインする場合：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。

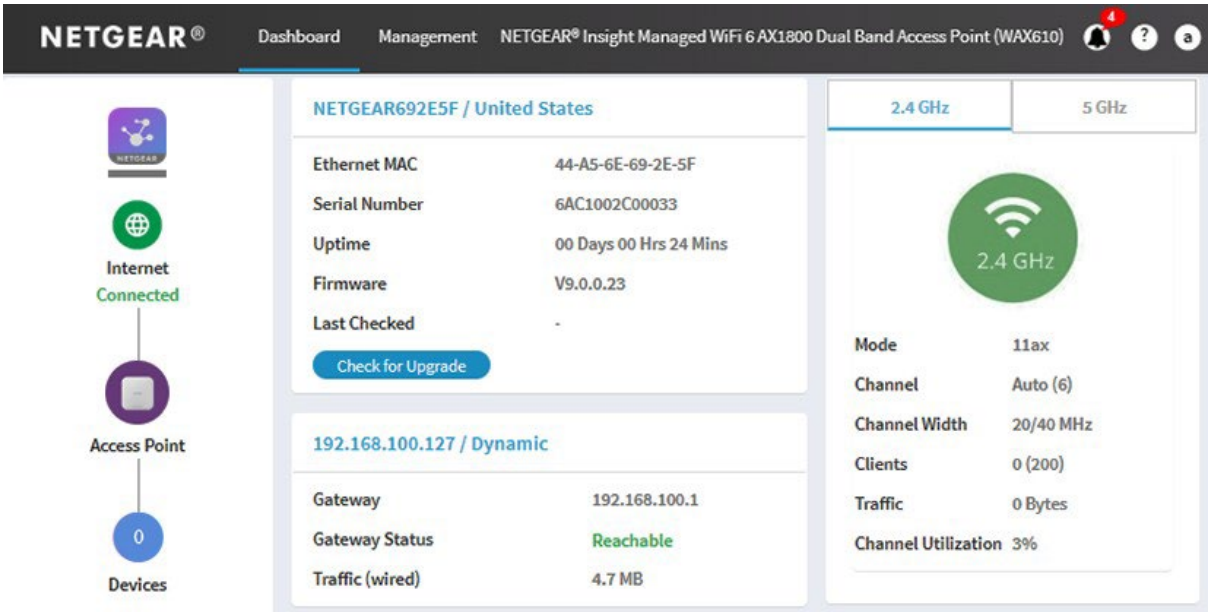
   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳しくは、「ブラウザのセキュリティ警告が表示された場合の対処方法（55ページ）」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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。

下図は、モデルWAX610のDashboardページの上部を示しています。モデル WAX610Y の Dashboard ページは同じです。



Dashboard 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。Dashboard ページとそのさまざまなペインの詳細については、「アクセスポイントとネットワークの監視」（193 ページ）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方法について

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、セキュリティ警告が表示される場合があります。これは予想される動作です。続行するか、セキュリティ警告の例外を追加してください。

セキュリティ警告を続行する、または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です：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。表示される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**：「詳細」＞「ウェブページに進む」を選択します。
- **Microsoft Internet Explorer**の場合：このウェブサイトへ進む（推奨しません）」のリンクをクリックしてください。

5

Insight Instant Mesh WiFiネットワークにアクセスポイントを追加する。

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（当社では*ルートと表記*）またはノードアクセスポイント（当社では*ノードと表記*）として機能することができます。
この章では、NETGEAR Insight Cloud Portal 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 Cloud Portal と Insight アプリは、Insight Premium と Insight Pro の契約者が利用できます。

注：ルートへの接続を持つ NETGEAR Insight Instant Mesh WiFi ネットワークのノードをセットアップするには、NETGEAR Insight Cloud Portal 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 接続をセットアップ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埋め込まれており、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。

この章には、次の項目があります：

注：本書において、***WiFi***ネットワークとは、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ネットワークという場合は、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？

WAX610、WAX610YともにInsight Instant Mesh WiFiネットワークのルートとして、またWAX610はノードとして機能することが可能です：

- **ルート（Root）**：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ために、ネットワークへの有線接続でセットアップするメッシュ対応アクセスポイントです。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使用します。ルートは、複数のノードを同時にサービスすることができます。
- **ノード（Node）**：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ています。

  注）モデルWAX610Yはノードとして機能しますが、PoEによる電源供給のみ可能です。

下図は屋内モデルWAX610の場合です。屋外モデルWAX610Yを屋内PoE+スイッチに接続してルートとして使用する場合、屋外モデルWAX610YとPoE+スイッチ間のEthernetケーブルにEthernetサージプロテクターが必要な設定です。

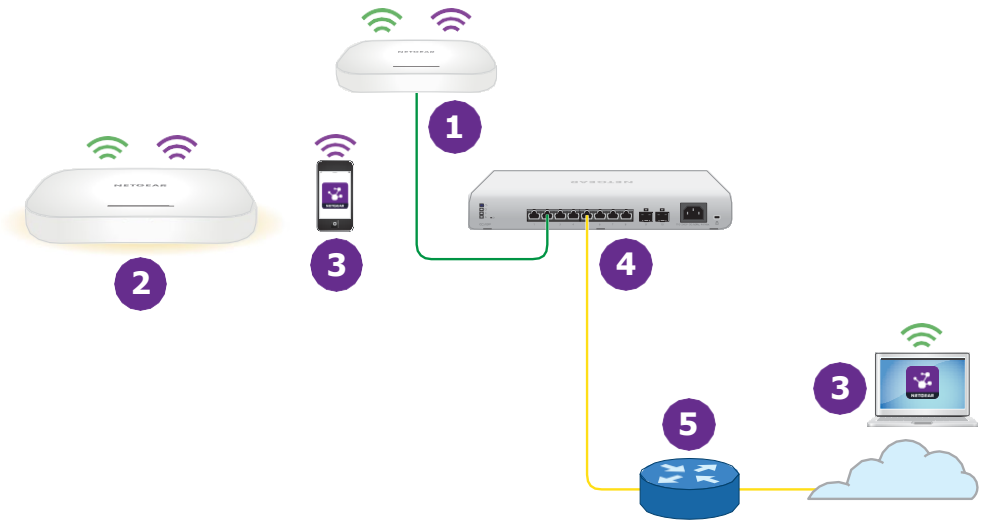


図9.ノードとワイヤード・ルートを持つメッシュ・ネットワーク

番号またはアイコンと説明
1 ルートはイーサネットでネットワークスイッチに接続
2 ルートと5GHzのバックホールWiFi接続でつながっているノード。 WAX610をノードとして機能させる場合は、PoEではなく電源アダプターで給電する必要があります。(電源アダプターはオプションで購入できます。モデルWAX610Yはノードとして機能しますが、電源はPoEのみとなります。
3 Insightアプリを搭載した携帯電話、またはInsight Cloud Portalにアクセスできるコンピューターまたはタブレットのいずれか。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および管理できます。
4 ネットワークスイッチのことです。 モデルWAX610Yがルートとして機能する場合、またはモデルWAX610が電源アダプタなしでルートとして機能する場合、スイッチはルートにPoE+を提供する必要があります。
5 インターネットに接続されたネットワーク・ルーターです。
2.4GHz帯の電波
5GHz帯の電波

Insight Instant Mesh 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を介してルートに接続する1つ以上のノードで構成されます（「ルートとノードとは」（58ページ）を参照）。ルートは、ルーター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、その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、WiFiネットワークで潜在的に広いエリアをカバーするために協力し、これがメッシュネットワークです。

以下のような環境にWiFiを導入したい場合、メッシュネットワークは良いソリューションとなります：

- ケーブル配線ができない近くの部屋（目視で、現在のWiFiの電波が届く範囲内）
- 近隣のオフィスビル（目視で現在のWiFi受信可能範囲内）
- ケーブルを走らせることができないあらゆる環境

メッシュWiFiネットワークでは、ノードはWiFi接続でルートに接続し、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）します：

- **バックホール接続**：ルートとノードの間の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クライアントの間のWiFi接続は、フロントホール接続と呼ばれます。

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ー UI からは行えません。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ネットワークや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可能です。

アクセスポイントは、5GHz帯（バックホール接続に適した帯域）および2.4GHz帯でブロードキャストすることができます。WiFiクライアントのWiFi能力に応じて、どの帯域でもフロントホール接続を提供することができます。

メッシュWiFiネットワークにノードを配置するための条件

Insight Instant Mesh WiFiネットワークにノードを配置するための条件は以下のとおりです：

- 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状態である必要があります。以前にネットワークでノードを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信号が届く範囲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、ノードを最も近いルートから7.5m以内に、障害物の少ない見通しの良い場所に設置します。
- 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アクセスポイント機種は、ルートとしてもノードとしても機能します：

- 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、WAX638***E***とWAC540、WAC564によるメッシュWiFiネットワークにおいて。
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利用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ません。

NETGEAR Insight Cloud Portalにアクセスし、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および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、アクセスポイントの設定、管理、監視を行うことができます。

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を経由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場合：

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 Account Login ページが表示されます。
2. インサイトアカウントをまだお持ちでない方は、今すぐアカウントを作成することができます。
   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接続を設定することができます。詳しくは、kb.netgear.com/000061304をご覧ください。

アクセスポイントをノードとして、クラウドポータルを使ってルートに接続する

NETGEAR Insight Cloud Portalは、Insight Premiumおよび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することができます。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セットアップする必要があります。

Insight Cloud Portal の詳細、および Insight Cloud Portal を通じて利用できる設定と管理オプションについては、netgear.com/insight を参照してください。Insight Cloud Portal 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知識ベース記事で文書化されています。

注）モデルWAX610Yはノードとして機能しますが、PoEによる電源供給のみ可能です。

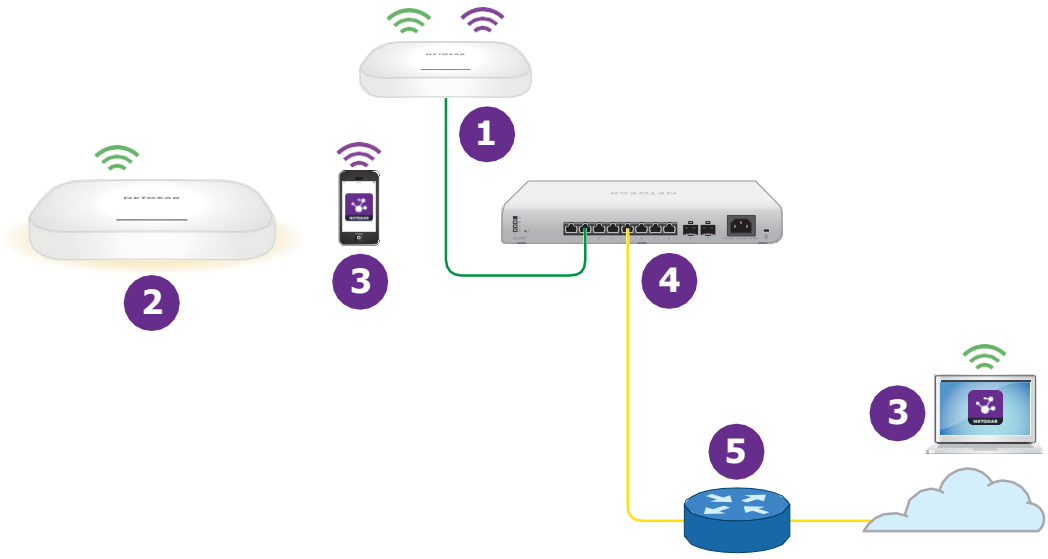


図 10.ノードを有線ルートに接続する

番号またはアイコンと説明
1 ルートはイーサネットでネットワークスイッチに接続
2 ルートと5GHzのバックホールWiFi接続でつながっているノード。 WAX610をノードとして機能させる場合は、PoEではなく電源アダプターで給電する必要があります。(電源アダプターはオプションで購入できます。)モデルWAX610Yはノードとして機能しますが、電源はPoEのみとなります。
3 Insightアプリを搭載した携帯電話、またはInsight Cloud Portalにアクセスできるコンピューターまたはタブレットのいずれか。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および管理できます。
4 ネットワークスイッチのことです。 モデルWAX610Yがルートとして機能する場合、またはモデルWAX610が電源アダプターなしでルートとして機能する場合、スイッチはアクセスポイントにPoE+を提供する必要があります。
5 インターネットに接続されたネットワーク・ルーターです。
2.4GHz帯の電波。
5GHz帯の電波。

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、どのバンドも使用することができます。しかし、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5GHz帯をサポートできる場合、ノードは自動的

にバックホール接続の優先バンドとして5GHz帯に切り替わります。Insight Cloud Portal を使用して、バックホール設定を変更することができます。

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場合：

1. Insight network location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ます。詳しくは、kb.netgear.com/000064931をご覧ください。
3. ノードが工場出荷時の状態であることを確認します。
   以前に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戻してください。
4. 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25フィート（7.5m）未満で、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Power/Cloud LEDがオレンジ色に点灯し、その後緑色に点灯します。

   注：ネットワークループを防ぐため、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+スイッチにノードを接続します。また、オプションの電源アダプター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. ノードを追加するロケーションを選択します。
9. **+ (Add Device)**ボタンをクリックします。
10. Add New Device］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、［**進む**］をクリックします。
    Insight 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て接続しようとします。

    注：初期接続と設定処理に最大10分かかる場合があります。また、設定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がオレンジ色、緑色、青色の点滅を止め、青色の点灯になるのを待ちます。
注：初期接続と設定処理に最大10分かかる場合があります。また、設定中にノードが再起動することがあります。

    初期接続・設定中は、Power/Cloud LEDが以下のように点灯します：

    - **緑色に点滅**：ノードはルートの検出を試みています。
    - **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の最初の接続を行っています。
    - **オレンジ色がゆっくり点滅**：ノードは、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ます。
      電源/クラウドLEDのオレンジ色の点滅が止まらない場合は、258ページの「電源/クラウドLEDがゆっくり、連続してオレンジ色に点滅している」を参照してください。
    - **オレンジ色、グリーン、ブルーが点滅**：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のオレンジ色、緑色、青色の点滅が止まらない場合は、「電源/クラウドLEDのオレンジ色、緑色、青色の点滅が止まらない（260ページ）」を参照してください。

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

    - **青色に点灯**：設定が完了し、ノードは操作可能な状態になります。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、ルートのWiFiネットワークをブロードキャスト（拡張）するように自動的に設定されます。ノードとルートが接続できない場合は、「ノードとルートが接続できない（261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 にアクセスしてください。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知識ベース記事で文書化されています。

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の契約者向けに提供されています。

NETGEAR Insightアプリを使用してアクセスポイントをInsight Instant Mesh WiFiネットワークに追加する前に、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：

1. モバイルデバイスで、アプリストアにアクセスし、NETGEAR Insightを検索して、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します。
3. インサイトアカウントをまだお持ちでない方は、今すぐアカウントを作成することができます。

   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、「**LOG IN**」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する（66ページ）」を参照）。

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することができます。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、ルートは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 アプリの詳細、および Insight アプリで利用できる設定と管理オプションについては、netgear.com/insight を参照してください。Insight アプリにはヘルプが組み込まれており、netgear.com/support 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。

注）モデルWAX610Yはノードとして機能しますが、PoEによる電源供給のみ可能です。

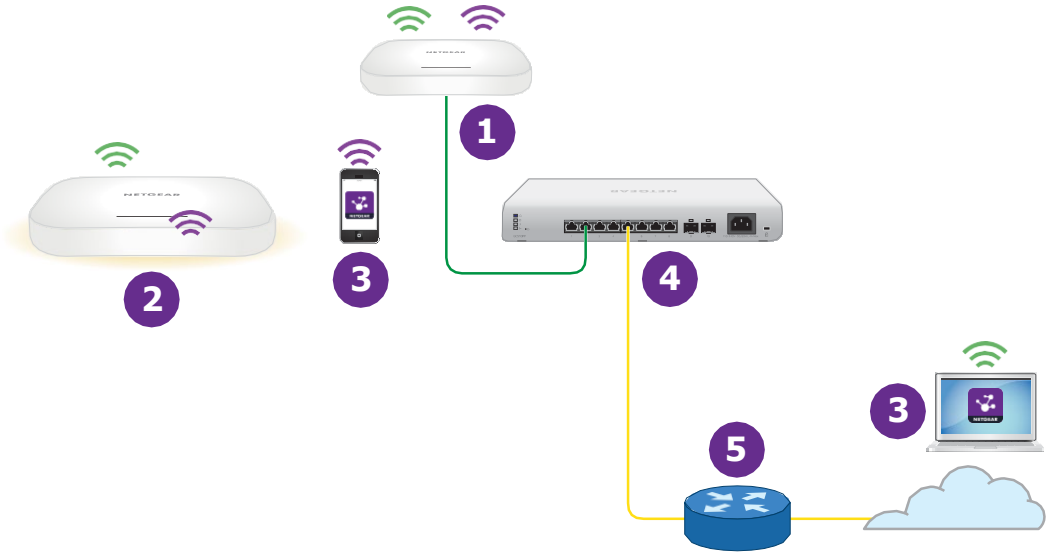


図 11.ノードを有線ルートに接続する

番号またはアイコンと説明
1 ルートはイーサネットでネットワークスイッチに接続
2 ルートと5GHzのバックホールWiFi接続で繋がっているノード。 WAX610をノードとして機能させる場合は、PoEではなく電源アダプターで給電する必要があります。(電源アダプターはオプションで購入できます。)モデルWAX610Yはノードとして機能しますが、電源はPoEのみとなります。
3 Insightアプリを搭載した携帯電話、またはInsight Cloud Portalにアクセスできるコンピューターまたはタブレットのいずれか。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および管理できます。
4 ネットワークスイッチのことです。 モデルWAX610Yがルートとして機能する場合、またはモデルWAX610が電源アダプタなしでルートとして機能する場合、スイッチはルートにPoE+を提供する必要があります。
5 インターネットに接続されたネットワーク・ルーターです。

番号またはアイコンと説明
2.4GHz帯の電波。
5GHz帯の電波。

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、どのバンドも使用することができます。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、ノードは自動的にバックホール接続の優先バンドとして 5 GHz バンドに切り替わります。Insight Cloud Portal を使用して、バックホール設定を変更することができます。

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場合：

1. Insight ネットワークのロケーション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ます。
   詳しくは、kb.netgear.com/000064929をご覧ください。

3. ノードが工場出荷時の状態であることを確認します。
   以前に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戻してください。

4. 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障害物の少ない見通しの良い場所に、25フィート（7.5m）未満で設置してください。

5. ノードを電源に接続する。
   ノードのPower/Cloud LEDがオレンジ色に点灯し、その後緑色に点灯します。

   注：ネットワークループを防ぐため、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+スイッチにノードを接続します。また、オプションの電源アダプターを使用することもできます。

6. モバイル機器を、1つ以上のルーツを含む既存のWiFiネットワークに接続します。

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. ルートでインサイトネットワークの場所を選択します。
   ほとんどの場合、Insightアプリ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。

9. 以下のいずれかを行い、ノードをインサイトネットワークの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、次のようにしてください。
     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ってください：
        - **SCAN BARCODE OR QR CODE**」ボタンをタップし、ノードのコードを読み取ります。
        - **シリアル番号の入力**」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て接続しようとします。

   注：初期接続と設定処理に最大10分かかる場合があります。また、設定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のオレンジ色、緑色、青色の点滅が止まり、青色の点灯になるのを待ちます。

    注：初期接続と設定処理に最大10分かかる場合があります。また、設定中にノードが再起動することがあります。

    初期接続・設定中は、Power/Cloud LEDが以下のように点灯します：

    - **緑色に点滅**：ノードはルートの検出を試みています。
    - **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の最初の接続を行っています。
    - **オレンジ色がゆっくり点滅**：ノードは、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ます。

電源/クラウドLEDのオレンジ色の点滅が止まらない場合は、258ページの「電源/クラウドLEDがゆっくり、連続してオレンジ色に点滅している」を参照してください。

- **オレンジ色、グリーン、ブルーが点滅**：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のオレンジ色、緑色、青色の点滅が止まらない場合は、「電源/クラウドLEDのオレンジ色、緑色、青色の点滅が止まらない（260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：

- **青色に点灯**：設定が完了し、ノードは操作可能な状態になります。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、ルートのWiFiネットワークをブロードキャスト（拡張）するように自動的に設定されます。

ノードとルートが接続できない場合は、「ノードとルートが接続できない（261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 にアクセスしてください。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知識ベース記事で文書化されています。

6

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、WiFi セキュリティを含む独自の WiFi 設定を持つ、8 つの WiFi ネットワークをサポートすることができます。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（214ページ）」をご覧ください。

この章には、以下の項目があります：

- オープンまたはセキュアなWiFiネットワークをセットアップする
- 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を隠したり、ブロードキャストしたりする。
- 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の有効／無効を設定します。
- WiFiネットワークにMulti PSKを設定する
- WiFiネットワークの無効化・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ネットワーク管理でバンドステアリングを有効または無効にすることができる。

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設定が有効になる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：本書において、***WiFi***ネットワークとは、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ネットワークという場合は、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いる、2.4 GHz 帯と 5 GHz 帯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をデフォルトのWiFiネットワークと呼び、ローカルブラウザのUIではSSID1として表示されます。SSIDはさらに追加することができます：アクセスポイントは、合計8つのSSIDをサポートすることができます。

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帯を同時にサポートすることができます。各バンドは2つのWiFiストリームをサポートし、合計4つのWiFiストリームをサポートします。

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、新しいWiFiネットワーク（仮想アクセスポイント（VAP）とも呼ばれる）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。

WiFi ネットワークに WPA2 Enterprise セキュリティまたは WPA3 Enterprise セキュリティを使用する場合は、まず RADIUS サーバーを設定します（「RADIUS サーバーの設定 (143 ページ)」を参照）。WPA2 Enterprise securityとWPA3 Enterprise securityは、マルチキャストDNS（mDNS）ゲートウェイと互換性が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（159ページ）」を参照）。

WiFiネットワークを設定する場合：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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。

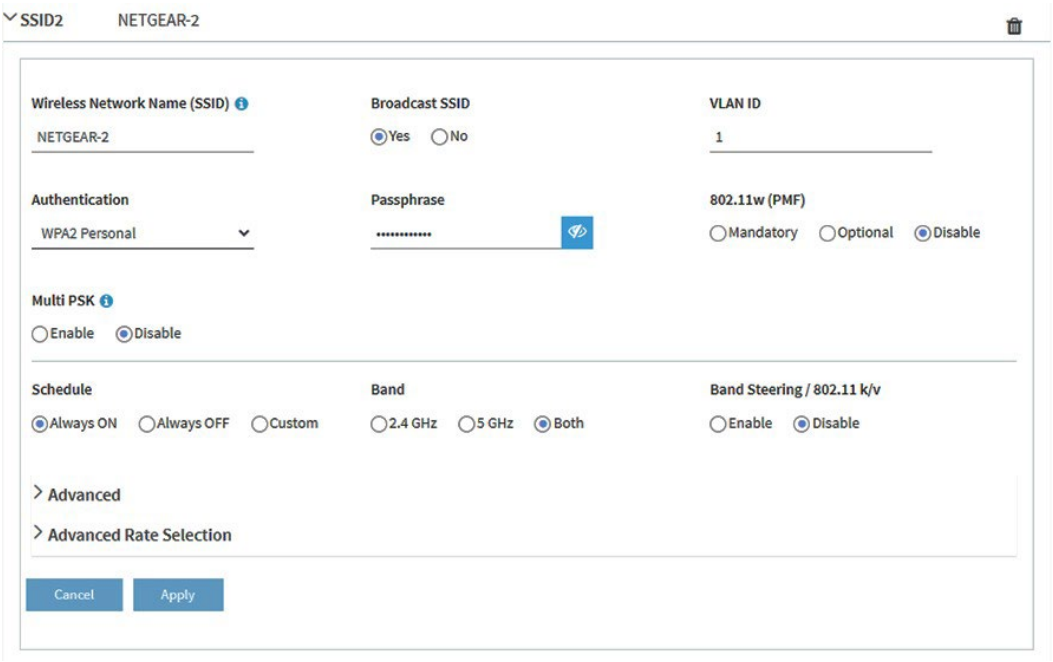
   ユーザー名は**admin**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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の選択と追加を行います。

5. Add SSID］の左側にある［＋］ボタンをクリックします。



前図では、SSID2 を例にしています。

6. WiFiネットワーク名（SSID）の指定、SSIDのブロードキャストの有無の選択、VLAN IDの指定は、次の表のとおりです。

設定	概要
Wireless Network Name (SSID)	SSID は、VAP の WiFi ネットワーク名です。SSID の名前は、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することができます。 WiFi機器がVAPに接続できるようにするには、WiFi機器の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はその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のセキュリティがさらに向上しますが、ユーザーはVAPに参加できるようにSSIDを知る必要があります。
VLAN ID	VAP に関連付ける必要のある VLAN ID を入力することができます。デフォルトでは、VLAN ID は 1 です。

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のチェックボックスが選択されていない**：WiFiネットワークは、セキュリティのないレガシー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のオプションです。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、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、デフォルトの設定で、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** authenticationを選択してください。
  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。

- **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 サーバーの設定（143 ページ）」を参照）。
暗号化」メニューから、データの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することを可能にします。このモードはデフォルトです。
  - **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。したがって、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**」のラジオボタンが表示されます：

  - **有効にする**：RADIUS サーバーがクライアントに 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、クライアントはSSIDに設定したVLAN IDが自動的に割り当てられます。
  - **無効にする**：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。これはデフォルトの設定です。
- **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。
- **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、および会計（AAA）を集中的に管理します。WPA3 Enterpriseセキュリティが機能するためには、RADIUSサーバーを設定する必要があります（「RADIUSの設定」を参照）。サーバー（143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 securityを選択すると、暗号化は自動的に256ビットの暗号化プロトコルであるGCMP256に設定されます。
  WPA3 Enterprise認証を選択すると、「**Dynamic VLAN**」のラジオボタンが表示されます：

  - **有効にする**：RADIUS サーバーがクライアントに 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、クライアントはSSIDに設定したVLAN IDが自動的に割り当てられます。
  - **無効にする**：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。これはデフォルトの設定です。

8. オプションで、802.11w Protected Management Frames (PMF)を有効にします。
   802.11w 規格に基づくProtected Management Frames (PMF) は、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、悪意のある目的に変更されるのを防ぐセキュリティ機能です。選択した認証の種類によって、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。また、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することができます。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、Multi PSKは、設定する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ます。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、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を設定する（90ページ）」を参照してください。

10. 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することができます：

    - **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は有効で、「**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場合は、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. ラジオボタンの横の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あらかじめ定義された時間を選択するか、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）であることを示します。タイムブロックの色がグレーであれば、VAPが無効（オフ）であることを示します。
      c. 完了」ボタンをクリックします。mポップアップウィンドウが閉じます。

      各SSIDに対して、1つのカスタムスケジュールを作成することができます。そ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を無効にする時間または時刻を指定します。

11. オプションで、単一の無線バンドのみを選択することができます。

    単一のバンド（**2.4GHz** または **5GHz**）のラジオボタンを選択するか、デフォルトの選択を維持します。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両方のバンドでSSIDをブロードキャストすることができます。

12. オプションとして、802.11k無線リソース管理（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 2.4 GHz または 5 GHz バンドに誘導することができます。5GHz帯は、2.4GHz帯に比べ、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、より良いユーザーエクスペリエンスを実現できます。

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

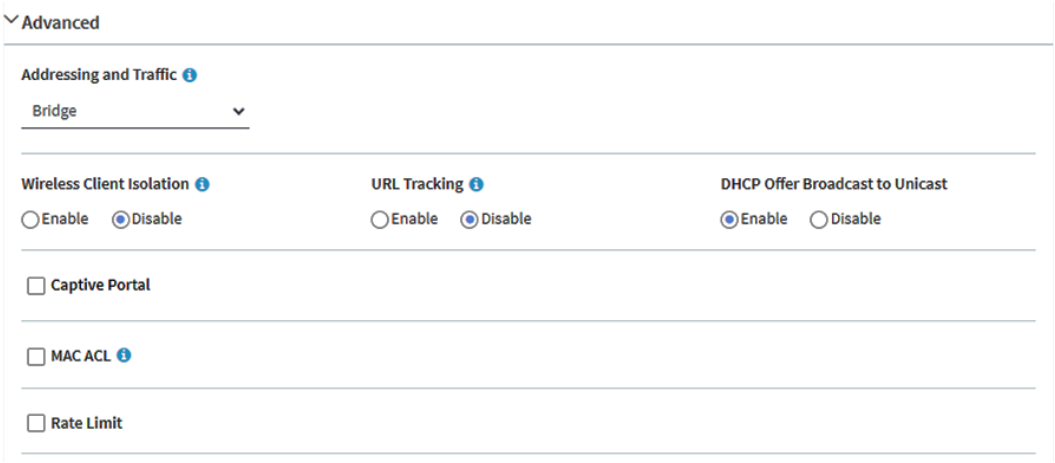
    - **802.11k RRM**：802.11k RRM： この機能により、アクセスポイントと 802.11k 対応クライアントは、利用可能な無線リ ソースを動的に測定することができます。802.11k対応ネットワークでは、アクセスポイントとクライアントは互いにネイバーレポート、ビーコンレポート、リンク測定レポー

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ー（RSSI）の閾値を自動的に設定します。(つまり、RSSI の閾値を手動で設定することはできません)。

13. 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。



14. 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します。デフォルトでは、アクセスポイントのアドレス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アドレスを受信することを意味します。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。

    また、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化する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、アクセスポイント本体の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モードとマルチPSK（手順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モードを選択します：

    - **Beidge**：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にある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**：このモードを選択すると、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。例えば、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アドレス範囲）である場合、192.168.0.0と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、前のステップで設定したWLANネットワークアドレスと異なる必要があります。

15. 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、クライアントアイソレーションは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。クライアントアイソレーションとマルチ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遮断する場合は、［**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、次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：**ネットワークデバイスの静的 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、クライアントからのアクセスを許可することで、隔離を免除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（216 ページ）」を参照してください。

16. オプションで、URLトラッキングを有効にします。

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の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ごと、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（207ページ）」をご覧ください。

17. オプションで、DHCP Offerメッセージの設定を変更します。

デバイスがWiFiネットワークに関連付けようとしてIPアドレスを交渉するとき、アクセスポイントはDHCPサーバーから受信するブロードキャスト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（つまり、［**Enable**］ラジオボタンが選択されています）。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。

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

    - キャプティブポータルのセットアップと管理」（111ページ
      Captive PortalとMulti PSK（手順9参照）は相互に互換性がありません。
    - ローカル MAC アクセス制御リストの管理 (130 ページ)、WiFi ネットワークの MAC ACL の選択 (221 ページ)
    - WiFi ネットワークの帯域幅レート制限を設定する（223 ページ

    これらの機能は、WiFiネットワークの設定中に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。

19. 事前レート選択を設定するには、「WiFiネットワークの事前レート選択を設定する（224ページ）」を参照してください。

20. **Apply**］ボタンをクリックします。設定が保存されます。

21. 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、お住まいの地域の別のWiFiネットワークにすで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て、正しいWiFiネットワークに接続してください。一部のWiFi機器は、WiFiセキュリティのないオープンなネットワークを最初に発見すると、自動的に接続するようになっています。
    - WiFi対応パソコンやモバイル機器が古い設定（設定変更前）でネットワークに接続しようとしている場合は、WiFi対応パソコンやモバイル機器のWiFiネットワーク選択を更新して、現在のネットワーク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ていますか？(クライアント分布、接続クライアント、クライアント傾向の表示(202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。
    - WiFiのネットワーク名（SSID）とパスワードは正しく使用されていますか？
    - WiFiの認証と暗号化がWPA3 Personalに設定されている場合は、WiFiアダプターのデバイスドライバーが最新版に更新されていることを確認してください。
      WiFi対応のパソコンまたはモバイル端末。

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）または任意のカスタムWiFiネットワークの設定を表示または変更することができます。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、ローカルブラウザーUIで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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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を選択することができます。
5. SSIDの左側にある「**＞」ボタンを**クリックします。選択したSSIDの設定項目が表示されます。
6. 必要に応じて、WiFiネットワークの設定を変更します。
   設定の詳細については、「オープンまたはセキュアなWiFiネットワークを設定する（72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、お住まいの地域の別のWiFiネットワークにすで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て、正しいWiFiネットワークに接続してください。一部のWiFi機器は、WiFiセキュリティのないオープンなネットワークを最初に発見すると、自動的に接続するようになっています。
   - WiFi対応パソコンやモバイル機器が古い設定（設定変更前）でネットワークに接続しようとしている場合は、WiFi対応パソコンやモバイル機器のWiFiネットワーク選択を更新して、現在のネットワーク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ていますか？(クライアント分布、接続クライアント、クライアント傾向の表示(202ページ)を参照)。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。
   - WiFiのネットワーク名（SSID）とパスワードは正しく使用されていますか？

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やVAP）を削除することができます。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、ローカルブラウザの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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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。

Dashboard」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を選択することができます。
5. SSIDの右側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**」ボタンをクリックします。
   ポップウィンドウが閉じ、WiFiネットワークが解除されます。

WiFiネットワークのSSIDを隠したり、ブロードキャストしたりする。

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：「WiFiブリッジのセットアップ（229ページ）」を参照）をセットアップする場合は、SSIDブロードキャスト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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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。

Dashboard」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を選択することができます。
5. SSIDの左側にある「**>**」**ボタンを**クリックします。
   選択したSSIDの設定項目が表示されます。
6. Broadcast SSID］で、次のラジオボタンのいずれかを選択します：
   - **Yes**：WiFiネットワークのSSIDが非表示になっています。
   - **No**：WiFiネットワークのSSIDが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（151 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が設定されていること、アクセスポイントとそのクライアントが新しいVLAN上で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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、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、35 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。

Dashboard」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を選択することができます。
5. SSIDの左側にある「**＞」ボタンを**クリックします。
   選択したSSIDの設定項目が表示されます。
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することができます。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、ローカルブラウザーUIで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る必要がある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。

WiFi ネットワークに WPA2 Enterprise セキュリティまたは WPA3 Enterprise セキュリティを使用する予定の場合は、まず RADIUS サーバーを設定します（「RADIUS サーバーの設定（143 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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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。

   Dashboard」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の選択と追加を行います。

5. SSIDを追加する］の左側にある［＋］**ボタンを**クリックします。
   選択したSSIDの設定項目が表示されます。

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のチェックボックスが選択されていない**：セキュリティのないレガシー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のオプションです。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（89 ページ）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 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（89 ページ）を参照）。**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。

- **WPA2 Personal**：このオプションは、WPA2-PSKと同じで、デフォルトの設定で、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/WPA Personal** authenticationを選択してください。
  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。

- **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 サーバーの設定（143 ページ）」を参照）。
  暗号化」メニューから、データの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。このモードはデフォルトです。
  - **AESです**：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のみをサポートしています。したがって、ネットワークにそのような古いデバイスが含まれる場合は、**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**」のラジオボタンが表示されます：

  - **Enable**：RADIUS サーバーがクライアントに 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。これはデフォルトの設定です。

- **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（89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場合があります。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。

- **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、および会計（AAA）管理を集中的に行います。WPA3 Enterprise セキュリティを機能させるには、RADIUS サーバーをセットアップする必要があります（「RADIUS サーバーのセットアップ（143 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（89 ページ）」を参照）。
  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である GCMP256 に設定されます。
  WPA3 Enterprise認証を選択すると、「**Dynamic VLAN**」のラジオボタンが表示されます：

  - **Enable**：RADIUS サーバーがクライアントに 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。これはデフォルトの設定です。

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、お住まいの地域の別のWiFiネットワークにすで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て、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対応パソコンやモバイル機器が古い設定（設定変更前）でネットワークに接続しようとしている場合は、WiFi対応パソコンやモバイル機器のWiFiネットワーク選択を更新して、現在のネットワーク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ていますか？(クライアント分布、接続クライアント、クライアント傾向の表示(202ページ)を参照)。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。
- WiFiのネットワーク名（SSID）とパスワードは正しく使用されていますか？
- WiFiの認証・暗号化をWPA3 Personalに変更した場合、 WiFi対応パソコンやモバイル端末で、WiFiアダプターのデバイスドライバーが最新版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の有効／無効を設定します。

802.11w 規格に基づくProtected Management Frames（PMF）は、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、悪意のある目的で変更されることを防ぐセキュリティ機能です。選択した認証の種類によって、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。また、手動で設定することもできます。

WiFiネットワークで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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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を選択することができます。

5. SSIDの左側にある「＞」ボタンをクリックします。
   選択したSSIDの設定項目が表示されます。

6. 802.11w（PMF）」で、次のラジオボタンのいずれかを選択します：

   - **Mandatory**：PMFを使用するデバイスが必要です。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。拡張オープン認証、WPA3 Personal認証、WPA3 Enterprise認証を選択した場合、PMFのラジオボタンは「**Mandatory**」に設定されており、変更することはできません。
   - **Optional**：アクセスポイントが PMF をサポートできるデバイスかどうかに基づいて、自動的に PMF を有効にします。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**：WiFiネットワークでPMFが無効になっています。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「Disable」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）。

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Multi PSKを設定する

Multi Pre-Shared Key (PSK)は、1つの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します。ある意味、マルチPSKは、1つの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が決定されます。

VLANとパスフレーズに加え、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ネットワーク内のVLANを識別できます。例えば、WiFiクライアントを表示する場合、キー識別子も表示できます（クライアント分布、接続クライアント、クライアント傾向の表示（202ページ）を参照）。

キー識別子の例として、corporatenetwork_22、corporatenetwork_23、corporatenetwork_24などの用語を使用することができます。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構成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 の場合に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 WiFiネットワークであるデフォルトのWiFiネットワーク（ローカルのクッパUIでSSID1と表示される）にマルチPSKを設定するには、最初に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、Multi PSKには以下の制約があります：

- 最大4つのWiFiネットワークでMulti PSKを設定することができます。
- マルチPSKを設定する各WiFiネットワークは、最大8つのVLAN-パスフレーズマッピングをサポートすることができます。(各 WiFi ネットワーク内では、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 Multi PSK VLAN-to-Passphrase 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 Multi PSK VLAN-to-passphrase マッピングをサポートすることができます。
- 1つのWiFiネットワーク上のMulti PSK内で、同じVLAN IDを異なるパスフレーズにマッピングすることができます。また、異なるWiFiネットワークでMulti PSKに同じVLAN IDを使用することも可能です。
- 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ネットワーク上で異なる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、互いに通信することができず、孤立したままです。
  - 異なるWiFiネットワークで*同じ*VLANに接続されているWiFi*クライアントが*を伝え合う。
- Multi PSKと以下の機能は相互に排他的です：
  - 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（111ページ）」をご参照ください。
  - mDNSゲートウェイ（「マルチキャストDNSゲートウェイの管理（159ページ）」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を設定する（215ページ）」を参照）。
  - 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（216ページ）参照

WiFiネットワークのMulti PSKを設定する場合：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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を選択することができます。

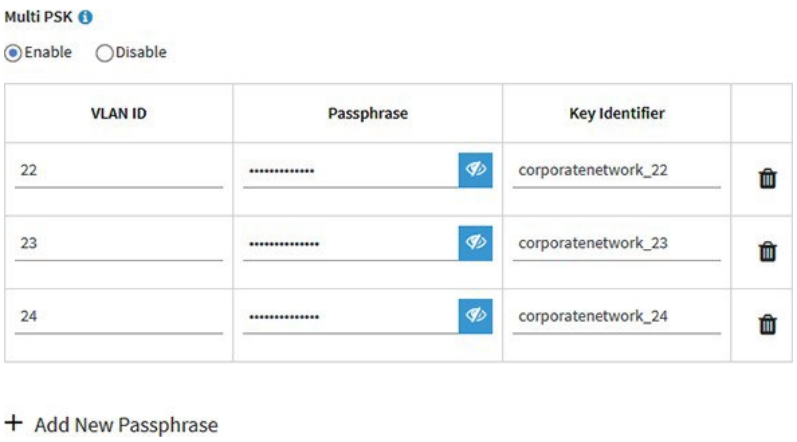
5. SSIDの左側にある「**＞」ボタンを**クリックします。

   選択したSSIDの設定項目が表示されます。

   マルチPSKは、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）には設定することができません。

6. Multi PSK **Enable**」ラジオボタンを選択します。

   下図に例を示します。



7. Add New Passphraseの左側にある＋ボタンをクリックします。

   ページが調整されます。

8. Multi PSKの設定を行います：
   - **VLAN ID**：WiFiクライアントが所属するようになるVLANであるVLAN IDを指定します。
   - **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する必要がある固有のパスフレーズ（WiFiパスワード）です。
   - **Key Identifier**：監視のためにWiFiネットワーク内のVLANを識別できるフレーズまたは用語です。最大長は、次の特殊文字：ハイフン（-）とアンダースコア（_）を含む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てください。

   Multi PSKエントリーを削除するには、エントリー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・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することが可能です。

WiFiネットワークのスケジューリング 休暇、オフィス閉鎖、夜間、週末にWiFiネットワークをオフにすることができるグリーン機能です。

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することができます。そ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を無効にする時間または時刻を指定します。

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したりする場合：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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を選択することができます。

5. SSIDの左側にある「**＞」ボタンを**クリックします。

   選択したSSIDの設定項目が表示されます。

6. Schedule］で、次のラジオボタンのいずれかを選択します：

   - **Always ON**：WiFiネットワークが有効になっています。
   - **Always OFF**：WiFiネットワークが無効になっています。
   - **Custom**：WiFiネットワークは、設定する必要がある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. 前の手順で「Custom」**を**選択した場合は、次のようにします：

   a. ラジオボタンの横の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あらかじめ定義された時間を選択するか、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）であることを示します。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ます。

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ネットワーク管理でバンドステアリングを有効または無効にする。

バンドステアリングは、アクセスポイントが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または5GHz帯に誘導することができます。2.4GHz帯と比較して、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、より良いユーザー体験を可能にします。バンドステアリングには、802.11k無線リソース管理（RRM）および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、次の方法でネットワークに影響を与えます：qq

- **802.11k RRM**：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が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し、802.11k対応クライアントが初期接続またはローミングに最適なアクセスポイントを自動的に選択できるようにします。
- **802.11v WiFiネットワーク管理**：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または5GHzバンド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ー（RSSI）の閾値を自動的に設定します。(つまり、RSSI の閾値を手動で設定することはできません)。

WiFi ネットワークの 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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、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、35 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。
   表示されたページで、SSIDを選択することができます。

5. SSIDの左側にある「**＞」ボタンを**クリックします。
   選択したSSIDの設定項目が表示されます。

6. Band Steering / 802.11 k/v］で、次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を無効にします。これはデフォルトの設定です。
   - **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または5GHzバンドに誘導します。

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

7

無線の基本機能を管理する

この章では、アクセスポイントの基本的な無線機能を管理する方法について説明します。高度な無線機能については、「高度な無線機能の管理」（235 ページ）を参照してください。

注意：2.4GHzの無線機能を変更すると、2.4GHz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 の無線機能を変更した場合、その変更は 5 GHz 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。

本章には、以下の項目があります：

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る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：本書において、***WiFi***ネットワークとは、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ネットワークという場合は、個々のSSIDまたはVAPを意味します。

無線の基本的なWiFi設定の管理

各無線の基本WiFi設定は、無線に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。2.4GHzと5GHzの無線の設定は、個別に指定できます。

無線の基本的なWiFi設定を管理するため：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。

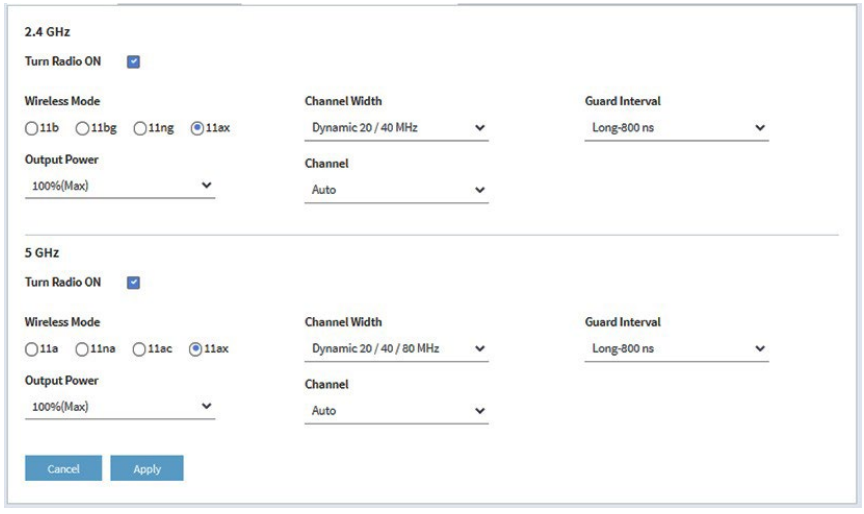
   ログインウィンドウが表示されます。

   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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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。



以下の説明は両方の無線に適用されますが、2.4GHzと5GHzの無線設定を個別に指定することができます。

5. 以下の設定を行います：

- **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。無線機をオフにすると、その帯域のWiFiアクセスが無効になるので、設定、ネットワークの調整、トラブルシューティングの際に便利です。
- **Wireless Mode**：
  2.4GHz無線の無線モード（WiFiモード）は、次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。これはデフォルトの設定です。
  - **11ng**：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可能です。ただし、802.11axクライアントの速度は、802.11ngでサポートされている最大速度（約400Mbps）に制限されています。
  - **11bg**：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。ただし、802.11axと802.11ngクライアントの速度は、802.11bgでサポートされている最大速度（約54Mbps）に制限されています。
  - **11b**：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可能です。ただし、802.11ax、802.11n、802.11bgクライアントの速度は、802.11bでサポートされている最大速度（約11Mbps）に制限されています。

  5GHz無線の無線モード（WiFiモード）を次の中から選択します：
  - **11ax**：802.11ax, 802.11ac, 802.11na, および 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。これはデフォルトの設定です。
  - **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でサポートされる最大速度（約867Mbps）に制限されています。
  - **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することができます。ただし、802.11ax、802.11ac、802.11naクライアントの速度は、802.11aでサポートされている最大速度（最大約54Mbps）に制限されています。
- **Channel Width**：メニューから、無線のチャンネル幅を選択します。Wireless Mode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、また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を参考にしてください：

- 広いチャンネルは性能を向上させます（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します）。
- 802.11n仕様では、他のモードで使用可能なレガシー20MHzチャンネルに加え、40MHz幅のチャンネルを使用することができます。
- 802.11ac仕様では、他のモードで使用可能な20MHz、40MHzのチャンネルに加え、80MHz幅のチャンネルを使用することができます。
- 40MHzと80MHzのチャンネルは、より高いデータレートを可能にしますが、使用できるチャンネルは少なくなります。

詳しくは、「無線のチャンネル幅を変更する（103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)** のいずれかを選択することができます。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、同じチャンネルで動作している場合、干渉が発生することがあります。このような状況では、アクセスポイントの出力パワーを下げるとよいでしょう。お住まいの国の無線周波数（RF）総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。

- **Channel**：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、アクセスポイントに選択した国と無線によって異なります。デフォルトは自動で、無線機が自動的に最適なチャンネルを選択できるようになっています。

  注：干渉が発生しない限り、WiFiチャンネルを変更する必要はありません（接続が失われることで示されます）。

  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ンネルを選択することで、干渉を低減してください。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帯の場合、チャンネル1と5、または6と10を使用します）。

6. **Apply**］ボタンをクリックします。
   警告のポップアップウィンドウが表示されます。
7. **OK**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、設定が保存されます。無線が再起動し、WiFiクライアントの再接続が必要になる場合があります。

無線をオン／オフする

デフォルトでは、2.4GHzと5GHzの両無線は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、そのバンド内のすべての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、ネットワークの調整、トラブルシューティングの際に便利です。

無線をオン／オフする場合：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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. 次のいずれかのアクションを行います：
   - **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**］ボタンをクリックします。
   警告のポップアップウィンドウが表示されます。
7. **OK**ボタンをクリックします。
   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クライアントの再接続が必要になる場合があります。

無線のWiFiモードを変更する

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、および 802.11a クライアントをサポートしています。WiFiモードを変更すると、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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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：

   - **2.4GHz**：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。これはデフォルトの設定です。
     - **11ng**：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可能です。ただし、802.11axクライアントの速度は、802.11ngでサポートされている最大速度（約400Mbps）に制限されています。
     - **11bg**：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。ただし、802.11axと802.11ngクライアントの速度は、802.11bgでサポートされている最大速度（約54Mbps）に制限されています。

  - **11b**：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可能です。ただし、802.11ax、802.11n、802.11bgクライアントの速度は、802.11bでサポートされている最大速度（約11Mbps）に制限されています。

- **5GHz**：5GHz 無線の WiFi モードとして、次のいずれかを選択します：
  - **11ax**：802.11ax, 802.11ac, 802.11na, および 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。これはデフォルトの設定です。
  - **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でサポートされる最大速度（約867Mbps）に制限されています。
  - **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に制限されます（約450Mbps）です。
  - **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することができます。ただし、802.11ax、802.11ac、802.11naクライアントの速度は、802.11aでサポートされている最大速度（最大約54Mbps）に制限されています。

6. **Apply**］ボタンをクリックします。
   警告のポップアップウィンドウが表示されます。

7. **OK**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、設定が保存されます。無線機または無線機が再起動し、WiFiクライアントの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定する際には、以下のガイドラインを参考にしてください：

- 広いチャンネルは一般的に性能を向上させます（干渉がない、または少ない、データレートが良い）。
- 一般的に狭いチャンネルはスループットが低下しますが、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、厳しい状況下でより安定した接続を提供できる場合があります。
- 802.11n仕様では、他のWiFiモードで使用できるレガシーな20MHzチャンネルに加えて、40MHz幅のチャンネルを使用することができます。

- 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幅のチャンネルを利用することができます。
- 40MHzと80MHzのチャンネルは、より高いデータレートを可能にしますが、使用できるチャンネルは少なくなります。

注：デフォルトのオプション（2.4GHz無線はDynamic 20 / 40 MHz、5GHz無線はDynamic 20 / 40 / 80 MHz）のままにすることをお勧めします。アクセスポイントは、WiFi環境に最適なチャンネル幅を自動的に選択することができます。

WiFiモード（無線のWiFiモードを変更する（102ページ）参照）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可能かが決まります。

無線のチャンネル幅を変更する場合：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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。
   - **20MHz**。
   - **40MHz**。
   - **80MHz**：この選択は、5GHzでのみ有効です。

- **Dynamic 20 / 40 MHz**。この選択は2.4GHzでのみ可能で、その無線のデフォルト設定です。
- **Dynamic 20 / 40 / 80 MHz**。この選択は5GHzでのみ可能で、その無線のデフォルト設定です。

6. **Apply**］ボタンをクリックします。
   警告のポップアップウィンドウが表示されます。
7. **OK**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、設定が保存されます。無線が再起動し 、WiFiクライアントの再接続が必要になる場合があります。

無線のガード間隔を変更する

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（102 ページ）参照）により、ガード間隔を設定できるかどうか、また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を参考にしてください：

- WiFi機器とアクセスポイントの距離が短い環境では、ガードインターバルを短くすることでスループットの向上をサポートします。
- 複数のSSIDが存在し、アクセスポイントから離れた場所で動作するWiFi機器がある環境では、ガードインターバルを長くすることが有効です。
- レガシーデバイスの中には、長い-800nsのガードインターバルのみで動作するものもあります。

無線のガード間隔を変更するには

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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。ワイヤレス設定］ページが表示されます。
5. 無線の「**Guard Interval**」メニューから、次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 モードで利用可能です。11ax WiFiモードでは、このオプションはデフォルト設定です。
   - **Double Long-1600ns**：このオプションは、11ax WiFiモードでのみ利用可能です。
   - **Quadruple Long-3200ns**：このオプションは、11ax WiFiモードでのみ使用可能です。
6. **Apply**］ボタンをクリックします。
   警告のポップアップウィンドウが表示されます。
7. **OK**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、設定が保存されます。無線が再起動し、WiFiクライアントの再接続が必要になる場合があります。

無線の出力パワーを変更する

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、同じチャンネルで2つ以上のアクセスポイントが動作している場合、干渉が発生することがあります。このような状況では、アクセスポイントの出力パワーを下げるとよいでしょう。お住まいの国の無線周波数（RF）総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。

無線の出力電力を変更する場合：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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。ワイヤレス設定］ページが表示されます。

5. **Output Power**メニューから、**100%（Max）**、**50%**、**25%**、**12.5%**、**4%（Min）**を選択します。

   デフォルトは100%(Max)です。

6. **Apply**］ボタンをクリックします。

   警告のポップアップウィンドウが表示されます。

7. **OK**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、設定が保存されます。無線が再起動し、WiFiクライアントの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、アクセスポイントや無線機で選択した国によって異なります。デフォルトは「自動」で、無線機が自動的に最適なチャンネルを選択できるようになっています。

注：干渉が発生しない限り、WiFiチャンネルを変更する必要はありません（接続が失われることで示されます）。

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ンネルを選択することで、干渉を低減してください。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帯の場合、チャンネル1と5、または6と10を使用します）。

無線のチャンネルを変更する場合：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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です。特定のチャンネルを選択すると、チャンネル選択が固定になります。
6. **Apply**］ボタンをクリックします。
   警告のポップアップウィンドウが表示されます。
7. **OK**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、設定が保存されます。無線が再起動し、WiFiクライアントの再接続が必要になる場合があります。

WiFi無線のサービス品質管理

2.4GHz 無線と 5GHz 無線の QoS（サービス品質）設定を個別に指定できます。これらの設定は、両方の無線で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を与える場合があります。

WiFi無線のQoS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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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 > 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、該当するものを選択します。
   ラジオボタンの**有効／無効を設定します：**

   - **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などの時間依存の情報は、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 が正しく機能するためには、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 で制御できるようになります。WMM では、優先順位の低い順に次の 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非常に適しています。
     - **Video**：遅延が少なく、2番目に優先度の高いキューです。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です。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。
     - **Background**：スループットの高い低優先度キューです。FTPなど、時間的な制約が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る。

- **WMM Powersave**：WMM Powersave機能を有効にすると、バッテリー駆動のデバイスの電力を節約し、消費電力を細かく調整することができます。

6. **Apply**］ボタンをクリックします。
   警告のポップアップウィンドウが表示されます。
7. **OK**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、設定が保存されます。無線機または無線機が再起動し、WiFiクライアントの再接続が必要になる場合があります。

8

キャプティブポータルのセットアップと管理

この章では、アクセスポイントにキャプティブポータルを設定し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は、ユーザーがWiFiネットワークに接続しようとするときに表示されるウェブページです。キャプティブポータルにはスプラッシュページがあり、通常、ユーザーに対して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です。WiFiネットワークごとに、独自のクリックスルー・キャプティブ・ポータルを設定することができます。
- **External captive portal**：外部キャプティブポータルベンダーによってホストされているポータルです。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可能です。
- **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することができます。

この章には、以下の項目があります：

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（90ページ）を参照）。

注：本書において、***WiFi***ネットワークとは、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ネットワークという場合は、個々のSSIDまたはVAPを意味します。

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

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ポータルであり、つまり外部キャプティブポータルではありません。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（EULA）への同意をユーザーに求め、特定のWebサイトにリダイレクトすることができます。クリックスルーの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。

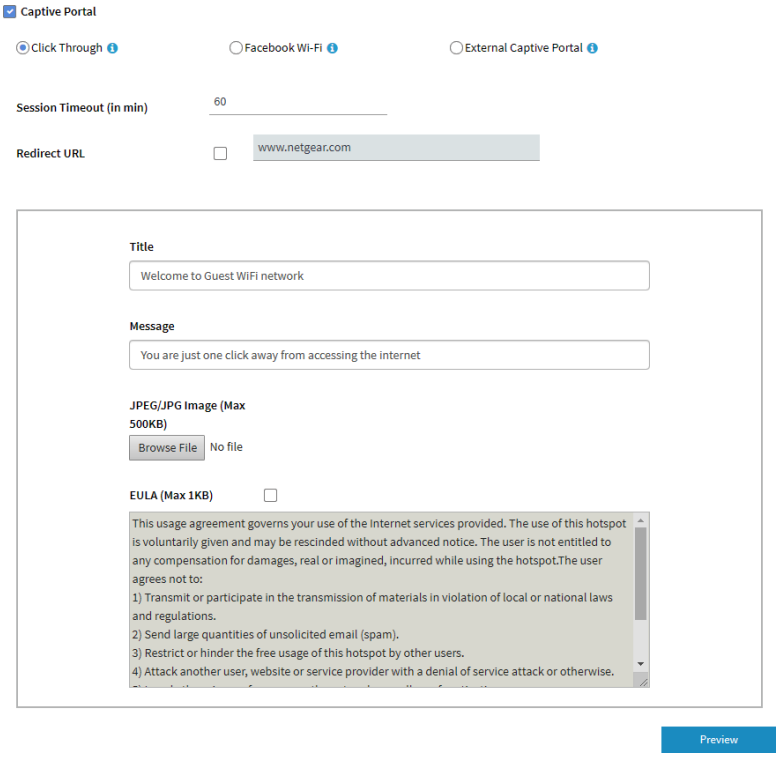
WiFiネットワークにクリックスルーのキャプティブポータルを設定するには：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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を選択することができます。
5. SSIDの左側にある「**＞」ボタンを**クリックします。
   選択したSSIDの設定項目が表示されます。
6. 下にスクロールして、「**＞Advanced**」タブをクリックします。
   ページが展開されます。
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。



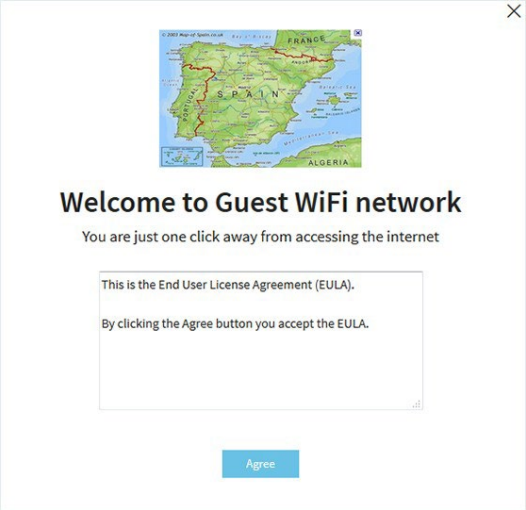
8. クリックスルーの設定は、次の表のように指定します。

設定	概要
Session Timeout (in min)	WiFiセッションが終了し、ユーザーが再ログインする必要があるまでの分数を1～1440の範囲で入力します。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、キャプティブポータルのログインページにはデフォルトのタイトルが表示されます。
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ログインページに表示されます。

(続き)

設定方法	概要
JPEG/JPG Image (Max 500 KB)	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、キャプティブポータルログインページにはデフォルトの画像が表示されます。
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することができます。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場合は、「**Preview**」ボタンをクリックします。
   次の図はその例です（つまり、図はデフォルトのキャプティブポータルではなく、カスタマイズされたものを示しています）。



10. **Apply**］ボタンをクリックします。
    設定が保存されます。SSIDに接続しようとするWiFiクライアントには、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。

    注意：キャプティブポータル認証が行われるまで、HTTPSセッションはブロックされます。

WiFiネットワークに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は、外部キャプティブポータルベンダーによってホストされるポータルである。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、一般に、ベンダーにデバイスを登録し、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可能です

WiFiネットワークに外部キャプティブポータルを設定する：

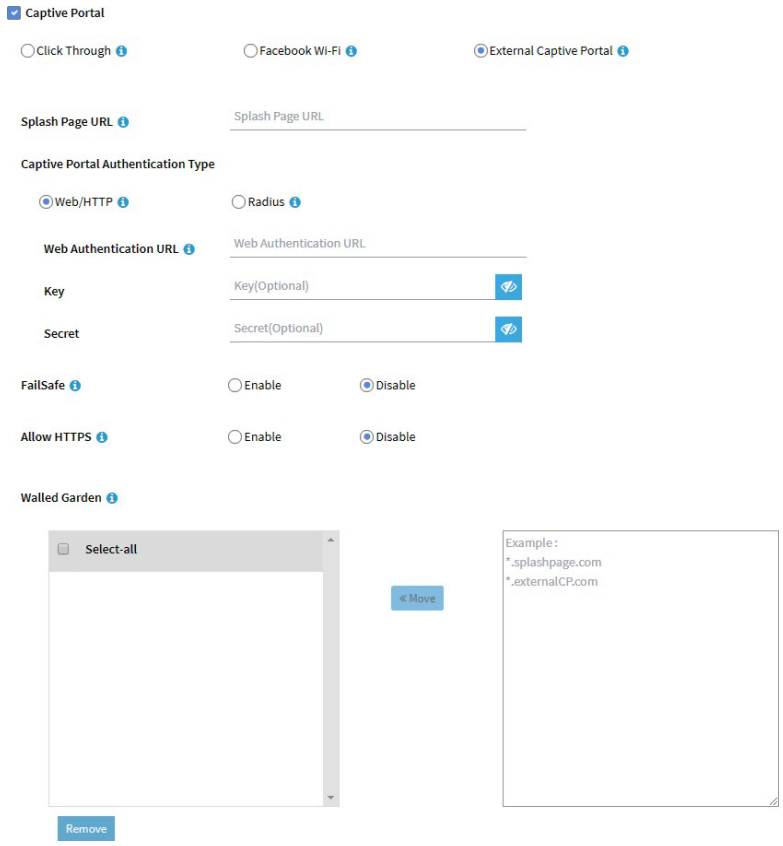
1. アクセスポイントと同じネットワークに接続されているパソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。
   ログインウィンドウが表示されます。

   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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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を選択することができます。
5. SSIDの左側にある「**＞」ボタンを**クリックします。
   選択したSSIDの設定項目が表示されます。
6. 下にスクロールして、「**＞Advanced**」タブをクリックします。
   ページが展開されます。
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**の欄には、ベンダーから提供される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Web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. **Captive Portal Authentication Type**］のラジオボタンで、次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ための認証は、HTTPSプロトコルを使用してアクセスポイント上で行われます。以下の設定を指定します：
  - **Web Authentication URL**：ベンダーから提供される 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します。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します。
  - **Secret**：ベンダーから提供されるシークレットクレデンシャルを入力します。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します。
- **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ます。また、ベンダーがアカウンティングRADIUSサーバーを指定する場合があります。

各 RADIUS サーバーについてベンダーの指示に従い、以下の設定を指定する：

- **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、ベンダーから提供されます。デフォルトでは、認証サーバーはポート番号1812を使用し、会計サーバーはポート番号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から提供されます。

11. 認証ができない場合に、ユーザーがスプラッシュページに到達して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するには、次の**FailSafe**ボタンのいずれかを選択します：

- **Enable**：キャプティブポータルサーバーが応答しないなど、認証ができない場合でも、30分間はインターネットへのアクセスが許可されます。
- **Disable**：これはデフォルト設定です。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ない。代わりに、次のようなメッセージが表示されます。おっと。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、安全な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ます。
- **Disable**：これはデフォルトの設定です。HTTPSトラフィックは認証が行われた後にのみ許可されます。

13. **Walled Garden**の設定を行います。

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します。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します。ベンダーのスプラッシュページ、ドメイン名、および認証サーバーもウォールド・ガーデンに含める必要があります。ベンダーの指示に従います。

ウォールードガーデンの構成は以下のようになります：

- **Add a single URL**：右のフィールドにURLを入力し、**Enter**キーを押して、「**Move**」をクリックします。ボタンをクリックします。
- **Add multiple URLs**：右側のフィールドにURLのリストを貼り付け、「**Move**」をクリックします。ボタンをクリックします。
- **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**］ボタンをクリックします。

    設定が保存されます。SSIDに接続しようとするWiFiクライアントには、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。

アクセスポイントにFacebook Wi-Fiを登録・設定する

アクセスポイントにFacebook Wi-Fiを設定し、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（WiFiネットワークにFacebook Wi-Fiキャプティブポータルを設定（120ページ）参照）前に、アクセスポイントをFacebookに登録しFacebook設定を行う必要があります。デフォルトでは、登録する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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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 **Yes**」ラジオボタンを選択します。

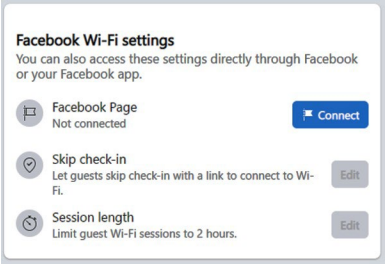
   登録する機能が有効になっています。デフォルトでは、この機能は無効になっています。

6. **Apply**］ボタンをクリックします。
   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**ボタンをクリックします。
   ポップアップウィンドウが閉じます。

   ブラウザページが起動し、Facebookページが表示されます。



9. Facebook Wi-Fiの設定をする：
   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省略させる場合は、「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場合は、「Session length Edit」ボタンをクリックし、設定を行ってください。
      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されます。

10. ローカルブラウザのUIでページをリフレッシュする。

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行われる*前に*安全なHTTP（HTTPS）セッションを確立できるようにするには、「Allow HTTPS **Enable**」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行われるまで、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 アクセスを提供することができます。これを行う前に、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 (118 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：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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を選択することができます。
5. SSIDの左側にある「**＞」ボタンを**クリックします。
   選択したSSIDの設定項目が表示されます。
6. 下にスクロールして、「**＞Advanced**」タブをクリックします。
   ページが展開されます。
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. **Facebook Wi-Fiの**ラジオボタンを選択します。

ページ上でそれ以上の設定を指定する必要がないため、ページが再び調整されます。

顧客は、Facebookのビジネスページにチェックインすることで、WiFiアクセスを受けることができます。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 の設定を行います（アクセスポイントのFacebook Wi-Fi の登録と設定 (118 ページ)を参照）。

9. **Apply**］ボタンをクリックします。

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

   注：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認証が発生する*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安全な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（アクセスポイントのFacebook Wi-Fiの登録と設定（118ページ）を参照ください）。

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ー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て、アクセスポイントのエントリーを削除する場合：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、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、35 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**」ラジオボタンを選択します。
   登録する機能は無効になっています。ただし、アクセスポイントのFacebookビジネスページへの登録はまだ削除されていません。
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、自分のアカウントにログインします。
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**」ボタンをクリックします。
   アクセスポイントのエントリーが削除されます。

9

アクセス・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、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、以下の項目があります：

- インターネットにアクセスする際に、特定のURLやキーワードをブロックすることができます。
- ユーザーアカウントの管理
- ローカルMACアクセスコントロールリストの管理
- 近隣APの検出を管理する
- RADIUSサーバーをセットアップする
- L2セキュリティの有効化

注：必須のWiFiセキュリティ（ネットワーク認証と暗号化）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（72ページ）」をご覧ください。

注：本書において、***WiFi***ネットワークとは、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ネットワークという場合は、個々のSSIDまたはVAPを意味します。

インターネットにアクセスする際に、特定のURLやキーワードをブロックすることができます。

ブラックリストは、インターネットへのアクセスを拒否するURL（ウェブアドレス）を指定することで設定できます。また、キーワードを指定すると、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ができます。

インターネットへのアクセスを遮断する必要があるURL**やキーワードを含むブラックリストを設定する：**

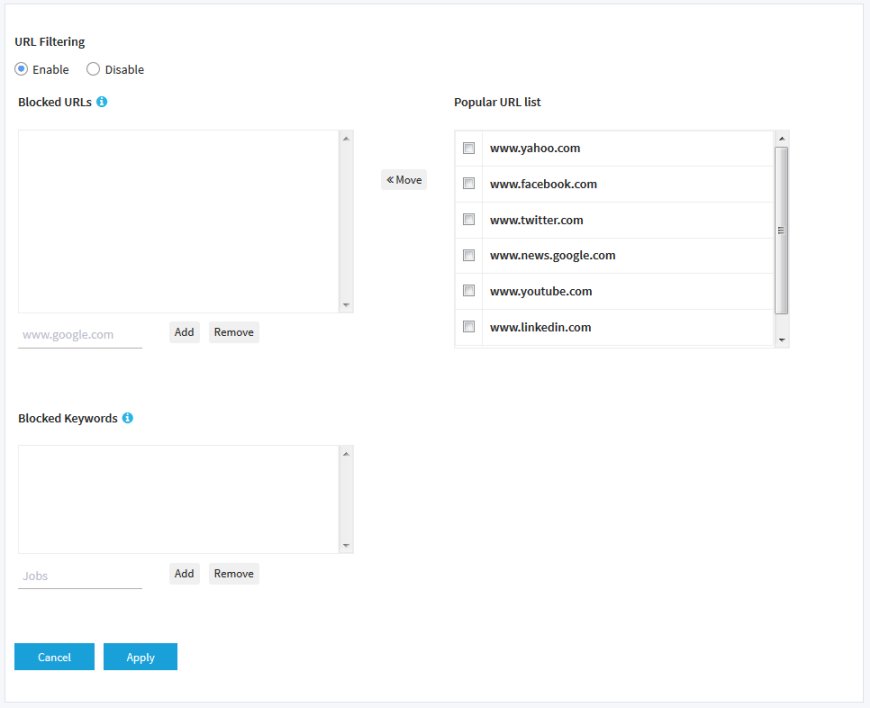
1. アクセスポイントと同じネットワークに接続されているパソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。
   ログインウィンドウが表示されます。

   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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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構成する：

- **Blocked URLs**：ブラックリストにURLを追加するには、**Addボタンの**左側にURLを入力またはコピーして、**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で、Popular URL list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、**Remove**ボタンをクリックします。
  URLをブロックすると、そのドメインとその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 ドメインのすべてのウェブページがブロックされ、たとえば、www.google.com/financeもブロックされます。
- **ブロックされたキーワード**キーワードエントリーをブラックリストに追加するには、下のフィールド（**Addボタンの**左側）にキーワードを入力し、**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ーを削除するには、そのエントリーのチェックボックスを選択し、下の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を追加した場合、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ーUIに対して、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。admin 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、パスワードの変更は可能です。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。

次のセクションでは、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：

- ユーザーアカウントを追加する
- 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を変更する（167ページ）」を参照してください。

ユーザーアカウントを追加する

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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、および1つの数字が含まれていなければなりません。以下の特殊文字が使用可能です：
     !@ # $ % ^ & * ( )
   - **Privilege**：メニューから、「**Read-Write**」または「**Read-Only**」を選択します。
   - **Session Timeout**：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するには、「**Hours**」と「**Minutes**」のフィールドを使用します。
     デフォルトでは、セッションは45分後に失効します。
7. **Apply**］ボタンをクリックします。設定が保存されます。

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ーUIにログインした場合、45分後にセッションが自動的にタイムアウトします。タイムアウト時間は変更可能で、管理者ユーザーを含む全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、次のようにします：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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. セッションタイムアウト］では、［**時間**］と［**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、セッションは45分後に失効します。

6. **Apply**］ボタンをクリックします。

   設定が保存されます。セッションが終了し、再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を変更することはできません。

ユーザーアカウントのユーザー名、パスワード、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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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します：

   - **User Name**：別のユーザー名を入力します。
   - **Password**：8文字から64文字の間で別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、および1つの数字が含まれていなければなりません。以下の特殊文字が使用可能です：
     !@ # $ % ^ & * ( )
   - **Privilege**：メニューから、「**Read-Write**」または「**Read-Only**」を選択します。

6. **Apply**］ボタンをクリックします。設定が保存されます。

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。デフォルトの管理者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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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にある「**X**」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ます。

6. **Delete**」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、ユーザーアカウントが削除されます。

ローカルMACアクセスコントロールリストの管理

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 は、合計 512 個の MAC アドレスを含むことができます。

アクセスを許可するポリシーを持つACLを設定し、そのACLをWiFiネットワーク（つまりSSID）に適用した場合、ACLは次のように機能します：

- ACLにMACアドレスを登録したWiFi機器に、WiFiネットワークへのアクセスを許可します。
- 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を持つ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は次のように機能します：

- ACLにMACアドレスを登録した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た後にのみ有効になります。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 を選択する (２２１ページ)」を参照してください。MAC ACL は、複数の WiFi ネットワークに適用することができます。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Listを手動で設定する。
- 既存のMACアクセスコントロールリストをインポートする

MACアクセス制御Listを手動で設定する。

それぞれ最大 512 の MAC アドレスに基づく最大 8 つのアクセス制御リスト（ACL）を構成することができます。アクセスポイントには、以下のデフォルトのグループ名と設定を持つ MAC ACL が含まれていますが、変更することができます：

- **Management**：有効な場合、デフォルトで信頼できるステーションへのアクセスを許可します。
- **Guest**：有効にすると、デフォルトで信頼できるステーションへのアクセスを許可します。
- **Guest1**：有効にすると、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します。
- **Custom**：有効にすると、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します。
- **Custom 1**：有効にすると、デフォルトで信頼できるステーションへのアクセスを許可します。
- **Custom 2**：有効にすると、デフォルトで信頼できるステーションへのアクセスを許可します。
- **Custom 3**：有効にすると、デフォルトで信頼できるステーションへのアクセスを許可します。
- **Custom 4**：有効にすると、デフォルトで信頼できるステーションへのアクセスを許可します。

デフォルトでは、これらのMAC ACLは無効であり、ステーションは含まれません。デバイスを手動で追加するか、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（134ページ）」を参照）、またはその両方を実行することができます。

MAC ACL を使用して、どの WiFi デバイス（ステーション）が WiFi ネットワークにアクセスできるかを制御することができます。1つのMAC ACLを複数のWiFiネットワークに適用することができます。

MAC ACLを手動で設定する場合：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。

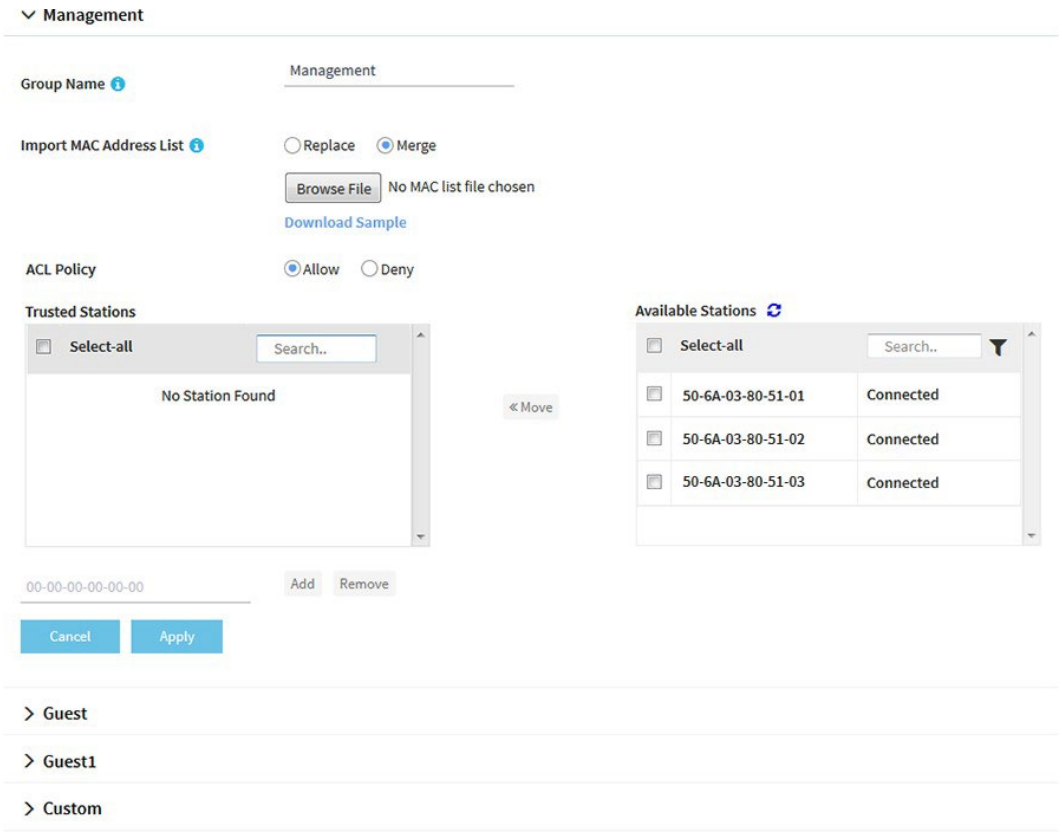
   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳しくは、「ブラウザのセキュリティ警告が表示された場合の対処方法（55ページ）」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

ユーザー名は**admin**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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. 設定する MAC ACL のグループ名をクリックします。



前の図では、いくつかの例を示しています。Available Stations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に共通するため、複数のMAC ACLにデバイスを追加することができます。近隣のステーション は 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場合は、「**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です。

7. ACL Policy **Allow** or **Deny** ラジオボタンを選択します。

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、その他の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、その他の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. 次のようにACLを構成する：

- 手順7で「**Allow**」ラジオボタンを選択したACLについて、以下を実行します：
  - 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MACアドレスを00-00-00-00のフォーマットで入力し、**Add**ボタンをクリックします。
    デバイスがTrusted Stationsテーブルに追加されます。
  - 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。Available Stationsテーブルを検索することができます。また、フィルターアイコンをクリックすると、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のテーブルを検索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。
- 手順7で「**Deny**」ラジオボタンを選択したACLについて、以下を実行します：
  - 手動でUntrusted Stationsテーブルにデバイスを追加するには、Untrusted Stationsテーブルの下のフィールドにMACアドレスを00-00-00-00の形式で入力し、「**Add**」ボタンをクリックします。
    Untrusted Stations テーブルにデバイスが追加されます。
  - 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、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、フィルター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ー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**」ボタンをクリックします。
    Untrusted Stationsテーブルを検索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ネットワークへのACL適用の詳細については、「WiFiネットワークのMAC ACLの選択（221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することができます。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することはできません。

既存のMACアクセスコントロール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）をインポートすることができます。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で使用したい場合は、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アドレスが記載されたファイルは、以下の形式である必要があります：

- ファイル内の項目は、00-11-22-33-44-55のように、各オクテットをハイフンで区切った16進数形式のMACアドレスのみでなければなりません。
- エントリーはカンマで区切る必要があります。
- ファイルはテキスト形式（つまり、拡張子が .txt または .cfg であること）でなければなりません。

MAC ACL を使用して、どの WiFi デバイスが WiFi ネットワークにアクセスできるかを制御することができます。MAC ACL は、複数の WiFi ネットワークに適用することができます。

既存の MAC ACL をインポートするには、次のようにします：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」を参照してください。

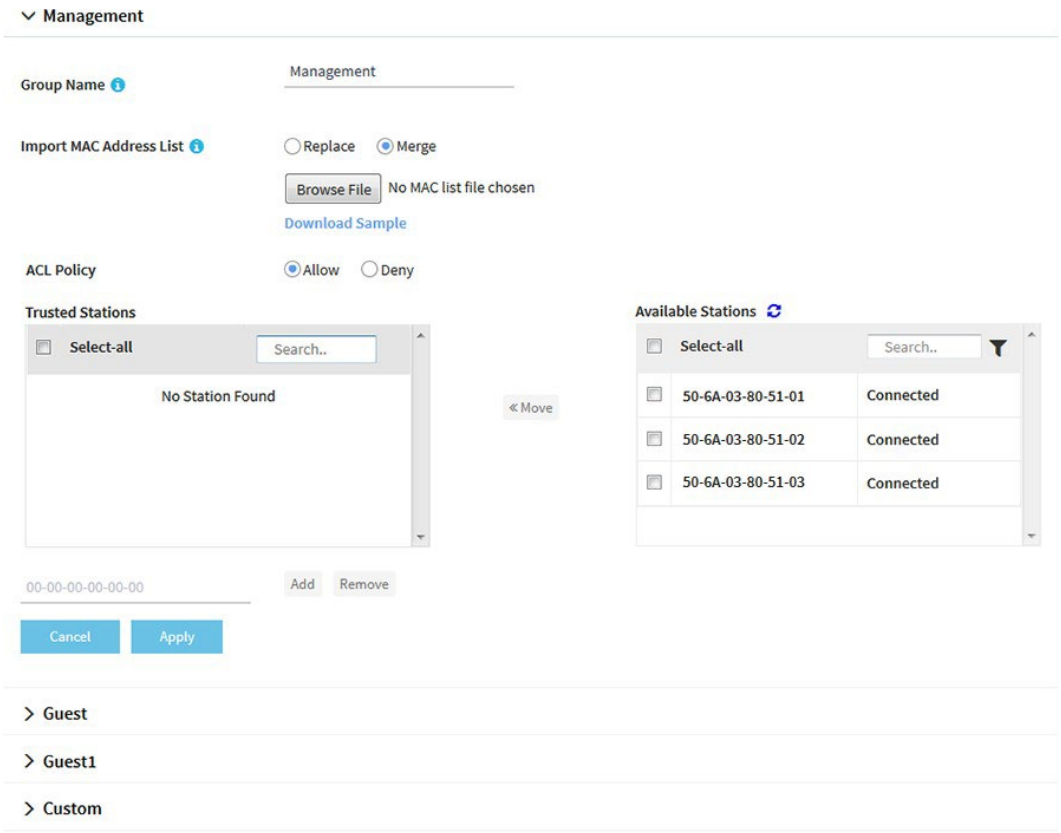
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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. 設定する MAC ACL のグループ名をクリックします。



前の図では、いくつかの例を示しています。Available Stations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に共通するため、複数のMAC ACLにデバイスを追加することができます。隣接するステーションは「Neighbor」と表示され、接続されたステーションは「connected」と表示されます。

6. グループ名を変更する場合は、「**グループ名**」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です。

7. ACL Policy **Allow** or **Deny** ラジオボタンを選択します。

   Allow］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が許可されますが、その他の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が拒否されますが、その他のすべての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**」リンクをクリックしてください。
9. 以下の方法でACLをインポートして構成します：

- 手順7で「**Allow**」ラジオボタンを選択したACLについて、以下を実行します：
  a. 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、またはマージするには、次のラジオボタンのいずれかを選択します（すでにテーブル内にMACアドレスがある場合）：
     - **Replace**：Trusted StationsテーブルのMACアドレスが、インポートリストのものに置き換えられます。
     - **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ます。
  b. **Browse**」ボタンをクリックし、インポートファイルを移動して選択します。インポートリストのMACアドレスは、Trusted Stationsテーブルに配置されます。
  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。

- 手順7で「**Deny**」ラジオボタンを選択したACLについて、以下を実行します：
  a. 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）に置換または統合するには、次のラジオボタンのいずれかを選択します：
     - **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に置き換えられます。
     - **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ます。
  b. **Browse**」ボタンをクリックし、インポートファイルを移動して選択します。インポートリストのMACアドレスは、「Untrusted Stations」テーブルに配置されます。

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**］ボタンをクリックします。
設定が保存されます。信頼できるステーション」テーブルまたは「信頼できないステーション」テーブルのMACアドレスを手動で追加する方法については、「MACアクセス制御リストを手動で設定する（P131）」を参照してください。

WiFiネットワークへのACL適用の詳細については、「WiFiネットワークのMAC ACLの選択（221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することができません。

近隣APの検出を管理する

アクセスポイントは、無線帯域で近隣のアクセスポイント（AP）を検出することができ、それを既知の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、チャンネル上のすべてのアクセスポイントの情報を収集し、エリア内で検出したアクセスポイントのリストを保持します。初期状態では、検出されたすべてのアクセスポイントが「不明な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」に追加することができます。また、Known AP Listにある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」のアクセスポイントは、さらに調査が必要です。これらは、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。このようなタイプのアクセスポイントは、深刻なセキュリティ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 List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 Listに移動させる。
- 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：Energy Efficiency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 を検出できなくなります。5 GHz ラジオバンドで近隣 AP の検出を使用するには、まず、Energy Efficiency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（190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 Listに移動させる。

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として分類することができます。近隣 AP 検出を有効にすると、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保持します。初期状態では、検出されたすべてのアクセスポイントは、「不明な AP リスト」に表示されます。アクセスポイントをUnknown AP ListからKnown AP Listに手動で移動させることができます。

デフォルトでは、近隣アクセスポイント検出は無効です。

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 Listに移動させる：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

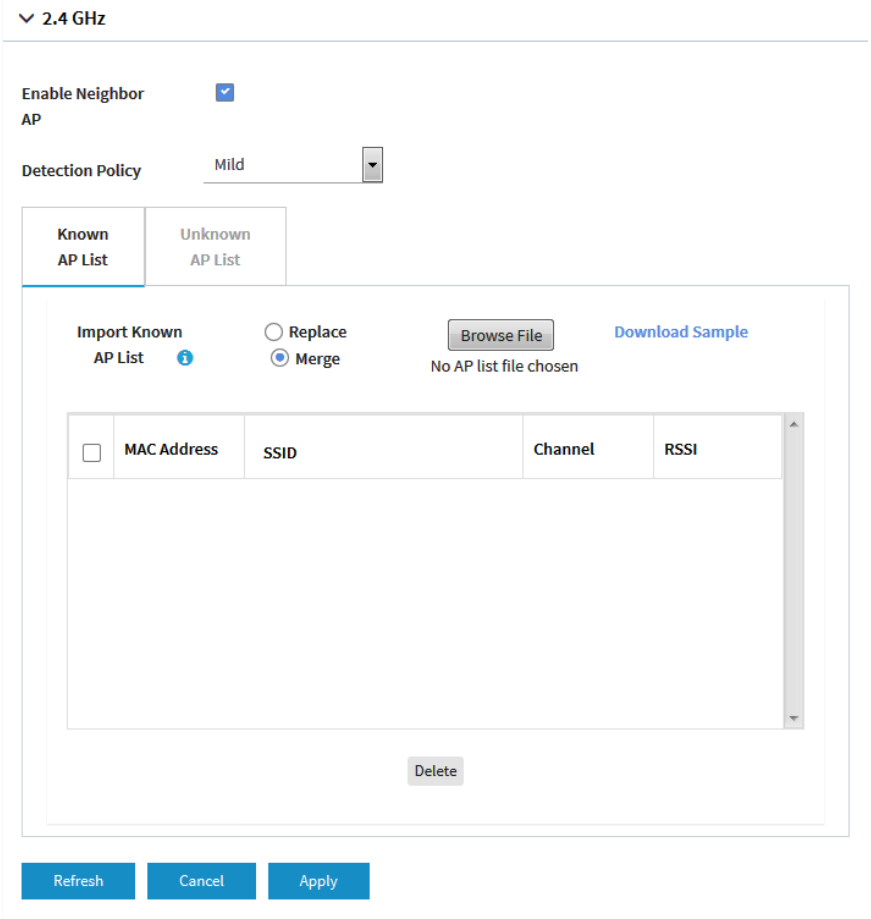
   以前にアクセスポイントを NETGEAR Insight ネットワークの場所に追加し、Insight Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の Insight ネットワークパスワードを入力します。詳細については、35 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   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。

   表示されたページで、無線バンド（2.4GHzまたは5GHz）を選択します。
5. 電波帯の左側にある「>」ボタンをクリックします。

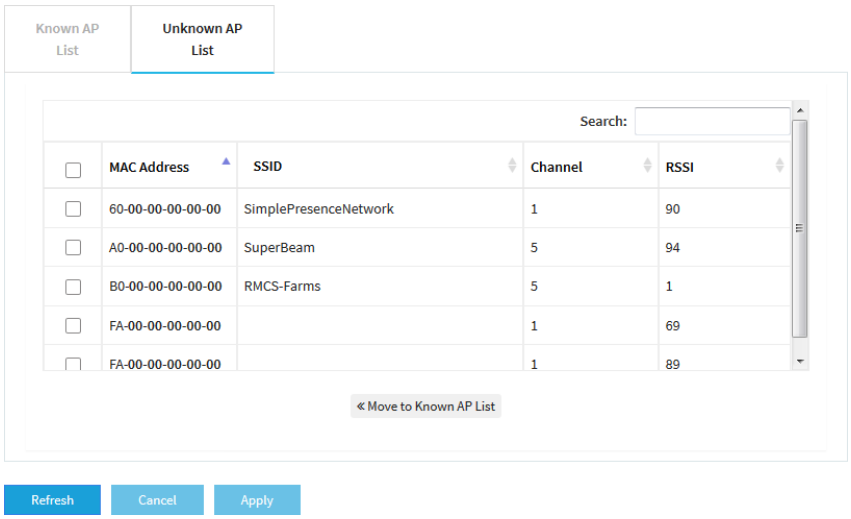
   選択した無線帯域の「Neighbor AP」ページが表示されます。
6. **Enable Neighbor AP**］チェックボックスを選択します。

7. **Apply**］ボタンをクリックします。
   設定が保存されます。Neighbor AP の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。これはデフォルトの設定です。
   - **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。検出された近隣のアクセスポイントは、「Unknown AP List」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、Unknown AP ListからKnown AP Listに移動するには、次のようにします：
   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てください。
   c. 使い慣れたアクセスポイント、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]**ボタンをクリックします。
   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 Listからアクセスポイントを削除することができます。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。

Known AP Listに、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インポートすることができます。

MACアドレスが記載されたファイルは、以下の形式である必要があります：

- ファイル内の項目は、00-11-22-33-44-55のように、各オクテットをハイフンで区切った16進数形式のMACアドレスのみでなければなりません。

- エントリーはカンマで区切る必要があります。
- ファイルはテキスト形式（つまり、拡張子が .txt または .cfg であること）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Known APリストへのアクセスポイントの移動（138ページ）」を参照してください。

Known AP Listに、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インポートする場合：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

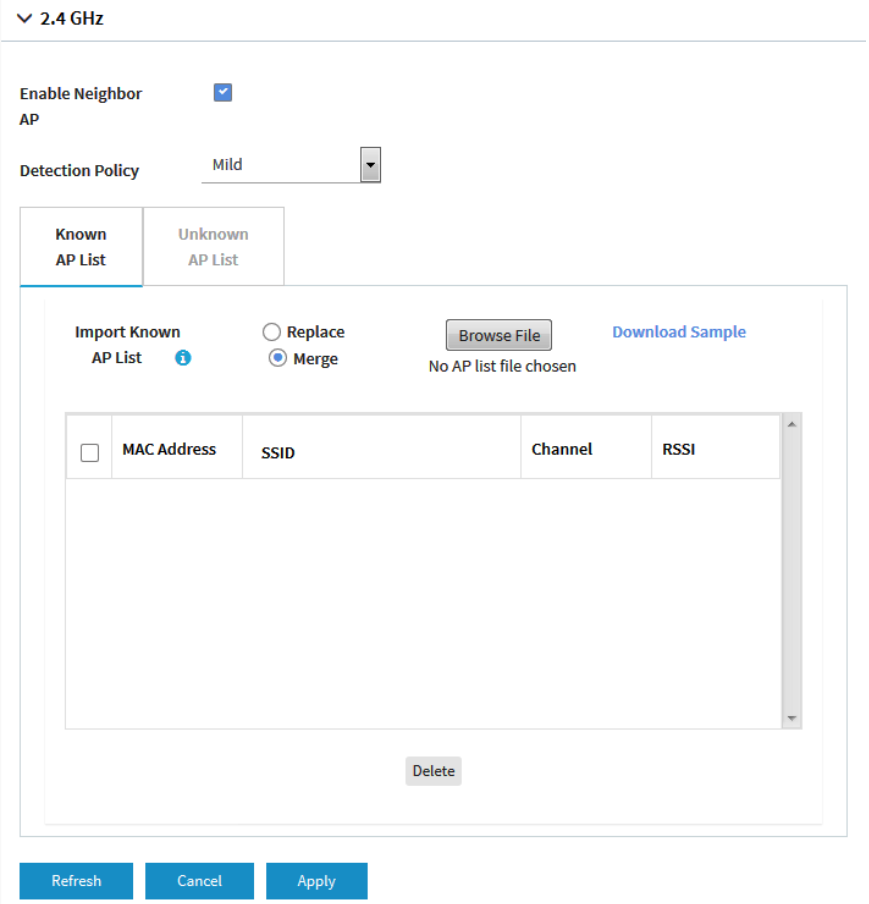
   以前にアクセスポイントを NETGEAR Insight ネットワークの場所に追加し、Insight Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の Insight ネットワークパスワードを入力します。詳細については、35 ページの「NETGEAR Insight アプリを使用して WiFi で接続する」を参照してください。

   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。

   表示されたページで、無線バンド（2.4GHzまたは5GHz）を選択します。

5. 電波帯の左側にある「>」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をインポートして構成します：
   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 ListのMACアドレスに置換またはマージします：
      - **Replace**：Known AP ListのMACアドレスが、インポートリストのものに置き換えられます。
      - **Merge**：Known AP ListのMACアドレスは、インポートリストのものとマージされます。
   b. **Browse**］ボタンをクリックし、インポートファイルを移動して選択します。インポートリストの MAC アドレスは、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 List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 Listに配置されます。

8. **Apply**］ボタンをクリックします。設定が保存されます。

RADIUSサーバーをセットアップする

WPA2 Enterprise security、WPA3 Enterprise security、またはRADIUS MAC ACLを使用する場合、認証用またはRADIUSを使用した認証とアカウンティングの両方にRADIUSサーバー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 サーバーを設定することができます。これらの RADIUS サーバーの設定は、WPA2 Enterprise セキュリティまたは WPA3 Enterprise 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（72 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します。

注：WPA2 Enterprise security または WPA3 Enterprise security と RADIUS MAC ACL のいずれかは、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（72 ページ）」を参照）。WiFi ネットワークに WPA2 Enterprise セキュリティまたは WPA3 Enterprise 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 (130 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MACアドレスに以下の例のような書式を使用して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 として指定します。

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。

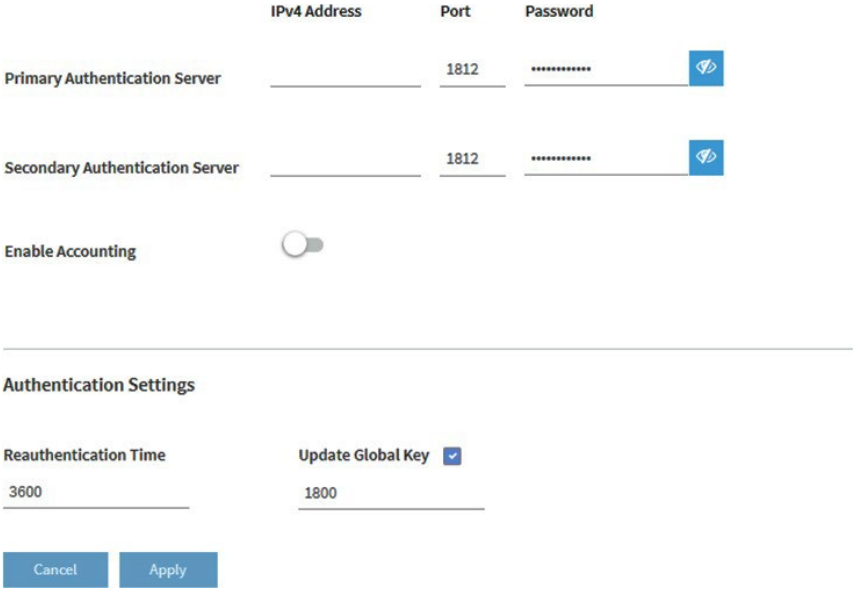
   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳しくは、「ブラウザのセキュリティ警告が表示された場合の対処方法（55ページ）」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。
   ユーザー名は**admin**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、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、35 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. 設定するRADIUSサーバーごとに、以下の設定を行います：

   - **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上の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処理中にアクセスポイントとRADIUSサーバーの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. 認証サーバーでアカウンティングを有効にするには、［**Enable Accounting**］をクリックし、ボタンが青く表示されるようにします。
7. 以下の認証設定を行い、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場合はチェックボックスを選択し、間隔を秒単位で入力します。デフォルトでチェックボックスが選択されており、デフォルトの間隔は1800秒（30分）です。グローバルキーの更新を行わないようにするには、チェックボックスをオフにします。

8. **Apply**］ボタンをクリックします。設定が保存されます。

L2セキュリティの有効化

L2 セキュリティは、WiFi インターフェース上の 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止できます。L2 セキュリティを有効にすると、アクセスポイントは、どの WiFi ネットワークでも ARP、IPv4、IPv6 トラフィックなど、特定の種類のクライアント トラフィックのみを許可します。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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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ます。

6. **Apply**］ボタンをクリックします。設定が保存されます。

10

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）およびIP設定を管理する方法について説明します。

この章には、以下の項目があります：

- DHCPクライアントを無効化し、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を設定する
- 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・無効化
- IGMP スヌーピングの有効化または無効化
- Ethernet LLDPの有効／無効を設定します。
- UPnPの有効化または無効化
- マルチキャストDNSゲートウェイを管理する

注：本書において、***WiFi***ネットワークとは、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ネットワークという場合は、個々のSSIDまたはVAPを意味します。

DHCPクライアントを無効化し、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や、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てください。

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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。

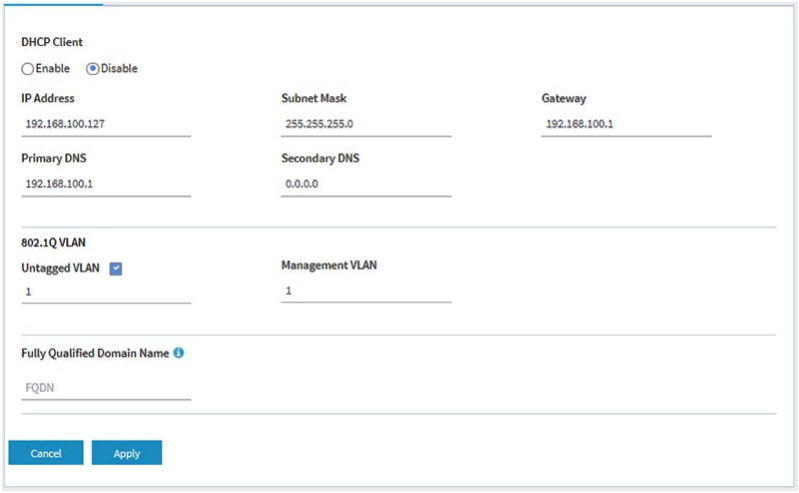
   ユーザー名は**admin**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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は、LANの設定を行うことができますが、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. 無効にする」ラジオボタンを選択します。



フィールドがマスクされなくなりました。

6. 次の表に記載されている設定を指定します。

設定	概要
IP Address	LANで使用する範囲のIPアドレス（通常は255.255.255.0）です。
Subnet Mask	サブネットマスクサブネットマスクは、お使いのLANに対応したものをご使用ください。
Gateway	LANのゲートウェイIPアドレスです。
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アドレスです。
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クライアントが有効になっており、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、再度有効にすることができます。

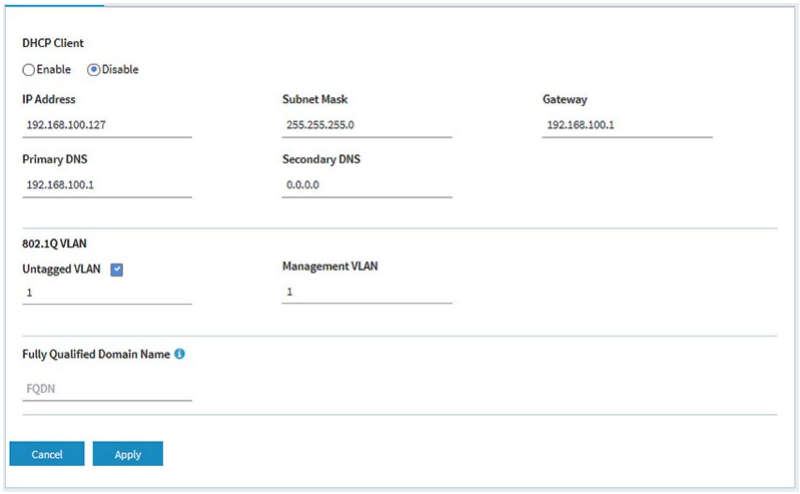
DHCPクライアントを有効にするには、次のようにします：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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**］ボタンをクリックします。
   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アドレスの設定を受信するまでには、しばらく時間がかかる場合があります。

802.1Q VLANと管理VLANを設定する

アクセスポイントの 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VLANとタグなしVLANで動作することができます：

- **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。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。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のみが受け入れられます。

管理 VLAN は、アクセスポイントとの間で送信される Telnet、SNMP、HTTP、HTTPS トラフィック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、トランクで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 のメンバーである場合、そのトラフィックはタグなしと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（159ページ）」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を設定する（215ページ）」を参照）。

802.1Q VLANと管理VLANを設定する：

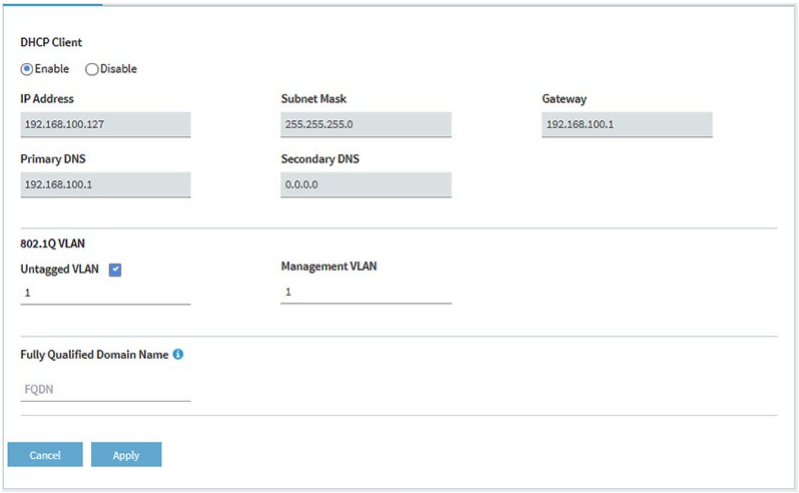
1. アクセスポイントと同じネットワークに接続されているパソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。
   ログインウィンドウが表示されます。

   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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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、その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を入力することができます。
   - **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クリアします。アクセスポイントは、その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のみ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、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**］ボタンをクリックします。

   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）を指定することで、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るようにすることができます。

FQDNは、DNS（Domain Name System）プロバイダーに登録されているドメイン名である必要があります。

FQDNに必要な条件は以下の通りです：

- 長さは1文字から64文字までです。
- 英数字は使用可能です（a-z、1-9）。
- ドット（...）とハイフン（-）は使用できますが、どちらかで始まる名前は

使用できません。例として、*myap01-firstfloor-myorganization.comがあります*。

既存のFQDNを設定する場合：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」を参照してください。

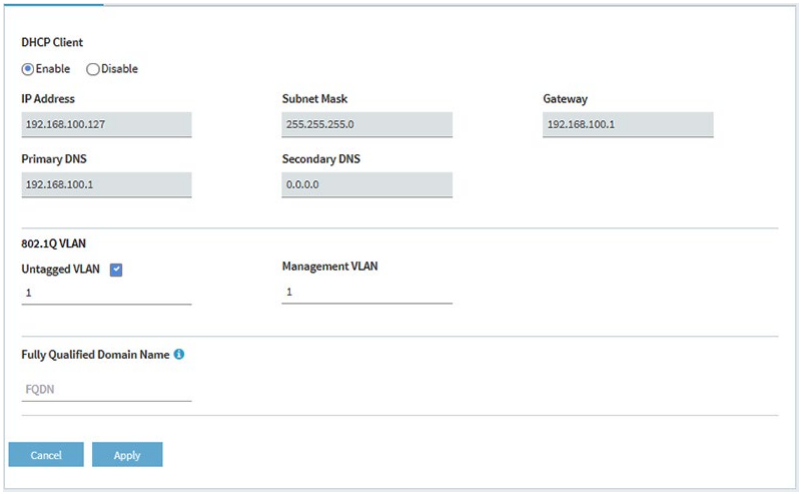
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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**」フィールドで、FQDNを指定します。
6. **Apply**］ボタンをクリックします。
   設定が保存されます。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、冗長な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）により、ネットワークのループを防ぐことができます。冗長な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の有効／無効を設定します：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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 が有効になっています。
   - **Disable**：STP が無効になります。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。

ネットワーク整合性チェック機能の有効化・無効化

ネットワーク整合性チェック機能により、アクセスポイントがWiFiアソシエーションを許可する前に、上流リンクがアクティブであるかどうかを検証することができます。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ます。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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、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、35 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です。
   - **Disable**：ネットワーク整合性チェック機能を無効にします。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。

IGMP スヌーピングの有効化または無効化

IGMP snooping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のみに送信することを可能にします。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、アクセスポイントでは IGMP スヌーピングは無効になっています。

IGMP snooping 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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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のラジオボタンを選択します：
   - **Enable**：IGMP snooping が有効です。
   - **Disable**：IGMP snooping を無効にします。この設定はデフォルトです。
6. **Apply**］ボタンをクリックします。設定が保存されます。

Ethernet LLDPの有効／無効を設定します。

IEEE 802.1AB で規定されている Link Layer Discovery Protocol (LLDP) 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することができます。たとえば、 LLDP を使用すると、 スイッチや管理装置などのネットワーク機器に、 ネットワーク内のアクセスポイントを発見させることができます。

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することができます。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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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：
   - **Enable**：LLDP が有効になっています。この設定はデフォルトです。
   - **Disable**：LLDP は無効です。

   注意：アクセスポイントがPoEスイッチから電力を受けていて、LLDPを無効にした場合、**適用**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てください。
6. **Apply**］**ボタンを**クリックします。設定が保存されます。

UPnPの有効化または無効化

ユニバーサルプラグアンドプレイ（UPnP）により、UPnPをサポートするネットワーク内の他のデバイスからアクセスポイントを検出することができます。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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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が有効になります。この設定はデフォルトです。
- **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。

マルチキャストDNSゲートウェイを管理する

アクセスポイントは、マルチキャストDNS（mDNS）ゲートウェイとして機能し、異なるVLANやWiFiネットワーク間でデバイスやサービスを共有することができます。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ても機能します。共有デバイスは、プリンター、スキャナー、ストレージデバイスなどのハードウェアデバイスです。サービスには、あらかじめ設定された複数の電話、音楽、映像の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ます。例えば、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VLAN20のWiFiネットワークに接続された電話を使用して、VLAN30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、有線またはWiFiデバイスのいずれかで実行できますが、WiFiクライアントがサービスにアクセスできるようにするには、WiFiクライアントがmDNSゲートウェイ機能を有効にしたアクセスポイント上のWiFiネットワークに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し、ネットワーク全体で共有する機器やサービスを再表示することができます。

mDNSゲートウェイと以下の機能は、相互に排他的です：

- ダイナミック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なWiFiネットワークのセットアップ（72ページ）」をご参照ください。
- マルチPSK（「WiFiネットワークにマルチPSKを設定する（90ページ）」をご参照ください。
- 管理 VLAN（「802.1Q VLAN と管理 VLAN を設定する（151 ページ）」を参照してください。
- 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を設定する（215ページ）」を参照）。
- 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（216ページ）参照

マルチキャストDNSゲートウェイを有効化し、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、共有できるデバイスとサービスを自動的に検出できるようになります。ポリシーは、次の2つのVLANの間にブリッジを形成します：

- **Service VLAN**：共有機器やサービスをメンバーとして含むVLAN。例えば、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は*Googlecast*で、*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上の共有機器やサービスを利用できる必要があるWiFi機器をメンバーとして含むVLANです。

ポリシーは最大8つまで追加することができます。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可能にします。WiFiクライアントが接続されているアクセスポイントに、共有デバイスやサービス用のポリシーが設定されている場合、その共有デバイスやサービスにアクセスすることができます。

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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. 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. ポリシーの追加＋］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. 以下のように指定して、mDNSゲートウェイポリシーを定義します：
   - **Policy Name**：ポリシーを識別するための名前です。ダブルクォート("")とバックスラッシュ("¬)を除く英数字と特殊文字を最大32文字まで使用することができます。
   - **Shared Services**：Shared Services］メニューから、共有する必要のあるデバイス（プリンターなど）またはサービス（Googlecastなど）の種類を選択します。
   - **Service VLAN**：「**Service VLAN**」フィールドに、「**Shared Services**」メニューで選択した共有機器やサービスの種類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機器やサービスの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必要がある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、前のステップを繰り返してください。
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のポリシーを変更または削除する

マルチキャストDNS（mDNS）ポリシーを変更または削除することができます。

mDNS ポリシーを変更または削除するには、次のようにします：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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場合：
   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. 設定を変更します。
      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（160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、次のようにします：
   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。

11

アクセスポイントの管理・メンテナンス

この章では、アクセスポイントを管理・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-browserに変更する。
- 使用する国や地域を変更する
- adminユーザーアカウントのパスワードを変更する
- システム名を変更する
- カスタムNTPサーバーを指定する
- タイムゾーンを設定する
- シスログの設定を管理する
- 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
- ローカルブラウザーの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設定に戻す
- SNMPを有効化し、SNMPの設定を管理する
- LEDを管理する
- エネルギー効率モードの管理

注：本書において、*WiFi*ネットワークとは、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ネットワークという場合は、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-browserに変更する。

アクセスポイントは、次のいずれかの管理モードで機能することができます：

- **NETGEAR Insightモード**：NETGEAR Insight PremiumとInsight Proの契約者は、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で管理できます。
  NETGEAR Insight モードが初期設定です。このモードでは、ローカル ブラウザ UI を介してアクセス ポイントに接続できますが、基本的かつ限定的なローカル ブラウザ UI しか使用できません。NETGEAR Insight Cloud Portal および Insight アプリについては、insight.netgear.com を参照し、netgear.com/support/product/insight.aspx で 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（xxxxx 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**。

- **ウェブブラウザモード**：WiFiまたは有線デバイスから、ローカルブラウザーUIを使用して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ネットワークの場所に追加し、Insight Cloud Portal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ブラウザモードに変更した場合、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UIにアクセスするにはInsightネットワークパスワードを使用し続ける必要があります。

管理モードをNETGEAR InsightモードまたはWeb-browserモードに変更する：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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］ページが表示されます。

5. 次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ブラウザー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（xxxxx 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. **Apply**］ボタンをクリックします。

   警告のポップアップウィンドウが表示されます。

7. **OK**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。

使用する国や地域を変更する

アクセスポイントが動作する国や地域を変更することができます。次のことに注意してください：

- 国がデバイスが動作している場所に設定されていることを確認してください。チャンネル、電力レベル、周波数範囲に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や地域以外では、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の場合、どのチャンネルを使用できるかについては、お住まいの地域の行政機関に確認するか、NETGEARのホームページで確認してください。
- 国によっては、アクセスポイントの国や地域があらかじめ設定された状態で販売されており、変更することができません。

操作する国や地域を変更する場合：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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］ページには、システムの基本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**］ボタンをクリックします。

   警告のポップアップウィンドウが表示されます。

7. **OK**ボタンをクリックします。
   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スタートします。

admin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、アクセスポイントのローカルブラウザUIにユーザー名adminでログインするためのパスワードです（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文字を含む必要があります。以下の特殊文字が使用可能です：

!@ # $ % ^ & * ( )

ユーザー名adminのパスワードを変更する場合：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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。表示されたページで、ユーザーアカウントを変更することができます。
5. adminの横にある「**Password**」フィールドに、新しいパスワードを入力します。
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。

注意：ユーザー名を変更することはできません。名前はadminのままでなければなりません。

7. **Apply**］ボタンをクリックします。
   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戻す必要があります。そうすることで、パスワードはデフォルトの パスワードに復元されます。

システム名を変更する

システム名（アクセスポイント名、または AP 名とも呼ばれる）は、アクセスポイントに固有の 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。デフォルトでは、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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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］ページには、システムの基本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します。

以下のガイドラインを参考にしてください：

- 名前は英数字を含む必要があり、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ません。
- 名前の先頭や末尾にハイフンを使用することはできません。
- 名前には、少なくとも1つのアルファベット文字が含まれていなければなりません。

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サーバーを指定する

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可能です。

カスタムNTPサーバーを指定する場合：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」を参照してください。

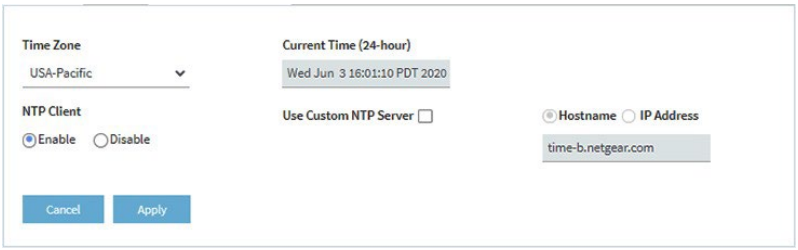
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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行います：
   - 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**の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**］ボタンをクリックします。
   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、 設定した内容にしたがって調整されます。

   タイムゾーンの設定については、「タイムゾーンを設定する」（P.170）を参照してください。

タイムゾーンを設定する

アクセスポイントがNTP（Network Time Protocol）サーバーと時計を同期させると、ページには日付と時刻が表示されます。ページに正しい日付と時刻が表示されない場合は、タイムゾーンの設定やサマータイム設定の調整が必要な場合があります。

タイムゾーンの設定やサマータイム設定の調整をする場合：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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。

   表示されたページで、時刻の設定を変更することができます。

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**］ボタンをクリックします。

   設定した内容が保存されます。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、設定した内容に応じて調整されます。

   その他の時間設定については、「カスタムNTPサーバーを指定する（169ページ）」を参照してください。

シスログの設定を管理する

ネットワーク上にsyslogサーバーがある場合、アクセスポイントのシステムログをsyslogサーバーに送信するように設定することができます。

syslog の設定を管理し、syslog 機能を有効にするには：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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. シスログサーバーのIPアドレスとポート番号を指定します：
   - **Syslog Server IP Address**：ネットワーク上のシスログサーバーの IP アドレスを入力します。
   - **Port Number**：シスログにアクセスできるポート番号を入力します。デフォルトでは、ポート番号は514です。
6. シスログ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、フラッシュメモリに格納されています。

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アップデートすることができます。また、NETGEAR のサポート Web サイトにアクセスして、ファームウェアを手動でローカル コンピュータにダウンロードし、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安全なFTP（SFTP）サーバーに置いた場合、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。

アクセスポイントとの接続方法に応じて、以下のファームウェア更新方法を推奨します：

- **WiFiで接続**：アクセスポイントにWiFiで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て、新しいファームウェアが利用可能かどうかを確認させてください。173ページの「アクセスポイントに新しいファームウェアの有無を確認させ、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入手できた場合、アクセスポイントに直接ダウンロードされます。

- **LANで接続**：アクセスポイントに LAN で接続している場合は、コンピュータまたは SFTP サーバーからファームウェアを手動で更新します。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（174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（177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入手できた場合、それをコンピューター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。

以下では、ファームウェアの管理方法について説明します：

- アクセスポイントに新しいファームウェアの有無を確認させ、ファームウェアを更新する
- 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アップデートする。
- 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の有無を確認させ、ファームウェアを更新する

アクセスポイントに新しいファームウェアを確認させるには、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確認させ、アクセスポイントを更新させるため：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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**」リンクをクリックします。
   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、表示される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出し、ダウンロードし、アップデートを開始します。
   警告：ファームウェアの破損のリスクを避けるため、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作業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。
7. アクセスポイントにログインし直すことで、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、Dashboard 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み、アップデート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。

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アップデートする。

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、次の手順で統合されます。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（「バックアップファームウェアに戻す（176ページ）」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、ファームウェアをアップデートするのではなく、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。ここで 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。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場合：

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てください。
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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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。Localはデフォルトで選択されています。
8. 次のようにして、パソコンでファームウェアファイルを探し、選択します：
   a. **Browse**」ボタンをクリックします。
   b. ファームウェアのファイルに移動します。
      ファイル名の末尾は「.tar」です。
   c. ファームウェアファイルを選択する。
9. **Upgrade**］ボタンをクリックします。

警告：ファームウェアの破損のリスクを避けるため、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作業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すことで、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、「Dashboard」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、元に戻せるようになっています。

注意：バックアップファームウェアに戻すとき、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のバージョンよりも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（xxxxxはアクセスポイントのMACアドレスの下6桁の16進数を表す）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。

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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のバージョンとバックアップファームウェアの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。
   警告の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（xxxxx 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**］ボタンをクリックします。
   ポップアップウィンドウが閉じると、ファームウェアの復帰処理が開始され、アクセスポイントが再起動します。
   警告：ファームウェアを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が緑色または青色で点灯した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すことで、アクセスポイントがバックアップファームウェアの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、「Dashboard」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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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。

   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します：

   - **Firmware File**：SFTPサーバーにあるアクセスポイントのファームウェアファイル名です。
   - **SFTP Server IP**：ネットワーク上のSFTPサーバーのIPアドレスです。
   - **User Name**：SFTPサーバーにアクセスするために必要なユーザー名です。
   - **Password**：SFTPサーバーにアクセスするために必要なパスワードです。

7. **Upgrade**］ボタンをクリックします。

   警告：ファームウェアの破損のリスクを避けるため、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作業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すことで、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、Dashboard 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 の構成ファイルに保存されます。このファイルは、パソコンにバックアップ（保存）したり、復元したり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

現在のコンフィギュレーション設定のコピーを保存することができます。必要に応じて、後でコンフィギュレーション設定を復元することができます。

注：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設定内容をバックアップする場合：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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とき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することができます。

   パスワードは8～63文字で、少なくとも大文字、小文字、数字を1つずつ含む必要があります。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、パスワードを保存することをお勧めします。

7. パソコンにファイルを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には
   `WAX6XX-NETGEARYYYYYY-dd-mm-yy_hh-mm-ss-config.tar` または
   `WAX6XX-WAX6XX-YYYYY-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は秒を示しています。

   バックアップファイルの名前の例としては
   `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することができます。

バックアップしたコンフィギュレーション設定を復元する場合：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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**］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には
   `WAX6XX-NETGEARYYYYYY-dd-mm-yy_hh-mm-ss-config.tar` または
   `WAX6XX-WAX6XX-YYYYY-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は秒を示しています。

   バックアップファイルの名前の例としては
   `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。

7. 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。

8. **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、アクセスポイントは再起動されます。この処理には約2分かかります。

   警告：ファームウェアが破損するリスクを避けるため、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が緑色または青色で点灯するまで待ちます。

ローカルブラウザーの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）、ローカルブラウザのUIを使用してアクセスポイントを再起動することができます。

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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。
   警告のポップアップウィンドウが表示されます。
6. **Reboot**］ボタンをクリックします。
   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、約1分ほどで終了します。

アクセスポイントの再起動をスケジュールする

アクセスポイントに接続するWiFiクライアントがいない（または数人しかいない）と予想されるときなど、ネットワークにとって都合のよい時間にアクセスポイントを再起動するようにスケジュール設定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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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、ボタンが青く表示されるようにします。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させる日のチェックボックスを選択します。複数の日を選択することができます。
7. **Start Time**］メニューを使用して、アクセスポイントが再起動しなければならない時間の時および分を指定します。
   時間を24時間表示で指定します。
8. **Apply**］**ボタンを**クリックします。設定が保存されます。

アクセスポイントを工場出荷時の設定に戻す

アクセスポイントの設定を変更した内容がわからなくなった場合や、アクセスポイントを別のネットワークに移動した場合など）状況によっては、設定を消去して、アクセスポイントを工場出荷時の設定に戻すことがあります。

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戻す前に、まずIPスキャナアプリケーションを使用してIPアドレスを検出することを試してください。

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。詳しくは、35 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。

アクセスポイントを工場出荷時の設定に戻すには、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のUIのリセット機能のいずれかを使用することができます。ただし、IPアドレスが見つからない場合や、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戻した後、管理者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、設定SSIDはNETGEARxxxxxx-SETUPの形式で表示、WiFiアクセス のデフォルトパスワードは**sharedsecretです**。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。

工場出荷時の設定の一覧は、「工場出荷時の設定（269ページ）」を参照してください。

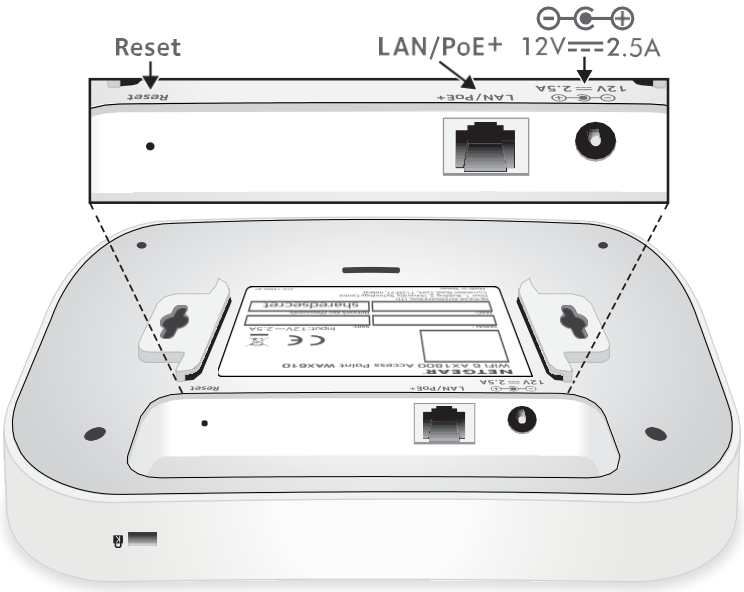
屋内型WAX610のリセットは、リセットボタンで行います

リセットボタンを使用すると、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、**リセットボタンの工場出荷時**デフォルト設定機能を利用する前に、まず Insight Cloud Portal 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：この処理を行うと、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戻すには、次のようにします：

1. アクセス ポイントの底部パネルに、凹型の**リセット** ボタンがあることを確認します。



2. まっすぐに伸ばしたペーパークリップで、**リセット**ボタンを10秒以上押し続ける。

   注：リセットボタンを10秒未満押したまま離すと、アクセスポイントは工場出荷時の設定に戻るのではなく、再起動されます。

3. **Reset**ボタンを離す。

   構成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されます。この処理は約 2 分間かかります。

   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終了し、Power/Cloud LED が緑色または青色で点灯するまで待ちます。

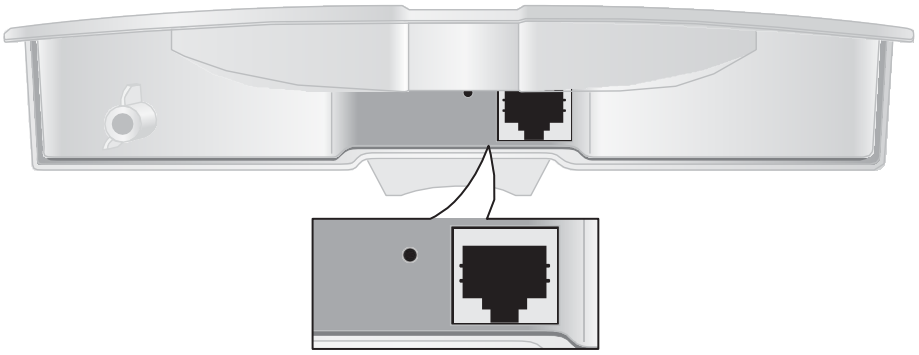
屋外用WAX610Yをリセットする場合は、リセットボタンを使用します。

リセットボタンを使用すると、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、**リセットボタンの工場出荷時**デフォルト設定機能を利用する前に、まず Insight Cloud Portal 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：この処理を行うと、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戻すには、次のようにします：

1. アクセスポイントの底面パネルで、LAN/PoE+ ポートの隣にある凹型の**リセット**ボタンを探します。



2. まっすぐに伸ばしたペーパークリップで、**リセット**ボタンを10秒以上押し続ける。

   注：リセットボタンを10秒未満押したまま離すと、アクセスポイントは工場出荷時の設定に戻るのではなく、再起動されます。

3. **Reset**ボタンを離す。

   構成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されます。この処理は約 2 分間かかります。

   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終了し、Power/Cloud LED が緑色または青色で点灯するまで待ちます。

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ーのUIを使用して、アクセスポイントを工場出荷時の設定に戻すことができます。

注意：この処理を行うと、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からアクセスポイントを工場出荷時の設定に戻すには：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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」ページが表示されます。
5. **Restore Defaults**］ボタンをクリックします。

   警告の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されます。この処理には、約2分かかります。

   警告：ファームウェアの破損のリスクを避けるため、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終了し、電源/クラウド LED が緑色または青色で点灯するまで待ちます。

SNMPを有効化し、SNMPの設定を管理する

SNMP（Simple Network Management Protocol）接続でアクセスポイントにアクセスすると、HP OpenView などの SNMP ネットワーク管理ソフトウェアが、SNMPv1 または SNMPv2 プロトコルを使用してアクセスポイントを管理できます。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の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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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。

   Remote Management］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. 以下の設定を指定します：

- **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を指定します。デフォルトは public です。
- **Read-Write Community Name**：SNMPマネージャ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ためのコミュニティ文字列です。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たコミュニティ名です。デフォルトはtrapです。
- **IP address (to receive traps)**：トラップを受信する必要がある SNMP マネージャーの IP アドレスを指定します。
- **Trap Port**：SNMPマネージャがトラップを受信する必要のあるポート番号です。デフォルトは162です。

7. **Apply**］ボタンをクリックします。設定が保存されます。

LEDを管理する

デフォルトでは、すべてのLEDが有効になり、「LED付きトップパネル、屋内モデルWAX610」（14ページ）、「LED付きサイドパネル、屋外モデルWAX610Y」（22ページ）の説明に従って機能します。LEDが全く点灯しないかどうかを管理することができます。この機能は、暗い環境でもアクセスポイントを機能させたい場合に便利です。

LEDの有効／無効を切り替えるには

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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. 次のラジオボタンのいずれかを選択またはクリアします：
   - **Enable All LEDs**：すべてのLEDが有効になります。初期設定では、この設定になっています。
   - **Disable All LEDs**：すべてのLEDを無効化します。
   - **Enable Power/Cloud LED**：Power/Cloud LEDを除くすべてのLEDが無効となります。
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、消費電力を減らしてエネルギーを節約することができます。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、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した場合、アンテナストリームは通常の動作を再開します。

以下の制約に注意してください：

- **Wireless distribution system**：EEMは、無線配信システム（WDS、229ページのWiFiブリッジのセットアップを参照）と相互排他的です。
- **Neighbor AP detection**：EEM は、5 GHz 無線で近隣 AP を検出させません（「近隣 AP 検出の管理（137 ページ）」を参照）。
- **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際、アクセスポイントがDFSチャンネルで動作している場合、5GHz無線通信が一時的に停止することがあります（DFSチャンネルの場合は約1分停止、天候DFSチャネルの場合は約10分停止）。

注：EEMを使用する場合、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推奨します。バンドステアリングを使用することで、5GHz対応のWiFiクライアントを 2.4 GHz バンドを 5 GHz バンドにステアリングし、パフォーマンスを向上させます。詳しくは、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または無効にする（95 ページ）を参照してください。

エネルギー効率化モードを有効または無効にするには、次のようにします：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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。

   Energy Efficiency Mode］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です。
   - **Disable**：エネルギー効率化モードは無効です。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。

12

アクセスポイントとネットワークを監視する

この章では、アクセスポイントおよびネットワークを監視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：

- アクセスポイントのインターネット、IP、システム設定を表示する
- WiFi設定を表示する
- 未知・既知の近隣アクセスポイントを表示
- 顧客分布、接続顧客、顧客動向を表示する。
- WiFiとEthernet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します。
- トラッキングされたURLの表示・ダウンロード
- ログの閲覧、保存、ダウンロード、クリアー
- WiFiブリッジ接続を表示する
- アラームや通知の表示

注：本書において、***WiFi***ネットワークとは、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ネットワークという場合は、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、システム設定を表示する

アクセスポイント、インターネット、IP、システムの設定を表示する：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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。

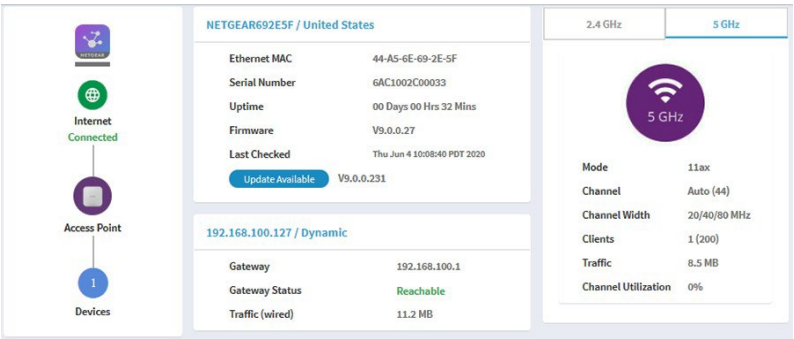
   ユーザー名は**admin**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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. ダッシュボード図の左側、中央上、中央下にそれぞれ表示されている「接続状態情報」ペイン、「システム情報」ペイン、「IP設定情報」ペインの位置を確認します。

   お使いの端末のページ幅が狭い場合、これらのペインがダッシュボードの他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の無線設定を表示する」（P.197）を参照してください。



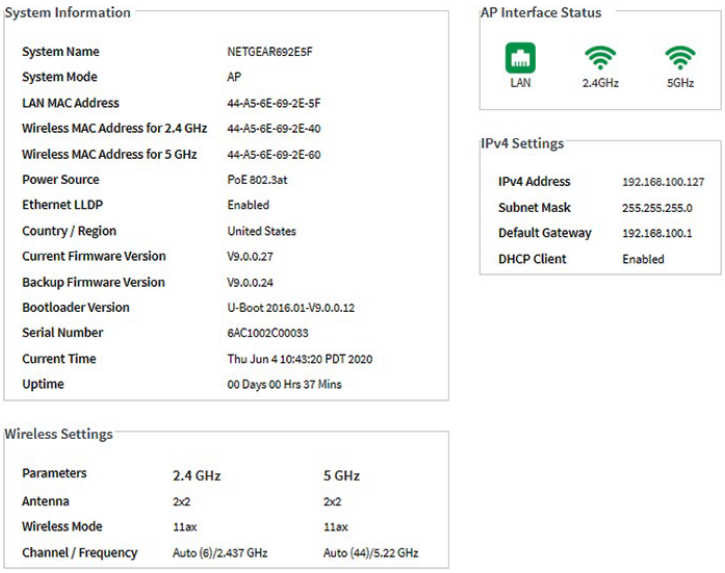
- **Connection Status Information pane**：このペインは、ダッシュボードの上部、左隅にあり（お使いのデバイスのページ幅が十分な場合、それ以外の場合は他の場所にある可能性があります）、次のように表示されます：
  - NETGEAR Insight クラウドベース管理プラットフォームへの接続状況がある場合、その状況。
  - インターネット接続の状態です。
  - アクセス ポイントの機能モード。常にアクセス ポイントになります。
  - アクセスポイントに接続されているクライアントの数。

- **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）、次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。
  - シリアルナンバー。
  - デバイスの稼働時間。
  - ファームウェアのバージョン。
  - アクセスポイント自身または誰かが手動で最後に新しいファームウェアが利用可能かどうかを確認した日付と時刻。

  このペインには、アクセスポイントのファームウェアの更新を確認するためにクリックできるボタンもあります。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、「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させる（173ページ）」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、そうでない場合は他の場所にある可能性があります）、次のように表示されます：
  - アクセスポイントのIPアドレスとDHCPの状態。
  - ゲートウェイIPアドレス。
  - ゲートウェイの状態。
  - 有線の通信量。

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ます：

- **System Information section**：以下の設定項目が表示されます：
  - **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）。
  - **LAN MAC Address**：アクセスポイントのLAN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**：アクセスポイントの5GHz WiFiインターフェースのMACアドレス。
  - **Power Source**：電源の種類（PoE 802.3atまたは電源アダプタ）。
  - **Ethernet LLDP**：Ethernet LLDP の状態（Enabled または Disabled）。

  - **Country / Region**：アクセスポイントが動作する国または地域、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未使用であることを示します。

- **IPv4 Settings section**：以下の設定項目が表示されます：
  - **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（EnabledまたはDisabled）。

- **Wireless Settings section**： 2.4GHzと5GHzの設定が表示されます：
  - **Antenna**: アンテナの種類（デフォルトでは2x2）。
  - **Wireless Mode**：無線の動作WiFiモード。
  - **Channel / Frequency**：無線機が使用しているチャンネルと周波数。

WiFi設定を表示する

アクセスポイントのWiFi設定を表示する：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」を参照してください。

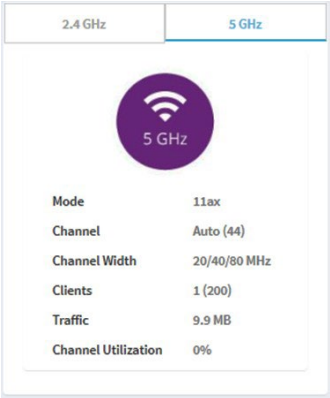
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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」ページの右上隅にある 無線情報ペインを見つけます (デバイスのページ幅が十分ではない場合は他の場所にある可能性があります)。

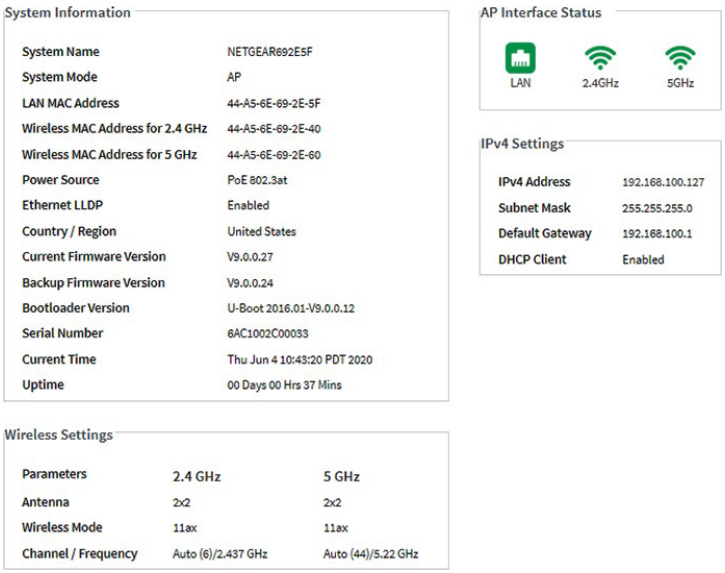


   以下の設定項目が表示されます：

   - 無線の状態(2.4GHzまたは5GHzのアイコンがグレーで表示されている場合は、無線がオフになっている)
   - **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
   - **Antenna**：アンテナの種類

5. もう一方の無線の情報を表示するには、**2.4GHz**または**5GHz**のいずれかのタブをクリックします。ペインが調整されます。

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ます：

- **System Information section**：以下の設定項目が表示されます：
  - **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）。
  - **LAN MAC Address**：アクセスポイントのLAN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**：アクセスポイントの5GHz WiFiインターフェースのMACアドレス。
  - **Power Source**：電源の種類（PoE 802.3atまたは電源アダプタ）。
  - **Ethernet LLDP**：Ethernet LLDP の状態（Enabled または Disabled）。
  - **Country / Region**：アクセスポイントが動作する国または地域、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未使用であることを示します。
- **IPv4 Settings section**：以下の設定項目が表示されます：
  - **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（EnabledまたはDisabled）。
- **Wireless Settings section**： 2.4GHzと5GHzの設定が表示されます：
  - **Antenna**: アンテナの種類（デフォルトでは2x2）。
  - **Wireless Mode**：無線の動作WiFiモード。
  - **Channel / Frequency**：無線機が使用しているチャンネルと周波数。

未知・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（「近隣のAP検出の管理」（137ページ）を参照）、不明なアクセスポイントを「不明AP」リストに、既知のアクセスポイントを「既知AP」リストに表示することができます。

検出された近隣のアクセスポイントを表示するには、次のようにします：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。

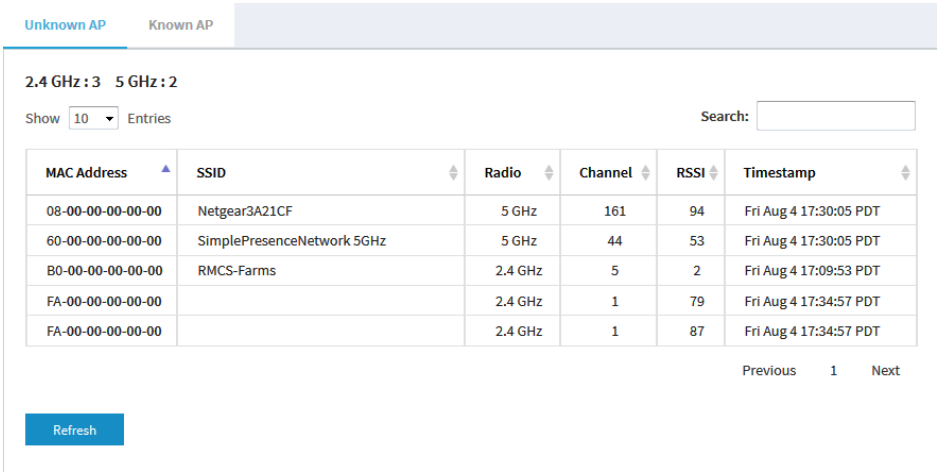
   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳しくは、「ブラウザのセキュリティ警告が表示された場合の対処法（55ページ）」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

ユーザー名は**admin**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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。

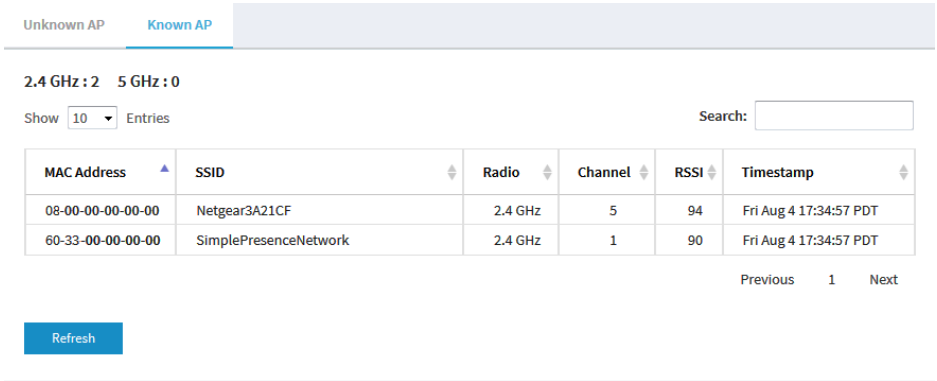
4. **Management > Monitoring > Neighbor AP**を選択します。



ページの上部には、各無線バンドごとに、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検出を有効にして、アクセスポイントをKnown APリストに移動する」（138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. Known 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、各無線バンドごとに、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。

接続端末の分布、接続、傾向を表示する。

WiFi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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。

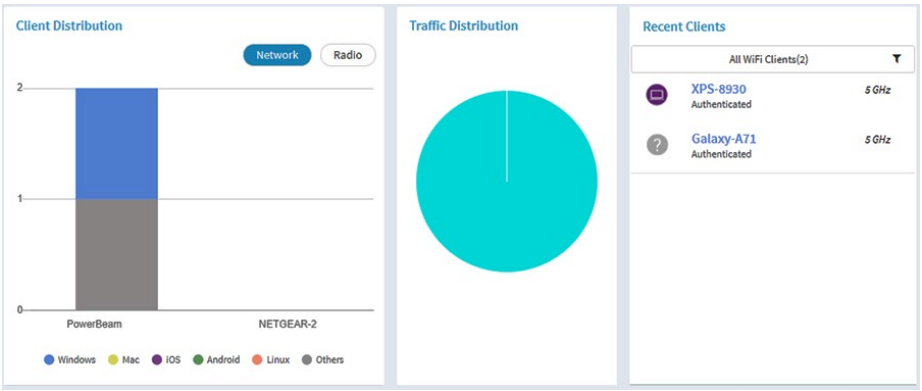
   ログインウィンドウが表示されます。

   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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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. **Client Distribution**ペイン（下図の左側）と**Recent Clients**ペイン（下図の右側）を見つけます。



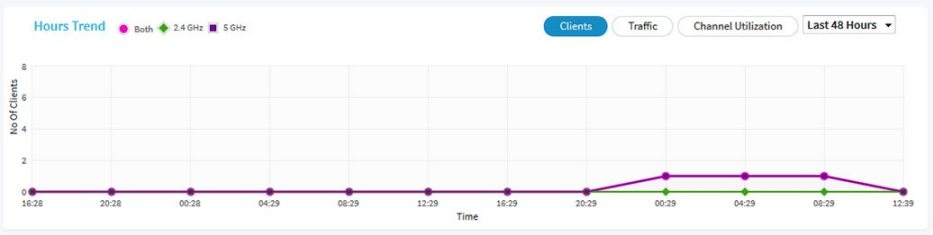
Client Distribution］ペインには、クライアントの種類（Windows、Mac、iOS、Android、Linux、その他のオペレーティングシステム）と、これらのクライアントがネットワーク上にどのように分布しているかが表示されます。(デフォルトでは、「**Network**」ボタンが選択されています)。Recent Clients」ペインには、最近接続したクライアントの上位 5 端末のリストが表示されます。

5. 無線へのクライアントの分散方法を表示するには、［Client Distribution］ペインで［**Radio**］ボタンをクリックします。
   各無線のクライアントの種類を調整し、表示するページです。

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 Clie］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。
   選択すると、ペインに接続されているクライアントの総数および接続されているクライアントの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、そのデバイス名をクリックします。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、およびSSIDが表示されます。また、非常に詳細な情報など、より多くの情報を表示することもできます（ステップ11、ステップ12参照）。

8. クライアントに関するトレンドを表示するには、「Hours Trend」ペインまでスクロールしてください。



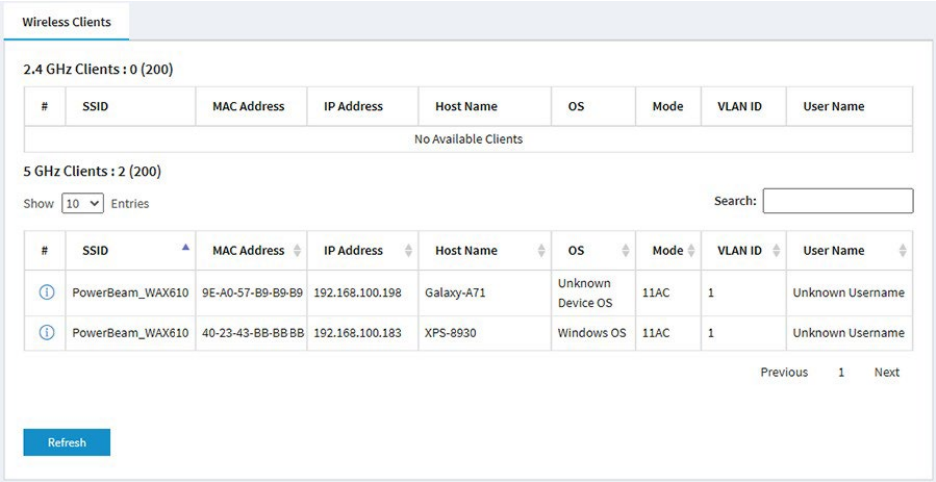
Hours Trend］ペインには、選択した期間のクライアント数、トラフィック（MBps）、チャンネル使用率のグラフが表示されます（前図は過去 48 時間のトレンド）。(デフォルトでは、クライアント情報が選択されており（つまり、クライアントボタンが選択されている）、グラフには両無線のクライアント数の合計と各無線（2.4GHz、5GHz）のクライアント数が表示されます。）

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、およびチャネル使用率の表示（205 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してください。

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. 現在接続しているクライアントの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、接続クライアント数およびサポートす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、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、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クライアントの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、次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。

- **State**：接続の QoS 状態。
- **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. クライアント情報の詳細」ページを開いた場合は、「**Close**」ボタンをクリックします。クライアント情報の詳細」ページが閉じます。

14. 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Ethernet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します。

WiFiとEthernet（有線LAN）のトラフィック、トラフィックとARPの統計、チャンネル使用率を表示する：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。

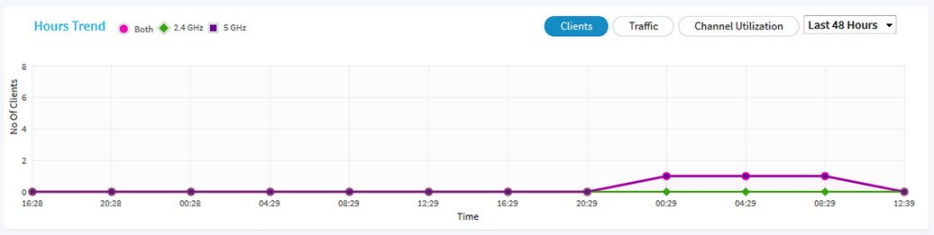
   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳しくは、「ブラウザのセキュリティ警告が表示された場合の対処法（55ページ）」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。
   ユーザー名は**admin**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、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、35 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. 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、次のようにします：

   a. **Traffic**］ボタンをクリックします。
   グラフには、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無線用WiFiトラフィック、5GHz無線用WiFiトラフィックの情報が表示されます。

   b. 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してください。

6. チャンネル使用率を表示するには、次のようにします：

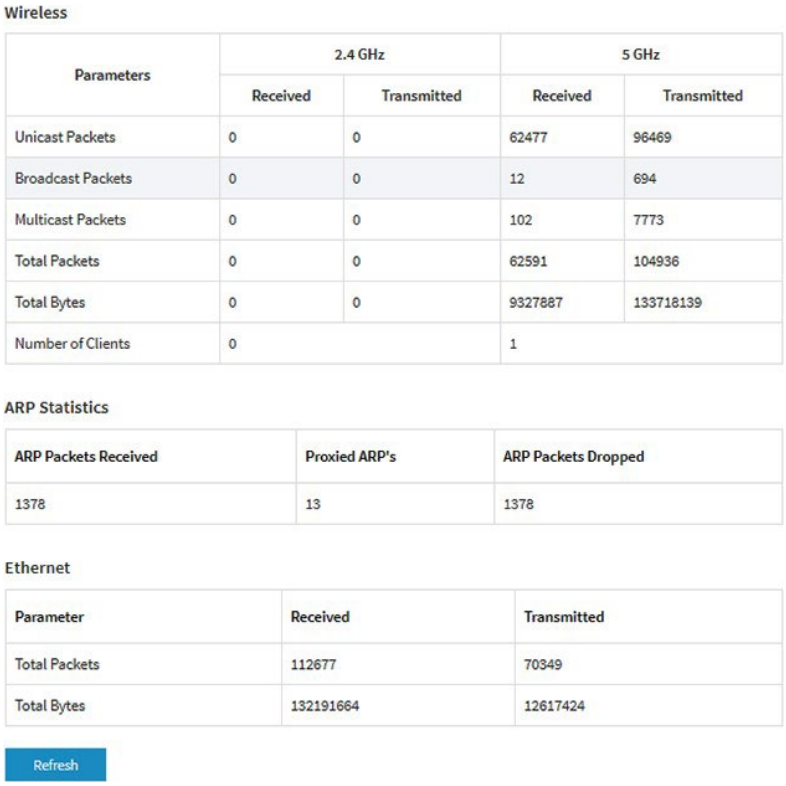
   a. **Channel Utilization**］ボタンをクリックします。
   グラフは、2.4GHz帯の無線のチャンネル使用率を示しています。

   b. 5GHz 無線のチャンネル使用率を表示するには、「**5GHz**」ボタンをクリックします。

   c. より詳しい情報を見るには、バーをポイントしてください。

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	
	Received	Transmitted	Received	Transmitted
Unicast Packets	0	0	62477	96469
Broadcast Packets	0	0	12	694
Multicast Packets	0	0	102	7773
Total Packets	0	0	62591	104936
Total Bytes	0	0	9327887	133718139
Number of Clients	0		1	

ARP Statistics

ARP Packets Received	Proxied ARP's	ARP Packets Dropped
1378	13	1378

Ethernet

Parameter	Received	Transmitted
Total Packets	112677	70349
Total Bytes	132191664	12617424

Refresh

このページでは、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およびイーサネットインターフェースの両方のネットワークトラフィックの統計情報を表示します。このページでは、各無線に関連付けられたクライアントの数も表示されます。ARPプロキシが有効な場合（「ARPプロキシの管理（246ページ）」を参照）、このページには、プロキシされたパケットとドロップされたパケットの数を含むARP統計情報も 表示されます。

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・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 追跡の有効化または無効化（218 ページ）参照）、URL、WiFi クライアント、SSID 別に追跡された URL を表示することができます。また、URL 追跡レポートを .csv ファイルとしてダウンロードすることもできます。

トラッキングされたURLを表示またはダウンロードする場合：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」を参照してください。

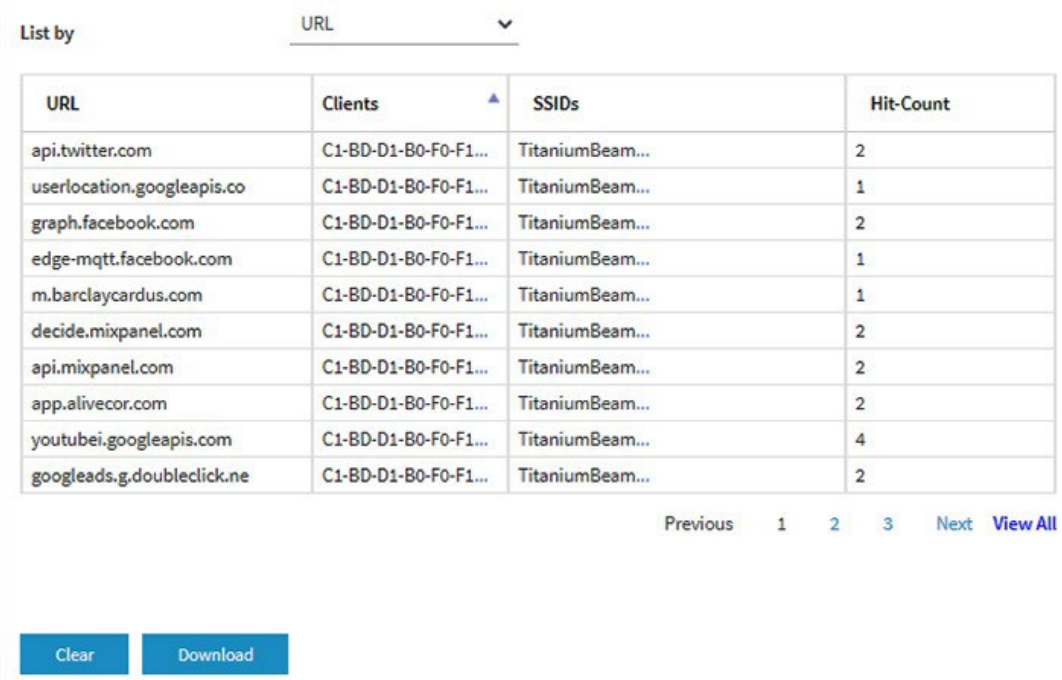
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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。

   Dashboard」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、アクセスされたURLと、その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、そのURLにアクセスしたWiFiクライアントの回数がそれぞれ表に表示されます。

5. 追加情報を表示するには、MACアドレスまたはSSIDの右側にある「**...**」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、次のようにします：
   a. **List by**」メニューから、「**Client**」を選択します。
      表には、WiFiクライアントのMACアドレスと、それぞれのクライアントホスト名、クライアントがアクセスしたURLのリストの最初の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の右側にある「**...**」リンクをクリックします。
      WiFiクライアントがアクセスしたすべてのURLをポップアップウィンドウで表示します。
   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ます。

7. SSIDごとのURL追跡情報を表示するには、次のようにします：
   a. **List by**」メニューから、「**SSID**」を選択します。
      表には、SSIDと、そのSSIDでアクセスされたURLの一覧の最初のURLが表示されます。
   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の右側にある「**...**」リンクをクリックします。
      SSIDにアクセスされたすべてのURLをポップアップで表示します。
   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ます。

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、**ダウンロード**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. URLのトラッキング情報をすべて消去するには、次のようにします：
   a. **Clear**］ボタンをクリックします。
      警告のポップアップウィンドウが表示されます。
   b. **OK**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、情報がクリアされます。

ログの閲覧、保存、ダウンロード、クリアー

アクセスポイントの活動ログを閲覧・管理することができます。また、詳細なログファイルをダウンロードすることができます。

注：アクセス ポイントが NETGEAR Insight 管理モードで機能する場合、アクセス ポイントの Insight クラウドベース管理プラットフォームへの接続を示すクラウド活動ログを表示および管理することもできます。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。

ログの閲覧、保存、ダウンロード、クリアを行う：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。

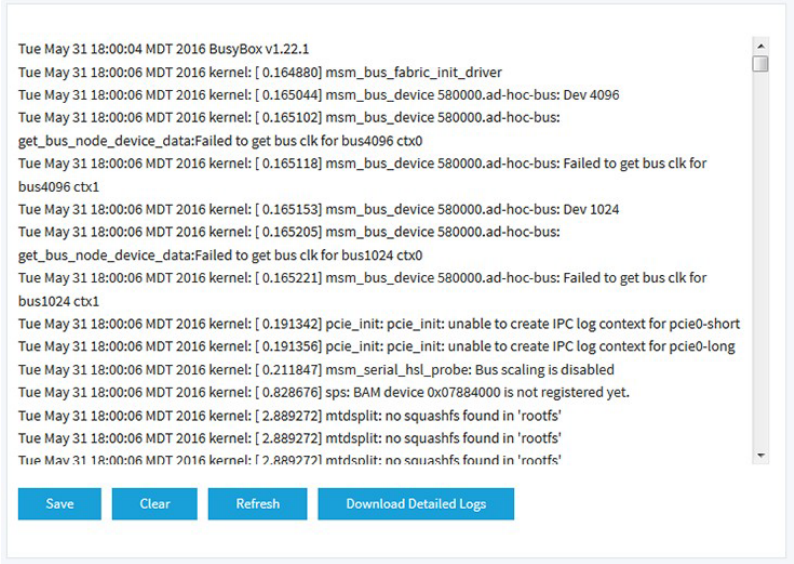
   ログインウィンドウが表示されます。

   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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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. ログを保存する場合は、次のようにします：
   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、次のようにします：
   a. **Download Detailed Logs**］ボタンをクリックします。
      ファイルサイズによっては、詳細なログエントリーのダウンロードに数分かかる場合があります。
   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。

7. 画面上のログエントリーを更新するには、［**Refresh**］ボタンをクリックします。
   警告：ログエントリーをクリアした後、保存やダウンロードはできなくなります。

8. ログを消去する場合は、［**Clear**］ボタンをクリックします。

WiFiブリッジ接続を表示する

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（229ページ）を参照）。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確認し、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、IPアドレスを確認することができます。

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」を参照してください。

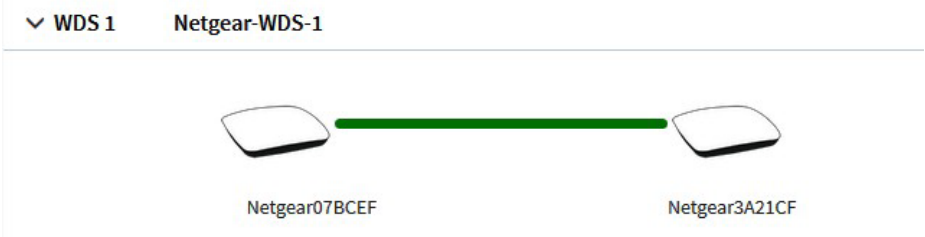
3. アクセスポイントのユーザー名とパスワードを入力します。
   ユーザー名は**admin**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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。

Dashboard page」ページが表示されます。

4. **Management > Monitoring > Wireless Bridge**を選択します。
   表示されるページでは、WDSプロファイル（WDS 1、WDS 2、WDS 3、WDS 4）を選択することができます。

5. WDSプロファイルの左側にある「**>**」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、アクセスポイントにカーソルを合わせます。

アラームや通知の表示

アラームや通知は、どのアクセスポイントのページからも見ることができます。次の手順では、Dashboard ページから表示する方法を説明します。

アラームや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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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。

Dashboard」ページが表示されます。

4. ページの右上にある警鐘のアイコンを探してください。
   アイコンに数字が表示され、前回アラームや通知を表示したときからの新着アラームや通知の総数が表示されます。

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）および通知（青いベルで表示）が説明と時間とともに表示されます。

6. より多くのアラームや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てください。

13

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（71ページ）」をご覧ください。

この章には、以下の項目があります：

- 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を設定します。
- WiFiネットワークのクライアント分離の有効化・無効化
- WiFiネットワークのURLトラッキングの有効化・無効化
- 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
- WiFi ネットワークの MAC ACL を選択します。
- 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設定が有効になる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：本書において、***WiFi***ネットワークとは、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ネットワークという場合は、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を設定します。

デフォルトでは、アクセスポイントのアドレス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アドレスを受信することを意味します。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。

また、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化する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、アクセスポイント本体のIPアドレスとは異なる範囲のIPアドレスを割り当てる。

NATモードと以下の機能は、相互に排他的です：

- マルチPSK「WiFiネットワークにマルチPSKを設定する（90ページ）」を参照
- 管理 VLAN「802.1Q VLAN と管理 VLAN を設定する（151 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（159ページ）」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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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を選択することができます。
5. SSIDの左側にある「**>**」ボタンをクリックします。

選択したSSIDの設定内容が表示されます。

6. 下にスクロールして、「**＞Advanced**」タブをクリックします。ページが展開されます。
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にある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、アクセスポイント上のプライベート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、デフォルトでは、WLAN ネットワークアドレスは 172.31.0.0 です。これは、WiFi クライアントに 172.31.0.2 から 172.31.3.254 までの範囲の 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アドレスプールのデフォルト範囲、デフォルトDNSサーバー、またはその両方を変更するには、次のようにします：
     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。例えば、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アドレス範囲）である場合、192.168.0.0と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、前のステップで設定したWLANネットワークアドレスと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の有効化・無効化

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た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、クライアント分離を有効にすると、同じまたは異なるWiFiネットワークに関連付けられたクライアント同士が通信 できなくなりますが、インターネット経由の通信は可能です。

クライアントアイソレーションは、Multi 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 Multi PSK を無効にします（WiFi ネットワークの Multi PSK の設定（90 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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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を選択することができます。
5. SSIDの左側にある「**＞」ボタンを**クリックします。
   選択したSSIDの設定項目が表示されます。
6. 下にスクロールして、「**＞Advanced**」タブをクリックします。
   ページが展開されます。
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**：WiFiネットワークでクライアント分離が無効になります。これはデフォルトの設定です。
   - **Enable**：WiFiネットワークでクライアント分離が有効になっています。以下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（次の手順参照）。
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）、WiFiネットワーク経由のアクセスを無効にしても、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。

9. **Allow access to devices listed below**」チェックボックスが表示された場合：隔離の対象外となるネットワークデバイスを追加して、クライアントからのアクセスを許可するようにするには、次のようにします：
   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クリアされています。
   Allowlist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たデバイスの静的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ーの静的IPアドレスまたはドメイン名を入力することができます。Allowlist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Allowlistに追加されます。
   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トラッキングの有効化・無効化

アクセスポイントが、WiFiネットワーク（SSIDまたはVAP）に接続されているWiFiクライアントから要求されるすべてのURLを追跡することを有効にできます。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ごと、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（207ページ）」をご覧ください。

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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を選択することができます。
5. SSIDの左側にある「**＞」ボタンを**クリックします。選択したSSIDの設定項目が表示されます。
6. 下にスクロールして、「**＞Advanced**」タブをクリックします。
   ページが展開されます。
7. URL トラッキング］で、次のラジオボタンのいずれかを選択します：
   - **Enable**：WiFiネットワークでURLトラッキングが有効になっています。
   - **Disable**：WiFiネットワークでURLトラッキングが無効になります。
8. **Apply**］**ボタンを**クリックします。設定が保存されます。

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

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アドレスを交渉するとき、アクセスポイントはDHCPサーバーから受信するブロードキャスト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メッセージの交換には、ユニキャストパケットの方が信頼性が高く、ネットワーク内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、そのWiFiネットワークのメッセージフォーマットを変更し、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*ようにすることができます。

WiFiネットワークでDHCPのオファーメッセージのフォーマットを変更する：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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を選択することができます。
5. SSIDの左側にある**「＞」ボタンを**クリックします。
   選択したSSIDの設定項目が表示されます。
6. 下にスクロールして、**「＞Advanced」**タブをクリックします。
   ページが展開されます。

7. DHCP Offer Broadcast to Unicast］で、次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、DHCPオファーメッセージをWiFiネットワーク内で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ネットワーク内の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 を選択します。

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 を通してアクセス ポイントへのアクセスを許可されるか、SSID へのアクセスが拒否されます。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のセキュリティを設定していない場合、別のSSIDを介してアクセスポイントに接続できる場合があります。

また、RADIUSサーバーを設定し（「RADIUSサーバーの設定（143ページ）」を参照）、RADIUS MAC ACLを選択することもできます。RADIUSサーバーでクライアント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 として指定します。

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 ネットワークに異なるタイプの 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を変更する（85 ページ）参照）。

WiFiネットワークに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へのアクセスが許可され、他のすべてのWiFiデバイスはSSIDへのアクセスが拒否されます。
- **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へのアクセスが許可されます。

WiFi ネットワークの MAC ACL を選択する場合：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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を選択することができます。
5. SSIDの左側にある「**＞」ボタンを**クリックします。
   選択したSSIDの設定項目が表示されます。
6. 下にスクロールして、「**＞Advanced**」タブをクリックします。
   ページが展開されます。
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ってください：
   - **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、グループの隣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MACアクセスコントロールリストの管理（130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サーバーを設定した場合のみ機能します（「RADIUSサーバーの設定（143ページ）」を参照）。
9. **Apply**］ボタンをクリックします。

設定した内容が保存されます。

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しているデバイスのアップロードとダウンロードの帯域幅のレート制限を設定できます。最小帯域幅のレートは64Kbps、最大帯域幅のレートは1024Mbpsです。アップロード帯域幅に1つのレートを設定し、ダウンロード帯域幅に別のレートを設定することができます。

注：帯域幅のレート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（254ページ）」を参照）。

WiFiネットワークに接続されているデバイスの帯域幅のレート制限を設定する場合：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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を選択することができます。

5. SSIDの左側にある**「＞」ボタンを**クリックします。
   選択したSSIDの設定項目が表示されます。

6. 下にスクロールして、**「＞Advanced」**タブをクリックします。
   ページが展開されます。

7. **Rate Limit**］チェックボックスを選択します。
8. 値を指定します：
   - **Upload**：アップロードの帯域制限について、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**：ダウンロードの帯域制限について、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）の容量を改善し、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）
- クライアントの数と近接性（クライアント密度）
- クライアントの種類（レガシーWiFiモードを含む、クライアントが対応可能な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数、およびクライアントを配置できる場所を決定することを推奨します。

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、通常のWiFiネットワーク内のWiFi接続にレートコントロール設定を適用しますが、ワイヤレスディストリビューションシステム（WDS）またはInsight Instant Mesh 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の無線帯域について、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つの要素からなる密度レベルを設定することができます。つまり、密度レベルには、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度）よりもはるかに多くのものが含まれます。
  WiFi ネットワークの密度レベルの利用可能な設定は、無線機が動作する WiFi モードに依存します。(WiFiモードの詳細については、「無線のWiFiモードを変更する(102ページ)」を参照してください)。
  密度レベルは、0（実際には0～4にまたがる、初期設定）、1（1～4にまたがる）、2（2～4にまたがる）、3（3～4にまたがる）、4で設定することができます。そして、その設定は、以下の*相互依存的な*構成要素に適用されます。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ません：
  - **Density**：WiFiネットワーク内のクライアントの密度（数と近さ）です。(密度は、密度*レベルの*4つの構成要素の1つです）0を設定すると、クライアント密度が非常に低くなることを意味します。4の設定は、クライアント密度が非常に高いことを意味します。
  - **Compatibility**：WiFiネットワーク内のレガシークライアントのWiFiモードとの互換性を示します。0を設定すると、802.11b/g/n/axクライアントと互換性があります。4は、802.11g/n/axクライアントとの互換性を意味し、802.11bレガシークライアントとは互換性がありません。
  - **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です。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、非常に広いカバーエリアを必要とする場合、意図的にパフォーマンスを下げることを選択することができます。
  - **Coverage**：WiFiネットワークがカバーしなければならないエリアです。0に設定すると、非常に広い範囲をカバーすることになります。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、意図的に非常に狭いエリアを選択することができます。

別の表現として、選択されたレベルは、対応するクライアントの密度レベル、WiFiモード、最小レガシーレート、ビーコンレート、最小MCS（Modulation Coding Scheme）レートにマッピングされています。

WiFiネットワークの高度なレート選択を設定するには、次のようにします：

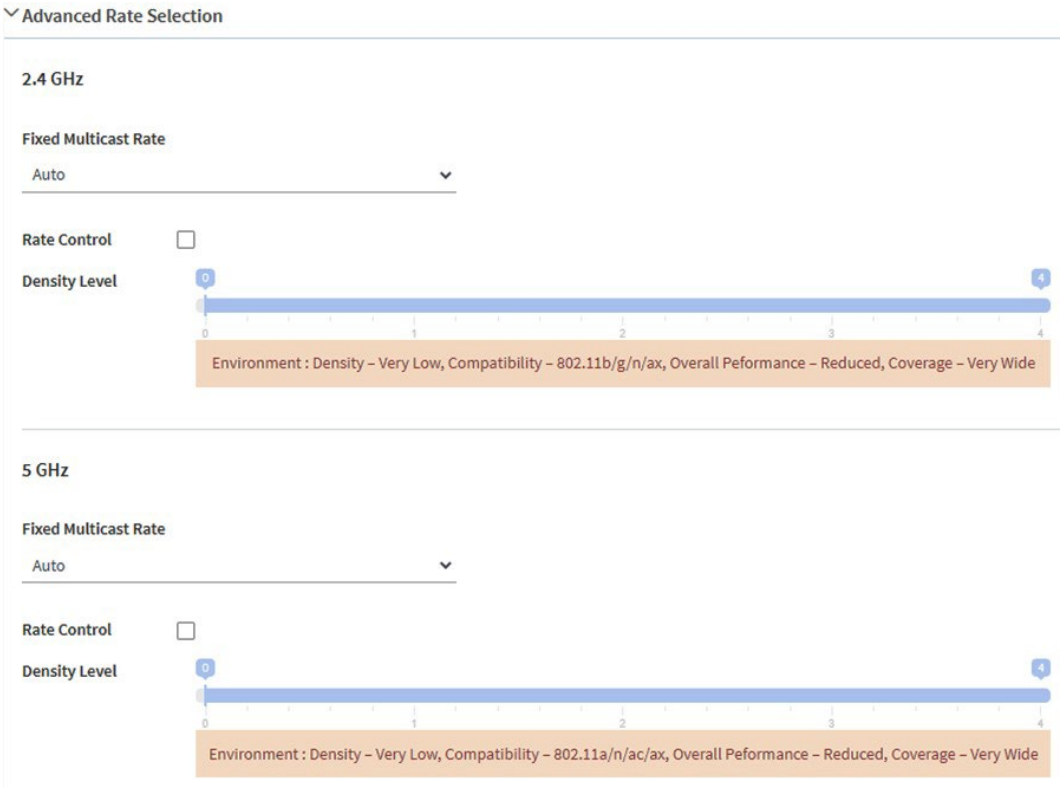
1. アクセスポイントと同じネットワークに接続されているパソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。
   ログインウィンドウが表示されます。

   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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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の選択と追加を行います。
5. SSIDの左側にある「**＞」ボタンを**クリックします。
   選択したSSIDの設定項目が表示されます。

6. 下にスクロールして、「**Advanced Rate Selection**」タブをクリックします。



注：選択したSSIDについて、2.4GHzと5GHzの無線帯域の無線設定を個別に指定することができます。以下のステップの説明は、両方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11Mbpsです）。
   - **5 GHz**：**6**、**12**、**24**MbpsまたはAuto。(デフォルトでは、Autoは24Mbps)

8. ビーコンとその他の管理フレーム、およびコントロール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、［**濃度レベル**］スライダーが使用可能になります。

9. 環境に応じた濃度レベルを設定するには、**Density Level**スライダーを**0**、**1**、**2**、**3**、**4のいずれかに動かします**。

   スライダーを動かすと、選択した密度レベルが、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（102 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ネットワークの密度レベルは、以下の相互依存的な構成要素に基づいており、スライダーの位置によって設定が割り当てられますが、*個別に設定することはできません*：

- **Density of 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、非常に低い、低い、中、高い、または非常に高いに設定することができます。
- **Compatibility with WiFi modes for legacy clients**：無線のデフォルトの11ax WiFiモードでは、以下のように設定することができます：
  - **2.4GHzです**：802.11bクライアントをサポートする802.11b/g/n/axと、サポートしない802.11g/n/axがあります。
  - **5GHzに対応**：802.11a/n/ac/ax、スライダーのどの位置でも5GHz帯のあらゆる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、または最適の設定が可能です。
- **WiFi coverage**：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、非常に狭い、狭い、平均的、広い、または非常に広いという設定が可能です。

注：ローカルブラウザUIのヘルプテキストには、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し、これらのコンポーネントがどのように互いに依存するかについての詳細情報が記載された表があります。

10. **Apply**］ボタンをクリックします。設定が保存されます。

14

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のポイントツーポイント WiFi ブリッジ接続で構成される無線配布システム（WDS）を設定する方法について説明します。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上で設定が一致しなければならない 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（57 ページ）」を参照）。

この章には、以下の項目があります：

注：Energy Efficiency Modeを有効にすると、WDSを使用することができません。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てください。詳細については、「エネルギー効率モードの管理（190ページ）」を参照してください。

注：本書において、***WiFi***ネットワークとは、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ネットワークという場合は、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リピーター、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ベースステーションとして機能し、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他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することができます。

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つまたは複数のアクセスポイントに送信する。有線およびWiFiクライアントもWiFiリピータに接続できますが、リピータはWiFiベースステーションを通じてインターネットに接続します。

下図は、WiFiリピートの設定で、左側にWiFiベースステーション、右側にWiFiリピータ1台という2つのアクセスポイントを示しています。

下図は屋内用WAX610を例にしています。

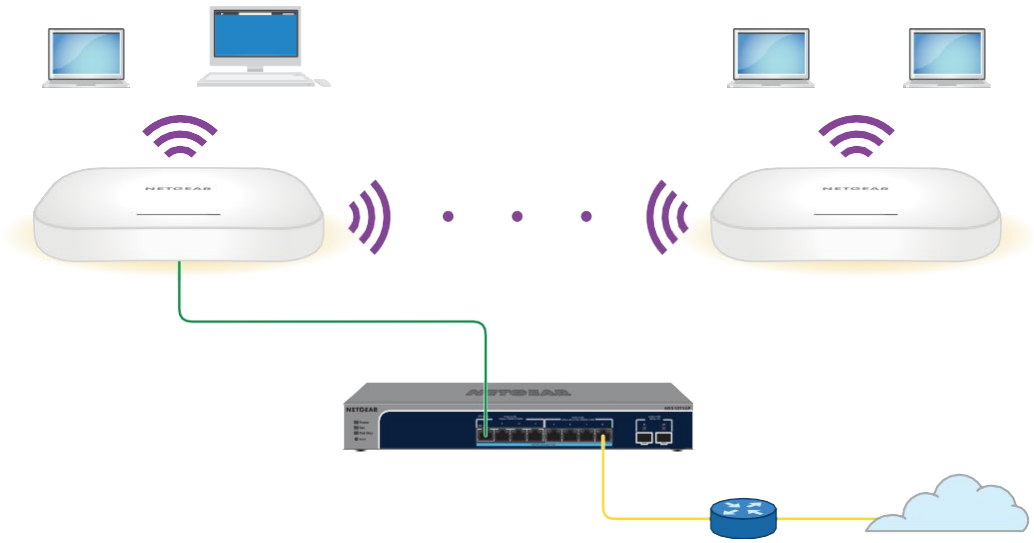


図 12.5GHz無線帯域の2つのアクセスポイント間のWiFiブリッジ構成

WiFiブリッジを使用するには、アクセスポイントのオートチャンネル機能を使用できず、SSIDブロードキャストが有効である必要があります。

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ベースステーション**：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 および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、リピーターの2.4GHzまたは5GHz無線のMACアドレスを知っている必要があります。

- **WiFiリピーター**：リピータは、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、ベースステーションからそのローカル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。

デフォルトでは、アクセスポイントはデュアルバンドコンカレントモードで機能します。いずれかの無線帯域でWiFiリピーターを有効にすると、もう一方の無線帯域ではWiFiベースステーションまたはWiFiリピーターを有効にすることができません。ただし、いずれかの無線帯域でWiFiベースステーションを有効にし、もう一方の無線帯域をクライアントアクセスまたはWiFiベースステーションとして使用する場合、デュアルバンドコンカレントモードには影響しません。

WDSでWiFiネットワークを構築する前に、構成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が同じ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は、同じLAN IPサブネット上にある必要があります。つまり、アクセスポイントのLAN IPアドレスがすべて同じネットワーク内にあることです。
- すべてのLAN機器（有線およびWiFiパソコン）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場合があります。

注意: 2 つのアクセスポイント間で WiFi ブリッジを設定する前に、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 (154 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有効にします。スイッチが STP をサポートしていない場合は、WiFi ブリッジの確立後、アクセスポイントの 1 つをそのスイッチから切断して、ネットワークのループと接続の問題を防ぎます。そのアクセスポイントにPoE+スイッチを使用していた場合は、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のWiFiブリッジを設定する

あるアクセスポイントでWiFiブリッジの設定を行い、別のアクセスポイントでも同様の設定を行うことで、WiFiブリッジを確立できるようにする手順を説明します。

2つのアクセスポイント間にWiFiブリッジを設定する場合：

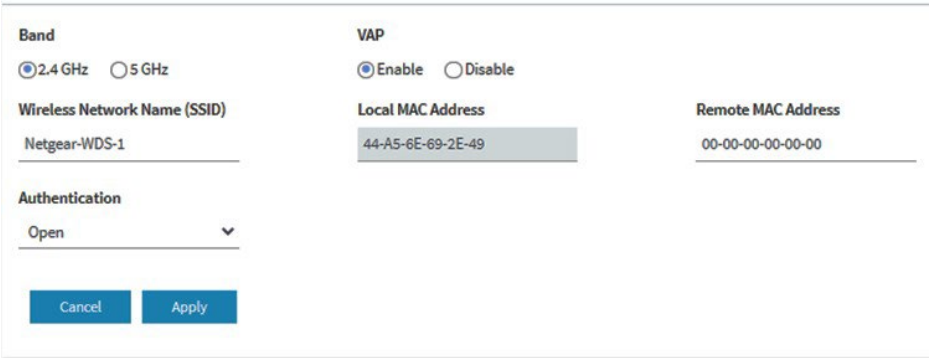
1. アクセスポイントと同じネットワークに接続されているパソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
2. アクセスポイントに割り当てられている IP アドレスを入力します。
   ログインウィンドウが表示されます。

   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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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。
   表示されるページでは、WDSプロファイル（WDS 1、WDS 2、WDS 3、WDS 4）を選択することができます。
5. WDSプロファイルの左側にある「**>**」ボタンをクリックします。
   WDSプロファイルのページが表示されます。
6. バンド**2.4GHz**または**5GHz**のラジオボタンを選択します。
   選択すると、WDSが確立される無線バンドが決まります。デュアルバンドに対応していない国の場合、電波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 プロファイルの設定を行います。

設定	概要
Wireless Network Name(SSID)	WDSが確立されているネットワークのWiFiネットワーク名です。デフォルトの名前はNetgear-WDS-xで、xはWDSの番号（1、2、3、または4）です。 **注**：WiFi ベースステーションと WiFi リピーターで WiFi ネットワーク名を同一にする必要があります。
Local MAC Address	ローカルWDS無線インターフェースの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MACアドレスは、このページでは変更できません。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、すなわちWDSが確立されているリモート無線の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： • **暗号化を行います**：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です。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ブリッジの設定を行い、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、再起動する必要がない場合があります。

WiFiブリッジが確立されます。

11. 両アクセスポイントのLAN間の接続を確認する。

    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ーは、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ーまたはサーバーとインターネットに接続したり、ファイルやプリンターを共有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ている無線のWiFiチャンネルを変更することはできません。

15

無線の高度な機能を管理する

この章では、アクセスポイントの高度な無線機能を管理する方法について説明します。基本的な無線機能については、「基本的な無線機能の管理」（97 ページ）を参照してください。

注意：2.4GHz無線の無線機能を変更すると、2.4GHz無線機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 無線の無線機能を変更した場合、その変更は 5 GHz 無線機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。

本章には、以下の項目があります：

- 無線の詳細なWiFi設定の管理
- 無線の最大クライアント数を管理する
- 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
- 無線のロードバランシングを管理する
- 粘着性のあるクライアントを管理する
- ARPプロキシを管理する
- ブロードキャストトラフィックの量を管理する

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る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：本書において、***WiFi***ネットワークとは、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ネットワークという場合は、個々のSSIDまたはVAPを意味します。

無線の詳細なWiFi設定の管理

無線の詳細な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。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 無線設定を変更することができます。2.4 GHz と 5 GHz の無線で個別に変更できます。

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。誤った設定を行うと、アクセスポイントに接続しようとする機器に接続上の問題が発生する場合があります。

設定を変更するには、無線がオンになっている必要があります。無線の電源の入れ方については、101ページ「無線のオン／オフを切り替える」をご覧ください。

無線のWiFiの詳細設定を管理する：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。

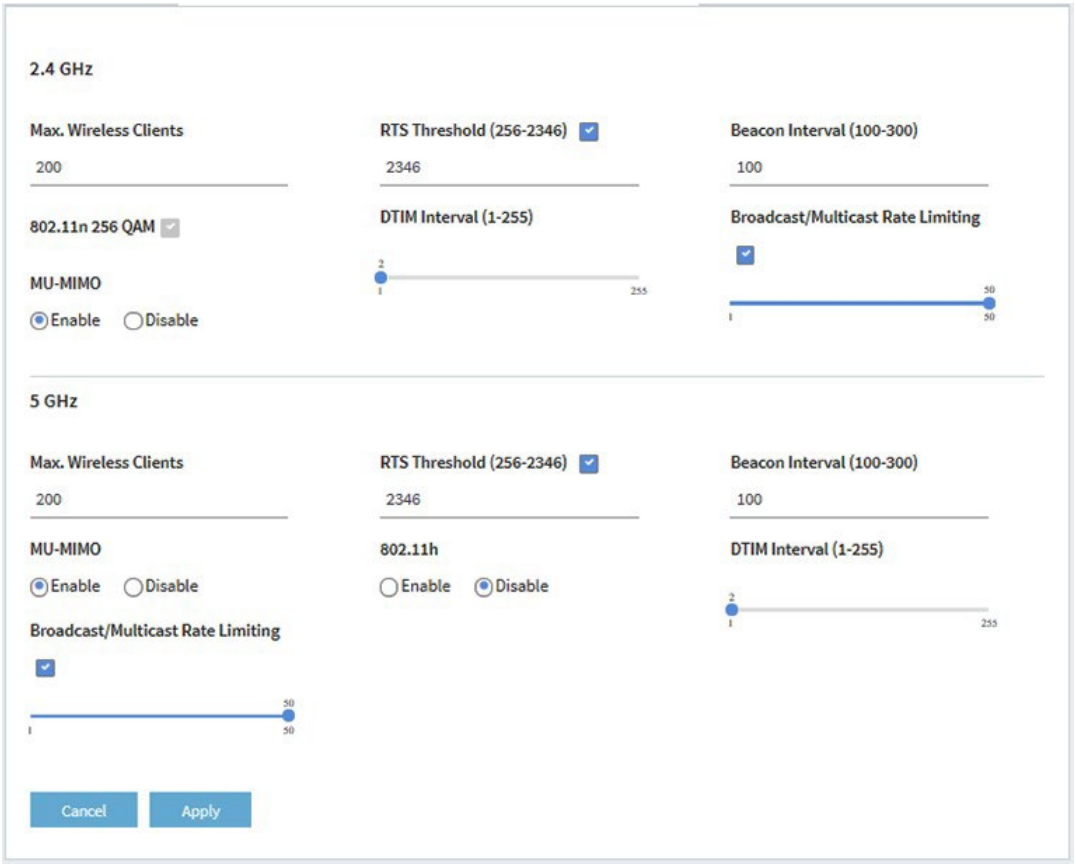
   ブラウザにセキュリティ警告が表示された場合は、先に進むか、セキュリティ警告の例外を追加してください。詳しくは、「ブラウザのセキュリティ警告が表示された場合の対処法（55ページ）」を参照してください。
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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. 下表のように設定します。

   表中の説明は、両方の無線に適用されます。2.4 GHz と 5 GHz の無線設定を個別に指定できますが、802.11n 256 QAM 機能のチェックボックスは 2.4 GHz 無線にのみ適用されます（この機能は 5 GHz 無線では常に有効です）。802.11h 機能は、5 GHz 無線にのみ適用されます。

設定	概要
Max. Wireless Clinents	無線機と同時に接続できるWiFiクライアントの最大数を入力します。 WiFiクライアントの数は1～200で、デフォルトは200です。
RTS Threshold（256-2346）	RTS（Request to Send）の閾値を入力します。256から2346の範囲で設定できます。デフォルトは2346です。 パケットサイズがRTS閾値と同じかそれ以下の場合、無線機はCSMA/CD（Carrier Sense Multiple Access with Collision Detection）メカニズムを使用し、データフレームは沈黙期間の後に直ちに送信されます。パケットサイズがRTS閾値より大きい場合は、CSMA with Collision Avoidance（CSMA/CA）機構を使用する。この場合、送信デバイスは受信デバイスにRTSパケットを送信し、受信デバイスがCTS（Clear to Send）パケットを返すのを待ってから実際のパケットデータを送信します。
Beacon Interval（100～300）	無線機がWiFiネットワークを同期させるためのビーコン送信の間隔を、100ms～300msの間で入力してください。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) で機能し、256 QAM をサポートできる 802.11n クライアントで 2.4 GHz 無線スループットを増加させることができます。デフォルトでは、256 QAM は 2.4 GHz 無線で無効になっています（つまり、チェックボックスはクリアされています）。 デフォルトでは、5GHz無線では256-QAMが有効になっており、無効にすることはできません（ページには5GHz無線用のチェックボックスは用意されていません）。
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、またはビーコンの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、1～255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	マルチキャストおよび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）であり、1秒間に50パケットの最大レート制限を指定する。設定を変更するには、スライダーを移動します。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	概要
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では、同じチャネルを使用して、複数のユーザーが同時にアクセスポイントからデータを受信することができます。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することができます。MU-MIMOはダウンストリーム方向で使用され、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に対応する必要があります。
802.11h	802.11h **Enable ラジオボタンを選択すると**、802.11h 対応の WiFi クライアントがアクセスポイントから切断することなく、またアクセスポイントが他のチャンネルに変更してもデータを失うことなく、自動的に新しいチャンネルに切り替えることができるようになります。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、5GHz 無線では有効または無効にできますが、2.4GHz 無線では無効です。

6. **Apply**］ボタンをクリックします。
   警告のポップアップウィンドウが表示されます。

7. **OK**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、設定が保存されます。無線機または無線機が再起動し、WiFiクライアントの再接続が必要になる場合があります。

無線の最大クライアント数を管理する

無線機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、数が多ければ信頼性とスループットが低下する可能性があります。

デフォルトでは、1つの無線機で最大200のクライアントと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ができます。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、その最大数を下回るまで無線機は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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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。
   Wireless Settings］ページが表示されます。
5. 無線の **Max.Wireless Clients** フィールドに、無線と同時に接続できる WiFi クライアントの最大数を入力します。
   WiFiクライアントは1～200の範囲で設定でき、デフォルトは200です。
6. **Apply**］ボタンをクリックします。
   警告のポップアップウィンドウが表示されます。
7. **OK**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、設定が保存されます。無線機または無線機が再起動し、WiFiクライアントの再接続が必要になる場合があります。

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

マルチキャストとブロードキャストのトラフィックは、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、マルチキャストおよびブロードキャストのレート制限が有効になっており、ネットワーク上で送信されるパケット数を制限することによって、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）であり、1秒間に50パケットの最大レート制限が指定されます。この数値は下げることができます。

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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、「無線のブロードキャスト/マルチキャストレートリミッティング」で、次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、スライダーを移動します。デフォルトでは、設定は50（可能な最大値）であり、最大レート制限を50パケット/秒に指定します。
   - 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**］ボタンをクリックします。

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

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

無線のロードバランシングを管理する

クライアントがWiFiネットワークに接続したり解除したりする際に、各無線機が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、無線の利用率の閾値を設定することができます。

ロードバランシングを有効にすると、クライアントの関連付けは、無線機ごとの最大クライアント数、無線機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ている場合、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では、無線機ごとのクライアントとトラフィックの分布、および無線機ごとのクライアント、トラフィック、チャネル利用率の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傾向の表示（202ページ）とWiFiおよびイーサネットトラフィック、トラフィックとARP統計、チャネル利用の表示（205ページ）を参照）。

デフォルトでは、以下のすべての種類のロードバランシングが、デフォルトの設定で有効になっています：

- **最大クライアント数に応じたロードバランシングを行う**：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。これはグローバルな設定ですが、無線ごとに実装されます。
- **チャネル負荷に基づくロードバランシングを行う**：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。最大チャネル利用率を超えると、新しいクライアントは拒否されます。これはグローバルな設定ですが、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にアクセスを許可します。

- **クライアントの**RSSI**に基づくロードバランシングを行う**：RSSIが定義された最小値と同じかそれ以上のクライアントは、アクセスポイントとの関連付けを許可されます。定義された最小値を下回るRSSIを持つクライアントは拒否されます。これはグローバルな設定ですが、無線機ごとに実装されています。

  注：クライアントが拒否されても、しつこくアクセスポイントとの関連付けを試みる場合、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ため：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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**Enable**にします。
   ページでは、ロードバランシングの種類やラジオごとに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ます。ロードバランシングを有効にすると、3種類のロードバランシングがすべて有効になります。個別に1つまたは複数のロードバランシングを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、次のようにします：

   - 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*」テキストの左側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*」テキストの左側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の設定を変更する場合は、次のようにします：

   - **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。
     各無線とも、クライアント数の最小値は5、最大値は200で、デフォルトの数は200です。
   - **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アソシエーションを受け付けなくなるまでの、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割合は50、最大割合は90、デフォルトの割合は70である。
   - **Based on Channel Receive Signal Strength**：各無線について、関連するスライダーを動かして、個々のクライアントに必要な最小限のRSSI値を指定し、それ以下では無線がクライアントの関連付けを受け付けないようにします。
     各無線のRSSI値の最小値は1、最大値は50、デフォルト値は23です。

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を管理する

ローミング中、粘着性のあるクライアントは、より信号の良い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も、最初のアクセスポイントに関連したまま（つまり、*粘着している*）。このような場合、そのアクセスポイントに接続している他のクライアントに遅延が発生します。

注：アクセスポイントが1つの家庭用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に接続できないため、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や企業のネットワークでは、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。

スティッキークライアントをアクセスポイントの無線機から強制的に切り離すことができます。クライアントのRSSIに基づく負荷分散が有効な場合（「無線の負荷分散の管理（242ページ）」を参照）、クライアントが強制的に切断された後、以下の状況でクライアントは再び参加できるようになります：

- クライアントのRSSIが最低限必要なRSSI以上であれば、再度アソシエイトすることができます。
- クライアントがアクセスポイントとのアソシエーションを持続的に試みる場合、そのクライアントのRSSIが最低必要RSSIを下回っていても、アクセスポイントはそのクライアントへのアクセスを許可します。

スティッキークライアントを管理するため：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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選択または解除します。

   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無線から強制的に切り離されます。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との関連付けを維持することができます。
6. **Apply**］ボタンをクリックします。

設定した内容が保存されます。

ARPプロキシを管理する

デフォルトでは、アクセスポイントではARPプロキシが有効になっており、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することができます。このように、アクセスポイントはクライアントに対する ARP 要求に応答することで、無線の不要なブロードキャストトラフィックを防止しています。

プロキシされたパケットとドロップされたパケットの数を含む ARP 統計については、WiFi とイーサネットのトラフィック、トラフィックと ARP 統計、およびチャネル利用率の表示（205 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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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. 次のラジオボタンのいずれかを選択します。
   - **Enable**：ARP プロキシが有効です。この設定はデフォルトです。
   - **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の量を管理する

アクセスポイントは、無線のブロードキャストトラフィックを低減するブロードキャストエンハンスメントに対応しているため、アクセスポイントに設定したすべてのWiFiネットワークでブロードキャストトラフィックを低減できます。ブロードキャスト機能拡張は、アクセスポイントが 5 GHz 無線で 20 人未満、2.4 GHz 無線で 10 人未満のクライアントをホストすることを想定している場合にのみ、有効にすることをお勧めします。デフォルトでは、ブロードキャスト拡張機能は無効になっています。

ブロードキャスト強化のための以下の制限に注意してください：

- WiFiネットワークに20台以上のクライアントが接続されている場合、そのWiFiネットワークではブロードキャストエンハンスメントが機能しません。
- 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・エンハンスメントを管理するため：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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。

   Dashboard」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. 次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・エンハンスメントが有効になっています。
   - **Disable**：ブロードキャストエンハンスメントが無効になります。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。

16

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、アクセスポイントや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、以下の項目があります：

注：本書において、***WiFi***ネットワークとは、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ネットワークという場合は、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機器やネットワークの場所のIPアドレスにpingを送信し、pingテストの結果を表示することができます。

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。

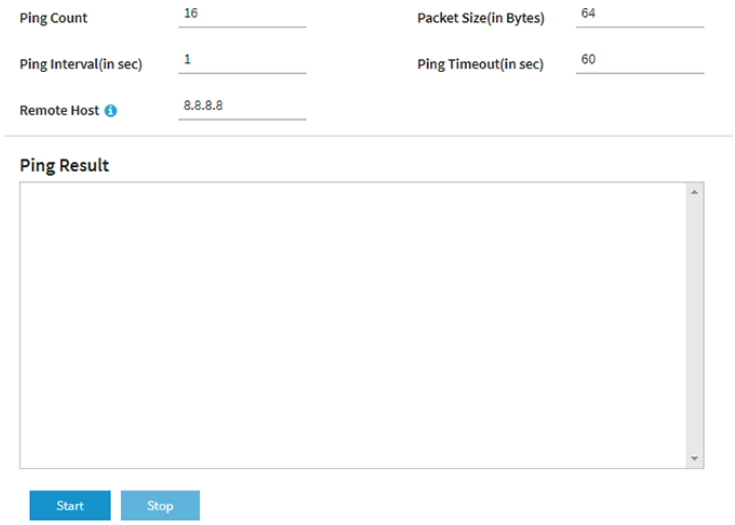
   ログインウィンドウが表示されます。

   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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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. 次の表に記載されている設定を指定します。

設定	概要
Ping Gount	アクセスポイントが送信しなければならないPingの数。デフォルトの数は 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までの時間。デフォルトは60秒です。
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テストの結果は、「Ping Result」フィールドに表示されます。
7. pingカウントに達する前、またはpingがタイムアウトした場合にpingテストを停止するには、「**Stop**」ボタンをクリックします。

WiFiやEthernetのパケットをキャプチャ

アクセスポイントが受信・送信するWiFiやEthernet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処理中、アクセスポイントの正常な機能に影響はありません。

パケットキャプチャ機能は、WiFi展開の分析、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ネットワークにおけるあらゆる不規則性のトラブルシューティングに有用であります。

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することができます。

注：キャプチャされたパケットを表示するには、.pcap ファイルを開くことができるアプリケーションが必要です。

パケットをキャプチャするには

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」を参照してください。

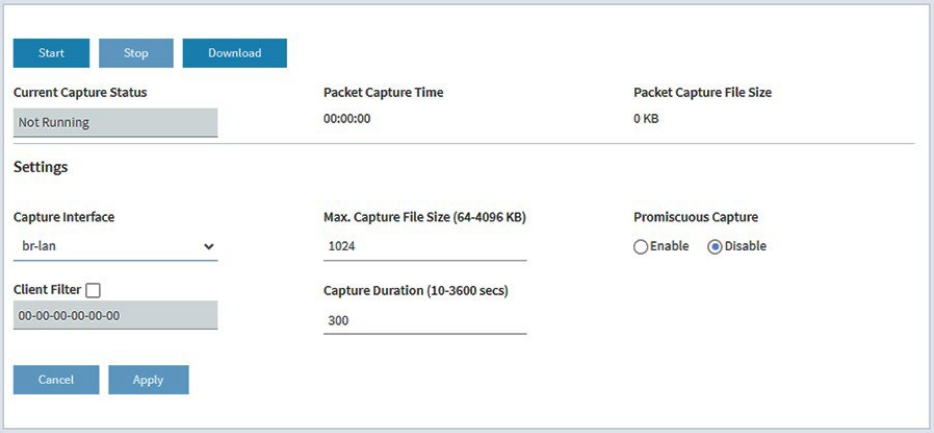
3. アクセスポイントのユーザー名とパスワードを入力します。

   ユーザー名は**admin**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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. 次の表に記載されている設定を指定します。

設定	概要
Capture Interface	**Capture Interface**メニューから、パケットをキャプチャする必要のある以下のインターフェースのいずれかを選択します： • **br-lan**：すべてのパケット、つまり、Ethernetインターフェース、2.4GHz無線機、5GHz無線のパケットをキャプチャします。これはデフォルトの設定です。 • **Eth0**：イーサネットインターフェイス上のパケットのみキャプチャされます。 • **radio1**：2.4GHzの無線のパケットのみキャプチャされます。 • **radio2**：5GHz無線のパケットのみキャプチャされます。
Max. Capture File Size（64～4096KB）	キャプチャしたパケットを含むファイルが制限される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1024KBです。

(続き)

設定	概要
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、次のように選択します。 **Enable**」チェックボックスをオンにします。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ます。 プロミスキャスモードでは、無線はアクセスポイント向け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します。無線がプロミスキャスモードで動作している間、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、無線は非プロミスキャスモードに復帰します。
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、クライアントのMACアドレスを入力すると、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することができます。 MACアドレスは、00-11-22-33-44-55のように、各オクテットをハイフンで区切った16進数で入力する必要があります。
Capture Duration （10～3600秒）	キャプチャープロセスの最大継続時間を入力します（つまり、クリックしない場合は**Stop**ボタン）。 10秒から3600秒までの範囲で設定できます。デフォルトでは、最大300秒です。

6. パケットキャプチャーの処理を開始するには、［Start］ボタンをクリックします。
   キャプチャし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、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処理を停止する場合は、［Stop］ボタンをクリックします。
   手動で処理を停止しない場合、キャプチャーの継続時間を超えると自動的に処理が停止されます。
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、次のようにします：
   a. **Download**」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。
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確認する

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ができます。結果は、帯域幅のレート制限を設定する場合に役立つ場合があります（「WiFiネットワークの帯域幅レート制限を設定する（223ページ）」を参照）。

インターネットの速度を確認するため：

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パソコン、またはイーサネットケーブルやWiFi接続でアクセスポイントに直接接続しているパソコンから、Webブラウザーを起動します。
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。詳しくは、「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（55ページ）」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**です。パスワードは、指定されたものです。ユーザー名とパスワードは、大文字と小文字が区別されます。

   以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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**」のリンクをクリックします。プライバシーポリシー」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「**X**」をクリックします。
7. **Test Speed**］ボタンをクリックします。
   しばらくすると、測定された遅延時間（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. テスト履歴を見るには、「**View History**」リンクをクリックします。
   以前のテスト結果が表で表示されます。

WiFiのトラブルシューティングのためのクイックヒント

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再起動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までのイーサネットケーブルを抜きます。
2. 電源アダプターを使用している場合は、アクセスポイントから取り外してください。
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分ほど待ちます。
4. 電源アダプターを使用する場合は、アクセスポイントに接続します。2分ほど待ちます。WiFiクライアント機器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 が消灯していて、LED を無効にしていない場合（LED の管理（189 ページ）を参照）、関連する WiFi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、101 ページの「無線機をオンまたはオフにする」を参照してください。
- WiFiクライアント機器とアクセスポイントのWiFi設定が完全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クライアント機器のWiFiネットワーク名（SSID）およびWiFiセキュリティ設定が完全に一致している必要があります。
  WiFi接続で初期設定のためにアクセスポイントにアクセスする方法については、「初期設定のためにアクセスポイントに接続する（33ページ）」を参照してください。
- WiFiクライアントデバイスが、WiFiネットワークに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を変更する（85ページ）」を参照してください。
  注：アクセスポイントのWiFi認証と暗号化がWPA3 Personalに設定されており、WiFiクライアント機器がWPA3をサポートしている場合、WiFiクライアント機器でWiFiアダプターのデバイスドライバー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に近づけ、少なくとも6フィート（1.8メートル）離してください。
- アクセスポイントとWiFiクライアントデバイスの間にある物によって、WiFi信号が遮られ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、ユーザー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 (83 ページ) を参照してください。

- WiFiクライアントデバイスが固定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てください。(ほとんどのデバイスでは、DHCPは の初期設定です)。

LEDを使った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、14ページの「LED付きトップパネル、屋内モデルWAX610」または22ページの「LED付きサイドパネル、屋外モデルWAX610Y」をご覧ください。

アクセスポイントを電源に接続し、LED を無効にしていない場合（「LED の管理（189 ページ）」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、最初はオレンジ色の点灯で、その後ゆっくりとオレンジ色に点滅します。約 2 分後、Power/Cloud 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、アクセスポイントの準備が整ったことを示します：
   - **緑色に点灯**：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。
   - **青色に点灯**：アクセスポイントはInsightモードで機能し、クラウドベースの管理プラットフォームInsightに接続されています。
2. 起動手順が完了したら、以下を確認します：
   - LAN LEDは、イーサネットリンクの速度に応じて、緑色の点灯またはオレンジ色の点灯になります。
     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が緑色で点灯します。
     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。無線機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をトラブルシューティングに利用することができます。詳しくは、次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がオレンジ色に点灯したまま
- 電源/クラウドLEDが橙色でゆっくり連続点滅している
- アクセスポイントはPoE PDとして機能し、Power/Cloud LEDはオレンジ色に点灯したままです。

電源/クラウドLEDは消灯したまま

PoE+接続を使用していて、EthernetケーブルをPoE+スイッチに接続したときに、Power/Cloud LEDと他のLEDが消灯している場合は、以下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（189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が両端とも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、PoE+スイッチのPoE+ポートに差し込まれ、電力が供給されていることを確認する。
- PoE+スイッチのPoEパワーバジェットがオーバーサブスクリプションでないことを確認し、PoE+スイッチがアクセスポイントにPoE+（802.3at）電力を供給できるようにすることです。

オプションの電源アダプターを使用し、アクセスポイントの電源を入れたときにPower/Cloud LEDやその他のLEDが消灯したままの場合は、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（189ページ）」を参照）。
- 電源アダプターがアクセスポイントに正しく接続されていること、電源アダプターが機能しているコンセントに正しく接続されていることを確認してください。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。
- この製品に 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がオレンジ色に点灯したまま

アクセスポイントを電源に接続すると、Power/Cloud LEDが最初はオレンジ色の点灯、次にオレンジ色の点滅が遅くなり、最後に緑の点灯または青の点灯となり、起動手順が完了し、アクセスポイントの準備が整ったことを示します。

5分経過してもPower/Cloud LEDがオレンジ色に点灯したままの場合は、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る可能性があります。

次のことを行ってください：

1. アクセスポイントを電源から外し、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. 起動手順が正常に完了せず、5 分経過しても Power/Cloud LED がオレンジ色に点灯したままの場合は、**Reset** ボタンを使用してアクセスポイントを工場出荷時の設定に戻してください。詳しくは、「リセットボタンを使って屋内型WAX610をリセットする（184ページ）」または「リセットボタンを使って屋外型WAX610Yをリセットする（185ページ）」をご覧ください。

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が橙色でゆっくり連続点滅している

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色の点灯になり、その後、緑色の点灯または青色の点灯になります。これは、起動手順が完了し、アクセスポイントの準備が整ったことを示します。通常動作時、Power/Cloud LEDが一時的にオレンジ色に点滅するのは、ファームウェアのアップグレード時のみです。また、その場合、Power/Cloud LEDはゆっくりではなく、素早くオレンジ色に点滅します。Power/Cloud LED がゆっくりと連続してオレンジ色に点滅する場合、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ないことを示します。

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 クライアントの有効化」（149 ページ）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）があること、DHCP サーバーがアクセスポイントに到達できること（どちらも同じネットワーク上にある必要があります）を確認し てください。

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（148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はオレンジ色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、Power/Cloud LEDが最初はオレンジ色の点灯、次にオレンジ色の点滅が遅くなり、最後に緑の点灯または青の点灯となり、起動手順が完了し、アクセスポイントの準備が整ったことを示します。

アクセス ポイントが PoE PD として機能し、5 分経過しても Power/Cloud LED がオレンジ色に点灯したままの場合、アクセス ポイントは必要な 802.3at (PoE+) レベルで電力を受け取っていない可能性があります。たとえば、アクセス ポイントが、802.3at（PoE+）ではなく 802.3af（PoE） のみを提供するスイッチに接続されている場合、この状況が発生することがあります。

次のことを行ってください：

1. アクセスポイントのLAN/PoE+ポートとPoE+スイッチの802.3at（PoE+）ポートでイーサネットケーブルを切断して再接続します。アクセスポイントが再起動します。
2. 5分経ってもPower/Cloud LEDがオレンジ色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理由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リプションであり、アクセスポイントに十分なPoEパワーを利用できるようにするためには、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、「Power/Cloud LEDがオレンジ色に点灯したまま（257ページ）」を参照してください。

NETGEAR Insightの管理モードでPower/Cloud 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、Power/Cloud 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、Power/Cloud LED が青く点灯せず、緑のままである場合、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、Power/Cloud 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試してください：

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-browser に変更する（164 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の接続が良好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ていること、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。

   詳しくは、「アクセスポイントのファームウェアを管理する（172ページ）」を参照してください。
5. LAN/PoE+ポートでイーサネットケーブルを抜き差しし、5分ほど待って、Power/Cloud LEDが青色で点灯するかどうかを確認します。

   アクセスポイントに電源アダプターを使用している場合は、電源アダプター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. それでも解決しない場合は、「**Reset**」ボタンでアクセスポイントを工場出荷時の

設定に戻し、アクセスポイントを再設定してください。詳しくは、「リセットボタンを使って屋内型WAX610をリセットする（184ページ）」または「リセットボタンを使って屋外型WAX610Yをリセットする（185ページ）」をご覧ください。

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のヘルプ 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のオレンジ色、グリーン、ブルーの点滅が止まらない

Insight Instant Mesh WiFi ネットワークの最初のインストールと構成プロセスでは、アクセスポイントをノードとして構成している間、Power/Cloud LED がオレンジ色、グリーン、ブルーに点滅します。詳しくは、「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（66 ページ）」を参照してください。

Power/Cloud LEDがオレンジ色、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。

以下の項目を確認するか、以下のトラブルシューティングをお試しください：

- ノードが接続できるルートが少なくとも 1 つあることを確認してください。
- 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てください。
- 各ルートの各無線の出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、無線の出力パワーを変更する（106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。詳しくは、「ノードとルートが接続できない（261ページ）」を参照してください。
- ノードを再起動します。
- 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、ノードを Insight アカウントに再度追加し、Insight ネットワークの場所に追加します。

2.4G または 5G WLAN LED が消灯しています。

2.4G WLAN LEDまたは5G WLAN LEDが消灯している場合は、次の操作を行います：

- 無線が無効になっていないか確認します（「無線のオン／オフを切り替える（101ページ）」を参照）。デフォルトでは、無線は有効で、WLAN LEDは次のように点灯します：
  - **緑色に点灯**：無線はクライアントがいない状態で動作しています。
  - **青色に点灯**：無線はクライアントが接続されています。
  - **青色に点滅**：無線はクライアントが接続されており、トラフィックを処理中です。

- PoE接続を使用している場合、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ます。アクセスポイントには、802.3at（PoE+）レベルの電力が必要です。PoE+ よりも低いレベルの電力は、無線に影響を及ぼします。詳細については、258 ページの「アクセス ポイントが PoE PD として機能し、Power/Cloud LED がオレンジ色のまま点灯している」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のヘルプ 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

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アクセスポイントを追加する場合（Insight アプリを使用してノードとしてアクセスポイントをルートに接続（66 ページ）参照）、最初の同期中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、ノードを使用する予定の場所に移動します。

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障害物の少ない見通しの良い場所に、25フィート（7.5m）未満で設置してください。

ノードをすでにInsightネットワークの場所に追加した後に、ノードとルートを同期するには、次のようにします：

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、シンク処理中にのみ使用します。
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電源コネクターに電源アダプターを接続します。
   ノードのPower/Cloud LEDがオレンジ色に点灯します。
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がオレンジ色、緑色、青色の点滅を止め、青色の点灯になるのを待ちます。

   注：初期接続と設定処理に最大10分かかる場合があります。また、設定中にノードが再起動することがあります。

   初期接続・設定中は、Power/Cloud LEDが以下のように点灯します：

   - **緑色に点滅**：ノードはルートの検出を試みています。
   - **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の最初の接続を行っています。

- **オレンジ色がゆっくり点滅**：ノードは、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ます。
  電源/クラウドLEDのオレンジ色の点滅が止まらない場合は、258ページの「電源/クラウドLEDがゆっくり、連続してオレンジ色に点滅している」を参照してください。
- **オレンジ色、グリーン、ブルーが点滅**：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のオレンジ色、緑色、青色の点滅が止まらない場合は、「電源/クラウドLEDのオレンジ色、緑色、青色の点滅が止まらない（260ページ）」を参照してください。

設定が完了すると、Power/Cloud LEDが次のように点灯します：

- **青色で点灯**：設定が完了し、ノードは操作可能な状態になります。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. ノードの接続を解除し、使用する場所に移動します。
5. 新しい場所で、Step 2とStep 3を繰り返します。
6. ノードがルートと再同期するのを待ちます。
   ノードのPower/Cloud LEDが青色で点灯したら、ノードとルートが正常に同期されたことになります。

   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、もう一度やり直してください。WiFi接続を良好または公正に確立するためには、ノードはルートのWiFiカバー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ト

WiFiクライアント機器がアクセスポイントに接続できない、またはWiFi接続が正常でない場合、問題の切り分けを試みてください：

- WiFiクライアント機器とアクセスポイントのWiFi設定が完全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）および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接続による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、「初期設定のためのアクセスポイントへの接続」（33ページ）をご参照ください。
- 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に対応していますか？

詳しくは、「WiFiネットワークの認証と暗号化を変更する（85ページ）」をご覧ください。

注：アクセスポイントのWiFi認証と暗号化がWPA3 Personalに設定されており、WiFiクライアント機器がWPA3をサポートしている場合、WiFiクライアント機器でWiFiアダプターのデバイスドライバー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クライアント機器は、WiFiネットワークを見つけることができますか？
  そうでない場合は、WLAN LED を確認してください。WLAN LED が消灯している場合、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、101 ページの「無線をオンまたはオフにする」を参照してください。
- アクセスポイントの WiFi ネットワークに対する SSID ブロードキャストを無効にすると、WiFi ネットワークが非表示になり、WiFi デバイスのネットワークスキャンリストに表示されなくなります。(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（83 ページ）を参照してください。

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設定が有効になる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クライアント機器がWiFiネットワークを見つけたが、信号強度が弱い場合、以下の条件を確認してください：

- WiFiクライアント機器がアクセスポイントから遠すぎる、または近すぎるのでは？
  WiFiクライアントデバイスをアクセスポイントの近くに置き、少なくとも6フィート（1.8メートル）、信号強度が改善されるかどうかを確認します。
- WiFiクライアント機器とアクセスポイントの間に、WiFi信号を遮るものがありませんか？

インターネットブラウジングのトラブルシューティング

WiFi機器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Webページを読み込むことができない場合、次のような理由が考えられます：

- WiFiデバイスがDNSサーバーの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設定時にDNSアドレスを手動で入力した場合（つまり、アクセスポイントは静的IPアドレス設定を使用している）、WiFiデバイスを再起動してDNSアドレスを確認してください。
- 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てください。

TCP/IPの問題については、「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（266ページ）」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することはできません

LAN上のコンピューターからアクセスポイントにログインして、アクセスポイントのローカルブラウザーUIを使用することができない場合は、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、大文字と小文字が区別されます。
  以前に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 Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の 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、35 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。
- パソコンのIPアドレスがアクセスポイントと同じサブネットにあることを確認してください。アクセスポイントをネットワークに接続したときに、アクセスポイントのDHCPクライアントを無効にして、固定（静的）IPアドレスを設定した場合（「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（148ページ）」を参照）、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サブネット内になるように、コンピュータ上のIPアドレスとサブネットマスクを変更します。
- ブラウザを終了して、再度起動してみてください。
- 古いタイプのブラウザをお使いの場合は、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をお使いの場合は、「**Refresh**」**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（例えば、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スキャナアプリケーションを使用してIPアドレスを検出することができます。
  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。詳しくは、35 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。

  それでも IP アドレスが見つからない場合は、アクセスポイントの設定を工場出荷時のデフォルトにリセットします。これにより、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、「リセットボタンを使用して屋内モデルWAX610をリセットする（184ページ）」または「リセットボタンを使用して屋外モデルWAX610Yをリセットする（185ページ）」を参照してください。

変更内容は保存されません

アクセスポイントのローカルブラウザーUIにログインしているときに、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、次のようにしてください：

- 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。
- Webブラウザの「**Refresh**」または「**Reload**」ボタンをクリックします。変更が行われたものの、Webブラウザのキャッシュに古い設定が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たため、アクセスポイントにログインできなくなった

間違ったadminパスワードを3回以上入力すると、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。例えば、間違ったパスワードを3回入力した場合、アクセスポイントへのアクセスは5分間ブロックされることがあります。

ブロック期間は、ログイン試行失敗回数によって異なります。ブロック期間中は、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の試みは無視されます。ブロック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*機会が一度だけ*あります。再度間違ったパスワードを入力すると、次の表のように遮断期間が延長されます。

表3.ログインブロック期間

失敗した回数	ブロック機関
3	5
4	10
5	20
6	40
などなど.....。	

また、ログイン失敗回数については、以下のルールが適用されます：

- ログイン失敗回数が再試行許可回数より少ない場合、ログイン失敗回数のカウンターは30分後にリセットされます。例えば、以下のようになります、

間違ったパスワードを2回入力し、3回目に正しいパスワードを入力した場合、30分後に2回のログイン失敗が記憶から消去されます。

- ログイン失敗回数が再試行許可回数より多い場合、ログイン失敗回数のカウンターは24時間後にリセットされます。例えば、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、24時間後に5回のログイン試行失敗はメモリーから消去されます。
- 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ーを増加させるかどうかが決定されます。
- 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ー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機器やルーターには、指定された機器にエコー要求パケットを送信するpingユーティリティが搭載されています。その後、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でpingユーティリティを使用すると、簡単にネットワークのトラブルシューティングを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

パソコンからアクセスポイントにpingを打ち、アクセスポイントまでのLAN経路が正しく設定されていることを確認することができます。

Windowsベースのコンピューターからアクセスポイントにpingを送信する場合：

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**」を検索して選択します。
2. 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**ボタンをクリックします。
   以下の様なメッセージが表示されます：

   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ります：

- 物理的な接続がおかしい
  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てください。
- ネットワーク構成がおかしい
  コンピューターとアクセスポイントのIPアドレスが正しいことを確認し、アドレスが同じサブネット内にあることを確認します。

パソコンからリモート機器までの経路をテストする

LAN経路が正しく動作することを確認したら、パソコンからリモート機器までの経路をテストしてください。

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場合：

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**検索して選択します。
2. 表示されたフィールドに、**ping -n 10** ***IP address*** と入力します。
   IPアドレスは、リモートDNSサーバーなど、リモート機器のIPアドレスです。

パスが正しく機能している場合は、「アクセスポイントへのLANパスのテスト（266ページ）」で説明したような返信が表示されます。返信がない場合は、次の操作を行ってください：

- お使いのコンピューターに、アクセスポイントが接続されているルーターのIPアドレスがデフォルトのルーターとしてリストアップされていることを確認します。パソコンのIP設定がDHCPで割り当てられている場合、この情報はパソコンのネットワークコントロールパネルに表示されません。
- お使いのパソコンのネットワークアドレス（IPアドレスのうちネットマスクで指定されている部分）が、リモート機器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

本付録には、以下の項目があります：

- 工場出荷時の設定
- 屋内用WAX610の技術仕様
- 屋外用WAX610Yの技術仕様

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設定に戻すことができます。

アクセスポイントを工場出荷時の設定に戻す方法の詳細については、「アクセスポイントを工場出荷時の設定に戻す」（184ページ）を参照してください。

表 4.工場出荷時の設定

設定項目	初期設定
管理・ログイン設定	
マネジメントモード	NETGEAR Insight(クラウド/リモート) **注**：ローカルブラウザーUIにアクセスするには、管理モードとしてWeb-browser（Local）を選択する必要があります。
ユーザーログイン URL	192.168.0.100、ネットワークに接続されていない場合。 **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サーバーやルーターからIPアドレスを受け取ります。
ユーザー名	**admin**, 設定変更不可
APログイン パスワード	**パスワード**、大文字小文字を区別する、設定可能 **注**：ローカルブラウザ UI に初めてログインする場合、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 ネットワークの場所に追加し、Insight Cloud Portal または Insight アプリでアクセスポイントを管理した場合、その場所の Insight ネットワークパスワードを入力します。詳しくは、35 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。
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	初期設定の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（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 ネットワークの場所に追加し、Insight Cloud Portal または Insight アプリでアクセスポイントを管理した場合、この要件が適用されない場合があります。
WiFiの初期セキュリティ	WPA2 Personal（WPA2-PSKのことです。） 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場合は、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 ネットワークの場所に追加し、Insight Cloud Portal または Insight アプリでアクセスポイントを管理した場合、この要件が適用されない場合があります。
RFチャンネル	両方の無線機で自動的に選択（Auto）されます。 **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、アクセスポイントに選択した国や地域によって異なります。
システム全般の設定	
動作モード	APモード

表4.工場出荷時の設定（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アドレスを受信できるように有効にします。
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
マルチキャストDNSゲートウェイ	無効
LED	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 Personal（WPA2-PSKのことです。） 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ON
WiFi設定	両方有効
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と自動802.11v WiFiネットワークマネジメントが含まれます。
WiFiクライアントの分離	無効
URLトラッキング	無効
DHCPオファーのユニキャスト化	有効

表4.工場出荷時の設定（続き）

設定項目	初期設定
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
アドバンスドレート選択	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：有効
WiFiモード	2.4GHz：11b、11bg、11naもサポートする11axモード 5GHz：11a、11na、11acもサポートする11axモード
チャンネル幅	2.4GHz：ダイナミック20/40MHz 5GHz：ダイナミック20/40/80MHz
ガードインターバル	2.4GHz：Long-800 ns 5GHz：Long-800 ns
出力電力	2.4GHz：最大（100%） 5GHz：最大（100%）
チャンネル	2.4GHz：オート 5GHz：オート
Wi-Fi マルチメディア（WMM）	2.4GHz：有効 5GHz：有効
WMM Powersave	2.4GHz：有効 5GHz：使用可能
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	2.4GHz：200 デフォルト（最大数も同様） 5GHz：200 デフォルト（最大数も同様）
RTS閾値	2.4GHz：2346でイネーブル 5GHz：2346で有効化
ビーコン間隔	2.4GHz：100ミリ秒 5GHz：100ミリ秒
802.11n 256 QAM	2.4GHz：無効 5GHz：コンフィギュレーション不可
MU-MIMO	2.4GHz：有効 5GHz：有効

表4.工場出荷時の設定（続き）

設定項目	初期設定
ブロードキャストとマルチキャスト	2.4GHz：有効、ただし50ppsに制限 5GHz：有効、ただし50ppsに制限
802.11h	2.4GHz：適用外 5GHz：無効
ロードバランシング	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	有効
ブロードキャスト機能強化	無効
ワイヤレスブリッジ	設定されていない
一般的なセキュリティ	
URLフィルタリング	無効
RADIUS	設定されていない
ネイバーAP検出	2.4GHz：無効 5GHz：無効
MAC ACL	デフォルトのACLは8個あるが、MACアドレスは設定されていない
L2セキュリティ	無効
リモート管理	
SNMP	無効

屋内用WAX610の技術仕様

屋内用モデルWAX610の技術仕様は以下の通りです。

表 5.技術仕様室内機WAX610

機能	説明
WiFiモード	2.4GHz：802.11ax, 802.11ng, 801.11bg, 802.11b 5GHz：802.11ax、802.11ac、802.11na、802.11a アクセスポイントは、2.4GHzと5GHzの同時動作に対応しています
理論上の最大スループット	同時スループット約1800Mbps（2.4GHz帯：600Mbps、5GHz帯：1200Mbps）。 **注**：スループットは変化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、データのスループット率に影響します。
対応クライアントの最大数	2.4GHz：200 5GHz：200 個々の無線機が200クライアントをサポートしても、アクセスポイントがサポートできるクライアント数は合計で200です。(例えば、2.4GHz無線で150クライアント、5GHz無線で50クライアントのように）。
802.11セキュリティ	WPA3 Personal、WPA3 Enterprise、WPA3/WPA2 Personal、WPA2 Personal、WPA2 Enterprise、WPA2/WPA Personal、Open Enhanced, and Open
WiFi規格	IEEE 802.11ax (WiFi 6) WiFi Multimedia Prioritization (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	4 (2+2)の流れがあります： 2.4GHz帯ラジオ：2ストリーム 5 GHz帯ラジオ：2ストリーム
動作周波数範囲	2.412-2.472 GHz 5.180-5.240 GHz 5.260-5.230 GHz 5.500-5.700GHz
パワーオーバーイーサネット	電源アダプタを使用しない場合、LAN/PoE+ポートは802.3at（PoE+）電源を必要としますが、802.3af（PoE）電源でも機能する場合があります。802.3at（PoE+）電源を使用することをお勧めします。 **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）とみなされるかもしれません。
PoE消費電力	15.5W
電源アダプター	DC12V、2.5A プラグは販売国にローカライズされています。 **注**）電源アダプターは付属しておりませんが、オプションとしてご注文いただけます。

表5.技術仕様室内モデルWAX610（続き）

特徴	説明
ハードウエア・インターフェース	2.5Gbps、1Gbps、100Mbps、10Mbpsに対応したRJ-45 LAN/PoE+ Ethernetポート1基。また、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：**電源アダプタを使用しない場合、LAN/PoE+ポートは802.3at（PoE+）電源を必要としますが、802.3af（PoE）電源でも機能する場合があります。802.3at（PoE+）電源を使用することをお勧めします。
寸法（幅×奥行×高さ）	6.3×6.3×1.3インチ（160×160×33mm）。
重量	0.9ポンド（412g）
動作温度	32°～104°F（0°～40°C）
動作湿度	10～90% 最大相対湿度、結露なし
保存温度	-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 Part 15 Report (EMI) SubPart B CE EMC Report, EN 55032/24 Report EN 301 489-17 EMC Report
規制対応 米国	FCC Grant, FCC Authorization FCC Spectrum Report, Part 15, SubPart C (15.247) FCC Spectrum Report, Part 15, SubPart E (15.407) FCC Standard Absorption Rate Report (SAR or MPE), FCC Part 2 SpJ
規制対応 欧州	EN 300 328, Radio Spectrum Report EN 301 893 Radio Spectrum Report EN 301 893 DFS Report EN RF Exposure (SAR or MPE), EN 62311(for Wi-Fi) , EN 62479 (for BT), EN 50385 (for AP router), EN 50566 (Body SAR)
安全・エネルギー対応	IEC 60950-1 CB Certificate and Test Report, CB IEC60950 / EN60950 CE LVD Report, EN60950 Report EC 278/2009, External Power Supply

屋外用WAX610Yの技術仕様

屋外用WAX610Yの技術仕様は以下の通りです。

表6.技術仕様室外機WAX610Y

特徴	説明
WiFiモード	2.4GHz帯の無線機：802.11ax, 802.11ng, 801.11bg, 802.11b 5GHz無線機：802.11ax、802.11ac、802.11na、802.11a アクセスポイントは、2.4GHzと5GHzの同時動作に対応しています
理論上の最大スループット	同時スループット約1800Mbps（2.4GHz帯：600Mbps、5GHz帯：1200Mbps）。 **注**：スループットは変化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、データのスループット率に影響します。
対応クライアントの最大数	2.4GHz：200 5GHz：200 個々の無線機が200クライアントをサポートしても、アクセスポイントがサポートできるクライアント数は合計で200です。(例えば、2.4GHz無線で150クライアント、5GHz無線で50クライアントのように）。
802.11セキュリティ	WPA3 Personal、WPA3 Enterprise、WPA3/WPA2 Personal、WPA2 Personal、WPA2 Enterprise、WPA2/WPA Personal、Open Enhanced, and Open
WiFi規格	IEEE 802.11ax (WiFi 6) WiFi Multimedia Prioritization (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	4 (2+2)ストリーム： 2.4GHz：2ストリーム 5 GHz：2ストリーム
動作周波数範囲	2.412-2.472 GHz 5.180-5.240 GHz 5.260-5.230 GHz 5.500-5.700GHz
パワーオーバーイーサネット	電源アダプタを使用しない場合、LAN/PoE+ポートは802.3at（PoE+）電源を必要としますが、802.3af（PoE）電源でも機能する場合があります。802.3at（PoE+）電源を使用することをお勧めします。 **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）とみなされるかもしれません。
PoE消費電力	15.5W

表6.技術仕様室外機WAX610Y（続き）

特徴	説明
ハードウエア・インターフェース	2.5Gbps、1Gbps、100Mbps、10Mbpsに対応したRJ-45 LAN/PoE+ Ethernetポート1基。また、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：**電源アダプタを使用しない場合、LAN/PoE+ポートは802.3at（PoE+）電源を必要としますが、802.3af（PoE）電源でも機能する場合があります。802.3at（PoE+）電源を使用することをお勧めします。
寸法（幅×奥行×高さ）	12.00×7.13×1.81インチ（305×181×46mm）。
重量	2.05 lb（930 g）
動作温度	14°～122°F（-10°～50°C）
動作湿度	10～90% 最大相対湿度、結露なし
保存温度	-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 Part 15 Report (EMI) SubPart B CE EMC Report, EN 55032/24 Report EN 301 489-17 EMC Report
規制対応 米国	FCC Grant, FCC Authorization FCC Spectrum Report, Part 15, SubPart C (15.247) FCC Spectrum Report, Part 15, SubPart E (15.407) FCC Standard Absorption Rate Report (SAR or MPE), FCC Part 2 SpJ
規制対応 欧州	EN 300 328, Radio Spectrum Report EN 301 893 Radio Spectrum Report EN 301 893 DFS Report EN RF Exposure (SAR or MPE), EN 62311(for Wi-Fi) , EN 62479 (for BT), EN 50385 (for AP router), EN 50566 (Body SAR)
安全・エネルギー対応	IEC 60529 Edition 2.1 2001-02 - IP55 IEC 60950-1 CB Certificate and Test Report, CB IEC60950 / EN60950 CE LVD Report, EN60950 Report EC 278/2009, External Power Supply

B

屋内用WAX610を壁や天井に取り付ける

アクセスポイントのパッケージには、壁掛け用と天吊り用の部品が含まれています。

アクセス ポイントは、9/16 インチ（14.3 mm）または 15/16 インチ（23.8 mm）の T バーで固体表面（壁または天井）または天井に取り付けるか、平らな面に自立して設置することができます。

アクセスポイントと設置または配置された表面の間の狭いスペースにケーブルが収まるように、フラットなイーサネットケーブルを使用することをお勧めします。

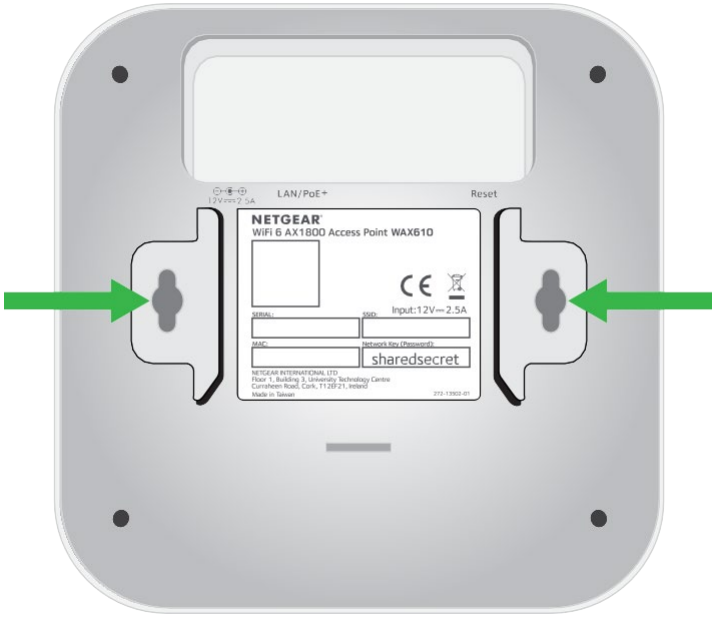
本付録には、以下の項目があります：

屋内用WAX610を壁面に取り付ける

注意：アクセスポイントを堅固な壁に取り付ける場合は、壁が損傷していないことを確認してください。たとえば、水害で乾式壁が破壊されることがあります。

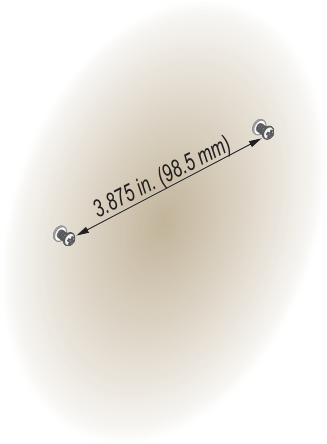
アクセスポイントを壁面に取り付けるには

1. アクセスポイントの底面には2つの穴があり、壁に挿した2本のネジにアクセスポイントを取り付けることができます。

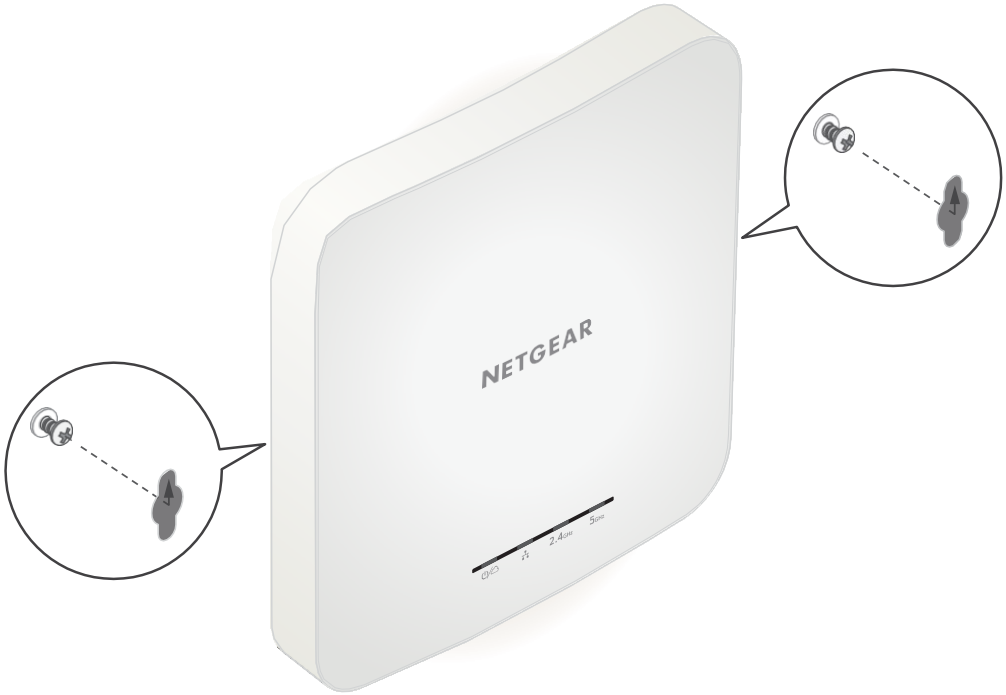


2. 付属のアンカーとネジを挿入する壁面に印を付け、3.875インチ（98.5mm）離してください。

3. アンカーとネジを挿入しますが、ネジがアクセス ポイントの底面にある穴に挿入できるように、各ネジの約 0.25 インチ (6 mm) を壁から突出させておいてください。



4. アクセスポイントの底面にある穴を壁のネジに合わせ、アクセスポイントを壁に取り付けます。

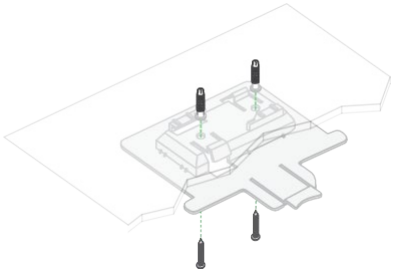


屋内用WAX610を堅固な天井に取り付ける

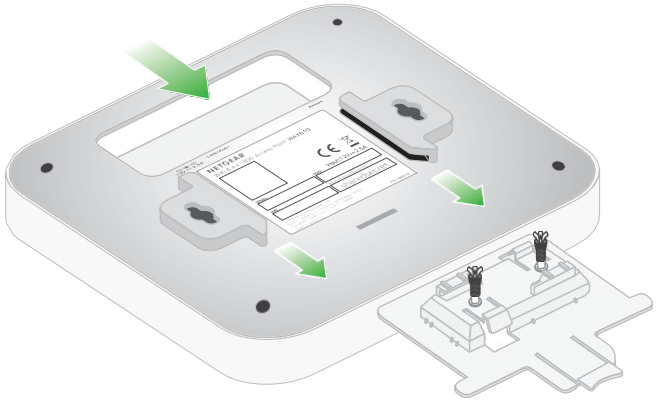
注意：アクセスポイントを堅固な天井に取り付ける場合は、天井が損傷していないことを確認してください。たとえば、水漏れがあると天井が損傷することがあります。

アクセスポイントを強固な天井に取り付ける場合：

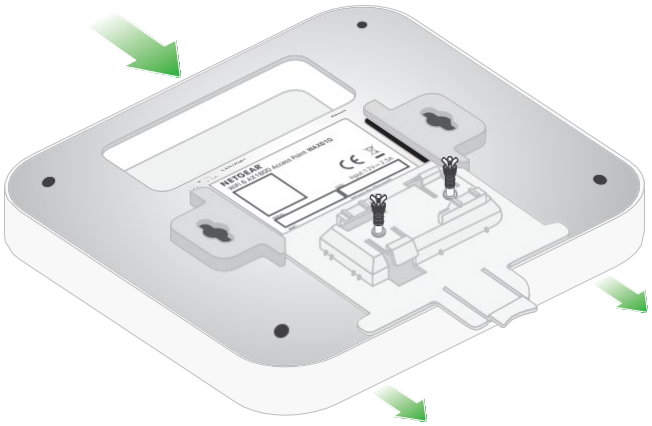
1. 付属のアンカーとネジを使って、ネジ穴のある15/16インチ（23.8mm）ブラケットを天井に取り付けます。
   ブラケットの長方形の突起部分が天井に向くようにしてください。

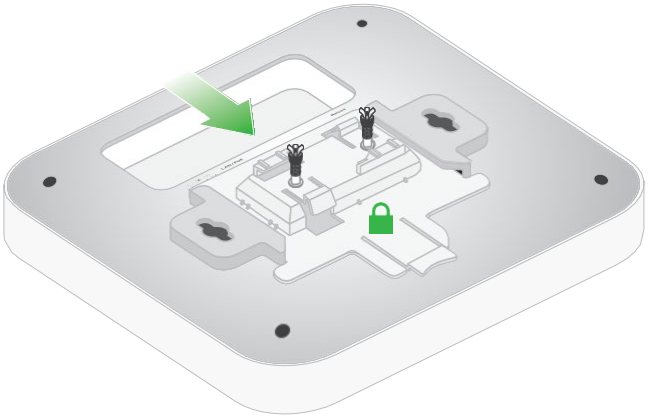


2. アクセス ポイントの前面がブラケットに向くように、アクセス ポイントを逆さまに持ちます。
3. アクセスポイントの底面にあるガイドをブラケットに合わせます。

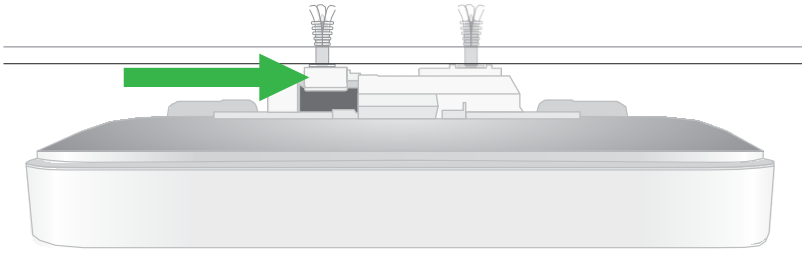


4. アクセスポイントをブラケットにロックされるまでスライドさせます。





注：アクセス ポイントのロックを解除するには、ロックタブを天井に向かって押し、アクセス ポイントをブラケットからスライドさせて外します。次の図は、天井に取り付けられたアクセス ポイントの側面図です。緑色の矢印は、ロックタブを示しています。



屋内用WAX610をTバーに取り付ける

Tバーのサイズに応じて、9/16インチ（14.3mm）または15/16インチ（23.8mm）のブラケットを使用してください。

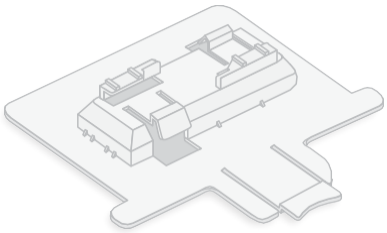


図 13.9/16インチ（14.3 mm）ブラケット

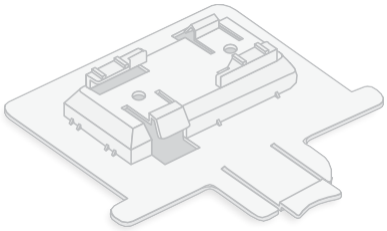
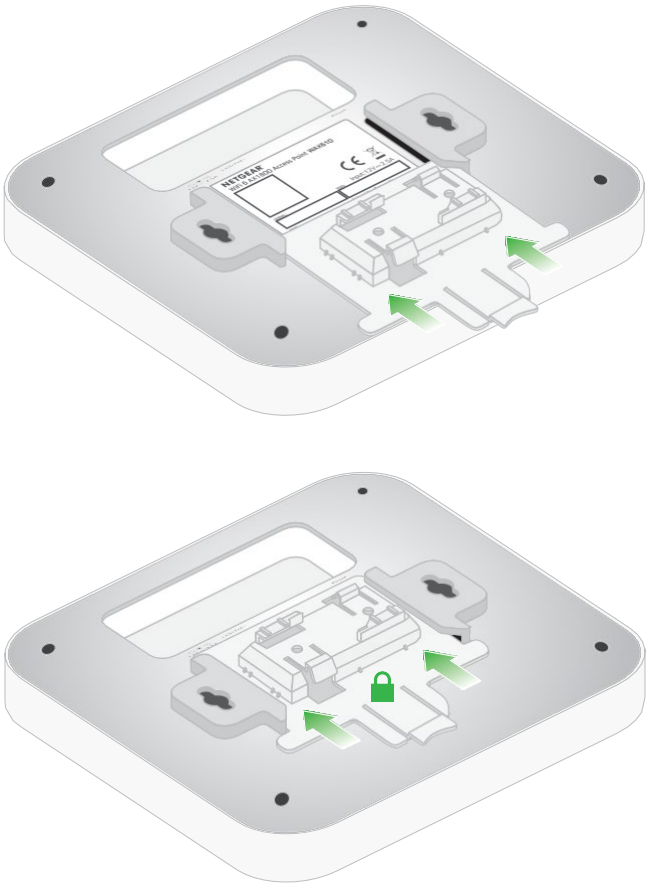


図14.15/16インチ（23.8mm）ブラケット

アクセスポイントをTバーに取り付ける場合：

1. 9/16 インチ（14.3 mm）または 15/16 インチ（23.8 mm）のブラケットを、アクセス ポイントの底面にあるガイドの間に、所定の位置にロックされるまでスライドさせます。
   ロックタブは、アクセスポイントの前面にある必要があります。



2. アクセスポイントを逆さまに持ちます。

   注：Tバーの後ろに手が届く場合は、片手でTバーを持ち、もう片方の手でアクセスポイントを持つようにしてください。

3. ブラケットの長方形の凸部をTバーに合わせる。
4. ブラケットをTバーの片側に引っ掛けます。

5. ブラケットをTバーの反対側に、ブラケットがTバーにロックされるまで引っ掛けます。

C

屋外用WAX610Yを壁や支柱に取り付ける

アクセスポイントのパッケージには、壁掛け用とポールマウント用の部品が含まれています。

アクセスポイントを屋外の壁面に取り付けることができます。パッケージには、ネジ2本、ワッシャー2枚、紙製のネジ配置ガイドが含まれています。

また、アクセスポイントをポールに取り付けることもできます。パッケージにはポール取り付け用ストラップが同梱されています。

注：アクセスポイントを屋外の定位置に設置する前に、ネットワーク環境に応じてアクセスポイントを設定し、セットアップをテストすることをお勧めします。

警告：アクセスポイントを屋外に設置した後は、湿気や虫がアクセスポイントの内部に入らないように、カバーをしっかりと閉めてください。

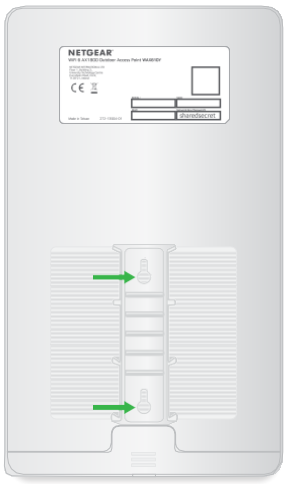
本付録には、以下の項目があります：

屋外用WAX610Yを壁面に取り付ける

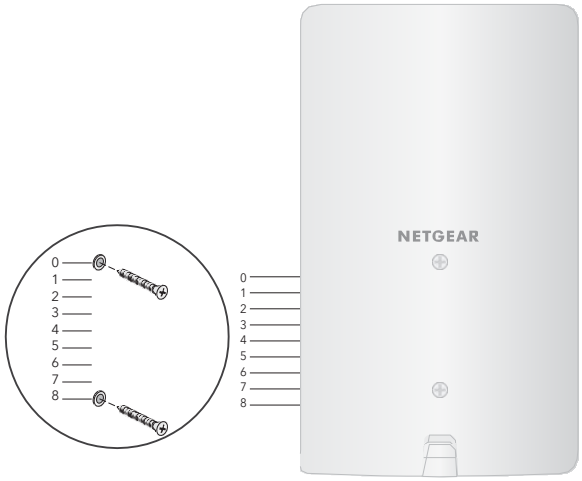
注意：壁を傷つけないように注意してください。

アクセスポイントを壁面に取り付けるには

1. アクセスポイントの背面にある壁掛け用の2つの穴の位置を確認します。
   下図の矢印は、穴を示しています。



2. ネジ配置ガイドを使用して、アクセスポイントを取り付ける壁の穴の位置をマークします。
   穴は、中心から中心まで3.15インチ（80mm）離れている必要があります。



3. ビスを差し込む2本のアンカー用の穴を壁に開ける。

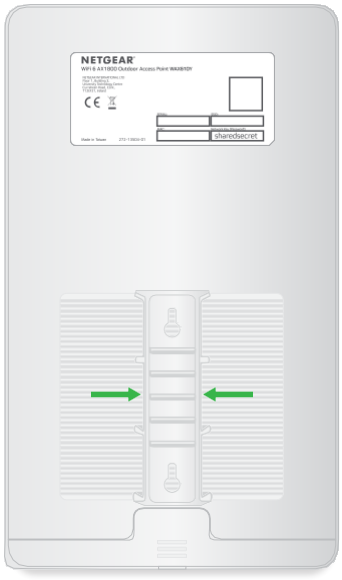
ネジとアンカーはパッケージの中のビニール袋に入っています。

4. アンカーを壁に差し込み、2号プラスドライバーでネジを締めます。
   アクセス ポイントの背面にある穴にネジを挿入できるように、各ネジの壁からの突出部分を約 6 mm (0.25 インチ) 残しておきます。
5. アクセスポイントの背面にある穴を壁のネジに合わせ、 アクセスポイントを壁に取り付けます。

屋外用WAX610Yをポールに取り付ける

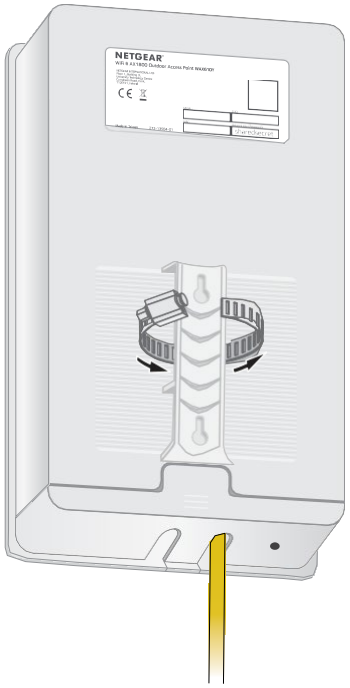
アクセスポイントをポールに取り付けるには

1. アクセス ポイントの背面にあるポール マウント ストラップ用の開口部の位置を確認します。次の図の矢印は、中央の開口部を示しています。

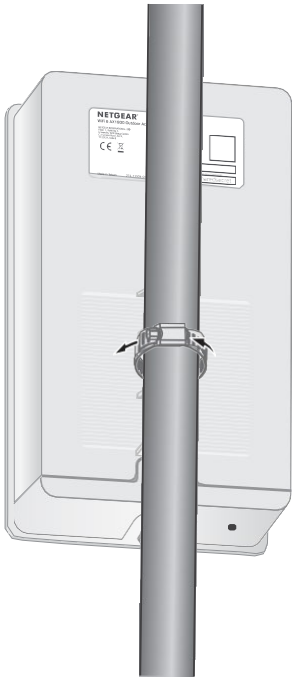


2. ドライバーで、付属のポールマウントストラップを開く。

3. アクセスポイントの背面にある開口部の1つにストラップを挿入します。



4. ストラップを開いたまま、付属のアクセスポイントが付いたストラップをポールに巻き付けます。
5. ストラップを閉じますが、締め付けないでください。



6. アクセスポイントを取り付けたストラップを定位置に移動します。
7. ドライバーを使い、ネジを締めてストラップとアクセスポイントをポールに固定します。