# PEAP ( Procted Extensible Authentication Protocol )

Q&A

---

# PEAP ( Procted Extensible Authentication Protocol )

---

**このドキュメントでは、Protected Extensible Authentication Protocol に関する質問に答えます。**

## 概要



## 機能と利点



## 導入



## EAP タイプの比較

- Microsoft PEAP サプリカントと Cisco PEAP サプリカントの相違点を教えてください。
- PEAP、EAP-Flexible Authentication via Secure Tunneling（FAST）、Cisco LEAP、および EAP-TLS の相違点を教えてください。

# 概要

Q: Protected Extensible Authentication Protocol とは何ですか。
**A:** Protected Extensible Authentication Protocol（PEAP）は、ワイヤレス LAN（WLAN）用 802.1X 認証タイプの 1 つです。強力なセキュリティおよびユーザ データベースの拡張性を提供するとともに、ワンタイム トークン認証およびパスワードの変更やエージングをサポートします。PEAP は、シスコシステムズ、Microsoft、および RSA Security が IETF に提出したインターネット ドラフト（I-D）に基づいています。かつてシスコシステムズのリード エンジニアであった Glen Zom 氏は、この I-D の共同作成者です。
Return to Top

Q: PEAP は、Cisco Unified Wireless Network、Wi-Fi Protected Access（WPA）、および Wi-Fi Protected Access 2（WPA2）でサポートされていますか。
**A:** はい。Cisco Unified Wireless Network は、PEAP を含むさまざまな EAP 認証タイプをサポートしています。他のすべての EAP タイプと同様に、PEAP も WPA および WPA2 ネットワークで使用できます。
Return to Top

Q: Cisco Unified Wireless Network とは何ですか。
**A:** Cisco Unified Wireless Network は、企業が直面している WLAN のセキュリティ、展開、管理、および制御の問題をコスト効率よく解決する、業界で唯一の有線/無線統合型ソリューションです。この強力なソリューションは、ワイヤレス ネットワーキングと有線ネットワーキングの優れた要素を組み合わせることにより、スケーラブルで、管理しやすく、安全な WLAN を少ない総所有コスト（TCO）で実現します。このソリューションには、基幹ビジネス アプリケーションへのリアルタイム アクセスを実現し、実績のあるエンタープライズクラスの安全な接続を提供する、先進的な RF 機能も含まれています。Cisco Unified Wireless Network は、企業が有線 LAN に対して期待するレベルのセキュリティ、スケーラビリティ、信頼性、展開のしやすさ、および管理性を、ワイヤレス LAN で実現します。

Cisco Unified Wireless Network は、エンタープライズに対応した、標準ベースのワイヤレス セキュリティ ソリューションです。このソリューションにより、ネットワーク管理者は、シスコ ワイヤレス関連製品、Cisco Aironet シリーズ製品、Cisco Compatible Extensions 製品、または Wi-Fi 認定 WLAN クライアント デバイスを使用するときに、データのプライバシーとセキュリティを確実に維持できます。このエンタープライズクラスのワイヤレス セキュリティ ソリューションは、有線 LAN のセキュリティとほぼ同レベルの強力なワイヤレス LAN セキュリティをサポートします。業界をリードする WLAN セキュリティ サービスを提供することにより、一貫性、信頼性、および安全性の高いモバイル ネットワーキングのニーズが満たされます。Cisco Unified Wireless Network は、巧妙なパッシブ/アクティブ WLAN 攻撃を軽減し、さまざまなクライアント デバイスと相互運用でき、信頼性が高く、スケーラブルで、集中管理されたセキュリティ環境を実現します。Cisco Unified Wireless Network を使用することにより、ネットワーク管理者は、IT スタッフの負担を増やさない、スケーラブルで、問題のないセキュリティ管理に基づく、大規模なエンタープライズ WLAN を展開できます。
Return to Top

Q: PEAP は、標準規格ですか。
**A:** 現時点では、まだ標準規格ではありません。PEAP は、IETF に提出された I-D に基づいています。シスコ、Microsoft、および RSA Security は、PEAP 実装の標準化を支援する IETF 標準化団体のメンバーです。
Return to Top

Q: IETF に提出された PEAP ドラフトに関する情報はどこで入手できますか。
**A:** IETF I-D 検索エンジンにアクセスし、"PEAP" を検索してください。

Return to Top

# 機能と利点

Q: PEAP のセキュリティ上の利点は何ですか。
**A:** PEAP には、セキュリティに関する次の利点があります。

- Transport Layer Security（TLS）に基づいた、EAP-Generic Token Card（GTC）や One Time Password（OTP; ワンタイム パスワード）サポートなどの非暗号化認証タイプの使用
- サーバ側での Public-Key Infrastructure（PKI; 公開キー インフラストラクチャ）ベースのデジタル証明書認証の使用
- Lightweight Directory Access Protocol（LDAP）、Novell NDS、OTP データベースなど、拡張された一連のディレクトリに対する認証が可能
- TLS を使用した、ユーザに固有のすべての認証情報の暗号化
- 有効期限に達したパスワードの変更が可能
- EAP 識別応答でログイン ユーザ名が公開されない
- 辞書攻撃に対して脆弱でない
- Temporal Key Integrity Protocol（TKIP）または Advanced Encryption Standard（AES）との組み合わせによる動的プライバシー保護の実現

Return to Top

Q: エンタープライズにとっての PEAP の利点は何ですか。
**A:** PEAP はサーバ側の EAP-TLS に基づいています。PEAP を使用すると、企業では、EAP-TLS に必要な各クライアント マシンへのデジタル証明書のインストールに関連した問題を回避でき、ログオン パスワードや OTP など、企業のニーズに最適なクライアント認証方法を選択できます。

Return to Top

# 導入

Q: PEAP の認証は、どのように行われますか。
**A:** PEAP の認証は、次の 2 つのフェーズに分かれて行われます。

- フェーズ 1 では、サーバ側で TLS 認証を実行することで、暗号化トンネルを作成し、一般的で信頼されたセキュリティ方法の 1 つである Secure Sockets Layer（SSL）を使用した Web サーバ認証に似た方法でサーバ側の認証を実現します。PEAP のフェーズ 1 が確立されると、ユーザに固有のすべての情報を含むすべてのデータが暗号化されます。
- PEAP 認証のフェーズ 2 のフレームワークは拡張可能であり、TLS トンネル内で EAP-GTC や Microsoft Challenge Authentication Protocol（MS-CHAP）Version 2 などの方法を使用してクライアントを認証できます。

Return to Top

Q: PEAP をサポートしているシスコ ワイヤレス製品を教えてください。
**A:** Cisco Aironet Autonomous アクセス ポイント、Cisco Aironet Lightweight アクセス ポイント、Cisco Wireless LAN Controller、Cisco Aironet クライアント デバイスなど、多数のシスコ ワイヤレス製品が PEAP をサポートしています。Cisco Compatible Extensions バージョン 4 以降が動作する Cisco Compatible クライアント デバイスも、PEAP をサポートしています。

Return to Top

Q: PEAP をサポートしているクライアント オペレーティング システムを教えてください。
**A:** PEAP は、Microsoft Windows 2000、Windows XP、および Windows CE でサポートされています。クライアント マシン上で PEAP を使用するための最新のソフトウェア情報とガイドラインについては、 Cisco Aironet WLAN クライアント ソフトウェアに関する Web ページを参照してください。

Return to Top

Q: シスコ以外のベンダーのワイヤレス クライアントでも PEAP 認証を利用できますか。
**A:** はい。PEAP IETF I-D 提案標準に準拠する PEAP対応サプリカントからであれば、PEAP 認証を利用できます。インストールを開始する前に、サポート状況と相互運用性についてベンダーに確認することをお勧めします。
Return to Top

Q: シスコの PEAP クライアント ソフトウェアと Microsoft の PEAP クライアント ソフトウェアの両方を 1 台のマシンにインストールできますか。
**A:** シスコの PEAP クライアント ソフトウェアは、Microsoft の PEAP クライアント ソフトウェアを補完します。どちらの PEAP 実装をクライアント マシンにインストールするかは自由に選択できます。シスコ PEAP サプリカントをクライアント マシンにインストールすると、既存の MS-CHAP Version 2 PEAP サプリカントは完全に置き換えられます。
Return to Top

Q: クライアント証明書認証を PEAP で使用できますか。
**A:** PEAP はサーバ側の EAP-TLS に基づいています。クライアント証明書認証は不要です。サーバだけが証明書を使用して認証されます。
Return to Top

Q: PEAP は、パスワードや OTP を使用した Windows ドメインへのシングル ログインをサポートしていますか。
**A:** PEAP は、クライアント サプリカントの機能であるシングル ログインと互換性があります。シングル ログイン機能は、サードパーティ製ユーティリティで利用できる場合があります。Windows の PEAP サプリカント（PEAP/MS-CHAPv2）は、シングル サインオンをサポートしています。シスコの PEAP/GTC サプリカントは、シングル サインオンをサポートしていません。
Return to Top

Q: PEAP セッション中のサイレント セッション レジュームは、どのように動作しますか。
**A:** EAP のフェーズ 1 が実行されたときだけ、サイレント セッション レジューム（「高速再接続」とも呼ぶ）がサポートされます。フェーズ 2 では、直前の認証状態が再利用されます。PEAP セッションがタイムアウトしない限り、ユーザの再認証は不要です。PEAP セッション タイマーは、EAP で使用される動的暗号キーの変動性の制御に使用する RADIUS セッション タイマーに依存しません。
Return to Top

Q: LDAP や Novell NDS のデータベースで PEAP を使用できますか。
**A:** はい。PEAP は、LDAP および Novell NDS と相互運用可能です。
Return to Top

Q: PEAP の導入に関するさらに詳しい情報はどこで入手できますか。
**A:** PEAP の詳しい導入方法については、「Protected EAP（PEAP）アプリケーション ノート」（英語）を参照してください。
Return to Top

Q: WLAN の導入に関するさらに詳しい情報はどこで入手できますか。
**A:** 安全な WLAN の詳しい導入方法については、次のドキュメントを参照してください。

- 導入ガイド：Cisco Wireless Security Suite の設定

Return to Top

Q: WLAN のセキュリティに関するさらに詳しい情報はどこで入手できますか。
**A:** WLAN のセキュリティについては、「シスコ Aironet WLAN のセキュリティの概要」を参照してください。
Return to Top

# EAP タイプの比較

Q: Microsoft PEAP サプリカントと Cisco PEAP サプリカントの相違点を教えてください。
**A:** どちらのサプリカントも PEAP をサポートしていますが、TLS トンネルによるクライアント認証方法が異なります。Microsoft PEAP サプリカントは MS-CHAP Version 2 によるクライアント認証だけをサポートしているので、Windows NT ドメインや Active Directory などの MS-CHAP Version 2 をサポートするユーザ データベースに限定されます。Cisco PEAP サプリカントは OTP およびログオン パスワードによるクライアント認証をサポートしているので、Microsoft のデータベースだけでなく、他のベンダーの（RSA Security や Secure Computing Corporation など）OTP データベースや、ログオン パスワード データベース（LDAP や Novell NDS など）に対応できます。また、Cisco PEAP クライアントには、TLS 暗号化トンネルが確立されるまでユーザ名のアイデンティティを隠匿する機能も組み込まれています。これにより、認証フェーズではユーザ名がブロードキャストされず、機密性が強化されます。
Return to Top

Q: PEAP、EAP-Flexible Authentication via Secure Tunneling（FAST）、Cisco LEAP、および EAP-TLS の相違点を教えてください。
**A:** 表 1 に、PEAP、EAP-FAST、Cisco LEAP、および EAP-TLS の相違点を示します。
**表 1** PEAP、EAP-FAST、Cisco LEAP、EAP-TLS の比較表

| | **PEAP - Generic Token Card（GTC）を使用** | **PEAP - Microsoft Protocol（MS-C** |
|---|---|---|
| ユーザ認証用のデータベースおよびサーバ | OTP、LDAP、Novell NDS、Windows NT ドメイン、Active Directory | Windows NT ド |
| サーバ証明書の必要性 | あり | あり |
| クライアント証明書の必要性 | なし | なし |
| オペレーティング システムのサポート | ドライバ：Windows XP、Windows 2000、Windows CE*<br>サードパーティ製ユーティリティ：その他の OS** | ドライバ：Wind<br>Windows CE<br>サードパーティ<br>OS** |
| Application-Specific Device（ASD; 特定用途向けデバイス）のサポート | なし | なし |
| 使用するクレデンシャル | クライアント：Windows、Novell NDS、LDAP<br>パスワード：OTP またはトークン<br>サーバ：デジタル証明書 | Windows パスワ |
| Windows ログインを使用したシングル サインオン | なし | あり |
| パスワードの有効期限および変更 | なし | あり |
| 高速セキュア ローミング対応 | なし | なし |
| WPA（Wi-Fi Protected Access）および WPA2 対応 | あり | あり |

* PEAP/GTC は、Cisco Compatible Version 2 クライアント以降でサポートされます。
** Meetinghouse および Funk のサプリカントでは、さらに多くのオペレーティング システムがサポートされます。
*** Cisco Aironet 350 シリーズ WLAN クライアント デバイスおよび Cisco Aironet 5 GHz 54 Mbps ワイヤレス LAN クライアント アダプタ（CB20A）は、Windows XP、Windows 2000、および Windows CE オペレーティング システム上で EAP-FAST をサポートします。
**** 強力なパスワードが必要です。詳細については、「Cisco LEAP に対する辞書攻撃へのシスコの対応」（英語）を参照してください。
Return to Top

## 関連情報

Cisco Unified Wireless Network の詳細については、http://www.cisco.com/jp/go/unifiedwireless/ を参照してください。
Cisco Aironet 製品の詳細については、http://www.cisco.com/jp/go/aironet/ を参照してください。
シスコ ワイヤレス LAN のセキュリティについては、「シスコ Aironet LAN のセキュリティの概要」も参考にしてください。
http://www.cisco.com/web/JP/product/hs/wireless/airo1200/prodlit/airowlso_ov.html
EAP-FAST の詳細については、
http://www.cisco.com/web/JP/solution/netsol/mobility/literature/prod_qas09186a00802030dc.html
を参照してください。
Cisco LEAP の詳細については、
http://www.cisco.com/web/JP/solution/netsol/mobility/literature/prod_qas0900aecd801764fa.html
を参照してください。
802.11i、WPA、および WPA2 の詳細については、
http://www.cisco.com/web/JP/solution/netsol/mobility/literature/prod_qas0900aecd801e3e59.html
を参照してください。
Return to Top