ワイヤレス デバイスのモニタ

コントローラのモニタ

すべてのワイヤレス コントローラを表示するには、[モニタ（Monitor）] > [管理対象要素（Managed Elements）] > [ネットワークデバイス（Network Devices）] の順に選択し、次に [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] の順に選択します。

関連トピック

システム パラメータのモニタ （1 ページ）

システム パラメータのモニタ

すべてのワイヤレス コントローラを表示するには、[モニタ（Monitor）] > [管理対象要素（Managed Elements）] > [ネットワークデバイス（Network Devices）] の順に選択し、次に [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] の順に選択します。デバイス名をクリックすると、詳細が表示されます。

リリース 3.2 以降では、**[デバイスの詳細（Device Details）] > [システム（System）]** の下にある次の [モニタ（Monitor）] ページでは、デフォルトで Prime Infrastructure データベースからデータが取得されます。ページの右上隅にある [デバイスから更新（Refresh from Device）] リンクをクリックすると、デバイスから更新するオプションを使用できます。Prime Infrastructure でデータが最後に更新された日時も表示されます。

- 要約
- CDP ネイバー
- WLAN

リリース 3.2 以降では、**[デバイスの詳細（Device Details）] > [システム（System）]** の下にある次の [モニタ（Monitor）] ページでは、データがデバイスから直接取得されます。

- CLIセッション
- DHCP 統計情報

表 *1*: モニタ ネットワーク デバイス ワイヤレス コントローラの詳細

表示する内容	選択するメニュー
システム情報（System Information）	[デバイスの詳細（Device Details）] タブの [システム（System）] > [概要（Summary）]
IP アドレス、デバイス タイプ、場所、到達可能性ステータス、説明、デバイス総数などの要約情報	
CLI セッションの詳細	[デバイスの詳細（Device Details）] タブの [システム（System）] > [CLIセッション（CLI Sessions）]
送受信されたパケット、DHCP サーバ応答情報、最新の要求タイムスタンプなどのDHCP統計情報（バージョン 5.0.6.0 以降のコントローラ向け）	[デバイスの詳細（Device Details）] タブの [システム（System）] > [DHCP統計情報（DHCP Statistics）]
マルチキャスト情報	[設定（Configuration）] タブの [システム（System）] > [マルチキャスト（Multicast）]
MAC アドレス、ロール、状態などのスタック情報	[デバイスの詳細（Device Details）] タブの [システム（System）] > [スタック（Stacks）]
STP 統計情報	[設定（Configuration）] タブの [システム（System）] > [スパニングツリープロトコル（Spanning Tree Protocol）]
ユーザ定義フィールドに関する情報	[デバイスの詳細（Device Details）] タブの [システム（System）] > [ユーザ定義フィールド（User Defined Field）]
コントローラで設定したワイヤレス ローカル アクセス ネットワーク（WLAN）	[デバイスの詳細（Device Details）] タブの [システム（System）] > [WLAN（WLANs）]
モビリティ（Mobility）	[デバイスの詳細（Device Details）] タブの [モビリティ（Mobility）] > [モビリティステータス（Mobility Stats）]
送受信エラー、ハンドオフ要求などのモビリティ グループ イベントの統計情報	
ポート	

表示する内容	選択するメニュー
選択したコントローラの物理ポートに関する情報	[設定（Configuration）] タブの [ポート（Ports）] > [全般（General）]
CDP インターフェイス	[設定（Configuration）] タブの [ポート（Ports）] > [CDPインターフェイスネイバー（CDP Interface Neighbors）]
セキュリティ	[デバイスの詳細（Device Details）] タブの [セキュリティ（Security）] > [RADIUSアカウンティング（RADIUS Accounting）]
RADIUS アカウンティング サーバ情報と統計情報	
RADIUS 認証サーバ情報	[デバイスの詳細（Device Details）] タブの [セキュリティ（Security）] > [RADIUS認証（RADIUS Authentication）]
ネットワーク アクセス コントロール リストに関する情報	**[システム（System）] > [セキュリティ（Security）] > [ネットワーク アクセス コントロール（Network Access Control）]**
ゲスト アクセスの展開とネットワーク ユーザ	[デバイスの詳細（Device Details）] タブの [セキュリティ（Security）] > [ゲストユーザ（Guest Users）]
管理フレーム保護（MFP）の要約情報	[デバイスの詳細（Device Details）] タブの [システム（System）] > [セキュリティ（Security）] > [管理フレーム保護（Management Frame Protection）]
現在コントローラに適用されているすべての不正アクセス ポイント ルールのリスト。	[デバイスの詳細（Device Details）] タブの [システム（System）] > [セキュリティ（Security）] > [不正APルール（Rogue AP Rules）]
スリープ状態にあるクライアントのリスト。スリープ状態にあるクライアントとは、Web 認証に成功したゲストアクセスを持ち、ログインページから別の認証プロセスを実行せずにスリープおよび復帰することを許可されているクライアントです。	[デバイスの詳細（Device Details）] タブの [セキュリティ（Security）] > [スリープ状態にあるクライアント（Sleeping Clients）]
IPv6	[設定（Configuration）] タブの [IPv6] > [ネイバーバインディングタイマー（Neighbor Binding Timers）]
IPv6アドレス、リンク、MTUなどを生成および取得するために、ホストまたはクライアントとルータの間で交換されたメッセージ数の統計情報。	
冗長性	[デバイスの詳細（Device Details）] タブの [システム（System）] > [冗長性の概要（Redundancy Summary）]
冗長性情報	
mDNS	

表示する内容	選択するメニュー
mDNS サービスおよびサービス プロバイダー情報のリスト。	[デバイスの詳細（Device Details）] タブの [mDNS] > [mDNSサービスプロバイダー（mDNS Service Provider）]

関連トピック

スパニング ツリー プロトコルとは （4 ページ）
管理フレーム保護とは （4 ページ）
不正アクセス ポイント ルールとは （4 ページ）

スパニング ツリー プロトコルとは

スパニング ツリー プロトコル（STP）はリンク管理プロトコルの 1 つです。Cisco WLAN ソリューションでは、メディア アクセス コントロール ブリッジ用に IEEE 802.1D 標準が実装されています。

スパニング ツリー アルゴリズムは、ステーション間の複数のアクティブ パスによって作成される、ネットワーク内の無用なループを避けるとともに、冗長性を備えています。STP では、任意の 2 台のネットワーク デバイス間で同時に 1 つのアクティブなパスのみが存在できますが（これによりループが防止されます）、初期リンクが障害になった場合のバックアップとして冗長リンクが確立されます。

スパニング ツリー プロトコルをサポートしていないコントローラは、WISM、2500、5500、7500、および SMWLC です。

管理フレーム保護とは

管理フレーム保護（MFP）は、802.11 管理フレームの認証を提供します。管理フレームを保護することにより敵対者を検知できるようになり、DoS 攻撃や、プローブのフラッディング、不正 AP の設置を検知でき、QoS および無線測定フレームへの攻撃を防止しネットワーク パフォーマンスへの影響を抑えます。

コントローラの 1 つ以上の WLAN で MFP が有効になっている場合、コントローラは各登録済みアクセス ポイントに、それらの WLAN についてアクセス ポイントが使用する各 BSSID の一意のキーを送信します。MFP が有効になっている WLAN 経由でアクセス ポイントによって送信された管理フレームは、フレーム保護情報要素（IE）で署名されます。フレームを変更しようとするとメッセージが無効になり、MFP フレームを検出するように設定されている受信側アクセス ポイントが WLAN コントローラに不一致を報告します。

不正アクセス ポイント ルールとは

不正アクセス ポイント ルールは、認証タイプ、一致する設定された SSID、クライアント カウント、および RSSI 値などの条件に基づいて、不正なアクセス ポイントを自動的に分類します。Prime Infrastructure では、不正アクセス ポイントの分類ルールをコントローラおよびそれぞれのアクセス ポイントに適用します。

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 ポイントを無視）、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。

不正アクセス ポイントのルールは、誤アラームを減らすのにも役立ちます。

不正クラスには以下の種類があります。

- [悪意のある不正（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アクセス ポイント カテゴリから手動で移動されたアクセス ポイント。
- [危険性のない不正（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。
- [未分類の不正（Unclassified Rogue）]：検出されたアクセス ポイントのうち、Malicious ルールにも Friendly ルールにも該当しないアクセス ポイント。

関連トピック

システム パラメータのモニタ （1 ページ）

サードパーティ製コントローラに関するシステム詳細の表示

Prime Infrastructure によって管理されているサードパーティ（シスコ以外の）コントローラに関する詳細情報を表示するには、[モニタ（Monitor）] > [管理対象要素（Managed Elements）] >[ネットワークデバイス（Network Devices）]>[サードパーティワイヤレスコントローラ（Third Party Wireless Controllers）] の順に選択します。

スイッチ コントローラに関するシステム詳細の表示とスイッチ リストの設定

スイッチに関する次の詳細情報を表示するには、[モニタ（Monitor）]>[管理対象要素（Managed Elements）] > [ネットワークデバイス（Network Devices）] > [スイッチとハブ（Switches and Hubs）] の順に選択します。

- スイッチの検索

特定のスイッチを検索するか、またはカスタム検索を作成して保存するには、Prime Infrastructure の検索機能を使用します。

- スイッチの表示

[スイッチリスト（Switch List）] ページの設定

[ビューの編集（Edit View）]ページでは、[スイッチ（Switches）]テーブルの列を追加、削除、または並べ替えできます。

テーブルの列を編集する手順は、次のとおりです。

ステップ 1 [モニタ（Monitor）] > [管理対象要素（Managed Elements）] > [ネットワーク デバイス（Network Devices）] > [スイッチとハブ（Switches and Hubs）] の順に選択します。

ステップ 2 [ビューの編集（Edit View）] リンクをクリックします。

ステップ 3 テーブルに新しい列を追加するには、左側の列で、追加する列見出しをクリックして強調表示します。[表示（Show）] をクリックして、選択した列見出しを右側の領域へ移動します。右側の領域にあるすべての項目が表に表示されます。

ステップ 4 テーブルから列を削除するには、右側の列で、削除する列見出しをクリックして強調表示します。[非表示（Hide）] をクリックして、選択した列見出しを左側の領域へ移動します。左側の領域にある項目はすべて、表に表示されません。

ステップ 5 [上へ（Up）] ボタンと [下へ（Down）] ボタンを使用して、表内での情報の並び順を指定します。目的の列見出しを選択し、[上へ（Up）] または [下へ（Down）] をクリックして、現在のリスト内での位置を上下に移動します。

ステップ 6 デフォルト表示に戻すには、[リセット（Reset）] をクリックします。

ステップ 7 [送信（Submit）] をクリックして、変更内容を確定します。

モニタ アクセス ポイント

この項では、コントローラのアクセス ポイントの概要の詳細へのアクセスについて説明します。それぞれのアクセス ポイントの詳細にアクセスするには、メインの日付領域を使用します。

このページにアクセスするには、[モニタ（Monitor）] > [ワイヤレス テクノロジー（Wireless Technologies）] > [アクセス ポイントの無線（Access Point Radios）] の順に選択します。

関連トピック

アクセス ポイントの表示 （6 ページ）
アクセス ポイントに関するシステムの詳細の表示 （9 ページ）

アクセス ポイントの表示

デフォルト情報を含むアクセス ポイントの概要を表示するには、[モニタ（Monitor）] > [ワイヤレステクノロジー（Wireless Technologies）]>[アクセスポイントの無線（Access Point Radios）] の順に選択するか、またはアクセス ポイントの検索を実行します。

関連トピック

アクセス ポイントのレポート タイプ （7 ページ）
スイッチ コントローラに関するシステム詳細の表示とスイッチ リストの設定 （5 ページ）

アクセス ポイントのレポート タイプ

次のレポートは、アクセスポイントに対して生成できます。次のレポートは、カスタマイズできません。

- [ロード（Load）]：トラフィック負荷は、トラフィックの送受信のために使用される合計帯域幅です。これにより、WLAN管理者は、ネットワークの拡大状況を追跡し、クライアントの需要を見越してネットワーク拡張の計画を立てることができます。
- [動的電力制御（Dynamic Power Control）]：動的電力制御情報が含まれるレポートを生成します。
- [ノイズ（Noise）]：ノイズ情報が含まれるレポートを生成します。ノイズレポートには、選択したアクセス ポイントの各チャネルのノイズ（dBm 単位の RSSI）の棒グラフが表示されます。
- [干渉（Interference）]：[干渉（Interference）] レポートには、各チャネルの干渉（dBm 単位の RSSI）の棒グラフが表示されます。
  - 高干渉：40 ～ 0 dBm
  - 中程度干渉：100 ～ -40 dBm
  - 低干渉：110 ～ -100 dBm
- [カバレッジ（RSSI）（Coverage (RSSI)）]：[カバレッジ（RSSI）（Coverage (RSSI)）] レポートには、クライアント数対 dBm 単位の RSSI を示す、受信信号強度ごとのクライアント分布の棒グラフが表示されます。
- [カバレッジ（SNR）（Coverage (SNR)）]：[アクセスポイントのカバレッジ（SNR）（Access Points Coverage (SNR)）] レポートには、クライアント数対 SNR を示す、信号対雑音比ごとのクライアント分布の棒グラフが表示されます。
- [アップ/ダウン統計情報（Up/Down Statistics）]：[アップ/ダウン統計情報（Up/Down Statistics）] レポートには、時間に対するアクセス ポイントのアップ タイムの折れ線グラフが表示されます。最後のリブートからの経過時間（日数、時間、および分単位）。
- [ネットワークエアタイムフェアネス統計情報（Network Airtime Fairness Statistics）]：[ネットワークエアタイムフェアネス統計情報（Network Airtime Fairness Statistics）] は、選択した時間間隔で複数の異なる WLAN プロファイルで使用された平均エアタイムの表形式の表示です。
- [音声統計情報（Voice Statistics）]：音声トラフィックによる無線使用率を示す、選択したアクセス ポイントのレポートを生成します。[音声統計情報（Voice Statistics）] レポートには、音声トラフィックごとの次の無線使用率の統計情報が表示されます。
  - アクセス ポイント名
  - 無線
  - 進行中のコール
  - 進行中のローミング コール
  - 使用中の帯域幅

音声統計情報レポートは、CAC/WMM クライアントのみに適用されます。

- [音声TSMテーブル（Voice TSM Table）]：[音声トラフィックストリームメトリックテーブル（Voice Traffic Stream Metrics Table）] は、選択したアクセス ポイントと無線に対して生成します。クライアント デバイスごとに、その音声トラフィック ストリームの QoS ステータス、PLR、および遅延が表示されます。
- [音声TSMレポート（Voice TSM Reports）]：[音声トラフィックストリームメトリックテーブル（Voice Traffic Stream Metrics Table）] レポートは、[音声トラフィックストリームメトリックテーブル（Voice Traffic Stream Metrics Table）] をグラフィカル表示したものです。ただし、複数のクライアントからのメトリックが選択したアクセスポイントのグラフ上で平均されています。
- [802.11のカウンタ（8o2.11 Counters）]：[8o2.11のカウンタ（8o2.11 Counters）] レポートには、MAC レイヤでのアクセス ポイントのカウンタが表示されます。エラー フレーム、フラグメント数、RTS/CTS フレーム数、再試行フレームなどの統計情報は、フィルタリング基準に基づいて生成され、MAC 層のパフォーマンス（および問題）を解釈するために役立ちます。
- [アクセスポイントのプロファイルステータス（Access Points Profile Status）]：[アクセスポイントのプロファイルステータス（Access Points Profile Status）] には、アクセス ポイントの負荷、ノイズ、干渉、およびカバレッジ プロファイルのステータスが表示されます。
- [電波品質と時間の対比（Air Quality vs. Time）]：[無線使用率（Radio Utilization）] レポートには、レポート生成時に使用したフィルタリング基準に基づき、アクセスポイント無線の使用率の傾向が表示されます。このレポートは、現在のネットワークのパフォーマンスを識別し、今後のスケーラビリティの必要性に応じて容量を計画するうえで役立ちます。[無線使用率（Radio Utilization）] レポートには、設定された期間の間のワイヤレス ネットワークの電波品質の指標が表示されます。
- [トラフィックストリームメトリック（Traffic Stream Metrics）]：[トラフィックストリームメトリック（Traffic Stream Metrics）] レポートは、指定したクライアントの現在および過去の Quality of Service（QoS）を無線レベルで判断する場合に役立ちます。また、パケット損失率、平均キューイング遅延、遅延パケットの配布、ローミング遅延などのアップリンクおよびダウンリンク統計情報も表示されます。
- [Tx Powerおよびチャネル（Tx Power and Channel）]：[Tx Powerおよびチャネル（Tx Power and Channel）] レポートには、レポートの生成時に使用したフィルタリング基準に基づき、デバイスのチャネル計画の割り当ておよび送信電力レベルの傾向が表示されます。予期しない動作やネットワークのパフォーマンスの問題を識別するために役立ちます。

Current Tx Power Level 設定は、最大伝導送信電力を制御します。最大使用可能送信電力は、設定されたチャネル、個々の国の規制、およびアクセス ポイントの機能に応じて異なります。アクセス ポイントの機能を確認するには、『Product Guide』または各モデルのデータ シートを参照してください。

[現在のTx Powerレベル（Current Tx Power Level）] の設定 1 は、アクセス ポイントの最大伝導電力設定を表します。それ以降のそれぞれの電力レベル（たとえば、2、3、4 など）は、直前の電力レベルからの約 50 %（または 3 dBm）の送信電力の低下を表します。実際の電力低下は、アクセス ポイントのモデルによって若干異なる場合があります。

設定されたアンテナのゲイン、設定されたチャネル、および設定された電力レベルに基づき、特定の国の規制を超えないように、アクセス ポイントでの実際の送信電力が低減されることがあります。

割り当て方式に[グローバル（Global）]と[カスタム（Custom）]のいずれを選択したかにかかわらず、アクセスポイントでの実際の伝導送信電力は、国固有の規制を超えないように確認されます。

次のコマンド ボタンは伝送レベルを設定するために利用できます。

- [保存（Save）]：現在の設定を保存します。
- [監査（Audit）]：このアクセス ポイントの現在のステータスを検出します。
- [VoIPコールのグラフ（VoIP Calls Graph）]：[VoIPコールのグラフ（VoIP Calls Graph）]は、ネットワーク上の VoIP コール（無線ごと）の数と期間の詳細を時間とともに表示するなど、音声の観点からワイヤレス ネットワークの使用状況を分析します。このレポートから有益なデータを収集できるようにするには、WLAN で VoIP スヌーピングを有効にする必要があります。このレポートでは、グラフで情報が表示されます。
- [VoIPコールの表（VoIP Calls Table）]：[VoIPコールの表（VoIP Calls Table）]には、[VoIPコールのグラフ（VoIP Calls Graph）]レポートと同じ情報が表形式で表示されます。
- [音声統計情報（Voice Statistics）]：[音声統計情報（Voice Statistics）]レポートは、ネットワーク上の音声クライアント、ボイス コール、ローミング コール、および拒否されたコール（無線ごと）によって使用された帯域幅のパーセンテージなどの詳細を表示することで、音声の観点からワイヤレス ネットワークの使用状況を分析します。このレポートから有用なデータを収集するためには、コール アドミッション制御（CAC）が音声クライアントでサポートされていることを確認してください。
- [電波品質が最低の AP（Worst Air Quality APs）]：干渉の問題がネットワークに影響を与えている箇所を理解できるように、概要的なわかりやすいメトリックが提供されます。電波品質（AQ）はチャネル、フロア、およびシステム レベルで報告され、AQ が望ましいしきい値を下回った場合に自動的に通知されるように AQ アラートがサポートされています。

アクセス ポイントに関するシステムの詳細の表示

[アクセスポイントの詳細（Access Points Details）]ページでは、1 つのアクセス ポイントのアクセス ポイント情報を参照できます。

このページにアクセスするには、[モニタ（Monitor）]>[ワイヤレス テクノロジー（Wireless Technologies）]>[アクセス ポイントの無線（Access Point Radios）]を選択して、[AP 名（AP Name）]列のアクセス ポイント名をクリックします。アクセス ポイントの種類に応じて、次のタブが表示されます。

- [全般（General）]タブ

[一般（General）]タブのフィールドは、Lightweight アクセス ポイントと Autonomous アクセス ポイントで異なります。

自律クライアントについては、Prime Infrastructure はクライアント数のみを収集します。[モニタ（Monitor）]ページとレポートのクライアント数には、自律クライアントが含まれています。クライアント検索、クライアント トラフィック グラフ、その他のクライアント レポート（一意のクライアント（Unique Clients）、最もビジーなクライアント（Busiest Clients）、クラ

イアント関連付け（Client Association）など）には、自律アクセス ポイントからのクライアントは含まれていません。

- [インターフェイス（Interfaces）] タブ
- [CDP ネイバー（CDP Neighbors）] タブ

このタブは、CDP が有効になっている場合のみ表示されます。

- [現在関連付けられているクライアント（Current Associated Clients）] タブ

このタブは、アクセス ポイント（CAPWAP またはAutonomous アクセス ポイント）に関連付けられているクライアントがある場合にのみ表示されます。

- [SSID] タブ

このタブは、アクセス ポイントが Autonomous アクセス ポイントであり、アクセス ポイントで SSID が設定されている場合のみ表示されます。

- [一定期間のクライアント（Clients Over Time）] タブ

このタブには、次のチャートが表示されます。

- [アクセスポイントでのクライアント数（Client Count on Access Point）] : アクセス ポイントに現在関連付けられているクライアントの総数が、時間とともに表示されます。
- [アクセスポイントでのクライアントトラフィック（Client Traffic on Access Point）] : アクセスポイントに接続されているクライアントによって生成されたトラフィックが、時間とともに表示されます。

これらのチャートに表示される情報は、時間ベースのグラフに表示されます。時間ベースのグラフには、グラフ ページの上部に、6 時間、1 日、1 週間、2 週間、4 週間、3 ヵ月、6 ヵ月、1 年、およびカスタムを表示するリンク バーがあります。選択すると、そのタイム フレームのデータが取得され、対応するグラフが表示されます。

関連トピック

アクセス ポイントのレポート タイプ （7 ページ）

アクセス ポイント無線 Air Time Fairness 情報の表示

High Density Experience（HDX）のためのシスコ エアタイム フェアネス（ATF）により、ネットワーク管理者は、定義済みカテゴリのデバイスをグループ化し、いくつかのグループがWLANからのトラフィックを他のグループよりも頻繁に受信できるようにします。したがって、あるグループには他のグループよりも多くのエア タイムが割り当てられます。

Cisco ATF には次の機能があります。

- ユーザ グループまたはデバイス カテゴリに対して Wi-Fi のエア タイムを割り当てる
- エア タイム フェアネスは、ネットワークではなくネットワーク管理者によって定義される
- エア タイムを割り当てるための簡素化された仕組みを提供する
- WLAN の状態の変化に動的に適応する

- サービス レベル契約をより効率的に実現する
- 各種の標準規格に準拠した Wi-Fi QoS のメカニズムを向上させる

ATF の統計情報をモニタするには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [ワイヤレステクノロジー（Wireless Technologies）] > [アクセスポイントの無線（Access Point Radios）]** の順に選択します。

ステップ 2 [無線（Radio）] 列から、目的の無線名をクリックします。

アクセス ポイントの種類に応じて、異なるタブが表示されます。

ステップ 3 [アクセス ポイントの無線の詳細（Access Point Radio Details）] で、[エア タイム フェアネス（Air Time Fairness）] タブを選択します。

次のチャートが表示されます。

- [エア タイム絶対使用率（Air Time Usage Absolute）]：このチャートは、測定された時間間隔における、無線上での WLAN のエア タイム使用率をパーセンテージで表します。
  - カレンダー アイコンをクリックして、開始日と年、および終了日と年を選択するか、プリセット値を選択します。利用可能なプリセット値は、1h、6h、1d、1w、2w、4w、3m、6m および 1y です。
- [エア タイム相対使用率（Air Time Usage Relative）]：このチャートは、無線上での WLAN 全体のうち、ある WLAN のエア タイム使用率をパーセンテージで表します。
- カレンダー アイコンをクリックして、開始日と年、および終了日と年を選択するか、プリセット値を選択します。利用可能なプリセット値は、1h、6h、1d、1w、2w、4w、3m、6m および 1y です。

不正アクセス ポイントとは

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。不正なアクセス 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して無線 LAN の運用を妨害する可能性があります。つまり、ハッカーは、不正なアクセス ポイントを使用することで、ユーザ名やパスワードなどの機密情報を入手することができます。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。アクセス ポイントになりすましてこの CTS フレームが送信され、特定のクライアントには送信を許可し、他のすべてのクライアントには待機するように指示が送られると、正規のクライアントは、ネットワーク リソースに接続できなくなってしまいます。このため、無線 LAN のサービス プロバイダーは、無線周波数帯で不正なアクセス ポイントを禁止する方法に強い関心を持っています。

不正なアクセス ポイントは安価で簡単に利用できることから、企業の従業員は、IT 部門に報告して同意を得ることなく、許可されていない不正なアクセス ポイントを既存の LAN に接続し、アドホック無線ネットワークを確立することがあります。これらの不正なアクセス 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 セキュリティ侵害につながるおそれがあります。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、セキュリティで保護されていないアクセス ポイントの場所が無線ユーザにより頻繁に公開されるため、企業のセキュリティが侵害される可能性も増大します。

関連トピック

Cisco Prime Infrastructure が不正アクセス ポイントを検出する仕組み （12 ページ）
不正アクセス ポイント状態の判断方法 （13 ページ）
不正アクセス ポイント アラームの表示 （16 ページ）
アドホック不正とは （18 ページ）
不正アクセス ポイント クライアントの表示 （17 ページ）
Prime Infrastructure が不正アクセス ポイントを検索、タグ付け、および包含する方法 （19 ページ）

Cisco Prime Infrastructure が不正アクセス ポイントを検出する仕組み

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。Prime Infrastructure は、すべてのコントローラの不正アクセス ポイント データを統合します。

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）に設定された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。

不正アクセス ポイントのパーティションは、検出中のいずれかのアクセス ポイント（最新または最も強い RSSI 値を持つアクセス ポイント）と関連付けられます。検出中のアクセス ポイント情報がある場合、Prime Infrastructure は検出中のコントローラを使用します。不正アクセス ポイントが異なるパーティションに存在する 2 つのコントローラによって検出された場合、不正アクセス ポイントのパーティションは随時変更される場合があります。

関連トピック

不正アクセス ポイントとは （11 ページ）
不正アクセス ポイント状態の判断方法 （13 ページ）
不正アクセス ポイント アラームの表示 （16 ページ）

アドホック不正アクセス ポイント アラームの表示 （18 ページ）

不正アクセス ポイント状態の判断方法

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。

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。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。

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む）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、未知のアクセス ポイントが安全な 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。

関連トピック

不正アクセス ポイントとは （11 ページ）
Cisco Prime Infrastructure が不正アクセス ポイントを検出する仕組み （12 ページ）
不正アクセス ポイントの分類方法 （14 ページ）

不正アクセス ポイントの分類方法

次の表に、未知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 *2:* 設定可能な分類タイプ/不正の状態の推移

送信元（From）	宛先
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。

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 [セキュリティ（Security）] ダッシュボードには、過去 1 時間、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 [危険性のないアクセスポイント（Friendly Access Point）] 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。

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。

ユーザのみが不正アクセス ポイントの MAC アドレスを [危険性のないアクセスポイント（Friendly Access Point）] リストに追加できます。Prime Infrastructure では、危険性のないアクセス ポイントの MAC アドレスはコントローラに適用されません。

Prime Infrastructure ホーム ページの [セキュリティ（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：不明なアクセス 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：不明なアクセス 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 [危険性のないアクセスポイント（Friendly Access Point）] 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。

[危険性のないアクセスポイント（Friendly Access Point）] リストから不正アクセス ポイントを削除するには、Prime Infrastructure とコントローラの両方で不正アクセス ポイントが [危険性のないアクセスポイント（Friendly Access Point）] リストから削除されることを確認します。不正アクセス ポイントを、[危険性のない内部アクセスポイント（Friendly Access Point Internal）] または [危険性のない外部アクセスポイント（Friendly Access Point External）] から [未分類アラート（Unclassified Alert）] または [悪意のあるアラート（Malicious Alert）] に変更します。

未分類の不正アクセス ポイント

不正アクセス ポイントは、[悪意のある（Malicious）] または [危険性のない（Friendly）] に分類されていない場合、未分類と呼ばれます。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 [セキュリティ（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、不明なアクセス 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、不明なアクセス 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 [危険性のないアクセスポイント（Friendly Access Point）] 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：不明なアクセス 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。

関連トピック

不正アクセス ポイントとは （11 ページ）
Cisco Prime Infrastructure が不正アクセス ポイントを検出する仕組み （12 ページ）

不正アクセス ポイント アラームの表示

不正アクセス ポイント無線は、1 つ以上の Cisco 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。[不正アクセスポイントアラーム（Rogue Access Point Alarms）] ページを開くには、次の手順を実行します。

- 不正 AP を検索します。

- [ダッシュボード（Dashboard）] > [ワイヤレス（Wireless）] > [セキュリティ（Security）] に移動します。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。
- [アラームのまとめ（Alarm Summary）] の [AP 番号（AP number）] リンクをクリックします。

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。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。

不正アクセス ポイントのパーティションは、検出中のいずれかのアクセス ポイント（最新または最も強い RSSI 値を持つアクセス ポイント）と関連付けられます。検出中のアクセス ポイント情報がある場合、Prime Infrastructure は検出中のコントローラを使用します。不正アクセス ポイントが異なるパーティションに存在する 2 つのコントローラによって検出された場合、不正アクセス ポイントのパーティションは随時変更される場合があります。

Prime Infrastructure によるポーリング時に、一部のデータが変更または更新されることがあります。このため、表示される不正データの一部（[Strongest AP RSSI]、[No. of Rogue Clients]、[Channel]、[SSID]、および [Radio Types]）が不正の存続期間中に変わることがあります。

[不正アクセスポイントアラーム（Rogue Access Point Alarms）] リスト ページで、各不正アクセス ポイントに関するアラーム イベントの詳細を参照できます。

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、[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）] の順に選択して、任意の行の矢印アイコンをクリックして [不正アクセスポイントアラームの詳細（Rogue Access Point Alarm Details）] ページを表示します。

[すべてのアラームの詳細（All Alarm Details）] ページのフィールド（[No. of Rogue Clients] 以外）は、ポーリングを通じてデータが設定され、2 時間ごとに更新されます。不正クライアントの数はリアルタイムの数であり、不正アクセス ポイント アラームの [アラームの詳細（Alarm Details）] ページにアクセスするたびに更新されます。

コントローラ（バージョン 7.4 または 7.5）がカスタムの不正アクセス ポイント アラームを送信すると、Prime Infrastructure は未分類の不正アラームとしてこれを表示します。これは、Prime Infrastructure がカスタムの不正アクセス ポイント アラームをサポートしていないためです。

Prime Infrastructure によるポーリング時に、一部のデータが変更または更新されることがあります。このため、表示される不正データの一部（[Strongest AP RSSI]、[No. of Rogue Clients]、[Channel]、[SSID]、および [Radio Types]）が不正の存続期間中に変わることがあります。

不正アクセス ポイント クライアントの表示

不正クライアントは、次のいくつかの方法で表示できます。

- Prime Infrastructure 機能を使用して不正クライアントを検索します。
- 該当する不正アクセス ポイントの [アラームの詳細（Alarm Details）] ページから、特定の不正アクセス ポイントの不正クライアントのリストを表示します。該当する不正クライア

ントの不正MACアドレスをクリックし、[不正クライアントの詳細（Rogue Client details）]ページを表示します。

- 不正アクセス ポイントの [アラームの詳細（Alarms Details）] ページで、[コマンドの選択（Select a command）] ドロップダウン リストから [不正クライアント（Rogue Clients）] を選択します。

[不正クライアント（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、そのコントローラ、および関連付けられている不正アクセス ポイントが表示されます。

不正クライアントのステータスには、Contained（コントローラにより、攻撃しているデバイスの信号が認可されたクライアントに干渉しないように封じ込められています）、Alert（コントローラは即時アラートをシステム管理者に転送し、さらなる処置を求めます）、およびThreat（不正は既知の脅威です）があります。不正アクセス ポイントの脅威が高いほど、高い封じ込め処理が必要です。

不正クライアントの**クライアント MAC アドレス**をクリックすると、[不正クライアントの詳細（Rogue Client details）] ページが表示されます。

関連トピック

不正アクセス ポイントとは （11 ページ）
不正アクセス ポイント アラームの表示 （16 ページ）
アドホック不正アクセス ポイント アラームの表示 （18 ページ）

アドホック不正とは

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 アドレスが認可された 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。

関連トピック

アドホック不正アクセス ポイント アラームの表示 （18 ページ）
不正アクセス ポイント クライアントの表示 （17 ページ）

アドホック不正アクセス ポイント アラームの表示

[アドホック不正アラーム（Adhoc Rogue Alarms）] ページには、アドホック不正のアラーム イベントが表示されます。[アドホック不正アラーム（Adhoc Rogue Alarms）] ページにアクセスするには、次の手順を実行します。

- アドホック不正のアラームの検索を実行します。
- [ダッシュボード（Dashboard）] > [ワイヤレス（Wireless）] > [セキュリティ（Security）] に移動します。このページには、過去 1 時間と過去 24 時間に検出されたアドホック不正がすべて表示されます。アドホック不正の番号をクリックすると、アドホック不正のアラームが表示されます。

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。

Prime Infrastructure によるポーリング時に、一部のデータが変更または更新されることがあります。このため、表示される不正データの一部（[Strongest AP RSSI]、[No. of Rogue Clients]、[Channel]、[SSID]、および [Radio Types]）が不正の存続期間中に変わることがあります。

[アドホック不正アラーム（Adhoc Rogue Alarms）] ページから、各アドホック不正に関するアラーム イベント情報を参照できます。不正アクセス ポイント無線は、Cisco 1000 シリーズ Lightweight AP によって検出された未許可のアクセス ポイントです。

アドホック不正無線のアラーム イベントを表示するには、[アドホック不正アラーム（Adhoc Rogue Alarms）] ページで該当する不正 MAC アドレスをクリックします。

Prime Infrastructure によるポーリング時に、一部のデータが変更または更新されることがあります。このため、表示される不正データの一部（[Strongest AP RSSI]、[No. of Rogue Clients]、[Channel]、[SSID]、[Radio Types] など）が不正の存続期間中に変更される可能性があります。

スイッチ ポート トレースは、重大度、状態などの不正の属性を更新しないので、不正がスイッチ ポート トレースを使用して検出された場合はアラームはトリガーされません。

Prime Infrastructure が不正アクセス ポイントを検索、タグ付け、および包含する方法

Prime Infrastructure は、不正なアクセス ポイント トラップとしてフラグを生成し、既知の不正アクセス ポイントを Cisco Unified Network Solution が監視している MAC アドレスで表示します。

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します。これらのアクセス ポイントは次のように分類されます。

- 既知または承認済みの不正アクセス ポイント（追加のアクションなし）
- アラートの不正アクセス ポイント（アクティブの場合は監視して通知）
- 封じ込められている不正アクセス ポイント

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 WLAN 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 WLAN 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。

関連トピック

不正アクセス ポイントを検出する Lightweight アクセス ポイントの識別 （20 ページ）

不正アクセス ポイントを検出する Lightweight アクセス ポイントの識別

不正アクセス ポイントを検出している Cisco Lightweight AP 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。

[不正アクセス ポイント アラーム（Rogue Access Point 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 [不正アクセス ポイント アラーム（Rogue Access Point Alarms）] ページを表示するには、次のいずれかを実行します。

- 不正アクセス ポイントの検索を実行します。
- [ダッシュボード（Dashboard）] > [ワイヤレス（Wireless）] > [セキュリティ（Security）] に移動します。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。
- [アラームのまとめ（Alarm Summary）] ボックスの [悪意のある AP 番号（Malicious AP number）] リンクをクリックします。

ステップ 2 [不正アクセス ポイント アラーム（Rogue Access Point Alarms）] ページで、該当する不正アクセス ポイントの [不正 MAC アドレス（Rogue MAC Address）] をクリックします。[不正アクセス ポイント アラーム（Rogue Access Point Alarms）] の詳細ページが表示されます。

ステップ 3 [コマンドの選択（Select a command）] ドロップダウン リストから、**[APの検出（Detecting APs）]** を選択します。

ステップ 4 **[移動（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。

関連トピック

Prime Infrastructure が不正アクセス ポイントを検索、タグ付け、および包含する方法 （19 ページ）

Spectrum Expert からのアクセス ポイント干渉情報の表示

Spectrum Expert クライアントは、リモート干渉センサーとして機能し、動的な干渉データを Prime Infrastructure に送信します。この機能により、Prime Infrastructure はネットワーク内の Spectrum Expert から詳細な干渉データと電波品質データを収集、保管、およびモニタできます。

[Spectrum Expert のモニタ（Monitor Spectrum Experts）] ページにアクセスするには、次の手順を実行します。

[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [Spectrum Experts] の順に選択します。

左側のサイドバーのメニューから、[Spectrum Expert の概要（Spectrum Experts Summary）] ページにアクセスできます。

WiFi TDOA レシーバのモニタ

WiFi TDOA レシーバは、追跡対象のタグ付き資産から送信される信号を受信するように設計された外部システムです。その後これらの信号は、資産の位置計算に役立つよう、Mobility Services Engine に転送されます。

関連トピック

WiFi TDOA レシーバによるタグ位置レポートの強化
Prime Infrastructure およびマップへの WiFi TDOA レシーバの追加

[無線リソース管理（Radio Resource Management Dashboard）] ダッシュボードを使用したRFパフォーマンスの表示

無線リソース管理（RRM）は Cisco Unified Wireless Network に組み込まれており、RF 環境で見つかったパフォーマンス上の問題をモニタし動的に修正します。Prime Infrastructure は、アクセス ポイントの送信電力またはチャネルが変化した際にトラップを受信します。こうしたトラップ イベントまたは RF の再グループ化などの同様のイベントは、Prime Infrastructure に記録され、イベント ディスパッチャによって保持されます。

RRM は、ネットワークに追加された新しいコントローラや Lightweight アクセス ポイントを自動的に検出して設定します。それは、アソシエートされている近くの Lightweight アクセス ポイントを自動的に調整して、カバレッジとキャパシティを最適化します。Lightweight アクセス ポイントは、使用国で有効なすべての 802.11b/g チャネルに加えて、他の地域で使用可能なチャネルも同時にスキャンできます。アクセス ポイントは、これらのチャネルのノイズや干渉を監視する際、最大で 60 ミリ秒の間オフチャネルになります。不正アクセス ポイント、不正クライアント、アドホック クライアント、干渉しているアクセス ポイントを検出するために、この間に収集されたパケットが解析されます。

次の通知は RRM ダッシュボードに送信されます。

- チャネルの変更通知は、チャネルの変更が発生すると送信されます。チャネルの変更は、動的チャネル割り当て（DCA）設定に左右されます。
- 送信電力の変更通知は、送信電力の変更が発生すると送信されます。原因コードは、イベントが発生した理由の数に関係なく、1 という係数が与えられます。
- RF グループ化通知は、RF グループ化のコンテンツの変更があり、自動グループ化がイネーブルの場合に送信されます。

RRM ダッシュボード情報を表示するには、[モニタ（Monitor）] > [ワイヤレステクノロジー（Wireless Technologies）] > [無線リソースの管理（Radio Resource Management）] を選択します。

アクセス ポイントのアラームとイベントの表示

ネットワークのアクセス ポイントのアラームをモニタリングするには、次の手順を実行します。

ステップ 1 次に対して詳細検索を実行します。

a) パフォーマンス アラーム
b) CleanAir セキュリティ アラーム
c) wIPS DoS アラーム

ステップ 2 アラームの横にあるチェックボックスを選択し、[アラーム ブラウザ（Alarm Browser）] ツールバーで必要なフィールドを変更します。

アクセス ポイント障害オブジェクトの表示

障害のあるオブジェクトをモニタリングするには、次の手順を実行します。

ステップ 1 [モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）] の順に選択し、[イベント（Events）] タブをクリックします。

ステップ 2 [説明（Description）] 列の左側にある展開アイコンをクリックします。選択したイベントの種類に応じて、関連付けられている詳細が異なります。

アクセス ポイントの不正アクセス ポイントの表示

不正アクセス ポイントのイベントをモニタリングするには、次の手順を実行します。

ステップ 1 [モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）] の順に選択し、[イベント（Events）] タブをクリックします。

ステップ 2 不正 AP をモニタするには、クイック フィルタまたは高度なフィルタ機能を使用します。

ステップ 3 不正アクセス ポイント無線のアラーム イベントを表示するには、展開アイコンをクリックします。

アクセス ポイントのアドホック不正の表示

アドホック不正のイベントをモニタリングするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）] の順に選択し、[イベント（Events）] タブをクリックします。	
ステップ 2	アドホック不正 AP のイベントをモニタするには、クイック フィルタまたは高度なフィルタ機能を使用します。	

	コマンドまたはアクション	目的
ステップ 3	アドホック不正アクセス ポイントのアラーム イベントを表示するには、展開アイコンをクリックします。	

関連トピック

不正アクセス ポイントとは （11 ページ）

アクセス ポイントの適応型 wIPS イベントの表示

Cisco Adaptive wIPS のイベントをモニタリングするには、次の手順を実行します。

ステップ 1 [モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）] の順に選択し、[イベント（Events）] タブをクリックします。

ステップ 2 検索結果を絞り込んで wIPS イベントをモニタするには、クイック フィルタまたは高度なフィルタ機能を使用します。1 つ以上のイベントによって、異常ステートまたはアラームが生成されることがあります。アラームはクリアできますが、イベントは残ります。

アクセス ポイントの CleanAir 電波品質イベントの表示

ワイヤレス ネットワークの CleanAir 電波品質に関して生成されたイベントを表示するには、次の手順を実行します。

パフォーマンス イベントの詳細検索を実行します。

[詳細検索（Search Results）] ページには、重大度、障害の発生源、および日時に関する情報が表示されます。

次のタスク

電波品質イベントの詳細を表示するには、[電波品質イベント（Air Quality Events）] ページの [重大度（Severity）] 列の横にある展開アイコンをクリックします。

アクセス ポイントの干渉源セキュリティ リスク イベントの表示

干渉源セキュリティ リスク イベントをモニタリングするには、次の手順を実行します。

ワイヤレス ネットワークで生成されたセキュリティ リスク イベントを表示するには、セキュリティ イベントの詳細検索を実行します。

[詳細検索（Search Results）] ページには、重大度、障害の発生源、日時に関する次の CleanAir 電波品質イベントの情報が表示されます。

次のタスク

干渉原セキュリティ イベントの詳細を表示するには、[重大度（Severity）] 列の横にある展開アイコンをクリックします。

アクセス ポイントのヘルス モニタ イベントの表示

ヘルス モニタ イベントを表示するには、次の手順を実行します。

Prime Infrastructure イベントの詳細検索を実行します。

[検索結果（Search Results）] ページには、重大度、障害の発生源、メッセージ、および日時に関する情報が表示されます。

ヘルス モニタ イベントの詳細の表示

ヘルス モニタ イベントの詳細を表示するには、[重要度（Severity）] 列の隣にある展開アイコンをクリックし、アラームの詳細ページにアクセスします。

関連トピック

アクセス ポイントのヘルス モニタ イベントの表示 （25 ページ）