CHAPTER 1

概要

- この章では、Cisco Unified Wireless Network（CUWN）全体における Cisco 3300 モビリティ サービス エンジン（MSE）および Cisco Adaptive Wireless Intrusion Prevention System（wIPS）のロールについて説明します。この章は、次の内容で構成されています。
- 「wIPS について」（P.1-1）
- 「Cisco Unified Wireless Network 内の wIPS」（P.1-2）
- 「コントローラ IDS と Adaptive wIPS の違い」（P.1-6）

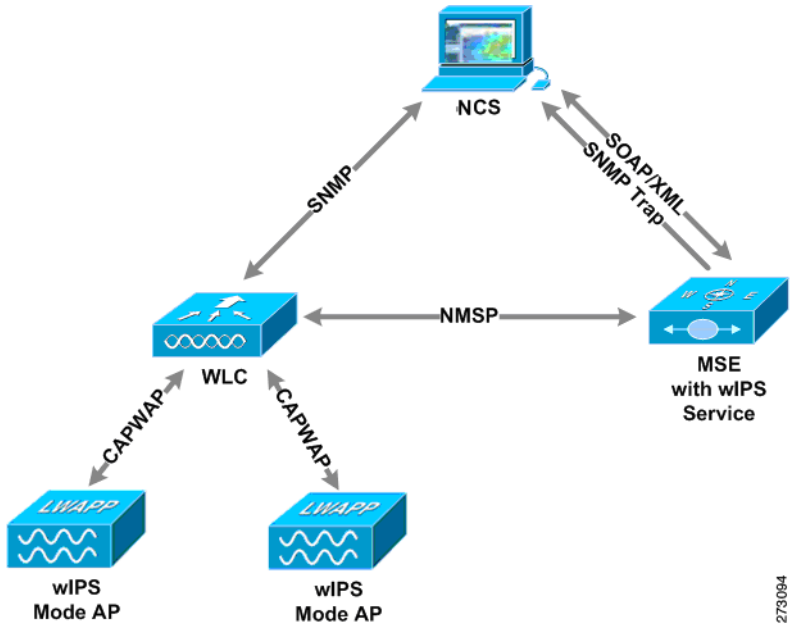
wIPS について

wIPS は、不正アクセス ポイント、不正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。

CUWN を基盤にし、Cisco Motion の効果を利用した wIPS は構成が強化され、企業に対応しています。wIPS は、連携して統合セキュリティ モニタリング ソリューションを実現する、次のコンポーネントで構成されています。

- wIPS ソフトウェア実行中のモビリティ サービス エンジン（MSE）：すべてのコントローラとそれぞれの wIPS 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モビリティ サービス エンジンに保存されます。
- wIPS モニタ モード アクセス ポイント：攻撃検出とフォレンジック（パケット キャプチャ）機能を備えた固定チャネル スキャンを提供します。
- ローカル モード アクセス ポイント：タイムスライス型不正スキャンに加え、ワイヤレス サービスをクライアントに提供します。
- ワイヤレス LAN コントローラ：wIPS モニタ モード アクセス ポイントから受信した攻撃情報をモビリティ サービス エンジンに転送し、設定パラメータをアクセス ポイントに配布します。
- Cisco Prime Network Control System（NCS）：モビリティ サービス エンジン上での wIPS サービスの設定、コントローラへの wIPS 設定内容のプッシュ、wIPS モニタ モードのアクセス ポイントの設定を行う、一元化された管理プラットフォームを管理者に提供します。NCS は、wIPS アラーム、フォレンジック、報告の表示や、攻撃百科事典へのアクセスにも使用されます（図 1-1 を参照）。

図 1-1　Wireless Intrusion Prevention System（ワイヤレス侵入防御システム）



システム コンポーネント間の通信には、次のプロトコルが使用されます。

- Control and Provisioning of Wireless Access Points（CAPWAP）：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用されます。これは、アラーム情報をコントローラに送信し、設定情報をアクセス ポイントに送信する双方向トンネルを提供します。
- ネットワーク モビリティ サービス プロトコル（NMSP）：このプロトコルは、コントローラとモビリティ サービス エンジン間の通信を処理します。wIPS 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集約して、モビリティ サービス エンジンに転送し、wIPS 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
- Simple Object Access Protocol（SOAP/XML）：モビリティ サービス エンジンと NCS 間の通信の方法。このプロトコルは、モビリティ サービス エンジンで実行する wIPS 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
- 簡易ネットワーク管理プロトコル（SNMP）：このプロトコルは、モビリティ サービス エンジンから NCS に wIPS アラーム情報を転送するために使用されます。また、コントローラから NCS に不正アクセス ポイント情報を伝えるためにも使用されます。

ガイドラインと制限事項

HREAP モード アクセス ポイントは、wIPS をサポートします。

Cisco Unified Wireless Network 内の wIPS

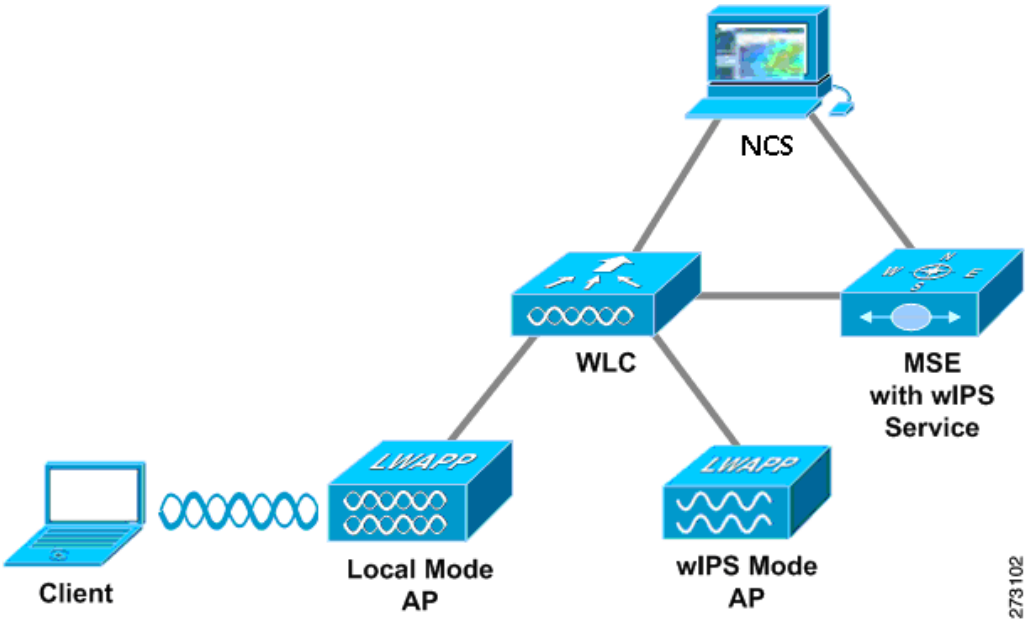
CUWN インフラストラクチャ内で wIPS を統合したり、CUWN やシスコの自律ワイヤレス ネットワーク（またはサードパーティのワイヤレス ネットワーク）に wIPS をオーバーレイしたりできます。

この項では、次のトピックを扱います。

Cisco Unified Wireless Network 内の統合された wIPS

統合 wIPS 構成は、*ローカル* モードと wIPS *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 NCS 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 サービング 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（図 1-2 を参照）。

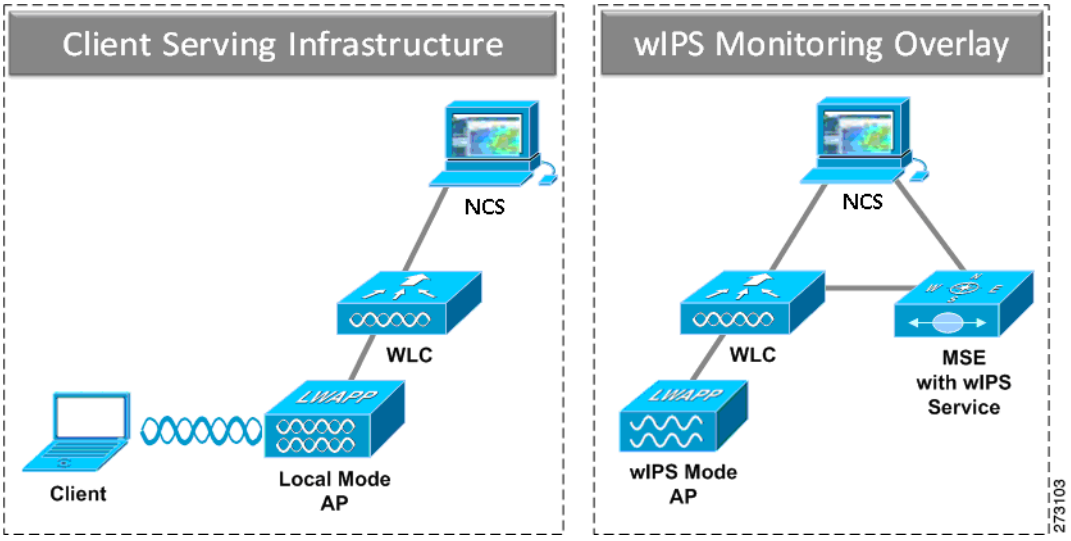
図 1-2　CUWN 内の統合された wIPS



Cisco Unified Wireless Network 内の wIPS オーバーレイ構成

wIPS オーバーレイ構成では、wIPS モニタリング インフラストラクチャはクライアント サービング 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 NCS 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（図 1-3 を参照）。また、この構成モデルは、アクセス ポイント（wIPS モニタとローカル モード）の合計数が NCS に含まれる 3000 アクセス ポイントの制限を超える場合にも使用されます。

図 1-3　CUWN 内の wIPs オーバーレイ モニタリング ネットワーク構成



wIPS 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 サービング 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。wIPS 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（図 1-4 を参照）。

図 1-4　wIPS オーバーレイ モニタリング ネットワークの同じ RF グループに属しているコントローラ

クライアント サービング インフラストラクチャを wIPS オーバーレイ モニタリング ネットワークから分離した結果として、いくつかのモニタリングの警告が発生します。

- wIPS アラームは、wIPS オーバーレイ NCS インスタンスにだけ表示されます。
- 管理フレーム保護（MFP）アラームは、クライアント インフラストラクチャ NCS 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 NCS 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 サービング インフラストラクチャ NCS の方が高くなります。この構成では、wIPS オーバーレイ構成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 アクセス ポイントを緩和操作で利用できるため、統合 wIPS 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 NCS インスタンスで不完全になります。wIPS などの一部のイベントが wIPS オーバーレイ NCS 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モニタするには、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。

表 1-1 にクライアント サービング構成とオーバーレイ構成の主な相違点のいくつかを示します。

表 1-1　wIPS クライアント サービングと wIPS モニタリング オーバーレイの比較

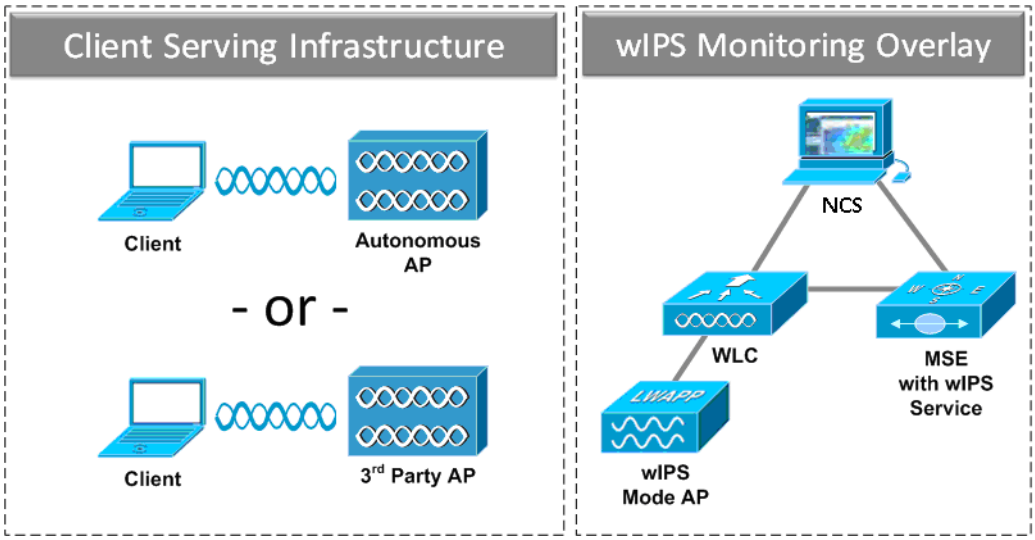
	クライアント サービング インフラストラクチャ NCS	wIPS モニタリング オーバーレイ NCS
wIPS アラーム	No	Yes
MFP アラーム	Yes	No
不正アラーム	Yes	Yes
不正位置	高精度	低精度
不正封じ込め	Yes	Yes、ただし拡張性あり

オーバーレイ ソリューションの課題の 1 つは、クライアント サービング インフラストラクチャまたは wIPS モニタリング オーバーレイ上の Lightweight アクセス ポイントが誤ったコントローラにアソシエートされる可能性です。誤ったコントローラとのアソシエーションは、各アクセス ポイント（ローカル モードと wIPS モニタ モード）で第 1、第 2、第 3 コントローラ名を指定することによって対処できます。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、アクセス コントロール リスト（ACL）を使用して 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推奨します。

自律ワイヤレス ネットワークまたはその他のワイヤレス ネットワークでの wIPS オーバーレイ

Adaptive wIPS ソリューションは、CUWN 以外の既存の 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。この構成の用途は、シスコの自律アクセス ポイントまたはサードパーティ アクセス ポイントのセキュリティ モニタリングです（図 1-5 を参照）。

図 1-5　自律での wIPS オーバーレイ



コントローラ IDS と Adaptive wIPS の違い

この項では、次のトピックを扱います。

ガイドラインと制限事項

フォレンジック

wIPS 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。これは主に、アクセス ポイントにかかる負荷が大きく、スケジュールされたチャネル スキャンへの割り込みが発生するためです。wIPS アクセス ポイントでは、チャネル スキャンを実行しながら、フォレンジック ファイルを生成することはできません。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 スキャンは遅延します。

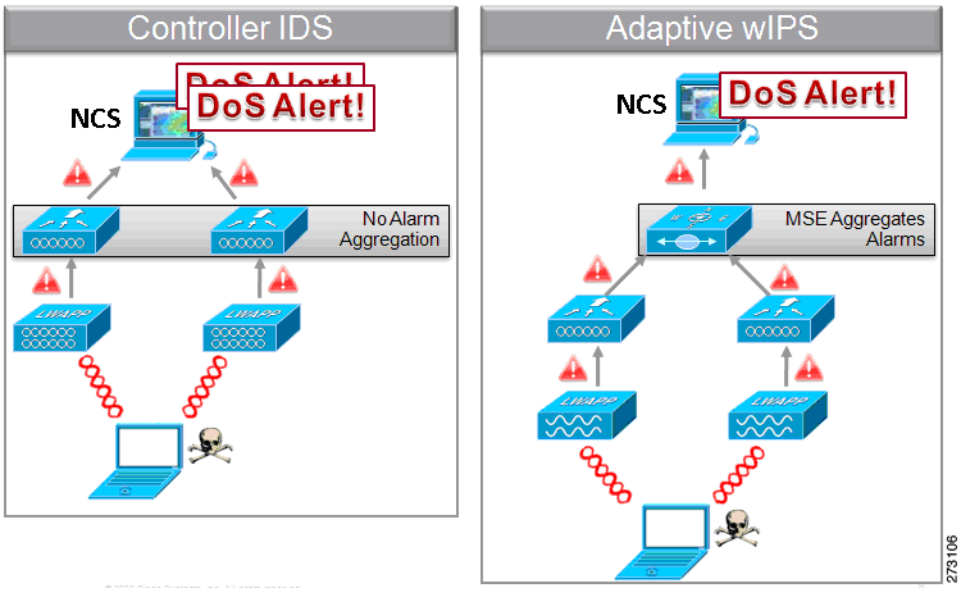
誤検出（False Positives）の削減

wIPS は、ワイヤレス ネットワークのセキュリティ モニタリングに関する誤検出を削減します。無線で多数の管理フレームを検出した場合に、アラームを生成する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、wIPS 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多数の管理フレームを無線で検出した場合にだけ、アラームを生成します。これは、wIPS 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 wIPS 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 wIPS 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、攻撃は NCS に 1 回だけ転送されます。既存のコントローラベースの IDS システムはアラームを集約しません（図 1-6 を参照）。

図 1-6　　シスコのコントローラベースの IDS と Adaptive wIPS を使用したアラームの集約



コントローラベースの IDS と wIPS 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。サブセクションの説明と表 1-2 および表 1-3 に示されているように、wIPS 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、サービス拒否（DoS）攻撃とセキュリティ突破攻撃の両方が含まれます。この項では、次のトピックを扱います。

- 「DoS 攻撃」（P.1-8）。
- 「セキュリティ突破攻撃」（P.1-8）
- 「ワイヤレス IPS アラーム フロー」（P.1-9）

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、多くの場合マイナスの影響はなくなります。表 1-2 に、コントローラベースの IDS と wIPS サービスで検出される Dos 攻撃の比較を示します。

表 1-2　コントローラ IDS と wIPS によって検出される DoS 攻撃

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		○
クイーンズランド工科大学により検出された脆弱性		○
RF 電波妨害攻撃		○
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	○	○
ディスアソシエーション ブロードキャスト攻撃		○
ディスアソシエーション フラッド攻撃	○	○
EAPOL-Logoff 攻撃	○	○
FATA-jack ツールの検出		○
不完全な EAP-failure 攻撃		○
不完全な EAP-success attack		○

セキュリティ突破攻撃

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突破は、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。セキュリティ突破攻撃には、インフラストラクチャに対するクエリや暗号キー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、セキュリティ突破攻撃は、ハニーポットなどの疑似アクセス ポイントにクライアントの誘導を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。表 1-3 に、コントローラベースの IDS と wIPS サービスで検出されるセキュリティ突破攻撃の比較を示します。

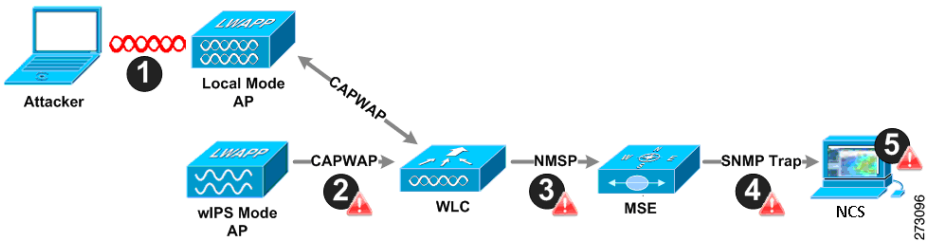
表 1-3　コントローラ IDS と wIPS によって検出されるセキュリティ突破攻撃

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		○
アクセス ポイントのデバイス 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		○
疑似アクセス ポイントの検出	○	○
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		○
中間者攻撃の検出		○
NetStumbler の検出	○	○
PSPF 違反		○
ASLEAP 攻撃の検出		○
ハニーポット アクセス ポイントの検出	○	○
ソフト アクセス ポイントまたはホスト アクセス ポイントの検出		○
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	○	○

ワイヤレス IPS アラーム フロー

Adaptive wIPS システムは、通信のリニア チェーンに従って、エアウェーブの初期スキャンから取得した攻撃情報を伝播して、情報を NCS に転送します（図 1-7 を参照）。

図 1-7　ネットワーク内のアラーム フロー



1. wIPS システムでアラームを生成させるには、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、CUWN 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アソシエートさ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. wIPS モニタ モード アクセス ポイントによって攻撃が識別されると、アラームの更新が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. 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 wIPS 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 Network Mobility Service Protocol（NMSP）です。
4. モビリティ サービス エンジン上の wIPS サービスが受信したアラームの更新は、アーカイブと攻撃の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 NCS に転送されます。SNMP トラップには攻撃情報が含まれています。同じ攻撃を参照する複数のアラーム更新を受信した場合（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）、1 つの SNMP トラップだけが NCS に送信されます。
5. アラーム情報を含む SNMP トラップは NCS によって受信され、表示されます。

フォレンジック

Cisco Adaptive wIPS 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提供します。基本レベルでは、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、取得する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、wIPS プロファイル内で、攻撃単位で有効になります。wIPS プロファイルは NCS 上に設定されます。

この機能を有効にすると、エアウェーブで特定の攻撃アラームが確認されると、フォレンジック機能がトリガーされます。元のアラームを生成した wIPS モニタ モード アクセス ポイント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 によってコントローラに転送されます。次に、この CAPWAP によって、NMSP 経由でフォレンジック ファイルが、モビリティ サービス エンジンで実行されている wIPS 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、モビリティ サービス エンジンのフォレンジック アーカイブに保存されます。デフォルトでは、この制限は 20 GB 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 ファイルには、フォレンジック ファイルへのハイパーリンクを含むアラームを NCS で開くことでアクセスできます。このファイルは、a.CAP ファイル形式で保存されており、WildPacket Omnipeek、AirMagnet WiFi Analyzer、Wireshark、またはこの形式をサポートしているその他のパケット キャプチャ プログラムを使用してアクセスできます。Wireshark は、http://www.wireshark.org から入手できます。

（注）　wIPS 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。これは主に、アクセス ポイントにかかる負荷が大きく、スケジュールされたチャネル スキャンへの割り込みが発生するためです。wIPS アクセス ポイントでは、チャネル スキャンを実行しながら、フォレンジック ファイルを生成することはできません。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 スキャンは遅延します。

不正検出

wIPS 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 CUWN 実装と同じロジックを使用して、不正の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、封じ込めることができます。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 NCS 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、攻撃封じ込めが起動された場合、封じ込めの間、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。

異常検出

wIPS 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が含まれます。異常検出システムでは、モビリティ サービス エンジン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、モビリティ サービス エンジンに保存されている履歴データと比較して、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 スプーフィング イベントを定期的にキャプチャしており、別の日に MAC スプーフィング イベントが 200 % 増加した場合、そのモビリティ サービス エンジン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 NCS 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が管理者に通知されます。さらに、異常検出アラームは、wIPS 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、wIPS には、特定の産業や導入のセキュリティ 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。テンプレートには、さまざまなリスク プロファイルおよび導入ごとに異なるセキュリティ モニタリングの要件が要約されています。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合わせてさらにカスタマイズできます。

リリース 7.0 機能への統合

wIPS は、以前のリリースで導入されたセキュリティ機能を利用するために、既存の CUWN 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、それぞれのカテゴリの下に wIPS イベントが表示されます。

設定と管理

NCS を使用して、モビリティ サービス エンジンの追加と削除、モビリティ サービス エンジン プロパティの設定、ユーザとグループの管理をはじめとした、さまざまな設定タスクと管理タスクを実行できます。

この項では、次のトピックを扱います。

モビリティ サービス エンジンの追加と削除

NCS を使用して、ネットワーク内のモビリティ サービス エンジンの追加と削除ができます。モビリティ サービス エンジンでサポートされているサービスを定義することもできます。設定の詳細については第 2 章「モビリティ サービス エンジンとライセンスの追加および削除」を参照してください。

モビリティ サービス エンジンの同期

NCS を使用して、Cisco Wireless LAN Controllers と NCS をモビリティ サービス エンジンと同期できます。詳細については、第 3 章「モビリティ サービス エンジンの同期」を参照してください。

ハイ アベイラビリティの設定

NCS を使用して、MSE にハイ アベイラビリティを設定できます。モビリティ サービス エンジンは、複数のモビリティ アプリケーションをホストするプラットフォームです。アクティブな各 MSE は別の非アクティブ インスタンスによりバックアップされます。アクティブな MSE はプライマリ MSE、非アクティブな MSE はセカンダリ MSE と呼ばれます。詳細については、第 4 章「ハイ アベイラビリティの設定」を参照してください。

仮想アプライアンスの設定

MSE は、さまざまなパフォーマンス特性を持つ物理アプライアンスにプリインストールされます。MSE は、物理アプライアンスと仮想アプライアンスの 2 つのモードで提供されます。詳細については、第 5 章「MSE 配信モード」を参照してください。

モビリティ サービス エンジンのプロパティの編集

NCS を使用して、モビリティ サービス エンジンの次のパラメータを設定できます。設定の詳細については第 6 章「システム プロパティの設定および表示」を参照してください。

- [General Properties]：連絡先名、ユーザ名、パスワード、およびモビリティ サービス エンジンの HTTP を割り当てることができます。
- [Active Sessions]：モビリティ サービス エンジン上のアクティブなユーザ セッションを確認できます。
- [Trap Destinations]：モビリティ サービス エンジンにより生成される SNMP トラップを受信する NCS または Cisco Security Monitoring, Analysis, and Response System（CS-MARS）ネットワーク管理プラットフォームを指定できます。
- [Advanced Parameters]：イベントを保存する日数、ハードウェアのリブート、ハードウェアのシャットダウン、またはデータベースのクリアの設定ができます。

ユーザとグループの管理

NCS を使用して、ユーザ、グループ、およびモビリティ サービス エンジンへのホスト アクセスを管理できます。設定の詳細については第 7 章「ユーザとグループの管理」を参照してください。

wIPS の設定およびプロファイル管理

NCS を使用して、Cisco Adaptive wIPS サービスを設定できます。詳細については、「wIPS プロファイルの設定」（P.8-4）を参照してください。

モニタリング機能

NCS を使用して、モビリティ サービス エンジンによって生成されるアラーム、イベント、およびログをモニタできます。モビリティ サービス エンジンのステータス、クライアント、干渉、タグ付きアセットもモニタできます。また、モビリティ サービス エンジンの使用率レポートを生成して、CPU とメモリの使用率を判断し、クライアント、タグ、および不正アクセス ポイントと不正クライアントをカウントすることができます。詳細については、第 9 章「システムとサービスのモニタリング」を参照してください。

MSAP 要件のプロビジョニング

Cisco Mobility Services Advertisement Protocol（MSAP）では、MSAP クライアントおよびサーバの要件を規定し、それらの間でのメッセージ交換を記述します。モバイルデバイスは、MSAP を使用して MSAP サーバから Wi-Fi インフラストラクチャを介してサービス アドバタイズメントを取得できます。このリリースのモビリティ サービス エンジン（MSE）では、MSAP が導入され、サーバ機能が提供されています。詳細については、第 10 章「MSAP」を参照してください。

メンテナンス操作

NCS に事前に定義した FTP フォルダにモビリティ サービス エンジンのデータを定義した間隔でバックアップし、その NCS からモビリティ サービス エンジンのデータを復元することができます。その他の実行できるモビリティ サービス エンジンのメンテナンス操作には、NCS ステーションからアソシエートされているすべてのモビリティ サービス エンジンへの新規ソフトウェア イメージのダウンロード、モビリティ サービス エンジンの設定のクリアなどがあります。詳細については、第 11 章「メンテナンス操作の実行」を参照してください。

（注）　NCS の代わりに、コマンドライン インターフェイスを使用して、モビリティ サービス エンジンの GRUB とルート パスワードを復元する方法の詳細については、第 11 章「メンテナンス操作の実行」も参照してください。

MSE システムとアプライアンスの強化

システムとアプライアンスを強化するには、正常に機能させるために一部のサービスとプロセスを公開する必要があります。MSE の強化には、不要なサービスの無効化、最新のサーバ バージョンへのアップグレード、ファイル、サービス、エンド ポイントへの適切な制限付き権限の適用が含まれます。

システム互換性

現在使用しているリリースに対する最新システム（コントローラ、NCS、モビリティ サービス エンジン）の互換性情報、機能のサポート、および操作上の注意については、次の URL で入手可能な『Cisco 3300 Mobility Services Engine Release Note』を参照してください。
http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html