CHAPTER 3

セキュリティ ソリューションの設定

この章では、無線 LAN のセキュリティ ソリューションについて説明します。ここで説明する内容は、次のとおりです。

Cisco Unified Wireless Network Solution セキュリティ

Cisco Unified Wireless Network Solution は、潜在的に複雑化する可能性のあるレイヤ 1、レイヤ 2、およびレイヤ 3 の 802.11 アクセス ポイントのセキュリティ コンポーネントを 1 つのシンプルなポリシー マネージャにまとめたもので、システム全体のセキュリティ ポリシーを無線 LAN ごとにカスタマイズできます。これにより、シンプルで統一された体系的なセキュリティ管理が実現します。

企業での無線 LAN 展開の最も大きな課題の 1 つが、脆弱な独立型の暗号化方式である Wired Equivalent Privacy（WEP）です。低価格なアクセス ポイントの登場も新たな問題で、企業ネットワークに接続して中間者攻撃および DoS 攻撃に利用される可能性があります。また、次々に追加されるセキュリティ ソリューションの複雑さから、多くの IT マネージャが無線 LAN セキュリティの最新技術を採用することをためらっています。

ここでは、次の内容について説明します。

レイヤ 1 ソリューション

Cisco Unified Wireless Network Solution オペレーティング システムのセキュリティ ソリューションによって、すべてのクライアントはアクセスの試行回数を、オペレータが設定した回数までに制限されます。クライアントがその制限回数内にアクセスできなかった場合、そのクライアントは、オペレータが設定したタイマーが切れるまで自動的に除外（アクセスをブロック）されます。そのオペレーティング システムは、無線 LAN ごとに SSID ブロードキャストを無効にすることもできます。

レイヤ 2 ソリューション

上位レベルのセキュリティと暗号化が必要な場合、ネットワーク管理者は、Extensible Protocol（EAP; 拡張認証プロトコル）を使用する 802.1X 動的キーや Wi-Fi Protected Access（WPA）動的キーなど業界標準のセキュリティ ソリューションも実装できます。Cisco Unified Wireless Network Solution の WPA 実装には、Advanced Encryption Standard（AES）動的キー、Temporal Key Integrity Protocol + Message Integrity Code Checksum（TKIP + Michael）動的キー、または WEP 静的キーが含まれます。無効化も使用され、オペレータが設定した回数だけ認証の試行に失敗すると、自動的にレイヤ 2 アクセスがブロックされます。

どの無線セキュリティ ソリューションを採用した場合も、コントローラとアクセス ポイントとの間のすべてのレイヤ 2 有線通信は、Lightweight Access Point Protocol（LWAPP; Lightweight アクセス ポイント プロトコル）トンネルを使用してデータを渡すことにより保護されます。

レイヤ 3 ソリューション

WEP の問題の解決をさらに進めるには、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）などの業界標準のレイヤ 3 セキュリティ ソリューションを使用します。

Cisco Unified Wireless Network Solution では、ローカルおよび RADIUS メディア アクセス コントロール（MAC）フィルタリングがサポートされています。このフィルタリングは、802.11 アクセス カードの MAC アドレス一覧情報が把握できている小規模のクライアント グループに適しています。Cisco Unified Wireless Network Solution は、ローカルおよび RADIUS ユーザ/パスワード認証もサポートします。この認証は、小規模から中規模のクライアント グループに適しています。

シングル ポイントでの設定ポリシー マネージャのソリューション

Cisco Unified Wireless Network Solution に Cisco Prime Infrastructure を装備した場合、システム全体のセキュリティ ポリシーを無線 LAN ごとに設定できます。スモール オフィス、ホームオフィス（SOHO）のアクセス ポイントでは、アクセス ポイントごとにセキュリティ ポリシーを個別に設定する必要があります。また、複数のアクセス ポイントにわたってセキュリティ ポリシーを設定するには、サードパーティのアプライアンスを使用する必要があります。Cisco Unified Wireless Network Solution セキュリティ ポリシーは Prime Infrastructure からシステム全体に適用できるため、エラーを除去することができ、全体的な作業量が大幅に減少します。

不正アクセス ポイントのソリューション

この項では、不正アクセス ポイントに対するセキュリティ ソリューションについて説明します。内容は次のとおりです。

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、他の DoS 攻撃、または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 ポイントのタギングと封じ込め」（P.3-3）の説明にあるように、無線リソース管理（RRM）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 ポイントのタギングと封じ込め

Prime Infrastructure 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。

不正アクセス ポイントに対するネットワークの保護

MAC フィルタ リストに定義されていないアクセス ポイントからのアクセス ポイント攻撃を禁止し、すべての不正アクセス ポイントからネットワークを保護することができます。

MAC フィルタリングを設定するには、次の手順を実行します。

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

ステップ 2　MAC フィルタを設定したいコントローラの 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] > [AAA] > [MAC Filtering] の順に選択します。[MAC Filtering] ページが表示されます。

RADIUS 互換モード、MAC デリミタ、MAC アドレス、プロファイル名、インターフェイス、および説明が表示されます。

ステップ 4　複数のデバイスにわたって同じ設定を行うには、[Select a command] ドロップダウン リストから [Add MAC Filter] を選択し、[Go] をクリックします。テンプレートがあり、それを適用できます。テンプレートを作成する必要がある場合は、URL をクリックすると、テンプレート作成ページにリダイレクトされます。

（注）　MAC フィルタ リスト内で指定されていなくてもコントローラに接続できるのは、メッシュ アクセス ポイントだけです。

ステップ 5　プロファイル名、インターフェイス、説明などを変更するには、[MAC Address] 列の特定の MAC アドレスをクリックします。

セキュリティ ダッシュボードの説明

無許可の不正アクセス ポイントは安価で入手しやすいことから、そうしたアクセス ポイントを従業員が既存の LAN に接続し、IT 部門の承諾を得ずにアドホック無線ネットワークを構築する場合があります。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内側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、従業員は不正なアクセス 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 Unified Wireless Network Solution では、担当者がスキャナを持って不正アクセス ポイントを手動で検出するのではなく、管理対象のアクセス ポイントにより MAC アドレスと IP アドレス情報をもとに不正アクセス ポイントを検出して、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 ポイントの位置の特定、タグ付け、および封じ込めができるようになります。また、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。

ネットワークの既存イベントおよびセキュリティ状態の概要については、Prime Infrastructure ホーム ページで [Security] ダッシュボードをクリックします。

ここでは、[Security] ダッシュボードのダッシュレットについて説明します。内容は次のとおりです。

- 「セキュリティ インデックス」（P.3-5）
- 「Malicious Rogue Access Points」（P.3-5）
- 「Adhoc Rogues」（P.3-6）
- 「CleanAir Security」（P.3-7）
- 「未分類の不正アクセス ポイント」（P.3-7）
- 「危険性のない不正アクセス ポイント」（P.3-7）
- 「アクセス ポイントの脅威または攻撃」（P.3-8）
- 「MFP Attacks」（P.3-9）
- 「Attacks Detected」（P.3-9）

[Security] ダッシュボードで表示する情報の順序はカスタマイズできます。ダッシュレットを移動して順序を変更できます。ダッシュレットに表示される情報をカスタマイズするには、[Edit Dashlet] アイコンを使用します。[Edit Dashlet] のアイコンを使用すると、ダッシュレットのタイトルの変更、リフレッシュの有効化、リフレッシュ間隔の設定ができます。

セキュリティ インデックス

[Security Index] ダッシュレットには Prime Infrastructure が管理するネットワーク全体のセキュリティ課題などの情報が表示されます。この情報は、日単位のバックグラウンド タスクの一部として計算されます。さまざまなセキュリティ設定に重みを割り当てることによって計算され、視覚的に表示されます。合算された重みの範囲は 0 ～ 100 です。0 は最も安全でないことを示し、100 は最も安全であることを示します。重みは、Prime Infrastructure 内で保持されている、セキュリティ設定と紐付くコントローラおよび Location Server/Mobility Service Engine の中で、最もスコアの低いものから導き出されます。Prime Infrastructure 管理ネットワークのセキュリティ インデックスは、最低スコアのコントローラと最低スコアの Location Service/Mobility Service Engine を加算した値と同等です。

セキュリティ サーモメータの色の範囲は、次のように表示されます。

- 80 以上：緑色
- 60 以上 80 未満：黄色
- 60 未満：赤色

（注） ゲスト WLAN は、スコアリング対象の WLAN から除外されます。Web 認証または Web パススルーが有効な WLAN は、ゲスト WLAN として識別されます。

最新リリースにおけるセキュリティ インデックスは、必要とされるセキュリティ設定に対する基準となります。たとえば、以前のバージョンのコードに AES 暗号化がない場合、AES 暗号化のセキュリティ設定に関連する数値分インデックスが減少します。同様に、新しい設定が行われると、重みが変わります。

（注） Prime Infrastructure で Refresh from Controller コマンドが実行されない場合、Prime Infrastructure に保存されている設定は、コントローラの設定を反映した最新の情報でないことがあります。設定の同期タスクでセキュリティ インデックスの計算を実行することで、すべてのコントローラから最新の設定データを取得できます。セキュリティ インデックスを有効にする手順については、「設定の同期の実行」（P.15-10）を参照してください。

Malicious Rogue Access Points

このダッシュレットには、[Malicious]（悪意あり）として分類された不正アクセス ポイントに関する情報が表示されます。表 3-1 では、危険性のない不正アクセス ポイントのパラメータについて説明します。これらの各パラメータについて、過去 1 時間および過去 24 時間に検出したアクセス ポイントに対する脅威または攻撃の回数と、現在まで合計が表示されます。いずれかの分類期間にある下線付きの数字をクリックすると、詳細情報のページが表示されます。

（注） 悪意のあるアクセス ポイントとは、システム内で検出される悪意のある信頼できないアクセス ポイントまたは未知のアクセス ポイントです。また、これらの分類には、ユーザが定義した Malicious ルールに合致したアクセス ポイント、または危険性のないアクセス ポイント分類から手動で移動したアクセス ポイントも含まれます。

表 3-1　悪意のある不正アクセス ポイントの詳細

フィールド	説明
Alert	アラート状態にある不正なアクセス ポイントの数を示します。 （注）　ネイバー リスト、またはユーザが定義する危険性のない AP リストに登録がないアクセス ポイントは、[Alert] 状態に分類されます。
Contained	封じ込められた不正アクセス ポイントの数を示します。
Threat	脅威を与える / 危険性の高い不正アクセス ポイントの数を示します。
Contained Pending	封じ込められた不正アクセス ポイントの保留の数を示します。 （注）　[Contained Pending] は、リソースを利用できないため、封じ込め処理が遅延していることを示しています。

Adhoc Rogues

[Adhoc Rogues] ダッシュレットには、過去 1 時間および過去 24 時間に発生した不正の件数と、アクティブな不正の合計数が表示されます。表 3-2 では、危険性のない不正アクセス ポイントのパラメータについて説明します。この任意の列にある数字をクリックすると、詳細情報を含むページが表示されます。

（注）　コントローラが最初にスキャンを実行したタイミングでは、不正アドホック アクセス ポイントの状態は [Alert] と表示され、オペレーティング システムの ID を確認中の場合は [Pending] と表示されます。

表 3-2　Ad hoc Rogues

フィールド	説明
Alert	アラート状態にある不正アドホック アクセス ポイントの数を示します。 （注）　ネイバー リスト、またはユーザが定義する危険性のない AP リストに登録がないアクセス ポイントは、[Alert] 状態に分類されます。
Contained	封じ込められた不正アクセス ポイントの数を示します。
Threat	脅威を与える / 危険性の高い不正アクセス ポイントの数を示します。
Contained Pending	封じ込められた不正アクセス ポイントの保留の数を示します。 （注）　[Contained Pending] は、リソースを利用できないため、封じ込め処理が遅延していることを示しています。

CleanAir Security

このダッシュレットは、CleanAir セキュリティに関する情報を提供し、またワイヤレス ネットワークにおける過去 1 時間および過去 24 時間内のセキュリティ リスク デバイスの数と、アクティブなセキュリティ リスク デバイスの合計数に関する情報を提供します。

次の情報が表示されます。

- Severity
- [Failure Source]：アラーム検出デバイス
- Owner
- Date/Time
- Message
- Acknowledged

セキュリティ リスク干渉に関する詳細については、「CleanAir セキュリティ アラームのモニタリング」（P.5-139）を参照してください。

未分類の不正アクセス ポイント

表 3-3 で、未分類の不正アクセス ポイント パラメータについて説明します。これらの各パラメータについて、過去 1 時間および過去 24 時間に検出したアクセス ポイントに対する脅威または攻撃の回数と、現在まで合計が表示されます。いずれかの分類期間にある下線付きの数字をクリックすると、詳細情報のページが表示されます。

（注） 未分類の不正アクセス ポイントとは、[Malicious]（危険性あり）または [Friendly]（危険性なし）のいずれにも分類されない不正アクセス ポイントです。これらのアクセス ポイントは封じ込め処理を行うことができ、また、危険性のない不正なアクセス ポイント リストへ手動で変更することもできます。

表 3-3　未分類の不正アクセス ポイント

フィールド	説明
Alert	アラート状態にある未分類のアクセス ポイントの数。コントローラで最初にスキャンすると、不正なアクセス ポイント無線が [Alert] と表示され、またオペレーティング システムの ID を確認中の場合は、[Pending] と表示されます。
Contained	封じ込められた未分類の不正アクセス ポイントの数。
Contained Pending	封じ込められた未分類の不正アクセス ポイントの保留の数。

危険性のない不正アクセス ポイント

このダッシュレットには、[Friendly]（危険性なし）として分類された不正アクセス ポイントに関する情報が表示されます。表 3-4 では、危険性のない不正アクセス ポイントのパラメータについて説明します。これらの各パラメータについて、過去 1 時間および過去 24 時間に検出したアクセス ポイントに対する脅威または攻撃の回数と、現在まで合計が表示されます。いずれかの分類期間にある下線付きの数字をクリックすると、詳細情報のページが表示されます。

（注）　危険性のない不正アクセス ポイントとは、既知のアクセス ポイント、認知済みアクセス ポイント、または信頼されたアクセス ポイントです。また、ユーザ定義の Friendly ルールと一致するアクセス ポイントを指します。危険性のない不正アクセス ポイントに対して封じ込め処理は実行できません。

表 3-4　危険性のない不正なアクセス ポイントの詳細

フィールド	説明
Alert	アラート状態にある不正なアクセス ポイントの数を示します。 （注）　ネイバー リスト、またはユーザが定義する危険性のない AP リストに登録がないアクセス ポイントは、[Alert] 状態に分類されます。
Internal	内部アクセス ポイント数を示します。 （注）　[Internal] とは、検出されたアクセス ポイントがネットワーク内にあり、手動で [Friendly - Internal] に設定されたことを示します。
External	外部アクセス ポイント数を示します。 （注）　[External] とは、検出されたアクセス ポイントがネットワーク外にあり、手動で [Friendly - External] に設定されたことを示します。

アクセス ポイントの脅威または攻撃

表 3-5 では、アクセス ポイントの脅威または攻撃のパラメータについて説明します。これらの各パラメータについて、過去 1 時間および過去 24 時間に検出したアクセス ポイントに対する脅威または攻撃の回数と、現在まで合計が表示されます。いずれかの分類期間にある下線付きの数字をクリックすると、詳細情報のページが表示されます。

表 3-5　AP Threats/Attacks

フィールド	説明
Fake AP Attacks	疑似攻撃数。
AP Missing	不明なアクセス ポイントの検出数。
AP Impersonation	アクセス ポイントのなりすまし数。
AP Invalid SSID	無効なアクセス ポイント SSID 数。
AP Invalid Preamble	無効なアクセス ポイント プリアンブル数。
AP Invalid Encryption	無効なアクセス ポイント暗号化数。
AP Invalid Radio Policy	無効なアクセス ポイント無線ポリシー数。
Denial of Service (NAV related)	DoS（NAV 関連）要求数。
AP Detected Duplicate IP	IP アドレス重複を検出したアクセス ポイント数。

MFP Attacks

インフラストラクチャおよびクライアント MFP 攻撃に対して、過去 1 時間、過去 24 時間の発生件数、および現在までの合計件数が表示されます。いずれかの分類期間にある下線付きの数字をクリックすると、詳細情報のページが表示されます。

Attacks Detected

過去 1 時間および過去 24 時間の wIPS サービス拒否攻撃、wIPS セキュリティ ペネトレーション攻撃、およびカスタム シグニチャ攻撃の数、およびアクティブなこれらの各攻撃の合計数に関する値が提供されます。いずれかの分類期間にある下線付きの数字をクリックすると、詳細情報のページが表示されます。

Recent Rogue AP Alarms

不正アクセス ポイント アラームのうち、最新 5 件分を表示します。[Alarms] ページを表示するには、カッコ内の番号をクリックします。アラームの詳細を表示するには、[MAC Address] の下の項目をクリックします。

Recent Adhoc Rogue Alarm

アドホックの不正アラームのうち、最新 5 件分を表示します。[Alarms] ページを表示するには、カッコ内の番号をクリックします。アドホックの詳細を表示するには、[MAC Address] の下の項目をクリックします。

Most Recent Security Alarms

セキュリティ アラームのうち、最新 5 件分を表示します。[Alarms] ページを表示するには、カッコ内の番号をクリックします。

不正アクセス ポイント、アドホック イベント、およびクライアント

この項では、不正なデバイスに対するセキュリティ ソリューションについて説明します。不正なデバイスとは、ネットワーク内で管理対象のアクセス ポイントによって検出される、未知（管理対象外）のアクセス ポイントまたはクライアントのことです。

コントローラは、すべての近隣のアクセス ポイントを継続的にモニタし、不正なアクセス ポイントおよびクライアントに関する情報を自動的に検出して収集します。コントローラで不正なアクセス ポイントが検出されると、不正ロケーション検出プロトコル（RLDP）を使用して、不正なアクセス ポイントがネットワークに接続されているかどうかが判定されます。

（注）　Prime Infrastructure は、コントローラのすべての不正アクセス ポイント データを集約します。

管理者は、すべてのアクセス ポイント上、もしくはモニタ モード（受信専用）アクセス ポイント上でのみ、RLDP を使用するようコントローラを設定することが可能です。この後者のオプションでは、輻輳している RF 空間での不正なアクセス ポイントを簡単に自動検出できるようになります。そして、不要な干渉を生じさせたり、通常のデータ アクセス ポイント機能に影響を与えたりすることなく、モニ

タリングを行えるようになります。すべてのアクセス ポイントで RLDP を使用するようにコントローラを設定した場合、モニタ モード アクセス ポイントとローカル（データ）通信用アクセス ポイントの両方が近くにあると、コントローラは常に RLDP 処理用アクセス ポイントとして、モニタ モード アクセス ポイントを選択します。ネットワーク上に不正があると RLDP で判断された場合は、検出された不正を手動で封じ込め処理を行うことも、自動的に封じ込め処理を行うこともできます。

ここでは、次の内容について説明します。

- 「不正なアクセス ポイントの分類」（P.3-10）
- 「不正アクセス ポイントの分類タイプ」（P.3-11）
- 「アドホックの不正」（P.3-13）

不正なアクセス ポイントの分類

不正なアクセス ポイントの分類および報告は、不正の状態と、不正なアクセス ポイントの状態を自動的に移行できるようにする、ユーザ定義の分類規則に従って行われます。コントローラに対し、不正なアクセス ポイントを Friendly、Malicious、または Unclassified に分類して表示させる各種ルールを作成できます。

（注）　Prime Infrastructure は、コントローラのすべての不正アクセス ポイント データを集約します。

デフォルトでは、いずれの分類ルールも有効になっていません。したがって、すべての未知（管理対象外）のアクセス ポイントは Unclassified に分類されます。ルールを作成し、その条件を設定して、ルールを有効にすると、未分類のアクセス ポイントは分類し直されます。ルールを変更するたびに、Alert 状態にあるすべてのアクセス ポイント（Friendly、Malicious、および Unclassified）にそのルールが適用されます。

（注）　ルール ベースの分類は、アドホック不正クライアントおよび不正クライアントには適用されません。

（注）　5500 シリーズ コントローラは最大で 2000 個の不正（認知済みの不正情報含め）に対応します。4400 シリーズ コントローラ、Cisco WiSM、および Catalyst 3750G 統合型無線 LAN コントローラ スイッチは最大で 625 個の不正に対応します。2100 シリーズ コントローラおよびサービス統合型ルータのコントローラ ネットワーク モジュールは最大で 125 個の不正に対応します。各コントローラは、不正アクセス ポイントの封じ込めを無線チャンネルごとに 3 台（モニタ モード アクセス ポイントの場合、無線チャネルごとに 6 台）に制限します。

コントローラは、管理対象のアクセス ポイントの 1 つから不正レポートを受信すると、次のように応答します。

1. コントローラは未知（管理対象外）のアクセス ポイントが危険性のない MAC アドレスのリストに含まれているか確認します。そのリストに含まれている場合、コントローラはそのアクセス ポイントを Friendly として分類します。
2. 未知（管理対象外）のアクセス ポイントが危険性のない MAC アドレスのリストに含まれていない場合、コントローラは、不正状態の分類ルール適用処理を開始します。
3. 不正なアクセス ポイントが Malicious、Alert または Friendly、Internal または External にすでに分類されている場合は、コントローラはそのアクセス ポイントを自動的に分類しません。不正なアクセス ポイントがそれ以外に分類されており、Alert 状態にある場合に限り、コントローラはそのアクセス ポイントを自動的に分類し直します。

4. コントローラは、優先度の一番高いルールを適用します。不正なアクセス ポイントがルールで指定された条件に一致すると、コントローラはそのアクセス ポイントをルールに設定された分類タイプに基づいて分類します。
5. 不正なアクセス ポイントが設定されたルールのいずれにも一致しないと、コントローラはそのアクセス ポイントを Unclassified に分類します。
6. コントローラは、すべての不正なアクセス ポイントに対して上記の手順を繰り返します。
7. 不正なアクセス ポイントが社内ネットワーク上にあると RLDP で判断されると、ルールが設定されていない場合でも、コントローラは不正の状態を Threat とマークし、そのアクセス ポイントを自動的に Malicious に分類します。その後、不正なアクセス ポイントに対して手動で封じ込め処理を行うことができますが（不正を自動的に封じ込めるよう RLDP が設定されていない限り）、その場合は不正の状態が Contained に変更されます。不正なアクセス ポイントがネットワーク上にないと、コントローラによって不正の状態が Alert とマークされ、そのアクセス ポイントを手動で封じ込め処理を行うことができるようになります。
8. 必要に応じて、各アクセス ポイントを本来とは異なる分類タイプや不正の状態に手動で変更することも可能です。

前述のように、コントローラでは、ユーザ定義のルールに基づいて未知（管理対象外）のアクセス ポイントの分類タイプと不正の状態が自動的に変更されます。もしくは、未知（管理対象外）のアクセス ポイントを本来とは異なる分類タイプと不正の状態に手動で変更することができます。表 3-6 に、未知（管理対象外）のアクセス ポイントに設定できる分類タイプや不正の状態の推移の組み合わせを示します。

表 3-6　設定可能な分類タイプ/不正の状態の推移

推移前	推移後
Friendly（Internal、External、Alert）	Malicious（Alert）
Friendly（Internal、External、Alert）	Unclassified（Alert）
Friendly（Alert）	Friendly（Internal、External）
Malicious（Alert、Threat）	Friendly（Internal、External）
Malicious（Contained、Contained Pending）	Malicious（Alert）
Unclassified（Alert、Threat）	Friendly（Internal、External）
Unclassified（Contained、Contained Pending）	Unclassified（Alert）
Unclassified（Alert）	Malicious（Alert）

不正の状態が Contained の場合、不正なアクセス ポイントの分類タイプを変更する前に、そのアクセス ポイントが封じ込められないようにする必要があります。不正なアクセス ポイントを Malicious から Unclassified に変更する場合は、そのアクセス ポイントを削除して、コントローラで分類し直せるようにする必要があります。

不正アクセス ポイントの分類タイプ

不正アクセス ポイントの分類タイプには次のものがあります。

- Malicious：システム内で検出されているが、悪意のある、信頼できない、または未知（管理対象外）のアクセス ポイント。また、これらの分類には、ユーザが定義した Malicious ルールに合致したアクセス ポイント、または危険性のないアクセス ポイント分類から手動で移動したアクセス ポイントも含まれます。詳細については、「Malicious Rogue Access Points」（P.3-5）を参照してください。

- Friendly：既知、認知済み、または信頼されたアクセス ポイント。また、ユーザ定義の Friendly ルールと一致するアクセス ポイントを指します。危険性のない不正アクセス ポイントに対して封じ込め処理は実行できません。詳細については、「危険性のない不正アクセス ポイント」（P.3-12）を参照してください。危険性のないアクセス ポイントのルールを設定するときの詳細については、「危険性のないアクセス ポイント テンプレートの設定」（P.11-79）を参照してください。
- Unclassified：Malicious または Friendly のいずれにも分類されない不正アクセス ポイントです。これらのアクセス ポイントは封じ込め処理を行うことができ、また、危険性のない不正なアクセス ポイント リストへ手動で変更することもできます。詳細については、「未分類の不正アクセス ポイント」（P.3-13）を参照してください。

悪意のある不正アクセス ポイント

悪意のある不正アクセス ポイントとは、システム内で検出される悪意のある信頼できないアクセス ポイントまたは未知（管理対象外）のアクセス ポイントです。また、これらの分類には、ユーザが定義した Malicious ルールに合致したアクセス ポイント、または危険性のないアクセス ポイント分類から手動で移動したアクセス ポイントも含まれます。

Prime Infrastructure ホーム ページの [Security] ダッシュボードには、過去 1 時間および過去 24 時間の各状態の悪意のある不正アクセス ポイントの数と、アクティブな悪意のある不正アクセス ポイントの総数が表示されます。

悪意のある不正アクセス ポイントの状態には次のものがあります。

- Alert：該当アクセス ポイントがネイバー リストまたはユーザ設定の [Friendly AP] リストにないことを示します。
- Contained：未知（管理対象外）のアクセス ポイントが封じ込められています。
- Threat：未知（管理対象外）のアクセス ポイントがネットワーク上に発見され、WLAN のセキュリティに脅威を与えています。
- Contained Pending：リソースを利用できないため、封じ込め処理が遅延することを示します。
- Removed：この未知（管理対象外）のアクセス ポイントは以前検出されたものの、現在は見つかりません。

悪意のある不正アクセス ポイントに関する詳細な情報を表示するには、いずれかの期間のカテゴリにある下線付きの数値をクリックします。詳細については、「不正アクセス ポイントのモニタリング」（P.5-88）を参照してください。

危険性のない不正アクセス ポイント

危険性のない不正アクセス ポイントとは、既知のアクセス ポイント、認知済みアクセス ポイント、または信頼されたアクセス ポイントです。また、ユーザ定義の Friendly ルールと一致するアクセス ポイントを指します。危険性のない不正アクセス ポイントに対して封じ込め処理は実行できません。

Prime Infrastructure ホーム ページの [Security] ダッシュボードには、過去 1 時間および過去 24 時間の各状態の危険性のない不正アクセス ポイントの数と、アクティブな危険性のない不正アクセス ポイントの総数が表示されます。

危険性のない不正アクセス ポイントの状態には次のものがあります。

- Internal：未知（管理対象外）のアクセス ポイントがネットワーク内に存在し、WLAN のセキュリティに脅威を与えない場合、手動で Friendly、Internal に設定します。たとえば、ラボ ネットワーク内のアクセス ポイントなどです。
- External：未知（管理対象外）のアクセス ポイントがネットワーク外に存在し、WLAN のセキュリティに脅威を与えない場合、手動で Friendly、External に設定します。たとえば、近所のコーヒーショップ設置されているアクセス ポイントなどです。

- Alert：未知（管理対象外）のアクセス ポイントはネイバー リストにもユーザ設定の [Friendly AP] リストにもありません。

危険性のない不正アクセス ポイントの詳細を参照するには、いずれかの分類期間にある下線付きの数字をクリックします。詳細については、「不正アクセス ポイントのモニタリング」（P.5-88）を参照してください。

未分類の不正アクセス ポイント

未分類の不正アクセス ポイントとは、[Malicious]（危険性あり）または [Friendly]（危険性なし）のいずれにも分類されない不正アクセス ポイントです。これらのアクセス ポイントは封じ込め処理を行うことができ、また、危険性のない不正なアクセス ポイント リストへ手動で変更することもできます。

Prime Infrastructure ホーム ページの [Security] ダッシュボードには、過去 1 時間および過去 24 時間の各状態の未分類の不正アクセス ポイントの数と、アクティブな未分類の不正アクセス ポイントの総数が表示されます。

未分類の不正アクセス ポイントの状態には次のものがあります。

- Pending：最初の検出で、未知（管理対象外）のアクセス ポイントは 3 分間 Pending 状態に置かれます。この間に、管理対象のアクセス ポイントでは、未知（管理対象外）のアクセス ポイントがネイバー アクセス ポイントであるかどうかが判定されます。
- Alert：未知（管理対象外）のアクセス ポイントはネイバー リストにもユーザ設定の [Friendly AP] リストにもありません。
- Contained：未知（管理対象外）のアクセス ポイントが封じ込められています。
- Contained Pending：未知（管理対象外）のアクセス ポイントが Contained とマークされましたが、リソースを使用できないため対処が遅れています。

詳細情報を参照するには、いずれかの分類期間にある下線付きの数字をクリックします。「不正アクセス ポイントのモニタリング」（P.5-88）を参照してください。

アドホックの不正

アドホック ネットワークで動作しているモバイル クライアントの MAC アドレスが許可された MAC アドレスのリストにない場合は、アドホックの不正であると識別されます。

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

Prime Infrastructure 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）。
- 未知（管理対象外）の不正アクセス ポイントが削除または認知されるまでモニタします。
- 最も近い場所の許可済みアクセス 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認知します。
  - 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 ポイントが排除または認知されるまで、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。

ここでは、次の内容について説明します。

- 「ネットワーク上のアクセス ポイントの検出」（P.3-14）
- 「コントローラ別不正アクセス ポイントの表示」（P.3-15）

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] 詳細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、「検索機能の使用方法」（P.2-37）を参照してください。
- Prime Infrastructure ホームページで、[Security] ダッシュボードをクリックします。このページには、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。
- ダッシュレットにある [Malicious AP] を示す数字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、[View AP 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
- 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）。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。

コントローラ別不正アクセス ポイントの表示

アクセス ポイント検出機能を使用すると、コントローラ別に不正アクセス ポイントに関する情報を表示できます。

[Rogue AP Alarms] 詳細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、「検索機能の使用方法」（P.2-37）を参照してください。
- Prime Infrastructure ホームページで、[Security] ダッシュボードをクリックします。このページには、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。
- ダッシュレットにある [Malicious AP] を示す数字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、[View AP Details by Controller] 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。

- Controller IP Address
- Detecting AP Name
- Radio
- 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）。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 ポイントがブロードキャストしているチャネル。
- [RSSI]：受信信号強度インジケータ（dBm）。

- [Classification]：不正 AP の分類を示します。
- [State]：アラームの状態を示します。可能な状態は、不正アクセス ポイントの分類タイプによって異なります。追加情報については、「不正アクセス ポイントの分類タイプ」（P.3-11）を参照してください。
- [On Network]：このネットワークに属しているかどうかで、「Yes」または「No」です。
- [Containment Level]：不正アクセス ポイントの封じ込め処理レベル、または Unassigned（封じ込めなし）を示します。
- Last Updated Time

アラームの処理

Prime Infrastructure を使用し、アクセス ポイントおよびモビリティ サービス エンジン上で、アラームとイベントを表示、割り当て、クリアできます。

アラームの電子メール通知を受信する方法の詳細についても説明します。ここでは、次の内容について説明します。

- 「アラームの割り当てと割り当て解除」（P.3-16）
- 「アラームの削除とクリア」（P.3-16）
- 「アラームの認知」（P.3-17）

アラームの割り当てと割り当て解除

自分にアラームを割り当てたり割り当て解除したりするには、次の手順を実行します。

ステップ 1　アクセス ポイント アラームについて高度な検索を実行します。詳細については、「検索機能の使用方法」（P.2-37）を参照してください。

ステップ 2　対応するチェックボックスをオンにすることで、自分に割り当てるアラームを選択します。

（注）　自分に割り当てられているアラームを割り当て解除するには、該当アラームの隣にあるボックスをオフにします。他の人に割り当てられているアラームの割り当ては解除できません。

ステップ 3　[Select a command] ドロップダウン リストから、[Assign to Me]（または [Unassign]）を選択し、[Go] をクリックします。

[Assign to Me] を選択した場合、自分のユーザ名が [Owner] 欄に表示されます。[Unassign] を選択した場合、ユーザ名の欄は空白になります。

アラームの削除とクリア

モビリティ サービス エンジンからアラームを削除またはクリアするには、次の手順を実行します。

ステップ 1　[Monitor] > [Alarms] ページで、対応するチェックボックスをオンにして、削除またはクリアするアラームを選択します。

（注）　アラームを削除すると、アラームは Prime Infrastructure によってデータベースから削除されます。アラームをクリアすると、アラームは Prime Infrastructure データベースには残りますが、[Clear] 状態になります。アラームは、その原因となった状況が存在しなくなったときにクリアします。

ステップ 2　[Select a command] ドロップダウン リストから、[Delete] または [Clear] を選択し、[Go] をクリックします。

（注）　古いアラームとクリアされたアラームのクリーンアップを設定するには、[Administration] > [Settings] > [Alarms] の順に選択します。

アラームの認知

状況によっては、特定のアラームを [Alarms] リストから削除した方がよい場合があります。たとえば、802.11g インターフェイス上で特定のアクセス ポイントから干渉アラームを継続的に受信している場合は、ページまたはその他のアラーム リストで、そのアクセス ポイントがアクティブなアラームとしてカウントされないように設定しておくと便利です。そのためには、[Alarms] リストで 802.11g インターフェイスのアラームを探し、チェックボックスをオンにして、[Select a command] ドロップダウン リストから [Acknowledge] を選択します。

これで、そのアクセス ポイントが同じインターフェイスで新しい違反を検出しても、Prime Infrastructure によって新しいアラームが生成されず、ページにも新しいアラームが表示されません。ただし、802.11a など別のインターフェイス上では干渉違反が検出され、新しいアラームが生成されます。

一度認知したすべてのアラームは、ページ上にも、アラーム リスト ページにも表示されません。さらに、アラームを認知済みとしてマークした場合は、電子メールも生成されません。デフォルトでは、認知済みアラームは検索対象となりません。このデフォルトを変更するには、[Administration] > [Settings] > [Alarms] ページを選択し、[Hide Acknowledged Alarms] 設定を無効にします。

（注）　アラームを認知すると、この機能を無効にしない限り、問題が再度発生しても別のアラームが生成されない旨の注意を促すために、警告が表示されます。この警告メッセージを無効にするには、[Administration] > [User Preferences] ページを使用します。

また、以前の認知済みアラームをすべて検索して、過去 7 日間に認知されたアラームを表示することもできます。Prime Infrastructure は、7 日以上経過した解除済みアラートを自動的に削除するため、検索結果として表示されるのは最近 7 日間のアクティビティのみです。既存のアラームが削除されるまで、Prime Infrastructure がすでにアラームを生成している管理対象エンティティに対して新しいアラームを生成できません。

不正アラーム イベントのモニタリング

[Events] 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。Prime Infrastructure では、不正アクセス ポイントが検出されるか、不正アクセス ポイントが手動で変更（状態の変更など）された場合に、イベントが生成されます。[Rogue AP Events] リスト ページには、すべての不正アクセス ポイント イベントが表示されます。

[Rogue AP Events] リスト 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　次のいずれかを実行します。

- Prime Infrastructure の Advanced Search 機能を使用して不正アクセス ポイント イベントを検索します。詳細については、「検索機能の使用方法」（P.2-37）を参照してください。
- [Rogue AP Alarms] 詳細ページで [Select a command] ドロップダウン リストから [Event History] を選択します。

ステップ 2　[Rogue AP Events] リスト ページには、次のイベント情報が表示されます。

- [Severity]：アラームの重大度を示します。
- [Rogue MAC Address]：[Rogue AP Event Details] ページを表示するには、不正な MAC アドレスをクリックします。詳細については、「不正 AP イベントの詳細の表示」（P.3-18）を参照してください。
- [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、Friendly、Unclassified。詳細については、「不正アクセス ポイントの分類タイプ」（P.3-11）を参照してください。
- [On Network]：不正が検出された方法を示します。
  - [Controller]：コントローラが不正を検出しました（Yes または No）。
  - [Switch Port Trace]：不正がスイッチ ポート トレースによって検出されました。[Traced but not found]、[Traced and found]、[Not traced] のいずれかで示されます。
- [Radio Type]：この不正アクセス ポイントに適用されるすべての無線タイプをリストします。
- [Date/Time]：イベントが生成された日時。
- [State]：アラームの状態を示します。可能な状態は、不正アクセス ポイントの分類タイプによって異なります。追加情報については、「不正アクセス ポイントの分類タイプ」（P.3-11）を参照してください。
- [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。

不正 AP イベントの詳細の表示

不正アクセス ポイント イベントの詳細を表示するには、次の手順を実行します。

ステップ 1　[Rogue AP Events] リスト ページで、[Rogue MAC Address] リンクをクリックします。

ステップ 2　[Rogue AP Events Details] ページに、次の情報が表示されます。

- Rogue MAC Address
- [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]：不正が検出された方法を示します。
  - [Controller]：コントローラが不正を検出しました（Yes または No）。
  - [Switch Port Trace]：不正がスイッチ ポート トレースによって検出されました。[Traced but not found]、[Traced and found]、[Not traced] のいずれかで示されます。
- [Classification Type]：Malicious、Friendly、Unclassified。詳細については、「不正アクセス ポイントの分類タイプ」（P.3-11）を参照してください。

- [State]：アラームの状態を示します。可能な状態は、不正アクセス ポイントの分類タイプによって異なります。追加情報については、「不正アクセス ポイントの分類タイプ」（P.3-11）を参照してください。
- [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 ポイントがブロードキャストしているチャネル。
- [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 ポイントに適用されるすべての無線タイプをリストします。
- [Created]：イベントが生成された日時。
- [Generated By]：イベントの生成方法（コントローラなど）。
- デバイスの IP アドレス
- [Severity]：アラームの重大度を示します。
- [Message]：現在のイベントの詳細を示します。

アドホック不正イベントのモニタリング

[Events] ページでは、アドホック不正イベントに関する情報を参照できます。アドホック不正が検出されるか、アドホック不正を手動で変更した場合（その状態を変更するなど）、Prime Infrastructure によりイベントが生成されます。[Adhoc Rogue Events] リスト ページには、すべてのアドホック不正イベントが表示されます。

[Rogue AP Events] リスト 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　次のいずれかを実行します。

- Prime Infrastructure の Advanced Search 機能を使用してアドホック不正イベントを検索します。詳細については、「検索機能の使用方法」（P.2-37）を参照してください。
- [Adhoc Rogue Alarms] 詳細ページで [Select a command] ドロップダウン リストから [Event History] を選択します。

ステップ 2　[Rogue AP Events] リスト ページには、次のイベント情報が表示されます。

- [Severity]：アラームの重大度を示します。
- [Rogue MAC Address]：[Rogue AP Event Details] ページを表示するには、不正な MAC アドレスをクリックします。詳細については、「アドホック不正 AP イベントの詳細の表示」（P.3-20）を参照してください。
- [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]：不正が検出された方法を示します。
  - [Controller]：コントローラが不正を検出しました（Yes または No）。
  - [Switch Port Trace]：不正がスイッチ ポート トレースによって検出されました。[Traced but not found]、[Traced and found]、[Not traced] のいずれかで示されます。
- [Radio Type]：この不正アクセス ポイントに適用されるすべての無線タイプをリストします。
- [Date/Time]：イベントが生成された日時。

- [State]：アラームの状態を示します。アドホック不正の可能な状態には、[Threat]、[Alert]、[Internal]、[External]、[Contained]、[Contained Pending]、および [Removed] があります。
- [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。

アドホック不正 AP イベントの詳細の表示

不正アクセス ポイント イベントの詳細を表示するには、次の手順を実行します。

ステップ 1　[Rogue AP Events] リスト ページで、[Rogue MAC Address] リンクをクリックします。

ステップ 2　[Rogue AP Events Details] ページに、次の情報が表示されます。

- Rogue MAC Address
- [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]：不正が検出された方法を示します。
  - [Controller]：コントローラが不正を検出しました（Yes または No）。
  - [Switch Port Trace]：不正がスイッチ ポート トレースによって検出されました。[Traced but not found]、[Traced and found]、[Not traced] のいずれかで示されます。
- [State]：アラームの状態を示します。アドホック不正の可能な状態には、[Threat]、[Alert]、[Internal]、[External]、[Contained]、[Contained Pending]、および [Removed] があります。
- [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 ポイントがブロードキャストしているチャネル。
- [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 ポイントに適用されるすべての無線タイプをリストします。
- [Created]：イベントが生成された日時。
- [Generated By]：イベントの生成方法（コントローラなど）。
- デバイスの IP アドレス
- [Severity]：アラームの重大度を示します。
- [Message]：現在のイベントの詳細を示します。

セキュリティの概要

Prime Infrastructure は、IT 管理者が一元化された場所から企業の無線ネットワークを設計、制御、保護、モニタできる、基礎になります。

Prime Infrastructure には、Cisco ワイヤレス ネットワーク インフラで、ワイヤレス セキュリティの設定とポリシーを管理および適用するための、次のツールが用意されています。

- ユーザ認証、暗号化、アクセス制御などのネットワーク セキュリティ ポリシーの作成と施行。

- ワイヤレス インフラストラクチャのセキュリティ設定。
- 不正 AP の検出、位置検知、封じ込め。
- ワイヤレス侵入防御システム（wIPS）。
- ワイヤレス IPS のシグニチャの修正と管理。
- 管理フレーム保護（MFP）。
- 無許可または悪意のあるワイヤレス ユーザ アクティビティのモニタリングと緩和措置のための Cisco 有線ネットワーク IPS とのコラボレーション。
- 包括的なセキュリティ イベント管理およびレポート機能。

セキュリティ脆弱性アセスメント

Cisco Unified Wireless Network バージョン 5.1 では、自動化されたセキュリティ脆弱性アセスメントを使用でき、企業の全体的なワイヤレス セキュリティ ポスチャを解析しやすくなるだけでなく、WLAN オペレータは、業界のベスト プラクティスを基準として、自社のセキュリティ サービス設定をリアルタイムで評価できます。自動化されたセキュリティ脆弱性アセスメントにより以下が提供されます。

- ワイヤレス ネットワーク全体の予防的な脆弱性モニタリング。
- データ損失、ネットワークへの侵入、または悪意のある攻撃を招くおそれのあるセキュリティの脆弱性に関する包括的な情報。
- ワイヤレス セキュリティ ポスチャの弱点の分析と是正に必要な時間と専門知識の削減。

自動化されたワイヤレス脆弱性アセスメントでは、ワイヤレス ネットワーク全体のセキュリティ ポスチャを脆弱性について監査します。これらの脆弱性は、次のような結果につながる可能性があります。

- 無許可の管理アクセス、または管理プロトコルを使用したネットワークの侵害またはネットワークへの悪影響。
- 無許可のネットワーク アクセス、データ漏えい、中間者攻撃、またはリプレイ アタック。
- サービス拒否（DoS）攻撃など、ネットワーク プロトコルとサービスの操作を介した、ネットワークへの侵害またはネットワークへの悪影響。

Prime Infrastructure では、ネットワーク全体が自動的にスキャンされ、その設定が、シスコが推奨するワイヤレス セキュリティ設定および業界のベスト プラクティスのワイヤレス セキュリティ設定と自動的に比較されます。Prime Infrastructure の自動化されたワイヤレス セキュリティ アセスメント機能では、Wireless LAN Controller、アクセス ポイント、およびネットワーク管理インターフェイスをスキャンして、設定、暗号化、ユーザ認証、インフラストラクチャ認証ネットワーク管理、およびアクセス制御における脆弱性を確認します。

ワイヤレス ネットワーク セキュリティのステータスは、ワイヤレス ネットワーク管理者がセキュリティ イベントをダッシュボードで簡単に参照できるよう、グラフィカルに表示されます。Prime Infrastructure では、Prime Infrastructure セキュリティ ダッシュボードに、セキュリティ インデックスを介して脆弱性評価の結果が表示されます。セキュリティ インデックスでは、単一の合成セキュリティ スコアと、優先度を付けた脆弱性のサマリーによって、ネットワーク セキュリティ ポスチャを要約しています。詳細については、「セキュリティ インデックス」（P.3-22）を参照してください。

セキュリティ サマリーに含まれているイベントについて詳細を調査する必要がある場合、管理者は、Security Index Detailed レポートにドリルダウンできます。Security Index Detailed レポートには、ネットワークをまたがる脆弱性の綿密な解析が含まれています。最適なセキュリティ設定の内容と、脆弱性を是正するために推奨される変更点も含まれています。管理者の行うすべての変更は、セキュリティ インデックス スコアを更新して反映されます。詳細については、「Security Index Detailed レポート」（P.3-22）を参照してください。

セキュリティ インデックス

セキュリティ インデックスは Prime Infrastructure 管理ネットワークのセキュリティの目安になります。セキュリティ インデックスは、さまざまなセキュリティ設定に重みを割り当てることで計算され、視覚的に表示されます。統合される重みの範囲は 0 ～ 100 です。0 は最も安全でないことを示し、100 は最も安全であることを示します。

重みは、Prime Infrastructure 内で保持されている、セキュリティ設定と紐付くコントローラおよび Location Server/Mobility Service Engine の中で、最もスコアの低いものから導き出されます。たとえば、Prime Infrastructure 管理ネットワークのセキュリティ インデックスは、最低スコアのコントローラと最低スコアの Location Service/Mobility Service Engine を加算した値と同等です。

セキュリティ インデックスには、次の配色が適用されます。

- 80 以上：緑色
- 60 以上 80 未満：黄色
- 60 未満：赤色

（注）　ゲスト WLAN は、スコアリング対象の WLAN から除外されます。Web 認証または Web パススルーが有効な WLAN は、ゲスト WLAN として識別されます。

最新リリースにおけるセキュリティ インデックスは、必要とされるセキュリティ設定に対する基準となります。たとえば、以前のバージョンのコードに AES 暗号化がない場合、AES 暗号化のセキュリティ設定に関連する数値分インデックスが減少します。同様に、新しい設定が行われると、重みが変わります。

Prime Infrastructure で Refresh from Controller コマンドが実行されない場合、Prime Infrastructure に保存されている設定は、コントローラの設定を反映した最新の情報でないことがあります。設定の同期タスクでセキュリティ インデックスの計算を実行し、すべてのコントローラから最新の設定データを取得できます。

主なセキュリティ問題

[Top Security Issues] セクションには、セキュリティ上の問題の上位 5 件が表示されます。[View All] と [Devices] のリンクは、関連する列を並べ替え、すべてのコントローラで発生したセキュリティ上の問題に関するレポートを表示します。Security Index Detailed レポートを開くには、[View All] をクリックします。Security Index Controller レポートを表示するには [Devices] をクリックします。

- 「Security Index Detailed レポート」（P.3-22）
- 「Security Index Controller レポート」（P.3-23）
- 「潜在的なセキュリティ問題」（P.3-23）

Security Index Detailed レポート

Security Index Detailed レポートには、すべてのコントローラ、ロケーション サーバ、およびモビリティ サービス エンジンをまたがって見つかった、すべてのセキュリティ上の問題が表示されます。デバイスから取得された特定のセキュリティ設定で検出された問題について、詳細に説明されています。特定の問題が認知された場合（アラームと同様）、設定の同期タスクが次回実行されるとき、この問題は無視されます（セキュリティ インデックスの計算が有効である場合）。

認知済みの問題があり、設定の同期タスクの次回実行時にこの問題が無視される一部のケースでは、最終的なセキュリティ インデックス スコアは変更されません。この事象には、次のような原因が考えられます。

- 認知済みの問題は、セキュリティ インデックス スコアに直接影響していないコントローラ（たとえば、最低スコア以外のコントローラ）に関連しています。
- 認知済みの問題は、セキュリティ インデックス スコアに直接影響していない WLAN に関連しています。最低スコアのコントローラの最低スコアの WLAN のみが、セキュリティ インデックス スコアに影響します。

コントローラ上で SSH と Telnet が有効化されており、このいずれも問題としてフラグ付けされている場合は、Telnet の問題の方が SSH の問題よりも優先されます。スコアが最も低いコントローラで SSH が認知されていても、セキュリティ インデックスに変化はありません。

すべてのセキュリティ上の問題（認知済みと未認知の両方）を表示するには、[Select a command] ドロップダウン リストから、[Show All] を選択します。未認知のセキュリティ上の問題のみを表示するには、[Show Unacknowledged] を選択します。これは、[Security Summary] ページから [View All] を選択した場合のデフォルト表示です。認知済みのセキュリティ上の問題のみを表示するには、[Show Acknowledged] を選択します。

（注） ユーザによるセキュリティ上の問題の認知または未認知のために、ユーザは「Ack and Unack Security Index Issues」権限を有効にしておく必要があります。

Security Index Controller レポート

このページには、セキュリティ違反のレポートが各コントローラの概要として表示されます。行ごとに、コントローラに発生したセキュリティ問題の数が表示され、すべてのセキュリティ問題へのリンクが表示されます。

[Security Issues Count] 列の数値をクリックすると、Security Index Detailed レポートが表示されます。

潜在的なセキュリティ問題

表 3-7 および表 3-8 では、潜在的なセキュリティ問題について説明してあります。

表 3-7　潜在的なセキュリティ問題

コントローラのセキュリティ問題	問題となる理由	ソリューション
コントローラ上の WLAN SSID の認証方式が脆弱です。	WLAN 認証方式としては弱いため、WLAN パケットが傍受される場合にオンラインで使用できるツールを使用して突破することができます。	最も安全な認証方式および WPA+WPA2 の方式を使用します。
コントローラ上の WLAN SSID に脆弱な認証方式（CKIP）が設定されています。	WLAN の認証方式としては弱くなります。	最も安全な認証方式および WPA+WPA2 の方式を使用します。
コントローラ上の WLAN SSID にユーザ認証が設定されていません。	認証方式を設定していないため、WLAN にセキュリティ上のリスクがあります。	WPA+WPA2 などの強い認証方式を設定します。

表 3-7　潜在的なセキュリティ問題 （続き）

コントローラのセキュリティ問題	問題となる理由	ソリューション
コントローラ上の WLAN SSID に脆弱な暗号化方式（CKIP WEP 40 ビット）が設定されています。	WLAN の暗号化方式としては弱くなります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。
コントローラ上の WLAN SSID に脆弱な暗号化方式（キー置換を含む CKIP WEP 40 ビット）が設定されています。	WLAN の暗号化方式としては弱くなります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。
コントローラ上の WLAN SSID に脆弱な暗号化方式（MMH を含む CKIP WEP 40 ビット）が設定されています。	WLAN の暗号化方式としては弱くなります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。
コントローラ上の WLAN SSID に脆弱な暗号化方式（MMH とキー置換を含む CKIP WEP 40 ビット）が設定されています。	WLAN の暗号化方式としては弱くなります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。
コントローラ上の WLAN SSID に脆弱な暗号化方式（WEP 104 ビット）が設定されています。	WLAN の暗号化方式としては弱くなります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。
コントローラ上の WLAN SSID に脆弱な暗号化方式（CKIP WEP 104 ビット）が設定されています。	WLAN の暗号化方式としては弱くなります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。
コントローラ上の WLAN SSID に脆弱な暗号化方式（MMH を含む CKIP WEP 104 ビット）が設定されています。	WLAN の暗号化方式としては弱くなります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。
コントローラ上の WLAN SSID に脆弱な暗号化方式（キー置換を含む CKIP WEP 104 ビット）が設定されています。	WLAN の暗号化方式としては弱くなります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。
コントローラ上の WLAN SSID に脆弱な暗号化方式（MMH とキー置換を含む CKIP WEP 104 ビット）が設定されています。	WLAN の暗号化方式としては弱くなります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。
コントローラ上の WLAN SSID に脆弱な暗号化方式（WEP 40 ビット）が設定されています。	WLAN の暗号化方式としては弱くなります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。
コントローラ上の WLAN SSID に脆弱な暗号化方式（WEP 128 ビット）が設定されています。	WLAN の暗号化方式としては弱くなります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。
コントローラ上の WLAN SSID に脆弱な暗号化方式（TKIP）が設定されています。	WLAN の暗号化方式としては弱くなります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。

表 3-7　潜在的なセキュリティ問題 （続き）

コントローラのセキュリティ問題	問題となる理由	ソリューション
コントローラ上の WLAN SSID に暗号化が設定されていません。	暗号化方式を設定していないため、WLAN に明確なセキュリティ上のリスクがあります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。
コントローラ上の WLAN SSID に脆弱な暗号化方式（WEP 104 ビット）が設定されています。	WLAN の暗号化方式としては弱くなります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。
コントローラ上の WLAN SSID にキー管理方式が設定されていません（WPA+WPA2 のみ該当）。	キー管理方式によって、キーのセキュリティが強化されます。キー管理方式を使用していない場合、WLAN は危険です。	CCKM などのキー管理方式を最低 1 つ設定します。
コントローラ上の WLAN SSID の MFP Client Protection に「Optional」が設定されています。	WLAN について MFP Client Protection がオプションに設定されると、認証済みクライアントがスプーフされたフレームから保護されない場合があります。	MFP Client Protection に「Required」を設定して、不正アクセス ポイントに接続しているクライアントから保護します。
コントローラ上の WLAN SSID の MFP Client Protection に「Disabled」が設定されています。	WLAN について MFP Client Protection が無効に設定されると、認証済みクライアントがスプーフされたフレームから保護されない場合があります。	MFP Client Protection に「Required」を設定して、不正アクセス ポイントに接続しているクライアントから保護します。
コントローラ上で WLAN SSID インターフェイスに「management」が設定されています。	SAFE から推奨されるように、ユーザ トラフィックは管理トラフィックと別にする必要があります。	コントローラ上で WLAN インターフェイスに「management」を設定することはできません。
WLAN について 1 を設定したインターフェイスは、VLAN です。	SAFE から推奨されるように、ユーザ トラフィックは VLAN トラフィックと別にする必要があります。	WLAN では、管理でなく、VLAN を含んでもいないインターフェイスに 1 を設定する必要があります。
コントローラ上の WLAN SSID で「Client Exclusion」が無効です。	Client Exclusion ポリシーが無効である場合、攻撃者は WLAN ネットワークへのアクセスを継続して試行できます。	「Client Exclusion」を有効にして、悪意のある WLAN クライアントの動作から保護します。
コントローラ上の WLAN SSID で「Broadcast SSID」が有効です。		「Broadcast SSID」を無効にして、ワイヤレス ネットワークを保護します。
コントローラ上の WLAN SSID で「MAC Filtering」が無効です。		「MAC Filtering」を有効にして、ワイヤレス ネットワークを保護します。

表 3-7　潜在的なセキュリティ問題 （続き）

コントローラのセキュリティ問題	問題となる理由	ソリューション
コントローラ上で [Protection Type] に「AP Authentication」が設定されています。	[AP Authentication] が設定されている場合、アクセス ポイントは、隣接するアクセス ポイントのビーコン/プローブ応答フレームをチェックして RF グループの情報要素（IE）と一致する認証された IE が含まれているかどうかを確認します。これによってある程度のセキュリティは確保されますが、一部の管理フレームは対象外であり、不正アクセス ポイントによる変更を受けてしまいます。	コントローラ上の [Protection Type] に「Management Frame Protection (MFP)」を設定します。
コントローラで [Protection Type] に「None」が設定されています。	802.11 管理メッセージのセキュリティがアクセス ポイントとクライアント間で受け渡されません。	コントローラ上の [Protection Type] に「Management Frame Protection (MFP)」を設定します。
無線の種類は、DCA チャネルでのみ不正を検出するように設定されています。	国またはすべてのチャネルのサブセットのみで不正検出を実行することは、国またはすべてのチャネルで実行することに比べて安全性が低くなります。	国チャネルまたはすべてのチャネルで不正を検出するように、無線の種類 802.11a/n および 802.11b/g/n を設定します。
無線の種類は、国チャネルと DCA チャネルのいずれの不正も検出するように設定されていません。	国チャネルと DCA チャネルのいずれでも不正検出を設定していない場合は、国またはすべてのチャネルで実施する場合に比べて安全性が低くなります。	国チャネルまたはすべてのチャネルで不正を検出するように、無線の種類 802.11a/n および 802.11b/g/n を設定します。
コントローラ上で、アドホック ネットワークを検出およびレポートする不正ポリシーが無効になっています。	アドホック ネットワークの検出およびレポートが無効である場合、アドホックの不正アクセス ポイントが検出されません。	アドホック ネットワークを検出およびレポートする不正ポリシーを有効にします。
コントローラ上で「すべての標準シグニチャおよびカスタム シグニチャのチェック」が無効になっています。	すべての標準シグニチャおよびカスタム シグニチャのチェックを無効にすると、受信 802.11 パケットのさまざまなタイプの攻撃が検出されないことがあります。	一部の標準シグニチャのみが無効な場合には、無効なシグニチャに関連する攻撃が検出されないことがあります。
一部の標準シグニチャがコントローラ上で無効です。	一部の標準シグニチャのみが無効な場合には、受信 802.11 パケットのさまざまなタイプの攻撃が検出されないことがあります。	コントローラですべての標準シグニチャを有効にします。

表 3-7　潜在的なセキュリティ問題 （続き）

コントローラのセキュリティ問題	問題となる理由	ソリューション
コントローラ上で「過剰な 802.11 のアソシエーションの失敗」によるクライアントの除外ポリシーが無効になっています。	アソシエーションの試みが過剰に失敗すると、システム リソースを消費して、インフラストラクチャに対する DoS 攻撃になることがあります。	コントローラ上で「過剰な 802.11 のアソシエーションの失敗」によるクライアントの除外ポリシーを有効にします。
コントローラ上で「過剰な 802.11 認証の失敗」によるクライアントの除外ポリシーが無効になっています。	認証の試みが過剰に失敗すると、システム リソースを消費して、インフラストラクチャに対する DoS 攻撃になることがあります。	コントローラ上で「過剰な 802.11 認証の失敗」によるクライアントの除外ポリシーを有効にします。
コントローラ上で「過剰な 802.1X 認証の失敗」によるクライアントの除外ポリシーが無効になっています。	802.1X 認証の試みが過剰に失敗すると、システム リソースを消費して、インフラストラクチャに対する DoS 攻撃になることがあります。	インフラストラクチャに対する DoS 攻撃を回避するには、過剰な 802.1X 認証の失敗によるクライアントの除外ポリシーを有効にする必要があります。
コントローラ上で「過剰な 802.11 Web 認証の失敗」によるクライアントの除外ポリシーが無効になっています。	802.11 Web の Web 認証の試みが過剰に失敗すると、システム リソースを消費して、インフラストラクチャに対する DoS 攻撃になることがあります。	コントローラ上で「過剰な 802.11 Web 認証の失敗」によるクライアントの除外ポリシーを有効にします。
コントローラ上で、「IP の盗難または IP の再使用」クライアント除外ポリシーが無効になっています。	IP の盗難または再使用のクライアントの除外ポリシーが無効である場合、別のクライアントになりすました攻撃者が禁止されなくなります。	コントローラ上で、「IP の盗難または IP の再使用」クライアント除外ポリシーを有効にします。
コントローラ上に CIDS センサーが設定されていません。	有効な IDS センサーが設定されていない場合、IP レベルの攻撃は通常は検出されません。	コントローラに 1 つ以上の CIDS センサーを設定します。
コントローラは、SNMP v1/v2 のデフォルト コミュニティ ストリングを使用して設定されています。	デフォルト コミュニティの SNMP V1 または V2 が設定されている場合、デフォルト コミュニティはよく知られているため、攻撃を受けやすくなります。	Auth タイプおよび Privacy タイプの SNMPv3 を使用します。
コントローラは、SNMP v1/v2 のデフォルトでないコミュニティ ストリングを使用して設定されています。	デフォルト コミュニティでない SNMP V1 または V2 はデフォルト コミュニティに比べてやや安全ですが、SNMP V3 に比べると安全ではありません。	Auth タイプおよび Privacy タイプの SNMPv3 を使用します。
コントローラ上で、SNMPv3 はデフォルト ユーザを使用して設定されています。	デフォルト ユーザを使用すると、SNMP V3 接続の安全性が低下します。	Auth タイプおよび Privacy タイプの SNMPv3 にデフォルト以外のユーザ名を使用します。
コントローラ上で SNMPv3 は Auth タイプも Privacy タイプも使用しないで設定されています。	Auth タイプまたは Privacy タイプの SNMP V3 が None に設定されている場合、SNMP V3 接続の安全性が低下します。	Auth タイプおよび Privacy タイプの SNMPv3 を使用して、ワイヤレス ネットワークを保護します。

表 3-7　潜在的なセキュリティ問題 （続き）

コントローラのセキュリティ問題	問題となる理由	ソリューション
コントローラ上で HTTP（Web モードは有効、セキュア Web モードは無効）が有効になっています。	HTTP は HTTPS に比べて安全性が低くなります。	コントローラ上で HTTPS（Web モードとセキュア Web モードの両方）を有効にします。
Telnet はコントローラ上で有効になっています。	Telnet が有効な場合、コントローラはハッキングされるリスクがあります。	コントローラ上の Telnet を無効にします。
コントローラ上で SSH は無効になっており、タイムアウト値はゼロに設定されています。	SSH が有効でタイムアウトが 0 に設定されている場合、コントローラはハッキングされるリスクがあります。	コントローラ上でゼロ以外のタイムアウト値を設定して SSH を有効にします。
Telnet は AP 上で有効になっています。	Telnet が有効な場合、アクセス ポイントはハッキングされるリスクがあります。	すべてのアクセス ポイントで Telnet を無効にします。
SSH は AP 上で有効になっています。		すべてのアクセス ポイントで SSH を無効にします。
AP の少なくとも 1 つが、デフォルト ユーザ名またはパスワードで設定されています。	デフォルトのパスワードが設定されている場合、アクセス ポイントはネットワーク外部からの接続により影響を受けやすくなります。	コントローラにアソシエートされているすべてのアクセス ポイントに、デフォルト以外のユーザ名および強度が高いパスワードを設定します。

表 3-8　潜在的なセキュリティ問題

ロケーション サーバ/モビリティ サーバ エンジンのセキュリティ問題	問題となる理由	ソリューション
HTTP がロケーション サーバ上で有効です。	HTTP は HTTPS に比べて安全性が低くなります。	ロケーション サーバ上で HTTPS を有効にします。
ロケーション サーバのユーザにデフォルトのパスワードが設定されています。	デフォルトのパスワードが設定されている場合、ロケーション サーバ/モビリティ サーバ エンジンはネットワーク外部からの接続により影響を受けやすくなります。	ロケーション サーバのユーザに強度が高いパスワードを設定します。
HTTP がモビリティ サービス エンジン上で有効です。	HTTP は HTTPS に比べて安全性が低くなります。	モビリティ サービス エンジン上で HTTPS を有効にします。

表 3-8　潜在的なセキュリティ問題 （続き）

ロケーション サーバ/モビリティ サーバ エンジンのセキュリティ問題	問題となる理由	ソリューション
モビリティ サービス エンジンのユーザにデフォルトのパスワードが設定されています。	デフォルトのパスワードが設定されている場合、ロケーション サーバ/モビリティ サーバ エンジンはネットワーク外部からの接続により影響を受けやすくなります。	モビリティ サービス エンジン上のユーザに、強度が高いパスワードを設定します。
wIPS サービスがモビリティ サービス エンジン上で有効ではありません。	ネットワークは、高度なセキュリティ上の脅威に対して脆弱です。	wIPS サービスを展開して、高度なセキュリティ上の脅威からネットワークを保護します。

スイッチ ポート トレース

現在、Prime Infrastructure では、コントローラから情報を取得することによって、不正アクセス ポイントを検出できます。不正アクセス ポイント表には、ネイバー リストにないフレームから検出された BSSID アドレスが記載されています。指定された期間の終わりに、不正アクセス ポイント表の内容が、CAPWAP Rogue AP Report メッセージでコントローラに送信されます。この方法を使用した場合、Prime Infrastructure では、そのまま、コントローラから受信した情報を収集します。一方、ソフトウェア リリース 5.1 では、有線の不正アクセス ポイントのスイッチ ポートに関するスイッチ ポート トレーシングを組み込むことができます。この機能拡張により、検出された不正なアクセス ポイントに対応し、今後発生する攻撃を回避できます。トレース情報は不正アクセス ポイントの Prime Infrastructure ログだけで使用でき、不正クライアントのログには使用できません。

（注）　不正アクセス ポイントに接続した不正クライアントの情報を使用して、ネットワークで不正アクセス ポイントに接続したスイッチ ポートを追跡します。

（注）　危険性のない不正アクセス ポイントまたは削除された不正アクセス ポイントにトレーシングを設定しようとすると、警告メッセージが表示されます。

（注）　スイッチ ポート トレーシングで、SNMP v3 を使用してスイッチ ポートを正常にトレースするには、すべての OID を SNMP v3 のビューに含める必要があり、SNMP v3 グループ内の VLAN ごとに VLAN の内容を作成する必要があります。

スイッチ ポート トレーシングの確立

スイッチ ポート トレーシングを確立するには、次の手順に従ってください。

ステップ 1　Prime Infrastructure ホームページで、[Security] ダッシュボードをクリックします。

ステップ 2　[Rogue APs and Adhoc Rogues] グループ ボックスで、「不正アクセス ポイント」の過去 1 時間以内、過去 24 時間以内、および合計のアクティブ数な指定する数値 URL をクリックします。

ステップ 3　[MAC Address] 列の URL をクリックして、スイッチ ポートを設定している不正アクセス ポイントを選択します。[Alarms] > [Rogue AP details] ページが開きます。

ステップ 4　[Select a command] ドロップダウン リストから、[Trace Switch Port] を選択します。[Trace Switch Port] ページが開き、Prime Infrastructure によってスイッチ ポート トレースが実行されます。

検索可能な MAC アドレスを 1 つ以上使用できる場合、Prime Infrastructure では CDP を使用して、検出中のアクセス ポイントから最大 2 ホップ離れて接続されているすべてのスイッチを検出します。各 CDP が検出したスイッチの MIB は、対象の MAC アドレスのいずれかが含まれているかどうかを確認するために検証されます。いずれかの MAC アドレスが見つかった場合、該当するポート番号が返され、不正アクセス ポイントのスイッチ ポートとして報告されます。

統合されたセキュリティ ソリューション

Cisco Unified Wireless Network Solution では、次の統合されたセキュリティ ソリューションも用意されています。

- Cisco Unified Wireless Network Solution オペレーティング システムのセキュリティは、堅牢な 802.1X AAA（認証、許可、アカウンティング）エンジンを中心に構築されており、オペレータは、Cisco Unified Wireless Network Solution 全体にわたってさまざまなセキュリティ ポリシーを迅速に設定および適用できます。
- コントローラおよびアクセス ポイントには、システム全体の認証および許可プロトコルがすべてのポートおよびインターフェイスに装備され、最大限のシステム セキュリティが実現されています。
- オペレーティング システムのセキュリティ ポリシーは個別の無線 LAN に割り当てられ、アクセス ポイントは設定されたすべての無線 LAN（最大 16）に同時にブロードキャストします。このポリシーにより、干渉の増加やシステム スループットの低下が発生する可能性のある、アクセス ポイントの追加が不要になる場合があります。
- オペレーティング システムのセキュリティは、RRM 機能を使用して、干渉およびセキュリティ侵犯がないか継続的に空間をモニタし、それらを検出したときはオペレータに通知します。
- オペレーティング システムのセキュリティは、業界標準の AAA サーバで動作し、システム統合が単純で簡単です。
- Cisco Intrusion Detection System（IDS; 侵入検知システム）/Intrusion Protection System（IPS; 侵入防御システム）は、特定のクライアントに影響を及ぼす攻撃を検出すると、コントローラにそれらのクライアントの無線ネットワークへのアクセスをブロックするように指示します。
- オペレーティング システムのセキュリティ ソリューションは、通常、高い処理能力を必要とする、包括的なレイヤ 2 およびレイヤ 3 の暗号化アルゴリズムを実現します。コントローラに VPN/ 拡張セキュリティ モジュールを装備することで、高度なセキュリティ設定に必要なハードウェアとしての機能も実現でき、暗号化を別のサーバで行う必要はありません。

Prime Infrastructure を使用した Cisco Unified Wireless Network Solution のレイヤ 3 モードからレイヤ 2 モードへの変換

Prime Infrastructure ユーザ インターフェイスを使用して Cisco Unified Wireless Network Solution をレイヤ 3 モードからレイヤ 2 LWAPP 転送モードに変換する手順は以下のとおりです。

（注） Cisco ベースの Lightweight アクセス ポイントでは、レイヤ 2 LWAPP モードはサポートされません。このようなアクセス ポイントは、レイヤ 3 でしか実行できません。

（注） この手順を実行すると、コントローラが再度ブートしてアクセス ポイントがコントローラと再アソシエートするまで、アクセス ポイントはオフラインになります。

ステップ 1　コントローラとアクセス ポイントはすべて同じサブネット上に配置するようにします。

（注） 変換を実行する前に、コントローラおよびアソシエートしているアクセス ポイントをレイヤ 2 モードで動作するように設定する必要があります。

ステップ 2　Prime Infrastructure ユーザ インターフェイスにログインします。LWAPP 転送モードをレイヤ 3 からレイヤ 2 に変換する手順は、次のとおりです。

a. [Configure] > [Controllers] の順に選択し、[All Controllers] ページに移動します。

b. 目的のコントローラの 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。

c. 左側のサイドバーのメニューから、[System] > [General] の順にクリックして、[IP Address] > [General] ページを表示します。

d. LWAPP 転送モードを [Layer2] に変更し、[Save] をクリックします。

e. Prime Infrastructure で次のメッセージが表示された場合、[OK] をクリックします。

```
Please reboot the system for the LWAPP Mode change to take effect.
```

ステップ 3　Cisco Unified Wireless Network Solution を再起動する手順は以下のとおりです。

a. [IP Address] > [Controller Properties] ページに戻ります。

b. [System] > [Commands] の順にクリックして、[IP Address] > [Controller Commands] ページを表示します。

c. [Administrative Commands] で、[Save Config To Flash] を選択し [Go] をクリックして、変更した設定をコントローラに保存します。

d. [OK] をクリックして作業を続行します。

e. [Administrative Commands] で、[Reboot] を選択し [Go] をクリックして、コントローラをリブートします。

f. [OK] をクリックし、設定を保存してリブートすることを確認します。

ステップ 4　コントローラが再度ブートした後で LWAPP 転送モードがレイヤ 2 になっていることを確認する手順は、次のとおりです。

a. [Monitor] > [Controllers] の順にクリックし、[Controllers] > [Search Results] ページに移動します。

b. 目的のコントローラの IP アドレスをクリックして、[Controllers] > [IP Address] > [Summary] ページを表示します。

c. [General] で、現在の LWAPP 転送モードが [Layer2] になっていることを確認します。

これで、レイヤ 3 からレイヤ 2 への LWAPP 転送モードの変換が完了しました。オペレーティング システムのソフトウェアによって、同じサブネット上のコントローラとアクセス ポイントとの間におけるすべての通信が制御されます。

Prime Infrastructure のファイアウォールの設定

Prime Infrastructure サーバと Prime Infrastructure ユーザ インターフェイスがファイアウォールの同じ側にない場合、ファイアウォール上の次のポートが双方向のトラフィックに対してオープンになっていない限り、これらは通信できません。

- 80（初期 HTTP 用）
- 69（TFTP）
- 162（トラップ）
- 443（HTTPS）
- 1522（プライマリとセカンダリの Prime Infrastructure 間で HA を設定する場合）

これらのポートをオープンにして、Prime Infrastructure サーバと Prime Infrastructure ユーザ インターフェイスとの間の通信を許可するようにファイアウォールを設定します。

アクセス ポイント許可

アクセス ポイントが許可に使用する証明書の種類とともに、許可済みアクセス ポイントの一覧を表示するには、次の手順を実行します。

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

ステップ 2　[IP Address] 列で URL の 1 つをクリックします。

ステップ 3　左側のサイドバーのメニューから [Security] > [AP/MSE Authorization] の順に選択します。

ステップ 4　ページの [AP Policies] 部分に、アクセス ポイントの許可が有効かどうかが示されます。また、自己署名証明書（SSC AP）の承認が有効かどうかも示されます。通常は、アクセス ポイントは AAA または証明書によって許可されます。（SSC は 4400 シリーズ コントローラおよび 2100 シリーズ コントローラのみに使用）。

これらの値を変更するには、[Select a command] ドロップダウン リストから [Edit AP Policies] を選択し、[Go] をクリックします。

ステップ 5　[AP Authorization List] 部分にアクセス ポイントの無線 MAC アドレス、証明書の種類、およびキー ハッシュが表示されます。別の許可エントリを追加するには、[Select a command] ドロップダウン リストから [Add AP/MSE Auth Entry] を選択し、[Go] をクリックします。

ステップ 6　ドロップダウン リストからこのコントローラに適用するテンプレートを選択して [Apply] をクリックします。アクセス ポイント許可の新しいテンプレートを作成するには、[click here] をクリックして、テンプレート作成ページにリダイレクトされるようにします。新しいテンプレートの作成手順については、「アクセス ポイント許可または MSE 許可テンプレートの設定」（P.11-59）を参照してください。

管理フレーム保護（MFP）

Management Frame Protection（MFP; 管理フレーム保護）では、アクセス ポイントとクライアント間で送受信される 802.11 管理メッセージを保護および暗号化することにより、セキュリティが確保されます。MFP は、インフラストラクチャとクライアント サポートの両方を実現します。

- インフラストラクチャ MFP：敵対者を発見することにより、管理フレームを保護します。敵対者は、DoS 攻撃を引き起こし、アソシエーションおよびプローブ パケットでネットワークを氾濫させ、不正アクセス ポイントをさしはさみ、QoS および無線測定フレームを攻撃してネットワーク パフォーマンスに影響を与えます。インフラストラクチャ MFP はまた、フィッシング インシデントの効果的かつ迅速な検出 / 報告手段を提供します。

  特に、インフラストラクチャ MFP では、アクセス ポイントによって送信される管理フレームに Message Integrity Check Information Element（MIC IE）を追加することにより、802.11 セッション管理機能を保護します。Message Integrity Check Information Element（MIC IE）はネットワーク内のその他のアクセス ポイントにより検証されます。インフラストラクチャ MFP はパッシブです。侵入を検知し報告しますが、それを止めることはできません。

- クライアント MFP：認証されたクライアントをスプーフィング フレームから保護し、無線 LAN に対する多くの一般化した攻撃が効力を発揮することのないようにします。認証解除攻撃などのほとんどの攻撃では、有効なクライアントとの競合により簡単にパフォーマンスを悪化させます。

  特に、アクセス ポイントとクライアントの両方が、スプーフされたクラス 3 管理フレーム（つまり、認証済みでアソシエートが完了しているアクセス ポイントとクライアント間で受け渡される管理フレーム）をドロップして予防措置を講じることができるように、クライアント MFP ではアクセス ポイントと Cisco Compatible Extension クライアント間で送信される管理フレームを暗号化します。クライアント MFP は、IEEE 802.11i によって定義されたセキュリティ メカニズムを利用し、アソシエーション解除、認証解除、および QoS（WMM）アクションといったタイプのクラス 3 ユニキャスト管理フレームを保護します。クライアント MFP はアクティブです。最も一般的な DoS 攻撃から、クライアントとアクセス ポイントとのセッションを保護できます。ここでは、セッションのデータ フレームで使用されるのと同じ暗号化方式を使用することにより、クラス 3 管理フレームが保護されます。アクセス ポイントまたはクライアントにより受信されたフレームの暗号化解除に失敗すると、そのフレームはドロップされ、イベントがコントローラに報告されます。

  クライアント MFP を使用するには、クライアントは Cisco Compatible Extensions（バージョン 5）MFP をサポートしている必要があり、TKIP または AES-CCMP のいずれかを使用する WPA2 をネゴシエートする必要があります。EAP または PSK は、PMK を取得するために使用できます。アクセス ポイント間、またはレイヤ 2 とレイヤ 3 の高速ローミングでセッション キーを配信するために、CCKM およびコントローラ モビリティ管理が使用されます。

  ブロードキャスト フレームに対する攻撃を防ぐために、Cisco Compatible Extensions（バージョン 5）をサポートしているアクセス ポイントは、ブロードキャスト クラス 3 管理フレーム（アソシエーション解除、認証解除、またはアクションなど）を送信しません。Compatible Extensions クライアント（バージョン 5）とアクセス ポイントは、ブロードキャスト クラス 3 管理フレームを破棄します。

  クライアント MFP は、インフラストラクチャ MFP を置き換えるのではなく、補足します。これは、インフラストラクチャ MFP が、無効なクラス 1 管理フレームとクラス 2 管理フレームだけでなく、クライアント MFP 対応ではないクライアントに送信される無効なユニキャスト フレームを検出して報告し続けるためです。インフラストラクチャ MFP は、クライアント MFP によって保護されていない管理フレームにのみ適用されます。

インフラストラクチャ MFP は次の 3 つの主要なコンポーネントで構成されます。

- 管理フレーム保護：アクセス ポイントは、送信される各管理フレームに MIC IE を追加することによってフレームを保護します。フレームのコピー、変更、再送が試みられた場合、MIC は無効となり、MFP フレームを検出するよう設定された受信アクセス ポイントは不具合を報告します。

- 管理フレーム検証：インフラストラクチャ MFP でアクセス ポイントは、ネットワーク内の他のアクセス ポイントから受信するすべての管理フレームを検証します。これにより、MC IE が存在し（発信側が MFP フレームを送信するよう設定されている場合）、管理フレームの中身が一致していることを確認できます。MFP フレームを送信するよう設定されているアクセス ポイントに属する BSSID からの正当な MIC IE が含まれていないフレームを受信した場合、不具合をネットワーク管理システムに報告します。タイムスタンプが適切に機能するには、すべてのコントローラでネットワーク タイム プロトコル（NTP）が同期されている必要があります。
- イベント報告：アクセス ポイントは異常を検出するとコントローラに通知し、コントローラは受信した異常イベントを集約して、SNMP トラップ経由でネットワーク管理システムに結果を報告します。

（注）　クライアント MFP は、インフラストラクチャ MFP と同じイベント報告メカニズムを使用します。

インフラストラクチャ MFP は、デフォルトで有効化されており、システム全体で無効化できます。以前のソフトウェア リリースからアップグレードする場合、アクセス ポイント認証が有効になっているときは、これら 2 つの機能は相互に排他的であるため、インフラストラクチャ MFP はシステム全体で無効になります。インフラストラクチャ MFP がシステム全体で有効にされている場合、選択した WLAN に対してシグニチャ生成（送信フレームへの MIC の追加）を無効にし、選択したアクセス ポイントに対して検証を無効にできます。

WLAN テンプレートで MFP を設定します。「WLAN テンプレートの設定」（P.11-19）を参照してください。

MFP の使用に関するガイドライン

MFP を使用する際のガイドラインは次のとおりです。

- MFP 機能では、AP 1500 シリーズのメッシュ アクセス ポイントを除く、Cisco Aironet Lightweight アクセス ポイントでの使用がサポートされています。
- Lightweight アクセス ポイントは、ローカル モードとモニタ モードでインフラストラクチャ MFP をサポートし、アクセス ポイントがコントローラに接続されているときには REAP モードと FlexConnect モードをサポートします。クライアント MFP は、ローカル モード、FlexConnect モード、およびブリッジ モードでサポートされます。
- クライアント MFP は、TKIP または AES-CCMP で WPA2 を使用する Cisco Compatible Extensions（バージョン 5）クライアントでだけ使用がサポートされています。
- Cisco Compatible Extensions（バージョン 5）以外のクライアントは、クライアント MFP が無効もしくはオプション設定の場合のみ、WLAN にアソシエートできます。

侵入検知システム（IDS）の設定

Cisco Intrusion Detection System（IDS; 侵入検知システム）/Intrusion Prevention System（IPS; 侵入防御システム）は、特定のクライアントに影響を及ぼす攻撃を検出すると、このクライアントのワイヤレス ネットワークへのアクセスをブロックするようにコントローラに指示します。このシステムにより、ワーム、スパイウェア/アドウェア、ネットワーク ウイルス、およびアプリケーションの不正使用などの脅威を検出し、分類し、阻止するための重要なネットワーク保護を実現できます。IDS で攻撃の検出に使用できる方法は 2 つあります。

- IDS センサー（レイヤ 3 用）
- IDS シグニチャ（レイヤ 2 用）

IDS センサーの表示

センサーが攻撃を識別した場合は、攻撃しているクライアントを回避するようにコントローラに警告します。新しい IDS センサーを追加した場合は、回避したクライアントのレポートをセンサーがコントローラに送信できるように、コントローラをその IDS センサーに登録します。また、コントローラは定期的にセンサーをポーリングします。

IDS センサーを表示する手順は、次のとおりです。

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

ステップ 2　IP アドレスをクリックしてコントローラを選択します。

ステップ 3　左側のサイドバーのメニューから、[Security] > [IDS Sensor Lists] の順に選択します。[IDS Sensor] ページが表示されます。このページでは、このコントローラに設定されているすべての IDS センサーが一覧表示されます。

IDS シグニチャの設定

コントローラ上で、*IDS シグニチャ*、または受信する 802.11 パケットにおけるさまざまなタイプの攻撃を識別するのに使用されるビット パターンのマッチング ルールを設定することができます。シグニチャが有効化されると、コントローラに接続されたアクセス ポイントでは、受信した 802.11 データまたは管理フレームに対してシグニチャ分析が行われ、整合性がない場合はコントローラに報告されます。攻撃が検出されると、適切な緩和措置が取られます。

シスコでは、標準シグニチャとカスタムなシグニチャのページで示すように、コントローラで 17 個の標準シグニチャをサポートします。このページを開くには、[Configure] > [Controllers] を選択し、コントローラの IP アドレスを選択して、左側のサイドバーのメニューから、[Security] > [Wireless Protection Policies] > [Standard Signatures] を選択します。

これらのシグニチャは 6 つの主要なグループに分かれます。最初の 4 つのグループには管理フレーム用シグニチャが含まれ、最後の 2 つのグループにはデータ フレーム用シグニチャが含まれます。

- ブロードキャスト解除フレーム シグニチャ：ブロードキャスト認証解除フレーム攻撃において、ハッカーは別のクライアントのブロードキャスト MAC 宛先アドレスに対して 802.11 認証解除フレームを送信します。この攻撃により、宛先クライアントは接続アクセス ポイントから強制的にアソシエーション解除させられ、ネットワークの接続断が発生します。この処理が繰り返されると、クライアントでサービス利用ができない状態が発生します。ブロードキャスト認証解除フレーム シグニチャ（優先順位 1）を使用してそのような攻撃を検出する場合、アクセス ポイントでは、シグニチャの特性と一致するクライアント送信ブロードキャスト認証解除フレームがリッスンされます。アクセス ポイントは、そのような攻撃を検出すると、コントローラに警告を送ります。システムの設定に応じて、危険性のあるデバイスが封じ込められて、そのデバイスの信号が許可されたクライアントに干渉しないようにされるか、コントローラからシステム管理者に、さらなる処理を行うよう即時に警告が転送されるか、または、その両方が実行されます。
- NULL プローブ応答シグニチャ：NULL プローブ応答攻撃において、ハッカーはワイヤレス クライアント アダプタに NULL プローブ応答を送信します。結果として、クライアント アダプタがロックされます。NULL プローブ応答シグニチャを使用してそのような攻撃が検出されると、アクセス ポイントはワイヤレス クライアントを特定し、コントローラに警告を送ります。NULL プローブ応答シグニチャには次のものがあります。
  - NULL probe resp 1（優先順位 2）
  - NULL probe resp 2（優先順位 3）

- 管理フレーム フラッドシグニチャ：管理フレーム フラッド攻撃において、ハッカーはアクセス ポイントに大量の 802.11 管理フレームを送り付けます。その結果、アクセス ポイントにアソシエートしている、もしくはアソシエートを試みているすべての端末に対して、サービス利用ができない状態が発生します。この攻撃は、アソシエーション要求、認証要求、再アソシエーション要求、プローブ要求、アソシエーション解除要求、認証解除要求、予約管理サブタイプなど、さまざまなタイプの管理フレームを使用して実行されます。

  管理フレーム フラッド シグニチャによってこれらの攻撃を検出すると、アクセス ポイントは、シグニチャの全体的な特性と合致する管理フレームを特定します。これらのフレームの検出頻度が、シグニチャで設定されたしきい値より大きくなると、これらのフレームを受信するアクセス ポイントによって警告が送信されます。コントローラではトラップが生成され、Prime Infrastructure に転送されます。

  管理フレーム フラッド シグニチャには次のものがあります。

  - Assoc flood（優先順位 4）
  - Auth flood（優先順位 5）
  - Reassoc flood（優先順位 6）
  - Broadcast probe flood（優先順位 7）
  - Disassoc flood（優先順位 8）
  - Deauth flood（優先順位 9）
  - Reserved mgmt 7（優先順位 10）
  - Reserved mgmt F（優先順位 11）

  予約管理フレーム シグニチャ（Reserved mgmt）7 および F は、将来使用するために予約されています。

- EAPOL フラッド シグニチャ：EAPOL フラッド攻撃において、ハッカーは 802.1X 認証要求を含む EAPOL フレームを大量に発生させます。結果として、802.1X 認証サーバはすべての要求に応答できなくなり、有効なクライアントに正常な認証応答を送信できなくなります。そして、その影響を受けるすべてのクライアントにおいてサービス利用ができない状況が発生します。EAPOL フラッド シグニチャ（優先順位 12）を使用してそのような攻撃が検出されると、アクセス ポイントは EAPOL パケットの最大許容数を超えるまで待機します。次に、コントローラに警告を送り、適切な緩和措置を実行します。

- NetStumbler シグニチャ：NetStumbler は、無線 LAN スキャン ユーティリティです。これによって、アクセス ポイントのブロードキャスト関連情報（動作チャネル、RSSI 情報、アダプタ製造業者名、SSID、WEP ステータス、GPS が接続された NetStumbler を実行するデバイスの経度と緯度など）が報告されます。NetStumbler は、アクセス ポイントに対する認証とアソシエーションに成功すると、次の文字列のデータ フレーム（表 3-9 にリストした NetStumbler のバージョンによって異なる）を送信します。

表 3-9　NetStumbler バージョン

バージョン	文字列
3.2.0	「Flurble gronk bloopit, bnip Frundletrune」
3.2.3	「All your 802.11b are belong to us」
3.3.0	ホワイト スペースを送信

NetStumbler シグニチャを使用してそのような攻撃が検出されると、アクセス ポイントは危険性のあるデバイスを特定してコントローラに警告を送ります。NetStumbler シグニチャには次のものがあります。

- NetStumbler 3.2.0（優先順位 13）
- NetStumbler 3.2.3（優先順位 14）
- NetStumbler 3.3.0（優先順位 15）
- NetStumbler generic（優先順位 16）

- Wellenreiter シグニチャ：Wellenreiter は、無線 LAN スキャンおよびディスカバリ ユーティリティです。これを使用すると、アクセス ポイントおよびクライアントに関する情報が漏洩してしまう可能性があります。Wellenreiter シグニチャ（優先順位 17）を使用してそのような攻撃が検出されると、アクセス ポイントは危険性のあるデバイスを特定し、コントローラに警告を送ります。

この項では、シグニチャを設定する手順について説明します。この項で取り上げるトピックは次のとおりです。

- 「IDS シグニチャのアップロード」（P.3-37）
- 「IDS シグニチャのダウンロード」（P.3-38）
- 「IDS シグニチャの有効化または無効化」（P.3-39）

IDS シグニチャのアップロード

コントローラから IDS シグニチャをアップロードする手順は、次のとおりです。

ステップ 1　シスコからシグニチャ ファイルを入手します（以降、*標準シグニチャ ファイル*）。「IDS シグニチャのダウンロード」（P.3-38）に従い、独自のシグニチャ ファイル（カスタム シグニチャ ファイル）を作成することもできます。

ステップ 2　シグニチャ ダウンロード用の TFTP サーバを設定します。TFTP サーバをセットアップする際の注意事項は次のとおりです。

- サービス ポート経由でダウンロードする場合、サービス ポートはルーティングできないため、TFTP サーバはサービス ポートと同じサブネット上になければなりません。ただし、管理ポートがダウンしている間、TFTP サーバを別のネットワークに配置する場合は、サービス ポートのあるサブネットにゲートウェイがあれば、スタティック ルートを追加します（config route add *IP address of TFTP server*）。
- ディストリビューション システム ネットワーク ポートを経由してダウンロードする場合、ディストリビューション システム ポートはルーティング可能なので、TFTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。
- Prime Infrastructure の組み込み TFTP サーバとサードパーティの TFTP サーバは同じ通信ポートを使用するため、サードパーティの TFTP サーバを Prime Infrastructure と同じコンピュータ上で実行することはできません。

ステップ 3　[Configure] > [Controllers] の順に選択します。

ステップ 4　IP アドレスをクリックしてコントローラを選択します。

ステップ 5　左側のサイドバーのメニューから [Security] を選択し、[Standard Signatures] または [Custom Signatures] を選択します。

ステップ 6　[Select a Command] ドロップダウン リストから、[Upload Signature Files from Controller] を選択します。

ステップ 7　転送に使用している TFTP サーバ名を指定します。

ステップ 8　新規の TFTP サーバを利用する場合は、[Server IP Address] フィールドで TFTP IP アドレスを入力します。

ステップ 9　[File Type] ドロップダウン リストから [Signature Files] を選択します。

ステップ 10　このシグニチャ ファイルは、TFTP サーバによる使用に対して設定されたルート ディレクトリにアップロードされます。[Upload to File] フィールドで別のディレクトリに変更できます（このフィールドは、[Server Name] がデフォルト サーバの場合のみ表示）。コントローラはベース ネームとしてこのローカル ファイル名を使用し、標準シグニチャ ファイルの拡張子として *_std.sig* を、カスタム シグニチャ ファイルの拡張子として *_custom.sig* を追加します。

ステップ 11　[OK] をクリックします。

IDS シグニチャのダウンロード

標準のシグニチャ ファイルがすでにコントローラ上にあり、カスタマイズされたシグニチャをコントローラにダウンロードする場合は、次の手順を実行します。

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

ステップ 2　IP アドレスをクリックしてコントローラを選択します。

ステップ 3　[System] > [Commands] の順に選択します。

ステップ 4　[Upload/Download Commands] ドロップダウン リストから、[Download IDS Signatures] を選択し、[Go] をクリックします。

ステップ 5　シグニチャ ファイル（*.sig）を TFTP サーバ上のデフォルト ディレクトリにコピーします。

ステップ 6　[File is Located On] フィールドから [local machine] を選択します。ファイル名および、サーバのルート ディレクトリに対する相対的なパスがわかる場合は、TFTP サーバを選択することもできます。

ステップ 7　[Maximum Retries] フィールドに、コントローラがシグニチャ ファイルのダウンロードを試みる最大回数を入力します。

ステップ 8　[Timeout] フィールドに、シグニチャ ファイルのダウンロードを試行する際、コントローラがタイムアウトになるまでの最大時間を秒単位で入力します。

ステップ 9　ファイルは /localdisk/tftp ディレクトリにアップロードされます。そのディレクトリでのローカル ファイル名を指定し、[Browse] ボタンを使用してそのファイル名に移動します。シグニチャ ファイルの「revision」行で、ファイルがシスコ提供の標準のシグニチャ ファイルか、またはサイトに合わせたカスタム シグニチャ ファイルかを指定します（カスタム シグニチャ ファイルには revision=custom が必須）。

ステップ 10　何らかの理由で転送がタイムアウトした場合には、[File Is Located On] フィールドの [TFTP] サーバ オプションを選択すると、[Server File Name] が読み込まれ、再試行されます。ローカル マシン オプションでは 2 段階の動作が起動されます。最初に、ローカル ファイルが管理者のワークステーションから Prime Infrastructure の組み込み TFTP サーバにコピーされます。次にコントローラがそのファイルを取得します。後の操作では、ファイルはすでに Prime Infrastructure サーバの TFTP ディレクトリにあるため、[download web] ページには、自動的にファイル名が入力されます。

ステップ 11　[OK] をクリックします。

IDS シグニチャの有効化または無効化

IDS シグニチャを有効または無効にする手順は、次のとおりです。

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

ステップ 2　IP アドレスをクリックしてコントローラを選択します。

ステップ 3　左側のサイドバーのメニューから [Security] を選択し、[Standard Signatures] または [Custom Signatures] を選択します。

ステップ 4　個々のシグニチャを有効または無効にするには、有効または無効にしたい攻撃の種類の [Name] 列をクリックします。

[Standard Signature Parameters] ページには、現在コントローラ上にあるシスコ提供のシグニチャの一覧が表示されます。[Custom Signatures] ページには、現在コントローラ上に存在する、カスタマー提供のシグニチャのリストが表示されます。シグニチャ ページまたは詳細シグニチャ ページに次の情報が表示されます。

- [Precedence]：コントローラがシグニチャ チェックを行う順序、または優先順位。
- [Name]：シグニチャによって検出を試みる攻撃の種類。
- [Description]：シグニチャによって検出を試みる攻撃の種類の詳細説明。
- [Frame Type]：シグニチャによってセキュリティ攻撃の調査が行われる管理フレームまたはデータフレームの種類。
- [Action]：シグニチャによって攻撃が検出されたときに実行する、コントローラへの指示。なにも処置をとらない場合は *None*、検出を報告する場合は *Report* となります。
- [Frequency]：シグニチャの検出頻度、もしくは攻撃が検出される前に、各アクセス ポイント レベルでの検出において識別されるべき、[Interval] 設定間隔におけるシグニチャに合致するパケット数。設定可能な値の範囲は、[Interval] 設定間隔あたり 1 ～ 32,000 パケットです。デフォルト値は [Interval] 設定間隔あたり 50 パケットです。
- [Quiet Time]：各アクセス ポイント レベルで攻撃が検出されなくなってから、アラームを停止するまでの時間の長さ（秒単位）。この設定は、次項の [MAC Information] の設定が [all] もしくは [both] の場合にだけ表示されます。設定可能な値の範囲は 60 ～ 32,000 秒で、デフォルト値は 300 秒です。
- [MAC Information]：アクセス ポイント レベルの検出においてシグニチャをネットワークごとまたは MAC アドレスごと、または両方で追跡するどうか。
- [MAC Frequency]：シグニチャ MAC の検出頻度、もしくは攻撃が検出される前にコントローラ レベルの検出において識別する必要のある、[Interval] 設定間隔ごとのシグニチャと一致するパケット数です。有効な範囲は [Interval] 設定間隔あたり 1 ～ 32,000 パケットです。デフォルト値は [Interval] 設定間隔あたり 30 パケットです。
- [Interval]：シグニチャの検出頻度がしきい値に達したかどうかをチェックする間隔（秒単位）を入力します。設定可能な値の範囲は 1 ～ 3600 秒で、デフォルト値は 1 秒です。
- [Enable]：セキュリティ攻撃の検出でこのシグニチャを有効にする場合に選択し、このシグニチャを無効にする場合に選択解除します。
- [Signature Patterns]：セキュリティ攻撃の検出に使用されるパターン。

ステップ 5　[Enabled yes or no] ドロップダウン リストで、[yes] を選択します。カスタマイズされたシグニチャをダウンロードしているため、_custom.sgi という名前の付いたファイルを有効にし、同じ名前で異なる拡張子を持つ標準シグニチャを無効にする必要があります。（たとえば、ブロードキャスト プローブの大量送信をカスタマイズしている場合に、ブロードキャスト プローブの大量送信を標準シグニチャでは無効にしたいがカスタム シグニチャでは有効にしたい場合がある）。

ステップ 6　現在コントローラ上にある標準シグニチャとカスタム シグニチャをすべて有効にするは、[Select a command] ドロップダウン リストから [Edit Signature Parameters] を選択し、[Go] を選択します。[Edit Signature Parameters] ページが表示されます。

ステップ 7　[Check for All Standard and Custom Signatures] フィールド、[Enable] チェックボックスをオンにします。これにより、ステップ 5 で個々に選択して有効にしたシグニチャすべてを有効にします。このチェックボックスをオフのままにすると、前にステップ 5 で有効にしていても、すべてのファイルは無効になります。シグニチャが有効化されると、コントローラに接続されたアクセス ポイントでは、受信した 802.11 データまたは管理フレームに対してシグニチャ分析が行われ、整合性がない場合はコントローラに報告されます。

ステップ 8　[Save] をクリックします。

Web ログインの有効化

Web 認証により、ゲストはブラウザを起動すると自動的に Web 認証ページにリダイレクトされます。ゲストは、この Web ポータルから WLAN にアクセスできます。この認証メカニズムを使用している無線 LAN 管理者は、ゲスト ユーザによるアクセスに対して、暗号化通信と非暗号化通信のどちらを設定するかを選択できます。ゲスト ユーザは、SSL で暗号化される有効なユーザ名とパスワードを使用して無線ネットワークにログインできます。Web 認証アカウントはローカルに作成するか、RADIUS サーバで管理できます。Cisco Wireless LAN Controller は Web 認証クライアントをサポートするように設定できます。コントローラで提供される Web 認証ページを置き換えるテンプレートを作成するには、「Web 認証テンプレートの設定」（P.11-63）を参照してください。

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

ステップ 2　[IP Address] 列で IP アドレス URL をクリックして、Web 認証を有効にするコントローラを選択します。

ステップ 3　左側のサイドバーのメニューから、[Security] > [AAA] > [Web Auth Configuration] の順に選択します。

ステップ 4　ドロップダウン リストから適切な Web 認証のタイプを選択します。選択肢は、デフォルトの内部、カスタマイズ Web 認証、または外部です。

- デフォルトの内部を選択した場合でも、ページ タイトル、メッセージ、リダイレクト URL、およびロゴを表示するかどうかを変更できます。ステップ 5 に進みます。
- カスタマイズされた Web 認証を選択する場合は、「カスタマイズされた Web 認証のダウンロード」（P.3-41）に進んでください。
- 外部を選択する場合は、認証に成功した後でリダイレクトする URL を入力する必要があります。たとえば、このテキスト ボックスに入力した値が http://www.example.com の場合、ユーザはこの会社のホーム ページに接続されます。

ステップ 5　会社のロゴを表示させたい場合は、[Logo Display] チェックボックスをオンにします。

ステップ 6　Web 認証ページに表示するタイトルを入力します。

ステップ 7　Web 認証ページに表示するメッセージを入力します。

ステップ 8　[Customer Redirect URL] フィールドに、認証に成功した後でユーザがリダイレクトされる URL を指定します。たとえば、このテキスト ボックスに入力した値が http://www.example.com の場合、ユーザはこの会社のホーム ページに接続されます。

ステップ 9　[Save] をクリックします。

カスタマイズされた Web 認証のダウンロード

カスタマイズされた Web 認証ページをコントローラにダウンロードできます。カスタマイズ Web ページは、ユーザ Web アクセス用のユーザ名とパスワードを設定するために作成されます。

カスタマイズ Web 認証をダウンロードする際は、次のガイドラインに従う必要があります。

- ユーザ名を指定する。
- パスワードを指定する。
- リダイレクト URL は、元の URL から引用した後、非表示の入力項目として保持する。
- 操作 URL は、元の URL から引用および設定する。
- 戻りステータス コードをデコードするスクリプトを含める。
- メイン ページで使用されるすべてのパスは相対パスとする。

前の項のステップ 4 において、カスタマイズされた Web 認証オプションを選択した場合は、ダウンロードの前に、次の手順を実行します。

ステップ 1　プレビュー画像をクリックして、サーバからサンプルの login.html バンドル ファイルをダウンロードします。login.html ファイルの例については、図 3-1 を参照してください。ダウンロードしたバンドルは .TAR ファイルとなります。

図 3-1　　Login.html

ステップ 2　Login.html を開いて編集し、これを .tar または .zip ファイルとして保存します。

（注）　任意のテキスト エディタまたは HTML エディタで [Submit] ボタンのテキストを「Accept terms and conditions and Submit」（条件を承諾して送信）などに変更できます。

ステップ 3　ダウンロードに Trivial File Transfer Protocol（TFTP）サーバを使用できることを確認します。TFTP サーバをセットアップする際の注意事項は次のとおりです。

- サービス ポート経由でダウンロードする場合、サービス ポートはルーティングできないため、TFTP サーバはサービス ポートと同じサブネット上になければなりません。
- ディストリビューション システム ネットワーク ポートを経由してダウンロードする場合、ディストリビューション システム ポートはルーティング可能なので、TFTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。

- Prime Infrastructure の組み込み TFTP サーバとサードパーティの TFTP サーバは同じ通信ポートを使用するため、サードパーティの TFTP サーバを Prime Infrastructure と同じコンピュータ上で実行することはできません。

ステップ 4　リンク「After editing the HTML you might click **here** to redirect to the Download Web Auth Page」の [here] をクリックして、.tar ファイルまたは .zip ファイルをコントローラにダウンロードします。[Download Customized Web Auth Bundle to Controller] ページが表示されます。

（注）　バンドルを受信するコントローラの IP アドレスとその現在のステータスが表示されます。

ステップ 5　[File is Located On] フィールドから [local machine] を選択します。ファイル名および、サーバのルート ディレクトリに対する相対的なパスがわかる場合は、TFTP サーバを選択することもできます。

（注）　ローカル マシンのダウンロードには、.zip または .tar のファイル オプションがありますが、Prime Infrastructure では自動的に .zip を .tar に変換します。TFTP サーバのダウンロードを選択した場合は、.tar ファイルだけを指定します。

ステップ 6　[Timeout] フィールドに、ファイルをダウンロードする際、コントローラがタイムアウトするまでの最大時間を秒単位で入力します。

ステップ 7　[Prime Infrastructure Server Files In field] は Prime Infrastructure サーバ ファイルのある場所を指定します。そのディレクトリでのローカル ファイル名を指定し、[Browse] ボタンを使用してそのファイル名に移動します。シグニチャ ファイルの「revision」行で、ファイルがシスコ提供の標準のシグニチャ ファイルか、またはサイトに合わせたカスタム シグニチャ ファイルかを指定します（カスタム シグニチャ ファイルには revision=custom が必須）。

ステップ 8　何らかの理由で転送がタイムアウトした場合には、[File Is Located On] フィールドの TFTP サーバ オプションを選択すると、[Server File Name] が読み込まれます。ローカル マシン オプションでは 2 段階の動作が起動されます。最初に、ローカル ファイルが管理者のワークステーションから Prime Infrastructure の組み込み TFTP サーバにコピーされます。次にコントローラがそのファイルを取得します。後の操作では、ファイルはすでに Prime Infrastructure サーバの TFTP ディレクトリにあるため、[download web] ページには、自動的にファイル名が入力されます。

ステップ 9　[OK] をクリックします。

何らかの理由で転送がタイムアウトした場合には、[File Is Located On] フィールドの TFTP サーバ オプションを選択すると、[Server File Name] が読み込まれます。

ステップ 10　ダウンロードが完了すると、新しいページに接続され、認証できます。

ゲスト WLAN への接続

ゲスト セントラル WLAN に接続して Web 認証プロセスを実行する手順は、次のとおりです。ゲスト ユーザ アカウントの詳細については、「ゲスト ユーザ アカウントの作成」（P.7-8）を参照してください。

ステップ 1　オープン認証の設定で接続されている場合は、ブラウザで仮想インターフェイスの IP アドレスにアクセスします（/209.165.200.225/login.html など）。

ステップ 2　Prime Infrastructure ユーザ インターフェイスに [Login] ページが表示されたら、ユーザ名とパスワードを入力します。

（注）　入力する文字はすべて、大文字と小文字が区別されます。

Lobby Ambassador は、ゲスト ユーザを追加する場合以外は、テンプレートにアクセスできません。

証明書署名要求（CSR）の生成

Prime Infrastructure を使用してサードパーティ証明書の証明書署名要求（CSR）を生成する方法については、付録 C「Cisco Prime Prime Infrastructure でのサードパーティ証明書の証明書署名要求（CSR）の生成」を参照してください。