

NETGEAR®

ProSAFE デュアルバンド
ワイヤレス LAN アクセスポイント
WNDAP360
管理マニュアル



350 East Plumeria Drive
San Jose, CA 95134
USA

Dec,2015
202-10826-01(英文参照文書)

WNDAP360 管理マニュアル

NETGEAR 製品をお選びいただきありがとうございます。

NETGEAR 製品のインストール、設定、または仕様に関するご質問や問題については、下記の NETGEAR カスタマーサポートまでご連絡ください。

無償保証を受けるためには、本製品をご購入後 30 日以内にユーザー登録が必要になります。ユーザー登録方法につきましては、別紙[ユーザー登録のお知らせ]をご確認ください。

NETGEAR カスタマーサポート

電話:フリーコール 0120-921-080

(携帯・PHS など、フリーコールが使用できない場合:03-6670-3465)

受付時間:平日 9:00 - 20:00、土日祝 10:00 - 18:00(年中無休)

E-mail: support@netgear.jp

テクニカルサポートの最新情報は、NETGEAR のウェブサイトをご参照ください。

<http://www.netgear.jp/support/>

商標

NETGEAR、NETGEAR ロゴは米国およびその他の国における NETGEAR, Inc.の商標または登録商標です。

その他のブランドおよび製品名は、それぞれの所有者の商標または登録商標です。

記載内容は、予告なしに変更されることがあります。

© 2015 NETGEAR, Inc. All rights reserved.

適合性

本製品をお使いになる前に、適合性の情報をお読みください。

各種規格との適合に関する情報は、ネットギアのウェブサイト (<http://www.netgear.com/about/regulatory/>) をご覧ください(英語)。

製品型番	ファームウェア
WNDAP360-100JPS	WNDAP360_V3.0.5.0

改版履歴

2015.12.21 : 初版

目次

改版履歴.....	3
目次.....	4
はじめに.....	8
ProSAFE デュアルバンドワイヤレスアクセスポイント WNDAP360 について.....	8
システム要件.....	8
主な機能と標準.....	9
サポートされる標準と慣例.....	9
主要な機能.....	9
802.11b/g/n と 802.11a/n ベースのワイヤレスネットワーク 11	11
イーサネット接続の自動検知とストレート・クロス自動判定.....	11
ハードウェア機能.....	11
上面.....	11
底面とプロダクトラベル.....	13
インストールと基本設定.....	14
設定する前に.....	14
ワイヤレス機器設定と範囲のガイドライン.....	14
イーサネット配線要件.....	15
LAN 設定要件.....	15
コンピューター要件.....	15
ワイヤレスアクセスポイントのインストールと設定.....	15
ワイヤレスアクセスポイントをコンピューターに接続する.....	16
ワイヤレスアクセスポイントを設定する.....	16
ワイヤレスアクセスポイントにログインする.....	17
ワイヤレスアクセスポイントにログインする.....	17
Web 管理インターフェース.....	18
基本システム設定と時間設定を行う.....	19
基本システム設定を行う.....	19
時間設定をする.....	20
IP 設定と DHCP サーバー設定.....	22
IP 設定をする.....	22
DHCP サーバー設定をする.....	23
IGMP Snooping 設定をする.....	24
基本ワイヤレス設定をする.....	24
802.11b/bg/ng ワイヤレス設定を行う.....	25
802.11a/na ワイヤレス設定を行う.....	28

WNDAP360 管理マニュアル

運用周波数(チャンネル)ガイドライン	30
基本ワイヤレス接続をテストする	30
ワイヤレス接続をテストする	30
ワイヤレスアクセスポイントを設置する	31
天井取り付け	31
天井取付キットを使ってワイヤレスアクセスポイントを取り付ける	31
壁面取り付け	33
壁面取付キットを使ってワイヤレスアクセスポイントを取り付ける	33
机に取り付ける	35
ワイヤレスアクセスポイントを机に取り付ける	35
ワイヤレス設定とセキュリティ	36
ワイヤレスデータセキュリティオプション	36
セキュリティプロファイル	37
SSID,WEP,WPA 設定を変更する前に	38
802.11b/bg/ng モード用シート	39
802.11a/an モード用シート	40
セキュリティプロファイルの設定と有効化	41
セキュリティプロファイルを設定し有効にする	41
Open System を WEP または WEP Shared KEY で設定する	45
レガシー802.1X を設定する	46
WPA with RADIUS、WPA2 with RADIUS、WPA & WPA2 with RADIUS を設定する	47
WPA-PSK、WPA2-PSK、および WPA-PSK & WPA2-PSK を設定する	48
RADIUS サーバー設定	49
RADIUS サーバー設定をする	50
MAC アドレスでワイヤレスアクセス制限をする	52
MAC アドレス制限をする	52
電波の停止スケジュール	53
電波のオンオフをスケジュールする	54
基本ワイヤレス QoS を設定する	54
基本ワイヤレス QoS を設定する	55
管理	57
リモート管理を有効にする	57
SNMP 管理	57
SNMP 管理インターフェースを設定する	57
Secure Shell(SSH)と Telnet 管理	58
リモートコンソール機能を設定する	58
シリアル接続でワイヤレスアクセスポイントを管理する	58
ワイヤレスアクセスポイントソフトウェアのアップグレード	59
Web ブラウザーでのアップグレード手順	60

WNDAP360 管理マニュアル

Web ブラウザーを使ってワイヤレスアクセスポイントのファームウェアをアップグレードする.....	60
TFTP サーバーアップグレード手順	61
TFTP サーバーを使ってワイヤレスアクセスポイントのファームウェアをアップグレードする	61
設定ファイルの管理とファクトリーデフォルト	63
設定の保存	63
設定を保存する	63
設定の復元	63
保存した設定ファイルから設定を復元する	64
ワイヤレスアクセスポイント設定を工場出荷状態に戻す	64
Web ブラウザーで工場出荷状態に戻す	65
リセットボタンで工場出荷状態に戻す	65
アクセスポイントの再起動	66
ワイヤレスアクセスポイントを再起動する.....	66
管理者パスワードの変更	66
管理者パスワードを変更する.....	67
Syslog サーバーを有効にする	67
Syslog サーバーを有効にする	68
ワイヤレスアクセスポイントの監視.....	68
システム情報を見る	68
システム画面を表示する	69
ワイヤレス端末の監視.....	71
接続されたワイヤレス端末を確認し、その詳細を見る.....	71
アクティビティログを確認する	73
アクティビティログを表示して保存する.....	74
トラフィック統計 Traffic Statistics	74
Statistics 画面を表示する。	74
不正 AP 検知を有効にする	76
不正 AP 検知の有効化と設定	76
不正 AP 検知を有効にし設定する.....	77
アクセスポイントを Know AP List から削除し、Unknown AP List に追加する.....	77
Known AP List にリストをインポートする.....	78
アクセスポイントリストを確認して保存する	78
Unknown AP List を確認しファイルに保存する.....	78
Known AP Lists を確認してファイルに保存する	79
拡張設定.....	81
STP(Spanning Tree Protocol)と 802.1Q VLAN	81
STP と VLAN を設定する	82
ホットスポット設定	82
ホットスポットサーバーを設定する	83
拡張ワイヤレス設定	83
拡張ワイヤレス設定をする.....	84

WNDAP360 管理マニュアル

拡張 QoS 設定をする.....	86
拡張 QoS を設定する	87
ワイヤレスブリッジ設定.....	88
Point-to-Point ワイヤレス設定.....	90
Point-to-point ワイヤレスネットワークを設定する	90
Point-to-Multipoint ワイヤレス設定.....	93
Point-to-multipoint ワイヤレスネットワーク設定をする	94
Point-to-Multipoint ブリッジモードを使ってワイヤレスアクセスポイントでワイヤレス信号をリポートする.....	98
ワイヤレスアクセスポイントでワイヤレス信号をリポートする	98
トラブルシューティング.....	103
基本機能	103
ワイヤレスアクセスポイントの LED がどれも点灯しない	103
アクティブ LED または LAN LED が点灯しない	104
無線 LAN LED が点灯しない.....	104
ワイヤレス可能なコンピューターからインターネットまたは LAN に接続できない.....	104
ブラウザからワイヤレスアクセスポイントを設定できない	105
ブラウザに URL や IP アドレスを入力してもタイムアウトが発生する.....	106
Ping を使って TCP/IP ネットワークをトラブルシュートする.....	106
ワイヤレスアクセスポイントへの LAN 接続を確認する	106
Windows コンピューターからワイヤレスアクセスポイントへ Ping する.....	107
お使いのコンピューターからリモートデバイスへの接続を確認する	108
日付と時間の問題.....	108
パケットキャプチャーツールを使う.....	109
パケットをキャプチャーする.....	109
A.補足情報.....	110
技術仕様.....	110
工場出荷設定	114
B.コマンドライン	116

はじめに

この章では、NETGEAR ProSAFE デュアルバンドワイヤレスアクセスポイント WNDAP360 の紹介といくつかの機能について説明します。

ProSAFE デュアルバンドワイヤレスアクセスポイント WNDAP360 について

ProSAFE デュアルバンドワイヤレスアクセスポイント WNDAP360(以下 WNDAP360)はワイヤレス LAN インフラストラクチャーの基本構成要素です。

WNDAP360 は 2.4GHz 802.11b/g/n および 5GHz 802.11a/n と有線イーサネットとの間の接続を提供します。WNDAP360 は周波数帯毎に 10-32 ユーザーをサポートします。

WNDAP360 は有線 LAN とワイヤレスクライアントの間のブリッジとして動作します。複数のワイヤレスアクセスポイントを有線イーサネットで接続することによって、ワイヤレスネットワークの範囲を広げることが可能です。モバイルコンピューティングデバイスが一つのアクセスポイントの範囲を出て、他の範囲に移動します。結果として、ワイヤレスクライアントは自由にローミングでき、ネットワークへのシームレスな接続を維持することができます。

WNDAP360 の自動検知機能によって、最大 300Mbps あるいは距離や電磁波の影響に合わせたそれ以下の速度でのパケット送信を可能にします。

同梱内容

製品には以下のものが同梱されています

- ProSAFE デュアルバンドワイヤレスアクセスポイント WNDAP360
- AC アダプター (12VDC, 1.0A)
- ストレートイーサネットケーブル
- インストールガイド
- リソース CD
- ウォールマウントキット

システム要件

ワイヤレスアクセスポイントをインストールする前に、お使いのシステムが要件に一致しているか確認してください。

- 10/100/1000 Mbps イーサネット接続可能なスイッチ等のネットワーク。

- カテゴリー5 以上の UTP イーサネットケーブル。
- 100-240V AC 電源
- Microsoft Internet Explorer 6.0 以上、Mozilla 1.5 以上のウェブブラウザ
- TCP/IP が動作するコンピューター。
- 802.11a/n または 802.11b/g/n のワイヤレスデバイス。

主な機能と標準

WNDAP360 は簡単に使え、堅実なワイヤレスネットワークを提供します。WNDAP360 は広範なセキュリティ機能も提供します。

サポートされる標準と慣例

WNDAP360 以下の標準と慣例をサポートします。

- **適合標準:** ワイヤレスアクセスポイントは IEEE 802.11a/b/g 標準に適合し、802.11n Wi-Fi Certified を取得しています。
- **完全 WPA と WPA2 サポート:** ワイヤレスアクセスポイントは WPA/WPA2 および WPA-PSK/WPA2-PSK をサポートしています。
- **マルチ BSSID:** ワイヤレスアクセスポイントは複数の BSSID をサポートします。ワイヤレスアクセスポイントが有線ネットワークといくつかのワイヤレス端末のセットに接続されると、そのセットは BSS(basic service set)と呼ばれます。BSSID(basic service set identifier)はワイヤレス LAN で送信されるパケットのヘッダーに付けられる一意の識別子で、ワイヤレス LAN を識別するものとなっています。

マルチ BSSID 機能は一つのワイヤレスアクセスポイントで 8 つまでの SSID を設定でき、それぞれの SSID に異なった設定をすることが可能です。

- **DHCP クライアントサポート:** ワイヤレスアクセスポイントは DHCP クライアントとして動作して DHCP サーバーから情報を得ることができます。DHCP サーバーとして動作し、ワイヤレスクライアントにネットワーク情報を提供することも可能です。
- **SNMP サポート:** SNMP MIB をサポートしています。
- **802.1Q VLAN サポート:** 802.1QVLAN をサポートしています。

主要な機能

WNDAP360 は以下の機能を提供します。

- **同時デュアルバンド:** ワイヤレスアクセスポイントは 2.4GHz と 5GHz 同時に動作します。
- **複数の動作モード**

- **ワイヤレスアクセスポイント:** 802.11b/g/n および 802.11a/n ワイヤレスアクセスポイントとして動作します。
- **ポイント-ポイントブリッジ:** このモードではワイヤレスアクセスポイントは一つのブリッジモードのワイヤレス端末またはワイヤレスアクセスポイントとだけ通信します。この通信を保護するためにネットワーク認証を使うべきです。
- **ポイント-マルチポイントブリッジ:** **Point-to-multipoint bridge.** Select this only if this ワイヤレスアクセスポイントが複数のブリッジモードワイヤレス端末のマスターである時のみ選択します。他のブリッジモードワイヤレス端末はマスターブリッジ経由でのみ通信し、直接は通信しません。このトラフィックを守るためにネットワーク認証を使うべきです。
- **ワイヤレス信号のリピート:** このモードでは、ワイヤレスアクセスポイントはアクセスポイントとしては動作せず、ワイヤレス信号をポイント-、マルチポイントブリッジモードでワイヤレス信号をリピートし、すべてのトラフィックをリモートアクセスポイントへ送信します。このトラフィックを守るためにネットワーク認証を使うべきです。
- **ホットスポット設定:** HTTP (TCP, port 80)リクエストを捕捉し指定した URL へリダイレクトします。
- **ファームウェアアップグレード:** ファームウェアはフラッシュメモリーに保存されます。Web ブラウザーを使ってリモートから簡単にアップデートできます。コマンドラインインターフェースを使うこともできます。
- **不正 AP 検知:** 不正 AP フィルタ機能で不明の AP が LAN にアクセスできないようにします。
- **アクセスコントロール:** MAC アドレスフィルタアクセスコントロール機能で信頼できるワイヤレス端末だけが LAN にアクセスするためにワイヤレスアクセスポイントを使う事ができます。
- **セキュリティプロファイル:** マルチ BSSID を使う際、それぞれの BSSID に対してセキュリティ設定(暗号化、SSID 等)をすることができます。
- **ステルスモード:** SSID のブロードキャストを停止して、SSID 設定を持っている端末のみが接続できるようにできます。
- **安全な Telnet コマンドインターフェース:** SSH クライアントが必要です。
- **設定バックアップ:** 設定をファイルに保存、復元が可能です。
- **PoE(Power over Ethernet):** 802.3af 対応の PoE 給電装置からワイヤレスアクセスポイントに給電が可能です。
- **オートネゴシエーションおよび Auto-MDI/MDI-X:** 10/100/1000 Mbps IEEE 802.3 イーサネットネットワークに接続可能です。
- **LED 表示:** 電源/テスト、アクティブ、LAN、2.4G/5G のラジオの状態を確認できます。
- **WMM(Wi-Fi マルチメディア)サポート:** ワイヤレスアクセスポイントは WMM をサポートしています。
- **QoS (Quality of Service) サポート:** ワイヤレスアクセスポイントは QoS をサポートしています。
- **VLAN セキュリティプロファイル:** 各セキュリティプロファイルには VLAN ID が割り当てられます。

802.11b/g/n と 802.11a/n ベースのワイヤレスネットワーキング

WNDAP360 はイーサネット LAN と 802.11b/g/n および 802.11a/n ワイヤレスネットワーク間のブリッジ機能を提供します。イーサネットネットワークとワイヤレス機能を持ったノートブック、プリントサーバー等との接続をします。

イーサネット接続の自動検知とストレート・クロス自動判定

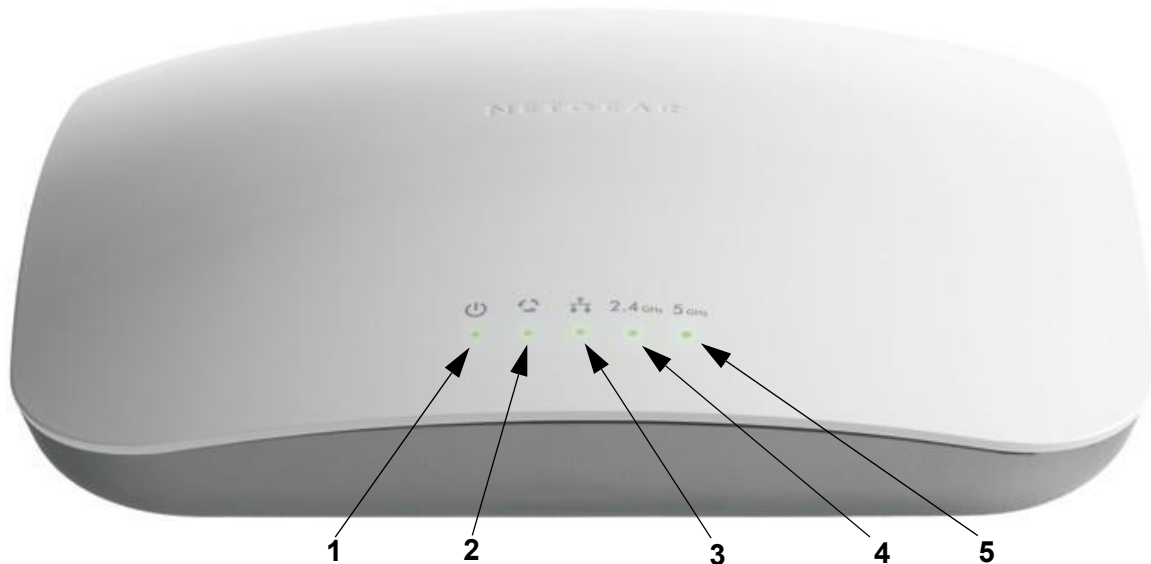
WNDAP360 は標準的なイーサネットネットワークに接続できます。速度とデュプレックスを自動設定します。クロス、ストレートの自動認識も行います。

ハードウェア機能



この章では WNDAP360 の上面と背面のハードウェア機能について記します。

上面

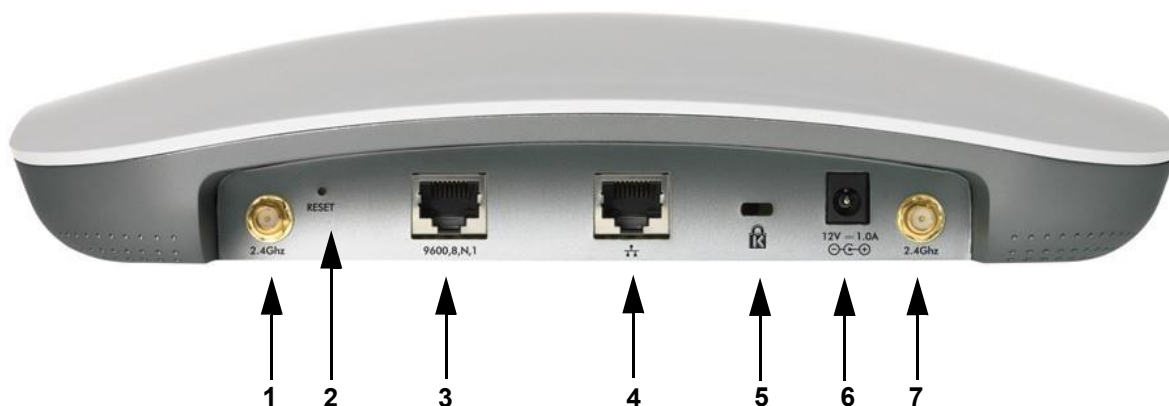
WNDAP360 の LED の説明を以下に記します。



番号	LED	説明		
1		電源/テスト	消灯	電源オフ
			緑点灯	電源オン
			オレンジ⇒緑点滅	セルフテスト実行中あるいはソフトウェアロード中。起動途中で、最初はオレンジ点灯⇒消灯

				=>緑点滅=>緑点灯(全行程約 45 秒)。約 1 分後にオレンジ点灯または緑点滅の場合は故障。
2		アクティブ	消灯	イーサネットトラフィックが存在しないまたはリンクダウン。
			緑点灯または点滅	イーサネットトラフィックが存在する。
3		LAN	消灯	10Mbps リンクまたはリンクダウン。
			オレンジ	100 Mbps リンク。
			緑	1000 Mbps リンク。
4	2.4 GHz	無線 LAN	消灯	2.4GHz の無線 LAN ダウン。
			緑点灯または点滅	2.4GHz の無線 LAN アップ。
5	5 GHz	無線 LAN	消灯	5GHz の無線 LAN ダウン。
			緑点灯または点滅	5GHz の無線 LAN アップ。

背面



以下に WNDAP360 の背面パネルの説明を記します。

1. 追加 2.4GHz アンテナ用のリバーズ SMA コネクタ
2. ファクトリーデフォルトボタン。5 秒以上押し続けてワイヤレスアクセスポイント設定を工場出荷時に戻します。
3. コンソールポート。9.600bps, (8) data bits, no (N) parity bit, and one (1) stop bit.
4. 10/100/1000BASE-T ギガビットイーサネット(RJ-45)ポート。(Auto MDI-X) IEEE 802.3af PoE(Power over Ethernet)
5. ケンジントンロック取り付け穴。
6. AC アダプター用ソケット(12 VDC, 1A)
7. 追加 2.4GHz アンテナ用のリバーズ SMA コネクタ

底面とプロダクトラベル

ワイヤレスアクセスポイントの底面にプロダクトラベルが貼付されており、工場出荷時設定等の情報が表示されています。

NETGEAR	 Power	 ACTIVE	 LAN	2.4 GHz 5 GHz	DC Input: DC 12 V --- 1.0 A
Prosafe Dual Band Wireless-N Access Point. Model: WNDAP360					
DEFAULT ACCESS IP: http://192.168.0.100 User Name: admin password: password	FCC ID: PY311100154	IC: 4054A-11100154	This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.		
		Made in China	272-11244-02	Network Name	<input type="text"/>
				Network Key	<input type="text"/>
				SERIAL	<input type="text"/>
				MAC	<input type="text"/>

インストールと基本設定

この章ではアクセスポイントのインストールと設定について記します。この基本設定により、2.4GHz 802.11b/g/n または 5GHz 802.11a/n のワイヤレスアダプターがインターネットに接続したり LAN のプリンターやファイルにアクセスしたりできるようになります。

ワイヤレスネットワークを計画するにあたり、必要とされるセキュリティレベルを検討してください。

設定する前に

ワイヤレスアクセスポイントを設定する前に、以下のガイドラインと要件を検討する必要があります。

ワイヤレス機器設定と範囲のガイドライン

ワイヤレス接続範囲はワイヤレスアクセスポイントの設置環境により様々です。遅延、スループットパフォーマンス、ノート PC のワイヤレスアダプターの消費電力も設定により様々です。

メモ: ガイドラインに従わないとパフォーマンス劣化やワイヤレスアクセスポイントへの接続ができなくなることがあります。

最良の結果を得るために、以下のガイドラインにしたがってワイヤレスアクセスポイントを設定してください。

- PC を動作させる場所の中心付近に設置します。
- PC から見えるような高い棚の上等に設置します。
- PC 電子レンジ、2.4GHz コードレスホン等の干渉源から離して設置します。
- 大きな金属面や水から離して設置します。
- 外部アンテナを垂直に設置すると水平方向のカバーをします。外部アンテナを水平方向に設置すると、上下方向をカバーします。(外部アンテナは WNDAP360 には付属していません。)

- ワイヤレスアクセスポイントを複数使用しているならば、隣接したアクセスポイントは異なる周波数(チャンネル)を使用するように設定します。2.4GHz 帯では 5 チャンネルを離して設定します。(例:チャンネル1と6等)

ワイヤレスコネクションを確立するのにかかる時間はセキュリティ設定と設置方法に依存します。WEP は比較的長い時間がかかります。ノート PC で WEP は電力消費も他の方式よりも多くなります。

イーサネット配線要件

ワイヤレスアクセスポイントは LAN との間を RJ-45 コネクタのツイストペアカテゴリ5 イーサネットケーブルで接続します。

LAN 設定要件

ワイヤレスアクセスポイントを初期設定するには、コンピューターとワイヤレスアクセスポイントを接続する必要があります。

コンピューター要件

ワイヤレスアクセスポイントに接続するには、コンピューターは 802.11b/g/n または 802.11a/n のワイヤレスアダプターがインストールされている必要があります。

ワイヤレスアクセスポイントのインストールと設定

ワイヤレスアクセスポイントをインストールする前に、お使いのイーサネットネットワークが稼働中であることを確認してください。ワイヤレスアクセスポイントをイーサネットネットワークに接続します。その後、802.11b/g/n または 802.11a/n ワイヤレスアダプターを持つコンピューターがイーサネットネットワークと通信します。

以下の手順でワイヤレスアクセスポイントをインストールして設定します。

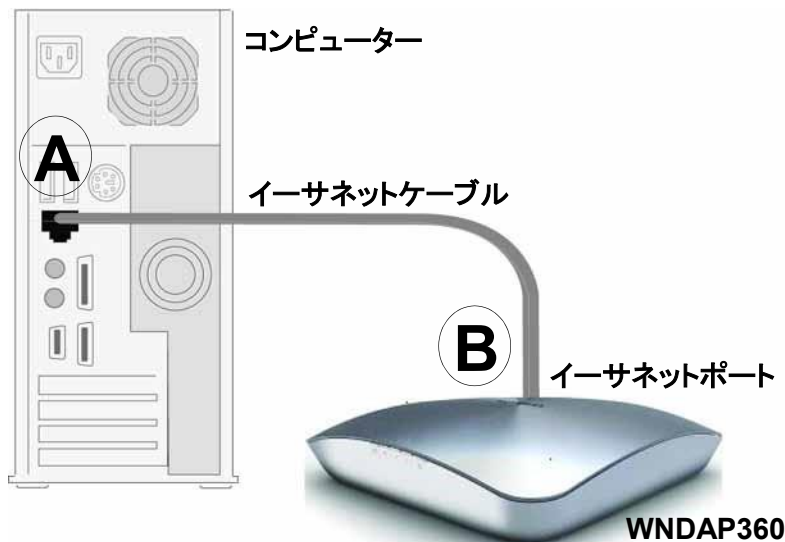
1. ワイヤレスアクセスポイントをコンピューターに接続します。
2. ワイヤレスアクセスポイントにログインします。
3. 基本設定と時間設定をします。
4. IP 設定と DHCP サーバー設定をします。
5. 基本ワイヤレス設定をします。

ワイヤレスアクセスポイントをコンピューターに接続する

メモ: ワイヤレスアクセスポイントをアクセスしにくい高所に取り付けの前にワイヤレスアクセスポイントの設定とテストをします。

ワイヤレスアクセスポイントを設定する

1. 箱を開けて中身を確認します。
2. イーサネット接続可能なコンピューターを準備します。コンピューターが既に使用中の場合は、コンピューターの TCP/IP 設定を記録します。
コンピューターの IP アドレスを 192.168.0.210、サブネットマスクを 255.255.255.0 に設定します。
3. コンピューターとワイヤレスアクセスポイントをイーサネットケーブルで接続します。



4. コンピューターを起動します。
5. ワイヤレスアクセスポイントの電源を入れます。
メモ: ワイヤレスアクセスポイントは PoE をサポートしています。PoE スイッチをお持ちの場合は、AC アダプターは不要です。
6. 以下を確認します。



Power/Test LED: 起動直後点滅します。(正確には、最初はオレンジ点灯⇒消灯⇒緑点滅⇒緑点灯(全行程約 45 秒)。約 1 分後にオレンジ点灯または緑点滅の場合は電源を確認します。



Active LED: イーサネットトラフィックがある場合に点滅します。



LAN LED:速度に応じて点灯します。10Mbps の場合は消灯。100Mbps の場合はオレンジ。1000Mbps の場合は緑。LED が点灯しない場合はイーサネットケーブルの接続を確認してください。

2.4 GHz WLAN LED:2.4GHz のワイヤレス状態を示します。

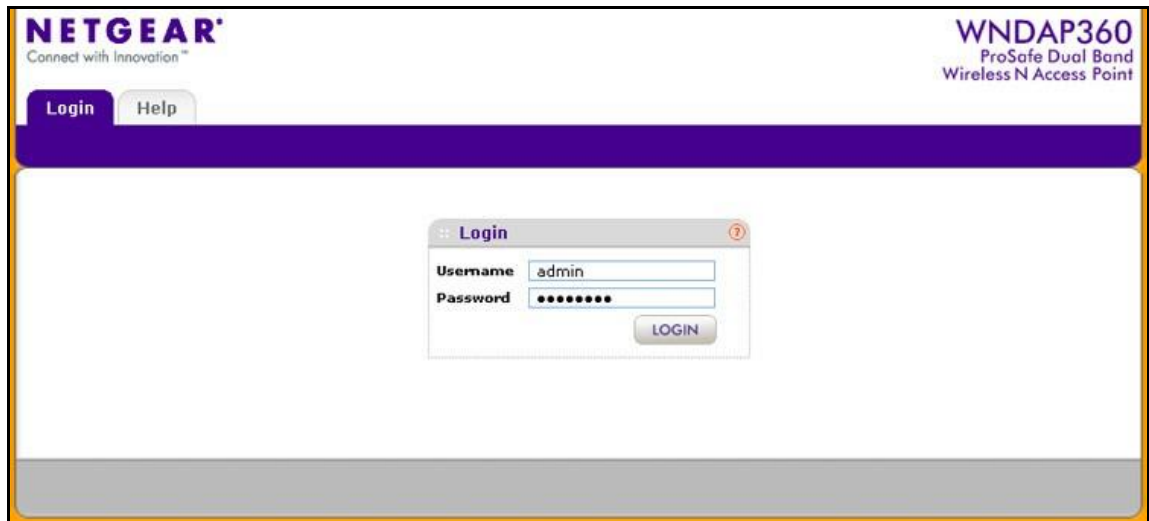
5 GHz WLAN LED:5GHz のワイヤレス状態を示します。

ワイヤレスアクセスポイントにログインする

ワイヤレスアクセスポイントのデフォルト IP アドレスは 192.168.0.100 です。ワイヤレスアクセスポイントはデフォルトで DHCP が有効になっています。(ファームウェアによって無効の場合もあります)

ワイヤレスアクセスポイントにログインする

1. Web ブラウザーを開きます。
2. ブラウザーのアドレスバーにワイヤレスアクセスポイントのデフォルト IP アドレス <http://192.168.0.100> を入力します。ログイン画面が表示されます。



3. ユーザーネームとパスワードを入力します。デフォルトは Username = “admin”, Password = “password”です。

4. Loginボタンをクリックします。General 設定画面が表示されます。

The screenshot shows the Netgear WNDAP360 web management interface. At the top left is the Netgear logo with the tagline "Connect with Innovation™". At the top right, it says "WNDAP360 ProSafe Dual Band Wireless N Access Point" and a "LOGOUT" button. Below the logo is a navigation bar with tabs for "Configuration", "Monitoring", "Maintenance", and "Support". Underneath is a purple bar with menu items: "System", "IP", "Wireless", "Security", and "Wireless Bridge". On the left side, there is a sidebar menu with "Basic", "Advanced", "General", and "Time". The main content area is titled "General" and contains two sections: "General" and "Cloud Settings". The "General" section has fields for "Access Point Name" (netgear848988) and "Country / Region" (United States). The "Cloud Settings" section has "Cloud Enabled" (Yes selected), "Cloud Activation Status" (Pending), and "Cloud Connectivity Status" (Disconnected). There is a link "Click here to open Cloud Management" and a note: "NOTE: If Cloud Enabled is set to Yes, this Access Point will periodically attempt to contact NETGEAR Cloud Wireless Server to check if this Access Point has been registered for cloud management." At the bottom right of the main content area are "CANCEL" and "APPLY" buttons. The footer says "Copyright © 1996-2015 Netgear ©".

Web 管理インターフェース

Web 管理インターフェースの上部にあるナビゲーションタブは常時表示されており、ワイヤレスアクセスポイントのすべての設定機能へアクセスすることができます。青いバーのメニュー項目は選択したナビゲーションタブにしたがって変化します。

This close-up screenshot shows the navigation tabs: "Configuration", "Monitoring", "Maintenance", and "Support". Below them is a purple bar with menu items: "System", "IP", "Wireless", "Security", and "Wireless Bridge". A "LOGOUT" button is visible in the top right corner.

右下には Apply, Cancel および画面によっては Edit ボタンが表示されます。

This close-up screenshot shows three buttons: "EDIT", "CANCEL", and "APPLY".

これらのボタンは以下の機能を持ちます。

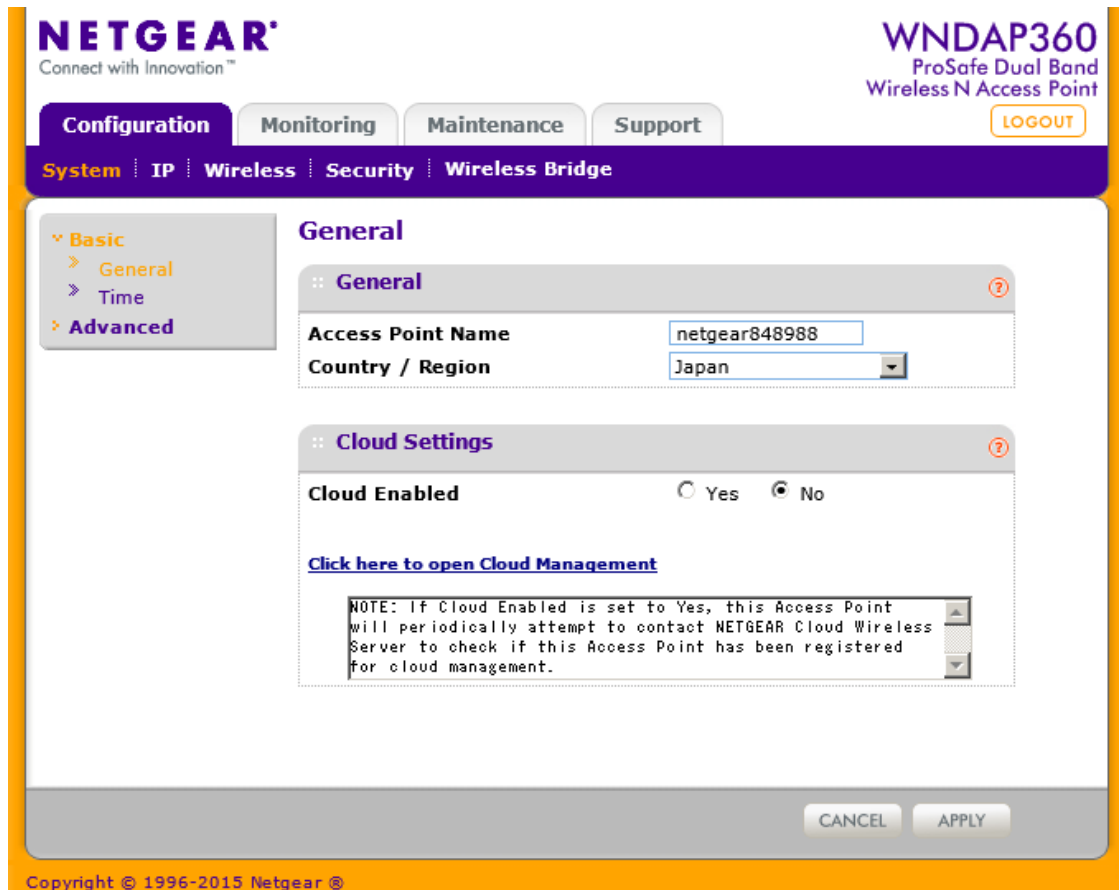
- **Edit:** 既存の設定を編集します。
- **Cancel:** 画面で行った設定変更をキャンセルします。
- **Apply:** 画面で行った設定変更を保存し適用します。

基本システム設定と時間設定を行う

メモ: ワイヤレスアクセスポイントにログインすると、General 画面が表示されます。

基本システム設定を行う

1. Configuration > System > Basic > General を選択して General 画面を表示します。



2. 以下の表の項目を設定します。

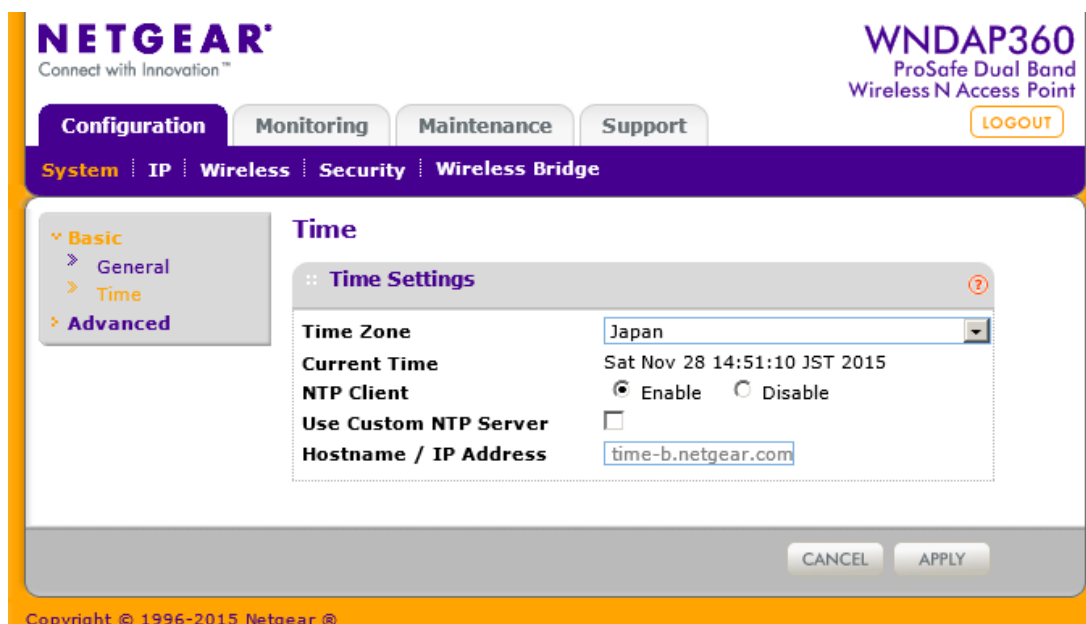
項目	説明
Access Point Name	ワイヤレスアクセスポイントの NetBIOS 名。ワイヤレスアクセスポイントの裏面のラベルに表示してあります。デフォルトは netgearxxxxxx です。xxxxxx はワイヤレスアクセスポイントの MAC アドレスの下 6 桁です。15 文字までの名前をつけることができます。この名前は SNMP で取得することができます。

Country/Region	<p>ワイヤレスアクセスポイントを設置する国を選択します。</p> <p>メモ: 必ず設置する国に設定してお使いください。</p> <p>この設定を変更すると、ワイヤレスアクセスポイントは再起動します。</p>
Cloud Enabled	<p>ビジネスセントラルワイヤレスマネージャー (BCWM) でワイヤレスアクセスポイントを管理する時に Yes を選択します。</p> <p>ワイヤレスアクセスポイントを単独 (スタンドアロン) で管理するときには No を選択します。このマニュアルでは No を選択します。</p> <p>この設定を変更すると、ワイヤレスアクセスポイントは再起動します。</p>
Cloud Activation Status	<p>このマニュアルの設定では使用しません。</p>
Cloud Connectivity Status	<p>このマニュアルの設定では使用しません。</p>

3. Apply ボタンをクリックして設定を保存します。

時間設定をする

1. Configuration > System > Basic > Time を選択して Time 画面を表示します。



2. 以下の項目を設定します。

項目	説明
----	----

Time Zone	設置場所のタイムゾーンを選択します。	
Current Time	現在の日時を表示します。	
NTP Client	ワイヤレスアクセスポイントの NTP(Network Time Protocol)クライアントを有効にして時間同期をします。デフォルトは Enable(有効)です。	
Use Custom NTP Server	デフォルト以外の NTP サーバーを指定するときに選択します。 メモ: ローカルネットワーク以外の NTP サーバーを使うにはインターネットへ接続する必要があります。	
	Hostname / IP Address	NTP サーバーの IP アドレスまたはホスト名を指定します。デフォルトは time-b.netgear.com です。 メモ: ホスト名を使うためには DNS サーバー設定がされていることを確認してください。

3. Apply ボタンをクリックして設定を保存します。

IP 設定と DHCP サーバー設定

IP 設定をする

1. Configuration > IP > IP Settings を選択して IP Settings 画面を表示します。

The screenshot shows the Netgear WNDAP360 web interface. The top navigation bar includes 'Configuration', 'Monitoring', 'Maintenance', and 'Support'. Below this, there are tabs for 'System', 'IP', 'Wireless', 'Security', and 'Wireless Bridge'. The 'IP Settings' page is displayed, showing a configuration window with the following fields:

- DHCP Client:** Enable Disable
- IP Address:**
- IP Subnet Mask:**
- Default Gateway:**
- Primary DNS Server:**
- Secondary DNS Server:**
- Network Integrity Check:**

At the bottom of the configuration window are 'CANCEL' and 'APPLY' buttons. The footer of the page reads 'Copyright © 1996-2015 Netgear ©'.

2. 以下の項目を設定します。

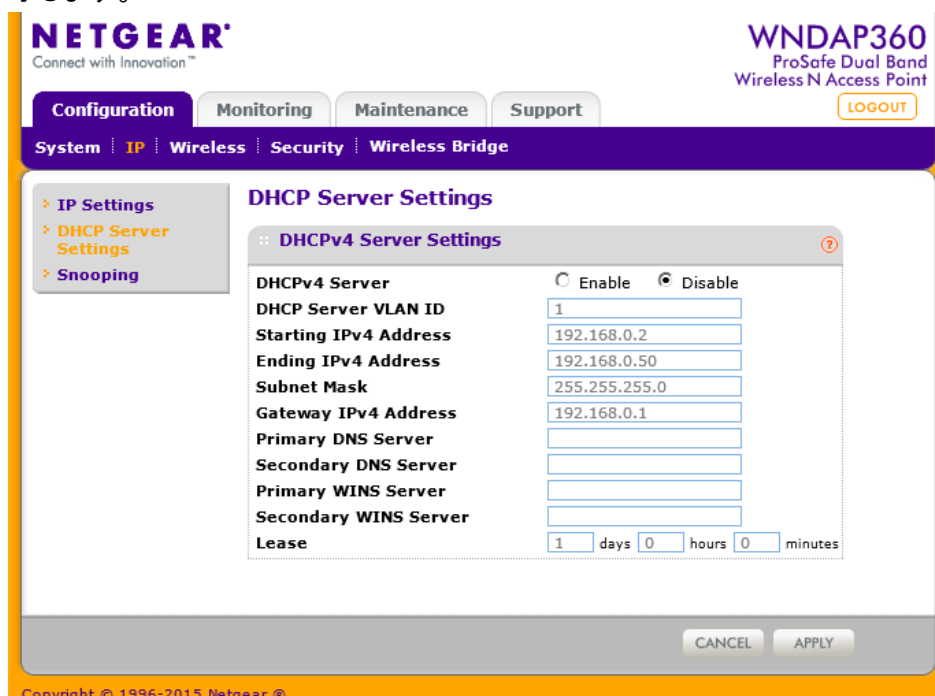
項目	説明
DHCP Client	アクセスポイントの DHCP クライアントを有効(Enable)にします。
IP Address	ワイヤレスアクセスポイントの IP アドレスを指定します。デフォルトは 192.168.0.100 です。
IP Subnet Mask	サブネットマスクを設定します。
Default Gateway	デフォルトゲートウェイの IP アドレスを設定します。
Primary DNS Server	
Secondary DNS Server	DNS サーバーを指定します。
Network Integrity Check	ワイヤレス接続をする前にアップストリームリンクが有効であることを確認します。デフォルトゲートウェイが設定されていることを確認してください。

4. Apply ボタンをクリックして設定を保存します。

ワイヤレスアクセスポイントは小さいネットワークで役に立つワイヤレスクライアントだけのための DHCP サーバー機能を提供することができます。DHCP サーバーを有効にすると、接続されたワイヤレス端末に TCP/IP 設定を提供することができます。

DHCP サーバー設定をする

1. Configuration > IP > DHCP Server Settings を選択して DHCP Server Settings 画面を表示します。



2. 以下の項目を設定します。

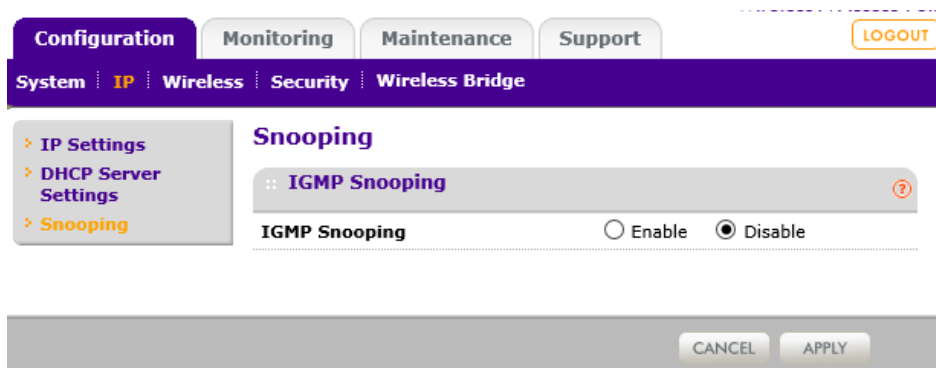
項目	説明
DHCP Server	DHCP Server チェックボックスを選択して DHCP サーバーを有効にします。割り当てる IP アドレスはアクセスポイントの LAN IP アドレスと同じサブネットの一部である必要があります。
DHCP Server VLAN ID	DHCP サーバーの VLAN ID を指定します。範囲は 1-4094 です。
Starting IP Address	DHCP クライアントに割り当てる IP アドレスの最初の値を指定します。デフォルトは 192.168.1.02 です。
Ending IP Address	DHCP クライアントに割り当てる IP アドレスの最後の値を指定します。デフォルトは 192.168.1.50 です。
Subnet Mask	サブネットマスクを指定します。デフォルトは 255.255.255.0 です。

Gateway IP Address	DHCP クライアントのデフォルトゲートウェイ IP アドレスを指定します。デフォルトは 192.168.0.1 です。
Primary DNS Address	プライマリーDNS の IP アドレスを指定します。
Secondary DNS Address	セカンダリーDNS の IP アドレスを指定します。
Primary WINS Server	プライマリーWINS サーバーの IP アドレスを指定します。
Secondary WINS Server	セカンダリーWINS サーバーの IP アドレスを指定します。
Lease	DHCP サーバーのリース時間を指定します。デフォルトは1日です。

3. **Apply** ボタンをクリックして設定を保存します。

IGMP Snooping 設定をする

1. **Configuration > IP > Snooping** を選択して **Snooping** 画面を表示します。
2. **IGMP Snooping: Enable (有効)** にすると IP マルチキャストパケットが対応するマルチキャスト



トグループのメンバーのみに転送されます。この機能によりマルチキャストトラフィックがブロードキャストドメインの全ポートにフラッディング (Flooding) されることを防ぎます。

3. **Apply** ボタンをクリックして設定を有効にします。

基本ワイヤレス設定をする

設定するエリアでのワイヤレス機器の法令遵守および適合性のために、動作チャンネルおよび国設定を含む 802.11b/g/n および 802.11a/n ワイヤレス設定を行う必要があります。ネットワークに接続するために、ワイヤレスデバイスの基本ワイヤレス設定を正しく設定する必要があります。

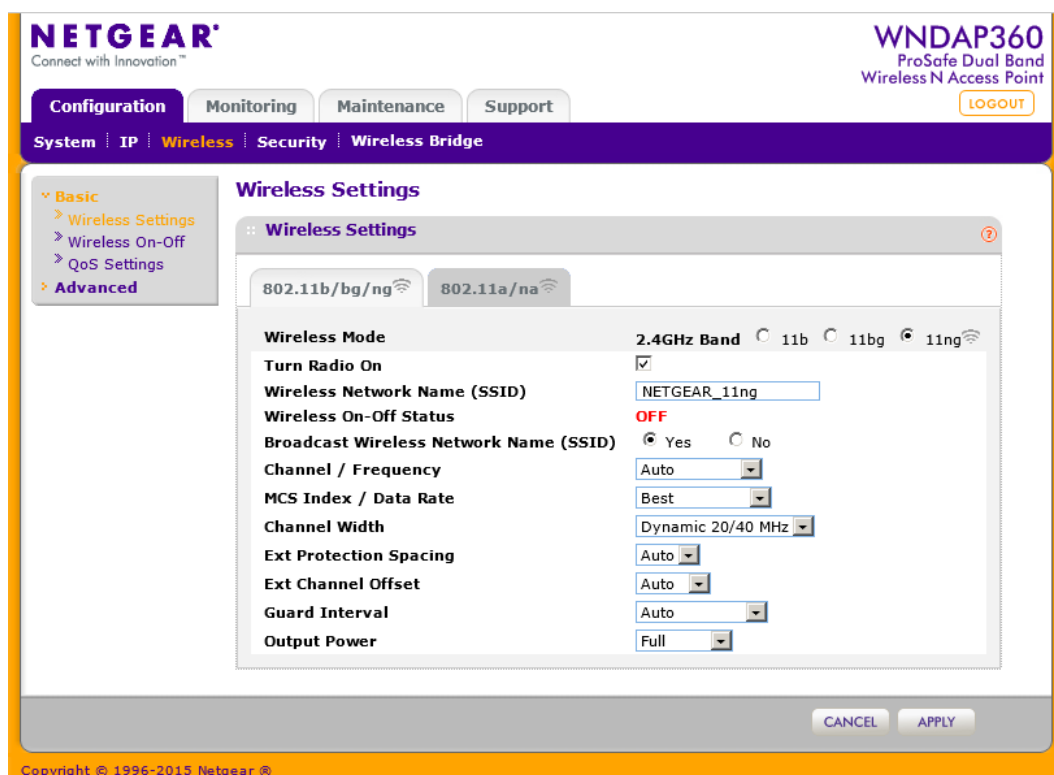


警告

ワイヤレスアクセスポイントをワイヤレスコンピューターから設定し、ワイヤレスアクセスポイントの SSID やワイヤレスセキュリティ設定を変更して、Apply ボタンをクリックすると、ワイヤレス接続を失います。新しいワイヤレスアクセスポイントの設定に合わせてコンピューターのワイヤレス設定を変更する必要があります。

802.11b/bg/ng ワイヤレス設定を行う

1. Configuration > Wireless > Basic > Wireless Settings を選択して Wireless Settings 画面を表示します。(以下の図は 802.11ng 設定画面です)



2. 2.4GHz バンドでのワイヤレスモードをラジオボタンで選択します。
 - 11b: 802.11b モードに設定します。バックワードコンパチブルな 802.11n と 802.11g デバイスも接続可能です。
 - 11bg: 802.11bg モードに設定します。バックワードコンパチブルな 802.11n デバイスも接続可能です。
 - 11ng: (デフォルト設定) 802.11ng モードに設定します。802.11b デバイスは接続できません。

ワイヤレスモードを変更すると、Turn Radio On チェックボックスは自動的にクリアされ、すべての設定項目がグレーアウトされます。

3. Turn Radio On: チェックボックスを選択するとポップアップスクリーンが表示されます。

メモ: 通常は電波をオンにしたいと思いますが、電波を止めることは設定やネットワークチューニングやトラブルシューティングには役に立ちます。

5. OK ボタンをクリックしてワイヤレスモードの変更を確認します。変更は設定終了して Apply ボタンをクリックするまでは有効になりません。
6. 残りの項目を設定します。

項目	説明	
Wireless Network Name (SSID)	最大32文字の SSID を設定します。大文字と小文字は区別されます。デフォルトは NETGEAR_11ng です。	
Wireless On-Off Status	ワイヤレスの状態を示します。	
Broadcast Wireless Network Name (SSID)	Yes: SSID をブロードキャストします。 No: SSID をブロードキャストしません。	
Channel / Frequency	チャンネル/周波数を選択します。デフォルトは Auto です。チャンネル/周波数は国設定とワイヤレスモードによって異なります。 メモ: 干渉等が発生しないかぎり変更する必要はありません。	
11ng モードの時のみ メモ: ほとんどの場合、デフォルト設定で問題ありません。	MCS Index / Data Rate	ドロップダウンリストから MCS (Modulation and Coding Scheme) index と無線データレートを選択します。デフォルトは Best です。
	Channel Width	チャンネル帯域幅を選択します。
	Ext Protection Spacing	チャンネル帯域幅で Dynamic 20/40 MHz または 40 MHz を選択すると設定できます。デフォルトの Auto に加えて 20 または 25 を選択できます。 メモ: Channel Width が 20MHz の場合は選択できません。
	Ext Channel Offset	チャンネル帯域幅で Dynamic 20/40 MHz または 40 MHz を選択すると設定できます。デフォルトの Auto に加えて Upper または Lower を選択できます。 メモ: Channel Width が 20MHz の場合は選択できません。

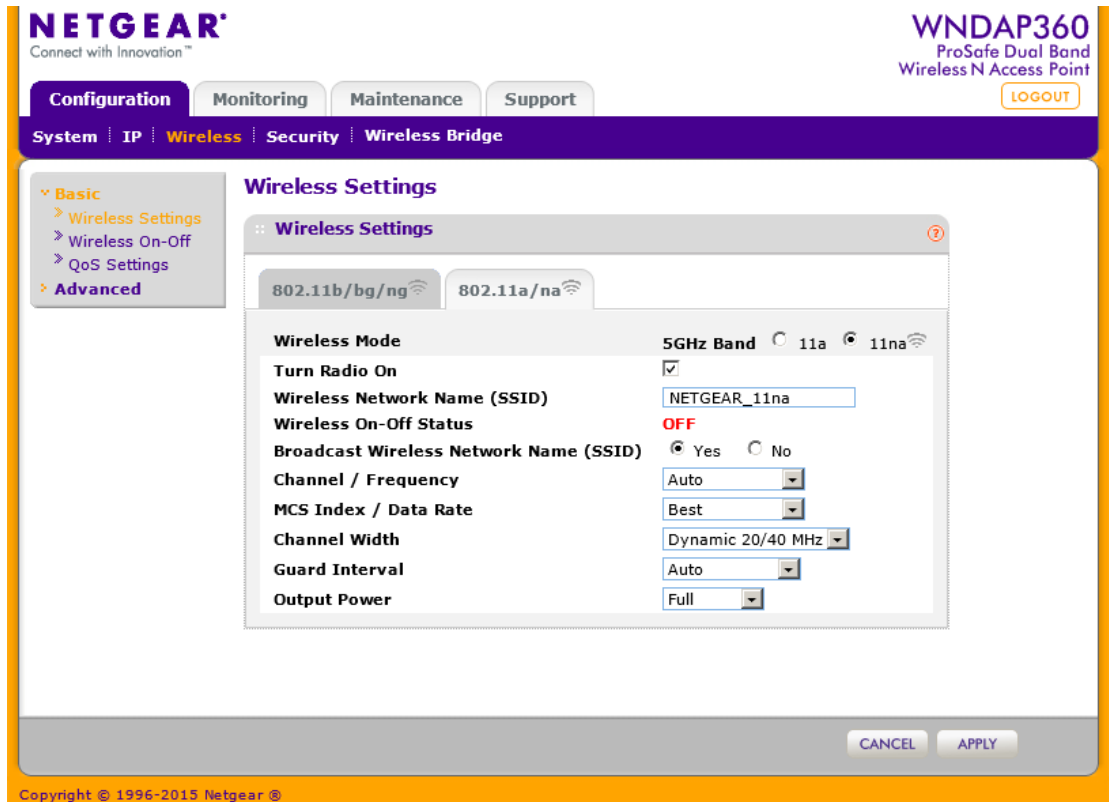
	Guard Interval	干渉から送信を保護するためにガードインターバルを選択します。デフォルトの Auto に加えて Long - 800 ns を選択できます。いくつかのレガシーデバイスは Long ガードインターバルのみで動作します。
11b と 11bg モードの時のみ	Data Rate	ドロップダウンリストから無線データレートを選択します。デフォルトは Best です。
Output Power		送信出力をドロップダウンリストから選択します。選択肢は Full, Half, Quarter, Eighth, Minimum です。デフォルトは Full です。 メモ: 出力を大きくすればパフォーマンスは改善しますが、同じエリアに同じチャンネルで動作しているアクセスポイントが複数ある場合は干渉が発生します。 メモ: お使いの国の出力規制に適合するようにしてください。

4. **Apply** ボタンをクリックして設定を保存して選択したワイヤレスモードを有効にします。

メモ: 電波アイコン (📶) は有効なワイヤレスモードを示します。

802.11a/na ワイヤレス設定を行う

1. Configuration > Wireless > Basic > Wireless Settings を選択して Wireless Settings 画面を表示します。(以下の図は 802.11na 設定画面です)



2. 5GHzバンドのワイヤレスモードラジオボタンで選択します。
 - 11a:802.11a モードに設定します。バックワードコンパチブルな 802.11n デバイスも接続可能です。
 - 11na:(デフォルト設定)802.11na モードに設定します。

ワイヤレスモードを変更すると、Turn Radio On チェックボックスは自動的にクリアされ、すべての設定項目がグレースアウトされます。

3. Turn Radio On: チェックボックスを選択するとポップアップスクリーンが表示されます。

メモ: 通常は電波をオンにしたいと思いますが、電波を止めることは設定やネットワークチューニングやトラブルシューティングには役に立ちます。
4. OK ボタンをクリックしてワイヤレスモードの変更を確認します。変更は設定終了して Apply ボタンをクリックするまでは有効になりません。
5. 残りの項目を設定します。

項目	説明
----	----

Wireless Network Name (SSID)	最大32文字の SSID を設定します。大文字と小文字は区別されません。デフォルトは NETGEAR_11ng です。	
Wireless On-Off Status	ワイヤレスの状態を示します。	
Broadcast Wireless Network Name (SSID)	Yes: SSID をブロードキャストします。 No: SSID をブロードキャストしません。	
Channel / Frequency	チャンネル/周波数を選択します。デフォルトは Auto です。チャンネル/周波数は国設定とワイヤレスモードによって異なります。 メモ: 干渉等が発生しないかぎり変更する必要はありません。	
11na モードの時のみ メモ: ほとんどの場合、デフォルト設定で問題ありません。	MCS Index / Data Rate	ドロップダウンリストから MCS (Modulation and Coding Scheme) index と無線データレートを選択します。デフォルトは Best です。
	Channel Width	チャンネル帯域幅を選択します。
	Guard Interval	干渉から送信を保護するためにガードインターバルを選択します。デフォルトの Auto に加えて Long - 800 ns を選択できます。いくつかのレガシーデバイスは Long ガードインターバルのみで動作します。
11a モードの時のみ	Data Rate	ドロップダウンリストから無線データレートを選択します。デフォルトは Best です。
Output Power	送信出力をドロップダウンリストから選択します。選択しは Full, Half, Quarter, Eighth, Minimum です。デフォルトは Full です。 メモ: 出力を大きくすればパフォーマンスは改善しますが、同じエリアに同じチャンネルで動作しているアクセスポイントが複数ある場合は干渉が発生します。 メモ: お使いの国の出力規制に適合するようにしてください。	

6. Apply ボタンをクリックして設定を保存して選択したワイヤレスモードを有効にします。

メモ: 電波アイコン (📶) は有効なワイヤレスモードを示します。

運用周波数(チャンネル)ガイドライン

干渉がある場合やワイヤレスアクセスポイントを他のワイヤレスアクセスポイントの近くに設置する場合以外は運用周波数(チャンネル)を変更すべきではありません。以下のガイドラインに従ってください。

- ワイヤレスアクセスポイントを固定チャンネルで使う。干渉の少なく最大のパフォーマンスが得られるチャンネルを選択します。
- 複数のワイヤレスアクセスポイントを使っているならば、干渉を減らすために隣接したワイヤレスアクセスポイントは異なるチャンネルを使うようにします。2.4GHz ではチャンネル間は5チャンネル間隔を開けることを推奨します。(例:1チャンネルと6チャンネル)
- インフラストラクチャーモードでは、ワイヤレスステーションは通常すべてのチャンネルをスキャンしてワイヤレスアクセスポイントを探索します。複数のワイヤレスアクセスポイントが使われるとき、一番信号が強いものが使われます。これはワイヤレスアクセスポイントが同じSSIDを使う場合に発生します。WNDAP360 はデフォルトがインフラストラクチャーモードです。

基本ワイヤレス接続をテストする

前章に従ってワイヤレスアクセスポイントを設定した後で、ワイヤレスアクセスポイントを設置する前にお使いのコンピューターでワイヤレス接続をテストします。

ワイヤレス接続をテストする

1. お使いのコンピューターの 802.11b/g/n と 802.11a/n ワイヤレスアダプターにワイヤレスアクセスポイントと同じ SSID とチャンネルを設定します。
2. コンピューターがワイヤレスアクセスポイントへのワイヤレスリンクを持っているかを確認し、ワイヤレスアクセスポイントで DHCP サーバーを有効にしているならば、ワイヤレスアクセスポイントの DHCP サーバーから IP アドレスが割り当てられるかどうかを確認します。
3. Web ブラウザーでインターネットに接続されていることを確認するか、プリンターやファイルにアクセスできるかを確認します。



警告

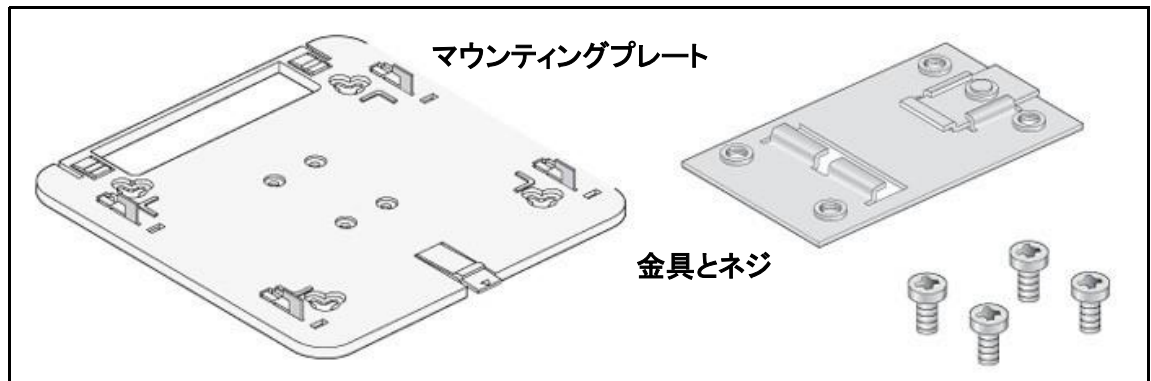
ワイヤレスアクセスポイントをネットワークに設置する前にワイヤレスセキュリティその他の設定をします。

ワイヤレスアクセスポイントを設置する

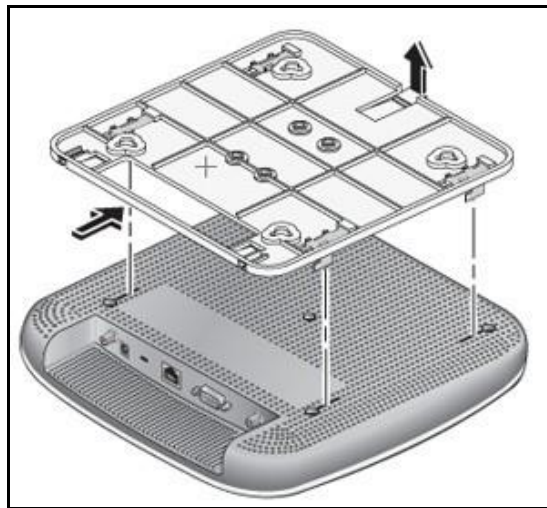
天井取り付け

天井取付キットを使ってワイヤレスアクセスポイントを取り付ける

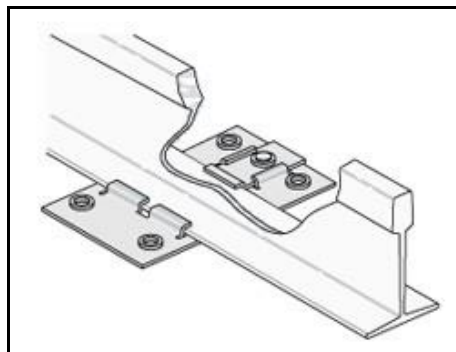
1. 天井取付キットを確認します。



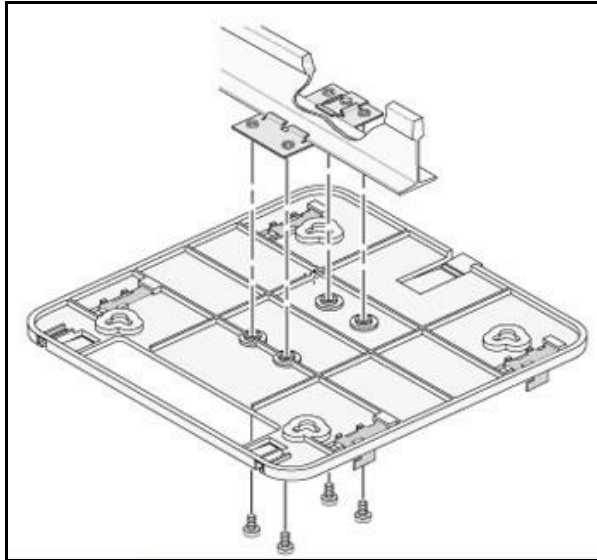
2. マウンティングプレートをワイヤレスアクセスポイントから取り外します。



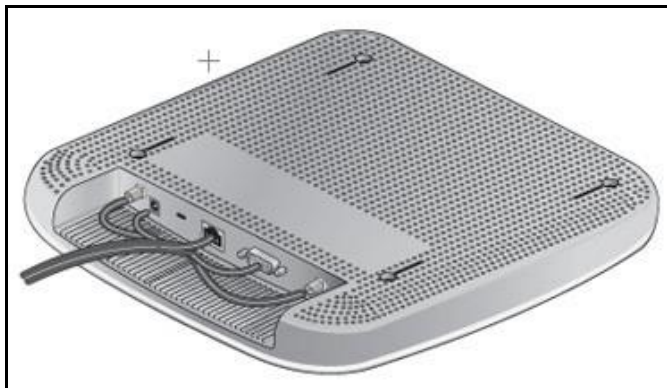
3. 金具を天井レールに取り付けます。



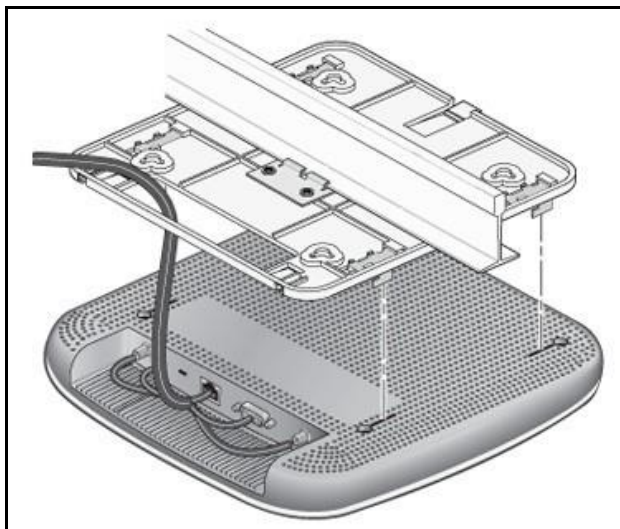
4. マウンティングプレートを金具に取り付けます。



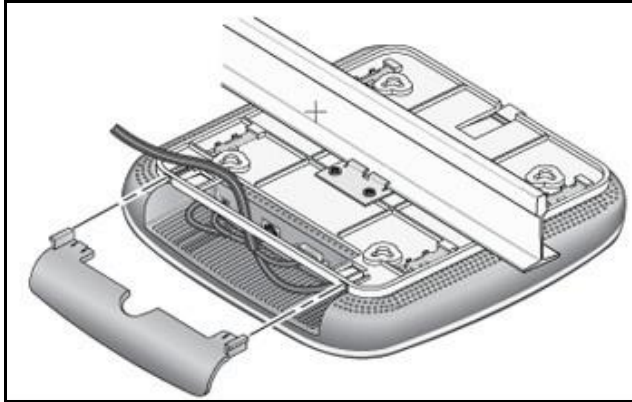
5. ケーブルをワイヤレスアクセスポイントに取り付けます



6. ワイヤレスアクセスポイントをマウンティングプレートに取り付けます。



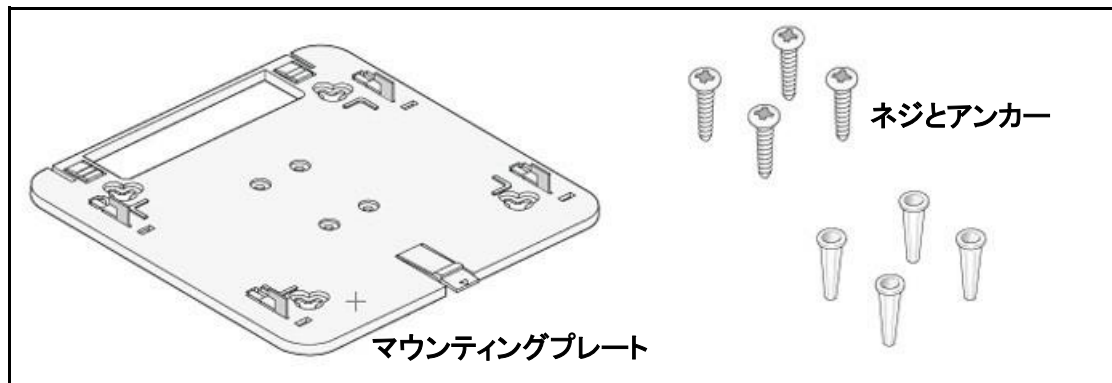
7. カバーをワイヤレスアクセスポイントに取り付けます。



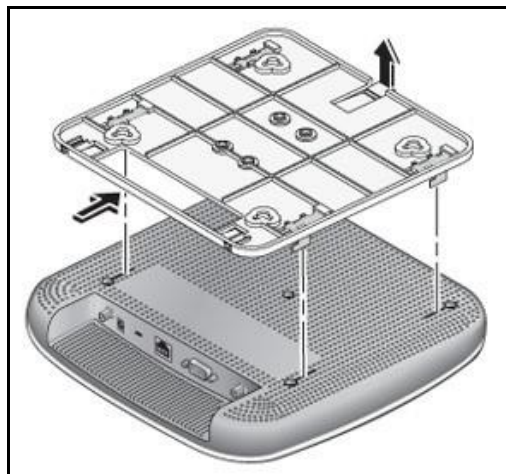
壁面取り付け

壁面取付キットを使ってワイヤレスアクセスポイントを取り付ける

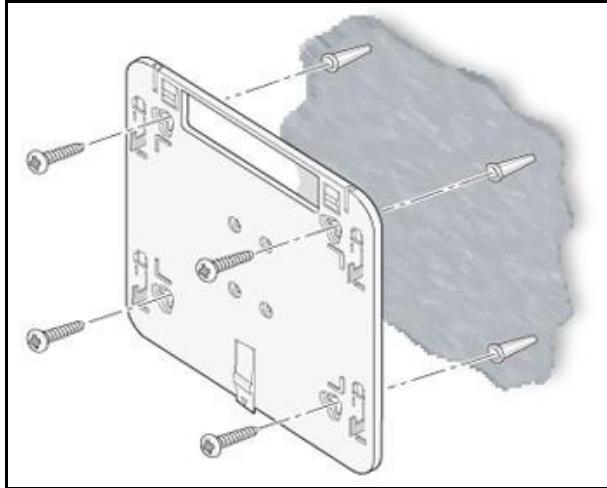
1. 壁面取付キットを確認します。



2. マウンティングプレートをワイヤレスアクセスポイントから取り外します。



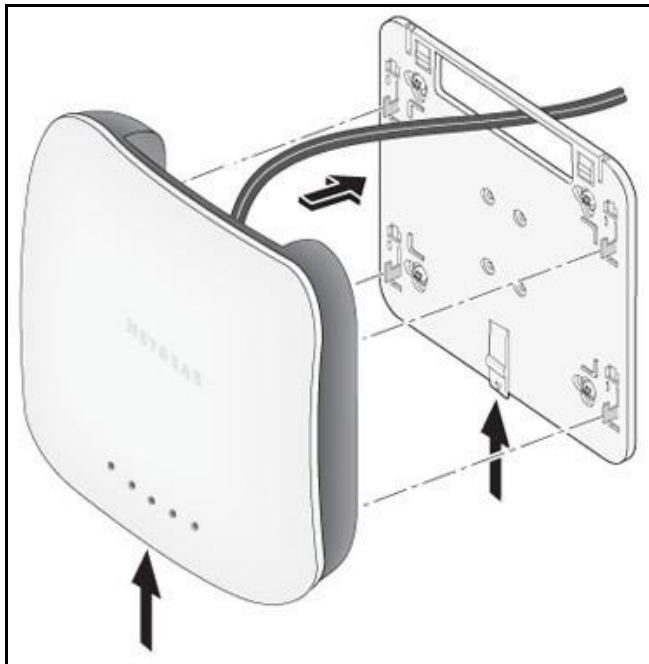
3. マウンティングプレートを壁に取り付けます。



4 ケーブルをワイヤレスアクセスポイントに取り付けます



5. ワイヤレスアクセスポイントをマウンティングプレートに取り付けます。



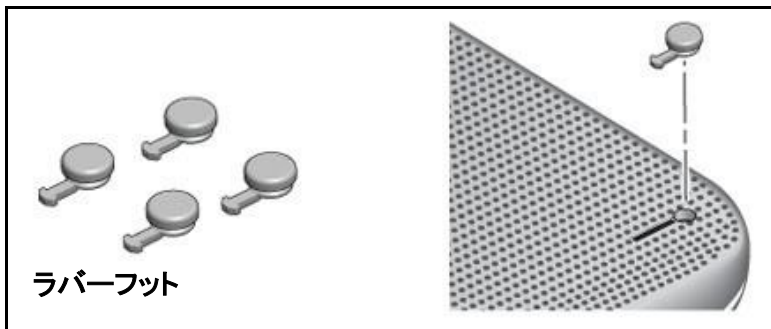
6. カバーをワイヤレスアクセスポイントに取り付けます。



机に取り付ける

ワイヤレスアクセスポイントを机に取り付ける

ラバーフットをワイヤレスアクセスポイントの底の穴に取り付けます。



ワイヤレス設定とセキュリティ

この章では WNDAP360 のワイヤレス機能の設定方法について記します。

ワイヤレスセキュリティと追加のワイヤレス機能を設定する前に、ワイヤレスアクセスポイントがイーサネットネットワークに接続され、802.11b, 802.11bg, 802.11ng, 802.11a, 802.11na のワイヤレス設定をしておきます。ワイヤレスネットワークを計画するには、必要とするセキュリティレベルを検討します。



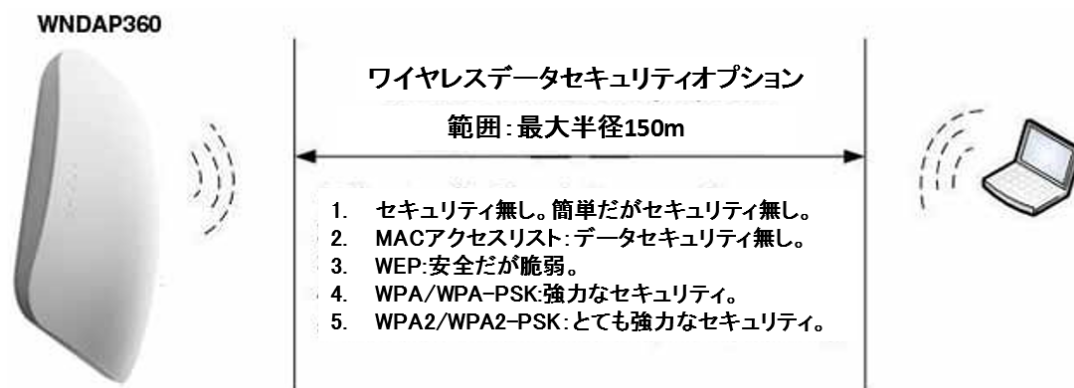
警告

ワイヤレスアクセスポイントをワイヤレスコンピューターから設定し、ワイヤレスアクセスポイントの SSID やチャンネル、ワイヤレスセキュリティ設定を変更して、Apply ボタンをクリックすると、ワイヤレス接続を失います。新しいワイヤレスアクセスポイントの設定に合わせてコンピューターのワイヤレス設定を変更する必要があります。

ワイヤレスデータセキュリティオプション

屋内ではコンピューターは 802.11n ワイヤレスネットワークで最大約 90 メートル離れて通信が可能です。一般的に、建物内では半径 30 メートル以内が最適です。

有線ネットワークデータとは異なり、ワイヤレスデータは壁を超えて伝わり、適合するアダプターを持っている機器はデータを受信することができます。ワイヤレスアクセスポイントはこの章でカバーされている有効なセキュリティ機能を提供します。お使いのネットワークに適したセキュリティを使います。



お使いのワイヤレスネットワークのセキュリティを高める方法がいくつかあります。

- **VLAN とともに複数の BSSID を使う:** VLAN と BSSID (セキュリティプロファイル) およびアクセスセキュリティを組み合わせて設定します。たとえば、訪問者にはワイヤレスインターネットアクセスは提供されるが、内部のネットワークへのアクセスは排除されます。

- **MAC アドレスでアクセスを制限する:**信頼できる PC のみを接続させることで不明な PC はワイヤレスアクセスポイントに接続できません。MAC アドレスでのアクセス制限はネットワークへの不要なアクセスは防ぐことはできるが、ワイヤレスネットワークでのデータブロードキャストは晒されたものとなっています。
- **ワイヤレスネットワーク名 (SSID) のブロードキャストを停止する:**SSID のブロードキャストを停止すると、正しい SSID を持っているデバイスのみが接続可能となります。これによって Windows XP のようないくつかの機器のワイヤレスネットワークディスカバリーは無効となりますが、データが晒される問題はまだ存在します。
- **WEP:**容易に解読されるようになり、WPA-PSK および WPA2-PSK に置き換えられています。
- **レガシー802.1X:**レガシー802.1X は RADIUS ベースの 802.1x 認証を使いますが、データの暗号化はありません。
- **WPA と WPA-PSK (TKIP):**WPA(Wi-Fi Protected Access)は強力なデータセキュリティを TKIP(Temporal Key Integrity Protocol)暗号化で提供します。
WPA は RADIUS ベースの 802.1x 認証を使います。
WPA-PSK は共有キー(PSK)を認証に使います。
- **WPA2 and WPA2-PSK (AES) :**WPA2(Wi-Fi Protected Access version 2)は強力なデータセキュリティを AES(Advanced Encryption Standard)暗号化で提供します。
WPA2 は RADIUS ベースの 802.1x 認証を使います。
WPA2-PSK は共有キー(PSK)を認証に使います。
- **WPA & WPA2 and WPA-PSK & WPA2-PSK mixed modes:**WPA/WPA2 および WPA-PSK/WPA2-PSK を使用します。

セキュリティプロファイル

セキュリティプロファイルで各周波数帯の SSID 毎に異なるセキュリティ設定をすることができます。各周波数帯でワイヤレスアクセスポイントは最大 8 つのセキュリティプロファイル(BSSID)をサポートします。

セキュリティプロファイルを設定するには、ネットワーク認証タイプ、データ暗号化、ワイヤレスクライアントセキュリティセパレーション、と VLAN ID を選択します。

- **ネットワーク認証**
ワイヤレスアクセスポイントはデフォルトでは認証なしのオープンシステムとなっています。ネットワーク認証を設定する時、すべてのワイヤレスアダプターが WPA または WPA2 をサポートしていないことに留意してください。
- **データ暗号化**
使用したいデータ暗号化を選択してください。デフォルトでは暗号化はなし(None)となっています。
- **ワイヤレスクライアントセキュリティセパレーション (Wireless client security separation)**

有効にすると、同じ SSID を利用するクライアント間で直接通信はできません。この機能はホットスポットのような公共でのアクセスの場合に役に立ちます。デフォルトは無効です。

- **VLAN ID**

有効にして LAN のネットワークデバイス(ハブやスイッチ)が VLAN(802.1Q)をサポートしているなら、ワイヤレスアクセスポイントのデフォルト VLAN ID は各プロファイルと関連付けられます。デフォルト VLAN ID は他のネットワークデバイスの ID と一致する必要があります。

SSID に関するいくつかの概念とガイドラインについては以下のリストで説明します。

- BSS(basic service set)はいくつかのワイヤレス端末と一つのワイヤレスアクセスポイントのグループであり、同じセキュリティプロファイルあるいは同じ BSSID を使います。実際の BSSID の ID はワイヤレス電波の MAC アドレスです。(ワイヤレスラジオはセキュリティプロファイル毎に MAC アドレスを持つことができます。)
- ESS(extended service set)は同じ ID(ESSID)を持つワイヤレス端末と複数のワイヤレスアクセスポイントのグループです。
- 一つの ESS 内の異なるワイヤレスアクセスポイントは異なるチャンネルを使うことができます。干渉を防ぐために、隣接したワイヤレスアクセスポイントは異なるチャンネルを使用すべきです。
- ローミングは同じ ESS 内で一つの BSS から他の BSS へ物理的に移動するときにワイヤレスで接続する能力です。ワイヤレス端末は自動的に最小の干渉または最良のパフォーマンスでワイヤレスアクセスポイントを移動します。

SSID,WEP,WPA 設定を変更する前に

新しいワイヤレスネットワークのために、以下のシートを印刷、コピーして設定を記入してください。既存のワイヤレスネットワークではネットワーク管理者はこの情報を提供できます。まず国情報を入手してください。

802.11b/bg/ng モード用シート

安全な場所にこの情報を保管してください。

- **SSID:** ワイヤレスローカルエリアネットワークの識別をします。最大 32 文字の英数字で設定できます。
- 下線部分に SSID を記入してください。

SSID: _____

ワイヤレスアクセスポイントの SSID はワイヤレスアダプターカードに設定する SSID です。同じネットワークのすべてのワイヤレス端末は同じ SSID を設定します。

- **WEP Key Size, Key Format Passphrase, and Authentication**

以下の Key サイズを選択します。

(64, 128, 152 ビット)

Key フォーマットを選択します。

(ASCII, HEX)

認証タイプ (Authentication Type) を選択します。

(Open, Shared)

パスフレーズ (Passphrase) を記入します。

- **WPA-PSK (Pre-Shared Key) と WPA2-PSK**

WPA-PSK パスフレーズを記録します

WPA-PSK Passphrase: _____

WPA-PSK パスフレーズを記録します

WPA2-PSK Passphrase: _____

- **WPA RADIUS 設定**

Primary RADIUS サーバー情報と Secondary RADIUS サーバー情報を記録します。

Primary Server Name/IP Address: _____

Secondary Server Name/IP Address: _____

Port: _____

Shared Secret: _____

- **WPA2 RADIUS 設定**

Primary RADIUS サーバー情報と Secondary RADIUS サーバー情報を記録します。

Primary Server Name/IP Address: _____

Secondary Server Name/IP Address: _____

Port: _____

Shared Secret: _____

802.11a/an モード用シート

安全な場所にこの情報を保管してください。

- **SSID:** ワイヤレスローカルエリアネットワークの識別をします。最大 32 文字の英数字で設定できます。
- 下線部分に SSID を記入してください。

SSID: _____

ワイヤレスアクセスポイントの SSID はワイヤレスアダプターカードに設定する SSID です。同じネットワークのすべてのワイヤレス端末は同じ SSID を設定します。

- **WEP Key Size, Key Format Passphrase, and Authentication**

以下の Key サイズを選択します。

(64, 128, 152 ビット)

Key フォーマットを選択します。

(ASCII, HEX)

認証タイプ (Authentication Type) を選択します。

(Open, Shared)

パスフレーズ (Passphrase) を記入します。

- **WPA-PSK (Pre-Shared Key) と WPA2-PSK**

WPA-PSK パスフレーズを記録します

WPA-PSK Passphrase: _____

WPA-PSK パスフレーズを記録します

WPA2-PSK Passphrase: _____

- **WPA RADIUS 設定**

Primary RADIUS サーバー情報と Secondary RADIUS サーバー情報を記録します。

Primary Server Name/IP Address: _____

Secondary Server Name/IP Address: _____

Port: _____

Shared Secret: _____

- **WPA2 RADIUS 設定**

Primary RADIUS サーバー情報と Secondary RADIUS サーバー情報を記録します。

Primary Server Name/IP Address: _____

Secondary Server Name/IP Address: _____

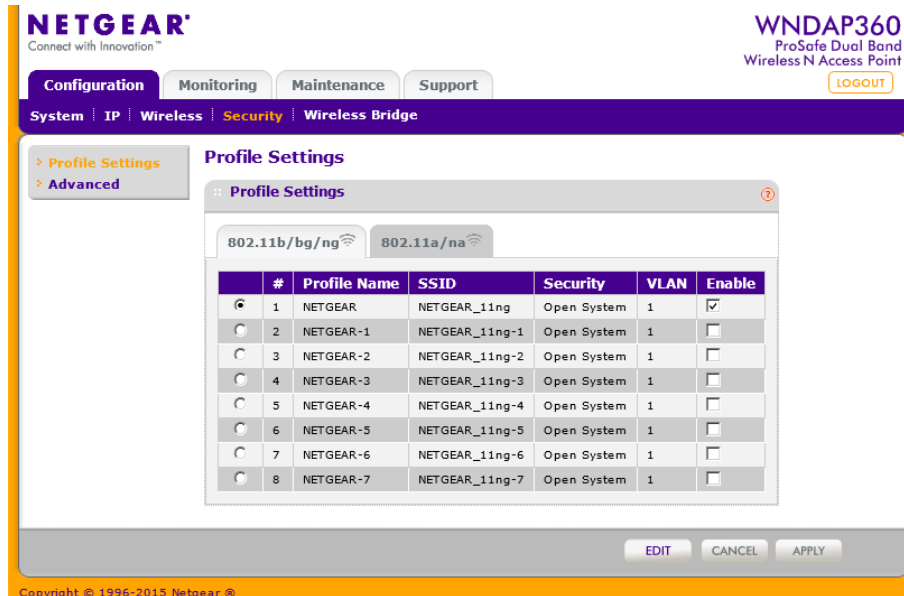
Port: _____

Shared Secret: _____

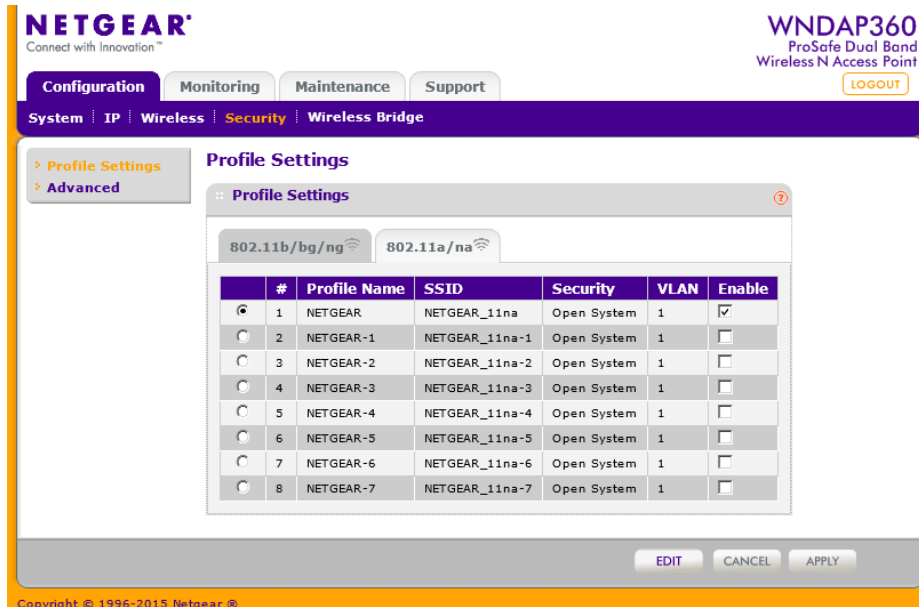
セキュリティプロファイルの設定と有効化

セキュリティプロファイルを設定し有効にする

1. Configuration > Security > Profile Settings を選択して Profile Settings 画面を表示します。802.11b/bg/ng モードの 8 つのセキュリティプロファイルが表示されます。



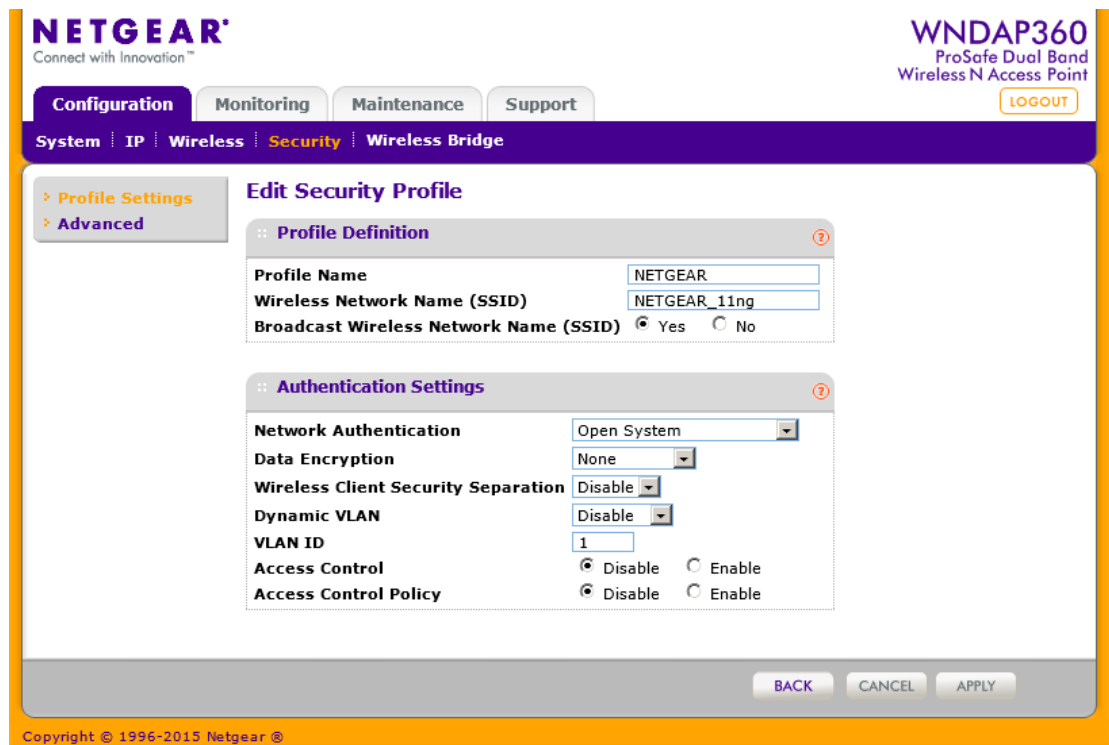
2. 802.11a/na モードのセキュリティプロファイルを表示するには、802.11a/na タブをクリックします。



Profile Settings 画面の項目の説明を以下に記します。

項目	説明
Profile Name	セキュリティプロファイル名。
SSID	セキュリティプロファイルのワイヤレスネットワーク名 (SSID)。
Security	設定されたワイヤレス認証方式。
VLAN	セキュリティプロファイルに関連付けられるデフォルト VLAN ID。
Enable	Apply チェックボックスをクリックしてセキュリティプロファイルを有効にします。

3. ワイヤレスセキュリティプロファイルを設定するには、設定するセキュリティプロファイルの左側のラジオボタンをクリックし Edit ボタンをクリックします。選択したセキュリティプロファイルの Edit Security Profile 画面が表示されます。



4. Profile Definition 欄の設定をします。

項目	説明
Profile Name	認識しやすいようなワイヤレスセキュリティプロファイル名を指定します。デフォルトは NETGEAR, NETGEAR-1, NETGEAR-2, …NETGEAR-7 です。英数字 32 文字まで設定可能です。

Wireless Network Name (SSID)	<p>ワイヤレスセキュリティプロファイルに対応したワイヤレスネットワーク名 (DSSID) を指定します。デフォルトは周波数帯に応じて設定されています。</p> <ul style="list-style-type: none"> • 802.11b/bg/ng: デフォルト名は NETGEAR_11ng, NETGEAR_11ng-1, NETGEAR_11ng-2, ~NETGEAR_11ng-7。 • 802.11a/na: デフォルト名は NETGEAR_11na, NETGEAR_11na-1, NETGEAR_11na-2, ~NETGEAR_11na-7。
Broadcast Wireless Network Name (SSID)	Yes ラジオボタンを押してワイヤレスアクセスポイントが SSID をブロードキャストします。デフォルトは Yes です。

5. Authentication Settings 欄の設定をします。

ワイヤレスアクセスポイントはデフォルトでは Open System で認証がありません。ネットワーク認証を設定するには以下の点を考慮してください。

- アクセスポイントモード(デフォルト)でお使いの場合、すべての設定が可能です。ブリッジモードの場合、いくつかの選択肢は選択できません。

すべてのワイヤレスアダプターが WPA や WPA2 をサポートしているわけではありません。

項目	説明	
Network Authentication と Data Encryption メモ: 画面に表示される Data Encryption 欄は Network Authentication の選択により変化します。	Open System	デフォルト設定。暗号化なし。
	Shared Key	WEP 暗号化で最低一つの共有キーを設定します。
	Legacy 802.1X	RADIUS サーバーを使用します。
	WPA with Radius	WPA で RADIUS サーバーを使用します。
	WPA2 with Radius	WPA2 で RADIUS サーバーを使用します。
	WPA & WPA2 with Radius	WPA/WPA2 で RADIUS サーバーを使用します。
	WPA-PSK	WPA-PSK を使用します。
	WPA2-PSK	WPA2-PSK を使用します。
	WPA-PSK & WPA2-PSK	WPA-PSK および WPA2-PSK を使用します。
Wireless Client Security Separation	この機能を有効(Enable)にすると、ワイヤレスクライアントセキュリティが有効になり、ワイヤレスクライアント間の直接通信はできなくなります。この機能はホットスポット等の公共でのアクセスに有効です。	

<p>Dynamic VLAN</p>	<p>ドロップダウンリストで VLAN の動作を選択します。</p> <ul style="list-style-type: none"> • Disable: ダイナミック VLAN を無効にしてスタティック VLAN を使います。これがデフォルト設定です。 • Optional: ダイナミック VLAN を有効にします。RADIUS サーバーが VLAN ID を返してこない場合でもワイヤレスデバイスはワイヤレスアクセスポイントに接続されます。 • Required: ダイナミック VLAN を有効にします。RADIUS サーバーが VLAN ID を返さなかった場合は、ワイヤレス端末は認証されずにワイヤレスアクセスポイントには接続されません。 <p>ダイナミック VLAN を運用するには(選択は Optional または Required)、以下の条件を満たす必要があります。</p> <ul style="list-style-type: none"> • ネットワークのスイッチは 802.1Q VLAN をサポートする必要があります。 • 認証はワイヤレスセキュリティプロファイルのネットワーク認証あるいは MAC アドレス認証機能のリモート MAC アドレス認証の RADIUS 認証タイプに設定します。
<p>VLAN ID</p>	<p>このワイヤレスセキュリティプロファイルに関連付けるデフォルト VLAN ID を指定します。デフォルト VLAN ID は1です。VLAN ID はネットワークの他のデバイスが使っている VLAN ID と一致する必要があります。</p>
<p>Access Control</p>	<p>メモ: アクセスコントロール (Access Control) 機能はスタティック VLAN が有効にされた時のみ動作します。すなわち、ダイナミック VLAN ドロップダウンリストで Disable を選択した時のみです。</p> <p>Access Control ラジオボタンでクライアントがワイヤレスアクセスポイントを介して正しい VLAN に接続出来るように RADIUS サーバーを介したアクセスコントロールを有効、無効にします。</p> <ul style="list-style-type: none"> • Disable: アクセスコントロールを無効にします。デフォルト設定。 • Enable: アクセスコントロールを有効にします。クライアントは RADIUS サーバーを介して認証されます。
<p>Access Control Policy</p>	<p>アクセスコントロールが有効にされた時、アクセスコントロールポリシーによって、VLAN ID が正しくない場合にクライアントが認証されなかった場合に、クライアントがワイヤレスアクセスポイントにアクセス出来るかどうかを指定します。</p> <p>ラジオボタンで有効(enable)、無効(disable)を選択します。</p> <ul style="list-style-type: none"> • Disable: RADIUS サーバーがクライアントを認証しなかった時、ワイヤレスアクセスポイントは RADIUS サーバーによって割り当てられる VLAN ではなく、デフォルト VLAN にアクセスすることを許可します。

- **Enable:** RADIUS サーバーがクライアントを認証しなかった時、クライアントはワイヤレスアクセスポイントに接続できません。

6. Apply ボタンをクリックして設定を保存します。



警告

ワイヤレスアクセスポイントをワイヤレスコンピューターから設定し、ワイヤレスアクセスポイントの SSID やワイヤレスセキュリティ設定を変更して、Apply ボタンをクリックすると、ワイヤレス接続を失います。新しいワイヤレスアクセスポイントの設定に合わせてコンピューターのワイヤレス設定を変更する必要があります。

Open System を WEP または WEP Shared KEY で設定する

Open System を WEP または WEP Shared KEY で設定するには以下の表の情報を設定します。

- **Open System で WEP**

Open system は暗号化なしあるいは RADIUS 認証を使わない pre-shared WEP Key での暗号化で機能します。WEP のセキュリティレベルは高くありません。

Network Authentication ドロップダウンリストで **Open System** を選択し、Data Encryption ドロップダウンリストで None 以外を選択すると、以下のような設定画面が表示されます。

- **WEP shared key**

Shared key は RADIUS 認証無しに pre-shared WEP key 暗号化を提供します。セキュリティレベルは高くありません。Network Authentication ドロップダウンリストから **Shared Key** を



選択すると、以下の画面が表示されます。

項目	説明
Data Encryption	<p>暗号化の鍵の長さを選択します。</p> <ul style="list-style-type: none"> • 64-bit WEP: 40/64 ビットの WEP 鍵。 • 128-bit WEP: 104/128 ビットの WEP 鍵。 • 152-bit WEP: 128+24 ビットの WEP 鍵。このモードはこのモードをサポートしている端末とのみ利用可能です。
Passphrase	<p>パスフレーズを入力します。パスフレーズ長は 8-63 文字です。Generate Keys をクリックすることによって Secret passphrase から自動的に Key を作成することができます。デフォルトの Passphrase は "sharedsecret" です。</p> <p>You can display the actual passphrase by selecting the Show Passphrase in Clear Text ラジオボタンを押すことによって passphrase を表示することができます。</p>
Encryption Key (Key1-Key4)	<p>Generate Key をクリックすることによって自動的に生成された Key または手動で入力した Key を使います。</p> <ul style="list-style-type: none"> • ASCII 形式の場合は鍵の長さに応じて 10 文字 (64-bit WEP)、26 文字 (128-bit WEP)、32 文字 (152-bit WEP) の英数字を使います。 • HEX 形式の場合は鍵の長さに応じて 5 文字 (64-bit WEP)、13 文字 (128-bit WEP)、16 文字 (152-bit WEP) の 16 進数を使います。 <p>メモ: ワイヤレス端末はワイヤレスアクセスポイントに接続するために Key を使います。</p> <p>メモ: すべてのワイヤレスアダプターがパスフレーズからの Key 生成をサポートしているとは限りません。</p>
Show Passphrase in Clear Text	<p>Yes ラジオボタンを選択すると Passphrase 欄のパスフレーズを表示することができます。</p>

レガシー802.1Xを設定する

レガシー802.1X セキュリティを使うためには、RADIUS サーバー設定をする必要があります。

Network Authentication ドロップダウンリストから **Legacy 802.1X** を選択すると、Data Encryption ドロップダウンリストは設定不可になります。Legacy 802.1X セキュリティを使うためには、RADIUS サーバー設定のみが必要です。



WPA with RADIUS、WPA2 with RADIUS、WPA & WPA2 with RADIUS を設定する

WPA, WPA2, および WPA & WPA2 セキュリティは RADIUS ベースの 802.1X 認証が必要であり、RADIUS サーバー設定をする必要があります。

Data Encryption ドロップダウンリストでの選択肢は Network Authentication ドロップダウンリストから選択した WPA 認証タイプにより異なります。項目については次の表に示します。

WPA with RADIUS



- WPA2 with RADIUS



- WPA & WPA2 with RADIUS



項目	説明
TKIP	TKIP(Temporal Key Integrity Protocol)は WPA とともに用いられる標準暗号化方式です。WPA2 とともに使うことも可能です。 メモ: TKIP はレガシー(低速、最大 54Mbps)な速度の動作のみを提供します。802.11n の速度を使うには WPA と AES を使うことを推奨します。
AES	AES(Advanced Encryption Standard) は WPA2 とともに用いられる標準暗号化方式です。 メモ: WPA と AES をサポートしているワイヤレスアクセスポイントもありますが、WNDAP360 は WPA と AES の組み合わせには対応しておりません。
TKIP + AES	TKIP + AES 暗号化方式は WPA と WPA2 でサポートされています。ブロードキャストパケットは TKIP を使います。ユニキャスト(ポイント・ポイント)転送には WPA クライアントは TKIP,WPA2 クライアントは AES を使います。WPA & WPA2 Mixed モードでは TKIP+AES のみがサポートされている暗号化方式です。

WPA-PSK, WPA2-PSK, および WPA-PSK & WPA2-PSK を設定する

WPA-PSK, WPA-PSK, および WPA-PSK & WPA2-PSK 認証は PSK(事前共有鍵)を使い、RADIUS サーバーの認証を必要としません。

Data Encryption ドロップダウンリストの選択肢は WPA-PSK 認証タイプによって異なります。

- WPA-PSK

Authentication Settings

Network Authentication: WPA-PSK

Data Encryption: TKIP

WPA Passphrase (Network Key): *****

Show Passphrase in Clear Text: No Yes

- WPA2-PSK

Authentication Settings

Network Authentication: WPA2-PSK

Data Encryption: AES

WPA Passphrase (Network Key): *****

Show Passphrase in Clear Text: No Yes

- WPA-PSK & WPA2-PSK

Authentication Settings

Network Authentication: WPA-PSK & WPA2-PSK

Data Encryption: TKIP + AES

WPA Passphrase (Network Key): *****

Show Passphrase in Clear Text: No Yes

項目	説明	
Data Encryption	TKIP	<p>TKIP(Temporal Key Integrity Protocol)は WPA とともに用いられる標準暗号化方式です。WPA2 とともに使うことも可能です。</p> <p>メモ: TKIP はレガシー(低速、最大 54Mbps)な速度の動作のみを提供します。802.11n の速度を使うには WPA と AES を使うことを推奨します。</p>

	AES	<p>AES(Advanced Encryption Standard) は WPA2 とともに用いられる標準暗号化方式です。</p> <p>メモ: WPA と AES をサポートしているワイヤレスアクセスポイントもありますが、WNDAP360 は WPA と AES の組み合わせには対応しておりません。</p>
	TKIP + AES	<p>TKIP + AES 暗号化方式は WPA と WPA2 でサポートされています。ブロードキャストパケットは TKIP を使います。ユニキャスト(ポイント・ポイント)転送には WPA クライアントは TKIP,WPA2 クライアントは AES を使います。WPA & WPA2 Mixed モードでは TKIP+AES のみがサポートされている暗号化方式です。</p>
Passphrase	<p>パスフレーズを入力します。パスフレーズ長は 8-63 文字です。Generate Keys をクリックすることによって Secret passphrase から自動的に Key を作成することができます。デフォルトの Passphrase は”sharedsecret”です。</p> <p>Show Passphrase in Clear Text ラジオボタンを押すことによって passphrase を表示することができます。</p>	
Show Passphrase in Clear Text	<p>Yes ラジオボタンを選択すると Passphrase 欄のパスフレーズを表示することができます。</p>	

RADIUS サーバー設定

RADIUS を使った認証あるいは課金、またはその両方のためにプライマリーとセカンダリー(オプション)サーバーを設定する必要があります。これらの RADIUS サーバー設定はワイヤレスアクセスポイントに接続されるすべてのデバイスに適用可能です。

RADIUS サーバー設定をする

1. Configuration > Security > Advanced > Radius Server Settings を選択して Radius Server Settings ページを表示します。

The screenshot shows the 'Radius Server Settings' configuration page. It is divided into two main sections: 'IPv4 RADIUS Server Settings' and 'Authentication Settings'. The 'IPv4 RADIUS Server Settings' section contains a table with four rows: Primary Authentication Server, Secondary Authentication Server, Primary Accounting Server, and Secondary Accounting Server. Each row has three columns: IPv4 Address, Port, and Shared Secret. The 'Authentication Settings' section includes a 'Reauthentication Time (Seconds)' field set to 3600 and a checked 'Update Global Key Every (Seconds)' field set to 1800. At the bottom right, there are 'CANCEL' and 'APPLY' buttons.

2. 各項目を設定します。

項目	説明	
RADIUS Server Settings		
Primary Authentication Server	IP Address	プライマリー認証 RADIUS サーバーの IP アドレスを指定します。
	Port	プライマリー認証 RADIUS サーバーにアクセスするワイヤレスアクセスポイントの UDP ポート番号を指定します。デフォルトは 1812 です。
	Shared Secret	ワイヤレスアクセスポイントとプライマリー認証 RADIUS サーバーの間で認証に使う共有キーを入力します。
Secondary Authentication Server	IP Address	セカンダリー認証 RADIUS サーバーの IP アドレスを指定します。
	Port	セカンダリー認証 RADIUS サーバーにアクセスするワイヤレスアクセスポイントの UDP ポート番号を指定します。デフォルトは 1812 です。

		ントの UDP ポート番号を指定します。デフォルトは 1812 です。
	Shared Secret	ワイヤレスアクセスポイントとセカンダリー認証 RADIUS サーバーの間で認証に使う共有キーを入力します。
Primary Accounting Server	IP Address	プライマリー課金 RADIUS サーバーの IP アドレスを指定します。
	Port	プライマリー課金 RADIUS サーバーをアクセスするワイヤレスアクセスポイントの UDP ポート番号を指定します。デフォルトは 1812 です。
	Shared Secret	ワイヤレスアクセスポイントとプライマリー課金 RADIUS サーバーの間で認証に使う共有キーを入力します。
Secondary Accounting Server	IP Address	セカンダリー課金 RADIUS サーバーの IP アドレスを指定します。
	Port	セカンダリー課金 RADIUS サーバーをアクセスするワイヤレスアクセスポイントの UDP ポート番号を指定します。デフォルトは 1812 です。
	Shared Secret	ワイヤレスアクセスポイントとセカンダリー課金 RADIUS サーバーの間で認証に使う共有キーを入力します。
Authentication Settings		
Reauthentication Time (Seconds)	サブリカントが RADIUS サーバーで再認証されるまでの周期。デフォルトは 3600 秒(1 時間)。0 を設定すると再認証は無効になります。	
Update Global Key Every (Seconds)	グローバルキーアップデートを有効にするにはチェックボックスを選択し、更新周期(秒)を入力します。デフォルトは選択されていて、周期は 1800 秒(30 分)です。グローバルキーアップデートを停止するには選択を外します。	

3. Apply ボタンをクリックして設定を保存します。

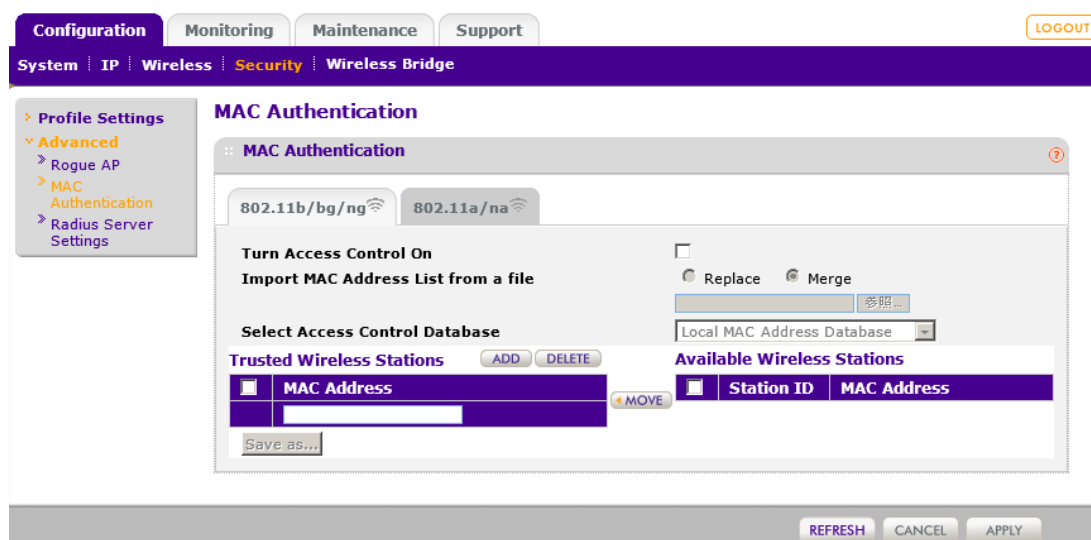
MAC アドレスでワイヤレスアクセス制限をする

セキュリティを強化するために、特定のコンピューターとワイヤレス端末に対して MAC アドレスでアクセスを許可することで SSID へのアクセスを制限できます。信頼出来るコンピューターのみアクセスを制限できるので、未知のコンピューターは無線でワイヤレスアクセスポイントに接続することはできません。MAC アドレスフィルタリングは期待しないアクセスに対する妨害にはなりますが、ワイヤレスリンクでのデータブロードキャストは完全に晒されています。

メモ: 通常 MAC アドレスはワイヤレスアダプターに印刷されています。

MAC アドレス制限をする

1. Configuration > Security > Advanced > MAC Authentication を選択して MAC Authentication ページを表示します。
2. 802.11a/na モードの MAC Authentication ページを表示するには 802.11a/na タブをクリック



クします。

3. Turn Access Control On: チェックボックスを選択してアクセス制御を有効にします。
4. Select Access Control Database: データベースオプションを選択します。
 - Local MAC Address Database: ワイヤレスアクセスポイントはアクセス制御のためにローカル MAC アドレスデータベースを使います。
 - Remote MAC Address Database: ワイヤレスアクセスポイントはアクセス制御のために LAN 上にある外部の RADIUS サーバーの MAC アドレスデータベースを使います。このデータベースを選択すると、最初に RADIUS サーバー設定をする必要があります。

5. **Refresh** ボタンをクリックして **Available Wireless Stations** テーブルを更新します。ワイヤレスアクセスポイントは接続されているワイヤレス端末の MAC アドレスを表示します。
6. 以下の手順で **Trusted Wireless Stations** テーブルを作成します。
 - **Available Wireless Stations** テーブルから MAC アドレスを選択する。
 - a. 個々の MAC addresses のチェックボックスを選択するか、先頭のチェックボックスですべての MAC アドレスを選択します。
 - b. **Move** ボタンをクリックして MAC アドレスを **Available Wireless Stations** テーブルから **Trusted Wireless Stations** テーブルへ移動します。
 - MAC アドレスを入力する。
 - a. **Trusted Wireless Stations** テーブルに MAC アドレスを直接入力する。
 - b. **Add** ボタンをクリックします。

Trusted Wireless Stations テーブルから MAC アドレスを削除するには、個々の MAC アドレスのチェックボックスを選択するか、先頭のチェックボックスですべての MAC アドレスを選択し、**Delete** ボタンをクリックします。

7. **Apply** ボタンをクリックして設定を保存します。

Trusted Wireless Stations テーブルにあるデバイスのみがワイヤレスアクセスポイントに接続できます。



警告！

ワイヤレスアクセスポイントをワイヤレスコンピューターから設定し、ワイヤレスアクセスポイントの SSID やワイヤレスセキュリティ設定を変更して、**Apply** ボタンをクリックすると、ワイヤレス接続を失います。新しいワイヤレスアクセスポイントの設定に合わせてコンピューターのワイヤレス設定を変更する必要があります。

電波の停止スケジュール

電波を停止する機能は休暇やオフィスの閉鎖、夜間や週末に無線を停止することが出来る省エネ機能です。

電波のオンオフをスケジュールする

1. Configuration > Wireless > Basic > Wireless On-Off を選択して Wireless On-Off ページを表示します。

2. 項目を設定します。

項目	説明
Wireless on-off	On ラジオボタンを選択してタイマーを有効にします。デフォルトは Off です。
Radio off schedule	電波を停止する日を選択します。デフォルトは土曜日 (Saturday) と日曜日 (Sunday) が選択されています。
Radio ON Time	電波をオンにする時間を 24 時間形式で指定します。
Radio OFF Time	電波を停止する時間を 24 時間形式で指定します。

3. Apply ボタンをクリックして設定を保存します。

基本ワイヤレス QoS を設定する

WMM (Wi-Fi マルチメディア) は 802.11e 標準の一部です。WMM はデータタイプに合わせてワイヤレストラフィックに優先度を持たせます。ビデオや音声のような遅延に敏感な情報は通常のトラフィックよりも高い優先度を持ちます。WMM が正しく動作するために、ワイヤレスクライアントも WMM をサポートする必要があります。

WMM を有効にすることによって、ワイヤレス端末からワイヤレスアクセスポイントへのアップストリームトラフィックと、ワイヤレスアクセスポイントからワイヤレス端末へのダウンストリームトラフィックに対して QoS(Quality of Service)制御を可能にします。

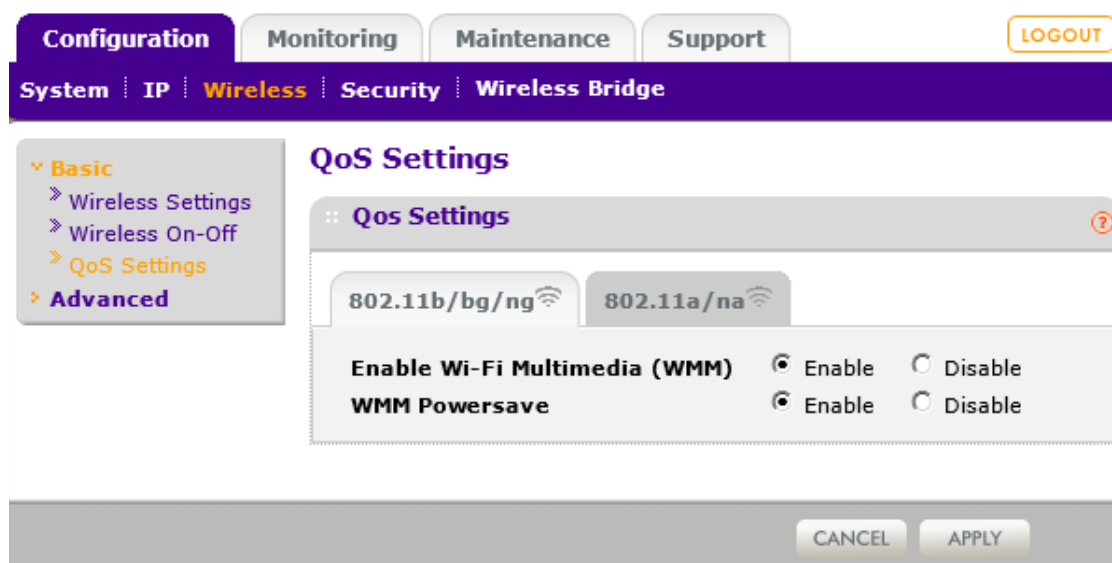
WMM は優先度の高い順から以下の 4 つのキューを定義しています。

- **Voice:** 最小遅延の最高の優先度。VoIP やストリーミングメディアのようなアプリケーションに適しています。
- **Video:** 低遅延の 2 番目の優先度。ビデオアプリケーションはこのキューを使います。
- **Best Effort:** 中間のプライオリティキュー。ほとんどの IP アプリケーションはこのキューを使います。
- **Background:** 最低の優先度。FTP のような遅延に敏感ではない、高いスループットを必要とするアプリケーションがこのキューを使います。

WMM パワーセーブ(Powersave)機能はデータ転送の効率と優先度を増すことによってバッテリー駆動の機器の電源消費を節約します。

基本ワイヤレス QoS を設定する

1. Configuration > Wireless > Basic > QoS Settings を選択して QoS Settings ページを表示します。



2. 802.11a/na タブをクリックすると 802.11a/na モードの QoS Settings ページを表示できます。
3. WMM 機能を有効・無効にする
 - **Enable Wi-Fi Multimedia (WMM):** Enable ラジオボタンをクリックしてこの機能を有効にします。デフォルトは有効です。

WNDAP360 管理マニュアル

- **WMM Powersave:Enable** ラジオボタンをクリックしてこの機能を有効にします。デフォルトは有効です。
4. **Apply** ボタンをクリックして設定を保存します。

管理

この章では WNDAP360 の管理機能と監視機能を使う方法について記します。

リモート管理を有効にする

SNMP (Simple Network Management Protocol) と SSH はデフォルトで有効になっており、SNMP 管理ソフトウェアおよび SSH を動作しているクライアントからワイヤレスアクセスポイントへのリモートアクセスが可能です。Telnet コンソールはデフォルトで無効になっています。

SNMP 管理

SNMP 管理インターフェースを設定する

1. Maintenance > Remote Management > SNMP を選択して SNMP ページを表示します。

The screenshot shows the WNDAP360 web interface. At the top, there are tabs for Configuration, Monitoring, Maintenance (selected), and Support. Below the tabs is a navigation bar with links for Password, Reset, Remote Management (selected), and Upgrade. On the left, there is a sidebar with links for SNMP (selected) and Remote Console. The main content area is titled 'SNMP' and contains a 'SNMP Settings' form. The form has a title bar with a question mark icon. The settings are as follows:

SNMP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Read-Only Community Name	<input type="text" value="public"/>
Read-Write Community Name	<input type="text" value="private"/>
Trap Community Name	<input type="text" value="trap"/>
IP Address to Receive Traps	<input type="text"/>
Trap Port	<input type="text" value="162"/>

At the bottom of the form, there are 'CANCEL' and 'APPLY' buttons.

2. 項目を設定します。

項目	設定
SNMP	Enable ラジオボタンを選択して SNMP を有効にして、ワイヤレスアクセスポイントを SNMPv1/v2 プロトコルで管理します。デフォルトは無効です。
Read-Only Community Name	コミュニティストリングを入力して SNMP マネージャーがワイヤレスアクセスポイントの MIB (Management Information Base) を読み取れるようにします。デフォルトは public です。

Read-Write Community Name	コミュニティストリングを入力して SNMP マネージャーがワイヤレスアクセスポイントの MIB (Management Information Base)を読み書きできるようにします。デフォルトは private です。
Trap Community Name	Trap 送信のためのコミュニティストリングを指定します。デフォルトは trap です。
IP Address to Receive Traps	ワイヤレスアクセスポイントから Trap を送信する SNMP マネージャーの IP アドレスを指定します。
Trap Port	ワイヤレスアクセスポイントから Trap を送信する SNMP マネージャーのポート番号を指定します。デフォルトは 162 です。

3. Apply ボタンをクリックして設定を保存します。

Secure Shell(SSH)と Telnet 管理

リモートコンソール機能を設定する

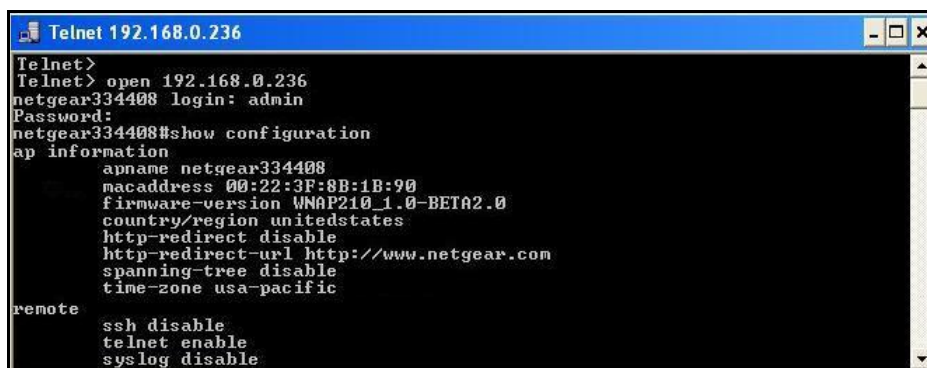
1. Maintenance > Remote Management > Remote Console を選択して Remote Console ページを表示します。

2. リモートコンソールを有効・無効にする。
 - Secure Shell (SSH): Enable ラジオボタンを選択して有効にします。デフォルトは有効です。
 - Telnet: Enable ラジオボタンを選択して有効にします。デフォルトは無効です。
3. Apply ボタンをクリックして設定を保存します。

シリアル接続でワイヤレスアクセスポイントを管理する

1. ワイヤレスアクセスポイントのコンソールポートにイーサネットケーブルを接続します。
2. ケーブルのもう一方を VT100/ANSI ターミナルまたはワークステーションに接続します。PC、アップルマッキントッシュまたは UNIX ワークステーションを接続した場合は、ターミナルエミュレーションプログラムに以下の設定をします。

- Baud rate: 9600 bps
 - Data bits: 8
 - Parity: none
 - Stop bit: 1
 - Flow control: none
3. ターミナルプログラムを起動すると以下の様な画面が表示されます。



```

Telnet 192.168.0.236
Telnet>
Telnet> open 192.168.0.236
netgear334408 login: admin
Password:
netgear334408#show configuration
ap information
  apname netgear334408
  macaddress 00:22:3F:8B:1B:90
  firmware-version WNAP210_1.0-BETA2.0
  country/region unitedstates
  http-redirect disable
  http-redirect-url http://www.netgear.com
  spanning-tree disable
  time-zone usa-pacific

remote
  ssh disable
  telnet enable
  syslog disable

```

4. ログイン名とパスワードを入力します。(デフォルトは **admin** と **password** です)
ログインに成功すると、アクセスポイント名が先頭に表示されるプロンプト”#”が表示されます。例では netgear334408#です。
5. CLI コマンドを入力します。show configuration と入力して可能な CLI コマンドを表示できます。

メモ: ワイヤレスアクセスポイントに Telnet や SSH セッションでアクセスすることも可能です。

ワイヤレスアクセスポイントソフトウェアのアップグレード

ワイヤレスアクセスポイントのソフトウェアはフラッシュメモリーに保存され、NETGEAR が新しいソフトウェアをリリースした際にアップグレード可能です。NETGEAR Web サイトからアップグレードファイルをダウンロードできます。ダウンロードしたアップグレードファイルが ZIP ファイル形式に圧縮されている場合はワイヤレスアクセスポイントに送る前に解凍して(.rmt)形式にする必要があります。Web ブラウザーでアップグレードファイルを送信することができます。以下に 2 つの方法でソフトウェアアップグレードする方法を示します。

- [Web ブラウザーでアップグレードする方法](#)
- [TFTP サーバーでアップグレードする方法](#)

メモ: Web ブラウザーは HTTP アップロードをサポートしている必要があります。

メモ: ワイヤレスアクセスポイントにワイヤレス接続しているコンピューターからソフトウェアアップグレードをすることはできません。イーサネットケーブル経由で接続されたコンピューターを使う必要があります。



警告！

When uploading software to the ワイヤレスアクセスポイントにソフトウェアにアップロードしている時に Web ブラウザーを閉じたり、リンクをクリックしたり、新しいページを表示したりしないでください。アップロードが失敗して、ソフトウェアが破損し、ワイヤレスアクセスポイントが動作しなくなる可能性があります。



重要

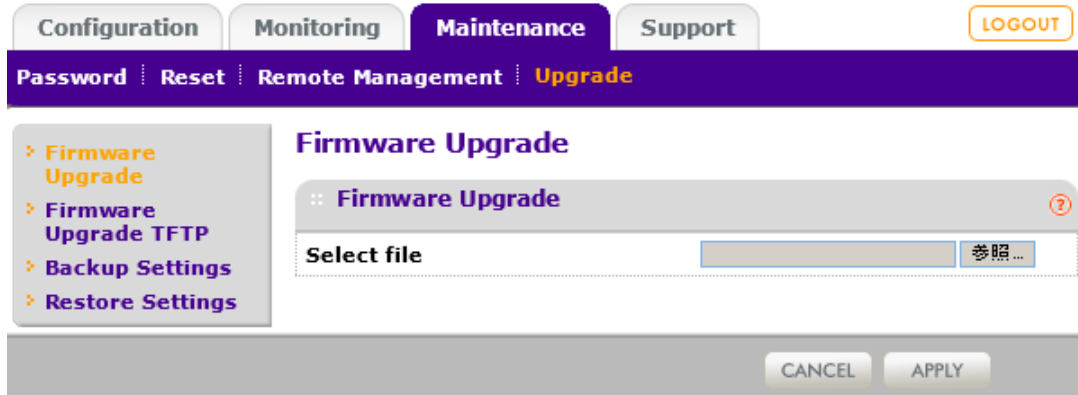
ソフトウェアの大きなアップデートのような場合、ワイヤレスアクセスポイントの設定を消去し、アップグレード後再度手動で設定する必要がある場合があります。アップグレードする前にリリースノートをよく読んで下さい。

Web ブラウザーでのアップグレード手順

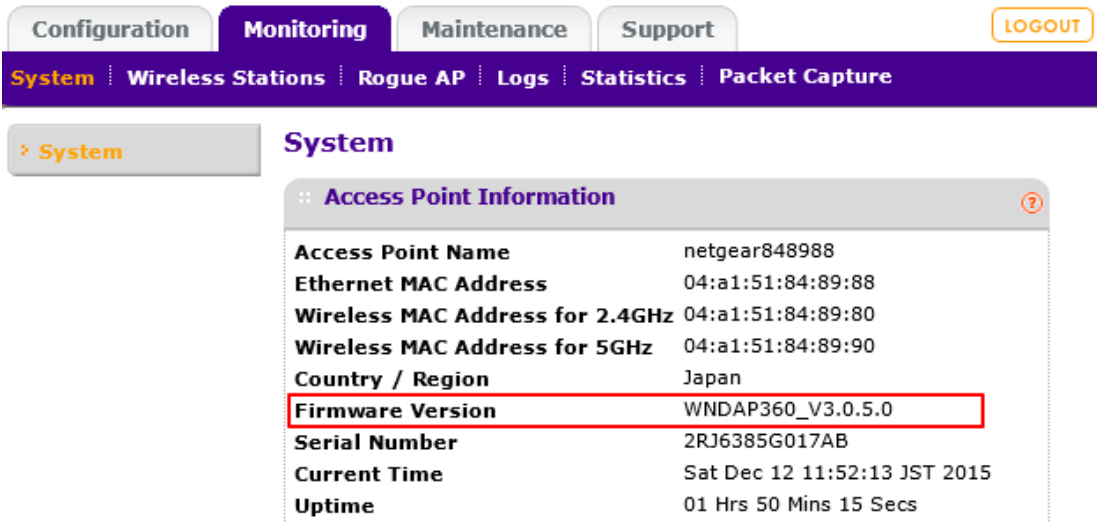
Web ブラウザーを使ってワイヤレスアクセスポイントのファームウェアをアップグレードする

1. NETGEAR Web サイトからソフトウェアをダウンロードしてコンピューターに保存します。
2. 必要ならば ZIP ファイルを解凍します。
3. ソフトウェアをアップデートする前に、リリースノート(ある場合は)をよく読みます。

4. Maintenance > Upgrade > Firmware Upgrade を選択して Firmware Upgrade ページを表示します。



5. 参照ボタンをクリックしてアップグレードファイルを指定します。
6. Apply ボタンをクリックしてアップグレードを開始します。
アップグレードの最中ワイヤレスアクセスポイントは自動的に再起動します。アップグレードには通常数分かかります。
7. Monitoring > System を選択して新しいファームウェアがインストールされたことを確認します。



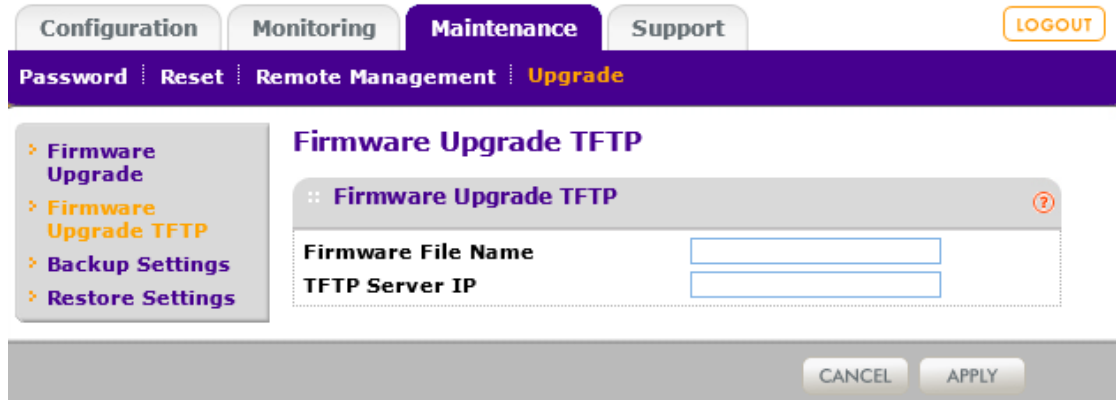
TFTP サーバーアップグレード手順

この手順を行うには TFTP サーバーを設定する必要があります。

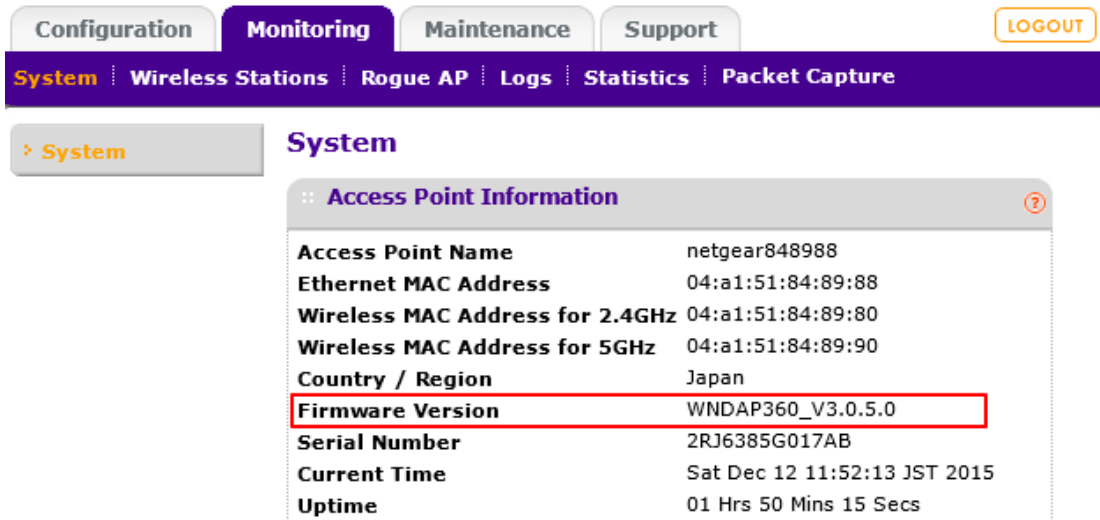
TFTP サーバーを使ってワイヤレスアクセスポイントのファームウェアをアップグレードする

1. NETGEAR Web サイトからソフトウェアをダウンロードしてコンピューターのに保存します。

2. TFTP サーバーのフォルダーにソフトウェアを保存します。
3. 必要ならば ZIP ファイルを解凍します。
4. ソフトウェアをアップデートする前に、リリースノート(ある場合は)をよく読みます。
5. **Select Maintenance > Upgrade > Firmware Upgrade TFTP** を選択して **Firmware Upgrade TFTP** ページを表示します。



6. 以下の情報を指定します。
 - **Firmware File Name:** ソフトウェアファイル名。
 - **TFTP Server IP:** TFTP サーバーの IP アドレス。
7. **Apply** ボタンをクリックしてアップグレードを開始します。
アップグレードの最中ワイヤレスアクセスポイントは自動的に再起動します。アップグレードには通常数分かかります。
8. **Monitoring > System** を選択して新しいファームウェアがインストールされたことを確認します。



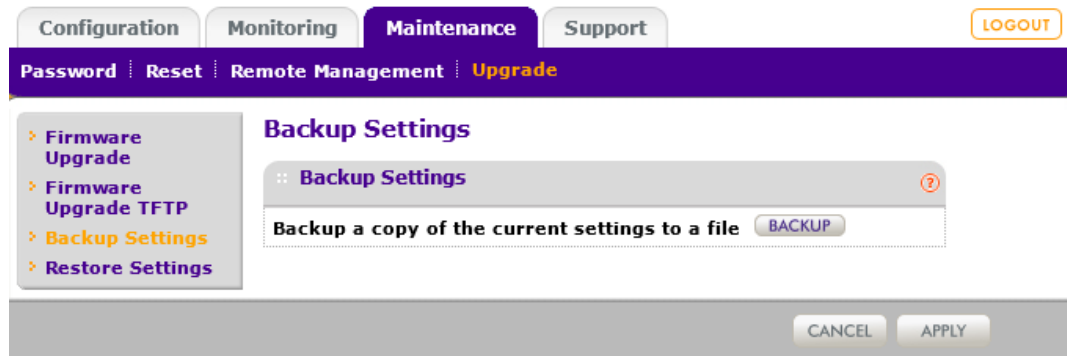
設定ファイルの管理とファクトリーデフォルト

ワイヤレスアクセスポイント設定は設定ファイルに保管されています。設定ファイルをコンピューターに保存(バックアップ)できます。また、ワイヤレスアクセスポイントを工場出荷状態に戻すことができます。

設定の保存

設定を保存する

1. Maintenance > Upgrade > Backup Settings を選択して Backup Settings ページを表示します。



2. Backup ボタンをクリックして設定ファイル(ファイル名は config)をワイヤレスアクセスポイントから抽出し、設定ファイルの保存場所をたずねてきます。
3. 指示にしたがってファイルを保存します。

設定の復元

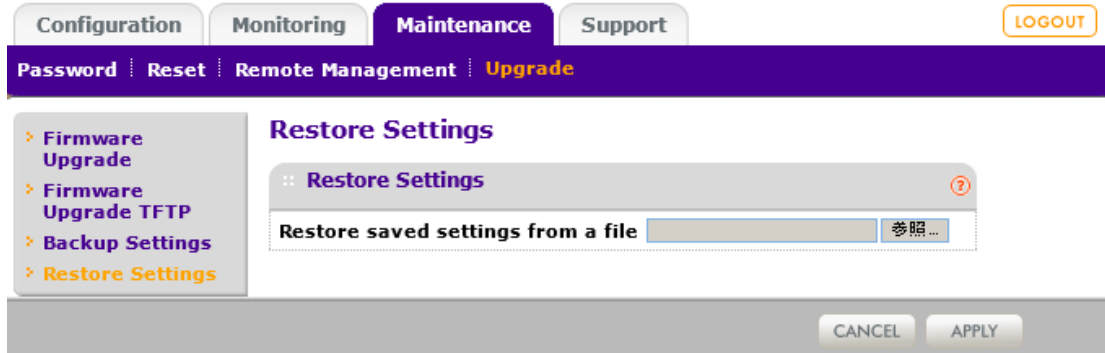


重要

復元の最中にワイヤレスアクセスポイントの電源を落としたり、コンピューターの電源を切るようなことはしないでください。

保存した設定ファイルから設定を復元する

1. Maintenance > Upgrade > Restore Settings を選択して Restore Settings ページを表示します。



2. 参照ボタンをクリックし、保存した設定ファイル(ファイル名は config)を指定します。
3. Apply ボタンをクリックして復元を開始します。復元の最中、ワイヤレスアクセスポイントは再起動します。復元には約 1 分かかります。

ワイヤレスアクセスポイント設定を工場出荷状態に戻す

2つの方法でワイヤレスアクセスポイントを工場出荷状態に戻します。

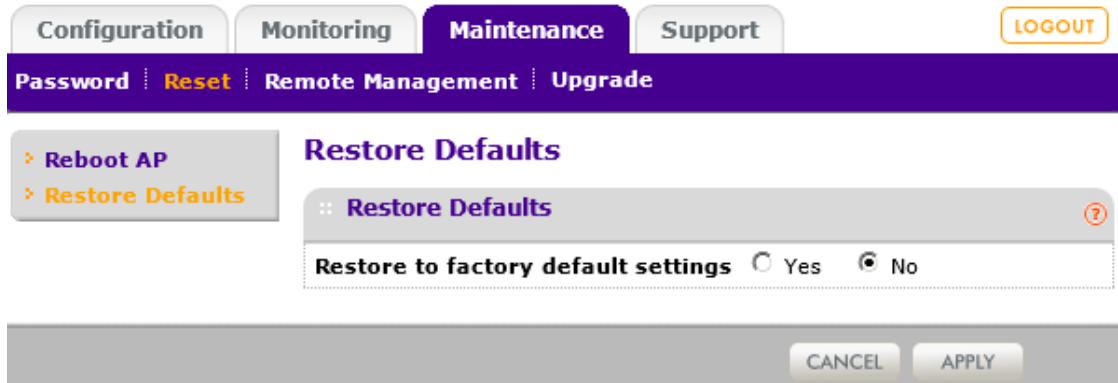
- Web ブラウザーで工場出荷状態に戻す
- リセットボタンで工場出荷状態に戻す

メモ: ワイヤレスアクセスポイントを工場出荷時に戻した場合、

- * 設定は初期化されます
 - * ログインパスワードは password になります
 - * ワイヤレスアクセスポイントの IP アドレスは 192.168.0.100 になります。
 - * DHCP クライアントは有効になります。(バージョンによって無効の場合もあります)
 - * ワイヤレスアクセスポイントの名前は netgearxxxxxx(xxxxxx は MAC アドレスの下 6 桁)となります。
-

Web ブラウザーで工場出荷状態に戻す

1. Maintenance > Reset > Restore Defaults を選択して Restore Defaults ページを表示します。



2. Yes ラジオボタン(デフォルトは No)を選択します。
3. Apply ボタンをクリックしてワイヤレスアクセスポイントを初期化します。
ワイヤレスアクセスポイントは自動的に再起動します。初期化には約 1 分かかります。

リセットボタンで工場出荷状態に戻す

ログインユーザー名、ログインパスワード、IP アドレス等が不明な場合は、ワイヤレスアクセスポイントのリアパネルのリセットボタンを使って工場出荷状態に初期化します。



1. 細長い棒を使って Reset ボタンを 5 秒以上電源/テスト LED が点滅するまで押し続けてください。

メモ: Reset ボタンを短時間押した場合はワイヤレスアクセスポイントの再起動となります。

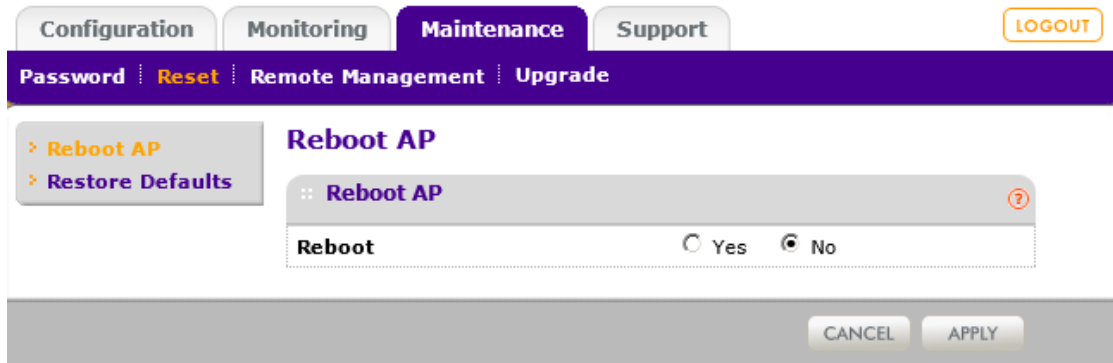
2. Reset ボタンから手を離します。
ワイヤレスアクセスポイントは自動的に再起動します。初期化には約 1 分かかります。

アクセスポイントの再起動

ワイヤレスアクセスポイントに物理的にアクセスが出来ない状態でアクセスポイントの電源のオンオフが出来ない場合、ソフトウェアでワイヤレスアクセスポイントを再起動できます。

ワイヤレスアクセスポイントを再起動する:

1. Maintenance > Reset > Reboot AP を選択して Reboot AP ページを表示します。



2. Yes ラジオボタンを選択します。(デフォルトは No)
3. Apply ボタンをクリックすると ワイヤレスアクセスポイントが再起動します。
再起動には約 1 分かかります。

管理者パスワードの変更

デフォルトパスワードは **password** です。より安全なパスワードに変更してください。管理者名 (admin) を変更することはできません。

理想的なパスワードはどの言語の辞書にも載っていない単語であり、大文字小文字、数字、記号の混ざったものが良いとされています。パスワードは最長 30 文字まで設定可能です。

管理者パスワードを変更する

1. Maintenance > Password > Change Password を選択して Change Password ページを表示します。

The screenshot shows the 'Change Password' page in the WNDAP360 management interface. The page has a navigation menu with 'Configuration', 'Monitoring', 'Maintenance', and 'Support' tabs. The 'Maintenance' tab is selected, and the 'Change Password' page is displayed. The page has a purple header with 'Password', 'Reset', 'Remote Management', and 'Upgrade' links. A 'LOGOUT' button is in the top right corner. The main content area has a 'Change Password' button and a 'Change Password' dialog box. The dialog box has a title bar with a question mark icon and contains the following fields and options:

- Current Password: [Text Input Field]
- New Password: [Text Input Field]
- Repeat New Password: [Text Input Field]
- Restore Default Password: Yes No

At the bottom of the dialog box, there are 'CANCEL' and 'APPLY' buttons.

2. Current Password 欄に現在のパスワードを入力し、以下のどちらかの手順で変更します。
 - 新しいパスワードを 2 回 (New Password 欄と Repeat New Password に) 入力する。
 - Restore Default Password で Yes ラジオボタンを選択してデフォルトパスワードを回復します。デフォルトは No です。
3. Apply ボタンをクリックして設定を保存します。
デフォルトパスワードを回復した場合、ログインパスワードは password となります。新しいパスワードを設定した場合は、安全な場所に保管してください。

Syslog サーバーを有効にする

LAN 上に Syslog サーバーがある場合は、Syslog 画面で Syslog オプションを有効にすることができます。Syslog を有効にすると、ワイヤレスアクセスポイントは syslog ファイルを syslog サーバーに送信します。

Syslog サーバーを有効にする

1. Configuration > System > Advanced > Syslog を選択して Syslog ページを表示します。

The screenshot shows the 'Syslog' configuration page. The left sidebar has a tree view with 'Basic', 'Advanced', 'General', 'Hotspot', and 'Syslog'. The main content area is titled 'Syslog' and contains a 'Syslog Settings' box. Inside this box, there are three rows: 'Enable Syslog' with a checked checkbox, 'Syslog Server IP Address' with an empty text input field, and 'Port Number' with a text input field containing '514'. At the bottom of the page, there are 'CANCEL' and 'APPLY' buttons.

以下の項目を設定します。

項目	説明
Enable Syslog	チェックボックスを選択して Syslog を有効にします。デフォルトは無効です。
Syslog Server IP Address	ワイヤレスアクセスポイントが Syslog ファイルを送信する Syslog サーバーの IP アドレスを指定します。
Port Number	Syslog サーバーのポート番号を指定します。デフォルトは 514 です。

2. Apply ボタンをクリックして設定を保存します。

ワイヤレスアクセスポイントの監視

ワイヤレスアクセスポイントは様々な監視機能があります。

システム情報を見る

System 画面で現在の IP 設定、ワイヤレス設定、を含む現在のワイヤレスアクセスポイントの設定の概要を表示します。情報は読み取りのみであり、変更が必要な場合は別の画面で変更をすることになります。

システム画面を表示する

Monitoring > System を選択して System ページを表示します。

The screenshot shows the WNDAP360 management interface. At the top, there are navigation tabs: Configuration, Monitoring (selected), Maintenance, and Support. A LOGOUT button is in the top right. Below the tabs is a purple navigation bar with links: System (selected), Wireless Stations, Rogue AP, Logs, Statistics, and Packet Capture. On the left, there is a 'System' sidebar button. The main content area is titled 'System' and contains four expandable sections:

- Access Point Information**:

Access Point Name	netgear848988
Ethernet MAC Address	04:a1:51:84:89:88
Wireless MAC Address for 2.4GHz	04:a1:51:84:89:80
Wireless MAC Address for 5GHz	04:a1:51:84:89:90
Country / Region	Japan
Firmware Version	WNDAP360_V3.0.5.0
Serial Number	2RJ6385G017AB
Current Time	Sat Dec 12 14:43:40 JST 2015
Uptime	04 Hrs 41 Mins 42 Secs
- Current IPv4 Settings**:

IPv4 Address	192.168.1.20
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DHCP Client	Enabled
- Current Wireless Settings for 802.11ng**:

Access Point Mode	Access Point
Channel / Frequency	Auto (11)
Rogue AP Detection	Disabled
- Current Wireless Settings for 802.11na**:

Access Point Mode	Access Point
Channel / Frequency	Auto (40)
Rogue AP Detection	Disabled

以下に表示される情報について示します。

項目	説明
Access Point Information	
Access Point Name	アクセスポイントの NetBIOS 名。
Ethernet MAC Address	ワイヤレスアクセスポイントのイーサネットポートの MAC アドレス。

WNDAP360 管理マニュアル

Wireless MAC Address	ワイヤレスアクセスポイントのワイヤレスカードの MAC アドレス。
Country/Region	ワイヤレスアクセスポイントの動作する国情報。 メモ: ワイヤレスアクセスポイントの国情報を異なる設定にすると違法になる可能性があります。
Firmware Version	現在インストールされているファームウェアのバージョン。
Current Time	現在の時間。
Current IP Settings	
IP Address	ワイヤレスアクセスポイントの IP アドレス。
Subnet Mask	ワイヤレスアクセスポイントのサブネットマスク。
Default Gateway	ワイヤレスアクセスポイントのデフォルトゲートウェイ。
DHCP Client	DHCP クライアントの有効、無効。
Current Wireless Settings for 802.11n/g	
Access Point Mode	ワイヤレスアクセスポイントの動作モード。 <ul style="list-style-type: none"> • Access Point • Point-to-Point Bridge • Point-to-Point Bridge with Access Point • Multi-Point Bridge with/without client association
Channel / Frequency	ワイヤレスポートが使用しているチャンネル。
Rogue AP Detection	不正 AP 検知の有効・無効。
Current Wireless Settings for 802.11n/a	
Access Point Mode	ワイヤレスアクセスポイントの動作モード。 <ul style="list-style-type: none"> • Access Point • Point-to-Point Bridge • Point-to-Point Bridge with Access Point • Multi-Point Bridge with/without client association
Channel / Frequency	ワイヤレスポートが使用しているチャンネル。
Rogue AP Detection	不正 AP 検知の有効・無効。

ワイヤレス端末の監視

Wireless Stations 画面は Available Wireless Stations テーブルを含んでいます。テーブルにはワイヤレスアクセスポイントに接続されているすべての IP デバイスを表示します。テーブルはワイヤレスモードごとに表示されます。

メモ: ワイヤレスネットワークは同じネットワーク名 (SSID) を使う複数のワイヤレスアクセスポイントからなることがあります。これがワイヤレスネットワークの範囲を広げ、ユーザーはワイヤレスアクセスポイント間を移動できるようになります。この環境では、Available Wireless Stations テーブルはこのワイヤレスアクセスポイントに接続されている端末だけが表示されることに注意してください。

接続されたワイヤレス端末を確認し、その詳細を見る

1. Monitoring > Wireless Stations. を選択して Wireless Stations ページを表示します。

MAC Address	BSSID	SSID	Channel	Rate	State	Type	AID	Mode	Status
D0:4F:7E:51:BD:88	04:a1:51:84:89:80	WNDAP360_24G	11	117.00	QOS/ERP/HT/PWR_MGT	wpa2	1	11ng	Associated

Refresh ボタンをクリックしてリストを更新します。ワイヤレスアクセスポイントが再起動するとワイヤレスアクセスポイントがワイヤレス端末を再発見するまで情報は失われます。接続されているデバイスを探すには Refresh ボタンをクリックします。

2.4GHz モードおよび 5GHz モードそれぞれに Available Wireless Stations テーブルがあります。それぞれのモードで Available Wireless Stations テーブルは MAC アドレス、BSSID、SSID、チャンネル、速度、タイプ、AID、モードおよび状態を表示します。

2. ワイヤレス端末の詳細を見るには、端末に対応するラジオボタンを選択し、Details ボタンをクリックします。

Wireless Stations Details	
MAC Address	D0:4F:7E:51:BD:B8
BSSID	04:a1:51:84:89:80
SSID	WNDAP360_24G
Channel	11
Rate	117.00
State	QOS/ERP/HT/PWR_MGT
Type	wpa2
AID	1
Mode	11ng
Status	Associated
RSSI	60
Idle Time	0
Tx Sequence	91
Rx Sequence	1456
Capability	EPSs
Cipher	aes
SNR	33
Recv. Bytes	16906
Trans. bytes	33613
Assoc. Time Stamp	00:00:07
IP Address	192.168.1.6
Channel Width	Static20

Close

以下に Wireless Stations Details 画面に表示される情報の説明を記します。

項目	説明
MAC Address	ワイヤレス端末の MAC アドレス。
BSSID	ワイヤレス端末が使っている BSSID。
SSID	ワイヤレス端末が使っている SSID。

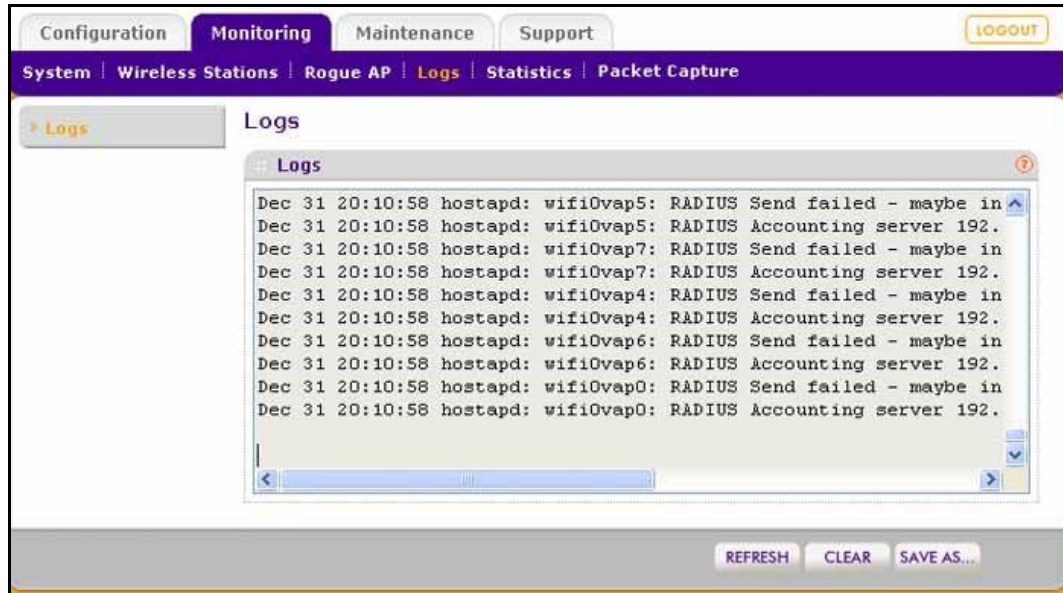
Channel	ワイヤレス端末が使っているチャンネル。
Rate	ワイヤレス端末の送信速度(Mbps)。
State	ワイヤレス端末で有効になっている機能。
Type	ワイヤレス端末が使っている認証と暗号化タイプ。
AID	ワイヤレス端末の AID(associated identifier)。
Mode	ワイヤレス端末が動作しているモード。
Status	ワイヤレス端末のワイヤレス状態。(Associated)。
RSSI	ワイヤレス端末の RSSI(received signal strength indicator)。
Idle Time	ワイヤレス端末から最後にフレームを受信してからの時間。
Tx Sequence	ワイヤレス端末に送信された最後のフレームのシーケンス番号。
Rx Sequence	ワイヤレス端末が受信した最後のフレームのシーケンス番号。
Capability	接続の際に検知したワイヤレス端末の能力概要。
Cipher	ワイヤレス端末が使っている暗号化方式。
SNR	SNR(signal-to-noise ratio)
Recv. Bytes	ワイヤレス端末が起動後受信したバイト数。
Trans. bytes	ワイヤレス端末が起動後送信したバイト数。
Assoc. Time Stamp	ワイヤレス端末の詳細情報を取得した時間。
IP Address	ワイヤレス端末の IP アドレス。
Channel Width	ワイヤレス端末が動作しているチャンネル幅。

アクティビティログを確認する

ワイヤレスアクセスポイントのアクティビティログを確認し保存することができます。

アクティビティログを表示して保存する

1. **Monitoring** > **Logs** を選択して **Logs** ページを表示します。



2. **Save As** ボタンをクリックしてログを保存することができます。
Refresh ボタンをクリックして画面を更新します。ログを削除するには **Clear** ボタンをクリックします。

トラフィック統計 Traffic Statistics

Statistics 画面は有線(LAN)とワイヤレス(WLAN)のトラフィック情報を表示します。

Statistics 画面を表示する。

Monitoring > **Statistics** を選択して **Statistics** ページを表示します。

Statistics

Statistics

Wired Ethernet ?

	Received	Transmitted
Packets	2388816	383815
Bytes	747040474	124688711

Wireless 802.11ng ?

	Received	Transmitted
Unicast Packets	347615	364693
Broadcast Packets	240	270481
Multicast Packets	387	42352
Total Packets	348242	677526
Total Bytes	27804890	562229977

Wireless 802.11na ?

	Received	Transmitted
Unicast Packets	43670	23494
Broadcast Packets	466	73330
Multicast Packets	165	11048
Total Packets	44301	107872
Total Bytes	1870469	46214789

Client Association ?

	Number of Associated Clients
802.11ng Radio	0
802.11na Radio	0

REFRESH

Refresh ボタンをクリックして情報を更新します。

以下の表に Statistics 画面に表示される情報の説明を記します。

項目	説明
Wired Ethernet	

Packets	ワイヤレスアクセスポイントが再起動してからのイーサネットコネクションで送受信したパケットの数。
Bytes	ワイヤレスアクセスポイントが再起動してからのイーサネットコネクションで送受信したバイト数。
Wireless 802.11b, Wireless 802.11bg, or Wireless 801.11ng 項目はワイヤレスモードの選択により異なります。	
Unicast Packets	ワイヤレスアクセスポイントが再起動してからのワイヤレスコネクションで送受信したユニキャストパケット数。
Broadcast Packets	ワイヤレスアクセスポイントが再起動してからのワイヤレスコネクションで送受信したブロードキャストパケット数。
Multicast Packets	ワイヤレスアクセスポイントが再起動してからのワイヤレスコネクションで送受信したマルチキャストパケット数。
Total Packets	ワイヤレスアクセスポイントが再起動してからのワイヤレスコネクションで送受信したパケット数。
Total Bytes	ワイヤレスアクセスポイントが再起動してからのワイヤレスコネクションで送受信したバイト数。
Wireless 802.11a or Wireless 801.11na 項目はワイヤレスモードの選択により異なります。 項目は 2.4GHz モードと同じです。	
Client Association	
802.11b Radio, 802.11bg Radio, or 802.11ng Radio	接続されているクライアント数。
802.11na Radio or 802.11a Radio	

不正 AP 検知を有効にする

不正 AP 検知の有効化と設定

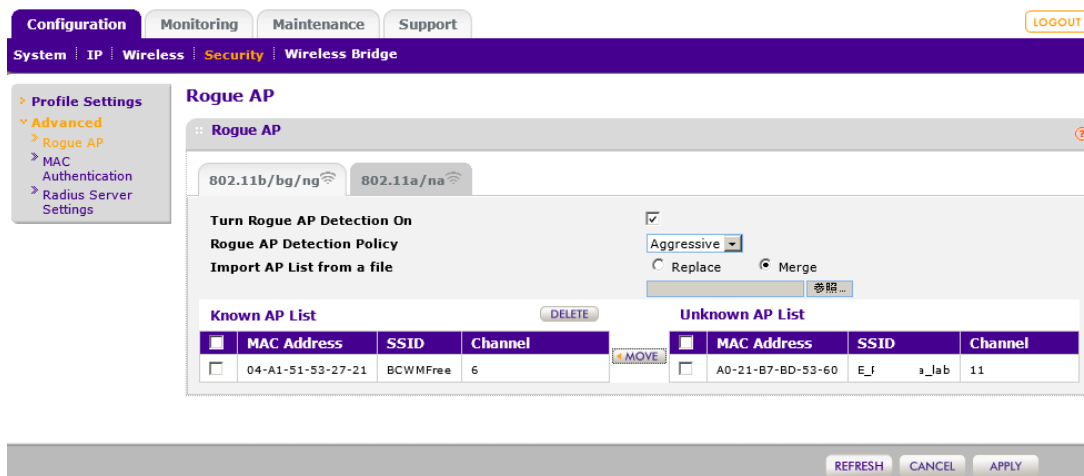
ワイヤレスアクセスポイントは不正アクセスポイントを検知し、ワイヤレスアクセスポイントに接続することを防ぐことができます。ワイヤレスアクセスポイントはその場所で検知したアクセスポイントのリストを維持します。最初は検知されたすべてのアクセスポイントは **Unknown AP List**

に表示されます。Know AP List に加えることによって承認したアクセスポイントだけに通信を制限し不正 AP 検知機能を有効にします。

不正 AP 検知を有効にすると、ワイヤレスアクセスポイントは常にワイヤレスネットワークをスキャンし、そのチャンネルのすべてのアクセスポイント情報を収集します。

不正 AP 検知を有効にし設定する

1. Configuration > Security > Advanced > Rogue AP を選択して Rogue AP ページを表示しま



2. 802.11a/na タブをクリックして 802.11a/na モードでも不正 AP 検知を有効にし、設定できます。
3. Refresh ボタンをクリックしてワイヤレスアクセスポイントにアクセスポイントを発見させたい Unknown AP List に追加させます。
4. Unknown AP List でチェックボックスを使ってアクセスポイントを選択します。
5. Move ボタンをクリックしてアクセスポイントを Unknown AP List から Known AP List へ移動します。
6. Turn Rogue AP Detection On チェックボックスを選択して不正 AP 検知を有効にします。
7. Rogue AP Detection Policy: 不正 AP 検知のスキャンの頻度を設定します。
Moderate: 5 秒
Mild: 10 秒
Aggressive: 1 秒
8. Apply ボタンをクリックして設定を保存します。

アクセスポイントを Know AP List から削除し、Unknown AP List に追加する

1. Known AP List で削除するアクセスポイントのチェックボックスを選択します。
2. Delete ボタンをクリックします。

Known AP List にリストをインポートする

- 以下のどちらかの方法で行います。
 - Replace ラジオボタンを選択し、既存の Known AP List と差し替える。
 - Merge ラジオボタンを選択し、既存の Known AP List と統合する。
- 参照ボタンをクリックしてファイルを選択します。ファイルは一行に1つの MAC アドレスを記載したテキストファイルです。
- ファイルを選択して開くボタンをクリックします。
- Apply ボタンをクリックして Known AP List をアップロードします。

アクセスポイントリストを確認して保存する

ワイヤレスアクセスポイント は近くのアクセスポイント(AP)とワイヤレス端末を検知しリストにして維持します。ワイヤレスアクセスポイントに接続しないようにこのリストを使うことができます。

Unknown AP List を確認しファイルに保存する

- Monitoring > Rogue AP > Unknown AP List を選択して Unknown AP List ページを表示します。

#	MAC Address	SSID	Privacy	Channel	Rate	Beacon Int.	# of Beacons	Last Beacon
1	00:1F:33:C4:F7:FB	EVA2000_WEP64	1	3	300.00	100	1264	745115
2	C0:3F:0E:B0:B7:A2	FULLRATEB7A2	0	3	270.00	100	336	744907
3	30:46:9A:05:A9:3E	XCES3700	1	1	144.44	100	8	730218
4	C0:3F:0E:05:C5:D1	nggquest	1	1	54.00	100	8	727936
5	00:24:B2:5A:1F:27	CES3703	1	3	300.00	100	536	745097

- Refresh ボタンをクリックしてワイヤレスアクセスポイントにアクセスポイントを発見させて、Unknown AP List に追加します。

以下の表に Unknown AP List の情報の説明を記します。

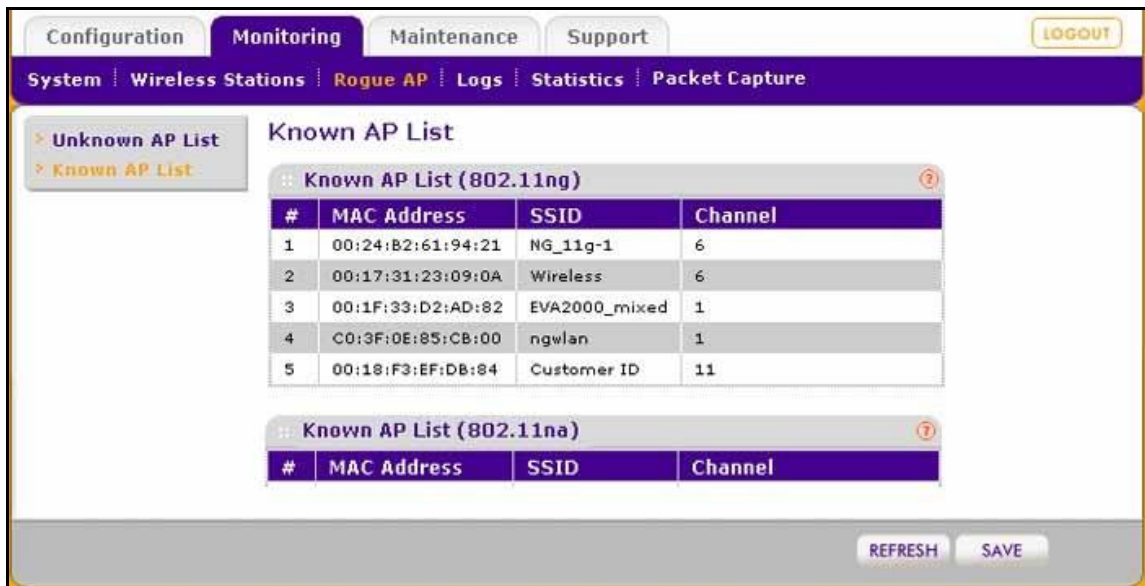
項目	説明
MAC Address	未知の AP の MAC アドレス。
SSID	未知の AP が使っている SSID。
Privacy	セキュリティの有効・無効(1:有効、2:無効)

Channel	未知の AP が使っているチャンネル。
Rate	未知の AP の送信速度。
Beacon Int.	ビーコンの送信周期(ms)
# of Beacons	The number of beacons transmitted by the unknown AP that the ワイヤレスアクセスポイントが検知した未知の AP が送信したビー コン数。
Last Beacon	最新のビーコン検知時間。

3. Save ボタンをクリックして未知の AP のリストをファイルに保存します。ウィンドウが表示され保存場所を選択できます。デフォルトのファイル名は macList.txt です。

Known AP Lists を確認してファイルに保存する

1. Monitoring > Rogue AP > Known AP List を選択して Known AP List ページを表示します。



2. Refresh ボタンをクリックしてワイヤレスアクセスポイントにアクセスポイントを発見させて、Known AP List に追加します。

以下の表に Known AP List の情報の説明を記します。

項目	説明
MAC Address	既知の AP の MAC アドレス。
SSID	既知の AP が使っている SSID。
Channel	既知の AP が使っているチャンネル。

3. **Save** ボタンをクリックして既知の AP のリストをファイルに保存します。ウィンドウが表示され保存場所を選択できます。デフォルトのファイル名は macList.txt です。

拡張設定

この章では WNDAP360 の拡張機能の設定方法を示します。

STP (Spanning Tree Protocol) と 802.1Q VLAN

Advanced General System 設定画面で STP(Spanning Tree Protocol)を有効にし、LVAN を設定します。

STP は複数のワイヤレスアクセスポイントが有効な時にネットワークトラフィック最適化を提供します。

ワイヤレスアクセスポイントでの 802.1Q VLAN は一つの物理ネットワークでトラフィックを論理的に分離します。

- Untagged VLAN:**これが選択されているときは、一つの VLAN は“Untagged VLAN”として設定されます。ワイヤレスアクセスポイントがイーサネットインターフェースで“Untagged VLAN”からのフレームを送信すると、これらのフレームにはタグは付きません。アクセスポイントがイーサネットインターフェースからタグのないフレームを受信すると、これあのフレームは Untagged VLAN に割り当てられます。
 選択されていないと、ワイヤレスアクセスポイントはイーサネットインターフェースで送信するフレームは全てにタグが付き、設定のある VLAN ID のタグのついたフレームのみを受け入れます。

メモ: ネットワークのスイッチが 802.1QVLAN をサポートしている時だけ **Untagged VLAN** チェックボックスを外してください。同様に、ネットワークのスイッチが 802.1QVLAN をサポートしている時だけ untagged VLAN 値を変更してください。Untagged VLAN チェックボックスを選択することや、untagged VLAN 値を変更すると、スイッチが対応する VLAN に設定されていないと IP 接続を失うことがあります。

- Management VLAN:** アクセスポイントと間で管理トラフィック (Telnet,SNMP,HTTP) のために使われます。
 Management VLAN に属するフレームはトランクで送信されるときには 802.1Q タグは付けられません。ポートに設定されているのが一つの VLAN だけの場合にはタグは付きません。しかしポートに複数の VLAN が割り当てられるときは、タグを付ける必要があります。

STP と VLAN を設定する

1. Configuring > System > Advanced > General を選択して General ページを表示します。



2. 以下の項目を設定します。

項目	説明
Spanning Tree Protocol	
Spanning Tree Protocol	Enable で STP を有効にします。
802.1Q VLAN	
Untagged VLAN	Untagged VLAN を選択して一つの VLAN を untagged VLAN とします。デフォルトは選択されています。VLAN ID を設定します。デフォルト VLAN ID は1です。
Management VLAN	Specify an ID for the VLAN from which the ワイヤレスアクセスポイント管理に使う VLAN ID を指定します。デフォルト VLAN ID は1です。 メモ: VLAN ID を0設定すると、ワイヤレスアクセスポイントはどの VLAN からでも管理可能になり、Management VLAN のフレームにはタグは付きません。

3. Apply ボタンをクリックして設定を保存します。

ホットスポット設定

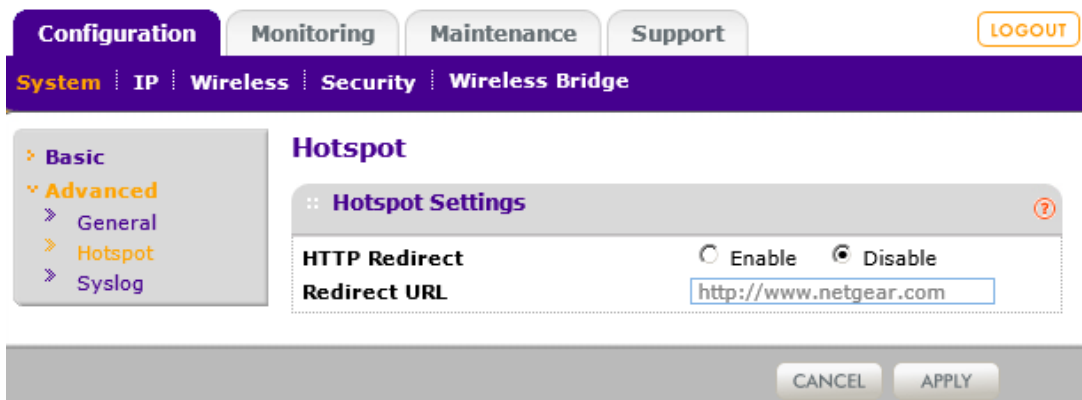
ワイヤレスアクセスポイントが公衆アクセスポイントとして動作する時にすべての HTTP 要求 (TCP、ポート 80) を捕捉しリダイレクトしたい時、ホットスポットサーバーを設定し、要求を特定の URL にリダイレクトしてクライアントを管理します。たとえば、HTTP 要求を認証の Web サー

バーやタイミング調整、広告へリダイレクトできます。ホテルではすべてのワイヤレス接続をホテルのサーバーにリダイレクトして課金処理を行いたいと思うかもしれません。

メモ: リダイレクトはワイヤレスクライアントが初めて Web ブラウザーを開いた時のみ発生します。

ホットスポットサーバーを設定する

1. Configuration > System > Advanced > Hotspot を選択して Hotspot ページを表示します。



2. HTTP Redirect: Enable を選択して HTTP リダイレクトを有効にします。デフォルトは Disable (無効) です。
3. Redirect URL: リダイレクト先の URL を記入します。
4. Apply ボタンをクリックして設定を保存します。すべての HTTP 要求は指定した URL にリダイレクトされます。

拡張ワイヤレス設定

Advanced Wireless Settings 画面で様々なワイヤレス設定をすることができます。

通常デフォルトワイヤレス設定で問題なく動作します。しかし、お使いの環境に合わせてワイヤレスアクセスポイントのパフォーマンスを微調整することができます。

拡張ワイヤレス設定をする

1. Configuration > Wireless > Advanced > Wireless Settings を選択して Wireless Settings ページを表示します。

The screenshot shows the 'Wireless Settings' configuration page. At the top, there are navigation tabs: Configuration, Monitoring, Maintenance, and Support. Below these are sub-tabs: System, IP, Wireless (selected), Security, and Wireless Bridge. A 'LOGOUT' button is in the top right. On the left, a sidebar shows a tree view with 'Basic', 'Advanced', 'Wireless Settings' (selected), and 'QoS Settings'. The main content area is titled 'Wireless Settings' and contains two tabs: '802.11b/bg/ng' (selected) and '802.11a/na'. The settings for the selected mode are as follows:

RTS Threshold (0-2347)	2347
Fragmentation Length (256-2346)	2346
Beacon Interval (100-1000)	100
Aggregation Length (1024-65535)	65535
AMPDU	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
RIFS Transmission	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DTIM Interval (1-255)	3
Preamble Type	<input checked="" type="radio"/> Auto <input type="radio"/> Long
Antenna	<input checked="" type="radio"/> Internal <input type="radio"/> External
802.11d	<input checked="" type="checkbox"/>
Client Isolation	Disable
Max. Wireless Clients	64

At the bottom of the configuration window, there are 'CANCEL' and 'APPLY' buttons.

2. 802.11a/na タブを選択して 802.11a/na モードの設定をすることもできます。
3. 以下の項目を設定します。

項目	説明
RTS Threshold (0-2347)	<p>RTS(Request to Send) threshold を設定します。デフォルトは 2347 です。</p> <p>パケットサイズが RTS Threshold 値以下の場合は、ワイヤレスアクセスポイントは SCMA/CD (Carrier Sense Multiple Access with Collision Detection) メカニズムを使い、サイレンス期間の後に直ちにデータフレームを送信します。</p> <p>パケットサイズが RTS Threshold 値よりも大きい場合は、ワイヤレスアクセスポイントは SCMA/CA (Carrier Sense Multiple Access with Collision Avoidance) メカニズムを使います。この場合、送信端末は RTS パケットを受信端末に送り、受信端末</p>

WNDAP360 管理マニュアル

	が CTS(Clear To Send)パケットを送り返すのを待ってからデータパケットを送信します。
Fragmentation Length (256-2346)	データパケットのフラグメントのために用いられる最大パケットサイズを指定します。この値よりも大きなパケットは送信前に小さなパケットに分割されます。この値は偶数である必要があります。デフォルト値は 2346 です。
Beacon Interval (100-1000)	ワイヤレスネットワークを同期するためにワイヤレスアクセスポイントが送信するビーコン送信間隔を 100ms~1000ms の間で指定します。デフォルト値は 100ms です。
Aggregation Length (1024-65535) メモ: 802.11ng, 802.11na モードのみに適用されます。	AMPDU(Aggregated MAC Protocol Data Unit) パケットの最大長を指定します。大きな値はネットワークパフォーマンスをよくします。デフォルト値は 65535 です。
AMPDU メモ: 802.11ng, 802.11na モードのみに適用されます。	Enable ラジオボタンを選択して複数の MAC フレームを一つのフレームとして送信して高いスループットを達成します。デフォルトは Enable(有効)です。
RIFS Transmission メモ: 802.11ng, 802.11na モードのみに適用されます。	Enable ラジオボタンを選択して RIFS(Reduced Interframe Space)を有効にします。デフォルトは Disable(無効)です。
DTIM Interval (1-255)	DTIM(Delivery Traffic Indication Message)を設定します。値の範囲は 1-255 です。デフォルト値は 3 です。
Preamble Type メモ: 802.11b, 802.11bg モードのみに適用されます。	<ul style="list-style-type: none"> • Long: 長いプリアンプルは信頼性の向上および範囲を広くすることに役立つことがあります。短いプリアンプルは高いパフォーマンスを得られます。 • Auto: 自動調整します。デフォルト設定です。
Antenna メモ: 802.11a, 802.11na モードには適用されません。	<ul style="list-style-type: none"> • Internal: 内部アンテナの場合に選択します。デフォルト。 • External: 外部アンテナの場合に選択します。
802.11d メモ: 802.11a, 802.11na モードには適用されません。	IEEE 802.11 規格が使用できない国や地域に向けた特殊仕様を作成することを目的とします。デフォルトで選択されています。
Client Isolation	<ul style="list-style-type: none"> • Enable: 同じ SSID に接続したクライアント同士で直接通信ができません。デフォルトは Disable(無効)です。

Max. Wireless Clients	ワイヤレスアクセスポイントに同時に接続可能なクライアント数。デフォルトは 64。
-----------------------	--

4. **Apply** ボタンをクリックして設定を保存します。

拡張 QoS 設定をする

ほとんどのネットワークではデフォルト QoS 設定で問題ありません。

ワイヤレスアクセスポイントの拡張 QoS 設定は以下のとおりです。

- **AP EDCA parameters:** ワイヤレスアクセスポイントからワイヤレスクライアントへの方向の設定をします。
- **Station EDCA parameters:** ワイヤレスクライアントからワイヤレスアクセスポイントへの方向の設定をします。WMM が無効になっていると設定できません。

EDCA 設定をすると、ワイヤレスアクセスポイントは ToS (Type of Service) に関連する IP パケットヘッダーの情報を利用します。ワイヤレスアクセスポイントはすべてのパケットのヘッダーの ToS フィールドを検査します。パケットの ToS フィールドの値をもとに、ワイヤレスアクセスポイントはパケットをキューに割り当てることでパケットの送信の優先度を決定します。異なるタイプのデータはそれぞれのキューに関連付けられます。ワイヤレスアクセスポイントがそれぞれのキューをどう扱うかを設定することができます。

キューの定義は以下の通り。

- **Data 0 (Best Effort):** 優先度、スループット、遅延が中間のキュー。ほとんどの IP データはこのキューで送信されます。
- **Data 1 (Background):** 最低の優先度、高いスループットのキュー。高いスループットで遅延に敏感でないものはこのキューに送られます。(例: FTP データ)
- **Data 2 (Video):** 2番めの優先度キュー。ビデオはこのキューに送られます。
- **Data 3 (Voice):** 再優先のキュー。VoP やストリーミングメディアはこのキューに送られません。

拡張 QoS を設定する

1. Configuration > Wireless > Advanced > QoS Settings を選択して QoS Settings ページを表示します。

The screenshot shows the QoS Settings page for the 802.11a/na mode. The page is divided into two main sections: AP EDCA parameters and Station EDCA parameters. Each section contains a table with columns for Queue, AIFS, cwMin, cwMax, and Max. Burst (or TXOP Limit for Station EDCA).

AP EDCA parameters				
Queue	AIFS	cwMin	cwMax	Max. Burst
Data 0 (Best Effort)	3	15	63	0
Data 1 (Background)	7	15	1023	0
Data 2 (Video)	1	7	15	3008
Data 3 (Voice)	1	3	7	1504

Station EDCA parameters				
Queue	AIFS	cwMin	cwMax	TXOP Limit
Data 0 (Best Effort)	3	15	1023	0
Data 1 (Background)	7	15	1023	0
Data 2 (Video)	2	7	15	3008
Data 3 (Voice)	2	3	7	1504

2. 802.11a/na タブを選択して 802.11a/na モードの設定をすることもできます。
3. 以下の項目を設定します。

項目	説明
AP EDCA parameters	
AIFS	AIFS(Arbitration Inter-Frame Spacing) はデータフレーム間の待機時間(ms)を指定します。大きな値は高いプライオリティを表します。範囲は 0-8 です。デフォルト Data 0: 3; Data 1: 7; Data 2: 1; Data 3: 1.
cwMin	cwMin(Minimum Contention Window: 最小コンテンションウィンドウ) はバックオフ時間の上限(ms)を指定します。小さい値は優先度が高くなります。cwMin は cwMax よりも小さな値である必要があります。有効な値は 0, 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023 です。デフォルト値は Data 0: 15; Data 1: 15; Data 2: 7; Data 3: 3.

cwMax	<p>cwMax (Maximum Contention Window: 最大コンテンションウィンドウ) はバックオフ時間の上限(ms)を指定します。小さい値は優先度が高くなります。cwMax は cwMin よりも大きな値である必要があります。有効な値は 0, 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023 です。</p> <p>デフォルト値は Data 0: 63; Data 1: 1023; Data 2: 15; Data 3: 7.</p>
Max. Burst	<p>最大バースト時間(ms)を設定します。小さくするとキューの優先度が高くなります。値の範囲は 0 と 8192 を含む 32 の整数倍です。</p> <p>デフォルト値: Data 0: 0; Data 1: 0; Data 2: 3008; Data 3: 1504.</p>
Station EDCA parameters	
AIFS	<p>AIFS(Arbitration Inter-Frame Spacing) はデータフレーム間の待機時間(ms)を指定します。大きな値は高いプライオリティを表します。範囲は 0-8 です。</p> <p>デフォルト: Data 0: 3; Data 1: 7; Data 2: 2; Data 3: 2.</p>
cwMin	<p>cwMin (Minimum Contention Window: 最小コンテンションウィンドウ) はバックオフ時間の上限(ms)を指定します。小さい値は優先度が高くなります。cwMin は cwMax よりも小さな値である必要があります。有効な値は 0, 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023 です。</p> <p>デフォルト値は Data 0: 15; Data 1: 15; Data 2: 7; Data 3: 3.</p>
cwMax	<p>cwMax (Maximum Contention Window: 最大コンテンションウィンドウ) はバックオフ時間の上限(ms)を指定します。小さい値は優先度が高くなります。cwMax は cwMin よりも大きな値である必要があります。有効な値は 0, 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023 です。</p> <p>デフォルト値は: Data 0: 1023; Data 1: 1023; Data 2: 15; Data 3: 7.</p>
TXOP Limit	<p>クライアントがワイヤレスメディアに送信を開始する時間間隔(ms)を TXOP(Transmission Opportunity)でさせてします。値の範囲は 0 と 8192 を含む 32 の整数倍です。</p> <p>デフォルト値: Data 0: 0; Data 1: 0; Data 2: 3008; Data 3: 1504.</p>

4. Apply ボタンをクリックして設定を保存します。

ワイヤレスブリッジ設定

ワイヤレスアクセスポイントは大きなブリッジされたワイヤレスネットワークを構成出来る WDS(Wireless Distributing System)をサポートしています。以下のワイヤレスアクセスポイントのモードを選択できます。

- **Wireless point-to-point bridge:** このモードでは、ワイヤレスアクセスポイントは他のブリッジモードのワイヤレス端末と(オプションとして)ワイヤレスクライアントと通信できます。WEP、PA-PSK、WPA2-PSK を使って通信のセキュリティを高くします。
- **Wireless point-to-multipoint bridge:** このモードでは、ワイヤレスアクセスポイントがブリッジモードのワイヤレス端末グループのマスターになります。オプションとして、ワイヤレスアクセスポイントは他のワイヤレスクライアントと通信することもできます。最大 4 つのプロファイルを設定できます。

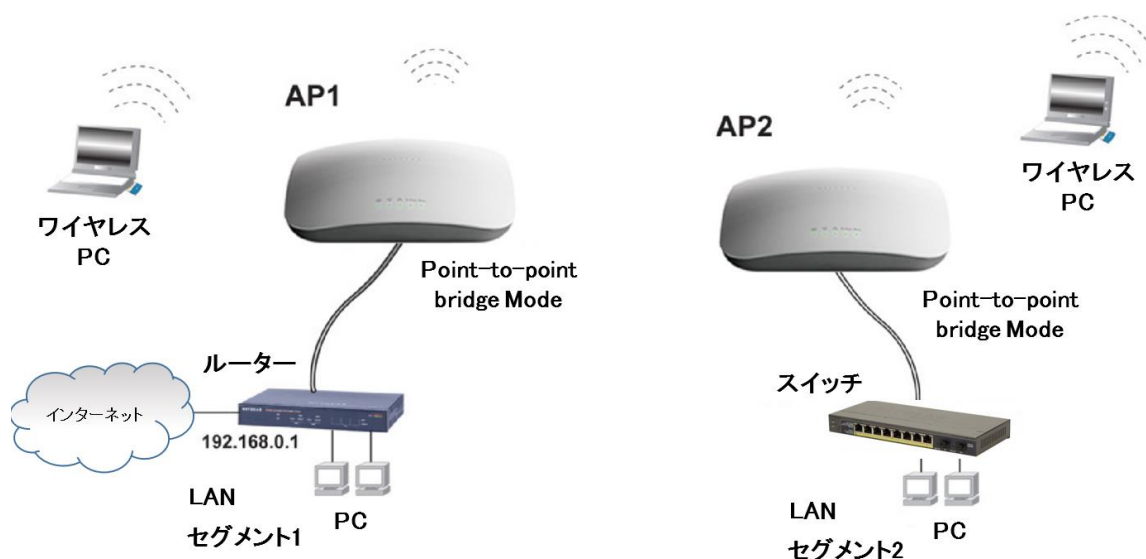
他のブリッジモードのワイヤレス端末はマスターのワイヤレスアクセスポイントの MAC アドレスを使って point-to-point bridge モード設定をする必要が他のすべてのブリッジモードのワイヤレス端末は、お互いに直接通信をするのではなく、マスターワイヤレスアクセスポイントを介して通信します。WEP、PA-PSK、WPA2-PSK を使って通信のセキュリティを高くします。

Repeating the wireless signal: このモードではワイヤレスアクセスポイントはワイヤレス信号をリピートします。ワイヤレスクライアント通信はサポートしていません。すべてのトラフィックをリモートアクセスポイントに転送します。このモードではワイヤレスクライアントはワイヤレスアクセスポイントと接続することはできません。WEP、PA-PSK、WPA2-PSK を使って通信のセキュリティを高くします。

メモ: チャンネルの自動設定が有効になっているとワイヤレスブリッジを設定することはできません。Wireless Settings 画面で Auto(自動)が選択されていないことを確認してください。

Point-to-Point ワイヤレス設定

Point-to-point bridge モードでは、ワイヤレスアクセスポイントは他のブリッジモードのワイヤレス端末と通信します。ワイヤレスセキュリティを使って通信を保護します。以下に 2 つのワイヤレスアクセスポイント (AP) が Point-to-point bridge モードで機能している図を示します。



Point-to-point ワイヤレスネットワークを設定する

1. Configuration > Wireless Bridge > Bridging を選択して Bridging ページを表示します。
2. 802.11b/bg/ng または 802.11a/na タブを選択します。

Configuration Monitoring Maintenance Support LOGOUT

System IP Wireless Security **Wireless Bridge**

> Bridging **Bridging**

802.11b/bg/ng 802.11a/na

Enable Wireless Bridging

Local MAC Address 04:A1:51:84:89:80

Wireless Point-to-Point Bridge **Wireless Point to Multi-Point Bridge**

Enable Wireless Client Association

#	Profile Name	Security	Enable
1	NETGEAR-WDS-1	Open System	<input checked="" type="checkbox"/>

EDIT CANCEL APPLY

3. ワイヤレスアクセスポイント (LAN セグメント 1 の AP1)を point-to-point bridge に設定します。
 - a. **Enable Wireless Bridging** チェックボックスを選択します。
 チャンネル設定が Auto の場合は警告が出ます。その場合は **Configuration > Wireless > Basic > Wireless Settings** ページで Channel を固定に設定します。
Local MAC Address 欄はワイヤレスアクセスポイントの MAC アドレスで変更不可の情報です。
 - b. **Wireless Point-to-Point Bridge** ラジオボタンを選択します。選択に従って画面表示が変更されます。
 - c. ワイヤレスアクセスポイント が point-to-point bridge のときにワイヤレスクライアントのアクセスも有効にしたい場合は、**Enable Wireless Client Association** チェックボックスをクリックします。
 - d. **Edit** ボタンをクリックしてセキュリティプロファイルを設定します。**Edit Security Profile** 画面が表示されます。

- e. 以下の項目を設定します。

項目	説明
Profile Definition	
Profile Name	わかりやすいプロファイル名を指定します。デフォルトは NETGEAR-WDS-1 です。

Remote MAC Address	リモート(対向)のワイヤレスアクセスポイントの MAC アドレス(LAN セグメント 2 の AP2 の MAC アドレス)	
Authentication Settings		
Network Authentication and Data Encryption	Network Authentication ドロップダウンリストから Open System , WPA-PSK , WPA2-PSK のいずれかを選択します。選択にしたがって設定項目が変更されます。	
	Open System	<p>認証および暗号化を使わないブリッジ通信設定は可能ですが、Open System の場合は WEP を使用することを推奨します。Data Encryption ドロップダウンリストから以下を選択します。</p> <ul style="list-style-type: none"> • None: 認証と暗号化を使用しません。 • 64-bit WEP: 40/64 ビットの WEP 鍵。 • 128-bit WEP: 104/128 ビットの WEP 鍵。 • 152-bit WEP: 128+24 ビットの WEP 鍵。このモードはこのモードをサポートしている端末とのみ利用可能です。
	WPA-PSK	<p>TKIP(Temporal Key Integrity Protocol)は WPA とともに用いられる標準暗号化方式であり、このドロップダウンリストで選択可能なものは TKIP のみです。WPA Passphrase (Network Key)欄にパスワードを入力します。パスワード長は 8-63 文字です。</p>
	WPA2-PSK	<p>AES(Advanced Encryption Standard) は WPA2 とともに用いられる標準暗号化方式であり、このドロップダウンリストで選択可能なものは AES のみです。WPA Passphrase (Network Key)欄にパスワードを入力します。パスワード長は 8-63 文字です。</p>
Link Test		

IP Address	<p>ワイヤレスアクセスポイントとワイヤレス端末の接続を確認するために、ワイヤレス端末の IP アドレスを入力し、Link Test ボタンをクリックします。Link Test Process Status 欄がテストの結果を表示します。(Uninitialized, In Process, Success, Timed Out, or Failure)</p> <p>メモ: 接続されたワイヤレス端末から両方のワイヤレスアクセルポイントの IP アドレスに対しても Ping してみるべきです。一つの AP に Ping 出来ない場合は、ブリッジ間の無線接続に問題があります。両方の AP に Ping 出来ない場合は、クライアントが正しく接続されていません。</p>
------------	---

- f. **Apply** ボタンをクリックして設定を保存します。**Bridging** 画面が再表示されます。
 - g. 正しいプロファイル名とセキュリティオプションが表示されたら、Enable 欄のチェックボックスを選択します。
 - h. 画面で **Apply** ボタンをクリックして設定を保存します。
3. LAN セグメント 2 の 2 台めのワイヤレスアクセスポイント (AP2) を point-to-point bridge モードに設定します。

AP1 の Remote MAC Address 欄に AP2 の MAC アドレスを設定します。AP2 の Remote MAC Address 欄に AP1 の MAC アドレスを設定します。

4. 両方のアクセスポイントで以下の設定を確認します。
 - ワイヤレスアクセスポイントの LAN ネットワーク設定を確認します。LAN デバイスと同じアドレスレンジで動作するようにします。
 - 両方のワイヤレスアクセスポイントは同じチャンネル、同じ認証方式、同じ暗号化設定を使います。
5. LAN1 から LAN2 までの接続を確認します。

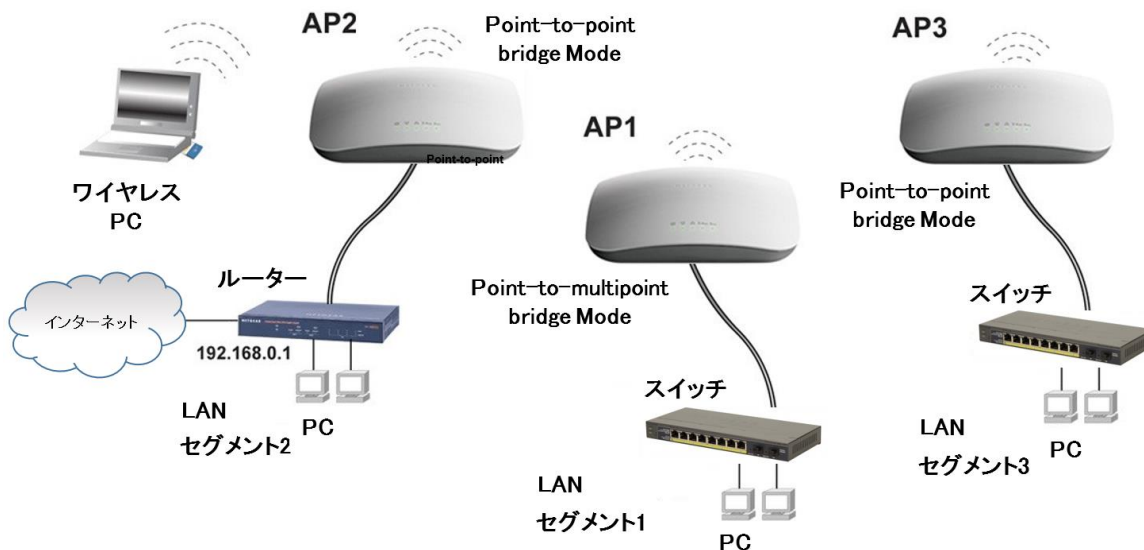
両側の LAN セグメントのコンピューターはインターネットや共有ファイル、プリンターにアクセスできます。

Point-to-Multipoint ワイヤレス設定

Point-to-multipoint bridge モードでは、ワイヤレスアクセスポイントはグループのブリッジモードワイヤレスアクセスポイントのマスターになります。すべてのトラフィックは他のワイヤレスアクセスポイントではなく、マスターワイヤレスアクセスポイントに送られます。ワイヤレスセキュリティを使って通信を保護します。

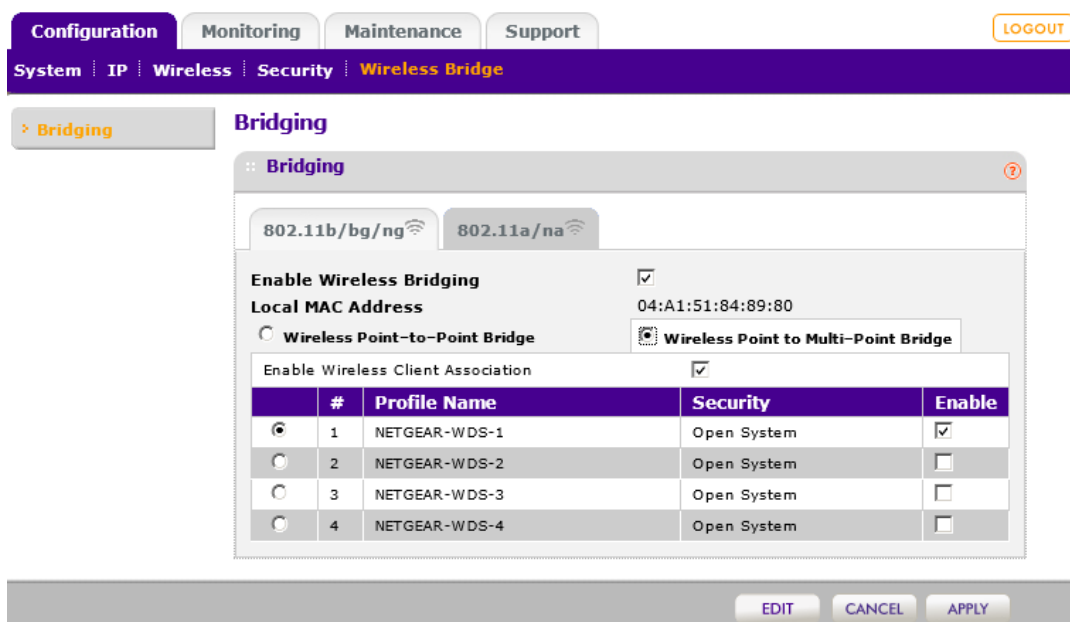
マスターに接続させたいワイヤレスアクセスポイントに対し、セキュリティプロファイルに識別可能な名前、およびワイヤレスアクセスポイントの MAC アドレスを設定します。4 つまでのセキュリティプロファイルを設定できます。(例: NETGEAR-WDS-1, NETGEAR-WDS-2, 等)

以下の図では AP1 が point-to-multipoint ブリッジモード、AP2 と AP3 が point-to-point ブリッジモードで動作しています。



Point-to-multipoint ワイヤレスネットワーク設定をする

1. Configuration > Wireless Bridge > Bridging を選択して Bridging ページを表示します。
2. 802.11b/bg/ng または 802.11a/na タブを選択します。
3. ワイヤレスアクセスポイント (LAN セグメント 1 の AP1) のセキュリティプロファイルを設定します。
 - a. Configuration > Wireless Bridge を選択します。Bridging 画面が表示されます。



- b. **Enable Wireless Bridging** チェックボックスを選択します。
 チャンネル設定が Auto の場合は警告が出ます。その場合は **Configuration > Wireless > Basic > Wireless Settings** ページで Channel を固定に設定します。
Local MAC Address 欄はワイヤレスアクセスポイントの MAC アドレスで変更不可の情報です。
- c. **Wireless Point-to-Multi-Point Bridge** ラジオボタンを選択します。選択に従って画面表示が変更されます。
- d. Profile テーブルは 4 つのセキュリティプロファイルを表示します。ラジオボタンで編集するセキュリティプロファイルを選択します。
- e. **Edit** ボタンをクリックしてセキュリティプロファイルを設定します。**Edit Security Profile** 画面が表示されます。

- f. 以下の項目を設定します。

項目	説明
Profile Definition	
Profile Name	わかりやすいプロファイル名を指定します。4 つのセキュリティプロファイルのデフォルトは NETGEAR-WDS-1、NETGEAR-WDS-2、NETGEAR-WDS-3、NETGEAR-WDS-4、です。
Remote MAC Address	リモート(対向)のワイヤレスアクセスポイントの MAC アドレス(LAN セグメント 2 の AP2 の MAC アドレス、LAN セグメント 3 の AP3 の MAC アドレス)

Authentication Settings	
Network Authentication and Data Encryption	<p>Network Authentication ドロップダウンリストから Open System, WPA-PSK, WPA2-PSK のいずれかを選択します。選択にしたがって設定項目が変更されます。</p>
	<p>Open System</p> <p>認証および暗号化を使わないブリッジ通信設定は可能ですが、Open System の場合は WEP を使用することを推奨します。Data Encryption ドロップダウンリストから以下を選択します。</p> <ul style="list-style-type: none"> • None: 認証と暗号化を使用しません。 • 64-bit WEP: 40/64 ビットの WEP 鍵。 • 128-bit WEP: 104/128 ビットの WEP 鍵。 • 152-bit WEP: 128+24 ビットの WEP 鍵。このモードはこのモードをサポートしている端末とのみ利用可能です。
	<p>WPA-PSK</p> <p>TKIP(Temporal Key Integrity Protocol)は WPA とともに用いられる標準暗号化方式であり、ここのドロップダウンリストで選択可能なものは TKIP のみです。WPA Passphrase (Network Key)欄にパスフレーズを入力します。パスフレーズ長は 8-63 文字です。</p>
	<p>WPA2-PSK</p> <p>AES(Advanced Encryption Standard) は WPA2 とともに用いられる標準暗号化方式であり、ここのドロップダウンリストで選択可能なものは AES のみです。WPA Passphrase (Network Key)欄にパスフレーズを入力します。パスフレーズ長は 8-63 文字です。 メモ: 802.11n の速度をえるために、WPA2-PSK 認証と AES 暗号化を推奨します。</p>
Link Test	
IP Address	<p>ワイヤレスアクセスポイントとワイヤレス端末の接続を確認するために、ワイヤレス端末の IP アドレスを入力し、Link Test ボタンをクリックします。Link Test Process Status 欄がテストの結果を表示します。(Uninitialized, In Process, Success, Timed Out, or Failure) メモ: 接続されたワイヤレス端末から両方のワイヤレスアクセルポイントの IP アドレスに対しても Ping してみるべきです。一つの AP に Ping 出来ない場合は、ブリッジ間の無線接続に問題がありま</p>

	す。両方の AP に Ping 出来ない場合は、クライアントが正しく接続されていません。
--	--

- g. **Apply** ボタンをクリックして設定を保存します。**Bridging** 画面が再表示されます。
- h. ステップ b~g を繰り返し、他のセキュリティプロファイルを編集します。
- 例えばセキュリティプロファイル NETGEAR-WDS-1 で AP2 の MAC アドレス、セキュリティプロファイル NETGEAR-WDS-2 で AP3 の MAC アドレスを設定します。
4. ワイヤレスアクセスポイント (LAN セグメント1の AP1)を point-to-multipoint bridge ブリッジとして(マスターとして)有効にします。
- Bridging 画面で **Enable Wireless Bridging** チェックボックスを選択します。
 - Wireless Point-to-Multi-Point Bridge** ラジオボタンを選択します。
 - Enable Wireless Client Association** チェックボックスをクリックしてワイヤレスクライアントアクセスを有効にします。
-
- メモ:** **Enable Wireless Client Association** チェックボックスを選択しないと、ワイヤレスアクセスポイントは point-to-multipoint ブリッジとしては動作せず、リピーターモードとして動作します。
-
- 正しいプロファイル名とセキュリティオプションが表示されている場合は、編集するセキュリティプロファイルの **Enable** 欄のチェックボックスを選択します。
 - Bridging 画面で **Apply** ボタンをクリックして point-to-point ブリッジ設定を有効にします。
5. LAN セグメント 2 の AP2 を AP1 のリモート MAC アドレスを使って point-to point モードに設定します。
6. すべてのワイヤレスアクセスポイントで以下の設定を確認します。
- LAN セグメント 1 の AP1 だけが point-to-multipoint ブリッジモード設定、他のすべての AP は point-to-point ブリッジモード設定である。
 - AP2 と AP3 (the point-to-point AP)は AP1 の MAC アドレスを Remote MAC Adress 欄に設定されている。
 - すべての AP は同じ LAN 上にある。すなわちすべての AP の LAN IP アドレスは LAN デバイスと同じネットワーク上にある。
 - DHCP を使っているなら、すべてのワイヤレスアクセスポイントは DHCP クライアントとして IP アドレスを取得する必要がある。
 - すべての ワイヤレスアクセスポイントは同じチャンネル、同じ認証モード、同じセキュリティ設定を持つ。

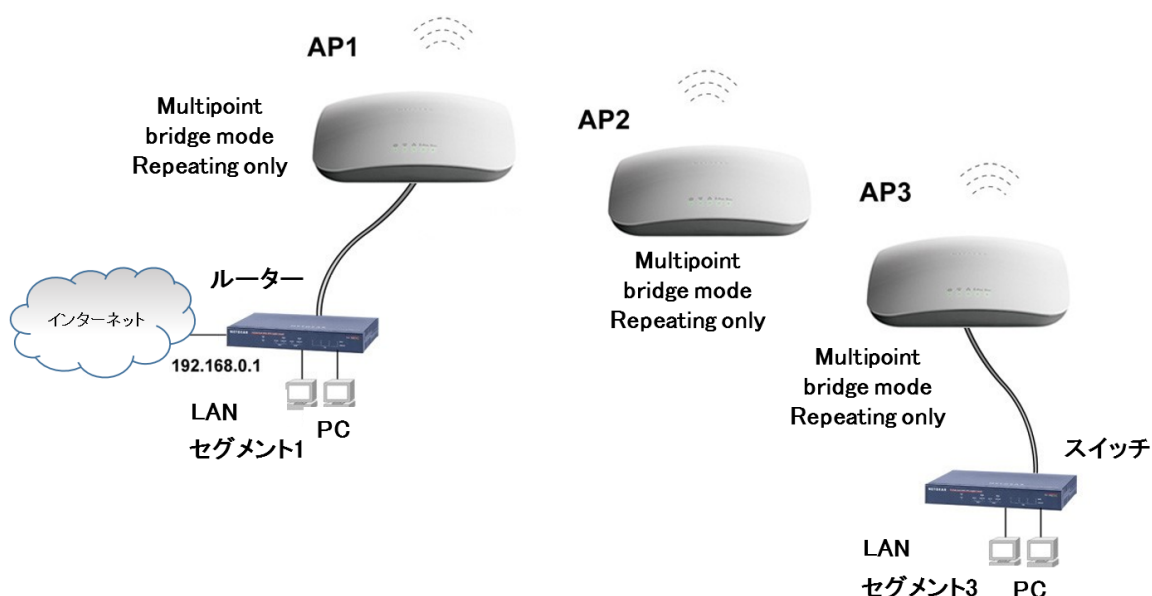
7. LAN 全体の接続性を確認します。

- どの LAN セグメントのコンピューターもどの LAN セグメントに接続されているインターネット、共有ファイル、プリンターにアクセス出来ます。

Point-to-Multipoint ブリッジモードを使ってワイヤレスアクセスポイントでワイヤレス信号をリピートする

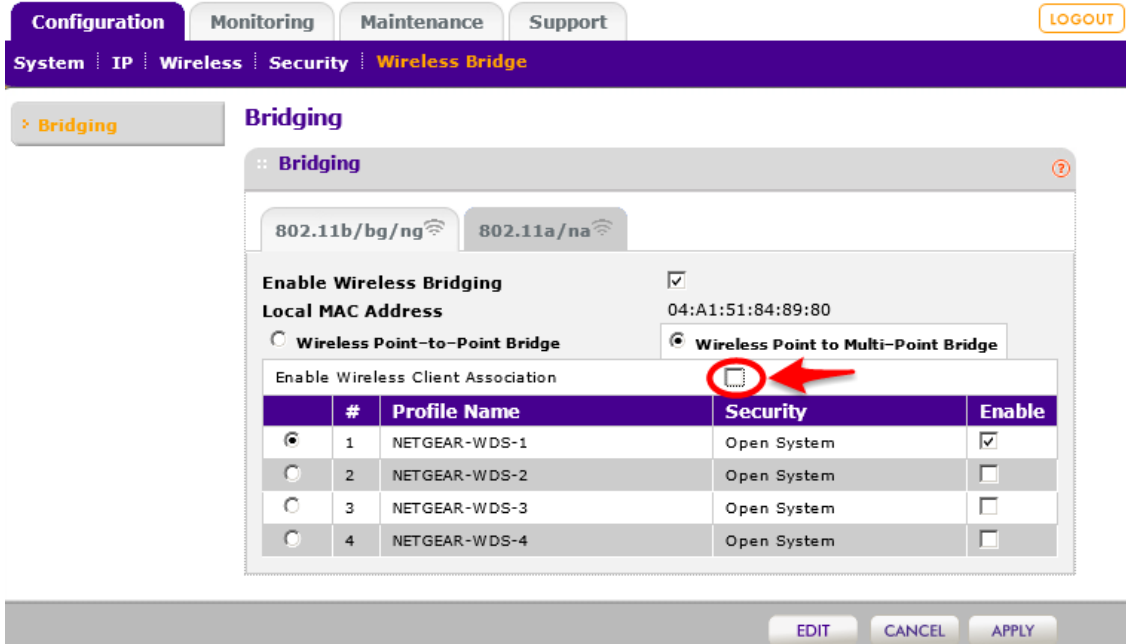
ワイヤレスアクセスポイントで他のワイヤレスクライアントに接続することなしにワイヤレス信号をリピートすることができます。すべてのトラフィックはリモートあるいは下位のワイヤレスアクセスポイントに送信されます。4つまでのセキュリティプロファイルを作成して4つのリモートのワイヤレスアクセスポイントへワイヤレス信号をリピートすることができます。それぞれのセキュリティプロファイルは異なった名前を保つ必要があり、リモートワイヤレスアクセスポイントのMACアドレスを持つ必要があります。4つまでのセキュリティプロファイルを設定できます。(NETGEAR-WDS-1, NETGEAR-WDS-2, 等)

以下の図では AP1、AP2、AP3 が point-to-multipoint ブリッジモードでワイヤレス信号をリピートしています。AP2 は AP1 用のセキュリティプロファイルと AP3 用のセキュリティプロファイルが必要です。

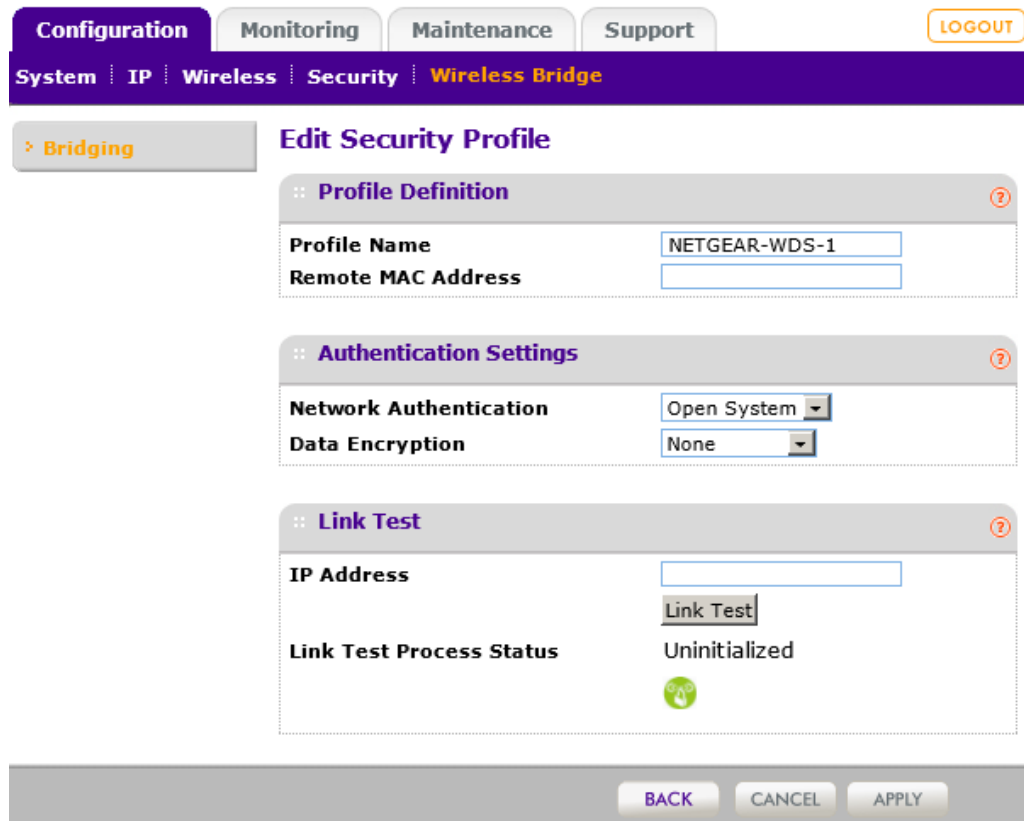


ワイヤレスアクセスポイントでワイヤレス信号をリピートする

1. (AP2 で) Configuration > Wireless Bridge > Bridging を選択して Bridging ページを表示します。



2. 802.11b/bg/ng または 802.11a/na タブを選択します。
 - a. Enable Wireless Bridging チェックボックスを選択します。Local MAC Address 欄はワイヤレスアクセスポイントの MAC アドレスで変更不可の情報です。



- b. **Wireless Point-to-Multi-Point Bridge** ボタンをクリックします。画面が選択に合わせて更新されます。
- c. **Enable Wireless Clinet Association** のチェックボックスをはずします。
- d. 4 つのセキュリティプロファイルが表示されます。編集するセキュリティプロファイルをラジオボタンで選択します。
- e. 以下の項目を設定します。

項目	説明	
Profile Definition		
Profile Name	わかりやすいプロファイル名を指定します。4 つのセキュリティプロファイルのデフォルトは NETGEAR-WDS-1、NETGEAR-WDS-2、NETGEAR-WDS-3、NETGEAR-WDS-4、です。	
Remote MAC Address	リモート(対向)のワイヤレスアクセスポイントの MAC アドレス(AP1 の MAC アドレスと AP3 の MAC アドレス)	
Authentication Settings		
Network Authentication and Data Encryption	Network Authentication ドロップダウンリストから Open System 、 WPA-PSK 、 WPA2-PSK のいずれかを選択します。選択にしたがって設定項目が変更されます。	
Network Authentication and Data Encryption (continued)	Open System	<p>認証および暗号化を使わないブリッジ通信設定は可能ですが、Open System の場合は WEP を使用することを推奨します。Data Encryption ドロップダウンリストから以下を選択します。</p> <ul style="list-style-type: none"> • None: 認証と暗号化を使用しません。 • 64-bit WEP: 40/64 ビットの WEP 鍵。 • 128-bit WEP: 104/128 ビットの WEP 鍵。 • 152-bit WEP: 128+24 ビットの WEP 鍵。このモードはこのモードをサポートしている端末とのみ利用可能です。
	WPA-PSK	<p>TKIP(Temporal Key Integrity Protocol)は WPA とともに用いられる標準暗号化方式であり、このドロップダウンリストで選択可能なものは TKIP のみです。WPA Passphrase (Network Key)欄にパスワードを入力します。パスワード長は 8-63 文字です。</p>
	WPA2-PSK	<p>AES(Advanced Encryption Standard) は WPA2 とともに用いられる標準暗号化方式であり、このドロップ</p>

		<p>ダウリストで選択可能なものは AES のみです。 WPA Passphrase (Network Key)欄にパスフレーズを入力します。パスフレーズ長は 8-63 文字です。 メモ: 802.11n の速度をえるために、WPA2-PSK 認証と AES 暗号化を推奨します。</p>
Link Test		
IP Address		<p>ワイヤレスアクセスポイントとワイヤレス端末の接続を確認するために、ワイヤレス端末の IP アドレスを入力し、Link Test ボタンをクリックします。Link Test Process Status 欄がテストの結果を表示します。(Uninitialized, In Process, Success, Timed Out, or Failure)</p>

- f. **Apply** ボタンをクリックして設定を保存します。Bridging 画面が表示されます。
 - g. ステップ d~f を繰り返し他のセキュリティプロファイルについても設定をします。
例: セキュリティプロファイル NETGEAR-WDS-1 に AP1 の MAC アドレス、NETGEAR-WDS-2 に AP3 の MAC アドレスを設定します。
3. ワイヤレスアクセスポイント(AP2)でリピーターモードを有効にします。
 - a. Bridging 画面で **Enable Wireless Bridging** チェックボックスを選択します。
 - b. **Wireless Point-to-Multi-Point Bridge** ラジオボタンを選択します。
 - c. **Enable Wireless Client Association** チェックボックスをはずしてワイヤレスクライアント接続を無効にします。

メモ: **Enable Wireless Client Association** のチェックボックスの選択をはずさないで、ワイヤレスアクセスポイントは通常の point-to-multipoint ブリッジモードで動作します。

 - d. 有効にするセキュリティプロファイルの **Enable** 欄のチェックボックスを選択します。
 - e. **Apply** ボタンをクリックしてリピーター設定を有効にします。
 4. LAN セグメント 1 の AP1 を AP2 のリモート MAC アドレスを使ってリピーターモードに設定します。
 5. LAN セグメント 3 の AP3 を AP2 のリモート MAC アドレスを使ってリピーターモードに設定します。
 6. すべてのワイヤレスアクセスポイントについて以下の設定を確認します。
 - すべての AP は同じ LAN 上にある。すなわちすべての AP の LAN IP アドレスは LAN デバイスと同じネットワーク上にある。

- DHCP を使っているなら、すべてのワイヤレスアクセスポイントは DHCP クライアントとして IP アドレスを取得する必要がある。
 - すべての ワイヤレスアクセスポイントは同じチャンネル、同じ認証モード、同じセキュリティ設定を持つ。
7. LAN 全体の接続性を確認します。
- どの LAN セグメントのコンピューターもどの LAN セグメントに接続されているインターネット、共有ファイル、プリンターにアクセス出来ます。

トラブルシューティング

この章では WNDAP360 のトラブルシューティングの情報を提供します。それぞれの問題の内容記述の後に、問題を診断、解決するために役立つ手順・方法を記述しています。

基本機能

ワイヤレスアクセスポイント起動後、以下のように LED の状態が変化します。

- 電源/テスト LED: **オレンジ点灯** => 消灯 => **緑点滅** => **緑点灯**(約 1 分経過後)
- アクティブ LED: イーサネットトラフィックがあるときには **緑点滅** します。
- LAN LED: 1000Mbps の時は **緑**、100Mbps の時は **オレンジ**、10Mbps のきは 消灯
- 無線 LAN LED: 無線 LAN が利用可能な場合は **緑点灯** あるいは **緑点滅** をします。

上の状態にならない場合は以下の該当する部分を参照してください。

ワイヤレスアクセスポイントの LED がどれも点灯しない

電源 LED が点灯するまで数秒かかることがあります。1 分ほど電源 LED が点灯するか待ってみてください。

もしもワイヤレスアクセスポイントに電源が入っていないならば:

PoE スイッチを使ってワイヤレスアクセスポイントに給電しているときは:

- ワイヤレスアクセスポイントと PoE スイッチの間のイーサネットケーブルがしっかりと接続されているか確認します。
- PoE スイッチの電源ケーブルがコンセントに接続されているか確認します。コンセントに電源が来ていることも確認します。
- PoE スイッチが正常に動作していることを確認します。

AC アダプターを使ってワイヤレスアクセスポイントに給電しているときは:

- AC アダプターがワイヤレスアクセスポイントに接続されていることを確認します。
- AC アダプターが電源を供給しているコンセントに接続されていることを確認します。
- ワイヤレスアクセスポイントに同梱されている AC アダプターを使っていることを確認します。

アクティブ LED または LAN LED が点灯しない

物理的な接続問題があります。

以下を確認します

- イーサネットケーブルのコネクタがワイヤレスアクセスポイントとスイッチ、ルーターと確実に接続されていることを確認します。
- 接続されている機器の電源が入っていることを確認します。
- 正しいケーブルを使っていることを確認します。カテゴリ5 以上のイーサネットケーブルを使用します。

無線 LAN LED が点灯しない

ワイヤレスアクセスポイントのアンテナが動作していません。

以下を確認します

- 無線 LAN が消灯したままの場合は、PoE スイッチと接続しているケーブルの抜き差しあるいは AC アダプターの接続しているコンセントの抜き差しをして電源の再起動を試みます。
- 外部アンテナを使用している場合は、アンテナの接続を確認します。

それでも点灯しない場合は NETGEAR カスタマーサポートに相談してください。

ワイヤレス可能なコンピューターからインターネットまたは LAN に接続できない

設定に問題があります。

以下を確認します

- ワイヤレスアダプターを持つコンピューターの TCP/IP 設定の変更が反映されていない場合があります。コンピューターを再起動を試みます。
- ワイヤレスアダプターを持つコンピューターの TCP/IP 設定が正しくない可能性があります。コンピューターを再起動して TCP/IP 設定が正しいか確認します。ウィンドウズコンピューターの場合には IP アドレスは自動で取得するように設定されています。
- ワイヤレスアクセスポイントのデフォルト設定値はお使いのネットワークでは動作しないかもしれません。ワイヤレスアクセスポイントのデフォルト設定とお使いのネットワークの他の機器の設定を比較してみてください。

- ワイヤレスアダプターを持つコンピューターの SSID、ネットワーク認証方式、データ暗号化方式設定がワイヤレスアクセスポイントの設定と同じか確認します。
- ワイヤレスアダプターを持つコンピューターとワイヤレスアクセスポイントの間の接続を確認するためにワイヤレスアクセスポイントの IP アドレスに Ping してみます。Ping が失敗した場合は、ネットワーク設定を再確認します。
- ワイヤレスアダプターを持つコンピューターからデフォルトゲートウェイへの接続を確認するためにデフォルトゲートウェイに Ping してみます。Ping が失敗した場合は、ネットワーク設定を見直し、インターネットサービスプロバイダーに連絡します。

ブラウザからワイヤレスアクセスポイントを設定できない

以下を確認します

- ワイヤレスアクセスポイントは正しくインストールされ、電源が入っており、LAN 接続もできているかを確認します。イーサネット接続に問題がないかアクティブ LED と LAN LED が点灯していることを確認します。
- コンピューターが固定 IP アドレスを使用しているならば、IP アドレスがワイヤレスアクセスポイントの IP アドレスの範囲に一致しているかを確認します。ワイヤレスアクセスポイントのデフォルト IP アドレスは 192.168.0.100、サブネットマスクは 255.255.255.0 です。DHCP クライアント機能の有効・無効はファームウェアのバージョンに依存します。ネットワーク設定が正しいか確認します。
- ワイヤレスアクセスポイントの NetBIOS 名を使って接続している場合は、お使いのコンピューターとワイヤレスアクセスポイントが同じネットワークセグメントにいるか、ネットワークに WINS サーバーが存在するかを確認します。
- コンピューターが IP アドレスを自動で取得 (DHCP クライアント機能を実行) するように設定されている場合はコンピューターを再起動します。
- お使いのブラウザで Java、JavaScript あるいは ActiveX が有効になっているか確認します。Internet Explorer をお使いの場合は Refresh を押して Java アプレットが読み込まれたか確認します。
- ブラウザーを終了し、キャッシュをクリアし、クッキーを削除した後ブラウザを起動してみます。
- 正しいログイン情報を使っているかを確認します。デフォルトログイン名は **admin**、パスワードは **password** です。入力する際に CAPS LOCK がオンになっていないことを確認します。

ワイヤレスアクセスポイントが Web 管理インターフェースで行った変更を保存していない場合は以下を確認します

- 設定をする際に、他の画面やタブに移動する前に確実に **Apply** ボタンをクリックしてください。クリックしない場合、設定は失われます。

- Web ブラウザーの **Refresh** または **Reload** ボタンをクリックしてみてください。Web ブラウザーが古い設定を表示している可能性があります。

ブラウザーに URL や IP アドレスを入力してもタイムアウトが発生する

いくつかの原因が考えられます。

以下のトラブルシューティングを試してみる

- LAN 上のコンピューターが正しく動作していることを確認します。コンピューターの TCP/IP 設定が正しいことを確認します。固定 IP アドレスを使用しているならば、サブネットマスク、デフォルトゲートウェイ、DNS、ワイヤレスアクセスポイントの IP アドレスを確認します。
- コンピューターが正しく設定されえいてもまだ接続できない時は、ワイヤレスアクセスポイントが接続されていて電源が入っていることを確認します。ワイヤレスアクセスポイントにアクセスして設定を確認します。ワイヤレスアクセスポイントにアクセスできない時は、LAN と電源を確認します。
- ワイヤレスアクセスポイントが正しく設定されているならば、お使いのインターネット接続（ブロードバンドルーターやモデム）が正しく動作しているかを確認します。

Ping を使って TCP/IP ネットワークをトラブルシュートする

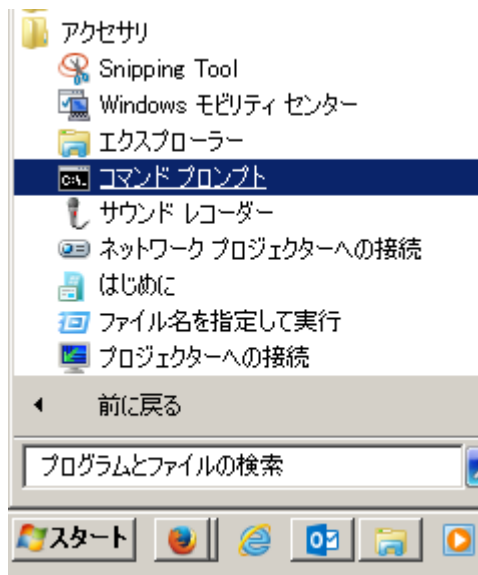
ほとんどの TCP/IP 端末やルーターはエコーリクエストパケットを特定のデバイスに送信する Ping ユーティリティを持っています。デバイスはエコーリプライで返答します。お使いのコンピューターで Ping ユーティリティを使うことで簡単に TCP/IP ネットワークをトラブルシュートできます。

ワイヤレスアクセスポイントへの LAN 接続を確認する

お使いのコンピューターからワイヤレスアクセスポイントへ Ping することでお使いのコンピューターからワイヤレスアクセスポイントへの LAN 接続が正しく設定できているかを確認することができます。

Windows コンピューターからワイヤレスアクセスポイントへ Ping する

1. スタート > すべてのプログラム > コマンドプロンプトを選択します。



コマンドプロンプトウィンドウが表示されます。

2. Ping のあとにワイヤレスアクセスポイントの IP アドレスを以下のように入力します。
`ping 192.168.1.12`
3. Enter キーを押します。

接続が正しい時は以下の図のような結果が表示されます。

```

C:\>ping 192.168.1.12

192.168.1.12 に ping を送信しています 32 バイトのデータ:
192.168.1.12 からの応答: バイト数 =32 時間 =2ms TTL=64
192.168.1.12 からの応答: バイト数 =32 時間 =2ms TTL=64
192.168.1.12 からの応答: バイト数 =32 時間 =3ms TTL=64
192.168.1.12 からの応答: バイト数 =32 時間 =2ms TTL=64

192.168.1.12 の ping 統計:
    パケット数: 送信 = 4、受信 = 4、損失 = 0 (0% の損失)、
ラウンド トリップの概算時間 (ミリ秒):
    最小 = 2ms、最大 = 3ms、平均 = 2ms

C:\>

```

接続が正しくない場合はタイムアウト等のエラー表示がされます。

4. 接続が正しくない場合、以下のどれかの理由が考えられます。

- 物理的な接続の誤り
 - アクティブ LED と LAN LED が点灯していることを確認します。
 - 接続されている機器のリンク LED が点灯していることを確認します。
- ネットワーク設定の誤り
 - コンピューターでイーサネットカードドライバと TCP/IP ソフトウェアがインストールされて設定されていることを確認します。
 - ワイヤレスアクセスポイントとお使いのワークステーションの IP アドレスが正しくかつ同じサブネット上にあることを確認します。

お使いのコンピューターからリモートデバイスへの接続を確認する

LAN 接続が正しく動作することを確認した後、お使いのコンピューターからリモートデバイスへの接続を確認します。

1. スタート > すべてのプログラム > コマンドプロンプトを選択します。
コマンドプロンプトウィンドウが表示されます。
2. Ping のあとに ISP の DNS サーバー等の IP アドレスへ Ping します。
3. 接続が正しくない場合は以下を確認します。
 - お使いのコンピューターがデフォルトアクセスポイントとしてルーターの IP アドレスを持っていること。お使いのコンピューターが DHCP でアドレスを取得している場合、この情報は見るできません。
 - お使いのコンピューターのネットワークアドレス(マスクで指定されている部分)リモートデバイスのネットワークアドレスと異なっていることを確認します。
 - ブロードバンドルーターやモデムが正しく接続されて動作していることを確認します。

日付と時間の問題

Configuration > System > Basic > Time で表示される Time 設定画面で現在の日付と時間を表示できます。ワイヤレスアクセスポイントは NTP(Network Time Protocol)を使って Time Setting 画面で設定したインターネット上のネットワークタイムサーバーから現在の日付と時間を取得します。ログ画面に記録されるエントリーには日時情報が記録されます。日付と時間機能の問題には以下のようなものがあります。

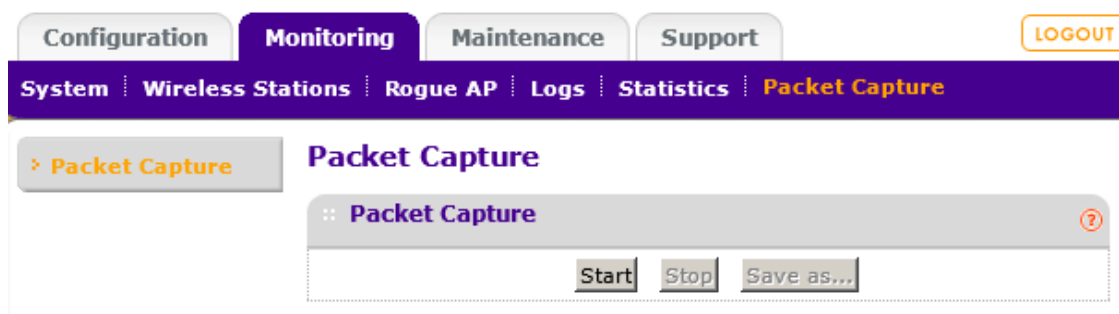
- 日付時間が正しくない。
原因: ワイヤレスアクセスポイントがまだネットワークタイムサーバーに接続できていない。インターネット接続設定が正しく設定されていることを確認します。ワイヤレスアクセスポイントを設定したばかりの時は最低 5 分間待ってから日時を確認してみます。
- 日付は正しいか 1 日前後している、時間が前後している。
原因: 異なるタイムゾーンを選択している。正しいタイムゾーンを選択します。

パケットキャプチャーツールを使う

ワイヤレスパケットをキャプチャーしてネットワークトラフィック解析ツールでトラフィックパターンを解析することができます。キャプチャーしたパケットフローは宛先にパケットが正しく流れているかパケットが廃棄されているかを見ることができます。ファイルにキャプチャーできるフローのサイズには限りがあります。

パケットをキャプチャーする

1. **Monitoring > Packet Capture** を選択して **Packet Capture** 画面を表示します。



2. **Start** ボタンをクリックしてワイヤレスアクセスポイントの使用中のチャンネルで送受信するワイヤレスパケットのキャプチャーを開始します。2.4GHz のパケットがキャプチャーできます。ワイヤレスアクセスポイントの通常動作には影響はありません

以前にキャプチャーしたパケットが存在する場合はそれらを廃棄する確認をする必要があり、新しいパケットのみをキャプチャーできます。
3. **Stop** ボタンをクリックしてキャプチャーを停止します。
4. **Save as** ボタンをクリックしてキャプチャーした capture.pcap ファイルをコンピューターに保存します。

A.補足情報

この付録では WNDAP360 の関連ドキュメント、工場出荷設定および技術資料を示します。以下の項目を含みます。

- [技術仕様](#)
- [工場出荷設定](#)

技術仕様

機能	仕様
802.11b/bg/ng ワイヤレス仕様	
802.11b データレート	1, 2, 5.5, 11 Mbps 自動可変
802.11bg データレート	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps, 自動可変
802.11ng MCS index と データレート	Data rates for a 20 MHz channel width and an automatic guard interval: 0 / 7.2 Mbps, 1 / 14.4 Mbps, 2 / 21.7 Mbps, 3 / 28.9 Mbps, 4 / 43.3 Mbps, 5 / 57.8 Mbps, 6 / 65 Mbps, 7 / 72.2 Mbps, 8 / 14.44 Mbps, 9 / 28.88 Mbps, 10 / 43.33 Mbps, 11 / 57.77 Mbps, 12 / 86.66 Mbps, 13 / 115.56 Mbps, 14 / 130 Mbps, 15 / 144.44 Mbps, 自動可変
	Data rates for a 20 MHz channel width and a long guard interval (800 ms): 0 / 6.5 Mbps, 1 / 13 Mbps, 2 / 19.5 Mbps, 3 / 26 Mbps, 4 / 39 Mbps, 5 / 52 Mbps, 6 / 58.5 Mbps, 7 / 65 Mbps, 8 / 13 Mbps, 9 / 26 Mbps, 10 / 39 Mbps, 11 / 52 Mbps, 12 / 78 Mbps, 13 / 104 Mbps, 14 / 117 Mbps, 15 / 130 Mbps, 自動可変
	Data rates for a 40 MHz channel width and an automatic guard interval: 0 / 15 Mbps, 1 / 30 Mbps, 2 / 45 Mbps, 3 / 60 Mbps, 4 / 90 Mbps, 5 / 120 Mbps, 6 / 135 Mbps, 7 / 150 Mbps, 8 / 30 Mbps, 9 / 60 Mbps, 10 / 90 Mbps, 11 / 120 Mbps, 12 / 180 Mbps, 13 / 240 Mbps, 14 / 270 Mbps, 15 / 300 Mbps, 自動可変

WNDAP360 管理マニュアル

	<p>Data rates for a 40 MHz channel width and a long guard interval (800 ms):</p> <p>0 / 13.5 Mbps, 1 / 27 Mbps, 2 / 40.5 Mbps, 3 / 54 Mbps, 4 / 81 Mbps, 5 / 108 Mbps,</p> <p>6 / 121.5 Mbps, 7 / 135 Mbps, 8 / 27 Mbps, 9 / 54 Mbps, 10 / 81 Mbps, 11 / 108 Mbps, 12 / 162 Mbps, 13 / 216 Mbps, 14 / 243 Mbps, 15 / 270 Mbps, 自動可変</p>
802.11b/bg/ng 動作周波数	<ul style="list-style-type: none"> • 2.412–2.462 GHz (US) • 2.457–2.462 GHz (Spain) • 2.410–2.484 GHz (Japan 11b) • 2.410–2.472 GHz (Japan 11ng) • 2.457–2.472 GHz (France) • 2.412–2.472 GHz (Europe ETSI) • 2.412–2.472 GHz (China)
802.11 b/bg/ng 暗号化	<ul style="list-style-type: none"> • 64-bit, 128-bit, and 52-bit WEP • AES • TKIP
802.11a/na ワイヤレス仕様	
802.11a データレート	6, 9, 12, 18, 24, 36, 48, 54 Mbps, 自動可変
802.11na データレート	<p>Data rates for a 20 MHz channel width and an automatic guard interval:</p> <p>0 / 7.2 Mbps, 1 / 14.4 Mbps, 2 / 21.7 Mbps, 3 / 28.9 Mbps, 4 / 43.3 Mbps,</p> <p>5 / 57.8 Mbps, 6 / 65 Mbps, 7 / 72.2 Mbps, 8 / 14.44 Mbps, 9 / 28.88 Mbps,</p> <p>10 / 43.33 Mbps, 11 / 57.77 Mbps, 12 / 86.66 Mbps, 13 / 115.56 Mbps, 14 / 130 Mbps, 15 / 144.44 Mbps, 自動可変</p>
	<p>Data rates for a 20 MHz channel width and a long guard interval (800 ms):</p> <p>0 / 6.5 Mbps, 1 / 13 Mbps, 2 / 19.5 Mbps, 3 / 26 Mbps, 4 / 39 Mbps, 5 / 52 Mbps,</p> <p>6 / 58.5 Mbps, 7 / 65 Mbps, 8 / 13 Mbps, 9 / 26 Mbps, 10 / 39 Mbps, 11 / 52 Mbps,</p> <p>12 / 78 Mbps, 13 / 104 Mbps, 14 / 117 Mbps, 15 / 130 Mbps, 自動可変</p>
	Data rates for a 40 MHz channel width and an automatic guard interval:

WNDAP360 管理マニュアル

	<p>0 / 15 Mbps, 1 / 30 Mbps, 2 / 45 Mbps, 3 / 60 Mbps, 4 / 90 Mbps, 5 / 120 Mbps, 6 / 135 Mbps, 7 / 150 Mbps, 8 / 30 Mbps, 9 / 60 Mbps, 10 / 90 Mbps, 11 / 120 Mbps, 12 / 180 Mbps, 13 / 240 Mbps, 14 / 270 Mbps, 15 / 300 Mbps, 自動可変</p> <p>Data rates for a 40 MHz channel width and a long guard interval (800 ms): 0 / 13.5 Mbps, 1 / 27 Mbps, 2 / 40.5 Mbps, 3 / 54 Mbps, 4 / 81 Mbps, 5 / 108 Mbps, 6 / 121.5 Mbps, 7 / 135 Mbps, 8 / 27 Mbps, 9 / 54 Mbps, 10 / 81 Mbps, 11 / 108 Mbps, 12 / 162 Mbps, 13 / 216 Mbps, 14 / 243 Mbps, 15 / 270 Mbps, 自動可変</p>
802.11a/na 動作周波数	<ul style="list-style-type: none"> • 5.180–5.240 GHz (US, lower frequencies) • 5.260–5.320 GHz (US, middle frequencies) • 5.180–5.240 GHz (CE [EU], lower frequencies) • 5.260–5.320 GHz (CE [EU], middle frequencies) • 5.500–5.680 GHz (CE [EU], upper frequencies)
802.11 a/na 暗号化	<ul style="list-style-type: none"> • 64-bit, 128-bit, and 52-bit WEP • AES • TKIP
管理およびその他の仕様	
ネットワーク管理	<ul style="list-style-type: none"> • Web 管理インターフェース、SNMP、Telnet または SSH (CLI) • SNMP MIB I, MIB II, 802.11 MIB 独自 MIB
最大クライアント	最大 64
ステータス LED	<ul style="list-style-type: none"> • 電源/テスト LED • リンク速度 LED • イーサネット LAN • ワイヤレス LAN (2.4 GHz と 5 GHz)
電気、物理仕様	
AC アダプター	12 VDC, 1A
物理仕様	<ul style="list-style-type: none"> • 寸法 (h x w x d): 253.75 x 253.75 x 54.76 mm • 重量: 0.886 kg
環境仕様	動作温度 0 to 55°C

WNDAP360 管理マニュアル

	動作湿度: 10-90%, 結露なきこと
法令遵守	
取得規格	FCC Part 15 Class B and Class E, CE, and C-TICK

工場出荷設定

ワイヤレスアクセスポイントの裏側のリセットボタンを長押ししてすべての設定を初期化して工場出荷設定に戻すことができます。これをハードリセットと呼びます。

ハードリセットを実行するには細長い棒のようなもので **Reset** ボタンを 5 秒以上 (電源/テスト LED が高速に点滅するまで) 長押しします。ワイヤレスアクセスポイントを次の表のように工場出荷状態に戻します。

メモ: リセットボタンを短時間押した場合はワイヤレスアクセスポイントの再起動のみとなります。

機能	設定
ログイン	
ユーザーログイン URL	192.168.0.100
ユーザー名 (大文字小文字を判別します)	admin
ログインパスワード (大文字小文字を判別します)	password
イーサネット	
固定 IP アドレス	192.168.0.210
イーサネット MAC アドレス	本体ラベルに記載
ポートスピード	10/100/1000Mbps
LAN	
LAN IP アドレス	192.168.0.100
サブネットマスク	255.255.255.0
ゲートウェイアドレス	0.0.0.0
DHCP サーバー	無効

DHCP クライアント	有効
タイムゾーン	USA-Pacific
SNMP	無効
Spanning Tree Protocol	無効
Secure Shell (SSH)	有効
Secure Telnet	無効
ワイヤレス LAN	
動作モード	アクセスポイント、インフラストラクチャーモード
ワイヤレスアクセスポイント名	netgearxxxxxx (xxxxxx はワイヤレスアクセスポイントの MAC アドレスの下 6 桁)
無線	有効
11 b/g/n SSID	NETGEAR_11ng
SSID のブロードキャスト	有効
セキュリティ	無効(open system)
転送速度	ベスト
802.11ng 電波、周波数チャンネル	自動
送信出力	Full
ワイヤレスアクセスリスト	すべてのワイヤレス端末を許可
WMM サポート	有効

B.コマンドライン

WNDAP360 は CLI、Web ブラウザーおよび MIB ブラウザーで設定ができます。
CLI を使って、Telnet または SSH 接続経由で設定を確認、変更することができます。

Keyword	Description
-backup-configuration	--backup configuration
-config>	--configuration setting
-apname	--access point name
-country	--country/region
-dhcp>	--DHCP server
-dns-server	--DNS server
-gateway	--default gateway
-ip-address	--IP range
-lease-time	--lease time
-status	--status
-subnet-mask	--subnet mask
-wins-server	--WINS server
-http-redirect	--enable HTTP redirection
-http-redirect-url	--HTTP redirection URL
-interface>	--select wireless lan interface
-wlan>	--wireless LAN interface setting
-2.4GHz>	--2.4 GHz wireless LAN interface setting
-aggregation-length	--aggregated packet size
-ampdu	--aggregated MAC Protocol Data Unit
-beacon-interval	--wireless beacon period in TU(1024 us)
-channel	--wireless channel (depends on country and wireless mode)
-channelwidth	--wireless channel width
-dtim-interval	--wireless DTIM period in beacon interval
-extension-protection-spacing	--wireless extension protection spacing
-fragmentation-length	--wireless fragmentation threshold(even only)
-guardinterval	--interval (from interference from other transmissions)
-knownap-add	--add known access point
-knownap-del	--delete known access point
-macacl-add	--add wireless access control (ACL)
-macacl-database	--delete wireless access control (ACL) database

WNDAP360 管理マニュアル

	-macacl-del	--delete wireless access control (ACL)
	-mcsrate	--transmit data rate
	-mode	--enable wireless access control (ACL)
	-operation-mode	--wireless operation mode
	-power	--wireless transmit power
	-preamble	--wireless preamble (only effect on 802.11b rates)
	-radio	--enable wireless radio
	-rate	--wireless transmission data rate
	-rifs-transmission	--enable successive frame transmission at different transmit powers
	-rogue-ap-detection	--enable rogue access point detection
	-rts-threshold	--wireless RTS/CTS threshold
	-security-profile>	--create security profile
	-1>	--1st security profile
	-authentication	--authentication type
	-encryption	--data encryption
	-hide-network-name	--hide network name
	-key1	--wireless wep key 1
	-key2	--wireless wep key 2
	-key3	--wireless wep key 3
	-key4	--wireless wep key 4
	-keyno	--key number
	-name	--profile name
	-presharedkey	--pre-shared key
	-security-separation	--disable associated wireless client communication
	-ssid	--network name (1-32 chars)
	-status	--profile status
	-vlan-id	--VLAN id
	-wep-pass-phrase	--wireless wep passphrase key
	-wepkeytype	--wireless wep key type
	-2>	--2nd security profile
	-authentication	--authentication type
	-encryption	--data encryption
	-hide-network-name	--hide network name
	-key1	--wireless wep key 1
	-key2	--wireless wep key 2
	-key3	--wireless wep key 3
	-key4	--wireless wep key 4
	-keyno	--key number
	-name	--profile name
	-presharedkey	--pre-shared key

WNDAP360 管理マニュアル

```
| | | | | |-security-separation    --disable associated wireless client communication
| | | | | |-ssid                    --network name (1-32 chars)
| | | | | |-status                  --profile status
| | | | | |-vlan-id                 --VLAN id
| | | | | |-wep-pass-phrase         --wireless wep passphrase key
| | | | | |-wepkeytype              --wireless wep key type
| | | | |
| | | | | |-3>                      --3rd security profile
| | | | | |-authentication          --authentication type
| | | | | |-encryption              --data encryption
| | | | | |-hide-network-name       --hide network name
| | | | | |-key1                    --wireless wep key 1
| | | | | |-key2                    --wireless wep key 2
| | | | | |-key3                    --wireless wep key 3
| | | | | |-key4                    --wireless wep key 4
| | | | | |-keyno                   --key number
| | | | | |-name                     --profile name
| | | | | |-presharedkey            --pre-shared key
| | | | | |-security-separation     --disable associated wireless client communication
| | | | | |-ssid                    --network name (1-32 chars)
| | | | | |-status                  --profile status
| | | | | |-vlan-id                 --VLAN id
| | | | | |-wep-pass-phrase         --wireless wep passphrase key
| | | | | |-wepkeytype              --wireless wep key type
| | | | |
| | | | | |-4>                      --4th security profile
| | | | | |-authentication          --authentication type
| | | | | |-encryption              --data encryption
| | | | | |-hide-network-name       --hide network name
| | | | | |-key1                    --wireless wep key 1
| | | | | |-key2                    --wireless wep key 2
| | | | | |-key3                    --wireless wep key 3
| | | | | |-key4                    --wireless wep key 4
| | | | | |-keyno                   --key number
| | | | | |-name                     --profile name
| | | | | |-presharedkey            --pre-shared key
| | | | | |-security-separation     --disable associated wireless client communication
| | | | | |-ssid                    --network name (1-32 chars)
| | | | | |-status                  --profile status
| | | | | |-vlan-id                 --VLAN id
| | | | | |-wep-pass-phrase         --wireless wep passphrase key
| | | | | |-wepkeytype              --wireless wep key type
```

WNDAP360 管理マニュアル

```
| | | | |
| | | | | |-5>                --5th security profile
| | | | | |-authentication    --authentication type
| | | | | |-encryption        --data encryption
| | | | | |-hide-network-name  --hide network name
| | | | | |-key1              --wireless wep key 1
| | | | | |-key2              --wireless wep key 2
| | | | | |-key3              --wireless wep key 3
| | | | | |-key4              --wireless wep key 4
| | | | | |-keyno             --key number
| | | | | |-name              --profile name
| | | | | |-presharedkey       --pre-shared key
| | | | | |-security-separation --disable associated wireless client communication
| | | | | |-ssid              --network name (1-32 chars)
| | | | | |-status            --profile status
| | | | | |-vlan-id           --VLAN id
| | | | | |-wep-pass-phrase    --wireless wep passphrase key
| | | | | |-wepkeytype        --wireless wep key type
| | | | |
| | | | | |-6>                --6th security profile
| | | | | |-authentication    --authentication type
| | | | | |-encryption        --data encryption
| | | | | |-hide-network-name  --hide network name
| | | | | |-key1              --wireless wep key 1
| | | | | |-key2              --wireless wep key 2
| | | | | |-key3              --wireless wep key 3
| | | | | |-key4              --wireless wep key 4
| | | | | |-keyno             --key number
| | | | | |-name              --profile name
| | | | | |-presharedkey       --pre-shared key
| | | | | |-security-separation --disable associated wireless client communication
| | | | | |-ssid              --network name (1-32 chars)
| | | | | |-status            --profile status
| | | | | |-vlan-id           --VLAN id
| | | | | |-wep-pass-phrase    --wireless wep passphrase key
| | | | | |-wepkeytype        --wireless wep key type
| | | | |
| | | | | |-7>                --7th security profile
| | | | | |-authentication    --authentication type
| | | | | |-encryption        --data encryption
| | | | | |-hide-network-name  --hide network name
| | | | | |-key1              --wireless wep key 1
```

WNDAP360 管理マニュアル

```
| | | | | |-key2          --wireless wep key 2
| | | | | |-key3          --wireless wep key 3
| | | | | |-key4          --wireless wep key 4
| | | | | |-keyno         --key number
| | | | | |-name          --profile name
| | | | | |-presharedkey  --pre-shared key
| | | | | |-security-separation --disable associated wireless client communication
| | | | | |-ssid          --network name (1-32 chars)
| | | | | |-status        --profile status
| | | | | |-vlan-id       --VLAN id
| | | | | |-wep-pass-phrase --wireless wep passphrase key
| | | | | |-wepkeytype    --wireless wep key type
| | | | |
| | | | | |-8>           --8th security profile
| | | | | |-authentication --authentication type
| | | | | |-encryption     --data encryption
| | | | | |-hide-network-name --hide network name
| | | | | |-key1           --wireless wep key 1
| | | | | |-key2           --wireless wep key 2
| | | | | |-key3           --wireless wep key 3
| | | | | |-key4           --wireless wep key 4
| | | | | |-keyno         --key number
| | | | | |-name          --profile name
| | | | | |-presharedkey  --pre-shared key
| | | | | |-security-separation --disable associated wireless client communication
| | | | | |-ssid          --network name (1-32 chars)
| | | | | |-status        --profile status
| | | | | |-vlan-id       --VLAN id
| | | | | |-wep-pass-phrase --wireless wep passphrase key
| | | | | |-wepkeytype    --wireless wep key type
| | | | |
| | | | |
| | | | | |-wireless-bridge> --wireless bridge setting
| | | | | |-security-profile> --create security profile
| | | | | |-1>           --1st security profile
| | | | | | |-authentication --authentication type
| | | | | | |-encryption     --data encryption
| | | | | | |-name          --profile name
| | | | | | |-presharedkey  --preshared key
| | | | | | |-remote-mac    --remote MAC
| | | | | | |-status        --profile status
| | | | | | |-wep-pass-phrase --wireless wep passphrase key
```


WNDAP360 管理マニュアル

```

| | | | | | | -wepkey             --wireless wep key
| | | | | | | -wepkeytype        --wireless wep key type
| | | | | | |
| | | | | | | |-2>              --2nd security profile
| | | | | | | |-authentication    --authentication type
| | | | | | | |-encryption       --data encryption
| | | | | | | |-name             --profile name
| | | | | | | |-presharedkey     --preshared key
| | | | | | | |-remote-mac      --remote MAC
| | | | | | | |-status          --profile status
| | | | | | | |-wep-pass-phrase  --wireless wep passphrase key
| | | | | | | |-wepkey          --wireless wep key
| | | | | | | |-wepkeytype      --wireless wep key type
| | | | | | |
| | | | | | | |-3>              --3rd security profile
| | | | | | | |-authentication    --authentication type
| | | | | | | |-encryption       --data encryption
| | | | | | | |-name             --profile name
| | | | | | | |-presharedkey     --preshared key
| | | | | | | |-remote-mac      --remote MAC
| | | | | | | |-status          --profile status
| | | | | | | |-wep-pass-phrase  --wireless wep passphrase key
| | | | | | | |-wepkey          --wireless wep key
| | | | | | | |-wepkeytype      --wireless wep key type
| | | | | | |
| | | | | | | |-4>              --4th security profile
| | | | | | | |-authentication    --authentication type
| | | | | | | |-encryption       --data encryption
| | | | | | | |-name             --profile name
| | | | | | | |-presharedkey     --preshared key
| | | | | | | |-remote-mac      --remote MAC
| | | | | | | |-status          --profile status
| | | | | | | |-wep-pass-phrase  --wireless wep passphrase key
| | | | | | | |-wepkey          --wireless wep key
| | | | | | | |-wepkeytype      --wireless wep key type
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | | |-wmm>             --wmm settings
| | | | | | | |-ap-data0-best-effort --access point best effort voice data
| | | | | | | |-ap-data1-background --access point low-priority data
| | | | | | | |-ap-data2-video    --access point video data

```

WNDAP360 管理マニュアル

```
| | | | |-ap-data3-voice          --access point voice data
| | | | |-station-data0-best-effort --station best effort voice data
| | | | |-station-data1-background  --station low-priority data
| | | | |-station-data2-video       --station video data
| | | | |-station-data3-voice       --station voice data
| | | | |-support                   --support
| | | |
| | | |
| | | |-5>                          --5 GHz wireless LAN interface setting
| | | |-aggregation-length         --aggregated packet size
| | | |-ampdu                       --aggregated MAC Protocol Data Unit
| | | |-beacon-interval            --wireless beacon period in TU(1024 us)
| | | |-channel                    --wireless channel (depends on country and wireless mode)
| | | |-channelwidth               --wireless channel width
| | | |-dtim-interval              --wireless DTIM period in beacon interval
| | | |-extension-protection-spacing --wireless extension protection spacing
| | | |-fragmentation-length       --wireless fragmentation threshold(even only)
| | | |-guardinterval              --interval (from interference from other transmissions)
| | | |-knownap-add                --add known access point
| | | |-knownap-del                --delete known access point
| | | |-macacl>                    --modify wireless access control (ACL)
| | | | |-add                       --add wireless access control (ACL)
| | | | |-del                       --delete wireless access control (ACL)
| | | |
| | | | |-macacl-add                --add wireless access control (ACL)
| | | | |-macacl-database           --delete wireless access control (ACL) database
| | | | |-macacl-del                --delete wireless access control (ACL)
| | | | |-mcsrate                   --transmit data rate
| | | | |-mode                      --enable wireless access control (ACL)
| | | | |-operation-mode            --wireless operation mode
| | | | |-power                     --wireless transmit power
| | | | |-radio                     --enable wireless radio
| | | | |-rate                      --wireless transmission data rate
| | | | |-rifs-transmission         --enable successive frame transmission at different
| | | | |                           transmit powers
| | | | |-rogue-ap-detection        --enable rogue access point detection
| | | | |-rts-threshold             --wireless RTS/CTS threshold
| | | | |-security-profile>        --create security profile
| | | | | |-1>                      --1st security profile
| | | | | | |-authentication        --authentication type
| | | | | | |-encryption            --data encryption
| | | | | | |-hide-network-name     --hide network name
```

WNDAP360 管理マニュアル

```
| | | | | |-key1          --wireless wep key 1
| | | | | |-key2          --wireless wep key 2
| | | | | |-key3          --wireless wep key 3
| | | | | |-key4          --wireless wep key 4
| | | | | |-keyno         --key number
| | | | | |-name          --profile name
| | | | | |-presharedkey  --pre-shared key
| | | | | |-security-separation --disable associated wireless client communication
| | | | | |-ssid          --network name (1-32 chars)
| | | | | |-status        --profile status
| | | | | |-vlan-id       --VLAN id
| | | | | |-wep-pass-phrase --wireless wep passphrase key
| | | | | |-wepkeytype     --wireless wep key type
| | | | |
| | | | | |-2>           --2nd security profile
| | | | | |-authentication --authentication type
| | | | | |-encryption     --data encryption
| | | | | |-hide-network-name --hide network name
| | | | | |-key1          --wireless wep key 1
| | | | | |-key2          --wireless wep key 2
| | | | | |-key3          --wireless wep key 3
| | | | | |-key4          --wireless wep key 4
| | | | | |-keyno         --key number
| | | | | |-name          --profile name
| | | | | |-presharedkey  --pre-shared key
| | | | | |-security-separation --disable associated wireless client communication
| | | | | |-ssid          --network name (1-32 chars)
| | | | | |-status        --profile status
| | | | | |-vlan-id       --VLAN id
| | | | | |-wep-pass-phrase --wireless wep passphrase key
| | | | | |-wepkeytype     --wireless wep key type
| | | | |
| | | | | |-3>           --3rd security profile
| | | | | |-authentication --authentication type
| | | | | |-encryption     --data encryption
| | | | | |-hide-network-name --hide network name
| | | | | |-key1          --wireless wep key 1
| | | | | |-key2          --wireless wep key 2
| | | | | |-key3          --wireless wep key 3
| | | | | |-key4          --wireless wep key 4
| | | | | |-keyno         --key number
| | | | | |-name          --profile name
```

WNDAP360 管理マニュアル

	-presharedkey	--pre-shared key
	-security-separation	--disable associated wireless client communication
	-ssid	--network name (1-32 chars)
	-status	--profile status
	-vlan-id	--VLAN id
	-wep-pass-phrase	--wireless wep passphrase key
	-wepkeytype	--wireless wep key type
	-4>	--4th security profile
	-authentication	--authentication type
	-encryption	--data encryption
	-hide-network-name	--hide network name
	-key1	--wireless wep key 1
	-key2	--wireless wep key 2
	-key3	--wireless wep key 3
	-key4	--wireless wep key 4
	-keyno	--key number
	-name	--profile name
	-presharedkey	--pre-shared key
	-security-separation	--disable associated wireless client communication
	-ssid	--network name (1-32 chars)
	-status	--profile status
	-vlan-id	--VLAN id
	-wep-pass-phrase	--wireless wep passphrase key
	-wepkeytype	--wireless wep key type
	-5>	--5th security profile
	-authentication	--authentication type
	-encryption	--data encryption
	-hide-network-name	--hide network name
	-key1	--wireless wep key 1
	-key2	--wireless wep key 2
	-key3	--wireless wep key 3
	-key4	--wireless wep key 4
	-keyno	--key number
	-name	--profile name
	-presharedkey	--pre-shared key
	-security-separation	--disable associated wireless client communication
	-ssid	--network name (1-32 chars)
	-status	--profile status
	-vlan-id	--VLAN id
	-wep-pass-phrase	--wireless wep passphrase key

WNDAP360 管理マニュアル

```
| | | | | |-wepkeytype          --wireless wep key type
| | | | |
| | | | | |-6>                  --6th security profile
| | | | | |-authentication      --authentication type
| | | | | |-encryption          --data encryption
| | | | | |-hide-network-name    --hide network name
| | | | | |-key1                --wireless wep key 1
| | | | | |-key2                --wireless wep key 2
| | | | | |-key3                --wireless wep key 3
| | | | | |-key4                --wireless wep key 4
| | | | | |-keyno               --key number
| | | | | |-name                 --profile name
| | | | | |-presharedkey         --pre-shared key
| | | | | |-security-separation  --disable associated wireless client communication
| | | | | |-ssid                 --network name (1-32 chars)
| | | | | |-status               --profile status
| | | | | |-vlan-id              --VLAN id
| | | | | |-wep-pass-phrase      --wireless wep passphrase key
| | | | | |-wepkeytype          --wireless wep key type
| | | | |
| | | | | |-7>                  --7th security profile
| | | | | |-authentication      --authentication type
| | | | | |-encryption          --data encryption
| | | | | |-hide-network-name    --hide network name
| | | | | |-key1                --wireless wep key 1
| | | | | |-key2                --wireless wep key 2
| | | | | |-key3                --wireless wep key 3
| | | | | |-key4                --wireless wep key 4
| | | | | |-keyno               --key number
| | | | | |-name                 --profile name
| | | | | |-presharedkey         --pre-shared key
| | | | | |-security-separation  --disable associated wireless client communication
| | | | | |-ssid                 --network name (1-32 chars)
| | | | | |-status               --profile status
| | | | | |-vlan-id              --VLAN id
| | | | | |-wep-pass-phrase      --wireless wep passphrase key
| | | | | |-wepkeytype          --wireless wep key type
| | | | |
| | | | | |-8>                  --8th security profile
| | | | | |-authentication      --authentication type
| | | | | |-encryption          --data encryption
```

WNDAP360 管理マニュアル

```
| | | | | |-hide-network-name      --hide network name
| | | | | |-key1                    --wireless wep key 1
| | | | | |-key2                    --wireless wep key 2
| | | | | |-key3                    --wireless wep key 3
| | | | | |-key4                    --wireless wep key 4
| | | | | |-keyno                   --key number
| | | | | |-name                    --profile name
| | | | | |-presharedkey            --pre-shared key
| | | | | |-security-separation     --disable associated wireless client communication
| | | | | |-ssid                    --network name (1-32 chars)
| | | | | |-status                  --profile status
| | | | | |-vlan-id                 --VLAN id
| | | | | |-wep-pass-phrase         --wireless wep passphrase key
| | | | | |-wepkeytype              --wireless wep key type
| | | | |
| | | | |
| | | | |-wireless-bridge>         --wireless bridge setting
| | | | |-security-profile>       --create security profile
| | | | | |-1>                     --1st security profile
| | | | | | |-authentication        --authentication type
| | | | | | |-encryption            --data encryption
| | | | | | |-name                  --profile name
| | | | | | |-presharedkey          --preshared key
| | | | | | |-remote-mac            --remote MAC
| | | | | | |-status                --profile status
| | | | | | |-wep-pass-phrase       --wireless wep passphrase key
| | | | | | |-wepkey                --wireless wep key
| | | | | | |-wepkeytype            --wireless wep key type
| | | | | |
| | | | | | |-2>                   --2nd security profile
| | | | | | | |-authentication      --authentication type
| | | | | | | |-encryption          --data encryption
| | | | | | | |-name                --profile name
| | | | | | | |-presharedkey        --preshared key
| | | | | | | |-remote-mac          --remote MAC
| | | | | | | |-status              --profile status
| | | | | | | |-wep-pass-phrase     --wireless wep passphrase key
| | | | | | | |-wepkey              --wireless wep key
| | | | | | | |-wepkeytype          --wireless wep key type
| | | | | | |
| | | | | | | |-3>                 --3rd security profile
| | | | | | | | |-authentication    --authentication type
```

WNDAP360 管理マニュアル

```

| | | | | | | -encryption          --data encryption
| | | | | | | -name                --profile name
| | | | | | | -presharedkey        --preshared key
| | | | | | | -remote-mac          --remote MAC
| | | | | | | -status              --profile status
| | | | | | | -wep-pass-phrase     --wireless wep passphrase key
| | | | | | | -wepkey              --wireless wep key
| | | | | | | -wepkeytype          --wireless wep key type
| | | | | | |
| | | | | | | |-4>                --4th security profile
| | | | | | | |-authentication     --authentication type
| | | | | | | |-encryption          --data encryption
| | | | | | | |-name                --profile name
| | | | | | | |-presharedkey        --preshared key
| | | | | | | |-remote-mac          --remote MAC
| | | | | | | |-status              --profile status
| | | | | | | |-wep-pass-phrase     --wireless wep passphrase key
| | | | | | | |-wepkey              --wireless wep key
| | | | | | | |-wepkeytype          --wireless wep key type
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | | |-wmm>              --wmm settings
| | | | | | | |-ap-data0-best-effort --access point best effort voice data
| | | | | | | |-ap-data1-background --access point low-priority data
| | | | | | | |-ap-data2-video      --access point video data
| | | | | | | |-ap-data3-voice     --access point voice data
| | | | | | | |-station-data0-best-effort --station best effort voice data
| | | | | | | |-station-data1-background --station low-priority data
| | | | | | | |-station-data2-video  --station video data
| | | | | | | |-station-data3-voice  --station voice data
| | | | | | | |-support            --???
| | | | | | |
| | | | | | |
| | | |
| | |
| |
| |-ip>                --set host IP
| | |-address           --host IP address
| | |-default-gateway  --IP address of default gateway
| | |-dhcp-client      --enable dhcp client
| | |-dns-server       --IP address of DNS server
| |

```

WNDAP360 管理マニュアル

```
| |-log> --syslog setting
| | |-syslog --enable syslog client
| | |-syslog-server-ip --syslog server IP address
| | |-syslog-server-port --syslog server port number
| |
| |-radius>
| | |-accounting-server-primary --primary accounting server
| | |-accounting-server-primary-port --primary accounting server port
| | |-accounting-server-primary-sharedsecret --primary accounting server shared secret
| | |-accounting-server-secondary --secondary accounting server
| | |-accounting-server-secondary-port --secondary accounting server port
| | |-accounting-server-secondary-sharedsecret --secondary accounting server shared secret
| | |-authentication-server-primary --primary authentication server
| | |-authentication-server-primary-port --primary system accounting server shared
| | | secret
| | |-authentication-server-primary-sharedsecret --primary authentication server shared secret
| | |-authentication-server-secondary --secondary authentication server
| | |-authentication-server-secondary-port --secondary authentication server port
| | |-authentication-server-secondary-sharedsecret --secondary authentication server shared
| | | secret
| |
| |-remote> --enable remote access via SSH
| | |-ssh-port --SSH port
| | |-sshd --SSH daemon
| | |-telnet --enable remote access via Telnet
| |
| |-snmp> --SNMP setting
| | |-description --SNMP system description
| | |-read-community --SNMP ReadCommunity
| | |-snmp-status --SNMP status
| | |-trap-community --SNMP ReadCommunity
| | |-trap-server --SNMP TrapServer IP address
| | |-write-community --SNMP WriteCommunity
| |
| |-spanning-tree --enable spanning tree protocol
| |-time> --time Setting
| | |-custom-ntp-server --custom NTP server host name
| | |-daylightsaving --daylight saving
| | |-ntp-client --NTP client host name
| | |-ntp-server --NTP server host name
| | |-time-zone --time zone
| |
```


WNDAP360 管理マニュアル

```
| |-vlan> --vlan settings
| | |-management-vlan --vlan management id
| | |-untagged-vlan --untagged vlan id
| | |-untagged-vlan-status --untagged vlan status
| |
|-exit --logout from CLI
|-file --
|-firmware-upgrade --upload new system firmware file
|-password --system password
|-restore-configuration --restore system configuration
|-restore-default-password --restore default system password
|-show> --show system settings
| |-configuration --show system configuration
| |-interface> --show wireless lan interface
| | |-eth> --ethernet interface
| | | |-statistics --show ethernet statistics
| | |
| | | |-wlan> --wlan interface settings
| | | | |-2.4GHz> --2.4GHz wlan interface settings
| | | | | |-configuration --interface configuration
| | | | | |-knownaplist --known access point list
| | | | | |-stationlist --station list
| | | | | |-statistics --interface statistics
| | | | | |-trusted-stationlist --trusted station list
| | | | | |-unknownaplist --unknown access point list
| | | |
| | | | |-5GHz> --5GHz wlan interface settings
| | | | | |-configuration --interface configuration
| | | | | |-knownaplist --known access point list
| | | | | |-stationlist --station list
| | | | | |-statistics --interface statistics
| | | | | |-trusted-stationlist --trusted station list
| | | | | |-unknownaplist --unknown access point list
| | | |
| | |
| |
| |-log --system log
| |-system --system setting
```