WEP と WEP 機能の設定

この章では、Wired Equivalent Privacy（WEP）、Message Integrity Check（MIC）、および Temporal Key Integrity Protocol（TKIP）を設定する方法を説明します。この章の内容は、次のとおりです。

- WEP の概要（P.9-2）
- 暗号スイートと WEP の設定（P.9-3）

WEP の概要

無線局範囲内の誰もが局の周波数にチューニングして信号を聞くことができるのと同じように、ブリッジの範囲内にあるすべての無線ネットワーキング デバイスがブリッジの無線伝送を受信できます。WEP は、不正侵入者に対する第一の防衛ラインであるため、シスコでは、無線ネットワークに完全な暗号化を使用することを推奨しています。

WEP 暗号化は、ブリッジ間の無線通信にスクランブルをかけ、通信のプライバシーを保護します。ブリッジとの通信では、同じ WEP キーを使用して、無線信号の暗号化および復号化を行います。WEP キーは、ユニキャストおよびマルチキャストの両方のメッセージを暗号化します。ユニキャスト メッセージは、ネットワーク上の 1 つのデバイスだけに送信されます。マルチキャスト メッセージは、ネットワーク上の複数のデバイスに送信されます。

Extensible Authentication Protocol（EAP）認証は、無線デバイスに動的な WEP キーを提供します。動的な WEP キーは、静的な、つまり変化のない WEP キーより安全性が高くなります。不正侵入者は、同じ WEP キーで暗号化されたパケットが多数送られてくるのを待つだけで、WEP キーを割り出す計算を実行し、そのキーを使ってネットワークに侵入できます。動的な WEP キーは頻繁に変化するため、不正侵入者は計算を実行してキーを割り出すことができなくなります。EAP とその他の認証タイプの詳細は、第 10 章「認証タイプの設定」を参照してください。

暗号スイートは、無線 LAN 上の無線通信を保護するように設計された暗号と完全性アルゴリズムのセットです。Wi-Fi Protected Acccess（WPA）または Cisco Centralized Key Management（CCKM）を有効にするには、暗号スイートを使用する必要があります。暗号スイートは認証済みキー管理の使用を許可しながら WEP の保護を行うため、CLI で **encryption mode cipher** コマンドを使用するか、Web ブラウザ インターフェイスの暗号化ドロップダウン メニューを使用して WEP を有効にすることをお勧めします。TKIP を含む暗号スイートは、無線 LAN に最適なセキュリティを提供しますが、WEP だけを含む暗号スイートは、安全性が最も劣ります。

無線 LAN 上のデータ トラフィックは、次のセキュリティ機能によって保護されます。

- WEP（Wired Equivalent Privacy）: WEP は 802.11 標準暗号アルゴリズムで、もともとは無線 LAN を有線 LAN で利用可能なプライバシーと同じ水準で提供するように設計されています。しかし、基本の WEP 構造には不備な点があり、侵入者はそれほど苦労することなく機密性を侵害できます。
- TKIP（Temporal Key Integrity Protocol）: TKIP は、WEP を実行するために構築された従来のハードウェアで利用可能な最善のセキュリティを達成するように設計された WEP 周辺の一組のアルゴリズムです。TKIP は WEP に対して、次の 4 つの点を改善しています。
  - weak-key（脆弱鍵）攻撃を阻止するための、パケットごとの暗号キー混合機能
  - リプレイ攻撃を検知するための、新しい IV キー作成ロジック
  - パケットの送信元と宛先の入れ替え（ビット フリップ攻撃）や変更のような偽造を検出するための *Michael* と呼ばれる暗号メッセージ完全性チェック（MIC）
  - キー更新の必要性をなくすための IV 長の拡張
- CKIP（Cisco Key Integrity Protocol）: IEEE 802.11i セキュリティ タスク グループによって提供された初期アルゴリズムに基づく、シスコの WEP キー置換技術です。
- CMIC（Cisco Message Integrity Check）: TKIP の *Michael* と同様、シスコのメッセージ完全性チェック メカニズムは、偽造攻撃を検出するように設計されています。

（注）　VLAN をブリッジで有効にした場合、WEP、MIC、および TKIP がサポートされるのはネイティブ VLAN 上だけです。

暗号スイートと WEP の設定

次の項では、暗号スイート、WEP、および MIC や TKIP などの WEP 追加機能の設定方法を説明します。

- WEP キーの作成（P.9-3）
- 暗号スイートと WEP の有効化（P.9-5）

WEP、TKIP、および MIC は、デフォルトでは無効になっています。

WEP キーの作成

イネーブル EXEC モードから、次の手順に従って、WEP キーを作成し、キーのプロパティを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル設定モードを開始します。
ステップ 2	**interface dot11radio 0**	無線インターフェイスのインターフェイス設定モードを開始します。
ステップ 3	**encryption** [**vlan** *vlan-id*] **key** *1-4* **size** { **40** | **128** } *encryption-key* [**transmit-key**]	WEP キーを作成し、そのプロパティを設定します。 • （オプション）キーを作成する VLAN を選択します。WEP、MIC、および TKIP がサポートされるのは、ネイティブ VLAN 上だけです。 • この WEP キーを配置するキー スロットの名前を指定します。各 VLAN に WEP キーを 4 つまで割り当てることができますが、キー スロット 4 はセッション キー用に予約されています。 • キーを入力し、キーのサイズを 40 ビットか 128 ビットのいずれかに設定します。40 ビット キーには、10 の 16 進数が含まれ、128 ビット キーには、26 の 16 進数が含まれています。 • （オプション）このキーを送信キーとして設定します。スロット 2 のキーは、デフォルトで送信キーとなります。MIC と共に WEP を有効にする場合は、ルート ブリッジと非ルート ブリッジの両方で、同じ WEP キーを同じキー スロットの送信キーとして使用します。
ステップ 4	**end**	イネーブル EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

次の例は、VLAN 1 のスロット 2 に 128 ビット WEP キーを作成し、そのキーを送信キーとして設定する方法を示します。

```
bridge# configure terminal
bridge(config)# configure interface dot11radio 0
bridge(config-if)# encryption vlan 1 key 2 size 128 12345678901234567890123456
transmit-key
bridge(config-if)# end
```

WEP キーの制限

表 9-1 は、それぞれのセキュリティ設定に基づいた WEP キーの制限の一覧を示しています。

表 9-1　WEP キーの制限

セキュリティ設定	WEP キーの制限
CCKM または WPA 認証済みキー管理	キー スロット 1 に WEP キーを設定できません。
LEAP または EAP 認証	キー スロット 4 に WEP キーを設定できません。
40 ビット WEP による暗号スイート	128 ビット キーを設定できません。
128 ビット WEP による暗号スイート	40 ビット キーを設定できません。
TKIP による暗号スイート	WEP キーを設定できません。
TKIP と 40 ビット WEP、または 128 ビット WEP による暗号スイート	WEP キーをキー スロット 1 と 4 に設定できません。
MIC または CMIC による静的 WEP	ルート ブリッジと非ルート ブリッジは、同じ WEP キーを送信キーとして使用する必要があります。また、このキーは、ルート ブリッジと非ルート ブリッジの両方で同じキー スロットに設定されている必要があります。

WEP キーの設定例

表 9-2 は、ルート ブリッジおよびアソシエートされた非ルート ブリッジで機能する WEP キーの設定例を示しています。

表 9-2　WEP キーの設定例

キー スロット	ルート ブリッジ		アソシエートされた非ルート ブリッジ	
	送信キー	キー値	送信キー	キー値
1	x	12345678901234567890abcdef	—	12345678901234567890abcdef
2	—	09876543210987654321fedcba	x	09876543210987654321fedcba
3	—	not set	—	not set
4	—	not set	—	FEDCBA09876543211234567890

ルート ブリッジの WEP キー 1 は送信キーとして選択されているため、非ルート ブリッジの WEP キー 1 も同じ内容に設定する必要があります。非ルート ブリッジに設定されている WEP キー 4 は、送信キーとして選択されていないため、ルート ブリッジの WEP キー 4 を設定する必要はありません。

（注）　MIC を有効にし、静的な WEP を使用する（いずれの EAP 認証も有効にしない）場合は、ルート ブリッジと通信先の非ルート ブリッジの両方で、データ送信用に同じ WEP キーを使用する必要があります。たとえば、MIC を有効にしたルート ブリッジでスロット 1 のキーを送信キーとして使用する場合は、ルート ブリッジにアソシエートされる非ルート ブリッジでも、同じキーをスロット 1 で使用し、これを送信キーとして選択する必要があります。

暗号スイートと WEP の有効化

イネーブル EXEC モードから、次の手順に従って暗号スイートを有効にします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル設定モードを開始します。
ステップ 2	**interface dot11radio 0**	無線インターフェイスのインターフェイス設定モードを開始します。
ステップ 3	**encryption** [**vlan** *vlan-id*] **mode ciphers** {[**aes-ccm** | **ckip** | **cmic** | **ckip-cmic** | **tkip**]} {[**wep128** | **wep40**]}	必要な WEP 保護機能を含む暗号スイートを有効にします。表 9-3 は、設定する認証キー管理のタイプに適した暗号スイートの選択についてのガイドラインを一覧にしています。 • （オプション）WEP および WEP 機能を有効にする VLAN を選択します。 • 暗号オプションと WEP のレベルを設定します。TKIP は、128 ビットまたは 40 ビットの WEP と組み合わせることができます。 （注）　2 つの要素（TKIP と 128 ビット WEP など）からなる暗号スイートを有効にすると、2 番目の暗号はグループ暗号となります。 （注）　静的 WEP は、**encryption mode wep** コマンドを使用して設定することもできます。ただし、**encryption mode wep** コマンドは、ルート ブリッジにアソシエートされている非ルート ブリッジがキー管理に対応していない場合に限り使用してください。**encryption mode wep** コマンドの詳細は、『Cisco IOS Command Reference for Cisco Access Points and Bridges』を参照してください。 （注）　いずれかの無線インターフェイスまたは VLAN で、（**TKIP + WEP 128** または **TKIP + WEP 40** の組み合わせではなく）**TKIP** 単独の暗号化を設定する場合は、この無線または VLAN 上の SSID を、WPA または CCKM のキー管理を使用するように設定する必要があります。無線または VLAN に対して TKIP を設定する場合、SSID にキー管理を設定しないと、SSID に対する非ルート ブリッジ認証が失敗します。
ステップ 4	**end**	イネーブル EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

暗号スイートを無効にするには、encryption コマンドの **no** フォームを使用します。

次の例では、CKIP、CMIC、128 ビット WEP を有効にする暗号スイートを VLAN 1 に設定しています。

```
bridge# configure terminal
bridge(config)# configure interface dot11radio 0
bridge(config-if)# encryption vlan 1 mode ciphers ckip-cmic wep128
bridge(config-if)# end
```

暗号スイートを WPA に一致させる

WPA または CCKM 認証キー管理を使用するようにブリッジを設定する場合は、これらのタイプの認証キー管理と互換性のある暗号スイートを選択する必要があります。表 9-3 は、WPA および CCKM と互換性のある暗号スイートを示します。

表 9-3　WPA および CCKM と互換性のある暗号スイート

認証済みキー管理のタイプ	互換性のある暗号スイート
CCKM	• encryption mode ciphers wep128 • encryption mode ciphers wep40 • encryption mode ciphers ckip • encryption mode ciphers cmic • encryption mode ciphers ckip-cmic • encryption mode ciphers tkip • encryption mode ciphers tkip wep128 • encryption mode ciphers tkip wep40
WPA	• encryption mode ciphers tkip • encryption mode ciphers tkip wep128 • encryption mode ciphers tkip wep40

（注）　いずれかの無線インターフェイスまたは VLAN で、（**TKIP + WEP 128** または **TKIP + WEP 40** の組み合わせではなく）**TKIP** 単独の暗号化を設定する場合は、この無線または VLAN 上の SSID を、WPA または CCKM のキー管理を使用するように設定する必要があります。無線または VLAN に対して TKIP を設定する場合、SSID にキー管理を設定しないと、SSID に対する非ルート ブリッジ認証が失敗します。

WPA および CCKM の説明と認証キー管理の設定方法の詳細は、「WPA キー管理の使用」の項（P.10-5）および「認証されたブリッジの CCKM の利用」の項（P.10-5）を参照してください。