Adaptive wIPS ELM設定および導入ガイド

内容

はじめに

Cisco Adaptive Wireless Intrusion Prevention System（wIPS）ソリューションは、Enhanced Local Mode（ELM）機能を追加します。これにより、管理者は、導入されたアクセス ポイント（AP）を使用して、個別のオーバーレイ ネットワークを必要することなく包括的に保護します（図 1）。ELM の前および従来の Adaptive wIPS 導入において、専用モニタ モード（MM）AP は、PCI 準拠ニーズ、または不正セキュリティ アクセス、ペネトレーションおよび攻撃を提供する必要があります（図 2）。ELM は、CapEx および OpEx コストを削減し、ワイヤレス セキュリティ実装を簡素化する同等のサービスを効果的に提供します。このドキュメントでは、ELM のみについて説明し、MM AP による既存の wIPS 展開の利点は修正しません。

図 1：拡張ローカル モード AP 導入

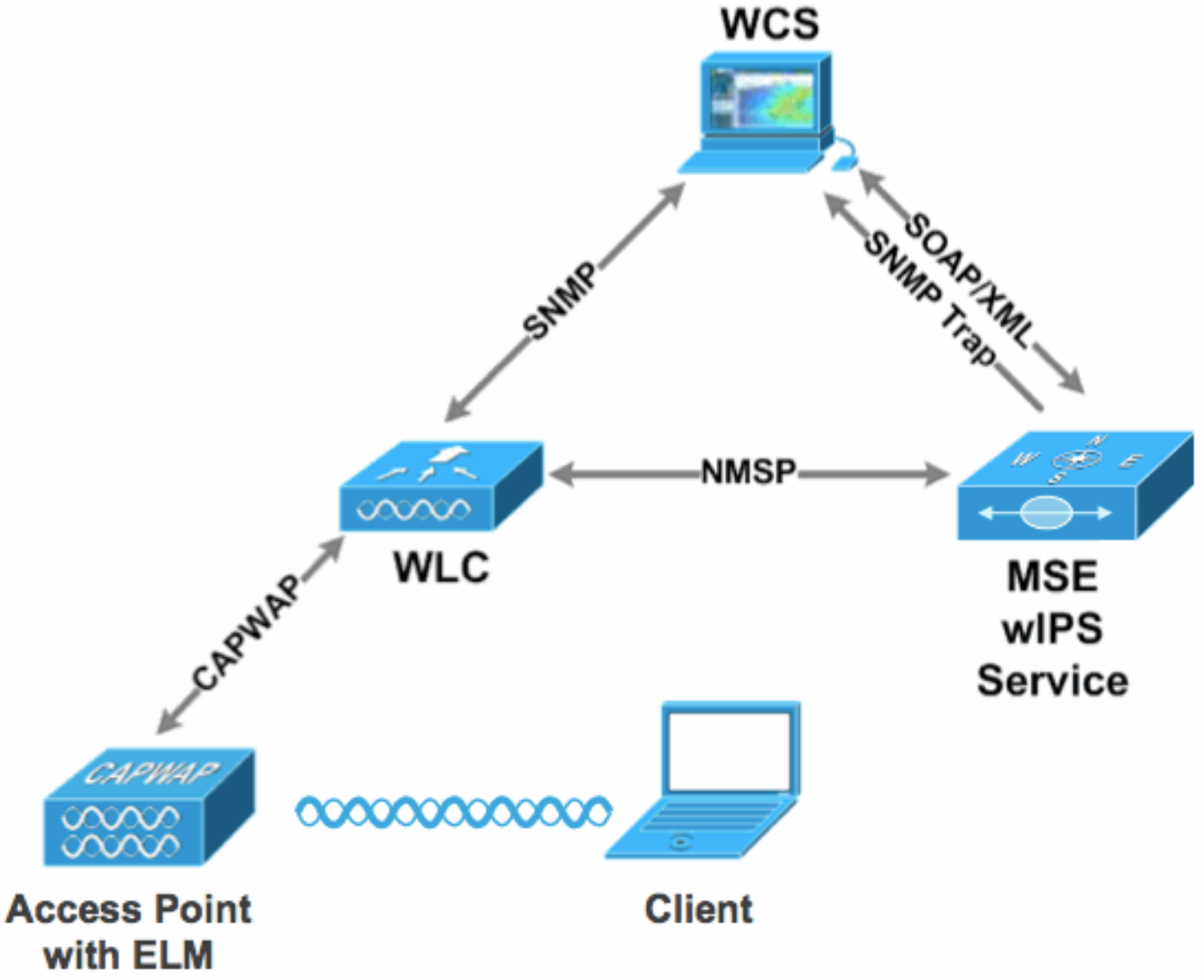
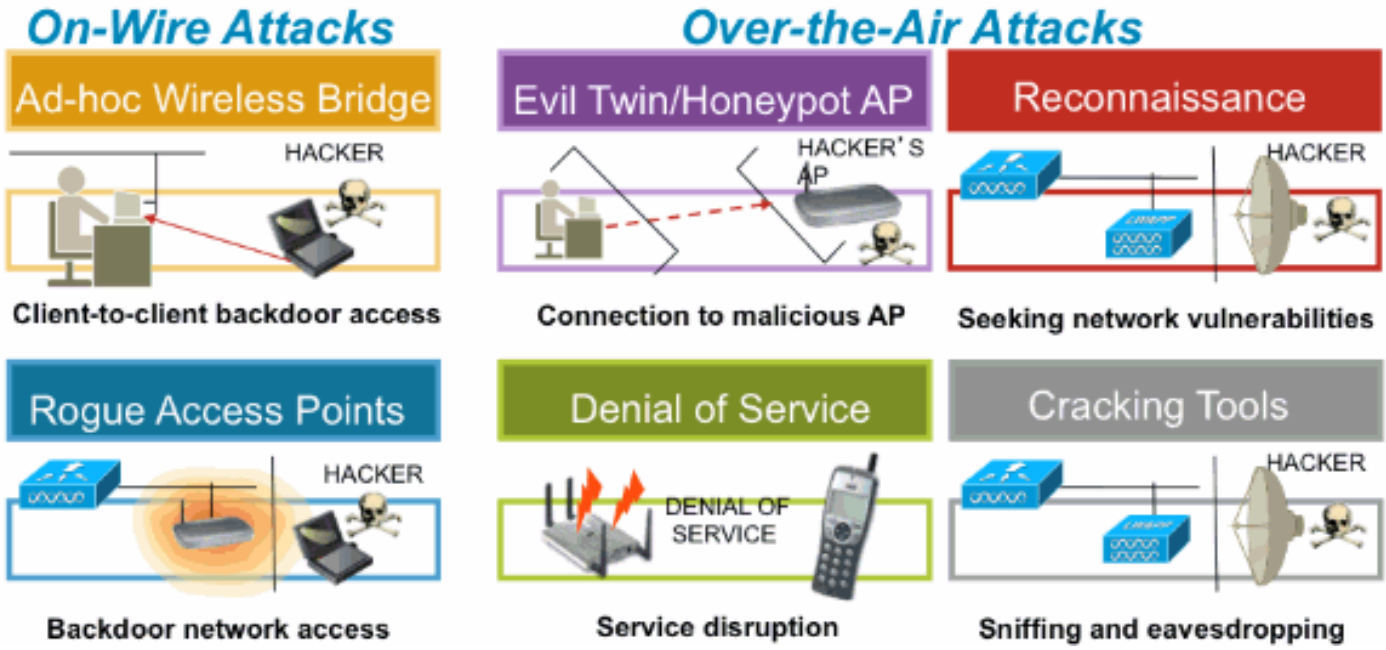


図 2：上位のワイヤレス セキュリティ脅威



前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

ELM の必須コンポーネントおよび最小コード バージョン

- Wireless LAN Controller（WLC）：バージョン 7.0.116.xx 以降
- AP：バージョン 7.0.116.xx 以降
- Wireless Control System（WCS）：バージョン 7.0.172.xx 以降
- モビリティ サービス エンジン：バージョン 7.0.201.xx 以降

WLC プラットフォームのサポート

ELM は、WLC5508、WLC4400、WLC 2106、WLC2504、WiSM-1 および WiSM-2WLC プラットフォームでサポートされます。

AP のサポート

ELM は、3500、1250、1260、1040 および 1140 などの 11n AP でサポートされます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

表記法の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

ELM wIPS アラーム フロー

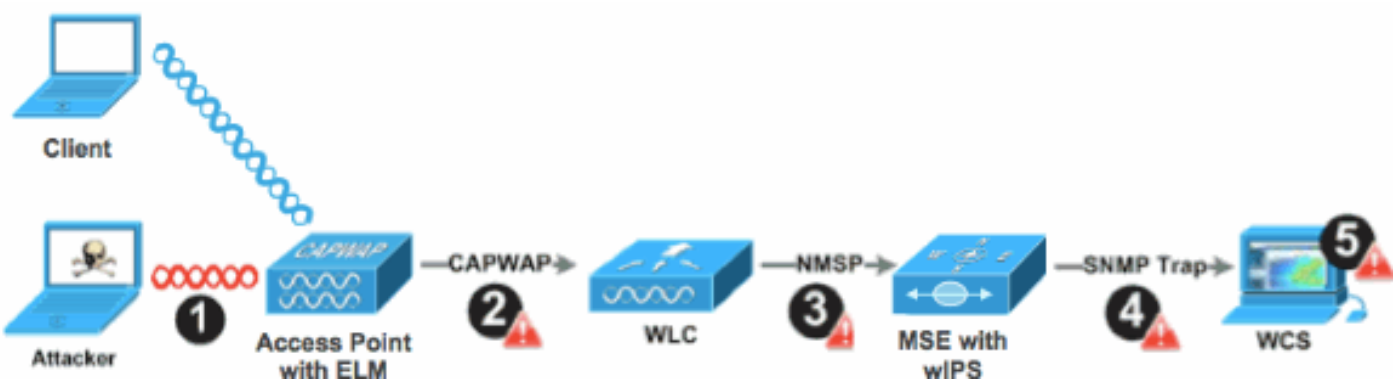
攻撃は、信頼できるインフラストラクチャ AP で発生した場合だけ意味があります。ELM AP は、コントローラを検出および通信して、WCS 管理での報告のために MSE とアソシエーションします。図 3 は、管理者側から見たアラーム フローを提供します。

1. 攻撃が、インフラストラクチャ デバイス（「信頼できる」AP）で発生する
2. CAPWAP から WLC で通信する ELM AP で検出される
3. NMSP を介して MSE に透過的に渡される

4. SNMP トラップを介して WCS に送信される MSE の wIPS データベースにログインする

5. WCS に表示される

図 3：脅威検出およびアラーム フロー



ELM の導入に関する考慮事項

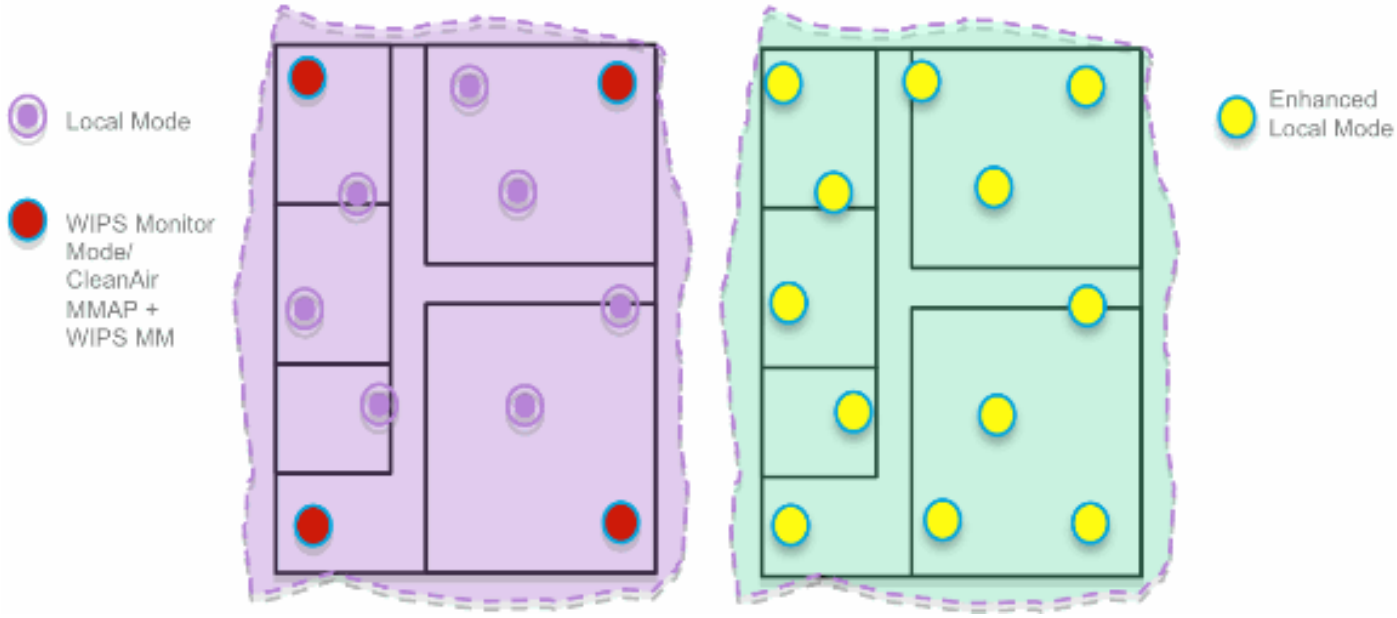
ネットワークのすべての AP で ELM を有効にすることを推奨します。これにより、ネットワーク オーバーレイまたはコスト、あるいはこれらの両方を考慮しながら、ほとんどのカスタマー セキュリティ ニーズを満たすことができます。ELM の主機能は、データ、音声およびビデオ クライアント、サービスのパフォーマンスに影響を及ぼすことなく、On-Channel 攻撃で効果的に機能します。

ELM と専用 MM の比較

図 4 は、wIPS MM AP および ELM の標準導入間の通常の接触を提供します。この例では、両方のモードの一般的なカバレッジ範囲は次のような前提です。

- 専用 wIPS MM AP の一般的なカバレッジ範囲：15,000 ~ 35,000 平方フィート
- クライアント サービス AP の一般的なカバレッジ範囲：3,000 ~ 5,000 平方フィート

図 4：MM とすべての ELM AP のオーバーレイ



従来の Adaptive wIPS 導入の場合、すべての 5 ローカル モード AP に対して 1 MM AP という比率を推奨します。これは、最適なカバレッジ範囲を実現するネットワーク設計や専門知識により異なる場合があります。ELM を考慮することで、管理者は、既存のすべての AP で ELM ソフトウェア機能を有効にするだけで、パフォーマンスを維持しつつ、MM wIPS 操作をローカル データ サービス モード AP に効果的に追加できます。

On-Channel および Off-Channel のパフォーマンス

MM AP は、無線の 100 % の時間を活用して、チャネルをすべてスキャニングします。WLAN クライアントにはサービスを提供しません。ELM の主機能は、データ、音声およびビデオ クライアント、サービスのパフォーマンスに影響を与えることなく、On-Channel 攻撃で効果的に機能します。主な違いは、ローカルモードでオフチャネルスキャンが異なる点です。アクティビティに応じて、オフチャネルスキャンでは、攻撃の分類と判別に使用できる十分な情報を収集するための最小限の滞留時間が提供されます。たとえば、アソシエートされる音声クライアントは、サービスに影響を与えないように、アソシエーションを解除するまで、AP の RRM スキャニングが遅れます。この場合、Off-Channel の ELM 検出が最適と見なされます。すべて、カントリーまたは DCA チャネルで機能する隣接 ELM AP は、効果的であるため、すべてのローカル モード AP で ELM を有効にして、保護カバレッジを最大にすることを推奨します。すべてのチャネルでのフルタイムの専用スキャニングが必要な場合、MM AP を導入することを推奨します。

次に、ローカル モードと MM AP の違いについて説明します。

- ローカル モード AP：WLAN クライアントにタイム スライシング Off-Channel スキャニングを提供し、各チャネルで 50 ms 間リスニングして、すべて/カントリー/DCA チャネルの設定可能なスキャニングを実行します。
- モニタ モード AP：WLAN クライアントにサービスを提供せず、スキャニングだけを行い、各チャネルで 1.2s 間リスニングして、すべてのチャネルをスキャンします。

WAN リンク全体での ELM

シスコは、低帯域幅 WAN リンクでの ELM AP の導入など、困難な状況で機能を最適化するために努力を重ねています。ELM 機能は、AP での攻撃シグニチャの判別における事前処理を行い、低速リンクで機能するように最適化されています。ベスト プラクティスとして、WAN 経由の ELM のパフォーマンスを検証する基準をテストおよび測定することを推奨します。

CleanAir 統合

ELM 機能は、CleanAir 操作を効率的に補助し、同様のパフォーマンスを実現して、次の既存の CleanAir スペクトラム対応のメリットを MM AP の導入に提供します。

- 専用シリコン レベル RF インテリジェンス
- スペクトラム対応、セルフ ヒーリングおよび自己最適化
- 非標準のチャネル脅威および干渉の検出および緩和
- Bluetooth、マイクロ波、コードレス電話などの非 Wi-Fi 検出
- RF ジャマーなどの RF 層 DOS 攻撃の検出および特定

ELM の機能と利点

- ローカルおよび H-REAP AP のデータ Adaptive wIPS スキャニング
- 個々のオーバーレイ ネットワークを必要としない保護
- 既存の wIPS カスタマーが無料 SW ダウンロードとして利用可能
- ワイヤレス LAN の PCI 準拠のサポート
- フル 802.11 および非 802.11 攻撃の検出
- 科学捜査およびレポーティング機能の追加
- 既存の CUWM および WLAN 管理との統合
- 統合または専用 MM AP の柔軟な設定
- AP での事前処理によるデータ バックホールの最小化（つまり、非常に低い帯域幅のリンクでも機能します）
- データ提供への影響の縮小

ELM ライセンス

ELM wIPS は、新しいライセンスをサービスに提供します。

- AIR-LM-WIPS-xx：Cisco ELM wIPS ライセンス

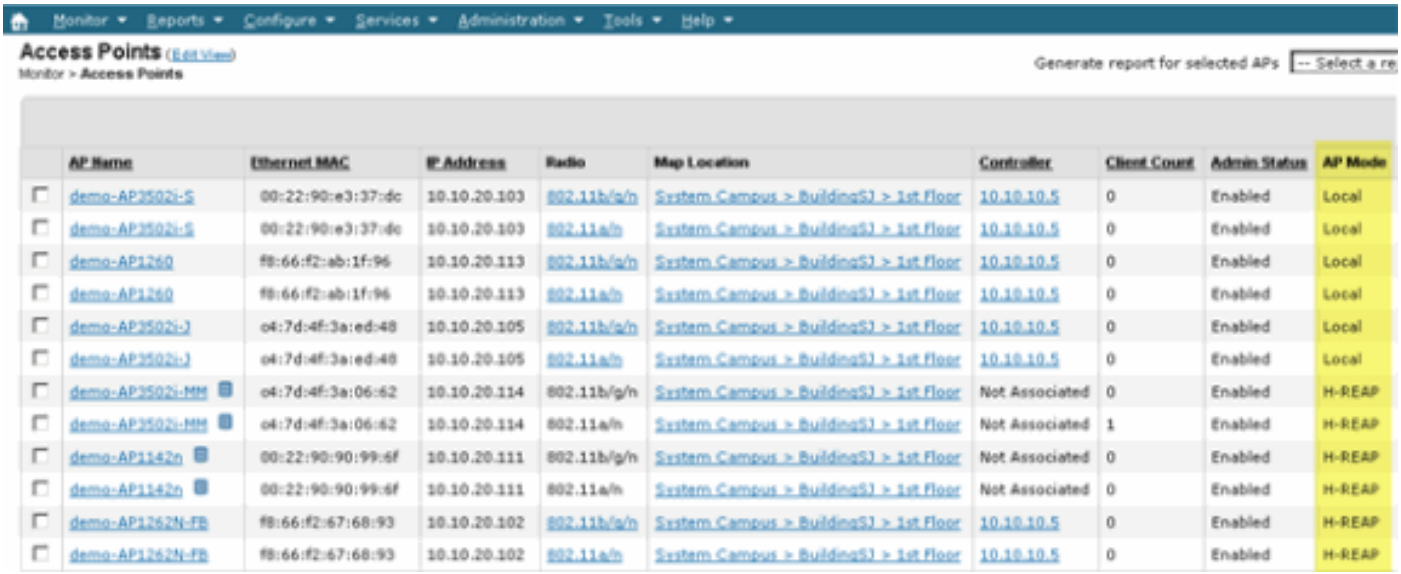
- AIR-WIPS-AP-xx：Cisco Wireless wIPS ライセンス

ELM ライセンスに関する追加の注意事項：

- wIPS MM AP ライセンス SKU がすでにインストールされている場合、これらのライセンスは ELM AP でも使用できます。
- wIPSライセンスとELMライセンスはともに、wIPSエンジンのプラットフォームライセンス制限にカウントされます。2000台のAPは3310で、3000台のAPは335xでサポートされます。
- 評価ライセンスには、wIPS で 10 AP、ELM で 10 が含まれ、期間は 60 日間です。ELM よりも前の評価ライセンスでは、20 wIPS MM AP が許可されていました。ELM をサポートするソフトウェア バージョンの最小要件を満たす必要があります。

WCS での ELM の設定

図 5：WCS を使用した ELM の設定

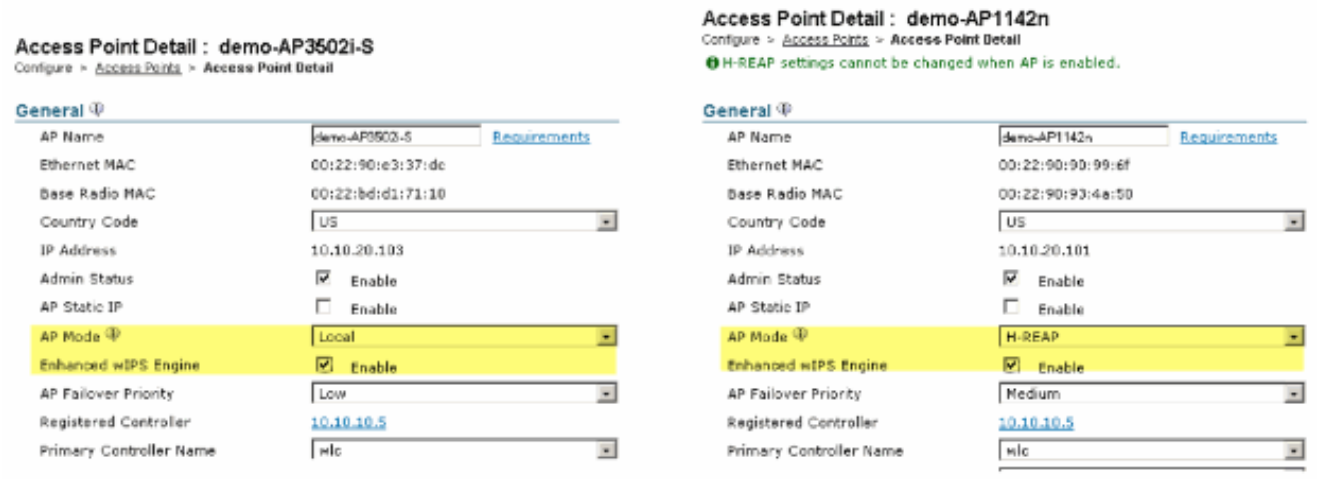


1. WCS から、「拡張 wIPS エンジン」を有効にする前に、AP の 802.11b/g および 802.11a の両方の無線を無効にします。

   注：関連付けられたすべてのクライアントが切断され、無線が有効になるまで参加しません。

2. 1 つの AP を設定するか、複数の Lightweight AP で WCS 設定テンプレートを使用します。図 6 を参照してください。

   図 6：拡張 wIPS エンジン（ELM）サブモードの有効化



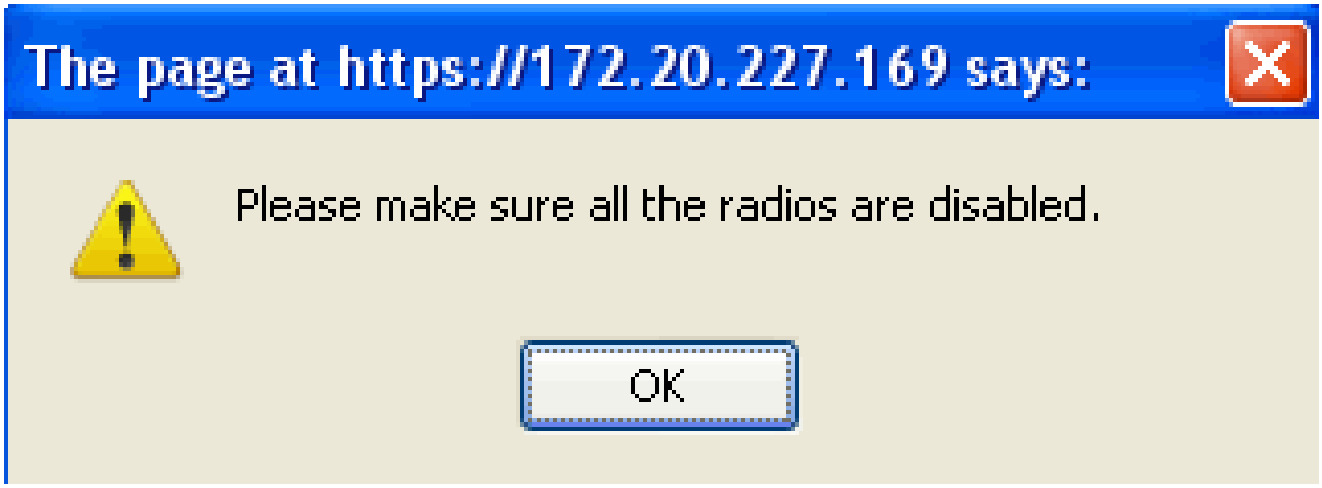
3. [Enhanced wIPS Engine] を選択して、[Save] をクリックします。

   a. 拡張 wIPS エンジンを有効にすると、AP はリブートされません。

   b. H-REAPがサポートされます。ローカルモードAPと同じ方法で有効にします。

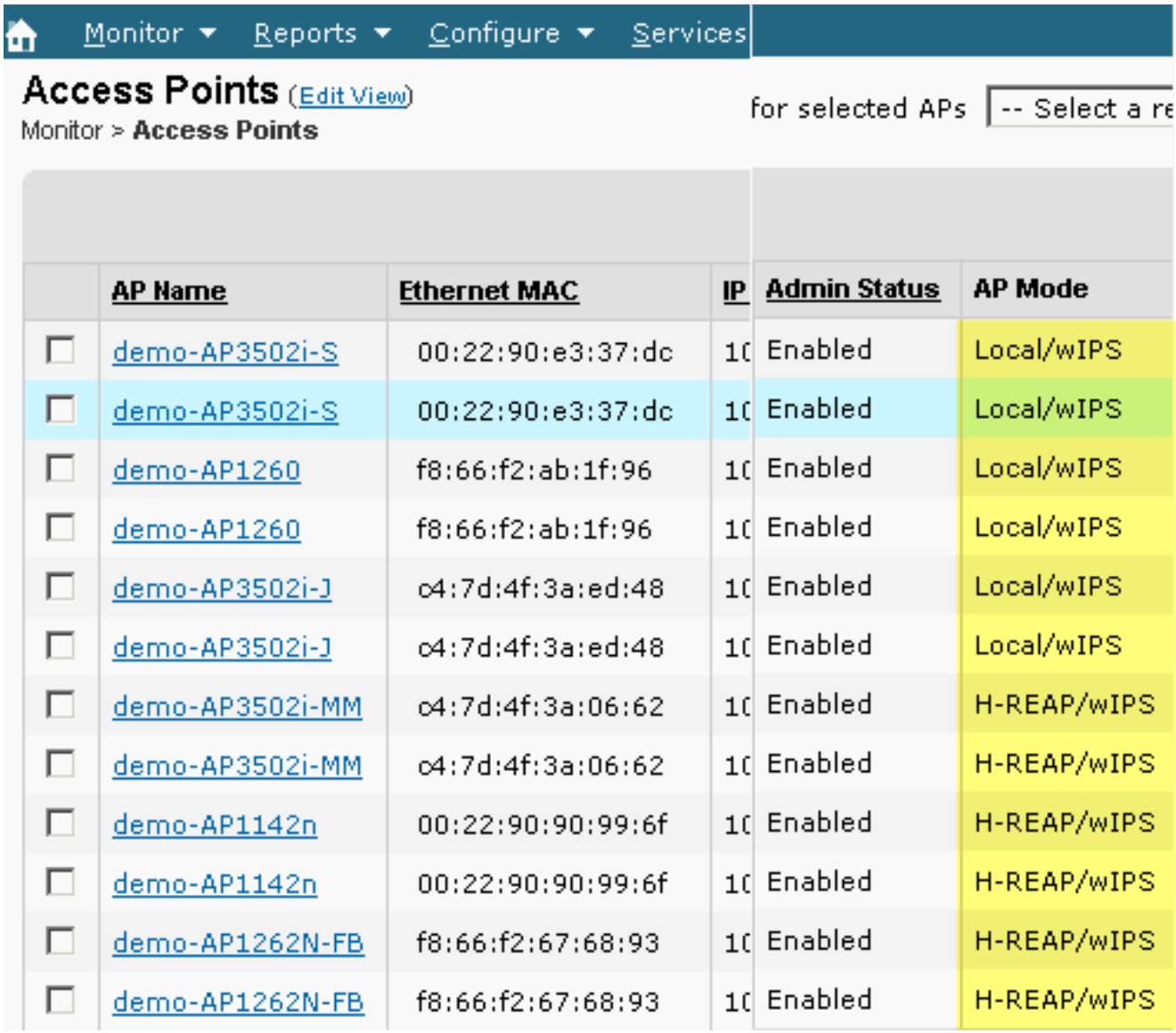
   注：このAPのいずれかの無線が有効な場合、WCSは設定を無視して、図7のようなエラーをスローします。

   図 7：ELM を有効にする前に AP 無線を無効にすることを通知する WCS リマインダ



4. 設定の成功は、AP モードが [Local] または [H-REAP] から [Local/wIPS] または [H-REAP/wIPS] に変わったことで確認できます。図 8 を参照してください。

   図 8：WCS による wIPS にローカルまたは H-REAP、あるいはこれらの両方を追加する AP モードの表示

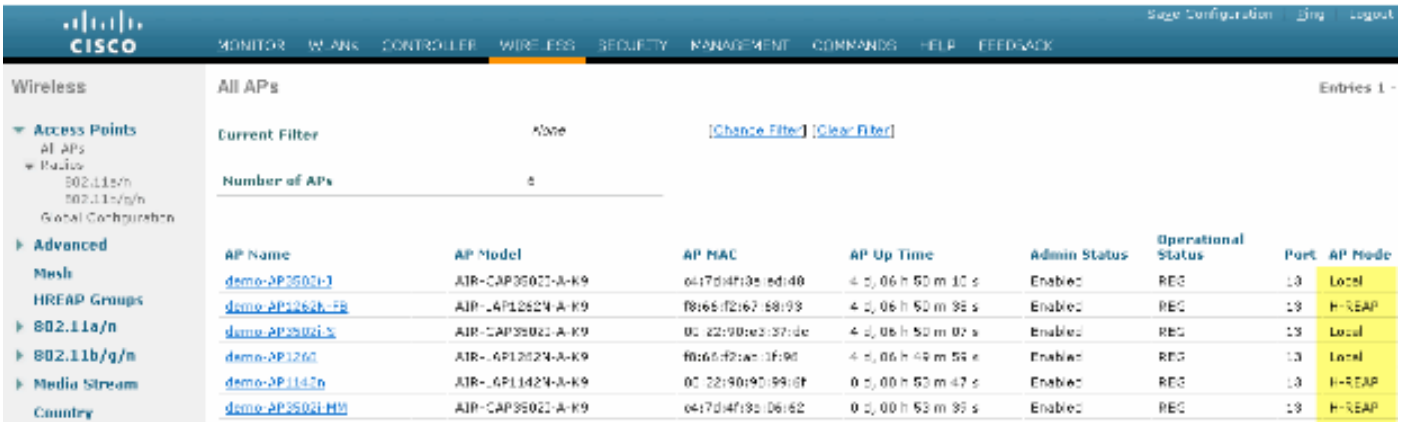


5. 手順 1 で無効にされた無線を有効にします。
6. wIPS プロファイルを作成し、コントローラにプッシュして、設定を完了します。

   注：wIPSの設定の詳細については、『Cisco Adaptive wIPS Deployment Guide』を参照してください。

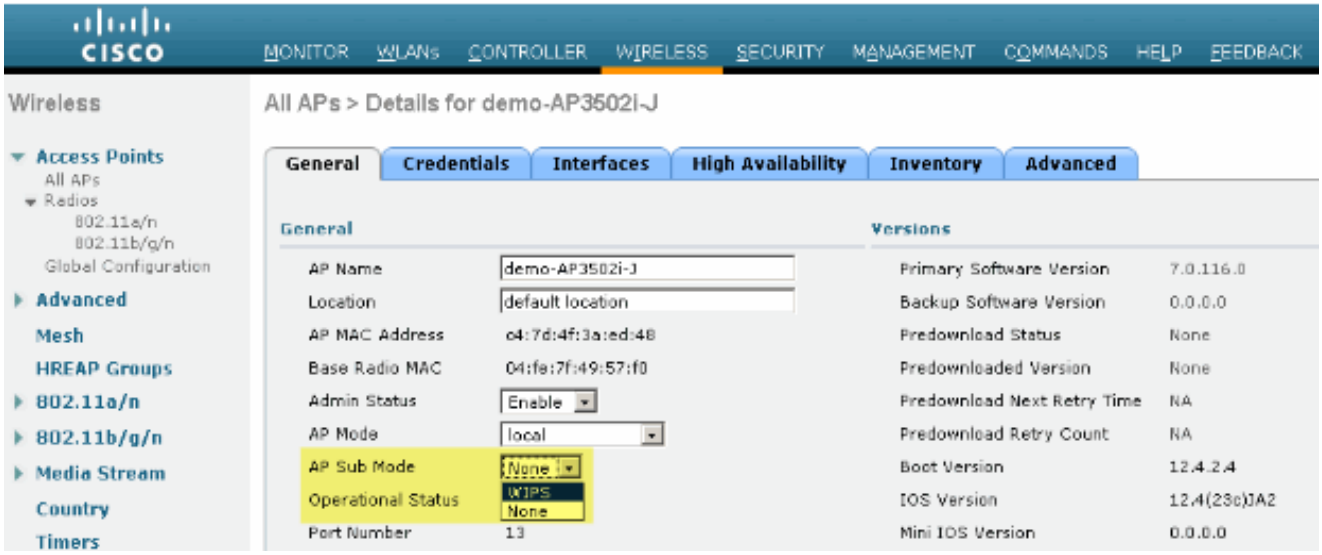
WLC からの設定

図 9：WLC での ELM の設定



1. [Wireless] タブから AP を選択します。

   図 10：wIPS ELM を追加するための WLC による AP サブモードの変更



2. [AP Sub Mode] ドロップダウン メニューから、[wIPS] を選択します（ 図 10 ）。

3. [Apply] をクリックし、設定を保存します。

注：ELM機能が動作するには、wIPSライセンスでMSEとWCSが必要です。AP サブモードを WLC から変更するだけでは ELM は有効になりません。

ELM で検出される攻撃

表 1：wIPS シグニチャ サポート一覧

検出される攻撃	ELM	MM
AP に対する DoS 攻撃		
アソシエーション フラッド	Y	Y
アソシエーション テーブル オーバーフロー	Y	Y
認証フラッド	Y	Y
EAPOL-Start 攻撃	Y	Y

PS-Poll フラッド	Y	Y
プローブ要求フラッド	N	Y
認証されないアソシエーション	Y	Y
インフラストラクチャに対する DoS 攻撃		
CTS フラッド	N	Y
クイーンズランド工科大学により検出された脆弱性	N	Y
RF 電波妨害	Y	Y
RTS フラッド	N	Y
仮想キャリア攻撃	N	Y
ステーションに対する DoS 攻撃		
認証失敗攻撃	Y	Y
ブロック ACK フラッド	N	Y
De-Auth ブロードキャスト フラッド	Y	Y
De-Auth フラッド	Y	Y
Dis-Assoc ブロードキャスト フラッド	Y	Y
Dis-Assoc フラッド	Y	Y
EAPOL-Logoff 攻撃	Y	Y
FATA-Jack ツール	Y	Y
不完全な EAP-Failure	Y	Y
不完全な EAP-Success	Y	Y
セキュリティ ペネトレーション攻撃		
ASLEAP ツール検出	Y	Y
Airsnarf 攻撃	N	Y
ChopChop 攻撃	Y	Y
WLAN のセキュリティ異常による Day-Zero 攻撃	N	Y
デバイスのセキュリティ異常による Day-Zero 攻撃	N	Y
AP のデバイス プローブ	Y	Y
EAP メソッドへの辞書攻撃	Y	Y
802.1x 認証に対する EAP 攻撃	Y	Y
偽の AP の検出	Y	Y
偽の DHCP サーバの検出	N	Y

高速 WEP クラック ツールの検出	Y	Y
フラグメンテーション攻撃	Y	Y
ハニーポット AP の検出	Y	Y
Hotspotter ツールの検出	N	Y
不正なブロードキャスト フレーム	N	Y
不正 802.11 パケットの検出	Y	Y
中間者攻撃	Y	Y
NetStumbler の検出	Y	Y
NetStumbler 犠牲者の検出	Y	Y
PSPF 違反の検出	Y	Y
ソフト AP またはホスト AP の検出	Y	Y
スプーフィングされた MAC アドレスの検出	Y	Y
疑わしい営業時間外のトラフィックの検出	Y	Y
ベンダー リストによる未承認アソシエーション	N	Y
未承認アソシエーションの検出	Y	Y
Wellenreiter の検出	Y	Y

注：CleanAirを追加すると、非802.11攻撃の検出も可能になります。

図 11：WCS wIPS プロファイル ビュー

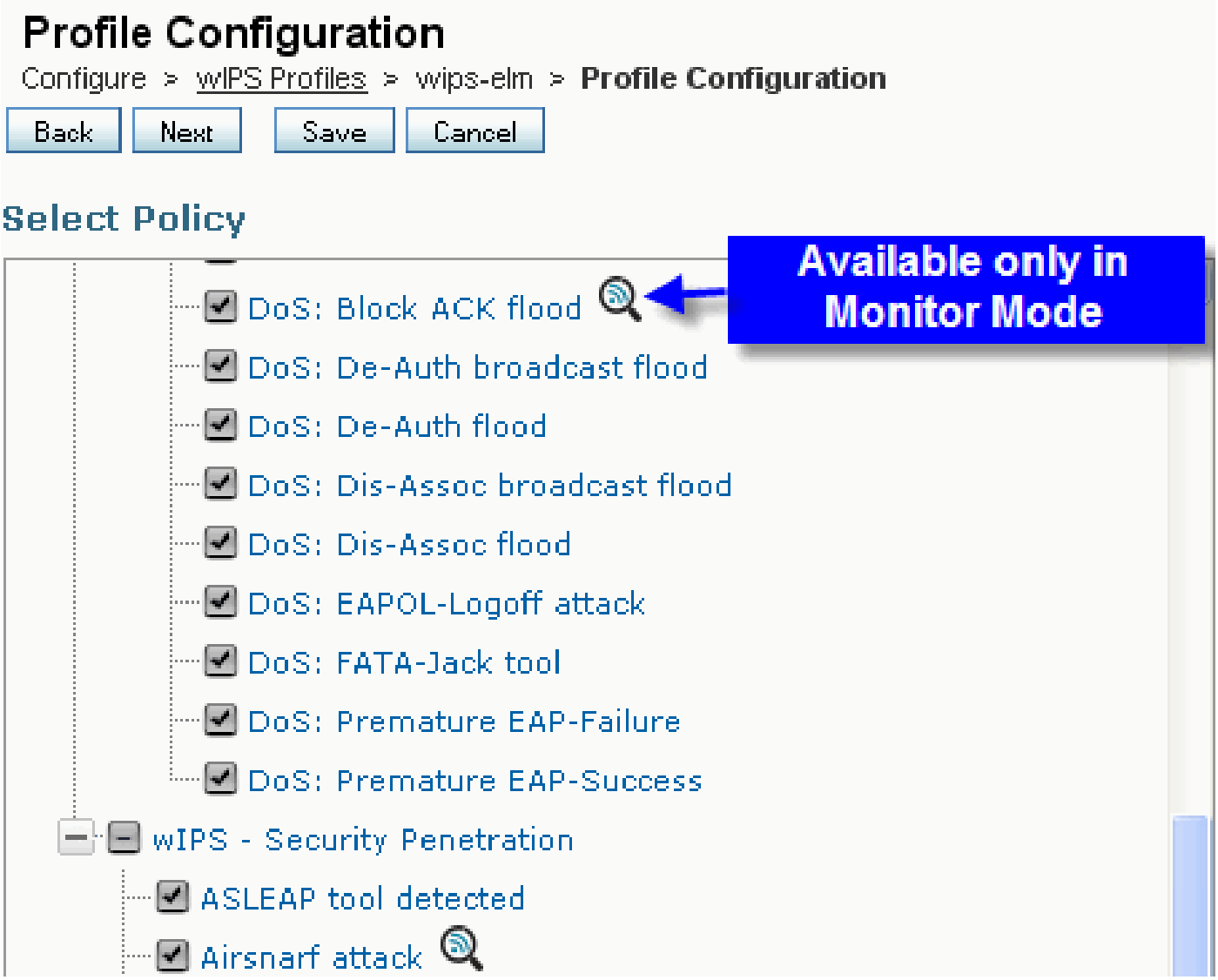
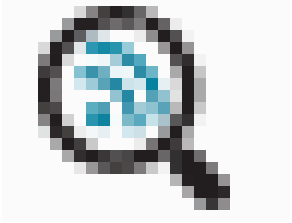


図 11 では、wIPS プロファイルを WCS から設定します。 アイコンは、AP が MM の場合だけ攻撃が検出され、ELM の場合はベスト エフォートだけであることを示します。



ELM のトラブルシューティング

次のことを確認してください。

- NTP が設定されていることを確認します。
- MSE 時間が UTC で設定されていることを確認します。
- デバイス グループが機能していない場合、[Any] でオーバーレイ プロファイル SSID を使用します。AP をリブートします。
- ライセンスが設定されていることを確認します (現在、ELM AP は KAM ライセンスを使用

しています）。

- wIPS プロファイルが頻繁に変更される場合、MSE コントローラを再び同期化します。プロファイルが WLC でアクティブになっていることを確認します。
- 次のように MSE CLI を使用して WLC が MSE の一部であることを確認します。

    1. SSH または telnet で MSE に接続します。
    2. /opt/mse/wips/bin/wips_cli を実行します。このコンソールは、適応 wIPS システムの状態に関する情報を収集するために、次のコマンドにアクセスするときに使用できます。
    3. show wlc all：wIPS コンソール内で実行します。このコマンドは、MSE で wIPS サービスとアクティブに通信するコントローラを確認するときに使用されます。図 12 を参照してください。

    図 12：MSE CLI による MSE wIPS サービスが WLC でアクティブかどうかの確認

```
<#root>

wIPS>

show wlc all


WLC MAC               Profile             Profile
Status                   IP
Onx Status Status
-----------------------------------------------
-----------------------------------------------
----
00:21:55:06:F2:80    WCS-Default         Policy
active on controller     172.20.226.197
Active
```

- MSE CLI を使用してアラームが MSE で検出されるか確認します。
    - show alarm list：wIPS コンソールないで実行します。このコマンドは、wIPS サービス データベース内に現在含まれているアラームをリストするときに使用されます。Key フィールドは、特定のアラームに割り当てられた一意なハッシュ キーです。Type フィールドは、アラームのタイプです。この図 13 は、アラーム ID および説明のリストを示しています。

    図 13：MSE CLI の show alarm list コマンド

```
<#root>

wIPS>

show alarm list
```

```
Key         Type  Src MAC
LastTime              Active          First Time
-----------------------------------------------
-----------------------------------------
89          89    00:00:00:00:00:00     2008/09/04
18:19:26  2008/09/07 02:16:58   1
65631       95    00:00:00:00:00:00     2008/09/04
17:18:31  2008/09/04 17:18:31   0
1989183     99    00:1A:1E:80:5C:40     2008/09/04
18:19:44  2008/09/04 18:19:44   0
```

First TimeフィールドとLast Timeフィールドは、アラームが検出されたタイムスタンプを示します。これらのタイムスタンプはUTC時間で保存されます。Active フィールドは、アラームが現在検出されているかどうかを示します。

- MSE データベースをクリアします。
  - MSE データベースが壊れている場合、または他のトラブルシューティング方法が機能しない場合、データベースをクリアして、やり直すことを推奨します。

    図 14：MSE サービス コマンド

```
1. /etc/init.d/msed stop
2. Remove the database using the command 'rm
/opt/mse/locserver/db/linux/server-eng.db'
3. /etc/init.d/msed start
```

関連情報

- Cisco Wireless LAN Controller コンフィギュレーション ガイド、リリース 7.0.116.0
- Cisco Wireless Control System コンフィギュレーション ガイド、リリース 7.0.172.0
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。