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 （1 ページ）
- 不正管理について （3 ページ）
- Advanced Wireless Intrusion Prevention System について （5 ページ）
- 拡張性に関する情報 （8 ページ）
- 基本的な設定のワークフロー （9 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 *1:* 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。

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。