CHAPTER 5

セキュリティ機能

この章では、セキュリティ機能について説明します。この章の内容は、次のとおりです。

- 概要（P. 5-2）
- 静的 WEP キー（P. 5-3）
- EAP（静的 WEP キーまたは動的 WEP キーで使用する場合）（P. 5-3）
- 新しい WEP キー セキュリティ機能（P. 5-11）
- セキュリティ機能の同期（P. 5-13）

概要

Wired Equivalent Privacy（WEP）暗号キーを使用してデータを暗号化することで、無線ネットワーク経由で転送されるデータを保護できます。WEP 暗号化では、送信側のデバイスが WEP キーで各パケットを暗号化し、受信側のデバイスが同じキーを使用して各パケットを復号化します。

転送データの暗号化および復号化に使用される WEP キーは、アダプタに静的に関連付けることも、EAP 認証プロセスの一部として動的に作成することもできます。使用する WEP キーのタイプを決定するには、以下の「静的 WEP キー」および「EAP（静的 WEP キーまたは動的 WEP キーで使用する場合）」が参考になります。EAP を使用した動的 WEP キーでは、静的 WEP キーよりも強固なセキュリティが確保されます。

WEP キーの長さは、静的または動的にかかわらず、40 ビットまたは 128 ビットです。128 ビットの WEP キーでは、40 ビットのキーよりも高いセキュリティが得られます。

（注）　WEP キーをさらに安全にする 3 つの機能に関する情報は、「新しい WEP キー セキュリティ機能」の項（P. 5-11）を参照してください。

静的 WEP キー

無線ネットワーク内の各デバイス（またはプロファイル）は、最大 4 つの WEP キーに割り当てることができます。適切なキー（相互通信を行うすべてのデバイスで同一の WEP キー）で暗号化されていないパケットを受信すると、デバイスはそのパケットを廃棄し、宛先に送信しません。

静的 WEP キーは、書き込み専用の一時的なキーなので、クライアント アダプタから再び読み取ることはできず、クライアント アダプタの電源が切られたり Windows デバイスが再度ブートされると失われます。キーは一時的なものですが、静的 WEP キーは、Windows デバイスのレジストリに保存されるので、クライアント アダプタを挿入するたび、あるいは Windows デバイスを再度ブートするたびに入力し直す必要はありません。セキュリティ上の理由により、静的 WEP キーは暗号化されて保存されます。ドライバは、クライアント アダプタのレジストリ パラメータをロードして読み取ると、静的 WEP キーを検出し、復号化して、アダプタの揮発性メモリに保存します。

Security タブ ウィンドウでは、クライアント アダプタに設定されている現在の WEP キーを確認して、新しい WEP キーの割り当てや既存の WEP キーの上書きができます。また、静的 WEP キーを有効または無効にすることもできます。その手順は、「新しい静的 WEP キーの入力」の項（P. 4-16）または「静的 WEP の無効化」の項（P. 4-17）を参照してください。

EAP（静的 WEP キーまたは動的 WEP キーで使用する場合）

無線 LAN のセキュリティに関する新しい規格は Institute of Electrical and Electronics Engineers（IEEE; 電気電子学会）で定義され、*802.1X for 802.11*、または単に *802.1X* と呼ばれています。802.1X とそのプロトコルである拡張認証プロトコル（EAP）をサポートしているアクセス ポイントは、無線クライアントと認証サーバ間のインターフェイスとして機能します。認証サーバとは、アクセス ポイントが有線ネットワークを介して通信する RADIUS サーバなどを指します。

ACAT では、次の 3 つの 802.1X 認証タイプから認証タイプを選択して、Windows オペレーティング システムで使用できます。

- **LEAP**：この認証タイプは、Windows 95、98、NT、2000、Me、および XP のほか、Windows 以外のシステムでも使用できます。LEAP のサポートは、Windows オペレーティング システムではなく、クライアント アダプタのファームウェアと、そのファームウェアをサポートするシスコのソフトウェアによって提供されます。LEAP をサポートする RADIUS サーバには、Cisco Secure ACS リリース 2.6 以降、Cisco Access Registrar リリース 1.7 以降、Funk Software の Steel-Belted RADIUS リリース 3.0 以降などがあります。

  LEAP は、ACAT を使用して、特定のプロファイルに対して有効または無効にできます。有効にすると、多数の設定オプションが利用可能になります。たとえば、ユーザ名とパスワードをいつ、どのように入力して認証プロセスを開始するかを設定できます。

  ユーザ名とパスワードは、クライアント アダプタがアクセス ポイント経由で RADIUS サーバとの相互認証を実行するために使用されます。ユーザ名とパスワードはクライアント アダプタの揮発性メモリに保存されるため、一時的なものです。したがって、クライアント アダプタを取り出したり、システムの電源を切断したりして、アダプタの電源を切断した場合は、そのたびに再入力する必要があります。

- **EAP-FAST**：この認証タイプ（Flexible Authentication via Secure Tunneling）は、Windows 2000 および XP で使用できます。EAP-FAST は、Windows オペレーティング システムではなく、クライアント アダプタのファームウェアと、そのファームウェアをサポートするシスコのソフトウェアでサポートされます。EAP-FAST をサポートする RADIUS サーバには、Cisco Secure ACS リリース 3.2.3 以降があります。

（注）　サポート対象でないオペレーティング システムで、EAP-FAST が指定されているプロファイルのインストールに失敗しても、Install Wizard からエラーは通知されません。

EAP-FAST は、ACAT を使用して、特定のプロファイルに対して有効または無効にできます。また、インストール時に EAP-FAST セキュリティ モジュールを選択した場合は、ACU を使用できます。EAP-FAST を有効にすると、多数の設定オプションが利用可能になります。たとえば、ユーザ名とパスワードをいつ、どのように入力して認証プロセスを開始するか、自動または手動の PAC（Protected Access Credentials）プロビジョニングを使用するかどうかなどを設定できます。

ユーザ名、パスワード、および PAC は、クライアント アダプタがアクセス ポイント経由で RADIUS サーバとの相互認証を実行するために使用されます。保存されている EAP-FAST クレデンシャルを使用するようアダプタを設定しない限り、クライアント アダプタを挿入するたび、あるいは Windows デバイスを再度ブートするたびに、ユーザ名とパスワードを入力し直す必要があります。

PAC は Cisco Secure ACS で作成され、ID で識別されます。ユーザは自分の PAC のコピーを Cisco Secure ACS から取得します。その PAC は、ID によって ACAT または ACU で作成されたプロファイルにリンクされています。手動 PAC プロビジョニングが有効な場合は、PAC ファイルをサーバから手動でコピーし、ACU を使用してクライアント デバイスにインポートします。PAC の保管には、次のルールが適用されます。

- 多くの場合、PAC は Windows ログオン ユーザ単位で別々にプロビジョニングされ保存されます。こうしたユーザ単位の PAC は、他のユーザからは見えません。
- 手動プロビジョニングを使用するようにプロファイルが設定されている場合、各ユーザは、ACU を使用して、そのプロファイルに対して自身の PAC を手動でプロビジョニングする必要があります。
- PAC ファイルは、ACU のインポート機能を利用して追加または入れ替えができますが、削除やエクスポートはできません。
- 保存されている EAP-FAST ユーザ名とパスワードを使用して設定されているプロファイルの場合、PAC はユーザ単位ではなく、すべてのユーザが共有するグローバル PAC 領域に保存されます。ACU で No Network Connection Unless User Is Logged In チェックボックスをオフにすると、グローバル PAC も有効になります。これらのグローバル PAC は、ACU を使用することですべてのユーザがインポートして使用できます。

（注）　ACAT で Use Saved Username and Password チェックボックスをオンにすると、ACU でこのオプションが有効になります。ACU を使用して、EAP-FAST のユーザ名とパスワードのパラメータを入力する必要があります。

（注）　また、PAC は、Novell Network ログイン プロンプト、または EAP-FAST サプリカントとクレデンシャルを共有しないその他のサード パーティ製ログイン アプリケーションを使用しているコンピュータ上にもグローバルに保存されます。

EAP-FAST 認証は、無線 LAN 経由で次のユーザ データベースをサポートするように設計されています。

- Cisco Secure ACS 内部ユーザ データベース
- Cisco Secure ACS ODBC ユーザ データベース
- Windows NT/2000/2003 ドメイン ユーザ データベース
- LDAP ユーザ データベース

NDS などの LDAP ユーザ データベースは、手動 PAC プロビジョニングのみをサポートしています。一方、他の 3 つのユーザ データベースは自動および手動 PAC プロビジョニングの双方をサポートしています。

（注）　インストール時に EAP-FAST セキュリティ モジュールを選択しなかった場合は、ACU で EAP-FAST オプションを使用できません。EAP-FAST を有効または無効に設定するには、ACAT または Install Wizard をもう一度実行して EAP-FAST を選択する必要があります。EAP-FAST は、ACAT および Install Wizard バージョン 1.3 以降でサポートされています。

- **EAP**：このオプションを選択すると、使用しているオペレーティング システムでサポートされているあらゆる 802.1X 認証タイプを使用できます。たとえば、オペレーティング システムで 802.1X サプリカントが使用されている場合、EAP-TLS 認証についてはネイティブ サポート、PEAP および EAP-SIM 認証については一般的なサポートが提供されます。

（注）　EAP-TLS、PEAP、または EAP-SIM を使用するには、Microsoft 802.1X サプリカント、および PEAP セキュリティ モジュールまたは EAP-SIM セキュリティ モジュールをインストールする必要があります。その上で、ACAT または ACU を使用してクライアント アダプタを設定し、目的の認証タイプを Windows で有効にして、Network-EAP をアクセス ポイントで有効にする必要があります。

  - **EAP-TLS**：EAP-TLS は、オペレーティング システムにより有効または無効にされ、クライアント アダプタおよび RADIUS サーバから取り出された動的セッションベース WEP キーを使用してデータを暗号化します。EAP-TLS を有効にした場合は、オペレーティング システムでいくつかのパラメータを設定する必要があります。

    EAP-TLS をサポートする RADIUS サーバには、Cisco Secure ACS リリース 3.0 以降、Cisco Access Registrar リリース 1.8 以降があります。

（注）　EAP-TLS　では、証明書を使用する必要があります。証明書のダウンロードとインストールは、Microsoft の資料を参照してください。

  - **Protected EAP**（または **PEAP**）：PEAP 認証は、無線 LAN 経由で One-Time Password（OTP; ワンタイム パスワード）、Windows NT ドメインまたは Windows 2000 ドメイン、LDAP ユーザ データベースをサポートするように設計されています。EAP-TLS 認証がベースとなっていますが、認証にクライアント証明書ではなくパスワードまたは PIN を使用します。また、オペレーティング システムにより有効または無効にされ、クライアント アダプタおよび RADIUS サーバから取り出された動的セッションベース WEP キーを使用してデータを暗号化します。PEAP 認証を使用する場合、ネットワークで OTP ユーザ データベースが使用されているときには、ハードウェア トークン パスワードまたはソフトウェア トークン PIN を入力し、EAP 認証プロセスを開始してネットワークにアクセスする必要があります。ネットワークで Windows NT または 2000 のドメイン ユーザ データベースあるいは LDAP ユーザ データベース（NDS など）が使用されている場合は、ユーザ名、パスワード、およびドメイン名を入力して認証プロセスを開始する必要があります。

    PEAP 認証をサポートする RADIUS サーバには、Cisco Secure ACS リリース 3.1 以降、Cisco Access Registrar リリース 3.5 以降などがあります。

（注）　Windows XP の Service Pack 1 と Windows 2000 向け Microsoft 802.1X サプリカントには、Microsoft の PEAP サプリカントが収められています。これは Windows のユーザ名とパスワードだけをサポートし、シスコの PEAP サプリカントと同時に使用することはできません。シスコの PEAP サプリカントを使用するには、Windows XP の Service Pack 1 または Windows 2000 向け Microsoft 802.1X サプリカントをインストールした後で Install Wizard をインストールします。この順序でインストールしない場合、シスコの PEAP サプリカントは Microsoft の PEAP サプリカントで上書きされます。

- **EAP-SIM**：EAP-SIM 認証は、公衆無線 LAN で使用できるように設計されており、PCSC 準拠のスマートカード リーダーが装備されているクライアントが必要です。Install Wizard ファイルに含まれる EAP-SIM サプリカントがサポートするのは Gemplus SIM+ カードだけですが、標準の GSM-SIM カードや最新バージョンの EAP-SIM プロトコルをサポートする最新のサプリカントが入手可能です。新しいサプリカントは、次の URL の ftpeng File Transfer Protocol（FTP; ファイル転送プロトコル）サーバからダウンロードできます。

  ftp://ftpeng.cisco.com/ftp/pwlan/eapsim/CiscoEapSim.dll

  EAP-SIM 認証を正常に実行するためには上記の要件を満たす必要がありますが、それだけでは不十分です。通常は、ネットワーク内で EAP-SIM 認証をサポートする WLAN サービス プロバイダとサービス契約を結ぶ必要もあります。また、PCSC スマートカード リーダーは標準 GSM-SIM カードまたはチップを読み取ることができる場合もありますが、通常、EAP-SIM 認証では、サービス プロバイダが WLAN サービス用の GSM 携帯電話のアカウントを提供する必要があります。

  EAP-SIM は、オペレーティング システムにより有効または無効にされ、クライアント アダプタおよび RADIUS サーバから取り出された動的セッションベース WEP キーを使用してデータを暗号化します。EAP-SIM では、SIM カードとの通信に際して、ユーザ検証コード、または PIN の入力が必要です。PIN はコンピュータに格納しておくことができますが、リブート後または認証のたびに PIN を入力するような設定も可能です。

  EAP-SIM をサポートする RADIUS サーバには、Cisco Access Register リリース 3.0 以降があります。

（注）　EAP-TLS、PEAP、および EAP-SIM 認証は、オペレーティング システムでは有効、ACU では無効になっているので、ACU でプロファイルを切り替えることによってこれらの認証タイプを切り替えることはできません。ACU でホストベース EAP を使用するプロファイルを作成できますが、Windows で特定の認証タイプを有効にする必要があります（Windows で Microsoft 802.1X サプリカントが使用されている場合）。また、Windows で一度に設定できるのは、1 つの認証タイプだけです。ACU でホストベース EAP を使用するプロファイルが複数ある場合に別の認証タイプを使用するには、ACU でプロファイルを切り替えた後、Windows で認証タイプを変更する必要があります。

アクセス ポイントで Network-EAP または Require EAP を有効にし、LEAP、EAP-FAST、EAP-TLS、PEAP、または EAP-SIM 用にクライアント アダプタを設定すると、ネットワークに対する認証は、次の順序で実行されます。

1. クライアントがアクセス ポイントにアソシエートし、認証プロセスを開始します。

（注）　クライアントと　RADIUS　サーバの間で認証が成功するまで、クライアントはネットワークにフル アクセスできません。

2. クライアントと RADIUS サーバは、アクセス ポイント経由で通信し、認証用の共有秘密情報を使用して認証プロセスを実行します。この共有秘密情報とは、LEAP、EAP-FAST、および PEAP ではパスワード、EAP-TLS では証明書、EAP-SIM では SIM カードおよびサービス プロバイダの Authentication Center に保存されている内部キーです。このプロセス実行中に、パスワード、証明書、または内部キーが送信されることはありません。
3. 認証が成功すると、クライアントと RADIUS サーバは、クライアントに固有の動的なセッションベース WEP キーを取り出します。
4. RADIUS サーバは、有線 LAN 上の安全なチャネルを使用してアクセス ポイントにキーを送信します。
5. セッションの間、アクセス ポイントとクライアントはこのキーを使用して、相互に伝送するすべてのユニキャスト パケットの暗号化または復号化を行います。また、ブロードキャスト パケットの暗号化や複合化が設定されているアクセス ポイントの場合は、それらの暗号化や複合化も実行します。

LEAP を有効にする手順は「LEAP の有効化」の項（P. 4-17）を、EAP-FAST を有効にする手順は「EAP-FAST の有効化」の項（P. 4-21）を、EAP-TLS、PEAP、または EAP-SIM を有効にする手順は「ホストベース EAP の有効化」の項（P. 4-26）をそれぞれ参照してください。

802.1X 認証の詳細は、IEEE 802.11 規格を参照してください。RADIUS サーバの詳細は、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt2/scrad.htm

Wi-Fi Protected Access（WPA）

Wi-Fi Protected Access（WPA）は、既存および将来の無線 LAN システムのデータ保護と、アクセス制御のレベルを大幅に向上する、標準の、相互運用性の優れたセキュリティ強化法です。WPA は、現在策定中の IEEE 802.11i 規格のサブセットで、この規格と互換性があります。WPA は、TKIP（Temporal Key Integrity Protocol）を使用してデータ保護し、802.1X を使用して認証キーを管理します。

WPA では、WPA と WPA-Pre-shared key（WPA-PSK）の 2 種類の相互に排他的なキー管理がサポートされています。クライアントと認証サーバは、WPA を使用してキーを管理し、EAP 認証方式で相互認証を行い、Pairwise Master Key（PMK）を生成します。サーバは WPA を使用し、PMK を動的に生成してアクセス ポイントに渡します。ただし、そのためには、WPA-PSK を使用してクライアントとアクセス ポイントの両方で事前共有キーを設定し、それが PMK として使用されるように設定します。

（注）　WPA で使用できるのは、Windows 2000 または Windows XP が動作し、LEAP、EAP-FAST、またはホストベース EAP 認証を実行しているコンピュータにインストールされた、350 シリーズまたは CB20A のいずれかのカードだけです。

WPA は、Install Wizard バージョン 1.2 以降でサポートされています。ただし、ホストベース EAP を WPA で使用する場合は、WPA をサポートするホスト サプリカントもインストールする必要があります。Cisco Aironet クライアント アダプタで使用するホスト サプリカントとして、以下をお勧めします。

- Funk Odyssey Client サプリカント リリース 2.2（Windows 2000 の場合）
- Windows XP Service Pack 1 および Microsoft サプリカント Q815485（Windows XP 用）

WPA で LEAP を有効にする手順は「LEAP の有効化」の項（P. 4-17）を、WPA で EAP-TLS、PEAP、または EAP-SIM を有効にする手順は「ホストベース EAP の有効化」の項（P. 4-26）をそれぞれ参照してください。

WPA はアクセス ポイントでも有効にする必要があります。アクセス ポイントでは、Cisco IOS リリース 12.2(11)JA 以降を使用して WPA を有効化している必要があります。この機能を有効にする手順は、アクセス ポイントの資料を参照してください。

高速ローミング（CCKM）

クライアント デバイス上で実行されるアプリケーションによっては、アクセス ポイント間の高速ローミングが必要です。たとえば、音声アプリケーションでは、会話が遅延したり途切れたりすることを防ぐために、シームレスなローミングが必要です。高速ローミングは、LEAP 対応のクライアントの場合は Install Wizard バージョン 1.1 以降で、EAP-FAST 対応のクライアントの場合は Install Wizard 1.6 以降でサポートされています。

通常の操作では、LEAP または EAP-FAST 対応クライアントは、メイン RADIUS サーバとの通信のような完全な LEAP または EAP-FAST 認証を実行することにより、新しいアクセス ポイントとの相互認証を行います。ただし、無線 LAN を高速ローミング用に設定すると、LEAP または EAP-FAST 対応クライアントが RADIUS サーバによる再認証を受けることなく、あるアクセス ポイントから別のアクセス ポイントへ安全にローミングできます。Wireless Domain Services（WDS）用に設定されたアクセス ポイントは、Cisco Centralized Key Management（CCKM）を使用し、高速キー再生成によってクライアント デバイスがあるアクセス ポイントから別のアクセス ポイントへ 150 ミリ秒（ms）以内にローミングできるようにします。高速ローミングでは、無線 Voice over IP（VoIP）、エンタープライズ リソース プラニング（ERP）、または Citrix ベースのソリューションなどの時間が重要視されるアプリケーションで、目に見えた遅れはなくなります。

高速ローミング機能は、インストールされているソフトウェアに応じて、次の 2 つの異なる方法によりクライアント アダプタ上で有効にできます。

- クライアント アダプタ ファームウェア バージョン 5.40.xx （Install Wizard 1.3 に付属）を使用している場合は、ACAT または Aironet Client Utility（ACU）6.3 で高速ローミングを有効にする必要があります。詳細は、「LEAP の有効化」の項（P. 4-17）の ステップ 12 、または「EAP-FAST の有効化」の項（P. 4-21）のステップ 13 を参照してください。
- クライアント アダプタ ファームウェア バージョン 5.20.17 （Install Wizard 1.1 に付属）を使用している場合、高速ローミングは自動的にサポートされます。

高速ローミングは、クライアント アダプタで有効になっているかどうかにかかわらず、アクセス ポイントでは有効にする必要があります。

（注）　高速ローミングを有効にするには、アクセス ポイントで Cisco IOS リリース 12.2(11)JA 以降を使用している必要があります。この機能を有効にする手順は、アクセス ポイントの資料を参照してください。

（注）　Microsoft 802.1X サプリカントがコンピュータにインストールされている場合は、この機能を正しく働かせるために、1 つまたは 2 つの Windows パラメータを無効にする必要があります。詳細は、「LEAP の有効化」の手順 13 を参照してください。

LEAP 認証または EAP-FAST 認証に失敗したアクセス ポイントの報告

クライアント アダプタ ファームウェア バージョン 5.02.20 以降および次のアクセス ポイント ソフトウェア リリースでは、LEAP 認証に失敗したアクセス ポイントの検出機能がサポートされています。

- VxWorks リリース 12.00T 以降（340、350、および 1200 シリーズ アクセス ポイント）
- Cisco IOS リリース 12.2(4)JA 以降（1100 シリーズ アクセス ポイント）

これらのいずれかのソフトウェア リリースを実行しているアクセス ポイントでは、バージョン 5.02.20 以降のファームウェアを実行しているクライアントにより、LEAP 認証または EAP-FAST 認証に失敗した他のアクセス ポイントが無線ネットワーク内で発見され、報告されると、システム ログにメッセージが記録されます。

このプロセスは、次のように実行されます。

1. LEAP プロファイルまたは EAP-FAST プロファイルを持つクライアントは、アクセス ポイント A へのアソシエートを試みます。
2. アクセス ポイント A は、LEAP 認証または EAP-FAST を認識できないか、信頼できる LEAP 認証サーバまたは EAP-FAST 認証サーバと通信できないことが原因で、LEAP 認証または EAP-FAST 認証を正常に処理しません。
3. クライアントは、アクセス ポイント A の Media Access Control（MAC; メディア アクセス制御）アドレスと、アソシエーションが失敗した理由を記録します。
4. クライアントは、アクセス ポイント B に正常にアソシエートします。
5. クライアントは、アクセス ポイント A の MAC アドレスと失敗の理由コードをアクセス ポイント B に送信します。
6. アクセス ポイント B は、失敗をシステム ログに記録します。

（注）　クライアント アダプタまたはアクセス ポイントでこの機能を有効にする必要はありません。この機能は両方のデバイスで自動的にサポートされます。ただし、クライアント アダプタとアクセス ポイントで、前述のバージョン以降のファームウェアまたは前述のリリース以降のソフトウェアを使用している必要があります。

新しい WEP キー セキュリティ機能

ここで説明した 3 つのセキュリティ機能（MIC、TKIP、およびブロードキャスト キー ローテーション）は、無線ネットワークの WEP キーに対する巧妙な攻撃を防ぎます。これらの機能は、Install Wizard のファイルに含まれているファームウェアやドライバでサポートされているため、クライアント アダプタで有効にする必要はありません。ただし、アクセス ポイントではこれらの機能を有効にする必要があります。

これらのセキュリティ機能をアクセス ポイントで有効にする手順は、該当のソフトウェアのコンフィギュレーション ガイド、または次の URL にあるインストレーション ガイドやコンフィギュレーション ガイドを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/wireless/index.htm

（注）　340 シリーズまたは 350 シリーズのアクセス ポイントでこれらのセキュリティ機能を有効にするには、VxWorks 11.10T 以降が必要です。これらのセキュリティ機能を有効にする手順は、アクセス ポイントの資料を参照してください。

Message Integrity Check（MIC）

MIC は、暗号化されたパケットへの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、受信側で正規のメッセージとして受信されます。MIC は、数バイトを各パケットに付加することによって、パケットの改ざんを防ぎます。

Status ウィンドウには、MIC が使用中であるかどうかが示され、Statistics ウィンドウには MIC 統計情報が表示されます。

（注）　アクセス ポイントで MIC を有効にする場合は、クライアント アダプタのドライバがこれらの機能をサポートしている必要があります。そうでないと、クライアントはアソシエートできません。

Temporal Key Integrity Protocol（TKIP）Temporal Key Integrity Protocol（TKIP）

この機能は *WEP キー ハッシュ*とも呼ばれます。不正侵入者は、暗号化されたパケットの初期設定ベクトル（IV）を使用して WEP キーを割り出し、WEP を攻撃しようとしますが、TKIP はこの攻撃に対する防御を提供します。TKIP は、不正侵入者が IV を利用して WEP キーを特定する際に利用する、推測可能な値を除去します。また、ユニキャストとブロードキャストの両方の WEP キーを保護します。

（注）　アクセス ポイントで TKIP を有効にする場合は、クライアント アダプタのファームウェアがこれらの機能をサポートしている必要があります。そうでないと、クライアントはアソシエートできません。

（注）　WPA が有効になると TKIP も自動的に有効になり、WPA が無効になると TKIP も無効になります。

ブロードキャスト キー ローテーション

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（マルチキャスト）キーです。ブロードキャスト WEP キー ローテーションを有効にすると、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。この機能を有効にした場合は、LEAP、EAP-TLS、PEAP、または EAP-SIM 認証を使用する無線クライアント デバイスだけがアクセス ポイントにアソシエートできます。静的 WEP（Open 認証または Shared key 認証）を使用したクライアント デバイスは、アソシエートできません。

セキュリティ機能の同期

この項で説明したセキュリティ機能を使用するには、クライアント アダプタおよびそのアソシエート先となるアクセス ポイントの双方を正しく設定する必要があります。表 5-1 では、各セキュリティ機能を使用する上で必要なクライアントおよびアクセス ポイントの設定を示しています。クライアント アダプタのセキュリティ機能のインストールと設定の手順は、第 2 章「Installed Components タブ ウィンドウ」と「Security タブ」の項（P. 4-10）を参照してください。これらの機能をアクセス ポイントで有効にする手順は、アクセス ポイントの資料を参照してください。

表 5-1　クライアントとアクセス ポイントのセキュリティ設定

セキュリティ機能	クライアントの設定	アクセス ポイントの設定
静的 WEP キー（Open 認証を使用）	Static WEP と Open Access Point Authentication を有効化、WEP キーを作成	WEP を設定および有効化、SSID に対して Open 認証を有効化
静的 WEP キー（Shared Key 認証を使用）	Static WEP と Shared Key Access Point Authentication を有効化、WEP キーを作成	WEP を設定および有効化、SSID に対して Shared Key 認証を有効化
LEAP 認証	LEAP セキュリティ モジュールをインストール、LEAP を有効化	WEP を設定および有効化、SSID に対して EAP を有効化
WPA による LEAP 認証	LEAP セキュリティ モジュールをインストール、WPA と LEAP を有効化 （注）　WPA アクセス ポイントと非 WPA アクセス ポイントの両方にクライアントをアソシエートできるようにするには、WPA と非 WPA の両方の認証者に対して　Allow Association を有効にします。	暗号スイートを選択、WEP を設定および有効化、SSID に対して EAP と WPA を有効化 （注）　WPA クライアント アダプタおよび非 WPA クライアント アダプタの両方で SSID を使用できるようにするには、オプションの WPA を有効にします。
EAP-FAST 認証	EAP-FAST セキュリティ モジュールをインストール、EAP-FAST を有効化	WEP を設定および有効化、SSID に対して EAP を有効化
WPA による EAP-FAST 認証	EAP-FAST セキュリティ モジュールをインストール、WPA と EAP-FAST を有効化 （注）　WPA アクセス ポイントと非 WPA アクセス ポイントの両方にクライアントをアソシエートできるようにするには、WPA と非 WPA の両方の認証者に対して　Allow Association を有効にします。	暗号スイートを選択、WEP を設定および有効化、SSID に対して EAP と WPA を有効化 （注）　WPA クライアント アダプタおよび非 WPA クライアント アダプタの両方で SSID を使用できるようにするには、オプションの WPA を有効にします。
EAP-TLS 認証		
ACAT または ACU を使用してクライアント アダプタを設定する場合	ACAT または ACU、および Windows で Host Based EAP と Dynamic WEP を有効化、EAP タイプとして Enable network access control using IEEE 802.1X および Certificates（または Smart Card or other Certificate）を選択	WEP を設定および有効化、SSID に対して EAP と Open Authentication を有効化
Windows XP を使用してクライアント アダプタを設定する場合	Windows で、EAP タイプとして Enable network access control using IEEE 802.1X および Smart Card or other Certificate を選択	WEP を設定および有効化、SSID に対して EAP と Open Authentication を有効化

表 5-1　クライアントとアクセス ポイントのセキュリティ設定（続き）

セキュリティ機能	クライアントの設定	アクセス ポイントの設定
WPA による EAP-TLS 認証		
ACAT または ACU を使用してクライアント アダプタを設定する場合	ACAT または ACU、および Windows で WPA、Host Based EAP、および Dynamic WEP を有効化、EAP タイプとして Enable network access control using IEEE 802.1X および Certificates（または Smart Card or other Certificate）を選択	暗号スイートを選択、WEP を設定および有効化、SSID に対して EAP、Open Authentication、および WPA を有効化 （注）　WPA クライアント アダプタおよび非 WPA クライアント アダプタの両方で SSID を使用できるようにするには、オプションの WPA を有効にします。
Windows XP を使用してクライアント アダプタを設定する場合	Windows で、WPA または WPA-PSK を有効化、EAP タイプとして Enable network access control using IEEE 802.1X および Smart Card or other Certificate を選択	暗号スイートを選択、WEP を設定および有効化、SSID に対して EAP、Open Authentication、および WPA を有効化 （注）　WPA クライアント アダプタおよび非 WPA クライアント アダプタの両方で SSID を使用できるようにするには、オプションの WPA を有効にします。
PEAP 認証		
ACAT または ACU を使用してクライアント アダプタを設定する場合	PEAP セキュリティ モジュールをインストール、ACAT または ACU、および Windows で Host Based EAP と Dynamic WEP を有効化、EAP タイプとして Enable network access control using IEEE 802.1X および PEAP を選択	WEP を設定および有効化、SSID に対して EAP と Open Authentication を有効化
Windows XP を使用してクライアント アダプタを設定する場合	Windows で、EAP タイプとして Enable network access control using IEEE 802.1X および PEAP を選択	WEP を設定および有効化、SSID に対して EAP と Open Authentication を有効化
WPA による PEAP 認証		
ACAT または ACU を使用してクライアント アダプタを設定する場合	ACAT または ACU、および Windows で WPA、Host Based EAP、および Dynamic WEP を有効化、WPA または WPA-PSK を有効化、EAP タイプとして Enable network access control using IEEE 802.1X および PEAP を選択	暗号スイートを選択、WEP を設定および有効化、SSID に対して EAP、Open Authentication、および WPA を有効化 （注）　WPA クライアント アダプタおよび非 WPA クライアント アダプタの両方で SSID を使用できるようにするには、オプションの WPA を有効にします。

表 5-1　クライアントとアクセス ポイントのセキュリティ設定（続き）

セキュリティ機能	クライアントの設定	アクセス ポイントの設定
Windows XP を使用してクライアント アダプタを設定する場合	Windows で、WPA または WPA-PSK を有効化、EAP タイプとして Enable network access control using IEEE 802.1X および PEAP を選択	暗号スイートを選択、WEP を設定および有効化、SSID に対して EAP、Open Authentication、および WPA を有効化 （注）　WPA クライアント アダプタおよび非 WPA クライアント アダプタの両方で SSID を使用できるようにするには、オプションの WPA を有効にします。
EAP-SIM 認証		
ACAT または ACU を使用してクライアント アダプタを設定する場合	EAP-SIM セキュリティ モジュールをインストール、ACAT または ACU、および Windows で Host Based EAP および Dynamic WEP を有効化、EAP タイプとして Enable network access control using IEEE 802.1X（または Enable IEEE 802.1X authentication for the network）および SIM Authentication を選択	WEP を設定および有効化、SSID に対して EAP と Open Authentication を有効化
Windows XP を使用してクライアント アダプタを設定する場合	Windows で、EAP タイプとして Enable network access control using IEEE 802.1X および SIM Authentication を選択	WEP を設定および有効化、SSID に対して EAP と Open Authentication を有効化
WPA による EAP-SIM 認証		
ACAT または ACU を使用してクライアント アダプタを設定する場合	EAP-SIM セキュリティ モジュールをインストール、ACAT または ACU、および Windows で WPA、Host Based EAP、および Dynamic WEP を有効化、WPA または WPA-PSK を有効化、EAP タイプとして Enable network access control using IEEE 802.1X（または Enable IEEE 802.1X authentication for the network）および SIM Authentication を選択	暗号スイートを選択、WEP を設定および有効化、SSID に対して EAP、Open Authentication、および WPA を有効化 （注）　WPA クライアント アダプタおよび非 WPA クライアント アダプタの両方で SSID を使用できるようにするには、オプションの WPA を有効にします。
Windows XP を使用してクライアント アダプタを設定する場合	Windows で、WPA または WPA-PSK を有効化、EAP タイプとして Enable network access control using IEEE 802.1X および SIM Authentication を選択	暗号スイートを選択、WEP を設定および有効化、SSID に対して EAP、Open Authentication、および WPA を有効化 （注）　WPA クライアント アダプタおよび非 WPA クライアント アダプタの両方で SSID を使用できるようにするには、オプションの WPA を有効にします。

表 5-1　クライアントとアクセス ポイントのセキュリティ設定（続き）

セキュリティ機能	クライアントの設定	アクセス ポイントの設定
高速ローミング（CCKM）	LEAP を有効化、Allow Fast Roaming (CCKM) を選択	Cisco IOS Release 12.2(11)JA 以降を使用、暗号スイートを選択、SSID に対して EAP および CCKM を有効化 （注）　WPA クライアント アダプタおよび非 WPA クライアント アダプタの両方で SSID を使用できるようにするには、オプションの WPA を有効にします。
LEAP 認証に失敗したアクセス ポイントの報告	バージョン 5.02.20 以降のファームウェアでは自動的に有効化されるので、設定は不要	次のリリースのソフトウェアでは自動的に有効化されるので、設定は不要 • VxWorks リリース 12.00T 以降（340、350、および 1200 シリーズ アクセス ポイント） • Cisco IOS リリース 12.2(4)JA 以降
MIC	Install Wizard ファイル付属のファームウェアにより自動的に有効化されるので、設定は不要	完全な暗号化で WEP を設定および有効化、MIC を MMH に設定、Use Aironet Extensions を Yes に設定
TKIPTKIP	Install Wizard ファイル付属のファームウェアにより自動的に有効化されるので、設定は不要	WEP を設定および有効化、TKIP を Cisco に設定、Use Aironet Extensions を Yes に設定
ブロードキャスト キー ローテーション	LEAP、EAP-TLS、PEAP、または EAP-SIM を有効化、Install Wizard ファイル付属のファームウェアを使用	WEP を設定および有効化、Broadcast WEP Key Rotation Interval を 0 以外の値に設定
LEAP 認証に失敗したアクセス ポイントの報告	バージョン 5.02.17 以降のファームウェアでは自動的に有効化されるので、設定は不要	次のリリースのソフトウェアでは自動的に有効化されるので、設定は不要 • VxWorks リリース 12.00T 以降（340、350、および 1200 シリーズ アクセス ポイント） • Cisco IOS リリース 12.2(4)JA 以降
高速で安全なローミング	LEAP を有効化、ファームウェア バージョン 5.20.17 以降を使用	Cisco IOS Release 12.2(11)JA 以降を使用、暗号スイートを選択、EAP または CCKM で Open 認証をを有効化 （注）　802.1x クライアントおよび非 802.1x クライアントの両方で SSID を使用できるようにするには、オプションの CCKM を有効にします。