Cisco 適応型ワイヤレス IPS 導入ガイド

Cisco Adaptive wIPS Deployment Guide

OL-18385-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。米国サイト掲載ドキュメントとの差異が生じる場合があるため、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

はじめに

本書では、Cisco モビリティ サービス エンジンを利用する Cisco 適応型ワイヤレス Intrusion Prevention System（wIPS）ソリューションの設定と構成のガイドラインについて説明します。この包括的なセキュリティ モニタリングおよび脅威検出システムを既存の Cisco ワイヤレス LAN ネットワークに統合したり、専用のワイヤレス セキュリティ オーバーレイ ソリューションとして構成したりすることができます。WLAN に統合されたシステムとして構成した場合に、最大の機能性が発揮されます。また、本書では、製品に関する情報ベースをいっそう強固なものにするために、トラブルシューティングのヒントと FAQ も取り上げています。

本書の目的は次のとおりです。

- Cisco 適応型ワイヤレス IPS ソリューションのさまざまなコンポーネントと通信フレームワークについて説明する
- Cisco 適応型ワイヤレス IPS ソリューションを実装するための一般的な構成のガイドラインを示す
- シスコの 5.2 以前のリリースのコントローラベースの IDS システムと Cisco 適応型ワイヤレス IPS システムの違いを説明する

製品情報

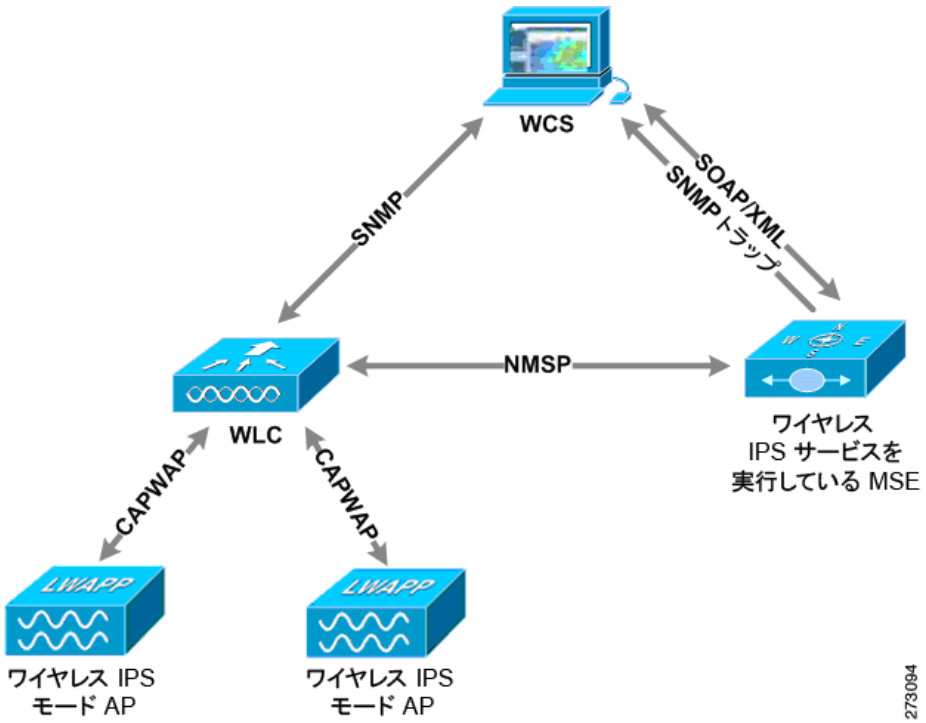
Cisco 適応型ワイヤレス Intrusion Prevention System（wIPS）は Cisco Unified Wireless Network インフラストラクチャに統合され、ワイヤレス特有のネットワークの脅威の検出と、悪意ある攻撃、セキュリティ脆弱性、およびパフォーマンス低下の原因の緩和を行います。Cisco 適応型ワイヤレス IPS はワイヤレスの脅威を検出、分析、識別する機能を備え、セキュリティとパフォーマンスの問題の緩和と解決を集中管理します。さらに、Cisco 適応型ワイヤレス IPS は、ほとんどのワイヤレス攻撃が侵入不可能な強固なワイヤレス ネットワーク コアの脅威予防機能に加え、Cisco Self-Defending Network セキュリティ ポートフォリオと連携して、有線と無線の両方のネットワークに、階層化された脅威検出のスーパーセットを提供する機能も備えています。

機能と利点

Cisco 適応型ワイヤレス IPS は、強力なワイヤレスの脅威の検出および緩和の機能をワイヤレス ネットワーク インフラストラクチャに組み込むことで、業界で最も包括的で正確な運用効率の高いワイヤレス セキュリティ ソリューションを実現します。適応型ワイヤレス IPS は、不正アクセス ポイント/クライアントおよびアドホック接続の検出と緩和、Over-the-Air ワイヤレス ハッキングおよび驚異の検出、セキュリティ脆弱性モニタリング、パフォーマンス モニタリングおよび自己最適化、脅威予防のためのネットワーク強化、強力なワイヤレス セキュリティ管理およびレポート作成を行います。Cisco Unified Wireless Network を基盤にし、Cisco Motion の効果を利用した 適応型ワイヤレス IPS は構成が強化され、企業に対応しています。

ワイヤレス IPS システムのアーキテクチャ

Cisco 適応型ワイヤレス Intrusion Prevention System（wIPS）は、連携して統合セキュリティ モニタリング ソリューションを提供する多数のコンポーネントから構成されています。現在 Cisco Unified Wireless Network ソリューションを構成する WLAN コントローラ、アクセス ポイント、およびワイヤレス制御システム コンポーネント に加え、ワイヤレス IPS 部分では 2 つの追加のコンポーネントが導入されています。これらの追加のハードウェア コンポーネントには、ワイヤレス IPS モニタ モードのアクセス ポイントおよびワイヤレス IPS サービス ソフトウェアを実行するモビリティ サービス エンジンがあります。



ワイヤレス IPS 構成のコンポーネントの機能

- ワイヤレス IPS モニタ モード アクセス ポイント：定期的なチャネル スキャンと攻撃検出およびフォレンジック（パケット キャプチャ）機能を提供します。
- モビリティ サービス エンジン（ワイヤレス IPS サービスを実行）：すべてのコントローラとそれらの各ワイヤレス IPS モニタ モード アクセス ポイントからのアラーム集約の中央ポイント。アラーム情報とフォレンジック ファイルはアーカイブ目的でシステムに保存されます。
- ローカル モード アクセス ポイント：時分割の不正および位置スキャンに加えて、クライアントにワイヤレス サービスを提供します。
- ワイヤレス LAN コントローラ：ワイヤレス IPS モニタ モード アクセス ポイントからの攻撃情報を MSE に転送し、AP に設定パラメータを配布します。
- ワイヤレス制御システム：管理者が MSE でワイヤレス IPS サービスを設定し、ワイヤレス IPS 設定をコントローラに適用して、アクセス ポイントをワイヤレス IPS モニタ モードに設定する手段を提供します。また、ワイヤレス IPS アラームの表示、フォレンジック、レポート、および threat encyclopedia（脅威百科事典）のアクセスにも使用します。

ワイヤレス IPS 通信プロトコル

各システム コンポーネント間の通信を行うため、多くのプロトコルが使われています。

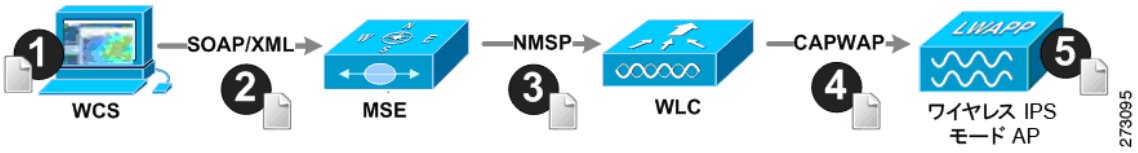
- CAPWAP（Control and Provisioning of Wireless Access Points）：このプロトコルは、LWAPP の後継で、アクセス ポイントとコントローラ間の通信に使われます。これは、アラーム情報をコントローラに行き来させ、設定情報をアクセス ポイントに適用する双方向トンネルを提供します。

- NMSP（Network Mobility Services Protocol）：ワイヤレス LAN コントローラとモビリティ サービス エンジン間の通信に使われるプロトコル。ワイヤレス IPS 構成の場合、このプロトコルは、アラーム情報をコントローラから MSE へ集約し、ワイヤレス IPS 設定情報をコントローラに適用する経路を提供します。このプロトコルは暗号化されます。
  - コントローラ TCP ポート：16113
- SOAP/XML（Simple Object Access Protocol）：MSE と WCS 間の通信の方法。このプロトコルは、MSE で実行するワイヤレス IPS サービスに設定パラメータを配布するために使用します。
  - MSE TCP ポート：443
- SNMP（Simple Network Management Protocol）：このプロトコルは、モビリティ サービス エンジンから、ワイヤレス制御システムにワイヤレス IPS アラーム情報を転送するために使われます。さらに、ワイヤレス LAN コントローラからワイヤレス制御システムに不正アクセス ポイント情報を伝えるためにも使われます。

ワイヤレス IPS 設定およびプロファイル管理

ワイヤレス IPS プロファイルの設定は、プロファイルの表示と変更に使用される WCS から始まるチェーン階層を進みます。実際のプロファイルは、MSE で実行するワイヤレス IPS サービス内に保存されます。プロファイルは、MSE 上のワイヤレス IPS サービスから、特定のコントローラに伝播され、次に、その目的のコントローラに関連付けられているワイヤレス IPS モード アクセス ポイントに透過的にこのプロファイルが伝達されます。

WCS でワイヤレス IPS プロファイルへの設定の変更が行われ、一連のモビリティ サービス エンジンおよびコントローラに適用される場合、変更を導入するために次の手順が実行されます。

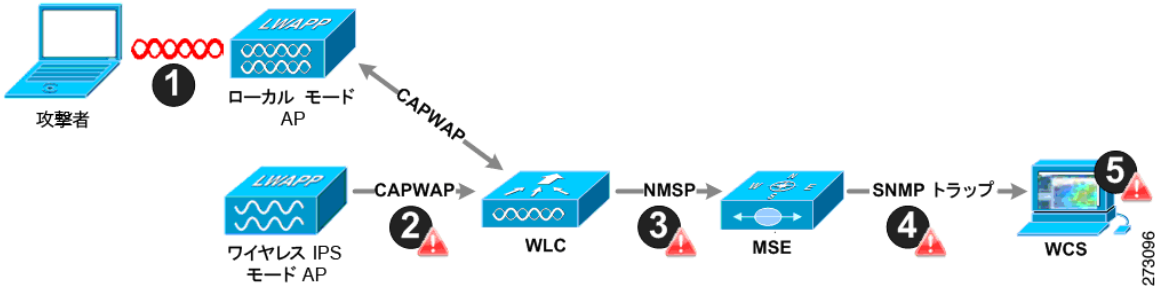


1. WCS で設定プロファイルが変更され、バージョン情報が更新されます。
2. XML ベースのプロファイルが MSE で実行するワイヤレス IPS エンジンに適用されます。この更新は、SOAP/XML プロトコルによって行われます。
3. MSE 上のワイヤレス IPS エンジンは、NMSP を使用して設定プロファイルを適用することによって、そのプロファイルに関連付けられている各コントローラを更新します。
4. ワイヤレス LAN コントローラは更新されたワイヤレス IPS プロファイルを受け取り、それを NVRAM に保存し（以前のすべてのバージョンのプロファイルを置き換える）、CAPWAP 制御メッセージを使用して、更新されたプロファイルをそれに関連付けられたワイヤレス IPS アクセス ポイントに伝播します。
5. ワイヤレス IPS モード アクセス ポイントはコントローラから更新されたプロファイルを受け取り、そのワイヤレス IPS ソフトウェア エンジンに変更を適用します。

モビリティ サービス エンジンは、1 つのワイヤレス制御システムだけから設定可能であることに注意する必要があります。これは必然的に 1 対 1 の関係になります。つまり、モビリティ サービス エンジンは、特定の WCS に関連付けられたら、別の WCS に追加できません。

ワイヤレス IPS アラーム フロー

適応型ワイヤレス IPS システムは、通信のリニア チェーンに従って、エアウェーブのスキャンから取得した攻撃情報をワイヤレス制御システムのコンソールに伝播します。



1. Cisco 適応型ワイヤレス IPS システムでアラームをトリガーさせるためには、正規のアクセス ポイントまたはクライアントに対して攻撃が仕掛けられる必要があります。正規のアクセス ポイントおよびクライアントは、同じ「RF グループ」名をブロードキャストする「信頼する」デバイスによって、Cisco Unified Wireless Network 内で自動的に検出されます。この設定では、ローカル モード アクセス ポイントとそれらに関連付けられたクライアントのリストが動的に管理されます。SSID グループ機能を使用して、SSID によって、デバイスを信頼するようにシステムを設定することもできます。WLAN インフラストラクチャに害を及ぼすと見なされた攻撃だけが残りのシステムに伝播されます。
2. ワイヤレス IPS モード アクセス ポイント エンジンによって攻撃が識別されると、アラームの更新がワイヤレス LAN コントローラに送信され、CAPWAP 制御トンネル内にカプセル化されます。
3. ワイヤレス LAN コントローラは、アラームの更新をアクセス ポイントから、モビリティ サービス エンジンを実行するワイヤレス IPS サービスに透過的に転送します。この通信に使用されるプロトコルは NMSP です。
4. モビリティ サービス エンジン上のワイヤレス IPS サービスによって受け取られたアラームの更新は、アーカイブと攻撃追跡のためにアラーム データベースに追加されます。SNMP トラップが攻撃情報を格納するワイヤレス制御システムに転送されます。同じ攻撃を参照する複数の更新が受け取られた（たとえば、複数のアクセス ポイントで同じ攻撃が認識された）場合、1 つの SNMP トラップだけが WCS に送信されます。
5. アラーム情報を含む SNMP トラップは WCS によって受信され、表示されます。

構成の考慮事項

必要なコンポーネント

Cisco 適応型ワイヤレス IPS システムの基本システム コンポーネントを次の通りです。

- ワイヤレス IPS モニタ モードのアクセス ポイント
- ワイヤレス LAN コントローラ
- ワイヤレス IPS サービスを実行するモビリティ サービス エンジン
- ワイヤレス制御システム

適応型ワイヤレス IPS システムに必要な最小コード バージョン：

- ワイヤレス LAN コントローラ：バージョン 5.2.XX 以上
- ワイヤレス制御システム：バージョン 5.2.XX 以上
- モビリティ サービス エンジン：バージョン 5.2.XX 以上

ワイヤレス IPS モニタ モードでサポートされているアクセス ポイントは、Cisco 1130、1140、1240、および 1250 シリーズです。

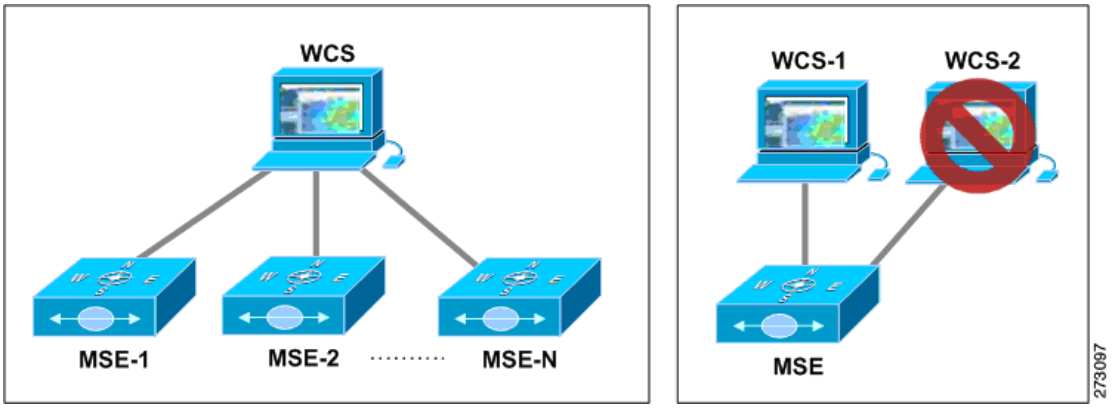
802.11n 攻撃

802.11n ではまったく新しい物理レイヤ仕様が採用されていることから、変調方式が基本的に異なるため、既存の 802.11a/b/g アクセス ポイントではこれらの新しい高スループット データ レートを復号化できません。これにより、ワイヤレス ネットワークが 802.11n レートで送信された攻撃を受けやすくなる可能性があります。802.11n 以外のデバイスではそれらの脅威を本質的に検知できないためです。

802.11a/b/g アクセス ポイントでは、ビーコンがレガシー レートで送信されるため、ほとんどの 802.11n 不正を検出できますが、Greenfield モードで動作する不正を検出できるのは、802.11n アクセス ポイントだけです。Greenfield モードは、デバイスが 802.11n 以外のレートで転送できないようにする 802.11n アクセス ポイントの設定パラメータです。802.11n Greenfield モードで動作しない不正は検出可能ですが、802.11n データ レートでの Greenfield 不正および攻撃は 802.11a/b/g アクセス ポイントで検出されません。お客様は Cisco 1140 および 1250 シリーズ アクセス ポイントを利用して、こうした 802.11n ベースの攻撃を検出できるようにすることをお勧めします。

システムのスケーラビリティ

モビリティ サービス エンジンは、1 つのワイヤレス制御システムからだけ管理できますが、ネットワークを拡張する場合に設計上の問題があります。1 つのワイヤレス制御システムから、複数のモビリティ サービス エンジンを管理させることができます。



システムの設計時には、次のスケーラビリティ項目を考慮してください。

- WCS はハイエンド サーバで最大 3000 アクセス ポイントをサポートできます。この 3000 の制限には、アクセス ポイントにサービスを提供するクライアントと、ワイヤレス IPS モニタ モードのアクセス ポイントの両方が含まれます。下の表に示すように、WCS あたり 3000 アクセス ポイントの上限に達するまで、ワイヤレス IPS およびデータ AP をさまざまな比率で混合することができます。これらの比率は、環境の RF 条件、既存の WLAN インストールの密度、およびセキュリティ モニタリングの必要なレベルによって異なります。

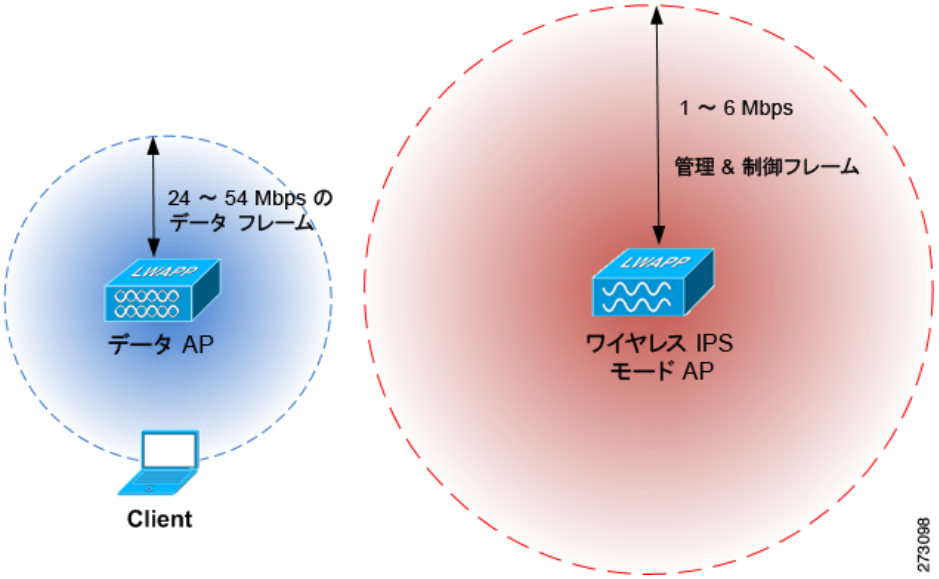
表 1　同じ WCS 上のワイヤレス IPS とデータ AP

	1:3 の比率	1:4 の比率	1:5 の比率	1:6 の比率	1:7 の比率	1:8 の比率
ワイヤレス IPS AP	750	600	500	429	375	333
データ AP	2250	2400	2500	2571	2625	2667
合計（WCS の制限）	3000	3000	3000	3000	3000	3000

- ワイヤレス IPS サービスを実行する MSE 3310 でサポートできるワイヤレス IPS モニタ モード アクセス ポイントの上限は 2000 です。上の図に示すように、ワイヤレス IPS およびデータ AP が同じ WCS 内に混合されている場合の制限要因は、WCS 自体のスケーラビリティです。MSE あたり 2000 ワイヤレス IPS AP の上限に達したら、個別のワイヤレス IPS だけのオーバーレイ構成を使用する必要があります。これについては、本書で後述します。
- ワイヤレス LAN コントローラはワイヤレス IPS モニタ モード アクセス ポイントとローカル モード アクセス ポイントの同時実行をサポートできます。ワイヤレス IPS モニタ モード アクセス ポイントが消費するコントローラ容量はローカル モード AP と同じです。たとえば、100 アクセス ポイントをサポートしている Cisco 4404 は 100 ワイヤレス IPS モニタ モード アクセス ポイントまたは、合計が 100 を超えない限り、任意の比率のワイヤレス IPS 対ローカル モード アクセス ポイントをサポートできます。

必要なワイヤレス IPS モニタ モード アクセス ポイント数

適応型ワイヤレス IPS システムを構成する前に、アクセス ポイントのセルの通信範囲が、フレームが受信され、復号化される実際の範囲より小さいことを考慮することが重要です。この相違の理由は、アクセス ポイントの通信範囲が、最弱リンク（一般的な構成では WLAN クライアント）によって制限されるためです。WLAN クライアントの出力がアクセス ポイントの最大出力より本質的に低いため、セルの範囲はクライアントの能力に制限されます。さらに、アクセス ポイントを全出力以下で実行し、ワイヤレス ネットワークに RF 冗長性とロード バランシングを組み込むことをお勧めします。これらの先述の事項とシスコのアクセス ポイントの優れたレシーバ感度の組み合わせによって、適応型ワイヤレス IPS システムは、広範囲の監視を行いながら、クライアントがサービスするインフラストラクチャより少ないアクセス ポイント密度で構成できます。



上の図で示すように、ワイヤレス IPS の構成は、大半の攻撃で障害の発生に使われる 802.11 管理および制御フレームの検知に基づきます。これは、24Mbps から 54Mbps の高いスループット データ レートを提供するために調査されるデータ アクセス ポイントと異なります。

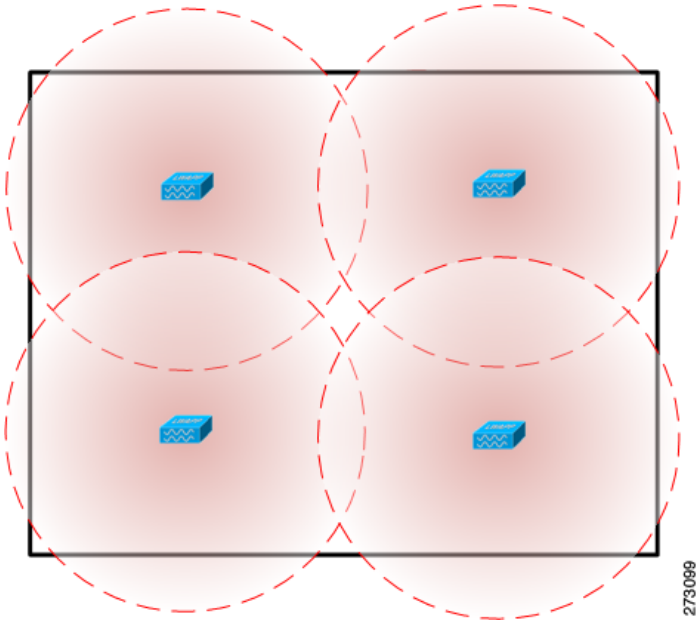
特定の環境に必要なワイヤレス IPS アクセス ポイント数を正確に決定するために、多数の要因があります。目的とする構成のセキュリティ要件と環境条件はそれぞれ異なるため、すべての構成のニーズに対処する確実なルールはありませんが、いくつかの一般的なガイドラインを考慮する必要があります。

必要なワイヤレス IPS アクセス ポイント数に影響する主な要因を次に示します。

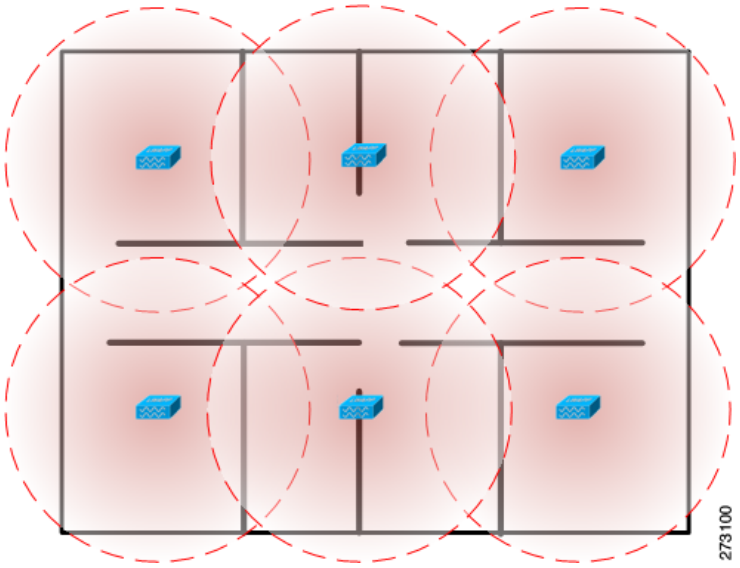
構成の条件

フロア レイアウトやビルディングの素材などの構成固有の環境条件 ワイヤレス信号の伝播は信号が通過する素材の種類に大きく依存するため、多数の壁のあるオフィス環境では、空の倉庫よりも多くのセンサーが必要になります。このことは、データ サービス アクセス ポイントの構成方法に関する既存の知識と同様です。RF 信号の減衰を引き起こす環境内の障害物が多いほど、ワイヤレス IPS アクセス ポイントを高い密度で構成する必要があります。

下の図では、ワイヤレス信号を妨害したり、弱めたりする壁がなければ、長距離の攻撃を「リッスン」できるワイヤレス IPS アクセス ポイントを構成したオープンな室内環境を示しています。



明確な対比として、下の図では、信号の減衰を引き起こす多数の厚い壁のある室内環境を示しています。この場合、攻撃を検出するために、多くのワイヤレス IPS アクセス ポイントを構成する必要があります。



監視する周波数帯域

2.4GHz および 5GHz 帯域の無線周波数伝播特性は、双方の波長の差の結果として異なります。簡単に述べると、2.4GHz ワイヤレス信号（802.11b/g/n）は、5GHz（802.11a/n）より長距離を伝送します。目的のインストールに必要なワイヤレス IPS アクセス ポイント数を正確に計算するには、ワイヤレス IPS 構成で監視する必要がある周波数帯域を考慮する必要があります。

ワイヤレス IPS AP（2.4GHz）あたりの監視範囲		
データ レート	壁のある室内	オープンな室内
6Mbps @ -86dBm	～ 35,000 sqft	～ 85,000 sqft

ワイヤレス IPS AP（5GHz）あたりの監視範囲		
データ レート	壁のある室内	オープンな室内
6Mbps @ -86dBm	～ 15,000 sqft	～ 30,000 sqft

上の表は、各周波数および各タイプの環境で、1 つのワイヤレス IPS モニタ モード アクセス ポイントでカバーできる円の平方フィートを示しています。これらのメトリックから、特定のフロア領域をカバーするために必要なワイヤレス IPS アクセス ポイント数の基準がわかります。このガイダンスで使用しているレシーバ感度は、ワイヤレス IPS をサポートするシスコのアクセス ポイントのライン間の最小公分母を示しています。

セキュリティの信頼度

さまざまな垂直産業のワイヤレス セキュリティ モニタリングのニーズは、特定の規制や使用状況によって大きく異なるため、1 つの特定の構成密度がすべてのインストールに適合するとは限りません。平方フィートあたりのワイヤレス IPS アクセス ポイントの特定数を簡単に選択するために、「セキュリティ信頼度」に基づいたスライド制を導入します。

壁のある室内環境では、2.4GHz の伝播特性により、密度の低いワイヤレス IPS アクセス ポイントの構成でも十分な検出信頼度を達成できますが、5GHz 帯域で高い信頼度を確保するには、高密度の構成が必要になります。下の表に、さまざまな構成密度を使用した場合の検出のレベルの違いを示します。この場合の構成密度とは、XX,000 平方フィートあたり 1 つの割合で、ワイヤレス IPS アクセス ポイントを構成することを意味します。

一般的な推奨事項として、政府、金融、小売などのセキュリティをより重視するお客様では、最も厳格な要件を必要とするため、「ゴールド」レベルの構成を使用します。カーペット敷きの企業や一般的なオフィス環境では、「シルバー」レベルを選択すれば、どちらの周波数帯域でも十分または良好な検出が可能です。5GHz のセキュリティにほとんど関心がない場合にだけ、「ブロンズ」レベルを使用します。この構成密度ではこの周波数帯域の検出が制限されます。

表 2　　壁のあるオフィス室内環境

信頼度	構成密度	2.4GHz 検出	5GHz 検出
ゴールド	15,000 sqft	網羅的	包括的
シルバー	20,000 sqft	包括的	適正
ブロンズ	25,000 sqft	適正	不足

オープンな室内環境は、ワイヤレス信号とセキュリティの脅威の検出を妨げる可能性のある障害物がほとんどまたはまったくない環境です。オープン室内環境では、2.4GHz の伝播特性により、密度の低いワイヤレス IPS アクセス ポイントの構成でも十分な検出信頼度を達成できますが、5GHz 帯域で、高い信頼度を確保するには、高密度の構成が必要になります。下の表に、さまざまな構成密度を使用した場合の検出のレベルの違いを示します。この場合の構成密度とは、XX,000 平方フィートあたり 1 つの割合で、ワイヤレス IPS アクセス ポイントを構成することを意味します。

表 3　　オープンな室内環境

信頼度	構成密度	2.4GHz 検出	5GHz 検出
ゴールド	30,000 sqft	網羅的	包括的
シルバー	40,000 sqft	包括的	適正
ブロンズ	50,000 sqft	適正	不足

下の表では、インストールのタイプに応じて使用するワイヤレス IPS アクセス ポイント数の違いを示すことを目的としています。この表は、例として提示しているだけで、すべての構成に対応する確実なルールを示しているのではありません。

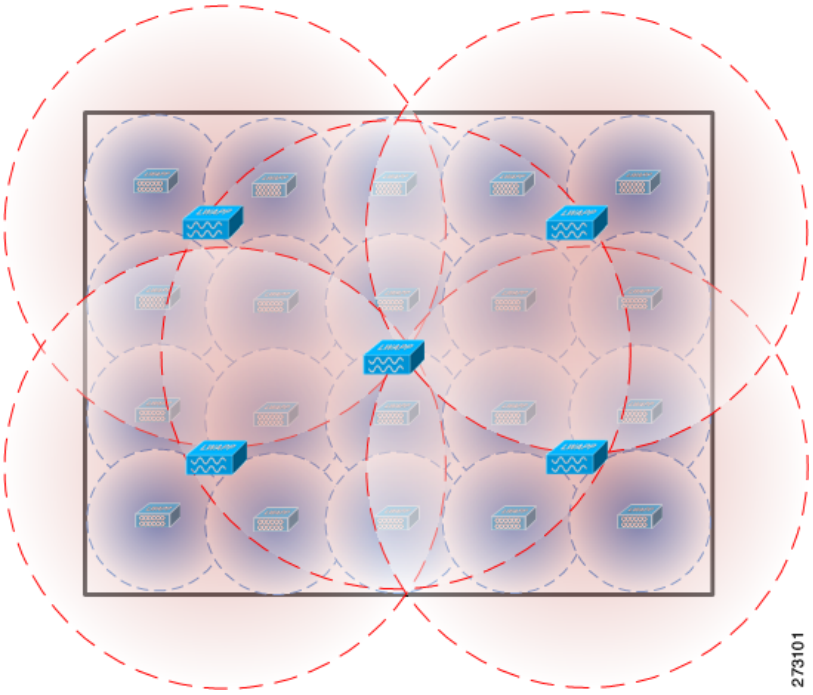
表 4　　構成の例

構成	レベル	サイズ	密度	ワイヤレス IPS AP 数
金融機関のオフィス	ゴールド	200,000 sqft	15,000 sqft	14
企業のオフィス	シルバー	200,000 sqft	20,000 sqft	10
倉庫	シルバー	200,000 sqft	30,000 sqft	5

ワイヤレス IPS アクセス ポイントの位置

ワイヤレス IPS モニタ モード アクセス ポイントの物理構成は、WLAN インフラストラクチャ全体を広く監視するという最終目標に基づきます。このため、ワイヤレス IPS モード AP は、2 つの一般的なガイドラインに従って配置します。まず、ワイヤレス IPS アクセス ポイントを物理的な位置の周辺に配置して、ビルディングの外部から仕掛けられた攻撃を十分に監視します。これは、ワイヤレス IPS モード アクセス ポイントをビルディングの物理的な先端に配置するのではなく、検出範囲が先端に達するように適切に配置する必要があることを意味します。次に、ワイヤレス IPS アクセス ポイントをビルディングの中心全体に配置し、物理的なビルディング内部から仕掛けられた攻撃を検出できるようにします。

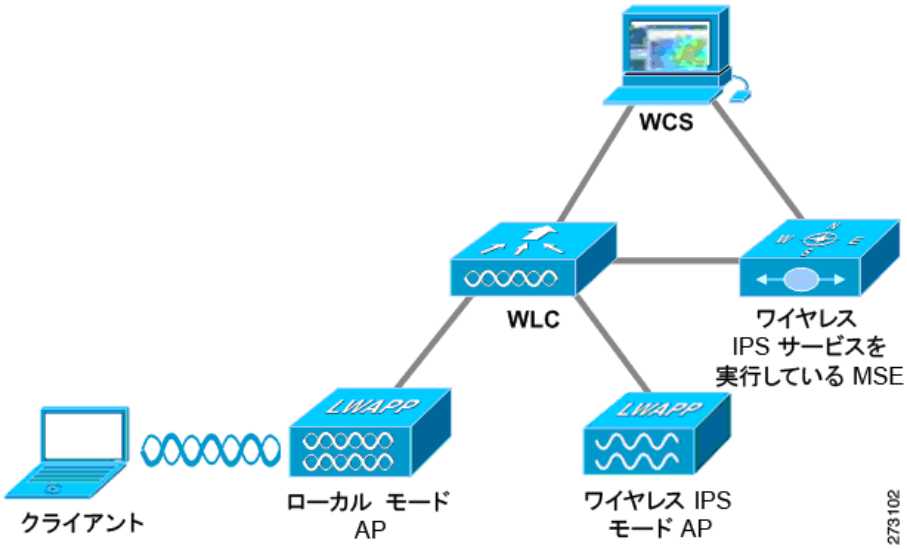
ワイヤレス IPS アクセス ポイントの物理的な設置位置は、データ サービス アクセス ポイントを設置する場合と同じベスト プラクティスに基づく必要があります。これらの規則に従って、ワイヤレス IPS アクセス ポイントのアンテナを厚いビルディング素材の陰に設置したり、吊り天井の上に設置したりしないことが重要です。アクセス ポイントを吊り天井の上に配置する場合、固有の外部アンテナを使用して、監視する同じ物理空間にアンテナを引き込む必要があります。



上の構成例では、4 つのワイヤレス IPS アクセス ポイントをビルディングの境界周辺に配置し、物理的なビルディングの周辺全体のセキュリティ モニタリングを実現します。さらに、1 つのワイヤレス IPS アクセス ポイントをビルディングの中心に配置して、ビルディング内部のセキュリティ モニタリングを実行します。

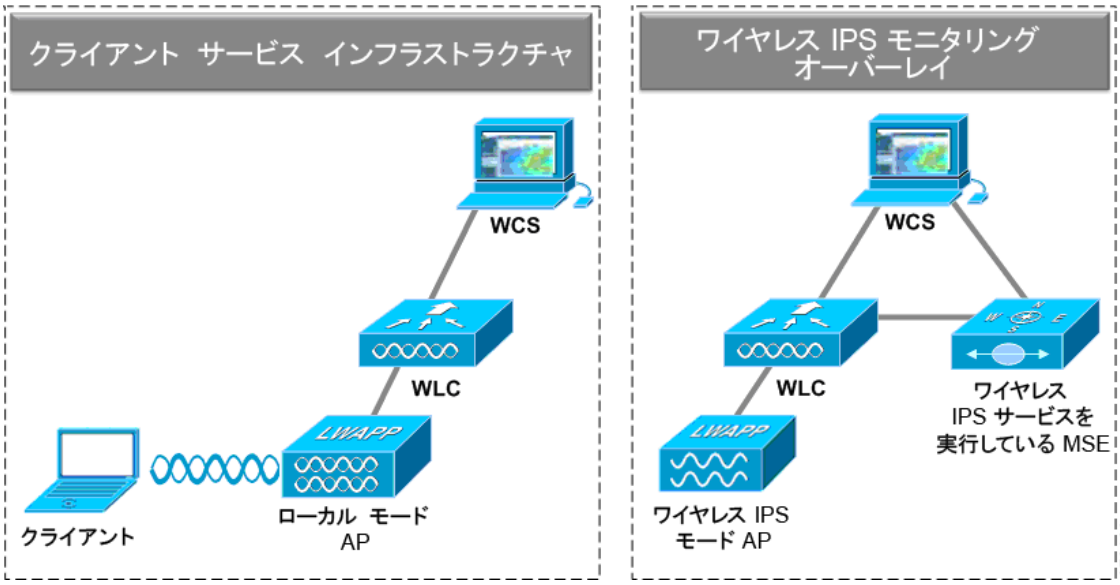
Cisco Unified Wireless Network に統合されたワイヤレス IPS

統合ワイヤレス IPS 構成は、ローカル モードとワイヤレス IPS モニタ モードの両方のアクセス ポイントを同じコントローラ上で混合させ、同じワイヤレス制御システムによって管理するシステム設計です。これは、クライアント サービス インフラストラクチャとモニタリング インフラストラクチャ間の緊密な統合を可能にするため、推奨される構成です。実際に、コントローラやワイヤレス制御システムなどの多くのコンポーネントは 2 つの用途を持つため、重複したインフラストラクチャのコストを削減します。

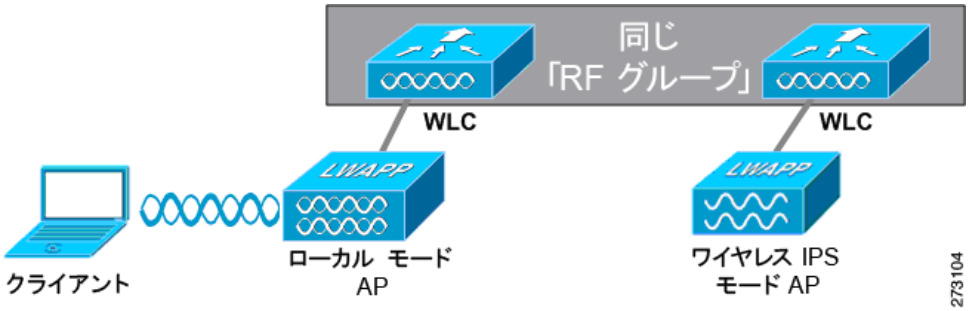


Cisco Unified Wireless Network 内のワイヤレス IPS オーバーレイ

ワイヤレス IPS オーバーレイ構成では、ワイヤレス IPS モニタリング インフラストラクチャはクライアント サービス インフラストラクチャから完全に分離されます。各システムが独自のコントローラ、アクセス ポイント、およびワイヤレス制御システムのセットを使用します。この構成モデルを選択する理由の多くは、個別の管理コンソールを使用した個別のネットワーク インフラストラクチャ システムとセキュリティ インフラストラクチャ システムを必要とするビジネス上の規定に起因します。また、この構成モデルは、アクセス ポイント（ワイヤレス IPS とローカル モード）の合計数が WCS に含まれる 3000 AP 制限を超える場合にも使用されます。



ワイヤレス IPS オーバーレイ モニタリング ネットワークを構成して、クライアント サービス インフラストラクチャのセキュリティ査定を行うには、特定の構成項目を実行する必要があります。ワイヤレス IPS システムは、「信頼される」デバイスに対する攻撃だけをログに記録するという前提で動作します。オーバーレイ システムで、個別の Cisco Unified WLAN インフラストラクチャを「信頼される」ものとして表示するには、コントローラが同じ RF グループに属している必要があります。



クライアント サービス インフラストラクチャをワイヤレス IPS モニタリング オーバーレイ インフラストラクチャから分離した結果として、業界で提供されているすべてのワイヤレス IPS オーバーレイ構成モデルに一般的ないくつかのモニタリングの警告が発生します。

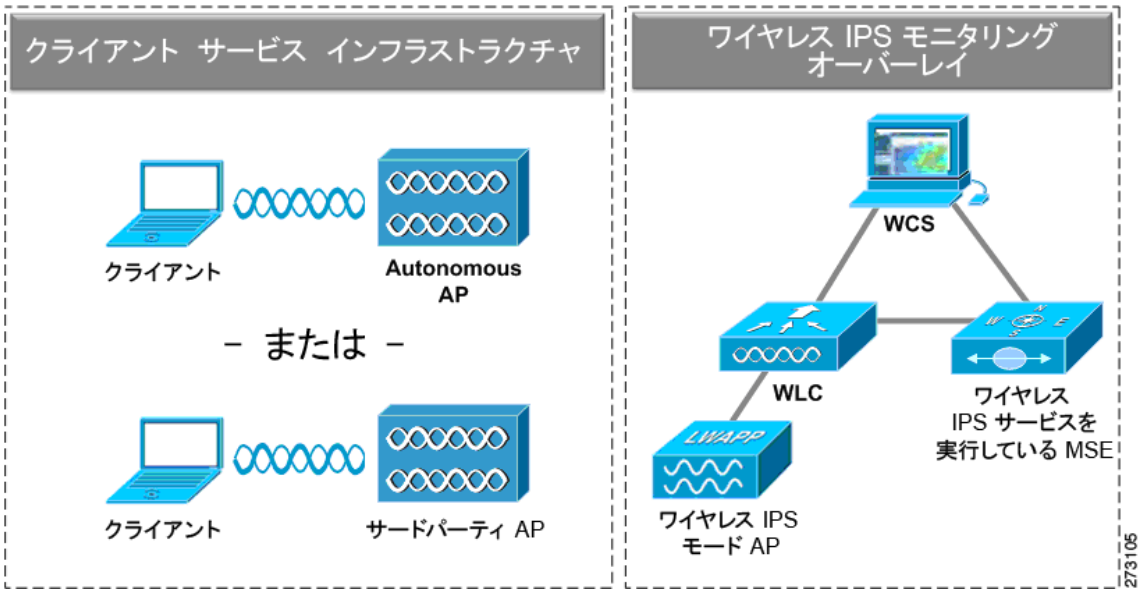
- ワイヤレス IPS アラームはワイヤレス IPS オーバーレイ WCS インスタンスにだけ表示されます。
- Management Frame Protection（MFP ; 管理フレーム保護）アラームは、クライアント インフラストラクチャ WCS インスタンスにだけ表示されます。
- 不正アラームは両方の WCS インスタンスに表示されます。
- 不正位置の精度は、クライアント サービス インフラストラクチャ WCS の方が高くなります。この構成では、ワイヤレス IPS オーバーレイよりも高密度のアクセス ポイントを使用するためです。
- Over-the-Air 不正緩和は、ローカル モード AP を緩和操作で利用できるため、統合モデルで拡張性が高くなります。
- セキュリティ モニタリング ダッシュボードは両方の WCS インスタンスで不完全になります。ワイヤレス IPS などの一部のイベントがワイヤレス IPS オーバーレイ WCS にだけ存在するためです。ワイヤレス ネットワークの包括的なセキュリティを真に監視するには、両方のセキュリティ ダッシュボード インスタンスを監視する必要があります。

	クライアント サービング インフラストラクチャ WCS	ワイヤレス IPS モニタリング オーバーレイ WCS
ワイヤレス IPS アラーム	なし	あり
MFP アラーム	あり	なし
不正アラーム	あり	あり
不正位置	高精度	低精度
不正阻止	あり	あり、ただし拡張性が低い

オーバーレイ ソリューションの考慮事項の 1 つは、クライアント サービス インフラストラクチャまたはワイヤレス IPS モニタリング オーバーレイ上の軽量アクセス ポイントが誤ったコントローラに関連付けられる可能性です。これは、各アクセス ポイント（ローカル モードとワイヤレス IPS モード）で第 1、第 2、第 3 ワイヤレス LAN コントローラ名を指定することによって阻止できます。さらに、各

ソリューションのコントローラにそれぞれのアクセス ポイントとの通信用の個別の管理 VLAN を備え、ACL を使用して LWAPP/CAPWAP トラフィックがこれらの VLAN 境界を超えないようにすることをお勧めします。

Autonomous またはその他のワイヤレス ネットワークでのワイヤレス IPS オーバーレイ



適応型ワイヤレス IPS ソリューションは、Cisco Unified WLAN ソリューションを使用しない既存の WLAN インフラストラクチャへのセキュリティ モニタリングも実行できます。この場合、クライアント サービス インフラストラクチャは完全に分離され、ワイヤレス IPS オーバーレイと連携しません。この構成シナリオの使用例には、シスコの Autonomous アクセス ポイントまたはサード パーティ アクセス ポイントが含まれています。

適応型ワイヤレス IPS の機能

コントローラ IDS と MSE ベースの適応型ワイヤレス IPS の違い

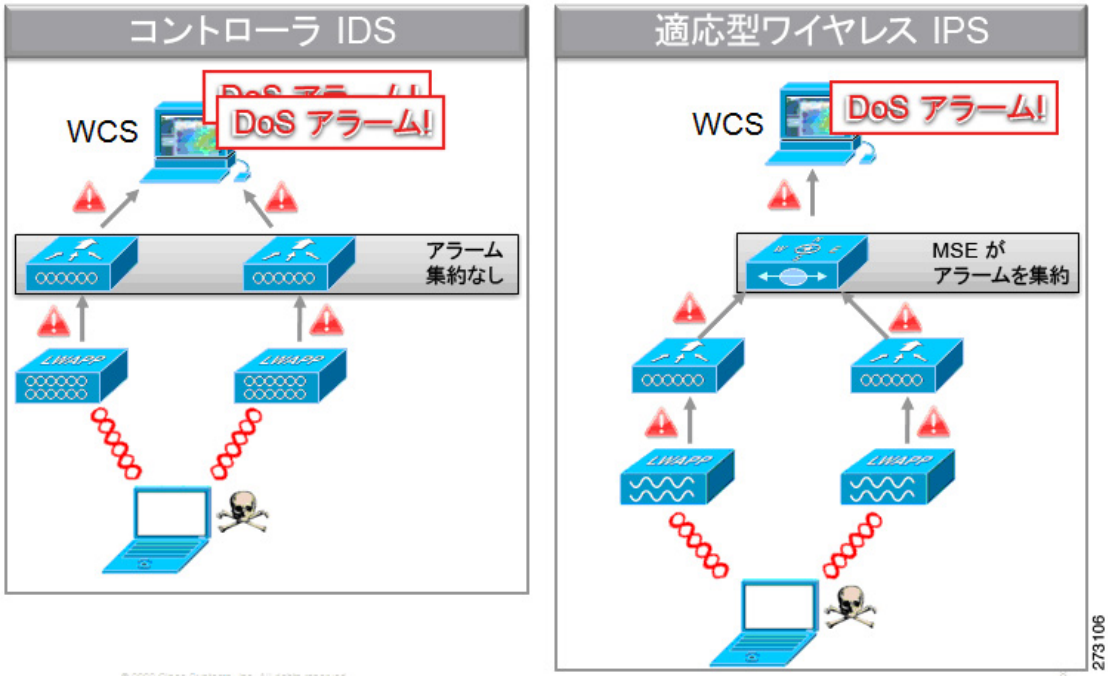
偽陽性（False Positives）の削減

シスコの 適応型ワイヤレス IPS ソリューションを使用すると、ワイヤレス ネットワークのセキュリティの監視に関して、偽陽性 を削減できます。無線で多数の管理フレームを検出した場合に、単にアラームをトリガーするだけのシスコのコントローラベースのソリューションと異なり、Cisco 適応型ワイヤレス IPS システムは、ワイヤレス インフラストラクチャ ネットワークに害を及ぼす無線での多数の管理フレームを検出した場合にだけ、アラームをトリガーします。これは、適応型ワイヤレス IPS シ

ステムがワイヤレス インフラストラクチャ内に存在するアクセス ポイントとクライアントの状態および有効性を動的に識別できる結果です。攻撃がインフラストラクチャに対して仕掛けられた場合にだけアラームが生成されます。

アラーム集約

シスコの既存のコントローラベースの IDS システムとシスコの MSE ベースの 適応型ワイヤレス IPS システムの大きな違いの 1 つは、無線で検出された一意の攻撃が 1 つのアラームに関連付けられ、集約されることです。これは、ワイヤレス IPS システムによって、特定の各攻撃が初めて識別されたときに、それらに一意のハッシュ キーを自動的に割り当てることで実行されます。複数のワイヤレス IPS アクセス ポイントで攻撃が受信された場合、モビリティ サービス エンジンでアラーム集約が行われるため、WCS に 1 回だけ転送されます。これは、アラームを集約しないシスコの既存のコントローラベースの IDS システムとはまったく対照的です。



シスコのコントローラベースの IDS と Cisco 適応型ワイヤレス IPS のもう 1 つの大きな違いは、各システムで検出可能な攻撃数です。サブセクションでの説明と下の表に示すように、ワイヤレス IPS は多数の攻撃と攻撃ツールを検出できます。これらの攻撃には、DoS 攻撃とセキュリティ ペネトレーション攻撃のどちらも含まれます。

DoS 攻撃

DoS 攻撃には、ワイヤレス ネットワーク内の正常な通信を妨害または遅延させるように設計されたメカニズムが含まれます。これらには、ワイヤレス ネットワーク内の正規の接続をドロップさせたり、不安定にさせるように設計された多数のスプーフされたフレームが組み込まれることがあります。DoS 攻撃は、ワイヤレス ネットワークの信頼できるサービスを提供する機能に打撃を与える可能性がありますが、データ違反にはならず、攻撃が停止すれば、多くはマイナスの影響がなくなります。

下の表に、コントローラベースのワイヤレス IDS と MSE ベースの適応型ワイヤレス IPS によって検出されるさまざまなクラスの DoS 攻撃を示します。各クラスにはいくつかの攻撃ツールと手法が関連付けられている場合があります。

アラーム名	コントローラ IDS によって検出	ワイヤレス IPS によって検出
アソシエーション フラッド	○	○
アソシエーション テーブル オーバーフロー		○
認証フラッド	○	○
EAPOL-Start 攻撃	○	○
PS-Poll フラッド		○
認証されないアソシエーション		○
CTS フラッド		○
Queensland University of Technology Exploit		○
RF Jamming 攻撃		○
RTS フラッド		○
仮想キャリア攻撃	○	○
認証失敗攻撃		○
認証解除ブロードキャスト攻撃	○	○
認証解除フラッド攻撃	○	○
アソシエーション解除ブロードキャスト攻撃		○
アソシエーション解除フラッド攻撃	○	○
EAPOL-Logoff 攻撃	○	○
FATA-Jack ツール検出		○
Premature EAP- 失敗攻撃		○
Premature EAP- 成功攻撃		○

セキュリティ ペネトレーション攻撃

ワイヤレス ネットワークを脅かす 2 つの攻撃タイプのうち、ほぼ間違いなく有害性の高いセキュリティ ペネトレーションは、機密データや後で機密データを見るために使用できる暗号キーなどの情報をキャプチャしたり、公開したりするように設計されています。セキュリティ ペネトレーション攻撃には、インフラストラクチャに対するクエリや暗号鍵を解読することを目的とした応答攻撃が含まれることがあります。さらに、セキュリティ ペネトレーション攻撃は、クライアントをハニーポットなどの偽のアクセス ポイントにクライアントを誘導しようと試みることによってクライアントに害を及ぼす可能性もあります。

下の表に、コントローラベースのワイヤレス IDS と MSE ベースの適応型ワイヤレス IPS によって検出されるさまざまなクラスのペネトレーション攻撃を示します。各クラスにはいくつかの攻撃ツールと手法が関連付けられている場合があります。

アラーム名	コントローラ IDS によって検出	ワイヤレス IPS によって検出
Airsnarf 攻撃		○
ChopChop 攻撃		○
WLAN のセキュリティ異常による Day-Zero 攻撃		○
デバイスのセキュリティ異常による Day-Zero 攻撃		○
AP のデバイス プローブ		○
EAP メソッドへの辞書攻撃		○
802.1x 認証に対する EAP 攻撃		○
偽の AP の検出	○	○
偽の DHCP サーバの検出		○
高速 WEP クラックの検出		○
フラグメンテーション攻撃		○
Hotspotter ツールの検出		○
不正 802.11 パケットの検出		○
Man in the Middle 攻撃の検出		○
NetStumbler の検出	○	○
NetStumbler 犠牲者の検出		○
PSPF 違反		○
ASLEAP 攻撃の検出		○
ハニーポット AP の検出	○	○
ソフト AP またはホスト AP の検出		○
スプーフされた MAC アドレスの検出		○
疑わしい営業時間外のトラフィック		○
ベンダー リストによる未承認アソシエーション		○
未承認アソシエーションの検出		○
Wellenreiter の検出	○	○

フォレンジック

Cisco 適応型ワイヤレス IPS システムは、詳しい調査とトラブルシューティングの目的で、攻撃フォレンジックをキャプチャする機能を備えます。基本レベルで、フォレンジック機能は、一連のワイヤレス フレームをログに記録し、抽出する機能を持つ切り替えベースのパケット キャプチャ ファシリティです。この機能は、WCS のワイヤレス IPS プロファイル設定内から攻撃単位でイネーブルにします。

この機能をイネーブルにすると、エアウェーブに特定の攻撃アラームが見られたら、フォレンジック機能がトリガーされます。元のアラームをトリガーしたワイヤレス IPS モニタ モード AP のバッファ内に格納されたパケットに基づいて、フォレンジック ファイルが作成されます。このファイルは CAPWAP によってワイヤレス LAN コントローラに転送され、次に NMSP によって、モビリティ サービス エンジンで実行するワイヤレス IPS サービスに転送されます。このファイルは、ユーザがフォレンジックに設定したディスク容量制限に達するまで、MSE のフォレンジック アーカイブに保存されま

す。デフォルトでこの制限は 20 ギガバイトで、この制限に達すると、最も古いフォレンジック ファイルが削除されます。フォレンジック ファイルにアクセスするには、フォレンジック ファイルへのハイパーリンクを含むワイヤレス制御システムのアラームを開きます。

（注） ワイヤレス IPS システムのフォレンジック機能はむやみに使用せず、目的の情報がキャプチャされたら無効にする必要があります。この推奨事項の理由は、アクセス ポイントにかかる負荷が大きく、この機能に必要とするスケジュールされたチャネル スキャンへの割り込みのためです。ワイヤレス IPS アクセス ポイントは、フォレンジック ファイルを生成している同じインスタンスで、チャネル スキャンを同時に実行できません。フォレンジック ファイルがダンプされている間、チャネル スキャンは最大 5 秒間遅延します。

不正検出

ワイヤレス IPS に最適化されたモニタ モードのアクセス ポイントは、現在の Cisco Unified Wireless Network 実装と同じロジックを使用して、不正脅威の査定と緩和を行います。これにより、ワイヤレス IPS モード アクセス ポイントは、不正アクセス ポイントおよびアドホック ネットワークをスキャンし、検出して、阻止することができます。不正ワイヤレス デバイスに関するこの情報が発見されると、不正アラーム集約が行われる WCS に報告されます。ただし、この機能を使用すると、ワイヤレス IPS モード アクセス ポイントを使用して、攻撃阻止が起動された場合、阻止の間、系統的な攻撃を狙いとしたチャネル スキャンを実行する機能が中断されます。

攻撃百科事典

適応型ワイヤレス IPS システムを使用するために必要な知識ベースを削減することを目的とした機能として、統合された攻撃百科事典は、システムで検出された各攻撃のビジュアルおよびテキストの説明を提供します。この攻撃百科事典は、任意のワイヤレス IPS アラームから、[Help] ハイパーリングをクリックするか、ワイヤレス IPS プロファイル設定画面を参照して使用できます。この統合百科事典は、管理者に、攻撃の実行方法、攻撃の起動に使用されるツール、可能性のある緩和方法に関する知識を提供します。

異常検出

適応型ワイヤレス IPS ソリューションには、キャプチャされた攻撃パターンやデバイス特性の異常性に関する特定のアラームも含まれます。異常検出システムでは、MSE 内に格納された攻撃履歴ログおよびデバイス履歴を考慮して、ワイヤレス ネットワークの「一般的な」特性の基準を定めます。システム上のイベントまたは攻撃に、MSE に保存されている物理データと比較して、ある程度の変化が見られた場合に、異常検出エンジンがトリガーされます。たとえば、システムで毎日わずかな MAC スプーフ イベントを定期的にキャプチャしており、別の日に MAC スプーフ イベントが 200% 増加した場合、その MSE で異常アラームがトリガーされます。次に、このアラームが WCS に送信され、システムで発生する可能性のある従来の攻撃を超えた何かがワイヤレス ネットワークで発生していることを管理者に通知されます。さらに、異常検出アラームは、ワイヤレス IPS システムに既存のシグニチャがない可能性のある Day-Zero 攻撃を検出するためにも使用できます。

デフォルトの設定プロファイル

特定の各 WLAN セキュリティ構成に合わせた設定の調整を容易にするため、適応型ワイヤレス IPS ソリューションには、特定の垂直産業のセキュリティ ニーズに合わせて作られた多数のデフォルトのプロファイルが用意されています。それらのプロファイルは、特定のインストールごとにさまざまなリスク プロファイルとセキュリティ モニタリングの要件を持つために利用されます。特定のプロファイルには、Education、Enterprise（Best）、Enterprise（Rogue）、Financial、Healthcare、Hotspot（Open Security）、Hotspot（802.1x Security）、Military、Retail、Tradeshow、Warehouse などがあります。プロファイルは、目的の構成の特定のニーズに対処するために、詳細にシステム調整するための開始点として使用することを目的としています。

リリース 5.1 機能への統合

Cisco 適応型ワイヤレス IPS ソリューションは、以前のリリースで導入された機能を使用する既存の Unified Wireless LAN に緊密に統合されます。セキュリティ ダッシュボードでは、同じ有益な警告表示の個別のカテゴリの下に適応型ワイヤレス IPS イベントが表示されます。

FAQ

Q. どのようにワイヤレス IPS 機能はライセンスされるのですか。

A. ワイヤレス IPS のライセンスは、モビリティ サービス エンジンで制御し、使用するワイヤレス IPS モード アクセス ポイント数に基づきます。ライセンス機能は、後日購入し、追加して、ソリューションのモニタリング総容量を増やすことができます。

Q. ワイヤレス IPS モニタ モード アクセス ポイントを持つワイヤレス LAN コントローラとモビリティ サービス エンジン間の予想されるトラフィック量はどれくらいになりますか。

A. WLC と MSE 間のトラフィックをキャプチャして実行されたトラフィック調査では、30 分間の平均利用率が 1,806 ビット/秒でした。この査定は、ワイヤレス IPS モニタ モードの単一のアクセス ポイントで実行されており、コントローラに関連付けられたワイヤレス IPS アクセス ポイント数に基づいて適切に見積もる必要があります。

統計	値
合計パケット数	1170
合計トラフィック数（バイト）	396,341
平均利用率（ビット/秒）	1,806
最大利用率（ビット/秒）	68,256

Q. MSE で実行しているワイヤレス IPS サービスでアーカイブできるアラーム数はいくつですか。

A. アラームはワイヤレス IPS サーバでデフォルトの 30 日間アーカイブされます。この設定は、WCS の [Mobility Services Engine] > [WIPS Service Settings] で構成の要件に基づいて増減できます。現在のリリースでアーカイブ可能なアラームの最大数は 6,000,000 で、構成環境に応じて数か月から数年のイベントを保存できます。データベースの空き容量が少なくなると、MSE から WCS にアラームが送信されます。これらのアラームの特定の間隔は総容量の 75%、85%、および 95% です。ワイヤレス IPS データベースが 95% の容量に達すると、システムが 70% 以下の容量に減少するまで最も古いアラーム レコードが強制的に無効になります。

Q. コンテキスト対応の位置と適応型ワイヤレス IPS 間の共存のレベルは何ですか。

A. ワイヤレス IPS モニタ モードのアクセス ポイントは、クライアント、不正、およびアセット タグの位置追跡に参加できます。ただし、5.2 リリースでは、モビリティ サービス エンジンは 1 つのポイントで 1 つだけサービスを実行できます。これは、ワイヤレス IPS と位置ベースのサービスを利用した Unified Wireless Network 構成では、物理的に 2 つのモビリティ サービス エンジンを使用する必要があることを意味します。この場合、1 つは適応型ワイヤレス IPS サービスを実行し、他方はコンテキスト対応サービスを実行します。2009 年度第一四半期に計画されているリリースでは、これらのサービスが同一の物理 MSE 上で共存できます。

適応型ワイヤレス IPS 設定

1：モビリティ サービス エンジンのセットアップ

ステップ 1 次の資格情報でログインします：***root/password***

ステップ 2 最初の起動時に、MSE からセットアップ スクリプトを起動するように求められます。このプロンプトに「**yes**」と入力します。

（注） MSE からセットアップが求められない場合は、次のコマンドを入力します：
/opt/mse/setup/setup.sh

ステップ 3 ホスト名と DNS ドメイン名を設定します。

```
Current hostname=[mse]
Configure hostname?  (Y)es/(S)kip/(U)se default [Skip]: y

The host name should be a unique name that can identify
the device on the network. The hostname should start with
a letter, end with a letter or number, and contain only
letters, numbers, and dashes.

Enter a host name [mse]: MSE-1

Current domain=[]
Configure domain name? (Y)es/(S)kip/(U)se default [Skip]: y

Enter a domain name for the network domain to which this device
belongs.  The domain name should start with a letter, and it should
end with a valid domain name suffix such as ".com".  It must contain
only letters, numbers, dashes, and dots.

Enter a domain name: cisco.com
```

273107

ステップ 4　イーサネット インターフェイス パラメータを設定します。

```
Current IP address=[1.1.1.10]
Current eth0 netmask=[255.255.255.0]
Current gateway address=[1.1.1.1]
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]: y

Enter an IP address for first ethernet interface of this machine.

Enter eth0 IP address [1.1.1.10]: 172.20.229.200

Enter the network mask for IP address 172.20.229.200.

Enter network mask [255.255.255.0]: 255.255.255.0

Enter an default gateway address for this machine.

Note that the default gateway must be reachable from
the first ethernet interface.

Enter default gateway address [1.1.1.1]: 172.20.229.1
```

273108

ステップ 5　eth1 インターフェイス パラメータの入力を求められた場合、2 つ目の NIC には操作が必要ないため、「**Skip**」と入力して、次の手順に進みます。

（注）　設定するアドレスは、このアプライアンスで使用する目的のワイヤレス LAN コントローラと WCS 管理システムへの IP 接続を提供する必要があります。

ステップ 6　DNS サーバ情報を入力します。正常なドメイン解決に必要な DNS サーバは 1 つだけですが、復元力のためバックアップ サーバを入力します。

```
Domain Name Service (DNS) Setup
DNS is currently enabled.
No DNS servers currently defined
Configure DNS related parameters? (Y)es/(S)kip/(U)se default [Skip]: y

Enable DNS (yes/no) [yes]: y
Enter primary DNS server IP address: 172.20.229.10
Enter backup DNS server IP address (or none) [none]: 172.20.229.20
Enter another backup DNS server IP address (or none) [none]:
```

273109

ステップ 7　タイム ゾーンを設定します。デフォルトの New York のタイム ゾーンが環境に当てはまらない場合は、[Location] メニューを参照して正しく設定します。

```
Current timezone=[America/New_York]
Configure timezone? (Y)es/(S)kip/(U)se default [Skip]: y

Enter the current date and time.

Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
 1) Africa
 2) Americas
 3) Antarctica
 4) Arctic Ocean
```

273110

ステップ 8 NTP またはシステム時間を設定します。NTP はオプションですが、システムで正確なシステム時間が維持できます。「**No**」を選択した場合、システムの現在の時間を設定するように求められます。

```
Network Time Protocol (NTP) Setup.

If you choose to enable NTP, the system time will be
configured from NTP servers that you select.  Otherwise,
you will be prompted to enter the current date and time.

NTP is currently disabled.
Configure NTP related parameters? (Y)es/(S)kip/(U)se default [Skip]: y

Enter whether or not you would like to set up the
Network Time Protocol (NTP) for this machine.

If you choose to enable NTP, the system time will be
configured from NTP servers that you select.  Otherwise,
you will be prompted to enter the current date and time.

Enable NTP (yes/no) [no]: yes
Enter NTP server name or address: time.nist.gov
Enter another NTP server IP address (or none) [none]:
```

273111

（注） モビリティ サービス エンジン、ワイヤレス LAN コントローラ、および WCS 管理システムには正しい時間を設定する必要があります。これは、3 つすべてのシステムで同じ NTP サーバをポイントし、それらに正しいタイム ゾーンが設定されるようにすることによって実現できます。

ステップ 9 ローカル コンソール ルート ログインを有効にします。このパラメータは、システムへのローカル コンソール アクセスを有効または無効にするために使用します。このパラメータは、ローカル トラブルシューティングを実行できるようにするために有効にする必要があります。

```
Remote root login is currently disabled.
Configure remote root access? (Y)es/(S)kip/(U)se default [Skip]: yes

Enter whether or not you would like to allow
remote root login via secure shell for this machine.

Enable remote root login (yes/no) [no]: yes
```

273112

ステップ 10 **（省略可能）**SSH（セキュア シェル）ルート ログインを有効にします。このパラメータは、システムへのリモート コンソール アクセスを有効または無効にするために使用します。このパラメータはリモート トラブルシューティングを実行できるようにするために有効にする必要がありますが、ただし、会社のセキュリティ ポリシーでこのオプションを無効にするように命じられている場合もあります。

```
SSH root access is currently disabled.
Configure ssh access for root (Y)es/(S)kip/(U)se default [Skip]: yes

Enter whether or not you would like to enable ssh
root login. If you disable this option, only console
root login will be possible.

Enable ssh root access (yes/no): yes
```

273113

ステップ 11 単一のユーザ モードおよびパスワードの強度を設定します。これらの設定パラメータは必要ではなく、デフォルトの設定は、「**s**」を入力して、それらをスキップすることです。

```
Single user mode password check is currently disabled.
Configure single user mode password check (Y)es/(S)kip/(U)se default [Skip]: s

Login and password strength related parameter setup
Maximum number of days a password may be used : 99999
Minimum number of days allowed between password changes : 0
Minimum acceptable password length : 5
Login delay after failed login :
Checking for strong passwords is currently disabled.
Configure login/password related parameters? (Y)es/(S)kip/(U)se default [Skip]:
s
```

273114

ステップ 12 ログイン バナーを設定します。

ログイン バナーは、システムのユーザに、未承認ユーザがシステムにアクセスできないようにするための警告を表示するために使用されます。ログイン バナーは複数行のメッセージの場合があるため、1 つのピリオド（.）でメッセージを終了し、次の手順に進みます。

```
Current Login Banner = [Cisco Mobility Service Engine]
Configure login banner (Y)es/(S)kip/(U)se default [Skip]: yes

Enter text to be displayed as login banner. Enter a single period
on a line to terminate.

Login banner [Cisco Mobility Service Engine]:
MSE-1
Unauthorized Access is not allowed
.
```

273115

ステップ 13 ルート パスワードを変更します。

この手順は、システムのセキュリティを確保するために重要であり、辞書にある単語ではない文字と数字から構成される強力なパスワードを選択してください。パスワードの最小文字数は 8 文字です。

```
Configure root password? (Y)es/(S)kip/(U)se default [Skip]: y

Enter a password for the superuser.

Enter root password:
Confirm root password:
```

273116

ステップ 14 （省略可能）GRUB パスワードを設定します。この設定パラメータは必要ではなく、デフォルトの設定は、「**s**」を入力して、それをスキップすることです。

```
GRUB password is not currently configured.
Configure GRUB password (Y)es/(D)isable/(S)kip/(U)se default [Skip]: s
```

273117

ステップ 15 WCS 通信パスワードを設定します。

```
Configure WCS communication password? (Y)es/(S)kip/(U)se default [Skip]: yes

Enter a password for the admin user.
The admin user is used by the WCS and other northbound systems
to authenticate their SOAP/XML session with the server.
Once this password is updated, it must correspondingly be updated
on the WCS page for MSE General Parameters so that the WCS can
communicate with the MSE.

Enter WCS communication password:
Confirm WCS communication password:
```

273118

ステップ 16 変更を保存して再起動します。セットアップ スクリプトが完了し、プロンプトが表示されたら、変更を保存します。保存後、プロンプトに従って MSE を再起動し、すべての設定が正しく適用されていることを確認します。

ステップ 17 ユーザ名 root と以前にステップ 13 で設定したパスワードを使用して、MSE にログインします。

ステップ 18 コマンド「service msed start」を実行して、MSE サービスを開始します。

```
login as: root
Cisco Mobility Service Engine

root@172.20.226.203's password:
Last login: Wed Jul 23 10:11:58 2008 from dhcp-171-71-123-7.cisco.com
[root@MSE-1 ~]# service msed start
Starting MSE Platform
Cannot find UDI information. Exiting
null
Invalid Platform type. Now Exiting.
Starting MSE Platform, waiting to check the status.
Starting MSE Platform, waiting to check the status.
MSE Platform is up, getting the status
```

273119

ステップ 19 起動時に MSE サービスの開始を有効にします。

コマンド「chkconfig msed on」を実行します。

```
[root@MSE-1 ~]#
[root@MSE-1 ~]# chkconfig msed on
[root@MSE-1 ~]#
```

273120

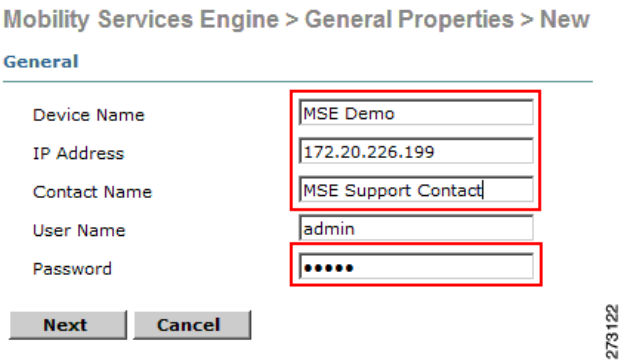
2：MSE を WCS に追加する

ステップ 1　Mobility Services 設定ページに移動します。

WCS にログインし、[Mobility] ドロップダウン メニューから [Mobility Services] をクリックします。

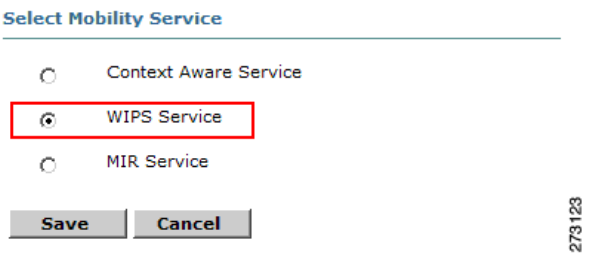
ステップ 2　WCS にモビリティ サービス エンジンを追加します。

右側のドロップ ダウンから、[Add Mobility Services Engine] を選択し、[Go] をクリックします。

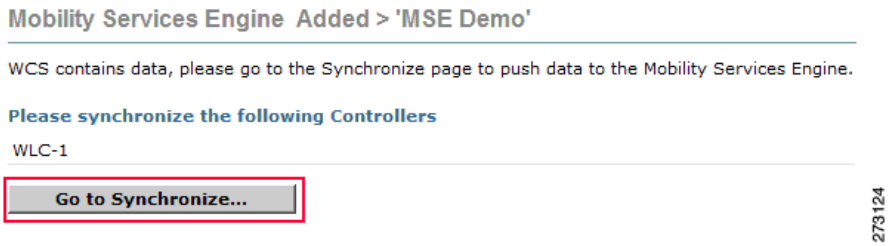


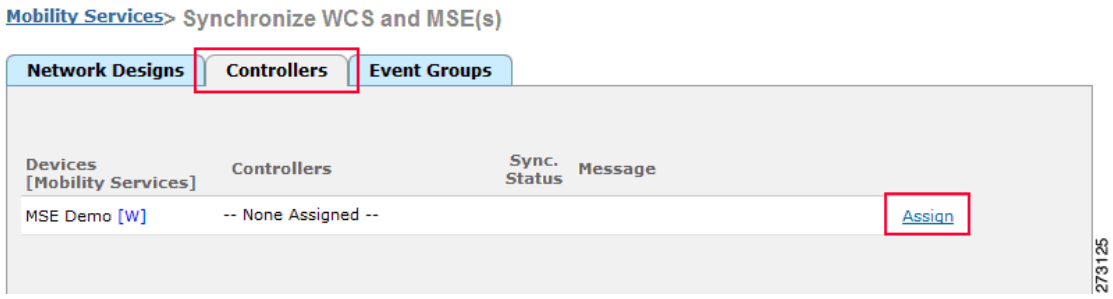
MSE の一意のデバイス名、MSE のセットアップ時に設定した IP アドレス、サポートの連絡先名、MSE のセットアップ時に設定した WCS 通信パスワードを入力します。ユーザ名をデフォルトの「admin」から変更しないでください。

ステップ 3　MSE で実行する WIPS サービスを選択します。



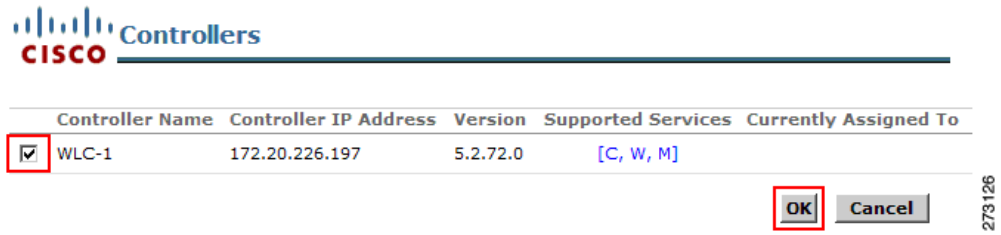
ステップ 4　同期させます。





ステップ 5 同期させるコントローラを選択します。

MSE と同期させるコントローラのリストを示すポップアップが表示されます。目的の同期させるコントローラを選択し、[OK] をクリックします。



ステップ 6 ポップアップ ウィンドウが閉じたら、[Synchronize WCS and MSE(s)] ダイアログの下部にある [Synchronize] ボタンをクリックします。

3：ワイヤレス IPS モニタ モードのアクセス ポイントを設定する

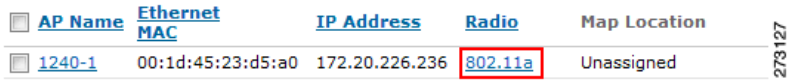
（注） ワイヤレス IPS モニタ モードをサポートしているのは、Aironet 1130、1140、1240、および 1250 シリーズのアクセス ポイントだけです。

ステップ 1 アクセス ポイント無線を無効にします。

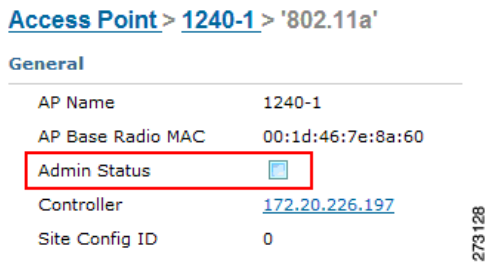
AP をワイヤレス IPS モニタ モードに設定する機能は、WCS またはワイヤレス LAN コントローラ コマンド ラインからだけアクセスできます。

a. WCS のトップ レベルのメニューから、[Configure] > [Access Points] に移動します。

b. 目的のアクセス ポイント無線を選択し、クリックします。



c. [Admin Status] をオフにして無線を無効にします。

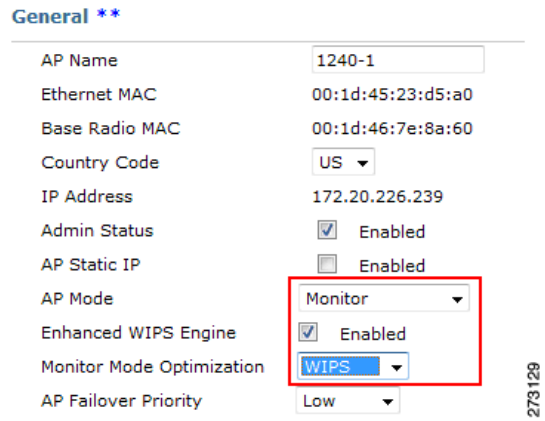


d. ページ下部の [Save] ボタンをクリックします。

（注） アクセス ポイント上のすべての無線ごとにこれらの手順を繰り返し、ワイヤレス IPS モニタ モードに設定します。たとえば Aironet 1130 では、この手順を 802.11a 無線と 802.11b/g 無線の両方で実行する必要があります。

ステップ 2 アクセス ポイントをモニタ モードに設定します。

a. 無線を無効にしたら、WCS の [Configure] > [Access Points] からアクセス ポイント設定メニューに入り、アクセス ポイントの名前をクリックします。



b. [AP Mode] を [Monitor] に変更します。

c. [Enhanced WIPS Engine] を有効にします。

d. [Monitor Mode Optimization] を [WIPS] に変更します。

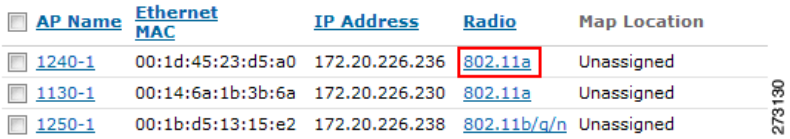
e. ページ下部の [Save] をクリックします。

f. アクセス ポイントを再起動するように求められたら、[OK] をクリックします。

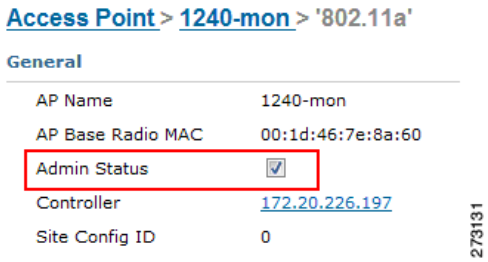
ステップ 3 アクセス ポイント無線を有効にします。

a. WCS のトップ レベルのメニューから、[Configure] > [Access Points] に移動します。

b. 目的のアクセス ポイント無線を選択し、クリックします。



c. [Admin Status] をオンにして、無線を有効にします。



d. ページ下部の [Save] をクリックします。

ワイヤレス IPS モニタ モードに設定した各アクセス ポイントおよびその各無線についてこの手順を繰り返します。

4：ワイヤレス IPS プロファイルを設定する

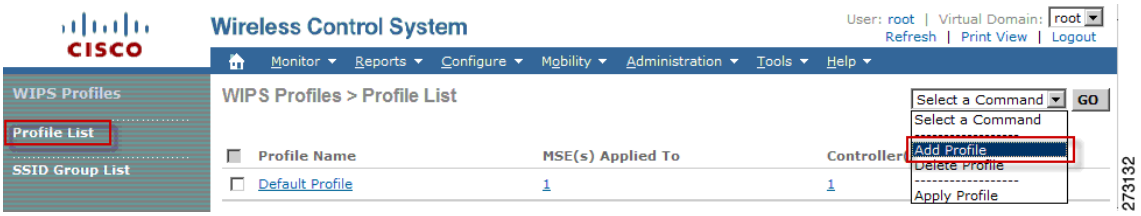
デフォルトで、MSE と対応するワイヤレス IPS アクセス ポイントは WCS からデフォルトのワイヤレス IPS プロファイルを継承します。このプロファイルは、デフォルトで有効にされている大部分の攻撃アラームによってあらかじめ調整されており、ワイヤレス IPS アクセス ポイントと同じ RF グループ内のアクセス ポイントに対する攻撃を監視します。このように、システムは WLAN インフラストラクチャとワイヤレス IPS アクセス ポイントの両方が同じコントローラ上に混合されている統合ソリューションを利用する構成モデルに対する攻撃を監視するようにあらかじめ設定されています。

（注） 下の手順の一部はオーバーレイだけとしてマークされており、Autonomous や完全に個別のコントローラベースの WLAN などの既存の WLAN インフラストラクチャを監視するように適応型ワイヤレス IPS ソリューションを構成している場合にだけ実行されます。

ステップ 1 ワイヤレス IPS プロファイルに移動します。

ステップ 2 WCS のトップ レベルのメニューから、[Configure] > [wIPS Profiles] をクリックします。

ステップ 3 新しいプロファイルを作成します。

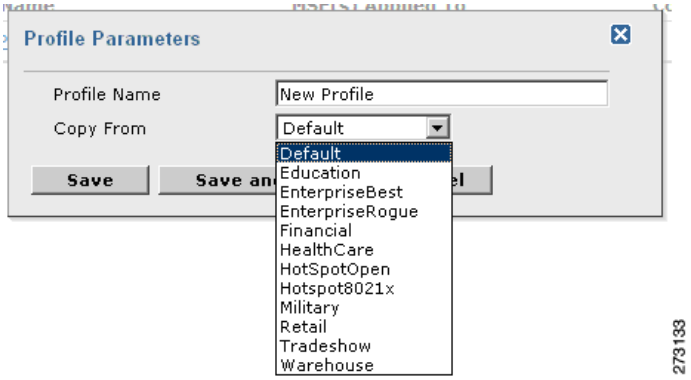


a. 左側の [Profile List] をクリックします。

b. 右上のドロップ ダウン メニューの [Add Profile] を選択します。

ステップ 4 プロファイル テンプレートを選択します。

Cisco 適応型ワイヤレス IPS システムには、一連のプロファイル テンプレートがあらかじめ定義されており、お客様はそれらを開始点として使用して、独自のカスタム プロファイルを作成できます。各プロファイル テンプレートは、特定の垂直産業に合わせて作成されており、どの特定のアラームが有効にされているかに関してはさまざまに異なります。



ステップ 5 プロファイルを選択し、名前を指定したら、[Save and Edit] をクリックします。

ステップ 6 （省略可能）監視する SSID を設定します。

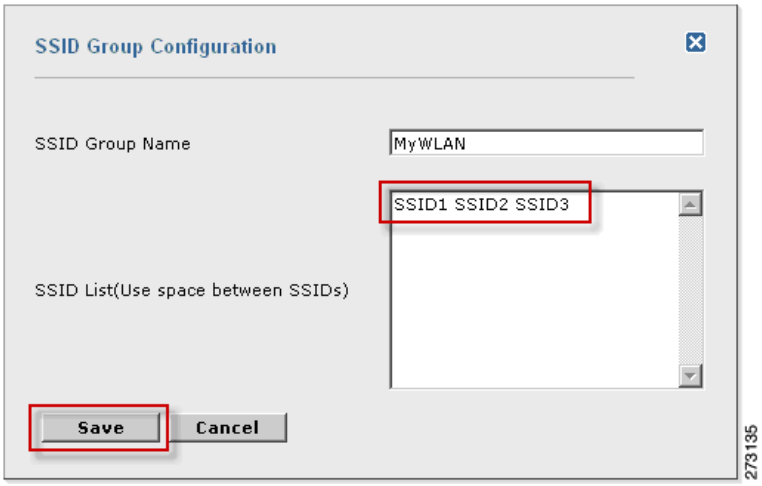
デフォルトで、ローカル ワイヤレス LAN インフラストラクチャ（同じ「RF グループ」名を持つ AP によって定義された）に対して仕掛けられた攻撃が監視されます。オーバーレイ構成モデルで構成する場合など、他のネットワークに対する攻撃を監視させる必要がある場合は、SSID グループ機能を使用する必要があります。

（注） この手順が必要ない場合は、単に [Next] をクリックします。

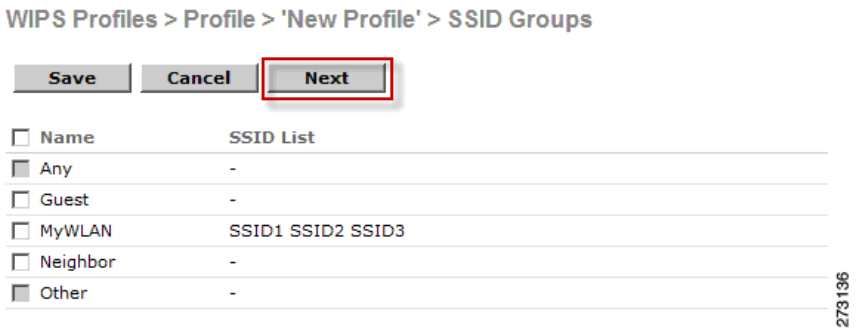
a. [MyWLAN] の横のボックスをオンにして、右上隅のドロップ ダウンから [Edit Group] を選択し、[Go] をクリックします。

b. 監視する SSID を入力します。

c. SSID（複数の場合は、1 つのスペースで区切る）を入力し、[Save] をクリックします。



[SSID Groups] ページは次のスクリーン ショットのようになり、SSID が正常に追加されたことを確認します。

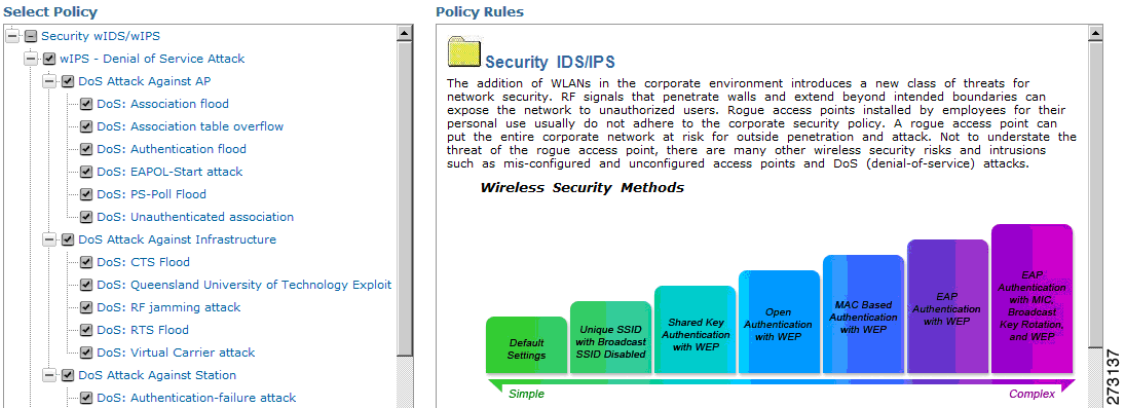


d. [Next] をクリックします。

ステップ 7 プロファイルを編集します。

この設定画面では、特定の攻撃を有効または無効にできます。さらに、管理者は特定のアラームをドリル ダウンし、それらの特定のしきい値を編集したり、フォレンジックを有効にしたりすることもできます。

アラームを有効または無効にするには、目的の特定のアラームの横のボックスをクリックするだけです。



ステップ 8 ポリシー パラメータを編集するには、アラームをクリックすると、右側のフレームが変更され、その攻撃のポイント設定が表示されます。

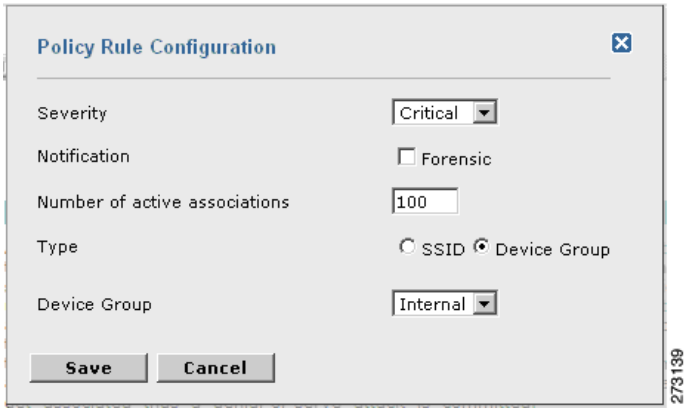
ステップ 9 ポリシー ルールを編集します。

特定のアラームを選択したら、そのアラームに関連付けられているポリシー ルールを変更できます。

a. ポリシー ルールを編集するには、ルールの横のボックスをオンにし、[Edit] をクリックします。

ポリシー ルール ウィンドウでは、多数のその他のパラメータに加え、アラームの重大度を変更できます。

b. 通知項目は、この特定のアラームにフォレンジック（パケット キャプチャ）を採用するかどうかを定義するチェック ボックスです。さらに、このアラームの特定のしきい値もあり、この例ではアクティブなアソシエーション数として定義されていますが、これはアラームごとに異なります。次に、タイプ パラメータで、システムに攻撃を監視させる WLAN インフラストラクチャを定義します。デフォルトで、これは [Device Group] と [Internal] に設定され、ワイヤレス IPS AP と同じ「RF グループ」名のすべての AP を指定します。タイプを [SSID] に変更すると、オーバーレイ構成に一般的な個別のネットワークを監視させることができます。この構成については後述します。



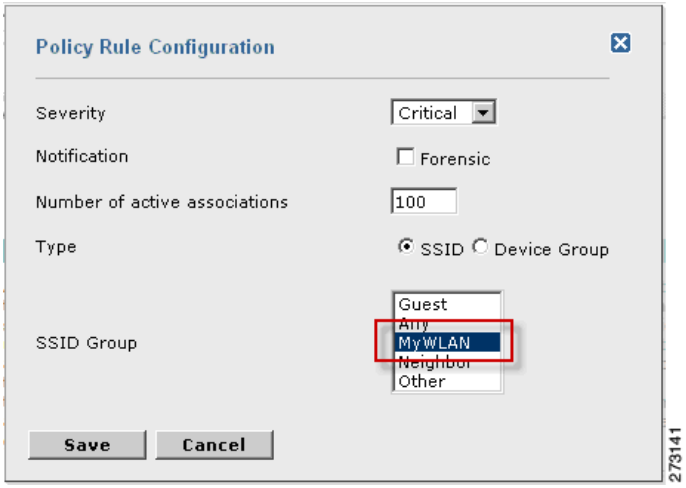
ステップ 10 （**省略可能**）ポリシー ルールを追加します。

ポリシー ルールの追加は、一般に、SSID によって別の WLAN インフラストラクチャを監視するように構成されるオーバーレイ構成でだけ必要になります。

a. ポリシー ルールを追加するには、[Add] をクリックします。

ポリシー ルール ウィンドウでは、多数のその他のパラメータに加え、アラームの重大度を変更できます。

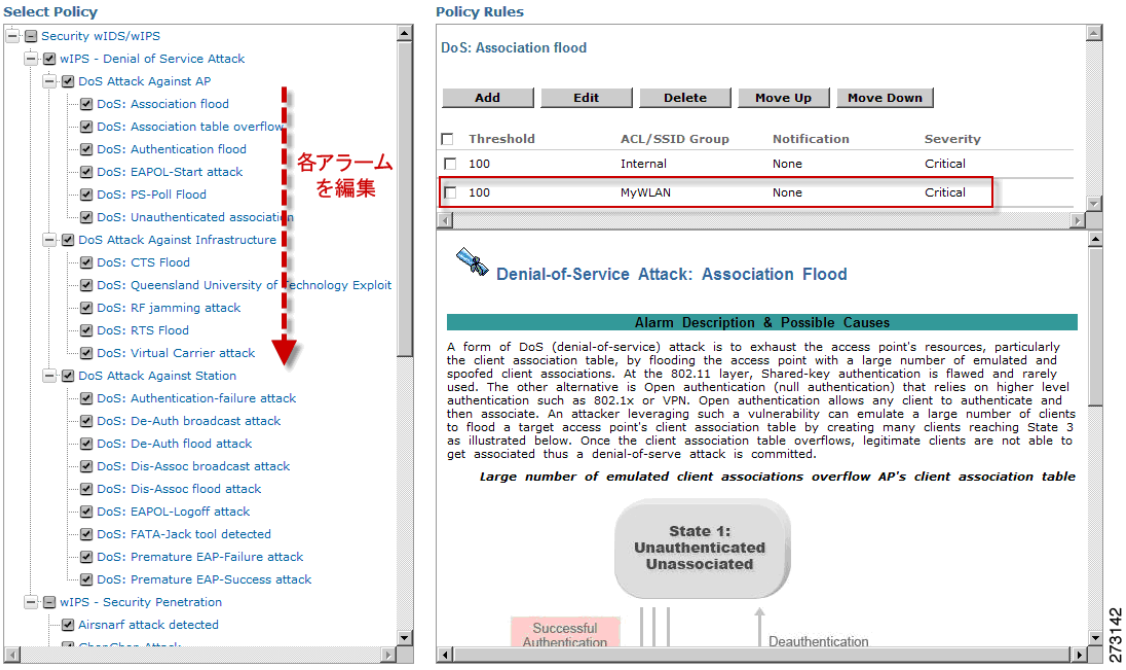
b. 通知項目は、この特定のアラームにフォレンジック（パケット キャプチャ）を採用するかどうかを定義するチェック ボックスです。さらに、このアラームの特定のしきい値もあり、この例ではアクティブなアソシエーション数として定義されていますが、これはアラームごとに異なります。次に、タイプ パラメータで、システムに監視させる SSID を定義します。タイプを [Device Group] に変更すると、システムは同じ「RF グループ」の AP に対する攻撃だけを監視します。[SSID] を選択している場合、先にセットアップで SSID グループによって定義したとおりに、システムを使用して、個別の WLAN インフラストラクチャに対する攻撃を監視することができます。



c. 変更したら、[Save] をクリックします。

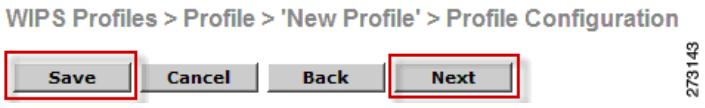
ステップ 11 （**省略可能**）追加のポリシー ルールを設定します。

SSID によって別の WLAN インフラストラクチャを監視するようにシステムを設定した場合、SSID によって監視するように、すべての各ポリシー ルールを変更する必要があります。個別の各アラームに、システムで以前に作成した SSID グループに対する攻撃を監視するように定義したポリシー ルールを作成する必要があります。



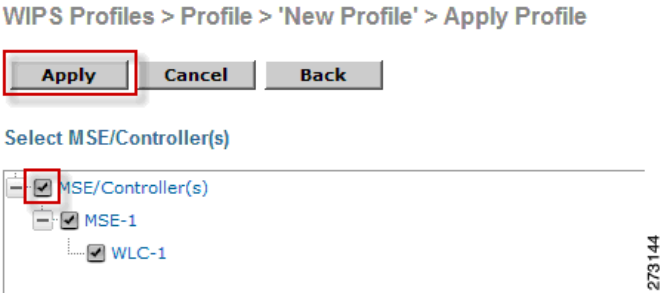
ステップ 12 プロファイルを保存します。

変更したら、[Save] をクリックして、プロファイルを WCS に保存し、終了したら、[Next] をクリックします。



ステップ 13 プロファイルを適用します。

プロファイルを適用する MSE/ コントローラの組み合わせを選択して、[Apply] をクリックします。



5. コントローラベースの IDS を無効にする

監視する領域全体に適応型ワイヤレス IPS システムをインストールしたら、シスコの従来のワイヤレス LAN コントローラ IDS を無効にすることをお勧めします。この手順を実行して、適応型ワイヤレス IPS と既存の IDS システムの両方で重複したアラートがトリガーされないようにします。

ステップ 1 コントローラにログインします。

ステップ 2 トップレベル コントローラ メニューの [Security] タブをクリックします。

ステップ 3 左側で、[Wireless Protection Policies] > [Standard Signatures] をクリックします。

ステップ 4 下のスクリーンショットに示すように、標準シグニチャをオフにします。