WLAN

- WLAN について （1 ページ）
- WLAN の前提条件 （4 ページ）
- WLAN の制約事項 （5 ページ）
- WLAN の設定方法 （7 ページ）
- WLAN プロパティの監視（CLI） （18 ページ）

WLAN について

この機能により、Lightweight アクセス ポイント全体に対して、最大 の WLAN を制御できます。各 WLAN には識別子である WLAN ID、プロファイル名、および WLAN SSID があります。すべてのdevicesは接続している各アクセス ポイントに対して最大 16 の WLAN を公開しますが、管理しやすくするため、サポートされる最大数の WLAN を作成し、これらの WLAN を異なるアクセス ポイントに選択的に公開する（アクセス ポイント グループを使用）ことができます。

異なる SSID または同じ SSID で WLAN を設定できます。SSID は、deviceがアクセスする必要がある特定の無線ネットワークを識別します。

（注） **no configure max-user-identity response** コマンドが設定されている場合でも、**wireless client max-user-login concurrent** コマンドは意図したとおりに機能します。

バンドの選択

帯域選択によって、デュアルバンド（2.4 GHz および 5 GHz）動作が可能なクライアントの無線を、輻輳の少ない 5 GHz アクセス ポイントに移動できます。2.4 GHz 帯域は、混雑していることがあります。この帯域のクライアントは一般に、Bluetooth デバイス、電子レンジ、およびコードレス電話機からの干渉を受けるだけでなく、他のアクセス ポイントからの同一チャネル干渉も受けます。これは、802.11b/g では、重複しないチャネルの数が 3 つに制限されているためです。このような干渉源を防ぎ、ネットワーク全体のパフォーマンスを向上させるには、deviceで帯域選択を設定します。

オフチャネル スキャンの保留

通常の動作状態では、Lightweightアクセス ポイントは定期的にオフ チャネルになり、別のチャネルをスキャンします。これは、次のような RRM 動作を実行するためのものです。

- 他の AP を使用した NDP パケットの送受信
- 不正 AP とクライアントの検出
- ノイズと干渉の測定

オフ チャネル期間は通常は約 70 ミリ秒で、この期間は AP は対応するチャネル上でデータの送受信ができません。したがって、パフォーマンスに若干の影響が及び、一部のクライアント送信がドロップされることがあります。

重要なデータをAPが送受信している間はオフチャネル スキャンを保留するように設定して、APがオフチャネルにならず、通常動作に影響を与えないようにすることができます。オフチャネルスキャンの保留は、指定した時間しきい値（ミリ秒単位）でWMMUPクラス単位でWLANごとに設定できます。AP が指定されたしきい値内の所定の UP クラスでマークされたデータフレームを特定の WLAN 上で送受信している場合、その AP は次の RRM オフチャネル スキャンを保留します。たとえば、デフォルトでは、オフチャネル スキャンの保留は UP クラス 4、5、および 6 に対して 100 ミリ秒の時間しきい値で有効になります。したがって、RRM がオフチャネル スキャンを実行しようとしているときに直近の 100 ミリ秒内に UP 4、5、または 6 でマークされたデータ フレームを受信すると、RRM はオフチャネルになるのを保留します。音声サンプルを送受信し、UP 6 としてマークされている音声コールが 20 ミリ秒ごとにアクティブになる場合は、AP 無線はオフチャネルになりません。

オフチャネル スキャンの保留ではトレードオフが生じます。オフチャネル スキャンは、設定やトラフィック パターンなどに応じて2%以上の影響をスループットに与える可能性があります。すべてのトラフィック クラスに対してオフチャネル スキャンの保留を有効にし、時間しきい値を引き上げると、スループットが若干改善する可能性があります。ただし、オフチャネルにならないようにすることによって、RRM は AP ネイバーや不正を識別できず、セキュリティ、DCA、TPC、および 802.11k メッセージに悪影響が及びます。

デフォルトのオフチャネル スキャンの保留設定を変更しないことを推奨します。

DTIM 期間

802.11 ネットワークでは、Lightweight アクセス ポイントは、Delivery Traffic Indication Map (DTIM) と一致するビーコンを定期的に送信します。アクセス ポイントでビーコンがブロードキャストされると、DTIM期間で設定した値に基づいて、バッファされたブロードキャストフレームおよびマルチキャスト フレームが送信されます。この機能により、ブロードキャストデータやマルチキャストデータが予想されると、適切なタイミングで省電力クライアントを再起動できます。

通常、DTIM の値は 1（ブロードキャスト フレームおよびマルチキャスト フレームはビーコンのたびに送信）または 2（ビーコン 1 回おきに送信）のいずれかに設定されます。たとえば、802.11 ネットワークのビーコン間隔が 100 ミリ秒で DTIM 値が 1 に設定されている場合、アク

セス ポイントは、バッファされたブロードキャスト フレームおよびマルチキャスト フレームを毎秒 10 回送信します。ビーコン期間が 100ms で DTIM 値が 2 に設定されていると、アクセス ポイントは、バッファされたブロードキャスト フレームおよびマルチキャスト フレームを毎秒5回送信します。これらの設定はいずれも、ブロードキャスト フレームおよびマルチキャスト フレームの頻度を想定する、Voice over IP（VoIP）を含むアプリケーションに適しています。

ただし、DTIM 値は、802.11 のすべてのクライアントで省電力モードがイネーブルである場合、255 まで設定できます（255 回のビーコンごとにブロードキャスト フレームおよびマルチキャスト フレームを送信します）。クライアントは DTIM 期間に達したときのみリッスンする必要があるため、ブロードキャストとマルチキャストをリッスンする頻度を少なく設定することで、結果的にバッテリー寿命を長くできます。たとえば、ビーコン期間が 100 ms、DTIM 値を 100 に設定すると、アクセス ポイントは、バッファされたブロードキャスト フレームおよびマルチキャスト フレームを 10 秒ごとに 1 回送信します。このレートにより省電力クライアントで、ブロードキャストとマルチキャストをリッスンし、ウェイク アップするまでのスリープ状態が長くなり、バッテリ寿命を長くできます。

（注） ビーコン期間は、deviceでミリ秒単位で指定され、ソフトウェアによって、802.11 の時間単位（TU）（1 TU = 1.024 ミリ秒）に、内部的に変換されます。Cisco の 802.11n アクセス ポイントでは、この値は直近の 17 TU の倍数に丸められます。たとえば、100 ミリ秒に設定されたビーコン間隔は 104 ミリ秒の実際のビーコン間隔の結果です。

多くのアプリケーションでは、ブロードキャスト メッセージとマルチキャスト メッセージとの間隔を長くすると、プロトコルとアプリケーションのパフォーマンスが低下します。このようなクライアントをサポートする 802.11 ネットワークでは、低い DTIM 値を推奨します。

セッション タイムアウト

WLAN にセッション タイムアウトを設定できます。セッション タイムアウトとは、クライアント セッションが再認証を要求することなくアクティブである最大時間を指します。

Cisco Client Extensions

Cisco Client Extensions（CCX）ソフトウェアは、サードパーティ製クライアント デバイスの製造業者およびベンダーに対してライセンスされます。これらのクライアント上の CCX コードにより、サードパーティ製クライアント デバイスは、シスコ製のアクセス ポイントと無線で通信できるようになり、セキュリティの強化、パフォーマンスの向上、高速ローミング、電源管理などの、他のクライアントデバイスがサポートしていないシスコの機能もサポートできるようになります。

- ソフトウェアは、CCX バージョン 1 ～ 5 をサポートします。これによって、devicesとそのアクセス ポイントは、CCX をサポートするサードパーティ製クライアント デバイスと無線で通信できます。CCX サポートは、device上の各 WLAN に対して自動的に有効にな

り、無効にすることはできません。ただし、Aironet Information Element（IE）を設定できます。

- Aironet IE のサポートが有効になっている場合、アクセス ポイントは、Aironet IE 0x85（アクセス ポイント名、ロード、アソシエートされたクライアントの数などを含む）をこの WLAN のビーコンやプローブ応答に格納して送信します。また、アクセス ポイントが再アソシエーション要求内の Aironet IE 0x85 を受信する場合、deviceは、Aironet IEs 0x85 および 0x95（deviceの管理 IP アドレスおよびアクセス ポイントの IP アドレスを含む）を再アソシエーション応答に格納して送信します。

ピアツーピア ブロッキング

ピアツーピアブロッキングは個別のWLANに対して適用され、各クライアントが、アソシエート先の WLAN のピアツーピア ブロッキング設定を継承します。ピア ツー ピアにより、トラフィックをリダイレクトする方法を制御できます。たとえば、トラフィックがdevice内でローカルにブリッジされたり、deviceによってドロップされたり、またはアップストリーム VLAN に転送されるように選択することができます。

ローカル スイッチングの WLAN にアソシエートしたクライアントに対して、ピアツーピアブロッキングはサポートされています。

診断チャネル

クライアントの WLAN による通信で問題が生じる理由についてトラブルシューティングする診断チャネルを選択できます。クライアントで発生している問題を識別し、ネットワーク上でクライアントを動作させるための修正措置を講じるために、クライアントとアクセスポイントをテストできます。診断チャネルを有効にするには、deviceの GUI または CLI を使用します。また、診断テストを実行するには、deviceの CLI を使用します。

（注） 診断チャネル機能は、管理インターフェイスを使用するアンカーされていない SSID に対してのみ有効にすることをお勧めします。CCX 診断機能は Cisco ADU カードを持つクライアントでのみテストされています。

WLAN の前提条件

- 最大 16 個の WLAN を各アクセス ポイント グループにアソシエートし、各グループに個々のアクセス ポイントを割り当てることができます。各アクセス ポイントは、有効化されている WLAN のうち、そのアクセス ポイント グループに属する WLAN だけをアドバタイズします。アクセス ポイント グループで無効化されている WLAN または別のグループに属する WLAN はアドバタイズしません。

- devicesがVLANトラフィックを正常にルーティングできるように、WLANと管理インターフェイスにはそれぞれ別のVLANを割り当てることをお勧めします。

（注） Cisco IOS XE Fuji 16.8.x リリース以降、BSSID は対応するすべての WLAN ID と AP 無線に対して動的に生成されます。

WLAN の制約事項

- WLAN のプロファイル名を変更すると、FlexConnect AP（AP 固有の VLAN マッピングを使用する）が WLAN 固有になります。FlexConnect グループが適切に設定されている場合、VLAN マッピングはグループ固有になります。
- Flex ローカル認証が有効にされている WLAN では、Fast Transition 802.1X キー管理でクライアント関連付けがサポートされないため、IEEE 802.1X Fast Transition を有効にしないでください。
- ピアツーピア ブロッキングは、マルチキャスト トラフィックには適用されません。
- WLAN 名と SSID は 32 文字以内にする必要があります。
- WLAN 名で特殊文字は使えません。
- WLAN 名はキーワードにはできません。たとえば、**wlan s** コマンドを入力して、「s」という名前で WLAN を作成しようとすると、「s」はシャットダウン用のキーワードとして使用されているため、すべての WLAN がシャットダウンします。
- WLAN から VLAN0 へのマッピング、VLAN 1002～1006 のマッピングはできません。
- 固定 IPv4 アドレスのデュアル スタック クライアントはサポートされません。
- 同じ SSID を持つ WLAN を作成するときには、各 WLAN に対して一意のプロファイル名を作成する必要があります。
- 同じ SSID を持つ複数の WLAN を同じ AP 無線に割り当てる場合は、クライアントがその中から安全に選択できるように、一意のレイヤ2セキュリティ ポリシーを使用している必要があります。
- WLAN がローカル スイッチングの場合、AVC が有効化されているローカル スイッチング WLAN にクライアントを関連付けます。AVC の統計 90 秒後を確認した時、クライアントからトラフィックを送信します。Cisco WLC はトップ アプリケーション下では表示されますが、クライアントには表示されません。タイマーの問題があるため、最初のスロットの Cisco WLC ではクライアントの統計が表示されない可能性があります。AP と WLC でのタイマーが 89 秒間オフであった場合、その前のわずか 1 秒間のクライアントの統計情報が表示されます。現在では統計の削除は 180 秒後であるため、91 秒から 179 秒までのクライアントの統計情報が表示されます。これは、各クライアントあたり 2 つのコピーの統計がメモリの制約で Cisco 5508 WLC に保持することができないために起こります。

- ユーザ プロファイルの一部として送信される SSID は、**aaa override** コマンドが設定されている場合にのみ機能します。
- WLAN ごとの RADIUS サーバ上書きインターフェイス機能はサポートされていません。ただし、次の設定を使用して同じ結果を得ることができます。
  - RADIUS 認証サーバの設定
  - RADIUS 認証サーバ グループの設定
  - 802.1x WLAN の作成
  - ワイヤレス プロファイル ポリシーの設定と VLAN への適用

RADIUS 認証サーバの設定

- Device (config)# **radius server** *server-name*
- Device (config-radius-server)# **address ipv4** *address* **auth-port** *auth_port_number* **acct-port** *acct_port_number*
- Device (config-radius-server)# **key** *key*

RADIUS 認証サーバ グループの設定

- Device(config)# **aaa group server radius** *server-name*
- Device(config)# **server name** *server-name*
- Device(config)# **ip radius source-interface vlan** *vlan-name*
- Device(config)# **aaa authentication dot1x** *dot1x_name* **group** *server-name*

802.1x WLAN の作成

- Device(config)# **wlan** *wlan-name id ssid*
- Device(config-wlan)# **security dot1x authentication-list** *list-name*
- Device(config-wlan)# **no shutdown**

ワイヤレス プロファイル ポリシーの設定と VLAN への適用

- Device(config)# **wireless profile policy** *profile-name*
- Device(config-wireless-policy)# **vlan** *vlan-name*
- Device(config-wireless-policy)# **no shutdown**

シスコ ワイヤレス コントローラでの設定例を次に示します。

```
radius server RAD_EXT_3

 address ipv4 9.2.62.56 auth-port 1812 acct-port 1813

 key cisco


aaa group server radius AAA_EXT_3
```

```
server name RAD_EXT_3
ip radius source-interface vlan 50

aaa authentication dot1x test_ext group AAA_EXT_3

wlan test_wpa2_dot1x 2 test_wpa2_dot1x
security dot1x authentication-list test_ext
no shutdown


wireless profile policy pp-1
vlan 50
no shutdown


radius server RAD_EXT_3

 address ipv4 9.2.62.56 auth-port 1812 acct-port 1813

 key cisco


aaa group server radius AAA_EXT_2
server name RAD_EXT_3
ip radius source-interface vlan 51

aaa authentication dot1x test_ext_2 group AAA_EXT_2

wlan test_wpa2 3 test_wpa3
security dot1x authentication-list test_ext_2
no shutdown


wireless profile policy pp-1
vlan 51
no shutdown
```

注意 一部のクライアントが複数のセキュリティ ポリシーで同じ SSID を検出すると WLAN に正しく接続できない場合があります。この機能を使用する際は、十分注意してください。

WLAN の設定方法

WLAN の作成（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。

ステップ 2 [Add] をクリックします。

[Add WLAN] ペインが表示されます。

ステップ 3 表示される [General] タブで、[Profile Name] フィールドに WLAN の名前を入力します。

ステップ 4 [Save & Apply to Device] をクリックします。

WLAN の作成（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name wlan-id* [*ssid*] 例： `Device(config)# wlan mywlan 34 mywlan-ssid`	WLAN の名前と ID を指定します。 • *profile-name* に、プロファイル名を入力します。入力できる範囲は英数字で 1 ～ 32 文字です。 • *wlan-id*に、WLAN ID を入力します。範囲は 1 ～ 512 です。 • *ssid* では、この WLAN に対する Service Set Identifier (SSID) を入力します。SSID を指定しない場合、WLAN プロファイル名は SSID として設定されます。 （注） WLAN はデフォルトでディセーブルにされています。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

WLAN の削除（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。

ステップ 2 削除する WLAN の横にあるチェックボックスをオンにします。

複数の WLAN を削除するには、複数の WLAN のチェックボックスをオンにします。

ステップ 3 [削除（Delete）] をクリックします。

ステップ 4 確認ウィンドウで [Yes] をクリックして WLAN を削除します。

WLAN の削除

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no wlan** *wlan-name wlan-id ssid* 例： `Device(config)# no wlan test2`	WLAN を削除します。引数は次のとおりです。 • *wlan-name*は WLAN プロファイル名です。 • *wlan-id*は、WLAN ID です。 • *ssid* は WLAN に設定された WLAN SSID 名前です。 （注） AP グループに属する WLAN を削除すると、WLAN は AP グループと AP の無線から削除されます。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

WLAN の検索

手順

	コマンドまたはアクション	目的
ステップ 1	**show wlan summary** 例： `Device# show wlan summary`	デバイスに設定されているすべての WLAN のリストを表示します。出力内で WLAN を検索できます。

例

```
Device# show wlan summary
Number of WLANs: 4

WLAN Profile Name                     SSID                           VLAN Status
-------------------------------------------------------------------------------
1    test1                             test1-ssid                     137  UP
3    test2                             test2-ssid                     136  UP
2    test3                             test3-ssid                     1    UP
45   test4                             test4-ssid                     1    DOWN
```

WLAN を検索するときにワイルドカードを使用できます。たとえば、**show wlan summary include** | *variable* などです。variable は、出力内の検索文字列です。

```
Device# show wlan summary | include test-wlan-ssid
1    test-wlan                       test-wlan-ssid                    137   UP
```

WLAN の有効化（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。

ステップ 2 [WLANs] ページで、WLAN 名をクリックします。

ステップ 3 [Edit WLAN] ウィンドウで、[Status] ボタンを [ENABLED] に切り替えます。

ステップ 4 [Update & Apply to Device] をクリックします。

WLAN のイネーブル化（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

WLAN の無効化（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。

ステップ 2 [WLANs] ページで、WLAN 名をクリックします。

ステップ 3 [Edit WLAN] ウィンドウで、[Status] ボタンを [DISABLED] に切り替えます。

ステップ 4 [Update & Apply to Device] をクリックします。

WLAN のディセーブル（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 2	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**shutdown** 例： `Device(config-wlan)# shutdown`	WLAN をディセーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 5	**show wlan summary** 例： `Device# show wlan summary`	デバイスに設定されているすべての WLAN のリストを表示します。出力内で WLAN を検索できます。

汎用 WLAN プロパティの設定（CLI）

次のパラメータを設定できます。

- メディア ストリーム
- ブロードキャスト SSID
- コール スヌーピング
- Radio
- インターフェイス
- ステータス

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例：	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設

	コマンドまたはアクション	目的
	`Device# wlan test4`	定されているWLANのプロファイル名です。
ステップ 3	**shutdown** 例： `Device# shutdown`	パラメータを設定する前に、WLANをディセーブルにします。
ステップ 4	**broadcast-ssid** 例： `Device(config-wlan)# broadcast-ssid`	この WLAN の SSID をブロードキャストします。このフィールドは、デフォルトでイネーブルにされています。
ステップ 5	**radio** {**all** | **dot11a** | **dot11ag** | **dot11bg** | **dot11g**} 例： `Device# radio all`	WLANで無線をイネーブルにします。キーワードは次のとおりです。 • **all**：の無線帯域でWLANを設定します。 • **dot1a**：802.11a の無線帯域だけに WLAN を設定します。 • **dot11g**：802.11ag の無線帯域でのみ WLAN を設定します。 • **dot11bg**：802.11b/g の無線帯域でのみWLANを設定します（802.11g が無効の場合、802.11b のみ）。 • **dot11ag**：802.11g の無線帯域だけに無線 LAN を設定します。
ステップ 6	**client vlan** *vlan-identifier* 例： `Device# client vlan test-vlan`	WLANのインターフェイス グループをイネーブルにします。 *vlan-identifier*：VLAN ID を指定します。次に、VLAN 名、VLAN ID、またはVLAN グループ名を指定できます。
ステップ 7	**ip multicast vlan** *vlan-name* 例： `Device(config-wlan)# ip multicast vlan test`	WLANのマルチキャストをイネーブルにします。キーワードは次のとおりです。 • **vlan**：VLAN ID を指定します。 • *vlan-name*：VLAN 名を指定します。

	コマンドまたはアクション	目的
ステップ 8	**media-stream multicast-direct** 例： `Device(config-wlan)# media-stream multicast-direct`	この WLAN でマルチキャスト VLAN をイネーブルにします。
ステップ 9	**call-snoop** 例： `Device(config-wlan)# call-snoop`	コール スヌーピング サポートをイネーブルにします。
ステップ 10	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 11	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。

高度な WLAN プロパティの設定（CLI）

次の高度なプロパティを設定できます。

- AAA オーバーライド
- カバレッジ ホールの検出
- セッション タイムアウト
- Cisco Client Extensions
- 診断チャネル
- インターフェイス オーバーライド ACL
- P2P ブロッキング
- Client Exclusion
- WLAN ごとの最大クライアント数
- オフ チャネル スキャンの延期

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 2	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**aaa-override** 例： `Device(config-wlan)# aaa-override`	AAA オーバーライドをイネーブルにします。
ステップ 4	**chd** 例： `Device(config-wlan)# chd`	この WLAN のカバレッジ ホールの検出をイネーブルにします。このフィールドは、デフォルトでイネーブルにされています。
ステップ 5	**session-timeout** *time-in-seconds* 例： `Device(config-wlan)# session-timeout 450`	セッション タイムアウトを秒単位で設定します。範囲とデフォルト値は、セキュリティ設定によって異なります。WLAN セキュリティが dot1x に設定されている場合、範囲は 300～86400 秒で、デフォルト値は 1800 秒です。他のすべての WLAN セキュリティ設定では、有効範囲は 1～65535 秒であり、デフォルト値は 0 秒です。値 0 は、セッション タイムアウトなしを示します。
ステップ 6	**ccx aironet-iesupport** 例： `Device(config-wlan)# ccx aironet-iesupport`	この WLAN の Aironet IE のサポートをイネーブルにします。このフィールドは、デフォルトでイネーブルにされています。
ステップ 7	**diag-channel** 例： `Device(config-wlan)# diag-channel`	WLAN でクライアントの通信の問題を修復するための診断チャネルのサポートをイネーブルにします。
ステップ 8	**ip access-group** [web] *acl-name* 例： `Device(config)# ip access-group test-acl-name`	WLAN ACL グループを設定します。可変 *acl* 名前はユーザ定義する IPv4 ACL の名前を指定します。キーワード **web** は、IPv4 Web ACL を指定します。
ステップ 9	**peer-blocking** ［**drop** ｜ **forward-upstream**］ 例：	ピアツーピア ブロッキング パラメータを設定します。キーワードは次のとおりです。

	コマンドまたはアクション	目的
	`Device(config)# peer-blocking drop`	• **drop**：ドロップアクションのピアツーピアブロッキングをイネーブルにします。 • **forward-upstream**：アップストリーム転送処理のピアツーピアブロッキングをイネーブルにします。
ステップ 10	**exclusionlist** *time-in-seconds* 例： `Device(config)# exclusionlist 10`	タイムアウトを秒単位で指定します。0 ～ 2147483647 の範囲の値を指定できます。タイムアウトなしでは、0 を入力します。ゼロ（0）タイムアウトは、クライアントが除外リストに追加されたことを示しています。
ステップ 11	**client association limit** *max-number-of-clients* 例： `Device(config)# client association limit 200`	WLAN で設定できる最大クライアント数を設定します。
ステップ 12	**channel-scan defer-priority** {**defer-priority** {**0-7**} | **defer-time** {**0 - 6000**}} 例： `Device(config)# channel-scan defer-priority 6`	チャネル スキャンの延期プライオリティと延期時間を設定します。引数は次のとおりです。 • **defer-priority**：オフチャネル スキャンを延期できるパケットのプライオリティマーキングを指定します。範囲は 0 ～ 7 です。デフォルト値は 3 です。 • **defer-time**：延期時間（ミリ秒単位）。範囲は 0 ～ 6000 です。デフォルトは 100 です。
ステップ 13	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。

高度な WLAN プロパティの設定（GUI）

始める前に

プライマリ コントローラとバックアップ コントローラを設定する前に、AP 参加プロファイルがすでに設定済みであることを確認します。

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[WLANs]** > **[Wireless Networks]** の順に選択します。

ステップ 2 [Wireless Networks] ページで [Add] をクリックします。

ステップ 3 [Advanced] タブで [Coverage Hole Detection] チェック ボックスをオンにします。

ステップ 4 [Aironet IE] チェック ボックスをオンにして、WLAN で Aironet IE を有効にします。

ステップ 5 [Diagnostic Channel] チェック ボックスをオンにして、WLAN で診断チャネルを有効にします。

ステップ 6 ドロップダウンリストから、必要な [P2P Blocking Action] 値を選択します。

ステップ 7 スライダを使用して、[Multicast Buffer] を有効または無効にします。

ステップ 8 [Media Stream Multicast-Direct] チェック ボックスをオンにして、この機能を有効にします。

ステップ 9 [Max Client Connections] セクションで、次のクライアント接続の最大数を指定します。

- WLAN 単位
- Per AP Per WLAN
- Per AP Radio Per WLAN

ステップ 10 [11v BSS Transition Support] セクションで次の設定タスクを実行します。

a) [BSS Transition] チェック ボックスをオンにして、802.11v BSS 移行サポートを有効にします。

b) [Disassociation Imminent] の値を入力します。

c) [Optimized Roaming Disassociation Timer] の値を入力します。

d) チェック ボックスをオンにして以下の項目を有効にします。

- BSS Max Idle Service
- BSS Max Idle Protected
- Disassociation Imminent Service
- Directed Multicast Service
- Universal Admin
- Load Balance
- 帯域選択
- IP ソース ガード

ステップ 11 [WMM Policy] で [Allowed]、[Disabled]、または [Required] を選択します。デフォルトでは、WMM ポリシーが許可されています。

ステップ 12 [Off Channel Scanning Defer] セクションで適切な延期プライオリティ値を選択し、必要なスキャン延期時間の値をミリ秒単位で指定します。

ステップ 13 [Assisted Roaming (11k)] セクションで、次について適切なステータスを選択します。

- Prediction Optimization
- ネイバー リスト
- Dual-Band Neighbor List

ステップ 14 [DTIM Period (in beacon intervals)] セクションで、802.11a/n 無線と 802.11b/g/n 無線の値を指定します。有効な範囲は 1 ～ 255 です。

ステップ 15 [Save & Apply to Device] をクリックします。

WLAN プロパティの監視（CLI）

コマンド	説明
show wlan id *wlan-id*	WLAN ID に基づいて WLAN プロパティを表示します。
show wlan name *wlan-name*	WLAN 名に基づいて WLAN プロパティを表示します。
show wlan all	設定されているすべての WLAN の WLAN プロパティを表示します。
show wlan summary	すべての WLAN の要約を表示します。サマリー詳細には、次の情報が含まれます。 • WLAN ID • プロファイル名 • SSID • VLAN • Status（ステータス）
show running-config wlan *wlan-name*	WLAN の名前に基づいて WLAN の実行コンフィギュレーションを表示します。
show running-config *wlan*	すべての WLAN の実行コンフィギュレーションを表示します。