APPENDIX B

不正アクセス ポイントの管理

この付録では、不正アクセス ポイントのセキュリティ問題とソリューションについて説明します。

この付録の構成は、次のとおりです。

不正アクセス ポイントの問題

不正アクセス ポイントは、正規のクライアントをハイジャックし、プレーン テキストまたは他の DoS 攻撃や中間者攻撃を使用することによって、無線 LAN の運用を妨害します。つまり、ハッカーは不正アクセス ポイントを使用して、パスワードやユーザ名などの機密情報を取得できるのです。すると、ハッカーは一連の Clear To Send（CTS; クリア ツー センド）フレームを送信できるようになります。このフレームはアクセス ポイントを模倣し、特定の無線 LAN クライアント アダプタに伝送して、他のすべてのアダプタには待機するように指示します。その結果、正規のクライアントは、無線 LAN リソースに接続できなくなります。したがって、無線 LAN サービス プロバイダーは、空間からの不正アクセス ポイントの締め出しに強い関心を持っています。

オペレーティング システムのセキュリティ ソリューションでは、「不正アクセス ポイントのロケーション、タギング、および封じ込め」（P.B-1）の説明にあるように、Radio Resource Management（RRM; 無線リソース管理）機能を使用して、すべての近隣アクセス ポイントを継続的にモニタし、不正アクセス ポイントを自動的に検出し、位置を特定します。

不正アクセス ポイントのロケーション、タギング、および封じ込め

NCS を使用して Cisco Unified Wireless Network Solution をモニタしている場合、不正アクセス ポイントが検出されるとフラグが生成され、既知の不正アクセス ポイントの MAC アドレスが表示されます。オペレータは、それぞれの不正アクセス ポイントに最も近いアクセス ポイントの場所を示すマップを表示できます。その後、それらを Known または Acknowledged 不正アクセス ポイントとしてマークする（追加の処置はなし）、それらを Alert 不正アクセス ポイントとしてマークする（監視し、アクティブになったときに通知）、それらを Contained 不正アクセス ポイントとしてマークする（1 ～ 4 台

のアクセス ポイントから、不正アクセス ポイントのクライアントが不正アクセス ポイントとアソシエートするたびにそれら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によって封じ込め処理を行う）のいずれかを実行します。

この組み込み型の検出、タギング、モニタリング、および封じ込め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 ポイントの通知を受け取ります（通路をスキャンして歩く必要なし）。
- 不明な不正アクセス ポイントが削除または認識されるまでモニタします。
- 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 ～ 4 台のアクセス ポイントから、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 ポイントを封じ込めます。この封じ込め処理は、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、未知（管理対象外）のアクセス ポイントとしてタグ付けします。
  - 不正アクセス ポイントを封じ込め処理済みとしてタグ付けし、1 ～ 4 台のアクセス ポイントから、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 ポイント上のすべて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 ポイントの電源が入りコントローラにアソシエートされると、NCS はすぐに不正アクセス ポイントのリスニングを開始します。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 NCS に通知され、NCS 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。

NCS 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 NCS ユーザ インターフェイス ページの左下隅にアラーム モニタが表示されます。

不正アクセス ポイントを検出して特定するには、次の手順を実行します。

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] の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 リスト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。
- [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、封じ込め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、封じ込め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、封じ込め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ディスアソシエーション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 リストから [Map (High Resolution)] を選択して、[Go] をクリックします。[Maps > Building Name > Floor Name] ページに、計算された不正アクセス ポイントの現在位置が表示されます。

NCS 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 信号強度を比較することによって、不正アクセス ポイントが存在する可能性が最も高い位置が特定され、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。アクセス ポイント 1 つと全方向性アンテナ 1 つだけの低展開ネットワークの場合、不正アクセス ポイントが存在する可能性が最も高い位置はアクセス ポイント周辺のリング上のいずれかの位置です。ただし、存在する可能性が高い位置の中心はアクセス ポイントとなります。NCS 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。

アラームのモニタリング

この項では、次のトピックを扱います。

不正アクセス ポイントに関するアラームの監視

不正アクセス ポイント無線は、Cisco Lightweight アクセス ポイントによって検出された未許可のアクセス ポイントです。このページには、[Alarm Monitor] でクリックした重大度に基づいて、不正アクセス ポイントのアラームが表示されます。

[Rogue AP Alarms] ページを表示する手順は、次のとおりです。

- [Monitor] > [Alarms] の順に選択します。[Search] をクリックし、[Alarm Category] ドロップダウン リストから [Rogue AP] を選択します。[Go] をクリックして、該当するアラームを表示します。
- [Monitor] > [Security] の順に選択します。左側のサイドバーから、[Rouge AP] を選択します。
- 左側のサイドバー メニューの [Alarm Summary] ボックスで、[Malicious AP] の件数のリンクをクリックします。

（注）　アラーム ページが複数ある場合は、ページ番号および他のページへ移動するためのスクロール矢印がページ上部に表示されます。これらのスクロール矢印を使用して、その他のアラームを表示します。

表 B-1 に、[Rogue Access Point Alarms] ページに表示されるパラメータの説明を示します。

表 B-1　アラーム パラメータ

パラメータ	説明
Check box	操作対象となるアラームを選択します。
Severity	アラームの重大度：Critical、Major、Minor、Clear が色分けして表示されます。
Rogue MAC Address	不正アクセス ポイントの Media Access Control（MAC; メディア アクセス コントロール）アドレス。[Monitor Alarms] > [Rogue AP Details] を参照。
Vendor	不正アクセス ポイントのベンダー名、または Unknown（不明）。
Classification Type	Malicious（危険性あり）、Friendly（危険性なし）、Unclassified（未分類）。
Radio Type	この不正アクセス ポイントの無線タイプ。
Strongest AP RSSI	受信信号強度インジケータの最大値（dBm）。
No. of Rogue Clients	このアクセス ポイントにアソシエートされている不正クライアントの数。
Owner	不正アクセス ポイントの「オーナー」。
Date/Time	アラームの発生時刻。
State	State of the alarm：Alert（アラート）、Known（既知）、または Removed（削除済み）。
SSID	不正アクセス ポイント無線によってブロードキャストされている Service Set Identifier（SSID; サービス セット ID）。SSID がブロードキャストされない場合は空欄になります。
Map Location	この不正アクセス ポイントのマップ位置。
Acknowledged	対象ユーザがこのアラームを確認済みであるかどうかが表示されます。

（注） アラームは NCS に保存されるため、アラーム検索機能を使用して、すべての認知しているアラームを検索できます。

[Rogue AP Alarms] ページには、次の追加フィールドがあります。

- [Unacknowledge]：すでに認知しているアラームを未認知にします。
- [E-mail Notification]：[All Alarms] > [E-mail Notification] ページへ移動し、電子メール通知を表示および設定できるようになります。詳細は、[Monitor Alarms] > [E-mail Notification] を参照してください。
- [Severity Configuration]：新しく生成されたアラームの重大度を変更します。詳細は、[Monitor Alarms] > [Severity Configuration] を参照してください。
- [Detecting APs]：現在、不正アクセス ポイントを検出している Cisco Lightweight アクセス ポイントを表示します。
- [Map (High Resolution)]：ここをクリックすると、不正アクセス ポイントの位置を示す高解像度マップが表示されます。
- [Rogue Clients]：ここをクリックすると、この不正アクセス ポイントにアソシエートされている不正クライアントが一覧表示されます。[Rogue Clients] ページには、クライアントの MAC アドレス、最終通信日時、現在のステータス、関連付けられているコントローラ、および不正アクセス ポイントが表示されます。
- [Set State to 'Unclassified - Alert']：このコマンドを選択して、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、封じ込め機能をオフにします。
- [Set State to 'Malicious - Alert']：このコマンドを選択して、不正アクセス ポイントを「危険性あり」としてタグ付けします。
- [Set State to 'Friendly - Internal']：このコマンドを選択して、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 AP リストに追加し、封じ込め機能をオフにします。
- [1 AP Containment]：不正アクセス ポイントを 1 つのアクセス ポイントで封じ込めます。（最小封じ込めレベル）。
- [2 AP Containment]：不正アクセス ポイントを 2 つの Cisco Lightweight アクセス ポイントで封じ込めます。
- [3 AP Containment]：不正アクセス ポイントを 3 つの Cisco Lightweight アクセス ポイントで封じ込めます。
- [4 AP Containment]：不正アクセス ポイントを 4 つの Cisco Lightweight アクセス ポイントで封じ込めます （最大封じ込めレベル）。

注意 不正アクセス ポイントの阻止は法的責任を伴う場合があります。いずれかの AP 封じ込めコマンドを選択し、[Go] をクリックすると、メッセージ「Containing a Rogue AP may have legal consequences. Do you want to continue?」が表示されます。処理を続行する場合は [OK] をクリックします。アクセス ポイントを封じ込めない場合は [Cancel] をクリックします。

不正アクセス ポイントの詳細な監視情報

[Rogue AP Alarms] ページでは、各不正アクセス ポイントに関するアラーム イベントの詳細を確認できます。

不正アクセス ポイント無線のアラーム イベントを確認するには、[Rogue AP Alarms] ページで [Rogue MAC Address] の下にある項目をクリックします。

このページには、不正アクセス ポイント無線のアラーム イベントが表示されます。不正アクセス ポイント無線は、Cisco Lightweight アクセス ポイントによって検出された未許可のアクセス ポイントです。表示される情報は次のとおりです。

- [General Info] :
  - [Rogue MAC Address] : 不正アクセス ポイントの MAC アドレス。
  - [Vendor] : 不正アクセス ポイントのベンダー名、または Unknown（不明）。
  - [On Network] : 不正アクセス ポイントがネットワーク上にあるかどうかを示します。
  - [Owner] : オーナー（または空白）。
  - [Acknowledged] : 担当ユーザがこのアラームを認知しているかどうかを示します。
  - [Classification Type] : Malicious、Friendly、Unclassified。
  - [State] : Alert（アラート）、Known（既知）、または Removed（削除済み）のアラームの状態を示します。
  - [SSID] : 不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。SSID がブロードキャストされない場合は空欄になります。
  - [Channel Number] : 不正アクセス ポイントのチャネル。
  - [Containment Level] : 不正アクセス ポイントの封じ込めレベル、または Unassigned（未割り当て）。
  - [Radio Type] : この不正アクセス ポイントの無線タイプ。
  - [Strongest AP RSSI] : 受信信号強度インジケータの最大値（dBm）。
  - [No. of Rogue Clients] : このアクセス ポイントにアソシエートされている不正クライアントの数。
  - [Created] : アラーム イベントが作成された日時。
  - [Modified] : アラーム イベントが修正された日時。
  - [Generated By] : アラーム イベントの生成元。
  - [Severity] : アラームの重大度 : Critical、Major、Minor、Clear が色分けして表示されます。
  - [Previous Severity] : アラームの以前の重大度 : Critical、Major、Minor、Clear が色分けして表示されます。
- [Annotations] : このテキスト ボックスに新しい注釈を入力して [Add] をクリックすると、該当するアラームが更新されます。
- [Message] : アラームに関する説明が表示されます。
- [Help] : アラームに関する最新情報が表示されます。
- [Event History] : ここをクリックすると、[Monitor Alarms > Events] ページが開きます。
- [Annotations] : このアラームの現在の注釈が表示されます。

ネットワーク上のアクセス ポイントの検出

不正アクセス ポイントを検出している Cisco Lightweight アクセス ポイントに関する情報を表示するには、アクセス ポイントの検出機能を使用します。

[Rogue AP Alarms] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Rogue AP Alarms] ページを表示するには、次のいずれかを実行します。

- 不正 AP の検索を実行します。この検索機能の詳細については、「Using the Search Feature」（P.2-34）を参照してください。
- NCS ホームページで、[Security] ダッシュボードをクリックします。このダッシュボードには、過去 1 時間と過去 24 時間に検出された不正アクセス ポイントがすべて表示されます。不正アクセス ポイント アラームを表示するには、不正アクセス ポイント番号をクリックします。
- [Alarm Summary] ボックスの [Malicious AP] の件数のリンクをクリックします。

ステップ 2　[Rogue AP Alarms] ページで、該当する不正アクセス ポイントの [Rogue MAC Address] をクリックします。[Rogue AP Alarms] 詳細ページが表示されます。

ステップ 3　[Select a command] ドロップダウン リストから、[Detecting AP on Network] を選択します。

ステップ 4　[Go] をクリックします。

いずれかのリスト項目をクリックすると、その項目に関するデータが表示されます。

- AP Name
- Radio
- Map Location
- Detecting AP Location
- [SSID]：不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。
- [Channel Number]：不正アクセス ポイントがブロードキャストしているチャネル。
- [WEP]：有効または無効。
- [WPA]：有効または無効。
- [Pre-Amble]：Long（長型）または Short（短型）。
- [RSSI]：受信信号強度インジケータ（dBm）。
- [SNR]：信号対雑音比。
- [Containment Type]：このアクセス ポイントによる封じ込め処理のタイプ。
- [Containment Channels]：このアクセス ポイントが現在封じ込め処理を実行しているチャネル。

不正アドホック無線に関するアラームの監視

[Rogue Adhoc Alarms] ページには、不正アドホック無線のアラーム イベントが表示されます。

[Rogue Adhoc Alarms] ページを表示する手順は、次のとおりです。

- [Monitor] > [Alarms] の順に選択します。左側のサイドバー メニューで [New Search] を選択し、[Alarm Category] ドロップダウン リストから [Rogue Adhoc] を選択します。[Go] をクリックして、該当するアラームを表示します。
- [Monitor] > [Security] の順に選択します。左側のサイドバー メニューで、[Rogue Adhocs] を選択します。

（注）　アラーム ページが複数ある場合は、ページ上部にページ番号とその両側に他のページへ移動するためのスクロール矢印が表示されます。これらのスクロール矢印を使用して、その他のアラームを表示します。

表 B-2 に、[Rogue Ad hoc Alarms] ページに表示されるフィールドの説明を示します。

表 B-2　不正アドホック無線のアラーム

パラメータ	説明
Check box	操作対象となるアラームを選択します。
Severity	アラームの重大度：Critical、Major、Minor、Clear が色分けして表示されます。
Rogue Adhoc MAC Address	不正アドホック無線デバイスの MAC アドレス。
Vendor	不正アドホック無線デバイスのベンダー名、または Unknown（不明）。
Classification Type	Malicious（危険性あり）、Friendly（危険性なし）、Unclassified（未分類）。
Radio Type	この不正アドホック無線の種類。
Strongest AP RSSI	受信信号強度インジケータの最大値（dBm）。
No.of Rogue Clients	この不正アドホック無線にアソシエートされている不正クライアントの数。
Owner	不正アドホック無線の「オーナー」。
Date/Time	アラームの発生時刻。
State	State of the alarm：Alert（アラート）、Known（既知）、または Removed（削除済み）。
SSID	不正アドホック無線によってブロードキャストされている Service Set Identifier。（SSID がブロードキャストされない場合は空欄になります）。
Map Location	この不正アドホック無線のマップ位置。
Acknowledged	対象ユーザがこのアラームを確認済みであるかどうかが表示されます。

Select a Command

対応するチェックボックスを選択して 1 つ以上のアラームを選択し、[Select a command] ドロップダウン リストから次のいずれかのコマンドを選択して、[Go] をクリックします。

- [Assign to me]：選択したアラームを現在のユーザに割り当てます。
- [Unassign]：選択したアラームの割り当てを解除します。
- [Delete]：選択し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。
- [Clear]：選択されたアラームをクリアします。
- [Acknowledge]：[Alarm Summary] ページに表示されないように、アラームを承認します。

（注）　アラームは NCS に保存されるため、アラーム検索機能を使用して、すべての認知しているアラームを検索できます。

- [Unacknowledge]：すでに認知しているアラームを未認知にします。
- [Email Notification]：電子メール通知を表示して設定するために、[All Alarms] > [Email Notification] ページを表示します。
- [Detecting APs]：不正なアドホックを現在検出している Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントを表示します。詳細については、ネットワーク上のアクセス ポイントの検出を参照してください。

- [Map (High Resolution)]：ここをクリックすると、不正アドホック無線の位置を示す高解像度マップが表示されます。
- [Rogue Clients]：ここをクリックすると、この不正アドホック無線にアソシエートされている不正クライアントが一覧表示されます。[Rogue Clients] ページには、クライアントの MAC アドレス、最終通信日時、現在のステータス、関連付けられているコントローラ、および不正アドホック無線が表示されます。
- [Set State to 'Alert']：このコマンドを選択して、不正アドホック無線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、封じ込め機能をオフにします。
- [Set State to 'Internal']：このコマンドを選択して、不正アドホック無線を内部としてタグ付けして既知の不正 AP リストに追加し、封じ込め機能をオフにします。
- [Set State to 'External']：このコマンドを選択して、不正アドホック無線を外部としてタグ付けして既知の不正 AP リストに追加し、封じ込め機能をオフにします。
- [1 AP Containment]：不正アドホック無線を 1 つのアクセス ポイントで封じ込めます。（最小封じ込めレベル）。
- [2 AP Containment]：不正アドホック無線を 2 つの Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。
- [3 AP Containment]：不正アドホック無線を 3 つの Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。
- [4 AP Containment]：不正アドホック無線を 4 つの Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。（最大封じ込めレベル）。

注意　不正 AP の阻止は法的責任を伴う場合があります。いずれかの AP 封じ込めコマンドを選択し、[Go] をクリックすると、メッセージ「Containing a Rogue AP may have legal consequences.Do you want to continue?」が表示されます。処理を続行する場合は [OK] をクリックします。アクセス ポイントを封じ込めない場合は [Cancel] をクリックします。

不正アドホック無線に関する詳細の監視

[Rogue Adhoc Alarms] ページでは、各不正アドホック無線に関するアラーム イベントの詳細を確認できます。

不正アドホック無線のアラーム イベントを確認するには、[Rogue Adhoc Alarms] ページで [Rogue MAC Address] の下にある項目をクリックします。

このページには、不正アクセス ポイント無線のアラーム イベントが表示されます。不正アクセス ポイント無線は、Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントによって検出された無認可のアクセス ポイントです。表示される情報は次のとおりです。

- General:
  - [Rogue MAC Address]：不正アドホック無線デバイスの MAC アドレス。
  - [Vendor]：不正アドホック無線デバイスのベンダー名、または Unknown（不明）。
  - [On Network]：不正アドホック無線デバイスがネットワーク上にあるかどうかを示します。
  - [Owner]：オーナー（または空白）。
  - [Acknowledged]：担当ユーザがこのアラームを認知しているかどうかを示します。
  - [Classification Type]：Malicious、Friendly、Unclassified。
  - [State]：Alert（アラート）、Known（既知）、または Removed（削除済み）のアラームの状態を示します。

  - [SSID]：不正アドホック無線によってブロードキャストされている Service Set Identifier。（SSID がブロードキャストされない場合は空欄になります）。
  - [Channel Number]：不正アドホック無線のチャネル。
  - [Containment Level]：不正アドホック無線の封じ込めレベル、または Unassigned（未割り当て）。
  - [Radio Type]：この不正アドホック無線の種類。
  - [Strongest AP RSSI]：受信信号強度インジケータの最大値（dBm）。
  - [No.of Rogue Clients]：このアドホック無線にアソシエートされている不正クライアントの数を示します。
  - [Created]：アラーム イベントが作成された日時。
  - [Modified]：アラーム イベントが修正された日時。
  - [Generated By]：アラーム イベントの生成元。
  - [Severity]：アラームの重大度：Critical、Major、Minor、Clear が色分けして表示されます。
  - [Previous Severity]：アラームの以前の重大度：Critical、Major、Minor、Clear が色分けして表示されます。
- [Annotations]：このテキスト ボックスに新しい注釈を入力して [Add] をクリックすると、該当するアラームが更新されます。
- [Message]：アラームに関する説明が表示されます。
- [Help]：アラームに関する最新情報が表示されます。
- [Event History]：ここをクリックすると、[イベントのモニタリング] ページが開きます。
- [Annotations]：このアラームの現在の注釈が表示されます。

Select a Command

対応するチェックボックスを選択して 1 つ以上のアラームを選択し、次のいずれかのコマンドを選択して、[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。
- [Acknowledge]：[Alarm Summary] ページに表示されないように、アラームを承認します。アラームは NCS に保存されるため、アラーム検索機能を使用して、すべての認知しているアラームを検索できます。
- [UnAcknowledge]：すでに認知しているアラームの認知を解除できます。
- [Email Notification]：電子メール通知を表示して設定するために、[All Alarms] > [Email Notification] ページを表示します。
- [Detecting APs]：不正なアドホックを現在検出している Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントを表示します。詳細については、「ネットワーク上のアクセス ポイントの検出」（P.B-6）を参照してください。
- [Map (High Resolution)]：ここをクリックすると、不正アドホック無線の位置を示す高解像度マップが表示されます。

- [Rogue Clients]：ここをクリックすると、この不正アドホック無線にアソシエートされている不正クライアントが一覧表示されます。[Rogue Clients] ページには、クライアントの MAC アドレス、最終通信日時、現在のステータス、関連付けられているコントローラ、および不正アドホック無線が表示されます。
- [Set State to 'Alert']：このコマンドを選択して、不正アドホック無線を最も低い脅威としてタグ付けして不正アドホック無線の監視を継続し、封じ込め機能をオフにします。
- [Set State to 'Internal']：このコマンドを選択して、不正アドホック無線を内部としてタグ付けして既知の不正 AP リストに追加し、封じ込め機能をオフにします。
- [Set State to 'External']：このコマンドを選択して、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 AP リストに追加し、封じ込め機能をオフにします。
- [1 AP Containment]：不正アドホック無線を 1 つのアクセス ポイントで封じ込めます。（最小封じ込めレベル）。
- [2 AP Containment]：不正アドホック無線を 2 つの Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。
- [3 AP Containment]：不正アドホック無線を 3 つの Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。
- [4 AP Containment]：不正アドホック無線を 4 つの Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。（最大封じ込めレベル）。

イベントのモニタリング

[Alarm Monitor] にある [Rogues] アラーム枠をクリックし、[Rogue MAC Addresses] のリスト項目をクリックします。次に、[Select a command] ドロップダウン リストから [Event History] を選択して、[Go] をクリックします。このページが表示されます。

[Monitor] > [Alarms] の順に選択し、左側のサイドバー メニューで [New Search] を選択します。[Severity] > [All Severities] および [Alarm Category] > [Rogue AP] の順に選択して、[Go] をクリックします。[Monitor Alarms > failure object] ページが表示されます。[Rogue MAC Address] 列の項目をクリックして、[Monitor Alarms > Rogue AP Details] ページを開きます。[Select a command] ドロップダウン リストから [Event History] を選択して、[Go] をクリックします。このページが表示されます。

このページでは、不正アラーム イベントに関する情報を参照できます。これらのイベントは発生した順に一覧表示されます。

各列のタイトルをクリックすると、表示順序を変更することができます。

- [Severity]：イベントの重大度が色分けして表示されます。
- [Rogue MAC Address]：リスト項目をクリックすると、そのエントリに関する情報が表示されます。
- [Vendor]：不正アクセス ポイントの製造業者名。
- [Type]：AP（アクセス ポイント）または AD-HOC（アドホック）。
- [On Network]：不正アクセス ポイントが、アソシエートされているポートと同じサブネットにあるかどうか。
- [On 802.11a]：不正アクセス ポイントが 802.11a 帯でブロードキャストしているかどうか。
- [On 802.11b]：不正アクセス ポイントが 802.11b/802.11g 帯でブロードキャストしているかどうか。
- [Date/Time]：アラームの日時。
- [Classification Type]：Malicious、Friendly、Unclassified。

- [State]：アラームの状態。Alert（アラート）、Removed（削除済み）など。
- [SSID]：不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。

不正クライアントの監視

[Monitor] > [Alarms] の順に選択し、左側のサイドバー メニューで [New Search] を選択します。[Severity] > [All Severities] および [Alarm Category] > [Rogue AP] の順に選択して、[Go] をクリックします。[Monitor Alarms > failure object] ページが表示されます。[Rogue MAC Address] 列の項目をクリックして、[Monitor Alarms > Rogue AP Details] ページを開きます。[Select a command] ドロップダウン リストから [Rogue Clients] を選択します。このページが表示されます。

このページでは、不正アクセス ポイントにアソシエートされているクライアントに関する情報を参照できます。

- [Client MAC Address]：不正アクセス ポイントのクライアントの MAC アドレス。
- [Last Heard]：シスコ アクセス ポイントが不正アクセス ポイントのクライアントを最後に検出した時刻。
- [Status]：不正アクセス ポイントのクライアントの状態。

コントローラの設定

この項では、次のトピックを扱います。

- 「不正ポリシーの設定」（P.B-12）
- 「不正 AP ルールの設定」（P.B-13）

不正ポリシーの設定

このページでは、不正アクセス ポイントのポリシーを設定できます。

[Rogue Policies] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　[IP Address] 列で IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[Security] > [Rogue Policies] の順に選択します。

- [Rogue Location Discovery Protocol]：[Enabled]、[Disabled]。
- Rogue APs
  - [Expiration Timeout for Rogue AP Entries (seconds)]：1 ～ 3600 秒（デフォルトは 1200）。
- Rogue Clients
  - [Validate rogue clients against AAA (check box)]：[Enabled]、[Disabled]
  - [Detect and report ad hoc networks (check box)]：[Enabled]、[Disabled] コマンド ボタン。
- [Save]：クライアント除外ポリシーへの変更を保存して、前のページに戻ります。
- [Audit]：NCS 値を、コントローラで使用された値と比較します。

不正 AP ルールの設定

このページでは、現在の不正 AP ルールの表示と編集ができます。

[Rogue AP Rules] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　[IP Address] 列で IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[Security] > [Rogue AP Rules] の順に選択します。[Rogue AP Rules] ページに、不正 AP ルール、ルール タイプ（[Malicious] または [Friendly]）、およびルールの順序が表示されます。

ステップ 4　ルールの詳細を表示または編集するには、不正 AP ルールを選択します。詳細については、「不正 AP ルールの設定」（P.B-14）を参照してください。

コントローラ テンプレートの設定

この項では、次のトピックを扱います。

不正ポリシーの設定

このページでは、コントローラに適用される（アクセス ポイントとクライアントに対する）不正ポリシー テンプレートを設定できます。

現在のテンプレート、テンプレートが適用されているコントローラ数を表示するには、[Configure] > [Controller Templates] > [Security] > [Rogue Policies] の順に選択します。

新しい不正ポリシー テンプレートを作成するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Templates] の順に選択します。

ステップ 2　左側のサイドバー メニューから、[Security] > [Rogue Policies] の順に選択します。

ステップ 3　[Select a command] ドロップダウン リストから、[Add Template] を選択します。

ステップ 4　[Go] をクリックします。

（注）　既存の不正ポリシー テンプレートに変更を加える場合、または現在のテンプレートをコントローラに適用する場合は、[Configure] > [Controller Templates] > [Security] > [Rogue Policies] の順に選択し、[Template Name] 列でテンプレート名をクリックします。テンプレートに必要な変更を加え、[Save] または [Apply to Controllers] をクリックします。

ステップ 5　[Rogue Location Discovery Protocol] チェックボックスをオンにして、有効にします。Rogue Location Discovery Protocol（RLDP）では、企業の有線ネットワークへの不正な接続の有無を判断します。

（注） RLDP が有効の場合、コントローラは管理対象のアクセス ポイントに対して、不正アクセス ポイントをアソシエートし、特殊なパケットをコントローラへ送信するよう指示します。コントローラがこのパケットを受信すると、不正アクセス ポイントが企業ネットワークに接続されます。この方法は、暗号化を有効にしていない不正アクセス ポイントに対して機能します。

ステップ 6　不正アクセス ポイント エントリの失効タイムアウトを秒単位で設定します。

ステップ 7　[Validate rogue clients against AAA] チェックボックスをオンにして、不正クライアントの AAA 検証を有効にします。

ステップ 8　[Detect and report Adhoc networks] チェックボックスをオンにして、アドホック ネットワーキングに参加している不正クライアントの検出とレポートを有効にします。

ステップ 9　次のいずれかのボタンをクリックします。

- [Save] : クリックして現在のテンプレートを保存します。
- [Apply to Controllers]: クリックして現在のテンプレートをコントローラに適用します。[Apply to Controllers] ページで該当するコントローラを選択し、[OK] をクリックします。
- [Delete] : クリックして現在のテンプレートを削除します。現在コントローラにそのテンプレートが適用されている場合は、[OK] をクリックして、テンプレートが適用されている選択したコントローラから、テンプレートを削除することを確定します。
- [Cancel] : クリックして現在のテンプレート作成または現在のテンプレートの変更をキャンセルします。

不正 AP ルールの設定

不正 AP ルールを使用すると、不正アクセス ポイントを自動的に分類するルールを定義できます。NCS は、不正アクセス ポイントの分類ルールをコントローラに適用します。これらのルールでは、RSSI レベル（それよりも弱い不正アクセス ポイントは無視）、または時間制限（指定された時間内に表示されない不正アクセス ポイントにはフラグを立てない）に基づいて、マップ上の不正表示を制限できます。

（注） 不正 AP ルールは、誤アラームを減らすのにも役立ちます。

現在の分類ルール テンプレート、ルールの種類、適用されているコントローラ数を表示するには、[Configure] > [Controller Templates] > [Security] > [Rogue AP Rules] の順に選択します。

（注） 不正クラスには以下の種類があります。
[Malicious Rogue] : 検出されたアクセス ポイントのうち、ユーザが定義した Malicious ルールに一致したアクセス ポイント、または危険性のない AP カテゴリから手動で移動されたアクセス ポイント。
[Friendly Rogue] : 既知、認識済み、または信頼できるアクセス ポイント、または検出されたアクセス ポイントのうち、ユーザが定義した Friendly ルールに該当するアクセス ポイント。
[Unclassified Rogue] : 検出されたアクセス ポイントのうち、Malicious ルールまたは Friendly ルールに該当しないアクセス ポイント。

不正アクセス ポイントの新しい分類ルール テンプレートを作成するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Templates] の順に選択します。

ステップ 2　左側のサイドバー メニューから、[Security] > [Rogue AP Rules] の順に選択します。

ステップ 3　[Select a command] ドロップダウン リストから、[Add Classification Rule] を選択します。

ステップ 4　[Go] をクリックします。

（注）　既存の不正 AP ルールのテンプレートに変更を加える場合、または現在のテンプレートをコントローラに適用する場合は、[Configure] > [Controller Templates] > [Security] > [Rogue AP Rules] の順に選択し、[Template Name] 列でテンプレート名をクリックします。テンプレートに必要な変更を加え、[Save] または [Apply to Controllers] をクリックします。

ステップ 5　次のフィールドに入力します。

- General:
  - [Rule Name]：テキスト ボックスにルールの名前を入力します。
  - [Rule Type]：ドロップダウン リストから [Malicious] または [Friendly] を選択します。

（注）　[Malicious Rogue]：検出されたアクセス ポイントのうち、ユーザが定義した Malicious ルールに一致したアクセス ポイント、または危険性のない AP カテゴリから手動で移動されたアクセス ポイント。
[Friendly Rogue]：既知、認識済み、または信頼できるアクセス ポイント、または検出されたアクセス ポイントのうち、ユーザが定義した Friendly ルールに該当するアクセス ポイント。

  - [Match Type]：ドロップダウン リストから [Match All Conditions] または [Match Any Condition] を選択します。
- Malicious Rogue Classification Rule
  - [Open Authentication]：オープン認証を有効にするには、このチェックボックスをオンにします。
  - [Match Managed AP SSID]：管理対象 AP SSID のルール条件との一致を有効にするには、このチェックボックスをオンにします。

（注）　管理対象 SSID は、WLAN に対して設定された SSID で、システムが既知のものです。

  - [Match User Configured SSID]：ユーザ設定の SSID のルール条件との一致を有効にするには、このチェックボックスをオンにします。

（注）　ユーザ設定の SSID は、手動で追加された SSID です。[Match User Configured SSID] テキスト ボックスに、ユーザ設定の SSID を（1 行に 1 つずつ）入力します。

  - [Minimum RSSI]：最小 RSSI 閾値制限を有効にするには、このチェックボックスをオンにします。

（注）　テキスト ボックスに RSSI 閾値の最小レベル（dB 単位）を入力します。検出されたアクセス ポイントがここで指定した RSSI 閾値を超えていると、そのアクセス ポイントは悪意のあるものとして分類されます。

– [Time Duration]：時間制限を有効にするには、このチェックボックスをオンにします。

（注） テキスト ボックスに制限時間（秒単位）を入力します。検出されたアクセス ポイントが指定した制限時間よりも長く表示されているとき、そのアクセス ポイントは悪意のあるものとして分類されます。

– [Minimum Number Rogue Clients]：悪意のあるクライアントの最小数の制限を有効にするには、このチェックボックスをオンにします。

（注） 悪意のあるクライアントを許可する最小数を入力します。検出されたアクセス ポイントにアソシエートされたクライアントの数が指定した値以上になると、そのアクセス ポイントは悪意のあるものとして分類されます。

ステップ 6　次のいずれかのボタンをクリックします。

- [Save]：クリックして現在のテンプレートを保存します。
- [Apply to Controllers]:クリックして現在のテンプレートをコントローラに適用します。[Apply to Controllers] ページで該当するコントローラを選択し、[OK] をクリックします。
- [Delete]：クリックして現在のテンプレートを削除します。現在コントローラにそのテンプレートが適用されている場合は、[OK] をクリックして、テンプレートが適用されている選択したコントローラから、テンプレートを削除することを確定します。
- [Cancel]：クリックして現在のテンプレート作成または現在のテンプレートの変更をキャンセルします。

不正 AP ルール グループの設定

不正 AP ルール グループ テンプレートを使用すると、複数の不正 AP ルールをコントローラに統合できます。

現在の不正 AP ルール グループ テンプレートを表示するには、[Configure] > [Controller Templates] > [Security] > [Rogue AP Rule Groups] の順に選択します。

新しい不正 AP ルール グループ テンプレートを作成するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Templates] の順に選択します。

ステップ 2　左側のサイドバー メニューから、[Security] > [Rogue AP Rule Groups] の順に選択します。

ステップ 3　[Select a command] ドロップダウン リストから、[Add Rogue Rule Group] を選択します。

ステップ 4　[Go] をクリックします。

（注） 既存の不正ポリシー テンプレートに変更を加える場合、または現在のテンプレートをコントローラに適用する場合は、[Configure] > [Controller Templates] > [Security] > [Rogue AP Rule Groups] の順に選択し、[Template Name] 列でテンプレート名をクリックします。テンプレートに必要な変更を加え、[Save] または [Apply to Controllers] をクリックします。

ステップ 5　次のパラメータを入力します。

- General

- [Rule Group Name]：テキスト ボックスにルール グループの名前を入力します。

ステップ 6　Rogue AP ルールを追加するには、左の列のルールをクリックして強調表示します。[Add] をクリックして、強調表示したルールを右側の列に移動します。

（注）　不正 AP ルールは、[Rogue AP Rules] グループ ボックスから追加できます。詳細については、「不正 AP ルールの設定」（P.B-14）を参照してください。

ステップ 7　不正 AP ルールを削除するには、右の列のルールをクリックして強調表示します。[Remove] をクリックして、強調表示したルールを左側の列に移動します。

ステップ 8　[Move Up]/[Move Down] ボタンをクリックして、ルールが適用される順序を指定します。任意のルールを強調表示し、[Move Up] または [Move Down] をクリックして、現在のリストで上下に移動させます。

ステップ 9　不正 AP ルール リストを保存するには、[Save] をクリックします。

ステップ 10　現在のリストに変更を加えずにページを終了するには [Cancel] をクリックします。

（注）　コントローラに適用されたルールを表示または編集するには、[Configure] > [Controller] の順に選択し、コントローラ名をクリックしてコントローラを開きます。