# Cisco Unified Wireless Network Solution セキュリティ


- セキュリティの概要，1 ページ
- レイヤ 1 ソリューション，1 ページ
- レイヤ 2 ソリューション，2 ページ
- レイヤ 3 ソリューション，2 ページ
- 統合されたセキュリティ ソリューション，2 ページ


## セキュリティの概要

Cisco Unified Wireless Network（UWN）セキュリティ ソリューションは、複雑になりがちなレイヤ 1、レイヤ 2、およびレイヤ 3 の 802.11 アクセス ポイントのセキュリティ コンポーネントを 1 つのシンプルなポリシーマネージャにまとめたもので、システム全体のセキュリティポリシーを WLAN 単位でカスタマイズできます。 Cisco UWN セキュリティ ソリューションは、シンプルで、統一された、体系的なセキュリティ管理ツールを提供します。

企業での WLAN 展開の最も大きな障害の 1 つが、脆弱な独立型の暗号化方式である Wired Equivalent Privacy（WEP）です。 低価格のアクセス ポイントの登場も新たな問題であり、それらは企業ネットワークに接続して man-in-the-middle 攻撃や DoS 攻撃（サービス拒絶攻撃）に利用される可能性があります。

## レイヤ 1 ソリューション

Cisco UWN セキュリティ ソリューションによって、すべてのクライアントのアクセス回数は、ユーザが設定した数値までに制限されます。 制限回数内でアクセスできなかった場合、そのクライアントはユーザが設定したタイマーが切れるまで自動的に除外（アクセスをブロック）されます。 オペレーティング システムでは、WLAN ごとに SSID ブロードキャストを無効にすることもできます。

# レイヤ 2 ソリューション

上位レベルのセキュリティと暗号化が必要な場合は、拡張認証プロトコル（EAP）やWi-Fi Protected Access（WPA）、およびWPA2など業界標準のセキュリティ ソリューションを実装することもできます。 Cisco UWN ソリューションの WPA 実装には、AES（Advanced Encryption Standard）ダイナミック キー、TKIP + Michael（Temporal Key Integrity Protocol + Message Integrity Code Checksum）ダイナミック キー、WEP（Wired Equivalent Privacy）スタティック キーが含まれます。 無効化も使用され、ユーザが設定した回数だけ認証の試行に失敗すると、自動的にレイヤ 2 アクセスがブロックされます。

どの無線セキュリティ ソリューションを採用した場合も、コントローラと Lightweight アクセス ポイントとの間のすべてのレイヤ 2 有線通信は、Control and Provisioning of Wireless Access Points（CAPWAP）トンネルを使用してデータを渡すことにより保護されます。

## レイヤ 2 ソリューションの制約事項

認証キー管理として WPA/WPA2 と CCKM が使用されている場合、Cisco Aironet クライアント アダプタ バージョン 4.2 で認証は行われず、コントローラと AP 間に 2 秒の遅延があります。

# レイヤ 3 ソリューション

WEP の問題は、パススルー VPN のような業界標準のレイヤ 3 セキュリティ ソリューションを使用すると、さらに進んだ解決が可能です。

Cisco UWN ソリューションでは、ローカルおよび RADIUS MAC（Media Access Control）フィルタリングがサポートされています。 このフィルタリングは、802.11 アクセス カードの MAC アドレス一覧情報が把握できている小規模のクライアント グループに適しています。

Cisco UWN ソリューションでは、ローカルおよび RADIUS ユーザおよびパスワード認証がサポートされています。 この認証は、小規模から中規模のクライアント グループに適しています。

# 統合されたセキュリティ ソリューション

統合されたセキュリティ ソリューションを次に示します。

- Cisco Unified Wireless Network（UWN）ソリューションオペレーティング システムのセキュリティは、802.1X AAA（認証、許可、アカウンティング）エンジンを中心に構築されており、ユーザは Cisco UWN ソリューション全体にわたってさまざまなセキュリティ ポリシーを迅速に設定および適用できます。
- コントローラおよび Lightweight アクセス ポイントには、システム全体の認証および認可プロトコルがすべてのポートおよびインターフェイスに装備され、最大限のシステムセキュリティが提供されています。

- オペレーティング システムのセキュリティ ポリシーは個々の WLAN に割り当てられ、Lightweight アクセス ポイントは設定されたすべての WLAN（最大 16）を同時にブロードキャストします。これによって追加のアクセス ポイントは不要になりますが、干渉が増加し、システム スループットが低下する可能性があります。
- オペレーティング システム セキュリティは RRM 機能を使用して、干渉およびセキュリティ違反がないか継続的に空間を監視し、それらを検出したときはユーザに通知します。
- オペレーティング システム セキュリティは、業界標準の認証、許可、アカウンティング（AAA）サーバで機能します。