



## WLAN セキュリティの設定

- [機能情報の確認, 1 ページ](#)
- [レイヤ 2 セキュリティの前提条件, 1 ページ](#)
- [AAA Override について, 2 ページ](#)
- [WLAN セキュリティの設定方法, 3 ページ](#)
- [Additional References, 12 ページ](#)
- [WLAN レイヤ 2 セキュリティに関する機能情報, 13 ページ](#)

### 機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。

### レイヤ 2 セキュリティの前提条件

同じ SSID を持つ WLAN は、ビーコン応答とプローブ応答でアドバタイズされる情報に基づいてクライアントが WLAN を選択できるように、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。使用可能なレイヤ 2 セキュリティ ポリシーは、次のとおりです。

- なし (オープン WLAN)
- Static WEP または 802.1X



(注) Static WEP と 802.1X は両方とも、ビーコン応答とプローブ応答で同じビットによってアドバタイズされるので、クライアントはこれらを区別できません。したがって、同じ SSID を持つ複数の WLAN では、Static WEP と 802.1X の両方を使用できません。

• WPA/WPA2



(注) 同じ SSID を持つ複数の WLAN で WPA と WPA2 を使用することはできませんが、同じ SSID を持つ2つの WLAN は、PSK を使用する WPA/TKIP と 802.1X を使用する Wi-Fi Protected Access (WPA) /Temporal Key Integrity Protocol (WPA) で設定するか、802.1X を使用する WPA/TKIP または 802.1X を使用する WPA/AES で設定することができます。

#### 関連トピック

[静的 WEP および 802.1X レイヤ 2 セキュリティ パラメータの設定 \(CLI\) , \(3 ページ\)](#)

[レイヤ 2 パラメータの設定 \(GUI\) , \(8 ページ\)](#)

[静的 WEP レイヤ 2 セキュリティ パラメータの設定 \(CLI\) , \(4 ページ\)](#)

[レイヤ 2 パラメータの設定 \(GUI\) , \(8 ページ\)](#)

[WPA + WPA2 レイヤ 2 セキュリティ パラメータの設定 \(CLI\) , \(5 ページ\)](#)

[レイヤ 2 パラメータの設定 \(GUI\) , \(8 ページ\)](#)

[802.1X レイヤ 2 セキュリティ パラメータの設定 \(CLI\) , \(7 ページ\)](#)

[レイヤ 2 パラメータの設定 \(GUI\) , \(8 ページ\)](#)

[高度な WLAN プロパティの設定 \(CLI\)](#)

[AAA Override について, \(2 ページ\)](#)

## AAA Override について

WLAN の AAA Override オプションを使用すると、WLAN で Identity ネットワーキングを設定できます。これにより、AAA サーバから返される RADIUS 属性に基づいて、個々のクライアントに VLAN タギング、Quality Of Service (QoS)、およびアクセス コントロール リスト (ACL) を適用することができます。

#### 関連トピック

[高度な WLAN プロパティの設定 \(CLI\)](#)

[レイヤ 2 セキュリティの前提条件, \(1 ページ\)](#)

# WLAN セキュリティの設定方法

## 静的WEPおよび802.1Xレイヤ2セキュリティパラメータの設定 (CLI)

はじめる前に  
管理者特権が必要です。

### 手順の概要

1. **configure terminal**
2. **wlan profile-name**
3. **security static-wep-key {authentication {open | sharedkey} | encryption {104 | 40} [ascii | hex] {0|8}} wep-key wep-key-index1-4**
4. **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例： Switch# <b>configure terminal</b>	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	<b>wlan profile-name</b>  例： Switch# <b>wlan test4</b>	WLAN コンフィギュレーション サブモードを開始します。 <i>profile-name</i> は設定されている WLAN のプロファイル名です。
ステップ 3	<b>security static-wep-key {authentication {open   sharedkey}   encryption {104   40} [ascii   hex] {0 8}} wep-key wep-key-index1-4</b>  例： Switch(config-wlan)# <b>security static-wep-key encryption 40 hex 0 test 2</b>	WLAN の静的 WEP セキュリティを設定します。次のキーワードと引数があります。 <ul style="list-style-type: none"> <li>• <b>authentication</b> : 802.11 認証を設定します。</li> <li>• <b>encryption</b> : 静的 WEP キーとインデックスを設定します。</li> <li>• <b>open</b> : オープン システム認証を設定します。</li> <li>• <b>sharedkey</b> : 共有キー認証を設定します。</li> <li>• <b>104, 40</b> : WEP キーのサイズを指定します。</li> <li>• <b>hex, ascii</b> : キーの入力形式を指定します。</li> <li>• <b>wep-key-index</b>、<b>wep-key-index1-4</b> 指定するパスワードのタイプです。値が 0 である場合は、暗号化されないパスワードを指定することを示します。値が 8 である場合は、AES 暗号化を指定することを示します。</li> </ul>

	コマンドまたはアクション	目的
ステップ 4	<b>end</b>  例： Switch(config)# <b>end</b>	特権 EXEC モードに戻ります。また、 <b>Ctrl+Z</b> 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。

#### 関連トピック

[レイヤ2セキュリティの前提条件, \(1 ページ\)](#)

## 静的 WEP レイヤ2 セキュリティ パラメータの設定 (CLI)

はじめる前に  
管理者特権が必要です。

#### 手順の概要

1. **configure terminal**
2. **wlan profile-name**
3. **security static-wep-key [authentication {open | shared} | encryption {104 | 40} {ascii | hex} [0 | 8]]**
4. **end**

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例： Switch# <b>configure terminal</b>	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	<b>wlan profile-name</b>  例： Switch# <b>wlan test4</b>	WLAN コンフィギュレーション サブモードを開始します。 <i>profile-name</i> は設定されている WLAN のプロファイル名です。
ステップ 3	<b>security static-wep-key [authentication {open   shared}   encryption {104   40} {ascii   hex} [0   8]]</b>  例： Switch(config-wlan)# <b>security static-wep-key authentication open</b>	キーワードは次のとおりです。 <ul style="list-style-type: none"> <li>• <b>static-wep-key</b> : 静的 WEP キーの認証を設定します。</li> <li>• <b>authentication</b> : ユーザが設定できる認証タイプを指定します。値は、open および shared です。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>encryption</b> : ユーザが設定できる暗号化タイプを指定します。有効な値は 104 と 40 です。40 ビットキーには、ASCII テキスト文字が 5 文字と 16 進数文字が 10 文字必要です。104 ビットキーには、ASCII テキスト文字が 13 文字と 16 進数文字が 26 文字必要です。</li> <li>• <b>ascii</b> : ASCII としてキー形式を指定します。</li> <li>• <b>hex</b> : HEX としてキー形式を指定します。</li> </ul>
ステップ 4	<b>end</b>  例 : Switch(config)# <b>end</b>	特権 EXEC モードに戻ります。また、 <b>Ctrl+Z</b> 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。

#### 関連トピック

[レイヤ 2 セキュリティの前提条件, \(1 ページ\)](#)

## WPA + WPA2 レイヤ 2 セキュリティ パラメータの設定 (CLI)



(注) デフォルト セキュリティ ポリシーは、WPA2 です。

#### はじめる前に

管理者特権が必要です。

#### 手順の概要

1. **configure terminal**
2. **wlan profile-name**
3. **security wpa**
4. **security wpa wpa1**
5. **security wpa wpa1 ciphers [aes | tkip]**
6. **security wpa wpa2**
7. **security wpa wpa2 ciphers [aes | tkip]**
8. **end**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例： Switch# <b>configure terminal</b>	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	<b>wlan profile-name</b>  例： Switch# <b>wlan test4</b>	WLAN コンフィギュレーション サブモードを開始します。 <i>profile-name</i> は設定されている WLAN のプロファイル名です。
ステップ 3	<b>security wpa</b>  例： Switch(config-wlan)# <b>security wpa</b>	WPA をイネーブルにします。
ステップ 4	<b>security wpa wpa1</b>  例： Switch(config-wlan)# <b>security wpa wpa1</b>	WPA1 をイネーブルにします。
ステップ 5	<b>security wpa wpa1 ciphers [aes   tkip]</b>  例： Switch(config-wlan)# <b>security wpa wpa1 ciphers aes</b>	WPA1 暗号を指定します。 次のいずれかの暗号化タイプを選択します。  <ul style="list-style-type: none"> <li>• <b>aes</b> : WPA/AES のサポートを指示します。</li> <li>• <b>tkip</b> : WPA/TKIP のサポートを指示します。</li> </ul>
ステップ 6	<b>security wpa wpa2</b>  例： Switch(config-wlan)# <b>security wpa</b>	WPA 2 をイネーブルにします。
ステップ 7	<b>security wpa wpa2 ciphers [aes   tkip]</b>  例： Switch(config-wlan)# <b>security wpa wpa2 ciphers tkip</b>	WPA2 暗号化を設定します。 次のいずれかの暗号化タイプを選択します。  <ul style="list-style-type: none"> <li>• <b>aes</b> : WPA/AES のサポートを指示します。</li> <li>• <b>tkip</b> : WPA/TKIP のサポートを指示します。</li> </ul>
ステップ 8	<b>end</b>  例： Switch(config)# <b>end</b>	特権 EXEC モードに戻ります。 また、 <b>Ctrl+Z</b> 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。

## 関連トピック

[レイヤ 2 セキュリティの前提条件, \(1 ページ\)](#)

## 802.1X レイヤ2 セキュリティ パラメータの設定 (CLI)

はじめる前に  
管理者特権が必要です。

### 手順の概要

1. **configure terminal**
2. **wlan profile-name**
3. **security dot1x**
4. **security [authentication-list auth-list-name | encryption {0 | 104 | 40}**
5. **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例： Switch# <b>configure terminal</b>	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	<b>wlan profile-name</b>  例： Switch# <b>wlan test4</b>	WLAN コンフィギュレーション サブモードを開始します。 <i>profile-name</i> は設定されている WLAN のプロファイル名です。
ステップ 3	<b>security dot1x</b>  例： Switch(config-wlan)# <b>security dot1x</b>	802.1X セキュリティを指定します。
ステップ 4	<b>security [authentication-list auth-list-name   encryption {0   104   40}</b>  例： Switch(config-wlan)# <b>security encryption 104</b>	次のキーワードと引数があります。  <ul style="list-style-type: none"> <li>• <b>authentication-list</b> : IEEE 802.1X の認証リストを指定します。</li> <li>• <b>encryption</b> : CKIP 暗号キーの長さを指定します。有効な値は、0、40、および 104 です。ゼロ (0) では暗号化されません。これはデフォルトです。</li> </ul> <p>(注) WLAN 内のすべてのキーは、同じサイズでなければなりません。</p>
ステップ 5	<b>end</b>  例： Switch(config)# <b>end</b>	特権 EXEC モードに戻ります。また、 <b>Ctrl+Z</b> 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。

## 関連トピック

[レイヤ2セキュリティの前提条件, \(1 ページ\)](#)

## レイヤ2パラメータの設定 (GUI)

## はじめる前に

- 管理者特権が必要です。

**ステップ 1** [Configuration] > [WLAN] > をクリックします。  
[WLANs] ページが表示されます。

**ステップ 2** 設定する WLAN の WLAN プロファイルをクリックします。  
[WLANs] > [Edit] > ページが表示されます。

**ステップ 3** [Security] > [Layer 2] > タブをクリックします。

パラメータ	説明
Layer2 Security	<p>選択した WLAN のレイヤ2セキュリティ。値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• None—No : レイヤ2セキュリティは選択されていません。</li> <li>• WPA+WPA2 : Wi-Fi Protected Access。</li> <li>• 802.1X : WEP 802.1X データ暗号化のタイプ。これらの設定については、レイヤ2 802.1X パラメータに関するトピックを参照してください。</li> <li>• Static WEP : 静的 WEP 暗号化パラメータ。</li> <li>• Static WEP + 802.1x : 静的 WEP および 802.1X の両パラメータ。</li> </ul>
MAC Filtering	<p>MAC アドレス フィルタリング [MAC Filters] &gt; [New page] で、実際の MAC アドレスによってローカルにクライアントを設定できます。そうでない場合は、RADIUS サーバのクライアントを構成します。</p> <p>(注) MAC フィルタは、MAC Authentication By Pass (MAB) として知られています。</p>
Fast Transition	<p>アクセス ポイント間的高速移行をイネーブルまたはディセーブルにするチェックボックス。</p>
Over the DS	<p>分散システム上的高速移行をイネーブルまたはディセーブルにするチェックボックス。</p>



パラメータ	説明
Reassociation Timeout	高速移行の再アソシエーションがタイムアウトになるまでの時間 (秒単位)。

WPA + WPA2 パラメータを設定するには、次の詳細情報を提供します。

パラメータ	説明
WPA Policy	WPA Policy をイネーブルまたはディセーブルにするチェックボックス。
WPA Encryption	WPA2 encryption type: TKIP または AES。WPA ポリシーがイネーブルな場合だけ使用可能です。
WPA2 Policy	WPA2 Policy をイネーブルまたはディセーブルにするチェックボックス。
WPA2 Encryption	WPA2 encryption type: TKIP または AES。WPA2 ポリシーがイネーブルな場合だけ使用可能です。
Authentication Key Management (認証キー管理)	再生成メカニズムパラメータ。値は次のとおりです。 <ul style="list-style-type: none"> <li>• 802.1X</li> <li>• CCKM</li> <li>• PSK</li> <li>• 802.1x + CCKM</li> </ul>
PSK Format	認証キー管理の PSK 値を選択するとイネーブルになります。ASCII 形式または 16 進形式を選択し、事前共有キーを入力します。

802.1x パラメータを設定するには、次の詳細情報を入力します。

パラメータ	説明
802.11 data encryption	WEP 802.11 データ暗号化タイプ。
Type	セキュリティタイプ。

パラメータ	説明
Key size	<p>キー サイズ。 値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• なし</li> <li>• 40 ビット</li> <li>• 104 ビット</li> </ul> <p>サードパーティの AP WLAN (17) は 802.1X 暗号化としてのみ設定できます。 ドロップダウン設定可能な 802.1X パラメータは、この WLAN には使用できません。</p>

静的 WEP を指定するには、次のパラメータを設定します。

パラメータ	説明
802.11 Data Encryption	静的 WEP 暗号化タイプ。
Current Key	現在選択されているキーの詳細を表示します。
Type	セキュリティタイプ。
Key size	<p>キー サイズ。 値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 未設定</li> <li>• 40 ビット</li> <li>• 104 ビット</li> </ul>
Key Index	<p>1~4 のインデックス。</p> <p>各 WLAN に 1 つの一意な WEP キー インデックスを適用できます。 WEP キー インデックスは 4 つしかないため、静的 WEP レイヤ 2 暗号化には 4 つの WLAN しか設定できません。</p> <p>WEP キー インデックスは 4 つしかないため、静的 WEP レイヤ 2 暗号化には 4 つの WLAN しか設定できません。</p>
Encryption Key	暗号化キー。
Key Format	ASCII または 16 進の暗号キー形式を選択します。
Allow Shared Key Authentication	自身がイネーブルまたはディセーブルに設定できる認証キー。

静的 WEP と 802.1X パラメータを設定するには

パラメータ	説明
<b>Static WEP Parameters</b>	
802.11 Data Encryption	静的 WEP 暗号化タイプ。
Current Key	現在選択されているキーの詳細を表示します。
Type	セキュリティタイプ。
Key size	キーサイズ。値は次のとおりです。 <ul style="list-style-type: none"> <li>• 未設定</li> <li>• 40 ビット</li> <li>• 104 ビット</li> </ul>
Key Index	1~4 のインデックス。 各 WLAN に 1 つの一意的な WEP キー インデックスを適用できます。WEP キー インデックスは 4 つしかないため、静的 WEP レイヤ 2 暗号化には 4 つの WLAN しか設定できません。 WEP キー インデックスは 4 つしかないため、静的 WEP レイヤ 2 暗号化には 4 つの WLAN しか設定できません。
Encryption Key	暗号化キー。
Key Format	ASCII または 16 進の暗号キー形式を選択します。
Allow Shared Key Authentication	自身がイネーブルまたはディセーブルに設定できる認証キー。
<b>802.1x Parameters</b>	
802.11 Data Encryption	静的 WEP 暗号化タイプ。
Current Key	表示のみ。現在選択されているキーの詳細。
Type	セキュリティタイプ。
Key size	キーサイズ。値は次のとおりです。 <ul style="list-style-type: none"> <li>• 未設定</li> <li>• 40 ビット</li> <li>• 104 ビット</li> </ul>

パラメータ	説明
Key Index	1~4 のインデックス。 各 WLAN に 1 つの一意な WEP キー インデックスを適用できることに注意してください。WEP キー インデックスは 4 つしかないため、静的 WEP レイヤ 2 暗号化には 4 つの WLAN しか設定できません。
Encryption Key	暗号化キー。
Key Format	ASCII または 16 進の暗号キー形式を選択します。
Allow Shared Key Authentication	自身がイネーブルまたはディセーブルに設定できる認証キー。

ステップ 4 [Apply] をクリックします。

#### 関連トピック

[レイヤ 2 セキュリティの前提条件, \(1 ページ\)](#)

[レイヤ 2 セキュリティの前提条件, \(1 ページ\)](#)

[レイヤ 2 セキュリティの前提条件, \(1 ページ\)](#)

[レイヤ 2 セキュリティの前提条件, \(1 ページ\)](#)

## Additional References

#### Related Documents

Related Topic	Document Title
WLAN command reference	<i>WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3650 スイッチ)</i>
Security configuration guide	<i>Security Configuration Guide (Catalyst 3650 Switches)</i>

**MIBs**

MIB	MIBs Link
本リリースでサポートするすべての MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

**Technical Assistance**

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

## WLAN レイヤ2 セキュリティに関する機能情報

次の表に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

機能名	リリース	機能情報
WLAN のセキュリティ機能	Cisco IOS XE 3.3SE	この機能が導入されました。

