CHAPTER 11

暗号スイートおよび WEP

このマニュアルでは、Wired Equivalent Privacy（WEP）、Message Integrity Check（MIC）、Temporal Key Integrity Protocol（TKIP）、および Advanced Encryption Standard（AES; 高度暗号化規格）の設定方法について説明します。このマニュアルの構成は次のとおりです。

暗号スイートおよび WEP の概要

無線ステーションの範囲内にあるすべてのユーザがステーションの周波数に調整して、信号を待ち受けることができるように、ブリッジ範囲内のすべての無線ネットワーキング デバイスは、ブリッジの無線送信を受信できます。WEP は侵入者を最前線で防御する機能であるため、無線ネットワークに完全な暗号化を施すことを推奨します。

通信のプライバシーを保持するために、WEP 暗号化ではブリッジ間の無線通信をスクランブルします。通信ブリッジでは無線信号の暗号化と暗号解除に同じ WEP キーを使用します。WEP キーはユニキャスト メッセージとマルチキャスト 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 つのデバイスにのみアドレス指定されます。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アドレス指定されます。

Extensible Authentication Protocol（EAP）認証を使用すると、ワイヤレス デバイスにダイナミック WEP キーが設定されます。ダイナミック WEP キーは、スタティック WEP キー（不変の WEP キー）よりもセキュリティが強固です。同じ WEP キーで暗号化されたパケットが必要な数だけ侵入者の手に渡ると、侵入者は WEP キーを計算して取得し、この鍵を使用してネットワークに参加できます。ダイナミック WEP キーを頻繁に変更することにより、侵入者は鍵を計算して取得できません。EAP やその他の認証タイプの詳細については、「認証タイプ」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ために設計された一連の暗号化および統合アルゴリズムです。Wi-Fi Protected Access（WPA）または Cisco Centralized Key Management（CCKM）をイネーブルにするには、暗号スイートを使用する必要があります。暗号スイートを使用すると、WEP を保護しながら、認証鍵管理を使用することもできるため、Command-Line Interface（CLI; コマンドライン インターフェイス）で **encryption mode cipher** コマンドを使用して、WEP をイネーブルにすることを推奨します。AES が組み込まれた暗号スイートは、無線 LAN に最高のセキュリティを実現します。WEP のみが組み込まれた暗号スイートは、セキュリティが最小です。

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。

- AES-CCMP：国立標準技術研究所の FIPS Publication 197 で定義されている AES に基づく AES-CCMP は、128、192、および 256 ビットの鍵を使用してデータの暗号化と復号化が可能な対称ブロック サイファです。AES-CCMP は WEP 暗号化よりも優れていて、IEEE 802.11i 規格で定義されています。
- WEP：WEP は 802.11 の標準暗号化アルゴリズムです。本来は、有線 LAN で使用可能なプライバシーと同じレベルのプライバシを無線 LAN 上で実現するように設計されています。ただし、WEP の基本構造には欠陥があるため、攻撃者は相応の手順を踏むことによりプライバシーを脅かすことができます。
- TKIP：TKIP は、WEP を包含するアルゴリズム スイートです。WEP を実行するために構築された従来のハードウェア上で、考え得る最高のセキュリティを実現するように設計されています。TKIP では、WEP と比べて 4 つの強化機能が追加されています。
  - パケット単位の鍵混在機能：脆弱な鍵に関する攻撃を防ぎます。
  - 新しい IV シーケンス化規則：繰り返し攻撃を検出します。
  - 暗号 MIC（別名 *Michael*）：ビット フリッピングやパケット送信元/宛先の変更などの改ざんを検出します。
  - IV スペースの拡張：鍵を再設定する必要がほとんどなくなります。
- Cisco Key Integrity Protocol（CKIP）：IEEE 802.11i セキュリティ タスク グループによって作成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 （CKIP および CKIP-CMIC は、2.4-GHz（802.11b/g）Cisco Wireless Mobile Interface Card（WMIC; ワイヤレス モバイル インターフェイス カード）でのみサポートされます）。
- Cisco Message Integrity Check（CMIC）：TKIP と同様に、改ざん攻撃を検出するように設計されたシスコのメッセージ インテグリティ チェック メカニズムです。

暗号スイートの設定

ここでは、暗号スイート、WEP、MIC などの追加 WEP 機能、および TKIP の設定方法について説明します。

- 「WEP の設定」（P.11-3）
- 「暗号スイートのイネーブル化」（P.11-6）

暗号化の暗号スイートおよび WEP は、デフォルトでディセーブルです。

WEP の設定

12.4(3)JK 以降のリリースでの WEP の設定

12.4(3)JK 以降のリリースの Cisco 3201 WMIC では、暗号化設定が dot11 インターフェイスから各 SSID 設定に移動しました。Csico 3202 WMIC および 3205 WMIC では、12.4(3)JL リリースからこの機能変更がサポートされます。

WEP 暗号化を設定するには、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	**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	**dot11** *ssid sample_ssid*	SSID 設定を開始します。
ステップ 3	**encryption key** *1-4* ***size*** {**40** | **128** } *encryption-key* [**transmit-key**]	この SSID に対して WEP キーを作成して、プロパティを設定します。 • この WEP キーを格納するキー スロットに名前を付けます。各 VLAN には最大 4 つの WEP キーを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。 • 鍵を入力して、鍵サイズを 40 ビットまたは 128 ビットに設定します。40 ビット鍵は 10 個の 16 進数で構成されます。128 ビット鍵は 26 個の 16 進数で構成されます。 • （任意）現在の鍵を送信キーとして設定します。デフォルトでは、スロット 2 の鍵が送信キーです。WEP および MIC をイネーブルにする場合は、ルート デバイスと非ルート ブリッジの同じキー スロットに同じ WEP キーを作成し、この鍵を送信キーとして使用します。
ステップ 4	**encryption mode wep { mandatory | optional }**	この VLAN の暗号化モードとして WEP を設定します。
ステップ 5	**end**	イネーブル EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config**	（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。

次に、128 ビット WEP キーを SSID sample_ssid のスロット 2 に作成し、この鍵を送信キーに設定する例を示します。

```
bridge# configure terminal
bridge(config)# dot11 ssid sample_ssid
bridge(config-ssid)# encryption mode mandatory
bridge(config-ssid)# encryption key 2 size 128 12345678901234567890123456 transmit-key
bridge(config-ssid)# end
```

12.3(8)JK 以前のリリースでの WEP の設定

WEP キーを作成してキー 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	**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	**interface dot11radio 0**	無線インターフェイスに対応するインターフェイス コンフィギュレーション 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 キーを作成して、プロパティを設定します。 • （任意）鍵を作成する VLAN を選択します。 • この WEP キーを格納するキー スロットに名前を付けます。各 VLAN には最大 4 つの WEP キーを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。 • 鍵を入力して、鍵サイズを 40 ビットまたは 128 ビットに設定します。40 ビット鍵は 10 個の 16 進数で構成されます。128 ビット鍵は 26 個の 16 進数で構成されます。 • （任意）現在の鍵を送信キーとして設定します。デフォルトでは、スロット 2 の鍵が送信キーです。WEP および MIC をイネーブルにする場合は、ルート デバイスと非ルート ブリッジの同じキー スロットに同じ WEP キーを作成し、この鍵を送信キーとして使用します。
ステップ 4	**encryption** [**vlan** ***vlan-id***] **mode wep** **{ mandatory | optional }**	この VLAN の暗号化モードとして WEP を設定します。
ステップ 5	**end**	イネーブル EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config**	（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。

次に、128 ビット WEP キーを VLAN 1 のスロット 2 に作成し、この鍵を送信キーに設定する例を示します。

```
bridge# configure terminal
bridge(config)# 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 11-1 に、各種のセキュリティ設定における WEP キーの制限事項を示します。

表 11-1　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 認証鍵管理	スロット 1 に WEP を設定できません。
LEAP または EAP 認証	スロット 4 に WEP 送信キーを設定できません。
40 ビット WEP を含む暗号スイート	128 ビット鍵を設定できません。
128 ビット WEP を含む暗号スイート	40 ビット鍵を設定できません。
TKIP を含む暗号スイート	どの WEP キーも設定できません。
AES を含む暗号スイート	どの WEP キーも設定できません。
TKIP および 40 ビット WEP または 128 ビット WEP を含む暗号スイート	キー スロット 1 およびキー スロット 4 に WEP キーを設定できません。
MIC または CMIC を含むスタティック WEP	ルート デバイスおよび非ルート 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、この鍵をルート デバイスおよび非ルート ブリッジの同じキー スロットに格納する必要があります。

WEP キーの設定例

表 11-2 に、ルート デバイスおよび対応する非ルート ブリッジに対する WEP キーの設定例を示します。

表 11-2　WEP キーの設定例

キー スロット	ルート デバイス		対応する非ルート ブリッジ	
	送信の有無	鍵の内容	送信の有無	鍵の内容
1	x	12345678901234567890abcdef	—	12345678901234567890abcdef
2	—	09876543210987654321fedcba	x	09876543210987654321fedcba
3	—	（設定しない）	—	（設定しない）
4	—	（設定しない）	—	FEDCBA09876543211234567890

ルート デバイスの 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 に同じ内容を設定する必要があります。非ルート ブリッジに WEP キー 4 が設定されていますが、この鍵は送信キーに選択されていないため、ルート デバイスの WEP キー 4 は設定する必要がありません。

（注） MIC をイネーブルにした状態でスタティック WEP を使用する場合（EAP 認証タイプをイネーブルにしない場合）は、ルート デバイスとルート デバイスが通信する任意の非ルート ブリッジで、データ送信に同じ WEP キーを使用する必要があります。たとえば、MIC 対応のルート デバイスでスロット 1 内の鍵を送信キーとして使用する場合は、ルート デバイスに対応する非ルート ブリッジでスロット 1 内の同じ鍵を使用し、この鍵を送信キーとして選択する必要があります。

暗号スイートのイネーブル化

12.4(3)JK 以降のリリースでの暗号スイートのイネーブル化

12.4(3)JK 以降のリリースの Cisco 3201 WMIC では､暗号設定が dot11 インターフェイスから各 SSID 設定に移動しました。Csico 3202 WMIC および 3205 WMIC では、12.4(3)JL リリースからこの機能変更がサポートされます。

暗号スイートの暗号化を設定するには、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	**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	**dot11** *ssid sample_ssid*	SSID 設定を開始します。
ステップ 3	**encryption mode ciphers** {[**aes-ccm** | **ckip** | **cmic** | **ckip-cmic** | **tkip**]} {[**wep128** | **wep40**]}	必要な WEP 保護が含まれる暗号スイートをイネーブル化します（表 11-3 に、設定する認証鍵管理のタイプに対応する暗号スイートを選択するためのガイドラインを示します）。 • 暗号オプションを設定します。 **（注）** TKIP と 128 ビットまたは 40 ビット WEP を組み合わせることができます。 **（注）** AES と TKIP を組み合わせることができます。その場合、AES はユニキャスト暗号であり、TKIP はグループ暗号になります。 **（注）** 2 つの要素（TKIP と 128 ビット WEP など）を含む暗号スイートをイネーブルにすると、2 番めの暗号はグループ暗号になります。 **（注）** **encryption mode wep** コマンドを使用すると、スタティック WEP も設定できます。ただし、**encryption mode wep** を使用するのは、ルート デバイスに対応するどの非ルート ブリッジにも鍵管理機能が備わっていない場合に限定してください。**encryption mode wep** コマンドの詳細については、『*Cisco IOS Command Reference for Cisco Access Points and Bridges*』を参照してください。 **（注）** 無線インターフェイスまたは VLAN に TKIP のみ、AES のみ、または AES と TKIP の組み合わせ（WEP はなし）を設定する場合は、WPA または CCKM 鍵管理を使用するように、この無線または VLAN の SSID を設定する必要があります。SSID に鍵管理を設定しなかった場合は、SSID に関する非ルート ブリッジ認証に失敗します。 **（注）** Cisco Key Integrity Protocol（CKIP）および CKIP-Cisco Message Integrity Protocol（CMIP）は、2.4-GHz（802.11b/g）WMIC でのみサポートされます。
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**	（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。

次に、SSID sample_ssid に、暗号化モードとして CKIP、CMIC、および 128 ビット WEP をイネーブルにする暗号スイートを設定する例を示します。

```
bridge# configure terminal
bridge(config)# dot11 ssid sample_ssid
bridge(config-ssid)# encryption mode ciphers ckip-cmic wep128
bridge(config-ssid)# end
```

次に、SSID sample_ssid に、暗号化モードとして AES をイネーブルにする暗号スイートを設定する例を示します。

```
bridge# configure terminal
bridge(config)# dot11 ssid sample_ssid
bridge(config-ssid)# encryption mode ciphers aes-ccm
bridge(config-ssid)# end
```

12.3(8)JK 以前のリリースでの暗号スイートのイネーブル化

暗号スイートをイネーブルにするには、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	**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	**interface dot11radio 0**	無線インターフェイスに対応するインターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**encryption** [**vlan** *vlan-id*] **mode ciphers** {[**aes-ccm** | **ckip** | **cmic** | **ckip-cmic** | **tkip**]} {[**wep128** | **wep40**]}	必要な WEP 保護が含まれる暗号スイートをイネーブル化します（表 11-3 に、設定する認証鍵管理のタイプに対応する暗号スイートを選択するためのガイドラインを示します）。 • （任意）WEP および WEP 機能をイネーブルにする VLAN を選択します。 • 暗号オプションを設定します。 **（注）** TKIP と 128 ビットまたは 40 ビット WEP を組み合わせることができます。 **（注）** AES と TKIP を組み合わせることができます。その場合、AES はユニキャスト暗号であり、TKIP はグループ暗号になります。 **（注）** 2 つの要素（TKIP と 128 ビット WEP など）を含む暗号スイートをイネーブルにすると、2 番めの暗号はグループ暗号になります。 **（注）** **encryption mode wep** コマンドを使用すると、スタティック WEP も設定できます。ただし、**encryption mode wep** を使用するのは、ルート デバイスに対応するどの非ルート ブリッジにも鍵管理機能が備わっていない場合に限定してください。**encryption mode wep** コマンドの詳細については、『*Cisco IOS Command Reference for Cisco Access Points and Bridges*』を参照してください。 **（注）** 無線インターフェイスまたは VLAN に TKIP のみ、AES のみ、または AES と TKIP の組み合わせ（WEP はなし）を設定する場合は、WPA または CCKM 鍵管理を使用するように、この無線または VLAN の SSID を設定する必要があります。SSID に鍵管理を設定しなかった場合は、SSID に関する非ルート ブリッジ認証に失敗します。 **（注）** Cisco Key Integrity Protocol（CKIP）および CKIP-Cisco Message Integrity Protocol（CMIP）は、2.4-GHz（802.11b/g）WMIC でのみサポートされます。
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**	（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。

暗号スイートをディセーブルにするには、encryption コマンドの **no** 形式を使用します。

次に、VLAN 1 に、CKIP、CMIC、および 128 ビット WEP をイネーブルにする暗号スイートを設定する例を示します。

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

次に、VLAN 1 に、暗号化モードとして AES をイネーブルにする暗号スイートを設定する例を示します。

```
bridge# configure terminal
bridge(config)# configure interface dot11radio 0
bridge(config-if)# encryption vlan 1 mode ciphers aes-ccm
bridge(config-if)# end
```

暗号スイートと WPA の対応

ブリッジを設定して WPA または CCKM 認証鍵管理を使用する場合は、認証鍵管理のタイプ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 11-3 に、WPA または CCKM と互換性のある暗号スイートを示します。

表 11-3　WPA および CCKM と互換性のある暗号スイート

認証鍵管理のタイプ	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 • encryption mode ciphers aes-ccm
WPA	• encryption mode ciphers tkip • encryption mode ciphers tkip wep128 • encryption mode ciphers tkip wep40 • encryption mode aes-ccm • encryption mode aes-ccm wep128 • encryption mode aes-ccm wep40 • encryption mode aes-ccm tkip • encryption mode aes-ccm tkip wep128 • encryption mode aes-ccm tkip wep40

（注）　SSID 設定に TKIP のみを使用した暗号（TKIP + WEP 128 または TKIP + WEP 40 の暗号以外）を設定する場合は、WPA または CCKM 鍵管理を使用するように、SSID を設定する必要があります。TKIP を設定したにもかかわらず、SSID に鍵管理を設定しなかった場合は、この SSID で認証に失敗します。

WPA および CCKM の詳細、および認証鍵管理の設定手順については、「認証タイプ」マニュアルを参照してください。