

DAP-X2850
802.11ax 4×4 PoE Access Point

ユーザマニュアル



目次

1. お使いになるまえに	4
本製品について	5
機能概要	5
本製品の特長	5
製品名/品番一覧	5
本製品の接続モード	6
Nuclias Connectについて	7
概要	7
Nuclias Connectの特長	7
本マニュアルについて	8
マニュアルの構成	8
マニュアルの対象者	8
表記規則	8
安全にお使いいただくために	9
ご使用上の注意	11
静電気障害を防止するために	11
電源の異常	11
無線LANについて	12
WLAN 技術を利用するさまざまな理由	12
無線に関するご注意	13
2. 設置のしかた	16
パッケージの内容	17
動作環境	17
ネットワーク接続前の準備	17
本体各部名称	18
前面パネル	18
背面パネル	18
製品の設置	19
イーサネットケーブルの接続/電源の投入	19
マウントキットによる設置	20
デスクトップでの使用	21
3. WEB GUI 画面について	22
WEB GUI画面へのログイン	23
初回ログイン時のセットアップ	24
画面の構成	26
4. Basic Settings (基本設定)	27
Basic Settings について	28
Wireless Settings (ワイヤレス設定)	28
Access Point モードを選択した場合	29
WDSモード/WDS with APモードを選択した場合	31
Wireless Clientモードを選択した場合	33
Authentication (認証) の設定について	35
LAN Settings (LAN設定)	39
IPv6 Settings (IPv6設定)	40
5. Advanced Settings (詳細設定)	41
Advanced Settings について	42
Performance Settings (パフォーマンス設定)	42
Wireless Resource Control (ワイヤレスリソースコントロール)	45
Multi-SSID Settings (マルチSSID設定)	46
VLAN Settings (VLAN設定)	48
Wireless Intrusion Protection (不正AP検知)	52
Wireless Schedule Settings (スケジュール設定)	53
Internal RADIUS Server (RADIUSサーバ)	54

ARP Spoofing Prevention Settings (ARPスプーフィング防止設定)	55
Bandwidth Optimization (帯域幅最適化)	56
Captive Portal (キャプティブポータル)	58
Login Page Upload (ログイン画面アップロード)	65
MAC Bypass (MAC Bypass 設定)	66
Walled Garden (ウォールドガーデン 設定)	67
DHCP Server (DHCPサーバ設定)	68
Dynamic Pool Settings (ダイナミックプール設定)	68
Static Pool Settings (スタティックプール設定)	69
Current IP Mapping List (IPマッピングリスト)	70
Filters (フィルタ)	71
Wireless MAC ACL Settings (ワイヤレスMAC ACL)	71
WLAN Partition (WLANパーティション)	72
IP Filter Settings (IPフィルタ)	73
Traffic Control (トラフィックコントロール)	75
Uplink and Downlink Setting (アップリンク/ダウンリンク設定)	75
QoS (QoS設定)	76
Traffic Manager (トラフィックマネージャ)	77
6. Status (ステータス)	79
Statusについて	80
Device Information (デバイス情報)	80
Client Information (クライアント情報)	82
WDS Information (WDS情報)	82
Channel Analyze (チャネル分析)	83
Statistics (統計情報)	84
Ethernet Traffic Statistics (イーサネットトラフィック統計情報)	84
WLAN Traffic Statistics (WLANトラフィック統計情報)	85
Log (ログ)	86
View Log (ログの表示)	86
Log Settings (ログ設定)	87
7. 管理メニュー	89
管理メニューについて	90
Home (ホーム画面)	90
Maintenance (メンテナンス)	91
Administration Settings (管理設定)	91
Firmware and SSL Certification Upload (ファームウェアとSSL証明書のアップロード)	98
Configuration File Upload and Download (コンフィグレーションファイルのアップロードとダウンロード)	99
Time and Date Settings (時刻と日付の設定)	100
Configuration (コンフィグレーション)	101
設定の保存と有効化	101
設定の破棄	101
System (システム設定)	102
本製品の再起動	102
工場出荷時設定へのリセット	102
Language Packの削除	103
Logout (ログアウト)	104
Help (ヘルプ)	104
8. 付録	105
工場出荷時設定に戻す	106
リセットボタンで設定リセットを行う	106
Web GUIから設定リセットを行う	106
FAQ	107
機能設定例	108
対象機器について	108
VLAN	108

お使いになるまえに

1

このたびは、弊社製品をお買い上げいただきありがとうございます。
本書は、製品を正しくお使いいただくための取扱説明書です。必要な場合には、いつでもご覧いただけますよう大切に保管してください。

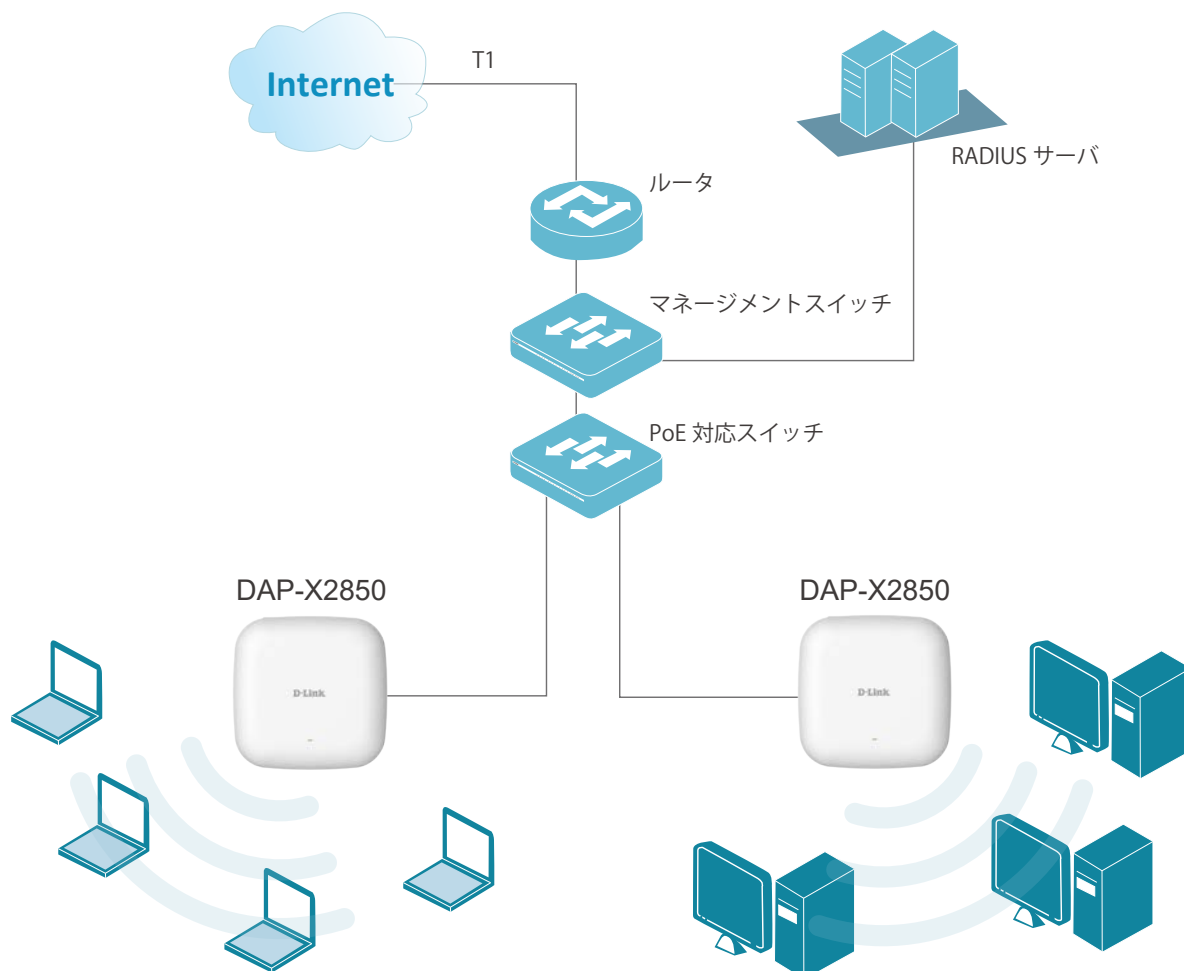
また、必ず本書および設置マニュアルをよくお読みいただき、内容をご理解いただいた上で記載事項に従ってご使用ください。

■ 本製品について.....	5
機能概要.....	5
本製品の特長.....	5
製品名/品番一覧.....	5
本製品の接続モード.....	6
■ Nuclias Connectについて.....	7
概要.....	7
Nuclias Connectの特長.....	7
■ 本マニュアルについて.....	8
マニュアルの構成.....	8
マニュアルの対象者.....	8
表記規則.....	8
■ 安全にお使いいただくために.....	9
■ ご使用上の注意.....	11
■ 静電気障害を防止するために.....	11
■ 電源の異常.....	11
■ 無線LANについて.....	12
WLAN 技術を利用するさまざまな理由.....	12
無線に関するご注意.....	13

本製品について

■機能概要

DAP-X2850は、エンタープライズユースに最適の2.4GHz/5GHz デュアルバンド同時利用対応アクセスポイントです。IEEE 802.11axに対応しています。



■本製品の特長

- IEEE 802.11a/b/g/n/ac/ax 準拠
- デュアルバンド通信 (2.4GHz/5GHz同時利用)
- WPA/WPA2/WPA3 Enterprise/Personal暗号方式
- MAC アドレスフィルタリング
- ARP スプーフィング防止
- マルチ SSID (周波数帯ごと 8個)
- QoS (WMM 準拠)
- 無線機能のスケジューリング
- GUI、SSL による設定 / 管理
- 4 つの通信モード (アクセスポイント/ワイヤレスクライアント/WDS/WDS with AP)
- Nuclias Connectによる管理※
- MU-MIMO

※対応予定

■製品名/品番一覧

製品名	品番
DAP-X2850	DAP-X2850/A1

■本製品の接続モード

本製品には以下の4つの接続モードがあります。

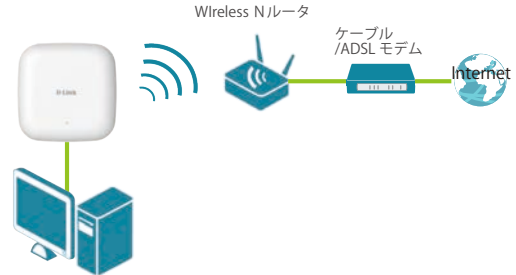
■アクセスポイントモード

無線アクセスポイントと無線クライアントのネットワークを構築します。



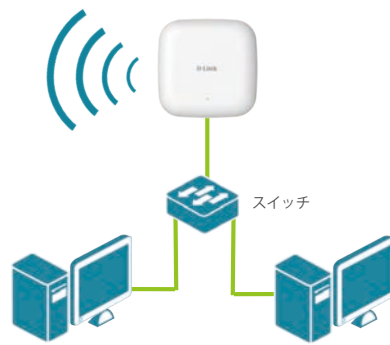
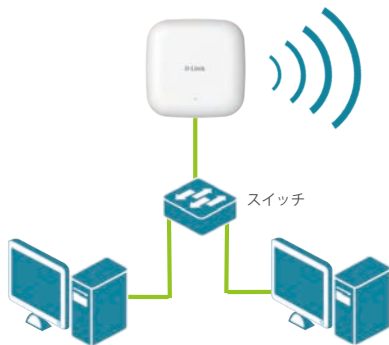
■ワイヤレスクライアントモード

イーサネット用機器向けの無線ネットワークアダプタとして動作します。



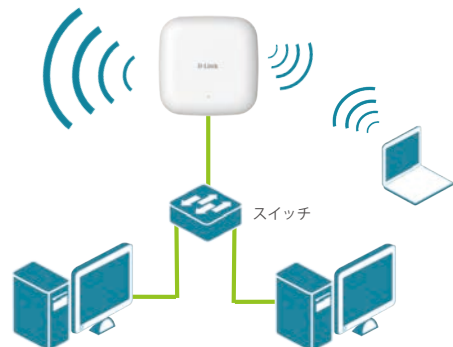
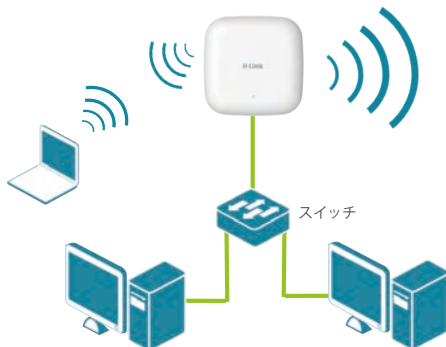
■WDS モード

複数のネットワークを無線接続します。



■WDS with AP モード

無線 LAN アクセスポイントとして動作しながら、複数のネットワークと無線接続します。



メモ

WDSモード及びWDS with APモードは、2.4GHz帯および5GHz帯のW52の周波数帯でのみ利用可能です。

重要

異機種間、異なるファームウェアバージョン間でWDSモード、WDS with APモードを使用することはできません。

Nuclias Connectについて

メモ

- ・本APはNuclias Connectをサポートしていません。将来のファームウェアで対応予定です。

概要

Nuclias Connectは、中小企業向けのD-Linkの一元管理ソリューションです。Nuclias Connectを使用することで、ネットワークの分析、自動化、設定、最適化、拡張、セキュリティ保護が容易になり、企業ネットワークの包括的な管理ソリューションを実現します。本システムでは、堅牢で一元化された管理システムの維持と、小規模ネットワークから大規模ネットワーク（最大1500AP）へ拡張可能なコスト的/技術的な柔軟性を提供します。

また、直感的なグラフィカルユーザインタフェース (GUI)、豊富な拡張AP機能、11言語をサポートするセットアップウィザードにより、導入、設定、および管理作業の煩わしさを最小限に抑えます。Nuclias Connectは無償のダウンロードソフトウェアであり、ライセンス不要でWindowsサーバ（またはDocker経由によりLinux^{※1}）、スマートフォン^{※2}（簡易マネージメントアプリ）に導入して最大1,500台まで管理することができます。Nuclias Connectを搭載した安価なアプライアンス製品（Nuclias Connect Hub）を利用することも可能です。

Nuclias Connectは、ネットワーク上のすべての無線アクセスポイント（AP）に対し、ソフトウェアベースによる監視・リモート管理を提供します。これにより、従来のハードウェアベースの統合管理システムに比べ、より柔軟性の高い管理ソリューションを実現します。（リモートからの設定、包括的/部分的なネットワークトラフィック分析、負荷分散、エアタイムフェアネス、ローカライズされたスロットリング）

Nuclias Connectでは、各ネットワークに対しローカル管理権限を付与することで、ネットワーク毎の管理を行うことができます。また、APは周波数帯ごとに8つのSSID（APごと最大16個のSSID）をサポートしており、管理者はこれらのSSIDを訪問者用のゲストネットワークとして設定することもできます。

Nuclias Connectは、APが同じレイヤ2/レイヤ3ネットワークに存在する場合に、最小限のユーザの労力によりAPの検出とプロファイルのインポートを実行します。これらの処理は、必要に応じてグループまたは個々のAPに対しても実施可能です。

Nuclias Connectのソフトウェアはネットワーク上で透過的に動作するため、APはNAT環境内の任意の場所に配置できます。管理者は各配信について、構成や管理者アカウントの設定など、さまざまな設定を提供および管理できます。

Nuclias Connectでは、SSIDごとにアクセス制御やユーザ認証を設定することが可能です。そのほか、キャプティブポータルやWi-Fiホットスポットなど、より高度な付加価値サービスを有効にすることもできます。これにより、異なるサブネットに対して個別の内部ネットワークを設定することができます。

※1 対応予定

※2 スマートフォンアプリは複数の拠点を管理したい場合に、プロファイルを適用するために必要となります。

Nuclias Connectの特長

- ・無償の管理ソフトウェア
- ・各種ログ
- ・トラフィックのレポートと分析
- ・カスタマイズ可能なキャプティブポータル、802.1X認証、MACフィルタリング
- ・リモート設定およびバッチ設定
- ・日本語GUI
- ・直感的なインタフェース
- ・ネットワーク毎のアクセス権限

本マニュアルについて

■マニュアルの構成

- 1章: お使いになるまえに**
本マニュアルの紹介と、本製品をお使いになる前の注意事項を記載しています。
→『[お使いになるまえに: p.4](#)』
- 2章: 設置のしかた**
本製品の各部名称と設置方法について説明します。
→『[設置のしかた: p.16](#)』
- 3章: WEB GUI画面について**
WEB GUIへのログイン方法と画面構成について説明します。
→『[WEB GUI画面について: p.22](#)』
- 4章: Basic Settings (基本設定)**
アクセスポイントの無線モードやセキュリティなど、基本的な設定について説明します。
→『[Basic Settings \(基本設定\): p.27](#)』
- 5章: Advanced Settings (詳細設定)**
マルチSSIDやVLAN、キャプティブポータルなど、アクセスポイントの詳細設定について説明します。
→『[Advanced Settings \(詳細設定\): p.41](#)』
- 6章: Status (ステータス)**
ファームウェアバージョンやクライアント情報、ログなど、ステータスの確認方法について説明します。
→『[Status \(ステータス\): p.79](#)』
- 7章: 管理メニュー**
本製品の再起動やファームウェアアップデート、設定のリセットなど、管理を行う方法を説明します。
→『[管理メニュー: p.89](#)』
- 8章: 付録**
製品を工場出荷時の設定に戻す方法と、FAQ (よくご質問いただく内容) について記載しています。
→『[付録: p.105](#)』

■マニュアルの対象者

本マニュアルは、本製品の設置および管理についての情報を記載しています。また、ネットワーク管理の概念や用語に十分な知識を持っているネットワーク管理者を対象としています。

■表記規則

本マニュアルでは以下の記号を使用します。

- ⚠ 警告** この表示を無視し、間違った使い方をすると、火災や感電などにより人身事故になるおそれがあります。
- ⚠ 注意** この表示を無視し、間違った使い方をすると、傷害または物的損害が発生するおそれがあります。
- 重要** 設定の組み合わせ、イベントや手順によりネットワークの接続状態やセキュリティなどに悪影響を及ぼす恐れのある事項について説明します。
- メモ** 特長や技術についての詳細情報を記述します。

本マニュアル中での字体、記号についての表記規則は以下のとおりです。

字体	解説	例
『水色』	マニュアル内の参照先	『 Basic Settings (基本設定): p.27 』

安全にお使いいただくために

ご自身の安全を確保し、システムを破損から守るために、以下に記述する安全のための指針をよくお読みください。

安全上のご注意

必ずお守りください

本製品を安全にお使いいただくために、以下の項目をよくお読みになり必ずお守りください。

	この表示を無視し、間違った使い方をすると、死亡または重傷を負うおそれがあります。
	この表示を無視し、間違った使い方をすると、火災や感電などにより人身事故になるおそれがあります。
	この表示を無視し、間違った使い方をすると、傷害または物的損害が発生するおそれがあります。

記号の意味 してはいけない「禁止」内容です。 必ず実行していただく「指示」の内容です。

危険

- | | |
|--|---|
| <p> 分解・改造をしない
火災、やけど、けが、感電などの原因となります。</p> <p> ぬれた手でさわらない
感電の原因となります。</p> <p> 水をかけたり、ぬらしたりしない
内部に水が入ると、火災、感電、故障の原因となります。</p> <p> 水などの液体（飲料水、汗、海水、ペットの尿など）でぬれた状態で触ったり、電源を入れたりしない
火災、やけど、けが、感電、故障の原因となります。</p> <p> 各種端子やスロットに水などの液体（飲料水、汗、海水、ペットの尿など）をいれない。万が一、入ってしまった場合は、直ちに電源プラグをコンセントから抜く
火災、やけど、けが、感電、故障の原因となります。</p> | <p> 油煙、湯気、湿気、埃の多い場所、高温になる場所や熱のこもりやすい場所（火のそば、暖房器具のそば、こたつや布団の中、直射日光の当たる場所、炎天下の車内、風呂場など）、振動の激しい場所では、使用、保管、放置しない
火災、やけど、けが、感電、故障の原因となります。</p> <p> 内部に金属物や燃えやすいものを入れない
火災、感電、故障の原因となります。</p> <p> 砂や土、泥をかけたり、直に置いたりしない。また、砂などが付着した手で触れない
火災、やけど、けが、感電、故障の原因となります。</p> <p> 電子レンジ、IH 調理器などの加熱調理機、圧力釜など高压容器に入れたり、近くに置いたりしない
火災、やけど、けが、感電、故障の原因となります。</p> |
|--|---|

警告

- | | |
|---|--|
| <p> 落としたり、重いものを乗せたり、強いショックを与えたり、圧力をかけたりしない
故障の原因となります。</p> <p> 発煙、焦げ臭い匂いの発生などの異常状態のまま使用しない
感電、火災の原因になります。使用を止めて、ケーブル/コード類を抜いて、煙が出なくなつてから販売店に修理をご依頼ください。</p> <p> 表示以外の電圧で使用しない
火災、感電、または故障の原因となります。</p> <p> たこ足配線禁止
たこ足配線などで定格を超えると火災、感電、または故障の原因となります。</p> <p> 設置、移動のときは電源プラグを抜く
火災、感電、または故障の原因となります。</p> <p> 雷鳴が聞こえたら、ケーブル/コード類にはさわらない
感電の原因となります。</p> <p> ケーブル/コード類や端子を破損させない
無理なねじり、引っ張り、加工、重いものの下敷きなどは、ケーブル/コードや端子の破損の原因となり、火災、感電、または故障の原因となります。</p> <p> 本製品付属の AC アダプタもしくは電源ケーブルを指定のコンセントに正しく接続して使用する
火災、感電、または故障の原因となります。</p> <p> 各光源をのぞかない
光ファイバケーブルの断面、コネクタおよび本製品のコネクタや LED をのぞきますと強力な光源により目を損傷するおそれがあります。</p> <p> 各種端子やスロットに導電性異物（金属片、鉛筆の芯など）を接触させたり、ほこりが内部に入ったりしないようにする
火災、やけど、けが、感電または故障の原因となります。</p> <p> 使用中に布団で覆ったり、包んだりしない
火災、やけどまたは故障の原因となります。</p> | <p> ガソリンスタンドなど引火性ガスが発生する可能性のある場所や粉じんが発生する場所に立ち入る場合は、必ず事前に本製品の電源を切る
引火性ガスなどが発生する場所で使用すると、爆発や火災の原因となります。</p> <p> カメラのレンズに直射日光などを長時間あてない
素子の退色、焼付きや、レンズの集光作用により、火災、やけど、けがまたは故障の原因となります。</p> <p> 無線製品は病院内で使用する場合は、各医療機関の指示に従って使用する
電子機器や医療電気機器に悪影響を及ぼすおそれがあります。</p> <p> 本製品の周辺に放熱を妨げるようなもの（フィルムやシールでの装飾を含む）を置かない
火災、または故障の原因となります。</p> <p> 耳を本体から離してご使用ください
大きな音を長時間連続して聞くと、難聴などの耳の障害の原因となります。</p> <p> 無線製品をご使用の場合、医用電気機器などを装着している場合は、医用電気機器メーカーもしくは、販売業者に、電波による影響について確認の上使用する
医療電気機器に悪影響を及ぼすおそれがあります。</p> <p> 高精度な制御や微弱な信号を取り扱う電子機器の近くでは使用しない
電子機器が誤作動するなど、悪影響を及ぼすおそれがあります。</p> <p> ディスプレイ部やカメラのレンズを破損した際は、割れたガラスや露出した端末内部に注意する
破損部や露出部に触れると、やけど、けが、感電の原因となります。</p> <p> ペットなどが本機に噛みつかないように注意する
火災、やけど、けがなどの原因となります。</p> <p> コンセントに AC アダプタや電源ケーブルを抜き差しするときは、金属類を接触させない
火災、やけど、感電または故障の原因となります。</p> <p> AC アダプタや電源ケーブルに海外旅行用の変圧器等を使用しない
発火、発熱、感電または故障の原因となります。</p> |
|---|--|

警告

-  ACアダプタもしくは電源プラグについたほこりは、拭き取るほこりが付着した状態で使用すると、火災、やけど、感電または故障の原因となります。
-  ACアダプタや電源ケーブルをコンセントにさしてむときは、確実に差し込む確実に差し込まないと、火災、やけど、感電もしくは故障の原因となります。
-  接続端子が曲がるなど変形した場合は、直ちに使用を中止する。また、変形をもとに戻しての使用も行わない端子のショートにより、火災、やけど、けが、感電または故障の原因となります。
-  各種接続端子を機器本体に接続する場合、斜めに差したり、差した状態で引っ張ったりしない火災、やけど、感電または故障の原因となります。
-  使用しない場合は、ACアダプタもしくは電源ケーブルをコンセントから抜く電源プラグを差したまま放置すると、火災、やけど、感電または故障の原因となります。
-  お手入れの際は、ACアダプタもしくは電源ケーブルをコンセントから抜く抜かずに行くと、火災、やけど、感電または故障の原因となります。
-  SD や MicroSD カード、USB メモリの使用中は、カードやメモリを取り外したり、本製品の電源を切ったりしないデータの消失、機器本体の故障の原因となります。
-  磁気カードや磁気を帯びたものを本製品に近づけない磁気カードのデータが消えてしまうおそれもしくは機器本体の誤作動の原因となります。
-  ディーリンクジャパンが販売している無線機器は国内専用のため、海外で使えない海外では国によって電波使用制限があるため、本製品を使用した場合、罰せられる場合があります。海外から持ち込んだディーリンク製品や並行輸入品を日本国内で使用する場合も同様に、罰せられる場合があります。

注意

-  乳幼児の手の届く場所では使わないやけど、ケガまたは感電の原因となります。
-  静電気注意コネクタや電源プラグの金属端子に触れたり、帯電したものを近づけると故障の原因となります。
-  コードを持って抜かないコードを無理に曲げたり、引っ張ると、コードや機器本体の破損の原因となります。
-  振動が発生する場所では使用しない故障の原因となります。
-  付属品の使用は取扱説明書に従う本製品の付属品は、取扱説明書に従い、他の製品に使用しないでください。機器の破損の原因となります。
-  破損したまま使用しない火災、やけどまたはけがの原因となります。
-  ぐらついた台の上や傾いた場所などの不安定な場所や高所には置かない落下して、けがなどの原因となります。
-  子供が使用する場合は、保護者が取扱いの方法を教え、誤った使い方をさせないけがや故障などの原因となります。
-  本製品を長時間連続使用する場合は、温度が高くなることもあるため、注意する。また、使用中に眠ってしまうなどして、意図せず長時間触れることがないようにする温度の高い部分に直接長時間触れるとお客様の体質や体調によっては肌の赤みやかゆみ、かぶれ、低温やけどの原因となります。
-  コンセントにつないだ状態で、ACアダプタや電源コンセントに長時間触れないやけど、感電の原因となります。
-  一般の電話機やコードレス電話、テレビ、ラジオなどをお使いになっている近くで使用しない近くで使用すると、本製品が悪影響を及ぼす原因となる場合があるため、なるべく離れた場所で使用してください。
-  D-Link が指定したオプション品がある場合は、指定オプションを使用する不正なオプション品を使用した場合、故障、破損の原因となります。

電波障害自主規制について

この装置は、クラス B 機器です。この装置は、住宅環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをして下さい。

ご使用上の注意

けがや感電、火災および装置の破損のリスクを減らすために、以下の注意事項を遵守してください。

- マニュアルなどに記載されている以外の方法でのご使用はやめてください。
- 食べ物や飲み物が本製品にかからないようにしてください。また、水気のある場所での運用は避けてください。
- 本製品の開口部に物をさしこまないでください。火事や感電を引き起こすことがあります。
- 付属の AC アダプタもしくは電源ケーブルのみを使用してください。
- 感電を防止するために、本製品と周辺機器の電源ケーブルは、正しく接地された電気コンセントに接続してください。
- やむなく延長コードや電源分岐回路を使用する場合においても、延長コードと電源分岐回路の定格を守ってください。延長コードまたは電源分岐回路に差し込まれているすべての製品の合計定格アンペア数が、その延長コードまたは、電源分岐回路の定格アンペア限界の 8 割を超えないことを確認してください。
- 一時的に急激に起こる電力の変動から本製品を保護するためには、サージサプレッサ、回線調整装置、または無停電電源装置（UPS）を使用してください。
- ケーブルと電源コードは慎重に取り付けてください。踏みつけられたり踏いたりしない位置に、ケーブルと電源コードを配線し、コンセントに差し込んでください。また、ケーブル上に物を置いたりしないようにしてください。
- 電源ケーブルや電源プラグを改造しないでください。
- システムに対応しているホットプラグ可能な電源装置に電源を接続したり、切り離したりする際には、以下の注意を守ってください。
 - 電源装置を取り付ける場合は、電源装置を取り付けてから、電源ケーブルを電源装置に接続してください。
 - 電源装置を取り外す場合は、事前に電源ケーブルを抜いておいてください。
 - システムに複数の電源がある場合、システムから電源を切り離すには、すべての電源ケーブルを電源装置から抜いておいてください。
- 抜け防止機構のあるコンセントをご使用の場合、そのコンセントの取り扱い説明書に従ってください。
- カバーを外す際、あるいは内部コンポーネントに触れる際は、製品の温度が十分に下がってから行ってください。
- 本製品は動作中に高温になる場合があります。本製品の移動や取り外しの際には、ご注意ください。
- 本製品は動作中に高温になる場合がありますが、手で触れることができる温度であれば故障ではありません。ただし長時間触れたまま使用しないでください。低温やけどの原因になります。
- 市販のオプション品や他社製品を使用する場合、当社では動作保証は致しませんので、予めご了承ください。
- 製品に貼られている製品ラベルや認証ラベルをはがさないでください。はがしてしまうとサポートを受けられなくなります。

静電気障害を防止するために

静電気は、本製品内部の精密なコンポーネントを損傷する恐れがあります。静電気による損傷を防ぐため、本製品に触れる前に、身体から静電気を逃がしてください。

さらに、静電気放出（ESD）による損傷を防ぐため、以下の手順を実行することをお勧めします。

1. 機器を箱から取り出すときは、機器をシステム等に取り付ける準備が完了するまで、本製品を静電気防止包装から取り出さないでください。静電気防止包装から取り出す直前に、必ず身体の静電気を逃がしてください。
2. 静電気に敏感な部品を運ぶ場合、最初に必ず静電気対策を行ってください。
3. 静電気に敏感な機器の取り扱いは、静電気のない場所で行います。可能であれば、静電気防止床パッド、作業台パッド、および帯電防止接地ストラップを使用してください。

電源の異常

万一停電などの電源異常が発生した / する場合は、必ず本スイッチの電源プラグを抜いてください。電源が再度供給できる状態になってから電源プラグを再度接続します。

無線LANについて

業界標準に基づく弊社の無線 LAN 製品は、ご家庭や職場または公共の施設において、使いやすく互換性の高い高速の無線接続を提供します。これらを使用して時間や場所に関わらず必要なデータにアクセスすることができます。

WLAN は家庭やオフィス環境のみならず、空港やコーヒESHOP、または大学など公共の施設においても幅広く利用されるようになってきました。

この WLAN 技術を用いることにより、仕事やコミュニケーションがさらに効率的に行えるようになってきています。無線技術により可動性が増し、配線や固定のインフラが減少したことでユーザに大きなメリットが生まれました。

ノート型やデスクトップ型 PC に使用する無線アダプタはイーサネットのアダプタカードと同じプロトコルをサポートしており、無線ユーザは有線ネットワークと同じアプリケーションを利用できるようになりました。

■ WLAN 技術を利用するさまざまな理由

可動性

WLAN の動作範囲内のどこからでもデータにアクセス可能であり、生産性を向上します。また、リアルタイムな情報に基づく管理により作業効率が向上します。

低い実現コスト

WLAN は設置、管理、変更、移転のすべてが簡単です。このような WLAN の扱いやすさはネットワークの変更が頻繁に要求される環境に適しています。WLAN は有線ネットワークでは困難であった場所へのネットワーク導入を可能にします。

簡単な設置と拡張

煩わしい複雑なケーブル配線作業、特に壁や天井へのケーブル敷設の必要がないため、手早く簡単にシステムの設置を行うことができます。無線技術は、ネットワークを家庭やオフィスを超えて拡張することで、さらなる多用途性を提供します。

低コストのソリューション

無線 LAN デバイスは、従来のイーサネット用機器とほぼ同等の価格設定となっています。本製品は設定可能な複数のモードで多機能性を提供し、コスト削減を行います。

柔軟性

配置する無線 LAN デバイスの数によって、ピアツーピアのネットワークが適している小さなユーザグループから大規模なインフラネットワークまで、自由自在に構築することができます。

■ 世界基準対応の技術

無線機器は、IEEE 802.11b、IEEE 802.11g、IEEE 802.11n、IEEE 802.11ac および IEEE 802.11ax に準拠しています。

● IEEE 802.11ax 規格

IEEE 802.11ax 規格は「Wi-Fi6」とも呼ばれ、最大通信速度は 1201Mbps です。2.4GHz 帯および 5GHz 帯の周波数を利用し、「OFDMA」技術をサポートしています。

● IEEE 802.11ac 規格

IEEE 802.11ac 規格の無線通信速度は、IEEE 802.11n 規格よりも高速化されており、5GHz 帯の周波数と「OFDM」技術をサポートしています。

● IEEE 802.11n 規格

IEEE 802.11n 規格は、従来の IEEE 802.11a、IEEE 802.11b および IEEE 802.11g の機能を拡張した規格です。無線通信速度は、最大 300Mbps までと高速化され、2.4GHz 帯および 5GHz 帯の周波数を利用し、こちらも「OFDM」技術をサポートしています。

これらにより、多くの環境化において、無線サービスエリア内でネットワークによる大容量の送受信や遅延の少ない MPEG 形式の映像の視聴などが可能になります。OFDM (Orthogonal Frequency Division Multiplexing) という技術により、この大容量のデジタルデータの高速伝送を無線で行うことができます。OFDM では、無線信号を小さいサブ信号に分割し、それらを同時に異なる周波数で送信します。OFDM により、信号伝送時のクロストーク (干渉) の発生を抑えることが可能です。

802.11n/802.11ac/802.11ax 規格は、「WPA」を含む現在最も先進的なネットワークセキュリティ機能を提供します。

WPA/WPA2/WPA3 には企業向けの「Enterprise」とホームユーザ向けの「Personal」の 2 種類があります。WPA3 は、無線 LAN の普及促進の業界団体である Wi-Fi Alliance によって 2018 年 6 月に策定された無線 LAN の暗号化技術の規格名称です。WPA2 に代る次世代セキュリティ規格で、よりセキュアな通信を実現します。

「WPA-Personal」「WPA2-Personal」「WPA3-Personal」は、ユーザ認証に必要なサーバ機器を持たないホームユーザを対象としています。その認証方法は、無線ルータやアクセスポイントに「Pre-Shared Key (事前共有鍵)」の定義を行うという点で WEP と似ています。クライアントとアクセスポイントの両方において、事前共有鍵が確認され条件が満たされた時にアクセスが認められます。

「WPA-Enterprise」「WPA2-Enterprise」「WPA3-Enterprise」は、既にセキュリティ用にインフラが整備されている企業を対象としています。ネットワーク内のサーバを中心にネットワーク管理とセキュリティの実施を行うような環境を想定しています。

ネットワーク管理者は、RADIUS サーバ上で 802.1X を使用し、無線 LAN へのアクセスを許可するユーザのリストを定義します。「WPA-Enterprise」「WPA2-Enterprise」「WPA3-Enterprise」を実装した無線 LAN にアクセスする場合、ユーザはユーザ名とパスワードの入力を要求されます。ユーザがネットワーク管理者によってアクセスを許可されており、正しいユーザ名とパスワードを入力すると、ネットワークへのアクセスが可能になります。例えば、ある社員が会社を辞めるというような場合、ネットワーク管理者がアクセス許可者のリストからその社員のデータを削除すれば、ネットワークを危険にさらすことは避けることができます。

EAP (Extensible Authentication Protocol) は Windows OS に実装されています。802.1X の機能を使用する際には、ネットワークにおけるすべてのデバイスの EAP タイプを同一にする必要があります。

重要

最大の無線信号速度は理論値であり、実際のデータスループットは異なります。ネットワーク条件と環境には、ネットワークトラフィック量、建築材料や工事、ネットワークオーバーヘッドが含まれ、実際のデータスループット速度は低くなります。環境条件は無線信号範囲に悪影響を与えます。

■無線に関するご注意

電波に関するご注意

本製品は、電波法に基づく小電力データ通信システムの無線製品として、技術基準適合証明を受けています。従って、本製品の使用する上で、無線局の免許は必要ありません。

本製品は、日本国内でのみ使用できます。

以下の注意をよくお読みになりご使用ください。

- 本製品を以下の場所では使用しないでください。
 - ・ 心臓ペースメーカー等の産業・科学・医療用機器の近くで使用すると電磁妨害を及ぼし、生命の危険があります。
 - ・ 工場の製造ライン等で使用されている移動体識別用の構内無線局（免許を必要とする無線局）および特定小電力無線局（免許を必要としない無線局）
 - ・ 電子レンジの近くで使用すると、電子レンジによって無線通信に電磁妨害が発生します。
 - ・ 電気製品、AV 機器、OA 機器などの磁気を帯びているところや電磁波が発生しているところで使用すると下記のような影響があります。
 - 磁気や電気雑音の影響を受けると雑音が大きくなったり、通信ができなくなったりすることがあります。
 - テレビ、ラジオなどに近いと受信障害の原因となったり、テレビ画面が乱れたりすることがあります。
 - 近くに複数の無線 LAN アクセスポイントが存在し、同じチャネルを使用していると、正しく検索できない場合があります。
- 本製品は技術基準適合証明を受けています。本製品の分解、改造、および裏面の製品ラベルをはがさないでください。

2.4GHz 帯使用の無線機器の電波干渉に関するご注意

本製品の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用している移動体識別用の構内無線局（免許を必要とする無線局）および特定小電力無線局（免許を必要としない無線局）並びにアマチュア無線局（免許を必要とする無線局）が運用されています。

- 本製品を使用する前に、近くで移動体識別用の構内無線局および特定小電力無線局並びにアマチュア無線局が運用されていないことを確認してください。
- 万一、本製品から移動体識別用の構内無線局に対して有害な電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか、または電波の発射を停止してください。
- その他、本製品から移動体通信用の特定小電力無線局に対して電波干渉の事例が発生した場合など、何かお困りのことが起きたときは、弊社サポート窓口へお問い合わせください。

使用周波数帯域	2.4GHz 帯
変調方式	DS-SS 方式 / OFDM 方式
想定干渉距離	40m 以下
周波数変更可否	全帯域を使用し、かつ移動体識別用の構内無線局および特定小電力無線局並びにアマチュア無線局の帯域を回避可能

5GHz 帯使用に関するご注意

無線 LAN の 5.2/5.3GHz (W52/W53) をご利用になる場合、電波法の定めにより屋外ではご利用になれません。

無線 LAN 製品ご使用時におけるセキュリティに関するご注意

無線 LAN では、LAN ケーブルを使用する代わりに、電波を利用してパソコン等と無線アクセスポイント間で情報のやり取りを行うため、電波の届く範囲であれば自由に LAN 接続が可能であるという利点があります。

その反面、電波はある範囲内であれば障害物（壁等）を越えてすべての場所に届くため、セキュリティに関する設定を行っていない場合、以下のような問題が発生する可能性があります。

● 通信内容を盗み見られる

悪意ある第三者が、電波を故意に傍受し、以下の通信内容を盗み見られる可能性があります。

- ID やパスワード又はクレジットカード番号等の個人情報
- メールの内容

● 不正に侵入される

悪意ある第三者が、無断で個人や会社内のネットワークへアクセスし、以下の行為を行う可能性があります。

- 個人情報や機密情報を取り出す（情報漏洩）
- 特定の人物になりすまして通信し、不正な情報を流す（なりすまし）
- 傍受した通信内容を書き換えて発信する（改ざん）
- コンピュータウイルスなどを流しデータやシステムを破壊する（破壊）

本来、無線 LAN カードや無線アクセスポイントは、これらの問題に対応するためのセキュリティの仕組みを持っていますので、無線 LAN 製品のセキュリティに関する設定を行って製品を使用することで、その問題が発生する可能性は少なくなります。

セキュリティの設定を行わないで使用した場合の問題を充分理解した上で、お客様自身の判断と責任においてセキュリティに関する設定を行い、製品を使用することをお奨めします。

このたびは、弊社製品をお買い上げいただきありがとうございます。

本書は、製品を正しくお使いいただくための取扱説明書です。

必要な場合には、いつでもご覧いただけますよう大切に保管してください。

また、必ず本書、設置マニュアル、および弊社 WEB に掲載された製品保証規程をよくお読みいただき、内容をご理解いただいた上で、記載事項に従ってご使用ください。

製品保証規定は以下を参照ください。

<https://www.dlink-jp.com/support/info/product-assurance-provision.html>

- 本書の記載内容に逸脱した使用の結果発生した、いかなる障害や損害において、弊社は一切の責任を負いません。あらかじめご了承ください。
- 弊社製品の日本国外でご使用の際のトラブルはサポート対象外になります。
- 弊社は、予告なく本書の全体または一部を修正・改訂することがあります。
- 弊社は改良のため製品の仕様を予告なく変更することがあります。

なお、本製品の最新情報やファームウェアなどを弊社ホームページにてご提供させていただく場合がありますので、ご使用前にご確認ください。

製品保証、保守サービス、テクニカルサポートご利用について、詳しくは弊社ホームページのサポート情報をご確認ください。

<https://www.dlink-jp.com/support>

警告

本書の内容の一部、または全部を無断で転載したり、複写することは固くお断りします。

設置のしかた

本製品の各部名称や、設置する際の準備・方法について説明します。
設置を行う際にお読みください。

2

■ パッケージの内容	17
■ 動作環境	17
■ ネットワーク接続前の準備	17
■ 本体各部名称	18
前面パネル	18
背面パネル	18
■ 製品の設置	19
イーサネットケーブルの接続/電源の投入	19
マウントキットによる設置	20
デスクトップでの使用	21

パッケージの内容

本製品には、以下のものが同梱されています。

- 本体
- マウントキット
- ゴム足
- クイックスタートガイド
- PLシート

※ ACアダプタは同梱されていません。本製品をPoE で使用しない場合は、別売りのAC アダプタ「PSE-M12V25A-I」をご使用ください。

万一、不足しているものや損傷を受けているものがありましたら、ご購入いただきました代理店にご連絡ください。

動作環境

本製品の動作には、以下の環境が必要です。

- Webブラウザ
 - Microsoft Internet Explorer 11 以降
 - Mozilla Firefox 28 以降
 - Apple Safari 7.0 以降
 - Google Chrome 33 以降

※ブラウザの仕様により互換性が確保されない場合があります。

- イーサネットへの接続

ネットワーク接続前の準備

アクセスポイントの設置場所が性能に大きな影響を与えます。以下の注意事項に従って本製品を設置してください。

● 設置にあたってのご注意

本製品の使用により、動作範囲内にて無線でネットワークアクセスが可能になります。しかし、壁や天井など、無線信号が通過する物体の数や厚さ・場所などにより、動作範囲が制約を受ける場合があります。一般的には、構造物の材質や設置場所での無線周波数のノイズが動作範囲に影響を与えます。

- ◆ 本製品と他のネットワークデバイスとの間に入る壁や天井の数をできるだけ少なくしてください。一枚の壁や天井の影響により、本製品の動作範囲は1～30メートルの範囲となります。間に入る障害物の数を減らすようデバイスの位置を工夫してください。
- ◆ ネットワークデバイス間の直線距離にご注意ください。厚さ50センチの壁を45度の角度で無線信号が通過する時、通り抜ける壁の厚みは約1メートルになります。2度の角度で通過すると、通り抜ける厚みは14メートルになります。信号が障害物になるべく直角に通過するような位置にデバイスを設置し、電波を受信しやすくしてください。
- ◆ 無線信号の通過性能は建築材料により異なります。金属製のドアやアルミの金具などは動作範囲を小さくする可能性があります。無線LAN デバイスや無線LAN アダプタ使用のコンピュータの設置は、信号がなるべく乾式壁が開放された戸口などを通るような位置に設置してください。
- ◆ 周波数ノイズを発生する電気機器や家電製品からは、最低でも1、2メートル離してデバイスを設置してください。
- ◆ 2.4GHz のコードレス電話またはX-10（シーリングファン、ライト、およびホームセキュリティシステムなどの無線製品）を使っている場合、ご使用の無線接続は著しく性能が低下するか、または完全に切断される可能性があります。2.4GHz 電話の親機は可能な限りご使用の無線機器から離れていることを確認してください。電話を使用していない場合でも、親機は信号を送信します。
- ◆ 必ず付属の UTP ケーブル、AC アダプタ*をご使用ください。

※本製品にはAC アダプタが付属していません。PoE でご使用いただくか、別売りのAC アダプタ「PSE-M12V25A-I」をご使用ください。

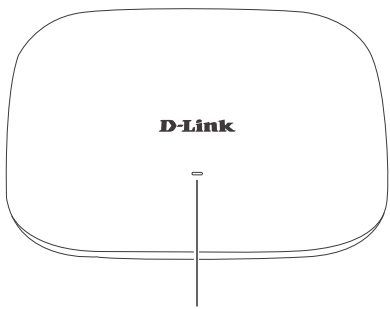
⚠ 注意

本アクセスポイントは、IEEE 802.3at 準拠の給電スイッチまたは弊社が承認する給電機器から受電することができます。弊社が承認していないPoE 給電機器に本アクセスポイントを接続すると、本アクセスポイントが破損する場合があります。

本体各部名称

アクセスポイントの各部名称について説明します。

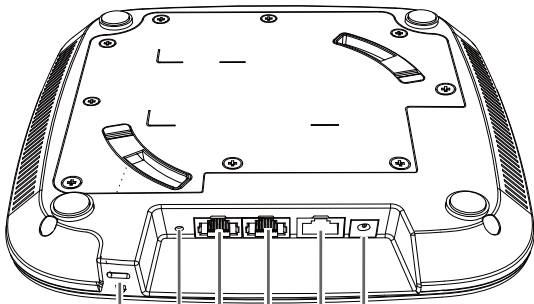
■前面パネル



Power/ステータスLED

LED	色	状態	状況説明
Power/ ステータス	緑	点灯	動作中です。 正しく起動しました。
	赤	点灯	故障・不具合が発生しています。
		点滅	起動中です。

■背面パネル



- セキュリティスロット
- リセットボタン
- コンソールポート
- 電源コネクタ
- LAN (PoE) ポート
- LAN ポート

名称	説明
セキュリティスロット	市販のセキュリティロックを使用して機器に鍵をかけることが可能です。
リセットボタン	本製品を工場出荷時設定にリセットします。
コンソールポート	RJ-45コンソールケーブルを挿入し、管理コンピュータに接続します。
LANポート (10/100/1000 BASE-T)	RJ-45ネットワークケーブルを挿入し、ネットワークへの接続を行います。
LAN (PoE) ポート (10/100/1000/2.5G BASE-T)	RJ-45ネットワークケーブルを挿入し、ネットワークへの接続を行います。 メモ PoE による受電を行うこともできます。
電源コネクタ	AC アダプタ*を接続します。 メモ PoE による受電を行う場合は接続する必要がありません。

※ ACアダプタは同梱されていません。本製品をPoE で使用しない場合は、別売りのAC アダプタ「PSE-M12V25A-I」をご使用ください。

メモ

「LAN ポート」と「LAN (PoE) ポート」でリンクアグリゲーションを設定することはできません。

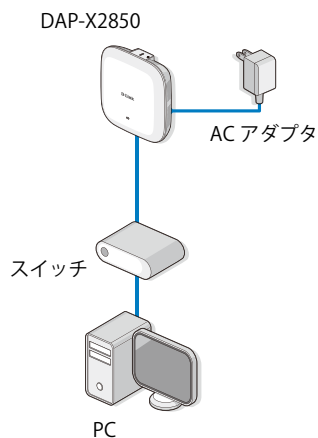
製品の設置

■イーサネットケーブルの接続/電源の投入

以下の方法でネットワークへの接続、及び電源の投入を行います。

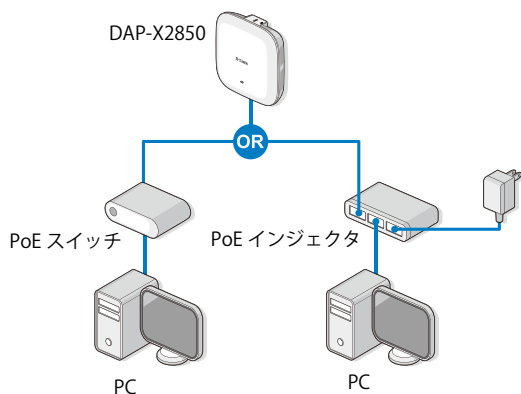
● ACアダプタを使用する接続

1. イーサネットケーブルの一端を本製品の背面にある LAN ポートに、もう一端をルータ/スイッチ等のネットワーク機器に接続します。
2. 別売りの AC アダプタ (PSE-M12V25A-I) を本製品に接続します。
3. AC アダプタのプラグを電源コンセントに接続します。



● PoEスイッチ/PoEインジェクタを使用したPoE接続

1. イーサネットケーブルの一端を本製品の背面にある LAN (PoE) ポートに接続し、もう一端を PoE スイッチ等の PoE 給電機能のあるネットワーク機器に接続します。



メモ

本スイッチに電源が供給されると、POWER/ステータス LED が点灯します。

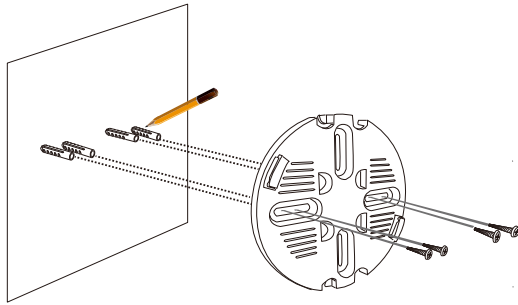
■マウントキットによる設置

本製品は、マウントキットを使用して壁面や天井に設置することができます。
設置の際は以下の手順を参照してください。

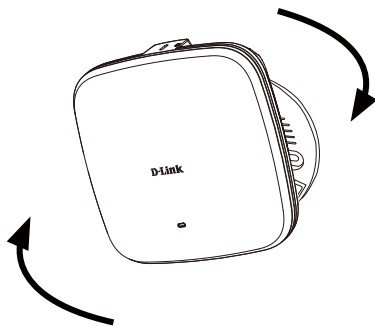
⚠警告

本製品を設置する際は、本製品の重さや壁面、天井の強度、材質などを勘案し、落下などに十分注意した上で設置してください。

●壁面または天井への設置



1. アクセスポイントを取り付ける壁または天井にマウントプレートを合わせ、アンカーを差し込む位置に印をつけます。
2. 印をつけた場所に穴をあけ、プラスチックのアンカーを挿入します。
3. マウントプレートをアンカーの上に配置し、付属のネジを使用してマウントプレートを表面に固定します。
4. アクセスポイントの「LAN ポート」または「LAN (PoE) ポート」にイーサネットケーブルを挿入します。(電源アダプタでデバイスの電源を入れる場合は、アダプタを電源コネクタに差し込みます。)
5. アクセスポイントをマウントプレートの溝に回して入れ、プレートに固定します。

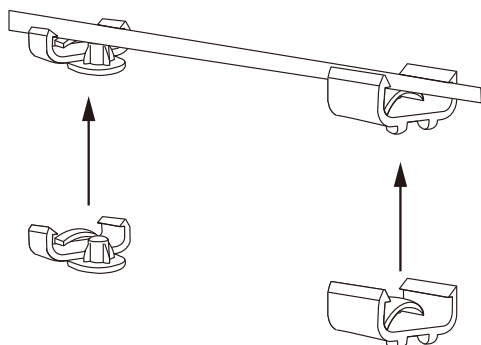


重要

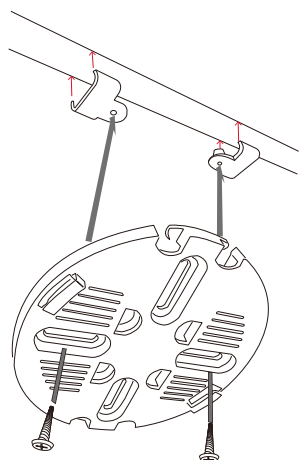
製品が落下しないように補強するなど環境に応じて適切な処理を行ってください。

● 天井ブラケットを使用した設置

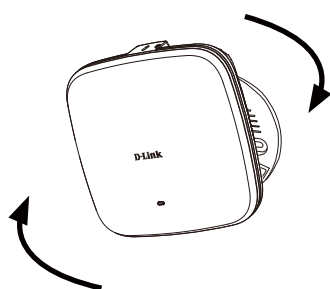
1. 天井のパネルに 2 つの天井ブラケットを挟みます。
両方のブラケットが直線になっていることを確認してください。



2. 同梱されているネジを使用し、天井ブラケットにマウントプレートを取り付けます。



3. アクセスポイントの「LAN ポート」または「LAN (PoE) ポート」にイーサネットケーブルを挿入します。(電源アダプタでデバイスの電源を入れる場合は、アダプタを電源入力コネクタに差し込みます。)
4. アクセスポイントをマウントプレートの溝に回して入れ、プレートに固定します。



重要

製品が落下しないように補強するなど環境に応じて適切な処理を行ってください。

■ デスクトップでの使用

本製品をデスクトップで使用する場合、背面に同梱のゴム足を取り付けてください。

WEB GUI 画面について 3

本製品は、WEB GUI画面から設定・操作を行うことができます。
WEB GUI画面へのログイン方法と画面構成について説明します。

■ WEB GUI画面へのログイン	23
初回ログイン時のセットアップ	24
■ 画面の構成	26

WEB GUI画面へのログイン

1. LAN に接続します。

◆ イーサネット接続の場合：

イーサネットケーブルを使用して、DAP-X2850を管理用コンピュータ、または管理用コンピュータが接続されているスイッチやルータに接続します。

◆ 無線接続の場合：

管理コンピュータをDAP-X2850のデフォルトのSSID「dlink」に接続します。

2. Web ブラウザを起動し、本製品のアドレスを入力します。



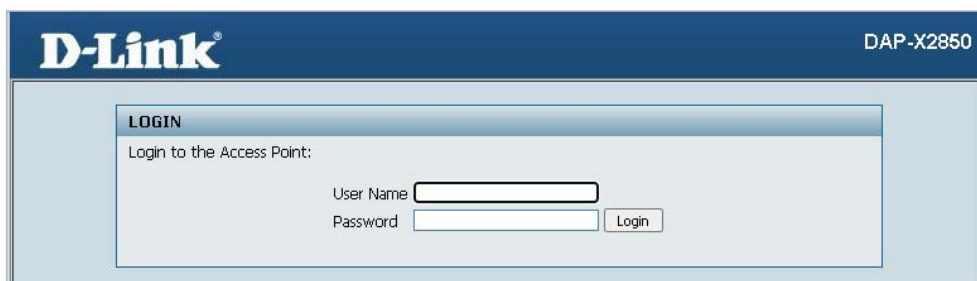
メモ

本製品は初期値で「DHCP クライアント」として設定されています。

- DHCP サーバからIP アドレスを割り振られる環境にある場合、「http://dapx2850XXXX.local」または「https://dapx2850XXXX.local」と入力し、ログインします。
- DHCP サーバが無効の環境の場合、「http://192.168.0.50」または「https://192.168.0.50」と入力しログインします。

※「XXXX」は、AP 本体の底面にあるデバイスラベルに記載されている、MAC アドレスの最後の 4 ケタです。
ご利用の環境に複数のAPが存在する場合は指定する必要があります。

3. 「User Name」と「Password」を入力します。



工場出荷時の設定は以下の通りです。

- User Name : admin
- Password : admin

■初回ログイン時のセットアップ

1. WEB GUI 画面への初回ログイン後、以下の画面が表示されます。

管理者パスワードや時刻、国の設定を行ってください。

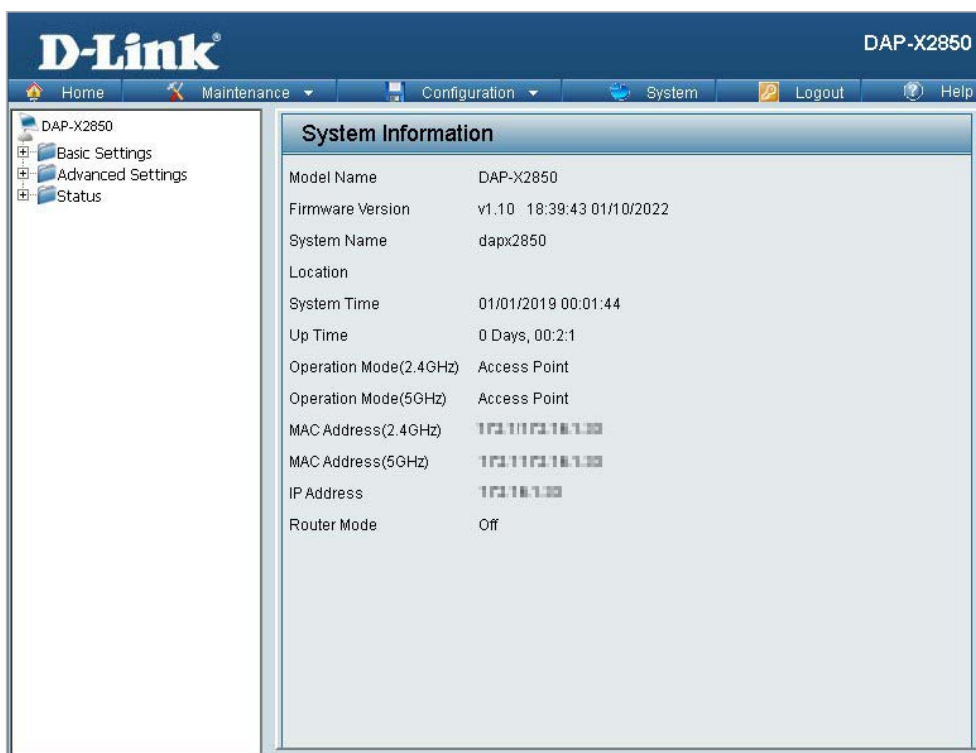
項目	説明
New Password	本製品の新しい管理者パスワードを入力します。 入力した文字は他人から見えないように「●●●」と表示されます。 ・入力可能文字数: 8-30文字 (半角英数字)
Confirm New Password	確認のため、新しい管理者パスワードを再度入力します。
System Time	時間の設定方法を以下から選択します。 ・ [Using Network Time Protocol (NTP)]: NTPサーバを使用して時間設定を行います。 ・ [Manually]: 手動で時間設定を行います。
NTP Server Address	NTPサーバのホスト名またはIPアドレスを設定します。 本項目は[Using Network Time Protocol (NTP)]を選択した場合にのみ表示されます。
Time Zone	プルダウンメニューからローカルタイムゾーンを選択します。 本項目は[Using Network Time Protocol (NTP)]を選択した場合にのみ表示されます。
System Date	本製品に設定する日付を設定します。 本項目は[Manually]を選択した場合にのみ表示されます。
System Time (24 HR)	本製品に設定する時刻を設定します。 本項目は[Manually]を選択した場合にのみ表示されます。
Enable Daylight Saving	チェックを入れ、Daylight Savings Time (DST/サマータイム) を有効化します。
DST Start (24 HR)	Daylight Savings Time (サマータイム) の開始日時を設定します。
DST End (24 HR)	Daylight Savings Time (サマータイム) の終了日時を設定します。
DST Offset (minutes)	Daylight Savings Time (サマータイム) のオフセット時間 (単位: 分) を設定します。
System Country	本製品をご利用になる国として、[Japan] (日本) を選択してください。
Update	設定を適用します。

2. 「Update」をクリックし、設定を適用します。

3. 本製品に新しいパスワードが適用されます。電源を切らずそのままお待ちください。



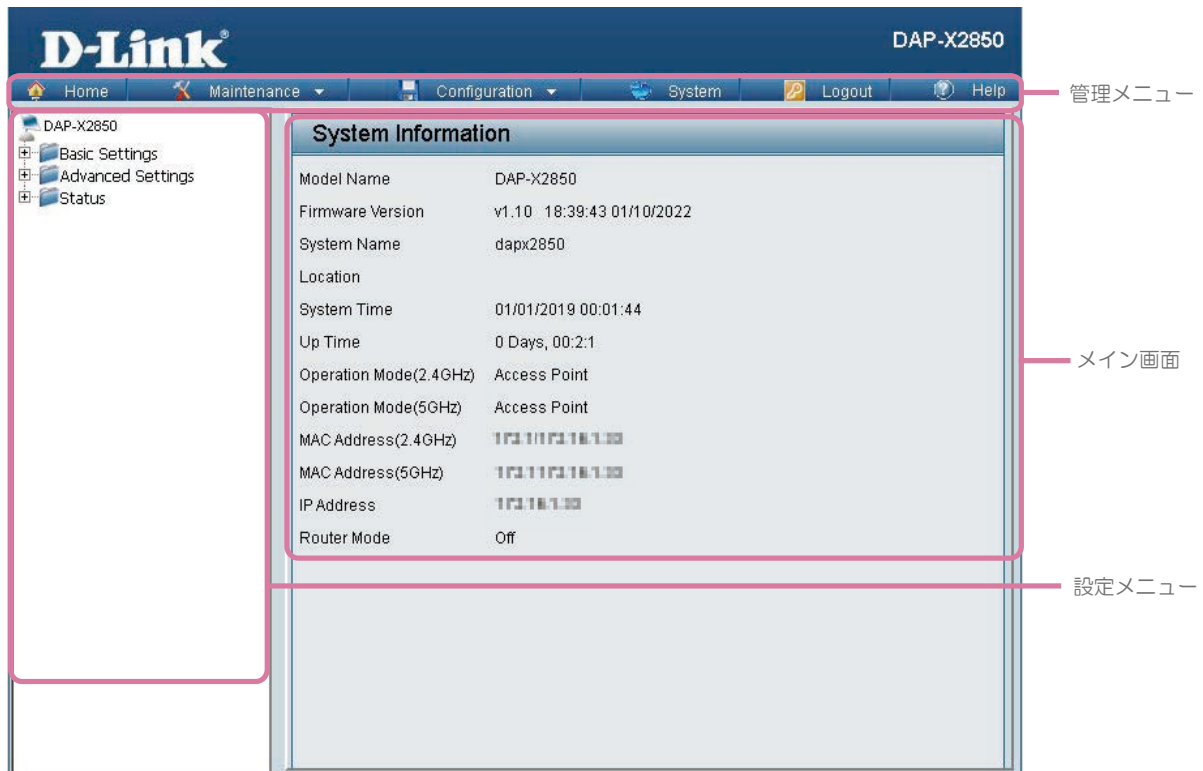
4. ログイン画面が表示されるので、新しいパスワードを入力して再度ログインします。以下の画面が表示されます。



WEB GUIからログアウトする場合は、画面右上の「Logout」からログアウトを行ってください。

画面の構成

WEB GUI画面の構成について説明します。



● 管理メニュー

- Home :
クリックすると、System Information 画面が表示されます。
- Maintenance :
管理者権限の設定やファームウェアのアップロードなど、本製品のメンテナンスを行います。
- Configuration :
設定の保存・取り消しを行います。
- System :
本製品の再起動・工場出荷時設定へのリセットを行います。
- Logout :
WEB GUIからのログアウトを行います。
- Help :
ヘルプ画面が表示されます。

メモ

管理メニューの詳細については、『[管理メニュー:p.89](#)』を参照してください。

● 設定メニュー

アクセスポイントの無線モードやセキュリティなど、各機能の設定を行います。

メモ

設定メニューの詳細については、『[Basic Settings \(基本設定\):p.27](#)』『[Advanced Settings \(詳細設定\):p.41](#)』『[Status \(ステータス\):p.79](#)』を参照してください。

● メイン画面

設定メニューおよび管理メニューで選択した項目の設定画面が表示されます。

Basic Settings (基本設定)

4

アクセスポイントの無線モードやセキュリティなどの設定を行います。

■ Basic Settings について	28
■ Wireless Settings (ワイヤレス設定)	28
Access Point モードを選択した場合	29
WDSモード／WDS with APモードを選択した場合	31
Wireless Clientモードを選択した場合	33
Authentication (認証) の設定について	35
■ LAN Settings (LAN設定)	39
■ IPv6 Settings (IPv6設定)	40

Basic Settings について

Basic Settings (基本設定) では、アクセスポイントの通信モードの選択やセキュリティ設定、LANの設定などを行います。



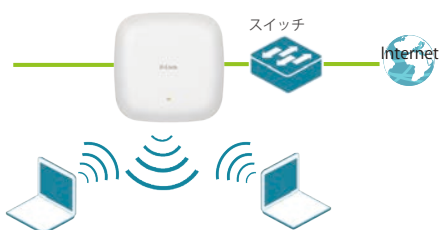
Wireless Settings (ワイヤレス設定)

アクセスポイントの通信モードを選択し、それに応じてネットワーク名 (SSID) や認証方法などの設定を行います。選択できる通信モードは以下の通りです。

※WDSモード及びWDS with APモードは、2.4GHz帯および5GHz帯のW52の周波数帯でのみ利用可能です。

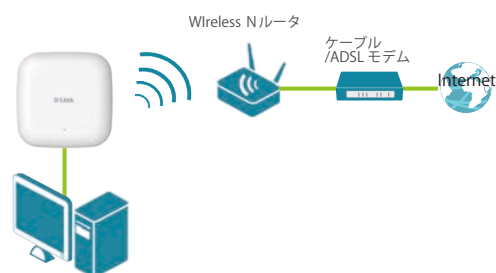
■アクセスポイントモード

無線アクセスポイントと無線クライアントのネットワークを構築します。



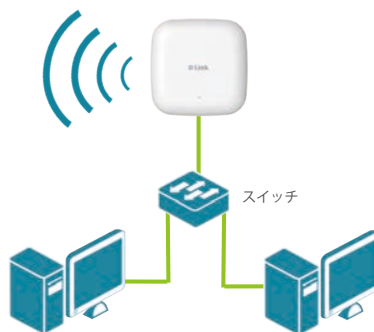
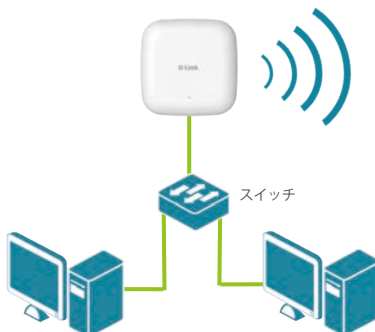
■ワイヤレスクライアントモード

イーサネット用機器向けの無線ネットワークアダプタとして動作します。



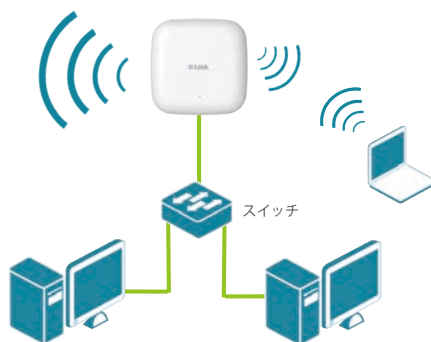
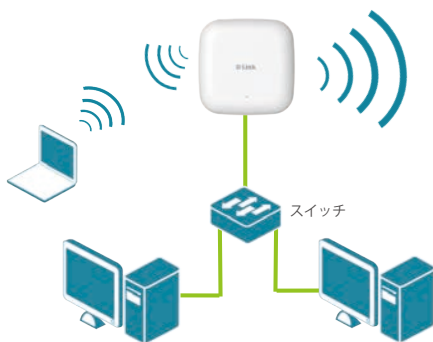
■WDS モード

複数のネットワークを無線接続します。



■WDS with AP モード

無線 LAN アクセスポイントとして動作しながら、複数のネットワークと無線接続します。



1. [Basic Settings] > [Wireless] を選択します。
2. [Wireless Band] で周波数帯を [2.4GHz] または [5GHz] に設定します。
3. 周波数帯を [5GHz] に設定した場合は、[Application] でインドアモードまたはアウトドアモードを選択します。
 - ・選択肢:[Concurrent 11a/n on W52/W53/W56 for indoor][Concurrent 11a/n on W56 for outdoor]
 - ※周波数帯を[2.4GHz]に設定した場合は[Concurrent 11b/g/n on 2.4GHz for indoor/outdoor]に固定されます。
4. [Mode] で、アクセスポイントの通信モードを以下から選択します。
 - ・ [Access Point] / [WDS with AP] / [WDS] / [Wireless Client]
 - ※WDSモード及びWDS with APモードは、2.4GHz帯および5GHz帯のW52の周波数帯でのみ利用可能です。
5. 選択した通信モードに応じて必要な設定を行います。
6. 設定完了後、[Save] をクリックします。

重要

周波数帯を5GHz帯に設定し[Application]で[Concurrent 11a/n on W56 for outdoor]を選択した場合、ビーコン内の Country Codeは「JB」になります。

■ Access Point モードを選択した場合

本製品は無線アクセスポイントとして動作し、無線クライアントとのネットワークを構築します。

The image shows a 'Wireless Settings' window with the following fields and options:

- Wireless Band:** 2.4GHz
- Application:** Concurrent 11b/g/n on 2.4GHz for indoor/outdoor
- Mode:** Access Point
- Network Name (SSID):** dlink
- SSID Visibility:** Enable
- Auto Channel Selection:** Enable
- Channel:** 6
- Channel Width:** 20 MHz
- Authentication:** Open System
- Key Settings:**
 - Encryption:** ☒ Disable ☐ Enable
 - Key Type:** HEX
 - Key Index(1~4):** 1
 - Key Size:** 64 Bits
 - Network Key:** (empty text box)
 - Confirm Key:** (empty text box)
- Save:** (button)

項目	説明
Mode	通信モードを[Access Point] に設定します。
Network Name (SSID)	ネットワーク名 (SSID) を入力します。 ・ 初期値: [dlink] ・ 入力可能文字数: 32文字以内 (大文字と小文字は区別されます。) SSID (Service Set Identifier) とは、無線LANのアクセスポイントを識別するための名前です。無線LANのアクセスポイントが複数ある場合、どのアクセスポイントに接続するかを指定する必要があり、SSIDはその際に使用されます。

項目	説明
SSID Visibility	SSIDの表示を有効または無効にします。 • 選択肢: [Enable] (有効) [Disable] (無効) [Enable](有効)に設定すると、SSIDがネットワークにブロードキャストされ、すべてのネットワークユーザがSSIDを閲覧できるようになります。
Auto Channel Selection	自動チャンネル選択を有効または無効にします。 • 選択肢: [Enable] (有効) [Disable] (無効) [Enable](有効)に設定すると、アクセスポイント起動時に、自動的に最適なチャンネルを選択します。
Channel	[Auto Channel Selection]を無効にした場合に、チャンネルを選択します。
Channel Width	チャンネル帯域を選択します。 • 選択肢: [20MHz] [Auto 20/40MHz] [Auto 20/40/80MHz] ※[Auto 20/40/80MHz]は5GHzを選択した場合のみ選択可能です。
Authentication	認証方式を選択します。 • 選択肢: [Open System] [Enhanced Open] [Enhanced Open + Open] [WPA-Personal] [WPA-Enterprise] [802.1X]

メモ

[Authentication] (認証) の設定内容は、選択した方式によって異なります。
詳細は『[Authentication \(認証\) の設定について:p.35](#)』を参照してください。

重要

Band Steeringを有効にするためには、2.4GHz、5GHzのPrimary SSIDを同一の文字列に設定する必要があります。

■ WDSモード／WDS with APモードを選択した場合

WDSモードの場合：

複数のネットワークと無線接続します。

WDS with APモードの場合：

本製品は無線LAN アクセスポイントとして動作しながら、複数のネットワークと無線接続します。

重要

- WDSモード及びWDS with APモードは、「2.4GHz帯」および「5GHz帯のW52の周波数帯」でのみ利用可能です。周波数帯を5GHzに設定し、[Application] で [Concurrent 11a/n on W56 for outdoor] を選択した場合、WDSモード／WDS with APモードは選択できません。

項目	説明
Mode	通信モードを [WDS with AP] または[WDS]に設定します。
Network Name (SSID)	ネットワーク名 (SSID) を入力します。 - 初期値: [dlink] - 入力可能文字数: 32文字以内 (大文字と小文字は区別されます。) SSID (Service Set Identifier) とは、無線LANのアクセスポイントを識別するための名前です。無線LANのアクセスポイントが複数ある場合、どのアクセスポイントに接続するかを指定する必要があり、SSIDはその際に使用されます。
Auto Channel Selection	通信モードに[WDS] [WDS with AP]を選択した場合はサポートされません。

項目	説明
Channel	固定のチャンネルを設定します。 ネットワーク上のすべてのデバイスが同じチャンネルを共有する必要があります。
Channel Width	チャンネル帯域を選択します。 • 選択肢: [20MHz] [Auto 20/40MHz] [Auto 20/40/80MHz] ※[Auto 20/40/80MHz]は5GHzを選択した場合のみ選択可能です。
AP MAC Address	ネットワーク上にある対向のアクセスポイントのMACアドレスを入力します。
Site Survey	[Scan]をクリックしてサイトサーベイを実行します。 サイトサーベイを実行し、検出された稼働中のアクセスポイントから、接続するネットワークをクリックします。
Authentication	認証方式を選択します。 • 選択肢: [Open System] [WPA-Personal]

メモ

- [Authentication](認証方式)の設定内容は、選択した方式によって異なります。
詳細は『[Authentication \(認証\) の設定について:p.35](#)』を参照してください。

重要

- 異機種間、異なるファームウェアバージョン間でWDSモード、WDS with APモードを使用することはできません。
- WDS間でVLANタグを通すにはVLAN設定が必要です。
- Band Steeringを有効にするためには、2.4GHz、5GHzのPrimary SSIDを同一の文字列に設定する必要があります。
- WDSの対向設定は1対向のみとしてください。

■ Wireless Clientモードを選択した場合

本製品は、イーサネット機器用の無線ネットワークアダプタとして動作します。

Wireless Settings

Wireless Band2.4GHz
ApplicationConcurrent 11b/g/n on 2.4GHz for indoor/outdoor
ModeWireless Client
Network Name (SSID)dlink
SSID VisibilityEnable
Auto Channel SelectionEnable
Channel1
Channel WidthAuto 20/40 MHz

Site Survey

Scan

CH	RSSI	BSSID	Security	SSID
6	100	#0:26:#0:26:#0:00	OPEN	#0:26:#0:00
6	100	#0:26:#0:26:#0:00	OPEN	#0:26:#0:00
1	100	#0:26:#0:26:#0:00	OPEN	#0:26:#0:00
3	100	#0:26:#0:26:#0:00	OPEN	#0:26:#0:00
10	100	#0:26:#0:26:#0:00	OPEN	#0:26:#0:00
11	100	#0:26:#0:26:#0:00	OPEN	#0:26:#0:00

AuthenticationOpen System

Key Settings

Encryption

☒ Disable
☐ Enable

Key TypeHEX
Key Index(1~4)1
Network Key
Confirm Key

Key Size64 Bits

Wireless MAC Clone

Enable

☐

MAC SourceAuto
MAC Address

Scan

MAC Address

Save

項目	説明
Mode	通信モードを [Wireless Client] に設定します。

項目	説明
Network Name (SSID)	ネットワーク名 (SSID) を入力します。 - 初期値: [dlink] - 入力可能文字数: 32文字以内 (大文字と小文字は区別されます。) SSID (Service Set Identifier) とは、無線LANのアクセスポイントを識別するための名前です。無線LANのアクセスポイントが複数ある場合、どのアクセスポイントに接続するかを指定する必要があり、SSIDはその際に使用されます。
Auto Channel Selection	通信モードに [Wireless Client] を選択した場合はサポートされません。
Channel	通信モードに [Wireless Client] を選択した場合はサポートされません。
Channel Width	通信モードに [Wireless Client] を選択した場合はサポートされません。
Site Survey	[Scan] をクリックしてサイトサーベイを実行します。 サイトサーベイを実行し、検出された稼働中のアクセスポイントから、接続するネットワークをクリックします。
Authentication	認証方式を選択します。 選択肢: [Open System] [WPA-Personal]
Wireless MAC Clone	Wireless MAC Clone を有効にすると、本製品のMACアドレスをクライアントのMACアドレスに変更できます。 [Enable] (有効) にチェックをいれると設定が有効になります。 - 有効にした場合、[MAC Source] を [Auto] (自動) または [Manual] (手動) に設定します。 [MAC Source] を [Manual] (手動) に設定した場合は [MAC Address] に MAC アドレスを入力します。または [Scan] をクリックして検索した MAC アドレスを選択します。

メモ

- [Authentication] (認証方式) の設定内容は、選択した方式によって異なります。詳細は『[Authentication \(認証\) の設定について:p.35](#)』を参照してください。

重要

- Wireless Client Model は既定で AP の MAC Address が使用されます。
- 複数 LAN 配下に複数端末を配置した場合も 1 つの MAC Address が使用されます。

■ Authentication (認証) の設定について

[Wireless Settings] 画面では、認証方式として以下を選択できます。

◆ Open System/Enhanced Open/Enhanced Open or Open

ネットワーク (WEP) を介して鍵を通信します。

設定方法については、『[\[Open System\]を選択した場合:p.35](#)』を参照してください。

◆ WPA-Personal

パスワードと認証キーの自動変更機能によりネットワークを保護します。

設定方法については、『[\[WPA-Personal\]を選択した場合:p.36](#)』を参照してください。

◆ WPA-Enterprise

RADIUS サーバを使用してネットワークを保護します。

設定方法については、『[\[WPA-Enterprise\]を選択した場合:p.37](#)』を参照してください。

◆ 802.1X

802.1X ネットワーク認証を行う場合に選択します。

設定方法については、『[\[802.1 X\]を選択した場合:p.38](#)』を参照

重要

[Authentication] で以下を選択した場合、[Advanced Settings] > [Performance Settings] 画面の [Wireless Mode] で [802.11n only] を選択できなくなります。

- [802.1X] を選択した場合
- [Open System] を選択し、[Encryption] を [Enable] に設定した場合

● [Open System]を選択した場合

項目	説明
Encryption	暗号化を有効または無効にします。 ・ 選択肢: [Enable] (有効) [Disable] (無効)
Key Type	キーのタイプを選択します。 ・ 選択肢: - [HEX] (16 進数) : 0 ~ 9, A ~ F までの半角英数字のキーを使用します。 - [ASCII] (半角英数字) : 半角英数字のキーを使用します。
Key Size	キーのサイズを選択します。 ・ 選択肢: [64 Bits] [128 Bits]
Key Index	有効にするキーを選択します。 ・ 選択肢: [1] [2] [3] [4]
Network Key	キーを入力します。
Confirm Key	確認のため、再度キーを入力します。

- [WPA-Personal]を選択した場合
以下の画面でパスフレーズの設定を行います。

Authentication WPA-Personal

PassPhrase Settings

WPA Mode AUTO (WPA or WPA2)

Cipher Type AES Group Key Update Interval 3600 (Sec)

☒ Manual ☐ Periodical Key Change

Activated From Sun : 00 : 00

Time Interval 1 (1~168)hour(s)

PassPhrase

Confirm PassPhrase

notice: 8~63 in ASCII or 64 in Hex.
(0-9,a-z,A-Z,~!@#\$%^&*()_+`-={}[];'":./,<>?)

項目	説明
WPA Mode	WPAのモードを選択します。 ・ 選択肢: [AUTO (WPA or WPA2)] [WPA2 or WPA3] [WPA2 Only] [WPA3 Only]
Cipher Type	暗号化タイプを選択します。 ・ 選択肢: [Auto] [AES] [TKIP] [WPA2 or WPA3]または[WPA3 Only]を選択した場合、[AES]のみ指定可能です。
Group Key Update Interval	グループキーを更新する間隔を設定します。間隔が短くなるとデータ転送速度が低下する可能性があります。 ・ 推奨値: 3600 (秒)
Manual	パスフレーズを手動で設定するようにします。 [Manual]を選択した場合、使用するパスフレーズを入力します。
Periodical Key Change	アクセスポイントが自動的にパスフレーズを変更するようにします。 [Periodical Key Change]を選択した場合、変更を行う周期を設定します。
Activated From	[Periodical Key Change]を選択した場合、パスフレーズの自動更新が開始される時刻を設定します。
Time Interval	[Periodical Key Change]を選択した場合、パスフレーズを変更する間隔を設定します。
PassPhrase	[Manual]を選択した場合、パスフレーズを入力します。
Confirm PassPhrase	[Manual]を選択した場合、確認のため再度パスフレーズを入力します。

メモ

- 以下の項目は、アクセスポイントの通信モードをAccess Point モードに設定した場合のみ表示されます。
- ・ [Manual] [Periodical Key Change] [Activated From] [Time Interval]

● [WPA-Enterprise]を選択した場合

Authentication: WPA-Enterprise

RADIUS Server Settings

WPA Mode: AUTO (WPA or WPA2)

Cipher Type: AES Group Key Update Interval: 3600 (Sec)

Network Access Protection

Network Access Protection: ☒ Disable ☐ Enable

RADIUS Server Mode

RADIUS Server: ☒ External ☐ Internal

Primary RADIUS Server Setting

RADIUS Server: RADIUS Port: 1812

RADIUS Secret:
(0-9,a-z,A-Z,~!@#\$%^&*()_+`-={[];'":|,./<>?)

Backup RADIUS Server Setting (Optional)

RADIUS Server: RADIUS Port: 1812

RADIUS Secret:
(0-9,a-z,A-Z,~!@#\$%^&*()_+`-={[];'":|,./<>?)

Primary Accounting Server Setting

Accounting Mode: Disable

Accounting Server: Accounting Port: 1813

Accounting Secret:
(0-9,a-z,A-Z,~!@#\$%^&*()_+`-={[];'":|,./<>?)

Backup Accounting Server Setting (Optional)

Accounting Server: Accounting Port: 1813

Accounting Secret:
(0-9,a-z,A-Z,~!@#\$%^&*()_+`-={[];'":|,./<>?)

項目	説明
WPA Mode	WPAのモードを選択します。 ・選択肢: [AUTO (WPA or WPA2)] [WPA2 Only] [WPA3 Only]
Cipher Type	暗号化タイプを選択します。 ・選択肢: [Auto] [AES] [TKIP] [WPA3 Only]を選択した場合、[AES]のみ指定可能です。
Group Key Update Interval	グループキーを更新する間隔を設定します。 間隔が短くなるとデータ転送速度が低下する可能性があります。 ・推奨値: 3600 (秒)
Network Access Protection	Microsoft Network Access Protectionを有効または無効に設定します。
Radius Server Mode	RADIUSサーバのモードを選択します。 ・選択肢: [External] (外部) [Internal] (内部)
Primary Radius Server Setting	プライマリRADIUSサーバの設定を行います。 ・RADIUS Server: RADIUS サーバのIP アドレスを入力します。 ・RADIUS Port: RADIUS サーバの認証に使用するポート番号を入力します。 初期値: [1812] ・RADIUS Secret: RADIUS シークレット (パスワード) を入力します。
Backup Radius Server Setting (Optional)	バックアップRADIUSサーバの設定を行います。 ・RADIUS Server: RADIUS サーバのIP アドレスを入力します。 ・RADIUS Port: RADIUS サーバの認証に使用するポート番号を入力します。 初期値: [1812] ・[RADIUS Secret: RADIUS シークレット (パスワード) を入力します。
Primary Accounting Server Setting	プライマリアカウントサーバの設定を行います。 ・Accounting Mode: アカウンティングモードを[Enable] (有効) [Disable] (無効) にします。 ・Accounting Server: アカウンティングサーバのIPアドレスを入力します。 ・Accounting Port: アカウンティングサーバの認証に使用するポート番号を入力します。 初期値: [1813] ・Accounting Secret: アカウンティングシークレット (パスワード) を入力します。

項目	説明
Backup Accounting Server Setting (Optional)	バックアップアカウンティングサーバの設定を行います。 - Accounting Server: アカウンティングサーバのIPアドレスを入力します。 - Accounting Port: アカウンティングサーバの認証に使用するポート番号を入力します。 初期値:[1813] - Accounting Secret: アカウンティングシークレット (パスワード) を入力します。

重要

RADIUSサーバのIPアドレスに、第3、第4 オクテットが .0.255/23のIPアドレスは設定できません。

● [802.1X]を選択した場合

Authentication: 802.1X

RADIUS Server Settings

Key Update Interval: 300 (Sec)

RADIUS Server Mode

RADIUS Server: ☐ External ☐ Internal

Primary RADIUS Server Setting

RADIUS Server: RADIUS Port: 1812

RADIUS Secret:
(0-9,a-z,A-Z,~!@#\$%^&*()_+`-={[];\:|,./<>?)

Backup RADIUS Server Setting (Optional)

RADIUS Server: RADIUS Port: 1812

RADIUS Secret:
(0-9,a-z,A-Z,~!@#\$%^&*()_+`-={[];\:|,./<>?)

Primary Accounting Server Setting

Accounting Mode: Disable

Accounting Server: Accounting Port: 1813

Accounting Secret:
(0-9,a-z,A-Z,~!@#\$%^&*()_+`-={[];\:|,./<>?)

Backup Accounting Server Setting (Optional)

Accounting Server: Accounting Port: 1813

Accounting Secret:
(0-9,a-z,A-Z,~!@#\$%^&*()_+`-={[];\:|,./<>?)

項目	説明
Key Update Interval	キーを更新する間隔を設定します。 推奨値: 300 (秒)
Radius Server Mode	RADIUSサーバのモードを選択します。 選択肢: [External] (外部) [Internal] (内部)
Primary Radius Server Setting	プライマリRADIUSサーバの設定を行います。 - RADIUS Server: RADIUS サーバのIP アドレスを入力します。 - RADIUS Port: RADIUS サーバの認証に使用するポート番号を入力します。 初期値:[1812] - RADIUS Secret: RADIUS シークレット (パスワード) を入力します。
Backup Radius Server Setting (Optional)	バックアップRADIUSサーバの設定を行います。 - RADIUS Server: RADIUS サーバのIP アドレスを入力します。 - RADIUS Port: RADIUS サーバの認証に使用するポート番号を入力します。 初期値:[1812] - RADIUS Secret: RADIUS シークレット (パスワード) を入力します。
Primary Accounting Server Setting	プライマリアカウンティングサーバの設定を行います。 - Accounting Mode: アカウンティングモードを[Enable] (有効) [Disable] (無効) にします。 - Accounting Server: アカウンティングサーバのIPアドレスを入力します。 - Accounting Port: アカウンティングサーバの認証に使用するポート番号を入力します。 初期値:[1813] - Accounting Secret: アカウンティングシークレット (パスワード) を入力します。

項目	説明
Backup Accounting Server Setting (Optional)	バックアップアカウントिंगサーバの設定を行います。 - Accounting Server: アカウントिंगサーバのIPアドレスを入力します。 - Accounting Port: アカウントिंगサーバの認証に使用するポート番号を入力します。 初期値:[1813] - Accounting Secret: アカウントिंगシークレット (パスワード)を入力します。

LAN Settings (LAN設定)

本製品のLAN インタフェースのIP 設定を行います。LAN IP アドレスは必要に応じて変更することも可能です。
LAN IP アドレスはネットワーク内部で使用され、インターネット上には公開されません。

- [Basic Settings] > [LAN] を選択します。
- 以下の画面で設定を行います。

項目	説明
Get IP From	IPアドレスの取得方法を選択します。 [Static IP (Manual)]: 固定のIPアドレスを手動で設定します。 [Dynamic (DHCP)]: DHCPサーバを使用してIPアドレスを設定します。 本製品のIPアドレスは、DHCPサーバから自動的に取得されます。[Dynamic (DHCP)]を選択した場合、その他の項目の設定は不要です。
IP Address	IPアドレスを入力します。 初期値: 192.168.0.50
Subnet Mask	サブネットマスクを入力します。 初期値: 255.255.255.0
Default Gateway	デフォルトゲートウェイのIP アドレスを入力します。
DNS	DNSのIPアドレスを入力します。

- [Save] をクリックして設定を保存します。

重要

サブネットマスクを /24未満に指定した場合、IPアドレスの第4 オクテットに「.255」「.0」を指定できません。

IPv6 Settings (IPv6設定)

LAN インタフェースのIPv6 設定を行います。
本機能を有効にすると、IPv6 アドレスを使用してDAP-X2850 にアクセスすることが可能となります。

- 1. [Basic Settings] > [IPv6] を選択します。
- 2. 以下の画面で設定を行います。

IPv6 Settings

☐ Enable IPv6

Get IP From

Dynamic IP (DHCP) ▼

IPv6 Address

Prefix

Default Gateway

Save

項目	説明
Enable IPv6	チェックを入れると、IPv6アドレスが有効になります。
Get IP From	IPv6アドレスの取得方法を選択します。 • [Static IP (Manual)] : 固定のIPv6アドレスを手動で設定します。 • [Dynamic IP (DHCP)] : 本製品のIPv6アドレスは、自動的に取得されます。 [Dynamic IP (DHCP)]を選択した場合、その他の項目の設定は不要です。
IP Address	IPv6アドレスを入力します。
Prefix	プレフィックス長の値を入力します。
Default Gateway	デフォルトゲートウェイのIP アドレスを入力します。

- 3. [Save] をクリックして設定を保存します。



WebUIについて、IPv6のHTTPSをサポートしません。

Advanced Settings (詳細設定)

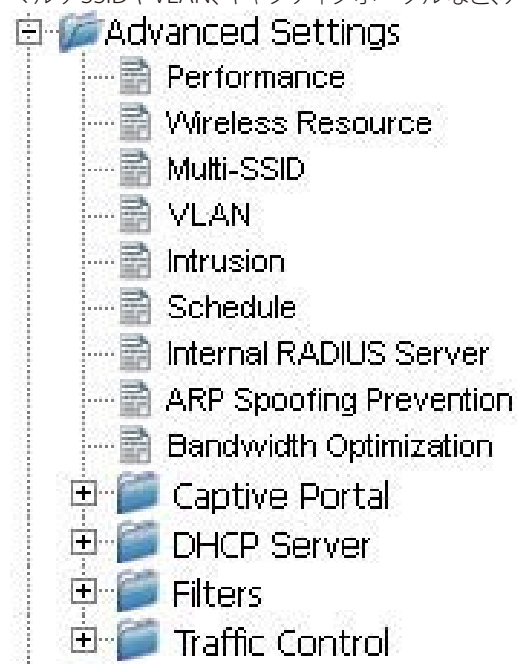
5

マルチSSIDやVLAN、キャプティブポータルなど、アクセスポイントの詳細設定を行います。

■ Advanced Settings について	42
■ Performance Settings (パフォーマンス設定)	42
■ Wireless Resource Control (ワイヤレスリソースコントロール)	45
■ Multi-SSID Settings (マルチSSID設定)	46
■ VLAN Settings (VLAN設定)	48
■ Wireless Intrusion Protection (不正AP検知)	52
■ Wireless Schedule Settings (スケジュール設定)	53
■ Internal RADIUS Server (RADIUSサーバ)	54
■ ARP Spoofing Prevention Settings (ARPスプーフィング防止設定)	55
■ Bandwidth Optimization (帯域幅最適化)	56
■ Captive Portal (キャプティブポータル)	58
Login Page Upload (ログイン画面アップロード)	65
MAC Bypass (MAC Bypass 設定)	66
Walled Garden (ウォールドガーデン 設定)	67
■ DHCP Server (DHCPサーバ設定)	68
Dynamic Pool Settings (ダイナミックプール設定)	68
Static Pool Settings (スタティックプール設定)	69
Current IP Mapping List (IPマッピングリスト)	70
■ Filters (フィルタ)	71
Wireless MAC ACL Settings (ワイヤレスMAC ACL)	71
WLAN Partition (WLANパーティション)	72
IP Filter Settings (IPフィルタ)	73
■ Traffic Control (トラフィックコントロール)	75
Uplink and Downlink Setting (アップリンク／ダウンリンク設定)	75
QoS (QoS設定)	76
Traffic Manager (トラフィックマネージャ)	77

Advanced Settings について

マルチSSIDやVLAN、キャプティブポータルなど、アクセスポイントの詳細設定を行います。



Performance Settings (パフォーマンス設定)

無線のパフォーマンス設定を行います。

1. [Advanced Settings] > [Performance] を選択します。
2. 以下の画面で設定を行います。

Performance Settings	
Wireless band	2.4GHz ▼
Wireless	On ▼
Wireless Mode	Mixed 802.11ax ▼
Data Rate	Best(Up to 1200) ▼ (Mbps)
Beacon Interval (40-500)	100
DTIM Interval (1-15)	1
Transmit Power	100% ▼
WMM (Wi-Fi Multimedia)	Enable ▼
Ack Time Out (2.4GHz, 48~200)	64 (μs)
Short GI	Enable ▼
IGMP Snooping	Disable ▼
Multicast Rate	Disable ▼ (Mbps)
Multicast Bandwidth Control	Disable ▼
Maximum Multicast Bandwidth	100 kbps
HT20/40 Coexistence	Enable ▼
Transfer DHCP Offer to Unicast	Enable ▼
STP Status	Disable ▼

Save

項目	説明
Wireless band	周波数帯を[2.4GHz]または[5GHz]から選択します。
Wireless	無線機能を[On]または[Off]に設定します。
Wireless Mode	ワイヤレスモードを選択します。選択肢は設定した周波数帯によって異なります。 - 選択肢 ([2.4GHz]を選択した場合) : [Mixed 802.11n, 802.11g and 802.11b] [Mixed 802.11g and 802.11b] [802.11n Only] [Mixed 802.11ax] - 選択肢 ([5GHz]を選択した場合) : [Mixed 802.11n, 802.11a] [802.11a Only] [802.11n Only] [Mixed 802.11ac] [Mixed 802.11ax] レガシークライアント (802.11a/g/b) 向けに互換性がある場合は、802.11n 規格の無線性能は低下します。
Data Rate	ワイヤレスアダプタのベース転送速度を設定します。(単位:Mbps) - 選択肢 ([2.4GHz]を選択した場合) :Best (Up to 54), 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1 - 選択肢 ([5GHz]を選択した場合) :Best (Up to 54), 54, 48, 36, 24, 18, 12, 9, 6 - 本製品のベース転送速度は接続しているデバイスのベース転送速度に左右されます。 - 障害物や干渉がある場合、転送速度は低下します。 - 本項目は、[Wireless Mode]で [802.11a Only] [Mixed 802.11g and 802.11b] (レガシークライアント) を選択した場合のみ設定できます。 それ以外の場合は[Best (Up to 1000)] [Best (Up to 1200)] [Best (Up to 2200)] [Best (Up to 2400)]のいずれかになります。
Beacon Interval (40-500)	ビーコンを送信する間隔を設定します。(単位:ミリ秒) - 初期値:100 - 推奨値:100 - 設定可能範囲:40-500 ビーコンとはアクセスポイントがネットワークと同期するために送信するパケットです。ビーコン間隔を長く設定すると、ワイヤレスクライアントの消費電力を節約できます。一方、短く設定すると、ワイヤレスクライアントがアクセスポイントに高速に接続できるようになります。
DTIM Interval (1-15)	DTIM (Delivery Traffic Indication Message) の間隔を設定します。 - 初期値:1 - 設定可能範囲:1-15 DTIM とは、省電力モードの無線クライアントに対して、パケットが送信待ちであることを伝えるメッセージです。
Transmit Power	無線の送信電力を設定します。 選択肢:100%、50%、25%、12.5% 送信電力を調整することで、2つのアクセスポイント間の干渉による無線適用範囲の重複を削減することができます。 例:無線適用範囲がエリアの半分をカバーしている場合は、50%を選択します。
WMM (Wi-Fi Multimedia)	WMM (Wi-Fi Multimedia) を有効または無効にします。 選択肢:[Enable] (有効) [Disable] (無効) 本機能を「Enable」(有効) にするとWi-Fiネットワークを使用して快適にオーディオやビデオアプリケーションを利用できるようになります。 本項目は、[Wireless Mode]で [802.11a Only] [Mixed 802.11g and 802.11b] (レガシークライアント) を選択した場合のみ設定できます。
Ack Time Out	「Acknowledgement Time Out」の値を入力します。 設定可能範囲は設定した周波数帯によって異なります。 設定可能範囲: 2.4GHzの場合:48-200 μs 5GHzの場合:25-200 μs 本項目を設定することで、効率的に長距離のスループットを最適化します。

項目	説明
Short GI	Short GI (ショートガードインターバル) を有効または無効にします。 選択肢: [Enable] (有効) [Disable] (無効) ショートガードインターバルを有効にすると、スループットが増加します。同時に無線周波数の感度が上がるため、設置環境によってはエラー率が増加する場合がありますので、ご注意ください。 本項目は、[Wireless Mode] で [802.11a Only] [Mixed 802.11g and 802.11b] (レガシークライアント) を選択した場合には使用できません。
IGMP Snooping	IGMP (Internet Group Management Protocol) スヌーピングを有効または無効にします。 選択肢: [Enable] (有効) [Disable] (無効) IGMPスヌーピング機能を利用すると、アクセスポイントはルータとIGMP ホスト間で送信されるIGMP クエリとIGMP レポートを認識ようになります。本機能が有効な場合、アクセスポイントを通過したIGMP メッセージに基づき、ホストにマルチキャストパケットを送信します。 本項目は、WDSモードを選択している場合は設定できません。
Multicast Rate	マルチキャストレートの数値を設定、またはマルチキャストレートを無効 ([Disable]) に設定します。(単位: Mbps) 本項目は、[Wireless Mode] で [Mixed 802.11n, 802.11g and 802.11b] [Mixed 802.11g and 802.11b] [Mixed a/n mode] [802.11a Only] を選択した場合に設定できます。
Multicast Bandwidth Control	マルチキャスト帯域幅管理を有効または無効にします。 選択肢: [Enable] (有効) [Disable] (無効) 本項目は、WDSモードを選択している場合、設定できません。
Maximum Multicast Bandwidth	イーサネットインタフェースとアクセスポイント間における、最大マルチキャスト帯域幅を設定します。 初期値: 100Kbps 本項目は、[Multicast Bandwidth Control] を有効にした場合のみ設定できます。
HT20/40 Coexistence	20/40MHz 通信の同時利用を有効または無効にします。 - 選択肢: [Enable] (有効) [Disable] (無効) - 本項目を有効化すると、エリア内の無線ネットワークからの干渉を抑制します。チャンネル帯域を40MHzで使用中に他の無線ネットワークチャンネルからの干渉を受ける場合、本製品は自動的に20MHzへ変更し干渉を避けます。 - 本項目は、[Basic Settings] > [Wireless] で [Channel Width] が [Auto 20/40MHz]、本画面の [Wireless band] が [2.4GHz] の場合に使用できます。
Transfer DHCP Offer to Unicast	LANからWANに対するユニキャストへのDHCPオファー送信を有効または無効にします。ステーション数が30台を超える場合は本機能を有効にすることを推奨します。 選択肢: [Enable] (有効) [Disable] (無効)
STP Status	STPステータスを有効または無効にします。 選択肢: [Enable] (有効) [Disable] (無効) STP (スパンニングツリープロトコル) を有効化すると、ネットワークにおけるループの発生を防止できます。

3. [Save] をクリックして設定を保存します。

重要

[Basic Settings] > [Wireless Settings] 画面の [Authentication] で以下を選択した場合、[Wireless Mode] で [802.11n only] を選択できなくなります。

- [802.1X] を選択した場合
- [Open System] を選択し、[Encryption] を [Enable] に設定した場合

Wireless Resource Control (ワイヤレスリソースコントロール)

ワイヤレス接続設定を行い、デバイスがより適したワイヤレス接続を検知できるようにします。

1. [Advanced Settings] > [Wireless Resource] を選択します。
2. 以下の画面で設定を行います。

Wireless Resource Control

Airtime Fairness: Disable

Band Steering: Disable

Wireless band: 2.4GHz

Connection Limit: Disable

User Limit (0 - 64): 20

11n Preferred: Disable

Network Utilization: 100%

Aging out: Disable

RSSI Threshold: 100%

Data Rate Threshold: 54

ACL RSSI: Disable

ACL RSSI Threshold: 60%

Save

項目	説明
Airtime Fairness	エアタイムフェアネス機能を [Enable] (有効) または [Disable] (無効) に設定します。
Band Steering	バンドステアリング機能を [Enable] (有効) または [Disable] (無効) に設定します。 バンドステアリングは、ワイヤレスクライアントが2.4GHzと5GHzの両方をサポートしている場合、クライアントを5GHzに誘導する機能です。 ※バンドステアリングを有効にするには、2.4GHz、5GHzの Primary SSIDを同一の文字列に設定する必要があります。
Wireless band	周波数帯を [2.4GHz] または [5GHz] から選択します。
Connection Limit	接続するユーザ数の制限を [Enable] (有効) または [Disable] (無効) に設定します。 Connection Limitが有効に設定され、接続ユーザ数がUser LimitまたはNetwork Utilizationの設定値を超えた場合、クライアントの接続を受け付けなくなります。 • User Limit (0-64) : 接続可能なユーザ数を0-64から指定します。初期値: 20 • 11n Preferredまたは11n/ac Preferred : [Enable] (有効) または [Disable] (無効) を選択します。 有効にすると、11nまたは11n/ac/axクライアントの接続が優先されます。 • Network Utilization : 最大ネットワーク使用率を100%、80%、60%、40%、20%、0%から選択します。設定値に達した場合、ネットワークの過密状態を解消するために1分間休止状態となります。 WDSモードでは使用できません。
Aging out	ワイヤレスクライアントを切断する基準を設定します。 [RSSI] [Data Rate] または [Disable] (無効) のいずれかを選択します。 • RSSI Threshold : RSSIのしきい値を10% - 100%間で指定します。 無線クライアントのRSSIが設定値を下回ると、無線接続が切断されます。 • Data Rate Threshold : データレートのしきい値を6、9、12、18、24、36、48、54から指定します。無線クライアントのデータレートが設定値を下回ると、無線接続が切断されます。
ACL RSSI	ACL RSSIを [Enable] (有効) または [Disable] (無効) に設定します。 本項目を有効化すると、下記項目で指定されたRSSIのしきい値を下回っている無線クライアントからの接続リクエストを拒否します。 • ACL RSSI Threshold : ACL RSSIのしきい値を10% - 100%間で指定します。

3. [Save] をクリックして設定を保存します。

Multi-SSID Settings (マルチSSID設定)

マルチSSIDの設定を行います。
本製品は周波数帯ごとに最大8個のSSIDをサポートしています。プライマリSSIDは [Basic] > [Wireless]画面から設定可能です。
SSIDの初期値は「dlink」です。

- 1. [Advanced Settings] > [Multi SSID] を選択します。
- 2. 以下の画面で設定を行います。

Multi-SSID Settings

☐ Enable Multi-SSID☐ Enable Priority

Wireless Settings

Band2.4 GHz

IndexPrimary SSID

SSIDdlink

SSID VisibilityEnable

SecurityOpen System

Priority0

WMM (Wi-Fi Multimedia)Enable

Key Settings

Encryption

☒ Disable☐ Enable

Key TypeHEX

Key Size64 Bits

Key Index(1~4)1

Network Key

Confirm Key

(0-9,a-z,A-Z,~!@#\$%^&*()_+`-={[]:;'",./<>?)

Add

Index	SSID	Band	Encryption	Delete
Primary SSID	dlink	2.4 GHz	None	

Save

項目	説明
Enable Multi-SSID	チェックを入れるとマルチSSIDが有効になります。
Enable Priority	チェックを入れるとSSID の優先機能が有効になります。 有効にすると、画面下部の [Priority]で0 から7 までの優先値をSSID に設定できます。

項目	説明
Wireless Settings	マルチSSIDのワイヤレス設定を行います。 • Band : 周波数帯を[2.4GHz]または[5GHz]に設定します。 • Index : マルチSSIDを以下から選択します。 [Primary SSID] [SSID1] [SSID2] [SSID3] [SSID4] [SSID5] [SSID6] [SSID7] • SSID : SSID名を入力します。 • SSID Visibility : [Enable] (有効) または [Disable] (無効) に設定します。 有効にするとSSID がネットワーク上にブロードキャストされ、すべてのネットワークユーザから閲覧できるようになります。 • Security セキュリティを[Open System] [Enhanced Open] [Enhanced Open + Open] [WPA-Personal] [WPA-Enterprise] [802.1X]から選択します。 WDSモードまたはWDS with APモードの場合、[Open System] [WPA-Personal]のみ選択できます。選択した設定によって、画面下部に詳細設定を行う項目が表示されます。 セキュリティの詳細設定については『Authentication (認証) の設定について:p.35』を参照してください。 • Priority SSIDの優先値を「0」-「7」の間で設定します。 • WMM (Wi-Fi Multimedia) [Enable] (有効) または [Disable] (無効) に設定します。 本機能を「Enable」(有効) にするとWi-Fiネットワークを使用して快適にオーディオやビデオアプリケーションを利用できるようになります。

3. [Add] をクリックし、SSID を追加します。

◆ 追加した SSID を削除する場合：

1. [Delete] 欄の  アイコンをクリックします。
2. 確認メッセージが表示されるので、「OK」をクリックします。

◆ 追加した SSID を編集する場合：

1. [Index] 欄でインデックス名を選択します。
2. [Add] をクリックして設定を保存します。

4. [Save] をクリックして設定を保存します。

VLAN Settings (VLAN設定)

本製品はVLAN をサポートしています。
VLAN は、名前、VID、Mgmt (TCP スタック)、LAN、プライマリ/ マルチSSID を指定して作成することができます。
VLAN タグなしで本製品に送信されたパケットには、すべてPVID を持つVLAN タグが付けられます。

- 1. [Advanced Settings] > [VLAN] を選択します。
- 2. [VLAN Status] で、VLAN を [Enable] (有効) または [Disable] (無効) に設定します。

メモ

[VLAN Mode]には、現在のVLANモードが表示されます。

- 3. 以下のタブを使用して必要な設定を行います。
 - ・『VLAN List タブ:p.48 』
 - ・『Port List タブ:p.48 』
 - ・『Add/Edit VLAN タブ:p.50 』
 - ・『PVID Settingタブ:p.51 』

● VLAN List タブ

現在設定されているVLANのリストが表示されます。



項目	説明
VID	VLAN のIDが表示されます。
VLAN Name	VLAN名が表示されます。
Untag VLAN Ports	タグ無しVLANポートが表示されます。
Tag VLAN Ports	タグ付きVLANポートが表示されます。
Edit	アイコンをクリックすると [Add/Edit VLAN] タブの内容が表示され、VLANの編集を行うことができます。
Delete	アイコンをクリックするとVLANを消去できます。

● Port List タブ

現在のポートのリストが表示されます。
VLAN にゲストネットワークと内部ネットワークを設定するためには、使用しているスイッチとDHCP サーバがVLAN をサポートしている必要があります。事前にスイッチのポートがIEEE 802.1Q 定義のVLAN タグ付きパケットをサポートするように設定を行ってください。

VLAN Settings

VLAN Status : ☒ Disable ☐ Enable Save

VLAN Mode : Static(2.4G), Static(5G)

VLAN List	Port List	Add/Edit VLAN	PVID Setting
Port Name	Tag VID	Untag VID	PVID
Mgmt		1	1
LAN		1	1
LAN(PoE)		1	1
Primary(2.4G)		1	1
Primary(5G)		1	1
S-1(2.4G)		1	1
S-2(2.4G)		1	1
S-3(2.4G)		1	1
S-4(2.4G)		1	1
S-5(2.4G)		1	1
S-6(2.4G)		1	1
S-7(2.4G)		1	1
S-1(5G)		1	1
S-2(5G)		1	1
S-3(5G)		1	1
S-4(5G)		1	1
S-5(5G)		1	1
S-6(5G)		1	1
S-7(5G)		1	1

項目	説明
Port Name	ポート名が表示されます。
Tag VID	タグ付きVLAN IDが表示されます。
Untag VID	タグ無しVLAN IDが表示されます。
PVID	ポートVLAN IDが表示されます。

● Add/Edit VLAN タブ

新しいVLANの追加または既存のVLANの編集を行います。

VLAN Settings

VLAN Status : ☒ Disable ☐ Enable

Save

VLAN Mode : Static(2.4G), Static(5G)

VLAN List

Port List

Add/Edit VLAN

PVID Setting

VLAN ID (VID)

VLAN Name

Port	Select All	Mgmt	LAN	LAN(PoE)
Untag	All	☐	☐	☐
Tag	All	☐	☐	☐
Not Member	All	☐	☐	☐

2.4GHz

MSSID Port	Select All	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
Untag	All	☐	☐	☐	☐	☐	☐	☐	☐
Tag	All	☐	☐	☐	☐	☐	☐	☐	☐
Not Member	All	☐	☐	☐	☐	☐	☐	☐	☐

5GHz

MSSID Port	Select All	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
Untag	All	☐	☐	☐	☐	☐	☐	☐	☐
Tag	All	☐	☐	☐	☐	☐	☐	☐	☐
Not Member	All	☐	☐	☐	☐	☐	☐	☐	☐

Save

項目	説明
VLAN ID (VID)	内部VLAN 用の番号を入力します。 ・ 設定可能範囲：1-4094
VLAN Name	追加または変更するVLAN 名を入力します。
Port MSSID Port	・ Untag：ポートをタグなしとして定義します。 ・ Tag：ポートをタグ付きとして定義します。 ・ Not Member：ポートをVLAN メンバとしないように定義します。 All を選択するとすべてのポートが選択されます。

◆ 新しい VLAN を追加する場合：

- [VLAN Status] を [Enable] にします。
- [VLAN ID (VID)] に識別番号、[VLAN Name] に識別名を入力します。
- VLAN ポートを編集します。
- [Save] をクリックして設定を保存します。

◆ 既存の VLAN を編集する場合：

- [VLAN List] タブで編集する VLAN の  アイコンをクリックします。
- [Add/Edit VLAN] タブが表示されるので、VLAN の編集を行います。
- [Save] をクリックして設定を保存します。

● PVID Settingタブ

PVID 自動割り当て設定および各PVID 設定を行います。

VLAN Settings

VLAN Status : ☐ Disable ☒ Enable Save

VLAN Mode : Static(2.4G), Static(5G)

VLAN List | Port List | Add/Edit VLAN | **PVID Setting**

PVID Auto Assign Status ☒ Disable ☐ Enable

Port	Mgmt	LAN	LAN(PoE)
PVID	1	1	1

2.4GHz

MSSID Port	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
PVID	1	1	1	1	1	1	1	1

5GHz

MSSID Port	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
PVID	1	1	1	1	1	1	1	1

Save

項目	説明
PVID Auto Assign Status	PVID自動割り当て設定を有効または無効にします。 ・ 選択肢:[Enable] (有効) [Disable] (無効)
Port MSSID Port	PVID自動割り当て設定を無効にした場合に、PVIDの設定を行います。

4. [Save] をクリックして設定を保存します。

Wireless Intrusion Protection (不正AP検知)

アクセスポイントの検知を行い、検知したアクセスポイントを分類することができます。

- 1. [Advanced Settings] > [Intrusion] を選択します。
- 2. 以下の画面でアクセスポイントの検知と分類を行います。

Wireless Intrusion Protection

Wireless Band

2.4GHz

Detect

AP List

All

	Type	Band	CH	SSID	BSSID	Last Seen	Status
--	------	------	----	------	-------	-----------	--------

Set as Valid

Set as Neighborhood

Set as Rogue

Set as New

☐ Mark All New Access Points as Valid Access Points

☐ Mark All New Access Points as Rogue Access Points

Save

項目	説明
Wireless Band	周波数帯を[2.4GHz]または[5GHz]から選択します。
Detect	アクセスポイントの検知を実行します。
AP List	検知したアクセスポイントのリストを表示します。 表示するアクセスポイントは以下から選択できます。 • [All] :すべてのアクセスポイント • [Valid] :正しいアクセスポイント • [Neighbor] :隣接したアクセスポイント • [Rogue] :不正なアクセスポイント (未認証) • [New] :新しいアクセスポイント
Set as Valid	チェックを入れたアクセスポイントを、正しいアクセスポイントとして分類します。
Set as Neighborhood	チェックを入れたアクセスポイントを、隣接したアクセスポイントとして分類します。
Set as Rogue	チェックを入れたアクセスポイントを不正なアクセスポイントとして分類します。
Set as New	チェックを入れたアクセスポイントを、新しいアクセスポイントとして分類します。

メモ

- [Mark All New Access Points as Valid Access Points]を選択すると、新たに検知されたすべてのアクセスポイントが正しいアクセスポイントとして分類されます。
- [Mark All New Access Points as Rogue Access Points]を選択すると、新たに検知されたすべてのアクセスポイントが不正なアクセスポイントとして分類されます。

- 3. [Save] をクリックして設定を保存します。

Wireless Schedule Settings (スケジュール設定)

無線機能のスケジュールルールを追加、または編集できます。

1. [Advanced Settings] > [Schedule] を選択します。
2. 以下の画面で設定を行います。

項目	説明
Wireless Schedule	無線スケジュール設定を有効または無効にします。
Add Schedule Rule	スケジュールルールの追加・編集を行います。 • Name : ルール名を入力します。 • Index : ドロップダウンリストから対象のSSIDを選択します。 • SSID : ネットワーク名 (SSID) が表示されます。 • Days : [All Week] (毎日) または [Select Day (s)] (曜日指定) を選択します。 [Select Day (s)] を選択した場合、ルールを適用する曜日を指定します。 • All Day(s) : チェックを入れると終日が指定されます。 • Start Time/End Time : 開始時刻と終了時刻を指定します。 [Overnight] にチェックを入れると、開始時刻から日付を跨いで終了時刻を設定できます。 (例: 21:00-07:00) 時刻は24時間表記で指定してください。 • Add : 設定した内容を追加します。 • Clear : 設定した内容を取り消します。
Schedule Rule List	設定したスケジュールルールが表示されます。

- ◆ スケジュールルールを削除する場合：
 1. [Schedule Rule List] 欄の アイコンをクリックします。
 2. 確認メッセージが表示されるので、「OK」をクリックします。
 - ◆ スケジュールルールを編集する場合：
 1. [Schedule Rule List] の アイコンをクリックします。
 2. [Add Schedule Rule] でルールを編集します。
 3. [Add] をクリックして設定を保存します。
3. [Save] をクリックして設定を保存します。

Internal RADIUS Server (RADIUSサーバ)

本製品はRADIUSサーバを内蔵しています。
本項目では、RADIUSアカウントの作成／削除方法およびアカウントを有効／無効にする方法について説明します。
作成するアカウント数は30個以内にすることをおすすめします。

- 1. [Advanced Settings] > [Internal RADIUS Server] を選択します。
- 2. 以下の画面で設定を行います。

Internal RADIUS Server

Add RADIUS Account

User Name

Password

Status

Enable ▾

RADIUS Account list

User Name	Enable	Disable	Delete

Save

項目	説明
Add RADIUS Account	RADIUSアカウントの追加を行います。 • User Name : アカウントのユーザ名を入力します。 • Password : アカウントのパスワードを入力します。 入力可能文字数:8～64文字以内 • Status : アカウントのステータスを[Enable](有効)または[Disable](無効)にします。
RADIUS Account list	作成したアカウントのリストが表示されます。 アカウントを削除する場合は、  アイコンをクリックします。

- 3. [Save] をクリックして設定を保存します。

ARP Spoofing Prevention Settings (ARPスプーフィング防止設定)

ARP スプーフィング防止機能は、IP/MAC アドレスをマッピングすることにより、ARP スプーフィング攻撃を防止する機能です。

1. [Advanced Settings] > [ARP Spoofing Prevention] を選択します。
2. 以下の画面で設定を行います。

項目	説明
ARP Spoofing Prevention	ARPスプーフィング防止を有効または無効にします。 ・選択肢:[Enable] (有効) [Disable] (無効)
Add Gateway Address	ゲートウェイアドレスの追加・編集を行います。 ・Gateway IP Address : ゲートウェイIPアドレスを入力します。 ・Gateway MAC Address : ゲートウェイMACアドレスを入力します。 ・Add :設定した内容を追加します。 ・Clear :設定した内容を取り消します。
Gateway Address List	ゲートウェイアドレスのリストが表示されます。

- ◆ ゲートウェイアドレスを削除する場合：
 1. [Gateway Address List] 欄の  アイコンをクリックします。
 2. 確認メッセージが表示されるので、「OK」をクリックします。
 - ◆ ゲートウェイアドレスを編集する場合：
 1. [Gateway Address List] の  アイコンをクリックします。
 2. [Add Gateway Address] でルールを編集します。
 3. [Add] をクリックして設定を保存します。
3. [Save] をクリックして設定を保存します。

Bandwidth Optimization（帯域幅最適化）

帯域幅最適化機能を使用すると、本製品およびワイヤレスクライアントの帯域幅を管理することができます。
本項目では、帯域幅最適化機能の設定方法について説明します。

- 1. [Advanced Settings] > [Bandwidth Optimization] を選択します。
- 2. 以下の画面で設定を行います。

Bandwidth Optimization

Enable Bandwidth Optimization

Disable

Downlink Bandwidth

80

Mbits/sec

Uplink Bandwidth

80

Mbits/sec

Add Bandwidth Optimization Rule

Rule Type

Allocate average BW for each station

Band

2.4 GHz

SSID Index

Primary SSID

Downlink Speed

Kbits/sec

Uplink Speed

Kbits/sec

Add

Clear

Bandwidth Optimization Rules

Band	Type	SSID Index	Downlink Speed	Uplink Speed	Edit	Del
------	------	------------	----------------	--------------	------	-----

Save

項目	説明
Enable Bandwidth Optimization	帯域幅最適化を有効または無効にします。 ・ 選択肢: [Enable] (有効) [Disable] (無効)
Downlink Bandwidth	本製品のダウンリンクの帯域幅を入力します。 単位: Mbits (秒)
Uplink Bandwidth	本製品のアップリンクの帯域幅を入力します。 単位: Mbits (秒)

項目	説明
Add Bandwidth Optimization Rule	帯域幅最適化ルールの追加・編集を行います。 • Rule Type :以下からルールタイプを指定します。 - Allocate average BW for each station Downlink/Uplink Speedの設定値を、各クライアントで平等にシェアします。 - Allocate maximum BW for each station Downlink/Uplink Speedの設定値が、各クライアントの最大値となります。 - Allocate different BW for a/b/g/n stations a/b/g/nのクライアントに異なる帯域幅を割り当てます。 • 11b/g/nクライアント:10% / 20% / 70% • 11a/nクライアント:20% / 80% - Allocate specific BW for SSID すべてのクライアントで全体の帯域幅をシェアします。 • Band : 周波数帯を[2.4GHz]または[5GHz]から選択します。 • SSID Index : ドロップダウンリストから対象のSSIDを選択します。 • Downlink Speed : ダウンリンクの速度を設定します。単位はKbits/秒またはMbps/秒から選択できます。 • Uplink Speed : アップリンクの速度を設定します。単位はKbits/秒またはMbps/秒から選択できます。 • Add : 設定を追加します。 • Delete : 設定した内容を取り消します。
Bandwidth Optimization Rules	作成したルールのリストが表示されます。

◆ 帯域幅最適化ルールを削除する場合：

1. [Bandwidth Optimization Rules] 欄の  アイコンをクリックします。
2. 確認メッセージが表示されるので、「OK」をクリックします。

◆ 帯域幅最適化ルールを編集する場合：

1. [Bandwidth Optimization Rules] の  アイコンをクリックします。
2. [Add Bandwidth Optimization Rule] でルールを編集します。
3. [Add] をクリックして設定を保存します。

3. [Save] をクリックして設定を保存します。

Captive Portal（キャプティブポータル）

キャプティブポータルは、Web認証を行う機能です。
認証されていないクライアントがアクセスポイントに接続すると、Webブラウザによって認証画面へリダイレクトされます。

重要

- Captive Portalの設定において、内部的に DNS宛での Static Routeを生成するため、構成によっては対象の DAP-X2850への通信が不可となる場合があります。

Captive Portal Authentication（キャプティブポータル認証）

キャプティブポータル認証の認証タイプを選択し、必要な設定を行います。

1. [Advanced Settings] > [Captive Portal] > [Authentication Settings] を選択します。
2. [Authentication Type] で認証タイプを選択します。

Captive Portal Authentication

Band

2.4GHz

SSID Index

Primary SSID

Idle Timeout (1-1440)

60

Minute(s)

Authentication Type

Disable

Save

Band	SSID Index	Captive Profile	Edit	Delete
------	------------	-----------------	------	--------

項目	説明
Band	周波数帯を[2.4GHz]または[5GHz]から選択します。
SSID Index	認証を行うSSIDを指定します。
Idle Timeout(1-1440)	タイムアウト値を設定します。クライアントがアクセスポイントから切断され、指定した時間が経過すると再認証が必要となります。 • 初期値：60分 • 設定可能範囲：1-1440（分）
Authentication Type	キャプティブポータル認証の認証タイプを設定します。 [Disable]（無効）に設定した場合は画面下部の設定項目は表示されません。 • 選択肢： [Disable] [Web Redirection Only] [Username/Password] [Passcode] [Remote RADIUS] [LDAP] [POP3] [Click Through]

3. 認証タイプごとに必要な設定を行います。

メモ

- ・非Mgmt VLANの無線接続について、キャプティブポータル認証前/認証済SSIDはTetnet/WebUI接続不可、ICMP接続は可能です。
- ・選択した認証タイプによって設定項目が異なります。
- ・選択できる認証タイプは以下の通りです。
 - Web Redirection Only → 『認証タイプを[Web Redirection Only]にした場合:p.59』を参照
 - Username/Password → 『認証タイプを[Username/Password]にした場合:p.60』を参照
 - Passcode → 『認証タイプを[Passcode]にした場合:p.61』を参照
 - Remote RADIUS → 『認証タイプを[Remote RADIUS]にした場合:p.62』を参照
 - LDAP → 『認証タイプを[LDAP]にした場合:p.63』を参照
 - POP3 → 『認証タイプを[POP3]にした場合:p.63』を参照
 - Click Through → [Web Redirection Only]を選択した場合と同じ項目が表示されます。

● 認証タイプを[Web Redirection Only]にした場合

Webリダイレクトを使用して認証を行います。

WEBリダイレクトとは、サイトにアクセスしようとしたユーザを、最初にリクエストされた URL とは別の URL に移動させることです。クライアントは、キャプティブポータルによる認証の際に本項目で設定したWebサイトにリダイレクトされます。

1. 以下の画面でWebリダイレクトの設定を行います。

項目	説明
Web Redirection State	Webリダイレクションのステートは[Enable]に固定されます。
URL Path	[http://] または [https://] を設定し、WebサイトのURLを入力します。
IRIF Status	キャプティブポータルのIPインタフェースを[Enable](有効)または[Disable](無効)に設定します。
VLAN Group	VLAN Group IDを入力します。
Get IP From	IPアドレスの取得方法を選択します。 • [Static IP (Manual)]: 固定のIPアドレスを手動で設定します。 • [Dynamic (DHCP)]: DHCPサーバを使用してIPアドレスを設定します。本製品のIPアドレスは、DHCPサーバから自動的に取得されます。[Dynamic (DHCP)]を選択した場合、その他の項目の設定は不要です。本項目を選択後、DHCPクライアントが機能するまで約2分かかります。
IP Address	IPアドレスを入力します。
Subnet Mask	サブネットマスクを入力します。
Gateway	ゲートウェイのIPアドレスを入力します。
DNS	Domain Name System (DNS)サーバのアドレスを入力します。

● 認証タイプを[Username/Password]にした場合

ユーザ名とパスワードを使用して認証を行います。

1. 以下の画面でユーザ名とパスワードの設定を行います。

Username/Password Settings

Username

Password

Add

Clear

Username

Edit

Delete

Save

項目	説明
Username/Password Settings	アカウントの設定を行います。 • User Name : アカウントのユーザ名を入力します。 • Password : アカウントのパスワードを入力します。 • Add : 設定した内容を追加します。 • Clear : 設定した内容をクリアします。

2. [Add]をクリックしてユーザ名とパスワードの設定を追加します。

◆ ユーザ名とパスワードの設定を削除する場合：

1. [Delete] 欄の  アイコンをクリックします。

◆ ユーザ名とパスワードの設定を編集する場合：

1. [Edit] 欄の  アイコンをクリックします。

2. 設定を編集します。

3. [Add] をクリックします。

● 認証タイプを[Passcode]にした場合

パスコードを使用して認証を行います。

- 以下の画面でパスコードの設定を行います。

項目	説明
Passcode Quantity	生成するパスコードの数を設定します。
Duration	生成したパスコードを有効にする時間(単位:時間)を設定します。
Last Active Time	生成したパスコードが有効となる最終日(年/月/日/時)を設定します。
User Limit	生成したパスコードを利用できるユーザ数の上限を設定します。
Add	設定した内容を追加します。
Clear	設定した内容を取り消します。
Delete All	設定したパスコードすべてを削除します。

- [Add]をクリックしてパスコード設定を追加します。

生成されたパスコードは以下のように表示されます。

Passcode	Duration	Last Active Time	User Limit	Delete
40499016	1	2019-01-01 01:00	1	

◆ パスコード設定を削除する場合：

- [Delete] 欄の アイコンをクリックします。
- 確認メッセージが表示されるので、「OK」をクリックします。

● 認証タイプを[Remote RADIUS]にした場合

リモートRADIUSを使用して認証を行います。

1. 以下の画面でユーザ名とパスワードの設定を行います。

Remote RADIUS Settings

RADIUS Server Settings

RADIUS Server

RADIUS Port

1812

RADIUS Secret

Remote RADIUS Type

SPAP

NAS ID

Disable

Secondary radius Server Settings

RADIUS Server

RADIUS Port

1812

RADIUS Secret

Remote RADIUS Type

SPAP

Third radius Server Settings

RADIUS Server

RADIUS Port

1812

RADIUS Secret

Remote RADIUS Type

SPAP

Radius account server

Primary Accounting Server Settings

Accounting Mode

Disable

Accounting Server

Accounting Port

1813

Accounting Secret

Secondary Accounting Server Settings (optional)

Accounting Server

Accounting Port

1813

Accounting Secret

Third Accounting Server Settings (optional)

Accounting Server

Accounting Port

1813

Accounting Secret

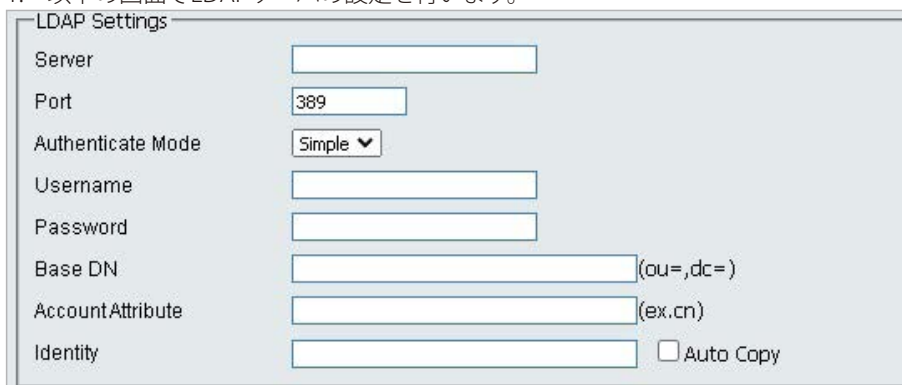
項目	説明
RADIUS Server Settings Secondary radius Server Settings Third radius Server Settings	RADIUSサーバ、セカンダリRADIUSサーバ、ターシャリRADIUSサーバの設定を行います。 • RADIUS Server : RADIUSサーバのIPアドレスを入力します。 • RADIUS Port : RADIUSサーバのポートを入力します。 初期値: 1812 • RADIUS Secret: RADIUSシークレット (パスワード) を入力します。 • Remote Radius Type: リモートRADIUSのタイプを選択します。 選択肢: [SPAP] [MS-CHAPv2] 初期値: [SPAP]
Primary Accounting Server Settings Secondary Accounting Server Settings (optional) Third Accounting Server Settings (optional)	RADIUSアカウントサーバの設定を行います。 オプションでセカンダリ/ターシャリアカウントサーバも設定できます。 • Accounting Mode: アカウントモードを有効または無効に設定します。 • Accounting Server: アカウントサーバのIPアドレスを入力します。 • Accounting Port : アカウントのポートを入力します。 初期値: 1813 • Accounting Secret : アカウントシークレット (パスワード) を入力します。

62

● 認証タイプを[LDAP]にした場合

LDAPサーバを使用して認証を行います。

1. 以下の画面でLDAPサーバの設定を行います。



The image shows a screenshot of the 'LDAP Settings' configuration window. It contains several input fields and a checkbox. The fields are: 'Server' (empty), 'Port' (389), 'Authenticate Mode' (Simple), 'Username' (empty), 'Password' (empty), 'Base DN' (empty with '(ou=,dc=)' as a hint), 'Account Attribute' (empty with '(ex,cn)' as a hint), and 'Identity' (empty). There is an 'Auto Copy' checkbox which is currently unchecked.

項目	説明
Server	LDAPサーバのIPアドレスまたはドメイン名を入力します。
Port	LDAPサーバのポートを入力します。 ・初期値:389
Authenticate Mode	認証モードを[Simple]または[TLS]から選択します。 ・ Simple :LDAPデータは暗号化されません。 ・ TLS : LDAPデータは暗号化されます。
Username	LDAPサーバアカウントのユーザ名を入力します。
Password	LDAPサーバアカウントのパスワードを入力します。
Base DN	ベースDNを入力します。
Account Attribute	LDAPアカウントの属性値を入力します。 この文字列はクライアントの検索に使用されます。
Identity	アイデンティティのパスストリング全体を入力してください。 [Auto Copy]にチェックを入れると、自動的にパスが入力されます。

● 認証タイプを[POP3]にした場合

POP3サーバを使用して認証を行います。

1. 以下の画面でPOP3サーバの設定を行います。



The image shows a screenshot of the 'POP3 Settings' configuration window. It contains three input fields: 'Server' (empty), 'Port' (110), and 'Connection Type' (None). The 'Connection Type' is a dropdown menu.

項目	説明
Server	POP3サーバのIPアドレスまたはドメイン名を入力します。
Port	POP3サーバのポート番号を入力します。 ・初期値:110
Connection Type	接続モードを選択します。 ・選択肢:[None] [SSL/TLS]

4. 画面下部の [Save] をクリックして、手順 3 で設定した内容をキャプティブポータルのプロファイルに追加・反映します。

設定した内容は以下のように表示されます。

Band	SSID Index	Captive Profile	Edit	Delete
2.4GHz	Primary SSID	Web Redirection Only Profile		

- ◆ キャプティブポータルのプロファイル削除する場合：
 1. [Delete] 欄の  アイコンをクリックします。
 2. 確認メッセージが表示されるので、「OK」をクリックします。
- ◆ キャプティブポータルのプロファイルを編集する場合：
 1. [Edit] 欄の  アイコンをクリックします。
 2. 設定を編集します。
 3. [Save] をクリックして設定を保存します。

■ Login Page Upload (ログイン画面アップロード)

キャプティブポータルに使用するカスタムのログインWeb画面をアップロードすることができます。

1. [Advanced Settings] > [Captive Portal] > [Login Page Upload] を選択します。
2. [ファイルを選択] をクリックし、アップロードするログインスタイルファイルを選択します。

項目	説明
Upload Login Style From Local Hard Drive	アップロードするログインスタイルファイルを選択します。 [The Left space]は、デバイス上の利用可能なメモリ (Bytes) を示しています。
Login Page Style List	• [Wireless Band] 周波数帯を選択します。 選択肢: [2.4GHz] [5GHz] • [ID / Style Name] 各SSIDで使用するファイルを選択します。 ファイルをダウンロードする場合は[Download]欄の  アイコン、削除する場合は [Del] 欄の  アイコンをクリックします。

3. [Upload] をクリックしてファイルをアップロードします。

◆ SSID に紐づけるログイン画面を変更する場合：

1. [Wireless Band] 欄で周波数帯を選択し、使用するファイルを選択します。
2. 「Save」をクリックします。

■MAC Bypass (MAC Bypass 設定)

本項目では、MAC Bypassの設定方法について説明します。

- 1. [Advanced Settings] > [Captive Portal] > [MAC Bypass Settings] を選択します。
- 2. 以下の画面で設定を行います。

MAC Bypass Settings

Wireless Band

2.4GHz

SSID Index

Primary SSID

MAC Address

Add

ID

MAC Address

Delete

Upload MAC File

Upload File :

ファイルを選択

選択されていません

Upload

Download MAC File

Load MAC File to Local Hard Driver :

Download

Save

項目	説明
Wireless Band	周波数帯を[2.4GHz]または[5GHz]に設定します。
SSID Index	SSIDを選択します。
MAC Address	以下の手順でMACアドレスを登録します。 1. MACアドレスを入力します。 2. [Add]をクリックします。 追加したMACアドレスを削除する場合は[Delete]欄のアイコンをクリックします。
Upload MAC File	MAC Bypassリストのファイルのアップロードを行います。 [ファイルを選択]をクリックしてMAC Bypassリストのファイルを選択し、[Upload]をクリックします。
Download MAC File	[Download]をクリックし、MAC Bypassリストのファイルをダウンロードします。

- 3. [Save] をクリックして設定を保存します。

メモ

- MAC Bypassエントリの最大数はSSID毎に64です。

■ Walled Garden (ウォールドガーデン 設定)

本項目では、ウォールドガーデン の設定方法について説明します。

ウォールドガーデンでは、" キャプティブポータルが設定された SSID " にアクセスしたユーザが、キャプティブポータルの認証なしでアクセスできるホスト名または IP アドレスを指定します。キャプティブポータルでの認証が完了していないユーザは、指定したホスト名または IP アドレスにのみアクセス可能となるため、認証されていないユーザのインターネットへのアクセスを制限できます。

1. [Advanced Settings] > [Captive Portal] > [Walled Garden] を選択します。
2. 以下の画面で設定を行います。

項目	説明
Wireless Band	周波数帯を[2.4GHz]または[5GHz]に設定します。
SSID Index	SSIDを選択します。
Walled Garden State	ウォールドガーデンを有効または無効に設定します。
Walled Garden Range	ウォールドガーデンの範囲をホスト名または IP アドレスで入力します。
Upload Walled Garden File	ウォールドガーデン範囲のリストをアップロードします。 [ファイルを選択] をクリックしてファイルを選択し、[Upload]をクリックします。
Download Walled Garden File	[Download]をクリックし、ウォールドガーデン範囲のリストをダウンロードします。

3. [Save] をクリックして設定を保存します。

DHCP Server (DHCPサーバ設定)

本製品のDHCP (Dynamic Host Configuration Protocol) サーバ機能の設定を行います。
DHCPサーバ機能により、IPアドレスなどネットワークに接続するために必要な情報を無線ステーションへ割り当てることができます。

Dynamic Pool Settings (ダイナミックプール設定)

IPアドレスを自動的に無線ステーションへ割り当てるDHCPダイナミックプールの設定を行います。
DHCPアドレスプールは、ネットワークのステーションに割り当てるIPアドレスの範囲を定義します。
無線ステーションは、設定されたリース期間中、利用可能なIPアドレスを割り当てられます。

- 1. [Advanced Settings] > [DHCP Server] > [Dynamic Pool Settings] を選択します。
- 2. 以下の画面で設定を行います。

Dynamic Pool Settings

DHCP Server Control

Function Enable/Disable

Disable

Dynamic Pool Settings

IP Assigned From

192.168.0.20

IP Pool Range(1-254)

235

Subnet Mask

255.255.255.0

Gateway

192.168.0.50

WINS

192.168.0.50

DNS

192.168.0.50

Domain Name

dlink-ap

Lease Time (60 - 31536000 sec)

604800

Save

項目	説明
DHCP Server Control	[Function Enable/Disable]でDHCPサーバ機能を有効または無効にします。 ・ 選択肢: [Enable] (有効) [Disable] (無効)
Dynamic Pool Settings	DHCPサーバ機能を有効にした場合、以下の項目で設定を行います。 ・ IP Assigned From : 割り当てを開始するIPアドレスを入力します。 ・ IP Pool Range (1-254) : 割り当てに使用可能なIPアドレスの数を入力します。[IP Assigned From]で指定したIPアドレスを起点とした範囲となります。 選択可能範囲: 1-254 ・ Subnet Mask : 割り当てるIPアドレスのサブネットマスクを入力します。 ・ Gateway : ゲートウェイIPアドレスを入力します。 ・ WINS : Windows Internet Naming Service (WINS)サーバのアドレスを入力します。 ・ DNS : Domain Name System (DNS)サーバのアドレスを入力します。 ・ Domain Name : ネットワークのドメイン名を入力します。 ・ Lease Time (60-31536000 sec): IPアドレスをリースする期間を入力します。リース期間を超過すると新しいIPアドレスが無線ステーションに割り当てられます。 設定可能範囲: 60-31536000 (秒)

- 3. [Save] をクリックして設定を保存します。

重要

・ Mgmt IPと異なるIPセグメントを指定したDHCPサーバは、Captive Portalで機能しません。

■ Static Pool Settings (スタティックプール設定)

固定のIPアドレスを無線ステーションへ割り当てるスタティックプールの設定を行います。

1. [Advanced Settings] > [DHCP Server] > [Static Pool Settings] を選択します。
2. 以下の画面で設定を行います。

項目	説明
DHCP Server Control	[Function Enable/Disable]でDHCPサーバ機能を有効または無効にします。 ・ 選択肢: [Enable] (有効) [Disable] (無効)
Static Pool Setting	DHCPサーバ機能を有効にした場合、以下の項目で設定を行います。 ・ Host Name : ホスト名を入力します。 ・ Assigned IP : 割り当てるIPアドレスを入力します。 ・ Assigned MAC Address : IPアドレスを割り当てる無線ステーションのMACアドレスを入力します。 ・ Subnet Mask : サブネットマスクを入力します。 ・ Gateway : ゲートウェイIPアドレスを入力します。 ・ WINS : Windows Internet Naming Service (WINS)サーバのアドレスを入力します。 ・ DNS : Domain Name System (DNS)サーバのアドレスを入力します。 ・ Domain Name : ネットワークのドメイン名を入力します。 スタティックプールリストで割り当てられるIPアドレスは、ダイナミックプールと同じIP範囲内とすることはできません。

3. [Save] をクリックして設定を保存します。

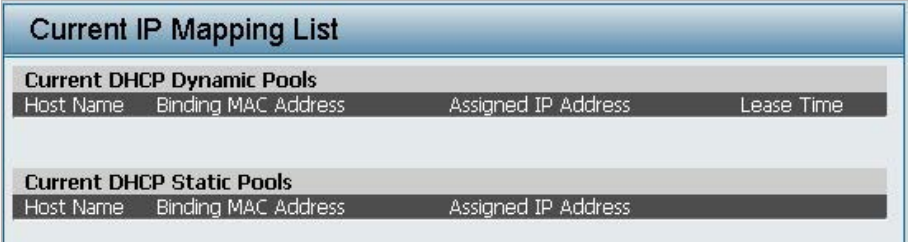
- ◆ エントリを削除する場合：
 1. [Delete] 欄の  アイコンをクリックします。
 2. 確認メッセージが表示されるので、「OK」をクリックします。

- ◆ エントリを編集する場合：
 1. [Edit] 欄の  アイコンをクリックします。
 2. 設定を編集します。
 3. [Save] をクリックして設定を保存します。

■ Current IP Mapping List (IPマッピングリスト)

ダイナミックプール設定・スタティックプール設定によって割り当てられたIPアドレスのリストを表示します。

1. [Advanced Settings] > [DHCP Server] > [Current IP Mapping] を選択します。
2. 以下の画面で IP アドレスのリストを確認します。



項目	説明
Current DHCP Dynamic Pools	ダイナミックプールで割り当てたIPアドレスのリストが表示されます。 • Host Name : ホスト名が表示されます。 • Binding MAC Address : IPアドレスを使用している無線ステーションのMACアドレスが表示されます。 • Assigned IP Address : 割り当てたIPアドレスが表示されます。 • Lease Time : IPアドレスのリース期間が表示されます。
Current DHCP Static Pools	スタティックプールで割り当てたIPアドレスのリストが表示されます。 • Host Name : ホスト名が表示されます。 • Binding MAC Address : IPアドレスを使用している無線ステーションのMACアドレスが表示されます。 • Assigned IP Address : 割り当てたIPアドレスが表示されます。

Filters (フィルタ)

■ Wireless MAC ACL Settings (ワイヤレスMAC ACL)

MACアドレスによるフィルタリングを行います。

メモ

MAC ACLはRadio単位で最大512までです。

1. [Advanced Settings] > [Filters] > [Wireless MAC ACL] を選択します。
2. 以下の画面で設定を行います。

Wireless MAC ACL Settings

Wireless Band: 2.4GHz ▼ **Total : 512 Used : 0**

Access Control List: Disable ▼

SSID Index: Primary SSID ▼

MAC Address: [] : [] : [] : [] : [] : [] **Add**

ID	MAC Address	Delete

Current Client Information

MAC Address	SSID	Band	Authentication	Signal	Add

Upload ACL File

Upload File : **ファイルを選択** 選択されていません **Upload**

Download ACL File

Load ACL File to Local Hard Driver : **Download**

Save

項目	説明
Wireless Band	周波数帯を[2.4GHz] または [5GHz] から選択します。
Access Control List	ACL (Access Control List) の設定を無効/許可/拒否のいずれかに設定します。 • Disable : アクセスコントロールリストは無効となります。 • Accept : アクセスコントロールリストに登録されているMAC アドレスを持つデバイスのみ接続を許可します。 • Reject : アクセスコントロールリストに登録されているMAC アドレスを持つデバイスとの接続を拒否します。
SSID Index	SSIDを選択します。

項目	説明
MAC Address	以下の手順でMACアドレスを登録します。 1. MACアドレスを入力します。 2. [Add]をクリックします。 追加したMACアドレスを削除する場合は[Delete]欄の  アイコンをクリックします。
Current Client Information	本製品に接続しているクライアントの情報が表示されます。 [Add]にチェックを入れると、クライアントはアクセスコントロールリストに追加されます。
Upload ACL File	以下の手順でアクセスコントロールリストのファイルをアップロードします。 1. [ファイルを選択]をクリックしてファイルを選択します。 2. [Upload]をクリックしてファイルをアップロードします。
Download ACL File	[Download]をクリックして、アクセスコントロールリストのファイルをダウンロードします。

メモ

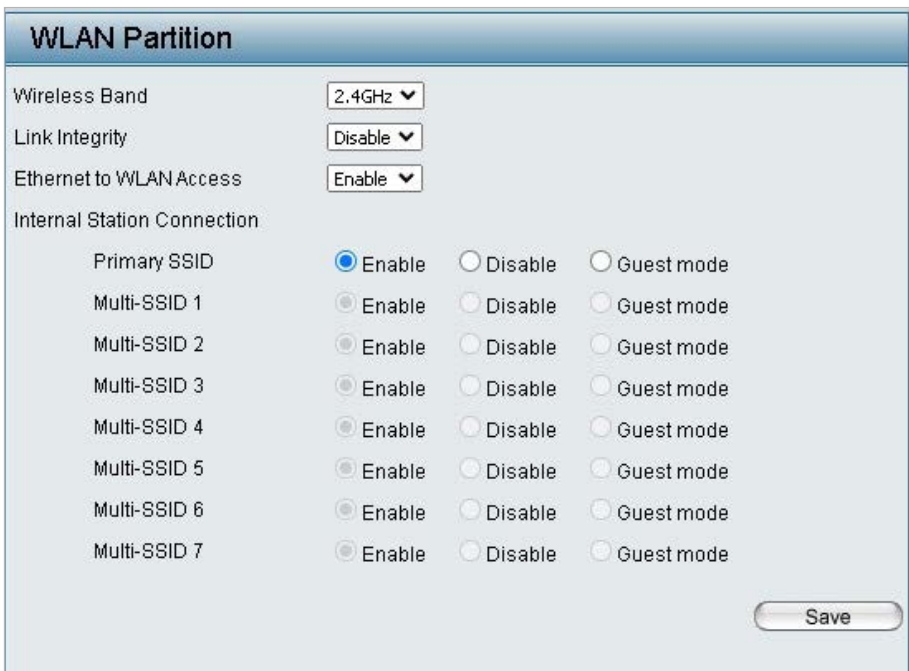
CLIからアクセスコントロールリストのファイルをアップロードする場合、ファイルに小文字は使用できません。

3. [Save] をクリックして設定を保存します。

■ WLAN Partition (WLANパーティション)

WLANパーティションの設定を行います。

1. [Advanced Settings] > [Filters] > [WLAN Partition] を選択します。
2. 以下の画面で設定を行います。



項目	説明
Wireless Band	周波数帯を[2.4GHz]または[5GHz]から選択します。
Link Integrity	Link Integrity機能を有効または無効にします。 ・ 選択肢:[Enable] (有効) [Disable] (無効) Link Integrityは、複数の無線LANアクセスポイントを運用している場合に、発生したネットワーク障害を回避するための機能です。 LANとアクセスポイントが切断されると、ワイヤレスクライアントは自動的にそのアクセスポイントから切断されます。

項目	説明
Ethernet to WLAN Access	有線LANから無線LANへのデータ送信を有効または無効にします。 - 選択肢: [Enable] (有効) [Disable] (無効) - 初期値: [Enable]
Internal Station Connection	SSIDごとにステーションとの通信モードを設定します。 • Enable : 同じSSIDに接続しているワイヤレスクライアント間での通信、および異なるSSIDに接続しているワイヤレスクライアント間での通信が可能です。 • Disable : 同じSSIDに接続しているワイヤレスクライアント間での通信はできません。 異なるSSIDに接続しているワイヤレスクライアント間での通信は可能です。 • Guest mode : 同じSSIDに接続しているワイヤレスクライアント間での通信、および異なるSSIDに接続しているワイヤレスクライアント間での通信ができません。

3. [Save] をクリックして設定を保存します。

メモ

WLAN Partitionは、上位でVLAN間ルーティングされる構成では無効です。

■ IP Filter Settings (IPフィルタ)

IPアドレス (192.168.70.66など) やネットワークアドレス (192.168.70.0など) を使用してフィルタリングを行います。
設定したアドレスはネットワークへのアクセスが無効になります。

1. [Advanced Settings] > [Filters] > [IP Filter Settings] を選択します。
2. 以下の画面で設定を行います。

項目	説明
Wireless Band	周波数帯を[2.4GHz]または[5GHz]に設定します。
SSID Index	SSIDを選択します。

項目	説明
Filter State	フィルタを有効または無効にします。 ・ 選択肢: [Enable] (有効) [Disable] (無効)
IP Address	IPアドレスまたはネットワークアドレスを入力します。
Subnet Mask	IPアドレスまたはネットワークアドレスのサブネットマスクを入力します。
Upload IP Filter File	IPフィルタリストのファイルをアップロードします。 [ファイルを選択]をクリックして、IPフィルタリストのファイルを選択し[Upload]をクリックします。
Download IP Filter File	IPフィルタリストのファイルをダウンロードします。 [Download]をクリックします。

◆ エントリを追加する場合：

1. [Wireless Band] [SSID Index] で IP フィルタを追加する周波数帯、SSID を選択します。
2. [Filter State] を [Enable] に設定します。
3. [IP Address] と [Subnet Mask] を入力し、[Add] をクリックします。

◆ エントリを削除する場合：

1. [SSID Index] で対象の SSID を選択します。
2. [Delete] 欄の  アイコンをクリックします。
3. 確認メッセージが表示されるので、「OK」をクリックします。

3. [Save] をクリックして設定を保存します。

メモ

IP Filterは、Wireless -> LAN方向の宛先ポート53の UDP、TCP、および宛先ポート67を除く、IPv4の UDP、TCPをフィルタします。

Traffic Control (トラフィックコントロール)

アップリンク/ダウンリンクの帯域幅設定、QoS設定などによりトラフィックをコントロールします。

■ Uplink and Downlink Setting (アップリンク/ダウンリンク設定)

アップリンク/ダウンリンクの帯域幅を設定します。

本項目で設定した内容は、QoS及びTraffic Managerの設定内容にも反映されます。

1. [Advanced Settings] > [Traffic Control] > [Uplink/Downlink Settings] を選択します。
2. 以下の画面で設定を行います。

項目	説明
Ethernet	[Downlink]または[Uplink]を選択します。
2.4GHz / 5GHz	周波数帯を[2.4GHz]または[5GHz]から選択します。
Downlink Interface	ダウンリンクインタフェースを選択します。
Uplink Interface	アップリンクインタフェースを選択します。
Downlink Bandwidth (1-2400)	ダウンリンクの帯域幅を入力します。 ・ 指定可能範囲：1-2400 (Mbps)
Uplink Bandwidth (1-2400)	アップリンクの帯域幅を入力します。 ・ 指定可能範囲：1-2400 (Mbps)

3. [Save] をクリックして設定を保存します。

■QoS (QoS設定)

本項目ではQoSの設定を行います。
QoS (Quality of Service) とは、各アプリケーションのトラフィックに優先順位を付けることで、ネットワークの利用を効率化する機能です。優先度を高く設定されたトラフィックが優先的に処理されます。

重要

QoS機能が有効化される場合、Bandwidth Optimization (帯域幅最適化) は無効となります。

- 1. [Advanced Settings] > [Traffic Control] > [QoS] を選択します。
- 2. 以下の画面で設定を行います。

QoS

Enable QoS☐

Advanced QoS

Downlink Bandwidth

100

Mbits/sec

Uplink Bandwidth

100

Mbits/sec

ACK/DHCP/ICMP/DNS Priority

Highest Priority

Limit

100

% Port

53,67,68,546,547

Mail Traffic Priority

Second Priority

Limit

100

% Port

25,110,465,995

Web Traffic Priority

Third Priority

Limit

100

% Port

80,443,3128,8080

Ftp Traffic Priority

Low Priority

Limit

100

% Port

20,21

User Defined-1 Priority

Highest Priority

Limit

100

% Port

0

-

0

User Defined-2 Priority

Second Priority

Limit

100

% Port

0

-

0

User Defined-3 Priority

Third Priority

Limit

100

% Port

0

-

0

User Defined-4 Priority

Low Priority

Limit

100

% Port

0

-

0

Other Traffic Priority

Low Priority

Limit

100

%

Save

項目	説明
Enable QoS	チェックを入れてQoSを有効にします。
Advanced QoS	QoSの詳細設定を行います。 • Downlink Bandwidth : [Uplink and Downlink Setting]で設定した帯域幅が表示されます。 →『Uplink and Downlink Setting (アップリンク/ダウンリンク設定) :p.75』 • Uplink Bandwidth : [Uplink and Downlink Setting]で設定した帯域幅が表示されます。 →『Uplink and Downlink Setting (アップリンク/ダウンリンク設定) :p.75』 • Priority : 各トラフィックの優先度を設定します。 - Highest Priority :最も高い優先度です。 - Second Priority :2番目に高い優先度です。 - Third Priority :3番目に高い優先度です。 - Low Priority :最も低い優先度です。 • Limit : [Downlink/Uplink Bandwidth]の設定値を元に、各トラフィックの最大帯域幅を設定します。 • Port : 対象ポートを指定します。

- 3. [Save] をクリックして設定を保存します。

■ Traffic Manager (トラフィックマネージャ)

トラフィックマネージャは、トラフィック管理ルールを作成し、クライアントのトラフィックとアップリンク／ダウンリンクのスピードを管理する機能です。

1. [Advanced Settings] > [Traffic Control] > [Traffic Manager] を選択します。
2. 以下の画面で設定を行います。

項目	説明
Traffic Manager	トラフィックマネージャを有効または無効にします。 ・選択肢: [Enable] (有効) [Disable] (無効)
Unlisted Clients Traffic	リストに登録されていないクライアントのトラフィックに対する対応を選択します。 ・選択肢: [Deny] (拒否) [Forward] (転送)
Downlink Bandwidth	[Uplink and Downlink Setting]で設定した帯域幅が表示されます。 →『 Uplink and Downlink Setting (アップリンク／ダウンリンク設定) :p.75』
Uplink Bandwidth	[Uplink and Downlink Setting]で設定した帯域幅が表示されます。 →『 Uplink and Downlink Setting (アップリンク／ダウンリンク設定) :p.75』
Add Traffic Manager Rule	トラフィック管理ルールを作成します。 ・Name : ルールの名前を入力します。 ・Client IP (optional) : クライアントのIPアドレスを入力します。 ・Client MAC (optional) : クライアントのMACアドレスを入力します ・Downlink Speed : ダウンリンクの速度を入力します。(単位:Mbits/秒) ・Uplink Speed : アップリンクの速度を入力します。(単位:Mbits/秒) ・Add : 設定した内容を追加します。 ・Clear : 設定した内容を取り消します。
Traffic Manager Rules	作成したトラフィック管理ルールが表示されます。

◆ エントリを削除する場合：

1. [Delete] 欄の  アイコンをクリックします。
2. 確認メッセージが表示されるので、「OK」をクリックします。

- ◆ エントリを編集する場合：
 1. [Edit] 欄の  アイコンをクリックします。
 2. 設定を編集します。
 3. [Add] をクリックして設定を保存します。
- 3. [Save] をクリックして設定を保存します。

Status (ステータス)

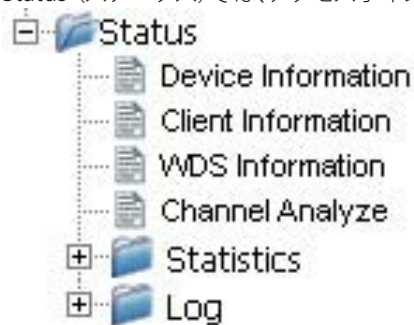
ファームウェアバージョンやクライアント情報、ログなど、アクセスポイントのステータスを確認できます。

6

■ Statusについて	80
■ Device Information (デバイス情報)	80
■ Client Information (クライアント情報)	82
■ WDS Information (WDS情報)	82
■ Channel Analyze (チャネル分析)	83
■ Statistics (統計情報)	84
Ethernet Traffic Statistics (イーサネットトラフィック統計情報)	84
WLAN Traffic Statistics (WLANトラフィック統計情報)	85
■ Log (ログ)	86
View Log (ログの表示)	86
Log Settings (ログ設定)	87

Statusについて

Status (ステータス) では、アクセスポイントのステータスを確認することができます。



Device Information (デバイス情報)

本画面には、ファームウェアバージョン、IPアドレス、MAC アドレス、ワイヤレス設定などの情報と、CPUおよびメモリ使用率に関する情報が表示されます。

1. [Status] > [Device Information] を選択します。
2. 以下の画面で情報を確認します。

Device Information	
Firmware Version:v1.10	
Ethernet MAC Address:	Ti:90:ad:b5:7a:58
Wireless MAC Address(2.4GHz):	Primary: Ti:90:ad:b5:7a:58 SSID 1~7: Ti:90:ad:b5:7a:58 ~ Ti:90:ad:b5:7a:58
Wireless MAC Address(5GHz):	Primary: Ti:90:ad:b5:7a:58 SSID 1~7: Ti:90:ad:b5:7a:58 ~ Ti:90:ad:b5:7a:58
Ethernet	
IP Address	172.16.1.33
Subnet Mask	255.255.255.0
Gateway	172.16.1.1
DNS	172.16.1.5 172.16.1.6
Wireless (2.4GHz)	
Network Name (SSID)	dlink
Channel	11
Data Rate	Auto
Security	None
Wireless (5GHz)	
Network Name (SSID)	dlink
Channel	140
Data Rate	Auto
Security	None
Device Status	
CPU Utilization	2%
Memory Utilization	30%
Nuclias Connect	
Connection Status	Disconnect
Server IP/PORT	
Group ID	

項目	説明
Ethernet MAC Address	イーサネットMACアドレスが表示されます。
Wireless MAC Address (2.4GHz)	2.4GHz無線MACアドレスが表示されます。
Wireless MAC Address (5GHz)	5GHz無線MACアドレスが表示されます。
Ethernet	
IP Address	割り当てられたIPアドレスが表示されます。
Subnet Mask	割り当てられたサブネットマスクが表示されます。
Gateway	割り当てられたゲートウェイが表示されます。
DNS	割り当てられたDNSが表示されます。
Wireless (2.4GHz)	
Network Name (SSID)	2.4GHzネットワークのSSIDが表示されます。
Channel	2.4GHzネットワークのチャンネルが表示されます。
Data Rate	2.4GHzネットワークのデータレートが表示されます。
Security	2.4GHzネットワークのセキュリティが表示されます。
Wireless (5GHz)	
Network Name (SSID)	5GHzネットワークのSSIDが表示されます。
Channel	5GHzネットワークのチャンネルが表示されます。
Data Rate	5GHzネットワークのデータレートが表示されます。
Security	5GHzネットワークのセキュリティが表示されます。
Device Status	
CPU Utilization	現在のCPU使用率が表示されます。
Memory Utilization	現在のメモリ使用率が表示されます。
Nuclias Connect	
Connection Status	現在の接続ステータスが表示されます。
Server IP/PORT	現在のサーバIPおよびポートが表示されます。
Group ID	現在のグループIDが表示されます。

Client Information (クライアント情報)

本製品に接続しているクライアントの情報が、帯域ごとに表示されます。

1. [Status] > [Client Information] を選択します。
2. 以下の画面で情報を確認します。

Client Information							
Client Information		Station association (2.4GHz) : 0					
SSID	MAC	Band	Authentication	RSSI	Power Saving Mode	System Info	
Client Information		Station association(5GHz) : 0					
SSID	MAC	Band	Authentication	RSSI	Power Saving Mode	System Info	

項目	説明
SSID	クライアントのSSIDが表示されます。
MAC	クライアントのMACアドレスが表示されます。
Band	クライアントが接続している無線帯域が表示されます。
Authentication	使用している認証方式が表示されます。
RSSI	クライアントの受信信号強度 (RSSI) が表示されます。
Power Saving Mode	省電力モードの状態が表示されます。
System Info	クライアントのシステム情報が表示されます。

WDS Information (WDS情報)

本製品に現在接続しているクライアントのWDS (アクセスポイント間接続) 情報を表示します。

1. [Status] > [WDS Information] を選択します。
2. 以下の画面で情報を確認します。

WDS Information					
WDS Information		Channel : (2.407 GHz)			
Name	MAC	Authentication		Signal	Status
WDS Information		Channel : (5 GHz)			
Name	MAC	Authentication		Signal	Status

項目	説明
Name	クライアントのSSIDが表示されます。
MAC	クライアントのMACアドレスが表示されます。
Authentication	クライアントが使用している認証方式が表示されます。
Signal	クライアントの信号強度が表示されます。
Status	WDS接続の状態が表示されます。

Channel Analyze (チャネル分析)

アクセスポイントのチャネル分析を行います。

⚠注意

DFS帯のチャネルを利用中にこの機能を実行する場合は、無線機能が一時停止しますので、使用する場合は十分に注意してください。

- 1. [Status] > [Channel Analyze] を選択します。
- 2. [Detect] をクリックして検知を行い、以下の画面で情報を確認します。

Channel Analyze

Wireless Band

2.4GHz

Detect

Wireless Summary

AP List

CH	AP Num	Total Rssi	Total Load	Noise Floor	Evaluation
1	54	3321	98	-70	BAD
6	21	2049	97	-66	BAD
11	30	2708	99	-94	BEST

* There are only three non-overlapped channels in 2.4G band, respectively 1,6 and 11.

項目	説明
Wireless Band	周波数帯を[2.4GHz]または[5GHz]から選択します。
Detect	チャネルの検知を行います。
Wireless Summary	チャネルの分析結果が表示されます。

Statistics（統計情報）

■Ethernet Traffic Statistics（イーサネットトラフィック統計情報）

有線ネットワークで送受信されたパケットの統計情報を表示します。

- 1. [Status] > [Statistics] > [Ethernet] を選択します。
- 2. 以下の画面で情報を確認します。

Ethernet Traffic Statistics			Clear	Refresh
	LAN1	LAN2		
Transmitted Count				
Transmitted Packet Count	0	24054		
Transmitted Bytes Count	0	27125600		
Dropped Packet Count	0	0		
Received Count				
Received Packet Count	0	39960		
Received Bytes Count	0	8350104		
Dropped Packet Count	0	15		

項目	説明
Transmitted Count	
Transmitted Packet Count	送信パケット数が表示されます。
Transmitted Bytes Count	送信バイト数が表示されます。
Dropped Packet Count	破棄されたパケット数が表示されます。
Received Count	
Received Packet Count	受信パケット数が表示されます。
Received Bytes Count	受信バイト数が表示されます。
Dropped Packet Count	破棄されたパケット数が表示されます。

- ◆ 統計情報のカウンタをクリアする場合：
 - 1. [Clear] をクリックします。
- ◆ 統計情報を更新する場合：
 - 1. [Refresh] をクリックします。

■ WLAN Traffic Statistics (WLANトラフィック統計情報)

無線ネットワークの送受信フレームおよびフレームエラーの統計情報を表示します。

1. [Status] > [Statistics] > [WLAN] を選択します。
2. 以下の画面で情報を確認します。

WLAN Traffic Statistics			Clear	Refresh
	2.4GHz	5GHz		
Transmitted Count				
Transmitted Packet Count	1146	5004		
Transmitted Bytes Count	142460	4666274		
Dropped Packet Count	0	0		
Transmitted Retry Count	0	0		
Received Count				
Received Packet Count	261	2609		
Received Bytes Count	18620	306020		
Dropped Packet Count	0	0		
Received CRC Count	0	0		
Received Decryption Error Count	0	0		
Received MIC Error Count	0	0		
Received PHY Error Count	0	0		

項目	説明
Transmitted Count	
Transmitted Packet Count	送信パケット数が表示されます。
Transmitted Bytes Count	送信バイト数が表示されます。
Dropped Packet Count	破棄されたパケット数が表示されます。
Transmitted Retry Count	送信リトライ回数が表示されます。
Received Count	
Received Packet Count	受信パケット数が表示されます。
Received Bytes Count	受信バイト数が表示されます。
Dropped Packet Count	破棄されたパケット数が表示されます。
Received CRC Count	受信したCRC数が表示されます。
Received Decryption Error Count	受信した復号エラー数が表示されます。
Received MIC Error Count	受信したMICエラー数が表示されます。
Received PHY Error Count	受信したPHYエラー数が表示されます。

- ◆ 統計情報のカウンタをクリアする場合：

1. [Clear] をクリックします。

- ◆ 統計情報を更新する場合：

1. [Refresh] をクリックします。

Log (ログ)

■View Log (ログの表示)

アクセスポイントの動作や無線LANクライアントとの接続記録などのログを表示します。

重要

保存できるログの数は500個までです。

- 1. [Status] > [Log] > [View Log] を選択します。
- 2. 以下の画面で情報を確認します。

View Log

First Page

Last Page

Previous

Next

Clear

Page 1 of 4

Time	Priority	Message
Jan 1 03:52:54	[SYSACT]	Web login success from 172.16.1.68
Jan 1 03:52:00	[SYSACT]	Web logout from 172.16.1.68
Jan 1 03:47:38	[Wireless]	5G:Deauth:STA 38:78:62:C5:4E:6D(reason 34)
Jan 1 03:45:02	[Wireless]	External DHCP Server assign IP 172.16.1.40 TO Mac :b6:18:ac:18:ce:b0
Jan 1 03:43:08	[Wireless]	External DHCP Server assign IP 172.16.1.42 TO Mac :38:78:62:c5:4e:6d
Jan 1 03:43:08	[Wireless]	5G:Association Success:STA 38:78:62:C5:4E:6D
Jan 1 03:36:37	[SYSACT]	Web login success from 172.16.1.68
Jan 1 03:34:44	[SYSACT]	Web logout from 172.16.1.68
Jan 1 03:31:36	[SYSACT]	Web login success from 172.16.1.68

項目	説明
First Page Last Page	最初のページ／最後のページを表示します。
Previous Next	前のページ／次のページを表示します。
Clear	ログを削除します。

■ Log Settings (ログ設定)

ログ取得に関する設定を行います。

1. [Status] > [Log] > [Log Settings] を選択します。
2. 以下の画面で設定を行います。

Log Settings

Log Settings

Log Server Settings

Log Server / IP Address

Log Type ☒ System Activity
☒ Wireless Activity
☒ Notice

EU directive Syslog Server Settings

Log Server / IP Address

Email Notification

Email Notification ☐ Enable

Outgoing mail server (SMTP)

Authentication ☐ Enable

SSL/TLS ☐ Enable

From Email Address

To Email Address

Email Server Address

SMTP Port

User Name

Password

Confirm Password

Email Log Schedule

Schedule hours or when Log is full

Save

項目	説明
Log Settings	ログを送信するサーバと送信するログのタイプを設定します。 • Log Server / IP Address : ログを送信するサーバのIP アドレスを入力します。 • Log Type : 送信するログのタイプを選択します。 - [System Activity] : 本アクセスポイントのアクティビティに関するログを取得します。 - [Wireless Activity] : 無線LAN クライアントの接続情報などのログを取得します。 - [Notice] : その他の情報のログを取得します。
EU directive Syslog Server Settings	日本では使用しません。

項目	説明
Email Notification	ログのE-Mail通知を設定します。 • Email Notification : チェックを入れるとE-Mail通知が有効になります。 • Outgoing mail server (SMTP) : 送信用のSMTP サーバを以下から選択します。 - [Internal] [Gmail] [Hotmail] • Authentication : チェックを入れると認証が有効になります。 • SSL/TLS : チェックを入れるとSSL/TLS 認証が有効になります。 • From Email Address : E-mail/SMTP 送信元のE-mail アドレスを入力します。 • To Email Address : E-mail/SMTP 送信先のE-mail アドレスを入力します。 • Email Server Address : E-mail/SMTP サーバのIP アドレスを入力します。 • SMTP Port : SMTP ポートの番号を入力します。Gmail SMTPポート465はサポートされません。 Gmail SMTPポート25または587に設定してください。 • User Name : SMTP サーバのユーザ名を入力します。 • Password : SMTP サーバのパスワードを入力します。 • Confirm Password : 確認のためにSMTP サーバのパスワードを再度入力します。
Email Log Schedule	ログのE-Mail通知を行う間隔を設定します。(単位:時間)

3. [Save] をクリックして設定を保存します。

メモ

- Cold StartのSyslog Trapは非対応です。
- Syslogの Facility、Levelは変更できません。

管理メニュー

7

ファームウェアアップデートや設定のリセットなど、本製品の管理を行う方法を説明します。

■ 管理メニューについて.....	90
■ Home (ホーム画面)	90
■ Maintenance (メンテナンス)	91
Administration Settings (管理設定)	91
Firmware and SSL Certification Upload (ファームウェアとSSL証明書のアップロード).....	98
Configuration File Upload and Download (コンフィグレーションファイルのアップロードとダウンロード).....	99
Time and Date Settings (時刻と日付の設定)	100
■ Configuration (コンフィグレーション)	101
設定の保存と有効化.....	101
設定の破棄	101
■ System (システム設定)	102
本製品の再起動.....	102
工場出荷時設定へのリセット.....	102
Language Packの削除.....	103
■ Logout (ログアウト)	104
■ Help (ヘルプ)	104

管理メニューについて

ファームウェアアップデートや設定の保存、リセットなどを行うことができます。
管理メニューには以下の項目があります。



- Home
System Information (システム情報) 画面を表示します。
『Home (ホーム画面):p.90』
- Maintenance
管理者設定やファームウェアアップグレードなど、本製品のメンテナンスを行います。
『Maintenance (メンテナンス):p.91』
- Configuration
設定の保存・有効化と、設定変更の取り消しを行います。
『Configuration (コンフィグレーション):p.101』
- System
本製品の再起動と、工場出荷時状態へのリセットを行います。
『System (システム設定):p.102』
- Logout
WebGUI画面からログアウトします。
『Logout (ログアウト):p.104』
- Help
ヘルプ画面を表示します。
『Help (ヘルプ):p.104』

Home (ホーム画面)

System Information (システム情報) 画面を表示します。

1. [Home] アイコンをクリックします。
2. 以下の画面で情報を確認します。

System Information	
Model Name	DAP-X2850
Firmware Version	v1.10 18:39:43 01/10/2022
System Name	dapx2850
Location	
System Time	01/01/2019 04:00:41
Up Time	0 Days, 4:00:57
Operation Mode(2.4GHz)	Access Point
Operation Mode(5GHz)	Access Point
MAC Address(2.4GHz)	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
MAC Address(5GHz)	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
IP Address	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Router Mode	Off

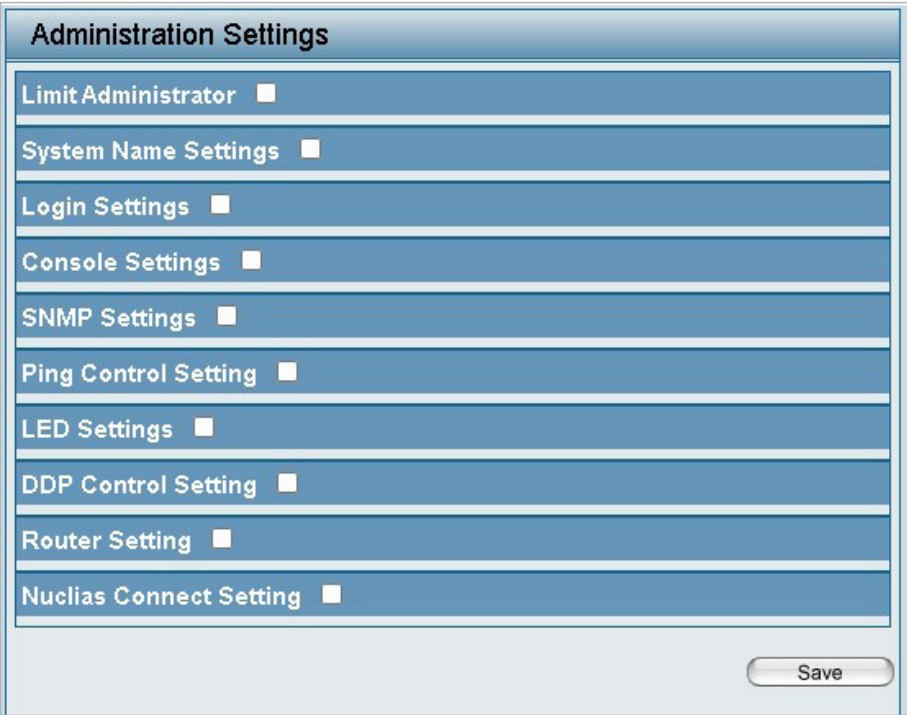
Maintenance（メンテナンス）

■Administration Settings（管理設定）

ログイン設定やコンソール設定など、管理設定を行います。
管理設定には以下の項目があります。

- Limit Administrator (管理者の制限)
→『[Limit Administrator:p.92](#)』を参照
- System Name Settings (システム名設定)
→『[System Name Settings:p.92](#)』を参照
- Login Settings (ログイン設定)
→『[Login Settings:p.93](#)』を参照
- Console Settings (コンソール設定)
→『[Console Settings:p.93](#)』を参照
- Ping Control Setting (Ping管理設定)
→『[Ping Control Setting:p.97](#)』を参照
- LED Settings (LED設定)
→『[LED Settings:p.97](#)』を参照
- DDP Control Setting (DDPコントロール設定)
→『[DDP Control Setting:p.97](#)』を参照
- Nuclias Connect Setting (Nuclias Connect設定)
→『[Nuclias Connect Setting:p.97](#)』を参照

1. [Maintenance] アイコンをクリック → [Administration Settings] を選択します。
2. 以下の画面で項目を選択し、設定を行います。



The image shows a screenshot of the 'Administration Settings' window. It has a title bar with the text 'Administration Settings'. Below the title bar is a list of settings, each with a checkbox to its right. The settings are: Limit Administrator, System Name Settings, Login Settings, Console Settings, SNMP Settings, Ping Control Setting, LED Settings, DDP Control Setting, Router Setting, and Nuclias Connect Setting. At the bottom right of the window is a 'Save' button.

Setting Name	Checkbox
Limit Administrator	☐
System Name Settings	☐
Login Settings	☐
Console Settings	☐
SNMP Settings	☐
Ping Control Setting	☐
LED Settings	☐
DDP Control Setting	☐
Router Setting	☐
Nuclias Connect Setting	☐

Save

● Limit Administrator

管理者の制限を行います。

Limit Administrator

LimitAdministrator VLAN ID

☐ Enable

1

LimitAdministrator IP

☐ Enable

IP Range

From:

To:

Add

Item	From	To	Delete
------	------	----	--------

項目	説明
Limit Administrator VLAN ID	[Enable] にチェックを入れ、管理者がログインを許可されるVLAN ID を入力します。
Limit Administrator IP	[Enable] にチェックを入れ、管理者がログインを許可されるIPアドレスを入力します。
IP Range	[Limit Administrator IP]を有効にした場合、管理者がログインを許可されるIPアドレス範囲を入力します。
Add	設定したIPアドレス範囲を追加します。

- ◆ IP アドレス範囲を削除する場合：
1. [Delete] 欄のアイコンをクリックします。

2. 確認メッセージが表示されるので、「OK」をクリックします。

● System Name Settings

システム名を設定します。

System Name Settings

System Name

dapx2850

Location

MDNS Name

dapx2850

項目	説明
System Name	本製品のシステム名を入力します。 ・初期値:dapx2850
Location	本製品の設置場所を入力します。
MDNS Name	マルチキャストDNS名を入力します。 ・初期値:dapx2850

- Login Settings

Web GUIにログインするためのログイン名とパスワードを設定します。

Login Settings ☒

Login Name

New Password

Confirm Password ☐ Apply New Password

項目	説明
Login Name	ログイン名が表示されます。
New Password	新しいパスワードを入力します。パスワードは大文字と小文字が区別されます。 入力可能文字数:12文字以内
Confirm Password	確認のため、新しいパスワードを再度入力します。
Apply New Password	チェックを入れると新しいパスワードが有効になります。

- Console Settings

コンソールセッションに関する設定を行います。

Console Settings ☒

Status ☒ Enable

Console Protocol ☒ Telnet ☐ SSH

Timeout

項目	説明
Status	[Enable] にチェックを入れ、コンソール接続を有効にします。
Console Protocol	コンソール接続で使用するプロトコルを選択します。 - 初期値: Telnet - 選択肢: [Telnet][SSH]
Timeout	タイムアウトの設定を選択します。(単位: 分) 選択肢: [1 Min][3 Mins][5 Mins][10 Mins][15 Mins][Never]

メモ

- Timeout設定はWebUIには適用されません。WebUIのセッションタイムアウトは3分(固定値)となります。

● SNMP Settings

SNMP設定を行います。

SNMP Settings

Status

☐ Enable

SNMPv2 Settings

Public Community String

public

(0-9,a-z,A-Z,~!@\$%^_+-~!@<>?)

Private Community String

private

(0-9,a-z,A-Z,~!@\$%^_+-~!@<>?)

Trap Status

☐ Enable

Trap Server

(IP Address or Domain Name)

項目	説明
Status	[Enable] にチェックを入れ、SNMPを有効にします。
Public Community String	パブリックSNMP コミュニティ名を入力します。

項目	説明
Private Community String	プライベートSNMP コミュニティ名を入力します。
Trap Status	[Enable] をチェックし、トラップを有効にします。
Trap Server IP	トラップサーバのIP アドレスまたはドメイン名を入力します。

メモ

- CLIからSNMPコミュニティの設定を行った場合、禁止文字を用いた場合でもエラーメッセージが表示されません。
- SNMPv3はCLIからのみ設定できます。
CLIによるSNMPv3設定については『[CLIによるSNMPv3設定例:p.94](#)』を参照してください。

● CLIによるSNMPv3設定例

SNMPv3では、認証と暗号化によるセキュリティ設定と、MIBごとのアクセス制限設定を行なうことができます。
以下の設定例を参考にCLIから設定を行ってください。

1. SNMP を有効にします。

1. 「snmp resume」で SNMP を有効化 → 「set apply」で設定を適用 → 「snmp status」で設定を表示します。

```
WAP-> snmp resume
SNMP Agent Status: Resume.
Please set apply to take effect
WAP-> set apply
WAP-> snmp status
SNMP Agent Status: Active.
```

2. SNMP ビューを追加し、MIB へのアクセス権を設定します。

1. 「snmp addview」を実行します。

【コマンド】

```
snmp addview <ViewName<string> OID<string> Type<1/2>(1:Included/2:Excluded)>
```

【パラメータ説明】

- ViewName<string> : ビュー名を指定します。
- OID<string> : OID (Object Identifier/管理対象のオブジェクト) を指定します。
- Type<1/2>(1:Included/2:Excluded): 指定したOIDを含める (1:Include)、または除外する (2:Excluded) かを設定します。

【コマンド例】

```
snmp addview CommunityView 1 1
```

```
WAP-> snmp addview CommunityView 1 1
The specified view is added!
```

2. 「snmp showview」で SNMP ビューを表示します。

```
WAP-> snmp showview

Vacm View Table Settings
View Name          Subtree          View Type
-----
CommunityView      1              included

Total Entries: 1
```

3. セキュリティレベルを持った SNMP グループを追加します。

1. 「snmp addgroup」を実行します。

【コマンド】

```
snmp addgroup <GroupName<string> Security Level<1/2/3>(1:noauth_nopriv/2:auth_nopriv/3:auth_priv)
ReadView<string>(none:NULL) WriteView<string>(none:NULL) NotifyView<string>(none:NULL) >
```

【パラメータ説明】

- GroupName<string> : グループ名を指定します。
- Security Level<1/2/3>(1:noauth_nopriv/2:auth_nopriv/3:auth_priv) : セキュリティレベルを指定します。
 - ・ 1:noauth_nopriv 認証なし/暗号化なし
 - ・ 2:auth_nopriv 認証あり/暗号化なし
 - ・ 3:auth_priv 認証あり/暗号化あり
- ReadView<string>(none:NULL): このグループのユーザが読み込み可能なMIBオブジェクトの範囲(ビュー)を指定します。
- WriteView<string>(none:NULL): このグループのユーザが書き込み可能なMIBオブジェクトの範囲(ビュー)を指定します。
- NotifyView<string>(none:NULL): このグループのユーザが受け取れる通知MIBオブジェクトの範囲(ビュー)を指定します。

【コマンド例】

```
snmp addgroup D-Link_group 3 CommunityView CommunityView CommunityView
```

```
WAP-> snmp addgroup D-Link_group 3 CommunityView CommunityView CommunityView
```

```
Group has created successfully
```

2. 「snmp showgroup」で SNMP グループを表示します。

```
WAP-> snmp showgroup
```

```
SNMP Group Settings
```

```
Group Name ReadView Name WriteView Name NotifyView Name SNMP Security
```

```
-----
```

Group Name	ReadView Name	WriteView Name	NotifyView Name	SNMP	Security
D-Link_group	CommunityView	CommunityView	CommunityView	v3	priv

```
Total Entries: 1
```

4. リクエストを受け付けるユーザをセキュリティレベルとともに追加します。

1. 「snmp adduser」を実行します。

【コマンド】

```
snmp adduser <UserName<string> GroupName<string> AuthProtocol<1/2/3>(1:none/2:MD5/3:SHA)
```

```
AuthKey<string>(Keys/none) PrivProtocol<1/2>(1:none/2:DES) PrivKey<string>(Keys/none) >
```

【パラメータ説明】

- UserName<string> : ユーザ名を指定します。
- GroupName<string> : グループ名を指定します。
- AuthProtocol<1/2/3>(1:none/2:MD5/3:SHA) : 認証プロトコルを選択します。
 - ・ 1:none 認証を行いません。
 - ・ 2:MD5 MD5による認証を行ないます。
 - ・ 3:SHA SHAによる認証を行ないます。
- AuthKey<string>(Keys/none): 認証のパスワードを設定します。(8-20文字以内)
- PrivProtocol<1/2>(1:none/2:DES): 暗号化プロトコルを指定します。
 - ・ 1:none 暗号化なし。
 - ・ 2:DES DESによる暗号化を行ないます。
- PrivKey<string>(Keys/none): 暗号化のパスワードを設定します。(8-20文字以内)

【コマンド例】

```
snmp adduser dlink D-Link_group 3 12345678 2 87654321
```

```
WAP-> snmp adduser dlink D-Link_group 3 12345678 2 87654321
```

```
Add user successfully!
```


5. 「snmp showuser」で SNMP ユーザの設定と Engine ID を確認します。

1. 「snmp showuser」を実行します。

```
WAP-> snmp showuser

EngineID 0x80001f88808ea7d933f63d2a5c00000000

Username          Group Name      SNMP Version  Auth-Protocol  Priv-Protocol
-----
dlink              D-Link_group   v3            SHA            DES

Total Entries: 1
```

SNMPv3設定例：使用コマンド一覧

コマンド	パラメータ	説明
snmp resume		Suspendされたエージェントを再開します。
set apply		設定を適用します。
snmp status		SNMPステータスを表示します。
snmp addview	ViewName<string> OID<string> Type<1/2>(1:Included/2:Excluded)	SNMPビューを追加します。
snmp showview		SNMPビューを表示します。
snmp addgroup	GroupName<string> Security Level<1/2/3> (1:noauth_nopriv/2:auth_nopriv/3:auth_priv) ReadView<string>(none:NULL) WriteView<string>(none:NULL) NotifyView<string>(none:NULL)	SNMPグループを追加します。
snmp showgroup		SNMPグループを表示します。
snmp adduser	UserName<string> GroupName<string> AuthProtocol<1/2/3>(1:none/2:MD5/3:SHA) AuthKey<string>(Keys/none) PrivProtocol<1/2>(1:none/2:DES) PrivKey<string>(Keys/none)	SNMPユーザを追加します。
snmp showuser		SNMPユーザを表示します。

● Ping Control Setting

Pingを有効または無効にします。

Ping Control Setting ☒	
Status	☒ Enable

項目	説明
Status	[Enable] にチェックを入れ、Pingを有効にします。

● LED Settings

LEDの設定を行います。

LED Settings ☒	
LED Status	☒ On ☐ Off

項目	説明
LED Status	LEDのステータスを設定します。 ・初期値: On ・選択肢: [On] [Off]

● DDP Control Setting

DDPコントロール設定を有効または無効にします。

DDP Control Setting ☒	
Status	☒ Enable

項目	説明
Status	[Enable] にチェックを入れ、DDPコントロール設定を有効にします。

● Router Settings

ルータ設定を行います。

Router Setting ☒	
Router Status	☐ On ☒ Off
WAN Port	☐ LAN(PoE) ☒ LAN

項目	説明
Router Status	ルータをオンまたはオフに設定します。
WAN Port	LAN (PoE) ポートまたはLANポートのいずれかをWANポートに指定します。

● Nuclias Connect Setting

Nuclias Connectを利用するとネットワーク上のAPをまとめて管理することができます。

Nuclias Connect Setting ☒	
Enable Nuclias Connect	Disable ▼

項目	説明
Enable Nuclias Connect	Nuclias Connectを有効化します。 ・初期値: [Disable] ・選択肢: [Disable][Enable]

メモ

- ・本APはNuclias Connectをサポートしていません。将来のファームウェアで対応予定です。
- ・スタンドアロンモードにおいて、「Nuclias Connect Setting」項目を有効化することはできません。Nuclias Connectのプロファイルが適用されると、本項目が有効(管理モード)になります。

6. [Save] をクリックして設定を保存します。

■Firmware and SSL Certification Upload（ファームウェアとSSL証明書のアップロード）

ファームウェア、Language Pack、SSL証明書のアップロードを行います。

●ファームウェアのアップロード

- 1. [Maintenance] アイコンをクリック→ [Firmware and SSL Certification Upload] を選択します。
- 2. 以下の画面で [ファイルを選択] をクリックし、ファームウェアを指定します。

Update Firmware From Local Hard Drive

Firmware Version v1.10

Upload Firmware From File :

ファイルを選択

選択されていません

Upload

Online Check Upgrade Firmware

Check

- 3. [Upload] をクリックします。

⚠注意

アップロード中に電源を切らないでください。
アップデート中に電源を切ると、起動に失敗し、正常に起動できなくなることがあります。故障の原因となりますので、ご注意ください。

●Language Packのアップロード

- 1. [Maintenance] アイコンをクリック→ [Firmware Upload] を選択します。
- 2. 以下の画面で [ファイルを選択] をクリックし、言語パックファイルを選択 します。

Language Pack Upgrade

Upload :

ファイルを選択

選択されていません

Upload

- 3. [Upload] をクリックします。

●SSL証明書のアップロード

- 1. [Maintenance] アイコンをクリック→ [Firmware Upload] を選択します。
- 2. 以下の画面で [ファイルを選択] をクリックし、ファイルを選択 します。

Update SSL Certification From Local Hard Drive

Upload Certificate From File :

ファイルを選択

選択されていません

Upload

Upload Key From File :

ファイルを選択

選択されていません

Upload

項目	説明
Upload Certificate From File	更新する証明書を指定します。
Upload Key From File	更新する認証キーを指定します。

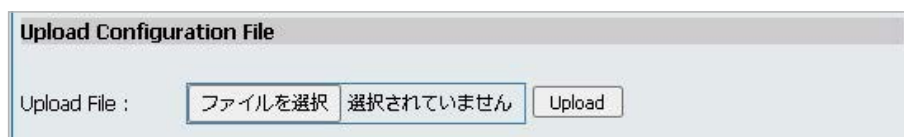
- 3. [Upload] をクリックします。

■ Configuration File Upload and Download (コンフィグレーションファイルのアップロードとダウンロード)

コンフィグレーションファイルのアップロードとダウンロードを行います。アクセスポイントの設定をバックアップまたはリカバリすることができます。

● コンフィグレーションのアップロード

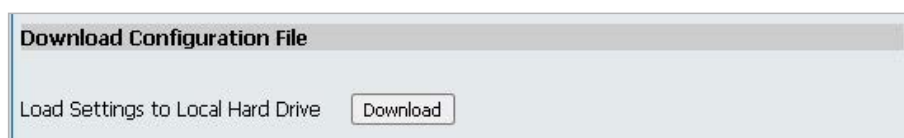
1. [Maintenance] アイコンをクリック→ [Configuration File] を選択します。
2. 以下の画面で [ファイルを選択] をクリックし、ファイルを選択 します。



3. [Upload] をクリックします。
4. 確認メッセージが表示されるので、[OK] をクリックして設定を更新します。

● コンフィグレーションのダウンロード

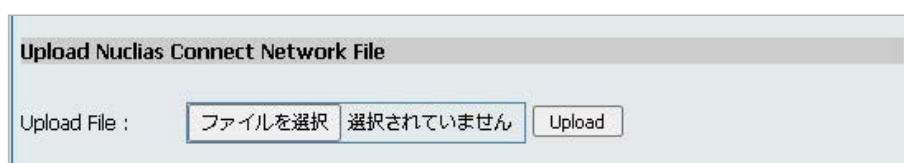
1. [Maintenance] アイコンをクリック→ [Configuration File] を選択します。
2. 以下の画面で [Download] をクリックし、ファイルをダウンロードします。



● Nuclias Connectプロファイルのアップロード

Nuclias Connectでエクスポートしたプロファイルをアップロードすることで、アクセスポイントをNuclias Connectの管理対象として追加することができます。

1. [Maintenance] アイコンをクリック→ [Configuration File] を選択します。
2. 以下の画面で [ファイルを選択] をクリックし、ファイルを選択 します。



3. [Upload] をクリックします。
4. 確認メッセージが表示されるので、[OK] をクリックしてプロファイルを適用します。

メモ

- Nuclias Connectは未サポートです。

■ Time and Date Settings (時刻と日付の設定)

本製品の時刻の設定を行います。

NTPサーバを使用して自動的に日時を設定、または手動で日時を設定することができます。

1. [Maintenance] アイコンをクリック→ [Time and Date] を選択します。
2. 以下の画面で設定を行います。

項目	説明
Time Configuration	[Current Time]に現在設定されている日時が表示されます。
Automatic Time Configuration	NTPサーバを使用して自動的に日時を設定します。 • Enable NTP : チェックを入れるとNTPサーバが有効になります。 • NTP Server : NTPサーバのホスト名またはIPアドレスを入力します。 • Time Zone : タイムゾーンを設定します。
Set the Date and Time Manually	日付と時刻を手動で設定します。 • Date And Time : 日付と時刻を入力します。 • Copy your computer's Time Settings : クリックすると、お使いのPCの日時をコピーできます。
Daylight Configuration	サマータイムを設定します。 • Enable Daylight Saving : チェックを入れ、Daylight Savings Time (DST/サマータイム) を有効化します。 • Daylight Saving Offset : Daylight Savings Time (サマータイム) のオフセット時間 (単位:分) を設定します。 • Daylight Saving Dates : - DST Start : Daylight Savings Time (サマータイム) の開始日時を設定します。 - DST End : Daylight Savings Time (サマータイム) の終了日時を設定します。

3. [Save] をクリックして設定を保存します。

Configuration（コンフィグレーション）

■ 設定の保存と有効化

設定した内容を保存・有効化します。

1. [Configuration] アイコンをクリック→ [Save and Active] を選択します。
2. 以下の画面が表示され、設定の保存と有効化が行われます。



⚠ 注意

再起動中は、電源を切らずにそのままお待ちください。

重要

本作業を行わない場合、各セクションで保存した設定は次のシステム再起動時に破棄されます。

■ 設定の破棄

設定した内容を破棄します。

1. [Configuration] アイコンをクリック→ [Discard Changes] を選択します。
2. 以下の画面が表示され、設定の破棄が行われます。



⚠ 注意

再起動中は、電源を切らずにそのままお待ちください。

System（システム設定）

■本製品の再起動

1. [System] アイコンをクリックします。
2. [Restart] をクリックします。



3. 確認画面が表示されるので、[OK] をクリックします。
4. 以下の画面が表示され、再起動が行われます。



⚠注意

再起動中は、電源を切らずにそのままお待ちください。

■工場出荷時設定へのリセット

工場出荷時の状態へ設定をリセットします。

1. [System] アイコンをクリックします。
2. [Restore] をクリックします。



3. 確認画面が表示されるので、[OK] をクリックします。

- 以下の画面が表示され、工場出荷時設定へのリセットが行われます。



⚠ 注意

再起動中は、電源を切らずにそのままお待ちください。

メモ

工場出荷時状態へのリセットは、本体のリセットボタンを押して行うこともできます。

■ Language Packの削除

現在適用されているLanguage Packを削除します。

- [System] アイコンをクリックします。
- [Clear] をクリックします。

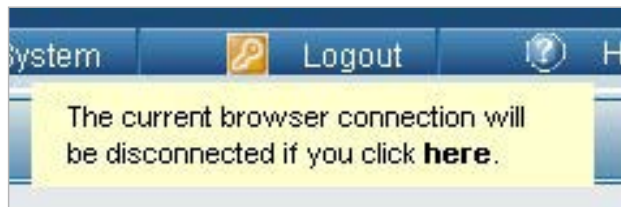


- 確認画面が表示されるので、[OK] をクリックします。

Logout（ログアウト）

Web GUI画面からのログアウトを行います。

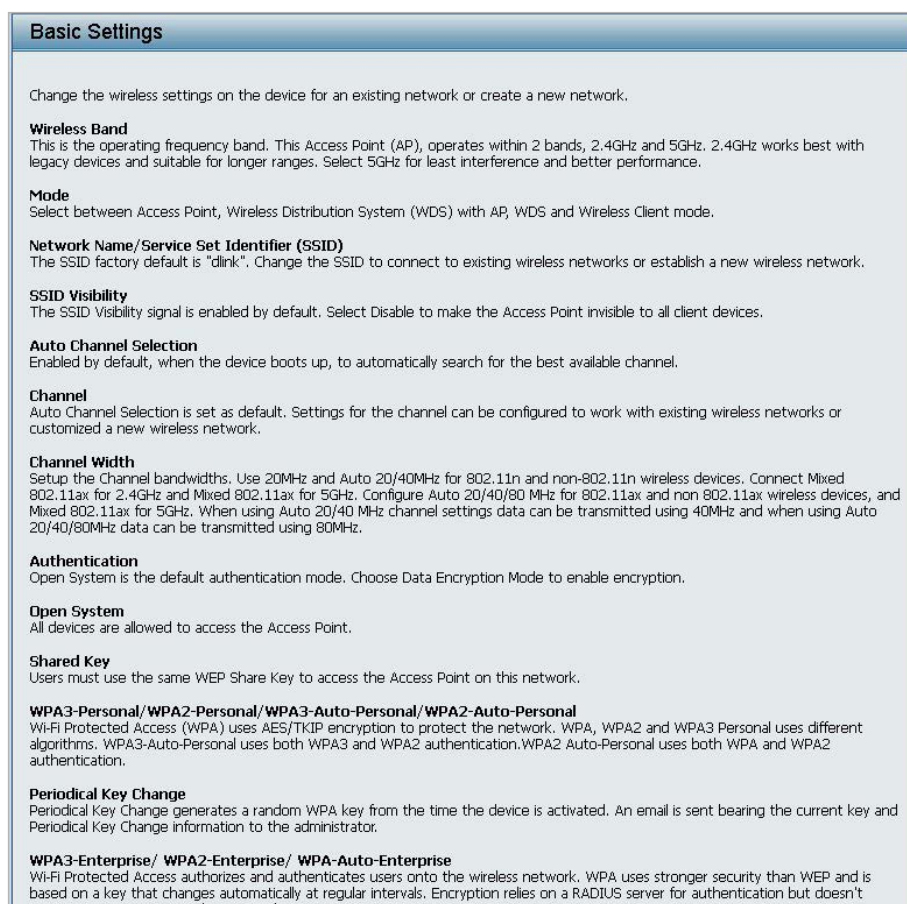
1. [Logout] アイコンをクリックします。
2. 以下のメッセージをクリックします。



Help（ヘルプ）

ヘルプ画面を表示します。

1. [Help] アイコンをクリックします。
2. 以下の画面でヘルプ情報を確認します。



付録

8

■ 工場出荷時設定に戻す	106
リセットボタンで設定リセットを行う	106
Web GUIから設定リセットを行う	106
■ FAQ	107
■ 機能設定例	108
対象機器について	108
VLAN	108

工場出荷時設定に戻す

本製品の設定を工場出荷時の状態に戻す方法について説明します。

重要

- 設定のリセットを行う前に、必要に応じて設定をバックアップしてください。
- リセット後のIPアドレスは「192.168.0.50」になります。

■リセットボタンで設定リセットを行う

1. 本体の電源を入れた状態で、本体背面のリセットボタンを5～10秒間押します。
2. ボタンを離すと、本体が再起動します。そのままお待ちください。

■Web GUIから設定リセットを行う

1. [System] アイコンをクリックします。
2. [Restore] をクリックします。



3. 確認画面が表示されるので、[OK] をクリックします。
4. 以下の画面が表示され、再起動が行われます。



⚠注意

電源を切らずにそのままお待ちください。

FAQ

よくお問い合わせいただく内容について記載しています。

Q 本製品の設定を行うコンピュータからWeb ベースの設定メニューにアクセスできません。

A ①Webブラウザが本製品の対応しているバージョンであるか確認してください。

②本製品前面にあるLAN LED が点灯していることを確認してください。
LED が点灯していない場合は、UTP ケーブルが正しくポートに接続されているか確認してください。

③設定用PC のIP アドレスが本製品と同じアドレス範囲およびサブネット内であるか確認してください。

④コンピュータ上のすべてのインターネットセキュリティソフトウェアの動作を無効にしてください。Zone Alarm、Black Ice、Sygate、Norton Personal ファイアウォール、およびWindows ファイアウォールなどのソフトウェアファイアウォールは設定ページへのアクセスを妨害する可能性があります。

⑤上記の点を確認してもアクセスできない場合は、一度本体の電源を抜いてから約10秒後に再度差し込み、約30秒後にWEBブラウザに再接続してみてください。

Q パスワードを忘れた場合はどうすればよいでしょうか。

A 設定のリセットを行ってください。→『工場出荷時設定に戻す : p.106 』

Q 無線接続が途切れます。対処方法を教えてください。

A ①アクセスポイントの向きを変えてみてください。

②電波の干渉要因となるものから遠ざけてください。2.4GHz 帯デジタルコードレス電話、X10 モジュールなどを使用したホームセキュリティシステム、天井設置型の扇風機、電灯、他の無線製品電波などとの干渉により、通信品質が激しく低下して通信ができなくなる場合があります。
ご使用のルータ、アクセスポイントおよび無線LAN アダプタのチャンネルを変えて、干渉を回避してください。

③本製品は、電子レンジやモニタ、モータなどRFノイズを発生する電気機器から90 ～ 180cm以上離れた場所に設置してください。

機能設定例

本項では、一般によく使う以下の機能について設定例を記載します。実際に設定を行う際の参考にしてください。

- ・『VLAN:p.108』

■対象機器について

本コンフィグレーションサンプルは以下の製品に対して有効な設定となります。

- ・ DAP-X2850

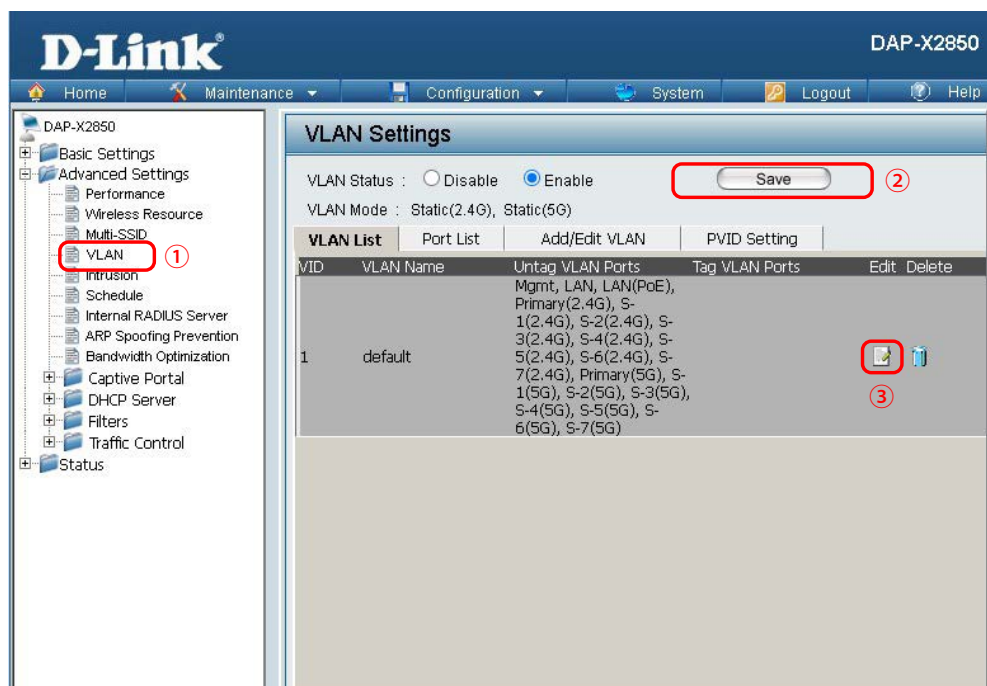
■VLAN

●概要

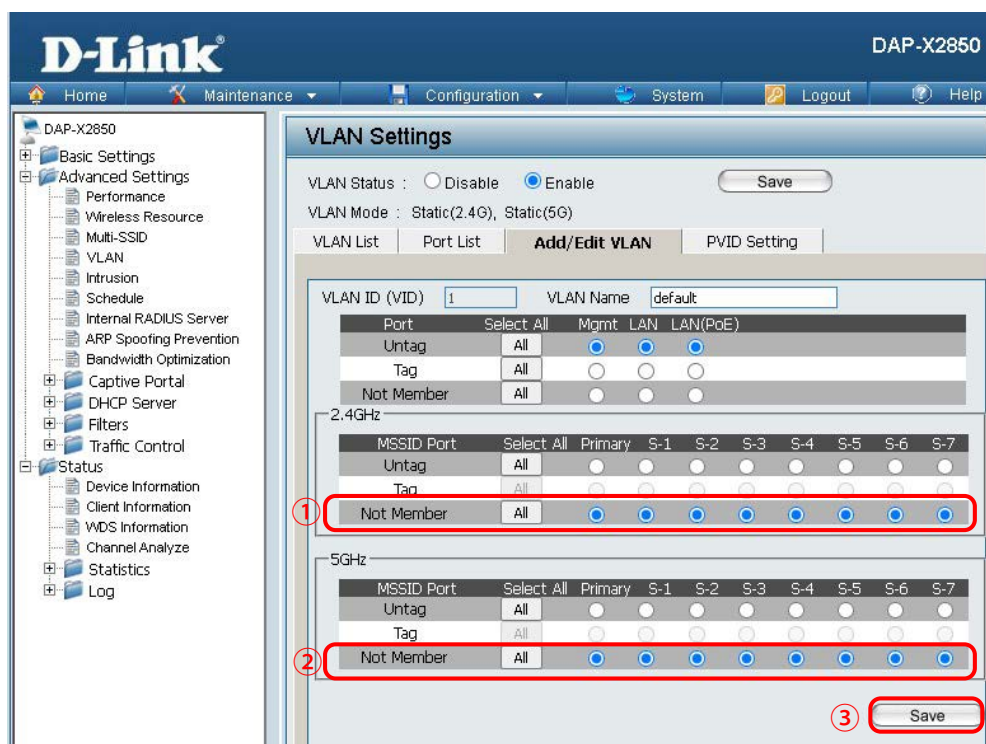
2.4GHz帯のすべてのSSIDに「VLAN10」、5GHz帯のすべてのSSIDに「VLAN20」を「Untag」で設定し、「Management VLAN」に「VLAN1」を「Untag」で設定します。

●設定手順

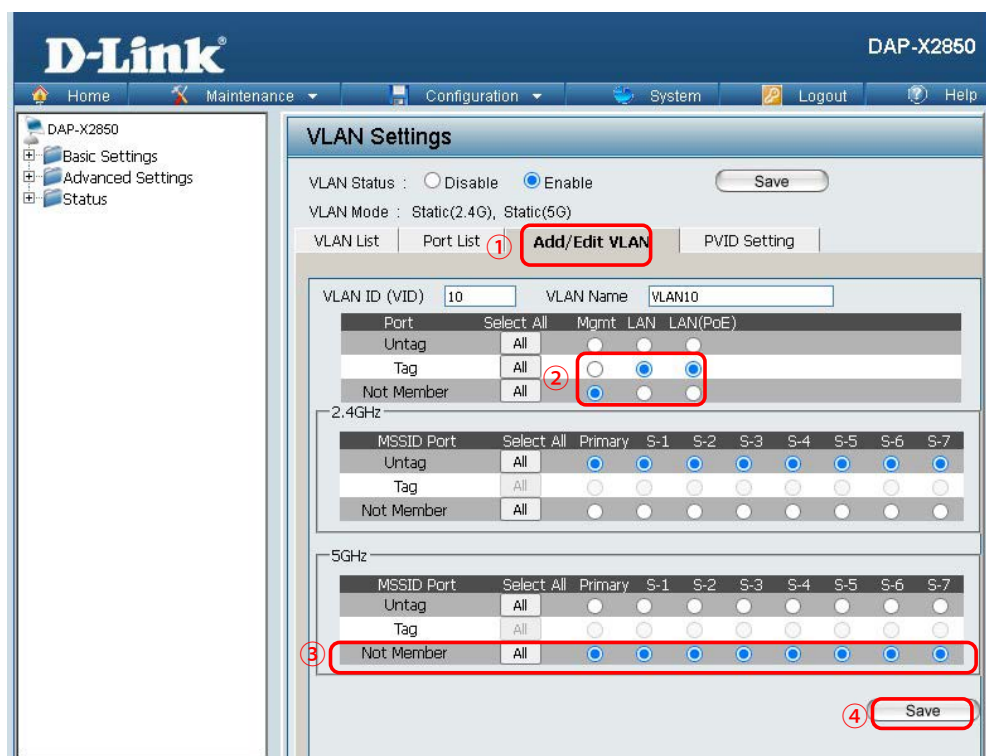
1. Advanced Settings > VLAN をクリックし、「VLAN Settings」を表示します。
2. 「VLAN Status」で「Enable」を選択し「Save」をクリック、次に③の「」をクリックします。



- 「Add/Edit VLAN」タブが表示されます。
- 「VLAN1」(VID1) の全ポートで「Not Member」にチェックを入れて、無線ネットワークから「VLAN1」を削除します。
- 「Save」をクリックします。



- 「Add/Edit VLAN」タブを開き、下図のように「2.4GHz 帯」のすべての SSID に「VLAN10」を「Untag」で設定します。



7. 下図のように「5GHz 帯」のすべての SSID に「VLAN20」を「Untag」で設定します。

D-Link DAP-X2850 VLAN Settings

VLAN Status : ☐ Disable ☒ Enable Save

VLAN Mode : Static(2.4G), Static(5G)

VLAN List | Port List | **Add/Edit VLAN** | PVID Setting

VLAN ID (VID) : 20 | VLAN Name : VLAN20

Port	Select All	Mgmt	LAN	LAN(PoE)
Untag	All	☐	☒	☒
Tag	All	☐	☒	☒
Not Member	All	☒	☐	☐

2.4GHz

MSSID Port	Select All	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
Untag	All	☐	☒	☒	☒	☒	☒	☒	☒
Tag	All	☐	☐	☐	☐	☐	☐	☐	☐
Not Member	All	☒	☒	☒	☒	☒	☒	☒	☒

5GHz

MSSID Port	Select All	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
Untag	All	☒	☒	☒	☒	☒	☒	☒	☒
Tag	All	☐	☐	☐	☐	☐	☐	☐	☐
Not Member	All	☐	☐	☐	☐	☐	☐	☐	☐

Save

8. 「PVID Setting」タブを選択し、各ポートの VID を設定します。

D-Link DAP-X2850 VLAN Settings

VLAN Status : ☐ Disable ☒ Enable Save

VLAN Mode : Static(2.4G), Static(5G)

VLAN List | Port List | Add/Edit VLAN | **PVID Setting**

PVID Auto Assign Status : ☐ Disable ☒ Enable

Port	Mgmt	LAN	LAN(PoE)
PVID	1	1	1

2.4GHz

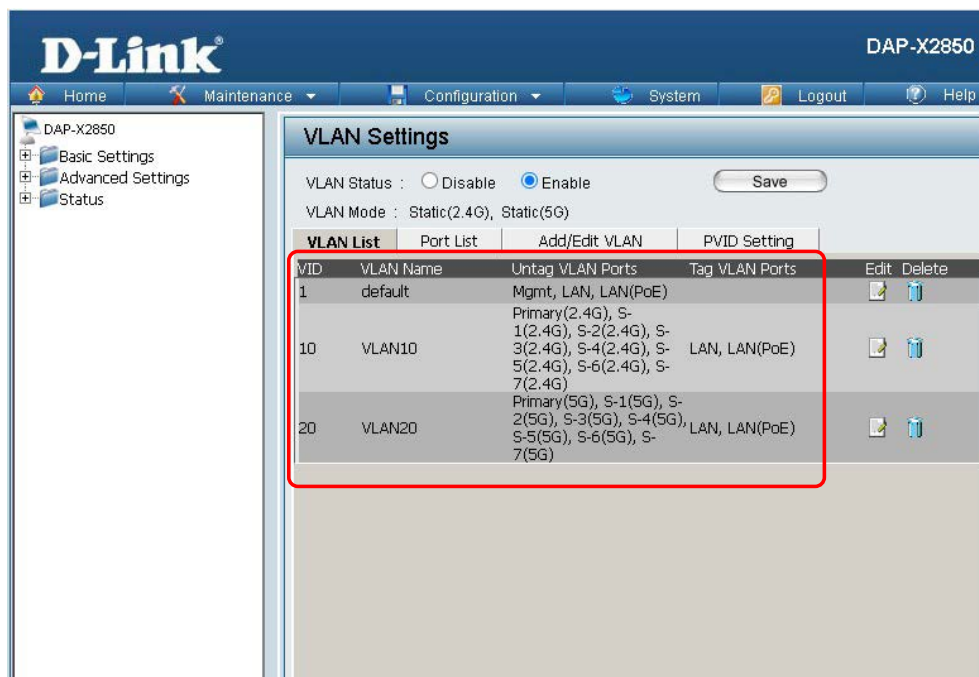
MSSID Port	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
PVID	1	1	1	1	1	1	1	1

5GHz

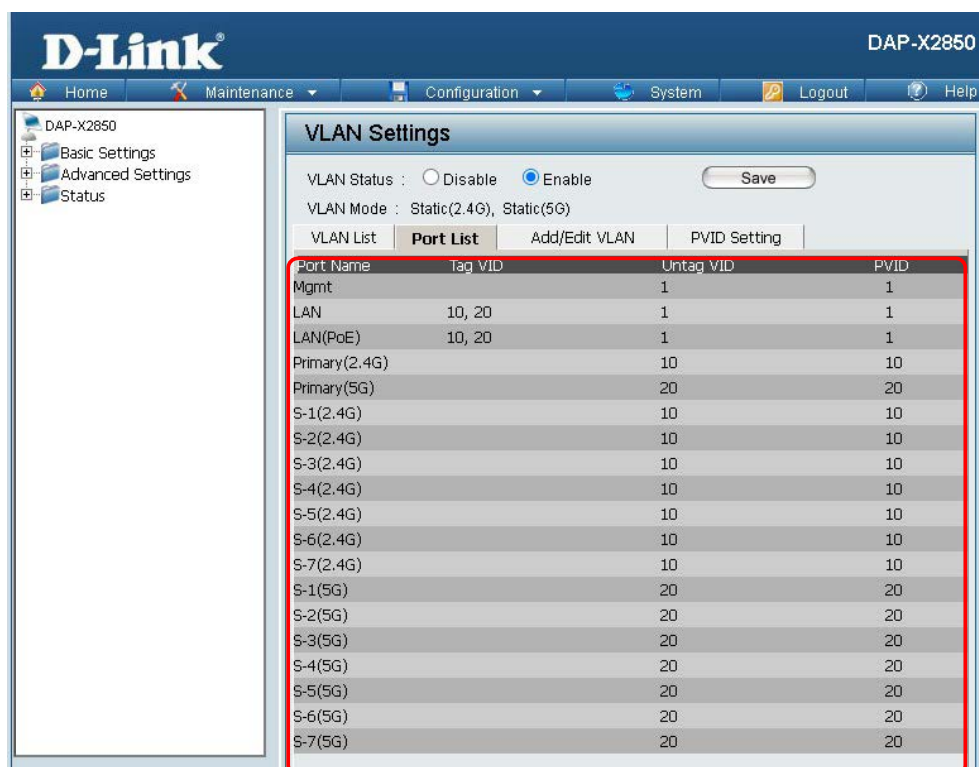
MSSID Port	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
PVID	1	1	1	1	1	1	1	1

Save

9. 「VLAN Settings」の「VLAN List」が下図の状態になっている事を確認します。



10. 「VLAN Settings」の「Port List」が下図の状態になっている事を確認します。



11. Configuration で「Save and Activate」をクリックし、設定内容を保存します。

下図のダイアログが表示され、しばらくの間設定の有効化を行います。
電源を落とさずにお待ちください。

