無線 LAN の監視

この章では、WCS を使って無線 LAN を監視する方法について説明します。この章の内容は、次のとおりです。

不正アクセス ポイントの監視

許可されていない不正アクセス ポイントは安価で簡単に利用できることから、従業員は、IT 部門に連絡して同意を得ることなく、それらのアクセス ポイントを既存の LAN やビルディング内のアドホック ネットワークに接続することがあります。これらの不正アクセス ポイントは、企業のファイアウォールの背後にあるネットワーク ポートに接続可能であるため、重大なネットワーク セキュリティ侵犯となることがあります。通常、従業員は不正アクセス ポイントのセキュリティ設定を有効にしないので、権限のないユーザがこのアクセス ポイントを使って、ネットワーク トラフィックを傍受し、クライアント セッションをハイジャックすることは簡単です。さらに警戒すべきことは、無線ユーザはセキュリティで保護されていないアクセス ポイントの場所を頻繁に公表するため、企業のセキュリティが侵害される危険性も増大します。

Cisco Wireless LAN Solution では、担当者がスキャナを持って不正アクセス ポイントを手作業で検出するのではなく、管理対象のアクセス ポイントに MAC アドレスと IP アドレスによって不正アクセス ポイントを検出させて、その情報を自動的に収集し、システム オペレータがその不正アクセス ポイントの特定、タグ付け、および阻止ができるようになります。また、4 つのアクセス ポイントの 1 つから、不正アクセス ポイントのクライアントに認証解除とアソシエート解除のメッセージを送信することで不正アクセス ポイントを防ぐこともできます。

不正アクセス ポイントのロケーション、タギング、および阻止

この組み込み型の検出、タギング、監視、および阻止の機能を使用すると、システム管理者は、次に挙げる適切な処理を実行できます。

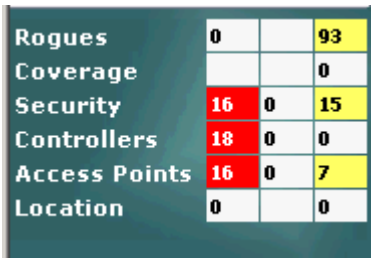
- 不正アクセス ポイントを特定します。
- 新しい不正アクセス ポイントの通知の受信します（通路をスキャンして歩く必要はなくなります）。
- 不明で不正アクセス ポイントが削除または認識されるまで監視します。
- 最も近い場所の認可済みアクセス ポイントを特定して、高速かつ効果的に誘導スキャンを行えるようにします。
- 1 つから 4 つのアクセス ポイントで、不正アクセス ポイントのクライアントに認証解除とアソシエーション解除のメッセージを送信して、不正アクセス ポイントを阻止します。この阻止は、MAC アドレスを使って個々の不正アクセス ポイントに対して行うことも、企業サブネットに接続されているすべての不正アクセス ポイントに対して要求することもできます。
- 不正アクセス ポイントにタグを付けます。
  - 不正アクセス ポイントが LAN の外部にあり、LAN または無線 LAN のセキュリティを脅かさない場合は承諾します。
  - 不正アクセス ポイントが LAN または無線 LAN のセキュリティを脅かさない場合は容認します。
  - 不正アクセス ポイントが削除または認識されるまで、不明なアクセス ポイントとしてタグ付けします。
  - 不正アクセス ポイントを阻止済みとしてタグ付けし、1 つから 4 つのアクセス ポイントで、すべての不正アクセス ポイント クライアントに認証解除およびアソシエーション解除のメッセージを転送することにより、クライアントが不正アクセス ポイントにアソシエートしないようにします。この機能は、同じ不正アクセス ポイント上のアクティブなチャネルに適用されます。

不正アクセス ポイントの検出と特定

無線 LAN 上のアクセス ポイントで、電源が入りコントローラにアソシエートされると、WCS ではすぐに不正アクセス ポイントのリスニングが開始します。コントローラによって、不正アクセス ポイントが検出されると、すぐに WCS に通知され、WCS によって、不正アクセス ポイントのアラームが作成されます。

WCS が不正アクセス ポイント メッセージをコントローラから受け取ると、すべての WCS ユーザ インターフェイス ページの左下に Alarm Monitor が表示されます。図 6-1 の Alarm Monitor は、93 個の不正アクセス ポイント アラームを示しています。

図 6-1　不正アクセス ポイント用の Alarm Monitor



不正アクセス ポイントを検出し特定する手順は、次のとおりです。

ステップ 1　**Rogues** インジケータをクリックして、Rogue AP Alarms ページを表示します。このページには、アラームの重大度、不正アクセス ポイントの MAC アドレス、不正アクセス ポイントのタイプ、不正アクセス ポイントが最初に検出された日時、および SSID が表示されます。

ステップ 2　**Rogue MAC Address** リンクをクリックして、それに関連付けられた Alarms > Rogue - *AP MAC Address* ページを表示します。このページには、不正アクセス ポイントのアラームに関する詳細情報が表示されます。

ステップ 3　アラームを変更するには、Select a Command ドロップダウン メニューから次のコマンドのいずれかを選択し、**GO** をクリックします。

- **Assign to me**：選択されたアラームを現在のユーザに割り当てます。
- **Unassign**：選択されたアラームの割り当てを解除します。
- **Delete**：選択されたアラームを削除します。
- **Clear**：選択されたアラームをクリアします。
- **Event History**：不正アラームのイベントを表示できます。
- **Detecting APs**（無線帯域、場所、SSID、チャネル番号、WEP 状態、短いプリアンブルまたは長いプリアンブル、RSSI、および SNR を含む）：不正アクセス ポイントを現在検出しているアクセス ポイントを表示できます。
- **Trend**：最新の RSSI 信号強度の傾向を表示します。
- **Rogue Clients**：この不正アクセス ポイントとアソシエートしているクライアントを表示できます。
- **Set State to 'Unknown - Alert'**：不正アクセス ポイントを最も低い脅威としてタグ付けして不正アクセス ポイントの監視を継続し、阻止機能をオフにします。

Set State to ‘Known - Internal’：不正アクセス ポイントを内部としてタグ付けして既知の不正アクセス ポイント リストに追加し、阻止機能をオフにします。

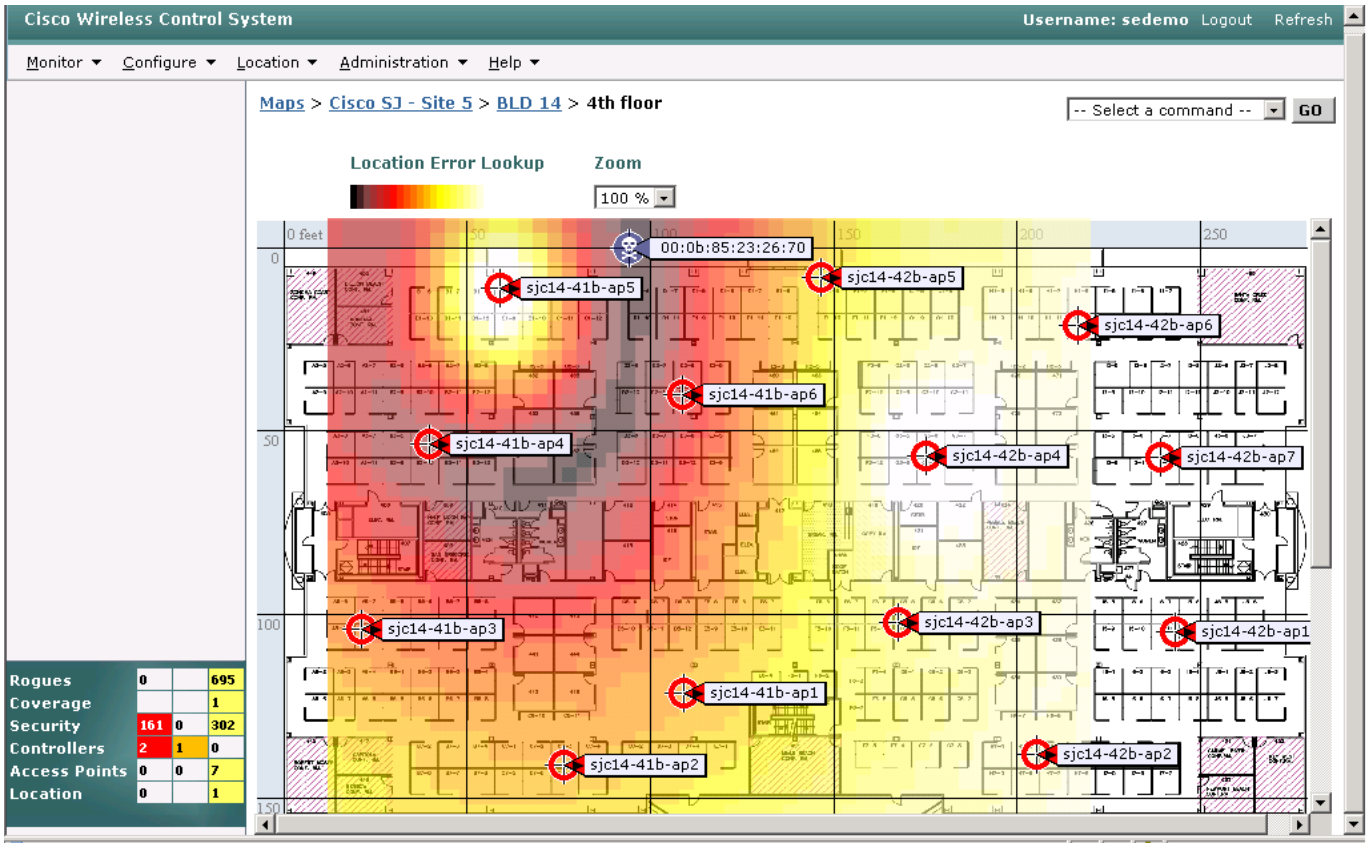
Set State to ‘Known - External’：不正アクセス ポイントを外部としてタグ付けして既知の不正アクセス ポイント リストに追加し、阻止機能をオフにします。

- **1 AP Containment ～ 4 AP Containment**：level 1 containment を選択した場合は、不正な機器の近辺にある 1 つのアクセス ポイントが、その不正な機器にアソシエートされたクライアント デバイスに認証解除とアソシエート解除のメッセージを送信します。level 2 containment を選択した場合は、不正な機器の近辺にある 2 つのアクセス ポイントが、その不正な機器のクライアントに認証解除とアソシエート解除のメッセージを送信します。この動作は level 4 まで同様です。

ステップ 4　Select a Command ドロップダウン メニューから、**Map (High Resolution)** を選択して、**GO** をクリックし、計算された不正アクセス ポイントの現在位置を Maps > *Building Name* > *Floor Name* ページに表示します。

WCS Location を使用している場合は、複数のアクセス ポイントからの RSSI 信号強度を比較して、不正アクセス ポイントの最も可能性の高い位置を見つけ、その位置に小さなドクロと交差した 2 本の骨の形のインジケータが表示されます。WCS Base を使用している場合は、不正アクセス ポイントからの RSSI 信号強度を頼りに、不正な機器から最も強力な RSSI 信号を受信しているアクセス ポイントの隣に小さなドクロと交差した 2 本の骨の形のインジケータが表示されます。図 6-2 は、不正な機器の位置を示すマップを示しています。

図 6-2　不正な機器の位置を示すマップ



不正アクセス ポイントの認識

不正アクセス ポイントを認識する手順は、次のとおりです。

ステップ 1　Rogue AP Alarms ページに移動します。

ステップ 2　認識する不正アクセス ポイントのチェックボックスをオンにします。

ステップ 3　Select a Command ドロップダウン メニューから、**Set State to 'Known - Internal'** または **Set State to 'Known - External'** を選択します。いずれの場合も、不正アクセス ポイントの項目が Rogue AP Alarms ページから削除されます。

クライアントの検索

WCS を使用して無線 LAN 上でクライアントを検索する手順は、次のとおりです。

ステップ 1　**Monitor > Devices > Clients** の順にクリックし、Clients Summary ページに移動します。

ステップ 2　サイドバーで、Search For Clients By ドロップダウン メニューの **All Clients** を選択し、**Search** をクリックして Clients ページを表示します。

（注）　WCS Controllers または Location Servers の下でクライアントを検索できます。

ステップ 3　場所を特定したいクライアントの username をクリックします。対応する Clients *Client Name* ページが表示されます。

ステップ 4　クライアントを検索するには、Select a Command ドロップダウン メニューから次のオプションのいずれかを選択し、**GO** をクリックします。

- **Recent Map (High Resolution)** : アソシエーションを解除せずにクライアントを検索します。
- **Present Map (High Resolution)** : クライアントとのアソシエーションを解除し再アソシエートしてからクライアントを検索します。この方法を選択した場合は、警告メッセージが表示され、続行するかどうかの確認を求められます。

WCS Location を使用している場合は、複数のアクセス ポイントからの RSSI 信号強度を比較して、クライアントの最も可能性の高い位置を見つけ、その位置に小さなラップトップ アイコンが表示されます。WCS Base を使用している場合は、クライアントからの RSSI 信号強度を頼りに、クライアントから最も強力な RSSI 信号を受信しているアクセス ポイントの隣に小さなラップトップ アイコンが表示されます。図 6-3 は、クライアントの位置を示すヒート マップを示しています。

図 6-3　クライアントの位置を示すマップ

カバレッジ ホールの検索

*カバレッジ ホール*とは、クライアントが無線ネットワークから信号を受信できない領域のことです。Cisco Wireless LAN Solution の Radio Resource Management（RRM）によって、これらのカバレッジ ホール領域が特定され WCS に報告されます。IT マネージャはユーザからの要求に基づいてカバレッジ ホールに対応します。無線 LAN 上でカバレッジ ホールを検索する手順は、次のとおりです。

ステップ 1　WCS ユーザ インターフェイスのページの左下にある **Coverage** インジケータをクリックして（または **Monitor > Alarms** の順にクリックして Alarm Category の下で **Coverage** を検索し）、Coverage Hole Alarms ページを表示します。

ステップ 2　**Monitor > Maps** の順にクリックして、access points を name で検索します（この検索ツールでは、大文字と小文字が区別されます）。検索されたアクセス ポイントが設置されているフロアと外部領域を含む Maps > Search Results ページが表示されます。

ステップ 3　フロアまたは外部領域のリンクをクリックして、関連する Maps > *Building Name* > *Floor Name* ページを表示します。

ステップ 4　カバレッジ ホールを報告したアクセス ポイントの近辺で信号強度の弱い領域を探します。その領域がカバレッジ ホールの可能性が最も高い領域です。信号強度の弱い領域が表示されない場合は、フロア図面マップが正確であることを確認してください。

コントローラからネットワーク デバイスへの ping

コントローラからネットワーク デバイスを ping する手順は、次のとおりです。

ステップ 1　**Configure** > **Controllers** の順にクリックし、All Controllers ページに移動します。

ステップ 2　目的の IP アドレスをクリックして、*IP Address* > Controller Properties ページを表示します。

ステップ 3　サイドバーで、**System > Commands** の順にクリックして、*IP Address* > Controller Commands ページを表示します。

ステップ 4　Administrative Commands ドロップダウン メニューから、**Ping From Controller** を選択し、**GO** をクリックします。

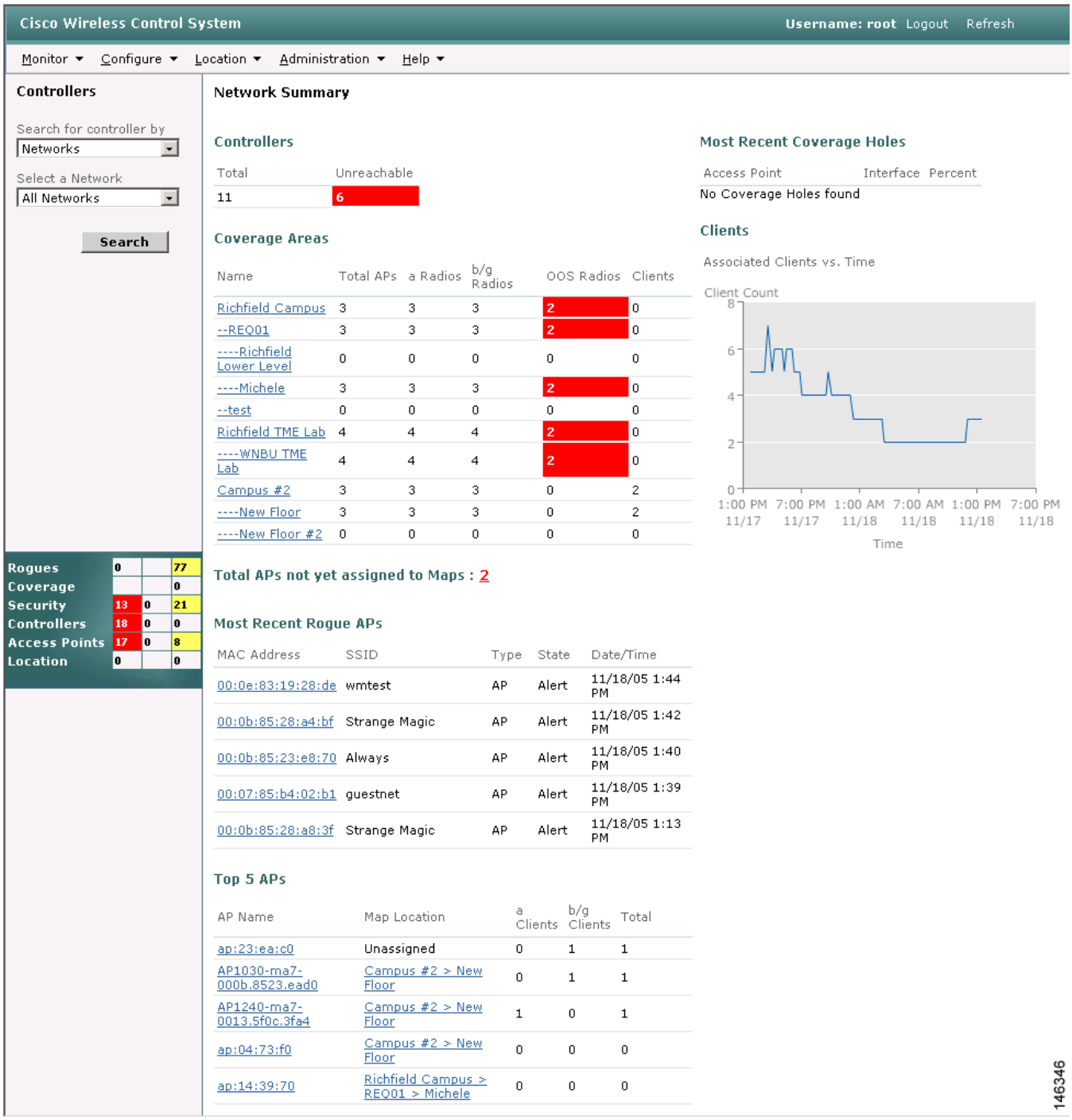
ステップ 5　Enter an IP Address (x.x.x.x) to Ping ウィンドウで、コントローラに ping させるネットワーク デバイスの IP アドレスを入力して、**OK** をクリックします。

Ping Results ウィンドウが開いて、送受信されたパケットが表示されます。ネットワーク デバイスに再度 ping するには、**Restart** をクリックします。または、ネットワーク デバイスへの ping を停止して、Ping Results ウィンドウを終了するには、**Close** をクリックします。

コントローラのステータスと設定の表示

コントローラとアクセス ポイントを WCS データベースに追加すれば、Cisco Wireless LAN Solution のステータスを表示できます。システム ステータスを表示するには、**Monitor > Network Summary** の順にクリックして Network Summary ページを表示します（図 6-4 を参照してください）。

図 6-4　Network Summary ページ



WCS の統計レポートの表示

WCS によって、クライアント カウント、無線の使用状況、送信電力レベルとチャネル情報、プロファイル ステータスなどの統計値が定期的に収集され、レポートにまとめられます。これらのレポートを表示するには、**Monitor** > **Reports** の順にクリックします。