Cisco DNA Center 不正管理および aWIPS アプリケーション リリース 2.3.7.0 および 2.3.7.3 クイックスタートガイド

最終更新：2025 年 4 月 7 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.

目 次

第 1 章 新機能および変更された機能に関する情報 1

第 2 章 Cisco DNA Center 不正管理および aWIPS アプリケーション 3

不正管理および aWIPS アプリケーションの概要 3

不正管理について 5

Advanced Wireless Intrusion Prevention System について 7

拡張性に関する情報 10

基本的な設定のワークフロー 11

第 3 章 Cisco DNA Center の不正管理アプリケーションパッケージのインストール 13

アプリケーション管理 13

Cisco DNA Center での不正管理および 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 13

第 4 章 不正管理および aWIPS ダッシュボードのモニタリング 15

不正管理および aWIPS アプリケーションへのアクセス 15

不正管理および aWIPS ダッシュボードのモニタリング 15

ネットワークの不正な脅威のモニタリング 21

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 25

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 28

第 5 章 aWIPS プロファイル 31

aWIPS プロファイルについて 31

aWIPS プロファイルの前提条件 32

aWIPS プロファイル構成ワークフローの作成 32
aWIPS プロファイルの表示 36
ネットワークデバイスへの aWIPS プロファイルの割り当て 36
aWIPS プロファイルの編集 38
aWIPS プロファイルの削除 38
aWIPS または aWIPS フォレンジックキャプチャの有効化または無効化 39

第 6 章 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 41
不正 AP の封じ込めの概要 41
有線ネットワーク上の不正 AP の封じ込め 42
無線ネットワーク上の不正 AP の封じ込め 43
Cisco 不正 AP 封じ込めアクションの互換性マトリックス 46
不正 AP の封じ込めタイプのタスクと監査ログの表示 47

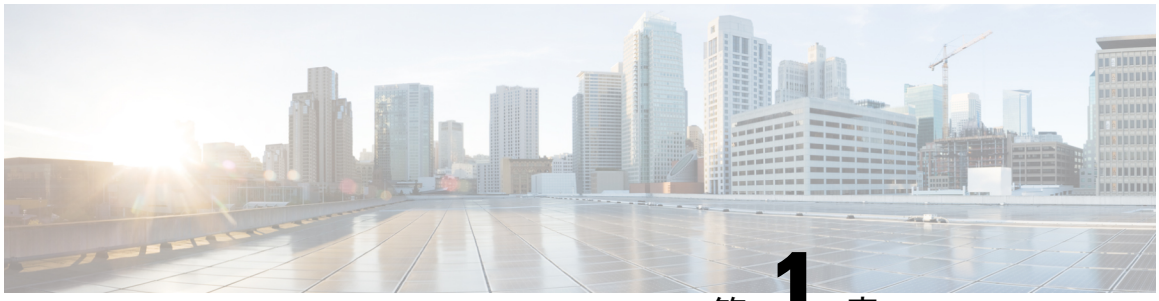
第 7 章 不正 AP のカスタム分類 49
許可リストワークフローについて 49
許可リストワークフローの設定 50
カスタム不正ルールの作成について 51
カスタム不正ルールの作成 52
不正ルールの編集 53
不正ルールの削除 54
不正ルールプロファイルについて 54
不正ルールプロファイルの作成 55
不正ルールプロファイルの編集 57
不正ルールプロファイルの削除 57
許可されたベンダーリストについて 58
許可されたベンダーのリストの作成 58
ベンダールールリスト情報の表示 59
ベンダールールの編集 59
ベンダールールの削除 60

第 8 章 不正および aWIPS イベント通知 61

不正および aWIPS イベント通知に関する情報 61

不正イベント 62

aWIPS イベント 63



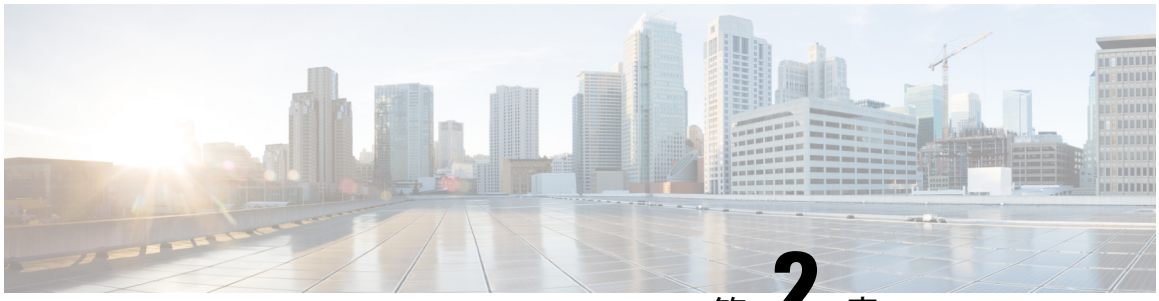
第 1 章

新機能および変更された機能に関する情報

次の表に、Cisco DNA Center 2.3.7 の新機能および変更された機能の概要と参照先を示します。

表 *1 : Cisco DNA Center* リリース *2.3.7* の新機能および機能変更

機能	説明
不正および aWIPS の可視性と制御	設定の可視化と制御機能は、不正および aWIPS サブスクリプションでサポートされています。 不正管理および aWIPS ダッシュボードのモニタリング （15 ページ）を参照してください。



第 2 章

Cisco DNA Center 不正管理および aWIPS アプリケーション

- 不正管理および aWIPS アプリケーションの概要 （3 ページ）
- 不正管理について （5 ページ）
- Advanced Wireless Intrusion Prevention System について （7 ページ）
- 拡張性に関する情報 （10 ページ）
- 基本的な設定のワークフロー （11 ページ）

不正管理および aWIPS アプリケーションの概要

（注） リリース 2.1.2.0 より前の Cisco Digital Network Architecture（DNA）Center リリースでは、不正管理機能がデバイスの可制御性の一部としてプロビジョニングされていました。Cisco DNA Center のアップグレード後、プロビジョニング済みの不正管理サブスクリプションは、以前に検出された シスコ ワイヤレス コントローラ から自動的には削除されません。新たに検出された ワイヤレスコントローラ で、不正管理の検出が不定期に報告される場合があります。

不正管理アプリケーションは、Cisco DNA Centerにインストールできるオプションのパッケージです。不正管理アプリケーションは、Cisco DNA Center 内で動作し、不正アクセスポイントからの脅威をモニタするのに役立ちます。Cisco DNA アシュアランス GUI Cisco DNA Centerでは、のダッシュボードとして不正管理機能にアクセスできます。

（注） Cisco DNA Center リリース 2.3.7 以降では、不正管理および aWIPS アプリケーションパッケージが仮想アプライアンス（VA）に適用されます。

Cisco DNA Center には Cisco Advanced Wireless Intrusion Prevention System（aWIPS）が統合されているため、不正および aWIPS ダッシュボードで aWIPS 署名をモニターできます。

このガイドでは、Cisco DNA Center で不正および aWIPS アプリケーションパッケージをアクティブ化する方法について説明します。また、前提条件と設定、不正管理および aWIPS ダッシュボードのモニタリング方法、重要な注意事項と制約事項も示します。

（注）
- 不正または aWIPS サブスクリプションの有効化や無効化などのプロビジョニングアクションは、IPv6 展開でサポートされています。
- aWIPS プロファイル設定や有線およびワイヤレスデバイスの手動封じ込めや自動封じ込めなどのプロビジョニングアクションは、IPv6 展開ではサポートされていません。

不正管理アプリケーションは、Cisco AireOS リリース 8.8.111.0 以降を実行する次の Cisco AireOS コントローラモデルをサポートしています。

- Cisco 3504 ワイヤレス コントローラ
- Cisco 5520 ワイヤレス コントローラ
- Cisco 8540 ワイヤレス コントローラ
- Cisco Mobility Express

不正管理アプリケーションをサポートする Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のモデルは次のとおりです。

- Catalyst 9300 シリーズ スイッチ用 Cisco Catalyst 9800 組み込みワイヤレス コントローラ
- Cisco Catalyst 9800-40 ワイヤレスコントローラ
- Cisco Catalyst 9800-80 ワイヤレスコントローラ
- Cisco Catalyst 9800-CL Cloud ワイヤレス コントローラ
- Cisco Catalyst 9800-L ワイヤレスコントローラ
- Cisco Embedded Wireless Controller on Catalyst Access Points

aWIPS は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ リリース 17.1.x 以降の Cisco Catalyst 9100 シリーズ アクセスポイントおよび Cisco 802.11ac Wave 2 Aironet アクセスポイントをサポートしています。

aWIPS アプリケーションをサポートする Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのモデルは次のとおりです。

- Catalyst 9300 シリーズ スイッチ用 Cisco Catalyst 9800 組み込みワイヤレス コントローラ
- Cisco Catalyst 9800-40 ワイヤレスコントローラ
- Cisco Catalyst 9800-80 ワイヤレスコントローラ
- Cisco Catalyst 9800-CL Cloud ワイヤレス コントローラ
- Cisco Catalyst 9800-L ワイヤレスコントローラ

• Cisco Embedded Wireless Controller on Catalyst Access Points

不正管理について

Cisco DNA Center の不正管理アプリケーションは、脅威を検出して分類し、ネットワーク管理者、ネットワークオペレータ、およびセキュリティオペレータがネットワークの脅威をモニタできるようにします。Cisco DNA Center は、最も優先度の高い脅威を迅速に特定するのに役立ち、Cisco DNA アシュアランス内の [Rogue and aWIPS] ダッシュボードでこれらの脅威をモニタできます。

不正なデバイスとは、ネットワーク内で管理対象の AP 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 AP は、正規のクライアントをハイジャックすることによって、無線 LAN の動作を妨害する可能性があります。ハッカーは不正 AP を使用して、ユーザ名やパスワードなどの機密情報を取得できます。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。このアクションは、特定のクライアントに送信するように通知し、他のすべてのユーザに待機するように指示する AP を模倣します。その結果、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ります。したがって、無線 LAN サービスプロバイダーは、境域からの不正なアクセスポイントの締め出しに強い関心を持っています。

不正な AP 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、認可されていない不正な AP 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 AP 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されているとき、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 AP 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 AP 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、無線ユーザはセキュリティで保護されていない AP の場所を頻繁に公表するため、企業のセキュリティが侵害される危険性も増大することです。

Cisco DNA Center は、すべての近隣の AP を継続的にモニタし、不正 AP に関する情報を自動的に検出して収集します。

Cisco DNA Centerは、管理対象 AP から不正なイベントを受信すると、次のように反応します。

- 不明な AP が Cisco DNA Center によって管理されていない場合は、Cisco DNA Center によって不正分類ルールが適用されます。
- 不明な AP がネットワークと同じ SSID を使用していない場合は、Cisco DNA Centerが、AP が企業の有線ネットワークに接続され、有線ネットワークに通じているかどうかを確認します。不正 AP が企業ネットワークのスイッチポートに物理的に接続されている場合、Cisco DNA Center は AP を**有線ネットワーク上の不正**として分類します。

  有線ネットワーク上の不正を検出するには、Cisco DNA Center で管理されているシスコスイッチが必要です。

（注） Cisco DNA Center により、有線ネットワーク上の不正でない AP が誤って有線ネットワーク上の不正として分類される場合があります。この誤った分類は、不正なクライアントが有線ネットワーク上の不正 AP から有線ネットワーク上の不正でない AP にローミングしている場合に発生します。新しい不正 AP の情報を含む新しい不正クライアントレポートが受信され、そのクライアントのホストエントリが、不正クライアント情報を削除する前に Cisco DNA Center で使用できるようになります。これは、不正なクライアントのスイッチポートの詳細がスイッチで削除され、Cisco DNA Center と同期されるまでに時間がかかるためです。そのため、クライアントがローミングする新しい不正 AP は、同期が発生する前に有線ネットワーク上の不正として分類されます。

- AP が Cisco DNA Center に対して不明で、ネットワークと同じ SSID を使用している場合、Cisco DNA Center は AP を**ハニーポット**として分類します。

（注）
- 以前にハニーポットとして分類された検出された SSID は、バックアップには保持されません。したがって、復元操作の後、SSID はハニーポットとして分類されません。
- Cisco DNA Center でハニーポットとして分類された SSID は、ワイヤレスコントローラから削除されてもその分類のままになります。検出された SSID が Cisco DNA Center のバックアップの復元時に Cisco DNA Center で復元されなければ、ハニーポットの分類は行われません 。

- 不明な AP がネットワークと同じ SSID を使用しておらず、社内ネットワークに接続されていない場合、Cisco DNA Centerは、干渉が発生しているかどうかを確認します。存在する場合は、Cisco DNA Centerは AP を**干渉源**として分類し、不正な状態を**潜在的な脅威**としてマークします。この分類のしきい値レベルは -75 dBm で、それを超える場合にネットワーク上の干渉源として分類されます。
- 不明な AP がネットワークと同じ SSID を使用しておらず、社内ネットワークに接続されていない場合、Cisco DNA Center はその AP がネイバーであるかどうかを確認します。ネイバーである場合、 Cisco DNA Centerは AP を**ネイバー**として分類し、不正状態を**情報**としてマークします。この分類のしきい値レベルは -75 dBm で、それ以下の場合に不正 AP がネイバー AP として分類されます。

Advanced Wireless Intrusion Prevention System について

Cisco Advanced Wireless Intrusion Prevention System（aWIPS）は、ワイヤレス侵入の脅威を検出して軽減するメカニズムです。ワイヤレスの脅威検出およびパフォーマンスの管理のための高度な手法を使用します。APは脅威を検出し、アラームを生成します。この手法では、ネットワーク トラフィック分析、ネットワーク デバイス/トポロジに関する情報、シグニチャベースの技法、および異常検出を組み合わせることにより、非常に正確で全面的な無線の脅威防御を実現できます。

インフラストラクチャに完全に統合されたソリューションを採用して、有線ネットワークと無線ネットワークの両方で無線トラフィックを継続的に監視し、ネットワーク インテリジェンスを使用してさまざまなソースからの攻撃を分析することにより、損害または漏洩が発生する前に、攻撃を正確に特定し事前に防止することができます。

Cisco DNA Center には aWIPS の機能が統合されているため、aWIPS で WIPS のポリシーとアラームを設定およびモニタし、脅威を報告することができます。

aWIPS は次の機能をサポートしています。

- スタティックシグニチャ
- スタンドアロンシグニチャ検出
- アラーム
- コントローラおよび AP イメージに付属のスタティック シグニチャ ファイル

Cisco DNA Center では、さまざまなサービス妨害（DoS）攻撃を検出する次のシグニチャがサポートされています。

- **認証フラッド**：多数のクライアントステーションを偽装（MACアドレススプーフィング）して AP に認証要求を送信し、AP のクライアント ステート テーブル（アソシエーション テーブル）のフラッディングを引き起こします。ターゲット AP では、個々の認証要求を受け取るたびにアソシエーションテーブルに状態 1 のクライアント項目が作成されます。オープンシステム認証が使用されている AP は、認証成功フレームを戻し、クライアントを状態 2 にします。共有キー認証（SHA）が AP に使用されている場合、AP は攻撃者の模倣クライアントに認証チャレンジを送信しますが、これは応答せず、AP はクライアントを状態 1 に保ちます。これらのシナリオのいずれにおいても、AP には、状態 1 または状態 2 のいずれかの状態にある複数のクライアントが含まれ、AP アソシエーションテーブルがいっぱいになります。テーブルが上限に達すると、正規のクライアントがこの AP に対して認証およびアソシエートできなくなります。
- **アソシエーションフラッド**：AP に大量のスプーフィングされたクライアント アソシエーションを送り付け、AP のリソース（特にクライアント アソシエーション テーブル）を枯渇させます。攻撃者はこの脆弱性を利用して大量のクライアントをエミュレートし、多数のクライアントを作成して、ターゲット AP のクライアント アソシエーション テーブルのフラッディングを発生させます。クライアント アソシエーション テーブルがオーバーフローすると、正規のクライアントをアソシエートできなくなります。

- **CTS フラッド**：特定のデバイスが同じ無線周波数（RF）メディアを共有するワイヤレスデバイスにバルク Clear To Send（CTS）制御パケットを送信し、CTS フラッドが停止するまでワイヤレスデバイスによる RF メディアの使用をブロックします。
- **RTS フラッド**：特定のデバイスが AP にバルク RTS 制御パケットを送信してワイヤレス帯域幅をブロックし、その AP 上のクライアントのパフォーマンス障害を引き起こします。
- **ブロードキャストプローブ**：特定のデバイスがブロードキャストプローブ要求を使用して、管理対象 AP をフラッディングしようとします。
- **ディスアソシエーション フラッド**：AP からクライアントへのディスアソシエーション フレームをスプーフィングして AP を状態 2（未アソシエートまたは未認証）にします。クライアントアダプタ実装では、この攻撃はこのクライアントに対してワイヤレスサービスを妨害する点で効果的かつ即効性があります。通常、クライアント ステーションは攻撃者が新たなディスアソシエーション フレームを送り付けるまで、サービスを回復するために再アソシエートと再認証を行います。攻撃者は繰り返しディスアソシエーション フレームをスプーフし、クライアントを使用不能な状態にします。
- **ディスアソシエーション ブロードキャスト**：特定のデバイスが関連付け解除ブロードキャストをトリガーして、すべてのクライアントを切断しようとすることです。

  この攻撃では、AP からブロードキャストアドレス（すべてのクライアント）へのディスアソシエーション フレームをスプーフィングして AP のクライアントを状態 2（未アソシエートまたは未認証）にします。現在のクライアントアダプタの実装では、この形式の攻撃は、複数のクライアントに対するワイヤレスサービスを即座に中断します。通常、クライアント ステーションは攻撃者が新たなディスアソシエーション フレームを送り付けるまで、サービスを回復するために再アソシエートと再認証を行います。攻撃者は繰り返しディスアソシエーション フレームをスプーフし、すべてのクライアントを使用不能な状態にします。
- **認証解除フラッド**：AP からクライアント ユニキャスト アドレスへの認証解除フレームをスプーフィングして AP のクライアントを状態 1（未アソシエートまたは未認証）にします。現在のクライアントアダプタの実装では、この形式の攻撃はクライアントに対するワイヤレスサービスを即座に中断します。通常、クライアント ステーションは攻撃者が新たな認証解除フレームを送り付けるまで、サービスを回復するために再アソシエートと再認証を行います。攻撃者は繰り返し認証解除フレームをスプーフし、すべてのクライアントを使用不能な状態にします。
- **認証解除ブロードキャスト**：この DoS 攻撃では、AP からブロードキャストアドレスへの認証解除フレームをスプーフィングして AP のすべてのクライアントを状態 1（未アソシエートまたは未認証）にします。クライアントアダプタの実装では、この形式の攻撃は、複数のクライアントに対するワイヤレスサービスを即座に中断します。通常、クライアント ステーションは攻撃者が新たな認証解除フレームを送り付けるまで、サービスを回復するために再アソシエートと再認証を行います。
- **EAPOL ログオフフラッド**：特定のデバイスが、LAN 上で動作する拡張可能な認証プロトコル（EAPOL）ログオフパケットを送信しようとすることです。このパケットが WPA および WPA2 認証で使用され、サービス妨害が引き起こされます。

EAPOL ログオフフレームは認証されないため、攻撃者はこのフレームをスプーフィングし、ユーザを AP からログオフさせることができます。これにより DoS 攻撃が成立します。クライアントが AP からログオフしたことは、クライアントが WLAN 経由で通信を試行するまでは明らかではありません。通常この妨害が検出されると、クライアントはワイヤレス接続を回復するため自動的に再アソシエートと認証を行います。攻撃者は、スプーフィングされた EAPOL-Logoff フレームを継続的に送信できます。

- **AirDrop セッション**：AirDrop セッション攻撃は、Apple 社の機能である AirDrop がファイル共有のためのピアツーピアリンクの設定に使用されている場合に発生します。この結果、WLAN 環境で未承認のピアツーピアネットワークが動的に作成されるため、セキュリティリスクが生じる可能性があります。
- **認証失敗フラッド**：認証失敗フラッド攻撃は、特定のデバイスが、有効なクライアントからスプーフィングされた無効な認証要求で AP をフラッディングしようとすると発生し、接続解除につながります。
- **ビーコンフラッド**：攻撃者が、有効な AP とステーション間の新しいアソシエーションを妨げることで、企業のインフラストラクチャ全体のワイヤレスアクティビティを阻害できる DoS 攻撃の形式。ビーコン フラッド攻撃では、ネットワークをアクティブに探しているステーションは、異なる MAC アドレスと SSID を使用して生成されたビーコンでネットワークから攻撃されます。このフラッドによって、有効なクライアントは企業 AP によって送信されるビーコンを検出できなくなり、DoS 攻撃を受けることになります。
- **ブロック ACK フラッド**：攻撃者が 802.11n AP を妨害し、特定の有効な企業クライアントからフレームを受信できないようにする DoS 攻撃の形式。802.11n 規格の導入に伴い、クライアントがフレームの大きなブロックをセグメントに分割することなく、同時に送信することができるトランザクションメカニズムが導入されました。この交換を開始するために、クライアントは Add Block Add Acknowledgment（ADDBA）要求を AP に送信します。この要求には、送信されているブロックのサイズを AP に通知するためのシーケンス番号が含まれています。AP は指定されているシーケンス内のすべてのフレームを受け入れ（範囲外のフレームはすべてドロップし）、トランザクションが完了したら BlockACK メッセージをクライアントに送信します。
- **EAPOL-Start V1 フラッド**：攻撃者は AP の内部リソースを使い果たすために EAPOL-Start フレームを大量に送り付け、AP をダウンさせようとします。
- **ファジングビーコン**：無効な、予期しない、またはランダムなデータがビーコンに取り込まれます。その変更されたフレームが空中にリプレイされます。このプロセスは接続先デバイスに、ドライバのクラッシュ、オペレーティングシステムのクラッシュ、スタックベースのオーバーフローなど予想外の動作を引き起こす場合があり、影響を受けたシステムで任意コードを実行できる状態にします。
- **ファジングプローブ要求**：無効な、予期しない、またはランダムなデータがプローブ要求に導入されます。その変更されたフレームが空中にリプレイされます。
- **ファジングプローブ応答**：無効な、予期しない、またはランダムなデータがプローブ応答に導入されます。その変更されたフレームが空中にリプレイされます。

- **無効な MAC OUI フレーム**：有効な OUI を持たないスプーフィングされた MAC アドレスが使用されます。
- **不正な形式の関連付け要求**：攻撃者が不正な形式の関連付け要求を送信します。その結果、DoS 攻撃につながる AP のバグがトリガーされる可能性があります。
- **不正な形式の認証**：攻撃者が不正な形式の認証フレームを送信し、ある場合は、一部のドライバの脆弱性が公開されます。
- **プローブ応答フラッド**：攻撃者がステーションを有効な企業 AP に関連付けられないようにする DoS の形式。一般的なワイヤレストランザクションでは、ステーションは AP と関連付けする場合、AP のネットワークに関する情報を取得するためにプローブ要求を送信します。その後、ステーションは AP からのプローブ応答フレームを待ちます。攻撃者は、無効なプローブ応答を環境に大量に送り付けることで、このプロセスを悪用し、ステーションが有効な AP からの応答を受信できないようにできます。結果として、そのステーションはワイヤレスネットワークに接続できなくなり、DoS 攻撃が開始されます。
- **PS ポールフラッド**：潜在的なハッカーによってワイヤレスクライアントのMACアドレスがスプーフィングされ、PS-Poll フレームのフラッドが送信されます。その後、AP からバッファされたデータフレームがワイヤレスクライアントに送信され、クライアントが省電力モードになっているために、データフレームが欠落することがあります。
- **再関連付け要求フラッド**：AP に大量のエミュレートおよびスプーフィングされたクライアント再関連付けを送り付け、AP のリソース（特にクライアント関連付けテーブル）を枯渇させる DoS 攻撃の形式。クライアント関連付けテーブルがオーバーフローすると、正規のクライアントを関連付けできなくなり、DoS 攻撃が成立します。
- **ターゲットの認証解除**：脅威のコンテキストを強化するために、攻撃の送信元と接続先の両方で可視化されます。
- **CTS 仮想キャリア検知攻撃**：802.11n AP の MAC アドレスが変更されたときの DoS 攻撃の形式。これにより、正規のユーザーへのチャネルアクセスを妨げることで、CTS フレームタイプの値をかなり長期間にすることができます。
- **RTS 仮想キャリア検知攻撃**：802.11n AP の MAC アドレスが変更されたときの DoS 攻撃の形式。これにより、正規のユーザーへのチャネルアクセスを妨げることで、送信要求（RTS）フレームタイプの値をかなり長期間にすることができます。

拡張性に関する情報

次の表に、異なるバージョンのCisco DNA Centerアプライアンスでサポートされている不正 AP および不正クライアントの数を示します。

表 *2:* サポートされている不正 *AP* および不正クライアントの数

Cisco DNA Center アプライアンス	サポートされる不正 AP の数	サポートされる不正クライアントの数	1 日あたりの aWIPS イベントの数

44 コアCisco DNA Centerアプライアンス	24000	32,000	20,000
56 コアCisco DNA Centerアプライアンス	24000	32,000	30,000
112 コアCisco DNA Centerアプライアンス	96,000	128,000	65,000

基本的な設定のワークフロー

手順

ステップ 1 Cisco DNA Center をインストールします。

詳細については、*Cisco DNA Center* 設置ガイドを参照してください。

ステップ 2 [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 での不正管理および 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 （13 ページ）を参照してください。

ステップ 3 リリース 1.3.3.0 以降では、[Rogue and aWIPS] アプリケーションは **[Assurance]** > **[Rogue and aWIPS]** ウィンドウで有効にする必要があります。

これにより、シスコ ワイヤレス コントローラとCisco Catalyst 9800 シリーズ ワイヤレス コントローラの不正検出が有効になります。

[Rogue and 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。左上隅にあるメニューアイコンをクリックして次を選択します。**[Assurance]** > **[Rogue and aWIPS]**。

ステップ 4 シスコ ワイヤレス コントローラのようなデバイスや AP を、ディスカバリ機能を使用して検出します。

サービスポート IP アドレスの代わりに管理 IP アドレスを使用してシスコ ワイヤレス コントローラ を検出します。

ステップ 5 検出されたデバイスが **[Device Inventory]** ウィンドウに表示されていることを確認します。

デバイスは到達可能で、[Device Inventory] ウィンドウで [Managed] 状態である必要があります。

ステップ 6 サイト、ビルディング、フロアを追加してネットワーク階層を設計すると、後で設計の設定や構成を適用する場所を簡単に特定できるようになります。

新しいネットワーク階層を作成できるほか、Cisco Prime Infrastructure に既存のネットワーク階層がある場合はその階層を Cisco DNA Center にインポートすることもできます。

ステップ 7 AP の位置情報を追加し、フロアマップに配置して、ヒートマップカバレッジを可視化します。

ステップ 8 （オプション）ネットワークでのユーザー認証に Cisco Identity Services Engine（ISE）を使用している場合、Cisco DNA アシュアランス を設定して Cisco ISE を統合できます。統合することで、Cisco DNA アシュアランスのユーザー名やオペレーティングシステムなど、有線クライアントの詳細な情報を参照できます。詳細については、『*Cisco DNA Assurance* ユーザーガイド』の「About Cisco ISE Configuration for Cisco DNA Center」のトピックを参照してください。

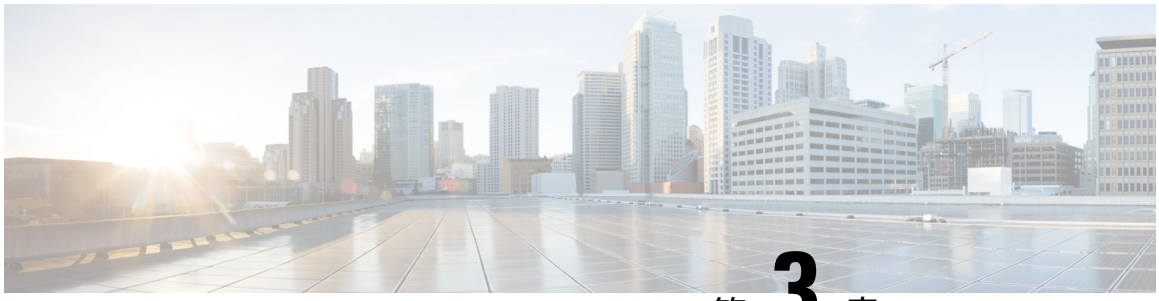
ステップ 9 （オプション）テレメトリを使用して Syslog、SNMP トラップ、Netflow コレクタサーバを設定します。詳細については、『*Cisco DNA Assurance* ユーザーガイド』の「Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry」のトピックを参照してください。

ステップ 10 Cisco DNA アシュアランス アプリケーションの使用を開始します。

ステップ 11 （オプション）Cisco Connected Mobile experience （CMX）を Cisco DNA Center と統合して同期します。詳細については、『*Cisco DNA Assurance* ユーザーガイド』の「About Cisco Connected Mobile Experiences Integration」のトピックを参照してください。

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 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。

（注）
Cisco CMX を Cisco DNA Center に統合していない場合、最も強力な RSSI で検出された不正 AP がサイトマップに表示されます。



第 3 章

Cisco DNA Center の不正管理アプリケーションパッケージのインストール

- アプリケーション管理 （13 ページ）
- Cisco DNA Center での不正管理および 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 （13 ページ）

アプリケーション管理

Cisco DNA Center はその多くの機能を、Cisco DNA Center コアインフラストラクチャとは別にパッケージ化された個別のアプリケーションとして扱います。ユーザは設定に応じて、必要なアプリケーションをインストールして実行し、使用していないアプリケーションをアンインストールできます。

左上隅にあるメニューアイコンをクリックして次を選択します。**[System]** > **[Software Updates]**。[Software Updates] ウィンドウに表示されるアプリケーションパッケージの数とタイプは、Cisco DNA Center のバージョンおよびライセンスレベルによって異なります。使用可能なアプリケーションパッケージはすべて、現在インストールされているかどうかに関係なく表示されます。

パッケージの説明とそれが必要かどうかについては、**[System]** > **[Software Updates]** ウィンドウの [Updates] タブでそのパッケージの名前にカーソルをホバーしてください。

Cisco DNA Center での不正管理および 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

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。

不正管理および aWIPS アプリケーションは、デフォルトでは Cisco DNA Center にインストールされていません。不正および aWIPS アプリケーションパッケージは、別途手動でインストールする必要があります。

不正管理には Cisco DNA Essentials ライセンスが必要であり、aWIPS には Cisco DNA Advantage ライセンスが必要です。

[Software Management] ウィンドウでアプリケーション管理手順を実行します。

1. Cisco DNA Center をインストールします。詳細については、*Cisco DNA Center* 設置ガイドを参照してください。
2. リリースノートに記載されているソフトウェア要件を確認します。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します。**[System]** > **[Software Management]** の順に選択します。

ステップ 2 [Available Applications for 2.3.xx-xxxxx] エリアまで下にスクロールし、[Rogue And AWIPS] を選択します。

ステップ 3 [Install] をクリックしてアプリケーションをインストールします。

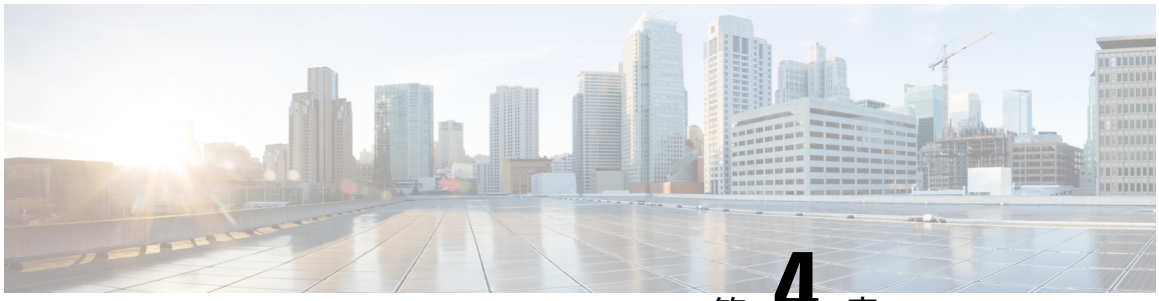
不正および aWIPS アプリケーションパッケージの更新をダウンロードしてインストールする方法の詳細については、『*Cisco DNA Center Administrator Guide*』の「Download and Install Application Updates」のトピックを参照してください。

ステップ 4 パッケージをインストールした後、不正管理アプリケーションを有効にします。

a) 左上隅にあるメニューアイコンをクリックして次を選択します。**[Assurance]** > **[Rogue and aWIPS]** の順に選択して不正管理および aWIPS アプリケーションを有効にします。

b) [Rogue Management] ウィンドウの右上隅にある [Rogue] ドロップダウンリストから、[Enable] を選択します。

これにより、シスコ ワイヤレス コントローラ と Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の不正 AP 検知が有効になります。



第 4 章

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 （15 ページ）
- 不正管理および aWIPS ダッシュボードのモニタリング （15 ページ）
- ネットワークの不正な脅威のモニタリング （21 ページ）
- 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 （25 ページ）
- 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 （28 ページ）

不正管理および aWIPS アプリケーションへのアクセス

手順

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 左上隅にあるメニューアイコンをクリックして次を選択します。**[Assurance]** > **[Rogue and aWIPS]**。

[Rogue and aWIPS] ダッシュボードが表示されます。

（注）
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 （11 ページ）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 署名の詳細な脅威分析とグローバルビューを表示するには、[Rogue and 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

不正管理および aWIPS ダッシュボードのモニタリング

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。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します。**[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。

（注）
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。

（注）
- 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っています。
- 内部にフロアを持たないサイト階層は、サイトセレクタのスライドインペイン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 で不正サブスクリプションを有効にするには、[Actions] ドロップダウンリストで、**[Rogue]** > **[Enable]**の順に選択します。

ステップ 4 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。

ステップ 5 [Rogue and aWIPS Subscription] スライドインペインで、次の手順を実行します。

（注）
[Configuration Preview] タブは、[Configuration Preview] が有効になっている場合にのみ表示されます。設定プレビューまたは ITSM 承認を有効にする方法については、『*Cisco DNA Center Administrator Guide*』の「Enable Visibility and Control of Configurations」のトピックを参照してください。

a) 不正なサブスクリプションの有効化について [Now] か [Later] のいずれかを選択し、[Apply] をクリックします。
b) CLI 設定をプレビューするには、[Generate Configuration Preview] オプションボタンをクリックします。
c) [Task Name] フィールドに任意のタスク名を入力し、[Apply] をクリックします。
d) CLI または NETCONF 設定の詳細を表示し、[Deploy] または [Submit for Approval] をクリックします。

（注）
[Submit for Approval] は、[ITSM Approval] が有効になっている場合に表示されます。

不正管理および aWIPS ダッシュボードのモニタリング

e) [Now] オプションボタンをクリックして、[Apply] をクリックします。
f) 将来の日付と時刻でタスクをスケジュールするには、[Later] オプションボタンをクリックして、展開する日時を定義します。
g) 確認ウィンドウで [Yes] をクリックします。

ステップ 6 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 7 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。

不正管理機能が無効になると、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 8 [Rogue and aWIPS Subscription] スライドインペインで、次の手順を実行します。

a) 不正なサブスクリプションの無効化について [Now] か [Later] のいずれかを選択し、[Apply] をクリックします。
b) CLI 設定をプレビューするには、[Generate Configuration Preview] オプションボタンをクリックします。
c) [Task Name] フィールドに任意のタスク名を入力し、[Apply] をクリックします。
d) CLI または NETCONF 設定の詳細を表示し、[Deploy] または [Submit for Approval] をクリックします。

（注）
[Submit for Approval] は、[ITSM Approval] が有効になっている場合に表示されます。

e) [Now] オプションボタンをクリックして、[Apply] をクリックします。
f) 将来の日付と時刻でタスクをスケジュールするには、[Later] オプションボタンをクリックして、展開する日時を定義します。
g) 確認ウィンドウで [Yes] をクリックします。

ステップ 9 **[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 10 [All]、[Failure]、[Success]、または [Progress] の各タブをクリックして、不正サブスクリプションの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。

サブスクリプションの設定の変更が 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 11 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。

ステップ 12 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。

ステップ 13 [Rogue and aWIPS Subscription] スライドインペインで、次の手順を実行します。

（注）
[Configuration Preview] タブは、[Configuration Preview] が有効になっている場合にのみ表示されます。設定プレビューまたは ITSM 承認を有効にする方法については、『*Cisco DNA Center Administrator Guide*』の「Enable Visibility and Control of Configurations」のトピックを参照してください。

a) aWIPS サブスクリプションの有効化について [Now] か [Later] のいずれかを選択し、[Apply] 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

b) CLI 設定をプレビューするには、[Generate Configuration Preview] オプションボタンをクリックします。
c) [Task Name] フィールドに任意のタスク名を入力し、[Apply] をクリックします。
d) CLI または NETCONF 設定の詳細を表示し、[Deploy] または [Submit for Approval] をクリックします。

（注）
[Submit for Approval] は、[ITSM Approval] が有効になっている場合に表示されます。

e) [Now] オプションボタンをクリックして、[Apply] をクリックします。
f) 将来の日付と時刻でタスクをスケジュールするには、[Later] オプションボタンをクリックして、展開する日時を定義します。
g) 確認ウィンドウで [Yes] をクリックします。

ステップ 14 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。

ステップ 15 [Rogue and aWIPS Subscription] スライドインペインで、次の手順を実行します。

a) aWIPS サブスクリプションの無効化について [Now] か [Later] のいずれかを選択し、[Apply] をクリックします。
b) CLI 設定をプレビューするには、[Generate Configuration Preview] オプションボタンをクリックします。
c) [Task Name] フィールドに任意のタスク名を入力し、[Apply] をクリックします。
d) CLI または NETCONF 設定の詳細を表示し、[Deploy] または [Submit for Approval] をクリックします。

（注）
[Submit for Approval] は、[ITSM Approval] が有効になっている場合に表示されます。

e) [Now] オプションボタンをクリックして、[Apply] をクリックします。
f) 将来の日付と時刻でタスクをスケジュールするには、[Later] オプションボタンをクリックして、展開する日時を定義します。
g) 確認ウィンドウで [Yes] をクリックします。

ステップ 16 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 17 [All]、[Failure]、[Success]、または [Progress] の各タブをクリックして、aWIPS サブスクリプションの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 aWIPS サブスクリプションの操作が正常に有効化されると、[Operation] 列に [Enable] と表示されます。

サブスクリプションの設定の変更が 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 18 次の情報を表示するには、[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。

不正管理および aWIPS ダッシュボードのモニタリング

- [ROGUES CONTAINED]：封じ込めら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 19 [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、[Hours] 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。

（注）
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 20 次の情報を表示するには、[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、[Top 10] または [All] の脅威の種類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して、脅威に関する詳細情報を表示します。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 21 次の情報を表示するには、[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] の下にあるそれぞれの脅威タイプをクリックします。脅威の情報はグラフビューで表示されます。 高い脅威偏差は、カラーの値のスケールで測定されます。 • 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します。高レベルの脅威のリストが表示されます。

ステップ 22 [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のマップビューが表示されます。 マップ内の対応する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のリストビューが表示されます。

ステップ 23 [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] の詳細を確認するには、[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] の情報を確認するには、[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。 不正ルールの詳細を確認するには、[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 24 （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に直接リンクするには [Tips] ダッシュレットを使用します。

ステップ 25 （オプション）[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

手順

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。

（注）
- 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っています。
- 内部にフロアを持たないサイト階層は、[Site Selector] のスライドインペインにリストされません。

ステップ 2 左上隅にある時間範囲設定（ ）をクリックして、[Threats] 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。

[Custom] 時間範囲を選択した場合は、[Start Date] と時間、および [End Date] と時間を指定します。

b) [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**	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
	脅威に関する次の情報をテーブルフォーマットで表示します。 • [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 攻撃のソースであるか、aWIPS 攻撃のターゲットであるかを示します。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 攻撃の両方に適用されます。 • [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 攻撃の両方に適用されます。 • [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]：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。 （注） [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、Cisco DNA Center リリース 2.3.2 以前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。 • Containment Status：不正 AP の有効な値（[Contained]、[Pending]、[Open]、[Partial]）

[Threats] テーブル	
アイテム	説明
	を表示します。自動で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。 1. [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。 2. [Edit Table Columns] タブで、表示するデータのチェックボックスをオンにします 3. [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正確な場所の詳細をすばやく表示できます。

ただし、これらの詳細の取得は、検出する最も強い AP の信号強度に依存します。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。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します。**[Assurance]** > **[Rogue and aWIPS]** > **[Threats]**。

ステップ 2 特定の不正 AP または aWIPS 脅威に対して [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。

（注）
フロアマップのセクションは、グローバルロケーションでは表示されません。

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、マップアイコンの詳細が表示されます。

次の表に、フロアマップアイコンの説明を示します。

表 *3:* 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

フロアマップアイコン	説明
	マーカー
	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 [Threat 360°] 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、[Host Mac]、[Device Name]、[Device IP]、[Interface Name]、[Last Updated]、[Port Mode]、[Admin Status] 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。

  （注）
  - [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。

  （注）
  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。
- [Forensic Captures] タブをクリックして、 [Detecting AP]、 [Detecting AP Site] 、[Last Updated] などの詳細を表示します。

  （注）
  [Forensic Captures] タブは、aWIPS 脅威に対してのみ表示されます。

- 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。

（注） 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では、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。

始める前に

AP 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。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します。**[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。

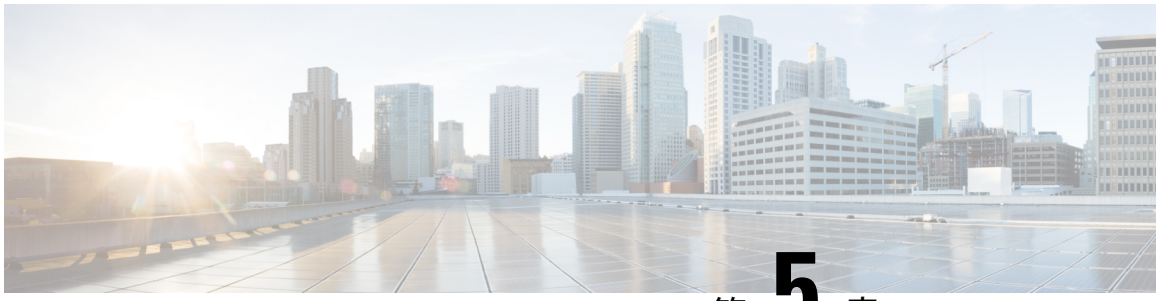
ステップ 4 [Capture Filename] 列で、**pcap** ファイルをクリックして aWIPS プロファイルのフォレンジックキャプチャをダウンロードします。

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。

（注）
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。



第 5 章

aWIPS プロファイル

- aWIPS プロファイルについて （31 ページ）
- aWIPS プロファイル構成ワークフローの作成 （32 ページ）
- aWIPS プロファイルの表示 （36 ページ）
- ネットワークデバイスへの aWIPS プロファイルの割り当て （36 ページ）
- aWIPS プロファイルの編集 （38 ページ）
- aWIPS プロファイルの削除 （38 ページ）
- aWIPS または aWIPS フォレンジックキャプチャの有効化または無効化 （39 ページ）

aWIPS プロファイルについて

aWIPS プロファイル構成では、必要な署名を選択し、aWIPS サービス妨害（DoS）攻撃の検出に使用するしきい値を設定し、署名レベルでフォレンジックキャプチャを有効にすることができます。しきい値の構成は、各 aWIPS 署名の特定期間に生成されるアラームの数を調整するのに役立ちます。

aWIPS プロファイル構成のサポートは、ソフトウェアバージョン 17.4 から 17.12 の次のデバイスで使用できます。

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ
- Cisco Catalyst 9800-CL Cloud ワイヤレス コントローラ
- Cisco Embedded Wireless Controller on Catalyst Access Points
- Catalyst 9300 シリーズ スイッチ用 Cisco Catalyst 9800 組み込みワイヤレス コントローラ
- Cisco Catalyst 9400 シリーズ スイッチ
- Cisco Catalyst 9500 シリーズ スイッチ

（注） Cisco Catalyst 9300 シリーズ スイッチ、Cisco Catalyst 9400 シリーズ スイッチ、および Cisco Catalyst 9500 シリーズ スイッチでは、aWIPS プロファイルを機能させる（SD-Access の使用例にのみ適用されます）には、ワイヤレスモジュールを有効にする必要があります。

を参照してください。

aWIPS プロファイルの前提条件

- シスコ ワイヤレス コントローラと Cisco DNA Center の間のネットワーク接続を確認してください。
- ネットワークデバイスに Cisco DNA Center から到達可能であり、aWIPS プロファイル構成が Cisco DNA Center からダウンロードされていることを確認してください。
- フォレンジックキャプチャを行うには、AP と Cisco DNA Center の間にネットワーク接続が確立されていることを確認してください。
- フォレンジックキャプチャを行うには、Google プロトコル RPC（gRPC）トンネルインターフェイスが AP と Cisco DNA Center の間に確立されていることを確認してください。**show ap icap connection** コマンドを使用して、ステータスが READY であることを確認してください。
- フォレンジックキャプチャを行うには、Cisco DNA Center とネットワークデバイスリンクの間で必要なポートが開いている必要があります。
- フォレンジックキャプチャを行うには、Cisco DNA Center とアクセスポイントの間にタイムラグがあってはなりません。
- Cisco DNA Center をリリース 2.2.1 以前のリリースからアップグレードした場合、追加のサブスクリプションに登録するには、[Rogue and aWIPS] ダッシュボードから [aWIPS] を無効にして有効にする必要があります。詳細については、不正管理および aWIPS ダッシュボードのモニタリング （15 ページ）を参照してください。

（注） Cisco DNA Center を新規にインストールする場合は、追加のサブスクリプションに登録するために、[Rogue and aWIPS] ダッシュボードから [aWIPS] を無効にして有効にする必要はありません。

aWIPS プロファイル構成ワークフローの作成

このセクションでは、aWIPS プロファイルを作成する方法について説明します。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します。**[Workflows]** > **[Create an aWIPS Profile]**。

aWIPS プロファイルは、**[Assurance]** > **[Rogue and aWIPS]** > **[aWIPS Profile]** > **[Add Profile]** を選択して、作成することもできます。

[Create an aWIPS Profile] 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。

[aWIPS Profile Creation] ウィンドウが表示されます。

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

ステップ 4 [Signatures] テーブルに、次の aWIPS プロファイルパラメータが表示されます。

- [Signature]：さまざまな DoS 攻撃を検出する標準の aWIPS 署名を示します。
- [Default Threshold]：各 aWIPS 署名の事前定義されたしきい値を示します。
- [Configure Threshold]：各 aWIPS 署名の手動で設定されたしきい値を示します。
- [Time Interval (In Seconds)]：パケットの時間間隔を示します。
- [Forensic Capture]：指定されたシグニチャの aWIPS DoS 攻撃パケットをリアルタイムでキャプチャします。

ステップ 5 [Signature] 列で、aWIPS プロファイルに対して選択（または選択解除）する aWIPS シグニチャの横にあるチェックボックスをオン（またはオフ）にします。

（注）
aWIPS シグニチャが aWIPS プロファイルに対して選択されていない場合、Cisco DNA Center は、その特定の aWIPS シグニチャに対する DoS 攻撃を検出しません。

ステップ 6 [Configure Threshold] 列で、選択した aWIPS シグニチャに対して、各 [Configure Threshold] フィールドの上に表示される指定範囲内のしきい値を入力します。

一部のシグニチャでは、構成しきい値は適用されません。これらの署名のしきい値構成値については、各 [Configure Threshold] フィールドの上部に [NA] と表示されます。

（注）
[Configure Threshold] の値に英数字を含めることはできません。

ステップ 7 [Forensic Capture] 列で、トグルボタンをクリックして、特定の aWIPS シグニチャのフォレンジックキャプチャを有効または無効にします。

（注）
- Cisco DNA Center では、aWIPS プロファイルの [Default Threshold] 値と [Time Interval (In Seconds)] 値を編集することはできません。

- aWIPS シグニチャのフォレンジックキャプチャを有効にすると、Cisco DNA Center では、[Threat 360] ウィンドウからパケットをダウンロードできます。
- aWIPS 署名のフォレンジックキャプチャを無効にすると、Cisco DNA Center は、該当の署名の aWIPS DoS 攻撃をキャプチャしません。
- RTS フラッドおよび CTS フラッドシグニチャの [Forensic Capture] を有効にすると、Cisco DNA Center のパフォーマンスに影響する可能性があります。

ステップ 8 （オプション）デフォルトの aWIPS プロファイル構成を取得するには、[Reset to Default] をクリックします。

（注）
デフォルトの aWIPS プロファイルは、高レベルのセキュリティ環境用に設定されているので、一般的な展開には適していません。要件に基づいて aWIPS プロファイルを設定します。

ステップ 9 [Next] をクリックします。

（注）
[Configure Threshold] 列で、選択した aWIPS 署名に対して、指定範囲外のしきい値を入力すると、[Create an aWIPS Profile] ウィンドウの上部にエラーメッセージが表示され、指定範囲内の値を入力するように求められます。

ステップ 10 [Profile Summary] ウィンドウで、[Profile Summary] テーブルに、[aWIPS Profile Creation] ウィンドウで設定したプロファイルの概要が表示されます。

ステップ 11 [Next] をクリックします。

ステップ 12 [Profile Creation Done] ウィンドウで、[Assign Profile to Device(s)] をクリックして、この aWIPS プロファイルをデバイスに割り当てます。

[Assign an aWIPS Profile] ウィンドウが表示されます。

[Assurance] > **[Rogue and aWIPS]** > **[aWIPS Profile]** ウィンドウで、aWIPS 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、**[More Actions]** > **[Assign]** を選択して、aWIPS プロファイルをデバイスに割り当てることもできます。

（注）
一度に複数の aWIPS プロファイルをデバイスに割り当てることはできません。

ステップ 13 [Assigned WLCs] 列で、数字のリンクをクリックして、aWIPS プロファイルに割り当てられているワイヤレスコントローラの数を表示します。

[Profile Assigned to WLC] ウィンドウに、ネットワークデバイスの次の属性が表示されます。

- [Device Name]：ネットワークデバイスの名前を示します。
- [IP Address]：ネットワークデバイスの IP アドレスを示します。
- [Profile Config URL Push Status]：ネットワークデバイスへのプロファイル構成の URL プッシュのステータスを示します。可能な値は、[Success]、[Failure]、および [In Progress] です。

[Failure] ステータスの場合は、[Failure] の横にある [i] アイコンにカーソルをホバーすると、失敗の理由が表示されます。

- [Profile Config Download Status (On Device)]：デバイスのプロファイル構成のダウンロードステータスを示します。可能な値は、[Success]、[Failure]、および [In Progress] です。

  [Failure] ステータスの場合は、[Failure] の横にある [i] アイコンにカーソルをホバーすると、失敗の理由が表示されます。

  （注）
  - Cisco DNA Center で aWIPS サブスクリプションが無効になっている場合、[aWIPS Profile] ダッシュボードの上部にエラーメッセージが表示されます。[Profile Config Download Status (On Device)] の値を表示するには、aWIPS サブスクリプションが必要です。aWIPS データ収集に登録するには、[Rogue and aWIPS] 概要ダッシュボードから [aWIPS] を有効にします。不正管理および aWIPS ダッシュボードのモニタリング （15 ページ）を参照してください。
  - デバイスでプロファイル構成の URL からプロファイル構成をダウンロードするには、デバイスと Cisco DNA Center の間の HTTP プロトコルの到達可能性が実現可能である必要があります。

- [Forensic capture config Status]：デバイスの **default-ap-profile** AP 参加プロファイルのフォレンジックキャプチャの構成ステータスを示します。可能な値は、[Success]、[Failure]、および [In Progress] です。

  [Failure] ステータスの場合は、[Failure] の横にある [i] アイコンにカーソルをホバーすると、失敗の理由が表示されます。

- [Forensic Capture]：デバイスの **default-ap-join** AP 参加プロファイルでフォレンジックキャプチャが有効か無効かを示します。カスタムの AP 参加プロファイルでのフォレンジックキャプチャはまだサポートされていません。

  対応するフォレンジックキャプチャの横にある [i] アイコンにカーソルをホバーします。[Shows the current Forensic Capture status on default-ap-profile AP Join Profile on the device] を示すツールチップが表示されます。

  （注）
  [Profile Assigned to WLC] ウィンドウでは、[Forensic Capture] を有効または無効にすることはできません。

- [Assigned On]：ワイヤレスコントローラに割り当てられた aWIPS プロファイルの日時を示します。

ステップ 14 [Next] をクリックします。

[Profile Creation Done] ウィンドウが表示されます。

aWIPS プロファイルの表示

手順

左上隅にあるメニューアイコンをクリックして次を選択します。**[Assurance]** > **[Rogue and aWIPS]** > **[aWIPS Profile]**。

[aWIPS Profile(s)] ダッシュボードが表示されます。

（注）
[aWIPS Profile] タブに初めて移動すると、[aWIPS Profile] ダッシュボードの上部にメッセージが表示され、Cisco DNA Center で [aWIPS] が有効になっている場合でも、アップグレードされたサブスクリプションに登録するように求められます。アップグレードされたサブスクリプションに登録するには、[Rogue and aWIPS] 概要ダッシュボードから [aWIPS] を無効にして有効にする必要があります。不正管理および aWIPS ダッシュボードのモニタリング （15 ページ）を参照してください。

[aWIPS Profile] ダッシュボードには、次の情報が表示されます。

- [Profile Name]：aWIPS プロファイル名のリストが表示されます。
- [Assigned WLCs]：aWIPS プロファイルに割り当てられたワイヤレスコントローラの数が表示されます。
- [Last Changed]：aWIPS プロファイルの最終作成日時または最終更新日時が表示されます。

ネットワークデバイスへの aWIPS プロファイルの割り当て

始める前に

Cisco DNA Center をリリース 2.2.2.0 以前のリリースからアップグレードする場合、追加のサブスクリプションに登録するには、[Rogue and aWIPS] 概要ダッシュボードから [aWIPS] を無効にして有効にする必要があります。不正管理および aWIPS ダッシュボードのモニタリング （15 ページ）を参照してください。

（注） Cisco DNA Center を新規にインストールする場合は、追加のサブスクリプションに登録するために、[Rogue and aWIPS] 概要ダッシュボードから [aWIPS] を無効にして有効にする必要はありません。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します。**[Workflows]** > **[Assign an aWIPS Profile]**。

[Assign an aWIPS Profile] ウィンドウが表示されます。

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。

ステップ 2 [Let's Do it] をクリックします。

[Assign an aWIPS Profile] ウィンドウが表示されます。

ステップ 3 [Profile Name] ドロップダウンリストから、デバイスに割り当てる aWIPS プロファイル名を選択します。

ステップ 4 左ペインで、[Find Hierarchy] フィールドに名前を入力してサイトを検索するか、[Global] を展開してサイトを選択します。

[Search Table] フィールドに名前を入力してネットワークデバイスを検索することもできます。

[Network Devices] テーブルにデバイスの**デバイス名**、**IP アドレス**、**ソフトウェアバージョン**、**到達可能性**、および**フォレンジックキャプチャ**が表示され、次のセクションにネットワークデバイスがリストされます。

- [Reachable & Supported]：ソフトウェアバージョン 17.4 で到達可能なサポートされているネットワークデバイスの一覧と、緑色のチェックマークの到達可能性ステータスが表示されます。
- [Not Reachable/Not Supported]：ソフトウェアバージョン 17.4 で到達不能またはサポートされていないネットワークデバイスの一覧が表示されます。到達不能またはサポートされていないネットワークデバイスに aWIPS プロファイルを割り当てることはできません。

ステップ 5 [Reachable & Supported] タブで、選択した aWIPS プロファイルに割り当てるデバイスの横にあるチェックボックスをオンにします。すべてのデバイスを選択することも、個々のデバイスを選択することもできます。

（注）
aWIPS プロファイルは、一度に最大 100 台のデバイスに割り当てることができます。

ステップ 6 [Next] をクリックします。

ステップ 7 [Profile and devices Mapped Summary] ウィンドウで、[aWIPS Profile Details] を展開して、選択した aWIPS プロファイルの構成サマリを表示し、[Device Map] を展開して、割り当てたデバイスの構成サマリを表示します。

ステップ 8 [Next] をクリックします。

[Profile Assignment to Devices initiated successfully] ウィンドウが表示されます。

（注）
デバイスへのプロファイルの割り当ては、完了するまでに時間がかかります。すぐに割り当てプロセスを再試行しないでください。

ステップ 9 デバイスに割り当てられた aWIPS プロファイルのステータスを表示するには、[Go to Rogue and aWIPS Home Page] リンクをクリックします。詳細については、aWIPS プロファイルの表示 （36 ページ）を参照してください。

aWIPS プロファイルの編集

この手順では、aWIPS プロファイルを編集する方法について説明します。

始める前に

追加のサブスクリプションに登録するには、[Rogue and aWIPS] 概要ダッシュボードから [aWIPS] を無効にして有効にする必要があります。不正管理および aWIPS ダッシュボードのモニタリング （15 ページ）を参照してください。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します。**[Assurance]** > **[Rogue and aWIPS]** > **[aWIPS Profile]**。

ステップ 2 [aWIPS Profile(s)] 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 3 表示される [Edit aWIPS Profile] ウィンドウで、必要な変更を行ってから [Save] をクリックします。

（注）
デフォルトの aWIPS プロファイルは編集できません。

プロファイルが保存され、指定の aWIPS プロファイルに割り当てられているすべてのデバイスにプッシュされます。

（注）
[Configure Threshold] 列で、選択した aWIPS 署名に対して、指定範囲外のしきい値を入力すると、[Edit aWIPS Profile] ウィンドウの上部にエラーメッセージが表示され、指定範囲内の正しい値を入力するように求められます。

aWIPS プロファイルの削除

この手順では、Cisco DNA Center から aWIPS プロファイルを削除する方法について説明します。

始める前に

追加のサブスクリプションに登録するには、[Rogue and aWIPS] 概要ダッシュボードから [aWIPS] を無効にして有効にする必要があります。不正管理および aWIPS ダッシュボードのモニタリング （15 ページ）を参照してください。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します。**[Assurance]** > **[Rogue and aWIPS]** > **[aWIPS Profile]**。

[aWIPS Profile] ダッシュボードが表示されます。

ステップ 2 [aWIPS Profile(s)] テーブルで、削除する aWIPS 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ます。

（注）
- デフォルトの aWIPS プロファイルは削除できません。
- ネットワークデバイスに割り当てられている aWIPS プロファイルは削除できません。このようなシナリオでは、デフォルトの aWIPS プロファイルにデバイスを再割り当てしてから削除する必要があります。

ステップ 3 [More Actions] ドロップダウンリストから [Delete] を選択します。

ステップ 4 確認のウィンドウで、[Delete] をクリックします。

aWIPS または aWIPS フォレンジックキャプチャの有効化または無効化

Cisco DNA Center によって、サイトレベルで aWIPS または aWIPS フォレンジックキャプチャを有効または無効にすることができます。ネットワーク内のすべての Cisco Catalyst 9800 ワイヤレスコントローラに対して aWIPS を有効または無効にすることができます。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します。**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側のペインで、[Global] が選択されていることを確認します。

（注）

サイト、ビルディング、フロアは、グローバルレベルから設定が継承されます。サイト、ビルディング、またはフロアレベルで保存された設定は、グローバルネットワーク設定を上書きします。

ステップ 4 [AP Profiles] をクリックします。

ステップ 5 [AP Profile] テーブルで、[Add] にカーソルを合わせて [AP Profile for IOS-XE] を選択します。

ステップ 6 [Security] タブをクリックします。

ステップ 7 aWIPS を有効にするには、[aWIPS] トグルボタンをクリックします。

デフォルトでは、[aWIPS] はグローバルレベルで有効になっています。

ステップ 8 （オプション）aWIPS を無効にするには、[aWIPS] トグルボタンをクリックします。

ステップ 9 フォレンジックキャプチャを有効にするには、[Forensic Capture] トグルボタンをクリックします。

（注）
フォレンジックキャプチャを有効にするには、aWIPS を有効にする必要があります。フォレンジックキャプチャが有効になっているときに aWIPS を無効化すると、フォレンジックキャプチャも無効化されます。

ステップ 10 [Save] をクリックします。

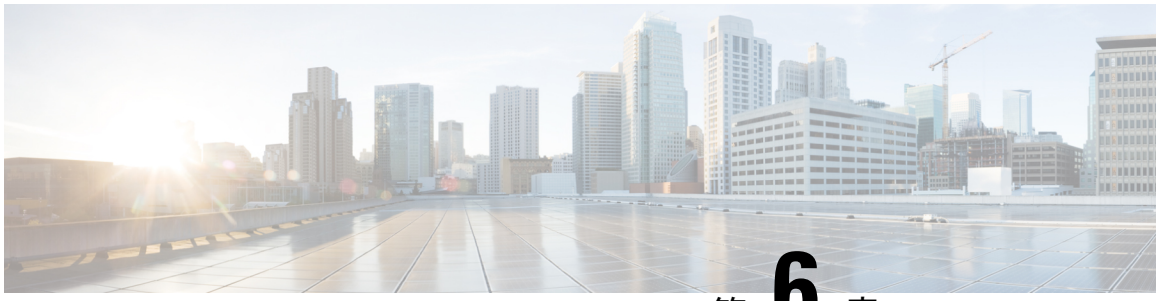
（注）
[aWIPS] または aWIPS フォレンジックキャプチャ設定を構成したら、デバイスをプロビジョニングまたは再プロビジョニングして、変更をデバイスにプッシュします。

ステップ 11 （オプション）[aWIPS and Forensic Capture Enablement] 設定をリセットするには、[Reset] をクリックします。

（注）
リリース 2.3.2.0 より前の Cisco DNA Center リリースから移行する場合は、ネットワーク設定を [aWIPS] または [aWIPS Forensic Capture] の設定で構成して、構成がワイヤレスコントローラで更新されるようにします。

[aWIPS] または [aWIPS Forensic Capture] の設定は、デバイスの AP 参加プロファイルに属します。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスがプロビジョニングされると、デバイスに関連付けられているすべての AP 参加プロファイルが取得され、次のアクションが実行されます。

- デフォルトの AP 参加プロファイルは、デバイスが割り当てられているサイトから [aWIPS] または [aWIPS Forensic Capture] の設定を継承します。
- row AP プロビジョニングの一部として Cisco DNA Center を使用して作成されたカスタムプロファイルは、対応する row AP プロファイルが作成される [Country] サイトレベルから [aWIPS] または [aWIPS Forensic] の設定を継承します。
- メッシュ AP プロビジョニングの一部として Cisco DNA Center を使用して作成されたカスタムプロファイルは、対応するメッシュ AP プロファイルが作成されるフロアサイトレベルから設定を継承します。
- Cisco DNA Center の外部で作成されたカスタム AP 参加プロファイルは、設定を継承しません。



第 6 章

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 （41 ページ）
- 有線ネットワーク上の不正 AP の封じ込め （42 ページ）
- 無線ネットワーク上の不正 AP の封じ込め （43 ページ）
- Cisco 不正 AP 封じ込めアクションの互換性マトリックス （46 ページ）
- 不正 AP の封じ込めタイプのタスクと監査ログの表示 （47 ページ）

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、有線およびワイヤレス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 封じ込めはさらに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 での不正管理および 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、および不正側から書き込み権限があることを確認してください。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します。**[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。

警告ダイアログボックスに、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と、[Configuration Preview] 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 （46 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 [Configuration Preview] タブで設定を確認し、[Yes] をクリックします。

（注）

[Configuration Preview] タブは、[Configuration Preview] が有効になっている場合にのみ表示されます。[Configuration Preview] を有効にする方法については、『*Cisco DNA Center Administrator Guide*』の「Enable Visibility and Control of Configurations」のトピックを参照してください。

ステップ 5 [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 （43 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、Cisco DNA Center での不正管理および 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 （13 ページ）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 からの書き込み権限があることを確認します。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します。**[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。

（注）
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラには、一度に 625 のみという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。

[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から、[Start Containment] と [Configuration Preview] を選択します。

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

（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 デフォルトでは、[Rogue BSSID] リストが表示されます。

[Configuration Preview] タブで設定を確認し、[Yes] をクリックします。

（注）
[Configuration Preview] タブは、[Configuration Preview] が有効になっている場合にのみ表示されます。[Configuration Preview] を有効にする方法については、『*Cisco DNA Center Administrator Guide*』の「Enable Visibility and Control of Configurations」のトピックを参照してください。

ステップ 5 [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。「This always shows current Wireless Containment Status」という説明のツールチップが表示されます。

ステップ 6 Cisco DNA Center では、アシュアランス 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 [Containment Status] をモニタリングできます。

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 *4:* 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。
Open	不正APは封じ込めらていません。
Partial	不正 BSSID の一部は [Open] の状態で、残りの部分は、[Contained] または [Containment Pending] の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 [Pending] の状態に保つことができます。

- [Resource outage]：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 [Contained] の状態から外れるまで、ワイヤレスコントローラによって [Pending] の状態になります。

- [Protected Management Frames (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 [Pending] の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。
- [Dynamic Frequency Selection (DFS)]：ワイヤレスコントローラは封じ込めステータスを [Pending] の状態に維持し、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 チャネルから移動した後、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 7 [Contained]、[Pending]、または [Partial] の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 [Open] の状態に戻すには、[Threat MAC address] 列の下にリストされている対象の不正 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 8 [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] の状態の場合にのみ、[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 （46 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

次の表は、[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 *5:* 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	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	無効	無効
	包含/保留中/部分	無効	有効

ビーコン DS 攻撃	開く	無効	無効
	包含/保留中/部分	無効	有効
AP 偽装	開く	無効	無効
	包含/保留中/部分	無効	有効
有線ネットワーク上の不正	開く/包含/保留中/部分	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	無効	無効
	包含/保留中/部分	無効	有効
ハニーポット	開く	イネーブル	ディセーブル
	包含/保留中/部分	無効	有効
干渉源	開く	イネーブル	ディセーブル
	包含/保留中/部分	無効	有効
危険性のない	開く	無効	無効
	包含/保留中/部分	無効	有効
ネイバー	開く	イネーブル	ディセーブル
	包含/保留中/部分	無効	有効
カスタムルール（高、潜在的）	開く	イネーブル	ディセーブル
	包含/保留中/部分	無効	有効
カスタムルール（情報）	開く	無効	無効
	包含/保留中/部分	無効	有効

不正 AP の封じ込めタイプ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。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します。**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、リストから [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。

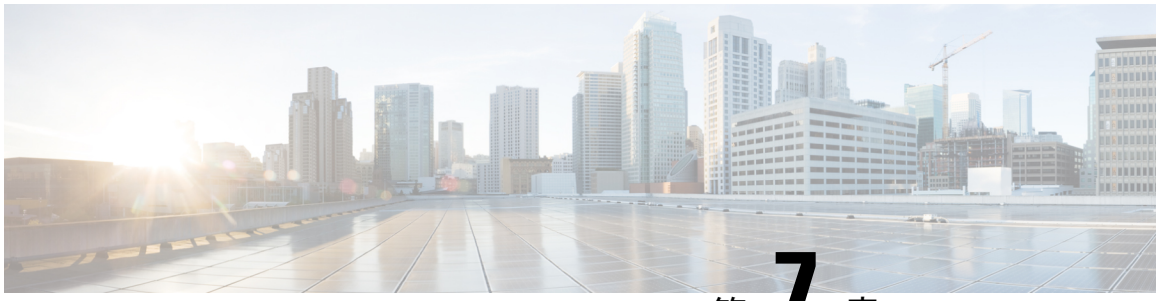
ステップ 4 対応する封じ込め要求をクリックします。

[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。



第 7 章

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 （49 ページ）
- カスタム不正ルールの作成について （51 ページ）
- 不正ルールプロファイルについて （54 ページ）
- 許可されたベンダーリストについて （58 ページ）

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 （50 ページ） に記載されている情報を使用して、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

次の不正 AP タイプは許可リストに移動できません。

- 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。

始める前に

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。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します。**[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。

今後このステップ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] フィールドを使用して、すでに 許可リストワークフローについて （49 ページ） に追加されている 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 [Download the sample CSV template from here] をクリックして、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。。

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 ファイルのサイズは 1.2 MB までにする必要があります。

（注）
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

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、こ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。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します。**[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、脅威レベルのオプションとして [High]、[Potential]、および [Informational] のいずれかを選択します。

ステップ 7 （オプション）不正なルールを自動で封じ込めるには、[Enable Auto-Containment] チェックボックスをオンにします。

（注）
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラには、一度に 625 のみという不正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] 脅威レベルに分類された不正ルールにのみ適用されます。デフォルトでは、[Potential] および [Informational] の脅威レベルに対して [Enable Auto-containment] は無効になっています。

ステップ 8 [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]、または任意の条件に一致させるための [Any] を選択します。

ステップ 9 [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 10 [Next] をクリックします。

ステップ 11 （オプション）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。

（注）
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 12 [Available rule profiles] テーブルで、対応する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。

（注）
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 13 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。

（注）
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 14 [Summary] ウィンドウで不正ルールの構成を確認します。

（注）
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 15 （オプション）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 を繰り返します。

ステップ 16 （オプション）作成した不正ルールを表示するには、[View all Rogue Rules and Profiles] をクリックします。

[Rogue Rules] タブに、作成されている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、次の方法で表示することもできます。メニューアイコンをクリックして、次を選択します。**[Assurance]** > **[Rogue and aWIPS]** > **[Rules]** > **[Rogue Rules]**。

不正ルールの編集

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します。**[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] ウィンドウで、必要に応じて変更を加えます。

（注）
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で封じ込めるには、[Enable Auto-Containment] チェックボックスをオンにします。

（注）
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラには、一度に 625 という不正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。
- 自動封じ込めができるのは、[Honeypot] と、[High] レベルの脅威のカスタムルールのみです。
- 自動封じ込めを自動的に無効にすることはできないため、自動封じ込めを有効にした後に自動封じ込めを無効にする場合は、手動で無効にする必要があります。

ステップ 5 **[Save]** をクリックします。

[Auto-Containment] 列から不正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

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します。**[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。

（注）
ルールプロファイルの不正ルールのみを削除した場合、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。

（注）
[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 （オプション）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。

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。

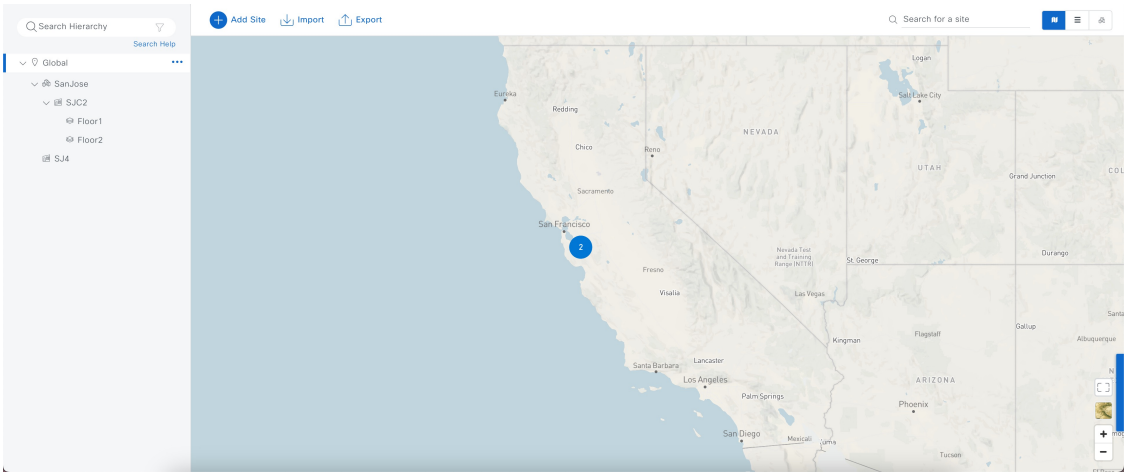
不正ルールプロファイルをサイトに割り当てると、サイトから報告される不正は、ルールプロファイルのルールと照合して検証されます。

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 つだけであることに注意してください。

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 は親サイトである [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。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します。**[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で封じ込めるには、[Enable Auto-Containment] チェックボックスをオンにします。

（注）

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラには、一度に 625 という不正封じ込め設定の制限があります。制限に達した場合、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。
- 自動封じ込めができるのは、[Honeypot] と、[High] 脅威レベルで分類されたカスタムルールのみです。

ステップ 5 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。

（注）
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 前のウィンドウで入力した値を変更する場合は、[Back] ボタンをクリックします。

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 （オプション）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、次の方法で表示することもできます。メニューアイコンをクリックして、次を選択します。**[Assurance]** > **[Rogue and aWIPS]** > **[Rules]** > **[Rogue Rule Profiles]**。

不正ルールプロファイルの編集

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します。**[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 [Edit Rule Profile] ウィンドウで、必要な変更を行います。

（注）
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修正後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で封じ込めるには、[Enable Auto-Containment] チェックボックスをオンにします。

（注）
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラには、一度に 625 という不正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。
- 自動封じ込めを自動的に無効にすることはできないため、自動封じ込めを有効にした後に自動封じ込めを無効にする場合は、手動で無効にする必要があります。

ステップ 6 確認ウィンドウで [Yes] をクリックします。

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

ステップ 8 [Auto-containment] 列から不正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 9 [Save] をクリックします。

不正ルールプロファイルの削除

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します。**[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。

許可されたベンダーリストについて

[Allowed Vendor List] 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 [High] のレベルの脅威としてマークされないようにすることができます。[Potential] または [Informational] の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。

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 [High] のレベルの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。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します。**[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 （オプション）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、ステップ 3 ～ 8 を繰り返します。

ステップ 11 （オプション）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。

ベンダールールリスト情報の表示

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します。**[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

手順

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します。**[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

手順

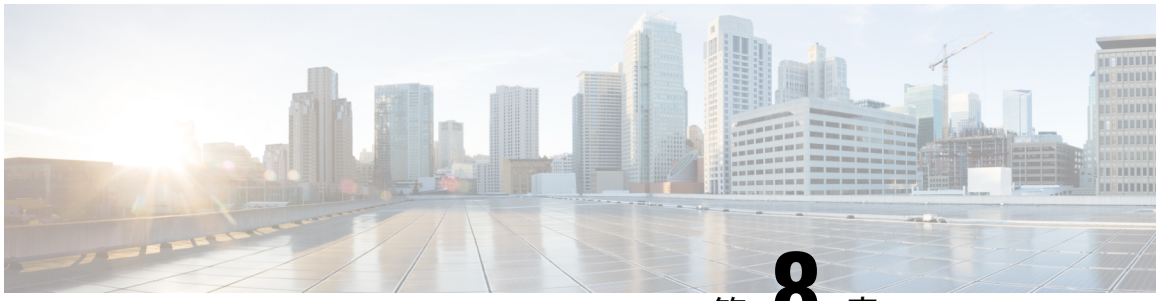
ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します。**[Assurance]** > **[Rogue and aWIPS]**。

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。



第 8 章

不正および aWIPS イベント通知

• 不正および aWIPS イベント通知に関する情報 （61 ページ）

不正および aWIPS イベント通知に関する情報

不正または aWIPS 攻撃が発生するたびに通知を送信するように Cisco DNA Center を構成できます。これらのイベントは、Cisco DNA Center 通知センターに記録されません。不正の脅威または aWIPS 脅威に登録した後にイベントが発生した場合、REST API（ウェブフック、PagerDuty、および Webex）または syslog サーバーを介して通知を受信できます。

- ウェブフックおよび syslog の接続先を設定するには、『*Cisco DNA Center* プラットフォーム ユーザガイド』の「Work with Events」のトピックを参照してください。
- PagerDuty の接続先を設定するには、『Cisco DNA Center ITSM Integration Guide』の「Cisco DNA Center to Cisco WebEx Integration」のトピックを参照してください。
- Webex の接続先を設定するには、『Cisco DNA Center ITSM Integration Guide』の「Cisco DNA Center to Cisco WebEx Integration」のトピックを参照してください。

この手順を完了したら、不正または aWIPS イベントを選択し、登録していることを確認します。

Cisco DNA Center GUI で不正または aWIPS イベントに登録するには、メニューアイコンをクリックして次を選択します。**[Platform]** > **[Developer Toolkit]** > **[Events]**。

（注） 不正または aWIPS イベントへの登録後にのみイベント通知を受け取ります。登録前に発生した脅威の場合は、Cisco DNA Center GUI でメニューアイコンをクリックして次を選択します。**[Reports]** > **[Report Templates]** > **[Rogue and aWIPS]**。

Webex および PagerDuty の接続先には、5 分ごとに 100 件のイベント通知の制限があります。5 分間に 100 件を超えるイベントを受信する場合は、ウェブフックまたは syslog の接続先を構成します。

不正イベント

不正イベントは、次の脅威レベルの高い不正に対してのみトリガーされます。

- ビーコン不正チャネル
- ビーコン DS 攻撃
- AP 偽装
- 有線ネットワーク上の不正
- ハニーポット
- 脅威レベルを高として作成されたカスタムルール

不正イベントは、次の場合にトリガーされます。

- 脅威レベルの高い不正がネットワークで初めて発見された（ROGUE_NEW_THREAT_DETECTED）
- 脅威レベルの高い不正がネットワークから削除された（ROGUE_THREAT_DELETED）
- 脅威レベルが [High] から [Potential] または [Informational] に変更された（ROGUE_THREAT_LEVEL_CHANGED）
- 脅威レベルが [Potential] または [Informational] から [High] に変更された（ROGUE_THREAT_LEVEL_CHANGED）
- 脅威レベルは [High] のままだが、脅威の種類が変わった（ROGUE_THREAT_TYPE_CHANGED）

不正イベントペイロードの詳細：

```
{
 "detectingApLocation": "string",
 "rssi": "int",
 "threatMacAddress": "string",
 "threatType": "string",
 "detectingApMacAddress": "string",
 "threatState": "string",
 "wlcIp": "string",
 "detectingApName": "string",
 "containmentState": "string",
 "vendorName": "string",
 "ssid": "string",
 "threatLevel": "string"
}
```

ペイロード内のコマンド：

- threatMacAddress：不正 AP の MAC アドレス
- ThreatType：不正の脅威のタイプ（ビーコン DS 攻撃、AP 偽装、有線ネットワーク上の不正、ハニーポット、または脅威レベルを高として作成されたカスタムルール)
- threatState：不正の脅威の状態（ROGUE_NEW_THREAT_DETECTED、ROGUE_THREAT_DELETED、ROGUE_THREAT_LEVEL_CHANGED）、ROGUE_THREAT_LEVEL_CHANGED、または ROGUE_THREAT_TYPE_CHANGED

- threatLevel：不正の状態（高、潜在的、または情報）
- detectingApName：最も強力な検出 AP の名前
- detectingApMacAddress：最も強力な検出 AP の MAC アドレス
- detectingApLocation：最も強力な検出 AP の場所
- rssi：不正 AP を検出する検出 AP の RSSI 値
- [containmentState]：不正 AP の封じ込め状態（[PENDING]、[NOTCONTAINED]、または [CONTAINED]）
- threatVendorName：不正 AP のベンダー名
- ssid：最新の SSID またはハニーポット SSID
- wlcIp：ワイヤレスコントローラ の IP アドレス

aWIPS イベント

aWIPS イベントは、ネットワーク内のすべての aWIPS 脅威に対してトリガーされます。

検出 AP ごとに通知が送信されます。複数の AP が同じ脅威を検出した場合、複数のイベント通知を受け取ります。

送信元ベースの aWIPS 脅威の場合、送信元情報が送信されます。接続先情報は [Not Applicabl] として送信されます。

接続先ベースの aWIPS 脅威の場合、接続先情報が送信されます。送信元情報は [Not Applicable] として送信されます。

ペアベースの aWIPS 脅威の場合、送信元と接続先の両方の情報が送信されます。

aWIPS イベントペイロードの詳細：

```
{
 "sourceVendorName": "string",
 "detectingApLocation": "string",
 "attackType": "string",
 "sourceMacAddress": "string",
 "detectingApMacAddress": "string",
 "wlcIp": "string",
 "detectingApName": "string",
 "targetMacAddress": "string"
}
```

ペイロード内のコマンド：

- **attackType**：aWIPS 攻撃の種類
- **sourceMacAddress**：攻撃者の MAC アドレス
- **sourceVendorName**：攻撃者のベンダー名
- **targetMacAddress**：ターゲットの MAC アドレス

- **detectingApLocation**：検出 AP の場所
- **detectingApMacAddress**：検出 AP の MAC アドレス
- **detectingApName**：検出 AP の名前
- **wlcIp**：ワイヤレスコントローラ の IP アドレス

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。