Cisco WAP581 Wireless-AC/N デュアル無線アクセス ポイント（2.5GbE LAN 対応）

初版：2016 年 11 月 23 日

最終更新：2018 年 7 月 16 日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

http://www.cisco.com/jp

お問い合わせ先：シスコ コンタクトセンター

0120-092-255 （フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

第 1 章 はじめに 1

設定の開始 1

アクセス ポイント セットアップ ウィザードの使用 3

モバイルでのアクセス ポイント セットアップ ウィザードの使用 5

パスワードの変更 7

TCP/UDP サービス 8

システムの状態 9

クイック スタート コンフィギュレーション 10

ウィンドウ ナビゲーション 11

ナビゲーション ペイン 11

管理ボタン 11

第 2 章 システム設定 13

LAN 13

IPv4 設定 13

DHCP 自動コンフィギュレーション設定 14

IPv6 設定 15

ポート設定 16

スパニング ツリー プロトコル 17

VLAN 設定 17

ネイバー探索 18

LLDP 19

IPv6 トンネル 20

時刻 21

NTP を通じた時刻設定の自動取得 21
時刻設定の手動指定 21
通知 22
LED ディスプレイ 22
ログ設定 23
リモート ログ サーバ 24
システム ログを表示する 25
電子メール アラート/メール サーバ/メッセージ構成 25
電子メール アラートの例 27
ユーザ アカウント 28
ユーザの追加 28
ユーザ パスワードの変更 29
管理 29
接続セッションの設定/HTTP/HTTPS サービス タスク 30
SSL 証明書ファイルのステータス 31
SNMP/SNMPv2c の設定 32
SNMPv3 ビュー 33
SNMPv3 グループ 35
SNMPv3 ユーザ 36
SNMPv3 ターゲット 37
セキュリティ 38
Radius サーバ 38
グローバル RADIUS サーバの設定 39
802.1x サプリカント 39
不正 AP 検出 40
不正 AP リストの表示 41
信頼 AP リストの保存 42
信頼できる AP リストのインポート 43
パスワード複雑性の設定 43
WAP-PSK 複雑性の設定 44

第 3 章 ワイヤレス 47
無線 47
ネットワーク 54
VAP の設定 54
セキュリティの設定 57
クライアント フィルタ 63
クライアント フィルタ リストを WAP デバイスにローカルで設定する 63
RADIUS サーバ上での MAC 認証の設定 64
スケジューラ 65
スケジューラ プロファイル構成 65
プロファイル ルール構成 65
QoS 66
第 4 章 ワイヤレス ブリッジ 69
ワイヤレス ブリッジ 69
WDS ブリッジの設定 70
WDS リンク上の WEP 71
WDS リンク上の WPA/PSK 71
ワークグループ ブリッジ 72
第 5 章 高速ローミング 77
高速ローミング 77
高速ローミングの設定 78
リモート キー ホルダー リスト プロファイルの設定 79
第 6 章 シングル ポイント設定 81
ACL 81
IPv4 と IPv6 の ACL 81
ACL を設定するためのワークフロー 82
IPv4 ACL の設定 82

IPv6 ACL の設定 85
MAC ACL の設定 88
クライアント QoS 90
IPv4 トラフィック クラスの設定 90
IPv6 トラフィック クラスの設定 93
MAC トラフィック クラスの設定 95
Qos ポリシー 97
QoS アソシエーション 98
ゲスト アクセス 98
ゲスト アクセス インスタンス テーブル 99
ゲスト グループ テーブル 101
ゲスト ユーザ アカウント 102
Web ポータルのカスタマイズ 103

第 7 章 アクセスコントロール 107
ACL 107
IPv4 と IPv6 の ACL 107
ACL を設定するためのワークフロー 108
IPv4 ACL の設定 108
IPv6 ACL の設定 111
MAC ACL の設定 114
クライアント QoS 116
IPv4 トラフィック クラスの設定 116
IPv6 トラフィック クラスの設定 119
MAC トラフィック クラスの設定 121
Qos ポリシー 123
QoS アソシエーション 124
ゲスト アクセス 124
ゲスト アクセス インスタンス テーブル 125
ゲスト グループ テーブル 127
ゲスト ユーザ アカウント 128

Web ポータルのカスタマイズ 129

第 8 章 Umbrella 133

Cisco Umbrella 133

第 9 章 モニタ 135

ダッシュボード 135

LAN ステータス 137

ワイヤレス ステータス 137

トラフィック統計 138

シングル ポイント設定 139

クライアント 140

ゲスト 142

第 10 章 管理 145

ファームウェア 145

ファームウェア イメージの切り替え 145

HTTP/HTTPS のアップグレード 146

TFTP アップグレード 146

コンフィギュレーション ファイル 147

バックアップ コンフィギュレーション ファイル 148

コンフィギュレーション ファイルのダウンロード 149

コンフィギュレーション ファイルのコピー 149

コンフィギュレーション ファイルのクリア 150

リブート 150

リブートのスケジュール 151

第 11 章 トラブルシュート 153

スペクトル インテリジェンス 153

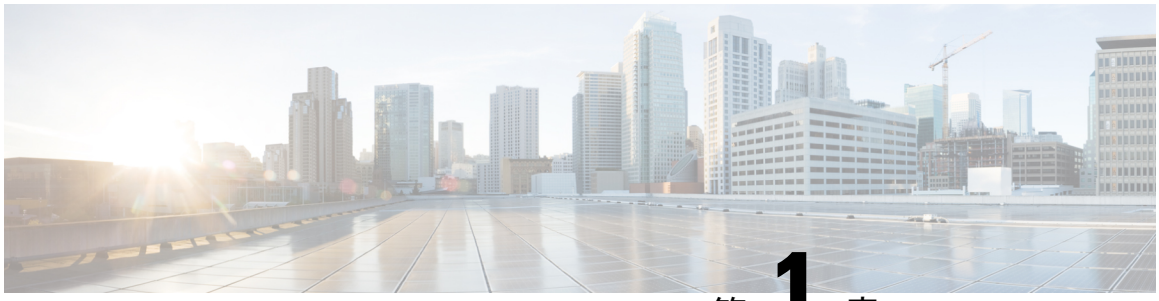
パケット キャプチャ 154

ローカル パケット キャプチャ 154

リモート パケット キャプチャ 156
リモート ホストへのストリーミング 156
CloudShark へのストリーム 157
Wireshark 158
パケット キャプチャ ファイルのダウンロード 160
HTTP の使用 161
サポート情報 161
CPU/RAM データのダウンロード 161

付録 A： 認証解除メッセージの理由コード 163
認証解除メッセージの理由コード 163
認証解除理由コード表 163

付録 B： 関連情報 165
関連情報 165



第 1 章

はじめに

この章の内容は、次のとおりです。

- 設定の開始 （1 ページ）
- アクセス ポイント セットアップ ウィザードの使用 （3 ページ）
- パスワードの変更 （7 ページ）
- TCP/UDP サービス （8 ページ）
- システムの状態 （9 ページ）
- クイック スタート コンフィギュレーション （10 ページ）
- ウィンドウ ナビゲーション （11 ページ）

設定の開始

ここでは、システム要件と Web ベースの設定ユーティリティへのアクセス方法について説明します。

サポートされるブラウザ

設定ユーティリティを使用する前に、Internet Explorer 9 以降、Firefox 46 以降、Chrome 49 以降、または Safari 5.0 以降が搭載されたコンピュータがあることを確認してください。

ブラウザについての制約事項

- Internet Explorer 9 を使用している場合は、次のセキュリティ設定を行います。
  - [ツール] > [インターネット オプション] を選択してから、[セキュリティ] タブを選択します。
  - [ローカル イントラネット] を選択してから、[サイト] を選択します。
  - [詳細設定] を選択し、[追加] を選択します。WAP デバイスのイントラネット アドレス（`http://<ip-address>`）をローカル イントラネット ゾーンに追加します。IP アドレスはサブネット IP アドレスとして指定することもできます。これにより、すべてのサブネット アドレスをローカル イントラネット ゾーンに追加できます。

- 管理ステーションに複数の IPv6 インターフェイスがある場合は、IPv6 ローカル アドレスではなく IPv6 グローバル アドレスを使用して、ブラウザから WAP デバイスにアクセスしてください。

Web ベースの設定ユーティリティの開始

次のステップに従って、コンピュータから設定ユーティリティにアクセスし、WAP デバイスを設定します。

1. WAP デバイスをコンピュータと同じネットワーク（IP サブネット）に接続します。WAP デバイスの工場出荷時のデフォルトの IP アドレス設定は、DHCP です。DHCP サーバが稼働しており、アクセス可能であることを確認します。
2. WAP デバイスの IP アドレスを特定します。
    1. Cisco FindIT Network Discovery Utility を使用すると、WAP デバイスにアクセスして管理できるようになります。このユーティリティにより、コンピュータと同じローカル ネットワーク セグメント内のサポートされているシスコ デバイスをすべて自動的に検出できます。各デバイスのスナップショットを表示することや、製品のコンフィギュレーション ユーティリティを起動して設定値を表示および指定することができます。詳細については、http://www.cisco.com/go/finditを参照してください。
    2. WAP デバイスは Bonjour 対応で、それ自体のサービスを自動的にブロードキャストし、他の Bonjour 対応のデバイスによってアドバタイズされたサービスをリッスンします。Bonjour プラグインが追加された Microsoft Internet Explorer、Apple Mac Safari ブラウザなどの Bonjour 対応のブラウザがある場合は、IP アドレスが不明でも、ローカル ネットワーク上の WAP デバイスを検索できます。

       Microsoft Internet Explorer ブラウザ対応の完全な Bonjour は、次の URL の Apple の Web サイトからダウンロードできます。http://www.apple.com/bonjour/。
    3. ルータまたは DHCP サーバにアクセスして、DHCP サーバによって割り当てられた IP アドレスを検索します。詳細については、DHCP サーバの取り扱い説明書を参照してください。
3. Microsoft Internet Explorer などの Web ブラウザを起動します。
4. アドレスバーにデフォルトの DHCP アドレスを入力し、Enter キーを押します。
5. デフォルトのユーザ名とパスワードを入力します。`cisco` を [ユーザ名] および [パスワード] フィールドに入力します。
6. [ログイン] をクリックします。アクセス ポイント セットアップ ウィザードが表示されます。

セットアップ ウィザードの手順に従ってインストールを完了します。初回インストール時には、セットアップ ウィザードを使用することを強くお勧めします。詳細については、「アクセス ポイント セットアップ ウィザードの使用 （3 ページ）」を参照してください。

スマートフォンやタブレットなどのポータブルデバイスで、Webベースの構成ユーティリティを起動するには、このセクションですでに説明した手順と同じ手順を実行します。ポータブルデバイスにログインした後、モバイルでの[アクセスポイントセットアップ ウィザード（Access Point Setup Wizard）] のページが表示されます。詳しくは、モバイルでのアクセス ポイント セットアップ ウィザードの使用を参照してください

ログアウト

デフォルトで、設定ユーティリティは 10 分間非アクティブな状態が続くとログアウトされるようになっています。デフォルトのタイムアウト時間を変更する手順については、「管理 （29 ページ）」を参照してください。

ログアウトするには、設定ユーティリティの右上隅の [ログアウト] をクリックします。

アクセス ポイント セットアップ ウィザードの使用

アクセスポイントに初めてログインすると（または工場出荷時設定にリセットされた後にログインすると）、初期設定の実行を支援するアクセス ポイント セットアップ ウィザードが表示されます。ウィザードを完了するには、次の手順を実行します。

（注） [キャンセル（Cancel）] をクリックしてウィザードをバイパスすると、[パスワードの変更（Change Password）] ページが表示されます。そこで、ログイン用のデフォルトのパスワードとユーザ名を変更できます。詳細については、パスワードの変更 （7 ページ） を参照してください。

パスワードを変更した後に再びログインする必要があります。

ステップ 1 ウィザードの初期ページで [次へ]をクリックします。ファームウェアアップグレードウィンドウが表示されます。

ステップ 2 ファームウェアをアップグレードするには、[アップグレード（Upgrade）] をクリックします。

（注） ファームウェアがアップグレードされると、デバイスは自動的にリブートし、ログイン ページが表示されます

ステップ 3 [スキップ（Skip）] をクリックします。 [構成の復元（Restore Configuration）] ウィンドウが表示されます。

ステップ 4 デバイスに適用する構成ファイルを選択し、[保存（Save）] をクリックします。

（注） [保存（Save）] をクリックします。デバイスに関係する構成が適用された後、自動的にリブートし、ログイン ページが表示されます。

ステップ 5 [スキップ（Skip）] をクリックします。[デバイスの構成 - IP アドレス（Configure Device - IP Address ）] ウィンドウが表示されます。

ステップ 6 DHCP サーバから IP アドレスを受信する場合は、[ダイナミック IP アドレス（DHCP）] をクリックします（推奨）。また、IP アドレスを手動で設定する場合は、[スタティック IP アドレス] をクリックします。これらのフィールドの説明については、「IPv4 設定」を参照してください。

ステップ 7 [次へ] をクリックします。[シングル ポイント設定 - クラスタの設定] ウィンドウが表示されます。シングル ポイント セットアップの説明については、「シングル ポイント設定」を参照してください。

ステップ 8 WAP デバイスの新しいシングル ポイント設定を作成するには、[新しいクラスタ名] をクリックし、新しいクラスタ名を指定します。同じクラスタ名でデバイスを設定し、他の WAP デバイスでシングル ポイントセットアップ モードを有効にすると、それらは自動的にグループに参加します。

ネットワーク上にすでにクラスタがある場合は、[既存のクラスタに参加] をクリックし、[既存クラスタ名] にクラスタ名を入力することにより、このデバイスをクラスタに追加できます。

このデバイスをこの時点でシングル ポイント設定に参加させない場合は、[シングル ポイント設定を有効にしない] をクリックします。

オプションで、[AP の位置] フィールドにアクセス ポイントの位置を入力して、WAP デバイスの物理的な位置を示すこともできます。

[既存のクラスタに参加（Join an Existing Cluster）]ラジオ ボタンをクリックすると、WAP により該当するクラスタを基にして残りの設定が行われます。[次へ（Next）] をクリックして、クラスタへの参加を確認します。 [送信（Submit）] をクリックして、クラスタに参加します。 設定が完了したら、[終了（Finish）] をクリックしてセットアップ ウィザードを終了します。

ステップ 9 [次へ] をクリックします。[デバイスの設定 - システム日時の設定] ウィンドウが表示されます。

ステップ 10 時間帯を選択し、NTP サーバからシステム時刻を自動的に設定するか、または手動で設定します。これらのオプションの説明については、「時刻 （21 ページ）」を参照してください。

ステップ 11 [次へ] をクリックします。[デバイスの設定 - パスワードの設定] ウィンドウが表示されます。

ステップ 12 [新しいパスワード] にパスワードを入力し、[パスワードの確認] フィールドにもう一度パスワードを入力します。

（注） パスワード セキュリティ ルールを無効にするには、[パスワードの複雑性] をオフにします。ただし、パスワードセキュリティ ルールは有効にしたままにすることを強くお勧めします。パスワードの詳細については、「セキュリティ （38 ページ）」を参照してください。

ステップ 13 [次へ] をクリックします。[無線 1 の構成 - ワイヤレス ネットワーク名の指定] ウィンドウが表示されます。

ステップ 14 [ネットワーク名] にネットワーク名を入力します。この名前は、デフォルト ワイヤレス ネットワークの SSID として使用されます。

ステップ 15 [次へ] をクリックします。[無線 1 の構成 - ワイヤレス ネットワークの保護] ウィンドウが表示されます。

ステップ 16 セキュリティ暗号化タイプを選択し、セキュリティ キーを入力します。これらのオプションの説明については、「セキュリティの設定 （57 ページ）」を参照してください。

ステップ 17 [次へ] をクリックします。[無線 1 の構成 - ワイヤレス ネットワークへの VLAN ID の割り当て] ウィンドウが表示されます。

ステップ 18 ワイヤレス ネットワークで受信されるトラフィックの VLAN ID を選択します。

ワイヤレス トラフィックを VLAN 1 の管理トラフィックと分離するために、デフォルト（1）とは異なる VLAN ID をワイヤレス トラフィックに割り当てることをお勧めします。

ステップ 19 [次へ] をクリックします。ステップ 13 ～ 18 を繰り返し、無線 2 のインターフェイスの設定を行います。

ステップ 20 [次へ] をクリックします。[キャプティブ ポータルの有効化 - ゲスト ネットワークの作成] ウィンドウが表示されます。

ステップ 21 ネットワーク上のゲストの認証方式をセットアップするかどうかを選択し、[次へ] をクリックします。

[いいえ] をクリックした場合は、ステップ 29 に進みます。

[はい] をクリックすると、[キャプティブ ポータルの有効化 - ゲスト ネットワーク名の指定] ウィンドウが表示されます。

ステップ 22 ゲスト ネットワーク名を指定します。

ステップ 23 [次へ] をクリックします。[キャプティブ ポータルの有効化 - ゲスト ネットワークの保護] ウィンドウが表示されます。

ステップ 24 ゲスト ネットワークのセキュリティ暗号化タイプを選択し、セキュリティ キーを入力します。これらのオプションの説明については、「セキュリティの設定 （57 ページ）」を参照してください。

ステップ 25 [次へ] をクリックします。[キャプティブ ポータルの有効化 - VLAN ID の割り当て] ウィンドウが表示されます。

ステップ 26 ゲスト ネットワークの VLAN ID を指定します。ゲスト ネットワークの VLAN ID は、管理 VLAN ID と異なっている必要があります。

ステップ 27 [次へ] をクリックします。[キャプティブ ポータルの有効化 - リダイレクト URL を有効化] ウィンドウが表示されます。

ステップ 28 [リダイレクト URL を有効化] をオンにし、[リダイレクト URL] フィールドに完全修飾ドメイン名（FQDN）または IP アドレス（「http://」を含む）を入力します。指定すると、ゲスト ネットワーク ユーザが、認証後に、指定された URL にリダイレクトされるようになります。

ステップ 29 [次へ] をクリックします。[概要 - 設定の確認] ウィンドウが表示されます。

ステップ 30 設定した値を確認します。[戻る] をクリックして、1 つまたは複数の設定を再設定します。[キャンセル] をクリックすると、すべての設定が前の値またはデフォルト値に戻ります。

ステップ 31 修正したら、[送信] をクリックします。セットアップ設定が保存され、確認ウィンドウが表示されます。

ステップ 32 [完了] をクリックします。

WAP デバイスは正常に設定されました。新しいパスワードでもう一度ログインする必要があります。

モバイルでのアクセス ポイント セットアップ ウィザードの使用

ポータブル デバイスでアクセス ポイントに初めてログインするか、または工場出荷時設定にリセットされると、初期設定の実行を支援するアクセス ポイント セットアップ ウィザードがモバイル スタイルで表示されます。このウィザードを使用してアクセス ポイントを構成するには、次の手順を実行します。

（注） 工場出荷時モードのデフォルトの SSID は CiscoSB-Setup です。この SSID と事前共有キー cisco123 を使用して、ポータブル デバイスとアクセス ポイントを関連付けます。ブラウザを起動して、任意の IP アドレスまたはドメイン名を入力します。Web ページにログイン フィールドが表示されます。デフォルトのユーザ名とパスワード、cisco を入力します。[ログイン（Log In）] をクリックします。[アクセスポイントセットアップウィザード（Access Point Setup Wizard）] が表示されます。

ステップ 1 ウィザードの [ようこそ（Welcome）] ページで [次へ（Next）] をクリックします。[IP アドレスの構成（Configure IP address ）] ウィンドウが表示されます。

ステップ 2 デフォルトでは、動的（DHCP）（推奨）が構成されており、DHCP サーバから IP アドレスを受信するようになっています。また、IP アドレスを手動で構成する場合は、[静的（Static）] をクリックします。これらのフィールドの説明については、「**IPv4 の構成**」を参照してください。

ステップ 3 [次へ（Next）] をクリックします。[シングルポイントセットアップの構成（Configure Single Point Setup）] ウィンドウが表示されます。

ステップ 4 [スキップ（Skip）] をクリックします。ステップ 6 に移動します。

ステップ 5 既存のクラスタに参加するには、クラスタ グループ名を入力して [次へ（Next）] をクリックします。サマリー ページにクラスタ情報が表示されます。データを確認して [送信（Submit）] をクリックします。

（注） 新しいクラスタを作成するには、[作成（Create）] をクリック後、クラスタ名を入力して、ステップ 6 に進みます。

ステップ 6 [デバイスの設定-パスワードの設定（Configure Device - Set Password）] ウィンドウで、新しいパスワードを入力し、[パスワードの確認（Confirm Password）] フィールドにパスワードを再入力します。

ステップ 7 [次へ（Next）] をクリックします。[ワイヤレス ネットワークの構成（Configure your Wireless Network ）] ウィンドウが表示されます。

a) デフォルト ワイヤレス ネットワークの SSID となるネットワーク名を入力します。
b) セキュリティ キーを入力します（デフォルトではセキュリティ タイプ、WPA2 パーソナル - AES
c) ワイヤレス ネットワークで受信されるトラフィックの VLAN ID を入力します。

（注） チェック ボックスにチェックを入れて Radio 2 に同じ設定を適用するか、別の無線タブに切り替えてから手順 7 を再度実行して再設定します

ステップ 8 [次へ（Next）] をクリックします。[キャプティブ ポータルのセットアップ（Setup Captive Portal）] ウィンドウが表示されます。

ステップ 9 [スキップ（Skip）] をクリックします。ステップ 12 に移動します。

ステップ 10 [はい（Yes）] をクリックします。[キャプティブ ポータルの構成（Captive Portal configuration ）] ウィンドウが表示されます。

ステップ 11 [無線1（5GHz）（Radio 1 (5 GHz)）] または [無線2（2.4GHz）（Radio 2 (2.4 GHz)）] を選択します

a) ゲスト ネットワーク名を指定します
b) セキュリティ キーを入力します（デフォルトではセキュリティ タイプ、WPA2 パーソナル - AES）

c) ゲスト ネットワークの VLAN ID を指定します。
d) オプションとして、完全修飾ドメイン名（FQDN）によるリダイレクトURLを指定することにより、ユーザ認証後に、指定した URL が表示されるようにすることができます。

ステップ 12 [次へ（Next）] をクリックします。[要約（Summary）] ウィンドウが表示されます。

ステップ 13 構成されている設定を確認してください。1つまたは複数の設定を再設定するには、[戻る（Back）] をクリックします。

ステップ 14 データが正しいことを確認した上で、[送信（Submit ）] をクリックして保存します。

ステップ 15 WAP デバイスは正常に設定されています。新しいパスワードでもう一度ログインする必要があります。

パスワードの変更

セキュリティ上の理由により、設定されている間隔で管理パスワードを変更する必要があります。[パスワード エージング タイム] に指定した期間が経過したときに、このページにアクセスする必要があります。

パスワード複雑度は、デフォルトで有効になっています。パスワード複雑性の最小要件が [パスワードの変更] ページに表示されます。新しいパスワードは、デフォルトの複雑性ルールに準拠する必要があります。または、[パスワードの複雑性] を無効にすることで、そのルールを一時的に無効にすることもできます。詳細については、「セキュリティ （38 ページ）」を参照してください。

デフォルト パスワードを変更するには、次のように設定します。

- [ユーザ名（Username）] : 新しいユーザ名を入力します。デフォルトの名前は cisco です。
- [古いパスワード] : 現在のパスワード（デフォルトは cisco）を入力します。
- [新しいパスワード] : 新しいパスワードを入力します。
- [パスワードの確認] : 新しいパスワードをもう一度入力します。
- [パスワード強度メーター] : 新しいパスワードの強度が表示されます。
- [パスワードの複雑性] : パスワードの複雑性はデフォルトで有効になっており、新しいパスワードは次のような複雑性の設定に準拠する必要があります。
  - ユーザ名とは異なるパスワードにすること。
  - 現在のパスワードとは異なるパスワードにすること。
  - 長さは 8 文字以上にすること。
  - 3 つ以上の文字クラスの文字（大文字、小文字、数字、標準キーボードで使用可能な特殊文字）を含むこと。

（注） パスワード複雑性ルールを無効にするには、[無効化]をオンにします。ただし、パスワード複雑性のルールは有効にしたままにすることを強くお勧めします。

TCP/UDP サービス

[TCP/UDP サービス] 表には、WAP で動作しているプロトコルとサービスが表示されます。

- [サービス]：サービス名。
- [プロトコル]：サービスで使用される基本的な転送プロトコル（TCP または UDP）。
- [ローカル IP アドレス]：接続デバイスの IP アドレス。[すべて] は、デバイス上のすべての IP アドレスでこのサービスを使用できることを示します。
- [ローカル ポート]：ローカル ポート番号。
- [リモート IP アドレス]：このサービスを使用しているリモート ホストの IP アドレス。[すべて] は、システムにアクセスするすべてのリモート ホストにサービスを使用できることを示します。
- [リモート ポート]：このサービスと通信するリモート デバイスのポート番号。
- [接続状態]：サービスの状態。UDP の場合、[アクティブ] または [確立済み] 状態の接続のみが表に表示されます。TCP の状態は次のとおりです。
  - [リスニング]：サービスは接続要求をリスニングしています。
  - [アクティブ]：接続セッションが確立され、パケットが送受信されています。
  - [確立済み]：WAPデバイスとサーバまたはクライアントの間で接続セッションが確立されています。
  - [待機中]：クロージング シーケンスが開始されていて、WAP デバイスは接続を終了するまでシステム定義のタイムアウト時間（通常は 60 秒）を待機しています。

（注） [TCP/UDP サービス] 表の中で順序を変更できます。[更新] をクリックすると画面が更新され、最新情報を表示します。

また、表示する TCP/UDP サービスをフィルタリングするために、サービス、プロトコル、その他の詳細に関連するパラメータを入力できます。

[作業の開始] ページに戻るには、[戻る] をクリックします。

システムの状態

[システムの状態] ページには、ハードウェア モデルの説明、ソフトウェア バージョン、および次のようなさまざまな設定パラメータが表示されます。

- [PID VID]：WAP デバイスのハードウェア モデルおよびバージョン。
- [シリアル番号]：WAP デバイスのシリアル番号。
- [ホスト名]：WAP デバイスに割り当てられているホスト名。
- [MAC アドレス]：WAP デバイスの MAC アドレス。
- [IPv4 アドレス]：WAP デバイスの IP アドレス。
- [IPv6 アドレス]：WAP デバイスの IPv6 アドレス。
- [LAN ポート]：イーサネット インターフェイスの状態を示します。
- [ETH1 ポート]：ETH1 インターフェイスの状態を示します。
- [無線 1（5GHz）]：無線 1 インターフェイスの 5GHz モードが有効または無効であるかを示します。
- [無線 2（2.4GHz）]：無線 2 インターフェイスの 2.4GHz モードが有効または無効であるかを示します。
- [電源]：システムは電源アダプタから電力を得るか、または 802.3.af と 802.3at の 2 つの電源モードが組み込まれた Power over Ethernet（PoE）を通じて給電側機器（PSE）から電力を得ることができます。

  電源が足りない場合（802.3af）、WAP デバイスは次の設定情報を維持します。

  - Radio1（5GHZ）が無効にされます。
  - Radio2（2.4GHZ）アンテナが 3 x3 から 2 x2 に切り替わり、TX の電力が 18dBm まで減少します。
  - ETH0/PD ポートの速度が 1Gbps にダウングレードします。
  - ETH1 ポートがオフにされます。

- [システム稼動時間]：最後の再起動から経過した時間。
- [システム時刻]：現在のシステム時刻。
- [ファームウェア バージョン（アクティブ イメージ）]：アクティブ イメージのファームウェア バージョン。
- [ファームウェアの MD5 チェックサム（アクティブイメージ）]：アクティブ イメージのチェックサム。

- [ファームウェア バージョン（非アクティブ）]：バックアップイメージのファームウェアバージョン。
- [ファームウェア MD5 チェックサム（非アクティブ）]：バックアップ イメージのチェックサム。

クイック スタート コンフィギュレーション

クイック ナビゲーションにより簡単にデバイス設定を実行できるように、[作業の開始]ページには、一般的なタスクを実行するためのリンクが用意されています。[作業の開始]ページは、開始時にデフォルトで表示されるウィンドウです。

カテゴリ	リンク名（ページ上）	リンク ページ
クイック アクセス	セットアップ ウィザード	アクセス ポイント セットアップ ウィザードの使用 （3 ページ）
	アカウント パスワードの変更	ユーザの追加 （28 ページ）
	構成のバックアップ/リストア	コンフィギュレーション ファイル （147 ページ）
	デバイスのファームウェアのアップグレード	ファームウェア （145 ページ）
詳細設定	ワイヤレス設定	無線 （47 ページ）
	管理設定	管理 （29 ページ）
	シングル ポイント セットアップの構成	シングル ポイント設定に関する WAP デバイスの設定
	LAN 設定	IPv4 設定 （13 ページ）
	ゲスト アクセス	ゲスト アクセス （98 ページ）
詳細情報	ダッシュボード	ダッシュボード
	TCP/UDP サービス	TCP/UDP サービス （8 ページ）
	システム ログを表示する	LED ディスプレイ （22 ページ）
	トラフィック統計	トラフィック統計 （138 ページ）

デバイスの追加情報については、次の手順で製品サポートページまたはシスコ サポート コミュニティにアクセスできます。

- 製品サポート ページにアクセスするには [サポート] をクリックします。

- シスコ サポート コミュニティ ページにアクセスするには [フォーラム] をクリックします。
- [FindIT についての詳細（More info on FindIT）] をクリックすると、FindIT ユーティリティについての詳細情報が表示されます。
- FindIT ユーティリティをダウンロードするには、[FindIT をダウンロード（Download FindIT）] をクリックします。

ウィンドウ ナビゲーション

WAP のグラフィック ユーザ インターフェイス内を移動するには、ナビゲーション ボタンを使用します。

設定ユーティリティのヘッダー

設定ユーティリティのヘッダーには標準的な情報が含まれており、各ページの上部に表示されます。ヘッダーには次のボタンがあります。

ボタン名	説明
（ユーザ）	WAP デバイスにログインしているユーザのアカウント名（Administrator または Guest）です。工場出荷時のユーザ名は **cisco** です。
（言語）	ボタンの上にマウス ポインタを移動させて、言語を選択します。工場出荷時設定の言語は英語です。
	クリックすると、設定ユーティリティからログアウトします。
	クリックすると、WAPデバイスのタイプおよびバージョン番号が表示されます。
	クリックすると、状況依存のオンライン ヘルプが表示されます。オンラインヘルプは、UTF-8 エンコーディングを使用するブラウザで表示されるように設計されています。オンライン ヘルプが文字化けする場合は、ブラウザのエンコーディング設定が UTF-8 に設定されていることを確認してください。

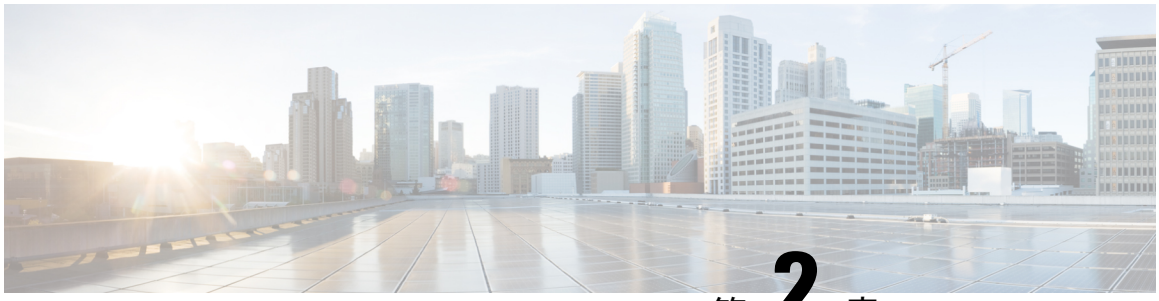
ナビゲーション ペイン

ナビゲーション ウィンドウ（またはメイン メニュー）は、各ページの左側にあります。ナビゲーション ウィンドウは、WAP デバイスの最上位機能のリストです。メイン メニュー項目の前に矢印がある場合は、選択して展開すると、各グループのサブメニューが表示されます。その後、必要なサブメニュー項目を選択して、関連ページを開くことができます。

管理ボタン

システム内のさまざまなページに表示されるよく使用されるボタンを次の表に示します。

ボタン名	説明
追加	新しいエントリをテーブルまたはデータベースに追加します。
キャンセル	ページに加えた変更をキャンセルします。
すべてクリア	ログ テーブルのすべてのエントリを消去します。
削除	テーブルのエントリを削除します。
[編集]	既存のエントリを編集します。
更新	現在のページを最新のデータで更新します。
保存	設定またはコンフィギュレーションを保存します。
更新	新しい情報でスタートアップ コンフィギュレーションを更新します。



第 2 章

システム設定

この章では、グローバルなシステム設定を設定し、診断を実施する方法を説明します。具体的な内容は次のとおりです。

- LAN （13 ページ）
- 時刻 （21 ページ）
- 通知 （22 ページ）
- ユーザ アカウント （28 ページ）
- 管理 （29 ページ）
- セキュリティ （38 ページ）

LAN

ここでは、WAP デバイスのポート、VLAN、LLDP、IPv4、IPv6 の設定方法について説明します。

IPv4 設定

[IPv4 設定] ページを使用して、IPv4 アドレスを設定します。

ステップ 1 [LAN] > [IPv4 設定] の順に選択します。

ステップ 2 次の IPv4 設定を行います。

- [接続タイプ]：デフォルトでは、WAP デバイス上の DHCP クライアントが、ネットワーク情報の要求を自動的にブロードキャストします。スタティック IP アドレスを使用する場合は、DHCP クライアントを無効にして、手動で IP アドレスとその他のネットワーク情報を設定する必要があります。

  次のいずれかのオプションを選択します。

  - [DHCP]：WAP デバイスは、LAN 上の DHCP サーバから IP アドレスを取得します。
  - [スタティック IP]：IPv4 アドレスを手動で設定します。IPv4 アドレスは、xxx.xxx.xxx.xxx（172.17.144.170）の形式にする必要があります。

- [スタティック IP アドレス、サブネット マスク、およびデフォルト ゲートウェイ] : スタティック IP アドレス、サブネット マスク、およびデフォルト ゲートウェイを入力します。
- [ドメイン ネーム サーバ] : 次のいずれかのオプションを選択します。
  - [ダイナミック] : WAP デバイスは、LAN 上の DHCP サーバから DNS サーバ アドレスを取得します。
  - [手動] : 表示されるフィールドに最大 2 つの IP アドレスを入力します。

ステップ 3 [保存] をクリックして変更内容を保存します。

DHCP 自動コンフィギュレーション設定

- [DHCP 自動コンフィギュレーション オプション] : このオプションはデフォルトで有効になっています。AP が工場出荷時の状態で起動される場合、最初に DHCP オプションを使用した自動コンフィギュレーションが試みられます。

  自動コンフィギュレーションの動作は次のとおりです。

  - イーサネット インターフェイスだけが有効であり、WLAN インターフェイスはダウンした状態で、AP が起動します。
  - ユーザが利用できるサービスはありません（ユーザインターフェイスは除きます）。
  - [待機間隔] に指定された時間が経過した時点、またはコンフィギュレーション ファイルの TFTP アップロードが完了した時点（どちらか早い方）で、[DHCP 自動コンフィギュレーション オプション] が自動的に無効になります。
  - DHCP クライアントを無効にした場合（つまり、スタティック IP アドレスを使用するように設定した場合）や、[DHCP 自動コンフィギュレーション オプション] を無効にした場合は、自動コンフィギュレーションは即時に中止されます。

  DHCP クライアントは、DHCP オプション 66 および 67 の要求を自動的にブロードキャストします。[DHCP] と [DHCP 自動コンフィギュレーション オプション] が有効である場合、アクセス ポイントは次のリブート時に、DHCP 要求に対して DHCP サーバが返した情報を使用して自動的に設定されます。

（注） ユーザ/シスコがコンフィギュレーション ファイルをアップロードすると、自動コンフィギュレーションはオーバーライドされて、その選択されたコンフィギュレーション ファイルが優先されます。それ以外の場合に AP がリブートされるとき（ファームウェアをアップグレードした場合やリブート操作を行った場合など）には、既存の自動コンフィギュレーション設定が適用されます。

- [TFTP サーバの IPv4 アドレス/ホスト名]：TFTP サーバのアドレスを設定すると、自動コンフィギュレーション中に DHCP サーバが指定する他の TFTP サーバからファイルを取得できなかった場合に、そのアドレスが使用されます。IPv4 アドレスまたはホスト名の情報を入力します。ホスト名の形式で入力する場合は、ホスト名を IP アドレスに変換するための DNS サーバが利用可能でなければなりません。

この値は、次の起動時に自動コンフィギュレーション プロシージャで使用されます。

- [コンフィギュレーション ファイル名]：コンフィギュレーション ファイル名を指定すると、AP の自動コンフィギュレーション中に DHCP サーバからブート ファイル名を受信しない場合に、指定したコンフィギュレーション ファイルが TFTP サーバから取得されます。この値が指定されていない場合は、「config.xml」が使用されます。ファイルを指定する場合、拡張子は xml でなければなりません。

この値は、次の起動時に自動コンフィギュレーション プロシージャで使用されます。

- [待機間隔]：待機間隔が設定されている場合、アクセス ポイントがローカル設定を使用して起動した後、待機間隔として設定された時間が経過してから、有効にされているサービスをユーザが利用できるようにします。指定された待機期間内に TFTP トランザクションが開始されなければ、アクセス ポイントは自動コンフィギュレーションを中止します。

この値は、次の起動時に自動コンフィギュレーション プロシージャで使用されます。

- [ステータス ログ]：このフィールドには、自動コンフィギュレーションの完了または中止理由が表示されます。

IPv6 設定

[IPv6 設定] ページを使用して、次の手順に従い IPv6 アドレスを設定します。

ステップ 1 [LAN] > [IPv6 設定] の順に選択します。

ステップ 2 次のパラメータを設定します。

- [IPv6 接続タイプ]：次のいずれかのオプションを選択します。
  - [DHCPv6]：DHCPv6 サーバによって IPv6 アドレスが割り当てられます。
  - [スタティック IPv6]：IPv6 アドレスを手動で設定します。IPv6 アドレスは、xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx（2001:DB8::CAD5:7D91）の形式にする必要があります。
- [IPv6 管理モード]：IPv6 管理モードを有効にするには [有効化] をオンにします。
- [IPv6 自動設定管理モード]：IPv6 自動アドレス設定を有効にするには、[有効化] をオンにします。

  IPv6 自動アドレス設定が有効な場合、WAP デバイスは、LAN ポートで受信したルータ アドバタイズメントを処理することによって、IPv6 アドレスとゲートウェイを認識します。WAP デバイスは、自動設定された複数の IPv6 アドレスを持つことができます。

- [スタティック IPv6 アドレス]：スタティック IPv6 アドレスを入力します。WAP デバイスは、アドレスがすでに自動設定されていても、スタティック IPv6 アドレスを持つことができます。
- [スタティック IPv6 アドレスのプレフィクス長]：スタティック アドレスのプレフィクス長を 0 ～ 128 の整数で入力します。デフォルトは 0 です。
- [スタティック IPv6 アドレスのステータス]：次のいずれかのオプションを選択します。
  - [稼働中]：IP アドレスは一意と確認され、LAN インターフェイスで使用可能です。
  - [試行中]：WAP デバイスは、スタティック IP アドレスが割り当てられると、重複アドレス検出（DAD）プロセスを自動的に開始します。この IPv6 アドレスは、ネットワーク上で検証中の仮のアドレスであるため、トラフィックの送受信には使用できません。
  - [空白（値なし）]：IP アドレスが割り当てられていません。
- [IPv6 自動設定グローバル アドレス]：このデバイスに自動的に割り当てられた IPv6 アドレスがリストされます。
- [IPv6 リンク ローカル アドレス]：ローカルの物理リンクに使用される IPv6 アドレス。リンク ローカル アドレスは設定できません。IPv6 ネイバー探索プロセスを使用することで割り当てられます。
- [デフォルト IPv6 ゲートウェイ]：静的に設定されたデフォルト IPv6 ゲートウェイ。
- [IPv6 ドメイン ネーム サーバ]：次のいずれかのオプションを選択します。
  - [ダイナミック]：DNS サーバは DHCPv6 を介してダイナミックに認識されます。
  - [手動]：最大 2 つの IPv6 DNS サーバを手動で指定します。

ポート設定

ポート設定テーブルを使用して、WAP デバイスを LAN に接続するポートの設定を表示および実行します。

ステップ 1 **[LAN]** > **[詳細]** > **[ポート設定テーブル]** の順に選択します。

[ポート設定テーブル] には、LAN インターフェイスの次のステータスと設定が表示されます。

- [リンク アグリゲーション]：リンク アグリゲーション グループ（LAG）を有効にします。
- [LAG モード]：次のオプションがあります。
  - [標準LAG]：2つのイーサネットインターフェイスの間でネゴシエートされた速度が異なる場合、後のほうのプラグインが一時停止されます。
  - [BW優先]：2つのイーサネットインターフェイスの間でネゴシエートされた速度が異なる場合、速度が遅いほうが一時停止されます。

- [冗長性および電力優先]：バインドのために 2 つのイーサネット インターフェイスの速度が同じになるように調整します。これがデフォルトのモードです。

（注） WAP581 は静的 LAG をサポートし、LACP はサポートしていません。WAP581 デバイスで LAG が機能するようにしてください。それにより、ユーザが LAG をデフォルトのモードから別のモードに切り替えられるようになります。

[ポート設定テーブル] には、次のインターフェイス（LAN）のステータスと設定が表示されます。

- [インターフェイス]：LAN のインターフェイスを指定します。
- [リンク ステータス]：現在のポートのリンク ステータスが表示されます。
- [ポートの速度]：レビュー モードでは、現在のポートの速度が表示されます。編集モードでは、自動ネゴシエーションが無効な場合、100 Mbps または 10 Mbps などのポート速度を選択します。1000 Mbps の速度は、自動ネゴシエーションが有効な場合にのみサポートされます。
- [デュプレックス モード]：レビュー モードでは、現在のポートのデュプレックス モードが表示されます。編集モードでは、自動ネゴシエーションが無効な場合、[半二重] または [全二重] のいずれかのモードを選択します。
- [自動ネゴシエーション]：有効な場合、ポートはリンク パートナーとネゴシエートして、最速のリンク速度と使用可能なデュプレックス モードを設定します。無効な場合、手動で [ポート速度] と [デュプレックス モード] を設定できます。
- [グリーン イーサネット]：グリーン イーサネット モードでは、自動パワーダウン モードと Energy Efficient Ethernet（EEE、IEEE 802.3az）モードの両方がサポートされています。グリーン イーサネット モードは、ポートの自動ネゴシエーションが有効な場合にのみ機能します。自動パワーダウン モードでは、リンク パートナーからの信号が存在しない場合にチップ電力が低減されます。WAP デバイスは、回線上のエネルギーが失われると自動的に低電力モードになり、エネルギーが検出されると通常動作に戻ります。EEE モードでは、リンク使用量が少ないときの待機時間がサポートされます。これにより、リンクの両側で各 PHY の動作回路の一部を無効にして電力を節約できます。

ステップ 2 [保存] をクリックします。

スパニング ツリー プロトコル

スパニング ツリー プロトコル モードで [有効化] チェックボックスをオンにして、Cisco WAP デバイスの STP モードを有効にします。有効にした場合は、STP がループの切り替えを防止できるようになります。WDS リンクを設定する場合は、STP を推奨します。

VLAN 設定

[VLAN 設定] ページを使用して VLAN 設定を表示および実行します。

ステップ 1 [LAN] > [詳細] > [VLAN 設定テーブル] の順に選択します。

ステップ 2 次のパラメータを設定します。

- [タグなし VLAN ID]：タグなし VLAN ID に 1 ～ 4094 の番号を指定します。デフォルトは 1 です。このフィールドで指定した VLAN 上のトラフィックは、ネットワークに転送される際に VLAN ID でタグ付けされません。
- [説明]：関連する VLAN の説明。
- [管理 VLAN]：管理 VLAN は、Telnet または Web GUI を通して WAP デバイスにアクセスするために使用する VLAN です。管理 VLAN にすることができる VLAN は 1 つのみです。インターフェイス（有線または無線）が管理 VLAN に割り当てられていない場合、ユーザが設定ユーティリティへのアクセスに使用できるインターフェイスはありません。
- [VLAN]：ドロップダウン リストから VLAN を選択します（[タグなし] または [タグ付き]）。

  デフォルトでは、WAP デバイス上のすべてのトラフィックが VLAN 1（デフォルトのタグなし VLAN）を使用します。つまり、すべてのトラフィックは、タグなしの VLAN を無効にし、タグなしトラフィックの VLAN ID を変更するか、VAP またはクライアントの VLAN ID を RADIUS で変更するまで、タグは設定されません。

ステップ 3 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

ネイバー探索

Bonjour を使用すると、マルチキャスト DNS（mDNS）を使用して WAP デバイスおよび Bonjour のサービスを検出できます。Bonjour ではサービスをネットワークにアドバタイズし、サポートしているサービスの種類に関するクエリーに答えることで、その環境でのネットワーク構成をシンプル化します。

WAP デバイスでは次のサービスの種類をアドバタイズします。

- **シスコ固有のデバイス記述（csco-sb）**：このサービスにより、クライアントでは、ネットワークに展開されている Cisco WAP デバイスおよびその他の製品を検出できます。
- **管理ユーザ インターフェイス**：このサービスは WAP デバイスで使用可能な管理インターフェイス（HTTP および SNMP）を識別します。

Bonjour 対応 WAP デバイスがネットワークに接続されたとき、すべての Bonjour クライアントでは、事前構成なしで設定ユーティリティを検出して利用できます。

システム管理者はインストールされている Internet Explorer プラグインを使用して WAP デバイスを検出できます。この Web ベースの設定ユーティリティはブラウザのタブとして表示されます。

（注） システム管理者は最新の Internet Explorer プラグイン（Cisco FindIT ツール）を使用して Bonjour 対応の WAP を表示できます。Bonjour の検出処理後、クラスタ内に存在するすべての WAP デバイスがクラスタ名の下に表示されます。管理者は、クラスタ名がネットワーク内で一意であることを確認する必要があります。

Bonjour は IPv4 と IPv6 の両方で機能します。

Bonjour を介して WAP デバイスを検出できるようにするには、次の手順に従います。

ステップ 1 [LAN] > [ネイバー探索] の順に選択します。

ステップ 2 [有効化] をオンにし、Bonjour を有効にします。

ステップ 3 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

LLDP

IEEE 802.1AB 標準で定義されているリンク層検出プロトコル（LLDP）を使用すると、UAP はシステム名、システム性能、および所要電力をアドバタイズできます。この情報から、システム トポロジを特定したり、LAN 上の不適切な設定を検出したりすることができます。AP は、Link Layer Discovery Protocol for Media Endpoint Devices（LLDP-MED）もサポートしています。LLDP-MED は、ネットワーク管理を向上するためにデバイスが相互に渡す追加の情報エレメントを標準化します。

ステップ 1 LLDP 設定を行うには、[LAN] > [LLDP] の順に選択します。

ステップ 2 次のパラメータを設定します。

- [LLDP モード] : LLDP を有効にするには [有効化] をオンにします。有効にすると、AP は LLDP プロトコル データ ユニットをネイバー デバイスに送信します。
- [TX 間隔] : LLDP メッセージ送信間隔の秒数。有効な範囲は、5 ～ 32768 秒です。デフォルト値は 30 秒です。
- [POE プライオリティ] : ドロップダウン リストからプライオリティ レベルを選択します（[クリティカル]、[高]、[低]、[不明]）。給電側機器（PSE）は、PoE プライオリティに基づき、すべての接続デバイスに給電するだけの能力がない場合にどの受電デバイスに優先的に電力を割り当てるべきかを判断できます。

ステップ 3 [保存] をクリックします。

IPv6 トンネル

WAP デバイスは、Intra-Site Automatic Tunnel Addressing Protocol（ISATAP）をサポートしています。ISATAP によって、WAP デバイスは IPv6 パケットを IPv4 パケット内にカプセル化し、LAN を介して送信できます。このプロトコルによって、WAP デバイスは、接続する LAN が IPv6 をサポートしていなくても、リモートの IPv6 対応ホストと通信できます。

WAP デバイスは、ISATAP クライアントとして機能します。ISATAP が有効なホストまたはルータが、LAN 上に存在している必要があります。ルータの IP アドレスまたはホスト名は、WAP デバイスで設定されます（デフォルトでは ISATAP）。ホスト名として設定される場合、WAP デバイスは DNS サーバと通信して、名前を 1 つまたは複数の ISATAP ルータ アドレスに解決します。その後、WAP デバイスはルータに送信要求メッセージを送信します。ISATAP が有効なルータがアドバタイズメント メッセージで応答すると、WAP デバイスおよびルータがトンネルを確立します。トンネルインターフェイスは、リンク ローカル アドレスおよびグローバル IPv6 アドレスが割り当てられ、IPv4 ネットワーク上で仮想 IPv6 インターフェイスとして機能します。

IPv6 ホストが ISATAP ルータ経由で接続された WAP デバイスと通信を開始すると、ISATAP ルータによって IPv6 パケットは IPv4 パケットにカプセル化されます。

- **[ISATAP ステータス]**：[有効化] をオンにすると、デバイスで ISATAP が有効になります。
- **[ISATAP 対応ホスト]**：ISATAP ルータの IP アドレスまたは DNS 名を入力します。デフォルト値は isatap です。
- **[ISATAP クエリー間隔]**：WAP デバイスが DNS サーバにクエリーを送信して ISATAP ホスト名から IP アドレスへの解決を試行する間隔を入力します。有効な範囲は、120 ～ 3600 秒です。デフォルト値は 120 秒です。
- **[ISATAP 送信要求間隔]**：WAP デバイスからルータ送信要求メッセージを ISATAP ルータに送信する間隔を入力します。WAP デバイスは、アクティブな ISATAP ルータがない場合にのみルータ送信要求メッセージを送信します。有効な範囲は、120 ～ 3600 秒です。デフォルト値は 120 秒です。
- **[ISATAP IPv6 リンク ローカル アドレス]**：ローカルの物理リンクに使用される IPv6 アドレス。リンク ローカル アドレスは設定できません。IPv6 ネイバー探索プロセスを使用することで割り当てられます。
- **[ISATAP IPv6 グローバル アドレス]**：WAP デバイスに 1つ以上の IPv6 アドレスが自動的に割り当てられている場合、そのアドレスが表示されます。

（注） トンネルが確立されると、[ISATAP IPv6 リンク ローカル アドレス] フィールドと [ISATAP IPv6 グローバル アドレス] フィールドがページに表示されます。これらは仮想 IPv6 インターフェイス アドレスです。

をクリックします **[保存]**。

時刻

システム クロックは、メッセージ ログ用にネットワークと同期したタイムスタンプを付けるサービスを提供します。システム クロックは、手動で設定するか、またはサーバからクロックデータを取得する Network Time Protocol（NTP）クライアントとして設定できます。

[時間設定] ページは、システム時刻を手動で設定するか、事前設定された NTP サーバからシステム時刻を設定するために使用します。デフォルトでは、WAP デバイスは、事前設定された NTP サーバのリストから時刻を取得するように設定されます。

現在のシステム時刻が [システム クロック ソース] オプションと合わせてページの先頭に表示されます。

NTP を通じた時刻設定の自動取得

NTP サーバから時刻設定を自動取得するには、次の手順に従います。

ステップ 1 [システム設定] > [時刻] を選択します。

ステップ 2 [システム クロック ソース] 領域で [Network Time Protocol（NTP）] をクリックします。

ステップ 3 次のパラメータを設定します。

- [NTP サーバ（1 ～ 4）]：NTP サーバの IPv4 アドレス、IPv6 アドレス、またはホスト名を指定します。デフォルトの NTP サーバがリストされます。

  ホスト名は、最大 63 文字の英数字のセットからなる 1 つ以上のラベルで構成できます。ホスト名に複数のラベルが含まれる場合、それぞれをピリオド（.）で区切ります。一連のラベルおよびピリオドの長さは、最大 253 文字にすることができます。

- **[タイムゾーン]**：場所に応じたタイムゾーンを選択します。
- **[夏時間に調整する]**：これをオンにすると、次のフィールドを有効にして設定できます。
  - **[開始]**：夏時間を開始する月、日、週、時間を選択します。
  - **[終わり]**：夏時間を終了する月、日、週、時間を選択します。
  - **[夏時間オフセット]**：夏時間の開始時にクロックを進めて終了時に戻す分数を指定します。

ステップ 4 をクリックします**[保存]**。 変更がスタートアップ コンフィギュレーションに保存されます。

時刻設定の手動指定

時間設定を手動で指定するには、次の手順を実行してください。

ステップ 1 [システム設定] > [時刻] を選択します。

ステップ 2 [システム クロック ソース] 領域で [手動で] を選択します。

ステップ 3 [PC と時間を同期] をクリックし、ローカル PC のシステム時刻設定を複製します。

ステップ 4 また、次のフィールドも設定します。

- [システム日付]：ドロップダウンリストから現在の月、日、および 1 年の何日目かを選択します。
- [システム時刻]：24 時間表記で現在の時間と分を選択します。
- [タイムゾーン]：場所に応じたタイムゾーンを選択します。
- [夏時間に調整する]：タイム ゾーンに夏時間が適用される場合は、このオプションをオンにして次のフィールドを設定します。
  - [開始]：夏時間を開始する月、日、週、時間を選択します。
  - [終わり]：夏時間を終了する月、日、週、時間を選択します。
  - [夏時間オフセット]：夏時間の開始時にクロックを進めて終了時に戻す分数を指定します。

ステップ 5 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

（注） [PC と時間を同期] をクリックします。デバイスのシステム時刻が PC と同じになります。

通知

ここでは、アクセス ポイントの通知を有効化し設定する手順を詳述します。

LED ディスプレイ

WAP デバイスには 2 つのタイプ LED があります。1 つはシステム LED、もう 1 つはイーサネット LED です。[LED ディスプレイ] ページを使用してすべての LED を設定します。

LED ディスプレイを設定するには、次の手順を実行します。

ステップ 1 [通知] > [LED ディスプレイ] を選択します。

ステップ 2 LED を有効にするには [有効化] を選択します。LED を無効にするには [無効化] を選択します。[スケジューラの関連付け] を選択してステップ 3 に進みます。

ステップ 3 [スケジューラの関連付け LED ディスプレイ] のドロップダウン リストからプロファイル名を選択します。デフォルトでは LED に関連付けられているプロファイルはありません。このドロップダウン選択項目には、[ワイヤレス] > [スケジューラ] ページで設定したスケジューラ プロファイル名が表示されます。

LED がスケジューラ プロファイルと関連付けられている場合、このカラムには、該当時刻にアクティブ プロファイル ルールが存在しているのかどうかに応じたステータスが表示されます。

ステップ 4 [保存] をクリックします。

ログ設定

[ログ設定] ページを使用して、永続的メモリへのログ メッセージの保存を有効にします。リモート ホストにログを送信することもできます。

システムが予期せずリブートした場合、ログ メッセージは原因の診断に役立つことがあります。ただし、永続的ロギングを有効にしていない場合は、システムがリブートするとログメッセージは消去されます。

⚠

注意 永続的ロギングを有効にすると、フラッシュ（不揮発性）メモリが消耗し、ネットワーク パフォーマンスが低下することがあります。永続的ロギングを有効にするのは問題をデバッグするときだけにしてください。問題のデバッグの完了後は、永続的ロギングを必ず無効にしてください。

永続的ログの設定

ステップ 1 [通知] > [ログ設定] の順に選択します。

ステップ 2 次のパラメータを設定します。

- [パーシステンス]：不揮発性メモリにシステム ログを保存して WAP デバイスの再起動時にログが維持されるようにするには、[有効化] をオンにします。保存できるログ メッセージは最大 1000 個です。1000 個の制限に到達すると、最も古いログ メッセージが最新のメッセージによって上書きされます。揮発性メモリにシステム ログを保存するにはこのフィールドをクリアします。揮発性メモリに格納されたログはシステムがリブートすると削除されます。
- [重大度]：不揮発性メモリに保存するイベント メッセージのフィルタリングに使用する重大度を、ドロップダウン リストから選択します（[緊急]、[アラート]、[クリティカル]、[エラー]、[警告]、[情報]、[デバッグ]）。その他のメッセージはすべて揮発性メモリに保存されます。
- [深度]：揮発性メモリに保管できるメッセージの最大数（最大 1000）を入力します。このフィールドに設定した数に到達すると、最も古いログ イベントが最新のログ イベントによって上書きされます。

ステップ 3 [保存] をクリックします。

リモート ログ サーバ

カーネル ログは、（[システム ログ] に表示される）システム イベントとカーネル メッセージを含む包括的なリストです。

カーネル ログ メッセージは、設定ユーティリティから直接表示できません。まず、ログを受信してキャプチャするようにリモート ログ サーバを設定する必要があります。その後、リモート ログ サーバにログを記録するように WAP デバイスを設定できます。WAP デバイスでは最大 2 つのリモート ログ サーバをサポートします。

syslog メッセージ用のリモート ログ サーバ収集は次の機能を提供します。

- 複数の AP からの syslog メッセージを集約。
- 単独の WAP デバイスに保持するよりも長くメッセージの履歴を保管。
- スクリプトによって管理される操作およびアラートをトリガー。

ネットワーク上のホストをリモート ログ サーバとして動作するように指定するには、次の手順を実行してください。

ステップ 1 [通知] > [ログ設定] の順に選択します。

ステップ 2 [リモート ログ サーバ テーブル] で、次のパラメータを設定します。

- [サーバ IPv4/IPv6 アドレス/名前]：リモート ログ サーバの IPv4 または IPv6 アドレスか、ホスト名を入力します。

  ホスト名は、最大 63 文字の英数字のセットからなる 1 つ以上のラベルで構成できます。ホスト名に複数のラベルが含まれる場合、それぞれをピリオド（.）で区切ります。一連のラベルおよびピリオドの長さは、最大 253 文字にすることができます。

- [有効化]：リモート ログ サーバを有効にするには [有効化] をオンにします。次に、ログの重大度と UDP ポートを定義します。
- [ログの重大度]：リモート ログ サーバに送信するために必要とされるイベントの重大度をオンにします。
- [UDP ポート]：リモート ホスト上の syslog プロセスの論理ポート番号を入力します。範囲は 1 ～ 65535 です。デフォルト ポートは 514 です。

  デフォルト ポートの使用をお勧めします。ログ ポートを設定し直す場合は、syslog に割り当てるポート番号が使用可能であることを確認します。

ステップ 3 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

（注） リモートログサーバを有効にした場合は、[保存]をクリックするとリモートロギングがアクティブになります。WAP デバイスは、設定に応じて、リモート ログ サーバ モニタ表示、指定されたカーネル ログ ファイル、または他のストレージにカーネルデータをリアルタイムで送信します。

リモート ログ サーバを無効にした場合は、[保存] をクリックするとリモート ロギングが無効になります。

システム ログを表示する

[システム ログを表示する] ページには、そのデバイスで発生したシステム イベントのリストが表示されます。ログは再起動時にクリアされます。管理者がクリアすることもできます。最大 1000 個のイベントが表示されます。古いエントリは、新しいイベント用にスペースを空けるために、必要に応じてリストから削除されます。

システム ログを表示するには、[通知] > [システム ログを表示する] の順に選択します。

次の情報が表示されます。

- [タイム スタンプ]：イベントが発生したシステム時刻。
- [重大度]：イベントの重大度レベル。
- [サービス]：イベントに関連付けられたサービス。
- [説明]：イベントの説明。

[システム ログを表示する] の設定をフィルタリングまたは再配置できます。

[更新] をクリックすると画面が更新され、最新情報を表示します。

[すべてクリア] をクリックすると、ログからすべてのエントリがクリアされます。

[ダウンロード] をクリックすると、ログからすべてのエントリがダウンロードされます。

電子メール アラート/メール サーバ/メッセージ構成

電子メールアラート機能では、メール サーバの構成、メッセージ重大度の構成、および最大3個の電子メール アドレスをサポートし、緊急および緊急でない電子メール アラートを送信します。[電子メール アラート] を使用すると、特定のシステム イベントが発生したときに、設定した電子メール アドレスにメッセージを送信できます。

ヒント　個人用の電子メール アドレスは使用しないでください。使用した場合、個人用の電子メール ログイン クレデンシャルが不用意に漏洩する可能性があります。代わりに個別の電子メール アカウントを使用してください。また、多くの電子メールアカウントでは、送信されたすべてのメッセージのコピーを保持する動作がデフォルトであることにも留意してください。この電子メールアカウントにアクセスできる全員が、送信されたメッセージにアクセスできます。電子メールの設定がプライバシー ポリシーに準拠していることを確認します。

電子メール アラートを送信するように WAP デバイスを設定するには、次の手順を実行します。

ステップ 1　[通知] > [電子メール アラート] を選択します。

ステップ 2　[グローバル設定] 領域で、次のパラメータを設定します。

- [管理モード] : [有効化] をオンにして、電子メール アラート機能を有効にします。
- [送信者電子メールアドレス] : 電子メールの送信者として表示する電子メールアドレスを入力します。このアドレスは、印字可能な文字のみによる 255 文字の文字列です。デフォルトではアドレスは設定されません。
- [ログ期間] : スケジュールされたメッセージの送信頻度を分単位で入力します。30 ～ 1440 分の範囲で入力します。デフォルトは 30 分です。
- [スケジュール済みメッセージ重大度] : [ログ期間] で指定した頻度で、設定した電子メール アドレスに送信されるイベントに必要とされる重大度を、ドロップダウン リストから選択します（[緊急]、[アラート]、[クリティカル]、[エラー]、[警告]）。デフォルトの重大度は [警告] です。
- [緊急メッセージ重大度] : 設定した電子メール アドレスに即時に送信されるイベントに必要とされる重大度を、ドロップダウン リストから選択します（[緊急]、[アラート]、[クリティカル]、[エラー]、[警告]）。デフォルトの重大度は [アラート] です。

ステップ 3　[メール サーバ構成] 領域で、次のパラメータを設定します。

- [サーバの IPv4 アドレス/名前] : 送信 SMTP サーバの IP アドレスまたはホスト名を入力します。このサーバ アドレスは、有効な IPv4 アドレスまたはホスト名でなければなりません。IPv4 アドレスは、xxx.xxx.xxx.xxx（192.0.2.10）の形式にする必要があります。

  ホスト名は、最大 63 文字の英数字のセットからなる 1 つ以上のラベルで構成できます。ホスト名に複数のラベルが含まれる場合、それぞれをピリオド（.）で区切ります。一連のラベルおよびピリオドの長さは、最大 253 文字にすることができます。
- [データ暗号化] : ドロップダウン リストから送信電子メール アラートのセキュリティ モードを選択します（[オープン] または [TLSv1]）。セキュアな TLSv1 プロトコルを使用すると、パブリック ネットワークを経由した通信中の傍受および改ざんを防止できます。
- [ポート] : 送信電子メールに使用する SMTP ポート番号を入力します。範囲は 0 ～ 65535 の有効なポート番号です。デフォルト ポートは 465 です。

- [ユーザ名]：これらの電子メールの送信に使用する電子メール アカウントのユーザ名を入力します。通常（常にではない）、このユーザ名はドメインを含む完全な電子メール アドレス（例：Name@example.com）です。指定したアカウントは送信者の電子メール アドレスとして使用されます。ユーザ名は 1 ～ 64 文字の英数字で指定できます。
- [パスワード]：これらの電子メールの送信に使用する電子メール アカウントのパスワードを入力します。パスワードには 1 ～ 64 個の文字を使用できます。

ステップ 4 [メッセージ構成] 領域で、電子メール アドレスと件名を設定します。

- [宛先電子メール アドレス 1/2/3]：電子メール アラートを受信するアドレスを最大 3 個入力します。各電子メール アドレスは有効なアドレスである必要があります。
- [電子メールの件名]：電子メールの件名行に表示されるテキストを入力します。最大255 文字の英数字文字列を使用できます。

ステップ 5 [保存] をクリックします。

電子メール アラートの例

次の例は、[メール サーバの構成] のパラメータを入力する方法を示しています。

```
Gmail
Server IPv4 Address/Name = smtp.gmail.com
Data Encryption = TLSv1
Port = 465
Username = Your full email address you can use to login to your email account
associated with the above server
Password = xxxxxxxx is a valid password of your valid email account
To Email Address 1 = myemail@gmail.com

Windows Live Hotmail
Windows Live Hotmail recommends the following settings: Data Encryption: TLSv1
SMTP Server: smtp.live.com
SMTP Port: 587
Username: Your full email address, such as myName@hotmail.com or
myName@myDomain.com
Password: Your Windows Live account password

Yahoo! Mail
Yahoo requires using a paid account for this type of service. Yahoo
recommends the following settings:
Data Encryption: TLSv1
SMTP Server: plus.smtp.mail.yahoo.com
SMTP Port: 465 or 587
Username: Your email address, without the domain name such as myName (without
@yahoo.com)
Password: Your Yahoo account password
```

次の例は、一般的なログ電子メールのフォーマット例を示しています。

```
From: AP-192.168.2.10@mailserver.com
Sent: Wednesday, September 09, 2009 11:16 AM
To: administrator@mailserver.com
Subject: log message from AP
```

```
TIME          Priority > Process Id > > > Message
Sep 8 03:48:25 info >> login[1457]> > > root login on ttyp0
Sep 8 03:48:26 info >> mini_http-ssl[1175]>Max concurrent connections of 20
reached
```

ユーザ アカウント

デフォルトでは、1 人の管理ユーザが WAP デバイスに設定されています。

- ユーザ名：**cisco**
- パスワード：**cisco**

[ユーザ アカウント] ページを使用すると、最大 4 人の追加ユーザを設定したり、ユーザ パスワードを変更したりできます。

ユーザの追加

新しいユーザを追加するには、次の設定を行います。

ステップ 1 [システム設定] > [ユーザ アカウント] を選択します。

[ユーザ アカウント] テーブルに現在設定されているユーザが表示されます。ユーザ cisco は事前にシステムに設定されており、読み取り/書き込み権限を持っています。

その他のすべてのユーザは読み取り専用アクセス権を持つことはできますが、読み取り/書き込みアクセス権を持つことはできません。

ステップ 2 [□] をクリックして新しい行を追加します。

ステップ 3 新しいユーザのボックスをオンにし、そのユーザの名前を入力します。

ステップ 4 [新しいパスワード] に 0 ～ 127 文字のパスワードを入力してから、[新しいパスワードの確認] フィールドに同じパスワードを入力します。

パスワードの強度が [パスワード強度メーター] フィールドに次のように示されます。

- **赤**：パスワードは複雑さの最小要件を満たしていません。
- **オレンジ**：パスワードは複雑さの最小要件を満たしていますが、パスワードの強度は脆弱です。
- **グリーン**：パスワードは堅牢です。

ステップ 5 [保存] をクリックします。

（注） ユーザを削除するには、ユーザ名を選択して [削除] をクリックします。既存のユーザを編集するには、ユーザ名を選択して [編集] をクリックし、[保存] をクリックして設定の変更内容をすべて保存します。

ユーザ パスワードの変更

ユーザ パスワードを変更するには、次の手順を実行してください。

ステップ 1 [システム設定] > [ユーザ アカウント] を選択します。

[ユーザ アカウント] テーブルに現在設定されているユーザが表示されます。ユーザ cisco は読み取り/書き込み権限を持つようにシステムに事前設定されています。ユーザ cisco のパスワードは変更できます。

ステップ 2 設定するユーザを選択し、[編集] をクリックします。

ステップ 3 [新しいパスワード] に 0 ～ 127 文字の新しいパスワードを入力してから、[新しいパスワードの確認] フィールドに同じパスワードを入力します。

パスワードの強度が [パスワード強度メーター] に次のように示されます。

- **赤**：パスワードは複雑さの最小要件を満たしていません。
- **オレンジ**：パスワードは複雑さの最小要件を満たしていますが、パスワードの強度は脆弱です。
- **グリーン**：パスワードは堅牢です。

ステップ 4 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

（注） パスワードを変更する場合は、システムにログインし直す必要があります。

管理

[システム設定] ページを使用して、ネットワーク内で WAP デバイスを識別する情報を設定します。

システム設定を指定するには、次の手順を実行してください。

ステップ 1 [システム設定] > [管理] の順に選択します。

ステップ 2 次のパラメータを設定します。

- [ホスト名]：WAP デバイスのホスト名を入力します。デフォルトでは、この名前はノードの完全修飾ドメイン名（FQDN）になります。デフォルト ホスト名は wap と、WAP デバイスの MAC アドレスの 16 進数値の末尾 6 桁を結合した文字列です。ホスト名ラベルに含めることができるのは、文字、数字、およびハイフンのみです。先頭や末尾にハイフンを使用することはできません。また、その他の記号、句読文字、スペースは使用できません。許可されるホスト名の長さは 1 ～ 63 文字です。
- [システム コンタクト先]：WAP デバイスの連絡担当者を入力します。[システムの連絡先] は 0 ～ 255 文字の長さで、スペースおよび特殊文字を含めることができます。

- [システムの場所]：WAP デバイスの物理的な場所を入力します。[システムの場所] は 0 ～ 255 文字の長さで、スペースおよび特殊文字を含めることができます。

ステップ 3 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

接続セッションの設定/HTTP/HTTPS サービス タスク

[HTTP/HTTPS サービス]ページは、Web ベースの管理接続の有効化と設定に使用します。HTTPS を使用して管理セッションを保護する場合は、このページを使用して必要な SSL 証明書を管理することもできます。

HTTP サービスおよび HTTPS サービスを設定するには、次の手順を実行します。

ステップ 1 [システム設定] > [管理] を選択します。

ステップ 2 [グローバル設定] 領域で、次のパラメータを設定します。

- [最大セッション数]：HTTP と HTTPS の両方を含む、同時に使用できる Web セッションの数を入力します。

  ユーザが WAP デバイスの設定ユーティリティにログオンすると、セッションが作成されます。このセッションは、ユーザがログオフするか、セッション タイムアウトが満了するまで維持されます。範囲は 1 ～ 10 セッションです。デフォルトは 5 です。最大セッション数に到達すると、設定ユーティリティへのログオンを次に試行したユーザには、セッション制限に関するエラー メッセージが表示されます。

- [セッション タイムアウト]：非アクティブなユーザがログオン状態を維持できる最大時間を分単位で入力します。設定されているタイムアウトに到達すると、ユーザは自動でログオフされます。範囲は 2 ～ 60 分です。デフォルトは 10 分です。

ステップ 3 HTTP サービスおよび HTTPS サービスを設定します。

- [HTTP サービス]：HTTP を介したアクセスを有効または無効にします。デフォルトでは、HTTP アクセスは無効になっています。無効にすると、このプロトコルを使用している現在の接続はすべて切断されます。
  - [HTTP ポート]：HTTP 接続に使用する 1025 ～ 65535 の論理ポート番号を入力します。HTTP 接続のデフォルト ポート番号は IANA のウェルノウン ポート番号 80 です。
  - [HTTP を HTTPS にリダイレクト]：HTTP ポートでの管理 HTTP アクセス試行を HTTPS ポートにリダイレクトします。このフィールドは HTTP アクセスが無効化されている場合のみ使用可能です。
- [HTTPS サービス]：セキュアな HTTP（HTTPS）を介したアクセスを有効または無効にします。デフォルトでは、HTTPS アクセスは有効です。無効にすると、このプロトコルを使用している現在の接続はすべて切断されます。

- [HTTPS ポート]：HTTPS 接続に使用する 1025 ～ 65535 の論理ポート番号を入力します。HTTPS 接続のデフォルト ポート番号は IANA のポート番号 443 です。

- [管理 ACL モード]：このモードが有効な場合、Web および SNMP を通じたアクセスは、指定された IP ホストに制限されます。この機能が無効化されている場合は、WAP デバイスの正しいユーザ名およびパスワードを入力することにより、誰もが任意のネットワーク クライアントから設定ユーティリティにアクセスできます。

（注） 入力するすべての IP アドレスを検証します。管理コンピュータと一致しない IP アドレスを入力した場合は、コンフィギュレーション インターフェイスへのアクセスを失うことになります。管理コンピュータには静的 IP アドレスを割り当てて、アドレスが経時的に変更されないようにすることをお勧めします。

ステップ 4 [保存] をクリックします。

SSL 証明書ファイルのステータス

HTTPS サービスを使用するには、WAP デバイスに有効な SSL 証明書が必要です。WAP デバイスで証明書を生成することができます。また、ネットワークまたは TFTP サーバから証明書をダウンロードすることもできます。

[SSL 証明書の生成] 領域で、[SSL 設定] をクリックし、次に [生成] をクリックして WAP デバイスの証明書を生成します。WAP デバイスが IP アドレスを取得した後でこの操作を実行することにより、証明書の共通名と WAP デバイスの IP アドレスが確実に一致するようにする必要があります。新しい SSL 証明書を生成すると、セキュア Web サーバが再起動します。セキュア接続は、新しい証明書がブラウザで受け入れられるまで機能しません。

[SSL 証明書ファイルのステータス] 領域で、WAP デバイス上の現在の証明書を参照できます。次の情報が表示されます。

- 証明書ファイルあり
- 証明書の失効日
- 証明書発行者の共通名

SSL 証明書（拡張子 .pem）が WAP デバイスに存在している場合は、コンピュータにダウンロードしてバックアップにすることができます。[SSL 証明書の転送元（デバイスから PC へ）] 領域でダウンロード オプションとして [HTTP/HTTPS] または [TFTP] を選択し、[転送] をクリックします。

- [HTTP/HTTPS] を選択した場合は、ダウンロードを確認してから、ネットワーク上のファイルを保存する場所を参照して指定します。
- [TFTP] を選択した場合は、ダウンロードしたファイルに割り当てる [ファイル名] を入力し、ファイルのダウンロード場所となる TFTP サーバの IPv4 アドレスを入力します。

ご使用のコンピュータから WAP デバイスに証明書ファイル（拡張子 .pem）をアップロードすることもできます。[SSL 証明書の転送元（PC からデバイスへ）] 領域でアップロードオプションとして [HTTP/HTTPS] または [TFTP] を選択し、[転送] をクリックします。

- HTTP/HTTPS の場合は、ネットワークの場所を参照し、ファイルを選択して [転送] をクリックします。
- TFTP の場合は [ファイル名] および [TFTP サーバの IPv4 アドレス] を入力してから [転送] をクリックします。ファイル名に、スペース、<、>、|、\、:、(、)、&、;、#、?aszxaa、* および複数の連続するピリオドを使用することはできません。

アップロードが成功すると確認メッセージが表示されます。

SNMP/SNMPv2c の設定

SNMP は、ネットワーク デバイスに関する情報の記録、保存、および共有の標準を定義します。また、ネットワーク管理、トラブルシューティング、および保守を容易にします。WAP は SNMP に対応しており、ネットワーク管理システムへのシームレスな統合のために SNMP 管理対象デバイスとして機能できます。

[SNMP/SNMPv2c 設定] ページを使用して SNMP を有効にしたり、基本的なプロトコル設定を行ったりします。

SNMP の全般設定を行うには

ステップ 1 [管理] > [SNMP 設定] の順に選択します。

ステップ 2 [有効化] をオンにし、SNMP を有効にします。

ステップ 3 SNMP トラフィックの UDP ポートを入力します。デフォルトは 161 です。ただし、エージェントが別のポートの要求をリッスンするように設定できます。有効な範囲は 1025 ～ 65535 です。

ステップ 4 [SNMPv2c 設定] 領域で SNMPv2c の設定を行います。

- [読み取り専用コミュニティ] : SNMPv2 アクセス用の読み取り専用コミュニティの名前を入力します。有効な範囲は、1 ～ 256 文字の英数字と特殊文字です。

  コミュニティ名は、SNMP エージェントからのデータを要求できるネットワーク上のデバイスを制限するための単純な認証機能としての役割を果たします。名前はパスワードとして機能します。送信者がパスワードを知っている場合に、要求は信頼できるものとみなされます。

- [読み取り/書き込みコミュニティ] : SNMP SET 要求に使用される読み書きコミュニティ名を入力します。有効な範囲は、1 ～ 256 文字の英数字と特殊文字です。コミュニティ名の設定は、パスワードの設定と同じです。このコミュニティ名と同じ名前のマシンからの要求のみが許可されます。

- [管理ステーション] : SNMP で WAP デバイスにアクセスできるステーションを決定します。次のオプションのいずれかを選択します。

  - [すべて] : すべてのステーションが SNMP で WAP デバイスにアクセスできます。
  - [ユーザ定義] : 許可されているユーザ定義 SNMP 要求のセット。

- [NMS IPv4 アドレス/名前]：ネットワーク管理システム（NMS）の IPv4 IP アドレス、DNS ホスト名、またはサブネットを入力します。

  DNS ホスト名は、最大 63 文字の英数字のセットからなる 1 つ以上のラベルで構成できます。ホスト名に複数のラベルが含まれる場合、それぞれをピリオド（.）で区切ります。一連のラベルおよびピリオドの長さは、最大 253 文字にすることができます。

  コミュニティ名と同様に、この設定で SNMP 設定にある程度のセキュリティが提供されます。SNMP エージェントは、ここに指定した IP アドレス、ホスト名、またはサブネットからの要求のみを受け入れます。

  サブネットを指定するには、アドレス/マスク長の形式で 1 つ以上のサブネットワーク アドレス範囲を入力します。このアドレスは IP アドレス、マスク長はマスク ビット数です。アドレス/マスクおよびアドレス/マスク長の両方の形式がサポートされます。たとえば、192.168.1.0/24 の範囲を入力すると、アドレスが 192.168.1.0 でサブネットマスクが 255.255.255.0 のサブネットワークを指定します。

- [NMS IPv6 アドレス/名前]：管理対象デバイスに GET 要求および SET 要求を実行できるデバイスの IPv6 IP アドレス、DNS ホスト名、またはサブネット。IPv6 アドレスは、xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx（2001:DB8::CAD5:7D91）の形式にする必要があります。

（注） ホスト名は、最大 63 文字の英数字のセットからなる 1 つ以上のラベルで構成できます。ホスト名に複数のラベルが含まれる場合、それぞれをピリオド（.）で区切ります。一連のラベルおよびピリオドの長さは、最大 253 文字にすることができます。

ステップ 5 [SNMPv2c トラップ設定] 領域で SNMPv2c トラップの設定を行います。

- [トラップ コミュニティ]：SNMP トラップに関連付けられるグローバルなコミュニティ文字列を入力します。デバイスから送信されたトラップは、コミュニティ名としてこの文字列を提供します。有効な範囲は、1 ～ 60 文字の英数字と特殊文字です。

- [トラップ宛先テーブル]：SNMP トラップを受信する最大 3 つの IP アドレスまたはホスト名のリストを入力します。このボックスをオンにして [ホスト IP アドレス タイプ]（IPv4 または IPv6）を選択してから、[ホスト名/IP アドレス] を追加します。

  DNS ホスト名の例は、snmptraps.foo.com です。SNMP トラップは SNMP エージェントからランダムに送信されるため、トラップの送信先を正確に指定することは重要です。最大 3 つの DNS ホスト名を指定できます。必ず [有効] をオンにしてから適切なホスト IP アドレスの種類を選択してください。

ステップ 6 [保存] をクリックします。

SNMPv3 ビュー

SNMP MIB ビューは、MIB 階層のビュー サブツリーのファミリです。ビュー サブツリーは、Object Identifier（OID; オブジェクト ID）サブツリーの値とビット文字列のマスク値のペアリングによって識別されます。各 MIB ビューは、MIB ビューに含まれるものまたは MIB ビューから除外されるものの 2 セットのビュー サブツリーで定義されます。MIB ビュー を作成して、SNMPv3 ユーザがアクセスできる OID 範囲を制御できます。

WAP デバイスは、最大 16 個のビューをサポートします。

ここでは、SNMPv3 ビュー設定に関する重要なガイドラインをまとめています。すべての注意を読んでから先に進んでください。

（注） 「すべて」が付く MIB ビューは、システムでデフォルトで作成されています。このビューには、システムでサポートされるすべての管理オブジェクトが含まれます。

（注） デフォルトでは、「ビュー - すべて」および「ビュー - なし」の SNMPv3 ビューは WAP デバイスで作成されます。これらのビューを削除したり変更したりすることはできません。

SNMP ビューを追加および設定するには、次の手順を実行します。

ステップ 1 **[管理]** > **[SNMPv3]** の順に選択します。

ステップ 2 [□] をクリックして [SNMPv3 ビュー] テーブルに新しい行を作成するか、既存のビューのチェックボックスをオンにしてから、[編集] をクリックします。

- [ビュー名]：MIB ビューを識別する名前を入力します。ビュー名には最大で 32 文字の英数字を含めることができます。
- [タイプ]：ビューのサブツリーまたはサブツリーのファミリを MIB ビューに含めるか、MIB ビューから除外するかを選択します。
- [OID]：ビューに含めるまたはビューから除外するサブツリーの OID 文字列を入力します。たとえば、システムのサブツリーは OID string.1.3.6.1.2.1.1 で指定されます。
- [マスク]：OID マスクを入力します。マスクの長さは 47 文字です。OID マスクの形式は、xx.xx.xx (.)... または xx:xx:xx....(:) で、長さは 16 オクテットです。各オクテットは、ピリオド（.）またはコロン（:）のいずれかで区切られた 2 つの 16 進数文字です。このフィールドには、16 進数文字のみを使用できます。たとえば、OID マスク FA.80 は、11111010.10000000 です。

ファミリ マスクは、ビュー サブツリーのファミリの定義に使用されます。ファミリ マスクは、関連するファミリ OID 文字列のサブ ID がファミリの定義に有効なことを示します。ビュー サブツリーのファミリによって、表内の 1 行に対して効果的なコントロール アクセスが可能になります。

ステップ 3 [保存] をクリックします。

（注） ビューを削除するには、リストでビューをオンにし、[削除] をクリックします。

SNMPv3 グループ

SNMPv3 グループによって、さまざまな認証およびアクセス権限のグループにユーザをまとめることができます。各グループは、次の 3 つのセキュリティ レベルのいずれかに関連付けられます。

- noAuthNoPriv
- authNoPriv
- authPriv

各グループの MIB へのアクセスは、MIB ビューを読み取りまたは書き込みアクセス用のグループに別々に関連付けることによって制御されます。

デフォルトでは、WAP デバイスには次の 2 つのグループがあります。

- **RO**：認証およびデータ暗号化を使用する読み取り専用グループ。このグループのユーザは、認証に SHA キーまたはパスワードを使用し、暗号化に DES または AES128 を使用します。SHA、DES、および AES128 キーまたはパスワードを定義する必要があります。デフォルトで、このグループのユーザには、デフォルトのすべての MIB ビューに対する読み取りアクセス権があります。
- **RW**：認証およびデータ暗号化を使用する読み取り/書き込みグループ。このグループのユーザは、認証に SHA キーまたはパスワードを使用し、暗号化に DES キーまたは AES128 を使用します。SHA、DES、および AES128 キーまたはパスワードを定義する必要があります。デフォルトで、このグループのユーザには、デフォルトのすべての MIB ビューに対する読み取りおよび書き込みアクセス権があります。

（注） デフォルト グループの RO および RW を削除することはできません。WAP デバイスは、最大 8 個のグループをサポートします。

SNMP グループを追加して設定するには、次の手順に従います。

ステップ 1 [管理] > [SNMPv3] の順に選択します。

ステップ 2 [□] をクリックして SNMPv3 グループ テーブルに新しい行を追加します。

ステップ 3 新しいグループのボックスを選択して、次のパラメータを設定します。

- [グループ名]：グループの名前を入力します。デフォルトのグループ名は RO および RW です。グループ名には最大で 32 文字の英数字を含めることができます。
- [セキュリティ レベル]：グループのセキュリティ レベルとして次のオプションから選択します。
  - [noAuthNoPriv]：認証なし、データ暗号化なし（セキュリティなし）。

- [authNoPriv]：認証あり、データ暗号化なし。ユーザはこのセキュリティ レベルでは、認証に SHA キーまたはパスワードを使用する一方、DES キーや AES128 で暗号化しない SNMP メッセージを送信します。
- [authPriv]：認証およびデータ暗号化あり。ユーザはこのセキュリティ レベルでは、認証用に SHA キーまたはパスワードを送信し、暗号化用に DES または AES128 を送信します。認証、暗号化、またはこの両方が必要なグループでは、[SNMP ユーザ] ページで SHA キー、DES キー、および AES128 キーまたはパスワードを定義する必要があります。

- [書き込みビュー]：グループの MIB への書き込みアクセス権限として次のオプションのいずれかを選択します。
  - [ビュー - すべて]：グループは、MIB を作成、変更、および削除できます。
  - [ビュー - なし]：グループは、MIB を作成、変更、削除できません。
- [読み取りビュー]：グループの MIB への読み取りアクセス権限として次のオプションのいずれかを選択します。
  - [ビュー - すべて]：グループは、すべての MIB を表示し、読み取ることができます。
  - [ビュー - なし]：グループは MIB を表示したり読み取ったりできません。

ステップ 4 [保存] をクリックして SNMPv3 グループ リストにグループを追加します。

（注） グループを削除するには、リストでグループをオンにして [削除] を選択します。グループを編集するには、リストでグループをオンにして [編集] を選択します。

SNMPv3 ユーザ

[SNMPユーザ]ページを使用して、ユーザを定義したり、セキュリティ レベルを各ユーザに関連付けたり、ユーザごとにセキュリティ キーを設定したりできます。

各ユーザは、定義済みグループまたはユーザ定義グループのいずれかから SNMPv3 グループにマップされ、オプションで認証および暗号化が設定されます。認証では、SHA タイプのみがサポートされます。暗号化では、DES および AES128 タイプのみがサポートされます。WAP デバイスにデフォルトの SNMPv3 ユーザが存在しない場合は、最大 8 つのユーザを追加できます。

SNMP ユーザを追加するには、次の手順に従います。

ステップ 1 [管理] > [SNMPv3] の順に選択します。

ステップ 2 [□] をクリックして SNMPv3 ユーザ テーブルに新しい行を追加します。

ステップ 3 新しい行のボックスをオンにして、次のパラメータを設定します。

- [ユーザ名]：SNMPv3 ユーザを識別する名前を入力します。ユーザ名には最大で 32 文字の英数字を含めることができます。
- [グループ]：ユーザのマップ先であるグループの名前を入力します。デフォルト グループは RW および RO です。[SNMP グループ] ページで追加グループを定義できます。
- [認証の種類]：ユーザからの SNMPv3 要求に使用する認証タイプを、次のオプションから選択します。
  - [SHA]：ユーザからの SNMP 要求に SHA 認証が必要です。
  - [なし]：このユーザからの SNMPv3 要求に認証は必要ありません。
- [認証パス フレーズ]：認証の種類に SHA を指定した場合、ユーザから送信される要求を SNMP エージェントが認証できるようにするためのパス フレーズを入力します。パス フレーズの長さは 8 ～ 32 文字にする必要があります。
- [暗号化タイプ]：ユーザの SNMP 要求に適用される暗号化/プライバシー タイプを、次のオプションから選択します。
  - [DES]：ユーザからの SNMPv3 要求に DES 暗号化を使用します。
  - [AES128]：ユーザからの SNMPv3 要求に AES128 暗号化を使用します。
  - [なし]：このユーザ からの SNMPv3 要求にプライバシーは必要ありません。
- [暗号化パス フレーズ]：暗号化タイプとして DES または AES128 を指定した場合、SNMP 要求の暗号化に使用するパス フレーズを入力します。パス フレーズの長さは 8 ～ 32 文字にする必要があります。

ステップ 4 [保存] をクリックします。ユーザが [SNMPv3 ユーザ] リストに追加され、変更がスタートアップ コンフィギュレーションに保存されます。

（注） ユーザを削除するには、リストでユーザを選択して [削除] を選択します。ユーザを編集するには、リストでユーザを選択して [編集] を選択します。

SNMPv3 ターゲット

SNMPv3 ターゲットは、Inform メッセージを使用して SNMP 通知を SNMP マネージャに送信します。SNMPv3 ターゲットでは、Inform のみが送信され、トラップは送信されません。SNMP バージョン 1 および 2 では、トラップが送信されます。各ターゲットは、ターゲット IP アドレス、UDP ポート、および SNMPv3 ユーザ名で定義されます。

（注） SNMPv3 ユーザ設定（[SNMPv3 ユーザ] ページを参照）を完了してから、SNMPv3 ターゲットを設定する必要があります。

WAP デバイスは、最大 8 個のターゲットをサポートします。

SNMP ターゲットを追加するには、次の手順に従います。

ステップ 1 [管理] > [SNMPv3 ターゲット] の順に選択します。

ステップ 2 [□] をクリックしてテーブルに新しい行を追加します。

ステップ 3 新しい行のチェックボックスをオンにして、次のパラメータを設定します。

- [IP アドレス] : ターゲットを受信するリモート SNMP マネージャの IPv4 アドレスまたは IPv6 アドレスを入力します。
- [UDP ポート] : SNMPv3 ターゲットの送信に使用する UDP ポートを入力します。
- [ユーザ] : ターゲットと関連付ける SNMP ユーザの名前を入力します。SNMP ユーザを設定するには、[SNMPv3 ユーザ （36 ページ）] ページを参照してください。

ステップ 4 [保存] をクリックします。ユーザが [SNMPv3 ターゲット] リストに追加され、変更がスタートアップ コンフィギュレーションに保存されます。

（注） SNMP ターゲットを削除するには、リストでユーザを選択して [削除] を選択します。SNMP ターゲットを編集するには、リストでユーザを選択して [編集] を選択します。

セキュリティ

ここでは、WAP デバイスのセキュリティを設定する方法について説明します。

Radius サーバ

複数の機能で、RADIUS 認証サーバと通信する必要があります。たとえば、AP の仮想アクセスポイント（VAP）を設定すると、ワイヤレスクライアントアクセスを制御するセキュリティ方法を設定できます。詳細については、「無線」を参照してください。WPA エンタープライズ セキュリティ方式では、外部の RADIUS サーバを使用してクライアントを認証します。クライアントアクセスがリストに限定されている場合、RADIUS サーバを使用してアクセスを制御するように MAC アドレス フィルタリング機能を設定することもできます。キャプティブ ポータル機能もクライアントの認証に RADIUS を使用します。

[RADIUS サーバ] ページを使用して、これらの機能で使用する RADIUS サーバを設定できます。グローバルに使用可能な IPv4 または IPv6 RADIUS サーバを最大 4 つ設定できます。ただし、グローバル サーバに対して RADIUS クライアントが IPv4 または IPv6 モードのどちらで動作するのかを選択する必要があります。1 台のサーバは必ずプライマリとして機能し、その他はバックアップ サーバとして機能します。

（注） グローバル RADIUS サーバを使用する以外に、特定の RADIUS サーバ セットを使用するように各 VAP を設定することもできます。「ネットワーク」を参照してください。

グローバル RADIUS サーバの設定

ステップ 1 **[セキュリティ]** > **[RADIUS サーバ]** の順に選択します。

ステップ 2 次のパラメータを設定します。

- [サーバの IP アドレスの種類]：RADIUS サーバが使用する IP のバージョンを選択します。IPv4 と IPv6 のグローバル RADIUS アドレス設定を設定するアドレス タイプを切り替えることができますが、WAP デバイスは RADIUS サーバまたはこのフィールドで選択したアドレス タイプのサーバとのみコンタクトできます。
- [サーバ IP アドレス - 1] または [サーバ IPv6 アドレス - 1]：プライマリ グローバル RADIUS サーバのアドレスを入力します。最初のワイヤレス クライアントが WAP デバイスで認証しようとすると、その WAP デバイスはプライマリ サーバに認証要求を送信します。プライマリ サーバが認証要求に応答する場合、WAP デバイスは引き続きこの RADIUS サーバをプライマリ サーバとして使用し、認証要求は指定アドレスに送信されます。
- [サーバの IP アドレス - 2] または [サーバの IPv6 アドレス - 2]：バックアップ IPv4 または IPv6 RADIUS サーバのアドレスを入力します。プライマリ サーバでの認証に失敗した場合、設定されているバックアップ サーバが試行されます。
- [キー 1]：WAP デバイスが認証のためにプライマリ RADIUS サーバに対して使用する共有秘密キーを入力します。1 ～ 64 文字の標準的な英数字と特殊文字を使用できます。キーは大文字と小文字が区別され、RADIUS サーバで設定されたキーと一致している必要があります。入力したテキストは、アスタリスクで表示されます。
- [キー - 2]：設定されたバックアップ RADIUS サーバに関連付けられている RADIUS キー。サーバ IP（IPv6）アドレス 2 のサーバはキー 2 を使用します。
- [RADIUS アカウンティングの有効化]：特定のユーザが消費したリソース（システム時刻や送受信されたデータ量など）の追跡および測定を可能にします。RADIUS アカウンティングを有効にすると、プライマリ RADIUS サーバとすべてのバックアップ サーバに対して有効になります。

ステップ 3 [保存] をクリックします。

802.1x サプリカント

IEEE 802.1X 認証によって、WAP デバイスは安全な有線ネットワークにアクセスできるようになります。WAP デバイスを有線ネットワーク上で 802.1X サプリカント（クライアント）とし

て有効化できます。WAP デバイスが 802.1X を使用して認証できるように、MD5 アルゴリズムを使用して暗号化されたユーザ名とパスワードを設定できます。

IEEE 802.1X ポートベースのネットワーク アクセス制御を使用するネットワークでは、802.1X オーセンティケータがアクセスを許可するまでサプリカントはネットワークにアクセスできません。ネットワークで 802.1X が使用されている場合は、オーセンティケータに提供できるように、WAP デバイスで 802.1X 認証情報を設定する必要があります。

802.1X サプリカントを設定するには、次の手順を実行します。

ステップ 1 [セキュリティ] > [802.1X サプリカント] をクリックします。

ステップ 2 [802.1x サプリカント] 領域で [有効化] をオンにして管理モードを有効にします。

ステップ 3 802.1X 動作ステータスと基本設定を次のように設定します。

- [EAP 方法]：認証ユーザ名とパスワードの暗号化に使用するアルゴリズムを選択します。次のオプションが用意されています。
  - [MD5]：基本的なセキュリティを提供する RFC 3748 で定義されているハッシュ関数。
  - [PEAP]：Protected Extensible Authentication Protocol（PEAP; 保護された拡張認証プロトコル）。TLS トンネル内で暗号化することで、MD5 よりも高いレベルのセキュリティを提供します。
  - [TLS]：Transport Layer Security。RFC 5216 で定義されているように、高レベルのセキュリティを提供するオープン標準です。
- [ユーザ名]：ユーザ名を入力します。
- [パスワード]：パスワードを入力します。

ステップ 4 [証明書ファイルのアップロード] 領域で、WAP デバイスに証明書ファイルをアップロードできます。

a) 転送方法として [HTTP] または [TFTP] のいずれかを選択します。
b) [HTTP] を選択した場合は、[参照] をクリックしてファイルを選択します。HTTP サーバ設定について詳しくは、「接続セッションの設定/HTTP/HTTPS サービス タスク」を参照してください。
c) [TFTP] を選択した場合は、ファイル名と TFTP サーバの IPv4 アドレスを入力します。
d) [アップロード]をクリックします。確認ウィンドウが表示され、経過表示バーでアップロードのステータスが示されます。

ステップ 5 [保存] をクリックします。

不正 AP 検出

不正 AP は、システム管理者からの明示的な許可なく安全なネットワーク上にインストールされているアクセス ポイントです。この施設にアクセスできる誰かが意図せずに、または悪意を持って安価なワイヤレス WAP デバイスをインストールすることにより、権限のない関係者がネットワークにアクセスできる可能性があるため、不正 AP はセキュリティ上の脅威をもたらします。

WAPデバイスは、ネットワークの近くにあるすべてのAPを検出するため、すべてのチャネルでRFスキャンを実行します。不正APが検出された場合、[不正AP検出]ページに表示されます。不正としてリストされているAPが正当なものである場合、それを[既知のAPリスト]に追加することができます。

（注） [検出された不正APリスト]および[信頼できるAPリスト]が情報を提供します。APはそのリスト上のAPを制御することはできず、またRFスキャンによって検出されたAPにセキュリティポリシーを適用することはできません。

不正AP検出を有効にすると、無線は定期的に動作チャネルから同じ帯域内の他のチャネルのスキャンに切り替えます。

不正 AP リストの表示

不正AP検出が機能するためには、ワイヤレス無線が有効になっている必要があります。無線インターフェイスの不正AP検出を有効にする前に、まず無線インターフェイスを有効に必要があります。

無線を有効にして、不正APに関する情報を収集するには、次の手順を実行します。

ステップ1 [セキュリティ]>[不正AP検出]の順に選択します。

ステップ2 [AP検出（無線1）]フィールドと[AP検出（無線2）]フィールドの横にある[有効化]をオンにします。

ステップ3 [保存]をクリックします。

[検出された不正APリスト]テーブルに、検出されたすべての不正APが表示されます。[信頼APリスト]には信頼されているすべてのAPが表示されます。不正APリストごとに次の設定が表示されます。

- [MACアドレス]：不正APのMACアドレス。
- [ビーコンの間隔]：不正APで使用されるビーコンの間隔。APはワイヤレスネットワークの存在を知らせるため、ビーコンフレームを通常の間隔で送信します。デフォルトの動作は、ビーコンフレームを100ミリ秒ごとに（または1秒間に10回）送信します。ビーコン間隔は、[無線（47ページ）]ページで設定します。
- [タイプ]：デバイスのタイプ。次のオプションが用意されています。
  - [AP]：インフラストラクチャモードでIEEE 802.11ワイヤレスネットワーキングフレームワークをサポートするAP不正デバイス。
  - [アドホック]：アドホックモードで実行されている不正ステーション。アドホックモードはIEEE802.11ワイヤレスネットワーキングフレームワークの1つで、ピアツーピアモードまたは独立基本サービスセット（IBSS）とも呼ばれます。
- [SSID]：WAPデバイスのService Set Identifier（SSID）。

- [プライバシー]：不正デバイスにセキュリティが設定されているかどうかを示します。次のオプションが用意されています。
  - [オフ]：セキュリティ モードはオフです（セキュリティなし）。
  - [オン]：セキュリティ モードはオンです。
- [WPA]：WPA セキュリティがその不正 AP に対してオンかオフかを示します。
- [バンド]：不正 AP で使用されている IEEE 802.11a、IEEE 802.11b、IEEE 802.11g などの IEEE 802.11 モード。

  ここに表示される数字がモードを示します。
  - 2.4 は IEEE 802.11b、802.11g、または 802.11n モード（またはこれらのモードの組み合わせ）を示します。
  - 5 は IEEE 802.11a または 802.11n モード（あるいはその両方）を示します。
- [チャネル]：不正 AP が現在ブロードキャストしているチャネル。
- [レート]：不正 AP が現在送信しているレート（メガビット/秒）。現在のレートは、常に、[サポートされるレート] フィールドに表示されるレートのいずれかです。
- [信号]：不正APが発する無線信号の強度。マウスのカーソルをバーに重ねると、強度を示す数字（デシベル）が表示されます。
- [ビーコン]：不正 AP が最初に検出された時点以降に、この AP から受信したビーコンの合計数。
- [最終ビーコン]：不正 AP から受信した最後のビーコンの日付と時間。
- [レート]：不正APでサポートされているレートと基本（アドバタイズされた）レートのセット。レートはメガビット/秒（Mbps）で表示されます。すべてのサポートされるレートがリストされ、基本レートが太字で表示されます。レート セットは [無線 （47 ページ）] ページで設定します。

ステップ 4 AP を [信頼 AP リスト] に移動するには、[AP リスト] をオンにして [信頼 AP リストに移動] をクリックします。AP が [信頼 AP リスト] にあり、その AP を [検出された不正 AP リスト] に移動するには、[検出された不正 AP リスト] をクリックします。

ステップ 5 [更新] をクリックすると画面が更新され、最新情報が表示されます。

信頼 AP リストの保存

信頼 AP リストを作成し、ファイルに保存するには、次の手順を実行します。

ステップ 1 [セキュリティ] を選択し、[不正 AP 検出] セクションで [不正 AP リストの表示...] をクリックします。[不正 AP 検出] ページが表示されます。

ステップ 2 [検出された不正 AP リスト] で、既知の AP の [信頼 AP リストに移動] をクリックします。信頼 AP が [信頼 AP リスト] に移動します。

ステップ 3 [信頼 AP リストのダウンロード/バックアップ] 領域で、[バックアップ（AP から PC）] を選択します。

ステップ 4 [保存] をクリックします。

リストには、[既知の AP リスト] に追加されたすべての AP の MAC アドレスが含まれます。デフォルトでは、ファイル名は Rogue2.cfg です。テキスト エディタまたは Web ブラウザを使ってファイルを開き、コンテンツを表示することができます。

信頼できる AP リストのインポート

保存されたリストから既知の AP リストをインポートできます。このリストは、別の AP から取得したり、またはテキスト ファイルから作成したりできます。AP の MAC アドレスが [信頼できる AP リスト] に表示される場合、それは不正として検出されていません。

AP リストをファイルからインポートするには、次の手順を実行します。

ステップ 1 [セキュリティ] > [不正 AP 検出] の順に選択します。

ステップ 2 [信頼 AP リストのダウンロード/バックアップ] 領域で、[ダウンロード（PC から AP）] を選択します。

ステップ 3 [送信元ファイル名] フィールドで [参照] をクリックし、インポートするファイルを選択します。

インポートするファイルは、.txt または .cfg 拡張子のプレーンテキスト ファイルでなければなりません。ファイルのエントリは、コロンで区切られた各オクテットの 16 進数表記の MAC アドレスです（例：00:11:22:33:44:55）。エントリはシングル スペースで分割する必要があります。AP がファイルを受け入れるためには、MAC アドレスのみを含める必要があります。

ステップ 4 [ファイル管理先] フィールドで、既存の [信頼 AP リスト] を置き換えるか、インポートしたファイルのエントリを [信頼 AP リスト] に追加するかを選択します。次のオプションが用意されています。

- [置換]：リストをインポートし、[既知の AP リスト] のコンテンツを置き換えます。
- [マージ]：リストをインポートし、インポートしたファイルの AP を現在 [既知の AP リスト] に表示されている AP に追加します。

ステップ 5 [保存] をクリックします。

インポートが完了したら、画面が更新され、インポートしたファイルの AP の MAC アドレスが [既知の AP リスト] に表示されます。

パスワード複雑性の設定

[パスワードの複雑性] ページを使用して、設定ユーティリティへのアクセスに使用するパスワードの複雑性の要件を変更します。パスワードを複雑にするとセキュリティが向上します。

パスワード複雑性の要件を設定するには、次の手順に従います。

ステップ 1 [セキュリティ] > [パスワード複雑性の設定] を選択します。

ステップ 2 [有効化] をオンにし、パスワード複雑性を有効にします。

ステップ 3 次のパラメータを設定します。

- [パスワード最小文字クラス] : パスワード文字列で表す必要がある文字クラスの最小数を入力します。使用可能な4つの文字クラスは、大文字、小文字、数字、標準キーボードで使用可能な特殊文字です。
- [現在と異なるパスワード] : 現在のパスワードの有効期限が切れたときに、ユーザに別のパスワードの入力を求める場合はオンにします。オンにしないと、有効期限が切れたときに同じパスワードを再入力できます。
- [最大パスワード長] : パスワード文字数の最大長は、64 ～ 127 の範囲です。デフォルトは 64 です。
- [最小パスワード長] : パスワード文字数の最小長は、0 ～ 32 の範囲です。デフォルトは 8 です。
- [パスワードのエージングのサポート] : 設定した期間が経過した後にパスワードの有効期限が切れるようにするには、これをオンにします。
- [パスワードのエージング タイム] : 新しく作成したパスワードの有効期限が切れるまでの日数（1 ～ 365）を入力します。デフォルトは 180 日です。

ステップ 4 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

（注） [パスワード エージング タイム] に指定した期間が経過した時点で、[パスワードの変更] ページにアクセスする必要があります。

WAP-PSK 複雑性の設定

WAP デバイスで VAP を設定するとき、クライアントを安全に認証する方法を選択できます。セキュリティ方式として WPA Personal プロトコル（WPA 事前共有キーまたは WPA-PSK とも呼ばれる）を選択すると、認証プロセスで使用する複雑性要件を [WPA-PSK 複雑性] ページで設定できます。キーを複雑にするほどセキュリティが向上します。

WPA-PSK 複雑性を設定するには、次の手順を実行します。

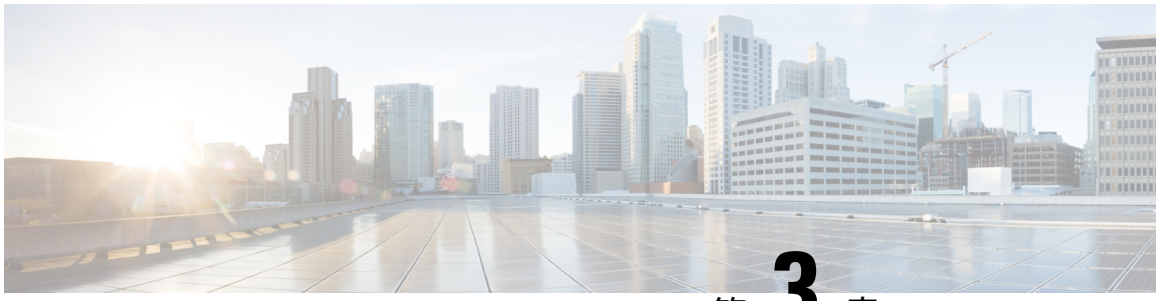
ステップ 1 [セキュリティ] > [WPA-PSK 複雑性の設定] を選択します。

ステップ 2 [有効化] をオンすると、WAP デバイスが WPA-PSK キーを設定条件と照合するようになります。無効な場合、設定されている設定はどれも使用されません。[WPA-PSK 複雑性] は、デフォルトでは無効です。

ステップ 3 次のパラメータを設定します。

- [WPA-PSK 最小文字クラス]：キー文字列で使用する必要がある文字クラスの最小数を選択します。使用可能な 4 つの文字クラスは、大文字、小文字、数字、標準キーボードで使用可能な特殊文字です。デフォルトは 3 です。
- [WPA-PSK 現在と異なる]：[有効化] をオンにすると、現在のキーの有効期限が切れた後に、ユーザは別のキーを設定できます。無効になっている場合は、現在のキーの有効期限が切れた後、ユーザは古いキーまたは以前のキーを使用できます。
- [WPA-PSK 最大長]：キー長の値を入力します。キーの最大長は 32 ～ 63 文字です。デフォルトは 63 です。
- [WPA-PSK 最小長]：キー長の値を入力します。キーの最小長は 8 ～ 16 文字です。デフォルトは 8 です。

ステップ 4 [保存] をクリックします。



第 3 章

ワイヤレス

この章では、ワイヤレス無線プロパティの設定方法について説明します。具体的な内容は次のとおりです。

- 無線 （47 ページ）
- ネットワーク （54 ページ）
- クライアント フィルタ （63 ページ）
- スケジューラ （65 ページ）
- QoS （66 ページ）

無線

無線は、ワイヤレス ネットワークを形成する WAP の物理部分です。WAP の無線設定は無線の動作を制御し、WAP から出力されるワイヤレス信号の種類を決定します。

ワイヤレス無線を設定するには、次の手順を実行します。

ステップ 1 [ワイヤレス] > [無線] の順に選択します。

ステップ 2 ラジオインタフェース

- [無線 1（5G）] : 4x4 MIMO モードで 5G 無線をサポートします。
- [無線 2（2.4 G）] : 3x3 MIMO モードで 2.4G 無線をサポートします。

ステップ 3 [インターフェイスごとの無線設定] 領域で、コンフィギュレーション パラメータを適用する無線インターフェイスを選択します。

ステップ 4 [基本設定] 領域で、選択した無線インターフェイスに次のパラメータを設定します。

（注） 各地域の規制により、特定の無線モードの使用を禁止されている場合があります。すべての国ですべてのモードが使用可能なわけではありません。

- [無線] : 無線インターフェイスを有効にするには [有効化] をオンにします。

- [ワイヤレス ネットワーク モード]：無線が使用する IEEE 802.11 標準および周波数。モードのデフォルト値は、無線 2 の場合は 802.11b/g/n、無線 1 の場合は 802.11a/n/ac です。各無線について、選択可能なモードのうち 1 つを選択します。

  無線 2（2.4G）は次の無線モードに対応しています。

  - [802.11b/g]：802.11b および 802.11g クライアントがこの WAP デバイスに接続できます。
  - [802.11b/g/n]（デフォルト）：2.4 GHz の周波数で動作する 802.11b、802.11g、および 802.11n クライアントがこの WAP デバイスに接続できます。
  - [2.4 GHz 802.11n]：2.4 GHz の周波数で動作する 802.11n クライアントがこの WAP デバイスに接続できます。

  無線 1（5G）は次の無線モードに対応しています。

  - [802.11a]：802.11a クライアントがこの WAP デバイスに接続できます。
  - [802.11a/n/ac]：5 GHz の周波数で動作する 802.11a クライアント、802.11n、および 802.11ac クライアントがこの WAP デバイスに接続できます。
  - [802.11n/ac]：5 GHz の周波数で動作する 802.11n クライアント、および 802.11ac クライアントがこの WAP デバイスに接続できます。

- [ワイヤレス バンドの選択]（802.11n および 802.11ac モードのみ）：802.11n 仕様では、他のモードで使用可能なレガシー 20 MHz 帯域に加え、20/40 MHz の帯域の共存も可能です。20/40 MHz 帯域ではより高いデータ レートが使用可能ですが、他の 2.4 GHz および 5 GHz のデバイスで使用可能な帯域が少なくなります。

  802.11ac の仕様では、20 MHz および 40 MHz の帯域に加え、80 MHz の帯域も使用できます。

  ワイヤレス帯域幅の選択を 20 MHz 帯域に限定するには、このフィールドを 20 MHz に設定します。802.11ac モードの場合、無線による 80 MHz ワイヤレス帯域の選択を防ぐため、このフィールドには 40 MHz を設定します。

- [プライマリ チャネル]（20/40 MHz 帯域幅の 802.11n モードのみ）：40 MHz のチャネルは、周波数領域で連続する 2 つの 20 MHz チャネルから構成されると考えられます。これら 2 つの 20 MHz チャネルは、多くの場合、プライマリ チャネルおよびセカンダリ チャネルと呼ばれます。プライマリ チャネルは、20 MHz チャネル帯域幅のみサポートする 802.11n クライアント、およびレガシー クライアントに使用します。

  次のオプションのいずれかを選択します。

  - [上位]：プライマリ チャネルを 40 MHz 帯域内の上位 20 MHz チャネルとして設定します。
  - [下位]：プライマリ チャネルを 40 MHz 帯域内の下位 20 MHz チャネルとして設定します。デフォルトでは [下方] が選択されています。

- [チャネル]：無線が送信および受信に使用する無線スペクトルの一部です。

使用可能なチャネルの範囲は、無線インターフェイスのモードと国コードの設定により決まります。チャネル設定で[自動]を選択した場合、WAPデバイスは使用可能なチャネルをスキャンし、トラフィックの検出量が最も少なかったチャネルを選択します。

各モードは、スペクトルが Federal Communications Commission（FCC; 米国連邦通信委員会）、または International Telecommunication Union（ITU-R; 国際電気通信連合）などの国内および国際機関により認可された方法に応じて、多くのチャネルを提供します。

- [スケジューラ]：無線インターフェイスの場合、このリストからプロファイルを選択します。

ステップ 5 [詳細設定] 領域で、次のパラメータを設定します。

- [DFS サポート]：このフィールドは、選択された無線モードが 5GHz の周波数で動作する場合のみ使用可能です。

  5 GHz 帯域の無線において、[DFS サポート] がオンで、規制ドメインがチャネル上でのレーダー検出を必要とする場合、802.11h の Dynamic Frequency Selection（DFS; 動的周波数選択）および Transmit Power Control（TPC; 送信電力制御）機能は有効になります。

  DFS は、5 GHz 帯域のレーダー システムとスペクトルを共有し、共同チャネル動作を回避するためにワイヤレス デバイスを必要とするメカニズムです。DFS の要件は、AP の国コード設定によって決まる規制ドメインに応じて異なります。

  802.11h ワイヤレス モードを使用する場合、IEEE 802.11h 標準についていくつか重要なポイントがあります。

  - 802.11h は 5 GHz 帯域でのみ有効です。これは 2.4 GHz 帯域では必要ありません。
  - 802.11h が有効なドメインで動作している場合、AP は割り当てられたチャネルを使おうとします。前のレーダー検出によってチャネルがブロックされたり、APがチャネル上でレーダーを検出した場合、AP は自動的に別のチャネルを選択します。
  - 802.11h が有効な場合、AP はレーダー スキャンのため、最低 60 秒間、5 GHz 帯域で動作しません。
  - 802.11h が動作する場合、WDS リンクを設定することが困難な場合があります。これは、WDS リンク上のこの 2 つのAP が動作するチャネルが、チャネルの使用状況およびレーダーの干渉に応じて、変化し続ける場合があるためです。WDS は、両方の AP が同じチャネルで動作する場合にのみ動作します。WDS の詳細については、「WDS ブリッジ」をご覧ください。

- [サポートされるショート ガード インターバル]：このフィールドは、選択された無線モードに 802.11n が含まれている場合のみ有効です。このガードインターバルはOFDM シンボル間のデッドタイム（ナノ秒）です。このガード インターバルは、シンボル間およびキャリア間の干渉（ISI、ICI）を防ぎます。802.11n モードでは、a および g の定義から、ガード インターバルを 800 ナノ秒から 400 ナノ秒に減らすことができます。ガード インターバルを短縮することにより、データ スループットが 10 % 向上します。WAP デバイスが通信しているクライアントもショート ガード インターバルに対応している必要があります。

  次のオプションのいずれかを選択します。

- [はい]：WAPデバイスは、ショートガードインターバルにも対応しているクライアントと通信する場合、400 ナノ秒のガードインターバルを使用してデータを送信します。デフォルトでは [はい] が選択されています。
- [いいえ]：WAP デバイスは、800 ナノ秒のガードインターバルを使ってデータを送信します。

- [保護]：この保護機能には、802.11 送信によってレガシー ステーションやアプリケーションとの干渉が引き起こされないことを保証するためのルールが含まれます。デフォルトでは、保護は有効です（自動）。保護を有効にすると、レガシー デバイスが WAP デバイスの範囲内にある場合、保護が起動されます。

  保護を無効（オフ）にすることができます。ただし、範囲内のレガシー クライアントまたは WAP デバイスが 802.11n 送信により影響を受ける場合があります。また、保護はモードが 802.11b/g の場合にも有効です。このモードで保護が有効な場合、802.11b クライアントと WAP デバイスを 802.11g 送信から保護します。

  （注）　この設定は、クライアントを WAP デバイスと関連付ける機能には影響を与えません。

- [ビーコン間隔]：ビーコン フレームの送信間隔。WAP デバイスはこれらのフレームを通常の間隔で送信し、ワイヤレス ネットワークの存在を通知します。デフォルトの動作は、ビーコン フレームを 100 ミリ秒ごとに（または 1 秒間に 10 回）送信します。20 ～ 2000 ミリ秒の間の整数を入力します。デフォルトは 100 秒です。

- [DTIM 期間]：Delivery Traffic Information Map（DTIM; 配信トラフィック情報マップ）期間。1 ～ 255 ビーコンの間の整数を入力します。デフォルトは 2 ビーコンです。

  DTIM メッセージは一部のビーコン フレームに含まれる要素です。これは、現在低電力モードでスリープ状態にあるクライアント ステーションのうち、どれがピックアップを待っている WAP デバイスにバッファされたデータを保有しているかを示します。

  DTIM 期間は、この WAP デバイスが処理するクライアントが、ピックアップを待っているバッファされたデータを、どの程度の頻度で確認するかを示します。

  測定はビーコンで行います。たとえば、これを 1 に設定すると、クライアントは WAP デバイス上でバッファされたデータをビーコンごとに確認します。これを 10 に設定すると、クライアントは 10 ビーコンごとに確認します。

- [フラグメンテーションしきい値]：フレーム サイズのしきい値（バイト）。有効な整数は偶数で、かつ 256 ～ 2346 の範囲内である必要があります。デフォルトは 2346 です。

  フラグメンテーションしきい値は、ネットワーク上を送信されるパケット（フレーム）のサイズを制限する方法です。設定したフラグメンテーションしきい値をパケットが超えた場合、フラグメンテーション機能が有効になり、パケットは複数の 802.11 フレームとして送信されます。

  送信されるパケットがしきい値以下である場合、フラグメンテーションは使用されません。しきい値に最大値（デフォルトの 2,346 バイト）を設定すると、効果的にフラグメンテーションを無効にします。

  デフォルトでは、フラグメンテーションはオフになっています。無線妨害が疑われる場合を除き、フラグメンテーションを使用しないことを推奨します。各フラグメントに適用される追加ヘッダーは、ネットワークのオーバーヘッドを増加させ、スループットを大幅に低下させる場合があります。

- [RTS しきい値]：送信要求（RTS）のしきい値。有効な整数の範囲は 0 ～ 65535 です。デフォルトは 65535 オクテットです。

  RTS しきい値は MPDU 内のオクテット数を示し、この値以下の場合 RTS/CTS ハンドシェイクは実行されません。

  RTS しきい値を変更することで、WAP デバイスを通過するトラフィック フローを制御できます。低いしきい値を指定した場合、RTSパケットはより頻繁に送信され、より多くの帯域幅を消費し、パケットのスループットが低下します。ただし、より多くの RTS パケットを送信することで、ビジーなネットワーク、または電磁干渉を受けるネットワーク上で発生する干渉や衝突からのネットワーク回復を助けることができます。

- [最大関連クライアント]：WAP デバイスにいつでもアクセスできるステーションの最大数。0 ～ 200 の間の整数を入力できます。デフォルトは 200 ステーションです。

- [送信電力]：WAP デバイスの送信電力レベルのパーセント値。

  デフォルト値の [フル - 100 %] では WAP デバイスに最大のブロードキャスト範囲が与えられ、必要なアクセス ポイント数が減るため、低い % 値に比べてコスト効率が高くなります。

  ネットワークのキャパシティを増やすには、WAPデバイスを近くに配置し、送信電力を減らします。この設定により、アクセス ポイント間のオーバーラップと干渉を減らすことができます。また、より弱いワイヤレス信号はネットワークの物理的な場所の外に伝播する可能性が低いため、より低い送信電力設定により、ネットワークをより安全な状態に維持できます。

  チャネル範囲と国コードの組み合わせによって、比較的低い最大送信電力の場合があります。送信電力を低い範囲（たとえば [中 - 25 %] または [低 - 12 %]）に設定しようとすると、パワー アンプによっては最小限の送信電力要件があるため、期待する電力低下が発生しない場合があります。

- [フレーム バースト サポート]：一般的に、フレーム バースト サポートを有効にすると、ダウンストリーム方向の無線性能が向上します。

- [エアタイム フェアネス モード]：エアタイム フェアネス（ATF）機能は、低速データ転送によって高速データ転送がスロットリングされる問題に対応する目的で実装されました。

- [最大使用率しきい値]：WAP デバイスが新規クライアントの関連付けの許可を停止するまでに無線に対して許可されるネットワーク帯域幅使用率をパーセンテージで入力します。有効な整数の範囲は 0 ～ 100 %です。デフォルトは 0 % です。0 を設定すると、使用率に関わらず、新規関連付けが許可されます。

- [固定マルチキャスト レート]：ブロードキャストおよびマルチキャスト パケットの送信レート（Mbps）。この設定は、ワイヤレス クライアントで設定レートを調整できる場合、ワイヤレス マルチキャスト ビデオ ストリーミングが発生する環境で役立ちます。

  [自動] が選択された場合、WAPデバイスは関連付けられたクライアントにとってのベスト レートを選択します。有効値の範囲は、設定された無線モードによって決まります。

- [レガシー レート設定]：レートはメガビット/秒で表されます。

  [サポートされるレート設定] は、WAP デバイスがサポートするレートを表します。複数のレートにチェックマークを付けることができます。WAP デバイスは、エラー率や WAP デバイスからクライアント ステーションまでの距離などの要素に基づき、最も効率的なレートを自動的に選択します。

[基本レートセット]は、ネットワーク上の他のアクセスポイントやクライアントステーションとの通信を設定する目的で、WAP デバイスがネットワークにアドバタイズするレートを表します。WAP デバイスにサポートされたレートセットのサブセットをブロードキャストさせると、より効率的です。

- [ブロードキャスト/マルチキャスト レート上限]：マルチキャストおよびブロードキャストのレート上限では、ネットワーク上を送信されるパケット数を制限することで、ネットワーク全体のパフォーマンスを向上させることができます。

  デフォルトでは、この機能は無効になっています。この機能を有効にするまで、次のフィールドは無効になっています。

  - [レート上限]：マルチキャストおよびブロードキャストのトラフィックのレート上限。上限は1より大きく、50未満（パケット/秒）でなければなりません。このレート上限を下回るトラフィックは常に適合し、適切な宛先に送信されます。デフォルトでもある最大のレート上限は50パケット/秒です。
  - [レート上限バースト]：定義された最大レートを超えている場合でも、一時的なバーストとして通過することが許可されるトラフィックの量（バイト単位）。デフォルトでもある最大のレート上限バーストは 75 パケット/秒です。

- [スペクトラム解析モード]：スペクトラム解析モードは次のいずれかのステータスに設定できます。
  - [専用スペクトル アナライザ]：専用モードでは、10 % 以上の時間でスペクトラム解析に無線が使用されるため、クライアント接続は機能するとしても保証はされません。
  - [ハイブリッド スペクトル アナライザ]：ハイブリッドモードでは、クライアント接続は保証されますが、スループットの劣化が予期されます。
  - [3+1 スペクトラム解析]：3+1 モードでは、スペクトラム解析が 1x1 チェーンで行われている間、クライアントが 3x3 チェーンに接続します。
  - [無効]：デフォルトは [無効] です。

- [VHT 機能]：この機能の目的は、Broadcom-to-Broadcom リンクの VHT で Broadcom 固有の拡張を有効または無効にすることです。VHT 機能は、802.11 ac ドラフトで指定されていない 256QAM VHT レートへの対応を可能にします。レートはすべて VHT LDPC モード、MCS 9 Nss 1 20Mhz、MCS 9 Nss 2 20Mhz、MCS 6 Nss 3 80Mhz です。VHT 機能は 802.11 ac PHY のためにサポートされています。

ステップ 6 [TSPEC の設定] をクリックし、次のパラメータを設定します。

- [TSPEC 違反間隔]：[TSPEC 違反間隔] フィールドには、必須アドミッション制御手順に従わなかった関連クライアントを、WAP デバイスが報告する時間間隔を秒単位で入力します。報告は、システムログおよび SNMP トラップを介して行われます。0 ～ 900 秒の間の時間を入力します。デフォルトは 300 秒です。
- [TSPEC モード]：WAP デバイスの全体的な TSPEC モードを規制します。デフォルトでは、TSPEC モードはオフです。次のオプションが用意されています。
  - [オン]：WAP デバイスは、[無線] ページで設定した TSPEC 設定に従って TSPEC 要求を処理します。

- [オフ]：WAP デバイスはクライアント ステーションからの TSPEC 要求を無視します。

- [TSPEC 音声 ACM モード]：音声アクセス カテゴリの必須アドミッション制御（ACM）を規制します。デフォルトでは、TSPEC 音声 ACM モードはオフです。次のオプションが用意されています。
  - [オン]：ステーションは、音声トラフィック ストリームを送信または受信する前に、WAP デバイスに帯域幅の TSPEC 要求を送信する必要があります。WAP デバイスは、TSPEC が許可された場合、割り当てられたメディア時間を含む要求の結果と共に応答します。
  - [オフ]：ステーションは、許可された TSPEC を必要とせずに、音声プライオリティ トラフィックを送受信できます。WAP デバイスはクライアント ステーションからの音声 TSPEC 要求を無視します。

- [TSPEC 音声 ACM の上限]：WAP デバイスがアクセスを得るために音声 AC を使って、ワイヤレス メディア上で送信しようとするトラフィック量の上限。デフォルトの上限は、合計トラフィックの 20 % です。

- [TSPEC ビデオ ACM モード]：ビデオ アクセス カテゴリの必須アドミッション制御を規制します。デフォルトでは、TSPEC ビデオ ACM モードはオフです。次のオプションが用意されています。
  - [オン]：ステーションは、ビデオ トラフィック ストリームを送信または受信する前に、WAP デバイスに帯域幅の TSPEC 要求を送信する必要があります。WAP デバイスは、TSPEC が許可された場合、割り当てられたメディア時間を含む要求の結果と共に応答します。
  - [オフ]：ステーションは、許可された TSPEC を要求せずに、ビデオのプライオリティ トラフィックを送受信できます。WAP デバイスは、クライアント ステーションからのビデオ TSPEC 要求を無視します。

- [TSPEC ビデオ ACM 上限]：WAP デバイスがアクセスを得るためにビデオ AC を使って、ワイヤレス メディア上で送信しようとするトラフィック量の上限。デフォルトの上限は、合計トラフィックの 15 % です。

- [TSPEC AP 非アクティブ タイムアウト]：WAP デバイスがダウンリンク トラフィックの仕様をアイドルとして検出し、削除するまでの時間。有効な整数の範囲は 0 ～ 120 秒で、デフォルトは 30 秒です。

- [TSPEC ステーション非アクティブ タイムアウト]：WAP デバイスがアップリンク トラフィックの仕様をアイドルとして検出し、削除するまでの時間。有効な整数の範囲は 0 ～ 120 秒で、デフォルトは 30 秒です。

- [TSPEC レガシー WMM キュー マップ モード]：ACM として動作するキューのレガシー トラフィックの混合を有効にするには、[有効化] をオンにします。デフォルトでは、このモードはオフです。

ステップ 7 [OK] をクリックし、次に [保存] をクリックします。

ネットワーク

Virtual Access Points（VAP; 仮想アクセスポイント）は、ワイヤレス LAN を、イーサネット VLAN と同等のワイヤレスの複数のブロードキャスト ドメインに分割します。VAP は、1 つの物理 WAP デバイスの複数のアクセス ポイントをシミュレートします。この Cisco WAP デバイスでは最大 4 つの VAP がサポートされています。

各 VAP は、VAP0 を除き、個別に有効または無効にすることができます。VAP0 は物理無線インターフェイスであり、無線が有効な限り有効のままです。VAP0 を無効にするには、無線自体を無効にする必要があります。

各 VAP は、ユーザが設定した Service Set Identifier（SSID）により識別できます。複数の VAP で同一の SSID 名を持つことはできません。SSID ブロードキャストは、各 VAP で個別に有効または無効にすることができます。[SSID ブロードキャスト] は、デフォルトで有効になっています。

SSID 命名規則

VAP0 のデフォルトの SSID は **ciscosb** です。追加で作成された VAP の SSID 名はすべてブランクです。すべての VAP の SSID には他の値を設定できます。SSID は大文字と小文字を区別し、2 ～ 32 文字の英数字のエントリが可能です。

指定可能な文字は、

- ASCII 0x20 から 0x7E です。
- 先頭および末尾にスペース（ASCII 0x20）は使用できません。

（注） つまり、スペースは SSID 内で使用できますが、最初または最後の文字としては使用できません。またピリオド「.」（ASCII 0x2E）も使用できます。

VLAN ID

各 VAP は VLAN に関連付けられ、VLAN ID（VID）により識別できます。VID は 1 ～ 4094 まで（1 と 4094 を含む）の任意の値を指定できます。この Cisco WAP デバイスは、9 個のアクティブな VLAN（WLAN 用の 8 個と、1 つの管理 VLAN）をサポートします。

デフォルトでは、WAP デバイスの設定ユーティリティに割り当てられる VID は 1 です。これはデフォルトのタグなし VID でもあります。管理 VID が VAP に割り当てられた VID と同じである場合、この VAP に関連付けられた WLAN クライアントで WAP デバイスを管理できます。必要な場合は、Access Control List（ACL; アクセス制御リスト）を作成して WLAN クライアントからの管理を無効にできます。

VAP の設定

VAP の設定方法：

ステップ 1 [ワイヤレス] > [ネットワーク] を選択します。

ステップ 2 [無線] フィールドで、VAP 設定パラメータを適用する無線インターフェイス（[無線 1] または [無線 2]）をクリックします。

ステップ 3 VAP0 がシステムで設定されている唯一の VAP である場合に VAP を追加するには、[□] をクリックします。次に VAP をオンにします。

ステップ 4 次のように設定します。

- [VLAN ID]：VAP と関連付ける VLAN の VLAN ID を指定します。

  必ずネットワーク上で適切に設定された VLAN ID を入力してください。VAP がワイヤレス クライアントを不適切に設定した VLAN と関連付けると、ネットワークに問題が生じる可能性があります。

  ワイヤレス クライアントがこの VAP を使って WAP デバイスに接続するとき、WAP デバイスはこのワイヤレス クライアントからのすべてのトラフィックに、設定された VLAN ID をタグ付けします（ただしポート VLAN ID を入力するか、RADIUS サーバを使用してワイヤレス クライアントを VLAN に割り当てる場合を除きます）。VLAN ID の範囲は 1 ～ 4094 です。

  VLAN ID を現在の管理 VLAN ID 以外の ID に変更した場合、この VAP に関連付けられた WLAN クライアントはこのデバイスを管理できません。[LAN] ページ上のタグなしの管理 VLAN ID の設定を確認できます。詳細については、「IPv4 設定 （13 ページ）」を参照してください。

- [SSID 名]：ワイヤレス ネットワークの名前を入力します。SSID は、最大 32 文字までの英数字の文字列です。各 VAP に対し、一意の SSID を選択します。

  管理している WAP デバイスと同じ WAP デバイスにワイヤレス クライアントとして接続した場合、SSID をリセットすると、その WAP デバイスへの接続は失われます。この新しい設定を保存した後、新しい SSID に再接続する必要があります。

- [SSID ブロードキャスト]：SSID のブロードキャストを有効および無効にします。

  WAP デバイスがこのビーコン フレームの SSID をブロードキャストすることを許可するかどうかを指定します。ブロードキャスト SSID パラメータは、デフォルトで有効になっています。VAP が SSID をブロードキャストしない場合、そのネットワーク名はクライアント ステーションで使用可能なネットワークのリストには表示されません。接続するには、代わりに、正確なネットワーク名をクライアントのワイヤレス接続ユーティリティに手動で入力する必要があります。

  ブロードキャスト SSID の無効化は、誤ってネットワークに接続するクライアントを防止するには十分ですが、ハッカーによる暗号化されていないトラフィックへの接続または監視などの単純な試行でさえ防止できません。SSID ブロードキャストの抑制は、プライオリティによりクライアントの接続が容易になり、抑制しないと無防備なネットワーク（ゲスト ネットワークなど）、および入手可能な機密情報がないネットワークに対し、最低限レベルの保護を提供します。

  [WMF]：ワイヤレス マルチキャスト転送は、ワイヤレス デバイスのマルチキャスト トラフィックを転送するための効率的な方法を提供し、マルチキャスト フレームのユニキャストを繰り返し使用する WLAN 上のマルチキャスト送信の問題を解決します。

- [セキュリティ]：VAP にアクセスするために必要な認証タイプを選択します。次のオプションが用意されています。

- なし
- 静的 WEP
- WPA パーソナル
- WPA エンタープライズ

[なし] 以外のセキュリティ モードを選択した場合、追加フィールドが表示されます。ワイヤレス セキュリティの設定に関する詳細については、「セキュリティの設定」を参照してください。

認証タイプとして、より強力なセキュリティ保護を提供する、[WPA パーソナル] または [WPA エンタープライズ] の使用を推奨します。

（注） [静的 WEP] は、WPA パーソナルと WPA エンタープライズに対応していないワイヤレス コンピュータまたはデバイスでのみ使用できます。セキュリティに [静的 WEP] を設定するには、無線を 802.11a または 802.11b/g モードとして設定します。802.11n モードでは、セキュリティとして [静的 WEP] を使用することを制限しています。

- [クライアント フィルタ]：この VAP にアクセスできるステーションが、設定された MAC アドレスのグローバル リストに限定されるかどうかを指定します。次のクライアント フィルタ タイプのいずれかを選択できます。
  - [無効]：クライアント フィルタを使用しません。
  - [ローカル]：[クライアント フィルタ] ページで設定した MAC 認証リストを使用します。
  - [RADIUS]：外部 RADIUS サーバの MAC 認証リストを使用します。
- [チャネル分離]：チャネル分離を有効にするには、これをオンにします。

  無効にすると、ワイヤレス クライアントは通常、WAP デバイスを介してトラフィックを送信することにより、お互いに通信できます。

  有効にすると、WAP デバイスは、同じ VAP 上のワイヤレス クライアント間の通信をブロックします。この場合、WAP デバイスは、ネットワーク上のワイヤレス クライアントと有線デバイス間の WDS リンクを介したデータ トラフィック、および別の VAP に関連付けられた他のワイヤレス クライアントとのデータ トラフィックは許可しますが、ワイヤレス クライアント間のデータ トラフィックは許可しません。
- [バンドステア]：両方の無線が動作する場合にバンドステアを有効にするには、これをオンにします。2.4 GHz バンドから 5 GHz バンドにデュアルバンド サポート対象のクライアントをステアリングすることによって、5 GHz バンドを有効に利用します。
  - これは VAP ごとに設定しますが、両方の無線で有効にする必要があります。
  - 時間的な制約のある音声トラフィックやビデオ トラフィックのある VAP では推奨されません。
  - 無線の n 帯域幅を考慮しません。5 HGz 無線が 20 MHz 帯域幅を使用したとしても、クライアントをその無線にステアリングしようとしません。

- [スケジューラ]：リストからスケジューラ プロファイルを選択します。VAP0 をスケジューラ プロファイルに関連付けることはできません。
- [ゲスト アクセス インスタンス]：CP インスタンスを VAP に関連付けます。関連付けられた CP インスタンス設定は、VAP で認証を試みるユーザに適用されます。インスタンスに関連付ける VAP ごとに、インスタンス名を選択します。

（注） **[アクセス コントロール]** > **[ゲスト アクセス]** ページでは VAP を 1 つのゲスト アクセス インスタンスに関連付けることができます。**ゲスト アクセス インスタンス**を最初に設定する必要があります。

ステップ 5 [保存] をクリックします。

注意 新しい設定を保存すると、対応するプロセスが停止され、再起動されることがあります。この事態が発生すると、WAP デバイスの接続が切断される可能性があります。この時点で WAP デバイス設定を変更することを推奨します。

（注） VAP を削除するには、削除する VAP をオンにし、[削除] をクリックします。VAP を編集するには、編集する VAP をオンにして [編集] をクリックします。変更を保存するには、作業が完了したときに [保存] をクリックします。

セキュリティの設定

ここでは、[ネットワーク] ページで設定できる WAP デバイスのセキュリティ設定について説明します。[なし]、[WPA パーソナル]、[WPA エンタープライズ] の 3 つのセキュリティ設定オプションから選択できます。

なし

セキュリティ モードとして [なし] を選択した場合、デバイス上で追加のセキュリティ設定を行う必要はありません。このモードは、WAP デバイスに転送された、または WAP デバイスから転送されたデータはすべて暗号化されないことを意味します。このセキュリティ モードは初期ネットワーク設定時または問題解決時には便利な場合がありますが、安全ではないため、社内ネットワークで日常的に使用することは推奨されません。

静的 WEP

有線と同等のプライバシー（WEP）は、802.11 ワイヤレス ネットワーク用のデータ暗号化プロトコルです。ネットワーク上のすべてのワイヤレス ステーションとアクセス ポイントは、静的な 64 ビット（40 ビットの秘密キー＋24 ビットの初期化ベクトル（IV））、または 128 ビット（104 ビットの秘密キー＋24 ビット（IV））のデータ暗号化共有キーで構成されています。

[静的 WEP] は最も安全なモードではありませんが、部外者が暗号化されていないワイヤレス トラフィックを簡単に傍受することを防ぐことができるため、セキュリティ モードに [なし]（プレーン テキスト）を設定するより安全な保護を提供します。

WEP は、静的キーに基づき、ワイヤレス ネットワークを通過するデータを暗号化します。暗号化アルゴリズムは、RC4 と呼ばれるストリーム暗号です。

次のパラメータを静的 WEP に設定します。

- [転送キー インデックス]：キーのインデックス リストを入力します。キーのインデックスには 1 ～ 4 が設定できます。デフォルトは 1 です。[転送キー インデックス] は、WAP デバイスが送信するデータを暗号化するためにどの WEP キーを使用するかを示します。
- [キーの長さ]：キーの長さとして [64 ビット] または [128 ビット] のいずれかを選択します。
- [キーの種類]：キーの種類として [ASCII] または [16 進数] のいずれかを選択します。
- [WEP キー]：最大 4 つの WEP キーを指定できます。各テキストボックスに、各キーの文字列を入力します。入力するキーは、選択した次のキー タイプによって異なります。
  - [ASCII]：大文字と小文字のアルファベット、数字、および @ や # などの特殊記号が含まれます。
  - [16 進数]：0 ～ 9 の数字と A ～ F の文字が含まれます。
- 各キーには、[必要な文字数] フィールドで指定されているのと同じ文字数を使用してください。これらは WAP デバイスを使ってステーションと共有される RC4 WEP キーです。各クライアント ステーションは、WAP デバイスに指定されているのと同じスロット内のこれらの同一 WEP キーのいずれかを使用するよう、設定する必要があります。
- [802.1X 認証]：この認証アルゴリズムは、静的 WEP がセキュリティ モードの場合、クライアント ステーションが WAP デバイスと関連付けられるかどうかを判断するために使用する方法を定義します。
- 次のいずれかのオプションを選択し、使用する認証アルゴリズムを指定します。
  - [オープン システム] は、クライアント ステーションが正確な WEP キーを持っているかどうかに関わらず、そのクライアント ステーションを WAP デバイスと関連付けることができます。このアルゴリズムは、プレーンテキスト、IEEE 802.1X、および WPA モードでも使用されます。認証アルゴリズムに [オープン システム] を設定した場合、どのクライアントも WAP デバイスと関連付けられます。

（注） クライアント ステーションへの関連付けが許可されていても、WAP デバイスとトラフィックを交換できるとは限りません。ステーションは、アクセスに成功し、WAP デバイスからのデータを暗号化し、読み取り可能なデータを WAP デバイスに送信するために、正確な WEP キーを持つ必要があります。

  - [共有キー] では、クライアント ステーションを WAP デバイスに関連付けるには、クライアント ステーションに正確な WEP キーがあることが必要です。認証アルゴリズ

ムに [共有キー] が設定された場合、不適切な WEP キーを持つステーションは、WAP デバイスと関連付けられません。

- [オープン システム] および [共有キー] の両方。両方の認証アルゴリズムを選択した場合、共有キー モードで WEP を使用するよう設定されたクライアント ステーションには、WAP デバイスに関連付けられるようにするために有効な WEP キーが必要です。またオープン システムとして WEP を使用するよう設定したクライアント ステーション（共有キー モードは無効）は、正確な WEP キーを持たない場合でも、WAP デバイスに関連付けることができます。

静的 WEP のルール

静的 WEP を使用する場合、次のルールが適用されます。

- すべてのクライアント ステーションは、ワイヤレス LAN（WLAN）のセキュリティに WEP を設定し、AP からステーションへのデータ送信を復号するため、すべてのクライアントが WAP デバイスで指定された WEP キーのいずれか 1 つを持っている必要があります。
- WAP デバイスは、クライアントがステーションから AP への送信に使用するすべてのキーを持つ必要があります。これにより、ステーションの送信を復号できます。
- 同一のキーは、すべてのノード（AP およびクライアント）において同一のスロットを占有する必要があります。たとえば、WAP デバイスが WEP key 3 として abc123 キーを指定する場合、クライアント ステーションは WEP key 3 としてこれと同じ文字列を定義する必要があります。
- クライアント ステーションはアクセス ポイントにデータを送信するために別のキーを使用できます（または同じキーを使用することもできますが、同じキーを使用すると、あるステーションが他のステーションから送信されたデータを復号できるため、安全性が低くなります）。
- 一部のワイヤレス クライアント ソフトウェアでは、複数の WEP キーを設定し、クライアント ステーションの転送キー インデックスを定義できます。これにより、異なるキーを使用して送信するデータを暗号化するよう、ステーションを設定できます。その結果、近隣のアクセス ポイントが他のアクセス ポイントの送信を復号することはできなくなります。
- アクセス ポイントとクライアント ステーション間で 64 ビットと 128 ビットの WEP キーを混合することはできません。

WPA パーソナル

WPA パーソナルは Wi-Fi アライアンス IEEE 802.11i 標準であり、AES-CCMP および TKIP の暗号化が含まれます。WPA パーソナルは、エンタープライズ WPA セキュリティ モードで使用されているように、IEEE 802.1X および EAP を使用する代わりに事前共有キー（PSK）を使用します。PSK はクレデンシャルの最初のチェックのみに使用されます。WPA パーソナルは、WPA-PSK とも呼ばれます。

このセキュリティ モードは、オリジナルの WPA をサポートするワイヤレス クライアントとの下位互換性があります。

WPA パーソナルは次のように設定します。

- [WPA バージョン]：クライアント ステーションのタイプとして次のいずれかを選択します。
  - [WPA-TKIP]：このネットワークには、オリジナルの WPA および TKIP セキュリティ プロトコルのみをサポートするクライアント ステーションがあります。WPA-TKIP だけを選択することは、最新の Wi-Fi アライアンス要件では許可されていません。
  - [WPA2-AES]：ネットワーク上のすべてのクライアント ステーションが WPA2 および AES-CCMP 暗号/セキュリティ プロトコルをサポートします。これは、IEEE 802.11i 標準の最適なセキュリティを提供します。最新の Wi-Fi アライアンス要件では、AP はこのモードを常にサポートする必要があります。

    ネットワークにクライアントが混在し、一部はWPA2をサポートし、一部はオリジナルの WPA のみサポートする場合、両方を選択します。これにより、両方の WPA と WPA2 クライアント ステーションが関連付けし、認証しますが、それをサポートするクライアントにはより堅牢な WPA2 を使用します。この WPA の設定は、セキュリティの代わりにより多くの相互運用性を可能にします。

    WAP デバイスと関連付けられるよう、WPA クライアントは次のキーのいずれか 1 つを持つ必要があります。
    - 有効な TKIP キー
    - 有効な AES-CCMP キー

- [PMF（保護管理フレーム）]：暗号化されない 802.11 管理フレームのセキュリティを提供します。セキュリティ モードが無効な場合、PMF が [PMF なし] に設定されており、編集できません（非表示または灰色表示）。セキュリティ モードが [WPA2-xxx] に設定されている場合、PMF はデフォルトで [対応] になっており編集可能です。次の 3 種類の値がチェックボックスで指定できます。
  - **不要**
  - **対応**
  - **必須**

（注） WiFi アライアンスは、PMF を有効にし、[対応]（デフォルト）として設定されていることを要求しています。非準拠のワイヤレス クライアントで不安定な動作や接続の問題が発生する場合は、無効にします。

- [キー]：WPA パーソナル セキュリティ用共有秘密キー。8 文字以上 63 文字以下の文字列を入力します。使用できる文字には、大文字と小文字のアルファベット、数字、および@や □ などの特殊記号が含まれます。
- [キーをクリアテキストとして表示]：有効になっている場合は、入力したテキストが表示されます。無効になっている場合、入力時にテキストはマスクされません。
- [キー強度メーター]：WAP デバイスは、使用される文字の種類（大文字と小文字のアルファベット、数字、特殊文字）や文字列の長さなどの複雑度の基準に照らしてキーを確認します。WPA-PSK 複雑度チェック機能が有効な場合、最低限の基準を満たしていないかぎり、キーは受け入れられません。複雑度チェックの設定情報については、「WAP-PSK 複雑性の設定 （44 ページ）」を参照してください。
- [ブロードキャスト キー更新レート]：この VAP に関連付けられているクライアントのブロードキャスト（グループ）キーが更新される間隔。デフォルトは 86400 秒ですが、0 ～ 86400 の範囲で選択できます。値 0 は、ブロードキャスト キーが更新されないことを示します。

WPA エンタープライズ

RADIUS を使用した WPA エンタープライズは Wi-Fi アライアンス IEEE 802.11i 標準を実装したもので、これには CCMP（AES）および TKIP の暗号化が含まれます。このエンタープライズ モードでは、RADIUS サーバを使用してユーザを認証する必要があります。

このセキュリティ モードは、オリジナルの WPA をサポートするワイヤレス クライアントとの下位互換性があります。

デフォルトでは動的 VLAN モードが有効になります。これにより、RADIUS 認証サーバはステーションに使用する VLAN を特定できます。

WPA エンタープライズは、次のパラメータで構成されます。

- [WPA バージョン]：サポートするクライアント ステーションのタイプを選択します。次のオプションが用意されています。
  - [WPA-TKIP]：ネットワーク上に、オリジナルの WPA および TKIP セキュリティ プロトコルのみをサポートしているクライアント ステーションがあります。アクセスポイントに WPA-TKIP のみ選択することは、最新の Wi-Fi アライアンス要件では許可されていません。
  - [WPA2-AES]：ネットワーク上のすべてのクライアント ステーションは WPA2 バージョンおよび AES-CCMP 暗号/セキュリティ プロトコルをサポートします。これは IEEE 802.11i 標準に準拠した最適なセキュリティを実現します。最新の Wi-Fi アライアンス要件では、AP はこのモードを常にサポートする必要があります。
- [事前認証の有効化]：WPA バージョンとして WPA2 を選択するか、または WPA と WPA2 の両方を選択した場合は、WPA2 クライアントに対する事前認証を有効にできます。

  WPA2 ワイヤレス クライアントに事前認証パケットを送信させる場合に、このオプションをオンにします。事前認証情報は、クライアントが現在使用している WAP デバイスから

対象の WAP デバイスに伝達されます。この機能を有効にすると、複数の AP に接続するクライアントがローミングするための認証を高速化できます。

WPA バージョンに WPA を選択した場合、オリジナルの WPA はこの機能をサポートしていないため、このオプションは適用されません。

RADIUS とともに WPA を使用するよう設定されたクライアント ステーションには、次のアドレスおよびキーのいずれか 1 つが必要です。

- 有効な TKIP RADIUS IP アドレスと RADIUS キー
- 有効な CCMP（AES）IP アドレスと RADIUS キー

- [PMF（保護管理フレーム）]：暗号化されない 802.11 管理フレームをセキュリティで保護します。セキュリティ モードが無効であるか [WEP] に設定されている場合、PMF は [PMF なし] に設定され、編集できません（非表示または灰色表示）。セキュリティ モードが [WPA2-xxx] に設定されている場合、PMF はデフォルトで [対応] に設定され、編集可能です。次の 3 種類の値がチェックボックスで指定できます。
  - **不要**
  - **対応**
  - **必須**

  （注） WiFi アライアンスには、PMF が [対応]（デフォルト）に設定されて有効になっている必要があります。非準拠のワイヤレス クライアントで不安定な動作や接続の問題が発生する場合は、無効にします。

- [グローバル RADIUS サーバ設定を使用]：デフォルトでは、各 VAP は WAP デバイスに定義したグローバル RADIUS 設定を使用します。ただし、RADIUS サーバの異なる設定を使用するよう、各 VAP を設定することができます。

  グローバル RADIUS サーバ設定を使用するには、このオプションをオンにします。また、VAP に別の RADIUS サーバを使用するにはこのオプションをオフにし、RADIUS サーバの IP アドレスとキーをそれぞれ該当するフィールドに入力します。

- [サーバの IP アドレス タイプ]：RADIUS サーバが使用する IP のバージョン。IPv4 と IPv6 のグローバル RADIUS アドレス設定を行うアドレス タイプを切り替えることができますが、WAP デバイスは RADIUS サーバまたはこのフィールドで選択したアドレス タイプのサーバとのみコンタクトできます。

- [サーバの IP アドレス - 1] または [サーバの IPv6 アドレス - 1]：この VAP のプライマリ RADIUS サーバのアドレス。

- [サーバの IP アドレス - 2] または [サーバの IPv6 アドレス - 2]：この VAP のバックアップ RADIUS サーバとして使用する、最大 3 つの IPv4 および（または）IPv6 アドレス。プラ

イマリ サーバでの認証に失敗した場合、設定された各バックアップ サーバが順番に試行されます。

- [キー - 1]：グローバル RADIUS サーバの共有秘密キー。最大 63 文字の標準英数字および特殊文字を使用できます。このキーは大文字と小文字を区別し、WAP デバイスおよび RADIUS サーバで設定されているものと同じキーを設定しなければなりません。入力時に RADIUS キーを他者から見られるのを防ぐため、入力するテキストはアスタリスクで表示されます。
- [キー - 2]：設定されたバックアップ RADIUS サーバに関連付けられた RADIUS キー。サーバ IP（IPv6）アドレス 2 のサーバはキー 2 を使用します。
- [RADIUS アカウンティングの有効化]：特定のユーザが消費したリソース（システム時刻や送受信されたデータ量など）を追跡および測定します。RADIUS アカウンティングを有効にすると、プライマリ RADIUS サーバとすべてのバックアップ サーバに対して有効になります。
- [アクティブ サーバ]：WAP デバイスが設定された各サーバに順番にコンタクトを試み、アップしている最初のサーバを選択するのではなく、アクティブな RADIUS サーバを管理的に選択できるようにします。
- [ブロードキャスト キー更新レート]：この VAP に関連付けられているクライアントのブロードキャスト（グループ）キーが更新される間隔。デフォルトは 86400 秒です。有効な範囲は 0 ～ 86400 秒です。値 0 は、ブロードキャスト キーが更新されないことを示します。
- [セッション キー更新レート]：WAP デバイスが、VAP に関連付けられている各クライアントのセッション（ユニキャスト）を更新する間隔。有効な範囲は 30 ～ 86400 秒です。値 0 は、セッション キーが更新されないことを示します。

クライアント フィルタ

WAP デバイスでの認証で、リストに含まれるクライアント ステーションを許可または拒否するには、クライアント フィルタを使用できます。MAC 認証は [ネットワーク （54 ページ）] ページで設定されます。VAP の設定に基づき、WAP デバイスは、外部 RADIUS サーバに保存されたクライアント フィルタ リストを参照するか、WAP デバイスにローカルで保存されたクライアント フィルタ リストを参照します。

クライアント フィルタ リストを WAP デバイスにローカルで設定する

WAP デバイスでは 1 つのローカル クライアント フィルタ リストだけを使用できます。フィルタは、リスト上の MAC アドレスのみアクセスを許可する、またはリスト上のアドレスのみアクセスを拒否するよう、設定できます。

フィルタ リストには最大 512 個のクライアント アドレスを追加できます。

クライアント フィルタを設定するには、次の手順に従います。

ステップ 1 [ワイヤレス] > [クライアント フィルタ] の順に選択します。

ステップ 2 WAP デバイスのフィルタ リストの使用方法を選択します。

- [許可（リストにあるクライアントのみを許可]）：ステーション リストにないステーションはすべて、WAP デバイスを介したネットワークへのアクセスを拒否されます。
- [拒否（リストにあるすべてのクライアントを拒否）]：リストにあるステーションのみ、WAP デバイスを介したネットワークへのアクセスを拒否されます。その他のステーションはアクセスを許可されます。

（注） フィルタ設定は、RADIUS サーバ（存在する場合）上に保存されたクライアント フィルタ リストにも適用されます。

ステップ 3 リストが完成するまで MAC アドレスの入力を続けます。[**関連付けられたクライアント**] の隣にある矢印をクリックすると、関連付けられているクライアントのリストが表示されます。MAC アドレスを 1 つ選択して、[**追加**] をクリックします。[MAC アドレス テーブル] にルールが 1 つ追加されます。[関連付けられたクライアント] のリストには以下が含まれています。

- [**MAC アドレス**]：関連付けられているワイヤレス クライアントの MAC アドレス。
- [**ホスト名**]：関連付けられているワイヤレス クライアントのホスト名。
- [**IP アドレス**]：関連付けられているワイヤレス クライアントの IP アドレス。
- [**ネットワーク（SSID）**]：WAP デバイスの Service Set Identifier（SSID）。SSID は、ワイヤレス ローカル エリア ネットワークを一意に識別する最大 32 文字の英数字の文字列です。これはネットワーク名とも呼ばれます。

ステップ 4 [**保存**] をクリックします。

RADIUS サーバ上での MAC 認証の設定

1 つ以上の VAP において、クライアント フィルタを使用するよう設定する場合、RADIUS サーバにステーション リストを設定する必要があります。リストの形式は次の表に示すとおりです。

RADIUS サーバ認証	説明	値
User-Name (1)	クライアント ステーションの MAC アドレス。	有効なイーサネット MAC アドレス
User-Password (2)	クライアント MAC エントリを検索するために使用する固定のグローバル パスワード。	NOPASSWORD

スケジューラ

無線および VAP スケジューラにより、VAP または無線を動作可能にする特定の時間間隔に関するルールを設定できます。

この機能を使用すると、セキュリティを強化し消費電力を低減する目的で、勤務時間にのみ VAP へのアクセスを許可したり無線が機能したりするようにスケジュールできます。

WAP デバイスは最大 16 プロファイルをサポートします。有効なルールだけがこのプロファイルに追加されます。最大 16 個までのルールがグループ化されて、スケジューリング プロファイルを形成します。同じプロファイルに属する定期的な時間のエントリが重複することはできません。

スケジューラ プロファイル構成

最大 16 個のスケジューラ プロファイル名を作成できます。デフォルトでは、プロファイルは何も作成されません。

スケジューラのステータスを表示し、スケジューラ プロファイルを追加するには、次の手順を実行します。

ステップ 1 [ワイヤレス] > [スケジューラ] を選択します。

ステップ 2 [有効化] をオンにし、管理モードが有効であることを確認します。デフォルトでは無効です。

[スケジューラ動作ステータス] 領域には、スケジューラの現在の動作ステータスが表示されます。

- [ステータス]：スケジューラの動作ステータス（[有効] または [無効]）。デフォルトは [無効] です。
- [理由]：スケジューラの動作ステータスの理由。選択項目は次のとおりです。
  - [アクティブ]：スケジューラは管理上有効です。
  - [管理モードが無効になっています]：スケジューラ管理モードが無効になっています。
  - [システム時刻が古くなっています]：システム時刻が古くなっています。
  - [管理モード]：スケジューラが管理モードになっています。

ステップ 3 プロファイルを追加するには、[スケジューラ プロファイル構成] テキストボックスにプロファイル名を入力し、[追加] をクリックします。プロファイル名は最大 32 文字の英数字です。

プロファイル ルール構成

プロファイルには最大 16 のルールを設定できます。各ルールでは、無線または VAP が動作可能な開始時刻、終了時刻、および 1 つ以上の曜日を指定します。ルールは本来定期的なもので

あり、毎週繰り返されます。有効なルールであるためには、開始時刻と終了時刻に関する次のパラメータ（曜日、時間、分）がすべて含まれている必要があります。競合するルールは設定できません。たとえば、あるルールを各平日に開始するよう設定し、各週末に開始する別のルールを設定することはできますが、あるルールを毎日開始するよう設定し、週末に開始する別のルールを設定することはできません。

プロファイル ルールを設定するには、次の手順に従います。

ステップ 1 [プロファイル名の選択] リストからプロファイルを選択します。

ステップ 2 [□] をクリックします。

新しいルールが [プロファイル ルール テーブル] に表示されます。

ステップ 3 [プロファイル名] の前にあるチェックボックスをオンにし、[編集] をクリックします。

ステップ 4 [曜日] メニューからそのルールの定期的なスケジュールを選択します。ルールは、毎日、各平日、各週末（土曜日と日曜日）、または特定の曜日に実行されるよう設定できます。

ステップ 5 開始および終了時刻を設定します。

- [開始時刻]：無線または VAP が有効になる時刻を設定します。時刻は hh:mm（24 時間）形式で設定します。範囲は <00 ～ 23>：<00 ～ 59> です。デフォルトは 00:00 です。
- [終了時刻]：無線または VAP が無効になる時刻を設定します。時刻は hh:mm（24 時間）形式で設定します。範囲は <00 ～ 23>：<00 ～ 59> です。デフォルトは 00:00 です。

ステップ 6 [保存] をクリックします。

（注） スケジューラ プロファイルを有効にするには、無線インターフェイスまたは VAP インターフェイスと関連付ける必要があります。

ルールを削除するには、[プロファイル名] 列からプロファイルを選択し、[削除] をクリックします。

QoS

Quality of Service（QoS）設定により、差別化されたワイヤレス トラフィックを処理する際にスループットを最適化してパフォーマンスを向上させるための送信キュー設定が可能になります。差別化されたワイヤレス トラフィックには、VoIP やその他のタイプのオーディオ、ビデオ、ストリーミング メディア、および従来の IP データなどが含まれます。

WAP デバイスに QoS を設定するには、送信キューにさまざまなタイプのワイヤレス トラフィックのパラメータを設定し、送信時の最小待機時間および最大待機時間を指定する必要があります。

WAP Enhanced Distributed Channel Access（EDCA）パラメータは、WAP デバイスからクライアント ステーションへのトラフィックの流れに影響を与えます。ステーション EDCA パラメー

タは、クライアント ステーションから WAP デバイスへのトラフィックの流れに影響を与えます。

通常の使用では、WAP デバイスとステーション EDCA のデフォルト値を変更すべきではありません。これらの値を変更すると、提供される QoS に影響を与えます。

WAP デバイスとステーション EDCA パラメータを設定するには、次の手順に従います。

ステップ 1 [ワイヤレス] > [QOS] の順に選択します。

ステップ 2 無線インターフェイス（[無線 1] または [無線 2]）を選択します。

ステップ 3 [EDCA] ドロップダウン リストから次のオプションのいずれかを選択します。

- [WFA デフォルト] : WAP デバイスとステーション EDCA のパラメータに Wi-Fi アライアンスのデフォルト値を取り込みます。このデフォルト値は、通常の混合トラフィックに最適です。
- [音声用に最適化] : WAP デバイスとステーション EDCA のパラメータに、音声トラフィックに最適な値を取り込みます。
- [カスタム] : カスタム EDCA パラメータを選択できるようにします。

これらの 4 つのキューは、WAP からステーションに送信されるさまざまなデータ タイプ用に定義されています。[カスタム] テンプレートを選択した場合、キューを定義するパラメータは設定可能です。それ以外の場合、選択に合わせた、事前に定義された値が設定されます。4 つのキューは以下のとおりです。

- [データ 0（音声）] : 優先度の高いキューで、遅延は最小。VoIP やストリーミング メディアなどの時間的制約のあるデータは、自動的にこのキューに送信されます。
- [データ 1（ビデオ）] : 優先度の高いキューで、遅延は最小。時間的制約のあるビデオデータは、自動的にこのキューに送信されます。
- [データ 2（ベストエフォート）] : 中程度の優先度のキューで、中程度のスループットと遅延。従来の IP データのほとんどは、このキューに送信されます。
- [データ 3（バックグラウンド）] : 優先度の最も低いキューで、高いスループット。最大のスループットを必要とし、時間的制約のないバルク データ（FTP データなど）は、このキューに送信されます。

ステップ 4 Wi-Fi MultiMedia（WMM）拡張を有効にするには、[有効化] をオンにします。

[Wi-Fi MultiMedia（WMM）] : このフィールドはデフォルトで有効にされています。WMM を有効にすると、QoS の優先順位付けとワイヤレス メディア アクセスの整合がオンになります。WMM を有効にすると、WAP デバイス上の QoS 設定は、WAP デバイスからクライアント ステーションに流れるダウンストリーム トラフィック（AP EDCA パラメータ）、およびステーションから AP に流れるアップストリーム トラフィック（ステーション EDCA パラメータ）を制御します。

WMM を無効にすると、QoS は、ステーションから WAP デバイスに流れるアップストリーム トラフィックのステーション EDCA パラメータを制御します。WMM を無効にしても、WAP デバイスからクライアント ステーションに流れるダウンストリーム トラフィックのパラメータ（AP EDCA パラメータ）を設定できます。

ステップ 5 次の EDCA およびステーション EDCA パラメータを設定します。

- [調停フレーム間スペース（AIFS）]：データ フレームの待機時間。待機時間はスロットで測定します。AIFS の有効な値は 1 ～ 255 です。
- [最小コンテンション ウィンドウ]：失敗した送信を再試行するための初期のランダム バックオフ待機時間（ウィンドウ）を決定するアルゴリズムへの入力。

  この値は、初期のランダム バックオフ待機時間の定義範囲の上限（ミリ秒）です。最初に生成されるランダムな数字は、0 とここで指定する数字の間の数字です。データ フレームが送信される前に、ランダム バックオフ待機時間が期限切れになった場合、リトライ カウンタが増え、ランダム バックオフ値（ウィンドウ）が倍になります。ランダムバックオフ値が [最大コンテンション ウィンドウ] で定義された数に達するまで、倍増され続けます。

  有効な値は、1、3、7、15、31、63、127、255、511、または 1023 です。この値は、[最大コンテンション ウィンドウ] の値よりも小さくなければなりません。
- [最大コンテンション ウィンドウ]：ランダムバックオフ値の倍増の上限（ミリ秒）。この倍増は、データ フレームが送信されるか、[最大コンテンション ウィンドウ] の上限に達するまで継続されます。

  [最大コンテンション ウィンドウ] の上限に達すると、最大再試行可能回数に達するまで再試行を続行します。

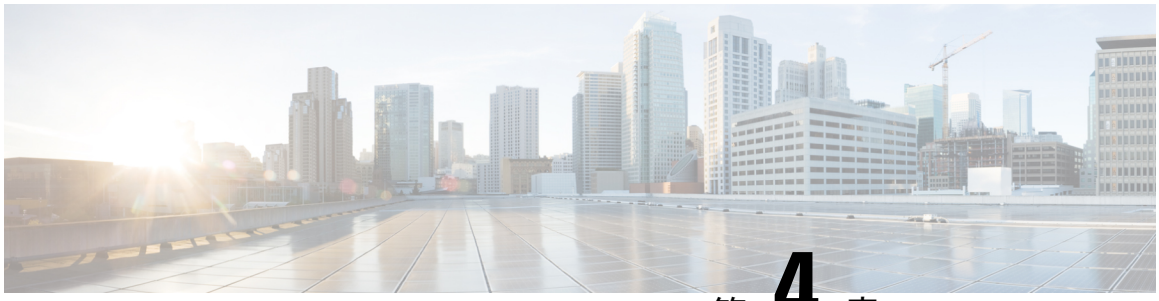
  有効な値は、1、3、7、15、31、63、127、255、511、または 1023 です。この値は、[最小コンテンション ウィンドウ] の値よりも大きくなければなりません。
- [最大バースト]：WAP からクライアント ステーションに流れるトラフィックのみに適用される WAP EDCA パラメータ。

  この値は、ワイヤレス ネットワーク上で可能なパケット バーストの最大バースト長（ミリ秒）を指定します。パケットバーストは、ヘッダー情報なしで送信される複数のフレームの集合体です。オーバーヘッドの低減によって、より高いスループットとより優れたパフォーマンスを実現します。有効な値は 0.0 ～ 999 です。
- [TXOP 上限]（ステーションのみ）：[TXOP 上限] はステーション EDCA パラメータで、クライアント ステーションから WAP デバイスに流れるトラフィックにのみ適用されます。Transmission Opportunity（TXOP; 送信機会）は、WME クライアント ステーションが WAP デバイス向けの Wireless Medium（WM; ワイヤレス メディア）への送信を開始する権限を持っている場合の時間間隔（ミリ秒）です。TXOP 制限の最大値は 65535 です。

ステップ 6 次の追加設定を行います。

- [否定確認応答]：サービス クラス値として QosNoAck を持つフレームに WAP デバイスが確認応答すべきでないことを指定するには、[有効化] をオンにします。
- [不定期自動省電力配信（APSD）]：APSD を有効にするには [有効化] をオンにします。VoIP 電話が WAP デバイスを介してネットワークにアクセスする場合には APSD が推奨されます。

ステップ 7 [保存] をクリックします。



第 4 章

ワイヤレス ブリッジ

この章では、ワイヤレスブリッジを設定する方法について説明します。具体的な内容は次のとおりです。

- ワイヤレス ブリッジ （69 ページ）
- WDS ブリッジの設定 （70 ページ）
- WDS リンク上の WEP （71 ページ）
- WDS リンク上の WPA/PSK （71 ページ）
- ワークグループ ブリッジ （72 ページ）

ワイヤレス ブリッジ

ワイヤレス分散システム（WDS）は複数の WAP デバイスの接続を可能にします。WDS を使用すると、WAP デバイスは無線で互いに通信できます。これにより、シームレスにクライアントをローミングし、複数のワイヤレス ネットワークを管理できます。WAP デバイスを、接続するリンクの数に基づき、ポイントツーポイントまたはポイントツーマルチポイントのブリッジ モードで設定できます。

ポイントツーポイント モードでは、WAP デバイスはクライアントの関連付けを受け入れ、ワイヤレス クライアントと通信します。WAP デバイスは、アクセス ポイント間に確立されたトンネルを介した他のネットワーク向けのすべてのトラフィックを転送します。ブリッジはホップ カウントには追加されません。これはシンプルな OSI レイヤ 2 ネットワーク デバイスとして動作します。

ポイントツーマルチポイントのブリッジ モードでは、WAP デバイスは複数のアクセス ポイント間の共通リンクとして機能します。このモードでは、中央の WAP デバイスがクライアントの関連付けを受け入れ、クライアントと通信します。他のすべてのアクセスポイントは、ルーティング目的でパケットを適切なワイヤレス ブリッジに転送する中央の WAP デバイスとのみ関連付けられます。

WAP デバイスはリピータとしても機能できます。このモードでは、WAP デバイスは非常に離れておりセル範囲内にできない 2 つの WAP デバイス間の接続として機能します。リピータとして機能する場合、WAP デバイスは LAN への有線接続を持たず、ワイヤレス接続を使用して信号を繰り返します。WAPデバイスがリピータとして機能するために特別な設定は必要なく、

リピータ モードの設定もありません。それでもワイヤレス クライアントは、リピータとして動作している WAP デバイスに接続することができます。

WAP デバイス上で WDS を設定する前に、次のガイドラインに注意してください。

- WDS リンクに参加するすべての Cisco WAP デバイスでは、次の同一の設定をする必要があります。
  - 無線
  - IEEE 802.11 モード
  - チャネル帯域幅
  - チャネル（自動を推奨）

  802.11n 2.4 GHz 帯域でブリッジングが動作する場合、チャネル帯域幅をデフォルトの 20/40 MHz ではなく、20 MHz に設定します。2.4 GHz、20/40 MHz 帯域の場合、その領域で 20 MHz の WAP デバイスが検出されると、動作帯域幅が 40 MHz から 20 MHz に変化する可能性があります。チャネル帯域幅の不一致は、リンクが切断される原因となります。
- WDS を使用する場合、WDS リンクに参加する両方の WAP デバイスに WDS を設定してください。
- WDS リンクは、WAP デバイスのいずれかのペア間でただ 1 つだけ設定できます。つまりリモート MAC アドレスは、ある WAP デバイスの WDS ページに一度だけ表示されます。

WDS ブリッジの設定

WDS ブリッジの設定方法：

ステップ 1 [ワイヤレス ブリッジ] を選択します。

ステップ 2 ワイヤレス ブリッジ モードとして [WDS] をクリックします。

ステップ 3 [有効化] をオンにし、WDS 設定で WDS ポートを有効にします。

ステップ 4 その他のパラメータの設定：

- [無線]：無線 ID（[無線 1（2.4 GHz）] または [無線 2（5GHz）]）を指定します。
- [ローカル MAC アドレス]：データ転送元の現在またはローカル WAP デバイスの物理アドレスまたは MAC アドレスを指定します。
- [リモート MAC アドレス]：宛先 WAP デバイスの MAC アドレスを指定します。[モニタ] > [ダッシュボード] > [ワイヤレス] ページで MAC アドレスを確認できます。
- [暗号化]：WDS リンクで使用する暗号化のタイプを選択します（[なし]、[静的 WEP]、または [WPA パーソナル]）。

  WDS リンク上のセキュリティの問題について懸念がない場合は、いずれのタイプの暗号化も設定しないことも可能です。あるいは、セキュリティ上の懸念がある場合は WPA パーソナルを選択できます。

WPA パーソナル モードでは、WAP デバイスは、WDS リンク上で CCMP（AES）暗号化と共に WPA2-PSK を使用します。暗号化のオプションの詳細については、「WDS リンク上の WPA/PSK （71 ページ）」を参照してください。

ステップ 5 この手順を繰り返し、最大 4 つの WDS インターフェイスを追加します。

ステップ 6 [保存] をクリックします。

ステップ 7 このブリッジに接続されるデバイスについて、この手順を繰り返します。

（注） **[モニタ]** > **[ダッシュボード]** > **[ワイヤレス]** ページにアクセスすると、ブリッジ リンクがアップしているかどうかを確認できます。[インターフェイス ステータス] テーブルで WDS(x) ステータスが [アップ] と表示されていれば、アップしています。

WDS リンク上の WEP

暗号化タイプとして WEP を選択すると、次の追加のフィールドが表示されます。

- [キーの長さ]：WEP が有効な場合、WEP キーの長さを 64 ビットまたは 128 ビットで指定します。
- [キーの種類]：WEP が有効な場合、Wep キーの種類として [ASCII] または [16 進数] のいずれかを選択します。
- [WEP キー]：[ASCII] を選択した場合、0 から 9、a から z、および A から Z の任意の組み合わせを入力します。[16 進数] を選択した場合、16 進数（0 から 9、および A から F の任意の組み合わせ）を入力します。これらは WAP デバイスを使ってステーションと共有される RC4 暗号化キーです。

  必要な文字数がこのフィールドの右側に表示され、選択した [キータイプ] および [キー長] フィールドに基づき変化します。

WDS リンク上の WPA/PSK

暗号化タイプとして WPA/PSK を選択すると、次の追加のフィールドが表示されます。

- [WDS ID]：作成した新規 WDS リンクに適切な名前を入力します。WDS リンクの他端にも同じ WDS ID が入力されていることが重要です。この WDS ID が WDS リンク上の両方の WAP デバイスで同じでない場合は、互いに通信してデータを交換することができません。

  WDS ID には任意の英数字の組み合わせを指定できます。

- [キー]：WDS ブリッジの一意の共有キーを入力します。この一意の共有キーは、WDS リンクの他端の WAP デバイスにも入力する必要があります。このキーが両方の WAP で同じでない場合は、互いに通信してデータを交換することができません。

WPA-PSK キーは、8 文字以上 63 文字以下の文字列です。使用できる文字には、大文字と小文字のアルファベット、数字、および @ や □ などの特殊記号が含まれます。

ワークグループ ブリッジ

ワーク グループ ブリッジ機能を使用すると、WAP デバイスはリモート ネットワークのアクセシビリティを拡張できます。ワーク グループ ブリッジ モードでは、WAP デバイスがワイヤレス LAN 上のワイヤレス ステーション（STA）として機能します。これにより、リモートの有線ネットワークまたは関連付けられたワイヤレス クライアントと、ワーク グループ ブリッジ モードで接続されているワイヤレス LAN 間のトラフィックをブリッジすることができます。

ワーク グループ ブリッジ機能は STA モードと AP モードの同時動作をサポートできるようにします。WAP デバイスは 1 つの基本サービス セット（BSS）内で STA デバイスとして動作する一方で、別の BSS では WAP デバイスとして動作することができます。ワーク グループ ブリッジ モードが有効になっている場合は、WAP デバイスはそのデバイスに関連付けられているワイヤレス クライアントの 1 つの BSS と、WAP デバイスがワイヤレス クライアントとして関連付ける別の BSS のみをサポートします。

WDS ブリッジ機能がピア WAP デバイスと連動できない場合にのみ、ワーク グループ ブリッジ モードを使用することを推奨します。WDS はワーク グループ ブリッジ ソリューションよりも優れた、より適切なソリューションです。Cisco WAP150 デバイスと Cisco WAP361 デバイスをブリッジングする場合、WDS を使用します。ブリッジングしない場合は、ワーク グループ ブリッジを検討します。ワーク グループ ブリッジ機能を有効にすると、VAP 設定は適用されず、ワーク グループ ブリッジの設定のみが適用されます。

（注） ワーク グループ ブリッジ モードが WAP デバイスで有効になっている場合、WDS 機能は動作しません。

ワーク グループ ブリッジ モードでは、WAP デバイス モードで動作中に WAP デバイスによって管理される BSS をアクセス ポイント インターフェイスと呼び、関連する STA をダウンストリーム STA と呼びます。他の WPA デバイスによって管理される BSS（つまり WAP デバイスが STA として関連付けるもの）はインフラストラクチャ クライアント インターフェイスと呼ばれ、他の WAP デバイスはアップストリーム AP と呼ばれます。

WAP デバイスの有線インターフェイスに接続されているデバイスと、デバイスのアクセス ポイント インターフェイスに関連付けられているダウンストリーム ステーションは、インフラストラクチャ クライアント インターフェイスによって接続されたネットワークにアクセスできます。パケットのブリッジングを可能にするには、アクセス ポイント インターフェイスと有線インターフェイスの VLAN 設定が、インフラストラクチャ クライアント インターフェイスの VLAN 設定と一致する必要があります。

ワーク グループ ブリッジ モードを範囲拡張機能として使用すると、リモートまたは到達が困難なネットワークへのアクセスを BSS で提供できます。関連付けられた STA から、同じ ESS

内の別の WAP デバイスに、WDS を使用せずに転送するように単一無線を設定することができます。

WAP デバイス上で**ワーク グループ ブリッジ**を設定する前に、次のガイドラインに注意してください。

- ワーク グループ ブリッジに参加するすべての WAP デバイスでは、次の同一の設定をする必要があります。
  - 無線
  - IEEE 802.11 モード
  - チャネル帯域幅
  - チャネル（自動を推奨）

  これらの設定情報については、「無線 （47ページ）」（基本設定）を参照してください。
- ワーク グループ ブリッジ モードは現在、IPv4 トラフィックのみをサポートしています。
- ワーク グループ ブリッジ モードはシングル ポイント設定ではサポートされていません。

ワーク グループ ブリッジ モードを設定するには、次の手順に従います。

ステップ 1 [ワイヤレス ブリッジ] を選択します。

ステップ 2 [ワークグループ] をクリックします。

ステップ 3 設定パラメータを適用する WGB ポートを選択します。

ステップ 4 [編集] をクリックし、インフラストラクチャ クライアント インターフェイス（アップリンク/ダウンリンク）の次のパラメータを設定します。

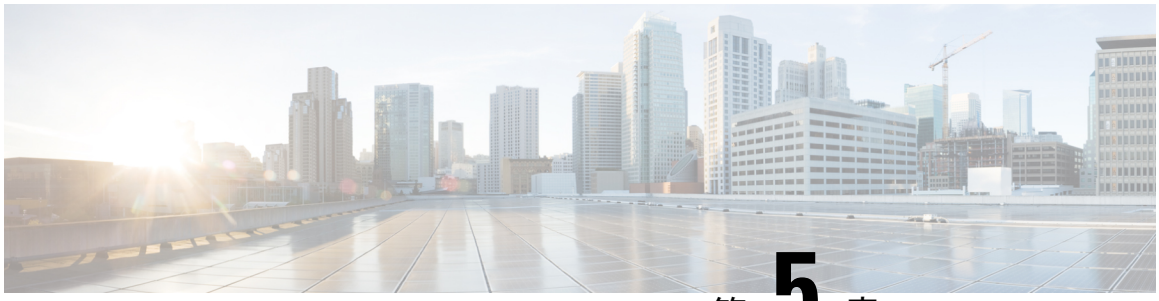
表 *1*: インフラストラクチャ クライアント インターフェイス（アップリンク/ダウンリンク）

WGB ポート	アップリンク	ダウンリンク
有効	インフラストラクチャ クライアント インターフェイスを有効にするには、このチェックボックスをオンにします。	インフラストラクチャ クライアントインターフェイスを有効にするには、このチェックボックスをオンにします。
無線	無線 ID（[無線 1（2.4 GHz）] または [無線 2（5GHz）]）を指定します。	無線 ID（[無線 1（2.4 GHz）] または [無線 2（5GHz）]）を指定します。

WGB ポート	アップリンク	ダウンリンク
SSID	BSS の現在の SSID を指定します。 （注） [SSID] の横に SSID スキャニング用の矢印があります。この機能はデフォルトでは無効になっていて、[不正 AP 検出]（これもデフォルトでは無効）で[AP 検出] が有効になっている場合のみ有効になります。	アクセス ポイント インターフェイスの SSID は、インフラストラクチャ クライアントの SSID と同じである必要はありません。
暗号化	アップストリーム WAP デバイスのクライアントステーションとしての認証に使用するセキュリティのタイプ。以下のいずれかのビューを選択できます。 • **なし** • **静的 WEP** • **WPA パーソナル** • **WPA エンタープライズ**	認証に使用するセキュリティのタイプ。次のオプションが用意されています。 • **なし** • **WPA パーソナル** • **静的 WEP**
接続ステータス	WAP がアップストリーム WAP デバイスに接続されているかどうかを示します。	該当なし（N/A）
VLAN ID	BSS に関連付けられている VLAN を指定します。	アクセスポイントインターフェイスを、インフラストラクチャクライアントインターフェイスでアドバタイズされる VLAN ID と同じ VLAN ID に設定します。
（注） インフラストラクチャ クライアント インターフェイスは、設定されたクレデンシャルと共に、アップストリーム WAP デバイスに関連付けられます。WAP デバイスは、アップストリーム リンク上の DHCP サーバから IP アドレスを取得できます。または、静的 IP アドレスを割り当てることができます。		
SSID ブロードキャスト	SSID のブロードキャストが使用可能か、有効であるか、または無効であるかを指定します。	ダウンストリーム SSID をブロードキャストにする場合はオンにします。[SSID ブロードキャスト] は、デフォルトで有効になっています。

WGB ポート	アップリンク	ダウンリンク
クライアント フィルタ	該当なし（N/A）	次のいずれかのオプションを選択します。 • [無効]：アップストリーム ネットワークにアクセスできる AP BSS 内のクライアントは、[MACアドレス] リストで指定されたクライアントに限定されません。 • [ローカル]：アップストリーム ネットワークにアクセスできる AP BSS 内のクライアントは、ローカルに定義された [MAC アドレス] リストで指定されたクライアントに限定されます。 • [RADIUS]：アップストリーム ネットワークにアクセスできる AP BSS 内のクライアントは、RADIUS サーバの [MAC アドレス] リストで指定されたクライアントに限定されます。
（注） [ローカル] または [RADIUS] を選択した場合は、クライアント フィルタ リストの作成手順を「クライアント フィルタ」で参照してください。		

ステップ 5 [保存] をクリックします。これで、関連付けられたダウンストリーム クライアントは、アップストリーム ネットワークと接続できるようになります。



第 5 章

高速ローミング

この章では、高速ローミングを設定する方法について説明します。具体的な内容は次のとおりです。

- 高速ローミング （77 ページ）
- 高速ローミングの設定 （78 ページ）
- リモート キー ホルダー リスト プロファイルの設定 （79 ページ）

高速ローミング

高速ローミング（IEEE 802.11r または高速 BSS 移行（FT）とも呼ばれる）により、クライアント デバイスはアクセス ポイント間をローミングするたびに RADIUS サーバで再認証する必要がないため、WPA2 エンタープライズ セキュリティを実装している環境内で高速にローミングできます。

高速移行ローミングは IEEE 802.11 標準の改訂で規定されている機能であり、ある AP から別の管理対象 AP へのシームレスで高速かつ安全なハンドオフにより、移動するワイヤレス デバイスで継続的な接続を許可します。音声品質とネットワーク セキュリティを確保するには、ポータブル ステーションが、他のトラフィックを処理する AP 間のローミング時に安全で低遅延の音声コールを維持できる必要があります。

このデバイスでは、WPA2 Enterprise セキュリティによる高速ハンドオフのために、802.11r で定義されている FBT（高速 BSS 移行）がサポートされています。Voice over Wi-Fi エンタープライズの場合、802.11r で定義されている機能の一部だけがサポートされます。高速 BSS 移行により、ローミング中の遅延が低下します。

FBT は無線の VAP ごとに有効に設定されます。

（注） VAP で FBT を設定する前に、VAP で WPA2 セキュリティが設定されており、事前認証と MFP が無効になっていることを確認してください。

高速ローミングの設定

以下の手順で、高速ローミングの設定方法を説明します。

ステップ 1 [高速ローミング] > [ローミング テーブル] を選択します。

ステップ 2 [□] をクリックしてローミング テーブルに新しい行を追加します。

ステップ 3 次のパラメータを設定します。

- [有効化]：このオプションはデフォルトでオンになっています。
- [BSSID]：有効にする VAP（[2.4GVAP 0] または [5G VAP 0]）を選択します。
- [モビリティ ドメイン]：FBT VAP のモビリティ ドメイン識別子（MDID）を指定します。MDID は、ESS 内の AP のグループを識別するために使用されます。これらの AP 間で STA が高速 BSS 移行サービスを使用できます。高速 BSS 移行は、同一 ESS 内にあり同一 MDID を持つ AP 間でのみ可能です。MDID が異なる AP、または異なる ESS 内の AP 間では実行できません。
- [FT モード]：Fast Transition プロトコルにより、モバイル ステーション（MS）がドメイン（FT プロトコルをサポートしており、分散システム（DS）経由で接続している AP のグループ）内の最初の AP でのみ完全な認証を行うことができ、同一ドメインの 2 番目以降の AP ではアソシエーション手続きが短くなります。次のいずれかの FT 方式を選択します。
  - [無線経由]：[無線経由] 方式では、モバイル ステーションはダイレクト 802.11 リンク経由で新しい AP と通信します。
  - [DS 経由]：[DS 経由] 方式では、MS は古い AP を経由して新しい AP と通信します。
- [R0 キー ホルダー]：RADIUS アクセス要求メッセージで送信する NAS 識別子を指定します。NAS 識別子は R0 キー ホルダー ID として使用されます。
- [R1 キー ホルダー]：オーセンティケータでの PMK-R1 のホルダーを指定する R1 キー ホルダー ID を指定します。
- [リモート キー ホルダー リスト]：ドロップダウンメニューから、作成したリモート キー ホルダー リストを選択します。

ステップ 4 [保存] をクリックします。

（注） ローミング設定を削除または変更するには、設定を選択してから [削除] または [編集] をクリックします。

FBT 設定後に [保存] をクリックして設定を保存します。一部の設定を変更すると、AP がシステムプロセスを停止して再起動することがあります。この状況が発生すると、ワイヤレス クライアントは一時的に接続を失います。WLAN トラフィックが少ないときに AP 設定を変更することを推奨します。

リモート キー ホルダー リスト プロファイルの設定

リモート R0 キー ホルダー リストのプロファイルを設定するには、次の手順に従います。

ステップ 1 [高速ローミング] > [リモート キー ホルダー リスト プロファイル] の順に選択します。

ステップ 2 新しいプロファイルを追加する場合は [□] をクリックし、既存のプロファイルを変更する場合は [編集] をクリックします。[リモート キー ホルダー リスト プロファイル] ページが表示されます。

ステップ 3 リモート キー ホルダー リスト プロファイルの名前を入力します。

ステップ 4 次のパラメータを設定します。VAP ごとに設定可能な R0 キー ホルダー エントリの数は最大 10 個です。

- [MAC アドレス] : R0 キー ホルダーである宛先の VAP MAC アドレスを入力します。PMKR1 キーを取得するために RRB PULL メッセージがこの AP MAC アドレスに送信されます。この MAC アドレスはすべての VAP にわたって一意である必要があります。
- [NAS ID] : 宛先 FBT 対応 VAP で設定されている NAS ID。
- [RRB キー] : RRM プロトコル メッセージの暗号化に使用するキー。

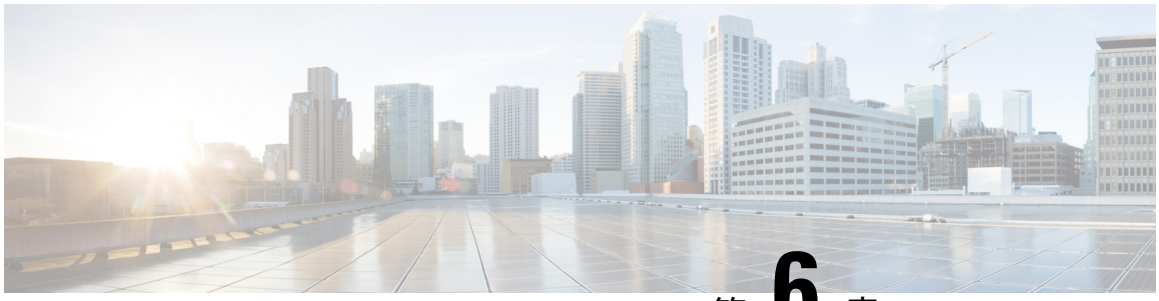
ステップ 5 ステップ 1 から 4 を繰り返し、R1 キー ホルダー データ リストで R1 キー ホルダーを設定します。VAP ごとに設定可能な R1 キー ホルダー エントリの数は最大 10 個です。キー ホルダー データは VAP ごとに設定されます。

- [MAC アドレス] : R1 キー ホルダーである宛先の VAP MAC アドレス。PMKR1 は RRB PUSH メッセージでこの AP MAC アドレスに送信されます。この MAC アドレスはすべての VAP にわたって一意である必要があります。
- [R1 キー ホルダー] : オーセンティケータで PMK-R1 のホルダーを指定する R1 キー ホルダー ID。
- [RRB キー] : RRM プロトコル メッセージの暗号化に使用するキー。

（注） リモート キー ホルダー データ リストの設定が完了したら、[復元] をクリックして古い設定を復元するか、または [保存] をクリックして設定を保存します。[キャンセル] をクリックすると [高速ローミング] ページの前に戻ります。

プロファイルをコピーまたは削除したら、[保存] をクリックします。

注意 プロファイルが選択されている状態で [エクスポート] をクリックすると、これらのプロファイルだけがエクスポートされます。プロファイルが選択されていない状態で [エクスポート] をクリックすると、すべてのプロファイルが**エクスポート**されます。



第 6 章

シングル ポイント設定

この章では、複数の WAP デバイスにわたるシングル ポイント設定を設定する方法について説明します。具体的な内容は次のとおりです。

- ACL （81 ページ）
- クライアント QoS （90 ページ）
- ゲスト アクセス （98 ページ）

ACL

アクセス コントロール リスト（ACL）は、ルールと呼ばれる許可条件および拒否条件を集めたものであり、権限を持たないユーザをブロックし、権限を持つユーザに特定のリソースへのアクセスを許可することによってセキュリティを提供します。ACL では、ネットワーク リソースに到達しようとする是認されていないすべての試行をブロックできます。

WAP デバイスは、最大 50 個の IPv4、IPv6、および MAC ACL と、各 ACL で最大 10 個のルールをサポートしています。各 ACL では複数のインターフェイスがサポートされています。

IPv4 と IPv6 の ACL

各 ACL は WAP デバイスが受信するトラフィックに適用されるルールのセットです。各ルールは、所定のフィールドの内容によって、ネットワークへのアクセスを許可するのか拒否するのかを指定します。さまざまな基準に基づいたルールを設定でき、それらを送信元または宛先の IP アドレス、送信元または宛先のポート、パケットで伝送されているプロトコルなど、パケット内の 1 個以上のフィールドに適用できます。IP ACL はレイヤ 3 および 4 用にトラフィックを分類します。

（注） 作成するすべてのルールの終わりに暗黙の拒否があります。すべて拒否することのないよう、ACL に許可ルールを追加して、トラフィックを許可することを強くお勧めします。

MAC ACL

MAC ACL はレイヤ 2 ACL です。送信元または宛先の MAC アドレス、VLAN ID、Class of Service など、フレームのフィールドを検査するルールを設定できます。フレームが WAP デバイスのポートに入ると、WAP デバイスはフレームを検査して、ACL ルールをフレームの内容と照合します。内容と一致するルールがあった場合、許可アクションまたは拒否アクションがフレームに対して実行されます。

ACL を設定するためのワークフロー

ACL ルールを使用して ACL を設定した後、指定したインターフェイスにルールを適用します。

ACL を設定するには、次の手順に従います。

ステップ 1 [アクセス コントロール] > [ACL] の順に選択します。

ステップ 2 ACL テーブルで [□] をクリックして新しい行を追加し、ACL を作成します。

ステップ 3 ACL の名前を入力します。

ステップ 4 ドロップダウン リストから ACL タイプを選択します（[IPv4]、[IPv6]、[MAC]）。

ステップ 5 [□] をクリックし、ACL を適用する関連インターフェイスを選択して、[OK] をクリックします。関連インターフェイスを変更するには、[□] をクリックして選択されているインターフェイスを削除し、[□] をクリックして新たな関連インターフェイスを選択します。

ステップ 6 [詳細] をクリックすると、ACL パラメータが表示されます。

ステップ 7 次に ACL のルールを設定します。IPv4 ACL の場合は「IPv4 ACL の設定 （82 ページ）」を参照してください。IPv6 ACL の場合は「IPv6 ACL の設定 （85 ページ）」を参照してください。MAC ACL の場合は「MAC ACL の設定 （88 ページ）」を参照してください。

ステップ 8 [保存] をクリックしてすべての変更内容を保存します。

IPv4 ACL の設定

IPv4 ACL を設定するには、次の手順を実行してください。

ステップ 1 [アクセス コントロール] > [ACL] の順に選択します。

ステップ 2 [□] をクリックして ACL を追加します。

ステップ 3 ACL 名フィールドに ACL の名前を入力します。この名前には、スペースなしで最大 31 文字の英数字と特殊文字を使用できます。

ステップ 4 [ACL タイプ] リストから、ACL のタイプとして [IPv4] を選択します。IPv4 ACL は、レイヤ 3 およびレイヤ 4 基準に基づいてネットワーク リソースへのアクセスを制御します。

ステップ 5 [□] をクリックし、ACL を適用する関連付けられているインターフェイスを選択します。[OK] をクリックします。関連付けられているインターフェイスを変更するには、[□] をクリックして選択されているインターフェイスを削除し、[□] をクリックして新たな関連インターフェイスを選択します。

ステップ 6 [詳細] をクリックすると、設定パラメータが表示されます。ルールを追加して次のフィールドを設定するには、[□] をクリックします。

（注） ルールを追加しない場合、デフォルトで DUT はすべてのトラフィックを拒否します。

- [ルールの優先度]：ACL に複数のルールが設定されている場合、ルールは優先度に従ってパケットまたはフレームに適用されます。番号が小さいほど優先度が高くなります。新しいルールの優先度は、すべての明示的なルールの中で最下位になります。最下位の優先度ですべてのトラフィックを拒否する暗黙のルールが常に存在している点に注意してください。
- [アクション]：アクションを [拒否] するかまたは [許可] するかを選択します。デフォルトのアクションは [拒否] です。

  [許可] を選択した場合、このルールは、ルール基準を満たすすべてのトラフィックが WAP デバイスに入ることを許可します。基準を満たさないトラフィックはドロップされます。

  [拒否] を選択した場合、このルールは、ルール基準を満たすトラフィックが WAP デバイスに入ることを必ずブロックします。基準を満たさないトラフィックは、このルールが最後のルールでなければ転送されます。すべての ACL の最後に暗黙のすべて拒否ルールがあるため、明示的に許可されないトラフィックはすべてドロップされます。
- [サービス（プロトコル）]：[IP プロトコル] フィールドの値に基づいてレイヤ 3 プロトコルまたはレイヤ 4 プロトコルの一致条件を使用します。次のいずれかのオプションを選択できます。
  - [すべてのトラフィック]：ルールの条件に一致するすべてのトラフィックを許可します。
  - [リストから選択]：次のプロトコルから選択します。IP、ICMP、IGMP、TCP、または UDP。
  - [カスタム]：IANA によって割り当てられている標準プロトコル ID 0 ～ 255 を入力します。[リストから選択] にリストされていないプロトコルを指定する場合にこの方法を選択します。
- [送信元 IPv4 アドレス]：パケットの送信元 IP アドレスが、該当するフィールドに定義されているアドレスと一致する必要があります。
  - [任意]：すべての IP アドレスが許容されます。
  - [シングル アドレス]：この基準を適用する IP アドレスを入力します。
  - [アドレス/マスク]：送信元 IP アドレスのワイルド カード マスクを入力します。ワイルド カード マスクによって、使用するビットおよび無視するビットが決まります。ワイルド カード マスク 255.255.255.255 は、どのビットも検査しないことを示します。ワイルド カード 0.0.0.0 はすべてのビットを検査することを示します。このフィールドは、[送信元 IP アドレス] をオンにする場合は必須です。

    ワイルド カード マスクは基本的にはサブネット マスクの逆です。たとえば、単一のホスト アドレスと一致する基準の場合は、ワイルド カード マスク 0.0.0.0 を使用します。基準を 24 ビット サブネット（192.168.10.0/24 など）と照合するには、0.0.0.255 のワイルド カード マスクを使用します。
- [送信元ポート]：ルールの一致条件に送信元ポートを含めます。送信元ポートは、データグラム ヘッダーで識別されます。

- [すべてのトラフィック] : ルールの条件に一致するすべてのトラフィックを許可します。
- [リストから選択] : 照合する送信元ポートに関連付けるキーワード（ftp、ftpdata、http、smtp、snmp、telnet、tftp、www）を選択します。これらの各キーワードは、同等のポート番号に変換されます。
- [カスタム] : データグラム ヘッダーに示される送信元ポートと照合する IANA ポート番号を入力します。ポートの範囲は 0 ～ 65535 で、3 種類のポートが含まれます。
  - 0 ～ 1023：ウェルノウン ポート
  - 1024 ～ 49151：登録済みポート
  - 49152 ～ 65535：ダイナミック ポート/プライベート ポート

- [宛先 IPv4 アドレス] : パケットの宛先 IP アドレスは、該当するフィールドに定義されているアドレスと一致する必要があります。
  - [任意] : 任意の IP アドレスを入力します。
  - [シングル アドレス] : この基準を適用する IP アドレスを入力します。
  - [アドレス/マスク] : 宛先 IP アドレスのワイルド カード マスクを入力します。ワイルド カード マスクによって、使用するビットおよび無視するビットが決まります。ワイルド カード マスク 255.255.255.255 は、どのビットも検査しないことを示します。ワイルド カード 0.0.0.0 はすべてのビットを検査することを示します。このフィールドは [送信元 IP アドレス] を選択する場合は必須です。

    ワイルド カード マスクは基本的にはサブネット マスクの逆です。たとえば、単一のホスト アドレスと一致する基準の場合は、ワイルド カード マスク 0.0.0.0 を使用します。基準を 24 ビット サブネット（192.168.10.0/24 など）と照合するには、0.0.0.255 のワイルド カード マスクを使用します。

- [宛先ポート] : ルールの一致条件に宛先ポートを含めます。宛先ポートは、データグラム ヘッダーで識別されます。
  - [任意] : ルールの条件に一致する任意のポート。
  - [リストから選択] : 照合する宛先ポートに関連付けるキーワード（ftp、ftpdata、http、smtp、snmp、telnet、tftp、www）を選択します。これらの各キーワードは、同等のポート番号に変換されます。
  - [カスタム] : データグラム ヘッダーに示されている宛先ポートと照合する IANA ポート番号を入力します。ポートの範囲は 0 ～ 65535 で、3 種類のポートが含まれます。
    - 0 ～ 1023：ウェルノウン ポート
    - 1024 ～ 49151：登録済みポート
    - 49152 ～ 65535：ダイナミック ポート/プライベート ポート

- [タイプ オブ サービス] : 特定のサービス タイプに基づいてパケットを照合します。

- [任意]：任意のタイプ オブ サービス。
- [リストから選択]：DSCP 確認転送（AS）、サービス クラス（CS）、または緊急転送（EF）の値に基づいてパケットを照合します。
- [DSCP]：カスタム DSCP 値に基づいてパケットを照合します。選択した場合は、0 ～ 63 の値をこのフィールドに入力してください。
- [プレシデンス]：IP プレシデンス値に基づいてパケットを照合します。選択した場合は、0 ～ 7 の IP Precedence 値を入力してください。
- [ToS/マスク]：IP ToS マスク値を入力します。この値によって、パケットの IP ToS フィールドとの比較に使用される IP ToS ビット値のビット位置が識別されます。

  IP ToS マスク値は、00 ～ FF の 2 桁の 16 進数で、反転（ワイルド カード）マスクを表します。IP ToS マスクの値が 0 のビットは、パケットの IP ToS フィールドとの比較に使用される IP ToS ビット値のビット位置を示します。たとえば、IP ToS 値でビット 7 および 5 が設定されていてビット 1 がクリアなことを確認するには、ビット 7 が最も重要な場合、IP ToS ビット値 0 と IP ToS マスク 00 を使用します。

ステップ 7 [OK] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

（注） ACL を削除または変更するには、ACL を選択してから [削除] または [編集] をクリックします。

ルールを削除または編集するには、[ルール設定] 領域でルールを選択し、[削除] または [編集] をクリックします。

ステップ 8 [保存] をクリックします。

IPv6 ACL の設定

IPv6 ACL を設定するには、次の手順を実行してください。

ステップ 1 [アクセス コントロール] > [ACL] の順に選択します。

ステップ 2 [□] をクリックして ACL を追加します。

ステップ 3 ACL 名フィールドに ACL の名前を入力します。

ステップ 4 [ACL タイプ] リストから、ACL のタイプとして [IPv6] を選択します。IPv4 ACL は、レイヤ 3 およびレイヤ 4 基準に基づいてネットワーク リソースへのアクセスを制御します。

ステップ 5 [□] をクリックし、ACL を適用する関連付けられているインターフェイスを選択します。次に [OK] をクリックします。関連付けられているインターフェイスを変更するには、[□] をクリックして選択されているインターフェイスを削除し、[□] をクリックして新たな関連インターフェイスを選択します。

ステップ 6 [詳細] をクリックすると、設定パラメータが表示されます。ルールを追加して次のフィールドを設定するには、[□] をクリックします。

（注） ルールを追加しない場合、デフォルトで DUT はすべてのトラフィックを拒否します。

- [ルールの優先度]：ACL に複数のルールが設定されている場合、ルールは優先度に従ってパケットまたはフレームに適用されます。番号が小さいほど優先度が高くなります。新しいルールの優先度は、すべての明示的なルールの中で最下位になります。その優先度を変更するには、上または下のボタンをクリックします。最下位の優先度ですべてのトラフィックを拒否する暗黙のルールが常に存在している点に注意してください。
- [アクション]：アクションを [拒否] するかまたは [許可] するかを選択します。デフォルトのアクションは [拒否] です。

  [許可] を選択した場合、このルールは、ルール基準を満たすすべてのトラフィックが WAP デバイスに入ることを許可します。基準を満たさないトラフィックはドロップされます。

  [拒否] を選択した場合、このルールは、ルール基準を満たすトラフィックが WAP デバイスに入ることを必ずブロックします。基準を満たさないトラフィックは、このルールが最後のルールでなければ転送されます。すべての ACL の最後に暗黙のすべて拒否ルールがあるため、明示的に許可されないトラフィックはすべてドロップされます。
- [サービス（プロトコル）]：[IP プロトコル] フィールドの値に基づいてレイヤ 3 プロトコルまたはレイヤ 4 プロトコルの一致条件を使用します。次のいずれかのオプションを選択できます。
  - [すべてのトラフィック]：ルールの条件に一致するすべてのトラフィックを許可します。
  - [リストから選択]：次のプロトコルから選択します。IPv6、ICMPv6、TCP、UDP。
  - [カスタム]：IANA によって割り当てられている標準プロトコル ID 0 ～ 255 を入力します。[リストから選択] にリストされていないプロトコルを指定する場合にこの方法を選択します。
- [送信元 IPv6 アドレス]：パケットの送信元 IP アドレスが、該当するフィールドに定義されているアドレスと一致する必要があります。
  - [任意]：すべての IP アドレスが許容されます。
  - [シングル アドレス]：この基準を適用する IP アドレスを入力します。
  - [アドレス/マスク]：送信元 IP アドレスのワイルド カード マスクを入力します。ワイルド カード マスクによって、使用するビットおよび無視するビットが決まります。ワイルド カード マスク 255.255.255.255 は、どのビットも検査しないことを示します。ワイルド カード 0.0.0.0 はすべてのビットを検査することを示します。このフィールドは、[送信元 IP アドレス] をオンにする場合は必須です。

    ワイルド カード マスクは基本的にはサブネット マスクの逆です。たとえば、単一のホスト アドレスと一致する基準の場合は、ワイルド カード マスク 0.0.0.0 を使用します。基準を 24 ビット サブネット（192.168.10.0/24 など）と照合するには、0.0.0.255 のワイルド カード マスクを使用します。
- [送信元ポート]：ルールの一致条件に送信元ポートを含めます。送信元ポートは、データグラム ヘッダーで識別されます。
  - [任意]：任意の送信元アドレスが許容されます。

- [リストから選択]：照合する送信元ポートに関連付けるキーワード（ftp、ftpdata、http、smtp、snmp、telnet、tftp、www）を選択します。これらの各キーワードは、同等のポート番号に変換されます。
- [カスタム]：データグラム ヘッダーに示される送信元ポートと照合する IANA ポート番号を入力します。ポートの範囲は 0 ～ 65535 で、3 種類のポートが含まれます。
  - 0 ～ 1023：ウェルノウン ポート
  - 1024 ～ 49151：登録済みポート
  - 49152 ～ 65535：ダイナミック ポート/プライベート ポート

- [宛先 IPv6 アドレス]：パケットの宛先 IP アドレスは、該当するフィールドに定義されているアドレスと一致する必要があります。
  - [任意]：任意の IP アドレスを入力します。
  - [シングル アドレス]：この基準を適用する IP アドレスを入力します。
  - [アドレス/マスク]：宛先 IP アドレスのワイルド カード マスクを入力します。ワイルド カード マスクによって、使用するビットおよび無視するビットが決まります。ワイルド カード マスク 255.255.255.255 は、どのビットも検査しないことを示します。ワイルド カード 0.0.0.0 はすべてのビットを検査することを示します。このフィールドは [送信元 IP アドレス] を選択する場合は必須です。

    ワイルド カード マスクは基本的にはサブネット マスクの逆です。たとえば、単一のホスト アドレスと一致する基準の場合は、ワイルド カード マスク 0.0.0.0 を使用します。基準を 24 ビット サブネット（192.168.10.0/24 など）と照合するには、0.0.0.255 のワイルド カード マスクを使用します。

- [宛先ポート]：ルールの一致条件に宛先ポートを含めます。宛先ポートは、データグラム ヘッダーで識別されます。
  - [任意]：ルールの条件に一致する任意のポート。
  - [リストから選択]：照合する宛先ポートに関連付けるキーワード（ftp、ftpdata、http、smtp、snmp、telnet、tftp、www）を選択します。これらの各キーワードは、同等のポート番号に変換されます。
  - [カスタム]：データグラム ヘッダーに示されている宛先ポートと照合する IANA ポート番号を入力します。ポートの範囲は 0 ～ 65535 で、3 種類のポートが含まれます。
    - 0 ～ 1023：ウェルノウン ポート
    - 1024 ～ 49151：登録済みポート
    - 49152 ～ 65535：ダイナミック ポート/プライベート ポート

- [フロー ラベル]：IPv6 パケット固有の 20 ビット値を指定します。
  - [任意]：任意の 20 ビット数値。

- [DSCP]：カスタム DSCP 値に基づいて数値を照合します。

- [DSCP]：IP DSCP 値に基づいてパケットを照合します。
  - [任意]：任意の DSCP 値が許容されます。
  - [リストから選択]：ドロップダウン リストから DSCP 値を選択します。
  - [カスタム]：0 ～ 63 のカスタム DSCP 値を入力します。

ステップ 7 [OK] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

（注） ACL を削除または変更するには、ACL を選択してから [削除] または [編集] をクリックします。

ルールを削除または編集するには、[ルール設定] 領域でルールを選択し、[削除] または [編集] をクリックします。

ステップ 8 [保存] をクリックします。

MAC ACL の設定

MAC ACL を設定するには、次の手順を実行してください。

ステップ 1 [アクセス コントロール] > [ACL] の順に選択します。

ステップ 2 [□] をクリックして MAC ACL を追加します。

ステップ 3 [ACL 名] フィールドに ACL を識別する名前を入力します。

ステップ 4 リストから ACL の種類として [MAC] を選択します。MAC ACL は、レイヤ 2 基準に基づいてアクセスを制御します。

ステップ 5 [□] をクリックし、ACL を適用する関連付けられているインターフェイスを選択して [OK] をクリックします。関連付けられているインターフェイスを変更するには、[□] をクリックして選択されているインターフェイスを削除し、[□] をクリックして新たな関連インターフェイスを選択します。

ステップ 6 次に [詳細] をクリックすると、設定パラメータが表示されます。ルールを追加して次のパラメータを設定するには、[□] をクリックします。

- [ルールの優先度]：ACL に複数のルールが設定されている場合、ルールは優先度に従ってパケットまたはフレームに適用されます。番号が小さいほど優先度が高くなります。新しいルールの優先度は、すべての明示的なルールの中で最下位になります。「上」または「下」ボタンをクリックすると、この優先度を変更できます。最下位の優先度ですべてのトラフィックを拒否する暗黙のルールが常に存在している点に注意してください。

- [アクション]：アクションを [拒否] するかまたは [許可] するかを選択します。デフォルトのアクションは [拒否] です。

  [許可] を選択した場合、このルールは、ルール基準を満たすすべてのトラフィックが WAP デバイスに入ることを許可します。基準を満たさないトラフィックはドロップされます。

[拒否] を選択した場合、このルールは、ルール基準を満たすトラフィックが WAP デバイスに入ることを必ずブロックします。基準を満たさないトラフィックは、このルールが最後のルールでなければ転送されます。すべての ACL の最後に暗黙のすべて拒否ルールがあるため、明示的に許可されないトラフィックはすべてドロップされます。

- [サービス（ETH タイプ）] : イーサネット フレームのヘッダーにある値と比較する一致基準を選択します。ドロップダウン リストから ETH タイプを選択できます。
  - [任意] : 任意のプロトコルが許容されます。
  - [リストから選択] : 次のプロトコル タイプから選択します。ARP、IPv4、IPv6、IPX、NetBIOS、PPPoE。
  - [カスタム] : パケットを照合するカスタム プロトコル識別子を入力します。この値は、0600 ～ FFFF の範囲の 4 桁の 16 進数です。
- [送信元 MAC アドレス] : パケットの送信元 MAC アドレスが、該当するフィールドに定義されているアドレスと一致する必要があります。
  - [任意] : 任意の送信元 MAC アドレスが許容されます。
  - [シングル アドレス] : イーサネット フレームと比較する送信元 MAC アドレスを入力します。
  - [アドレス/マスク] : イーサネット フレームと比較する送信元 MAC のビットを指定する送信元 MAC アドレス マスクを入力します。

    MAC マスクのそれぞれのビット位置について、0 は対応するアドレス ビットが有効なことを示し、1 はアドレス ビットが無視されることを示します。たとえば、MAC アドレスの最初の 4 オクテットのみをチェックするには、MAC マスク 00:00:00:00:ff:ff を使用します。MAC マスク 00:00:00:00:00:00 ではすべてのアドレス ビットがチェックされるため、単一の MAC アドレスを照合する場合に使用します。
- [宛先 MAC アドレス] : パケットの宛先 MAC アドレスが、該当するフィールドに定義されているアドレスと一致する必要があります。
  - [任意] : 任意の宛先 MAC アドレスが許容されます。
  - [シングル アドレス] : イーサネット フレームと比較する宛先 MAC アドレスを入力します。
  - [アドレス/マスク] : イーサネット フレームと比較する宛先 MAC のビットを指定する宛先 MAC アドレス マスクを入力します。
- [VLAN ID] : イーサネット フレームと比較する VLAN ID です。
  - [任意] : 任意の VLAN ID 値が許容されます。
  - [カスタム] : イーサネット フレームと比較する具体的な VLAN ID を入力します。このフィールドは最初または唯一の 802.1Q VLAN タグのみにあります。ポートの範囲は 1 ～ 4094 です。
- [サービス クラス] : パケットを照合するためのサービス クラス 802.1p のユーザ プライオリティ値を指定します。

- [任意]：任意のサービス クラスが許容されます。
- [カスタム]：イーサネット フレームと比較する 802.1p ユーザ プライオリティを入力します。有効な範囲は 0 ～ 7 です。

ステップ 7 [OK] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

（注） ACL を削除または変更するには、ACL を選択してから [削除] または [編集] をクリックします。ルールを削除または編集するには、[ルール設定] 領域でルールを選択し、[削除] または [編集] をクリックします。

ステップ 8 [保存] をクリックします。

クライアント QoS

クライアント Quality Of Service（QoS）は、ネットワークに接続するワイヤレス クライアント接続の制御に使用され、使用帯域幅を管理します。クライアント QoS は、HTTP トラフィックや特定のサブネットからのトラフィックなどを、アクセス コントロール リスト（ACL）を使って制御できます。ACL は、ルールと呼ばれる許可条件および拒否条件を集めたものであり、権限を持たないユーザをブロックし、権限を持つユーザに特定のリソースへのアクセスを許可することによってセキュリティを提供します。ACL では、ネットワーク リソースに到達しようとする是認されていないすべての試行をブロックできます。

トラフィック クラス

QoS 機能に含まれている差別化サービス（DiffServ）サポートにより、トラフィックをストリームに分類できます。また、ホップ別に定義されている動作に基づいて特定の QoS 処理も行われます。

標準の IP ベース ネットワークは、ベストエフォート型のデータ配信サービスを提供するように設計されています。ベストエフォート型サービスでは、保証はされませんが、ネットワークによってタイミング良くデータが配信されます。輻輳が発生している場合、パケットが遅延したり、散発的に送信されたり、ドロップしたりすることがあります。電子メールやファイル転送などの一般的なインターネット アプリケーションでは、サービスのわずかな低下は許容範囲内であり、たいていの場合は気づきません。ただし、音声やマルチメディアなどのタイミング要件が厳しいアプリケーションでは、サービスの低下が望ましくない影響を及ぼします。

DiffServ 設定は、IP プロトコルやその他の基準に従ってトラフィックを分類するクラス マップを定義することから始まります。その後、各クラス マップをトラフィック クラスの処理方法を定義するポリシー マップに関連付けることができます。時間的な制約のあるトラフィックが含まれるクラスを、ポリシー マップに割り当てることができます。

IPv4 トラフィック クラスの設定

IPv4 クラス マップを追加して設定するには

ステップ 1 [クライアント QoS] > [トラフィック クラス] の順に選択します。

ステップ 2 [□] をクリックしてトラフィック クラスを追加します。

（注） クラス マップの最大数は 50 です。

ステップ 3 [トラフィック クラス名] テキスト フィールドに、新しいクラス マップの名前を入力します。名前には、1 ～ 31 文字の英数字と特殊文字を使用できます。スペースは使用できません。

ステップ 4 [クラス タイプ] のリストから [IPv4] を選択します。IPv4 トラフィック クラスは、WAP デバイスの IPv4 トラフィックにのみ適用されます。

ステップ 5 次のように設定します。

- [送信元アドレス] : パケットの送信元 IPv4 アドレスと、適切なフィールドで定義された IPv4 アドレスが一致する必要があります。
  - **[任意]** : 任意の IPv4 アドレスを送信元アドレスとして使用できます。
  - [シングル アドレス] : この基準を適用する 1 つの IPv4 アドレスを入力します。
  - [アドレス/マスク] : 送信元 IPv4 アドレス マスクを入力します。DiffServ のマスクは、ドット付き 10 進表記の IP のネットワーク方式ビット マスクです。宛先 IP アドレスのどの部分を使用してパケット コンテンツと照合するのかを示します。

    DiffServ マスク 255.255.255.255 はすべてのビットが重要であること、マスク 0.0.0.0 は重要なビットがないことを示します。ACL ワイルド カード マスクでは反対になります。たとえば、基準と単一ホスト アドレスを照合するには、255.255.255.255 のマスクを使用します。基準を 24 ビット サブネット（192.168.10.0/24 など）と照合するには、255.255.255.0 のマスクを使用します。

- [宛先アドレス] : パケットの宛先 IPv4 アドレスと、適切なフィールドで定義された IPv4 アドレスが一致する必要があります。
  - **[任意]** : 任意の IPv4 アドレスを宛先アドレスとして使用できます。
  - [シングル アドレス] : この基準を適用する IPv4 アドレスを入力します。
  - [アドレス/マスク] : 宛先 IP アドレス マスクを入力します。

ステップ 6 [詳細] をクリックして次のパラメータを設定します。

- [プロトコル] : IPv4 パケットの IP プロトコル フィールドまたは IPv6 パケットのネクスト ヘッダー フィールドの値に基づく、レイヤ 3 またはレイヤ 4 プロトコルの一致条件を使用します。照合するプロトコルをキーワードで選択するか、プロトコル ID を入力します。
  - [すべてのトラフィック] : 任意のプロトコルからのすべてのトラフィックを許可します。
  - [リストから選択] : 選択したプロトコルを照合します（IP、ICMP、IGMP、TCP、UDP）。
  - [カスタム] : リストに名前がないプロトコルを照合します。プロトコル ID を入力します。プロトコル ID は、IANA によって割り当てられた標準値です。数値の範囲は 0 ～ 255 です。

（注） [プロトコル] が [すべてのトラフィック] である場合、[送信元アドレス] と [宛先アドレス] は必須です。

- [送信元ポート]：ルールの一致条件に送信元ポートを含めます。送信元ポートは、データグラム ヘッダーで識別されます。
  - [任意]：任意のポートを送信元ポートとして使用できます。
  - [リストから選択]：送信元ポートに関連付けられたキーワードを照合します（ftp、ftpdata、http、smtp、snmp、telnet、tftp、www）。これらの各キーワードは、同等のポート番号に変換されます。
  - [カスタム]：データグラム ヘッダーの送信元ポート番号と、指定した IANA ポート番号を照合します。ポートの範囲は 0 ～ 65535 で、3 種類のポートが含まれます。
    - 0 ～ 1023：ウェルノウン ポート
    - 1024 ～ 49151：登録済みポート
    - 49152 ～ 65535：ダイナミック ポート/プライベート ポート

- [宛先ポート]：ルールの一致条件に宛先ポートを含めます。宛先ポートは、データグラム ヘッダーで識別されます。
  - [任意]：任意のポートを宛先ポートとして使用できます。
  - [リストから選択]：送信元ポートに関連付けられたキーワードを照合します（ftp、ftpdata、http、smtp、snmp、telnet、tftp、www）。これらの各キーワードは、同等のポート番号に変換されます。
  - [カスタム]：データグラム ヘッダーの送信元ポート番号と、指定した IANA ポート番号を照合します。ポートの範囲は 0 ～ 65535 で、3 種類のポートが含まれます。
    - 0 ～ 1023：ウェルノウン ポート
    - 1024 ～ 49151：登録済みポート
    - 49152 ～ 65535：ダイナミック ポート/プライベート ポート

- [サービス タイプ]：パケットとクラス基準の照合に使用するサービスのタイプを指定します。
  - [任意]：任意のサービス タイプを一致条件として使用できます。
  - [IP DSCP] [リストから選択]：一致基準として使用する DSCP 値を選択します。
  - [IP DSCP] [値と照合]：0 ～ 63 のカスタム DSCP 値を入力します。
  - [IP プレシデンス]：パケットの IP プレシデンス値と、このフィールドで定義する IP プレシデンス値を照合します。IP プレシデンスの範囲は 0 ～ 7 です。
  - [IP ToS ビット]：一致基準として、IP ヘッダー内のパケットのタイプ オブ サービス（ToS）ビットを使用します。IP ToS ビット値の範囲は、00 ～ FF です。上位 3 ビットは、IP プレシデンス値を表します。上位 6 ビットは、IP DSCP 値を表します。

- [IP ToS マスク] : IP ToS マスク値を入力します。この値によって、パケットの IP ToS フィールドとの比較に使用される IP ToS ビット値のビット位置が示されます。

  IP ToS マスク値は 00 ～ ff の 2 桁の 16 進数です。IP ToS マスクの値が非 0 のビットは、パケットの IP ToS フィールドとの比較に使用される IP ToS ビット値のビット位置を示します。

ステップ 7 [OK] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

（注） クラスマップを削除または変更するには、リストからクラスマップ名を選択して[削除]をクリックします。ポリシーに割り当てられている場合は、そのクラスマップを削除することはできません。

ステップ 8 [保存] をクリックします。

IPv6 トラフィック クラスの設定

IPv6 クラス マップを追加して設定するには

ステップ 1 [クライアント QoS] > [トラフィック クラス] の順に選択します。

ステップ 2 [□] をクリックしてトラフィック クラスを追加します。

（注） クラス マップの最大数は 50 です。

ステップ 3 [トラフィック クラス名] フィールドに、新しいクラス マップの名前を入力します。名前には、1 ～ 31 文字の英数字と特殊文字を使用できます。スペースは使用できません。

ステップ 4 リストからトラフィック クラスの種類として [IPv6] を選択します。IPv6 トラフィック クラスは、WAP デバイスの IPv6 トラフィックにのみ適用されます。

ステップ 5 次のように設定します。

- [送信元アドレス] : パケットの送信元 IPv6 アドレスと、適切なフィールドで定義された IPv6 アドレスが一致する必要があります。
  - **[任意]** : 任意の IPv6 アドレスを送信元アドレスとして使用できます。
  - [シングル アドレス] : この基準を適用する IPv6 アドレスを入力します。
  - **[アドレス/マスク]** : 送信元 IPv6 アドレスのプレフィクス長を入力します。
- [宛先アドレス] : パケットの宛先 IPv4 アドレスと、適切なフィールドで定義された IPv4 アドレスが一致する必要があります。
  - **[任意]** : 任意の IPv6 アドレスを宛先アドレスとして使用できます。
  - [シングル アドレス] : この基準を適用する IPv6 アドレスを入力します。
  - [アドレス/マスク] : 宛先 IPv6 アドレスを入力し、宛先 IPv6 アドレスのプレフィクス長を入力します。

ステップ 6 [詳細] をクリックして次のパラメータを設定します。

- [プロトコル]：IPv4 パケットの IP プロトコル フィールドまたは IPv6 パケットのネクスト ヘッダー フィールドの値に基づく、レイヤ 3 またはレイヤ 4 プロトコルの一致条件を使用します。照合するプロトコルをキーワードで選択するか、プロトコル ID を入力します。
  - [すべてのトラフィック]：任意のプロトコルからのすべてのトラフィックを許可します。
  - [リストから選択]：選択したプロトコルを照合します（IP、ICMP、IGMP、TCP、UDP）。
  - [カスタム]：リストに名前がないプロトコルを照合します。プロトコル ID を入力します。プロトコル ID は、IANA によって割り当てられた標準値です。数値の範囲は 0 ～ 255 です。
- [送信元ポート]：ルールの一致条件に送信元ポートを含めます。送信元ポートは、データグラム ヘッダーで識別されます。

  （注） [プロトコル] が [すべてのトラフィック] である場合、[送信元アドレス] と [宛先アドレス] は必須です。

  - [任意]：任意のポートを送信元ポートとして使用できます。
  - [リストから選択]：送信元ポートに関連付けられたキーワードを照合します（ftp、ftpdata、http、smtp、snmp、telnet、tftp、www）。これらの各キーワードは、同等のポート番号に変換されます。
  - [カスタム]：データグラム ヘッダーの送信元ポート番号と、指定した IANA ポート番号を照合します。ポートの範囲は 0 ～ 65535 で、3 種類のポートが含まれます。
    - 0 ～ 1023：ウェルノウン ポート
    - 1024 ～ 49151：登録済みポート
    - 49152 ～ 65535：ダイナミック ポート/プライベート ポート
- [宛先ポート]：ルールの一致条件に宛先ポートを含めます。宛先ポートは、データグラム ヘッダーで識別されます。
  - [任意]：任意のポートを宛先ポートとして使用できます。
  - [リストから選択]：送信元ポートに関連付けられたキーワードを照合します（ftp、ftpdata、http、smtp、snmp、telnet、tftp、www）。これらの各キーワードは、同等のポート番号に変換されます。
  - [カスタム]：データグラム ヘッダーの送信元ポート番号と、指定した IANA ポート番号を照合します。ポートの範囲は 0 ～ 65535 で、3 種類のポートが含まれます。
    - 0 ～ 1023：ウェルノウン ポート
    - 1024 ～ 49151：登録済みポート
    - 49152 ～ 65535：ダイナミック ポート/プライベート ポート
- [IPv6 フロー ラベル]：フロー ラベルは、フロー内のパケットにラベルを付けるためにノードで使用されます。

- [任意]：IPv6 パケット固有の任意の 20 ビット値。
- [ユーザ定義]：IPv6 パケット固有の 20 ビット値を入力します。ルータでの QoS 処理を表すためにエンド ステーションで使用されます（0 ～ FFFFF の範囲）。

- [サービス タイプ]：パケットとクラス基準の照合に使用するサービスのタイプを指定します。
  - [任意]：任意のサービス タイプを一致条件として使用できます。
  - [IP DSCP] [リストから選択]：一致基準として使用する DSCP 値を選択します。
  - [IP DSCP] [値と照合]：0 ～ 63 のカスタム DSCP 値を入力します。

ステップ 7 [OK] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

（注） クラスマップを削除または変更するには、リストからクラスマップ名を選択して [削除] をクリックします。ポリシーに割り当てられている場合は、そのクラスマップを削除することはできません。

ステップ 8 [保存] をクリックします。

MAC トラフィック クラスの設定

MAC クラス マップを追加して設定するには、次の手順を実行します。

ステップ 1 [クライアント QoS] > [トラフィック クラス] の順に選択します。

ステップ 2 [□] をクリックしてトラフィック クラスを追加します。

（注） クラス マップの最大数は 50 です。

ステップ 3 [トラフィック クラス名] フィールドに、新しいクラス マップの名前を入力します。名前には、1 ～ 31 文字の英数字と特殊文字を使用できます。スペースは使用できません。

ステップ 4 [クラス マップ タイプ] リストから、クラス マップの種類として [MAC] を選択します。MAC クラス マップは、レイヤ 2 基準に適用されます。

ステップ 5 [送信元アドレス]：ルールの一致条件に送信元 MAC アドレスを含めます。

- **[任意]**：任意の MAC アドレスを送信元アドレスとして使用できます。
- [シングル アドレス]：イーサネット フレームと比較する送信元 MAC アドレスを入力します。
- [アドレス/マスク]：イーサネット フレームと比較する宛先 MAC アドレスのビットを指定する送信元 MAC アドレス マスクを入力します。

  MAC マスクのそれぞれのビット位置について、1 は対応するアドレス ビットが有効なことを示し、0 はアドレス ビットが無視されることを示します。たとえば、MAC アドレスの最初の 4 オクテットの

みをチェックするには、MAC マスク ff:ff:ff:ff:00:00 を使用します。MAC マスク ff:ff:ff:ff:ff:ff ではすべてのアドレス ビットがチェックされるため、単一の MAC アドレスを照合する場合に使用します。

ステップ 6 [宛先アドレス]：ルールの一致条件に宛先 MAC アドレスを含めます。

- **[任意]**：任意の MAC アドレスを宛先アドレスとして使用できます。
- [シングル アドレス]：イーサネット フレームと比較する宛先 MAC アドレスを入力します。
- [アドレス/マスク]：イーサネット フレームと比較する宛先 MAC アドレスのビットを指定する宛先 MAC アドレス マスクを入力します。

ステップ 7 [詳細] をクリックして次のパラメータを設定します。

- [プロトコル]：一致基準とイーサネット フレームのヘッダーにある値を比較します。EtherType のキーワードを選択するか、EtherType の値を入力して、一致基準を指定します。
  - [すべてのトラフィック]：任意のプロトコルからのすべてのトラフィックを許可します。
  - [リストから選択]：データグラム ヘッダーの Ethertype と、選択したプロトコル タイプを照合します。（Apple Talk、ARP、IPv4、IPv6、IPX、NETBIOS、PPPoE）。
  - [カスタム]：データグラム ヘッダーの Ethertype と、指定したカスタム プロトコル識別子を照合します。値は、0600 ～ FFFF の範囲の 4 桁の 16 進数を使用できます。

  （注） [プロトコル] が [すべてのトラフィック] である場合、[送信元アドレス] と [宛先アドレス] は必須です。

- [サービス クラス]：パケットを照合するためのサービス クラス 802.1p のユーザ プライオリティ値を指定します。
  - [任意]：任意のサービス クラスが許容されます。
  - [ユーザ定義]：イーサネット フレームと比較する 802.1p ユーザ プライオリティを入力します。有効な範囲は 0 ～ 7 です。
- [VLAN ID]：イーサネット フレームと比較する VLAN ID です。
  - [任意]：任意の VLAN ID 値が許容されます。
  - [ユーザ定義]：イーサネット フレームと比較する具体的な VLAN ID を入力します。このフィールドは最初または唯一の 802.1Q VLAN タグのみにあります。ポートの範囲は 1 ～ 4094 です。

ステップ 8 [OK] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

（注） クラス マップを削除または変更するには、リストからクラス マップを選択して [削除] をクリックします。ポリシーに割り当てられている場合は、そのクラス マップを削除することはできません。

ステップ 9 [保存] をクリックします。

Qos ポリシー

パケットは、定義された基準に基づいて分類および処理されます。分類基準は、[クラス マップ] ページのクラスで定義されます。処理は、[ポリシー マップ] ページのポリシー属性で定義されます。ポリシー属性は、クラスごとのインスタンスベースで分類され、クラス基準と照合するトラフィックの処理方法を決定します。

WAP デバイスには最大 50 個のポリシーと、ポリシーあたり最大 10 個のクラスを維持できます。

ポリシー マップを追加および設定するには

ステップ 1 [クライアント QoS] > [QoS ポリシー] の順に選択します。

ステップ 2 [□] をクリックして QoS ポリシーを追加します。[QoS ポリシー名] フィールドに、QoS ポリシーの名前を入力します。名前には、1 ～ 31 文字の英数字と特殊文字を使用できます。スペースは使用できません。

ステップ 3 以前に作成した関連付けられているトラフィック クラスを選択できます□。

ステップ 4 [QoS ポリシー定義] 領域で、ポリシー マップの次のパラメータを設定します。

- [認定レート] : トラフィックが準拠する必要がある認定レート（Kbps 単位）。範囲は 1 ～ 1000000 Kbps です。
- [認定バースト] : トラフィックが準拠する必要がある認定バースト サイズ（バイト単位）。範囲は 1 ～ 1600000 Kbps です。
- [アクション] : 次のいずれかのオプションを選択します。
  - [送信] : トラフィック クラス基準を満たす場合に、関連するトラフィック ストリームのすべてのパケットを転送するよう指定します。
  - [ドロップ] : トラフィック クラス基準を満たす場合に、関連するトラフィック ストリームのすべてのパケットをドロップするよう指定します。
- [リマーク トラフィック] : 関連するトラフィック ストリームのすべてのパケットを、802.1p ヘッダーのプライオリティ フィールドで指定したサービス クラス値でマークします。パケットにこのヘッダーが含まれていない場合は、ヘッダーを挿入します。CoS 値は、0 ～ 7 の整数です。
  - [COS のリマーク] : ネットワーク トラフィックを複数のプライオリティ レベルまたはサービス クラスに分割できます。CoS 値は 0 ～ 7 で、0 が最もプライオリティが低く、7 が最もプライオリティが高くなります。
  - [DSCP のリマーク] : 指定された QoS に基づき、パケットに適用される特定の Per-Hop Behavior（PHB）を指定します。ドロップダウン リストから値を選択します。
  - [IP プレシデンスのリマーク] : 関連するトラフィック ストリームのすべてのパケットを、指定した IP プレシデンス値でマークします。IP プレシデンス値は、0 ～ 7 の整数です。

ステップ 5 [ポリシー属性の追加] をクリックします。他のクラス マップを追加できますが、この特定ポリシーのクラス マップ数は最大 10 個に制限されています。

ステップ 6 [保存] をクリックします。

（注） QoS ポリシーを削除または変更するには、リストから QoS ポリシーを選択して [削除] または [編集] をクリックします。

QoS アソシエーション

[QoS アソシエーション] ページでは、ワイヤレスおよびイーサネット インターフェイスの QoS の特定の側面に対する制御を提供します。

QoS では一般的なトラフィック カテゴリの制御に加えて、QoS ポリシー名を使用してさまざまなマイクロフローをクライアントごとに調整できます。QoS ポリシー名は、一般的なマイクロフローの定義や処理の特徴を確立するのに便利なツールです。ネットワーク上で認証されている場合は、送受信両方のワイヤレス クライアントに適用できます。

QoS アソシエーション パラメータを設定するには、次の手順に従います。

ステップ 1 **[クライアント QoS]** > **[クライアント QoS アソシエーション]** の順に選択します。

ステップ 2 [□] をクリックしアソシエーションを追加します。

ステップ 3 [QoS ポリシー名] ドロップダウン リストから QoS ポリシー名を選択します。

ステップ 4 次のように設定します。

- [レート制限（AP からクライアント）] : WAP デバイスからクライアントへの最大許容送信レートを 1 秒あたりのビット数（bps）で入力します。有効な範囲は 0 ～ 1733 Mbps です。
- [レート制限（クライアントから AP）] : クライアントから WAP デバイスへの最大許容送信レートを 1 秒あたりのビット数（bps）で入力します。有効な範囲は 0 ～ 1733 Mbps です。

ステップ 5 [保存] をクリックします。

（注） インターフェイスは QoS ポリシーまたは ACL のいずれかにバインドできますが、両方にはバインドできません。

ゲスト アクセス

WAP デバイスでデフォルトの CP インスタンスを設定できます。CP インスタンスは、複数のインスタンス パラメータからなる定義済みセットです。インスタンスは、1 つまたは複数の VAP と関連付けることができます。

VAP に接続しているワイヤレス クライアントを使用して任意の URL にアクセスすると、[アクセス コントロール/ゲスト アクセス] ページで設定した [Web ポータル ロケール] ページへの URL が Web によりハイジャックされます。

[Web ポータル ロケール] によりハイジャック GUI ページの表示スタイルが定義され、[ゲスト グループ] によりユーザのユーザ名とパスワードが決定します。

ゲスト アクセス インスタンスを設定するには、次の手順に従います。

ステップ 1 [Web ポータル ロケール テーブル] を編集し、ハイジャックされる GUI ページの表示を設計します。[プレビュー] タブをクリックすると、表示を確認できます。

ステップ 2 [ゲスト グループ テーブル] を編集し、[ゲスト ユーザの合計] の数値リンクをクリックしてユーザを追加し、[保存] をクリックします。

ステップ 3 [ゲスト アクセス インスタンス テーブル] を設定し、前述の手順で設定した [ゲスト グループ] と [Web ポータル ロケール] を選択します。

ステップ 4 **[ワイヤレス]i** > **[ネットワーク]** に移動し、VAP ゲスト アクセスを関連付け、ゲスト アクセス インスタンスを設定します。

ゲスト アクセス インスタンス テーブル

ステップ 1 **[ゲスト アクセス]** > **[ゲスト アクセス インスタンス テーブル]** の順に選択します。

ステップ 2 [ゲスト アクセス インスタンス名] フィールドに CP インスタンスの名前を指定します。この名前には最大で 32 文字の英数字を含めることができます。

ステップ 3 [キャプティブ ポータルインスタンス パラメータ]エリアが、追加のオプションとともに再表示されます。次のパラメータを設定します。

- [プロトコル]：検証プロセスで使用する CP インスタンスのプロトコルとして、[HTTP] または [HTTPS] を選択します。
  - [HTTP]：検証時に暗号化を使用しません。
  - [HTTPS]：暗号化のために証明書を必要とするセキュア ソケット レイヤ（SSL）を使用します。証明書は、接続時にユーザに提示されます。
- [認証方式]：CP がクライアントを検証するために使用する認証方式を選択します。次のオプションが用意されています。
  - [ローカル データベース]：この WAP デバイスは、ローカル データベースを使用してユーザを認証します。[ローカル データベース] 設定を使用する場合は次のように設定します。
    - [ゲスト グループ名]：ゲスト グループの名前を入力します。
    - [アイドル タイムアウト]：アイドル タイムアウトの時間を分数単位で入力します。

- [最大帯域幅アップストリーム]：キャプティブ ポータルを使用する場合にクライアントがトラフィックを送信できる最大アップロード速度をMbps単位で入力します。この設定により、ネットワークにデータを送信するために使用される帯域幅が制限されます。範囲は 0 ～ 1733 Mbps です。デフォルトは 0 です。
- [最大帯域幅ダウンストリーム]：キャプティブ ポータルを使用する場合にクライアントがトラフィックを受信できる最大ダウンロード速度をMbps単位で入力します。この設定により、ネットワークからデータを受信するために使用される帯域幅が制限されます。範囲は 0 ～ 1733 Mbps です。デフォルトは 0 です。
- [ゲスト ユーザの合計]：ゲスト ユーザの合計数。

- [RADIUS 認証]：この WAP デバイスは、リモート RADIUS サーバ上のデータベースを使用してユーザを認証します。[RADIUS 認証] 設定を使用する場合は次のように設定します。
  - [RADIUS IP ネットワーク]：ドロップダウン リストから RADIUS IP ネットワークを選択します（[IPv4] または [IPv6]）。
  - [グローバル RADIUS]：グローバル RADIUS を有効にするには [有効化] をオンにします。CP 機能に異なる一連の RADIUS サーバを使用させる場合は、このチェックボックスをオフにして、このページのフィールドでサーバを設定します。
  - [RADIUSアカウンティング]：特定のユーザが消費したリソース（システム時間、送受信データ量など）を追跡および測定するには、[有効化] をオンにします。

    RADIUSアカウンティングを有効にすると、プライマリRADIUSサーバ、すべてのバックアップ サーバ、およびすべての設定済みサーバに対してこれが有効になります。
  - [サーバのIPアドレス - 1] または [サーバのIPv6アドレス - 1]：このVAPのプライマリ RADIUS サーバの IPv4 または IPv6 アドレスを入力します。IPv4 アドレスは、xxx.xxx.xxx.xxx（192.0.2.10）の形式にする必要があります。IPv6 アドレスは、xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx（2001:DB8::CAD5:7D91）の形式にする必要があります。

    最初のワイヤレス クライアントが VAP による認証を試みると、WAP デバイスは認証要求をプライマリ サーバに送信します。プライマリ サーバが認証要求に応答すると、WAP デバイスはこのRADIUSサーバを引き続きプライマリ サーバとして使用し、認証要求が指定されたアドレスに送信されます。

    [サーバの IP アドレス - 2] または [サーバの IPv6 アドレス - 2]：バックアップ RADIUS サーバの IPv4 または IPv6 アドレスを最大 3 つまで入力します。プライマリ サーバでの認証に失敗した場合、設定された各バックアップ サーバが順番に試行されます。
  - [キー - 1]：WAPデバイスがプライマリ RADIUSサーバへの認証に使用する共有秘密キーを入力します。最大63文字の標準英数字および特殊文字を使用できます。キーは大文字と小文字が区別され、RADIUS サーバで設定されたキーと一致している必要があります。入力するテキストはアスタリスクとして表示されます。

    [キー - 2]：設定されたバックアップ RADIUS サーバに関連付けられている RADIUS キー。[サーバ IP アドレス 1] のサーバは [キー 1] を使用し、[サーバ IP アドレス 2] のサーバは [キー 2] を使用します。以降も同様です。

- [認証なし]：ユーザは、データベースによって認証される必要がありません。
- [サードパーティ クレデンシャル（Party Credentials）]：WAP デバイスでは、ユーザ認証のために、ソーシャル メディア上のクレデンシャルが使用されます。認証済みサードパーティ クレデンシャルの設定を使用する場合は、次のように構成します
  - [受け入れられたクレデンシャル（Accepted credentials）]：クレデンシャル認証として、Facebook または Google、あるいはその両方を選択します。
  - [Walled Garden]：[受け付けられたクレデンシャル（Accepted credentials）] が選択されている間、関係するデフォルト構成が自動的に設定されます

（注） シスコでは、データ保護、プライバシー、およびセキュリティ要件を、新商品のコンセプト考案から発売までの製品設計および開発手法に統合します。詳細については、*https://www.cisco.com/c/en/us/about/trust-center/gdpr.html*を参照してください。

- [Active Directory サービス（Active Directory Service）]：この WAP デバイスは、リモート ADS サーバ上のデータベースを使用してユーザを認証します。ADS 認証の設定を使用する場合は次のように設定します。
  - [Active Directory サーバ（Active Directory Servers）]：[□] アイコンをクリックすることにより、新しい ADS サーバを追加します。サーバは 3 個まで追加できます。矢印を使用することにより、サーバを移動して優先順位を決めます。構成を削除するには、[ゴミ箱（trash can）] を選択します。[テスト（Test）] を使用して、ADS サーバが有効かどうかを確認します。

- [ゲスト グループ]：[認証方式] に [ローカル データベース] または [RADIUS 認証] が設定されている場合は、以前に作成したゲスト グループを選択します。このグループに属しているすべてのユーザは、このポータルを介してネットワークにアクセスすることが許可されます。
- [リダイレクト URL]：URL リダイレクトを有効にするには、URL（http:// を含む）を入力します。0 ～ 256 文字で入力します。
- [セッション タイムアウト]：CP セッションが有効な状態である残り時間を秒単位で入力します。この時間が 0 に達すると、クライアントの認証が解除されます。範囲は 0 ～ 1440 分です。デフォルト値は 0 です。
- [Web ポータル ロケール]：ドロップダウン リストから、以前に作成した Web ポータル ロケールを選択します。

ステップ 4 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

ゲスト グループ テーブル

デバイスでは各ローカル ユーザがユーザ グループに割り当てられ、このユーザ グループが CP インスタンスに割り当てられます。このグループにより、CP インスタンスへのユーザ割り当ての管理が容易になります。

「Default」という名前のユーザ グループが組み込まれており、削除できません。

ローカル ユーザを設定するには、次の手順を実行します。

ステップ 1 [ゲスト アクセス] > [ゲスト グループ テーブル] の順に選択します。

ステップ 2 [ゲスト グループ設定] 領域で、次のパラメータを設定します。

- [ゲスト グループ名] : 新しいゲスト グループの名前を指定します。デフォルトのゲスト グループ名は [デフォルト] です。

ステップ 3 次のパラメータを設定します。

- [アイドル タイムアウト] : クライアントと WAP デバイスとの関連付けが解除された後に、ユーザが CP 認証済みクライアント リストに保持される時間を入力します。クライアントが再認証を試みる前に、このフィールドで指定された時間が経過すると、クライアント エントリが認証済みクライアント リストから削除されます。範囲は 0 ～ 1440 分です。デフォルト値は 60 です。ここで設定したタイムアウト値は、ユーザ値が 0 に設定されないかぎり、CP インスタンスに関して設定された値よりも優先されます。0 に設定されている場合は、CP インスタンスに関して設定されているタイムアウト値が使用されます。
- [最大帯域幅アップストリーム] : キャプティブ ポータルを使用する場合にクライアントがトラフィックを送信できる最大アップロード速度を Mbps 単位で入力します。この設定により、ネットワークにデータを送信するために使用される帯域幅が制限されます。0 ～ 1733 Mbps の範囲で入力します。デフォルトは 0 です。
- [最大帯域幅ダウンストリーム] : キャプティブ ポータルを使用する場合にクライアントがトラフィックを受信できる最大ダウンロード速度を Mbps 単位で入力します。この設定により、ネットワークからデータを受信するために使用される帯域幅が制限されます。0 ～ 1733 Mbps の範囲で入力します。デフォルトは 0 です。
- [ゲスト ユーザの合計] : ゲスト ユーザの合計数を表示します。[ゲスト ユーザの合計] の数値リンクをクリックすると、[ゲスト ユーザ アカウント] ページが表示されます。

ステップ 4 [保存] をクリックします。

ゲスト ユーザ アカウント

ゲスト ユーザ アカウントを設定するには、次の手順に従います。

ステップ 1 [ゲスト アクセス] > [ゲスト グループ テーブル] の順に選択します。

ステップ 2 [ゲスト ユーザの合計] フィールドの数値リンクをクリックします。[ゲスト ユーザ アカウント] ページに [ゲスト ユーザ アカウント テーブル] が表示されます。

ステップ 3 [□] をクリックしてユーザを追加します。

ステップ 4 [ゲスト ユーザ名] : 新しいゲスト ユーザの名前を入力します。この名前には最大で 32 文字の英数字を含めることができます。

ステップ 5 [ゲスト ユーザ パスワード] : パスワードを入力します。パスワードには、8 ～ 64 文字の英数字と特殊文字を使用できます。

ステップ 6 [保存] をクリックします。

（注） [ゲスト アクセス] ページを表示するには [戻る] ボタン リンクをクリックします。

ゲスト ユーザを削除または変更するには、ゲスト ユーザを選択してから [削除] または [編集] をクリックします。

Web ポータルのカスタマイズ

CP インスタンスを VAP に関連付けた後、ロケールを作成して、それを CP インスタンスにマッピングします。CP インスタンスに関連付けられた VAP にユーザがアクセスすると、認証ページが表示されます。

[Web ポータルのカスタマイズ] ページを使用して、ネットワーク上のさまざまなロケールに固有のページを作成し、ページのテキストと画像をカスタマイズします。

ステップ 1 **[ゲスト アクセス]** > **[Web ポータル ロケール テーブル]** の順に選択します。

ステップ 2 このテーブルで [追加] をクリックし、[キャプティブ ポータルのカスタマイズ] ページにアクセスします。ロケールを変更するには、当該行をオンにして [編集] をクリックするか、削除する場合は [削除] をクリックします。

ネットワーク上の異なるロケールによって最大 3 つの異なる認証ページを作成できます。

ステップ 3 [キャプティブ ポータル Web ロケール パラメータ] 領域で、次の設定を行います。

- [Web ポータル ロケール名] : ページに割り当てる Web ロケールの名前を入力します。この名前は 1 ～ 32 文字の英数字で指定できます。

ステップ 4 [キャプティブ ポータル Web ロケール パラメータ] 領域に、ロケールを変更するための追加のオプションが表示されます。[ゲスト アクセス インスタンス名] は編集できません。編集可能なフィールドにはデフォルト値が表示されます。次のパラメータを設定します。

- [ゲスト アクセス インスタンス名] : ゲスト アクセス インスタンスの名前を表示します。
- [背景画像] : [参照] をクリックして画像を選択します。[アップロード] をクリックすると、CP インスタンス用の画像をアップロードできます。
- [ロゴ画像] : [参照] をクリックしてロゴ画像を選択します。[アップロード] をクリックすると、ロゴ画像をアップロードできます。
- [前景の色] : 前景の色の HTML コードを 6 桁の 16 進数形式で入力します。1 ～ 32 文字で入力します。デフォルトは #FFFFFF です。

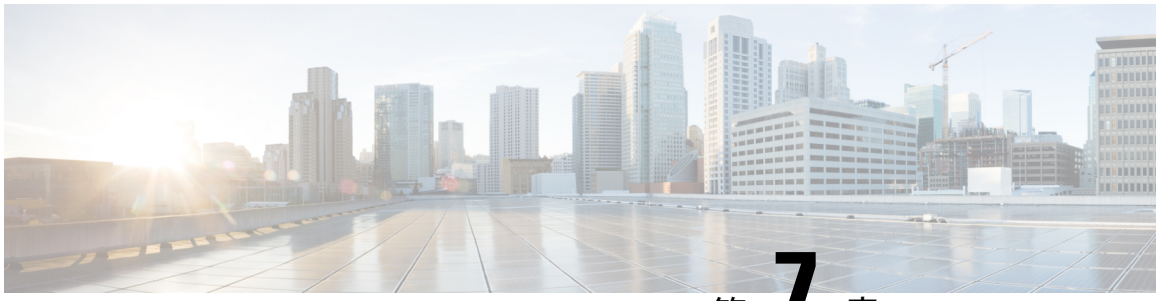
- [背景の色]：背景の色の HTML コードを 6 桁の 16 進数形式で入力します。1 ～ 32 文字で入力します。デフォルトは #FFFFFF です。
- [セパレータの色]：ページの見出し部とページの本文部を区切る太い横線の色の HTML コードを 6 桁の 16 進数形式で入力します。1 ～ 32 文字で入力します。デフォルトは #FFFFFF です。
- [アカウント画像]：[参照] をクリックして画像を選択します。[アップロード] をクリックすると、アカウント画像をアップロードできます。
- [フォント]：ドロップダウン リストからフォントを選択します。このフォントは、すべてのテキストを表示するときに使用されます。
- [アカウントのプロンプティング]：ユーザ名を入力します。1 ～ 32 文字で入力します。
- [ユーザ名のプロンプティング]：ユーザ名テキスト ボックスのラベルです。1 ～ 32 文字で入力します。
- [パスワードのプロンプティング]：ユーザ パスワード テキスト ボックスのラベルです。1 ～ 64 文字で入力します。
- [ボタンのプロンプティング]：認証のためにユーザ名とパスワードを送信する際にユーザがクリックするボタンのラベルです。2 ～ 32 文字で入力します。デフォルトは Connect です。
- [ブラウザ ヘッドのプロンプティング]：ブラウザのタイトル バーに表示されるテキストです。1 ～ 128 文字で入力します。デフォルトは Captive Portal です。
- [ポータル タイトルのプロンプティング]：ページ見出し部のロゴの右側に表示されるテキストです。1 ～ 128 文字で入力します。デフォルトは Welcome to the Wireless Network です。
- [アカウントのヒントのプロンプティング]：ページ本体のユーザ名とパスワードのテキスト ボックスの下に表示されるテキストです。1 ～ 256 文字で入力します。デフォルトは「このサービスの使用を開始するには、クレデンシャルを入力して [接続] ボタンをクリックします」です。
- [受け入れポリシー]：[利用規約] ボックスに表示されるテキストです。1 ～ 4096 文字で入力します。デフォルトは [利用規約] です。
- [受け入れのプロンプティング]：利用規約を読んで同意したことを確認するためにチェックボックスをオンにするようユーザに指示するテキストです。1 ～ 128 文字で入力します。
- [受け入れなしの警告]：ユーザが [利用規約] チェックボックスをオンにしないでログイン資格情報を送信した場合にポップアップ ウィンドウに表示されるテキストです。1 ～ 128 文字で入力します。
- [作業進行中のプロンプティング]：認証プロセス実行中に表示されるテキストです。1 ～ 128 文字で入力します。
- [無効な資格情報のプロンプティング]：ユーザが認証に失敗したときに表示されるテキストです。1 ～ 128 文字で入力します。
- [接続成功のプロンプティング]：クライアントが VAP に対して認証されたときに表示されるテキストです。1 ～ 128 文字で入力します。
- [ウェルカム プロンプティング]：クライアントがネットワークに接続されたときに表示されるテキストです。1 ～ 256 文字で入力します。

- [復元]：現在のロケールを削除します。

ステップ 5 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

ステップ 6 [プレビュー] をクリックすると、更新されたページが表示されます。

[プレビュー] をクリックすると、すでにスタートアップ コンフィギュレーションに保存されているテキストと画像が表示されます。変更を加えた場合、変更を確認するには、[プレビュー] をクリックする前に [保存] をクリックしてください。



第 7 章

アクセスコントロール

この章では、WAP デバイスの ACL と Quality Of Service（QoS）機能を設定する方法について説明します。具体的な内容は次のとおりです。

- ACL （107 ページ）
- クライアント QoS （116 ページ）
- ゲスト アクセス （124 ページ）

ACL

アクセス コントロール リスト（ACL）は、ルールと呼ばれる許可条件および拒否条件を集めたものであり、権限を持たないユーザをブロックし、権限を持つユーザに特定のリソースへのアクセスを許可することによってセキュリティを提供します。ACL では、ネットワーク リソースに到達しようとする是認されていないすべての試行をブロックできます。

WAP デバイスは、最大 50 個の IPv4、IPv6、および MAC ACL と、各 ACL で最大 10 個のルールをサポートしています。各 ACL では複数のインターフェイスがサポートされています。

IPv4 と IPv6 の ACL

各 ACL は WAP デバイスが受信するトラフィックに適用されるルールのセットです。各ルールは、所定のフィールドの内容によって、ネットワークへのアクセスを許可するのか拒否するのかを指定します。さまざまな基準に基づいたルールを設定でき、それらを送信元または宛先の IP アドレス、送信元または宛先のポート、パケットで伝送されているプロトコルなど、パケット内の 1 個以上のフィールドに適用できます。IP ACL はレイヤ 3 および 4 用にトラフィックを分類します。

（注） 作成するすべてのルールの終わりに暗黙の拒否があります。すべて拒否することのないよう、ACL に許可ルールを追加して、トラフィックを許可することを強くお勧めします。

MAC ACL

MAC ACL はレイヤ 2 ACL です。送信元または宛先の MAC アドレス、VLAN ID、Class of Service など、フレームのフィールドを検査するルールを設定できます。フレームが WAP デバイスのポートに入ると、WAP デバイスはフレームを検査して、ACL ルールをフレームの内容と照合します。内容と一致するルールがあった場合、許可アクションまたは拒否アクションがフレームに対して実行されます。

ACL を設定するためのワークフロー

ACLルールを使用してACLを設定した後、指定したインターフェイスにルールを適用します。

ACL を設定するには、次の手順に従います。

ステップ 1 [アクセス コントロール] > [ACL] の順に選択します。

ステップ 2 ACL テーブルで [□] をクリックして新しい行を追加し、ACL を作成します。

ステップ 3 ACL の名前を入力します。

ステップ 4 ドロップダウン リストから ACL タイプを選択します（[IPv4]、[IPv6]、[MAC]）。

ステップ 5 [□] をクリックし、ACL を適用する関連インターフェイスを選択して、[OK] をクリックします。関連インターフェイスを変更するには、[□] をクリックして選択されているインターフェイスを削除し、[□] をクリックして新たな関連インターフェイスを選択します。

ステップ 6 [詳細] をクリックすると、ACL パラメータが表示されます。

ステップ 7 次に ACL のルールを設定します。IPv4 ACL の場合は「IPv4 ACL の設定 （82 ページ）」を参照してください。IPv6 ACL の場合は「IPv6 ACL の設定 （85 ページ）」を参照してください。MAC ACL の場合は「MAC ACL の設定 （88 ページ）」を参照してください。

ステップ 8 [保存] をクリックしてすべての変更内容を保存します。

IPv4 ACL の設定

IPv4 ACL を設定するには、次の手順を実行してください。

ステップ 1 [アクセス コントロール] > [ACL] の順に選択します。

ステップ 2 [□] をクリックして ACL を追加します。

ステップ 3 ACL 名フィールドに ACL の名前を入力します。この名前には、スペースなしで最大 31 文字の英数字と特殊文字を使用できます。

ステップ 4 [ACL タイプ] リストから、ACL のタイプとして [IPv4] を選択します。IPv4 ACL は、レイヤ 3 およびレイヤ 4 基準に基づいてネットワーク リソースへのアクセスを制御します。

ステップ 5 [□] をクリックし、ACL を適用する関連付けられているインターフェイスを選択します。[OK] をクリックします。関連付けられているインターフェイスを変更するには、[□] をクリックして選択されているインターフェイスを削除し、[□] をクリックして新たな関連インターフェイスを選択します。

ステップ 6 [詳細] をクリックすると、設定パラメータが表示されます。ルールを追加して次のフィールドを設定するには、[□] をクリックします。

（注） ルールを追加しない場合、デフォルトで DUT はすべてのトラフィックを拒否します。

- [ルールの優先度]：ACL に複数のルールが設定されている場合、ルールは優先度に従ってパケットまたはフレームに適用されます。番号が小さいほど優先度が高くなります。新しいルールの優先度は、すべての明示的なルールの中で最下位になります。最下位の優先度ですべてのトラフィックを拒否する暗黙のルールが常に存在している点に注意してください。
- [アクション]：アクションを [拒否] するかまたは [許可] するかを選択します。デフォルトのアクションは [拒否] です。

  [許可] を選択した場合、このルールは、ルール基準を満たすすべてのトラフィックが WAP デバイスに入ることを許可します。基準を満たさないトラフィックはドロップされます。

  [拒否] を選択した場合、このルールは、ルール基準を満たすトラフィックが WAP デバイスに入ることを必ずブロックします。基準を満たさないトラフィックは、このルールが最後のルールでなければ転送されます。すべての ACL の最後に暗黙のすべて拒否ルールがあるため、明示的に許可されないトラフィックはすべてドロップされます。
- [サービス（プロトコル）]：[IP プロトコル] フィールドの値に基づいてレイヤ 3 プロトコルまたはレイヤ 4 プロトコルの一致条件を使用します。次のいずれかのオプションを選択できます。
  - [すべてのトラフィック]：ルールの条件に一致するすべてのトラフィックを許可します。
  - [リストから選択]：次のプロトコルから選択します。IP、ICMP、IGMP、TCP、または UDP。
  - [カスタム]：IANA によって割り当てられている標準プロトコル ID 0 ～ 255 を入力します。[リストから選択] にリストされていないプロトコルを指定する場合にこの方法を選択します。
- [送信元 IPv4 アドレス]：パケットの送信元 IP アドレスが、該当するフィールドに定義されているアドレスと一致する必要があります。
  - [任意]：すべての IP アドレスが許容されます。
  - [シングル アドレス]：この基準を適用する IP アドレスを入力します。
  - [アドレス/マスク]：送信元 IP アドレスのワイルド カード マスクを入力します。ワイルド カード マスクによって、使用するビットおよび無視するビットが決まります。ワイルド カード マスク 255.255.255.255 は、どのビットも検査しないことを示します。ワイルド カード 0.0.0.0 はすべてのビットを検査することを示します。このフィールドは、[送信元 IP アドレス] をオンにする場合は必須です。

    ワイルド カード マスクは基本的にはサブネット マスクの逆です。たとえば、単一のホスト アドレスと一致する基準の場合は、ワイルド カード マスク 0.0.0.0 を使用します。基準を 24 ビット サブネット（192.168.10.0/24 など）と照合するには、0.0.0.255 のワイルド カード マスクを使用します。
- [送信元ポート]：ルールの一致条件に送信元ポートを含めます。送信元ポートは、データグラム ヘッダーで識別されます。

- [すべてのトラフィック] : ルールの条件に一致するすべてのトラフィックを許可します。
- [リストから選択] : 照合する送信元ポートに関連付けるキーワード（ftp、ftpdata、http、smtp、snmp、telnet、tftp、www）を選択します。これらの各キーワードは、同等のポート番号に変換されます。
- [カスタム] : データグラム ヘッダーに示される送信元ポートと照合する IANA ポート番号を入力します。ポートの範囲は 0 ～ 65535 で、3 種類のポートが含まれます。
  - 0 ～ 1023：ウェルノウン ポート
  - 1024 ～ 49151：登録済みポート
  - 49152 ～ 65535：ダイナミック ポート/プライベート ポート

- [宛先 IPv4 アドレス] : パケットの宛先 IP アドレスは、該当するフィールドに定義されているアドレスと一致する必要があります。
  - [任意] : 任意の IP アドレスを入力します。
  - [シングル アドレス] : この基準を適用する IP アドレスを入力します。
  - [アドレス/マスク] : 宛先 IP アドレスのワイルド カード マスクを入力します。ワイルド カード マスクによって、使用するビットおよび無視するビットが決まります。ワイルド カード マスク 255.255.255.255 は、どのビットも検査しないことを示します。ワイルド カード 0.0.0.0 はすべてのビットを検査することを示します。このフィールドは [送信元 IP アドレス] を選択する場合は必須です。

    ワイルド カード マスクは基本的にはサブネット マスクの逆です。たとえば、単一のホスト アドレスと一致する基準の場合は、ワイルド カード マスク 0.0.0.0 を使用します。基準を 24 ビット サブネット（192.168.10.0/24 など）と照合するには、0.0.0.255 のワイルド カード マスクを使用します。

- [宛先ポート] : ルールの一致条件に宛先ポートを含めます。宛先ポートは、データグラム ヘッダーで識別されます。
  - [任意] : ルールの条件に一致する任意のポート。
  - [リストから選択] : 照合する宛先ポートに関連付けるキーワード（ftp、ftpdata、http、smtp、snmp、telnet、tftp、www）を選択します。これらの各キーワードは、同等のポート番号に変換されます。
  - [カスタム] : データグラム ヘッダーに示されている宛先ポートと照合する IANA ポート番号を入力します。ポートの範囲は 0 ～ 65535 で、3 種類のポートが含まれます。
    - 0 ～ 1023：ウェルノウン ポート
    - 1024 ～ 49151：登録済みポート
    - 49152 ～ 65535：ダイナミック ポート/プライベート ポート

- [タイプ オブ サービス] : 特定のサービス タイプに基づいてパケットを照合します。

- [任意]：任意のタイプ オブ サービス。
- [リストから選択]：DSCP 確認転送（AS）、サービス クラス（CS）、または緊急転送（EF）の値に基づいてパケットを照合します。
- [DSCP]：カスタム DSCP 値に基づいてパケットを照合します。選択した場合は、0 ～ 63 の値をこのフィールドに入力してください。
- [プレシデンス]：IP プレシデンス値に基づいてパケットを照合します。選択した場合は、0 ～ 7 の IP Precedence 値を入力してください。
- [ToS/マスク]：IP ToS マスク値を入力します。この値によって、パケットの IP ToS フィールドとの比較に使用される IP ToS ビット値のビット位置が識別されます。

  IP ToS マスク値は、00 ～ FF の 2 桁の 16 進数で、反転（ワイルド カード）マスクを表します。IP ToS マスクの値が 0 のビットは、パケットの IP ToS フィールドとの比較に使用される IP ToS ビット値のビット位置を示します。たとえば、IP ToS 値でビット 7 および 5 が設定されていてビット 1 がクリアなことを確認するには、ビット 7 が最も重要な場合、IP ToS ビット値 0 と IP ToS マスク 00 を使用します。

ステップ 7 [OK] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

（注） ACL を削除または変更するには、ACL を選択してから [削除] または [編集] をクリックします。

ルールを削除または編集するには、[ルール設定] 領域でルールを選択し、[削除] または [編集] をクリックします。

ステップ 8 [保存] をクリックします。

IPv6 ACL の設定

IPv6 ACL を設定するには、次の手順を実行してください。

ステップ 1 [アクセス コントロール] > [ACL] の順に選択します。

ステップ 2 [□] をクリックして ACL を追加します。

ステップ 3 ACL 名フィールドに ACL の名前を入力します。

ステップ 4 [ACL タイプ] リストから、ACL のタイプとして [IPv6] を選択します。IPv4 ACL は、レイヤ 3 およびレイヤ 4 基準に基づいてネットワーク リソースへのアクセスを制御します。

ステップ 5 [□] をクリックし、ACL を適用する関連付けられているインターフェイスを選択します。次に [OK] をクリックします。関連付けられているインターフェイスを変更するには、[□] をクリックして選択されているインターフェイスを削除し、[□] をクリックして新たな関連インターフェイスを選択します。

ステップ 6 [詳細] をクリックすると、設定パラメータが表示されます。ルールを追加して次のフィールドを設定するには、[□] をクリックします。

（注） ルールを追加しない場合、デフォルトで DUT はすべてのトラフィックを拒否します。

- [ルールの優先度]：ACL に複数のルールが設定されている場合、ルールは優先度に従ってパケットまたはフレームに適用されます。番号が小さいほど優先度が高くなります。新しいルールの優先度は、すべての明示的なルールの中で最下位になります。その優先度を変更するには、上または下のボタンをクリックします。最下位の優先度ですべてのトラフィックを拒否する暗黙のルールが常に存在している点に注意してください。
- [アクション]：アクションを [拒否] するかまたは [許可] するかを選択します。デフォルトのアクションは [拒否] です。

  [許可] を選択した場合、このルールは、ルール基準を満たすすべてのトラフィックが WAP デバイスに入ることを許可します。基準を満たさないトラフィックはドロップされます。

  [拒否] を選択した場合、このルールは、ルール基準を満たすトラフィックが WAP デバイスに入ることを必ずブロックします。基準を満たさないトラフィックは、このルールが最後のルールでなければ転送されます。すべての ACL の最後に暗黙のすべて拒否ルールがあるため、明示的に許可されないトラフィックはすべてドロップされます。
- [サービス（プロトコル）]：[IP プロトコル] フィールドの値に基づいてレイヤ 3 プロトコルまたはレイヤ 4 プロトコルの一致条件を使用します。次のいずれかのオプションを選択できます。
  - [すべてのトラフィック]：ルールの条件に一致するすべてのトラフィックを許可します。
  - [リストから選択]：次のプロトコルから選択します。IPv6、ICMPv6、TCP、UDP。
  - [カスタム]：IANA によって割り当てられている標準プロトコル ID 0 ～ 255 を入力します。[リストから選択] にリストされていないプロトコルを指定する場合にこの方法を選択します。
- [送信元 IPv6 アドレス]：パケットの送信元 IP アドレスが、該当するフィールドに定義されているアドレスと一致する必要があります。
  - [任意]：すべての IP アドレスが許容されます。
  - [シングル アドレス]：この基準を適用する IP アドレスを入力します。
  - [アドレス/マスク]：送信元 IP アドレスのワイルド カード マスクを入力します。ワイルド カード マスクによって、使用するビットおよび無視するビットが決まります。ワイルド カード マスク 255.255.255.255 は、どのビットも検査しないことを示します。ワイルド カード 0.0.0.0 はすべてのビットを検査することを示します。このフィールドは、[送信元 IP アドレス] をオンにする場合は必須です。

    ワイルド カード マスクは基本的にはサブネット マスクの逆です。たとえば、単一のホスト アドレスと一致する基準の場合は、ワイルド カード マスク 0.0.0.0 を使用します。基準を 24 ビット サブネット（192.168.10.0/24 など）と照合するには、0.0.0.255 のワイルド カード マスクを使用します。
- [送信元ポート]：ルールの一致条件に送信元ポートを含めます。送信元ポートは、データグラム ヘッダーで識別されます。
  - [任意]：任意の送信元アドレスが許容されます。

- [リストから選択]：照合する送信元ポートに関連付けるキーワード（ftp、ftpdata、http、smtp、snmp、telnet、tftp、www）を選択します。これらの各キーワードは、同等のポート番号に変換されます。
- [カスタム]：データグラム ヘッダーに示される送信元ポートと照合する IANA ポート番号を入力します。ポートの範囲は 0 ～ 65535 で、3 種類のポートが含まれます。
  - 0 ～ 1023：ウェルノウン ポート
  - 1024 ～ 49151：登録済みポート
  - 49152 ～ 65535：ダイナミック ポート/プライベート ポート

- [宛先 IPv6 アドレス]：パケットの宛先 IP アドレスは、該当するフィールドに定義されているアドレスと一致する必要があります。
  - [任意]：任意の IP アドレスを入力します。
  - [シングル アドレス]：この基準を適用する IP アドレスを入力します。
  - [アドレス/マスク]：宛先 IP アドレスのワイルド カード マスクを入力します。ワイルド カード マスクによって、使用するビットおよび無視するビットが決まります。ワイルド カード マスク 255.255.255.255 は、どのビットも検査しないことを示します。ワイルド カード 0.0.0.0 はすべてのビットを検査することを示します。このフィールドは [送信元 IP アドレス] を選択する場合は必須です。

    ワイルド カード マスクは基本的にはサブネット マスクの逆です。たとえば、単一のホスト アドレスと一致する基準の場合は、ワイルド カード マスク 0.0.0.0 を使用します。基準を 24 ビット サブネット（192.168.10.0/24 など）と照合するには、0.0.0.255 のワイルド カード マスクを使用します。

- [宛先ポート]：ルールの一致条件に宛先ポートを含めます。宛先ポートは、データグラム ヘッダーで識別されます。
  - [任意]：ルールの条件に一致する任意のポート。
  - [リストから選択]：照合する宛先ポートに関連付けるキーワード（ftp、ftpdata、http、smtp、snmp、telnet、tftp、www）を選択します。これらの各キーワードは、同等のポート番号に変換されます。
  - [カスタム]：データグラム ヘッダーに示されている宛先ポートと照合する IANA ポート番号を入力します。ポートの範囲は 0 ～ 65535 で、3 種類のポートが含まれます。
    - 0 ～ 1023：ウェルノウン ポート
    - 1024 ～ 49151：登録済みポート
    - 49152 ～ 65535：ダイナミック ポート/プライベート ポート

- [フロー ラベル]：IPv6 パケット固有の 20 ビット値を指定します。
  - [任意]：任意の 20 ビット数値。

- [DSCP]：カスタム DSCP 値に基づいて数値を照合します。

- [DSCP]：IP DSCP 値に基づいてパケットを照合します。
  - [任意]：任意の DSCP 値が許容されます。
  - [リストから選択]：ドロップダウン リストから DSCP 値を選択します。
  - [カスタム]：0 ～ 63 のカスタム DSCP 値を入力します。

ステップ 7 [OK] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

（注） ACL を削除または変更するには、ACL を選択してから [削除] または [編集] をクリックします。

ルールを削除または編集するには、[ルール設定] 領域でルールを選択し、[削除] または [編集] をクリックします。

ステップ 8 [保存] をクリックします。

MAC ACL の設定

MAC ACL を設定するには、次の手順を実行してください。

ステップ 1 [アクセス コントロール] > [ACL] の順に選択します。

ステップ 2 [□] をクリックして MAC ACL を追加します。

ステップ 3 [ACL 名] フィールドに ACL を識別する名前を入力します。

ステップ 4 リストから ACL の種類として [MAC] を選択します。MAC ACL は、レイヤ 2 基準に基づいてアクセスを制御します。

ステップ 5 [□] をクリックし、ACL を適用する関連付けられているインターフェイスを選択して [OK] をクリックします。関連付けられているインターフェイスを変更するには、[□] をクリックして選択されているインターフェイスを削除し、[□] をクリックして新たな関連インターフェイスを選択します。

ステップ 6 次に [詳細] をクリックすると、設定パラメータが表示されます。ルールを追加して次のパラメータを設定するには、[□] をクリックします。

- [ルールの優先度]：ACL に複数のルールが設定されている場合、ルールは優先度に従ってパケットまたはフレームに適用されます。番号が小さいほど優先度が高くなります。新しいルールの優先度は、すべての明示的なルールの中で最下位になります。「上」または「下」ボタンをクリックすると、この優先度を変更できます。最下位の優先度ですべてのトラフィックを拒否する暗黙のルールが常に存在している点に注意してください。

- [アクション]：アクションを [拒否] するかまたは [許可] するかを選択します。デフォルトのアクションは [拒否] です。

  [許可] を選択した場合、このルールは、ルール基準を満たすすべてのトラフィックが WAP デバイスに入ることを許可します。基準を満たさないトラフィックはドロップされます。

[拒否] を選択した場合、このルールは、ルール基準を満たすトラフィックが WAP デバイスに入ることを必ずブロックします。基準を満たさないトラフィックは、このルールが最後のルールでなければ転送されます。すべての ACL の最後に暗黙のすべて拒否ルールがあるため、明示的に許可されないトラフィックはすべてドロップされます。

- [サービス（ETH タイプ）]：イーサネット フレームのヘッダーにある値と比較する一致基準を選択します。ドロップダウン リストから ETH タイプを選択できます。
  - [任意]：任意のプロトコルが許容されます。
  - [リストから選択]：次のプロトコル タイプから選択します。ARP、IPv4、IPv6、IPX、NetBIOS、PPPoE。
  - [カスタム]：パケットを照合するカスタム プロトコル識別子を入力します。この値は、0600 ～ FFFF の範囲の 4 桁の 16 進数です。
- [送信元 MAC アドレス]：パケットの送信元 MAC アドレスが、該当するフィールドに定義されているアドレスと一致する必要があります。
  - [任意]：任意の送信元 MAC アドレスが許容されます。
  - [シングル アドレス]：イーサネット フレームと比較する送信元 MAC アドレスを入力します。
  - [アドレス/マスク]：イーサネット フレームと比較する送信元 MAC のビットを指定する送信元 MAC アドレス マスクを入力します。

    MAC マスクのそれぞれのビット位置について、0 は対応するアドレス ビットが有効なことを示し、1 はアドレス ビットが無視されることを示します。たとえば、MAC アドレスの最初の 4 オクテットのみをチェックするには、MAC マスク 00:00:00:00:ff:ff を使用します。MAC マスク 00:00:00:00:00:00 ではすべてのアドレス ビットがチェックされるため、単一の MAC アドレスを照合する場合に使用します。
- [宛先 MAC アドレス]：パケットの宛先 MAC アドレスが、該当するフィールドに定義されているアドレスと一致する必要があります。
  - [任意]：任意の宛先 MAC アドレスが許容されます。
  - [シングル アドレス]：イーサネット フレームと比較する宛先 MAC アドレスを入力します。
  - [アドレス/マスク]：イーサネット フレームと比較する宛先 MAC のビットを指定する宛先 MAC アドレス マスクを入力します。
- [VLAN ID]：イーサネット フレームと比較する VLAN ID です。
  - [任意]：任意の VLAN ID 値が許容されます。
  - [カスタム]：イーサネット フレームと比較する具体的な VLAN ID を入力します。このフィールドは最初または唯一の 802.1Q VLAN タグのみにあります。ポートの範囲は 1 ～ 4094 です。
- [サービス クラス]：パケットを照合するためのサービス クラス 802.1p のユーザ プライオリティ値を指定します。

- [任意]：任意のサービス クラスが許容されます。
- [カスタム]：イーサネット フレームと比較する 802.1p ユーザ プライオリティを入力します。有効な範囲は 0 ～ 7 です。

ステップ 7 [OK] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

（注） ACL を削除または変更するには、ACL を選択してから [削除] または [編集] をクリックします。ルールを削除または編集するには、[ルール設定] 領域でルールを選択し、[削除] または [編集] をクリックします。

ステップ 8 [保存] をクリックします。

クライアント QoS

クライアント Quality Of Service（QoS）は、ネットワークに接続するワイヤレス クライアント接続の制御に使用され、使用帯域幅を管理します。クライアント QoS は、HTTP トラフィックや特定のサブネットからのトラフィックなどを、アクセス コントロール リスト（ACL）を使って制御できます。ACL は、ルールと呼ばれる許可条件および拒否条件を集めたものであり、権限を持たないユーザをブロックし、権限を持つユーザに特定のリソースへのアクセスを許可することによってセキュリティを提供します。ACL では、ネットワーク リソースに到達しようとする是認されていないすべての試行をブロックできます。

トラフィック クラス

QoS 機能に含まれている差別化サービス（DiffServ）サポートにより、トラフィックをストリームに分類できます。また、ホップ別に定義されている動作に基づいて特定の QoS 処理も行われます。

標準の IP ベース ネットワークは、ベストエフォート型のデータ配信サービスを提供するように設計されています。ベストエフォート型サービスでは、保証はされませんが、ネットワークによってタイミング良くデータが配信されます。輻輳が発生している場合、パケットが遅延したり、散発的に送信されたり、ドロップしたりすることがあります。電子メールやファイル転送などの一般的なインターネット アプリケーションでは、サービスのわずかな低下は許容範囲内であり、たいていの場合は気づきません。ただし、音声やマルチメディアなどのタイミング要件が厳しいアプリケーションでは、サービスの低下が望ましくない影響を及ぼします。

DiffServ 設定は、IP プロトコルやその他の基準に従ってトラフィックを分類するクラス マップを定義することから始まります。その後、各クラス マップをトラフィック クラスの処理方法を定義するポリシー マップに関連付けることができます。時間的な制約のあるトラフィックが含まれるクラスを、ポリシー マップに割り当てることができます。

IPv4 トラフィック クラスの設定

IPv4 クラス マップを追加して設定するには

ステップ 1 [クライアント QoS] > [トラフィック クラス] の順に選択します。

ステップ 2 [□] をクリックしてトラフィック クラスを追加します。

（注） クラス マップの最大数は 50 です。

ステップ 3 [トラフィック クラス名] テキスト フィールドに、新しいクラス マップの名前を入力します。名前には、1 ～ 31 文字の英数字と特殊文字を使用できます。スペースは使用できません。

ステップ 4 [クラス タイプ] のリストから [IPv4] を選択します。IPv4 トラフィック クラスは、WAP デバイスの IPv4 トラフィックにのみ適用されます。

ステップ 5 次のように設定します。

- [送信元アドレス] : パケットの送信元 IPv4 アドレスと、適切なフィールドで定義された IPv4 アドレスが一致する必要があります。
  - **[任意]** : 任意の IPv4 アドレスを送信元アドレスとして使用できます。
  - [シングル アドレス] : この基準を適用する 1 つの IPv4 アドレスを入力します。
  - [アドレス/マスク] : 送信元 IPv4 アドレス マスクを入力します。DiffServ のマスクは、ドット付き 10 進表記の IP のネットワーク方式ビット マスクです。宛先 IP アドレスのどの部分を使用してパケット コンテンツと照合するのかを示します。

    DiffServ マスク 255.255.255.255 はすべてのビットが重要であること、マスク 0.0.0.0 は重要なビットがないことを示します。ACL ワイルド カード マスクでは反対になります。たとえば、基準と単一ホスト アドレスを照合するには、255.255.255.255 のマスクを使用します。基準を 24 ビット サブネット（192.168.10.0/24 など）と照合するには、255.255.255.0 のマスクを使用します。

- [宛先アドレス] : パケットの宛先 IPv4 アドレスと、適切なフィールドで定義された IPv4 アドレスが一致する必要があります。
  - **[任意]** : 任意の IPv4 アドレスを宛先アドレスとして使用できます。
  - [シングル アドレス] : この基準を適用する IPv4 アドレスを入力します。
  - [アドレス/マスク] : 宛先 IP アドレス マスクを入力します。

ステップ 6 [詳細] をクリックして次のパラメータを設定します。

- [プロトコル] : IPv4 パケットの IP プロトコル フィールドまたは IPv6 パケットのネクスト ヘッダー フィールドの値に基づく、レイヤ 3 またはレイヤ 4 プロトコルの一致条件を使用します。照合するプロトコルをキーワードで選択するか、プロトコル ID を入力します。
  - [すべてのトラフィック] : 任意のプロトコルからのすべてのトラフィックを許可します。
  - [リストから選択] : 選択したプロトコルを照合します（IP、ICMP、IGMP、TCP、UDP）。
  - [カスタム] : リストに名前がないプロトコルを照合します。プロトコル ID を入力します。プロトコル ID は、IANA によって割り当てられた標準値です。数値の範囲は 0 ～ 255 です。

（注） [プロトコル] が [すべてのトラフィック] である場合、[送信元アドレス] と [宛先アドレス] は必須です。

- [送信元ポート]：ルールの一致条件に送信元ポートを含めます。送信元ポートは、データグラム ヘッダーで識別されます。
  - [任意]：任意のポートを送信元ポートとして使用できます。
  - [リストから選択]：送信元ポートに関連付けられたキーワードを照合します（ftp、ftpdata、http、smtp、snmp、telnet、tftp、www）。これらの各キーワードは、同等のポート番号に変換されます。
  - [カスタム]：データグラム ヘッダーの送信元ポート番号と、指定した IANA ポート番号を照合します。ポートの範囲は 0 ～ 65535 で、3 種類のポートが含まれます。
    - 0 ～ 1023：ウェルノウン ポート
    - 1024 ～ 49151：登録済みポート
    - 49152 ～ 65535：ダイナミック ポート/プライベート ポート

- [宛先ポート]：ルールの一致条件に宛先ポートを含めます。宛先ポートは、データグラム ヘッダーで識別されます。
  - [任意]：任意のポートを宛先ポートとして使用できます。
  - [リストから選択]：送信元ポートに関連付けられたキーワードを照合します（ftp、ftpdata、http、smtp、snmp、telnet、tftp、www）。これらの各キーワードは、同等のポート番号に変換されます。
  - [カスタム]：データグラム ヘッダーの送信元ポート番号と、指定した IANA ポート番号を照合します。ポートの範囲は 0 ～ 65535 で、3 種類のポートが含まれます。
    - 0 ～ 1023：ウェルノウン ポート
    - 1024 ～ 49151：登録済みポート
    - 49152 ～ 65535：ダイナミック ポート/プライベート ポート

- [サービス タイプ]：パケットとクラス基準の照合に使用するサービスのタイプを指定します。
  - [任意]：任意のサービス タイプを一致条件として使用できます。
  - [IP DSCP] [リストから選択]：一致基準として使用する DSCP 値を選択します。
  - [IP DSCP] [値と照合]：0 ～ 63 のカスタム DSCP 値を入力します。
  - [IP プレシデンス]：パケットの IP プレシデンス値と、このフィールドで定義する IP プレシデンス値を照合します。IP プレシデンスの範囲は 0 ～ 7 です。
  - [IP ToS ビット]：一致基準として、IP ヘッダー内のパケットのタイプ オブ サービス（ToS）ビットを使用します。IP ToS ビット値の範囲は、00 ～ FF です。上位 3 ビットは、IP プレシデンス値を表します。上位 6 ビットは、IP DSCP 値を表します。

- [IP ToS マスク] : IP ToS マスク値を入力します。この値によって、パケットの IP ToS フィールドとの比較に使用される IP ToS ビット値のビット位置が示されます。

  IP ToS マスク値は 00 ～ ff の 2 桁の 16 進数です。IP ToS マスクの値が非 0 のビットは、パケットの IP ToS フィールドとの比較に使用される IP ToS ビット値のビット位置を示します。

ステップ 7 [OK] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

（注） クラスマップを削除または変更するには、リストからクラスマップ名を選択して[削除]をクリックします。ポリシーに割り当てられている場合は、そのクラスマップを削除することはできません。

ステップ 8 [保存] をクリックします。

IPv6 トラフィック クラスの設定

IPv6 クラス マップを追加して設定するには

ステップ 1 [クライアント QoS] > [トラフィック クラス] の順に選択します。

ステップ 2 [□] をクリックしてトラフィック クラスを追加します。

（注） クラス マップの最大数は 50 です。

ステップ 3 [トラフィック クラス名] フィールドに、新しいクラス マップの名前を入力します。名前には、1 ～ 31 文字の英数字と特殊文字を使用できます。スペースは使用できません。

ステップ 4 リストからトラフィック クラスの種類として [IPv6] を選択します。IPv6 トラフィック クラスは、WAP デバイスの IPv6 トラフィックにのみ適用されます。

ステップ 5 次のように設定します。

- [送信元アドレス] : パケットの送信元 IPv6 アドレスと、適切なフィールドで定義された IPv6 アドレスが一致する必要があります。
  - **[任意]** : 任意の IPv6 アドレスを送信元アドレスとして使用できます。
  - [シングル アドレス] : この基準を適用する IPv6 アドレスを入力します。
  - **[アドレス/マスク]** : 送信元 IPv6 アドレスのプレフィクス長を入力します。
- [宛先アドレス] : パケットの宛先 IPv4 アドレスと、適切なフィールドで定義された IPv4 アドレスが一致する必要があります。
  - **[任意]** : 任意の IPv6 アドレスを宛先アドレスとして使用できます。
  - [シングル アドレス] : この基準を適用する IPv6 アドレスを入力します。
  - [アドレス/マスク] : 宛先 IPv6 アドレスを入力し、宛先 IPv6 アドレスのプレフィクス長を入力します。

ステップ 6 [詳細] をクリックして次のパラメータを設定します。

- [プロトコル]：IPv4 パケットの IP プロトコル フィールドまたは IPv6 パケットのネクスト ヘッダー フィールドの値に基づく、レイヤ 3 またはレイヤ 4 プロトコルの一致条件を使用します。照合するプロトコルをキーワードで選択するか、プロトコル ID を入力します。
  - [すべてのトラフィック]：任意のプロトコルからのすべてのトラフィックを許可します。
  - [リストから選択]：選択したプロトコルを照合します（IP、ICMP、IGMP、TCP、UDP）。
  - [カスタム]：リストに名前がないプロトコルを照合します。プロトコル ID を入力します。プロトコル ID は、IANA によって割り当てられた標準値です。数値の範囲は 0 ～ 255 です。
- [送信元ポート]：ルールの一致条件に送信元ポートを含めます。送信元ポートは、データグラム ヘッダーで識別されます。

  （注） [プロトコル] が [すべてのトラフィック] である場合、[送信元アドレス] と [宛先アドレス] は必須です。

  - [任意]：任意のポートを送信元ポートとして使用できます。
  - [リストから選択]：送信元ポートに関連付けられたキーワードを照合します（ftp、ftpdata、http、smtp、snmp、telnet、tftp、www）。これらの各キーワードは、同等のポート番号に変換されます。
  - [カスタム]：データグラム ヘッダーの送信元ポート番号と、指定した IANA ポート番号を照合します。ポートの範囲は 0 ～ 65535 で、3 種類のポートが含まれます。
    - 0 ～ 1023：ウェルノウン ポート
    - 1024 ～ 49151：登録済みポート
    - 49152 ～ 65535：ダイナミック ポート/プライベート ポート
- [宛先ポート]：ルールの一致条件に宛先ポートを含めます。宛先ポートは、データグラム ヘッダーで識別されます。
  - [任意]：任意のポートを宛先ポートとして使用できます。
  - [リストから選択]：送信元ポートに関連付けられたキーワードを照合します（ftp、ftpdata、http、smtp、snmp、telnet、tftp、www）。これらの各キーワードは、同等のポート番号に変換されます。
  - [カスタム]：データグラム ヘッダーの送信元ポート番号と、指定した IANA ポート番号を照合します。ポートの範囲は 0 ～ 65535 で、3 種類のポートが含まれます。
    - 0 ～ 1023：ウェルノウン ポート
    - 1024 ～ 49151：登録済みポート
    - 49152 ～ 65535：ダイナミック ポート/プライベート ポート
- [IPv6 フロー ラベル]：フロー ラベルは、フロー内のパケットにラベルを付けるためにノードで使用されます。

- [任意]：IPv6 パケット固有の任意の 20 ビット値。
- [ユーザ定義]：IPv6 パケット固有の 20 ビット値を入力します。ルータでの QoS 処理を表すためにエンド ステーションで使用されます（0 ～ FFFFF の範囲）。

- [サービス タイプ]：パケットとクラス基準の照合に使用するサービスのタイプを指定します。
  - [任意]：任意のサービス タイプを一致条件として使用できます。
  - [IP DSCP] [リストから選択]：一致基準として使用する DSCP 値を選択します。
  - [IP DSCP] [値と照合]：0 ～ 63 のカスタム DSCP 値を入力します。

ステップ 7 [OK] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

（注） クラスマップを削除または変更するには、リストからクラスマップ名を選択して [削除] をクリックします。ポリシーに割り当てられている場合は、そのクラスマップを削除することはできません。

ステップ 8 [保存] をクリックします。

MAC トラフィック クラスの設定

MAC クラス マップを追加して設定するには、次の手順を実行します。

ステップ 1 [クライアント QoS] > [トラフィック クラス] の順に選択します。

ステップ 2 [□] をクリックしてトラフィック クラスを追加します。

（注） クラス マップの最大数は 50 です。

ステップ 3 [トラフィック クラス名] フィールドに、新しいクラス マップの名前を入力します。名前には、1 ～ 31 文字の英数字と特殊文字を使用できます。スペースは使用できません。

ステップ 4 [クラス マップ タイプ] リストから、クラス マップの種類として [MAC] を選択します。MAC クラス マップは、レイヤ 2 基準に適用されます。

ステップ 5 [送信元アドレス]：ルールの一致条件に送信元 MAC アドレスを含めます。

- **[任意]**：任意の MAC アドレスを送信元アドレスとして使用できます。
- [シングル アドレス]：イーサネット フレームと比較する送信元 MAC アドレスを入力します。
- [アドレス/マスク]：イーサネット フレームと比較する宛先 MAC アドレスのビットを指定する送信元 MAC アドレス マスクを入力します。

  MAC マスクのそれぞれのビット位置について、1 は対応するアドレス ビットが有効なことを示し、0 はアドレス ビットが無視されることを示します。たとえば、MAC アドレスの最初の 4 オクテットの

みをチェックするには、MAC マスク ff:ff:ff:ff:00:00 を使用します。MAC マスク ff:ff:ff:ff:ff:ff ではすべてのアドレス ビットがチェックされるため、単一の MAC アドレスを照合する場合に使用します。

ステップ 6 [宛先アドレス] : ルールの一致条件に宛先 MAC アドレスを含めます。

- **[任意]** : 任意の MAC アドレスを宛先アドレスとして使用できます。
- [シングル アドレス] : イーサネット フレームと比較する宛先 MAC アドレスを入力します。
- [アドレス/マスク] : イーサネット フレームと比較する宛先 MAC アドレスのビットを指定する宛先 MAC アドレス マスクを入力します。

ステップ 7 [詳細] をクリックして次のパラメータを設定します。

- [プロトコル] : 一致基準とイーサネット フレームのヘッダーにある値を比較します。EtherType のキーワードを選択するか、EtherType の値を入力して、一致基準を指定します。
  - [すべてのトラフィック] : 任意のプロトコルからのすべてのトラフィックを許可します。
  - [リストから選択] : データグラム ヘッダーの Ethertype と、選択したプロトコル タイプを照合します。（Apple Talk、ARP、IPv4、IPv6、IPX、NETBIOS、PPPoE）。
  - [カスタム] : データグラム ヘッダーの Ethertype と、指定したカスタム プロトコル識別子を照合します。値は、0600 ～ FFFF の範囲の 4 桁の 16 進数を使用できます。

  （注） [プロトコル] が [すべてのトラフィック] である場合、[送信元アドレス] と [宛先アドレス] は必須です。

- [サービス クラス] : パケットを照合するためのサービス クラス 802.1p のユーザ プライオリティ値を指定します。
  - [任意] : 任意のサービス クラスが許容されます。
  - [ユーザ定義] : イーサネット フレームと比較する 802.1p ユーザ プライオリティを入力します。有効な範囲は 0 ～ 7 です。

- [VLAN ID] : イーサネット フレームと比較する VLAN ID です。
  - [任意] : 任意の VLAN ID 値が許容されます。
  - [ユーザ定義] : イーサネット フレームと比較する具体的な VLAN ID を入力します。このフィールドは最初または唯一の 802.1Q VLAN タグのみにあります。ポートの範囲は 1 ～ 4094 です。

ステップ 8 [OK] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

（注） クラス マップを削除または変更するには、リストからクラス マップを選択して [削除] をクリックします。ポリシーに割り当てられている場合は、そのクラス マップを削除することはできません。

ステップ 9 [保存] をクリックします。

Qos ポリシー

パケットは、定義された基準に基づいて分類および処理されます。分類基準は、[クラス マップ] ページのクラスで定義されます。処理は、[ポリシー マップ] ページのポリシー属性で定義されます。ポリシー属性は、クラスごとのインスタンスベースで分類され、クラス基準と照合するトラフィックの処理方法を決定します。

WAP デバイスには最大 50 個のポリシーと、ポリシーあたり最大 10 個のクラスを維持できます。

ポリシー マップを追加および設定するには

ステップ 1 [クライアント QoS] > [QoS ポリシー] の順に選択します。

ステップ 2 [□] をクリックして QoS ポリシーを追加します。[QoS ポリシー名] フィールドに、QoS ポリシーの名前を入力します。名前には、1 ～ 31 文字の英数字と特殊文字を使用できます。スペースは使用できません。

ステップ 3 以前に作成した関連付けられているトラフィック クラスを選択できます□。

ステップ 4 [QoS ポリシー定義] 領域で、ポリシー マップの次のパラメータを設定します。

- [認定レート] : トラフィックが準拠する必要がある認定レート（Kbps 単位）。範囲は 1 ～ 1000000 Kbps です。
- [認定バースト] : トラフィックが準拠する必要がある認定バースト サイズ（バイト単位）。範囲は 1 ～ 1600000 Kbps です。
- [アクション] : 次のいずれかのオプションを選択します。
  - [送信] : トラフィック クラス基準を満たす場合に、関連するトラフィック ストリームのすべてのパケットを転送するよう指定します。
  - [ドロップ] : トラフィック クラス基準を満たす場合に、関連するトラフィック ストリームのすべてのパケットをドロップするよう指定します。
- [リマーク トラフィック] : 関連するトラフィック ストリームのすべてのパケットを、802.1p ヘッダーのプライオリティ フィールドで指定したサービス クラス値でマークします。パケットにこのヘッダーが含まれていない場合は、ヘッダーを挿入します。CoS 値は、0 ～ 7 の整数です。
  - [COS のリマーク] : ネットワーク トラフィックを複数のプライオリティ レベルまたはサービス クラスに分割できます。CoS 値は 0 ～ 7 で、0 が最もプライオリティが低く、7 が最もプライオリティが高くなります。
  - [DSCP のリマーク] : 指定された QoS に基づき、パケットに適用される特定の Per-Hop Behavior（PHB）を指定します。ドロップダウン リストから値を選択します。
  - [IP プレシデンスのリマーク] : 関連するトラフィック ストリームのすべてのパケットを、指定した IP プレシデンス値でマークします。IP プレシデンス値は、0 ～ 7 の整数です。

ステップ 5 [ポリシー属性の追加] をクリックします。他のクラス マップを追加できますが、この特定ポリシーのクラス マップ数は最大 10 個に制限されています。

ステップ 6 [保存] をクリックします。

（注） QoS ポリシーを削除または変更するには、リストから QoS ポリシーを選択して [削除] または [編集] をクリックします。

QoS アソシエーション

[QoS アソシエーション] ページでは、ワイヤレスおよびイーサネット インターフェイスの QoS の特定の側面に対する制御を提供します。

QoS では一般的なトラフィック カテゴリの制御に加えて、QoS ポリシー名を使用してさまざまなマイクロフローをクライアントごとに調整できます。QoS ポリシー名は、一般的なマイクロフローの定義や処理の特徴を確立するのに便利なツールです。ネットワーク上で認証されている場合は、送受信両方のワイヤレス クライアントに適用できます。

QoS アソシエーション パラメータを設定するには、次の手順に従います。

ステップ 1 **[クライアント QoS]** > **[クライアント QoS アソシエーション]** の順に選択します。

ステップ 2 [□] をクリックしアソシエーションを追加します。

ステップ 3 [QoS ポリシー名] ドロップダウン リストから QoS ポリシー名を選択します。

ステップ 4 次のように設定します。

- [レート制限（AP からクライアント）] : WAP デバイスからクライアントへの最大許容送信レートを 1 秒あたりのビット数（bps）で入力します。有効な範囲は 0 ～ 1733 Mbps です。
- [レート制限（クライアントから AP）] : クライアントから WAP デバイスへの最大許容送信レートを 1 秒あたりのビット数（bps）で入力します。有効な範囲は 0 ～ 1733 Mbps です。

ステップ 5 [保存] をクリックします。

（注） インターフェイスは QoS ポリシーまたは ACL のいずれかにバインドできますが、両方にはバインドできません。

ゲスト アクセス

WAP デバイスでデフォルトの CP インスタンスを設定できます。CP インスタンスは、複数のインスタンス パラメータからなる定義済みセットです。インスタンスは、1 つまたは複数の VAP と関連付けることができます。

VAP に接続しているワイヤレス クライアントを使用して任意の URL にアクセスすると、[アクセス コントロール/ゲスト アクセス] ページで設定した [Web ポータル ロケール] ページへの URL が Web によりハイジャックされます。

[Web ポータル ロケール] によりハイジャック GUI ページの表示スタイルが定義され、[ゲスト グループ] によりユーザのユーザ名とパスワードが決定します。

ゲスト アクセス インスタンスを設定するには、次の手順に従います。

ステップ 1 [Web ポータル ロケール テーブル] を編集し、ハイジャックされる GUI ページの表示を設計します。[プレビュー] タブをクリックすると、表示を確認できます。

ステップ 2 [ゲスト グループ テーブル] を編集し、[ゲスト ユーザの合計] の数値リンクをクリックしてユーザを追加し、[保存] をクリックします。

ステップ 3 [ゲスト アクセス インスタンス テーブル] を設定し、前述の手順で設定した [ゲスト グループ] と [Web ポータル ロケール] を選択します。

ステップ 4 **[ワイヤレス]i** > **[ネットワーク]** に移動し、VAP ゲスト アクセスを関連付け、ゲスト アクセス インスタンスを設定します。

ゲスト アクセス インスタンス テーブル

ステップ 1 **[ゲスト アクセス]** > **[ゲスト アクセス インスタンス テーブル]** の順に選択します。

ステップ 2 [ゲスト アクセス インスタンス名] フィールドに CP インスタンスの名前を指定します。この名前には最大で 32 文字の英数字を含めることができます。

ステップ 3 [キャプティブ ポータルインスタンス パラメータ]エリアが、追加のオプションとともに再表示されます。次のパラメータを設定します。

- [プロトコル]：検証プロセスで使用する CP インスタンスのプロトコルとして、[HTTP] または [HTTPS] を選択します。
  - [HTTP]：検証時に暗号化を使用しません。
  - [HTTPS]：暗号化のために証明書を必要とするセキュア ソケット レイヤ（SSL）を使用します。証明書は、接続時にユーザに提示されます。
- [認証方式]：CP がクライアントを検証するために使用する認証方式を選択します。次のオプションが用意されています。
  - [ローカル データベース]：この WAP デバイスは、ローカル データベースを使用してユーザを認証します。[ローカル データベース] 設定を使用する場合は次のように設定します。
    - [ゲスト グループ名]：ゲスト グループの名前を入力します。
    - [アイドル タイムアウト]：アイドル タイムアウトの時間を分数単位で入力します。

- [最大帯域幅アップストリーム]：キャプティブ ポータルを使用する場合にクライアントがトラフィックを送信できる最大アップロード速度をMbps単位で入力します。この設定により、ネットワークにデータを送信するために使用される帯域幅が制限されます。範囲は 0 ～ 1733 Mbps です。デフォルトは 0 です。
- [最大帯域幅ダウンストリーム]：キャプティブ ポータルを使用する場合にクライアントがトラフィックを受信できる最大ダウンロード速度をMbps単位で入力します。この設定により、ネットワークからデータを受信するために使用される帯域幅が制限されます。範囲は 0 ～ 1733 Mbps です。デフォルトは 0 です。
- [ゲスト ユーザの合計]：ゲスト ユーザの合計数。

- [RADIUS 認証]：この WAP デバイスは、リモート RADIUS サーバ上のデータベースを使用してユーザを認証します。[RADIUS 認証] 設定を使用する場合は次のように設定します。
  - [RADIUS IP ネットワーク]：ドロップダウン リストから RADIUS IP ネットワークを選択します（[IPv4] または [IPv6]）。
  - [グローバル RADIUS]：グローバル RADIUS を有効にするには [有効化] をオンにします。CP 機能に異なる一連の RADIUS サーバを使用させる場合は、このチェックボックスをオフにして、このページのフィールドでサーバを設定します。
  - [RADIUSアカウンティング]：特定のユーザが消費したリソース（システム時間、送受信データ量など）を追跡および測定するには、[有効化] をオンにします。

    RADIUSアカウンティングを有効にすると、プライマリRADIUSサーバ、すべてのバックアップ サーバ、およびすべての設定済みサーバに対してこれが有効になります。
  - [サーバのIPアドレス - 1] または [サーバのIPv6アドレス - 1]：このVAPのプライマリ RADIUS サーバの IPv4 または IPv6 アドレスを入力します。IPv4 アドレスは、xxx.xxx.xxx.xxx（192.0.2.10）の形式にする必要があります。IPv6 アドレスは、xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx（2001:DB8::CAD5:7D91）の形式にする必要があります。

    最初のワイヤレス クライアントが VAP による認証を試みると、WAP デバイスは認証要求をプライマリ サーバに送信します。プライマリ サーバが認証要求に応答すると、WAP デバイスはこのRADIUSサーバを引き続きプライマリ サーバとして使用し、認証要求が指定されたアドレスに送信されます。

    [サーバの IP アドレス - 2] または [サーバの IPv6 アドレス - 2]：バックアップ RADIUS サーバの IPv4 または IPv6 アドレスを最大 3 つまで入力します。プライマリ サーバでの認証に失敗した場合、設定された各バックアップ サーバが順番に試行されます。
  - [キー - 1]：WAPデバイスがプライマリ RADIUSサーバへの認証に使用する共有秘密キーを入力します。最大63文字の標準英数字および特殊文字を使用できます。キーは大文字と小文字が区別され、RADIUS サーバで設定されたキーと一致している必要があります。入力するテキストはアスタリスクとして表示されます。

    [キー - 2]：設定されたバックアップ RADIUS サーバに関連付けられている RADIUS キー。[サーバ IP アドレス 1] のサーバは [キー 1] を使用し、[サーバ IP アドレス 2] のサーバは [キー 2] を使用します。以降も同様です。

- [認証なし]：ユーザは、データベースによって認証される必要がありません。
- [サードパーティ クレデンシャル（Party Credentials）]：WAP デバイスでは、ユーザ認証のために、ソーシャル メディア上のクレデンシャルが使用されます。認証済みサードパーティ クレデンシャルの設定を使用する場合は、次のように構成します
  - [受け入れられたクレデンシャル（Accepted credentials）]：クレデンシャル認証として、Facebook または Google、あるいはその両方を選択します。
  - [Walled Garden]：[受け付けられたクレデンシャル（Accepted credentials）] が選択されている間、関係するデフォルト構成が自動的に設定されます

（注） シスコでは、データ保護、プライバシー、およびセキュリティ要件を、新商品のコンセプト考案から発売までの製品設計および開発手法に統合します。詳細については、*https://www.cisco.com/c/en/us/about/trust-center/gdpr.html*を参照してください。

- [Active Directory サービス（Active Directory Service）]：この WAP デバイスは、リモート ADS サーバ上のデータベースを使用してユーザを認証します。ADS 認証の設定を使用する場合は次のように設定します。
  - [Active Directory サーバ（Active Directory Servers）]：[□] アイコンをクリックすることにより、新しい ADS サーバを追加します。サーバは 3 個まで追加できます。矢印を使用することにより、サーバを移動して優先順位を決めます。構成を削除するには、[ゴミ箱（trash can）] を選択します。[テスト（Test）] を使用して、ADS サーバが有効かどうかを確認します。

- [ゲスト グループ]：[認証方式] に [ローカル データベース] または [RADIUS 認証] が設定されている場合は、以前に作成したゲスト グループを選択します。このグループに属しているすべてのユーザは、このポータルを介してネットワークにアクセスすることが許可されます。
- [リダイレクト URL]：URL リダイレクトを有効にするには、URL（http:// を含む）を入力します。0 ～ 256 文字で入力します。
- [セッション タイムアウト]：CP セッションが有効な状態である残り時間を秒単位で入力します。この時間が 0 に達すると、クライアントの認証が解除されます。範囲は 0 ～ 1440 分です。デフォルト値は 0 です。
- [Web ポータル ロケール]：ドロップダウン リストから、以前に作成した Web ポータル ロケールを選択します。

ステップ 4 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

ゲスト グループ テーブル

デバイスでは各ローカル ユーザがユーザ グループに割り当てられ、このユーザ グループが CP インスタンスに割り当てられます。このグループにより、CP インスタンスへのユーザ割り当ての管理が容易になります。

「Default」という名前のユーザ グループが組み込まれており、削除できません。

ローカル ユーザを設定するには、次の手順を実行します。

ステップ 1 [ゲスト アクセス] > [ゲスト グループ テーブル] の順に選択します。

ステップ 2 [ゲスト グループ設定] 領域で、次のパラメータを設定します。

- [ゲスト グループ名] : 新しいゲスト グループの名前を指定します。デフォルトのゲスト グループ名は [デフォルト] です。

ステップ 3 次のパラメータを設定します。

- [アイドル タイムアウト] : クライアントと WAP デバイスとの関連付けが解除された後に、ユーザが CP 認証済みクライアント リストに保持される時間を入力します。クライアントが再認証を試みる前に、このフィールドで指定された時間が経過すると、クライアント エントリが認証済みクライアント リストから削除されます。範囲は 0 ～ 1440 分です。デフォルト値は 60 です。ここで設定したタイムアウト値は、ユーザ値が 0 に設定されないかぎり、CP インスタンスに関して設定された値よりも優先されます。0 に設定されている場合は、CP インスタンスに関して設定されているタイムアウト値が使用されます。
- [最大帯域幅アップストリーム] : キャプティブ ポータルを使用する場合にクライアントがトラフィックを送信できる最大アップロード速度を Mbps 単位で入力します。この設定により、ネットワークにデータを送信するために使用される帯域幅が制限されます。0 ～ 1733 Mbps の範囲で入力します。デフォルトは 0 です。
- [最大帯域幅ダウンストリーム] : キャプティブ ポータルを使用する場合にクライアントがトラフィックを受信できる最大ダウンロード速度を Mbps 単位で入力します。この設定により、ネットワークからデータを受信するために使用される帯域幅が制限されます。0 ～ 1733 Mbps の範囲で入力します。デフォルトは 0 です。
- [ゲスト ユーザの合計] : ゲスト ユーザの合計数を表示します。[ゲスト ユーザの合計] の数値リンクをクリックすると、[ゲスト ユーザ アカウント] ページが表示されます。

ステップ 4 [保存] をクリックします。

ゲスト ユーザ アカウント

ゲスト ユーザ アカウントを設定するには、次の手順に従います。

ステップ 1 [ゲスト アクセス] > [ゲスト グループ テーブル] の順に選択します。

ステップ 2 [ゲスト ユーザの合計] フィールドの数値リンクをクリックします。[ゲスト ユーザ アカウント] ページに [ゲスト ユーザ アカウント テーブル] が表示されます。

ステップ 3 [□] をクリックしてユーザを追加します。

ステップ 4 [ゲスト ユーザ名] : 新しいゲスト ユーザの名前を入力します。この名前には最大で 32 文字の英数字を含めることができます。

ステップ 5 [ゲスト ユーザ パスワード] : パスワードを入力します。パスワードには、8 ～ 64 文字の英数字と特殊文字を使用できます。

ステップ 6 [保存] をクリックします。

（注） [ゲスト アクセス] ページを表示するには [戻る] ボタン リンクをクリックします。

ゲスト ユーザを削除または変更するには、ゲスト ユーザを選択してから [削除] または [編集] をクリックします。

Web ポータルのカスタマイズ

CP インスタンスを VAP に関連付けた後、ロケールを作成して、それを CP インスタンスにマッピングします。CP インスタンスに関連付けられた VAP にユーザがアクセスすると、認証ページが表示されます。

[Web ポータルのカスタマイズ] ページを使用して、ネットワーク上のさまざまなロケールに固有のページを作成し、ページのテキストと画像をカスタマイズします。

ステップ 1 **[ゲスト アクセス]** > **[Web ポータル ロケール テーブル]** の順に選択します。

ステップ 2 このテーブルで [追加] をクリックし、[キャプティブ ポータルのカスタマイズ] ページにアクセスします。ロケールを変更するには、当該行をオンにして [編集] をクリックするか、削除する場合は [削除] をクリックします。

ネットワーク上の異なるロケールによって最大 3 つの異なる認証ページを作成できます。

ステップ 3 [キャプティブ ポータル Web ロケール パラメータ] 領域で、次の設定を行います。

- [Web ポータル ロケール名] : ページに割り当てる Web ロケールの名前を入力します。この名前は 1 ～ 32 文字の英数字で指定できます。

ステップ 4 [キャプティブ ポータル Web ロケール パラメータ] 領域に、ロケールを変更するための追加のオプションが表示されます。[ゲスト アクセス インスタンス名] は編集できません。編集可能なフィールドにはデフォルト値が表示されます。次のパラメータを設定します。

- [ゲスト アクセス インスタンス名] : ゲスト アクセス インスタンスの名前を表示します。
- [背景画像] : [参照] をクリックして画像を選択します。[アップロード] をクリックすると、CP インスタンス用の画像をアップロードできます。
- [ロゴ画像] : [参照] をクリックしてロゴ画像を選択します。[アップロード] をクリックすると、ロゴ画像をアップロードできます。
- [前景の色] : 前景の色の HTML コードを 6 桁の 16 進数形式で入力します。1 ～ 32 文字で入力します。デフォルトは #FFFFFF です。

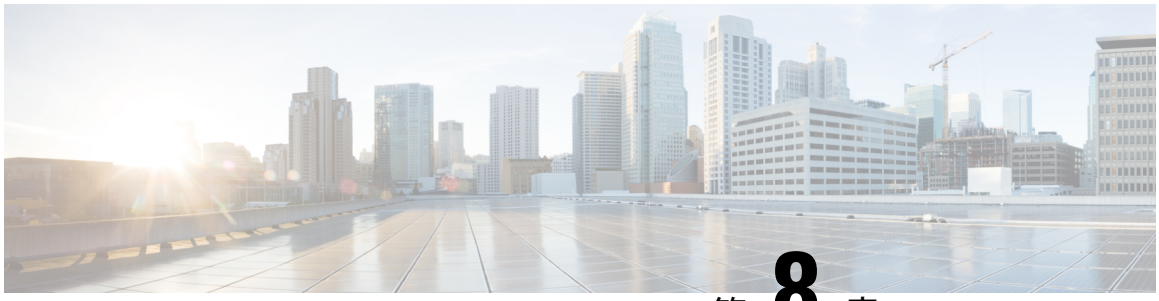
- [背景の色]：背景の色の HTML コードを 6 桁の 16 進数形式で入力します。1 ～ 32 文字で入力します。デフォルトは #FFFFFF です。
- [セパレータの色]：ページの見出し部とページの本文部を区切る太い横線の色の HTML コードを 6 桁の 16 進数形式で入力します。1 ～ 32 文字で入力します。デフォルトは #FFFFFF です。
- [アカウント画像]：[参照] をクリックして画像を選択します。[アップロード] をクリックすると、アカウント画像をアップロードできます。
- [フォント]：ドロップダウン リストからフォントを選択します。このフォントは、すべてのテキストを表示するときに使用されます。
- [アカウントのプロンプティング]：ユーザ名を入力します。1 ～ 32 文字で入力します。
- [ユーザ名のプロンプティング]：ユーザ名テキスト ボックスのラベルです。1 ～ 32 文字で入力します。
- [パスワードのプロンプティング]：ユーザ パスワード テキスト ボックスのラベルです。1 ～ 64 文字で入力します。
- [ボタンのプロンプティング]：認証のためにユーザ名とパスワードを送信する際にユーザがクリックするボタンのラベルです。2 ～ 32 文字で入力します。デフォルトは Connect です。
- [ブラウザ ヘッドのプロンプティング]：ブラウザのタイトル バーに表示されるテキストです。1 ～ 128 文字で入力します。デフォルトは Captive Portal です。
- [ポータル タイトルのプロンプティング]：ページ見出し部のロゴの右側に表示されるテキストです。1 ～ 128 文字で入力します。デフォルトは Welcome to the Wireless Network です。
- [アカウントのヒントのプロンプティング]：ページ本体のユーザ名とパスワードのテキスト ボックスの下に表示されるテキストです。1 ～ 256 文字で入力します。デフォルトは「このサービスの使用を開始するには、クレデンシャルを入力して [接続] ボタンをクリックします」です。
- [受け入れポリシー]：[利用規約] ボックスに表示されるテキストです。1 ～ 4096 文字で入力します。デフォルトは [利用規約] です。
- [受け入れのプロンプティング]：利用規約を読んで同意したことを確認するためにチェックボックスをオンにするようユーザに指示するテキストです。1 ～ 128 文字で入力します。
- [受け入れなしの警告]：ユーザが [利用規約] チェックボックスをオンにしないでログイン資格情報を送信した場合にポップアップ ウィンドウに表示されるテキストです。1 ～ 128 文字で入力します。
- [作業進行中のプロンプティング]：認証プロセス実行中に表示されるテキストです。1 ～ 128 文字で入力します。
- [無効な資格情報のプロンプティング]：ユーザが認証に失敗したときに表示されるテキストです。1 ～ 128 文字で入力します。
- [接続成功のプロンプティング]：クライアントが VAP に対して認証されたときに表示されるテキストです。1 ～ 128 文字で入力します。
- [ウェルカム プロンプティング]：クライアントがネットワークに接続されたときに表示されるテキストです。1 ～ 256 文字で入力します。

- [復元]：現在のロケールを削除します。

ステップ 5 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

ステップ 6 [プレビュー] をクリックすると、更新されたページが表示されます。

[プレビュー] をクリックすると、すでにスタートアップ コンフィギュレーションに保存されているテキストと画像が表示されます。変更を加えた場合、変更を確認するには、[プレビュー] をクリックする前に [保存] をクリックしてください。



第 8 章

Umbrella

この章では、**Cisco Umbrella** サービスを構成する方法について説明します。具体的な内容は、次のとおりです。

• Cisco Umbrella （133 ページ）

Cisco Umbrella

Cisco Umbrella は、インターネット上の脅威に対する防御の最前線となるクラウド セキュリティ プラットフォームです。これは、インターネットとシステムやデータの間のゲートウェイとして機能し、どのポート、プロトコル、アプリケーションについても、マルウェア、ボットネット、フィッシングをブロックします。

Umbrella アカウントを使用すれば、この統合によって DNS クエリが透過的にインターセプトされ、Umbrella にリダイレクトされます。このデバイスは、Umbrella ダッシュボードにネットワーク デバイスとして表示され、ポリシーを適用したり、レポートを閲覧したりすることができます。

ステップ 1 Umbrella の機能を有効にするには、このチェックボックスをオンにします

ステップ 2 Umbrella の Web サイトから入手したシークレットと API キーを該当するフィールド入力します

（注） Cisco Umbrella にログインし、ダッシュボードに移動します。[管理プラットフォームAPIキー（Admin >Platform API Keys）] に移動して、名前を追加し、シークレットとキーの情報を作成します。

ステップ 3 [バイパスするローカル ドメイン（オプション）（Local Domains to Bypass (optional)）] フィールドに信頼するドメイン名を入力します。パケットが、Umbrella を経由することなく宛先に達するようになります。

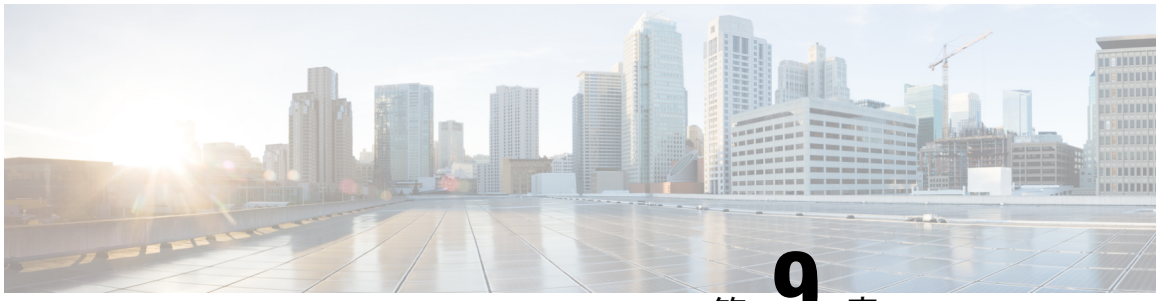
（注） これは、すべてのイントラネット ドメインおよびスプリット DNS ドメインに必要です。

ステップ 4 [デバイス タグ（オプション）（Device Tag (optional)）] フィールドにタグ名を入力して、デバイスにタグを付けます。

ステップ 5 DNS 暗号化を有効にするには、このチェックボックスをオンにします。

（注） DNSCrypt は、DNS クライアントと DNS リゾルバの間の DNS 通信を保護するために使用されます。それにより、いくつかのタイプの DNS 攻撃と、スヌーピングを防ぎます。デフォルトは有効です。

ステップ 6 [保存（Save）] をクリックして、これらの構成を適用します。登録のステータスは、[登録ステータス（Registration Status）] フィールドに表示されます。



第 9 章

モニタ

この章では、WAPデバイスのステータスおよび統計情報を表示する方法について説明します。具体的な内容は次のとおりです。

- ダッシュボード （135 ページ）
- シングル ポイント設定 （139 ページ）
- クライアント （140 ページ）
- ゲスト （142 ページ）

ダッシュボード

ダッシュボードには、スループット ステータスと、ネットワーク デバイスを設定またはモニタするための簡単な手順が表示されます。このページは 30 秒間隔で更新されます。

接続済みのクライアント

現在 WAP デバイスに関連付けられているクライアントの合計数。このボックスをクリックすると「クライアント」ページにリダイレクトされます。

インターネット/LAN/ワイヤレス

ページ右上の丸いアイコンは、インターネット接続、LAN 接続、ワイヤレス接続のステータスを示します。

インターネット

- **赤色の丸**：インターネットに接続していません。
- **緑色の丸**：インターネット接続は良好です。

LAN

- **赤色の丸**：有線接続していません。
- **緑色の丸**：有線接続しています。

[LAN] リンクをクリックすると [LAN ステータス] ページが表示されます。

ワイヤレス

- **赤色の丸**：すべての無線が無効になっています。
- **緑色の丸**：少なくとも 1 つの無線が機能しています。1 つまたは 2 つの無線が有効になっています。

[ワイヤレス] リンクをクリックすると [ワイヤレス ステータス] ページが表示されます。

2.4G 無線スループット

この折れ線グラフは 2.4G 無線スループットを表示し、30 秒間隔で更新されます。

- [アップロード]：過去 30 秒間の送信スループット。
- [ダウンロード]：過去 30 秒間の受信スループット。

データを非表示にするには、[アップロード] または [ダウンロード] をクリックします。

5G 無線スループット

この折れ線グラフは 5G 無線スループットを表示し、30 秒間隔で更新されます。

- [アップロード]：過去 30 秒間の送信スループット。
- [ダウンロード]：過去 30 秒間の受信スループット。

データを非表示にするには、[アップロード] または [ダウンロード] をクリックします。

トップ クライアント

この棒グラフには、トラフィックの順序に基づく上位 5 つのトラフィック クライアント デバイスが表示されます。

- [アップロード]：過去 30 秒間の送信スループット。
- [ダウンロード]：過去 30 秒間の受信スループット。

データを非表示にするには、[アップロード] または [ダウンロード] をクリックします。

SSID 使用率

この円グラフには、トラフィックの順序に基づく上位 5 つのトラフィック SSID が表示されます。

- [トラフィック]：合計送受信バイト数。

ネットワーク使用量

この折れ線グラフには eth スループットが表示されます。

- [アップロード]：過去 30 秒間の送信スループット。
- [ダウンロード]：過去 30 秒間の受信スループット。

データを非表示にするには、[アップロード] または [ダウンロード] をクリックします。

クイック アクセス

クイック ナビゲーションにより簡単にデバイス設定を実行できるように、[作業の開始]ページには、一般的なタスクを実行するためのリンクが用意されています。詳細については、クイック スタート コンフィギュレーション （10 ページ）を参照してください。

LAN ステータス

LAN を示す円をクリックすると、LAN インターフェイスの次のコンフィギュレーションとステータス設定が表示されます。

- [MAC アドレス] : WAP デバイスの MAC アドレス。
- [IP アドレス] : WAP デバイスの IP アドレス。
- [サブネット マスク] : WAP デバイスのサブネット マスク。
- [デフォルト ゲートウェイ] : WAP デバイスのデフォルト ゲートウェイ。
- [ドメイン ネーム サーバ -1] : WAP デバイスで使用されるドメイン ネームサーバ 1 の IP アドレス。
- [ドメイン ネーム サーバ -2] : WAP デバイスで使用されるドメイン ネームサーバ 2 の IP アドレス。
- [IPv6 アドレス] : WAP デバイスの IPv6 アドレス。
- [IPv6 自動設定グローバル アドレス] : IPv6 の自動設定済みグローバル アドレス。
- [IPv6 リンク ローカル アドレス] : WAP デバイスの IPv6 リンク ローカル アドレス。
- [デフォルト IPv6 ゲートウェイ] : WAP デバイスのデフォルト IPv6 ゲートウェイ。
- [IPv6-DNS-1] : WAP デバイスで使用される IPv6 DNS サーバ 1 の IPv6 アドレス。
- [IPv6-DNS-2] : WAP デバイスで使用される IPv6 DNS サーバ 2 の IPv6 アドレス。

（注） 次の設定は、内部インターフェイスに適用されます。設定を変更するには、[編集]をクリックします。[LAN] ページにリダイレクトされます。

[更新] をクリックすると画面が更新され、最新情報を表示します。

[ダッシュボード] ページに戻るには、[戻る] をクリックします。

ワイヤレス ステータス

[ワイヤレス]の円をクリックすると、次のようなワイヤレス無線インターフェイスが表示されます。

- [ワイヤレス無線] : ワイヤレス無線モードが無線インターフェイスに対して有効または無効になっています。

- [MAC アドレス]：無線インターフェイスに関連付けられた MAC アドレス。
- [モード]：無線インターフェイスで使用される 802.11 モード（a/b/g/n/ac）。
- [チャネル]：無線インターフェイスで使用されるチャネル。
- [動作帯域幅]：無線インターフェイスで使用される動作帯域幅。

設定を変更するには、[編集] をクリックします。[無線] ページにリダイレクトされます。

[更新] をクリックすると画面が更新され、最新情報を表示します。

[ダッシュボード] ページに戻るには、[戻る] をクリックします。

インターフェイス ステータス

[インターフェイス ステータス] 表には、各仮想アクセス ポイント（VAP）および各ワイヤレス配信システム（WDS）インターフェイスの次のステータス情報が示されます。

- [ネットワーク インターフェイス]：WAP デバイスのワイヤレス インターフェイス。
- [名前（SSID）]：ワイヤレス インターフェイス名。
- [ステータス]：VAP の管理ステータス（[動作中] または [停止]）。
- [MAC アドレス]：無線インターフェイスの MAC アドレス。
- [VLAN ID]：無線インターフェイスの VLAN ID。
- [プロファイル]：関連するスケジューラ プロファイルの名前。
- [状態]：現在の状態（[アクティブ] または [非アクティブ]）。この状態は、VAP がクライアントとデータをやり取りしているかどうかを示します。

トラフィック統計

[トラフィック統計] ページでは、イーサネット インターフェイス、仮想アクセス ポイント（VAP）およびすべての WDS インターフェイスの送受信の統計がリアルタイムで表示されます。すべての送受信の統計には、WAP デバイスが最後に起動されてからの合計数が反映されます。WAPデバイスを再起動すると、これらの数値は再起動後の送受信数の合計を示します。

トラフィック統計情報を表示するには、**[モニタ]** > **[ダッシュボード]** > **[クイック アクセス]** > **[トラフィック統計情報]** の順に選択します。

次の情報が表示されます。

- [インターフェイス]：イーサネット インターフェイス、各 VAP インターフェイス、および各 WDS インターフェイスの名前。各 VAP インターフェイスの名前の後にカッコにかこまれた SSID が続きます。
- [合計パケット数]：WAP デバイスが送信（[送信] テーブル）または受信（[受信] テーブル）したパケットの合計数。

- [合計バイト数]：WAP デバイスが送信（[送信] テーブル）または受信（[受信] テーブル）したバイトの合計数。
- [合計廃棄パケット数]：WAP デバイスが送信（[送信] テーブル）または受信（[受信] テーブル）した廃棄パケットの合計数。
- [合計廃棄バイト数]：WAP デバイスが送信（[送信] テーブル）または受信（[受信] テーブル）した廃棄バイトの合計数。
- [エラー]：WAP デバイスでのデータの送受信に関連するエラーの合計数。

（注） [更新] をクリックすると、最新情報を表示できます。

シングル ポイント設定

[シングル ポイント設定] ページには、クラスタ メンバーと、現在クラスタに参加している WAP デバイスのトラフィックが表示されます。

トラフィック使用量のトップ AP

この棒グラフには、トラフィック使用量の順で上位 5 つのトラフィック WAP デバイスが表示されます。

- [アップロード]：送信スループット。
- [ダウンロード]：受信スループット。

（注） データを非表示にするには、[アップロード] または [ダウンロード] をクリックします。

クライアント接続のトップ AP

クライアント接続数の順に基づきます。この棒グラフには、上位 5 つの WAP デバイスが表示されます。

チャネル割り当てテーブル

[チャネル割り当て] テーブルには、シングル ポイント設定クラスタに含まれるすべての WAP デバイスが IP アドレスごとにリスト表示されます。

このテーブルには、現在のチャネル割り当てに関する次の詳細情報が示されます。

- [AP の位置]：WAP デバイスの物理的な位置。
- [無線チャネル]：この WAP デバイスが現在ブロードキャストしている無線チャネル。

- [IP アドレス]：WAP デバイスの IP アドレス。
- [トラフィック（アップ/ダウン）]：クライアントデバイスの合計送信バイト数（アップ）と合計受信バイト数（ダウン）。
- [クライアント接続（2.4G/5G）]：WAP デバイスに接続しているクライアントの数。

クライアント

クライアント

[クライアント]ページには、デバイスに関連付けられているクライアント ステーションが表示されます。

[関連クライアントの合計数]：WAP デバイスのクライアントの合計数。

クライアントの概要

デバイス上の現在の 802.11 クライアント タイプのクライアント概要を表示します。

平均帯域幅

クライアント平均帯域幅を Mbps 単位で表示します。

- [アップロード]：過去 30 秒間の送信スループット。
- [ダウンロード]：過去 30 秒間の受信スループット。

（注） データを非表示にするには、[アップロード] または [ダウンロード] をクリックします。

最小信号対雑音比（SNR）クライアント

最小 SNR の上位 5 つのデバイスをリストします。

最低速クライアント

最低速の上位 5 つのデバイスをリストします。

関連付けられたクライアント

- [クライアントの詳細]：関連付けられているワイヤレス クライアントのホスト名と MAC アドレス。
- [IP アドレス]：関連付けられているワイヤレス クライアントの IP アドレス。

- [ネットワーク（SSID）]：WAP デバイスの Service Set Identifier（SSID）。SSID は、ワイヤレス ローカル エリア ネットワークを一意に識別する最大 32 文字の英数字の文字列です。これはネットワーク名とも呼ばれます。
- [モード]：クライアントで使用されている IEEE 802.11a、IEEE 802.11b、IEEE 802.11g などの IEEE 802.11 モード。
- [データ レート]：現在の送信データレート。
- [チャネル]：クライアントが現在接続しているチャネル。チャネルは、無線が送信および受信に使用する無線スペクトルの一部を定義します。[無線]ページでチャネルを設定できます。
- [トラフィック（アップ/ダウン）]：クライアントデバイスの合計送信バイト数（アップ）と合計受信バイト数（ダウン）。
- [SNR（dB）]：SNR の強度をデシベル（dB）で表示します。
- [スループット メーター]：過去 30 秒間のスループット/データレート。

（注） クライアントを[クライアントの詳細]、[ネットワーク（SSID）]などに基づいて並べ替えできます。

クライアントを[クライアントの詳細]、[ネットワーク（SSID）]などに基づいてフィルタリングできます。

シングル ポイント設定のクライアント

- [クライアントの詳細]：関連付けられているワイヤレス クライアント IPv4 アドレス（WAP デバイスの IP アドレス）の MAC アドレス。
- [IP アドレス]：WAP デバイスの IP アドレス。
- [ネットワーク（SSID）]：WAP デバイスの Service Set Identifier（SSID）。SSID は、ワイヤレス ローカル エリア ネットワークを一意に識別する最大 32 文字の英数字の文字列です。これはネットワーク名とも呼ばれます。
- [モード]：クライアントで使用されている IEEE 802.11a、IEEE 802.11b、IEEE 802.11g などの IEEE 802.11 モード。
- [データ レート]：現在の送信レート。
- [AP の位置]：WAP デバイスの物理的な位置。
- [チャネル]：クライアントが現在接続しているチャネル。チャネルは、無線が送信および受信に使用する無線スペクトルの一部を定義します。[無線]ページでチャネルを設定できます。
- [トラフィック（アップ/ダウン）]：クライアントデバイスの合計送信バイト数（アップ）と合計受信バイト数（ダウン）。

- [SNR（db）]：強度を示す数字（デシベル）が表示されます。
- [スループット メーター]：過去 30 秒間のスループット/データ レート。

（注） [クライアントの詳細]、[ネットワーク（SSID）] などに基づいて、クライアントを並べ替えたり、フィルタリングしたりできます。

ゲスト

[ゲスト] ページには 2 つのテーブルが表示されます。1 つは、いずれかのキャプティブ ポータルインスタンスで認証済みのクライアントを表示する [認証済みクライアント] テーブルです。もう 1 つは、キャプティブ ポータルで認証を試みて失敗したクライアントに関する情報を表示する [認証に失敗したクライアント] テーブルです。

認証済みクライアントのリストまたは認証に失敗したクライアントのリストを表示するには、[モニタ] > [ゲスト] の順に選択します。

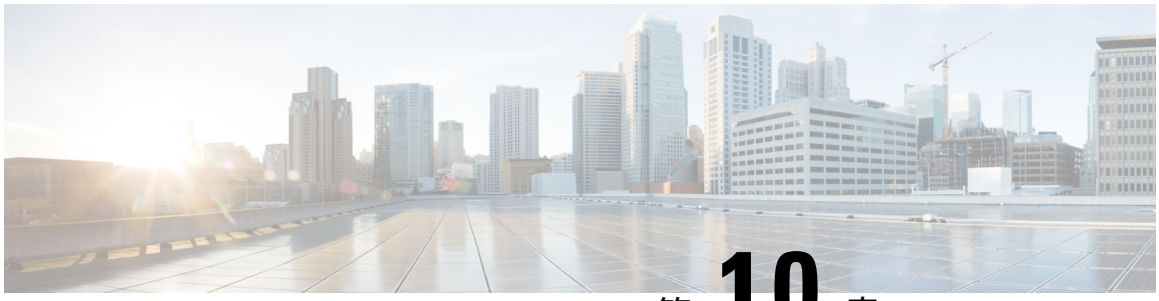
次の情報が表示されます。

- [MAC]：クライアントの MAC アドレスです。
- [IP アドレス]：クライアントの IP アドレスです。
- [ユーザ名]：クライアントのキャプティブ ポータル ユーザ名です。
- [プロトコル]：ユーザが接続を確立するために使用したプロトコル（HTTP または HTTPS）です。
- [検証]：キャプティブ ポータルでのユーザ認証に使用される方式で、値は次のいずれかです。
  - [ゲスト]：ユーザは、データベースによって認証される必要がありません。
  - [ローカル]：WAP デバイスは、ローカル データベースを使用してユーザを認証します。
  - [RADIUS]：WAP デバイスは、リモート RADIUS サーバ上のデータベースを使用してユーザを認証します。
- [VAP/無線 ID]：ユーザが関連付けられている VAP および無線です。
- [キャプティブ ポータル ID]：ユーザが関連付けられているキャプティブ ポータル インスタンスの ID です。
- [タイムアウト]：CP セッションが有効である残り時間（秒単位）です。この時間が 0 に達すると、クライアントの認証が解除されます。

- [退席時間]：クライアントエントリが有効である残り時間（秒単位）です。クライアントの CP との関連付けが解除されると、タイマーが起動します。この時間が 0 に達すると、クライアントの認証が解除されます。
- [アップ/ダウン（MB）]：WAPデバイスによってユーザ ステーションとの間で送受信されたバイト数です。
- [障害時刻]：認証障害が発生した時刻です。障害の時刻を示すタイムスタンプが含まれています。

[エクスポート] をクリックして、現在の認証済みクライアント/失敗したクライアントのメッセージをアップロードできます。

（注） [エクスポート] ボタンをクリックする前に [認証済みクライアント] または [失敗したクライアント] をクリックします。その後 [エクスポート] をクリックします。



第 10 章

管理

この章では、管理設定と診断を実施する方法を説明します。具体的な内容は次のとおりです。

- ファームウェア （145 ページ）
- コンフィギュレーション ファイル （147 ページ）
- リブート （150 ページ）

ファームウェア

WAPデバイスは2個のファームウェアイメージを維持しています。イメージの1つはアクティブでもう1つは非アクティブです。ブートアップ時にアクティブイメージをロードできなかった場合は、非アクティブ イメージがロードされてアクティブ イメージになります。アクティブ イメージと非アクティブ イメージを切り替えることもできます。

新しいバージョンのファームウェアの提供に伴って、WAPデバイス上のファームウェアをアップグレードして新機能および拡張機能を利用できます。WAP デバイスでは、ファームウェア アップグレードに TFTP または HTTP/HTTPS クライアントを使用します。

新しいファームウェアをアップロードし、システムがリブートすると、新しく追加したファームウェアがプライマリ イメージになります。アップグレードが失敗した場合は、元のファームウェアが引き続きプライマリ イメージです。

（注） ファームウェアをアップグレードする場合、WAP デバイスでは既存の設定を維持します。

ファームウェア イメージの切り替え

WAP デバイスで実行されているファームウェア イメージを切り替えるには、次の手順を実行します。

ステップ 1 [管理] > [ファームウェア] の順に選択します。

製品 ID（PID VID）およびアクティブと非アクティブのファームウェアのバージョンが表示されます。

ステップ 2 [イメージの切り替え] をクリックします。

ファームウェア イメージの切り替えと、これに続くリブートを確認するダイアログボックスが表示されます。

ステップ 3 [OK] をクリックして続行します。

この処理は数分かかることがあり、この間は WAP デバイスは使用できません。イメージの切り替えの進行中は WAP デバイスの電源を切らないでください。イメージの切り替えが完了すると、WAP デバイスが再起動します。WAP デバイスはアップグレード前と同じ構成時の設定を使用して通常の動作を再開します。

HTTP/HTTPS のアップグレード

HTTP/HTTPS を使用してアップグレードするには、次の手順を実行します。

ステップ 1 転送方法として [HTTP/HTTPS] を選択します。

ステップ 2 [参照] をクリックして、ネットワーク上のファームウェア イメージ ファイルを検索します。

使用するファームウェア アップグレード ファイルは tar ファイルである必要があります。bin ファイルまたはその他の形式のファイルをアップグレードに使用しないでください。これらのタイプのファイルは機能しません。

ステップ 3 [アップグレード] をクリックして新しいファームウェア イメージを適用します。

新しいファームウェアのアップロードには数分かかる場合があります。新しいファームウェアのアップロード中は、ページを更新したり、別のページに移動したりしないでください。ファームウェアのアップロードが中止されます。プロセスが完了すると、WAP デバイスが再起動して通常の動作を再開します。

ステップ 4 ファームウェアが正常にアップグレードされたことを確認するには、Web ベースの設定ユーティリティにログインし、[ファームウェアのアップグレード] ページを開いてアクティブなファームウェアのバージョンを表示します。

TFTP アップグレード

TFTP を使用し WAP デバイス上のファームウェアをアップグレードするには、次の手順を実行します。

ステップ 1 転送方法として [TFTP] を選択します。

ステップ 2 [ソース ファイル名] フィールドに、イメージ ファイルの名前（1 ～ 256 文字）を入力します。これには、アップロードするイメージを格納しているディレクトリのパスを含めます。

たとえば、/share/builds/ap ディレクトリにある ap_upgrade.tar イメージをアップロードするには、次のように入力します。/share/builds/ap/ap_upgrade.tar

使用するファームウェア アップグレード ファイルは tar ファイルである必要があります。bin ファイルまたはその他の形式のファイルをアップグレードに使用しないでください。これらのタイプのファイルは機能しません。

ファイル名に、スペース、<、>、|、\、:、(、)、&、;、#、?、*、および 2 つ以上の連続したピリオドを使用することはできません。

ステップ 3 TFTP サーバの IPv4 アドレスを入力し、[アップグレード] をクリックします。

新しいファームウェアのアップロードには数分かかる場合があります。新しいファームウェアのアップロード中は、ページを更新したり、別のページに移動したりしないでください。ファームウェアのアップロードが中止されます。プロセスが完了すると、WAP デバイスが再起動して通常の動作を再開します。

ステップ 4 ファームウェア アップグレードが正常に完了したことを確認するには、設定ユーティリティにログインし、[ファームウェアのアップグレード] ページを開いてアクティブなファームウェアのバージョンを表示します。

コンフィギュレーション ファイル

WAP デバイスのコンフィギュレーション ファイルは XML 形式であり、WAP デバイスに関するすべての情報を格納しています。コンフィギュレーション ファイルはネットワーク ホストまたは TFTP サーバにバックアップ（アップロード）して、内容を手動で編集したり、バックアップを作成したりできます。バックアップしたコンフィギュレーション ファイルは、編集後に WAP デバイスにダウンロードして、コンフィギュレーションを変更できます。WAP デバイスは、次のコンフィギュレーション ファイルを維持しています。

- **スタートアップ コンフィギュレーション**：フラッシュ メモリに保存されたコンフィギュレーション ファイルです。
- **バックアップ コンフィギュレーション**：バックアップとして使用するために WAP デバイスに保存された追加のコンフィギュレーション ファイルです。
- **ミラー コンフィギュレーション**：スタートアップ コンフィギュレーションが 24 時間以上変更されていない場合は、ミラー コンフィギュレーション ファイルに自動で保存されます。ミラー コンフィギュレーション ファイルは、過去のスタートアップ コンフィギュレーションのスナップショットです。ミラー コンフィギュレーションは出荷時設定へのリセットをまたがって保存されます。このため、ミラー コンフィギュレーションをスタートアップ コンフィギュレーションにコピーすることで、出荷時設定へのリセット後にシステム コンフィギュレーションを回復するために使用できます。

（注） これらのファイルは別のシステムとのダウンロードおよびアップロードに加え、WAP デバイス上の異なるファイル タイプにコピーすることもできます。

バックアップ コンフィギュレーション ファイル

コンフィギュレーション ファイルをネットワーク ホストまたは TFTP サーバにバックアップ（アップロード）するには、次の手順を実行してください。

ステップ 1 [管理] > [コンフィギュレーション ファイル] > [ダウンロード/バックアップ] の順に選択します。

ステップ 2 転送方法として [TFTP 経由] または [HTTP/HTTPS 経由] を選択します。

ステップ 3 コンフィギュレーション データを PC にバックアップするには、[バックアップ（アクセス ポイントから PC）] を選択します。

ステップ 4 TFTP バックアップの場合、拡張子 xml を付けて宛先ファイル名を入力します。サーバ上のファイルを保存するパスも含めてから、[TFTP サーバの IPv4 アドレス] を入力します。

ファイル名に、スペース、<、>、|、\、:、(、)、&、;、#、?、*、および 2 つ以上の連続したピリオドを使用することはできません。

ステップ 5 TFTP バックアップの場合、TFTP IPv4 アドレスを入力します。

ステップ 6 バックアップするコンフィギュレーション ファイルを選択します。

- **スタートアップコンフィギュレーション**：WAPデバイスの最後の起動で使用されたコンフィギュレーション ファイル タイプです。これには、適用されただけで WAP デバイスにはまだ保存されていないコンフィギュレーション変更は含まれていません。
- **バックアップ コンフィギュレーション**：WAP デバイスに保存されたバックアップ コンフィギュレーション ファイル タイプです。
- **ミラー コンフィギュレーション**：スタートアップ コンフィギュレーションが 24 時間以上変更されていない場合は、ミラー コンフィギュレーション ファイルに自動で保存されます。ミラー コンフィギュレーションは、過去のスタートアップ コンフィギュレーションのスナップショットです。ミラー コンフィギュレーションは出荷時設定へのリセットをまたがって保存されます。このため、ミラー コンフィギュレーションをスタートアップ コンフィギュレーションにコピーすることで、出荷時設定へのリセット後にシステム コンフィギュレーションを回復するために使用できます。

ステップ 7 [保存] をクリックしてバックアップを開始します。HTTP/HTTPS バックアップの場合は、ウィンドウが表示されて、ファイルを保存する目的の場所を参照して指定できます。

コンフィギュレーション ファイルのダウンロード

ファイルを WAP デバイスにダウンロードすることにより、コンフィギュレーションを更新したり、以前バックアップしたコンフィギュレーションに WAP デバイスを戻したりできます。

コンフィギュレーション ファイルを WAP デバイスにダウンロードするには、次の手順を実行してください。

ステップ 1 [管理] > [コンフィギュレーション ファイル] > [ダウンロード/バックアップ] の順に選択します。

ステップ 2 転送方法として [TFTP 経由] または [HTTP/HTTPS 経由] を選択します。

ステップ 3 コンフィギュレーション データを PC にバックアップするには、[ダウンロード（アクセス ポイントから PC）] を選択します。

ステップ 4 TFTP バックアップの場合、拡張子 xml を付けて宛先ファイル名を入力します。サーバ上のファイルを保存するパスも含めてから、[TFTP サーバの IPv4 アドレス] を入力します。

ファイル名に、スペース、<、>、|、\、:、(、)、&、;、#、?、*、および 2 つ以上の連続したピリオドを使用することはできません。

ステップ 5 ファイルをダウンロードしたファイルで置き換えるため、[スタートアップ コンフィギュレーション] または [バックアップ コンフィギュレーション] を選択します。

ダウンロードしたファイルによってスタートアップ コンフィギュレーション ファイルが上書きされ、このファイルが妥当性検査に合格すると、ダウンロードしたコンフィギュレーションは WAP デバイスを次回リブートしたときに有効になります。

ステップ 6 [保存] をクリックしてアップグレードまたはバックアップを開始します。HTTP/HTTPS ダウンロードの場合は、ウィンドウが表示されて、ダウンロードするファイルを参照して選択できます。

注意 コンフィギュレーション ファイルのダウンロード中は、WAP デバイスへの電力が遮断されていないことを確認してください。コンフィギュレーション ファイルのダウンロード中に電源異常が発生すると、ファイルは失われるため処理を再開する必要があります。

コンフィギュレーション ファイルのコピー

WAP デバイス ファイル システム内でファイルをコピーすることができます。たとえば、バックアップ コンフィギュレーション ファイルをスタートアップ コンフィギュレーション ファイルタイプにコピーして、WAP デバイスの次回起動時に使用されるようにすることができます。

別のファイル タイプにファイルをコピーするには、次の手順を実行してください。

ステップ 1 [管理] > [コンフィギュレーション ファイル] > [コピー] の順に選択します。

ステップ 2 [コピー元] フィールドで、次のいずれかからコピーするソース ファイル タイプを選択します。

- [スタートアップ コンフィギュレーション] : スタートアップに使用されるコンフィギュレーション ファイル。
- [バックアップ コンフィギュレーション] : WAPデバイスに保存されているバックアップ コンフィギュレーション ファイル。
- [ミラー コンフィギュレーション] : スタートアップ コンフィギュレーションが24時間以上変更されていない場合は、ミラー コンフィギュレーション ファイルに自動で保存されます。ミラー コンフィギュレーションは、過去のスタートアップ コンフィギュレーションのスナップショットです。ミラー コンフィギュレーションは出荷時設定へのリセットをまたがって保存されます。このため、ミラー コンフィギュレーションをスタートアップ コンフィギュレーションにコピーすることで、出荷時設定へのリセット後にシステム コンフィギュレーションを回復するために使用できます。

ステップ 3 [コピー先] フィールドで、コピーするファイルによって置き換えられるファイル タイプを選択します。

ステップ 4 [保存] をクリックしてコピー処理を開始します。

コンフィギュレーション ファイルのクリア

スタートアップ コンフィギュレーション ファイルまたはバックアップ コンフィギュレーション ファイルをクリアすることができます。スタートアップ コンフィギュレーション ファイルをクリアすると、WAPデバイスを次回リブートしたときにバックアップ コンフィギュレーション ファイルがアクティブになります。

スタートアップ コンフィギュレーション ファイルまたはバックアップ コンフィギュレーション ファイルを削除するには、次の手順を実行してください。

ステップ 1 [管理] > [コンフィギュレーション ファイル] > [クリア] の順に選択します。

ステップ 2 [スタートアップ コンフィギュレーション] または [バックアップ コンフィギュレーション] を選択します。

ステップ 3 [ファイルのクリア] をクリックします。

ステップ 4 [OK] をクリックします。

リブート

[リブート] ページを使用して、WAP デバイスをリブートするか、または WAP デバイスを工場出荷時のデフォルトにリセットします。WAP デバイスをリブートまたはリセットするには、次の手順を実行します。

ステップ 1 [管理] > [リブート] の順に選択します。

ステップ 2 工場出荷時のデフォルトのコンフィギュレーション ファイルを使用して WAP デバイスをリブートするには、[工場出荷時設定に戻す] をオンにします。カスタマイズしたすべての設定が失われます。

ステップ 3 [リブート] をクリックします。リブートの確認またはキャンセルを促すウィンドウが表示されます。
ステップ 4 [OK] をクリックしてリブートします。

リブートのスケジュール

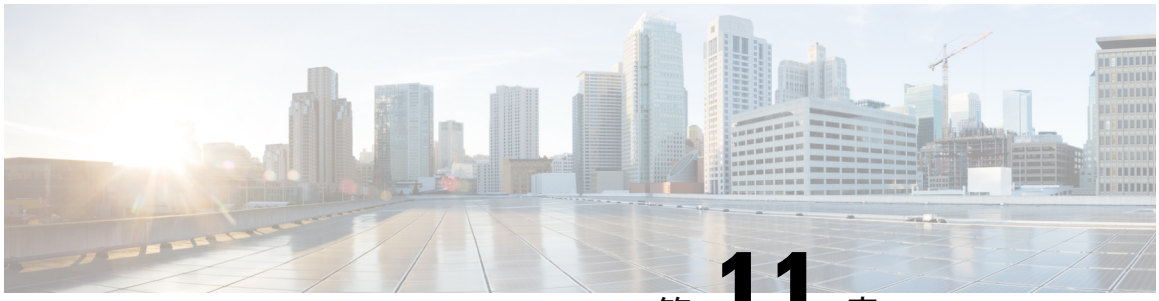
WAP デバイスでのリブートをスケジュールするには、次の手順に従います。

ステップ 1 [リブートのスケジュール] チェックボックスをオンにし、リブート スケジュール機能を有効にします。
ステップ 2 リブートをスケジュールする際には次の 2 つのオプションを使用できます。

- [日付]：デバイスをリブートする正確な日時を設定します。
- [設定時間]：機能を有効にした後でリブートを実行するリブート時間を設定します。

（注） [設定時間] の場合、デバイスのリブート後もリブート スケジューラは引き続き有効です。

ステップ 3 [保存] をクリックします。



第 11 章

トラブルシュート

この章では、トラブルシューティング用に複数の WAP デバイスでパケット キャプチャを設定する方法について説明します。具体的な内容は次のとおりです。

- スペクトル インテリジェンス （153 ページ）
- パケット キャプチャ （154 ページ）
- サポート情報 （161 ページ）

スペクトル インテリジェンス

[スペクトル インテリジェンス] ページには、スペクトル アナライザ機能のステータスとスペクトラム データを表示するためのリンクが示されます。次のページに、スペクトル アナライザに関する詳細が説明されています。

[スペクトラム解析モードの有効化]：スペクトラム解析モードは[専用スペクトルアナライザ]、[ハイブリッド スペクトル アナライザ]、または [3+1 スペクトラム解析] のいずれかです。

ステップ 1 **[トラブルシュート] > [スペクトル インテリジェンス]** の順に選択します。

ステップ 2 無線インターフェイスを選択し、[設定] ボタンをクリックしてスペクトル インテリジェンスを開始します。

ステップ 3 [スペクトラム データの表示] をクリックし、[チャネル品質] および [非 WLAN チャネルの使用率] の詳細を確認します。

[スペクトラム データの表示]：スキャン モードが [専用スペクトル アナライザ]、[ハイブリッド スペクトル アナライザ]、または [3+1 スペクトル アナライザ] に設定されていて、無線がオンのステータスになっており、Web ページに IPv4 アドレス経由でのみアクセスできる場合に、スペクトラム ビューアを起動します。

ステップ 4 [スペクトラム解析モード] のステータスを無効にするには、[停止] をクリックします。

パケット キャプチャ

ワイヤレス パケット キャプチャ機能を使用すると、WAP デバイスによって送受信されたパケットをキャプチャおよび保管できます。キャプチャされたパケットは、次に、トラブルシューティングやパフォーマンスの最適化のためにネットワーク プロトコル アナライザで分析できます。

パケット キャプチャには 2 通りの方式があります。

- **ローカル キャプチャ方式**：キャプチャされたパケットは WAP デバイス上のファイルに保管されます。WAP デバイスでこのファイルを TFTP サーバに送信できます。このファイルは pcap 形式でフォーマットされており、Wireshark を使用して検査できます。[このデバイスにファイルを保存する]を選択してローカルキャプチャ方法を選択します。
- **リモート キャプチャ方式**：キャプチャされたパケットは Wireshark を実行している外部コンピュータにリアルタイムでリダイレクトされます。リモートキャプチャ方式を選択するには、[リモートホストへのストリーム]を選択します。

  キャプチャしたパケットは、Web ベースのパケット デコーダおよびアナライザ サイトである CloudShark にリアルタイムでリダイレクトされます。それは、パケット分析のための Wireshark UI に似ています。[CloudShark へのストリーム（Stream to CloudShark）] を選択することにより、リモート キャプチャ方式を選択できます。

WAP デバイスでは次のタイプのパケットをキャプチャできます。

- 無線インターフェイスで送受信された 802.11 パケット。802.11 ヘッダーを含む、無線インターフェイスでキャプチャされたパケット。
- イーサネット インターフェイスで送受信された 802.3 パケット。
- VAP インターフェイス、WDS インターフェイスなどの内部論理インターフェイスで送受信された 802.3 パケット。

[パケット キャプチャ] ページを使用して、パケット キャプチャのパラメータの設定、ローカルまたはリモートでのパケット キャプチャの開始、現在のパケット キャプチャのステータスの表示、およびパケット キャプチャ ファイルのダウンロードを行うことができます。

ローカル パケット キャプチャ

ローカル パケット キャプチャを開始するには、次の手順を実行してください。

ステップ 1 [トラブルシュート] > [パケット キャプチャ] の順に選択します。

ステップ 2 [パケット キャプチャ方式] で [このデバイスにファイルを保存] が選択されていることを確認します。

ステップ 3 次のパラメータを設定します。

- [インターフェイス]：パケット キャプチャのキャプチャ インターフェイス タイプを入力します。

- [イーサネット]：イーサネット ポート上の 802.3 トラフィック。
- [無線 1]/[無線 2]：無線インターフェイス上の 802.11 トラフィック。

- [期間]：キャプチャの期間を秒数で入力します。範囲は 10 ～ 3600 です。デフォルトは 60 です。
- [最大ファイル サイズ]：キャプチャ ファイルの最大許容サイズをキロバイト（KB）単位で入力します。範囲は 64 ～ 4096 です。デフォルトは 1024 です。

ステップ 4 パケット キャプチャには 2 種類のモードがあります。

- [すべてのワイヤレス トラフィック]：すべてのワイヤレス パケットをキャプチャします。
- [この AP への、またはこの AP からのトラフィック]：この AP から送信されるパケットまたはこの AP が受信するパケットをキャプチャします。

ステップ 5 [フィルタを有効にする] をクリックします。3 つのチェックボックスを設定できます（[ビーコンを無視する]、[クライアントのフィルタ]、[SSID のフィルタ]）。

- [ビーコンを無視する]：無線によって検出または伝送された 802.11 ビーコンのキャプチャを有効または無効にします。
- [クライアントのフィルタ]：WLAN クライアント フィルタ用の MAC アドレスを指定します。クライアント フィルタは、802.11 インターフェイスでキャプチャを実行している場合に限りアクティブである点に注意してください。
- [SSID のフィルタ]：パケット キャプチャの SSID 名を選択します。

ステップ 6 [設定を保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

ステップ 7 [キャプチャの開始] をクリックし、[更新] をクリックすると、次のデータが示されている [パケット キャプチャ ステータス] が表示されます。

a) **現在のキャプチャ ステータス**
b) **パケット キャプチャ時間**
c) **パケット キャプチャ ファイル サイズ**

ローカル パケット ファイル キャプチャ モードでは、WAP デバイスはキャプチャしたパケットを RAM ファイル システムに保管します。有効化したパケット キャプチャは、次のいずれかのイベントが発生するまで持続します。

- キャプチャ時間が設定した期間に到達する。
- キャプチャ ファイルが最大サイズに到達する。
- 管理者がキャプチャを停止する。

リモート パケット キャプチャ

リモート パケット キャプチャ機能では、パケット キャプチャの宛先ポートとしてリモート ポートを指定できます。この機能は Windows 用 Wireshark ネットワーク アナライザ ツールと連携して動作します。パケット キャプチャ サーバは WAP デバイス上で実行され、キャプチャしたパケットは TCP 接続を通じて Wireshark ツールに送信されます。Wireshark はオープン ソースのツールで、https://www.wireshark.org/ からダウンロードして無料で利用できます。

Wireshark ツールを実行している Microsoft Windows コンピュータでは、キャプチャしたトラフィックを表示、記録、および分析できます。リモート パケット キャプチャ機能は、Windows 用 Wireshark ツールの標準機能です。Linux バージョンは WAP デバイスでは機能しません。

リモート キャプチャ モードを使用している場合、WAP デバイスでは、キャプチャしたデータをローカルのファイル システムに保管しません。

Wireshark コンピュータと WAP デバイスの間にファイアウォールが設置されている場合は、ファイアウォールを通過するように、該当ポートのトラフィックを許可する必要があります。ファイアウォールは、Wireshark コンピュータから WAP デバイスへの TCP 接続の開始を許可するように設定する必要もあります。

リモート ホストへのストリーミング

WAP デバイスでリモート キャプチャを開始するには、[リモートホストへのストリーミング（Stream to a Remote Host）] オプションを使用します。

ステップ 1 [トラブルシュート] > [パケット キャプチャ] の順に選択します。

ステップ 2 [パケット キャプチャ方式] で [リモート ホストへのストリーム] オプション ボタンをクリックします。

ステップ 3 [リモート キャプチャ ポート] フィールドでデフォルト ポート（2002）を使用します。デフォルト以外のポートを使用する場合は、Wireshark を WAP デバイスに接続するために使用するポート番号を入力します。ポートの範囲は 1025 ～ 65530 です。

ステップ 4 パケット キャプチャには 2 種類のモードがあります。

- [すべてのワイヤレス トラフィック] : 無線通信のすべてのワイヤレス パケットをキャプチャします。
- [この AP への、またはこの AP からのトラフィック] : この AP から送信されるパケットまたはこの AP が受信するパケットをキャプチャします。

ステップ 5 次に [フィルタを有効にする] をオンにします。次のいずれかのオプションを選択します。

- [ビーコンを無視する] : 無線によって検出または伝送された 802.11 ビーコンのキャプチャを有効または無効にします。
- [クライアントのフィルタ] : WLAN クライアント フィルタ用の MAC アドレスを指定します。クライアント フィルタは、802.11 インターフェイスでキャプチャを実行している場合に限りアクティブである点に注意してください。
- [SSID のフィルタ] : パケット キャプチャの SSID 名を選択します。

ステップ 6 別の機会に使用するために設定を保存するには、[保存] をクリックします。ただし、[パケット キャプチャ方式] として [リモート] を選択しても、その選択は保存されません。

ステップ 7 [キャプチャの開始] をクリックしてキャプチャを開始します。キャプチャを停止するには、[キャプチャの停止] をクリックします。

CloudShark へのストリーム

[CloudShark へのストリーム（Stream to CloudShark）] オプションを使用して WAP デバイス上でリモート キャプチャを開始するには、次のことを実行します。

ステップ 1 [トラブルシュート（Troubleshoot ）] > [パケット キャプチャ（Packet Capture）] の順に選択します。

ステップ 2 [パケット キャプチャ方式（Packet Capture Method）] で [CloudShark へのストリーム（Stream to CloudShark）] オプション ボタンをクリックします。

ステップ 3 次のパラメータを設定します。

a) [インターフェイス（Interface ）] : パケット キャプチャのキャプチャ インターフェイス タイプを入力します

b) [イーサネット（Ethernet ）] : イーサネット ポート上の 802.3 トラフィック

c) [無線 1（5GHz）]/[無線 2（2.4GHz）（Radio 1 (5GHz) / Radio 2 (2.4GHz)）] : 無線インターフェイス上の 802.11 トラフィック

d) [期間（Duration）] : キャプチャの期間を秒数で入力します。 CloudShark からの期間の制限はありません。デフォルトは 60 です

e) [最大ファイル サイズ（Max File Size）] : キャプチャ ファイルの最大許容サイズをキロバイト（KB）単位で入力します。 ここではサイズの制限はありません。デフォルトは 1024 です。

（注） 注：CloudShark には、2 つの有効なアカウント タイプがあります。つまり、パーソナルとビジネスです。1 回でアップロードできる最大サイズは、パーソナル アカウント タイプの場合は 25MB、ビジネス アカウント タイプの場合は 150MB です。サイズを超える部分は、アカウント タイプに基づいて CloudShark により切り捨てられます。

f) [CloudShark URL] - CloudShark のホスト名を入力します。デフォルト URL: *https://www.cloudshark.org*

g) [CloudShark API キー（CloudShark API Key）] : CloudShark から登録した有効な API トークンを入力します

ステップ 4 CloudShark との通信は HTTPS で行います。自己署名 SSL 証明書を使用する場合は、[はい（Yes）] オプションを選択し、[証明書のアップロード（Upload a certificate）] をクリックして、署名した証明書をアップロードします。

ステップ 5 [フィルタ式（Filter expression）] フィールドにキャプチャするプロトコルを入力します。CloudShark に転送されるのは、フィルタ後のパケットのみです

ステップ 6 パケット キャプチャには 2 種類のモードがあります。

a) [すべてのワイヤレス トラフィック（All Wireless Traffic ）] : すべてのワイヤレス パケットをキャプチャします。

b) [この AP で送受信するトラフィック（Traffic To/From this AP）]：この AP から送信されるパケットまたはこの AP が受信するパケットをキャプチャします

ステップ 7 [フィルタを有効にする（Enable Filters）] をクリックします。次の 3 オプションの中から選択できます。

a) [ビーコンを無視する（Ignore Beacons）]：無線によって検出または伝送された 802.11 ビーコンのキャプチャを有効または無効にします

b) [クライアントのフィルタ（Filter on Client）]：WLAN クライアント フィルタ用の MAC アドレスを指定します。

（注） クライアント フィルタは、802.11 インターフェイスのキャプチャを実施している場合に限りアクティブです。

c) [SSID のフィルタ（Filter on SSID）]：パケット キャプチャの SSID 名を選択します。

ステップ 8 [保存（Save）] をクリックします。変更が、スタートアップ コンフィギュレーションに保存されます。

ステップ 9 [キャプチャ開始（Start Capture）] をクリックします。パケット キャプチャ モードの場合、キャプチャされたパケットはリアルタイムで CloudShark サイトに送信されます。有効化したパケット キャプチャは、次のいずれかのイベントが発生するまで持続します。

a) キャプチャ時間が設定した期間に到達する

b) キャプチャ ファイルが最大サイズに到達する。

c) 管理者がキャプチャを停止する

Wireshark

最初に Wireshark をダウンロードし、コンピュータにインストールします。Wireshark は https://www.wireshark.org/ からダウンロードできます。

Microsoft Windows 用 Wireshark ネットワーク アナライザ ツールを開始するには、次の手順に従います。

ステップ 1 コンピュータで Wireshark ツールを開始します。

ステップ 2 メニューで [キャプチャ] > [オプション] を選択します。ポップアップ ウィンドウが表示されます。

ステップ 3 [インターフェイス] フィールドで [リモート] を選択します。ポップアップ ウィンドウが表示されます。

ステップ 4 [ホスト] フィールドに WAP デバイスの IP アドレスを入力します。

ステップ 5 [ポート] フィールドに WAP デバイスのポート番号を入力します。たとえば、デフォルトを使用した場合は 2002 を入力し、デフォルト以外のポートを使用した場合は使用したポート番号を入力します。

ステップ 6 [OK] をクリックします。

ステップ 7 パケットをキャプチャする必要のあるインターフェイスを選択します。Wireshark ポップアップ ウィンドウの IP アドレスの横に、インターフェイスを選択するためのドロップダウン メニューがあります。インターフェイスは次のいずれかにすることができます。

Linux bridge interface in the wap device

```
--rpcap://[192.168.1.220]:2002/brtrunk
```

Wired LAN interface

-- rpcap://[192.168.1.220]:2002/eth0

VAP0 traffic on radio 1

-- rpcap://[192.168.1.220]:2002/wlan0

802.11 traffic

-- rpcap://[192.168.1.220]:2002/radio1

At WAP361, VAP1 ~ VAP7 traffic

-- rpcap://[192.168.1.220]:2002/wlan0vap1 ~ wlan0vap7

At WAP150, VAP1 ~ VAP3 traffic

-- rpcap://[192.168.1.220]:2002/wlan0vap1 ~ wlan0vap3

WAP デバイス上の最大 4 個のインターフェイスを同時にトレースできます。ただし、インターフェイスごとに別々の Wireshark セッションを開始する必要があります。追加のリモート キャプチャ セッションを開始するには、Wireshark の構成手順を繰り返します。WAP デバイスを設定する必要はありません。

（注） システムでは、リモート パケット キャプチャ セッション用に設定されたポートから始まる連続する 4 個のポート番号を使用します。連続する 4 個のポート番号を使用できることを確認してください。デフォルト ポートを使用しない場合は、1024 よりも大きいポート番号を使用することをお勧めします。

無線インターフェイスのトラフィックをキャプチャする際、ビーコン キャプチャを無効化することはできますが、その他の 802.11 制御フレームは引き続き Wireshark に送信されます。次の情報のみを表示するように表示フィルタを設定できます。

- トレース内のデータ フレーム。
- 特定の Basic Service Set ID（BSSID）のトラフィック。
- 2 つのクライアント間のトラフィック。

次に有用な表示フィルタの例をいくつか示します。

- ビーコンおよび ACK/RTS/CTS フレームを除外：

  !(wlan.fc.type_subtype == 8 | | wlan.fc.type == 1)

- データ フレーム限定：

  wlan.fc.type == 2

- 特定の BSSID 上のトラフィック：

  wlan.bssid == 00:02:bc:00:17:d0

- 特定のクライアントとの間の全トラフィック：

  wlan.addr == 00:00:e8:4e:5f:8e

リモートキャプチャモードでは、トラフィックは、いずれかのネットワークインターフェイスを通じて、Wireshark を実行しているコンピュータに送信されます。トラフィックは、Wireshark ツールの場所に応じて、イーサネットインターフェイスまたはいずれかの無線で送信できます。パケットをトレースしたため

にトラフィックがフラッディングしないために、WAP デバイスでは、Wireshark アプリケーションを宛先とするすべてのパケットをフィルタ処理して除外するキャプチャ フィルタを自動で設定します。たとえば、Wireshark IP ポートが 58000 に設定されている場合は、次のキャプチャ フィルタが WAP デバイスに自動で設定されます。

ポート範囲 58000 ～ 58004 以外

パフォーマンスおよびセキュリティ上の問題から、パケット キャプチャ モードは WAP デバイス上の NVRAM には保存されません。WAP デバイスをリセットすると、キャプチャ モードは無効になるため、トラフィックのキャプチャを再開するには、再度有効にする必要があります。パケット キャプチャ パラメータ（モードを除く）は NVRAM に保存されます。

パケット キャプチャ機能を有効化すると、次のセキュリティ上の問題が発生することがあります。権限を持たないクライアントが WAP デバイスに接続してユーザ データをトレースするおそれがあります。パケットのキャプチャ中は WAP デバイスのパフォーマンスにも悪影響があり、この影響はアクティブ Wireshark セッションがない場合でも、ある程度続くことがあります。トラフィック キャプチャ中に WAP デバイスでのパフォーマンスへの影響を最小限にするには、Wireshark ツールに送信されるトラフィックを制限するキャプチャ フィルタを設定します。802.11 トラフィックをキャプチャする場合、キャプチャしたフレームの大部分はビーコンである傾向があります（通常、すべてのアクセス ポイントから 100 ミリ秒ごとに送信されます）。Wireshark ではビーコン フレームの表示フィルタをサポートしている一方で、WAP デバイスがキャプチャしたビーコン パケットを Wireshark ツールに転送しないようにするキャプチャ フィルタはサポートしていません。802.11 ビーコンのキャプチャ処理によるパフォーマンス上の影響を削減するには、キャプチャ ビーコン モードを無効にします。

パケット キャプチャ ファイルのダウンロード

キャプチャ ファイルは、TFTP を介して設定した TFTP サーバにダウンロードするか、HTTP/HTTPS を介してコンピュータにダウンロードできます。キャプチャ ファイルのダウンロード コマンドがトリガーされると、キャプチャは自動的に停止します。

キャプチャ ファイルは RAM ファイル システムにあるため、WAP デバイスがリセットされると消去されます。

TFTP を使用してパケット キャプチャ ファイルをダウンロードするには、次の手順を実行してください。

ステップ 1 [TFTP サーバにダウンロード] をクリックします。

ステップ 2 表示されるフィールドに TFTP サーバの IPv4 アドレスを指定します。

ステップ 3 デフォルトと異なる場合は、ダウンロードする TFTP サーバ ファイル名を入力します。デフォルトでは、キャプチャされたパケットは WAP デバイスの /tmp/apcapture.pcap フォルダ ファイルに保管されます。

ステップ 4 [ダウンロード] をクリックします。

HTTP の使用

HTTP を使用してパケット キャプチャ ファイルをダウンロードするには、次の手順を実行してください。

ステップ 1 [このデバイスにダウンロード] をクリックします。確認ポップアップ メッセージが表示されます。

ステップ 2 [OK] をクリックします。ポップアップが表示され、ファイルを保存するネットワーク場所を選択できます。

サポート情報

この [サポート情報] ページには、CPU と RAM のステータスが表示されます。

CPU/RAM アクティビティを記録して表示するには、次の手順に従います。

ステップ 1 [トラブルシュート] > [サポート情報] を選択します。

ステップ 2 [CPU]（CPU アクティビティを記録および表示するためのデバイス）をクリックします。記録を停止するには、[CPU] をもう一度クリックします。

ステップ 3 [RAM]（RAM アクティビティを記録および表示するためのデバイス）をクリックします。記録を停止するには、[RAM] をもう一度クリックします。

グラフに CPU/RAM ステータスが次のように表示されます。

- 青色の線は CPU アクティビティを示します。
- 赤色の線は RAM アクティビティを示します。
- 1 番目の折れ線グラフのデータは、1 秒ごとに更新されます。これは 60 秒間の CPU/RAM アクティビティを示します。
- 2 番目の折れ線グラフのデータは、5 秒ごとに更新されます。これは 5 分間の CPU/RAM アクティビティを示します。

ステップ 4 [保存] をクリックします。

CPU/RAM データのダウンロード

選択した時間の CPU/RAM アクティビティをダウンロードするには、[サポート情報] ページを使用します。このテキスト ファイルはテクニカル サポート担当者に提供して、問題のトラブルシューティングに役立てることができます。CPU/RAM データをダウンロードするには、次の手順に従います。

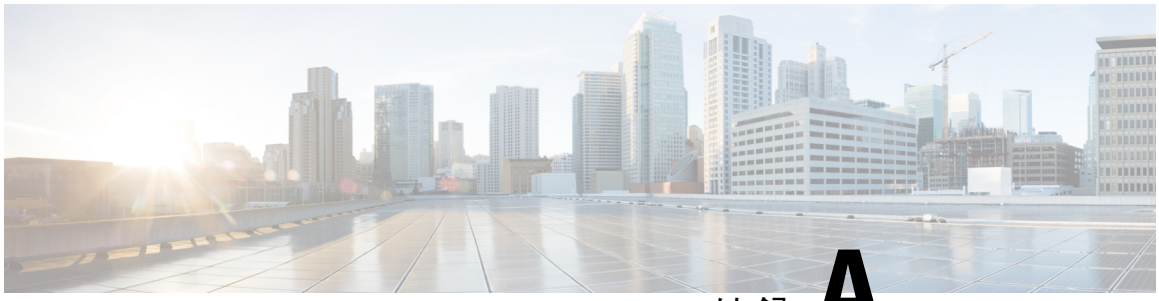
ステップ 1 [トラブルシュート] > [サポート情報] を選択します。

ステップ 2 [データのダウンロード] 領域で [有効化] をオンにし、ダウンロードを有効にします。

ステップ 3 ダウンロードを実行する時間を選択します（[今日]、[過去 7 日間]、[過去 30 日間]、[すべて]、[カスタム]）。

ステップ 4 [終了日時] フィールドと [開始日時] フィールドに yyyy-mm-dd 形式で値を入力し、次に hh:mm:ss 形式で時刻を設定します。

ステップ 5 [ダウンロード] をクリックして、現在のシステム設定に基づいてファイルを生成します。短い待ち時間の後でウィンドウが表示されて、ファイルをコンピュータに保存できます。



付録 A

認証解除メッセージの理由コード

この付録は、以下のセクションから構成されています。

- 認証解除メッセージの理由コード （163 ページ）
- 認証解除理由コード表 （163 ページ）

認証解除メッセージの理由コード

クライアントが WAP デバイスから認証解除されると、メッセージがシステム ログに送られます。このメッセージには、クライアントが認証解除された原因を特定するために役立つことのある理由コードが含まれています。[システム構成]> [通知]> [システムログの表示]をクリックすると、ログメッセージを表示できます。

詳細は、次を参照してください 認証解除理由コード表 （163 ページ）。

認証解除理由コード表

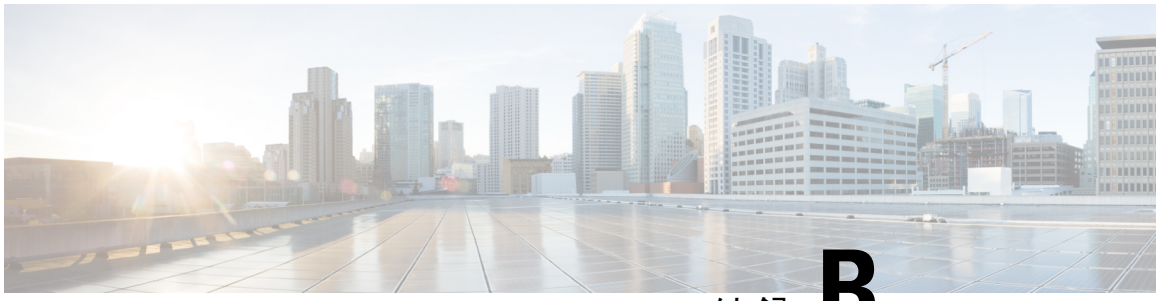
次の表に、認証解除理由コードを示します。

表 *2:* 認証解除理由コード表

理由コード	意味
0	予約済み
1	理由の指定なし
2	直前の認証が有効ではなくなった
3	送信側ステーション（STA）が独立基本サービス セット（IBSS）または ESS を去ろうとしているか去ったため認証解除されました
4	非アクティブであるため認証解除されました

認証解除メッセージの理由コード

理由コード	意味
5	WAP デバイスで現在関連付けられている STA の一部を処理できないため認証解除されました
6	関連付けられていない STA からクラス 2 フレームを受信しました
7	関連付けられていない STA からクラス 3 フレームを受信しました
8	送信側 STA が基本サービス セット（BSS）を去ろうとしているか去ったため認証解除されました
9	関連付け（または再関連付け）を要求している STA は応答側 STA で認証されていません
10	Power Capability 要素に含まれている情報が許容されないため認証解除されました
11	Supported Channels 要素に含まれている情報が許容されないため認証解除されました
12	予約済み
13	無効な要素（この標準規格に定義されており、内容が Clause 8 の指定を満たさない要素）
14	メッセージ完全性符号（MIC）エラー
15	4 ウェイ ハンドシェイク タイムアウト
16	グループ鍵ハンドシェイク タイムアウト
17	4 ウェイ ハンドシェイクに含まれている要素が Association Request/Reassociation Request/Probe Response/Beacon フレーム内の要素と異なる
18	無効なグループ暗号方式
19	無効なペアワイズ暗号方式
20	無効な AKMP
21	サポートされていない RSNE バージョン
22	無効な RSNE 機能
23	IEEE 802.1X 認証失敗
24	セキュリティ ポリシーによって暗号スイートが拒否されました



付 録 B

関連情報

この付録は、以下のセクションから構成されています。

• 関連情報 （165 ページ）

関連情報

サポート

シスコ サポート コミュニティ	http://www.cisco.com/go/smallbizsupport
シスコ サポートおよびリソース	http://www.cisco.com/go/smallbizhelp
電話サポートのお問い合わせ先	http://www.cisco.com/c/en/us/support/web/tsd-cisco-small-business-support-center-contacts.html
シスコ ファームウェアのダウンロード	http://www.cisco.com/go/smallbizfirmware リンクを選択して、シスコ製品のファームウェアをダウンロードできます。ログインは不要です。
シスコ オープン ソース リクエスト	アプリケーションの無料/オープン ソース ライセンス（GNU Lesser/一般公的使用許諾など）により使用資格が与えられているソース コードのコピーを受け取るには、次の宛先にリクエストを送信してください。 external-opensource-requests@cisco.com リクエストには、製品のオープン ソース マニュアルに記載されている、シスコ製品の名前、バージョン、18 桁の参照番号（例：7XEEX17D99-3X49X08 1）を明記してください。
Cisco WAP581 アドミニストレーション ガイド	http://www.cisco.com/go/500_wap_resources

関連情報

シスコ電源アダプタ	http://www.cisco.com/go/wap_accessories