aWIPS プロファイル

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 以降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。

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の場合は、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の場合は、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の場合、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の場合、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、b_rogue_management_qsg_2_3_4_chapter3.pdf#nameddest=unique_14 unique_14_Connect_42_monitor_security_dashboard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。

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**[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。

[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。

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 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 の間に HTTP プロトコルの到達可能性が存在する必要があります。

- [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。

  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

メニューアイコン（☰）をクリックして選択します**[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。

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**[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。

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 （5 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を参照してください。

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]** > **[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を参照してください。

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]** > **[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。代わりに、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 警告ウィンドウで [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。

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**[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 [aWIPS and Forensic Capture Enablement] エリアまで下にスクロールします。

ステップ 5 aWIPS を有効にするには、[Enable aWIPS] チェックボックスをオンにします。

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 6 aWIPS を無効にするには、[Enable aWIPS] チェックボックスをオフにします。

ステップ 7 フォレンジックキャプチャを有効にするには、[Enable Forensic Capture] チェックボックスをオンにします。

（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 8 **[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 9 [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 フォレンジックキャプチャ設定で構成して、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 フォレンジックキャプチャ設定は、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 フォレンジックキャプチャ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、Row AP プロファイルが作成される国サイトレベルから aWIPS または aWIPS フォレンジック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、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。

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。