不正管理および aWIPS ダッシュボードのモニタリング

不正管理および aWIPS アプリケーションへのアクセス

ステップ 1 不正管理および aWIPS アプリケーションにアクセスするには、Cisco DNA Center にログインします。

ステップ 2 メニューアイコン（☰）をクリックして、**[Assurance]** > **[Rogue and aWIPS]**。

[Rogue and aWIPS] ダッシュボードが表示されます。

Note Cisco DNA アシュアランス アプリケーションを使用する前に、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。

不正管理および aWIPS ダッシュボードのモニタリング

ネットワークで検出されたすべての不正 AP と aWIPS シグニチャの詳細な脅威分析とグローバルビューを表示するには、不正管理および aWIPS ダッシュボードを使用します。また、不正管理および aWIPS 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 AP のデータを取得します。

不正管理および aWIPS ダッシュボードのモニタリング

ステップ 1 メニューアイコン（☰）をクリックして、**[Assurance]** > **[Rogue and aWIPS]**。

[Rogue and aWIPS] ウィンドウが表示されます。デフォルトでは、Cisco DNA Center に [Overview] ダッシュボードが表示されます。

Note Cisco AireOS コントローラが必要な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 [**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。

ステップ 2 [Site] メニューで、[Global] をクリックします。

[Site Selector] スライドインペインが表示されます。

a) [Search Hierarchy] 検索バーにサイト名を入力するか、[Global] を展開してサイトを選択します。

Note
- サイトに 254 を超えるサブサイトがある場合、そのサイトはデフォルトで無効になります。
- 内部にフロアを持たないサイト階層は、サイトセレクタにリストされません。

ステップ 3 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、[Actions] ドロップダウンリストで、**[Rogue]** > **[Enable]** の順に選択します。

不正管理機能は、Cisco DNA Center リリース 1.3.3.x から Cisco DNA Center リリース 2.2.1.0 以降への移行中にすでに有効になっている場合、デフォルトでは有効になっています。

ステップ 4 不正管理のアクションを一時的に無効にするには、**[Rogue]** > **[Disable]** の順に選択します。

ステップ 5 表示される **[Warning]** ダイアログボックスで [Yes] をクリックします。

不正管理機能を無効にすると、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。

ステップ 6 **[Rogue]** > **[Status]** を選択して、不正構成ジョブのステータスを表示します。

ステップ 7 [All]、[Failure]、[Success]、または [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。

ワイヤレスコントローラ で不正管理の検出操作が正常に有効化されると、[Operation] 列に [Enable] と表示されます。

設定の変更が ワイヤレスコントローラ に正常にプッシュされると、[Status] 列に [Success] と表示されます。

ステップ 8 Cisco DNA Center で aWIPS のデータ収集を有効にするには、**[aWIPS]** > **[Enable]** の順に選択します。

Cisco DNA Center リリース 1.3.3.x から Cisco DNA Center リリース 2.2.1.0 以降に移行する場合は、Cisco DNA Center リリース 2.2.1.0 以降で aWIPS 機能を有効にする必要があります。

ステップ 9 aWIPS のアクションを一時的に無効にするには、**[aWIPS]** > **[Disable]** の順に選択します。

表示される **[Warning]** ダイアログボックスで [Yes] をクリックします。

不正管理および aWIPS ダッシュボードのモニタリング

ステップ 10 aWIPS のサブスクリプション ステータスを確認するには、**[aWIPS]** > **[Status]** の順に選択します。

ステップ 11 [All]、[Failure]、[Success]、または [In Progress] の各タブをクリックして、aWIPS の設定ステータスをフィルタ処理します。

ワイヤレスコントローラ で aWIPS の検出操作が正常に有効化されると、[Operation] 列に [Enable] と表示されます。

設定の変更が ワイヤレスコントローラ に正常にプッシュされると、[Status] 列に [Success] と表示されます。

ステップ 12 次の情報については、[Threats] ダッシュレットを使用します。

- TOTAL ROGUE THREATS：不正な脅威の総数を表示します。
- TOTAL AWIPS THREATS：AWIPS 脅威の総数を表示します。
- TOTAL UNIQUE ROGUE CLIENTS： 固有の不正クライアントの総数を表示します。
- ROGUES CONTAINED：封じ込まれている不正の総数を表示します。

タイムラインスライダの下にある [Active High Threats] と [High Threats Over Time] のグラフに、該当する脅威の詳細が表示されます。

ステップ 13 [Active High Threats]、[Top Locations Affected] および [High Threats Over Time] のグラフには、デフォルトでは過去 3 時間に検出された不正 AP に関する情報が表示されます。グラフの情報は、時間を選択するドロップダウンリストで選択した時間間隔に基づきます。

- オプションは、[Last 3 Hours]、[Last 24 Hours]、および [Last 7 Days] です。

Note 特定の時間範囲を選択するには、[Custom] を選択します。

ステップ 14 次の情報については、[High Threats Summary] ダッシュレットを使用します。

[High Threats Summary] ダッシュレット	
アイテム	**説明**
Active High Threats	ドーナツグラフの形式でアクティブな脅威レベルに関する情報を提供します。アクティブな高脅威を脅威の種類、[Top 10] または [All] でフィルタ処理できます。 ドーナツグラフの色付きの各スライスをクリックすると、脅威の表に脅威の詳細情報が表示されます。グラフにカーソルをホバーすると、アクティブで高レベルの脅威の数が表示されます。 [All] をクリックすると、脅威の種類と数が表形式で表示されます。
Top Locations Affected	選択したサイトごとに、高レベルの脅威の影響を受ける上位 5 つの場所を表示します。

ステップ 15 次の情報については、[High Threats Over Time] ダッシュレットを使用します。

不正管理および aWIPS ダッシュボードのモニタリング

[High Threats Over Time] ダッシュレット	
アイテム	説明
Threats Over Time	選択した期間に基づいて、経時的に高レベルの脅威に関する詳細情報を表示します。 [Total Active High Threat] の下にある使用可能な各脅威の種類をクリックすると、脅威情報がグラフビューに表示されます。 高い脅威偏差は、値から値の段階で測定されます。 • 緑色は脅威偏差が 0 未満であることを示します。 • オレンジ色は脅威偏差が 0 ～ 9 であることを示します。 • 赤色は脅威偏差が 10 以上であることを示します。 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。
View Threats	[View Threats] をクリックして脅威テーブルを表示すると、高レベルの脅威のリストが表示されます。

ステップ 16 [Threats By Location] ダッシュレットを使用して、脅威に関する情報をマップビューで表示します。

ロケーションオプション	
アイテム	説明
 [Map View]	このトグルボタンをクリックすると、脅威の影響を受ける場所がマップビューに表示されます。 マップ内の目的の場所にカーソルをホバーすると、すべての脅威のレベルと数が表示されます。
 [List View]	このトグルボタンをクリックすると、脅威の影響を受ける場所に関する情報がリストビューに表示されます。

ステップ 17 [Threat Setting Summary] ダッシュレットを使用して、次の情報を確認できます。

[Threat Setting Summary] ダッシュレット	
アイテム	説明
Allowed AP List	許可された AP の数と設定されている脅威レベルに関する情報を表示します。 [Allowed Access Point List] の詳細については、[View Details] をクリックして [Allowed List] ウィンドウを表示します。.

[Threat Setting Summary] ダッシュレット	
アイテム	説明
Allowed Vendor List	許可されたベンダーの総数と設定されている脅威レベルに関する情報を表示します。 [Allowed Vendor List] の詳細については、[View Details] をクリックして [Allowed List] ウィンドウを表示します。
Rogue Rule	ルール、その条件タイプ、それに関連付けられたルールプロファイル、および脅威レベルに関する情報を表示します。 [Rogue Rules] の詳細については、[View Details] をクリックして [Rules] ウィンドウを表示します。

ステップ 18 （オプション）許可された AP リストの作成、許可されたベンダーリストの作成、不正ルールの作成などのワークフローを使用するには、直接リンクを提供する [Tips] ダッシュレットを使用します。

[View All] をクリックして、使用可能なすべてのワークフローを表示します。

ネットワークの不正な脅威のモニタリング

ステップ 1 [Site] メニューで、[Global] をクリックします。

[Site Selector] スライドインペインが表示されます。

a) [Search Hierarchy] 検索バーにサイト名を入力するか、[Global] を展開してサイトを選択します。

Note
- サイトに 254 を超えるサブサイトがある場合、そのサイトはデフォルトで無効になります。
- 内部にフロアを持たないサイト階層は、サイトセレクタにリストされません。

ウィンドウ：

ステップ 2 左上隅にある時間範囲設定（ ）をクリックして、脅威テーブルに表示するデータの時間範囲を指定します。

a) ドロップダウンメニューから、時間範囲として [3 hours]、[24 hours]、[7 days]、または [Custom] を選択します。
b) [Custom] 時間範囲では、[Start Date] と時間、および [End Date] と時間を指定します。
c) [Apply] をクリックします。

ステップ 3 [Threat] テーブルを使用して、ネットワーク内の脅威に関する詳細情報を表示します。

[Threats] テーブル	
アイテム	説明
▽ **[Filter]** アイコン	[Threats] テーブルの右上隅にあるこのアイコンをクリックすると、次の基準に基づいてテーブルに表示されるデータをフィルタ処理できます：ID、Threat Level、Threat MAC Address、Type、State、Connection、Detecting AP、Detecting AP Site、RSSI (dBm)、SSID、Clients、Containment Status、Last Reported、および Vendor。 **RSSI**、**SSID**、および [Clients] は、aWIPS の場合は表示されません。

[Threats] テーブル	
アイテム	説明
[Threats] テーブル	

[Threats] テーブル	
アイテム	説明
	次の情報をテーブルフォーマットで表示します。[Threats] テーブルには次の情報が表示されます。 • Threat Level：色別に分類された脅威レベルを表示します。Cisco DNA Center では脅威を次のカテゴリに分類します。 • **高レベルの脅威** • **潜在的な脅威** • **情報** • Mac Address：不正 AP の MAC アドレスを表示します。 • Type：脅威の種類を表示します。 • State：不正 AP または aWIPS 攻撃の状態を表示します。 • [Source/Target]：表示されている MAC アドレスが aWIPS 攻撃の送信元であるか、または aWIPS 攻撃のターゲットであるかを表示します。この列は不正データには適用されません。 • 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表示します。この列には、ワイヤレスネットワークに対する aWIPS 攻撃が示されます。 • Detecting AP：不正 AP を現在検出している AP の名前を表示します。複数の AP で不正が検出された場合は、信号強度が最も高い検出 AP が表示されます。この列は、不正 AP および aWIPS 攻撃に適用されます。 • Detecting AP Site：検出 AP のサイトの場所を表示します。この列は、不正 AP および aWIPS 攻撃に適用されます。 • RSSI (dBm)：検出 AP から報告された RSSI の値を表示します。RSSI（dBm）は不正 AP にのみ適用されます。 • SSID：不正 AP がブロードキャストするサービスセット ID を表示します。SSID は、不正 AP にのみ適用されます。 • Clients：この AP に関連付けられている不正クライアントの数を表示します。この列は、不正 AP にのみ適用されます。 **Note** [Threats] テーブルに表示されるクライアント数は、[Threats 360 degrees] ウィンドウに表示されるクライアント数とは異なります。これは、リリース 2.3.2 以前の Cisco DNA Center のリリースで処理されたデータが Cisco DNA Center 2.3.2 以降に移行された場合に発生します。Cisco DNA Center 2.3.2 以降では、選択した時間範囲に新しいデータがある場合、新しく処理されたデータの正しいクライアント数が表示されます。

[Threats] テーブル	
アイテム	説明
	• Containment Status：不正 AP の有効な値（[Contained]、[Pending]、[Open]、[Partial]）を表示します。自動封じ込められた不正 AP の場合、ステータスは [Contained (Auto)]、[Pending (Auto)]、[Open (Auto)]、[Partial (Auto)] として表示されます。ワイヤレス封じ込めステータスは、不正 AP にのみ適用されます。 • Last Reported：不正 AP および aWIPS 攻撃が最後に報告された日付、月、年、および時刻を表示します。 • Vendor：不正 AP のベンダーの情報を表示します。この列は、aWIPS 攻撃には適用されません。
⚙	テーブルに表示するデータをカスタマイズします。 **a.** [Table Appearance] タブで、テーブルの密度とストライピングを設定します。 **b.** [Edit Table Columns] タブで、テーブルに表示するデータのチェックボックスをオンにします **c.** [Apply] をクリックします。

脅威 360° ビューから不正 AP および不正クライアントの詳細を取得

[Threat 360°] ビュー内で、フロアマップ上の特定の不正 AP または不正クライアントの場所の詳細をすばやく表示できます。

検出 AP の最も強力な信号強度に応じて、フロアマップ上の特定の不正 AP または不正クライアントの正確な場所の詳細を取得できます。Cisco Connected Mobile Experiences（CMX） または Cisco Spaces の統合により、不正 AP または不正クライアントの正確な場所を取得できます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Assurance]** > **[Rogue and aWIPS]** > **[Threats]**。

ステップ 2 特定の不正 AP または不正クライアントに対して [Threat 360°] ビューを起動するには、[Threat] テーブルで対象の行をクリックします。

[Threat 360°] ペインが表示されます。

ペイン上部には、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
- ベンダー
- 封じ込め
- カウント
- 最後のレポート

ペインの中央部分には、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。

ステップ 3 必要に応じて、次のタスクを実行します。

- 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、到達可能性ステータスとともに AP を管理する ワイヤレスコントローラ 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、場所を拡大します。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。

次の表に、フロアマップアイコンの説明を示します。

Table 1: マップアイコンと説明

フロアマップアイコン	説明
デバイス	
	アクセスポイント
	センサー
	不正 AP
	マーカー

フロアマップアイコン	説明
	計画済み AP
	スイッチ
	干渉源
	クライアント
	不正なクライアント
	AP の報告
	検出 AP
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 4 ペインの下部領域では、次のタスクを実行できます。

- [Switch Port Detail] タブをクリックすると、**ホスト Mac**、**デバイス名**、**デバイス IP**、**インターフェイス名**、**最終更新日**、**ポートモード**、**管理ステータス**などの情報を含む不正なワイヤに関する詳細を取得できます。

Note
- [Admin Status] 列には、インターフェイスのステータスが [UP] または [DOWN] として表示されます。
- [Port Mode] 列には、インターフェイスモードが [ACCESS] または [TRUNK] として表示されます。

Note 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。

- [Detections] タブをクリックすると、[Detecting AP]、[Detecting AP Site]、[Adhoc]、[Rogue SSID]、[RSSI (dBM)]、[Channels]、[Radio Type]、[SNR]、[State]、[Last Updated] などの情報が表示されます。
- テーブルの左端にある **[Filter]**（ ） アイコンをクリックして、**[Rogue SSID]** 、 **[RSSI]**、**[Radio Type]**、**[Security]**、**[SNR]** に基づいて検索結果を絞り込むことができます。
- [Export] アイコンをクリックして、システムに保存します。
- [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、[MAC Address]、[Gateway Mac]、[Rogue AP Mac]、[IP Address]、および [Last Heard] などの詳細情報が表示されます。
- テーブルの左端にある **[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。

脅威 360° ビューから aWIPS プロファイルのフォレンジックキャプチャをダウンロード

この手順では、脅威 360 ビューからさまざまな DoS 攻撃のフォレンジックキャプチャをダウンロードする方法について説明します。

Note Cisco DNA Center では、デフォルトの AP プロファイルでのみフォレンジックキャプチャが有効または無効になります。カスタム AP 参加プロファイルを作成した既存の展開の場合は、フォレンジックキャプチャを有効または無効にする必要があります。

Before you begin

アクセスポイントと Cisco DNA Center の間のネットワーク接続を確認する必要があります。

ステップ 1 メニューアイコン（≡）をクリックして、**[Workflows]** > **[Rogue and aWIPS]** > **[Threats]**。

ステップ 2 [Threat MAC address] 列で、aWIPS 攻撃リンクをクリックします。

[Threat 360] ウィンドウが表示されます。

ステップ 3 [Forensic Capture] タブをクリックして、[Detecting AP]、[Alarm ID]、 [Capture Filename]、[Last Updated] などの情報を表示します。

ステップ 4 [Capture Filename] 列で、**pcap** ファイルをクリックして aWIPS プロファイルのフォレンジックキャプチャをダウンロードします。

ステップ 5 [Download All] をクリックして、すべての **pcap** ファイルをダウンロードします。

ステップ 6 [Filter] アイコンをクリックして、[Detecting AP] に基づいて検索結果を絞り込みます。

ステップ 7 [Export] アイコンをクリックして、**CSV** ファイルをワークスペースに保存します。

Note Cisco DNA Center では、一度に最大 50 のフォレンジックキャプチャが表示されます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。