CHAPTER 10

WLAN 認証および暗号化の設定

この章では、WLAN を保護するための認証方式および暗号化方式を設定する方法について説明します。

暗号化には、共有キーまたは個々のクライアント キーを使用します。個々のクライアント キーを使用するほうが確実ですが、その場合、キーの管理が必要になります。キーを管理するには、Wi-Fi Protected Access（WPA）バージョン 1 またはバージョン 2 と、Cisco Centralized Key Management（CCKM）認証済みキー管理による暗号スイートを使用します。

暗号化の堅牢性を確保するには、Wired Equivalent Privacy（WEP）を使用します。WEP 機能には、AES、Temporal Key Integrity Protocol（TKIP）、Message Integrity Check（MIC）、およびブロードキャスト キー ローテーションが含まれます。認証には、共有キー（WEP）、事前共有キー（WPAv1 または WPAv2）、個々のクライアント認証（802.1x/EAP）を使用します。

認証および暗号化メカニズムについて

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 ポイントおよび任意の無線クライアントの無線伝送を受信できます。また、アクセス ポイントは一般に有線インフラストラクチャに接続します。アクセス ポイントの無線信号はアクセス ポイントが展開されている施設の壁を越えて伝送できるため、外部ユーザがアクセス ポイントを介して有線インフラストラクチャにアクセスできる場合があります。したがって、WLAN セキュリティは主に次の 2 つの機能によって確保されます。

- ユーザの認証。有効なユーザだけに、アクセス ポイントを介した通信が許可されるようにします。
- 無線通信の暗号化。傍受者がアクセス ポイントやクライアント通信から捕捉した信号を解読できないようにします。

Cisco Aironet アクセス ポイントでは、SSID が直接アクセス ポイントの無線、または AP 無線インターフェイスに設定された VLAN にマッピングされます。暗号化は、無線レベルで設定されるか（無線インターフェイスに VLAN が定義されていない場合）、（無線インターフェイスに 1 つ以上の VLAN が定義されると同時に）VLAN レベルで設定されます。つまり、特定の無線インターフェイスや特定の VLAN で複数の SSID を有効にする場合は、それらすべての SSID が共通の暗号化方式を共有する必要があります。

認証は SSID レベルで設定されます。SSID ごとの異なる認証メカニズムを使用できます。ただし、SSID は VLAN（または無線インターフェイス）にマッピングされるため、SSID レベルで定義された認証メカニズムが、その SSID の VLAN（または無線）レベルで定義されている暗号化メカニズムと互換性があることを確認する必要があります。

無線（または VLAN）レベルで定義する暗号化には、次のいずれかの方式を使用できます。

- 暗号化なし
- オプションの（40 ビット長または 128 ビット長のキーを使用した）静的 WEP 暗号化。WEP をサポートしているクライアントと、暗号化をサポートしていないクライアントの両方が、SSID に参加できます。
- 必須の（40 ビット長または 128 ビット長のキーを使用した）静的 WEP 暗号化。クライアントは静的 WEP 暗号化をサポートしていなければ、SSID に参加できません。
- 40 ビットまたは 128 ビット暗号のキー管理が有効な WEP 暗号化。ユニキャスト WEP キー ローテーション（認証メカニズムが個々のクライアント キー決定に対応する場合）および/またはブロードキャスト キー ローテーション（認証メカニズムが個々のクライアント キー決定に対応する場合）が使用可能になります。
- 暗号 TKIP、CKIP、CMIC、CKIP-CMIC、または AES（認証メカニズムが個々のクライアント キー決定に対応する場合）
- 2 つまたは 3 つの暗号の組み合わせ。
  このタイプの組み合わせは、SSID のセキュリティ レベルを上げる必要がある一方、弱い暗号化方式しかサポートしていないクライアントも引き続きサポートする必要がある場合に使用します。この場合、クライアントは SSID で許可される最も強力な暗号化メカニズムを使用します。ブロードキャスト キーには、すべてのクライアントでサポートされている暗号化メカニズムを使用します。
  サポートされているすべての暗号化方式のうち、最も強力なのは AES-CCMP で、次に TKIP が続きます。WEP は脆弱な暗号化メカニズムと見なされているため、IEEE 802.11 標準で非推奨となっています。
  たとえば、AES+TKIP+WEP 暗号化を定義するとします。この場合、AES をサポートしているクライアントは、ユニキャスト キーの暗号化に AES を使用します。AES はサポートしていないが、TKIP はサポートしているクライアントにはセルへの参加が許可されます。これらのクライアントはユニキャスト キーの暗号化に TKIP を使用します。WEP のみをサポートしているクライアントにもセルへの参加が許可されます。これらのクライアントはユニキャスト キーの暗号化に WEP を使用します。セルに AES、TKIP、および WEP クライアントが含まれている場合、ブロードキャスト キーには WEP 暗号化が使用されます（WEP がすべてのクライアントでサポートされる唯一の共通の暗号化方式であるため）。セルに AES と TKIP クライアントが含まれていて、WEP クライアントが含まれていない場合、ブロードキャスト キーには TKIP が使用されます（WEP クライアントがセルに参加すると、ブロードキャスト キーの暗号化は WEP に変更されます）。セルに AES クライアントだけが含まれている場合、ブロードキャスト キーには AES が使用されます（TKIP クライアントがセルに参加すると TKIP に変更され、WEP クライアントがセルに参加すると WEP に変更されます）。

（注）　暗号化メカニズムのサポートは、増分式です。WEP をサポートするクライアントは、TKIP や AES をサポートすることもあれば、サポートしないこともあります。ただし、TKIP をサポートするクライアントは、必ず WEP をサポートします。同様に、AES クライアントは必ず TKIP と WEP をサポートします。

各暗号化メカニズムの詳細については、この章の暗号化モードについての項に記載されています。

暗号化は無線または VLAN レベルで設定されます。認証は SSID レベルで設定されます。次のいずれかの認証方式、あるいはこのうちの複数の認証方式を組み合わせて使用できます。

- Open：認証を行わずにアクセス ポイントにアソシエートできます。
- Shared Key：静的 WEP 認証を使用します。
- Network EAP：LEAP を使用します。

(注)　Open モードと Shared Key モードは、どちらも他のモードと組み合わせて使用できます。たとえば、EAP/802.1x と組み合わせると、アクセス ポイントとのアソシエーションが行われた後に認証が行われます。MAC 認証と組み合わせた場合は、アクセス ポイントとのアソシエーションの最終フェーズで認証が行われます。

各認証メカニズムの詳細については、この章の「認証メカニズムについて」の項を参照してください。

さまざまな認証メカニズムと暗号化メカニズムの組み合わせによって、SSID のセキュリティ スキームが変わってきます。次の表に、サポートされる組み合わせまとめます。

SSID 認証	インターフェイス暗号化	サポートされるセキュリティ
Open	WEP（オプション）	AP は SSID を Open/Open として宣言し、WEP の明示的サポートをブロードキャストしません。ただし、クライアント コンフィギュレーションが WEP 暗号化および/または WEP 認証に設定されている場合、AP はクライアント アソシエーションも受け入れます。WEP を使用するクライアントでこのモードを使用する場合は、WEP キーを定義する必要があります。
Open	WEP（必須）	AP は SSID を WEP 対応の SSID として宣言します。クライアント コンフィギュレーションが Open/None、WEP 暗号化および/または WEP 認証に設定されている場合、AP はクライアント アソシエーションを受け入れます。アソシエーション フェーズの完了後、トラフィックをアクセス ポイントを介して転送するには、WEP サポートが必須です。WEP を使用するクライアントでこのモードを使用する場合は、WEP キーを定義する必要があります。
Open + MAC	Open 認証でサポートされるすべてのモード	AP とのクライアント アソシエーションの最終フェーズに、クライアント MAC 認証が追加されます（詳細については、ネットワークに対する MAC アドレス認証（11-5 ページ）を参照してください）。
Open + EAP	任意の暗号（WEP 40、WEP 128、TKIP、CKIP、CMIC、CKIP-CMIC、TKIP + WEP 40、TKIP + WEP 128、AES-CCMP、AES-CCMP + TKIP、AES-CCMP + TKIP + WEP 40、AES-CCMP + TKIP + WEP 128）	AP とのクライアント アソシエーションの後に、802.1x/EAP 認証が行われます（サポートされる EAP モードは、LEAP、EAP-FAST、PEAP/GTC、MSPEAP、EAP-TLS および EAP-FAST です）。このプロセス中に、個々のクライアント キーが生成されます。複数の暗号が許可される場合、クライアントでサポートされる最も強力な暗号を使用してキーが生成されます。ブロードキャスト キーは、すべてのクライアントでサポートされる暗号を使用してすべてのクライアントに転送されます。

SSID 認証	インターフェイス暗号化	サポートされるセキュリティ
Open + MAC + EAP	任意の暗号（WEP 40、WEP 128、TKIP、CKIP、CMIC、CKIP-CMIC、TKIP + WEP 40、TKIP + WEP 128、AES-CCMP、AES-CCMP + TKIP、AES-CCMP + TKIP + WEP 40、AES-CCMP + TKIP + WEP 128）	アクセス ポイントとのクライアント アソシエーションの最終フェーズにクライアント MAC 認証が追加されます。AP とのクライアント アソシエーションの後、802.1x/EAP 認証が行われます。このプロセス中に、個々のクライアント キーが生成されます。複数の暗号が許可される場合、クライアントでサポートされる最も強力な暗号を使用してキーが生成されます。ブロードキャスト キーは、すべてのクライアントでサポートされる暗号を使用してすべてのクライアントに転送されます。
Open + EAP（オプション）	任意の暗号（WEP 40、WEP 128、TKIP、CKIP、CMIC、CKIP-CMIC、TKIP + WEP 40、TKIP + WEP 128、AES-CCMP、AES-CCMP + TKIP、AES-CCMP + TKIP + WEP 40、AES-CCMP + TKIP + WEP 128）	EAP に設定されたクライアントは個々の認証を使用し、個々のキーで暗号化を使用します。セキュリティが設定されていないクライアントも、AP とアソシエートできます。このモードは、より強力なセキュリティへの移行メカニズムとして設計されています。ブロードキャスト キーには、すべてのクライアントでサポートされる共通のセキュリティ メカニズムが使用されます。EAP クライアントと Open クライアントの両方がアソシエートされる場合、ブロードキャスト キーは暗号化されません。
共有認証	WEP（オプション）	AP は SSID を WEP 対応の SSID として宣言します。AP は WEP 認証が設定されたクライアントだけを受け入れます。アソシエーション後の WEP 暗号化はサポートされますが、これはオプションです。
共有認証	WEP（必須）	AP は SSID を WEP 対応の SSID として宣言します。AP は WEP 認証が設定されたクライアントだけを受け入れます。アソシエーション後の WEP 暗号化は必須です。
共有認証 + MAC	共有認証でサポートされるすべてのモード	WEP 認証の後、アソシエーションの最終フェーズで MAC 認証が行われます。
共有認証 + EAP	共有認証でサポートされるすべてのモード	WEP 認証の後、AP との Open アソシエーションが行われます。アソシエーションの後、個々のクライアント EAP 認証と個々のキー生成が行われます。
共有認証 + EAP + MAC	共有認証でサポートされるすべてのモード	WEP 認証の後、アソシエーションの最終フェーズで MAC 認証が行われます。アソシエーションの後、個々のクライアント EAP 認証と個々のキー生成が行われます。

SSID 認証	インターフェイス暗号化	サポートされるセキュリティ
Network EAP	任意の暗号（WEP 40、WEP 128、TKIP、CKIP、CMIC、CKIP-CMIC、TKIP + WEP 40、TKIP + WEP 128、AES-CCMP、AES-CCMP + TKIP、AES-CCMP + TKIP + WEP 40、AES-CCMP + TKIP + WEP 128）	AP とのクライアント アソシエーションの後、Cisco LEAP 認証が行われます。このプロセス中に、個々のクライアント キーが生成されます。複数の暗号が許可される場合、クライアントでサポートされる最も強力な暗号を使用してキーが生成されます。ブロードキャスト キーは、すべてのクライアントでサポートされる暗号を使用してすべてのクライアントに転送されます。
Network EAP + MAC	任意の暗号（WEP 40、WEP 128、TKIP、CKIP、CMIC、CKIP-CMIC、TKIP + WEP 40、TKIP + WEP 128、AES-CCMP、AES-CCMP + TKIP、AES-CCMP + TKIP + WEP 40、AES-CCMP + TKIP + WEP 128）	アクセス ポイントとのクライアント アソシエーションの最終フェーズにクライアント MAC 認証が追加されます。AP とのクライアント アソシエーションの後、LEAP を使用した 802.1x/EAP 認証が行われます。このプロセス中に、個々のクライアント キーが生成されます。複数の暗号が許可される場合、クライアントでサポートされる最も強力な暗号を使用してキーが生成されます。ブロードキャスト キーは、すべてのクライアントでサポートされる暗号を使用してすべてのクライアントに転送されます。
Web 認証	いずれか（Any）	Web 認証は、単独で（他の SSID 認証または暗号化を使用せずに）使用することも、他のいずれかの認証および暗号化方式と組み合わせて使用することもできます。

Open との組み合わせで Network EAP 認証を有効にすることができます（EAP、MAC の組み合わせ（つまり、Network EAP または Network EAP + MAC）、Open、Open + EAP、MAC、EAP + MAC を使用するかどうかは問いません）。Network EAP は LEAP を使用しますが、AP 宣言で LEAP フォーマットのサポートが必要です。この特定の宣言フォーマットをサポートしていないクライアントは、（LEAP または別の EAP メカニズムを使用した）Open モードを使用できます。クライアントは常に、アクセス ポイントでサポートされる最も安全な認証メカニズム、および最も強力な暗号化メカニズムの使用を試みます。ただし、（ブリッジまたはワークグループ ブリッジ モードの）クライアント アクセス ポイントは、クライアント サイドで Network EAP より強力な認証メカニズムを使用するように明示的に設定しない限り、デフォルトで Network EAP を使用します。

SSID を設定する際に、暗号を使用すると、各クライアントの個別のキーを管理できます。このキーの管理方法は、SSID の設定時に定義できます。暗号を使用するようにインターフェイスを設定する場合は、SSID の設定時にキー管理も有効にする必要があります。キー管理は「なし」（セキュリティまたは共有キー セキュリティを使用しない場合）、「必須」（暗号を使用する場合）、または「オプション」（Open とオプション EAP、または共有キーとオプション EAP 認証を使用する場合）に設定できます。各種のキー管理モードの詳細については、この章のキー管理に関する項を参照してください。

暗号化モードについて

暗号化はアクセス ポイントのインターフェイス（VLAN または無線）レベルで定義されて、複数の SSID で共通して使用可能になることから、一般に、暗号化を設定してから、SSID とその認証メカニズムを設定します。

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。通信の暗号化は、攻撃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。

802.11 標準で最初に規定された暗号化メカニズムは WEP（Wired Equivalent Privacy）です。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。802.11 標準では、シスコと一部の他のベンダーが静的 WEP と規定している暗号化を規定しています。このモードでは、WEP キーがクライアントと AP に静的に定義されます。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。

WEP は 802.11 標準で非推奨となっているレガシー プロトコルです。シスコでは可能な場合は常に、これより強力なプロトコル（AES/CCMP など）を使用することを推奨しています。

SSID の認証メカニズムが 802.1x 認証で Extensible Authentication Protocol（EAP）を使用する場合（および WPAv1 または WPAv2 をサポートしていない場合）は、無線ユーザごとに動的 WEP キーを生成できます。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。WPA、WPA2、または CCKM を使用する場合は、暗号スイートを使用する必要があります。WEP 暗号化を使用する場合、WEP 暗号化コマンド（暗号コマンド）を使用して WEP を設定するという選択肢があります。WEP 暗号化コマンドを使用すると、認証や暗号化に静的 WEP キーを使用できます。ただし、このモードでは（802.1x を使用した）ユーザごとのセキュア認証を使用できません。暗号スイートは WEP 暗号化を提供すると同時に、個々のユーザ認証とキー管理も使用できるようにするため、シスコでは、CLI で暗号化モードの暗号コマンドを使用するか、あるいは WEP 暗号化コマンドの代わりに Web ブラウザ インターフェイスで暗号ドロップダウン リストを使用して、WEP を有効にすることを推奨しています。ただし、WEP は IEEE で非推奨となっているプロトコルであるため、シスコではクライアント ドライバが他のより強力なセキュリティ メカニズムをサポートしていない場合に限り、WEP を使用するように推奨しています。推奨されるセキュリティは AES-CCMP 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：米国国立標準技術研究所による *FIPS Publication 197* で定義されている Advanced Encryption Standard（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)　802.11n 改訂は、暗号化なし、または AES-CCMP 暗号化の実装に依存しています。したがって、802.11n 無線では、暗号化なし、または AES-CCMP を設定して 802.11n レートをサポートする必要があります。

- 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。
- 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
  - 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。WPA TKIP は、ほとんどの CKIP 実装を置き換えました。
- 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。CMIC を使用するには Cisco CKIP が必要です。
- 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」セクション（11-7 ページ）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 ローテーションは、キー管理（動的 WEP（802.1x）、EAP を使用した WPA、または事前共有キーなど）を使用する場合のみサポートされます。

(注)　暗号化は、インターフェイスまたは VLAN レベルで設定され、認証はそれぞれの VLAN またはインターフェイスでサポートする SSID ごとに設定されます。このようにして、暗号化と認証が組み合わされます。暗号化と認証の組み合わせの詳細については、第 11 章「認証タイプの設定」を参照してください。

暗号化モードの設定

暗号化は、VLAN または無線インターフェイス レベルで設定されます。有効にする暗号化が、該当する VLAN または無線インターフェイスにマッピングされている SSID で使用する予定の認証メカニズムと互換性があることを確認してください。暗号化と認証方式の互換性の詳細については、認証および暗号化メカニズムについてを参照してください。

(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。

静的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。 2.4 GHz 無線および 2.4 GHz 802.11n 無線は 0 です。 5 GHz 無線および 5 GHz 802.11n 無線は 1 です。

	コマンド	目的
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。VLAN ごとに最大 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) このコマンドで入力したキー文字列が暗号化された文字列であるか、プレーン テキスト キーであるかどうかを指定します。プレーン テキスト キーは、Enter キーを押すと暗号化されます。 • (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 (キー ハッシュ) 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)　CMIC を使用した静的 WEP の設定はサポートされていません。 (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」セクション (10-10 ページ) 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 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 ローテーションは、キー管理（動的 WEP（802.1x）、EAP を使用した WPA、または事前共有キーなど）を使用する場合のみサポートされます。

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る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	—	not set	—	not set
4	—	not set	—	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。2.4 GHz 無線は Radio 0、5 GHz 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 | ckip-cmic | cmic | tkip | wep128 | wep40}**	必要な保護が含まれる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）暗号タイプを有効にする VLAN を選択します。 • 必要な暗号オプションを選択します。複数の暗号を選択できます。 次の点に注意してください。 • 2 つまたは 3 つの要素で暗号スイートを有効にすると、各クライアントは、インターフェイスで有効にされていて、そのクライアントがサポートする最も強力な暗号化メカニズムを使用します。ブロードキャスト キーは、すべてのクライアントがサポートする要素を使用します。詳細については、認証および暗号化メカニズムについてを参照してください。 • **ckip** 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。 • 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。 • 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。 • 暗号化モード **TKIP + WEP 128** または **TKIP + WEP 40** を設定するには、WPA キー管理をオプションとして設定する必要があります。
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。

WPA または 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 • encryption mode aes
WPA	• encryption mode ciphers tkip • encryption mode ciphers tkip wep128 • encryption mode ciphers tkip wep40 • encryption mode ciphers eas (注)　WPA がオプションとして設定されている場合、encryption mode ciphers tkip wep128 および tkip wep-40 だけを使用できます。

(注)　キー管理として WPA および CCKM を使用している場合は、tkip および aes の暗号方式だけがサポートされます。キー管理として CCKM だけを使用している場合は、ckip、cmic、ckip-cmic、tkip、wep、および aes の各暗号方式がサポートされます。

(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 の説明と認証済みキー管理の設定方法の詳細は、「WPA キー管理の使用」セクション（11-7 ページ）を参照してください。

(注)　Wi-Fi 認定アクセス ポイントは、WPA/TKIP 設定をサポートしなくなりました。後方互換性を確保して以前の TKIP 専用デバイスのアソシエーションを可能にするために、TKIP は WPA2/AES との組み合わせでのみ使用できます。WPA バージョン 1 オプションは認証キー管理の wpa cli から削除されたため、このインターフェイスでの TKIP の設定はサポートされません。

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 ローテーションは、キー管理（動的 WEP（802.1x）、EAP を使用した WPA、または事前共有キーなど）を使用する場合のみサポートされます。

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。 2.4 GHz 無線および 2.4 GHz 802.11n 無線は 0 です。 5 GHz 無線および 5 GHz 802.11n 無線は 1 です。
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。

	コマンド	目的
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
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。