IPv6 WLAN セキュリティの設定

IPv6 WLAN セキュリティの前提条件

クライアント VLAN をスイッチで設定された WLAN にマッピングする必要があります。

IPv6 WLAN セキュリティの制限

RADIUS サーバのサポート

- 冗長性を保つために複数の RADIUS サーバが設定されている場合、バックアップが適切に機能するようにするには、すべてのサーバでユーザ データベースを同一にする必要があります。

Radius ACS サポート

- Cisco Secure Access Control Server（ACS）とスイッチの両方で、RADIUS を設定する必要があります。
- RADIUS は、Cisco Secure ACS バージョン 3.2 以降のリリースでサポートされます。

IPv6 WLAN セキュリティについて

RADIUS の概要

Remote Authentication Dial-In User Service（RADIUS）とは、ネットワークへの管理アクセス権を取得しようとするユーザに対して中央管理されたセキュリティ機能を提供する、クライアント/サーバプロトコルです。これは、ローカルEAPに類似したバックエンドデータベースとして機能し、認証サービスおよびアカウンティング サービスを提供します。

- 認証：スイッチにログインしようとするユーザを検証するプロセス。

  スイッチで RADIUS サーバに対してユーザが認証されるようにするには、ユーザは有効なユーザ名とパスワードを入力する必要があります。複数のデータベースを設定する場合は、バックエンド データベースを試行する順序を指定します。

- アカウンティング：ユーザによる処理と変更を記録するプロセス。

  ユーザによる処理が正常に実行される度に、RADIUSアカウンティング サーバでは、変更された属性、変更を行ったユーザのユーザ ID、ユーザがログインしたリモート ホスト、コマンドが実行された日付と時刻、ユーザの認可レベル、および実行された処理と入力された値の説明がログに記録されます。RADIUSアカウンティング サーバが到達不能の場合、ユーザは中断なく、セッションを続行できます。

ユーザ データグラム プロトコル：RADIUS では、その転送にユーザ データグラム プロトコル（UDP）を使用します。RADIUS では、1 つのデータベースが保持されます。そして、UDP ポート 1812 で受信認証要求がリッスンされ、UDP ポート 1813 で受信アカウンティング要求がリッスンされます。アクセス コントロールを要求するスイッチは、クライアントとして動作し、サーバからAAAサービスを要求します。スイッチとサーバ間のトラフィックは、プロトコルで定義されるアルゴリズムと、両方のデバイスにおいて設定される共有秘密キーによって暗号化されます。

複数の RADIUS アカウンティングおよび認証サーバを設定します。たとえば、1 台の RADIUS 認証サーバを中央に配置し、複数の RADIUS アカウンティング サーバを異なる地域に配置できます。同じタイプのサーバを複数設定すると、最初のサーバで障害が発生したり、接続不能になったりしても、コントローラは、必要に応じて 2 台目や 3 台目あるいはそれ以降のサーバへの接続を自動的に試行します。

RADIUS 方式が WLAN に対して設定されている場合、スイッチは WLAN に対して設定されている RADIUS 方式を使用します。ローカル EAP を使用するように WLAN を設定すると、WLAN で設定されているRADIUS方式はローカルをポイントします。WLANには、使用するローカルEAPプロファイルの名前を設定する必要もあります。

RADIUS 方式が WLAN に対して設定されていない場合、スイッチはグローバル モードで定義されているデフォルトの RADIUS 方式を使用します。

ローカル EAP について

ローカルEAPは、ユーザおよびワイヤレス クライアントのローカル認証を可能にする認証方式です。この方式は、バックエンド システムが妨害されたり、外部認証サーバが停止した場合でも、ワイヤレス クライアントへの接続を維持できるように、リモート オフィスで使用する目的で設計

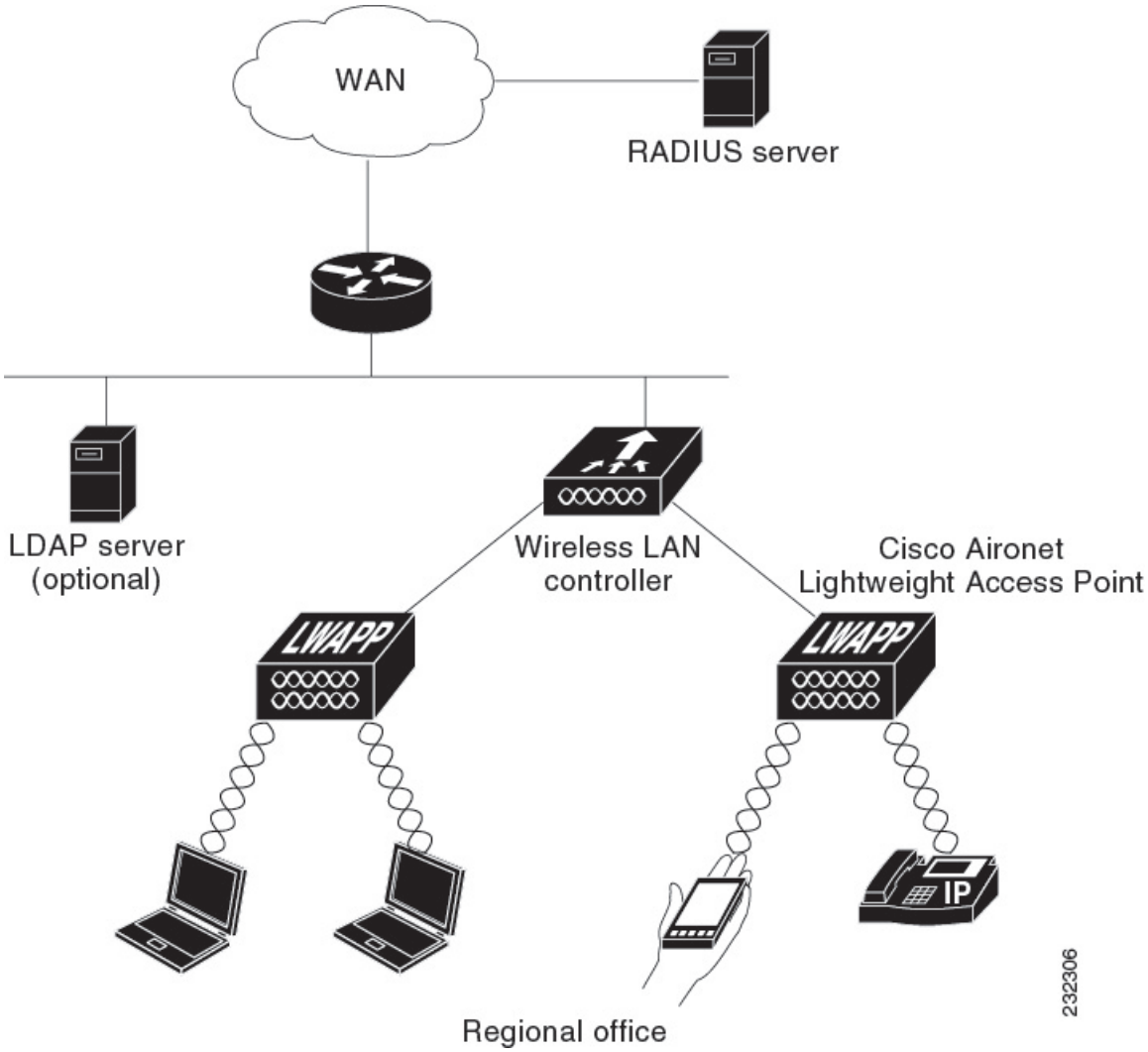
されています。ローカルEAPを有効にすると、スイッチは認証サーバおよびローカルユーザデータベースとして機能するため、外部認証サーバに依存する必要がなくなります。ローカル EAP は、ローカル ユーザ データベースまたは LDAP バックエンド データベースからユーザのクレデンシャルを取得して、ユーザを認証します。ローカルEAPでは、コントローラとワイヤレスクライアント間で、LEAP、EAP-FAST、EAP-TLS、PEAPv0/MSCHAPv2、および PEAPv1/GTC 認証方式をサポートします。

EAPプロファイル名なしで実施される、または存在しない名前のEAPプロファイルが実施される場合、EAP はデフォルトでローカル認証用の EAP 方式を割り当てません。

（注） LDAPバックエンドデータベースでは、ローカルEAP方式として、EAP-TLS、EAP-FAST/GTC、および PEAPv1/GTC がサポートされます。LEAP、EAP-FAST/MSCHAPv2、および PEAPv0。MSCHAPv2は平文のパスワードを返すようにLDAPサーバが設定されている場合にのみサポートされます。

（注） スイッチは、Microsoft Active Directory や Novell の eDirectory などの外部 LDAP データベースに対するローカルEAP認証をサポートしています。Novell の eDirectory に対するローカルEAP認証用にコントローラを設定する方法の詳細については、『Configure Unified Wireless Network for Authentication Against Novell's eDirectory Database』ホワイトペーパーを参照してください。

図 *1*：ローカル *EAP* の例



関連トピック

ローカル ユーザの作成, （5 ページ）
クライアント VLAN とインターフェイスの作成, （6 ページ）
EAP プロファイルの設定, （7 ページ）
クライアント VLAN の作成, （21 ページ）
外部 RADIUS サーバを使用した 802.1x WLAN の作成, （22 ページ）

IPv6 WLAN セキュリティの設定方法

ローカル認証の設定

ローカル ユーザの作成

手順の概要

1. **configure terminal**
2. **username** aaa_test
3. **password 0** aaa_test
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	**configure terminal** 例： `Switch# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**username** aaa_test 例： `Switch(config)# username aaa_test`	ユーザ名を作成します。
ステップ 3	**password 0** aaa_test 例： `Switch(config)# username aaa_test password 0 aaa_test`	ユーザ名のパスワードを割り当てます。
ステップ 4	**end** 例： `Switch(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。

```
Switch# configure terminal
Switch(config)# username aaa_test password 0 aaa_test
Switch(config)# end
```

関連トピック

IPv6 WLAN セキュリティについて，（2 ページ）

クライアント VLAN とインターフェイスの作成

手順の概要

1. **configure terminal**
2. **vlan**
3. **exit**
4. **interface vlan** vlan_ID
5. **ip address**
6. **ipv6 address**
7. **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	**configure terminal** 例： `Switch# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**vlan** 例： `Switch(config)# vlan 137`	VLAN を作成します。
ステップ 3	**exit** 例： `Switch (config-vlan)# exit`	VLAN コンフィギュレーション モードを終了します。
ステップ 4	**interface vlan** vlan_ID 例： `Switch (config)# interface vlan 137`	インターフェイスに VLAN を関連付けます。
ステップ 5	**ip address** 例： `Switch(config-if)# ip address 10.7.137.10 255.255.255.0`	VLAN インターフェイスに IP アドレスを割り当てます。
ステップ 6	**ipv6 address** 例： `Switch(config-if)#ipv6 address 2001:db8::20:1/64`	VLAN インターフェイスに IPv6 アドレスを割り当てます。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Switch(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。

```
Switch# configure terminal
Switch(config)# vlan 137
Switch(config-vlan)#exit
Switch(config)#interface vlan 137
Switch(config-if)#ip address 10.7.137.10 255.255.255.0
Switch(config-if)#ipv6 address 2001:db8::20:1/64
Switch(config-if)#end
```

関連トピック

IPv6 WLAN セキュリティについて，（2 ページ）

EAP プロファイルの設定

手順の概要

1. **eap profile** name
2. **method leap**
3. **method tls**
4. **method peap**
5. **method fast**
6. **method mschapv2**
7. **method md5**
8. **method gtc**
9. **method fast profile** my-fast
10. **description** my_local**eap profile**
11. **exit**
12. **eap method fast profile**myFast
13. **authority-id** [identity|information]
14. **local-key 0** key-name
15. **pac-password 0** password
16. **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	**eap profile** name 例： `Switch(config)# eap profile wcm_eap_prof`	EAP プロファイルを作成します。
ステップ 2	**method leap** 例： `Switch(config-eap-profile)# method leap`	プロファイルで EAP-LEAP 方式を設定します。
ステップ 3	**method tls** 例： `Switch(config-eap-profile)# method tls`	プロファイルで EAP-TLS 方式を設定します。
ステップ 4	**method peap** 例： `Switch(config-eap-profile)# method peap`	プロファイルで PEAP 方式を設定します。
ステップ 5	**method fast** 例： `Switch(config-eap-profile)# method fast`	プロファイルで EAP-FAST 方式を設定します。
ステップ 6	**method mschapv2** 例： `Switch(config-eap-profile)# method mschapv2`	プロファイルで EAP-MSCHAPV2 方式を設定します。
ステップ 7	**method md5** 例： `Switch(config-eap-profile)# method md5`	プロファイルで EAP-MD5 方式を設定します。
ステップ 8	**method gtc** 例： `Switch(config-eap-profile)# method gtc`	プロファイルで EAP-GTC 方式を設定します。

ステップ 9	**method fast profile** my-fast
	
	例：
	`Switch(config-eap-profile)# eap method fast profile my-fast`
	`Switch (config-eap-profile)#description my_local eap profile`
		my-fast という EAP プロファイルを作成します。

	コマンドまたはアクション	目的
ステップ 10	**description** my_local**eap profile** 例： `Switch (config-eap-profile)#description my_local eap profile`	ローカルプロファイルの説明を指定します。
ステップ 11	**exit** 例： `Switch (config-eap-profile)# exit`	eap プロファイル コンフィギュレーション モードを終了します。
ステップ 12	**eap method fast profile**myFast 例： `Switch (config)# eap method fast profile myFast`	EAP 方式プロファイルを設定します。

ステップ 13	**authority-id** [identity|information]
	
	例：
	`Switch(config-eap-method-profile)# authority-id identity my_identity`
	`Switch(config-eap-method-profile)#authority-id information my_information`
		EAP 方式プロファイルの認証局 ID および情報を設定します。

ステップ 14	**local-key 0** key-name 例： `Switch(config-eap-method-profile)# local-key 0 test`	ローカル サーバ キーを設定します。
ステップ 15	**pac-password 0** password 例： `Switch(config-eap-method-profile)# pac-password 0 test`	手動の PAC プロビジョニング用の PAC パスワードを設定します。
ステップ 16	**end** 例： `Switch(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。

```
Switch(config)#eap profile wcm_eap_prof
Switch(config-eap-profile)#method leap
Switch(config-eap-profile)#method tls
Switch(config-eap-profile)#method peap
Switch(config-eap-profile)#method mschapv2
Switch(config-eap-profile)#method md5
Switch(config-eap-profile)#method gtc
Switch(config-eap-profile)#eap method fast profile my-fast
Switch (config-eap-profile)#description my_local eap profile
Switch(config-eap-profile)# exit
Switch (config)# eap method fast profile myFast
Switch(config-eap-method-profile)#authority-id identity my_identity
Switch(config-eap-method-profile)#authority-id information my_information
Switch(config-eap-method-profile)#local-key 0 test
```

```
Switch(config-eap-method-profile)#pac-password 0 test
Switch(config-eap-method-profile)# end
```

関連トピック

IPv6 WLAN セキュリティについて，（2 ページ）

ローカル認証モデルの作成

手順の概要

1. **aaa** 新しいモデル
2. **authentication dot1x default local**
3. **dot1x** 方式リスト **local**
4. **aaa authentication dot1x** dot1x_ 名 **local**
5. **aaa authorization credential-download** name **local**
6. **aaa local authentication** auth-name **authorization** authorization-name
7. **session ID**
8. **dot1x system-auth-control**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**aaa** 新しいモデル 例： `Switch(config)# aaa new-model`	AAA 認証モデルを作成します。
ステップ 2	**authentication dot1x default local** 例： `Switch(config)# aaa authentication dot1x default local`	他の方法が見つからない場合、dot1x でデフォルトのローカル RADIUS を使用する必要があることを意味します。
ステップ 3	**dot1x** 方式リスト **local** 例： `Switch(config)# aaa authentication dot1x wcm_local local`	wcm_local 方式リスト用のローカル認証を割り当てます。
ステップ 4	**aaa authentication dot1x** dot1x_ 名 **local** 例： `Switch(config)# aaa authentication dot1x aaa_auth local`	dot1x 方式用のローカル認証を設定します。

	コマンドまたはアクション	目的
ステップ 5	**aaa authorization credential-download** name **local** 例： `Switch(config)# aaa authorization credential-download wcm_author local`	Local/RADIUS/LDAP から EAP クレデンシャルをダウンロードするようにローカル データベースを設定します。
ステップ 6	**aaa local authentication** auth-name **authorization** authorization-name 例： `Switch(config)# aaa local authentication wcm_local authorization wcm_author`	ローカル認証および許可を選択します。
ステップ 7	**session ID** 例： `Switch(config)# aaa session-id common`	AAA のセッション ID を設定します。
ステップ 8	**dot1x system-auth-control** 例： `Switch(config)# dot1x system-auth-control`	dot.1x システム認証制御をイネーブルにします。

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default local
Switch(config)# aaa authentication dot1x wcm-local local
Switch(config)# aaa authentication dot1x aaa_auth local
Switch(config)# aaa authorization credential-download wcm_author local
Switch(config)# aaa local authentication wcm_local authorization wcm_author
Switch(config)# aaa session-id common
Switch(config)# dot1x system-auth-control
```

クライアント WLAN の作成

（注） この例では、ダイナミック WEP の 802.1x を使用しています。ワイヤレス クライアントでサポートされ、スイッチで設定可能な他の任意のセキュリティ メカニズムも使用できます。

手順の概要

1. **configure terminal**
2. **wlan** wlan name **<identifier>** SSID
3. **broadcast-ssid**
4. **no security wpa**
5. **security dot1x**
6. **security** dot1x authentication-list *wcm-local*
7. **local-auth** wcm_eap_prof
8. **client vlan** *137*
9. **no shutdown**
10. **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	**configure terminal** 例： `Switch# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**wlan** wlan name **<identifier>** SSID 例： `Switch(config)# wlan wlanProfileName 1 ngwcSSID`	WLAN を作成します。
ステップ 3	**broadcast-ssid** 例： `Switch(config-wlan)# broadcast-ssid`	WLAN で SSID をブロードキャストするように設定します。
ステップ 4	**no security wpa** 例： `Switch(config-wlan)# no security wpa`	WLAN の wpa をディセーブルにして、802.1x をイネーブルにします。
ステップ 5	**security dot1x** 例： `Switch(config-wlan)# security dot1x`	WLAN の 802.1x 暗号化セキュリティを設定します。
ステップ 6	**security** dot1x authentication-list *wcm-local* 例： `Switch(config-wlan)# security dot1x authentication-list wcm-local`	dot1x 認証用に WLAN へのサーバ グループ マッピングを設定します。

	コマンドまたはアクション	目的
ステップ 7	**local-auth** wcm_eap_prof 例： `Switch (config-wlan)# local-auth wcm_eap_profile`	ローカル認証用に WLAN に eap プロファイルを設定します。
ステップ 8	**client vlan** *137* 例： `Switch(config-wlan)# client vlan 137`	WLAN に VLAN を関連付けます。
ステップ 9	**no shutdown** 例： `Switch(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 10	**end** 例： `Switch(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。

```
Switch# config terminal
Switch(config)#wlan wlanProfileName 1 ngwcSSID
Switch(config-wlan)#broadcast-ssid
Switch(config-wlan)#no security wpa
Switch(config-wlan)#security dot1x
Switch(config-wlan)#security dot1x authentication-list wcm-local
Switch (config-wlan)# local-auth wcm_eap_prof
Switch(config-wlan)#client vlan 137
Switch(config-wlan)#no shutdown
Switch(config-wlan)#end
Switch#
```

関連トピック

WPA2+AES 用クライアント VLAN の作成, （15 ページ）

WPA2+AES でのローカル認証の設定

手順の概要

1. **configure terminal**
2. **aaa** 新しいモデル
3. **dot1x system-auth-control**
4. **aaa authentication dot1x default local**
5. **aaa local authorization credential-download default local**
6. **aaa local authentication default authorization default**
7. **eap profile** wcm_eap_プロファイル
8. **method leap**
9. **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	**configure terminal** 例： `Switch# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**aaa** 新しいモデル 例： `Switch(config)# aaa new-model`	AAA 認証モデルを作成します。
ステップ 3	**dot1x system-auth-control** 例： `Switch(config)# dot1x system-auth-control`	dot1x システム認証制御をイネーブルにします。
ステップ 4	**aaa authentication dot1x default local** 例： `Switch(config)# aaa authentication dot1x default local`	デフォルト dot1x 方式用のローカル認証を設定します。
ステップ 5	**aaa local authorization credential-download default local** 例： `Switch(config)# aaa authorization credential-download default local`	ローカル サーバから EAP クレデンシャルをダウンロードするようにデフォルト データベースを設定します。

	コマンドまたはアクション	目的
ステップ 6	**aaa local authentication default authorization default** 例： `Switch(config)# aaa local authentication default authorization default`	デフォルトのローカル認証および許可を選択します。
ステップ 7	**eap profile** wcm_eap_プロファイル 例： `Switch(config)#eap profile wcm_eap_profile`	EAP プロファイルを作成します。
ステップ 8	**method leap** 例： `Switch(config)# method leap`	プロファイルで EAP-LEAP 方式を設定します。
ステップ 9	**end** 例： `Switch(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。

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# dot1x system-auth-control
Switch(config)# aaa authentication dot1x default local
Switch(config)# aaa authorization credential-download default local
Switch(config)# aaa local authentication default authorization default
Switch(config)#eap profile wcm_eap_profile
Switch(config)# method leap
Switch(config)# end
```

WPA2+AES 用クライアント VLAN の作成

ローカル認証の WPA2+AES タイプの VLAN を作成します。この VLAN は、後で WLAN にマッピングされます。

手順の概要

1. **configure terminal**
2. **vlan** vlan_ID
3. **exit**
4. **interface** vlan vlan_ID
5. **ip address**
6. **ipv6 address**
7. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**vlan** vlan_ID 例： `Switch (config)# vlan 105`	VLAN を作成します。
ステップ 3	**exit** 例： `Switch (config-vlan)# exit`	VLAN モードを終了します。
ステップ 4	**interface** vlan vlan_ID 例： `Switch(config)# interface vlan 105`	インターフェイスに VLAN を関連付けます。
ステップ 5	**ip address** 例： `Switch(config-if)# ip address 10.8.105.10 255.255.255.0`	VLAN インターフェイスに IP アドレスを割り当てます。
ステップ 6	**ipv6 address** 例： `Switch(config-if)#ipv6 address 2001:db8::10:1/64`	VLAN インターフェイスに IPv6 アドレスを割り当てます。
ステップ 7	**exit** 例： `Switch (config-if)# exit`	インターフェイス モードを終了します。

```
Switch# configure terminal
Switch(config)# vlan105
Switch (config-vlan)# exit
Switch (config)# interface vlan 105
Switch(config-if)#ip address 10.8.105.10 255.255.255.0
Switch(config-if)#ipv6 address 2001:db8::10:1/64
Switch(config-if)#exit
Switch(config)#
```

関連トピック

クライアント WLAN の作成, （11 ページ）

WPA2+AES 用 WLAN の作成

WLAN を作成し、WPA2+AES 用に作成されたクライアント VLAN にマッピングします。

手順の概要

1. **configure terminal**
2. **wlan** wpas2-aes-wlan 1 wpas2-aes-wlan
3. **client vlan** 105
4. **local-auth** wcm_eap_プロファイル
5. **security dot1x authentication-list default**
6. **no shutdown**
7. **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	**configure terminal** 例： `Switch# configure terminal`	グローバル コマンド モードを開始します。

ステップ 2	**wlan** wpas2-aes-wlan 1 wpas2-aes-wlan
	
	例：
	`Switch(config)#wlan wpa2-aes-wlan 1 wpa2-aes-wlan`
	`Switch(config-wlan)#`
		WLAN を作成します。

ステップ 3	**client vlan** 105
	
	例：
	`Switch(config-wlan)#client vlan 105`
	`Switch(config-wlan)#`
		クライアント VLAN に WLAN をマッピングします。

ステップ 4	**local-auth** wcm_eap_プロファイル 例： `Switch(config-wlan)#local-auth wcm_eap_profile`	WLAN に EAP プロファイルを作成し、設定します。
ステップ 5	**security dot1x authentication-list default** 例： `Switch(config-wlan)#security dot1x authentication-list default`	デフォルトの dot1x 認証リストを使用します。

ステップ 6	**no shutdown**
	
	例：
	`Switch(config-wlan)#no shutdown`
	`Switch(config-wlan)#`
		WLAN をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Switch(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。

```
Switch# configure terminal
Switch(config)#wlan wpa2-aes-wlan 1 wpa2-aes-wlan
Switch(config-wlan)#client vlan 105
Switch(config-wlan)#local-auth wcm_eap_profile
Switch(config-wlan)#security dot1x authentication-list default
Switch(config-wlan)#no shutdown
Switch(config-wlan)# exit
```

外部 RADIUS サーバの設定

RADIUS 認証サーバ ホストの設定

手順の概要

1. **configure terminal**
2. **radius server One**
3. **address ipv4** address **auth-port**auth_port_number **acct-port** acct_port_number
4. **address ipv6** address **auth-port**auth_port_number **acct-port** acct_port_number
5. **key** 0cisco
6.

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**radius server One** 例： `Switch (config)# radius server One`	RADIUS サーバを作成します。

	コマンドまたはアクション	目的
ステップ 3	**address ipv4** address **auth-port**auth_port_number **acct-port** acct_port_number 例： `Switch (config-radius-server)# address ipv4 10.10.10.10 auth-port 1812 acct-port 1813`	RADIUS サーバの IPv4 アドレスを設定します。
ステップ 4	**address ipv6** address **auth-port**auth_port_number **acct-port** acct_port_number 例： `Switch (config-radius-server)# address ipv6 2001:db8::25:2 auth-port 1812 acct-port 1813`	RADIUS サーバの IPv6 アドレスを設定します。
ステップ 5	**key** 0cisco 例： `Switch (config-radius-server)# key 0 cisco`	**exit**
ステップ 6	例： `Switch (config-radius-server)# exit`	RADIUS サーバモードを終了します。

```
Switch# configure terminal
Switch (config)# radius server One
Switch (config-radius-server)# address ipv4 10.10.10.10 auth-port 1812 acct-port 1813
Switch (config-radius-server)# address ipv6 2001:db8::25:2 auth-port 1812 acct-port 1813
Switch (config-radius-server)# key 0 cisco
Switch (config-radius-server)#exit
```

関連トピック

RADIUS 認証サーバ グループの設定, （19 ページ）

RADIUS 認証サーバ グループの設定

手順の概要

1. **configure terminal**
2. **aaa new-model**
3. **aaa group server radius** wcm_rad
4. **server** <ip address>**auth-port**1812**acct-port**1813
5. **aaa authentication dot1x** method_list **group** wcm_rad
6. **dot1x system-auth-control**
7. **aaa session-idcommon**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**aaa new-model** 例： `Switch(config)#aaa new-model`	AAA 認証モデルを作成します。

ステップ 3	**aaa group server radius** wcm_rad
	
	例：
	`Switch(config)# aaa group server radius wcm_rad`
	`Switch(config-sg-radius)#`
		RADIUS サーバ グループを作成します。

ステップ 4	**server** <ip address>**auth-port**1812**acct-port**1813
	
	例：
	`Switch(config-sg-radius)# server One auth-port 1812 acct-port 1813`
	`Switch(config-sg-radius)# server Two auth-port 1812 acct-port 1813`
	`Switch(config-sg-radius)# server Three auth-port 1812 acct-port 1813`
		ステップ 3 で作成した RADIUS グループにサーバを追加します。RADIUS アカウンティング サーバおよび認証サーバの UDP ポートを設定します。

ステップ 5	**aaa authentication dot1x** method_list **group** wcm_rad 例： `Switch(config)# aaa authentication dot1x method_list group wcm_rad`	RADIUS グループに方式リストをマッピングします。
ステップ 6	**dot1x system-auth-control** 例： `Switch(config)# dot1x system-auth-control`	RADIUS グループのシステム認証制御をイネーブルにします。
ステップ 7	**aaa session-idcommon** 例： `Switch(config)# aaa session-id common`	RADIUS グループから、特定のコールに対して送信されるすべてのセッション ID 情報が同じであることを確認します。

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa group server radius wcm_rad
Switch(config-sg-radius)# server One auth-port 1812 acct-port 1813
Switch(config-sg-radius)# server Two auth-port 1812 acct-port 1813
Switch(config-sg-radius)# server Three auth-port 1812 acct-port 1813
Switch(config)# aaa authentication dot1x method_list group wcm_rad
Switch(config)# dot1x system-auth-control
Switch(config)# aaa session-id common
Switch(config)#
```

関連トピック

RADIUS 認証サーバ ホストの設定, （18 ページ）

クライアント VLAN の作成

手順の概要

1. **configure terminal**
2. **vlan** 137
3. **exit**
4. **interface vlan** 137
5. **ip address** 10.7.137.10 255.255.255.0
6. **ipv6 address** 2001:db8::30:1/64
7. **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	**configure terminal** 例： `Switch# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**vlan** 137 例： `Switch(config)# vlan 137`	VLAN を作成してインターフェイスに関連付けます。
ステップ 3	**exit** 例： `Switch (config-vlan)# exit`	VLAN モードを終了します。
ステップ 4	**interface vlan** 137 例： `Switch (config)# interface vlan 137`	インターフェイスに VLAN を割り当てます。
ステップ 5	**ip address** 10.7.137.10 255.255.255.0 例： `Switch(config-if)# ip address 10.7.137.10 255.255.255.0`	VLANインターフェイスにIPv4アドレスを割り当てます。

	コマンドまたはアクション	目的
ステップ 6	**ipv6 address** 2001:db8::30:1/64 例： `Switch(config-if)# ipv6 address 2001:db8::30:1/64`	VLANインターフェイスにIPv6アドレスを割り当てます。
ステップ 7	**end** 例： `Switch(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。

```
Switch# configure terminal
Switch(config)# vlan137
Switch(config-vlan)# exit
Switch(config)# interface vlan137
Switch(config-if)# ip address 10.7.137.10 255.255.255.0
Switch(config-if)# ipv6 address 2001:db8::30:1/64
Switch(config-if)# end
```

関連トピック

IPv6 WLAN セキュリティについて, （2 ページ）
外部 RADIUS サーバを使用した 802.1x WLAN の作成, （22 ページ）

外部 RADIUS サーバを使用した 802.1x WLAN の作成

手順の概要

1. **configure terminal**
2. **wlan** ngwc-1x**<ssid>**ngwc-1x
3. **broadcast-ssid**
4. **no security wpa**
5. **security dot1x**
6. **security dot1x authentication-list** wcm-rad
7. **client vlan** 137
8. **no shutdown**
9. **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	**configure terminal** 例： `Switch# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**wlan** ngwc-1x**<ssid>**ngwc-1x 例： `Switch(config)# wlan ngwc_8021x 2 ngwc_8021x`	802.1x 認証用の新しい WLAN を作成します。
ステップ 3	**broadcast-ssid** 例： `Switch(config-wlan)# broadcast-ssid`	WLAN で SSID をブロードキャストするように設定します。
ステップ 4	**no security wpa** 例： `Switch(config-wlan)# no security wpa`	WLAN の WPA をディセーブルにして、802.1x をイネーブルにします。
ステップ 5	**security dot1x** 例： `Switch(config-wlan)# security dot1x`	WLAN の 802.1x 暗号化セキュリティを設定します。
ステップ 6	**security dot1x authentication-list** wcm-rad 例： `Switch(config-wlan)# security dot1x authentication-list wcm-rad`	dot1x 認証用に WLAN へのサーバ グループ マッピングを設定します。
ステップ 7	**client vlan** 137 例： `Switch(config-wlan)# client vlan 137`	WLAN に VLAN を関連付けます。
ステップ 8	**no shutdown** 例： `Switch(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 9	**end** 例： `Switch(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。

```
Switch# configure terminal
Switch(config)#wlan ngwc_8021x 2 ngwc_8021x
Switch(config-wlan)# broadcast-ssid
```

```
Switch(config-wlan)# no security wpa
Switch(config-wlan)# security dot1x
Switch(config-wlan)# security dot1x authentication-list wcm-rad
Switch(config-wlan)# client vlan 137
Switch(config-wlan)# no shutdown
Switch(config-wlan)# end
```

関連トピック

クライアント VLAN の作成，（21 ページ）
IPv6 WLAN セキュリティについて，（2 ページ）

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 コマンド リファレンス	*IPv6 Command Reference (Catalyst 3850 Switches)IPv6 Command Reference (Cisco WLC 5700 Series)*
WLAN コマンド リファレンス	*WLAN Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
WLAN の設定	*WLAN Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)WLAN Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IPv6 WLAN セキュリティの機能情報

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

機能	リリース	変更内容
IPv6 WLAN セキュリティ機能	Cisco IOS XE 3.2SE	この機能が導入されました。