



## 不正管理ダッシュボードのモニタリング

- [不正管理アプリケーション \(1 ページ\)](#)
- [不正管理ダッシュボードの監視 \(1 ページ\)](#)
- [脅威 360° ビューから不正 AP の詳細を取得する \(3 ページ\)](#)

### 不正管理アプリケーション

不正管理アプリケーションにアクセスするには、Cisco DNA Center にログインし、Cisco DNA Center ホームページで、[\[アシュアランス \(Assurance\)\]](#) > [\[ダッシュボード \(Dashboard\)\]](#) > [\[不正管理 \(Rogue Management\)\]](#) を選択します。

[\[不正管理 \(Rogue Management\)\]](#) ダッシュボードウィンドウが表示されます。



- (注) アシュアランスアプリケーションを使用する前に、Cisco DNA アシュアランスを設定する必要があります。詳細については、「[基本的な設定のワークフロー](#)」を参照してください。

### 不正管理ダッシュボードの監視

ネットワークで検出されたすべての不正 AP の詳細な脅威分析とグローバルビューを表示するには、不正管理ダッシュボードを使用します。また、不正管理ダッシュボードは、最も優先度の高い脅威についての洞察を提供し、迅速に識別できるようにします。不正管理アプリケーションは、ストリーミングテレメトリを使用して不正上のデータを取得します。

**ステップ 1** Cisco DNA Center ホームページから [\[アシュアランス \(Assurance\)\]](#) > [\[ダッシュボード \(Dashboard\)\]](#) > [\[不正アクセスポイントの管理 \(Rogue Management\)\]](#) を選択します。

**ステップ 2** [\[不正管理 \(Rogue Management\)\]](#) ウィンドウには、次の情報が表示されます。

- (注) Cisco AireOS コントローラが最小ソフトウェアバージョンを満たしていない場合は、ダッシュボードの上部に通知が表示されます。通知の [\[デバイスに移動 \(Go To Devices\)\]](#) をクリックして、サポートされているバージョンにアップグレードします。

- **[不正管理 (Rogue Management)]** ウィンドウの右上隅にある **[不正 (Rogue)]** ドロップダウンリストから、次の機能を実行できます。
  - シスコ ワイヤレス コントローラおよび Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで不正検出を有効にするには、**[有効化 (Enable)]** を選択します。  
Cisco DNA Center リリース 1.3.1.x から Cisco DNA Center リリース 1.3.3.0 に移行する場合は、不正管理サブスクリプションを有効にする必要があります。Cisco DNA Center リリース 1.3.3.0 で追加された新しいデバイスで不正管理サブスクリプションが有効になっていない場合、これらのデバイスは有効になるまで不正管理設定を取得しません。不正管理アプリケーションを有効にすると、不正管理をサポートする新しいワイヤレス コントローラが Cisco DNA Center に追加されると、不正管理アプリケーションが有効になります。
  - 不正アクションを一時的に無効にするには、**[無効化 (disable)]** を選択します。  
表示される **[警告 (Warning)]** ダイアログボックスで **[はい (Yes)]** をクリックします。  
不正管理機能が無効にすると、ワイヤレス コントローラのデータは、不正管理機能が有効になるまで、Cisco DNA Center にプッシュされません。
  - **[ステータス (Status)]** を選択して、不正な設定ジョブのステータスを表示します。
    - **[すべて (All)]**、**[失敗 (Failure)]**、**[成功 (Success)]**、または **[進行中 (Progress)]** の各タブをクリックして、不正な設定ステータスをフィルタリングします。
    - コントローラで不正検出操作が正常に有効化された場合は、**[操作 (Operation)]** 列に **[有効 (Enable)]** が表示されます。  
設定の変更がコントローラに正常にプッシュされた場合、**[ステータス (Status)]** 列に **[成功 (Success)]** と表示されます。
- 時間とアクティブな高脅威グラフの高い脅威は、デフォルトで過去 3 時間に検出された不正 AP に関する情報を表示します。グラフ情報は、**[不正管理 (Rogue Management)]** ウィンドウの右上隅にあるドロップダウンリストから選択した時間間隔に基づいています。  
オプションは、**[直近3時間 (Last 3 Hours)]**、**[直近24時間 (Last 24 Hours)]**、および **[直近7日間 (Last 7 Days)]** です。
- ネットワーク内のサイトのグローバルマップビューを表示するには、 **[不正管理 (Rogue Management)]** ウィンドウの右上隅にある **[マップの表示 (Show map)]** アイコンをクリックします。
- タイムスライダを移動して、特定の時間の脅威に関するデータを表示します。タイムラインスライダの下にある **[時間の経過に伴う高レベルの脅威 (High Threats Over Time)]** と **[活発で高レベルの脅威 (Active High Threats)]** のグラフには、それぞれ詳細が表示されます。
- **[活発で高レベルの脅威 (Active High Threats)]** ウィジェットは、ドーナツグラフの形式で脅威レベルに関する情報を提供します。グラフにカーソルを合わせると、各脅威レベルで検出された不正 AP の数が表示されます。

- **[時間の経過に伴う高レベルの脅威 (High Threats Over Time)]** には、ドロップダウンリストから選択した時間間隔に基づいて、時間の経過に伴う高レベルの脅威に関する情報が示されます。グラフの上にカーソルを合わせると、特定の時点で発生した高レベルの脅威の数が表示されます。

**ステップ 3** ダッシュボードの下部には、ネットワーク上に存在する不正 AP のリストが表示されます。

**ステップ 4** デフォルトの列表示設定では一部の列が非表示になっています。これは、列の見出しの右端にある 3 つの点  をクリックするとカスタマイズできます。

 をクリックしてレイアウトプリセット (**[基本 (Basic)]** または **[すべて (All)]**) を選択します。

**ステップ 5** テーブルの左端にある **[フィルタ (Filter)]** アイコン () をクリックして、次の条件に基づいて不正 AP リストを絞り込みます。**脅威レベル、不正 AP MAC アドレス、タイプ、検出 AP、検出 AP サイト、RSSI、および SSID。**

**ステップ 6** ネットワーク上の各不正 AP について、次の情報が表示されます。

- **ID** : 不正 AP の ID。
- **Threat Level** : 色別に分類された脅威レベル。Cisco DNA Center は脅威を、**高レベルの脅威、潜在的な脅威、情報**というカテゴリに分類します。
- **Rogue AP Mac Address** : 不正 AP の MAC アドレス。
- **タイプ (Type)** : 不正 AP のカテゴリタイプ。分類タイプは、**有線ネットワーク上の不正、ハニーポット、干渉源、およびネイバー**です。
- **状態 (State)** : 不正 AP の状態。
- **接続 (Connection)** : 不正 AP が有線ネットワークまたはワイヤレスネットワーク上にあるかどうかを示します。
- **検出 AP (Detecting AP)** : 不正 AP を現在検出している AP の名前。複数の AP が不正を検出すると、信号強度が最高の AP の検出が表示されます。
- **AP サイトの検出 (Detecting AP Site)** : 検出する AP のサイトロケーション。
- **RSSI** : 検出中の AP によって報告された RSSI 値。
- **SSID** : 不正 AP をブロードキャストするサービスセット ID。
- **最後のレポート** : 不正 AP が最後に報告された日付、月、年、および時刻。

## 脅威 360° ビューから不正 AP の詳細を取得する

脅威 360° ビュー内で、フロアマップ上の特定の不正 AP のロケーションの詳細をすばやく表示できます。

X座標とY座標が使用可能な場合は、APの最も強力な信号強度、またはCisco Connected Mobile Experience (CMX) からのXおよびY座標情報の検出に応じて、フロアマップ上の特定の不正APの正確なロケーションの詳細を取得できます。

**ステップ 1** Cisco DNA Center ホームページから [アシュアランス (Assurance)] > [ダッシュボード (Dashboard)] > [不正アクセスポイントの管理 (Rogue Management)] を選択します。

**ステップ 2** 特定の AP に対して脅威 360° ビューを起動するには、[脅威 (Threat)] テーブルで対象の不正 AP の行をクリックします。

[脅威 360° (Threat 360°)] スライドインペインが表示されます。

**ステップ 3** 上部ペインには、次の情報が表示されます。

- 不正 AP の MAC アドレス
- 脅威レベル
- 脅威のタイプ
- ステータス
- 不正なベンダー
- 最後のレポート

**ステップ 4** 中央のペインには、不正 AP またはフロアマップ上の脅威の推定位置が表示されます。

- サイトの詳細とフロア番号。
- フロアマップには、管理対象 AP の名前が表示されます。
- フロアマップ  の右上隅にあるアイコンをクリックすると、ワイヤレスコントローラ到達可能性ステータスとともに AP を管理するの IP アドレスが表示されます。
- フロアマップの右隅にある  アイコンをクリックして、場所をズームインします。ズームレベルは画像の解像度によって異なります。高解像度の画像の場合、より高倍率のズームレベルを使用できます。各ズームレベルはさまざまなスケールで表示される各種スタイルマップで構成されていて、対応する詳細が表示されます。マップの中にはスケールを小さくしても大きくしても同じ状態のマップもあります。
-  アイコンをクリックすると、広範囲のマップが表示されます。
-  アイコンをクリックすると、マップアイコンの凡例が表示されます。

表 1: マップアイコン

フロアマップアイコン	説明
[ デバイス (Devices) ]	

フロアマップアイコン	説明
	アクセス ポイント (Access Points)
	センサー
	不正 AP (Rogue AP)
	マーカー
正常性スコアの平均	
	正常性スコア : 8 ~ 10
	正常性スコア : 4 ~ 7
	正常性スコア : 1 ~ 3
	正常性スコア : 不明
AP ステータス	
	センサーのカバー内
	センサーのカバー外

ステップ 5 下部の領域には、次の情報が表示されます。

- [スイッチポートの詳細 (Switch Port Detail)] タブをクリックして、有線ネットワーク上の不正に関する詳細を取得します。[スイッチポートの詳細 (Switch Port Detail)] タブには、ホスト Mac、デバイス名、デバイス IP、インターフェイス名、最後の更新などの情報が表示されます。

シスコのスイッチは、有線ネットワーク上の不正の検出に必要です。

- [検出 (Detections)] タブをクリックして、[AP の検出 (Detecting AP)]、[AP ドメイン (AP Domain)]、[不正な SSID (Rogue SSID)]、[RSSI]、[チャネル (Channels)]、[無線タイプ (Radio Type)]、[セキュリティ (Security)]、[SNR] などの情報を表示します。

テーブルの左端にある [フィルタ (Filter)] () アイコンをクリックして、[不正な SSID (Rogue SSID)]、[RSSI]、[無線タイプ (Radio Type)]、[セキュリティ (Security)]、[SNR] に基づいて検索結果を絞り込むことができます。

情報をエクスポートするには、[エクスポート (export)] アイコンをクリックして、システムに保存します。

- [クライアント (clients)] タブをクリックすると、不正 AP に関連付けられているクライアントに関する次の詳細情報が表示されます。MAC アドレス、ゲートウェイ MAC、不正 AP Mac、IP アドレス、および最終検知です。

テーブルの左端にある [フィルタ (Filter)] (  ) アイコンをクリックして、検索条件に基づいて検索結果を絞り込むことができます。

---