Cisco Adaptive Wireless Intrusion Prevention System：Cisco Motion における情報の保護

はじめに

多くの IT 組織において、ワイヤレス通信は新たな領域です。サイトでワイヤレス ネットワークを展開していない場合でも、他のネットワーク媒体と同様に、ワイヤレス通信を適切にセキュリティ保護する必要があります。

Cisco® Adaptive Wireless Intrusion Prevention System（IPS）は Cisco® Unified Wireless Network インフラストラクチャに統合されており、ワイヤレス特有のネットワークの脅威の検知し、悪意のある攻撃、セキュリティの脆弱性、およびパフォーマンスを低下させる要因を緩和します。Cisco Adaptive Wireless IPS は、ワイヤレスの脅威を視覚化、分析、および識別し、セキュリティとパフォーマンスに関する問題の緩和と解決を中央で管理します。また、Cisco Adaptive Wireless IPS は、ほとんどのワイヤレスの攻撃に耐える強化されたワイヤレス ネットワーク コア向けに、プロアクティブな脅威防御機能を提供します。

ビジネス上の課題

ワイヤレス ネットワーキングの成長と非常に多くの新しいモバイル コンピューティング デバイスの登場により、信頼できるネットワークと信頼できないネットワークとの間の従来の境界があいまいになり、セキュリティの優先事項も、ネットワーク周辺部から情報保護およびユーザ セキュリティへと移行しました。移動中の情報を保護し、ワイヤレス環境を制御して未許可のアクセスを防止することが、企業の情報とシステムの完全性を維持するための急務となっています。ワイヤレス ネットワーキングを導入している企業でも、未承認のワイヤレス通信が使用されていないことを確実にしたい企業でも、電波をセキュリティ保護する必要があります。

2007 年に、National Cyber Security Alliance とシスコがワイヤレス ネットワーキングを使用している企業を対象として行った調査によると、67 パーセントの企業が自社のワイヤレス セキュリティ ポリシーを把握していないか、不十分または旧式なワイヤレス セキュリティ

手法を使用しており、RF 環境を定期的にスキャンしている企業は 52 パーセントのみでした。ワイヤレスの脅威に対して適切な防御を行わない場合、顧客のネットワークは次のような脅威に対して脆弱になります。

- 悪意のない社員または悪意のある部外者によって知らない間に導入され、いずれの場合も企業のネットワークへのバックドア アクセスを可能にする、不正なワイヤレス アクセス ポイント。これは、ワイヤレス ネットワーキングを展開している企業とワイヤレス ネットワーキングを展開していない企業の両方にとっての懸案事項です。
- 同じく企業のネットワークへのバックドア アクセスを可能にする恐れがある、さまざまな種類の Wi-Fi 対応クライアント。
- ネットワーク　プロファイリングや機密情報の盗用のためにユーザをおびき寄せて接続させようと試みる、ハッカーのアクセス ポイント。
- ワイヤレス ネットワークを混乱させたり使用不能にしたりするサービス拒否攻撃。
- 無線ネットワークの偵察、傍受、およびトラフィック クラッキング。
- より入手しやすく強力になった一方で、重大な脅威をもたらす恐れがある非 802.11 ワイヤレス デバイス（Bluetooth など）によるセキュリティ脆弱性。

企業の境界内の RF スペクトルは、ビジネス上の利益のために管理および保護する必要があるビジネス資産です。かつては名声を得ることのみを目的としていたハッカーも、現在では、財務情報や機密情報を得るために新しい攻撃方法を次々と編み出す国際的犯罪組織の一員である場合が増えています。最近、RF 環境の保護を怠った企業がハッカーに顧客の財務データを悪用される事件が大々的に報じられています。そのような企業は社会的な批判を浴び、巨額の罰金の支払いを余儀なくされています。顧客データや財務データの機密保護違反に関するコストには、次のものがあります。

- 法的な罰金
- サードパーティによるセキュリティ監査のコスト
- 顧客またはパートナーへの補償金
- 将来の収益減少につながる、顧客の信頼の喪失
- 企業ブランドへのダメージ
- 株式時価総額の減少

モビリティは、IT 管理者に二者択一を迫ります。モビリティには、よりオープンなネットワークと企業情報への自由なアクセスが必要ですが、これは、アクセスをより少なくし、より厳密に制御することを必要とする多くのセキュリティ ポリシーと矛盾します。その結果、多くの管理者は、さまざまなツールを使用してネットワークを保護します。しかし、通常、これらのツールではセキュリティの脅威を個別に監視するので、イベントを相互に関連付けて攻撃を診断することはできません。

ワイヤレス セキュリティには多くの考慮事項がありますが、Cisco Unified Wireless Network インフラストラクチャを構成しているワイヤレス コントローラ、アクセス ポイント、モビリティ サービス エンジン、およびワイヤレス コントロール システム（WCS）に組み込みのセキュリティ技術を使用することにより、これらの懸案事項のすべてに対処できます。ユーザに接続性を提供するのと同じワイヤレス機器によって、展開全体のセキュリティも提供されます。

安全なモビリティの利点

シスコでは、ビジネスにおける安全なワイヤレス アクセスの提供を支援するために、安全なワイヤレス展開に必要とされるすべてのコンポーネントを Unified Wireless Network インフラストラクチャに組み込みました。シスコは、ネットワーク サービスと高度なセキュリティを提供するのと同じインフラストラクチャを使用して包括的なワイヤレス セキュリティと侵入防御を提供し、資本コストを抑えてセキュリティ操作を合理化します。シスコは、他の専用機器、ソフトウェア、または管理ツールを必要とせずに、ワイヤレス IPS 用の完全な統合ソリューションを提供します。

Cisco Adaptive Wireless IPS ソリューションの核となっているのは、プロアクティブな脅威防御用に設計されたネットワークです。ワイヤレス IPS は、未知の脅威を識別するために、WLAN インフラストラクチャ内のトラフィックとデバイスの両方を有線ネットワークと無線ネットワークの両方でリアルタイムに監視します。これにより、検知機能と関連付け機能が強化され、脅威の検知の精度も向上します。この方法は、単に RF 環境を監視するよりもはるかに効率的です。

シスコ自己防衛型ネットワークの不可欠な部分である Cisco Adaptive Wireless IPS は、シスコの有線ネットワーク セキュリティ ポートフォリオと連携して、有線ネットワークと無線ネットワークの両方にネットワーク全体にわたる脅威防御機能のスーパーセットを提供します。階層化された防御を作成することにより、さらに徹底的で精度の高い保護が可能になり、IT 部門内のネットワーク業務チームとセキュリティ業務チームの両方の業務効率が向上します。

Cisco Adaptive Wireless IPS は、モバイル デバイスの普及をサポートし、移動中のビジネスアプリケーションへのアクセスを可能にする安全なネットワークの作成を支援します。また、クレジットカード業界（PCI）、SOX 法、医療保険の携行性と責任に関する法律（HIPAA）などの法規制で定められたコンプライアンス要件への対応を可能にします。企業は、Cisco Adaptive Wireless IPS により、重要なビジネス資産と情報を確実に保護しながらモビリティの可能性を実現し続けることができます。

包括的な脅威検知とプロアクティブな防御、および有線セキュリティ コラボレーションの結合

シスコは、ワイヤレスの脅威の徹底的な検知と緩和を有線および無線のネットワーク インフラストラクチャと統合することにより、業界で最も包括的な、高精度で低コストのワイヤレス セキュリティ ソリューションを提供します。この基盤の上に RF インテリジェンス、ワイヤレス侵入検知、および有線ネットワーク セキュリティ コラボレーションのレイヤーが構築され、レイヤ 1（物理周波数）からレイヤ 7（アプリケーション レイヤ）までのあらゆる層の攻撃を防止します。

ワイヤレスの侵入防御に対するこの独自の包括的なアプローチの基礎となっているのは、次の 3 つのコンポーネントです。

- 不正なアクセスポイントとユーザ、ワイヤレスの脅威、ゼロデイ攻撃、パフォーマンスの低下、およびセキュリティ構成の脆弱性からの保護を提供する、ワイヤレス インフラストラクチャに統合されたネットワーク分析およびシグネチャベースの技術。新しい検知および緩和技術を開発するための、脅威の継続的な研究。

- ネットワーク全体にわたるユーザとインフラストラクチャの認証と暗号化、ワイヤレス管理フレーム保護、およびワイヤレスのセキュリティ脆弱性の自動的な評価および報告を使用してワイヤレス ネットワーク コアを強化する、ワイヤレス インフラストラクチャに統合されたプロアクティブな脅威防御。
- ワイヤレス セキュリティ保護のための階層化されたスーパーセットを提供する、シスコの有線ネットワーク セキュリティ ポートフォリオとの連携。

図 1　完全な防御 : Cisco Wireless IPS の脅威検知と、プロアクティブな防御および有線セキュリティ コラボレーションの結合

ワイヤレスの脅威の包括的な検知と緩和

Cisco Adaptive Wireless IPS は、Cisco Unified Wireless Network インフラストラクチャに直接統合されています。シスコの標準ワイヤレス コントローラ、アクセス ポイント、Cisco モビリティ サービス エンジン、および Wireless Control System を利用してワイヤレスの脅威を検知および防御することにより、コストを削減し、業務を合理化し、包括的な防御を行うことができます。

Cisco Adaptive Wireless IPS の中核を成すのは、ワイヤレスの脅威の検知とパフォーマンス管理に対する高度なアプローチです。市場のほとんどのソリューションが無線の受動的なトラフィック監視のみに頼っているのに対し、Cisco Adaptive Wireless IPS はネットワーク トラフィック分析、ネットワーク デバイスとトポロジーの情報、シグネチャベースの技術、および異常検知を組み合わせて、非常に正確かつ徹底的にワイヤレスの脅威を防止します。このソリューションはインフラストラクチャに統合されているため、有線と無線の両方のネットワーク上のワイヤレス トラフィックを継続的に監視できます。被害が発生するまで待つのではなく、さまざまな情報源に基づいて攻撃を分析するネットワーク インテリジェンスを使用して、ピンポイントかつプロアクティブに攻撃を防ぐことができます。

核となる検知機能の上に構築される Cisco Adaptive Wireless IPS には、攻撃のさまざまな分類と、緩和に関する警告および報告機能が用意されています。分類の見地からは、セキュリティ イベントを自動的に分類するための柔軟な規則が提供されます。システム本来の正確性に自動分類機能を加えることにより、システムで検出された潜在的な脅威を手動で調査するための経費を大幅に削減できます。この分類を脅威の緩和処置と関連付けて、セキュリティ イベントの重大度に応じて手動または自動で緩和処置を実行することもできます。また、イベントの重大度の分類に応じて、検知イベントと緩和イベントの両方に関する警告を IT オペレータに自動的に表示することもできます。

ワイヤレス環境における高い可視性を保証するために、Cisco Adaptive Wireless IPS では、パフォーマンス関連の問題と、非 802.11 デバイス（Bluetooth、レーダー、マイクロ波など）および攻撃も検知できます。無線リソース管理（RRM）の利用により、他に類を見ないパフォーマンスとネットワーク自己回復機能が提供されます。ノイズと妨害に関して収集された情報とクライアントの信号強度などのデータを使用してチャネルが動的に割り当てられ、アクセス ポイントの送信電力がリアルタイムに調整されます。これにより、同一チャネル干渉を回避し、障害が発生したデバイスを迂回し、カバレッジ ホールを最小限に抑えることができます。非 802.11 ソースによって生じるパフォーマンスの低下および攻撃に対しては、非 802.11 デバイス、または非 802.11 デバイスによって生じたサービス拒否攻撃を隠す恐れがある干渉ソースを検知できる、RF スペクトル専用の機能が用意されています。Bluetooth アクセス ポイントなどの非 802.11 デバイスは、ワイヤレス ネットワークのパフォーマンスに影響を及ぼすだけでなく、認証されたクライアント デバイスを通じてワイヤレス ネットワークへのアドホック接続を作成する恐れがあります。

Cisco Wireless Control System（WCS）は、ワイヤレス IPS によるネットワーク管理と、統合された構成に関するレポート機能に加えて、セキュリティ イベントの管理と、ネットワーク上のセキュリティ イベントの物理的な発生場所を追跡するレポート機能も備えています。管理者は、システムの分析機能を利用して、あらゆる WLAN イベントと RF イベントを追跡、検索、および捕捉し、イベントを実際にプレイ バックすることができます。セキュリティ ポスチャおよびセキュリティ イベントは、WCS の統合セキュリティ ダッシュボードを通じてリアルタイムに確認できます。モビリティ サービス エンジンをプラットフォームとして使用してイベントの履歴データを保存すると、WCS からアクセス可能な、多年にわたる分析データのレポートが含まれる大規模なファイルにアクセスできるようになります。これにより、長期にわたる複雑な分析だけでなく、コンプライアンスの報告も可能になります。

強化されたネットワーク コアとプロアクティブな防御

ネットワークをセキュリティ保護するための最良の方法は、損害を受ける前に攻撃を防ぐシステムを設計することです。シスコのワイヤレス IPS ソリューションは、強化されたワイヤレス インフラストラクチャを基盤としています。このインフラストラクチャでは、IEEE 802.11i と 802.1X、シスコのワイヤレス管理フレーム保護（MFP）、およびワイヤレスのセキュリティ脆弱性の自動評価・報告機能を利用して、ネットワーク全体にわたるユーザとインフラストラクチャの認証および暗号化が行われます。さらに、ワイヤレス クライアントのアクティビティを常時監視することにより、ポリシー違反のクライアントや悪意のあるクライアントによるネットワークへのアクセスが防止されます。

有線ポートに接続する Cisco Aironet® アクセス ポイントに有効な 801.1X 有線ポート認証を要求することにより、不正なアクセス ポイントの有線ネットワークへの接続が根本的に防止されます。高度な暗号化によって移動中のデータが保護され、管理フレーム保護（IEEE

802.11w 標準の基盤）では、無線でやり取りされる 802.11 管理フレームを保護することにより、ほとんどのワイヤレス攻撃が防止されます。強力な認証と MFP の連携によって、ほとんどのワイヤレスの攻撃をプロアクティブに防止できます。また、無線デジタル署名を使用して不正なアクセスポイントを高精度に検知することにより、無線の偵察を防止できます。

ワイヤレス ネットワークでは、ワイヤレスの脆弱性の監視および評価が年中無休で自動的に実行され、ネットワークのセキュリティ構成上の弱点が予防的かつ持続的にスキャンされます。ワイヤレス ネットワークのセキュリティ ポスチャをリアルタイムで把握することは、攻撃の防御における最も重要な側面です。

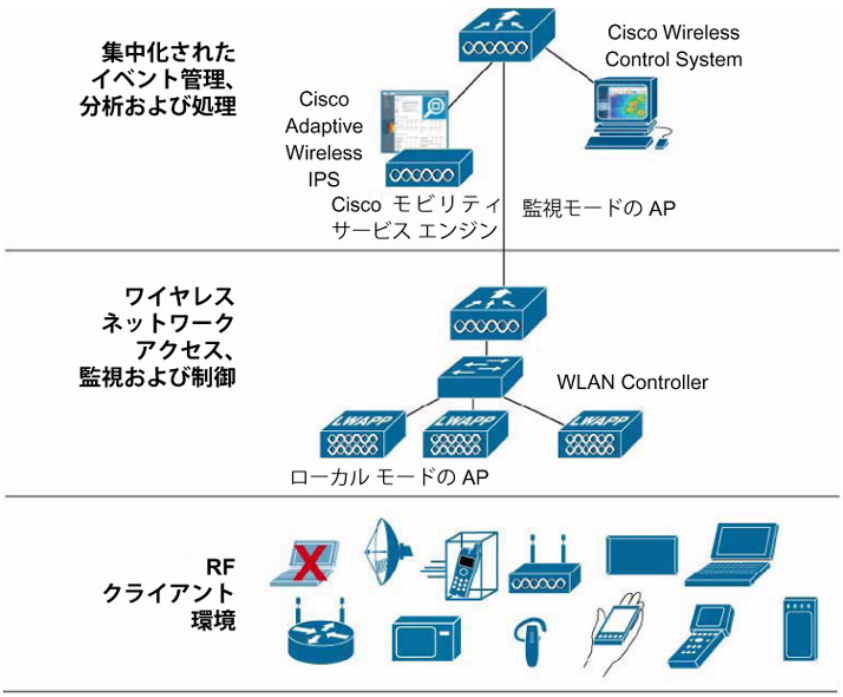
Cisco Adaptive Wireless IPS の展開に使用されるコンポーネント

ワイヤレス ネットワーク インフラストラクチャの安全な展開および操作に必要なすべてのコンポーネントは、Cisco Unified Wireless Network に組み込まれています。Adaptive Wireless IPS システムは、次の CUWN コンポーネントで構成されます（下のネットワーク図に概要を示します）。

- Cisco モビリティ サービス エンジンと Cisco Adaptive Wireless IPS
- Cisco Aironet アクセス ポイント
- Cisco WLAN Controller と Wireless Control System

Cisco Adaptive Wireless IPS は、Cisco Unified Wireless Network 内で Cisco モビリティ サービス エンジンを使用することにより、非常に大規模なネットワークの高度なニーズに応えることができます。Cisco Aironet アクセス ポイントでは継続的に監視が行われ、モビリティ サービス エンジン内の集中処理プラットフォームに情報がフィードバックされます。このような方法で、ネットワークのあらゆる部分からワイヤレス トラフィックの分析とセキュリティ状況が効率的に収集されて相互に関連付けられ、ワイヤレス ネットワークのセキュリティ状況に関する単純で統合されたビューが提供されます。

図 2　Cisco Adaptive Wireless IPS ソリューションのコンポーネント



Cisco モビリティ サービス エンジンは、分析処理のパフォーマンスとスケーラビリティ、履歴レポートと分析データの保管機能、および場所/接続ベースの資産トラッキングやクライアント セキュリティ管理などのサービスの統合機能を備えています。Cisco Adaptive Wireless IPS ソリューションは、企業のモバイル ネットワークの拡張に伴って増え続ける新しいデバイスとスペクトルの用途を監視および分析し、重要な企業情報を確実に保護します。

シスコのアクセス ポイントは、ユーザ トラフィックにサービスを提供しながらワイヤレス IPS スキャンを実行することも、フルタイムでワイヤレス IPS 監視だけを実行するように構成することもできます。共有と専用の両方の監視オプションによって、サイト固有の展開要件に柔軟に対応することが可能になります。ローカル モードのシスコ アクセス ポイントでは、ワイヤレス クライアントへのデータの提供を行いながらワイヤレス IPS スキャンが実行されます。監視モードのアクセス ポイントでは、ワイヤレス IPS スキャンがフルタイムで実行されます。ローカル モード（パートタイム）のアクセス ポイントと監視モード（フルタイム）のアクセス ポイントを組み合わせることにより、ネットワーク アーキテクチャ全体の要件を満たすことができます。

Wireless Control System（WCS）は、集中化された計画、構成、管理、およびレポート機能を提供して、IT 管理者が地理的に分散した多数の Cisco WirelessLAN Controller およびアクセス ポイントを 1 つのコンソールで設計、制御、および管理できるようにし、操作を単純化するとともに総所有コストを削減します。WCS では、ワイヤレス LAN の管理者が簡単な操作で確実に WLAN のセキュリティ設定を行うことができるように、機能豊富なグラフィカル ユーザ インターフェイス、ポリシー テンプレート、脆弱性スキャン、およびシスコのベスト プラクティスに基づいて推奨される緩和処理を提供し、管理者によるワイヤレス LAN のセキュリティの構成、監視、および管理を支援します。また、すべてのセキュリティ イベントやコンプライアンス報告（PCI 評価レポートなど）が表示される統合ダッシュボードなどの、ネットワーク全体のレポート機能を提供します。WCS は、ワークフローの単純化、操作担当者のトレーニング時間の削減、およびソフトウェア コストの削減を実現する、すべてのワイヤレス業務とワイヤレス セキュリティ業務の管理ツールです。

有線ネットワーク セキュリティとの連携によるワイヤレス セキュリティの強化

Adaptive Wireless IPS システムは、シスコの有線ネットワーク セキュリティ ポートフォリオと連携して、ワイヤレス セキュリティ保護のスーパーセットを提供します。有線ネットワークとの連携によって、マルウェアからの防御、クライアントのセキュリティ ポスチャの安定した実施、および ネットワーク全体にわたる有線および無線の統合されたセキュリティ監視が可能になります。これにより、ワイヤレス セキュリティへの階層化されたアプローチが実現します。

たとえば、シスコのワイヤレス IPS プラットフォームと有線 IPS プラットフォームをリアルタイムに連携させて、ウイルスやワームを広めるワイヤレス ユーザを切断することができます。Cisco Network Admission Control では、ワイヤレス クライアントのセキュリティ ポスチャを実施できます。また、シスコのワイヤレス IPS から Cisco MARS セキュリティ情報管理システムにすべてのワイヤレス セキュリティ イベントを送信すると、有線と無線の両方のセキュリティをネットワーク全体にわたって監視および分析できます。有線と無線のネットワークに共通のプラットフォームを作成することにより、さらに徹底的で精度の高い階層化された防御が可能になり、IT 部門内のネットワーク業務チームとセキュリティ業務チームの両方の業務効率が向上します。

従来のツールとは異なり、Cisco Adaptive Wireless IPS ソリューションでは、プロアクティブな保護を実現するために設計された全体的な脅威防御システムと、有線・無線のネットワークにわたる唯一で真の脅威抑制機能が提供されます。

シスコが選ばれる理由

企業は、Cisco® Unified Wireless Network を利用して、異種のネットワークにモビリティ アプリケーションを実装できます。パーソナル ネットワーク、プライベート ネットワーク、およびパブリック ネットワークの区別なく、安全で一貫したモビリティ エクスペリエンスを得ることができます。Cisco Unified Wireless Network を展開される際には、シスコの専門技術と展開エクスペリエンス、およびシスコのパートナー ソリューションが、高性能で柔軟かつスケーラブルなワイヤレス インフラストラクチャのメリットを享受できるようにお客様を支援します。

シスコは、IT 部門が従業員と資産のビジネス モビリティのニーズを満たし、さらにそれを超えるソリューションを提供できるように、次のサポートを行います。

- 異種のネットワークにまたがる共同セキュリティの提供
- 多種多様なモバイル デバイスの増加によって生じる脅威のプロアクティブな防御
- デバイス、ネットワーク、およびアプリケーションの統合とセキュリティの提供
- モビリティ アプリケーションの開発のための安全なオープン プラットフォームの作成

Cisco Services と Wireless LAN Specilized パートナーは、ビジネス モビリティへの新しい実践的なアプローチをサポートするサービスを提供して、企業の技術上の目標とビジネス上の目標の達成を支援します。シスコが提供するブループリントは、モビリティ ネットワークを統合し、モバイル デバイスを保護および管理し、モビリティ アプリケーション用のオープンなエコシステムを作成します。このブループリントは、非常に効率の高いモビリティ ソリューションを計画、配置、および管理して統合プラットフォームを構築することによって実現し、アプリケーションのモビリティを強化し企業の資産を保護するサービスのエンドツーエンドな管理と提供を通じて、ワイヤレス クライアント管理、コンテキスト アウェアなソリューション サービス、および固定通信と移動通信の融合の領域における大幅な機能拡張を可能にします。

関連情報

Cisco Adaptive Wireless Intrusion Prevention ソリューションの詳細については、次の URL を参照してください。
http://www.cisco.com/jp/go/wips/

シスコ自己防衛型ネットワークの詳細については、次の URL を参照してください。
http://www.cisco.com/jp/go/sdn/

Cisco モビリティ サービス エンジンの詳細については、次の URL を参照してください。
http://www.cisco.com/jp/go/mse/

Cisco Unified Wireless Network の詳細については、次の URL を参照してください。
http://www.cisco.com/jp/go/unifiedwireless/

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

お問い合せ先

08.08