

## 政府機関向けの安全なワイヤレス アーキテクチャ

### 概要

#### Cisco Unified Wireless アーキテクチャの主な利点

Cisco Unified Wireless アーキテクチャの利点を次に挙げます。

- 従業員やゲスト ユーザが、会議室、オフィス、および公共の場からデータやビジネスクリティカルなアプリケーションに安全にアクセスできるため、生産性が向上し、より円滑なコラボレーションが実現します。
- 簡素化されたネットワーク展開と運用機能により、運用コストを削減できます。
- スタッフが 1 台の管理コンソールから数百または数千のワイヤレス アクセス ポイントを制御できるため、合理化され、リアルタイムで動的なネットワーク管理が実現します。
- 有線および無線ソリューションを使用して、組織に特有のニーズを考慮したネットワークが形成されるため、柔軟性が向上します。
- ワイヤレス アーキテクチャのすべてのコンポーネントに、エンドツーエンドの FIPS セキュリティを提供します。

#### ビジネス上の課題

特に総務および国防機関において、政府機関が直面している最も解決が困難な課題の 1 つは、ワイヤレス ネットワークにおける送信中のデータの保護と、各機関によるモバイル コンピューティングの活用を同時に実現することです。2004 年 4 月、国防長官府 (OSD) は、DoD 810 0.2 「Use of Commercial Wireless Devices, Services and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)」を発行しました。これは、ワイヤレス セキュリティに関するさまざまな要件を定めたポリシーです。このポリシーでは、すべての機関がレイヤ 2 暗号化を採用し、ソリューションが特定の連邦安全認定 (National Institute of Standards and Technology Federal Information Processing Standards [FIPS] 140-2、NIAP Common Criteria 検証など) に従うことを義務付けています。その結果、各政府機関が独自のさまざまなソリューションを導入したため、既存のネットワークにこれらのソリューションを適用する必要がありました。

2006 年 6 月、OSD は 2004 年 4 月の通達を補足するガイダンスとして、「Use of Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)」を発表しました。この新たな文書では、802.11i/WPAv2 がレイヤ 2 暗号化の新しい標準になり、FIPS 140-2 暗号化要件への対応と同時に ユーザ認証の実施も義務付けられています。また、データの機密性、データの正真正性、ユーザまたはデバイスの認証、否認防止、高可用性、ロケーション ベースのサービス、および無線侵入防御機能も必須になっています。

これらの運用要件に加えて、政府機関はビジネスレベルの問題も検討する必要があります。安全なワイヤレス アーキテクチャは、各機関の総所有コストの削減、既存の有線インフラストラクチャの活用、共通のアクセス ポイント/センサ ハードウェアの利用、投資保証の実現、低コストでの将来のロケーション ベース サービスのサポート、有線/無線セキュリティの集

約を実現する必要があります。シスコは、DoD ポリシーのすべての内容に対応すると同時に、無線インフラストラクチャと有線インフラストラクチャを統合し、安全でシームレスかつ一貫性のあるエンドユーザ エクスペリエンスを実現する、完全なソリューションを提供します。

Cisco® Unified Wireless アーキテクチャは、有線と無線の両方のコンポーネントからキー コントロールとセキュリティ テクノロジーを透過的に統合します。これにより、多層防御のセキュリティ アーキテクチャが構築されます。これには、標準ベースのエンタープライズ ソリューションにおけるポリシーベースのセキュリティ、攻撃緩和、802.1X ユーザ認証および承認、無線データの機密性と正真性を維持するために Advanced Encryption Standard (AES) を使用して FIPS により検証された 802.11i/WPAv2、高速で安全なローミング、組み込みの無線侵入検知および防御が含まれます。このソリューションにより、各機関は、有線ネットワークにおける長期的でコスト効率の高いスケーラビリティ、展開の容易性、および信頼性を実現できます。

### ソリューション

Cisco Unified Wireless アーキテクチャは、従業員の生産性向上、コラボレーションの強化、および顧客対応の向上を実現すると同時に、大企業の WLAN を実装する際に組織が直面する、セキュリティ、展開、管理、および制御の問題に低コストで対処できる、業界で唯一の有線および無線の統合ソリューションです。このソリューションは、企業のオフィス、病院、小売店、製造現場、倉庫環境、教育機関、金融機関、地方および政府の機関、およびモバイル接続を必要とするその他の事業体向けに設計されています。

Cisco Unified Wireless Network はマルチサービス ソリューションとして設計されているため、E メールやインターネット アクセスのような一般的なビジネス アプリケーションだけでなく、モバイル医療システム、在庫管理、監視カメラ、資産トラッキングのような特殊なアプリケーションもサポートします。これらのデータ向けアプリケーション以外に、必要に応じて、ゲスト アクセス、Voice over WLAN、無線侵入検知および防御、正確なロケーショントラッキング、ネットワーク アドミッション コントロール (NAC) などのサービスも実装できます。

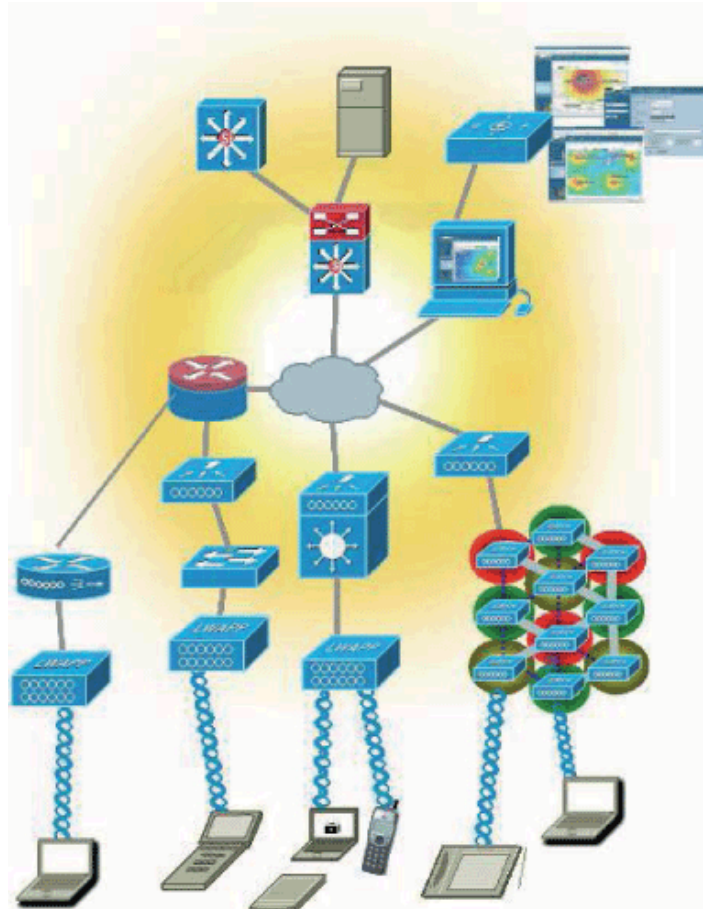
Cisco Unified Wireless Network は、業界標準 (IEEE 802.11、ドラフトの IETF CAPWAP 標準など) に基づいており、クライアント デバイスおよびアクセス ポイントからネットワーク インフラストラクチャ、ネットワーク管理、高度なワイヤレス サービス、表彰対象となった世界規模での 24 時間体制の製品サポートまで、WLAN のすべてを網羅した総合的なエンドツーエンド ソリューションです。Cisco Unified Wireless Network の主要なコンポーネントは次のとおりです。

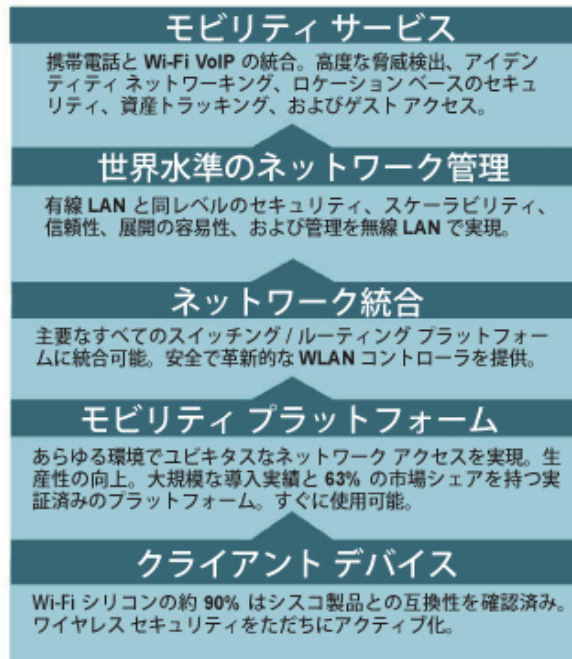
- **モビリティ サービス** : Voice over Wireless LAN (VoWLAN)、高度な無線侵入検知および防御、正確なロケーション トラッキング、ゲスト アクセス、およびサービスをビジネス固有のデバイス (POS、バーコード スキャンなど) に提供します。
- **世界水準のネットワーク管理** : 中央集中型の管理により、有線 LAN と同じレベルのセキュリティ、スケーラビリティ、信頼性、および展開の容易性を実現します。
- **Wireless LAN Controller** : 革新的な中央集中型のインテリジェンスにより、高度なサービスを実現します。有線ネットワーク統合は、選択したスイッチングルーティング プラットフォームとの統合により実現します。

- **アクセス ポイント**：屋内の展開から屋外の NEMA エンクロージャ ブリッジング/メッシュ ソリューションまで、さまざまなシナリオで業界最先端のアクセス ポイントを使用できます。
- **モバイル クライアント**：このソリューションは、ビジネスおよびセキュリティの要件を満たすさまざまなクライアントを提供します。Wi-Fi シリコンの約 90% は Cisco Compatible であることが認定されており、ピーク時のパフォーマンスと相互運用性が保証されます。

Cisco Unified Wireless Network は、長年にわたるユーザの経験と業界最大の導入実績に基づいており、クライアントからアプリケーション レイヤまで、WLAN 全体でエンドツーエンドにモビリティ サービスに対応する唯一の統合ソリューションです。シスコは常に、クライアントがネットワークで果たす重要な役割に留意しています。VoWLAN や RF Identification (RFID) など、業界をリードするサービスを提供するために、シスコはネットワークのあらゆるレイヤにモビリティを組み込み、有線 LAN と同等の信頼性をクライアントにおいて実現できるようにしています。セキュリティ、サービス品質 (QoS)、高速かつ安全なローミングなどの高度な機能をクライアントで有効にすることで、一貫したエンドユーザ エクスペリエンスを容易に実現できます。

図 1 Cisco Unified Wireless Network アーキテクチャでの複数サービスの利用





### 投資回収率の改善

運営予算が厳しい状況であるにもかかわらず、WLAN の市場は拡大しています。その理由は単純で、ワイヤレス ネットワーキングが優れた投資対象であるためです。ワイヤレス ネットワーキングは、生産性の向上、資本コストと運用コストの削減、および収益の改善を実現します。NOP World の調査により、WLAN は従業員の生産性を平均 22% 向上させることがわかりました。このように生産性が向上するのは、ユーザが E メールの確認、会議のスケジューリング、およびファイルやアプリケーションへのアクセスを、会議室、教室、同僚のデスク、およびビルや社内のその他のほぼすべての場所から実行できるためです。

Cisco Unified Wireless Network を実装すると、企業は次のようなプラスの成果を上げることができます。

- 総所有コストの削減
- 従業員のコラボレーションの強化
- 従業員のモビリティの向上

### 総所有コストの削減

総所有コスト (TCO) は、営利目的の企業のネットワークに限らず、駐屯軍や戦地の軍人など、政府機関のアプリケーションにとっても重要な要素です。Cisco Unified Wireless Network により、次のような TCO 削減を実現できます。

中央集中型の管理により、IT スタッフは Wireless LAN Controller からネットワークを設定および管理し、すべてのアクセス ポイントに更新を適用できます。これにより、初期設定やソフトウェアの継続的なメンテナンスまたはアップグレードのコストが削減されます。また、集中管理されていないネットワークで設定またはアップグレードを行う場合は、アクセス ポイントごとに平均 20 分の作業が必要になると仮定すると、スタッフの工数も削減できます。

通信機能ごとに独立したネットワークを持つ多くのシステムと異なり、Cisco Unified Wireless Network は、音声、ビデオ、およびデータ通信を統合型の WLAN で実現します。これにより、システムとデバイスの数を削減し、高コストのメンテナンス計画を縮小または中止することができます。

シスコのワイヤレス アーキテクチャは業界標準に基づいているため、ユーザは独自の RF 要件を満たす最高クラスのソリューションを選択できます。IETF Control and Provisioning of Wireless Access Points (CAPWAP) ワーキング グループは、CAPWAP プロトコルの基盤として Lightweight Access Point Protocol (LWAPP) を選択しました。この標準が浸透するにつれて、業界全体で総所有コストが削減され、機能と相互運用性が向上するものと思われます。

シスコは、侵入検知、ロケーション サービス、およびワイヤレス クライアント アクセスを組み込んだ業界唯一の統合型ワイヤレス ネットワーク ソリューションを提供します。ネットワークの計画にあたって、ほとんどのベンダーでは、無線がオーバーレイ アーキテクチャであり、侵入検知および RFID 機能は追加のオーバーレイと見なします。シスコは、無線テクノロジーを有線ネットワークに統合し、Wireless Intrusion Detection System (WIDS) とアクティブな RFID トラッキングを 1 つのソリューションに統合します。この統合ソリューションにより、資本コストと運用コストの両方が大幅に削減されると同時に、モバイル従業員の生産性が向上します。

#### コラボレーションの強化

組織では、より少ない労力でより多くの作業を行うことが求められるようになってきています。ワイヤレス ソリューションはコラボレーションの機会を増やすことでこの課題に対応します。

Cisco Unified Wireless Network を使用すると、従業員は、会議室やデスクなど、どこからでも E メールを送受信したり、ネットワーク サーバ上の情報にアクセスして、時間を節約できます。

Cisco Unified Wireless Network と Voice over WLAN ソリューションを組み合わせれば、従業員は企業内のどこにいてもお互いに連絡を取り合うことができるため、圏外に入ると接続できない携帯電話に依存する必要がなくなります。

#### 従業員のモビリティの向上

変化を続ける経営状況への迅速な対応は、現在の世界経済において不可欠です。Cisco Unified Wireless Network を使用して、この課題に対応できます。

モバイル従業員は、ローカル オフィスから迅速かつ簡単にネットワークに接続して、E メールを取得し、音声通信を受信できます。IT スタッフによる事前の設定は必要ありません。これにより、固定の就業場所を確保する必要がなくなり、コストを削減できます。

IT スタッフは、少ないリソースで、新しいロケーションや容量を迅速に追加できます。集中管理された WLAN により、ネットワークの移動、追加、および変更が簡単になります。いくつかのアクセス ポイントと Wi-Fi 対応のノート型パソコンがあれば、一時的な就業場所が迅速に用意できます。

自動 RF 管理は WLAN カバレッジの変更を常に検出し、RF 環境の変化によるホールやデッド スポットを補正することで、ネットワークの停止に対処します。

## シスコの差別化ポイント

シスコは、WLAN ソリューションの分野では世界のリーダー的存在であり、企業向け製品の市場シェアは 63% を超えています。2003 年には Wireless LAN Magic Quadrant リーダーとして Gartner Group から承認されており、包括的な統合型の有線/無線ソリューションを提供しています。WLAN の展開が、重要性の低いアプリケーションをサポートする個別の領域から、ワイヤレス VoIP やエンタープライズ リソース プランニングのようなミッションクリティカルなアプリケーションを実行する企業全体のネットワークに発展するにつれて、統合ソリューションの重要性も飛躍的に増大しました。Cisco WLAN ソリューションの長所は次のとおりです。

### 唯一の統合型無線/有線ソリューション

企業全体を対象とする広範囲の WLAN 展開によって、レイヤ 2 およびレイヤ 3 の有線インフラストラクチャ内で無線固有の機能を統合するための技術開発が推進されてきました。この機能の統合には、ネットワークの帯域幅、セキュリティ、冗長性、および管理機能が含まれており、拡張のための強力なプラットフォームが提供されます。シスコは業界に先駆けて、Cisco Catalyst® 6500 シリーズ Wireless Services Module (WiSM) およびサービス統合型ルータ用の Cisco Wireless LAN Controller モジュールによる次世代型の WLAN ソリューションを発表しました。

### 業界をリードするセキュリティ

ワイヤレス エンドポイント（ノート型パソコン、PDA、スマートフォンなど）の数が急激に増加するにつれて、ワイヤレス ネットワークを保護するだけでは、企業全体のセキュリティとしては不十分になっています。企業ネットワークは、無線メディアが原因である脅威の危険にさらされています。IEEE 802.11i、無線侵入検知および防御、および Cisco Network Admission Control（シスコ自己防衛型ネットワーク構想の重要なコンポーネント）により、シスコはワイヤレス ネットワークと企業ネットワークの両方を、リモート ユーザ、モバイル従業員、またはワイヤレス クライアントがもたらす脅威から保護します。

### 豊富な機能と標準への対応

Cisco Unified Wireless Network には、自動 RF 管理、ユーザとクライアントのタイプごとに異なる複数のサービス レベルなどの業界をリードする機能が用意されており、卓越した QoS およびセキュリティ レベル、VoWLAN、Wi-Fi デバイスと RFID タグのロケーション ट्रacking を実現します。Cisco Unified Wireless Network サービスは、IEEE 802.11、近々リリース予定の IETF CAPWAP など、業界標準に対応した強力な基盤の上に構築されています。つまり、このサービスはお客様の既存の投資内容と簡単に統合できます。たとえば、Cisco Catalyst 6500 Wireless Services Module を使用する展開では、既存のインフラストラクチャの強力なセキュリティ、音声、および高可用性機能を活用します。

標準がまだ提供されていない場合、シスコは、新しい機能がマルチベンダー環境で使用できるように業界全体を主導します。Cisco Compatible Extensions プログラムはそのような活動の一例で、新しい機能の実装を迅速に進め、Wi-Fi クライアント市場の 90% を超えるようにすることを目指します。

### 管理性とスケーラビリティ

表彰実績のあるシスコの管理機能を使用して、最大数千のアクセス ポイントを設定および監視できます。新しいアクセス ポイントを自動的に認識して正しく設定することで、大規模なオフィスと同じセキュリティ プロトコルをリモート オフィスでも使用できるようにします。中央集中型の管理により、ネットワーク管理者は手作業から解放され、WLAN ネットワークを大規模エンタープライズの要件にも対応するように拡張できます。

### 可用性と信頼性

シスコの自動 RF 管理、冗長性に対応した Wireless LAN Controller クラスタリング、およびインテリジェントなネットワーク モニタリングにより、可用性の高い WLAN ソリューションを容易に実現できます。リモート ブランチ オフィスへの WAN 接続に障害が発生した場合、WAN リンクが修復されるまで、Cisco Unified Wireless Network ソリューションをローカルで管理できます。Cisco Aironet<sup>®</sup> アクセス ポイントは、コアなセキュリティ機能とQoS 処理をローカルで実行するため、WAN リンクがオーバーサブスクライブされることはなく、お客様は、予測可能で一貫したレベルのサービスを利用できます。

### テストおよび実証

シスコのテスト ラボにより、Cisco Unified Wireless Network のエンドツーエンド ソリューションが管理性、スケーラビリティ、アベイラビリティ、および信頼性が保証されます。ネットワーク オペレータは、シスコの包括的な設計ガイドを利用することで、Cisco Unified Wireless Network ソリューションを簡単かつ確実に実装および管理できます。このソリューションは、世界中に展開された WLAN ソリューションと約 300 万のシスコ アクセス ポイントを使用する 70,000 を超えるシスコのお客様によって実証済みです。

### まとめ

Cisco Unified Wireless アーキテクチャは、業界をリードするモビリティ サービスが最先端の安全な環境でサポートされるように設計されています。この環境により、複数のメディアを使用する従業員がいつでも、どこからでもネットワークに接続できるようになり、エンドユーザ エクスペリエンスが向上します。このアーキテクチャは、安全でスケーラビリティと柔軟性を備え、容易に管理できる、ビジネス目標の達成に役立つソリューションを提供します。WLAN に関する幅広い経験に基づき、従業員の生産性の向上、顧客満足度の向上、コストの削減、およびビジネスへの適用力の向上を実現する WLAN ソリューションを提供することによって、シスコはお客様のネットワークの価値の向上をサポートします。

### 技術概要

ワイヤレス ネットワーキング テクノロジーは、この数年、さまざまなビジネスに好影響を与えてきました。たとえば、クライアントにモビリティを提供し、リモート領域での接続コストを削減し、小売市場での生産性を向上しました。小売市場では、ワイヤレス テクノロジーは POS アプリケーションで幅広く使用されています。多くの政府機関は、標準が設定されたワイヤレス テクノロジー特有のセキュリティの脆弱性により、これらの利点を活用していませんでした。この数年間で、802.11 プロトコルの向上により、WLAN セキュリティが強化されました。まず、安全性に問題のある Wireless Equivalence Privacy (WEP) に始まり、次に Wi-Fi Protected Access (WPA)、そして 2004 年 6 月にワイヤレス セキュリティの新しい標準を設定する IEEE ratified 802.11i が発表されました。

3 つの主要な連邦政府政策とガイドラインにより、安全なエンタープライズ ワイヤレス アーキテクチャを設計するための要素が設定されています。その内容は次のとおりです。

- **DoD 8100.2** : 「Use of Commercial Wireless Devices, Services and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)」
- **DoD 8100.2** : 「Use of Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)」
- **NIAP Common Criteria** : 「U.S. Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments」

最初の文書は、国防長官府が発行したもので、DoD 公開鍵インフラストラクチャ (PKI) に従って、強力な認証、否認防止、および個人識別情報を使用することを義務付けています。また、確実なチャネルを経由したワイヤレス トラフィックの暗号化、および FIPS140-2 の検証が必須である旨明言されています。さらに、無線侵入検知、サービス拒否攻撃の低減、およびワイヤレス デバイスのアクティブなスクリーニングも義務付けられました。

2006 年 6 月、DoD は DoD 8100.2 を補足するガイダンスとして、2 番目の文書を発行しました。この文書では、レイヤ 2 暗号化の新しい標準は 802.11i/WPAv2 であり、Extensible Authentication Protocol Transport Layer Security (EAP-TLS) を使用してユーザ認証を実行することが義務付けられました。

3 番目の文書では、は脅威の少ない環境で使用される商用ワイヤレス システムを対象として、WLAN に対する 攻撃を緩和するために階層化セキュリティで必要な Protection Profile、およびシステムの個別のコンポーネントではなく全体的なセキュリティ要件と機能要件が指定されました。また、FIPS 140-2 で承認された暗号化も必須となりました。

Cisco Unified Wireless アーキテクチャは連邦政府のワイヤレス ポリシーと認証要件に対応すると同時に、堅牢で豊富な機能を備えた、低コストの統合型ソリューションを提供します。FIPSCertified 802.11i アーキテクチャには以前の展開とは大きく異なる概念が採用されています。これにより、連邦政府機関も標準ベースのネットワークキングの経済性の恩恵にあずかることができるようになりました。

エンタープライズ ワイヤレス アーキテクチャのあらゆる側面を保護するために、ネットワーク全体の各レイヤにセキュリティ メカニズムを設定する必要があります。送信中のデータの暗号化はプライバシーだけを保証し、エンドツーエンドのセキュリティは保証しません。シスコは WLAN セキュリティ対策として、次のようなさまざまな保護機能を提供しています。

- **RF セキュリティ** : 802.11 干渉を検出して回避し、不要な RF の伝播を抑制します。
- **WLAN の侵入防御と特定** : 不正なデバイスまたは潜在的なワイヤレス上の脅威を検出し、これらの位置を特定します。これにより、IT 管理者は脅威のレベルをただちに判断し、必要に応じて迅速に脅威を軽減できます。
- **アイデンティティベースのネットワークキング** : 企業は、ユーザ アクセス権限、デバイス形式、およびアプリケーション要件別に、ワイヤレス ユーザまたはユーザ グループごとに個別のセキュリティ ポリシーを提供できます。たとえば、次のセキュリティ ポリシーを適用できます。
  - **レイヤ 2 セキュリティ** : 802.1X (PEAP、LEAP、TTLS)、WPA、802.11i (WPA2)、802.11w。
  - **レイヤ 3 (およびそれ以上の) セキュリティ** : 有線侵入防止システム (IPS) との統合。

- **アクセス コントロール リスト** : IP 制限、プロトコル タイプ、ポート、および Differentiated Services Code Point 値。
- **QoS** : 複数のサービス レベル、帯域幅契約、トラフィック シェーピング、および RF 使用率。
- **認証、承認、アカウントティング/RADIUS** : ユーザ セッション ポリシーおよび権限の管理。
- **Network Admission Control (NAC)** : クライアントの設定および動作に関連するポリシーを適用して、セキュリティ ポリシーに適合するエンドユーザ デバイスのみが、ネットワークへのアクセス権を取得するようにします。
- **セキュアなモビリティ** : Cisco Proactive Key Caching を使用して、モバイル環境のセキュリティを最高レベルで維持します。Cisco Proactive Key Caching は、802.11i 標準の拡張機能であると同時に 802.11r 標準の先行機能であり、Advanced Encryption Standard (AES) 暗号化と RADIUS 認証を使用してセキュアなローミングを可能にします。

Cisco Unified Wireless アーキテクチャは、セキュリティに対する階層的なアプローチにより、次の 3 つの重要なタスクに対応するコンポーネントに分割できます。

- クライアント アクセスの制御
- クライアントの正真性の確保
- ネットワークの保護

#### クライアント アクセスの制御

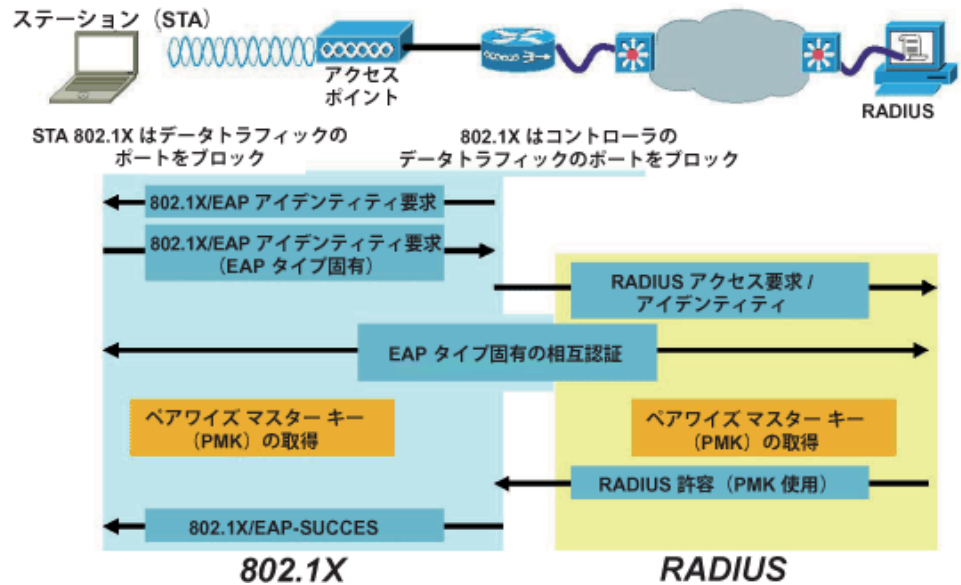
セキュリティに関する新しいポリシーとガイドライン、特に最近の 802.11i 標準に対する要求を考慮すると、連邦政府機関がワイヤレス ネットワークが安全であることを確認するためにはどのような手順が必要でしょうか。最初の最も重要な手順は、クライアント アクセスを制御することです。そのためには、適切なクライアント認証とデータ暗号化を使用して、ワイヤレス ネットワークの信頼性を確保する必要があります。

#### 認証

ネットワーク アクセス コントロールは、政府機関のワイヤレス アーキテクチャのセキュリティにとって基盤となるものです。ワイヤレス メディアへのアクセスを制限し、ユーザを認証する必要があります。IEEE 802.1x 標準は、ユーザベースまたはマシンベースの認証のためのトランスポート メカニズムとして使用されます。これはメディアレベルのアクセス コントロールに対応した標準であり、ネットワーク接続の許可または拒否、VLAN アクセスの制御、およびトラフィック ポリシーの適用の各機能を提供します。802.1x プロトコルは 802.11 ワイヤレス標準セットの一部ではなく、高レベルの認証プロトコルを伝送するために使用される標準のリンクレイヤ プロトコルです。802.1x 認証では、ワイヤレス エンド デバイスに存在するサブリカント (クライアント)、ネットワーク アクセス サーバ (WLAN コントローラ)、および認証者 (Cisco Secure Access Control Server) の 3 つの重要な要素が対話します。認証に成功するまで、クライアントからネットワークにネットワーク トラフィックを送信することはできません。クライアントは認証されるまで IP アドレスを取得できないため、IP 接続を必要とするログイン スクリプトまたはその他の認証メカニズムは、認証が完了するまで成功しません。FIPS で検証されたアーキテクチャでは、802.1x サブリカント、アクセス ポイント、およびワイヤレス LAN コントローラも FIPS 140-2 に適合している必要があります。

802.11i 標準の採用の一部として、Extensible Authentication Protocol (RFC 3748 で指定された) を使用してクライアント認証を送信する必要があります。当初はポイントツーポイント プロトコル (PPP [RFC 1661]) で使用するように設計されたため、EAP は 802.1x ベースのネットワークに対応していました。EAP メッセージは 802.1x パケットで認証情報を送信します。EAP-TLS、Protected EAP (PEAP)、EAP-Flexible Authentication via Secure Tunneling (EAP-FAST) など、複数の EAP メソッドを使用できます。

図 2 EAP 認証の概要



DoD 8100.2 の 6 月の補足では、802.11i をレイヤ 2 暗号化の新しい標準として定め、DoD ポリシーに従って、PKI を使用する相互認証に EAP-TLS を使用することも指定しました。(RFC 2716 で指定された) EAP-TLS は TLS を使用する認証プロトコルで、暗号スイート (暗号パラメータ) ネゴシエーション、相互認証、および鍵管理機能を提供します。EAP-TLS では、PKI が発行したデジタル証明書を使用して、認証サーバでサブリカントを認証し、必要に応じてサブリカントで認証サーバを認証します。

認証サーバを起動するには、デジタル証明書をサブリカントに送信します。現在、Secure Sockets Layer (SSL) は Web で使用される最も一般的な認証方法です。SSL は一方向の認証です。つまり、サーバがブラウザに証明書を送信してアイデンティティを証明します。ただし、EAP-TLS では相互認証を使用して man-in-the-middle 攻撃からネットワークを保護します。

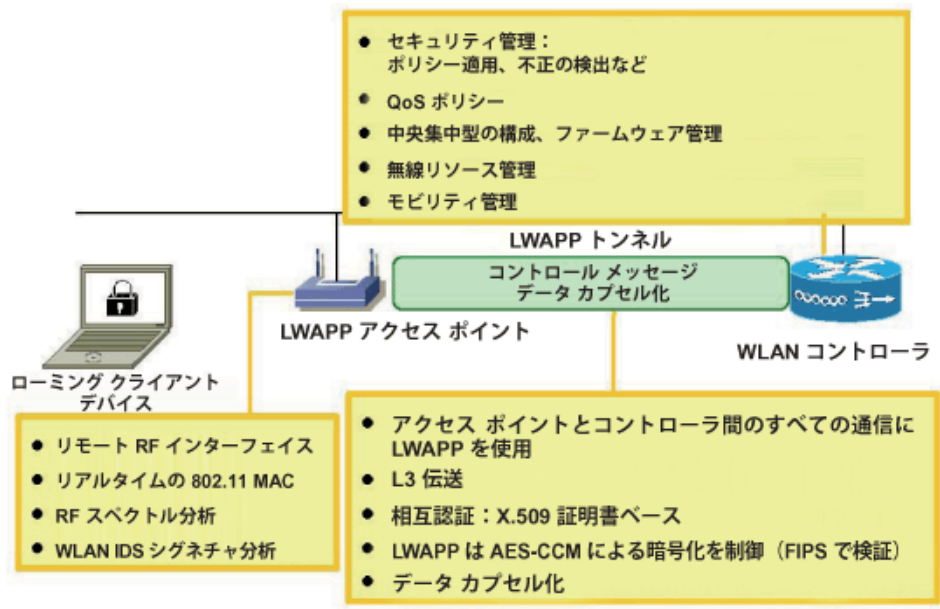
最後に、TLS が FIPS 140-2 検証を実行し、認証メッセージを安全に暗号化して送信するために、TLS プロトコルが連邦政府の暗号化標準を満たしていることを認定します。

EAP-TLS と 802.1x を導入して安全なワイヤレス環境を構築する場合、クライアント証明書とマシン証明書の 2 つの認証方法を使用できます。ほとんどの場合、EAP-TLS 認証に使用される X.509 証明書は、スマート カード (コモン アクセス カード (CAC)) によって提供されます。DoD 導入時の EAP-TLS の影響をわかりやすくするために、付録 A で、PKI 認証に使用される CAC (スマート カード) の概要について説明しています。展開要件に応じて、ネットワークへのアクセスを提供するために、クライアント証明書とマシン証明書の両方を識別情報として使用できます。

## 暗号化

Cisco Unified Wireless アーキテクチャには LightWeight Access Point Protocol (LWAPP) が不可欠です。LWAPP は、IETF CAPWAP ワーキング グループの基盤である IETF RFC ドラフト文書によって定義されています。CAPWAP ワーキング グループは最終的に業界標準のワイヤレス制御プロトコルを作成する予定ですが、現在のところは LWAPP が最も完成度の高いプロトコルです。付録 B に、LWAPP の詳細に関する追加情報が記載されています。送信中のワイヤレス データが暗号化されるだけでなく、初期認証プロセスのすべてのフェーズが FIPS で検証された暗号化アルゴリズム (AES 128 ビット鍵を使用) を使用して保護されます。クライアント ステーションからアクセス ポイント (AP) へのすべてのユーザトラフィックが、802.11i 仕様に従って暗号化されます。設定情報を送信するために AP とワイヤレス LAN コントローラ (WLC) の間で使用される LWAPP コマンドおよび制御チャネルは、暗号化され、FIPS で検証されます。WLC と RADIUS サーバ間の RADIUS トラフィックはすべて、(IETF の「draft zorn-radius-keywrap-10」で指定された) RADIUS キーラッププロトコルを使用して暗号化されます。このエンドツーエンドのセキュリティ アプローチにより、EAP 認証、アクセス ポイント設定、および 802.11i 暗号鍵配布におけるすべての側面が保護されます。このシスコ独自アプローチにより、多層防御のセキュリティ フレームワークが提供され、1 台のデバイスの脆弱化によりネットワーク全体にアクセスできるようになることを防止します。

図 3 Cisco Secure Wireless アーキテクチャのエンドツーエンドのセキュリティ アプローチ



## 送信中のデータの暗号化 : 802.11i

ワイヤレス ネットワークでステーションまたはユーザが認証されたあと、そのネットワークでの伝送中にデータがハイジャックまたは脆弱化されないようにすることが重要です。送信中のデータの正真性を保持するには、暗号化テクノロジーに基づいた標準を使用することが最善の方法です。802.11i 標準は、主にワイヤレス セキュリティのこの領域に重点を置いています。802.11i 仕様では、AES in Counter mode CBC-MAC (AES-CCM) 128 ビット鍵の使用が送信中のデータの正真性を保証するために義務付けられ、Temporal Key Integrity

Protocol (TKIP) に対する規定が下位互換性のために 802.11i 標準の一部として追加されました。FIPS で検証されたモードで動作する場合は、FIPS が検証できない RC4 暗号化アルゴリズムを使用するため、TKIP を無効にする必要があります。AES-CCM は、機密性を確保するためのカウンタ、1 つの鍵で信頼性を確保するための CBCDC を含む、認証された暗号化モードを使用します。また、認証、正真性、およびプレイ保護を実現するために Cipher Block Chaining Message Authentication Code (CBC-MAC) を使用し、TKIP の 20 ビット Message Integrity Check (MIC) を上回る 64 ビットの MIC を提供します。IEEE 802.11i 仕様は最も堅牢なレイヤ 2 セキュリティを連邦政府機関に提供すると同時に、FIPS 140-2 要件に対応し、標準ベースの仕様としてベンダー間の相互運用性を向上します。

### コントロールプレーン暗号化

LWAPP コントロールプレーンは、AP が WLC に最初に接続するときのデバイスの相互認証、およびすべての LWAPP コントロールメッセージのコントロールメッセージペイロードの暗号化によって保護されます。LWAPP コントロールメッセージペイロードは、FIPS 140-2 で検証された業界標準の AES-CCM アルゴリズムを使用して暗号化されます。

LWAPP コントロールプレーンがどのように保護されるかを説明する前提として、まず次の主要な事項を確認する必要があります。

- AP と WLC の保護されたフラッシュに X.509 証明書が焼き付けられていること。
- X.509 証明書が、製造時にデバイスに焼き付けられた秘密鍵によって署名されていること。AP と WLC の両方に、適切な公開暗号鍵がインストールされています。
- AP と WLC に、(AP または WLC 証明書の) 発行元の認証局を信頼できる証明書がインストールされていること。

AP が WLC に結合要求を送信すると、LWAPP メッセージに X.509 証明書が埋め込まれます。また、ランダムセッション ID が生成され、LWAPP 結合要求に追加されます。WLC は LWAPP 結合要求を受信すると、AP の公開鍵を使用して X.509 証明書の署名を検証し、証明書が信頼できる認証局によって発行されたことを確認します。また、AP 証明書の有効期間の開始日時を参照し、X.509 証明書の日時と比較します。X.509 証明書が有効な場合、WLC はランダムな AES 暗号鍵を生成します。次に、WLC は AP の公開鍵を使用して鍵を暗号化し、作成された暗号文と結合要求のセッション ID を連結したあと、独自の秘密鍵を使用して連結された値を暗号化します。WLC は結果を X.509 証明書とともに LWAPP 結合応答にコピーします。AP は LWAPP 結合応答を受信すると、WLC の公開鍵を使用して WLC 証明書の署名を検証し、証明書が信頼できる認証局によって発行されたことを確認します。WLC 証明書が認証されると、AP は暗号化された鍵の部分を抽出します。AP は WLC の公開鍵を使用して連結された暗号文を復号化し、セッション ID を検証します。その後、秘密鍵を使用して AES 鍵を復号化します。

AP は鍵ライフタイムタイマーを保持します。タイマーの期限が切れると、AP は新しいセッション ID を生成し、WLC への LWAPP 鍵更新要求メッセージに埋め込みます。WLC は前に説明した鍵生成および配布プロセスを繰り返し、新しい暗号文を LWAPP 鍵更新応答に埋め込みます。鍵ライフタイムタイマーは 8 時間です。

## 認証/RADIUS 暗号化

2001年、NISTはドラフトのAESキーラップ仕様を公開しました。これはNISTで承認された暗号化プロトコルで、機密性の高い暗号化キー関連情報の送信への使用を想定したものです。これに続いて、RADIUS属性とAESキーラップアルゴリズムを使用して鍵を配布する安全な手段が提案され、現在IETFドラフトとして検討されています。

RADIUSキーラップサポートは、基本的にはRADIUSプロトコルの拡張機能であり、Cisco Secure ACSがRADIUSメッセージを認証してセッション鍵を配布するために使用される、FIPSで認定された手法です。RADIUSは(EAP-Message属性での)EAPメッセージの送信に使用されるため、RADIUSメッセージを安全に認証することで、EAPメッセージ交換も安全に認証されます。

RADIUSキーラップは、802.1x認証サーバ(Cisco Secure Access Control Server [ACS])からネットワークアクセスサーバ(NAS、Wireless LAN Controllerなど)に、802.11iペアワイズマスターキー(PMK)を安全に送信するために使用されます。次に、WLCはユーザ単位のセッション鍵またはPair Wise Transient Key (PTK)を取得し、FIPSで検証されたLWAPP暗号化制御チャネルを経由して適切なアクセスポイントに送信します。同時に、FIPSで検証されたWLANクライアントはEAP認証プロセスで取得された情報からPMKを生成したあと、セッション単位のPTKを生成します。認証プロセスでは、暗号化キー関連情報が保護されずに送信されることはありません。具体的には、キー関連情報(PMKまたはPTK)が、802.11ネットワークを経由してクライアントに送信されることはありません。

## クライアントの正真性の確保

クライアントの正真性を確保するために、ネットワークはモバイルコンピューティングに固有の問題に対処する必要があります。特に、コンピュータを使用して安全性の低い場所からネットワークにアクセスするモバイル従業員に関しては注意が必要です。前に説明したように、安全なネットワークはデータの正真性を維持し、不正なアクセスを避ける必要があります。また、クライアント上の異常な動作、およびクライアントによる異常な動作も報告する必要があります。

クライアントの安全性を維持するために、従来は、強力なウイルス対策やファイアウォールがモバイルデバイスにインストールされていました。しかし、安全なネットワークでは、不正利用(ネットワーク内の悪意のある、または不正なアクティビティ)と侵入(ネットワーク外部からの侵害)の両方を特定できる、ホストベースの侵入検知システム(IDS)も使用する必要があります。

## ホストベースのIDS

ホストベースのIDSは、インバウンドとアウトバウンドのポートブロッキング、フラグメント化されたパケット攻撃からの保護、および「回避」技術を使用する攻撃からの保護を行う必要があります。また、設定可能なIDSルール、アプリケーション実行保護、およびロケーション対応の保護も必要です。

ウイルスやワームはエンドポイントに感染するうえに、しばしば急速に増殖することでネットワーク輻輳までも引き起こします。シスコでは、Cisco Security Agentというエンドポイント侵入防御機能を提供することで、双方の問題への対処を開始しました。Cisco Security Agentは新しい動作セキュリティを使用してウイルスやワームを検出し、ウイルスやワーム

がエンドポイント システム上で拠点を確保したり、ネットワークに拡散することを防ぎます。実際には、Cisco Security Agent はウイルスやワームの拡大に対する一次抑制装置になります。

Cisco Security Agent を展開するもう一つの重要な理由は、エンドポイントとネットワーク間のフィードバック ループの確立に使用されるエンドポイント上に設置することで、ネットワークが新たな脅威にも迅速に対応できるためです。Cisco Security Agent は、サーバおよびデスクトップ コンピューティング システムを脅威から保護します。Cisco Security Agent は、複数のセキュリティ機能を集約し、ホスト侵入防御機能、分散ファイアウォール機能、悪意のあるモバイル コードに対する保護、オペレーティング システムの真正性の保証、および監査ログの統合を、1つのエージェント パッケージに統合します。Cisco Security Agent は全体的なセキュリティ戦略のうち、多層防御のアーキテクチャに追加されるエンドツーエンドのセキュリティ アプローチを実現します。

猛威を振るった Code Red や SQL Slammer ワームなどの事例からもわかるように、進化する新種の攻撃に対しては、従来のホストおよびデスクトップ セキュリティ テクノロジーでは対応に限界があります。従来のシグニチャ マッチングによるセキュリティ テクノロジーとは異なり、Cisco Security Agent は動作を解析することで、少ない運用コストで堅牢なセキュリティ保護を実現します。Cisco Security Agent は、不正な動作が発生する前に識別して阻止することで、企業ネットワークやアプリケーションを脅かす潜在的な既知または未知（「Day Zero」）のセキュリティ リスクを除去することができます。

### ネットワーク アドミッション コントロール

ワイヤレス ネットワークを安全に保つために、802.1X を使用してクライアント アクセスを制御する以外に、ワイヤレス ユーザのために定期的なポスチャ評価および修正サービスを行う必要があります。ポスチャ評価を使用してクライアントの真正性を定期的に検証することでネットワークでエンドポイントに関する規制の遵守が強制され、適切なセキュリティ パッチ、ウイルス ソフトウェアが適用され、かつセキュリティ ポリシーに適合したモバイル デバイスにのみアクセス権が付与されます。デバイスが適合していない場合、適合していないマシンを遮断、分離、および修復することで、ネットワークでセキュリティ ポリシーが強制されます。マシンは検疫エリアへリダイレクトされ、管理者の判断に応じて修復されます。

クライアントの真正性を確保するために、次のセキュリティ機能が用意されています。

- Web ログイン認証（RADIUS、Kerberos、LDAP、NTLM など、1つ以上の認証サーバを導入）
- カスタム スプラッシュ Web ページ（管理対象のサブネット、VLAN、またはオペレーティング システムごとに異なる）
- レイヤ 3/レイヤ 4 のロールベース アクセス コントロール（RBAC）（特定のポート、プロトコル、またはサブネットへのアクセスを許可）
- ユーザ ロールごとの帯域幅スロットリング（共有または専用の帯域幅使用を割り当て）
- ゲスト セッションのタイムアウト管理（ビジターの場合は 2 時間、従業員の場合は 24 時間など）
- 事前に定義されたページへのカスタム URL リダイレクション（受け入れ可能なユーザ ポリシー通知に使用）

- 事前に設定された、Windows の重要なホットフィックスとウイルス対策アプリケーションの確認
- 隔離されたユーザの自己修復

### ネットワークの保護

ネットワークを保護するために、連邦政府機関には、階層的なセキュリティ アプローチを使用する多層防御アーキテクチャが必要です。セキュリティ アーキテクチャには、ワイヤレス 侵入検知システム (WIDS)、ロケーション サービス、および管理フレーム保護 (MFP) のための新しい IEEE 802.11w 標準の 3 つのコンポーネントが必要です。

ワイヤレス ネットワークは WIDS を使用して、不正なアクセス ポイントとクライアントを検出および抑制し、802.11 ベースの攻撃をスキャンします。システムは、不正なデバイスを追跡するだけでなく、その場所を特定し、攻撃が開始されるかどうかを判断して、可能な限り迅速にネットワークから除去する必要があります。インテリジェントなオフ チャネル スキャンにより、不正をその場で迅速に検出できます。

ロケーション サービスは、不正なクライアントの検出および抑制において、実証済みの優れた機能を提供します。これらのサービスにより、ワイヤレス ネットワークにアクセスするクライアントを効率的に追跡できます。また、次の 4 つの事項を明確にしておくことで、ワイヤレス ネットワークの透過性が向上します。

- 既存のデバイスの種類
- 既存のデバイスの数
- 既存のデバイスの場所
- 既存のデバイスの状態

ロケーション サービスでは、物理的な場所に基づいてアクセスを許可することで、クライアントを別のレベルで制御します。たとえば、クライアントが規定の領域を離れると同時に、ワイヤレス ネットワークへのクライアント アクセスを切断できます。

ワイヤレス IDS/IPS は、ワイヤレス DoS 攻撃 (サービス拒絶攻撃) のみを検出するため、レイヤ 3 IP DoS 攻撃を誤って開始する可能性がある有効な認証済みユーザを保護できないという制限があります。シスコでは、有線および無線のセキュリティ システムを統合することで、統合されたセキュリティ アーキテクチャを作成するための総合的なアプローチを行ってきました。Cisco Unified Wireless アーキテクチャとシスコの有線 IPS デバイスを組み合わせることで、IPS デバイスは、ネットワークを経由して不正なレイヤ 3 トラフィックを送信するアソシエートされたクライアント デバイスを検出できます。その後、有線 IPS デバイスは Wireless LAN Controller に遮断要求を送信します。これにより、ネットワーク エッジのクライアント デバイスを効率的に遮断/アソシエーション解除し、セキュリティ制御を周辺機器まで拡張できます。

新しいワイヤレス標準である 802.11w は、管理フレーム保護 (MFP) を提供します。MFP は、認証された署名付きの MAC (AES Hashed Message Authentication Code [HMAC]) を追加することで、クライアントと AP の間の管理フレーム通信を保護します。802.11 で使用される管理フレーム通信が開放的であることが原因で起こる、さまざまな攻撃やセキュリティ リスクからクライアントを保護します。これにより、異常がただちに検出され報告されます。

シスコの 802.11w 以前の実装は Management Frame Protection (MFP) と呼ばれています。アクセス ポイントとクライアント ステーションの間でやり取りされる、保護および暗号化されていないその他の 802.11 管理メッセージにセキュリティ機能を提供します。

MFP には、次の 2 つの機能が用意されています。

- ・ インフラストラクチャのサポート
- ・ クライアントのサポート

インフラストラクチャのサポートにより、スプーフィング イベントを迅速かつ正確に検出できます。署名付きビーコンと組み合わせることで、WLAN 上の最新型の攻撃であるフィッシングを効率的に検出して報告できます。(クライアント ステーションではなく) アクセス ポイントが生成する管理フレームに MIC 情報要素を追加することで、802.11 セッション管理機能を保護します。次に、ネットワーク内の他のアクセス ポイントによってこのアクセス ポイントが検証されます。

クライアントのサポートにより、偽造されたフレームから認証済みのクライアントを保護し、WLAN に対する一般的な各種攻撃の多くを無効にします。ほとんどの攻撃(非認証攻撃など)は、復元しても有効なクライアントとの競争によりパフォーマンスを低下させるだけです。これにより、スプーフィングされた管理フレーム(認証およびアソシエートされた AP とクライアント ステーションの間でやり取りされる管理フレーム)を廃棄することで、AP とクライアントの両方が予防処置を講じることができるようになり、AP と FMP に対応したクライアント ステーションの間で送信される管理フレームが暗号化されます。データ フレームの場合と似たような方法で AES-CCM を適用することで、ネットワークは管理フレームを保護できます。

## チェック事項のまとめ

無線ネットワークポリシー	クライアント認証	IDS/IPS
<p><b>クライアント アクセスの制御</b></p> <ul style="list-style-type: none"> <li>・ 強力な相互認証</li> <li>・ 強力な暗号化</li> <li>・ 本格的なワイヤレス IPS</li> <li>・ 適応性可能なクライアント ポリシー</li> </ul>	<p><b>クライアントの正 真性の確保</b></p> <ul style="list-style-type: none"> <li>・ ネットワーク アドミッション コントロール</li> <li>・ 動的なリアルタイムのポリシー アップデート</li> </ul>	<p><b>ネットワークの保護</b></p> <ul style="list-style-type: none"> <li>・ 不正な AP の検出と抑制</li> <li>・ マルチレイヤのクライアント排除</li> </ul>
<ul style="list-style-type: none"> <li>✓ 802.1X</li> <li>✓ FIPS WPA2 (AES)</li> <li>✓ Management Frame Protection</li> <li>✓ Cisco CSA</li> </ul>	<ul style="list-style-type: none"> <li>✓ 有線および無線対応の Cisco NAC</li> <li>✓ Cisco CSA</li> <li>ゲスト: 統合型のキャプティブポータル (トラフィック トンネリング使用)</li> </ul>	<ul style="list-style-type: none"> <li>✓ 不正の検出</li> <li>✓ 不正の抑制</li> <li>✓ ロケーション サービス</li> <li>✓ セキュリティ 管理</li> </ul>

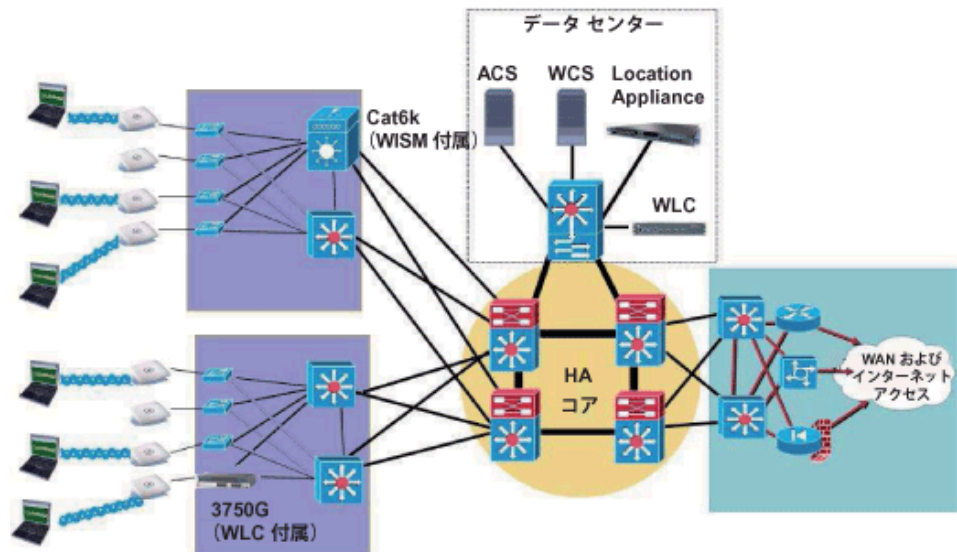
## アーキテクチャの設計

Cisco Unified Wireless アーキテクチャには、FIPS の検証要件を満たす 3 つの主要なコンポーネントがあります。無線侵入検知および防御に使用される他の 2 つのコンポーネントは、Common Criteria の認定のために NIAP に提出される WLAN アーキテクチャに必須です。

- FIPS で検証された Wireless LAN Controller (WLC)
- FIPS で検証されたアクセス ポイント
- Cisco Secure Access Control Server (RADIUS サーバ)
- 無線侵入検知/侵入防御
  - Wireless Control Software
  - Location Appliance

アクセス ポイントとコントローラをエンタープライズ アーキテクチャ内に配置することで、WLAN キャンパス展開の一般的なガイドラインと推奨事項に従うことができます (図 4 を参照)。

図 4 WLAN キャンパス展開の一般的なガイドライン



## アーキテクチャのコンポーネント

### Wireless LAN Controller

Cisco Wireless LAN Controller は、統合された侵入防御機能、リアルタイムでの RF 管理、手動操作なしの展開、N+1 冗長構成など、システムワイドな WLAN 機能を処理します。現在のレイヤ 2/レイヤ 3 インフラストラクチャの要件に応じて、ネットワーク上に展開できる FIPS で検証された WLC の 3 つのフォーム ファクタがあります。

- Cisco Catalyst 6500 シリーズ Wireless Services Module (WiSM) : Cisco WiSM は、Cisco Catalyst 6500 シリーズ レイヤ 3 スイッチと Supervisor 720 を展開したネットワークにシームレスに統合されます。WiSM は、業界をリードするセキュリティ、モビリティ、冗長性、TCO 削減、および使いやすさを、大規模な WLAN において実現します。WiSM は、ローミングドメインごとに最大 3600 のライトウェイト アクセス ポイントのクラスタリング能力を持つ、中規模および大規模企業の設備に対

象に設計されています。モジュールごとにライトウェイト アクセス ポイントを 300 まで拡張可能で、10,000 を超えるワイヤレス クライアント デバイスをサポートします。



Cisco Wireless Services Module

- Cisco Catalyst 3750G Integrated Wireless LAN Controller : この Cisco WLC は、1 つの論理ユニットで 50 ~ 200 のライトウェイト アクセス ポイントのサポートを必要とする中規模企業やブランチ オフィスで、安全なエンタープライズクラスのワイヤレス アクセスを展開します。論理ユニットは、最大 9 個の 3750G スイッチのスタックです。Cisco Catalyst 3750G Integrated Wireless LAN Controller は、集中型のセキュリティ ポリシー、ワイヤレス IPS 機能、表彰実績のある RF 管理、QoS、およびレイヤ 3 高速セキュア ローミングを提供します。Cisco Catalyst 3750G Integrated Wireless LAN Controller は、[Cisco Unified Wireless Network](#) の主要コンポーネントとして、優れた制御機能、セキュリティ、冗長性、および信頼性を備えています。そのため、有線ネットワークの場合と同等の拡張性と管理性を備えたワイヤレス ネットワークを実装できます。



Cisco Catalyst 3750G Integrated WLC

- Cisco 4400 シリーズ Wireless LAN Controller (スタンドアロン) : この WLC はネットワーク インフラストラクチャと完全に統合され、拡張セキュリティ機能、QoS ポリシーの実施などの高度なサービスを提供します。4000 シリーズ WLC のキャパシティ範囲は、12 のアクセス ポイントから最大 100 のアクセス ポイントまでです。これらのコントローラをクラスタ編成にすることにより、ローミングドメインごとに最大 2400 のアクセス ポイントをサポート可能です。



Cisco 4400 シリーズ WLC

## アクセス ポイント

Cisco Aironet Lightweight アクセス ポイントの 2 つのシリーズは、FIPS 140-2 検証の基準を満たしており、DoD 8100.2 ポリシーに準拠しています。1130 AG と 1240 AG の両方のアクセス ポイントが、優れたキャパシティ、レンジ、およびパフォーマンスを備え、管理しやすく信頼性の高い安全なワイヤレス接続を提供します。シングル無線またはデュアル無線、内蔵アンテナまたは外部アンテナ、堅牢な金属筐体など、幅広い展開方式に対応します。Cisco

Aironet アクセス ポイントは、WLAN に要求される多機能性、高容量、セキュリティ、およびエンタープライズ クラスの機能を提供します。これらのアクセス ポイントには、すぐに使用できるワイヤレス機能が標準装備されているので、手動操作での設定は不要です。どちらのシリーズも Cisco Wireless LAN Controller と Cisco Wireless Control System (WCS) によって完全に管理されます。WCS は WLAN の主要な機能を集中管理して、屋内外間の展開でスケーラブルな管理、セキュリティ、およびモビリティを実現します。

- Cisco Aironet 1130 AG シリーズ: このアクセス ポイントは、高容量、高度なセキュリティ、およびエンタープライズ クラスの機能を備え、WLAN アクセスの TCO を削減します。オフィスなどの RF 環境での WLAN を考慮した設計になっており、内蔵のアンテナや IEEE 802.11a/g デュアル無線によって、安定的で予測どおりのカバレッジを実現しながら、108 Mbps という総容量を提供します。
- Cisco Aironet 1240 AG シリーズ: この IEEE 802.11a/b/g アクセス ポイントは 1130 AG と同様のエンタープライズ クラスの機能を提供しますが、付け替え可能な多種類のアンテナ、堅牢な金属製エンクロージャ、幅広い動作温度といった厳しい要件を持つ RF 環境向けに設計されています。



Cisco Aironet 1130 AG シリーズおよび Cisco Aironet 1240 AG シリーズ アクセス ポイント

### Cisco Secure Access Control Server

Cisco Secure Access Control Server (ACS) は、ユーザおよび管理者のアクセスを制御するための、パフォーマンスとスケーラビリティに優れたソリューションで、中央集中型の RADIUS サーバまたは TACACS+ サーバシステムとして運用されます。802.11i との関連では、Cisco Secure ACS は複数の EAP メソッド (EAP-TLS、PEAP、および EAP-FAST) を使用してユーザをネットワークに対して認証する際に重要な役割を果たす以外に、802.11i で必要なユーザ単位の個別のセッション鍵に使用される 802.11i PMK も生成します。Cisco Secure ACS は、RADIUS キー ラップ プロトコルの FIPS 検証のために NIST に提出される最初の RADIUS サーバです。前に説明したように、RADIUS キー ラップ プロトコルは WLC と ACS の間の RADIUS トラフィックを保護し、FIPS で承認された方法を使用して鍵を配布します。

### ロケーション対応の無線侵入検知/防御

ワイヤレス メディアを使用すると、未承認のユーザが企業にさまざまな新種の脅威をもたらす可能性があります。最も一般的なのは不正なアクセス ポイントですが、その他の脅威として、MAC スプーフィング攻撃、クライアントの不適切な設定、DoS 攻撃などがあります。このような攻撃に対処するために、Cisco Unified Wireless Network は高度な無線侵入検知および防御サービスをサポートしています。この機能により、ネットワークは、攻撃の発生をリアルタイムで自動的に識別できます。不正なアクセス ポイントの場合、無線/有線双方での抑制方式が実装されます。不正なアクセス ポイントに接続しようとするクライアントは自動的に遮断され、承認された WLAN アクセス ポイントの動作に悪影響を与えることはありません。

ません。無線と有線の両方で収集された情報を使用して、ポート抑制が自動的に開始され、不正なアクセス ポイントが有線にトラフィックを渡すことを防ぐことができます。正確なロケーショントラッキングは、不正なデバイスを物理的に削除できる最終的な手段です。

### Wireless Control Software

Cisco Wireless Control Software は、Cisco Aironet Lightweight アクセス ポイント、Cisco Wireless LAN Controller、および Cisco Wireless Location Appliance と連携して動作します。Cisco WCS という単一のソリューションにより、ネットワーク管理者は、RF 予測、ポリシー プロビジョニング、ネットワーク最適化、トラブルシューティング、ユーザトラッキング、セキュリティ監視、および WLAN システム管理を行うことができます。機能豊富なグラフィカル インターフェイスを使用して、シンプルでコスト効率に優れた WLAN の展開と運用を実現できます。また、Cisco WCS が提供する詳細な傾向調査および分析レポート機能は、実稼働ネットワークの運用に不可欠です。Cisco Wireless Location Appliance と組み合わせて使用すると、WCS はシスコのワイヤレス アーキテクチャの侵入検知および防御に不可欠なコンポーネントとして機能します。

### Wireless Location Appliance

Cisco Wireless Location Appliance は、WLAN 全体で不正な AP とクライアントを追跡するために不可欠です。高度な RF フィンガープリント テクノロジーを使用してロケーションを追跡すると同時に、WLAN インフラストラクチャ内から直接、数千の 802.11 ワイヤレス デバイスを追跡するため、ワイヤレス環境の資産の視認性と管理性が向上します。Cisco Wireless Location Appliance は、ロケーションの傾向分析、迅速な問題解決、および RF 容量管理に使用される豊富な履歴ロケーション情報も記録します。

### WIDS : WCS + ロケーション

Cisco Wireless Intrusion Detection System には 17 の標準 WIDS シグニチャがあり、不正なデバイス（アクセス ポイントおよびクライアント）やその他の悪意のあるアクティビティの検出に使用されます。Cisco Aironet アクセス ポイントに電源を入れ、WLAN コントローラに関連付けると、環境内で動作している可能性がある不正な AP、不正なクライアント、および疑わしいワイヤレストラフィックについて、カバレッジ エリアが 1 日 24 時間スキャンされます。コントローラが侵入を検知すると、WCS 管理コンソールでただちに更新されるリアルタイムのアラートが生成されます。コントローラは、有害なアクティビティに関する詳細とともに、アラーム通知を管理者に送信することもできます。

検出された 1 つの不正な AP または不正なクライアント デバイスの物理的な場所を追跡するために、AP、コントローラ、および WCS コンポーネントの組み合わせによりロケーション機能が提供されます。Cisco 2700 シリーズ Wireless Location Appliance を追加すると、数千のワイヤレス デバイス（不正な AP や不正なクライアントが含まれる可能性がある）の物理的な位置をリアルタイムで追跡できます。Wireless Location Appliance は、環境内の RFID タグや任意の 1 つのデバイスの物理的な移動を追跡するための、オンデマンドのロケーショントラッキング履歴を WCS に提供します。WCS は 1 つ、2 つ、またはそれ以上のアクセス ポイントからの RSSI 信号強度を比較し、RF フィンガープリント アルゴリズムを分析して、不正な AP と不正なクライアントが存在する可能性が最も高い場所を探します。不正が検出されると、WCS は直接カバレッジ エリアのマップに独自の不正アイコンを配置して、最も可能性の高い場所を表示します。

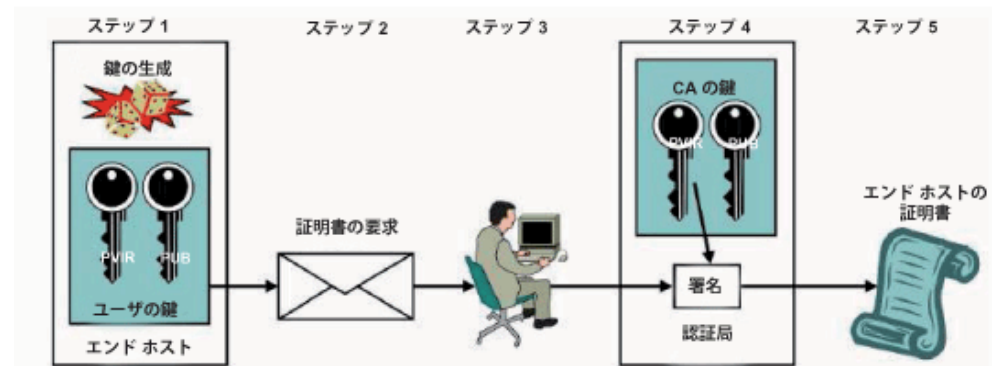
WIDS とロケーション トラッキング機能がシステムに直接統合され、これにより、WLAN データ分散サービスと WIDS サービスが同時に提供されます。システムには専用モニタ AP は不要ですが、必要に応じて専用モニタ モードに設定できます。モニタ モードでは、AP はオーバーレイ ワイヤレス モニタリング システムとして機能しますが、WLAN データ サービスは送信されません。このモードは、有線のためのネットワークに「ワイヤレスなし」ポリシーを適用するために使用されます。両方の動作モード（WLAN サービス モードまたは専用モニタ モード）で、WIDS 機能が提供する抑制機能により、管理者はワイヤレス ネットワーク上のデバイスごとに無線通信を手動で禁止することができます。抑制サービスは、コントローラに関連付けられた 1 つ、2 つ、または 3 つの AP によって行われます。

## 付録 A : DOD 公開鍵インフラストラクチャとコモン アクセス カード

### 公開鍵インフラストラクチャの概要

公開鍵インフラストラクチャ (PKI) は、IP Security、Secure Shell、Secure Sockets Layer などのセキュリティ プロトコルを展開することで、ネットワークの保護、管理上のオーバーヘッドの軽減、およびネットワーク インフラストラクチャの展開の簡素化を実現するスケーラブルな手法です。PKI は暗号鍵を管理し、安全な通信に関与するネットワークの人的および機械的コンポーネントの情報を識別します。ユーザまたは機器を PKI に登録するには、ユーザのコンピュータ上のソフトウェアで、安全な通信に使用される暗号鍵のペア (公開鍵と秘密鍵) を生成する必要があります。コモン アクセス カード (CAC) の場合、鍵と証明書は CAC スマート カードに格納されます。秘密鍵は配布または公開されることはありません。逆に、公開鍵は安全な通信を行う相手に自由に配布されます。(図 1 に示すように) 登録プロセスでは、ユーザの公開鍵が証明書を要求するために、認証希望者の組織の所属部門を担当する認証局 (CA) に送信されます。ユーザは公開鍵を CA の登録コンポーネントに送信します。次に、管理者が要求を承認し、CA はユーザの証明書を生成します。ユーザが証明書を受信してコンピュータにインストールすると、安全なネットワークに参加できるようになります。CAC の場合、CAC を設定するときこのプロセス全体が処理されます。

図 1 公開鍵インフラストラクチャへの登録



アイデンティティ コンポーネントは、ユーザの ID、ネゴシエーション中の特定の通信へのユーザのアクセス レベル、およびアクセスを許可されていない相手からの通信を保護する暗号化情報を決定します。通信時に証明書が交換され、提示された情報が調べられます。証明書が有効期限内で、信頼できる PKI によって生成されたかどうかを確認されます。すべてのアイデンティティ情報が適切な場合、証明書から公開鍵が抽出され、暗号化セッションの確立に使用されます。

PKI の詳細については、インターネットや各種の出版物を参照してください。

### CAC コンポーネント

CAC は二因子認証を行います。CAC で証明書のロックを解除するには、ユーザは物理的な CAC をリーダーに提示し、Personal Identification Number (PIN) を入力する必要があります。これにより、CAC に格納された秘密鍵のロックが解除されます。秘密鍵は、エクスポートされたり、ワークステーションに配置されることはありません。

**CAC リーダー**

CAC リーダーは国際標準化機構（ISO）7816 標準のスマート カード リーダーです。カードの情報を読み取るには、CAC をリーダーに提示する必要があります。CAC を別のソフトウェア（ミドルウェアと呼ばれます）で読み取るには、PC にドライバをインストールする必要があります。

**ミドルウェア**

CAC へのユーザ インターフェイスは、ワークステーションにインストールされたミドルウェアです。ミドルウェアはユーザに PIN の入力を要求し、CAC のロックを解除して、オペレーティング システムと CAC リーダー間の通信を提供します。一般的なミドルウェアには、ActivCard Gold for CAC、Datakey Middleware for CAC、Netsign CAC などがあります。CAC ミドルウェアと Windows オペレーティング システム（OS）との通信は、Microsoft Certificate Application Programming Interface（CAPI）を通じて行われます。ミドルウェアは CAPI を使用して、証明書を OS に提示します。CAPI を使用するアプリケーションは証明書にアクセスできます。

## 付録 B : LWAPP の概要

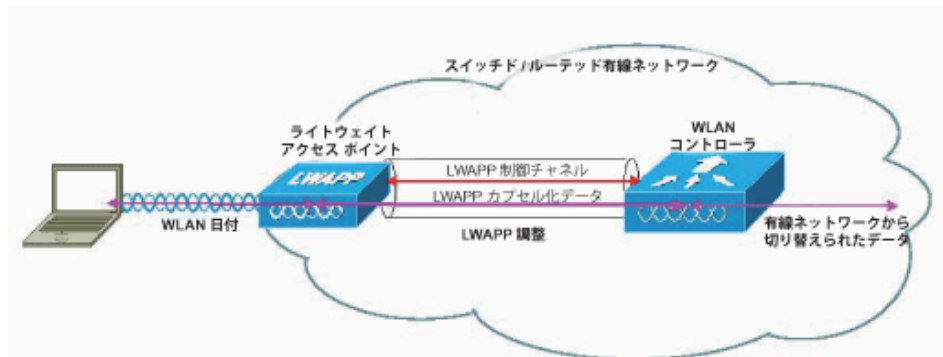
Cisco Unified Wireless アーキテクチャでは、WLAN の設定と制御を Wireless LAN Controller (WLC) と呼ばれるデバイスで集中管理します。これにより、WLAN はインテリジェントな情報ネットワークとして機能し、自律した個別のエンティティから構築された従来の 802.11 WLAN インフラストラクチャとは異なる、高度なサービスをサポートできます。Cisco Unified Wireless Network アーキテクチャは、多数の管理対象エンドポイント（自律アクセス ポイント）を WLAN コントローラの 1 つの管理対象システムに集約することで、運用管理を簡素化します。このアーキテクチャでは、アクセス ポイントはライトウェイトです。つまり WLC から独立して動作することはできません。WLC は AP の設定とファームウェアを管理します。AP は「手動操作なし」で展開され、アクセス ポイントの個別の設定は不要です。AP は、リアルタイムのメディア アクセス制御（MAC）機能のみを扱うという意味でもライトウェイトです。非リアルタイムの MAC 機能はすべて、WLC で処理されます。これはスプリット MAC アーキテクチャと呼ばれます。図 1 に示すように、AP は Lightweight Access Point Protocol (LWAPP) を経由して WLAN コントローラと対話します。LWAPP は次の事項を定義します。

- コントロール メッセージング プロトコルと形式
- データ カプセル化

WLAN クライアント データ パケットは、AP と WLC の間の LWAPP でカプセル化されます。フレームのカプセル化またはカプセル化解除のあと、WLC は WLAN クライアントとの間でデータ フレームを転送します。WLAN クライアントがパケットを送信すると、AP が受信し、必要に応じて復号化したあと、LWAPP ヘッダーを使用してカプセル化し、コントローラに転送します。コントローラでは、LWAPP ヘッダーが削除され、フレームがコントローラからスイッチング インフラストラクチャの VLAN に切り替わります。有線ネットワーク上のクライアントが WLAN クライアントにパケットを送信すると、まず WLC がパケットを受け取ります。WLC では、LWAPP を使用してパケットがカプセル化され、適切な AP に転送されます。AP は LWAPP ヘッダーを削除し、必要に応じてフレームを暗号化したあと、フレームを RF メディアに渡します。

LWAPP コントロール メッセージは、FIPS で検証された業界標準の AES-CCM 暗号化方法を使用して暗号化されます。共有暗号鍵が取得され、AP が WLC と結合するときに交換されます。カプセル化された LWAPP データ メッセージのペイロードは特に暗号化されません。有線ネットワークは信頼されたものであることが想定されており、ネットワークを保護するための標準のベスト プラクティスに従う必要があります。FIPS で検証された標準ベースの 802.11i ワイヤレス レイヤ 2 暗号化がアクセス ポイントで処理されます。

図 1 LWAPP を経由して WLAN コントローラと対話するアクセス ポイント



©2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(0805R)

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社  
〒107-6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー  
<http://www.cisco.com/jp>  
お問い合わせ先 (シスコ コンタクト センター)  
<http://www.cisco.com/jp/go/contactcenter>  
0120-092-255 (通話料無料)  
電話受付時間: 平日 10:00 ~ 12:00, 13:00 ~ 17:00

お問い合わせ先