不正 AP のカスタム分類

許可リストワークフローについて

Cisco DNA Center 不正管理および aWIPS ワークフローを使用すると、許可リストに一括で移動する不正アクセスポイントの MAC アドレスを確認してマークを付け、選択した AP の MAC アドレスの一括許可リストを処理できます。

不正管理および aWIPS ワークフローは、Cisco AireOS 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に関連付けられている AP をサポートします。

許可リストワークフローの設定 （2 ページ） を使用して、次の不正 AP タイプを許可リストに移動できます。

- 有線ネットワーク上の不正
- ハニーポット

- 干渉源
- ネイバー

許可リストワークフローの設定 （2 ページ） を使用して、次の不正 AP タイプを許可リストに移動できます。

- ビーコン不正チャネル
- ビーコン DS 攻撃
- AP 偽装
- 危険性のない

許可リストワークフローの設定

この手順では、不正 AP の MAC アドレスを許可リストに一括で移動する方法を示します。これらのアドレスは、Cisco DNA Center で高脅威として報告しないアドレスです。

Before you begin

次のタスクを実行するには、SUPER-ADMIN-ROLE または NETWORK-ADMIN-ROLE 権限が必要です。

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

[Set up Rogue Management and aWIPS] ウィンドウが表示されます。

ステップ 2 [Let's Do it] をクリックします。

今後このウィンドウをスキップするには、[Don't show this to me again] チェックボックスをオンにします。

[Bulk upload allowed access Points] ウィンドウが表示されます。

ステップ 3 [Search] フィールドでは、すでに 許可リストワークフローについて, on page 1 に追加された MAC アドレスを検索します。

ステップ 4 [Export] をクリックし、許可リストをエクスポートします。

ステップ 5 サンプル CSV テンプレートファイルをダウンロードし、MAC アドレス、操作、およびカテゴリを手動で追加して、一括許可リストテンプレートを作成できます。[Download the sample CSV template from here] リンクをクリックします。

通知記号にカーソルをホバーすると、許可されている MAC アドレス、操作、およびカテゴリのフォーマットを表示できます。

ステップ 6 CSV ファイルをボックス領域にドラッグアンドドロップするか、[Choose a file] をクリックしてシステム上の CSV ファイルを参照します。CSV ファイルの最大サイズは 1.2 MB です。

Note Cisco DNA Center で検証チェックが実行されます。アップロードされた CSV ファイルが次の要件を満たしていない場合、エラーメッセージが表示されます。

- MAC アドレスが有効な不正ポイント MAC アドレスではありません。
- すべての不正アクセスポイントの MAC アドレスがシステムにすでに存在しているか、または削除操作の対象となる不正アクセスポイントの MAC アドレスがありません。
- 緑色のチェックマークは、アップロードされた CSV ファイルの内容が有効であることを示します。

ステップ 7 [Next] をクリックします。

ステップ 8 [Summary] ウィンドウの [Uploaded bulk allowed list MAC addresses] テーブルに、許可された MAC アドレスのリスト、およびそれぞれの動作とアクションが表示されます。

- [All]：すべての MAC アドレスのリスト、およびそれぞれの動作とアクションを一括して表示します。
- [Create]：作成された MAC アドレスのリスト、およびそれぞれの操作とアクションをまとめて表示します。
- [Delete]：削除された MAC アドレスのリスト、およびそれぞれの動作とアクションが一括して表示されます。
- [No Action]：すでに削除されている MAC アドレスのリスト、およびそれぞれの操作とアクションが表示されます。

ステップ 9 [Continue to allowed list] をクリックし、表示されるダイアログ ボックスで [Yes] をクリックします。

タスク完了**[Allowed List Updated]** ウィンドウが表示されます。

ステップ 10 [Go to Rogue and aWIPS Home Page] をクリックします。

[Rogue and aWIPS] ダッシュボードが表示されます。

[Threats] テーブルを表示している [Threat] タブをクリックすると、Cisco DNA Center により、指定した不正 AP MAC アドレスが [Type] 列の下の [Allowed List] に分類されます。

ステップ 11 不正 AP MAC アドレスを個別に追加または削除するには、[Threat MAC address] 列の下にリストされている不正 MAC アドレスをクリックします。

[Threat 360] ウィンドウが表示されます。

ステップ 12 [Action] ドロップダウンリストから、[Add to Allowed list] を選択します。

許可リストから不正 AP MAC アドレスを個別に削除するには、[Action] ドロップダウンリストで [Remove from Allowed list] を選択します。

カスタム不正ルールの作成について

不正ルールは、異なるリスクプロファイルを持つ不正を簡単に分別して管理する方法です。不正ルールは設定が容易で、優先順位に従って適用されます。これにより、誤検出、干渉源のあるサイトのノイズ、アラートの数が減り、グローバルおよびサイトベースで組織のリスクプロファイルを調整できるようになります。

次の不正 AP タイプをカスタム分類タイプに移動できます。

- 干渉源
- ネイバー

不正ルールの編集

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

ステップ 2 [Rogue Rules] テーブルで、編集するルール名をクリックします。

ステップ 3 [Edit Rogue Rule] ウィンドウが表示されたら、必要な変更を行います。

Note 古いルールに基づく以前の分類は、ルール条件が変更されても変更されません。変更は、新しいデータ分類にのみ影響します。

ステップ 4 （オプション）不正なルールを自動封じ込めるには、[Enable Auto-Containment] チェックボックスをオンにします。

Note
- **Cisco Catalyst 9800 シリーズ ワイヤレス コントローラには、一度に 625 の不正な封じ込め設定の制限があります。制限に達すると、封じ込めはそれらのデバイスで検出された新しい不正に対して機能しなくなります。**
- [Honeypot] と脅威レベルが [High] であるカスタムルールのみの自動封じ込めを有効にすることができます。

ステップ 5 [Save] をクリックします。

[Auto-containment] 列から封じ込めが有効になっているかどうかを確認します。

不正ルールの削除

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

ステップ 2 [Rogue Rules] テーブルで、削除する [Rule Name] をクリックし、[Delete] をクリックします。

Note 削除する不正ルールがルールプロファイルで使用可能な唯一のルールである場合は、そのルールプロファイルも削除されます。

ステップ 3 確認のダイアログボックスで [Delete] をクリックします。

Note [Honeypot] は事前定義されたルールです。削除することはできません。

ステップ 4 削除されたルールを表示するには、[Rogue Rules] テーブルの [Inactive] タブをクリックします。

カスタム不正ルールの作成

特定の条件を持つルールを作成し、そのルールをルールプロファイルに関連付けることができます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Workflows]** > **[Create a Rogue Rule]**。

ステップ 2 [Create a Rogue Rule] ウィンドウで、[Get Started] をクリックします。

ステップ 3 [Rule Name] フィールドに、ルールの一意の名前を入力します。

新しい不正ルールの作成時、以前に削除された不正ルール名を入力することはできません。

ステップ 4 [Description] フィールドに、ルールの説明を入力します。

ステップ 5 [Next] をクリックします。

ステップ 6 [Create Rogue Rule] ウィンドウで、脅威レベルを選択し、ルールの条件を追加します。

ステップ 7 [Threat Level] オプションボタンのいずれかをクリックして、脅威レベルをルールに追加します。使用可能なオプションは、[High]、[Potential]、または [Informational] です。

ステップ 8 （オプション）不正なルールを自動封じ込めるには、[Enable Auto-Containment] チェックボックスをオンにします。

Note
- **Cisco Catalyst 9800 シリーズ ワイヤレス コントローラには、一度に 625 の不正な封じ込め設定の制限があります。制限に達すると、封じ込めはそれらのデバイスで検出された新しい不正に対して機能しなくなります。**
- 自動封じ込めは、[High] レベルの脅威にのみ適用されます。デフォルトでは、[Potential] および [Informational] レベルの脅威に対して [Enable Auto-containment] は無効になっています。

ステップ 9 [Match] ドロップダウンリストから、すべての条件に一致させるための [All]、またはいずれかの条件に一致させるための [Any] を選択します。

ステップ 10 [Add Condition] ドロップダウンリストから、ルール条件を選択します。

1 つのルールに複数の条件を追加できます。使用可能なルール条件は、[SSID]、[RSSI]、[Encryption Condition]、[Minimum Rogue Client Count] です。

ステップ 11 [Next] をクリックします。

ステップ 12 このルールを既存のルールプロファイルに割り当てるには、[Do you want to assign this rule to a rule profile?] ダイアログボックスで [Yes] をクリックします。

不正ルールを作成しただけではエンティティとして機能しません。不正ルールは常にルールプロファイルに割り当てる必要があります。

ステップ 13 [Available rule profiles] テーブルで、プロファイル名の横にあるチェックボックスをオンにし、[Next] をクリックします。

1 つ以上のルールプロファイルを選択できます。1 つのルールプロファイルに割り当てることができるルールは 5 つまでです。

ステップ 14 表示される確認ダイアログボックスで [Proceed] をクリックします。

新しいルールは、最も低い優先順位に設定されます。ルールプロファイルを編集して優先順位を変更できます。

Note 不正ルールの作成後、同じ不正ルール名を使用して別の不正ルールを作成することはできません。

ステップ 15 [Summary] ウィンドウで不正ルールの構成を確認します。

Note 古いルールに基づく以前の分類は、新しいルール条件と一致しても変更されません。変更は、新しいデータ分類にのみ影響します。

ステップ 16 別の不正ルールを作成するには、[Create Another Rogue Rule] ボタンをクリックし、この手順のステップ 3 ー 13 を実行します。

ステップ 17 作成した不正ルールを表示するには、[View all Rogue Rules and Profiles] ボタンをクリックします。

[Rogue Rules] タブに、作成したすべての不正ルールが表示されます。

作成された不正ルールは、メニューアイコン（☰）をクリックし、**[Assurance]** > **[Rogue and aWIPS]** > **[Rules]** > **[Rogue Rule]** を選択して表示することもできます。

不正ルールプロファイルについて

特定の条件を持つ不正ルールを作成し、ルールプロファイルに関連付けることができます。不正ルールを不正ルールプロファイルに関連付けた後、優先順位を付けることができます。

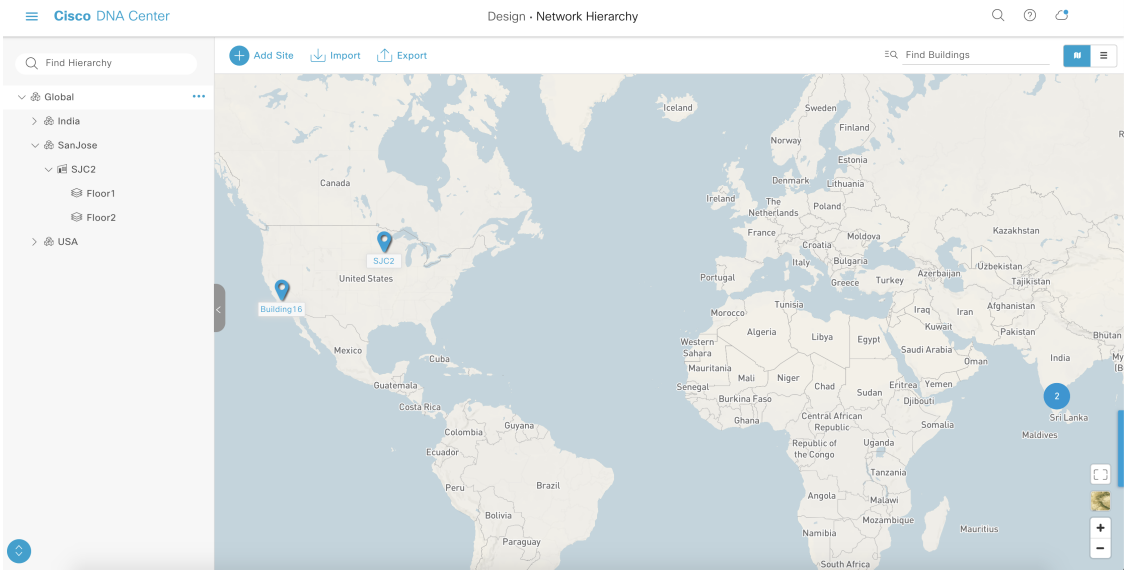
不正ルールプロファイルをサイトに割り当てると、そのサイトから報告される不正は、ルールプロファイルで定義されているルールに対して検証されます。

1 つのサイトに割り当てることができる不正ルールプロファイルは 1 つだけです。

サイトの継承により、特定のサイトのすべてのフロアは、エリア、サイト、またはビルディングレベルでマッピングされている不正ルールプロファイルを継承します。たとえば、次の図に示すように、Floor1 と Floor2 は、SanJose レベルでマッピングされている不正ルールプロファイルを継承します。

フロアにマッピングされた不正ルールプロファイルは、親サイトから継承された不正ルールよりも優先されます。たとえば、次の図に示すように、不正ルールプロファイル A が Floor1 に直接マッピングされている場合、不正ルールプロファイル A は親サイトの SJC2 に割り当てられているルールプロファイル B よりも優先されます。

図 *1* : ネットワーク階層



不正ルールプロファイルの編集

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

ステップ 2 [Profile Rule] タブをクリックします。

ステップ 3 [Rogue Rule Profiles] テーブルで、編集するプロファイル名をクリックします。

ステップ 4 表示される [Edit Rule Profile] ウィンドウで、必要な変更を行います。。

Note ルールプロファイルを編集しても、以前に分類されたデータは変更されません。編集した内容は、変更後に処理される新しいデータにのみ適用されます。

ステップ 5 （オプション）不正なルールを自動封じ込めるには、[Enable Auto-Containment] チェックボックスをオンにします。

Note
- **Cisco Catalyst 9800 シリーズ ワイヤレス コントローラには、一度に 625 の不正な封じ込め設定の制限があります。制限に達すると、封じ込めはそれらのデバイスで検出された新しい不正に対して機能しなくなります。**
- [Honeypot] は定義済みのルールであり、新しく作成されたすべての不正ルールプロファイルにデフォルトで追加されます。

ステップ 6 表示される確認ウィンドウで [Yes] をクリックします。

ステップ 7 [User Defined] と [Predefined] を切り替えて、対応するルールを表示できます。

[Auto-containment] 列から封じ込めが有効になっているかどうかを確認します。

ステップ 8 [Save] をクリックします。

不正ルールプロファイルの削除

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

ステップ 2 [Profile Rule] タブをクリックします。

ステップ 3 [Rogue Rules] テーブルで、削除するプロファイル名をクリックし、[Delete] をクリックします。

ステップ 4 確認のダイアログボックスで [Delete] をクリックします。

不正ルールプロファイルの作成

特定の条件を持つルールを作成し、ルールプロファイルに関連付けることができます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Workflows]** > **[Create a Rogue Rule Profile]**。

ステップ 2 [Create Rogue Rule Profile] ウィンドウで、[Get Started] をクリックします。

ステップ 3 [Profile Name] フィールドに、ルールプロファイルの一意の名前を入力します。

ステップ 4 （オプション）不正なルールを自動封じ込めるには、[Enable Auto-Containment] チェックボックスをオンにします。

Note
- **Cisco Catalyst 9800 シリーズ ワイヤレス コントローラには、一度に 625 の不正な封じ込め設定の制限があります。制限に達すると、封じ込めはそれらのデバイスで検出された新しい不正に対して機能しなくなります。**
- [Honeypot] と脅威レベルが [High] であるカスタムルールのみの自動封じ込めを有効にすることができます。

ステップ 5 表示される確認ウィンドウで [Yes] をクリックします。

ステップ 6 [Next] をクリックします。

ステップ 7 [Rule List] テーブルで、ルール名の横にあるチェックボックスをオンにし、[Next] をクリックします。

1 つのプロファイルに最大 5 つの不正ルールを追加できます。

ステップ 8 [Sort rules in order of priority] ウィンドウで、ルールを目的の優先順位（最も高い優先順位が一番上）にドラッグアンドドロップして、優先順位に基づいてルールを並べ替えます。

ステップ 9 [Next] をクリックして、不正ルールプロファイルを場所に関連付けます。

ステップ 10 このルールプロファイルを関連付けるサイトの横にあるチェックボックスをオンにし、[Next] をクリックします。

ルールプロファイルは、どのサイトに割り当てられていなくても存在できます。ルールプロファイルがサイトに割り当てられていない限り、ルールはチェックされません。

Note ベンダールールとルールプロファイルが同じサイトにマッピングされている場合は、ベンダールールが優先されます。

ステップ 11 [Summary] ウィンドウで不正ルールプロファイルの構成を確認します。

ステップ 12 [Summary] ウィンドウで、[Back] ボタンをクリックすると、前のウィンドウで入力した値を変更できます。

ステップ 13 [Create Rule Profile] をクリックします。

ルールプロファイルが正常に作成されたことを示すメッセージが表示されます。

ステップ 14 すべての不正ルールおよびプロファイルを表示するには、[View all Rogue Rules and Profiles] をクリックします。

[Rogue Rule Profiles] タブに、作成されたすべての不正ルールとルールプロファイルが表示されます。

作成されたルールプロファイルは、メニューアイコン（☰）をクリックし、**[Assurance]** > **[Rogue and aWIPS]** > **[Rules]** > **[Rogue Rule Profiles]**を選択して表示することもできます。

許可されたアクセスポイントリストの表示

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] ダッシュボードが表示されます。

ステップ 2 [Allowed List] タブで、[Allowed Access Points List] をクリックします。

[Allowed Access Points List] テーブルには、許可されたすべてのアクセスポイントの [MAC Address] と [Last Changed] の詳細が表示されます。

ステップ 3 検索アイコンまたはフィルタ処理アイコンをクリックして、許可リストで特定のアクセス ポイントを見つけます。

ステップ 4 [Add Access Point List] をクリックして、不正 AP MAC アドレスを許可リストに追加します。詳細については、許可リストワークフローの設定, on page 2を参照してください。

ステップ 5 CSV ファイルに許可されたアクセスポイントをエクスポートするには、[Export] をクリックします。

ステップ 6 アクセスポイントを選択し、[Delete] をクリックして、アクセスポイントを許可リストから削除します。

許可されたベンダーリストについて

許可されたベンダーリスト機能では、特定のベンダーの AP が特定の脅威レベルをトリガーするかどうかを定義できます。許可されたベンダーのリストを作成し、これらのベンダーからの脅威が高脅威としてマークされないようにすることができます。潜在的な脅威または情報における脅威としてマークする必要があるかどうかを指定できます。1 つのワークフローで、最大 5 つのベンダーを許可リストに追加できます。

いずれかのレベルでマッピングされている許可されたベンダールールは、継承されたルールよりも優先されます。たとえば、許可されたベンダールール A がフロア レベルにマッピングされている場合、ベンダールール A は、サイト、エリア、またはビルディング レベルに存在する許可されたベンダールール B よりも優先されます。

ベンダールールリスト情報の表示

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

ステップ 2 [Allowed List] タブをクリックします。
[Allowed Vendor List] テーブルに、許可されたベンダーのリストと次の詳細が表示されます。各ベンダールールはエンティティとして表示されます。

- **ベンダー名**
- **一致基準**
- **脅威レベル**
- **関連付けられたサイト**
- **前回の変更**

ベンダールールの編集

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

ステップ 2 [Allowed List] タブをクリックします。

ステップ 3 [Allowed Vendor List] テーブルで、編集するベンダー名をクリックします。

ステップ 4 [Edit Allowed Vendor List] ウィンドウで、必要に応じて次のパラメータを編集します。

- **脅威レベル**
- **一致基準**
- **ベンダー名**
- **関連付けられたサイト**

ステップ 5 [Save] をクリックします。

ベンダールールの削除

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

ステップ 2 [Allowed List] タブをクリックします。

ステップ 3 [Allowed Vendor List] テーブルで、削除するベンダー名ののチェックボックスをオンにし、[Delete] をクリックします。

次のメッセージが表示されます：`Deleting the selected allowed vendor(s) will impact all sites associated with it. There is 1 site associated with this allowed vendor(s).`

ステップ 4 [Delete] をクリックします。

許可されたベンダーのリストの作成

許可リストに登録するベンダーのリストを作成し、これらのベンダーからの脅威が高脅威としてマークされないようにすることができます。

一連のサイトに対する 1 つのワークフローに 5 つのベンダーを追加できます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Workflows]** > **[Create Allowed Vendor List]**。

許可されたベンダーのリストは、メニューアイコンをクリックし、**[Assurance]** > **[Rogue and aWIPS]** > **[Allowed List]**を選択して作成することもできます。

ステップ 2 [Create Allowed Vendor List] ウィンドウで、[Let's Do it] をクリックします。

今後このウィンドウをスキップするには、[Don't show this to me again] チェックボックスをオンにします。

[Create Allowed Vendor List] ウィンドウが表示されます。

ステップ 3 [Selection Criteria] ドロップダウンリストから、ベンダー名の選択基準（[Exactly Matches] または [Contains]）を選択します。

ステップ 4 [Vendor Name] フィールドに、ベンダー名を入力します。

ベンダー名の照合では、大文字と小文字が区別されます。

ステップ 5 さらにベンダーを許可リストに追加するには、⊕をクリックします。

1 つのワークフローで、最大 5 つのベンダーを許可リストに追加できます。

ステップ 6 [Site Selection] 画面で、許可されたベンダーリストを適用するサイトの横にあるチェックボックスをオンにします。

サイトの継承により、特定のサイトのすべてのフロアは、エリア、サイト、またはビルディングレベルでマッピングされているベンダールールを継承します。

ステップ 7 [Next] をクリックします。

ステップ 8 [Summary] ウィンドウ、許可されたベンダーとサイト選択の詳細を確認できます。

ステップ 9 [Done] をクリックします。

[Allowed Vendor List Created] ウィンドウが表示されます。

ステップ 10 別の許可されたベンダーリストを作成するには、[Create New Allowed Vendor List] をクリックし、手順 3 ～ 8 を繰り返し。

ステップ 11 作成したベンダーリストを表示するには、[View all allowed Lists] をクリックします。

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。