有線およびワイヤレスネットワークでの不正 AP の封じ込め

不正 AP の封じ込めの概要

Cisco DNA Center 不正 AP 封じ込め機能には、有線および無線ネットワーク上の不正APが含まれます。有線ネットワーク上の不正 AP 封じ込めの場合、Cisco DNA Center により、不正 AP が接続されている **ACCESS** モードのスイッチポート インターフェイスを **DOWN** 状態にします。**ワイヤレスネットワーク上の不正 AP 封じ込め**の場合、Cisco DNA Center は最も強力な検出ワイヤレスコントローラにワイヤレスネットワーク上の不正 BSSID の封じ込めを開始するように指示します。次に、ワイヤレスコントローラは、これらの BSSID の最強の検出 AP に、認証解除パケットをストリーミングして、不正 AP とその不正 AP のワイヤレスクライアント間の通信を中断するように指示します。

不正 AP 封じ込めは次のように分類されます。

- [Wired Rogue AP Containment]：Cisco DNA Center 不正な脅威のダッシュボードで [Rogue on Wire] として分類された不正 AP の MAC アドレス。
- [Wireless Rogue AP Containment]：Cisco DNA Center 不正な脅威のダッシュボードで [Honeypot]、[Interferer]、または[Neighbor] として分類された不正 AP MAC アドレス。

不正 AP の封じ込めは、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 でサポートされています。

（注） 封じ込めは、aWIPS 脅威ではサポートされていません。

有線ネットワーク上の不正 AP の封じ込め

有線ネットワーク上の不正 AP 封じ込め機能を使用すると、Cisco DNA Center では不正 AP が物理的に接続されているスイッチの ACCESS モードインターフェイスをシャットダウンできます。 Cisco DNA Center では他のモードをシャットダウンするとネットワークがダウンする可能性があるため、ACCESS モードインターフェイスでのみ有線ネットワーク上の不正 AP 封じ込めを実行します。

不正 AP が非 ACCESS モードのインターフェイスに接続されている場合、ネットワーク管理者は手動で、または CLI コマンドを使用してインターフェイスを含める必要があります。

この手順では、Cisco DNA Center の [Rogue on Wire] に分類された ACCESS モードインターフェイスで有線ネットワーク上の不正 AP の封じ込めを実行する方法について説明します。

始める前に

[Rogue and aWIPS] アプリケーションパッケージをダウンロードしてインストールします。詳細については、「Cisco DNA Center での不正および aWIPS アプリケーションパッケージのダウンロードとインストール」を参照します。

この手順を実行するには、プロビジョニング API、スケジューラ API、および不正側から G 書き込み権限があることを確認してください。

ステップ 1 メニューアイコン（≡）をクリックして選択します**[Assurance]** > **[Rogue and aWIPS]** > **[Threats]**。

ステップ 2 [Threat MAC address] 列の [Rogue on Wire] に分類された不正 AP 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 3 [Action] ドロップダウンリストから、[Shutdown Switchport] を選択します。

警告ポップアップウィンドウに、対応するデバイスでシャットダウンする ACCESS モードインターフェイスのリストが表示されます。

（注） [Shutdown Switchport] オプションは、不正 AP MAC アドレスが [Rogue on Wire] としてマークされている場合にのみ、[Action] ドロップダウンリストに表示されます。詳細については、Cisco 不正 AP 封じ込めアクションの互換性マトリックス （6 ページ）を参照してください。

[Shutdown Switchport] アクションは元に戻せません。スイッチポートを手動で再起動する必要があります。

ステップ 4 警告ダイアログボックスで、[Yes] をクリックします。

[Threat 360] ウィンドウには、次のように有線ネットワーク上の不正 AP 封じ込めステータスが表示されます。

- 青色のチェックマークが付いたバナーは、無線ネットワーク上の不正 AP 封じ込め要求が進行中であることを示します。

- 緑色のチェックマークが付いたバナーは、対応するインターフェイスで優先ネットワーク上の不正AP封じ込めが正常に開始されたことを示します。
- 赤いチェックマークが付いたバナーは、有線ネットワーク上の不正 AP 封じ込め要求が失敗したことを示します。

（注）
- 封じ込めが開始されると、インターフェイスの状態が [Rogue on Wire] から別の脅威分類タイプに更新されるまでに時間がかかります。
- [Rogue on Wire] 分類タイプは、同じ不正 AP の次の無線ネットワーク上の不正メッセージの到着時に別の分類タイプに変更されます。

不正 AP の MAC アドレスが [Rogue on Wire] に分類されているが、封じ込めを開始する ACCESS モードのインターフェイスがない場合、Cisco DNA Center により、[Action] ドロップダウンリストで [Shutdown Switchport] オプションが無効になります。

（注） 対応する不正 AP が [Rogue on Wire] 分類タイプである場合を除き、[Wireless Rogue AP Containment] は開始できません。詳細については、無線ネットワーク上の不正 AP の封じ込め （3 ページ）を参照してください。

無線ネットワーク上の不正 AP の封じ込め

ネットワーク上の不正 AP 封じ込め機能により、Cisco DNA Center は不正 AP に接続されたワイヤレスクライアントを封じ込めることができます。

封じ込めは、不正な AP に接続されているクライアント間の通信を妨害するため、一部の国では違法です。 Cisco DNA Center は、無線ネットワーク上の不正 AP 封じ込めを開始する際の法的影響について警告します。

この手順では、不正 AP に接続されているワイヤレスクライアントで無線ネットワーク上の不正 AP の封じ込めを開始および停止する方法について説明します。

始める前に

[Rogue and aWIPS] アプリケーションパッケージをダウンロードしてインストールします。詳細については、不正および aWIPS アプリケーションパッケージのダウンロードとインストール Cisco DNA Centerを参照してください。

この手順を実行するには、プロビジョニング API とスケジューラ API からの G の書き込み権限があることを確認します。

ステップ 1 メニューアイコン（≡）をクリックして選択します**[Assurance]** > **[Rogue and aWIPS]** > **[Threats]**。

ステップ 2 ワイヤレスネットワーク上の不正 AP の封じ込めを実行するには、[Threat MAC address] 列の下に表示されている、[Honeypot]、[Interferer]、または [Neighbor] 分類タイプとしてマークされている不正 AP 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。

（注） 不正 AP MAC アドレスは、複数の不正 BSSID で構成されます。

ステップ 3 [Action] ドロップダウンリストをクリックし、[Stop] を選択します。

警告ダイアログボックスが表示され、法的結果に関する情報とワイヤレスコントローラに含まれる不正な BSSID のリストが表示されます。

（注） 不正 AP の MAC アドレスが [Honeypot]、[Interferer]、または [Neighbor] 分類タイプとしてマークされている場合にのみ、[Start Containment] オプションが、[Action]ドロップダウンリストに表示されます。詳細については、「Cisco 不正 AP 封じ込めアクションの互換性マトリックス」を参照してください。

ステップ 4 警告ダイアログボックスで [OK] をクリックします。

[Threat 360] ウィンドウには、次のように有線ネットワーク上の不正 AP 封じ込めステータスが表示されます。

- 青色のチェックマークが付いたバナーは、無線ネットワーク上の不正 AP 封じ込め要求が進行中であることを示します。
- 緑のチェックマークが付いたバナーは、無線ネットワーク上の不正 AP 封じ込め要求が最も強力な検出 AP に正常に送信されたことを示します。RSSI 値に基づいて最も強力な検出 AP の横に赤い縦線が表示されます。
- 赤色のチェックマークが付いたバナーは、無線ネットワーク上の不正 AP 封じ込め要求が失敗したことを示します。

（注） 封じ込めが開始されると、[Containment Status] 列が別のワイヤレス封じ込めステータスで更新されるまでに時間がかかります。

[Threat 360] ウィンドウで、[Containment] 列の横にある [i] アイコンにカーソルを合わせます。**これは常に現在のワイヤレス封じ込めステータスを示しているという**ツールチップが表示されます。

ステップ 5 Cisco DNA Center では、Cisco DNA Assurance 内の [Rogue and aWIPS] ダッシュボードの脅威テーブルで、ワイヤレス不正 AP の**封じ込め**ステータスをモニタできます。

次の可能な値を表示するには、[Containment Status] 列の横にある [i] アイコンにカーソルをホバーします。

表 *1 :* ワイヤレス封じ込めステータス可能な値

ワイヤレス封じ込めステータス	意味
Contained	ワイヤレスコントローラによってアクティブに封じ込められている不正 AP

Pending	ワイヤレスコントローラではこの不正は封じ込め保留状態に保持されています。
オープン（Open）	不正APは封じ込めらていません。
一部	不正 BSSID の一部は開いており、残りの部分は、封じ込められた状態または封じ込め保留状態になっています。

（注） ワイヤレス封じ込めステータスが [Partial] の不正 AP の場合、[Threat 360] ウィンドウの [Containment] 列の [Partial] 状態の横に [i] アイコンが表示されます。カーソルを [i] アイコンにホバーすると、**不正 SSID** の現在のワイヤレス封じ込めステータスが表示されます。

ワイヤレスコントローラは、次の理由により、ワイヤレスネットワーク上の不正 AP 封じ込めを保留状態に保つことができます。

- **リソースの停止**：不正な BSSID 封じ込め要求が送信されると、ワイヤレスコントローラは、不正な BSSID 封じ込めを [Containment] または [Containment Pending] のいずれかの状態にします。これは、クライアントがサービスを提供する無線の無線制限が 3 つの不正 BSSID、モニターモードの無線制限が 6 つの不正 BSSID であるためです。無線が指定された制限を超えると、封じ込めのために次に送信された不正な BSSID は、いずれかの不正な BSSID が封じ込め状態から外れるまで、ワイヤレスコントローラによって保留状態になります。
- **保護された管理フレーム（PMF）**：ワイヤレスコントローラは、保護された管理フレーム（PMF）が不正 BSSID で有効であり、封じ込めステータスを保留状態に維持している限り、封じ込めを開始しません。PMF が無効になると、ワイヤレスコントローラが封じ込めを開始します。
- **動的周波数選択（DFS）**：ワイヤレスコントローラは封じ込めステータスを保留状態に維持し、動的周波数選択（DFS）チャネルでブロードキャストする場合、不正なBSSIDを封じ込めようとしません。不正な BSSID が DFS チャネルから移動すると、ワイヤレスコントローラは封じ込めを開始します。

ステップ 6 **封じ込め済み**、**保留中**、または**部分的な**状態としてマークされた無線ネットワーク上の不正 AP のすべての不正 BSSID を**オープン状態**に戻すには、[Threat MAC address] 列の下にリストされている不正 AP 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 7 [Action] ドロップダウンをクリックし、[Stop Containment] を選択します。

（注） [Stop Containment] オプションは、ワイヤレスネットワーク上の不正 AP が [Contained]、[Pending]、または [Partial] 状態の場合にのみ、[Action] ドロップダウンメニューに表示されます。詳細については、Cisco 不正 AP 封じ込めアクションの互換性マトリックス （6 ページ）を参照してください。

- [Threat 360] ウィンドウに青色のチェックマーク通知がバナーとして表示され、ワイヤレスネットワーク上の不正 AP で [Stop Containment] プロセスが進行中であることが示されます。

- [Threat 360] ウィンドウに緑色のチェックマーク通知がバナーとして表示され、ワイヤレスネットワーク上の不正 AP で [Stop Containment] プロセスが進行中であることが示されます。

Cisco 不正 AP 封じ込めアクションの互換性マトリックス

この表は、[Threat 360] ウィンドウでの不正 AP の現在の状態に対する不正 AP 封じ込めアクションの動作を示しています。

表 *2 :* 不正 *AP* 封じ込めアクションの互換性マトリックス

不正 AP 脅威タイプ	**無線ネットーワーク上の不正 AP の現在の封じ込め状態**	**[Actions] ドロップダウンリストの [Start Containment] オプション**	**[Actions] ドロップダウンリストの [Stop Containment] オプション**
ビーコン不正チャネル	開く	ディセーブル	ディセーブル
	包含/保留中/部分	無効	イネーブル
Beacon DS Attack	開く	ディセーブル	ディセーブル
	包含/保留中/部分	無効	イネーブル
AP Impersonation	開く	ディセーブル	ディセーブル
	包含/保留中/部分	無効	イネーブル
Rogue on Wire	Open/Contained/Pending/Partial	非表示 **スイッチポートのシャットダウン**が表示されています	非表示 **スイッチポートのシャットダウン**が表示されています
許可リスト	開く	ディセーブル	ディセーブル
	包含/保留中/部分	無効	イネーブル
ハニーポット	開く	イネーブル	無効
	包含/保留中/部分	無効	イネーブル
Interferer	開く	イネーブル	無効
	包含/保留中/部分	無効	イネーブル
Friendly	開く	ディセーブル	ディセーブル
	包含/保留中/部分	無効	イネーブル

Neighbor	開く	イネーブル	無効
	包含/保留中/部分	無効	イネーブル
カスタムルール（高、潜在的）	開く	イネーブル	無効
	包含/保留中/部分	無効	イネーブル
カスタムルール（情報）	開く	ディセーブル	ディセーブル
	包含/保留中/部分	無効	有効

不正 AP の封じ込めのタスクと監査ログの表示

封じ込めに失敗した場合は、Cisco DNA Center では送信された有線および無線ネットワーク上の不正 AP 封じ込め要求のタスクと監査ログを表示できます。

ステップ 1 メニューアイコン（≡）をクリックして選択します**アクティビティ**。

ステップ 2 [Activity] ウィンドウで、[Tasks] タブをクリックします。

ステップ 3 [Search] フィールドに **ROGUE** と入力するか、[ROGUE] を選択します。

有線およびワイヤレスの不正 AP 封じ込めに関連する送信済み要求のリストが表示されます。

ステップ 4 対応する封じ込め要求をクリックします。

[ROGUE] ウィンドウが表示され、不正 AP 封じ込め操作の詳細、ステータス、日時が表示されます。

ステップ 5 [Audit Logs] タブをクリックして、不正 AP 封じ込めタイプと対応するデバイス IP アドレスを表示します。

（注）
- Cisco AireOS の場合、封じ込め要求の監査ログには CLI コマンドが表示されます。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の場合、封じ込め要求の監査ログには NETCONF 要求が表示されます。
- **有線ネットワーク上の不正 AP 封じ込め**の場合、監査ログには、スイッチポートをダウンさせるためにスイッチで実行された CLI コマンドが表示されます。

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。