



WEP および WEP 機能の設定

この章では、Wired Equivalent Privacy (WEP)、Message Integrity Check (MIC)、Temporal Key Integrity Protocol (TKIP) およびブロードキャスト キー循環を設定する手順について説明します。この章では、次の項目について説明します。

- [WEP の概要 \(9-2 ページ \)](#)
- [WEP および WEP 機能の設定 \(9-3 ページ \)](#)

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ように、アクセスポイントの範囲内にあるすべてのワイヤレス ネットワーキング デバイスがアクセスポイント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、ワイヤレス 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、アクセスポイントとクライアントデバイス間の通信をスクランブルし、通信機密を保護します。アクセスポイントとクライアントデバイスはどちらも同じ 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せん。

Extensible Authentication Protocol (EAP) 認証は、ワイヤレス ユーザに、動的な WEP キーを提供します。動的な WEP キーは、静的、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 および認証タイプについて詳しくは、[第 10 章「認証タイプの設定」](#)を参照してください。

次の 3 つのセキュリティ機能が、ワイヤレス ネットワークの WEP キーを保護します。

- Message Integrity Check (MIC): 暗号化されたパケットへの攻撃 (ビットフリップ攻撃) を阻止します。ビットフリップ攻撃では、暗号化されたメッセージが不正侵入者によって傍受され、簡単な変更が加えられます。その後、このメッセージは不正侵入者から再び送信され、受信側に正規のメッセージとして受信されます。MIC は、アクセスポイントと、それに結合されるすべてのクライアントデバイスに実装され、数バイトを各パケットに付加することによって、パケットの不正変更を防ぎます。
- Temporal Key Integrity Protocol (TKIP、「WEP キー ハッシュ」ともいいます): この機能は、不正侵入者による、暗号化されたパケットに含まれる非暗号化初期設定ベクトル (IV) を使用した WEP キー割り出しを防ぎます。TKIP は、不正侵入者が IV を使用して WEP キーを特定するのに利用する、推測可能な値を除去します。
- ブロードキャストキー循環: EAP 認証は、クライアントデバイスに動的なユニキャスト WEP キーを提供しますが、使用するのは静的なブロードキャストキーです。ブロードキャスト WEP キー循環を有効にすると、アクセスポイントは動的なブロードキャスト WEP キーを生成し、指定された間隔でそのキーを変更します。ブロードキャストキー循環は、ワイヤレス LAN に使用されているワイヤレスクライアントデバイスがシスコ製品でない場合、またはシスコクライアントデバイス用の最新のファームウェアにアップグレード不可能である場合に、TKIP に代わる、優れた機能を提供します。

WEP および WEP 機能の設定

ここでは、WEP および、MIC、TKIP、ブロードキャスト キー循環のような追加の WEP 機能を設定する手順を説明します。

- [WEP キーの生成 \(9-3 ページ\)](#)
- [WEP の有効化と無効化、および TKIP と MIC の有効化 \(9-4 ページ\)](#)
- [ブロードキャスト キー循環の有効化と無効化 \(9-4 ページ\)](#)

WEP、TKIP、MIC、およびブロードキャスト キー循環は、デフォルトで無効に設定されています。

WEP キーの生成

WEP キーを生成し、主要なプロパティを設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードに入ります。
ステップ 2	<code>interface dot11radio 0</code>	無線インターフェイス用のインターフェイス コンフィギュレーション モードに入ります。
ステップ 3	<code>encryption [vlan <i>vlan-id</i>] key 1-4 size { 40 128 } encryption-key [transmit-key]</code>	WEP キーを生成し、そのプロパティを設定します。 <ul style="list-style-type: none"> • (任意) キーを生成したい VLAN を選択します。 • この WEP キーが存在するキー スロットに名前をつけます。各 VLAN に対して最大 4 つの WEP キーを割り当てることができます。 • キーを入力し、キーのサイズを、40 ビットまたは 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。 • (任意) このキーを転送キーとして設定します。スロット 1 のキーはデフォルトでは転送キーですが、別のキーを転送キーとして設定することができます。
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例は、VLAN 22 に対してスロット 1 に 128 ビットの WEP キーを生成し、そのキーを転送キーとして設定する手順を示しています。

```
ap1100# configure terminal
ap1100(config)# configure interface dot11radio 0
ap1100(config-if)# encryption vlan 22 key 1 size 128 12345678901234567890123456
transmit-key
ap1100(config-ssid)# end
```

WEP の有効化と無効化、および TKIP と MIC の有効化

WEP、TKIP、および MIC を有効に設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードに入ります。
ステップ 2	<code>interface dot11radio 0</code>	無線インターフェイス用のインターフェイス コンフィギュレーション モードに入ります。
ステップ 3	<code>encryption</code> <code>[vlan vlan-id]</code> <code>mode wep {optional [key-hash] </code> <code>mandatory [mic] [key-hash]}</code>	WEP、TKIP、および MIC を有効にします。 <ul style="list-style-type: none"> (任意) WEP および WEP 機能を有効にしたい VLAN を選択します。 WEP レベルを設定し、TKIP と MIC を有効にします。 <code>optional</code> を入力する場合、クライアント デバイスは WEP が有効であるかどうかにかかわらずアクセス ポイントに結合できます。<code>optional</code> に設定されている WEP が備わっている TKIP は有効にできませんが、MIC は有効にできません。<code>mandatory</code> を入力する場合は、クライアント デバイスはアクセス ポイントと結合するために、WEP を有効にしなければなりません。<code>mandatory</code> に設定されている WEP が備わっている TKIP と MIC 両方を有効にできます。
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

WEP を無効にするか、WEP 機能を無効にするには、`no` 形式の暗号化コマンドを使用します。

VLAN 22 に対して WEP を `mandatory` に設定して、MIC と TKIP を有効にする例を示します。

```
ap1100# configure terminal
ap1100(config)# configure interface dot11radio 0
ap1100(config-if)# encryption vlan 22 mode wep mandatory mic key-hash
ap1100(config-ssid)# end
```

ブロードキャスト キー循環の有効化と無効化

ブロードキャスト キー循環は、デフォルトで無効に設定されています。ブロードキャスト キー循環を有効に設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードに入ります。
ステップ 2	<code>interface dot11radio 0</code>	無線インターフェイス用のインターフェイス コンフィギュレーション モードに入ります。
ステップ 3	<code>broadcast-key change seconds</code> <code>[vlan vlan-id]</code>	ブロードキャスト キー循環を有効にします。 <ul style="list-style-type: none"> ブロードキャスト キーの各循環の間隔(秒数)を入力します。 (任意)ブロードキャスト キー循環を有効にしたい VLAN を入力します。
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。

	コマンド	目的
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ブロードキャスト キー循環を無効にするには、`no` 形式の暗号化コマンドを使用します。

VLAN 22 でブロードキャスト キー循環を有効にし、循環間隔を 300 秒に設定する例を次に示します。

```
ap1100# configure terminal
ap1100(config)# configure interface dot11radio 0
ap1100(config-if)# broadcast-key vlan 22 change 300
ap1100(config-ssid)# end
```

