CHAPTER 10

暗号スイートと WEP の設定

この章では、Wi-Fi Protected Access（WPA）および Cisco Centralized Key Management（CCKM）認証済みキー管理、Wired Equivalent Privacy（WEP）、AES などの WEP 機能、Message Integrity Check（MIC; メッセージ完全性チェック）、Temporal Key Integrity Protocol（TKIP）、およびブロードキャスト キー ローテーションを使用するために必要な暗号スイートの設定方法について説明します。この章で説明する内容は、次のとおりです。

暗号スイートと WEP の概要

この項では、無線 LAN 上のトラフィックを WEP と暗号スイートを使って保護する仕組みについて説明します。

ラジオ局の受信範囲内にいる人すべてが、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様に、アクセス ポイントの範囲内にあるすべての無線ネットワーキング デバイスは、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、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、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、通信機密を維持します。アクセス ポイントとクライアント デバイスはいずれも同じ 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す。

Extensible Authentication Protocol（EAP; 拡張認証プロトコル）認証は 802.1x 認証とも呼ばれ、無線ユーザに動的な 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 11 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 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推奨します。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。

- AES-CCMP：国立標準技術研究所（NIST）による *FIPS Publication 197* で定義されている高度暗号化規格（AES）に基づいています。AES-CCMP は、128 ビット、192 ビット、および 256 ビットのキーを使用してデータの暗号化および復号化を行う対称ブロック暗号です。AES-CCMP は、WEP 暗号化よりも優れており IEEE 802.11i 規格で定義されています。

（注） Cisco Aironet 1130 および 1230 シリーズ アクセス ポイントは WPA2 をサポートしています。Cisco IOS ソフトウェアをリリース 12.3(2)JA 以降にアップグレードした Cisco Aironet 1100、1200、および 1300 シリーズ 802.11g 無線は WPA2 をサポートしています。

（注） 部品番号 AIR-RM21A または AIR-RM22A の Cisco Aironet 1200 シリーズの無線モジュールは WPA2 または AES をサポートしています。

- Wired Equivalent Privacy（WEP）：WEP は 802.11 標準暗号アルゴリズムであり、もともとは有線 LAN で可能なレベルのプライバシーを、無線 LAN で実現できるように設計されたものです。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。

- Temporal Key Integrity Protocol（TKIP）：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上で、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（脆弱キー）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）
  - キー更新をほとんど不要にするための IV 長の拡張
- 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。
- Cisco Message Integrity Check（CMIC）：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。
- ブロードキャスト キー ローテーション（グループ キー更新とも呼ばれる）：ブロードキャスト キー ローテーションにより、アクセス ポイントは最良のランダム グループ キーを生成でき、キー管理可能なクライアントすべてを定期的に更新できるようになります。Wi-Fi Protected Access（WPA）も、グループ キー更新の追加オプションを提供します。WPA の詳細は、「WPA キー管理の使用」（P.11-7）を参照してください。

（注）　ブロードキャスト キー ローテーションを有効にすると、静的 WEP を使用しているクライアント デバイスはアクセス ポイントを使用できなくなります。ブロードキャスト キー ローテーションを有効にした場合は、802.1x 認証（LEAP、EAP-TLS、PEAP など）を使用する無線クライアント デバイスだけがアクセス ポイントを使用できます。

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 などの WEP 追加機能、TKIP、ブロードキャスト キー ローテーションの設定方法について説明します。

- 「WEP キーの作成」（P.10-3）
- 「暗号スイートと WEP の有効化」（P.10-6）
- 「ブロードキャスト キー ローテーションの有効化と無効化」（P.10-8）

（注）　WEP、TKIP、MIC、およびブロードキャスト キー ローテーションは、デフォルトで無効に設定されています。

WEP キーの作成

（注）　静的 WEP キーの設定は、静的 WEP を使用するクライアント デバイスをアクセス ポイントがサポートしなければならない場合にだけ必要となります。アクセス ポイントにアソシエートするすべてのクライアント デバイスがキー管理（WPA、CCKM、または 802.1x 認証）を使用する場合は、静的 WEP キーを設定する必要はありません。

特権 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 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** | **1** }	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。2.4GHz 無線は Radio 0、5GHz 無線は Radio 1 です。
ステップ 3	**encryption** [**vlan** *vlan-id*] **key** *1-4* **size** { **40** | **128** } *encryption-key* [**0** | **7**] [**transmit-key**]	WEP キーを作成し、そのプロパティを設定します。 • （任意）キーを作成する VLAN を選択します。 • 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。最大 16 個の VLAN を割り当てることができます。VLAN ごとに最大 4 つの WEP キーを 1 つの VLAN に最大 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。 • （任意）このキーを暗号化するか（**7**）、または暗号化しないか（**0**）を指定します。 • （任意）このキーを送信キーとして設定します。スロット 1 のキーは、デフォルトで送信キーとなります。 **（注）** 静的 WEP を MIC または CMIC とともに設定する場合、アクセス ポイントおよびアソシエートされているクライアント デバイスは送信キーとして同じ WEP キーを使用する必要があり、そのキーは、アクセス ポイントとクライアントで同じキー スロットに設定されていなければなりません。 **（注）** 認証済みキー管理などのセキュリティ機能を使用すると、WEP キーの設定を制限できます。WEP キーに影響を与える機能の一覧は、「WEP キーの制限」（P.10-5）を参照してください。
ステップ 4	**end**	特権 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。

次の例は、VLAN 22 のスロット 3 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。

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# encryption vlan 22 key 3 size 128 12345678901234567890123456
transmit-key
ap1200(config-if)# end
```

WEP キーの制限

表 10-1 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 10-1　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	アクセス ポイントとクライアント デバイスは、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、アクセス ポイントとクライアントの両方で同じキー スロットに設定されている必要があります。
ブロードキャスト キー ローテーション	ブロードキャスト キー ローテーションにより、スロット 2 と 3 のキーが上書きされます。 **（注）** ブロードキャスト キー ローテーションを有効にすると、静的 WEP を使用しているクライアント デバイスはアクセス ポイントを使用できなくなります。ブロードキャスト キー ローテーションを有効にした場合は、802.1x 認証（LEAP、EAP-TLS、PEAP など）を使用する無線クライアント デバイスだけがアクセス ポイントを使用できます。

WEP キーの設定例

表 10-2 は、アクセス ポイントおよびアソシエートされたデバイスで機能する WEP キーの設定例を示しています。

表 10-2　WEP キーの設定例

キー スロット	アクセス ポイント		アソシエートされるデバイス	
	送信キー	キー値	送信キー	キー値
1	○	12345678901234567890abcdef	—	12345678901234567890abcdef
2	—	09876543210987654321fedcba	○	09876543210987654321fedcba
3	—	未設定	—	未設定
4	—	未設定	—	FEDCBA09876543211234567890

アクセス ポイントの WEP キー 1 は送信キーとして選択されているため、アソシエートされるデバイスの WEP キー 1 も同じ内容に設定する必要があります。アソシエートされるデバイスに設定されている WEP キー 4 は、送信キーとして選択されていないため、アクセス ポイントの 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、アクセス ポイントと通信先のデバイスの両方で、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 を有効にしたアクセス ポイントでスロット 1 のキーを送信キーとして使用する場合は、そのアクセス ポイントにアソシエートされるクライアント デバイスでも、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

特権 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 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** | **1** }	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。2.4GHz 無線は Radio 0、5GHz 無線は Radio 1 です。

	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 保護を含む暗号スイートを有効にします。 表 10-3 は、設定する認証済みキー管理タイプと一致する暗号スイートを選択するためのガイドラインです。 • （任意）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）** **ckip**、**cmic**、または **ckip-cmic** を設定する場合は、Aironet 拡張機能も有効にする必要があります。Aironet 拡張機能を有効にするコマンドは、**dot11 extension aironet** です。 **（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、アクセス ポイントにアソシエートされているクライアント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）** SSID に（**TKIP + WEP 128** でも **TKIP + WEP 40** でもない）暗号化 TKIP を設定する場合は、その SSID では WPA または CCKM キー管理を使用する必要があります。WPA または CCKM キー管理を有効にせずに暗号化 TKIP を使用した SSID では、クライアント認証が失敗します。
ステップ 4	**end**	特権 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。

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

次の例では、CKIP（サポートされない）、CMIC（サポートされない）、および 128 ビット WEP を有効にする暗号スイートを VLAN 22 に設定します。

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# encryption vlan 22 mode ciphers ckip-cmic wep128
ap1200(config-if)# exit
```

WPA および CCKM に一致する暗号スイート

WPA または CCKM 認証済みキー管理を使用するようにアクセス ポイントを設定する場合は、そ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 10-3 は、WPA および CCKM と互換性のある暗号スイートを示しています。

表 10-3　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
WPA	• encryption mode ciphers tkip • encryption mode ciphers tkip wep128 • encryption mode ciphers tkip wep40

（注）　SSID に（**TKIP + WEP 128** でも **TKIP + WEP 40** でもない）暗号化 TKIP を設定する場合は、その SSID では WPA または CCKM キー管理を使用する必要があります。WPA または CCKM キー管理を有効にせずに暗号化 TKIP を使用した SSID では、クライアント認証が失敗します。

WPA および CCKM の詳細、および認証キー管理の設定手順については、「認証されたクライアントの CCKM の利用」（P.11-6）、および「WPA キー管理の使用」（P.11-7）を参照してください。

ブロードキャスト キー ローテーションの有効化と無効化

ブロードキャスト キー ローテーションは、デフォルトでは無効になっています。

（注）　ブロードキャスト キー ローテーションを有効にすると、静的 WEP を使用しているクライアント デバイスはアクセス ポイントを使用できなくなります。ブロードキャスト キー ローテーションを有効にした場合は、802.1x 認証（LEAP、EAP-TLS、PEAP など）を使用する無線クライアント デバイスだけがアクセス ポイントを使用できます。

特権 EXEC モードから、次の手順に従ってブロードキャスト キー ローテーションを有効にします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル 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 | 1 }**	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。2.4GHz 無線は Radio 0、5GHz 無線は Radio 1 です。

	コマンド	目的
ステップ 3	**broadcast-key change** *seconds* [**vlan** *vlan-id*] [**membership-termination**] [**capability-change**]	ブロードキャスト キー ローテーションを有効にします。 • ブロードキャスト キーのローテーションの間隔を秒単位で入力します。 • （任意）ブロードキャスト キー ローテーションを有効にする VLAN を入力します。 • （任意）WPA 認証済みキー管理を有効にすると、アクセス ポイントが WPA グループ キーを変更および配布するための条件を追加指定できます。 – Membership termination：アクセス ポイントは、任意の認証済みクライアント デバイスがアクセス ポイントからアソシエーションを解除されたときに、新しいグループ キーを生成、配布します。この機能はアソシエートされたクライアントのグループ キーの機密性を保護します。しかし、ネットワーク上のクライアントが頻繁にローミングする場合、オーバーヘッドが生じる可能性があります。 – Capability change：アクセス ポイントは、最後の非キー管理（静的 WEP）クライアントがアソシエーションを解除されたときに、動的グループ キーを生成、配布します。また、最初の非キー管理（静的 WEP）クライアントが認証するときに、静的に設定された WEP キーを配布します。WPA 移行モードでは、アクセス ポイントにアソシエートしている静的 WEP クライアントが存在しない場合は、この機能により、キー管理が可能なクライアントのセキュリティが大幅に向上します。 認証済みキー管理を有効にする方法の詳細については、第 11 章「認証タイプの設定」を参照してください。
ステップ 4	**end**	特権 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。

ブロードキャスト キー ローテーションを無効にするには、encryption コマンドの **no** 形式を使用します。

次の例は、VLAN 22 でブロードキャスト キー ローテーションを有効にし、ローテーション間隔を 300 秒に設定しています。

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# broadcast-key vlan 22 change 300
ap1200(config-if)# end
```