Cisco Aironet ワイヤレス セキュリティに関する FAQ

内容

概要

このドキュメントでは、Cisco Aironet ワイヤレス セキュリティに関して最もよく寄せられる質問（FAQ）について説明します。

一般的な FAQ

Q.ワイヤレスセキュリティの必要性は何ですか。

A.有線ネットワークでは、データはエンドデバイスを接続するケーブルに残ります。しかし、無線ネットワークでは、RF 信号をブロードキャストすることにより、データを空間で送受信します。WLAN で使用しているブロードキャストの性質により、データにアクセスまたはデータを破壊しようとするハッカーや侵入者からの大きな脅威が存在します。この問題を軽減するために、すべての WLAN には次の機能が必要とされます。

1. ネットワーク リソースへの不正アクセスを防ぐためのユーザ認証。
2. 送信されるデータの整合性とプライバシーを保護するためのデータ プライバシー（暗号化とも呼ばれます）。

Q.無線LANの802.11規格で定義されている認証方式にはどのようなものがありますか。

A. 802.11標準では、無線LANクライアントの認証に次の2つのメカニズムが定義されています。

1. オープン認証
2. 共有キー認証

この他に一般的に使用されているメカニズムが 2 種類あります。

1. SSID ベースの認証
2. MAC アドレス認証

Q.オープン認証とは何ですか。

A.オープン認証は基本的にヌル認証アルゴリズムです。つまり、ユーザまたはマシンの検証は行われません。オープン認証では、どのデバイスも Access Point (AP; アクセス ポイント) に対して認証要求を出せます。 オープン認証では、クライアントに AP との関連付けを許可するために、クリアテキスト転送が使用されます。暗号化がイネーブルになっていない場合、WLAN の SSID を知っているあらゆるデバイスが、このネットワークにアクセスできます。AP で Wired Equivalent Privacy (WEP) が有効になっていれば、WEP キーがアクセス コントロールの手段となります。正しい WEP キーを持たないデバイスは、認証が成功した場合でも AP 経由でデータを送信できません。また、これらのデバイスでは AP が送信したデータを復号化することもできません。

Q.クライアントをAPに関連付けるためにオープン認証にはどのような手順が必要ですか。

1. クライアントは AP にプローブ要求を送ります。
2. AP はプローブ応答を返します。
3. クライアントは複数の AP からの応答を評価して、最適な AP を選択します。
4. クライアントは AP に認証要求を送ります。
5. AP は認証を確認して、クライアントを登録します。
6. その後、クライアントが AP に関連付け要求を送ります。
7. AP は関連付けを確認して、クライアントを登録します。

Q.オープン認証の長所と短所は何ですか。

A.オープン認証の長所と短所は次のとおりです。

利点：オープン認証は基本的な認証メカニズムであり、複雑な認証アルゴリズムをサポートしていない無線デバイスでも使用できます。802.11 仕様での認証は、コネクション型です。認証要求で、デバイスがネットワークにすばやくアクセスできる設計です。このような場合に、オープン認証を使用できます。

短所：オープン認証には、クライアントが正当なクライアントであって、ハッカー クライアントではないことをチェックする方法はありません。オープン認証で WEP 暗号化を使用しないと、WLAN の SSID を知っているすべてのユーザがネットワークにアクセスできます。

Q.共有キー認証とは何ですか。

A.共有キー認証はオープン認証と同様に動作しますが、大きな違いがあります。WEP 暗号化キーと一緒にオープン認証を使用する場合、WEP キーはデータの暗号化と復号化に使用されますが、認証手順では使用されません。共有キー認証では、認証に WEP 暗号化を使用します。オープン認証と同様に、共有キー認証ではクライアントと AP が同じ WEP キーを持つ必要があります。共有キー認証を使用する AP では、クライアントにチャレンジ テキスト パケットを送信します。クライアントはローカルで設定された WEP キーを使用してチャレンジ テキストを暗号化し、これに続く認証要求で返します。この認証要求を AP で復号化して、元のチャレンジ テキストが得られれば、AP はクライアントにアクセス権を与える認証応答を返します。

Q.クライアントをAPに関連付けるために共有キー認証にはどのような手順が必要ですか。

1. クライアントは AP にプローブ要求を送ります。
2. AP はプローブ応答を返します。

3. クライアントは複数の AP からの応答を評価して、最適な AP を選択します。
4. クライアントは AP に認証要求を送ります。
5. AP は暗号化されていないチャレンジ テキストを含む認証応答を送ります。
6. クライアントは WEP キーを使用してチャレンジ テキストを暗号化し、このテキストを AP に送ります。
7. AP は暗号化されていないチャレンジ テキストと、暗号化されたチャレンジ テキストを比較します。認証を復号化でき、元のチャレンジ テキストが得られれば、認証は成功です。

共有キー認証では、クライアントの関連付けプロセスの際に WEP 暗号化を使用します。

Q.共有キー認証の長所と短所は何ですか。

A.共有キー認証では、クライアントとAPはチャレンジテキスト（クリアテキスト）と暗号化されたチャレンジを交換します。したがって、このような認証タイプは、man-in-the-middle（中間者）攻撃に対しては脆弱です。ハッカーは暗号化されていないチャレンジと暗号化されたチャレンジを傍受して、この情報から WEP キー（共有キー）を抽出します。ハッカーが WEP キーを知ってしまうと、この認証メカニズム全体が無力化され、ハッカーが WLAN ネットワークにアクセスできるようになります。これは共有キー認証の大きな欠点です。

Q. MACアドレス認証とは何ですか。

A. 802.11標準ではMACアドレス認証は指定されていませんが、WLANネットワークでは一般的にこの認証技術が使用されます。したがって、シスコを含むほとんどの無線デバイス ベンダーでは、MAC アドレス認証をサポートしています。

MAC アドレス認証では、クライアントは自身の MAC アドレスに基づいて認証を受けます。クライアントの MAC アドレスは、AP にローカルに保存されている MAC アドレス リスト、または外部の認証サーバに保存されている MAC アドレス リストと照らし合わせて確認されます。MAC 認証は、802.11 で提供されているオープン認証や共有キー認証よりも強固なセキュリティ メカニズムです。この認証方法では、不正なデバイスがネットワークにアクセスできる可能性が非常に小さくなります。

Q. Cisco IOSソフトウェアリリース12.3(8)JA2でMAC認証がWi-Fi Protected Access(WPA)と連携しないのはなぜですか。

A. MAC認証の唯一のセキュリティレベルは、クライアントのMACアドレスを許可されたMACアドレスのリストと照合することです。これは非常に脆弱であると考えられています。以前の Cisco IOS ソフトウェア リリースでは、MAC 認証と WPA を設定して、情報を暗号化できていました。しかし、WPA 自体に照合する MAC アドレスがあるため、新しい Cisco IOS ソフトウェア リリースではこの種の設定は許可されず、セキュリティ機能の改善だけが行われています。

Q.ワイヤレスデバイスを認証する方法としてSSIDを使用できますか。

A. Service Set Identifier(SSID)は、WLANがネットワーク名として使用する、大文字と小文字を区別する一意の英数字の値です。SSID は、複数のワイヤレス LAN を論理的に区別するためのメカニズムです。SSID にはデータ プライバシー機能はなく、また実際にはクライアントの AP に対する認証を行うものではありません。SSID の値は、ビーコン、プローブ要求、プローブ応答およびその他のタイプのフレームで、クリア テキストとしてブロードキャストされます。802.11 ワイヤレス LAN パケット アナライザ（たとえば Sniffer Pro など）を使用すると、盗聴者は SSID を簡単に判別できます。シスコでは、SSID を WLAN ネットワークのセキュリティ保護の方式として使用することを推奨しません。

Q. SSIDブロードキャストを無効にすると、WLANネットワークのセキュリティを強化できますか。

A. SSIDブロードキャストを無効にすると、ビーコンメッセージでSSIDが送信されません。しかし、プローブ要求やプローブ応答などの他のフレームでは、引き続き SSID がクリア テキストで使用されます。したがって、SSID を無効にしてもワイヤレス セキュリティを高めることはできません。SSID は、セキュリティ メカニズムとして設計されておらず、セキュリティ メカニズムとしての使用は意図されていません。さらに、SSID ブロードキャストをディセーブルにすると、さまざまなクライアントが配置されている場合に Wi-Fi の相互運用性の問題が生じる可能性があります。したがって、シスコでは、SSID をセキュリティ モードとして使用することを推奨しません。

Q. 802.11セキュリティで発見された脆弱性は何ですか。

A. 802.11セキュリティの主な脆弱性は次のとおりです。

- デバイスのみ認証の脆弱性：ユーザではなく、クライアント デバイスが認証されます。
- データ暗号化の脆弱性：Wired Equivalent Privacy（WEP）は、データ暗号化の手段として効果がないことが明らかになっています。
- メッセージの完全性なし：Integrity Check Value（ICV; 整合性チェック値）は、メッセージ整合性を確保する手段として効果がないことが明らかになっています。

Q. WLANにおける802.1x認証の役割は何ですか。

A. 802.11標準で定義されている元の認証方式の欠点とセキュリティの脆弱性に対処するために、802.1X認証フレームワークが802.11 MACレイヤのセキュリティ拡張のドラフトに含まれています。IEEE 802.11 Task Group i（TGi; タスク グループ i）では現在、これらの拡張を開発中です。802.1X フレームワークでは、通常では上位レイヤでのみ使用される拡張性の高い認証をリンク層で行います。

Q. 802.1xフレームワークで定義されている3つのエンティティは何ですか。

A.802.1x フレームワークでは、WLAN ネットワーク上のデバイスを検証するために、3 つの論理的な要素が必要です。

1. **サプリカント**：サプリカントは無線 LAN クライアント上にあり、EAP クライアントとも呼ばれます。
2. **オーセンティケータ**：オーセンティケータは AP 上にあります。
3. **認証サーバ**：認証サーバは、RADIUS サーバ上にあります。

Q. 802.1x認証フレームワークを使用すると、ワイヤレスクライアント認証はどの

ように行われますか。

A.無線クライアント（EAPクライアント）がアクティブになると、無線クライアントはオープン認証または共有認証を使用して認証します。802.1x はオープン認証とともに動作し、クライアントが AP への関連付けに成功した後に開始されます。クライアント ステーションは関連付けが行われますが、802.1x 認証が成功した後でなければ、データ トラフィックを渡すことができません。次に、802.1x 認証手順を示します。

1. 802.1x 用に設定された AP（オーセンティケータ）がクライアントのユーザ ID を要求します。
2. クライアントは、規定の時間内に自身の ID を応答します。
3. サーバはユーザ ID を確認し、ユーザ ID がサーバのデータベースに存在していれば、そのクライアントの認証を開始します。
4. サーバは AP に成功のメッセージを送ります。
5. クライアントが認証されると、サーバは、クライアントと送受信するトラフィックの暗号化および復号化に使用する暗号化キーを AP に転送します。
6. 手順 4 で、ユーザ ID がデータベースに存在しない場合、サーバは認証をドロップし、失敗のメッセージを AP に送ります。
7. AP はこのメッセージをクライアントに転送し、クライアントは正しいクレデンシャルで再度認証される必要があります。

注：802.1x認証(AP)全体を通じて、APはクライアントとの間で認証メッセージを転送するだけです。

Q. 802.1x認証フレームワークで使用できるEAPバリアントにはどのようなものがありますか。

A.802.1x ではクライアント認証の手続きを定義します。802.1x フレームワークで使用される EAP の種類は、802.1x の交換で使用されるクレデンシャルの種類および認証方式を定義します。802.1x フレームワークでは、次のいずれかの EAP バリアントを使用できます。

- EAP-TLS：Extensible Authentication Protocol Transport Layer Security
- EAP-FAST：EAP Flexible Authentication via Secured Tunnel
- EAP-SIM：EAP 加入者識別モジュール
- Cisco LEAP：Lightweight Extensible Authentication Protocol
- EAP-PEAP：EAP Protected Extensible Authentication Protocol
- EAP-MD5：EAP–Message Digest アルゴリズム 5
- EAP-OTP：EAP オンタイム パスワード
- EAP-TTLS：EAP Tunneled Transport Layer Security

Q. 802.1x EAP方式を利用可能なさまざまなバリアントから選択するにはどうすればよいのですか。

A.考慮する必要がある最も重要な要素は、EAP方式が既存のネットワークと互換性があるかどうかです。さらに、シスコでは、相互認証をサポートしている方式を選択することを推奨します。

Q.ローカルEAP認証とは何ですか。

A.ローカルEAPは、WLCが認証サーバとして機能するメカニズムです。ユーザ クレデンシャルは

、ワイヤレス クライアントを認証するために WLC 上にローカルに保存されます。これは、サーバがダウンした場合にリモート オフィスのバックエンド プロセスとして動作します。ユーザ クレデンシャルは、WLC 上のローカル データベースまたは外部 LDAP サーバから取得できます。LEAP、EAP-FAST、EAP-TLS、PEAPv0/MSCHAPv2、および PEAPv1/GTC は、ローカル EAP でサポートされる各種 EAP 認証です。

Q. Cisco LEAPとは何ですか。

A. Lightweight Extensible Authentication Protocol(LEAP)は、シスコ独自の認証方式です。Cisco LEAP は、Wireless LAN（WLAN; ワイヤレス LAN）用の 802.1X 認証タイプです。 Cisco LEAP では、クライアントと RADIUS サーバの間において、ログオン パスワードを共有秘密として使用する、強固な相互認証をサポートします。Cisco LEAP では、ユーザごと、セッションごとのダイナミックな暗号化キーを提供します。LEAP は、802.1x を展開する最も簡単な方式で、必要なのは RADIUS サーバだけです。LEAP の詳細は、『Cisco LEAP』を参照してください。

Q. EAP-FASTはどのように動作するのですか。

A. EAP-FASTでは、対称キーアルゴリズムを使用して、トンネル化された認証プロセスを実現します。トンネルの確立は、Protected Access Credential（PAC）に依存しています。PAC は、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバ（Cisco Secure Access Control Server（ACS）v. 3.2.3 など）を使用して、EAP-FAST によってダイナミックにプロビジョニングおよび管理できます。 EAP-FAST では、相互認証されたトンネルを使用して、辞書攻撃や man-in-the-middle（中間者）攻撃に対する脆弱性を保護します。EAP-FAST のフェーズは次のとおりです。

EAP-FAST は、辞書攻撃や man-in-the-middle（中間者）攻撃を受けるリスクを軽減するだけでなく、現在配置されているインフラストラクチャをベースとした安全な認証を行えるようにします。

- フェーズ 1：相互認証されたトンネルを確立：クライアントと AAA サーバが PAC を使用して相互に認証し、安全なトンネルを確立します。
- フェーズ 2：確立されたトンネル内でクライアントの認証を実行：クライアントがユーザ名とパスワードを送信して認証を行い、クライアントの認証ポリシーを確立します。
- フェーズ 0（オプション）：EAP-FAST 認証では、まれにこのフェーズを使用して、クライアントが PAC によってダイナミックにプロビジョニングされるようにできます。このフェーズでは、ユーザとネットワーク間で、ユーザごとのアクセス クレデンシャルを安全に作成します。認証のフェーズ 1 では、このユーザごとのクレデンシャル（別名 PAC）を使用します。

詳細は、『Cisco EAP-FAST』を参照してください。

Q. cisco.comには、Cisco WLANネットワークでEAPを設定する方法を説明したドキュメントはありますか。

A. WLANネットワークでEAP認証を設定する方法については、『RADIUSサーバによるEAP認証』を参照してください。

PEAP 認証を設定する方法については、『Protected EAP（PEAP）アプリケーション ノート』を参照してください。

LEAP 認証を設定する方法については、『ローカル RADIUS サーバを使った LEAP 認証』を参照

してください。

Q.ワイヤレスネットワークで最も一般的に使用される暗号化メカニズムにはどのようなものがありますか。

A.無線ネットワークで最もよく使用される暗号化方式を次に示します。

- WEP
- TKIP
- AES

AES はハードウェアの暗号化方式であるのに対し、WEP と TKIP の暗号化はファームウェア上で処理されます。ファームウェアをアップグレードすることで、WEP デバイスは TKIP をサポートでき、相互運用が可能になります。AES は最も安全で高速な方式であるのに対し、WEP は安全性の最も低い方式です。

Q. WEP暗号化とは何ですか。

A. WEPは Wired Equivalent Privacy(WEP)を意味します。WEP は、WLAN デバイス間で送信されるデータ信号の暗号化および復号化に使用されます。WEP は IEEE 802.11 のオプション機能で、転送中のパケットの暴露や改ざんを防止し、ネットワーク使用のアクセス コントロールを行います。WEP によって、WLAN リンクは有線リンクと同程度の安全性になります。この規格で規定されているように、WEP では 40 ビットまたは 104 ビットのキーによる RC4 アルゴリズムが使用されます。RC4 ではデータの暗号化と復号化に同一のキーを使用するため、RC4 は対称アルゴリズムです。WEP をイネーブルにすると、各無線「ステーション」にはキーが配備されます。このキーは、電波を介してデータを送信する前に、データをスクランブルするために使用されます。あるステーションが適切なキーでスクランブルされていないパケットを受信すると、そのステーションはそのパケットを廃棄します。このようなパケットはホストに配信されません。

WEP の設定方法については、『Wired Equivalent Privacy（WEP）の設定』を参照してください。

Q. Broadcast Key Rotationとは何ですか。Broadcast Key Rotation の頻度とは何ですか。

A.ブロードキャストキーのローテーションにより、APは可能な限り最適なランダムグループキーを生成できます。Broadcast Key Rotation では、キー管理対応のすべてのクライアントが定期的に更新されます。WEP キーの Broadcast Key Rotation を有効にすると、ダイナミック ブロードキャスト WEP キーが提供され、ユーザが設定した間隔でそのキーが変更されます。ワイヤレス LAN がシスコ以外のワイヤレス クライアント デバイスに対応しているか、またはシスコのクライアント デバイスの最新のファームウェアにアップグレードできないデバイスに対応している場合、Broadcast Key Rotation は TKIP に代わる優れた手段となります。ブロードキャスト キー ローテーション機能を設定する方法については、『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』を参照してください。

Q. TKIPとは何ですか。

A. TKIPは Temporal Key Integrity Protocolを意味します。TKIP は WEP による暗号化の欠点に対処するために導入されました。TKIPはWEPキーハッシュとも呼ばれ、当初はWEP2と呼ばれていました。TKIPは、WEPキーの再利用の問題を修正する一時的なソリューションです。TKIP では RC4 アルゴリズムを使用して暗号化を行っています。これは WEP と同じです。WEP との大き

な違いは、TKIP ではパケットごとに一時的なキーを変更することです。一時的なキーがパケットごとに変わるのは、各パケットに対するハッシュ値が変わるためです。

Q. TKIPを使用するデバイスは、WEP暗号化を使用するデバイスと相互運用できますか。

A. TKIPの利点は、既存のWEPベースのAPと無線を備えたWLANが、単純なファームウェアパッチを使用してTKIPにアップグレードできることです。また、WEP 専用の装置も、WEP を使用する TKIP 対応のデバイスと相互運用できます。

Q. Message Integrity Check(MIC)とは何ですか。

A. MICは、WEP暗号化の脆弱性に対処するためのもう1つの機能拡張です。MIC は暗号化されたパケットに対するビットフリップ攻撃を防止します。ビットフリップ攻撃の際、侵入者は暗号化されたメッセージを傍受し、メッセージを改ざんして、改ざんしたメッセージを再送信します。このメッセージが破壊されていて正当なものではないことが、受信者には分かりません。この問題に対処するために、MIC 機能ではワイヤレス フレームに MIC フィールドを追加します。MIC フィールドは、フレームの整合性チェック機能を提供し、ICV と同様の演算上の欠点に対する脆弱性がなくなります。また、MIC ではワイヤレス フレームにシーケンス番号フィールドも追加します。順序が誤って受信されたフレームは AP で廃棄されます。

Q. WPAとは何ですか。WPA 2 と WPA はどこが異なりますか。

A. WPAは、ネイティブWLANの脆弱性に対処するWi-Fi Allianceの標準ベースのセキュリティソリューションです。WPA は、WLAN システムに対する拡張データ保護とアクセス コントロール機能を提供します。WPA は、従来の IEEE 802.11 によるセキュリティ実装における Wired Equivalent Privacy（WEP）の既知のすべての脆弱性に対処し、企業環境と Small Office, Home Office（SOHO）環境の両方において、WLAN ネットワークに即座に適用できるセキュリティ ソリューションです。

WPA2 は次世代の Wi-Fi セキュリティ機能です。WPA2は、IEEE 802.11i規格の相互運用可能な Wi-Fi Alliance実装です。WPA2 では、Counter Mode with Cipher Block Chaining Message Authentication Code Protocol（CCMP）を使用して、National Institute of Standards and Technology（NIST; 国立標準技術研究所）が推奨する Advanced Encryption Standard（AES; 高度暗号化規格）の暗号化アルゴリズムを実装しています。AES カウンタ モードは、データの 128 ビットのブロックを 128 ビットの暗号化キーを使用して一度に暗号化する、ブロック暗号です。WPA2 では、WPA よりも高いセキュリティ レベルが提供されます。WPA2は、すべてのアソシエーションに新しいセッションキーを作成します。ネットワーク上のクライアントごとに WPA2 が使用する暗号化キーは、クライアントごとに一意で固有なものです。最終的に、無線で送信される各パケットは、一意のキーで暗号化されます。

WPA1 と WPA2 のどちらも、TKIP または CCMP の暗号化を使用できます（アクセス ポイントおよびクライアントの中にはこれらの組み合わせを制限するものもありますが、4 つの組み合わせが可能になります）。 WPA1 と WPA2 との違いは、ビーコン、アソシエーション フレーム、および 4 方向のハンドシェイク フレームに取り込まれる情報要素です。これらの情報要素のデータは基本的に同じですが、使用される識別子が異なります。鍵ハンドシェイクの主な違いは、WPA2 では 4 方向のハンドシェイクに初期グループ鍵が含まれ、初期グループ鍵ハンドシェイクがスキップされるのに対して、WPA では初期グループ鍵を配信するためにこの余分なハンドシェイクが必要になる点です。グループ鍵の再生成も同じように行われます。ハンドシェイクは、ユーザ データグラムの送信用に暗号スイート（TKIP または AES）を選択および使用する前に行われます。WPA1 または WPA2 のハンドシェイク時に、使用する暗号スイートが決まります。一度

選択された暗号スイートは、どのユーザ トラフィックにも使用されます。したがって、WPA1とAESはWPA2ではありません。WPA1では、TKIP暗号またはAES暗号のいずれかを使用できます（ただし、クライアント側で制限されることがよくあります）。

Q. AESとは何ですか。

A. AESは Advanced Encryption Standard（高度暗号化規格）を意味します。AES では、はるかに強固な暗号化が提供されます。AESでは、128、192、および256ビットのキーをサポートするブロック暗号であるRijndaelアルゴリズムを使用し、RC4よりもはるかに強力です。WLANデバイスでAESをサポートするには、ハードウェアでWEPをサポートする必要があります。

Q. Microsoft Internet Authentication Service(IAS)サーバでは、どのような認証方式がサポートされていますか。

A. IAS**は**、次の認証プロトコルをサポートしています。

- Password Authentication Protocol（PAP; パスワード認証プロトコル）
- Shiva パスワード認証プロトコル（SPAP）
- チャレンジ ハンドシェーク認証プロトコル（CHAP）
- Microsoft Challenge Handshake Authentication Protocol（MS-CHAP; マイクロソフト チャレンジ ハンドシェイク認証プロトコル）
- Microsoft Challenge Handshake Authentication Protocol version 2（MS-CHAP v2; マイクロソフト チャレンジ ハンドシェイク認証プロトコル バージョン 2）
- Extensible Authentication Protocol-Message Digest 5 CHAP（EAP-MD5 CHAP）
- EAP-Transport Layer Security（EAP-TLS）
- Protected EAP-MS-CHAP v2（PEAP-MS-CHAP v2）（PEAPv0/EAP-MSCHAPv2 とも呼ばれています）

Windows 2000 Server Service Pack 4 がインストールされている場合、Windows 2000 Server の PEAP-TLS IAS では、PEAP-MS-CHAP v2 および PEAP-TLS がサポートされています。詳細は、『Authentication Methods for use with IAS』を参照してください。

Q. VPNはワイヤレス環境でどのように実装されるのですか。

A. VPNはレイヤ3セキュリティメカニズムです。ワイヤレス暗号化メカニズムはレイヤ2に実装されます。VPNは、802.1x、EAP、WEP、TKIP、およびAESを介して実装されます。レイヤ 2 メカニズムが実装されている場合、VPN はその実装に対するオーバーヘッドを追加します。パブリック ホットスポットやホテルなど、セキュリティが実装されていない場所において、VPN の実装は有効なソリューションになります。

トラブルシューティングと設計に関する FAQ

Q.屋外のワイヤレスLANにワイヤレスセキュリティを導入するベストプラクティスはありますか。

A. 『**屋外**無線セキュリティのベストプラクティス』を参照してください。このドキュメントでは、屋外のワイヤレス LAN を導入する場合のセキュリティに関するベスト プラクティスについて説明しています。

Q. RADIUSサーバにActive Directoryを備えたWindows 2000または2003サーバを使用して、ワイヤレスクライアントを認証できますか。

A. Active Directoryを備えたWindows 2000または2003サーバは、RADIUSサーバとして動作できます。シスコでは Windows サーバの設定のサポートは行っていないため、この RADIUS サーバを設定する方法については Microsoft にお問い合わせください。

Q.私のサイトは、オープンワイヤレスネットワーク（350および1200シリーズ AP）からPEAPネットワークに移行しようとしています。OPEN SSID（オープン認証用に設定された SSID）と PEAP SSID（PEAP 認証用に設定された SSID）の両方を、同時に同じ AP で機能させたいと考えています。これにより、クライアントが PEAP SSID に移行する期間を設けることができます。同じ AP 上で Open SSID と PEAP SSID を同時にホスティングする方法はありますか。

A. Cisco APはVLANをサポートします（レイヤ2のみ）。 実際にこれが、必要な機能を実現させる唯一の方法になります。2 つの VLAN（ネイティブ VLAN とそれ以外の VLAN）を作成する必要があります。 そして、片方には WEP キーを使用し、もう一方には WEP キーを使用しないようにできます。この方法によって、一方の VLAN をオープン認証用に、もう一方の VLAN を PEAP 認証用に設定できます。VLAN の設定方法については、『Cisco Aironet ワイヤレス装置との VLAN の併用』を参照してください。

dot1Q および VLAN 間ルーティング用にスイッチ、L3 スイッチ、またはルータを設定する必要があることに注意してください。

Q. Cisco AP 1200 VxWorksを設定して、ワイヤレスユーザがCisco 3005 VPNコンセントレータに対して認証されるようにしたいと思います。このためには、AP やクライアントに対してどのような設定を行う必要がありますか。

A.このシナリオでは、APまたはクライアントに固有の設定は必要ありません。設定はすべて VPN コンセントレータ上で行う必要があります。

Q. Cisco 1232 AG APを導入しています。この AP を使用して展開できる最も安全な方法について知りたいと考えています。AAA サーバはなく、使用しているリソースは AP と Windows 2003 のドメインだけです。スタティックな 128 ビットの WEP キーの使用方法、非ブロードキャスト SSID、および MAC アドレスの制限については理解しています。ユーザのほとんどは Windows XP ワークステーションを使用し、一部が PDA を使用しています。この設定について最も安全な実装はどのようなものでしょうか。

A. Cisco ACSのようなRADIUSサーバがない場合は、APをLEAP、EAP-FAST、またはMAC認証用のローカルRADIUSサーバとして設定できます。

注：考慮する必要がある非常に重要な点は、クライアントをLEAPとEAP-FASTのどちらで使用するかです。使用する場合は、クライアントに LEAP または EAP-FAST をサポートするユーティリティを持たせる必要があります。Windows XP のユーティリティでサポートされているのは、PEAP または EAP-TLS だけです。

Q. PEAP認証が「EAP-TLS or PEAP authentication failed during SSL handshake」

エラーで失敗します。 これは、なぜですか。

A.このエラーは、Cisco Bug ID CSCee06008(登録ユーザ**専用)が原因で発生する可能性があります。**ADU 1.2.0.4でPEAPが失敗します。この問題の回避策は、最新バージョンのADUを使用することです。

Q. WPAとローカルMAC認証を同じSSIDで使用できますか。

A. Cisco APは、同じService Set Identifier(SSID)でローカルMAC認証とWi-Fi Protected Access(WPA)事前共有キー(WPA-PSK)をサポートしていません。 ローカルの MAC 認証と WPA-PSK を一緒にイネーブルにすると、WPA-PSK が動作しません。この問題は、ローカル MAC 認証によって、設定から WPA-PSK の ASCII のパスワード行が削除されるために発生します。

Q.現在、データVLANに対してCiphers 128-bit WEP暗号化を使用して3つのCisco 1231ワイヤレスAPを設定しています。SSID のブロードキャストは行っていません。環境内には別個の RADIUS サーバはありません。何者かがスキャニング ツールを使用して WEP キーを突き止め、このツールを使用して数週間にわたって無線トラフィックを監視していました。これを阻止して、ネットワークを安全にするにはどのようにしたらよいですか。

A. Static WEPはこの問題に対して脆弱で、ハッカーが十分なパケットをキャプチャし、同じ初期化ベクトル(IV)を持つ2つ以上のパケットを取得できる場合に導出できます。

このような問題が発生するのを防ぐには、次に示すいくつかの方法があります。

1. ダイナミックな WEP キーを使用する。
2. WPA を使用する。
3. シスコのアダプタだけを使用している場合は、Per Packet Key と MIC を有効にします。

Q. Wi-Fi Protected Access(WPA)-Pre-Shared Key(PSK)用に2つの異なるWLANが設定されている場合、事前共有キーはWLANごとに異なる可能性がありますか。個別にした場合、異なる事前共有キーが設定されている他の WLAN は影響を受けますか。

A. WPA-PSKの設定はWLANごとに行う必要があります。ある WPA-PSK を変更しても、設定済みの他の WLAN は影響を受けません。

Q.環境では、Intel Pro/Wireless、Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling(EAP-FAST)、およびWindows Active Directory(AD)アカウントにリンクされたCisco Secure Access Control Server(ACS)3.3を使用しています。問題は、ユーザ パスワードの期限が迫っていても、ユーザにパスワードの変更を求めるメッセージが表示されないことです。最終的に、アカウントが期限切れになります。ユーザにパスワードの変更を求めるメッセージを表示するための方法はありますか。

A. Cisco Secure ACSパスワードエージング機能を使用すると、次の1つ以上の条件でユーザにパスワードを変更させることができます。

- 指定した日数が経過した後（日数によるエージング規則）
- 指定したログイン回数が終了した後（使用回数によるエージング規則）
- 新規ユーザが初めてログインするとき（パスワード変更規則）

Cisco Secure ACS でこの機能を設定する方法の詳細は、『CiscoSecure ユーザ データベースのパスワード エージングをイネーブルにする』を参照してください。

Q.ユーザがLEAPを使用して無線でログインすると、ネットワークドライブをマッピングするためのログインスクリプトが表示されます。しかし、Wi-Fi Protected Access（WPA）または PEAP 認証を使用した WPA2 では、ログイン スクリプトは実行されません。クライアントとアクセス ポイントの両方が、RADIUS（ACS）と同様に Cisco 製品です。 RADIUS（ACS）でログイン スクリプトが実行されないのはなぜですか。

A.ログインスクリプトが機能するには、マシン認証が必須です。マシン認証により、ワイヤレス ユーザはログオンする前にスクリプトをロードするためにネットワーク アクセスを取得できます。

PEAP-MS-CHAPv2 でマシン認証を設定する方法の詳細は、『PEAP-MS-CHAPv2 マシン認証が設定された Cisco Secure ACS for Windows v3.2』を参照してください。

Q. Cisco Aironet Desktop Utility(ADU)リリース3.0では、ユーザがExtensible Authentication Protocol-Transport Layer Security(EAP-TLS)のマシン認証を設定する場合、ADUではプロファイルの作成が許可されません。これは、なぜですか。

A.これは、Cisco Bug ID CSCsg32032(登録ユーザ専用)が原因です。 この問題は、クライアント PC にマシン証明書はインストールされているがユーザ証明書がない場合に発生することがあります。

回避策は、ユーザ ストアにマシン証明書をコピーし、EAP-TLS プロファイルを作成してから、ユーザ ストアからマシン証明書を削除してマシン認証のみの設定にすることです。

Q.クライアントのMACアドレスに基づいてワイヤレスLAN上のVLANを割り当てる方法はありますか。

A.いいえ。これは不可能です。RADIUS サーバからの VLAN 割り当ては、MAC 認証ではなく、802.1x でのみ機能します。MAC アドレスが RADIUS サーバで認証されている（LEAP/PEAP にユーザ ID/パスワードとして定義されている）場合は、RADIUS を使用して MAC 認証で VSA を強制的に設定できます。

関連情報

- ワイヤレス ネットワーク セキュリティ
- White Paper：無線 LAN のセキュリティ
- ワイヤレス LAN セキュリティの概要
- ワイヤレス LAN ネットワークへの EAP-TLS の導入ガイド
- Cisco LEAP
- Wired Equivalent Privacy（WEP）の設定
- ワイヤレス製品に関するサポート

- テクニカル サポートとドキュメント – Cisco Systems