Cisco AI エンドポイント分析

Cisco AI エンドポイント分析の概要

可視性は、エンドポイントを保護するための最初のステップです。Cisco AI エンドポイント分析は、エンドポイントと Internet of Things（IoT）デバイスの識別とプロファイリングに役立つエンドポイント可視性ソリューションです。Cisco AI エンドポイント分析エンジンを使用すると、さまざまなソースからネットワーク経由で受信したテレメトリ情報を使用して、エンドポイントにラベルを割り当てることができます。

Cisco AI エンドポイント分析で使用できるプロファイリングラベルは、エンドポイントタイプ、ハードウェアモデル、製造元、およびオペレーティング システム タイプです。これは多要素分類と呼ばれます。

Cisco AI エンドポイント分析は、潜在的に危険なエンドポイントやデバイスを特定して対処することを可能にする信頼スコアなどの機能により、ネットワークにおける繊細な可視化と処置を実現します。Cisco AI エンドポイント分析の GUI から Cisco ISE を介して ANC ポリシーを適用することにより、潜在的なリスクを管理することもできます。Cisco AI エンドポイント分析でエンドポイントのランダムおよび変更 MAC アドレスの問題をモニターして回避し、MAC アドレスの代わりに「DUID」と呼ばれる一意の属性を使用してエンドポイントを正確に識別することができます。

Cisco AI エンドポイント分析は、さまざまなソースからエンドポイントテレメトリを収集するのに役立ちます。主要なソースは、Network-Based Application Recognition（NBAR）メカニズムです。NBAR メカニズムは、Cisco Catalyst 9000 シリーズ スイッチ（アクセスデバイス）に組み込まれていて、ディープ パケット インスペクション（DPI）を実行します。Cisco AI エンド

ポイント分析は、Cisco DNA トラフィック テレメトリ アプライアンスからテレメトリを受信することもできます。

Cisco ISE、自己登録型ポータル、ServiceNow のような構成管理データベース（CMDB）ソフトウェアなど、さまざまなソースからエンドポイントコンテキスト情報を収集できます。

Cisco AI エンドポイント分析を使用すると、さまざまなネットワークデバイスからのデータインフローが可能になり、エンドポイントをより高い精度で容易に識別してプロファイリングし、異常に対処する機能が拡張されます。Cisco AI エンドポイント分析では、さまざまなエンドポイント情報を集約し、そのデータを使用してエンドポイントをプロファイリングできます。エンドポイントのプロファイリング後、AI と機械学習アルゴリズムを使用して、さまざまな方法を直感的に活用することで不明なエンドポイントの数を減らすこともできます。

Cisco AI エンドポイント分析の主な機能

- **Cisco AI エンドポイント分析ダッシュボード**

  Cisco AI エンドポイント分析ダッシュボードでは、ネットワークに接続されているエンドポイントの全体像を確認できます。既知のエンドポイント、不明なエンドポイント、プロファイリングされたエンドポイント、プロファイリングされていないエンドポイントの数を表示できます。インテリジェントなプロファイリング提案を表示して、エンドポイントのプロファイリングと管理をどのように強化できるかを確認することもできます。

- **機械学習機能を使用したネット内の不明なエンドポイントの削減**

  Cisco AI エンドポイント分析では、エンドポイントのグループ化で学習した情報に基づいてプロファイリング提案が提供されます。このような提案を使用して、ネットワーク内の不明なエンドポイントやプロファイリングされていないエンドポイントの数を減らすことができます。

- **システムルールおよびカスタム プロファイリング ルールによるエンドポイントの管理**

  ネットワークに接続されたエンドポイントを確実にプロファイリングおよび管理するには、シスコが提供するシステムルールと自分で設計したカスタムルールを使用します。

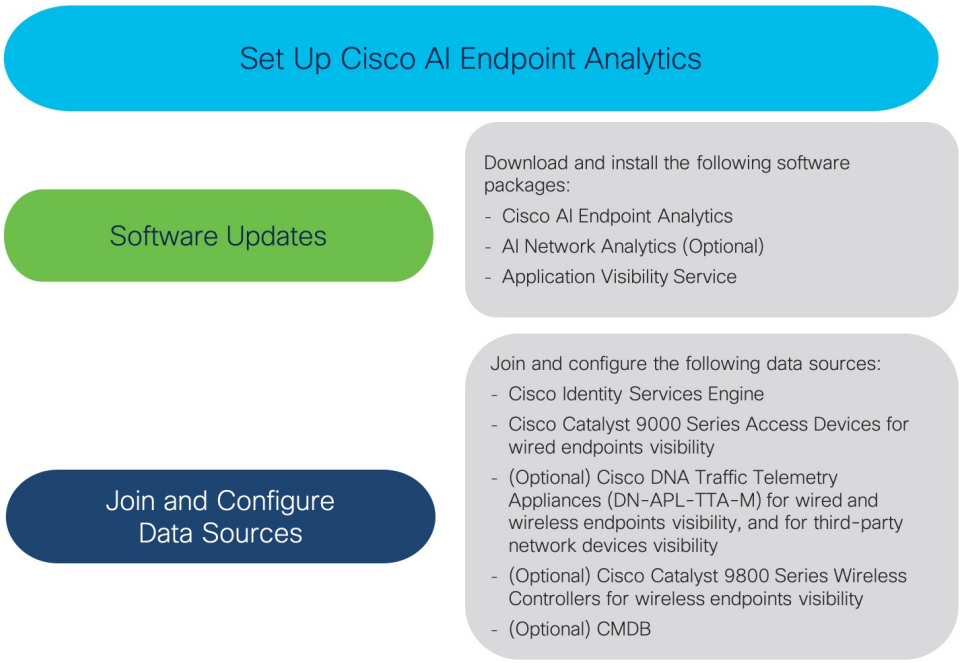
- **Cisco AI エンドポイント分析によるエンドポイントの登録**

  Cisco AI エンドポイント分析を使用して、エンドポイントをオンボードおよびプロファイリングできます。この登録プロセスでエンドポイント属性データが収集されて、エンドポイントのプロファイリングに使用されます。

- **外部ソースを使用したエンドポイントの登録**

  構成管理データベース（CMDB）などエンドポイントデータの外部ソースの中には、Cisco AI エンドポイント分析に接続できるものがあります。これにより、ネットワーク内のエンドポイントを簡単に登録、管理、およびプロファイリングできます。

Cisco DNA Center での Cisco AI エンドポイント分析のセットアップ



ソフトウェア アップデートのインストール

次の手順で説明するように、Cisco AI エンドポイント分析を使用するためのソフトウェアアップデートを Cisco DNA Center にインストールします。

ステップ 1 Cisco DNA Center にログインします。

ステップ 2 Cisco DNA Center GUI で、[Menu] アイコン（☰）をクリックし、**[System]** > **[Software Updates]** の順に選択します。

ステップ 3 表示される [Updates] タブで、[Cisco AI Endpoint Analytics]、[AI Network Analytics]、および [Application Visibility Service] が [Application Updates] セクションにリストされているかどうかを確認してください。これらのアプリケーション更新のいずれかが表示されている場合は、[Install All] ボタンをクリックします。

- Cisco DNA Center でエンドポイント プロファイリング ソリューションにアクセスするには、[Cisco AI Network Analytics] 更新をインストールします。
- 機械学習と AI の機能を使用してインテリジェントなプロファイリング提案を受け取るには、[AI Network Analytics] 更新をインストールします。

- NBAR およびコントローラベースのアプリケーション認識（CBAR）の技術を使用してエンドポイント プロファイリングを通知するには、[Application Visibility Service] 更新をインストールします。

ステップ 4 これらの更新のいずれも [Updates] タブにリストされていない場合は、[Installed Apps] タブをクリックして、更新がすでにインストールされ、使用可能であるかどうかを確認してください。[Installed Apps] タブでは、ソフトウェアインストールが正常に完了しているかどうかも確認できます。

データソースの接続と有効化

（注） Cisco AI エンドポイント分析が使用するデータソースが、Cisco DNA Center にすでに接続されている可能性があります。データソースが接続されている場合は、次の手順を参照して、Cisco AI エンドポイント分析でデータソースを使用できることを確認します。

Cisco AI エンドポイント分析が結果を提供できるようにするには、Cisco ISE または Catalyst 9000 シリーズ アクセスデバイスを Cisco DNA Center に追加する必要があります。

1. **Cisco ISE を Cisco DNA Center に接続します。**

   『*Cisco DNA Center Appliance Installation Guide*』の「Complete First-Time Setup」にある「Integrate Cisco ISE with Cisco DNA Center」セクションを参照してください。

   次の Cisco ISE リリースが Cisco AI エンドポイント分析をサポートしています。

   - 2.4 パッチ 11 以降
   - 2.6 パッチ 5 以降
   - 2.7 パッチ 1 以降
   - 3.0 以降のリリース

   Cisco ISE 管理ポータルで、次の手順を実行します。

   1. **[Work Centers]** > **[Profiler]** > **[Settings]** の順に選択します。
   2. [Endpoint Analytics Settings] エリアで、次のチェックボックスをオンにします。
      - [Publish Endpoint Attributes to AI Endpoint Analytics]
      - [Consume Endpoint Profiles from AI Endpoint Analytics]

   Cisco ISE が 802.1X または MAB 認証方式でエンドポイントを認証すると、収集されたエンドポイント属性が Cisco AI エンドポイント分析で使用可能になります。

2. **有線エンドポイントが表示されるように、Cisco 9000 シリーズ アクセス デバイスを Cisco DNA Center に接続します。**

   『*Cisco DNA Center User Guide*』の「Discover Your Network」を参照してください。

Cisco AI エンドポイント分析の機能を有効にするには、Cisco 9000 シリーズ アクセスデバイスを Cisco IOS-XE リリース 17.6 以降にアップグレードします。

必要なアクセスデバイスの CBAR を有効にするには、Cisco DNA Center で [Menu] アイコン（☰）をクリックします。

1. **[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。
2. データが必要な Cisco Catalyst 9000 アクセスデバイスを選択します。[Site Devices] セクションのデバイス名の横にあるチェックボックスをオンにします。
3. [Enable CBAR] をクリックします。

3. **（任意）ワイヤレスエンドポイントを可視化するには、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを Cisco DNA Center に接続します。**

   次の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ モデルが、Cisco AI Endpoint Analytics の非ファブリックモードでサポートされています。

   - 9800-CL
   - 9800-40
   - 9800-80
   - 9800-L

   Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの概要 で Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを設定およびプロビジョニングするには、Cisco DNA Centerを参照してください。

4. **（任意）有線およびワイヤレスエンドポイントを可視化し、サードパーティのネットワークデバイスを可視化するには、Cisco DNA トラフィック テレメトリ アプライアンスを Cisco DNA Center に接続します。**

   Cisco DNA トラフィック テレメトリ アプライアンス（DN-APL-TTA-M）は、ミラーリングされたネットワークトラフィックからテレメトリを生成してエンドポイントを分析できるようにします。このアプライアンスでは、Network-Based Application Recognition（NBAR）ベースでプロトコルを検査し、エンドポイント属性を抽出できます。

   テレメトリアプライアンスで収集されたエンドポイント属性を Cisco AI エンドポイント分析で受信するには、Cisco ISE と Cisco DNA Center を統合する必要があります。

   Cisco DNA Center でのアプライアンスのインストール、接続の構成、およびアプライアンスの管理については、『Cisco DNA Traffic Telemetry Appliances』を参照してください。

   Cisco DNA トラフィック テレメトリ アプライアンスに接続されたアクセススイッチのスイッチドポートアナライザ（SPAN）受信ポートで CBAR を有効にするには、次のコマンドを使用します。

   ```
   ip nbar protocol-discovery
   ```

   テレメトリアプライアンスに接続されているすべてのエンドポイントが Cisco AI エンドポイント分析に表示されるわけではありません。Cisco DNA アシュアランス で管理される

ネットワーク アクセス デバイス（NAD）にも接続されているエンドポイントのみが、Cisco AI エンドポイント分析に表示されます。

5. **（任意）Cisco DNA Center で ServiceNow を有効にします。**

   ServiceNow を Cisco DNA Center に接続した後に、Cisco DNA Center の [Menu] アイコン（☰）をクリックし、**[Platform]** > **[Manage]** > **[Bundles]** を選択します。

   バンドル [Endpoint Attribute Retrieval with ITSM (ServiceNow)] の [Status] が [New] の場合は、バンドルの [Enable] をクリックします。

6. **（任意）Cisco DNA Center で Cisco AI 分析を有効にします。**

   AI ベースのエンドポイントグループ化、カスタム プロファイリング ルール自動化、およびエンドポイントラベルに関する提案を受け取るには、また、ネットワーク内のスプーフィングされている可能性のあるデバイスを検出するには、[Cisco AI Analytics] ウィンドウで、必要な設定を有効にする必要があります。

   これらの AI ベースの提案を受け取るには、AI ネットワーク分析ソフトウェアをインストールする必要があります。

   1. Cisco DNA Center のメインメニューから、**[System]** > **[Settings]** > **[External Services]** > **[Cisco AI Analytics]** の順に選択します。
   2. 有効にする次の各サービスのトグルボタンをクリックします。

      - **AI エンドポイント分析**：AI ネットワーク分析は、機械学習を利用してネットワークのインテリジェンスを推進し、ネットワークパフォーマンスを効果的に改善して問題解決を加速できるようにします。AI ネットワーク分析は、ネットワークの動作を分析し、ネットワーク環境に適応することで、ノイズや誤検出を大幅に削減します。
      - **エンドポイント スマートグループ化**：エンドポイントスマート グループ化は、AI と機械学習を使用して、AI ベースのエンドポイントグループ化、自動化されたカスタムプロファイリングルール、クラウドソーシングされたエンドポイントラベルを提供することにより、ネットワーク内の不明なエンドポイントの数を減らします。
      - **AI スプーフィング検出**：AI スプーフィング検出は、動作モデルに基づいてスプーフィングされているエンドポイントを識別します。モデルは現在、デバイスから収集されたフロー情報を使用して構築されています。[Send data to help Cisco improve the model] トグルボタンを有効にすることにより、シスコによるデータ収集を可能にすることもできます。これにより、シスコによって動作モデルがさらに強化されます。

エンドポイント テレメトリ ソース

Cisco AI エンドポイント分析は、次の方法でテレメトリデータを受信します。

- **ディープ パケット インスペクション**

ディープ パケット インスペクションは、Cisco Catalyst 9000 シリーズ アクセス デバイスによって実行される高度なパケット分析方法です。これらのアクセスデバイスは、NBAR を実行します。NBAR は、アプリケーション トラフィックを検査し、プロトコル分析を実行して、精度の高いエンドポイントを検出および識別し、プロファイリングします。

ディープ パケット インスペクションのプロファイリングは、ネットワークへのエンドポイントトラフィックから収集されたさまざまな属性に基づいています。これらの属性は、パケットヘッダーレイヤ 4 ～ 7 から複数のプロトコルにわたって収集されます。

- **構成管理データベース接続**

  Cisco AI エンドポイント分析は、エンドポイント プロファイリングの精度を高めるために、構成管理データベース（CMDB）接続からエンドポイントデータを受信します。ServiceNow との接続により、CMDB から Cisco AI エンドポイント分析への情報を受信できます。

- **機械学習機能**

  プロファイリング用に収集されたデータは、匿名化されて、Cisco Cloud でデバイスデータレイクとして機能する場所に送信されます。ここでは、機械学習アルゴリズムで使用可能なデータを分析し、必要に応じて評価して適用できるプロファイリングルールを作成します。エンドポイント プロファイリングと管理を簡素化かつ効率化できるように、Cisco AI エンドポイント分析によってスマート プロファイリング ルールが提案されます。既存のルールも評価され、この継続学習に基づいて改善提案が提供されます。

[Cisco AI Endpoint Analytics Overview] ウィンドウ

Cisco DNA Center のメインメニューから **[Policy]** > **[AI Endpoint Analytics]** の順に選択します。

[Overview] ウィンドウに次のダッシュレットが表示されます。

- **合計エンドポイント数**

  このダッシュレットでは、ネットワーク内のエンドポイントの合計数が [Fully Profiled] と [Missing Profiles] の 2 つのグループに分かれて表示されます。Cisco AI エンドポイント分析は、エンドポイントタイプ、OS タイプ、ハードウェアモデル、およびハードウェア製造元の 4 つの要因に基づいてエンドポイントをプロファイリングします。エンドポイントにこれらの要因の 1 つ以上が欠落している場合は、[Missing Profiles] グループにプロファイリングされます。

- **AI 提案**

  Cisco AI エンドポイント分析は、スマートグループ化アルゴリズムを使用して、ネットワーク内で類似するプロファイリングデータを持つ不明なエンドポイントをグループ化します。AI エンドポイント分析を有効にした場合、次のタイプのルール提案が表示されます。これらのルール提案は、次のようにエンドポイントクラスタから学習した内容に基づいています。

- 類似している可能性があるエンドポイントをプロファイリングするための新しいルール。
- 以前に受け入れられていたルールの変更提案。
- 不要になったプロファイリングルールの確認。

詳細については、プロファイリングルール提案の変更（19ページ）を参照してください。

- **プロファイルラベルが欠落したエンドポイント**

  このダッシュレットには、ネットワーク内のプロファイルが欠落しているエンドポイントの数が、プロファイルラベルタイプで分類されて表示されます。表示される数は一部重複しています。たとえば、エンドポイントに OS タイプとハードウェアモデルの両方の情報がない場合、そのエンドポイントは両方のラベルの数に含まれます。

  特定のプロファイルラベルが欠落しているエンドポイントを確認するには、このダッシュレットのラベルをクリックします。[Endpoint Inventory] ウィンドウには、エンドポイントのリストが表示されます。このリストは、選択したプロファイルラベルが不明であるエンドポイントが表示されるようにフィルタ処理されます。

Endpoint Inventory

[Endpoint Inventory] タブで、データソースを介して Cisco AI エンドポイント分析に接続されているエンドポイント。このタブには、[Focus] ドロップダウンリストを使用して選択できる 2 つのビューがあります。

- [All Endpoints]：これは [Endpoint Inventory] タブのデフォルトビューです。このビューには、接続されているすべてのエンドポイントのプロファイリング情報が表示されます。

  [All Endpoints] ビューには、**エンドポイントタイプ**、**OS タイプ**、**ランダム MAC かどうか**、**信頼スコア**などのプロファイリング情報が表示されます。表示するエンドポイントのプロファイリング情報を選択するには、テーブルの右上隅にある垂直省略記号アイコンをクリックします。次のプロファイリング情報セットのいずれかを選択し、[Apply] をクリックします。

  - [All]：使用可能なすべてのプロファイリング情報が表示されます。このセットは編集できません。
  - [General]：これを選択すると、エンドポイントの全体図を確認できるプロファイリング情報が表示されます。これは、デフォルトで表示される列のセットです。このセットは編集できません。
  - [Detailed]：これを選択すると、エンドポイントを深く洞察できるプロファイリング情報が表示されます。このセットは編集できません。
  - [Custom]：これは編集可能な唯一のセットです。[Endpoint Inventory] ウィンドウに表示するプロファイリング情報をオンまたはオフにします。

必要な [View Known Profiles] ボタンをクリックして、[All Endpoints] ビューに表示されるエンドポイントのリストをフィルタ処理することもできます。**エンドポイントタイプ**、**ハードウェア製造元**、**ハードウェアモデル**、および **OS タイプ**でエンドポイントのリストをフィルタ処理できます。

- [Trust Score]：このビューでは、エンドポイント インベントリ リストがフィルタ処理され、信頼スコアが割り当てられているエンドポイントだけが表示されます。

  [Trust Score] ビューには、エンドポイントの全体的な信頼スコアを示すさまざまな要因の列が表示されます。信頼スコアは、動作異常が検出されたエンドポイントを特定するために役立ちます。これにより、エンドポイントの詳細情報を調べて、必要な修復アクションを実行することができます。低い信頼スコアを管理するためにエンドポイントに ANC ポリシーを適用する場合、[Trust Score] ビューには、適用された ANC ポリシーの名前とポリシーが適用された日時も表示されます。エンドポイントの信頼スコアを参照してください。

要件に基づいて一連のエンドポイントを簡単にフィルタ処理できます。エンドポイントを登録したり、登録済みのエンドポイントを編集、削除、およびプロファイリングしたりできます。単一または複数のエンドポイントを選択するには、MAC アドレスの横にあるチェックボックスをオンにします。これにより、選択したエンドポイントに対して、[Actions] ドロップダウンリストから特定のアクションを実行することができます。

エンドポイントのプロファイリングの完全な詳細を表示するには、エンドポイントの [MAC Address] をクリックします。表示されるスライドインダイアログボックスには、ユーザーの詳細、エンドポイントの詳細、およびエンドポイントの属性の詳細が含まれます。

[Details] タブには、Cisco DNA Center リリース 2.2.2 以降の次の新しいフィールドが Cisco ISE から受信した詳細とともに表示されます。

- [Authentication Status]：このフィールドには、エンドポイントが Cisco ISE で認証された場合は [Started]、そうでない場合は [Disconnected] と表示されます。
- [Authorization Profile]：Cisco ISE のエンドポイントに設定されている認証ポリシーがここに表示されます。
- [Scalable Group Tag]：Cisco ISE のエンドポイントに設定されたスケーラブルグループタグがここに表示されます。

これらの属性の詳細については、使用する Cisco ISE リリースの Cisco ISE 管理者ガイド [英語] を参照してください。

Cisco DNA Center リリース 2.2.2 以降では、エンドポイントの詳細を示すスライドイン ダイアログボックスに [Trust Score] タブがあります。このタブには、エンドポイントの信頼スコアを示すさまざまな要因の詳細が表示されます。エンドポイントの信頼スコアを参照してください。

Cisco DNA Center リリース 2.2.3 以降では、[Details] タブに [Previous MAC Addresses] エリアがあり、MAC ランダム化機能が有効になっているエンドポイントで使用された MAC アドレスが表示されます。ランダムおよび変更 MAC アドレスを持つエンドポイントの信頼スコアを参照してください。

Cisco AI エンドポイント分析データのエクスポート

このウィンドウからエンドポイントとエンドポイントの詳細のリストをエクスポートするには、[Export] をクリックします。[Endpoint Inventory] ウィンドウでフィルタを適用すると、フィルタ処理されたエンドポイントのみがエクスポート用に処理されます。すべてのエンドポイントの詳細をエクスポートするには、フィルタが適用されていないことを確認して、[Export] をクリックします。

[Export] をクリックすると、[Reports] ウィンドウで新しいタブが開きます。[Generated Reports] ウィンドウには、開始されたエクスポートのリストが表示され、リストの一番上に最新のエクスポート要求が表示されます。[Endpoint Inventory] ウィンドウから生成されたレポートの [Template Category] 列に [AI Endpoint Analytics] が含まれています。レポートの生成には数分かかります。レポートのダウンロード準備ができると、[Last Run] 列の値が [Not Initiated] から、その横にダウンロードアイコンがあるタイムスタンプに変わります。タイムスタンプは、エクスポートリストが生成された時刻を示します。ダウンロードアイコンをクリックして、エンドポイントのリストの CSV ファイルをシステムにダウンロードします。

次の手順で、[Reports] ウィンドウから Cisco AI エンドポイント分析データをエクスポートすることもできます。

（注） エンドポイントの AI エンドポイント分析データの最初のエクスポートは [Endpoint Inventory] ウィンドウから実行する必要があります。その後、[Reports] ウィンドウから直接 AI エンドポイント分析レポートを生成できます。

1. メインメニューから [Reports] を選択します。
2. [Report Templates] をクリックし、メニューから [AI Endpoint Analytics] を選択します。
3. [Generate a New Report] ダイアログボックスで [Let's Do It] をクリックします。
4. [Select Report Template] ウィンドウでは、[Endpoint Profiling] テンプレートがデフォルトで適用されています。[Next] をクリックします。
5. [Setup Report Scope] ウィンドウで、[Report Name] フィールドに値を入力します。[Endpoint Inventory] ウィンドウからエクスポートするエンドポイントのリストに適用するフィルタを定義します。すべてのエンドポイントの詳細をエクスポートするには、[Scope]エリアで値を選択しないでください。[Next] をクリックします。
6. [Select File Type] ウィンドウの [Client Details] エリアで、選択したパラメータを確認できます。関連するフィールドの横にあるチェックボックスをオンまたはオフにして、エクスポートする情報を編集します。[Next] をクリックします。
7. [Schedule Report] ウィンドウで、[Run Now]、[Run Later] （[One-Time] または [Run Recurring]）のオプションボタンをクリックします。[Run Later] の [One-Time] および [Run Recurring] オプションには、エクスポートの時間を定義するスケジューリングフィールドが表示されます。[Next] をクリックします。

8. [Delivery and Notification] ウィンドウでは、[Email Report] チェックボックスをオンにしないでください。[Next] をクリックします。
9. [Summary] ウィンドウで、このワークフローで選択したすべての設定を確認します。設定を編集するには、対応する [Edit] オプションをクリックします。[Next] をクリックします。
10. ワークフローの最後のウィンドウで、レポートが生成されていることが通知されます。生成されたレポートのリストを表示するには、このウィンドウの [View Reports] リンクをクリックします。レポートが生成され、このウィンドウに表示されるまでに数分かかります。

エンドポイントのフィルタ処理

フィルタオプションを使用すると、一連のエンドポイントを表示してアクションを実行できます。これらのエンドポイントは、プロファイリングデータ、プライマリ プロファイリング ラベル、既知のプロファイル、および正常性ステータスに基づいてフィルタ処理できます。

エンドポイントをフィルタ処理するには、次の手順を実行します。

1. [Endpoint Inventory] ウィンドウで、[Filter] をクリックします。
2. 次の各ドロップダウンリストから、値を選択します。
   - **Mac Address**
   - **エンドポイント タイプ**
   - **ハードウェア モデル**
   - **ハードウェア製造元**
   - **OS Type**
   - **登録ステータス（Registration status）**
3. [Apply] をクリックします。

また、4つのプライマリ プロファイリング ラベルで表示されるプロファイリング済みのエンドポイントをフィルタ処理することもできます。[View Known Profiles] セクションで 1 つ以上のラベルをクリックします。

エンドポイントの正常性ステータスは 5 分ごとに更新されます。次の [In Network] オプションのいずれかをクリックして、正常性ステータスに基づいてエンドポイントをフィルタ処理できます。

- [All]：正常性ステータスに関係なく、ネットワーク内のすべてのエンドポイントが表示されます。
- [Active]：ネットワークでアクティブなエンドポイントのみが表示されます。
- [Inactive]：ネットワークでアクティブでなくなったエンドポイントのみが表示されます。

属性用語集

属性用語集は、Cisco ISE プローブデータから使用可能なすべてのプロファイリング属性のリストです。

すべてのプロファイリング属性を表示するには、次の手順を実行します。

1. [Endpoint Inventory] ウィンドウで、エンドポイントの MAC アドレスをクリックします。
2. 右側に表示される新しい領域で、[View Attribute Glossary] をクリックします。

[Attribute Glossary] ウィンドウに、属性ごとに次の情報が表示されます。

- **キープロファイリング属性**
- **説明**
- **関連付けられたプロファイルラベル**
- **[Source]**
- **Dictionary**
- **ディスカバリの方法**

用語集では、すべてのプロファイリング属性の詳細ビューが表示されます。プロファイリング属性がプロファイルラベルの作成に頻繁に使用される場合は、そのラベルが [Associated Profile Labels] 列に一覧表示されます。

また、ルールの論理条件の作成中に、[Choose Attribute Condition] ウィンドウに属性用語集を表示することもできます。詳細については、「カスタムルールの作成」を参照してください。

エンドポイントの登録

新しいエンドポイントをオンボードおよびプロファイリングするには、そのエンドポイントを Cisco AI エンドポイント分析に登録します。エンドポイントのプロファイリング情報は、分類のための信頼できる情報源です。また、[Register Endpoint] オプションを使用して、登録済みのエンドポイントの新しいプロファイル情報を更新することもできます。

ステップ 1 **[Actions]** > **[Register Endpoints]** の順に選択します。

ステップ 2 [Single] または [Bulk] のいずれかのオプションボタンをクリックして、単一のエンドポイントまたは複数のエンドポイントを登録するかどうかを選択します。

オプション	手順
シングル	[MAC Address]、[Endpoint Type]、[Hardware Model]、および [Hardware Manufacturer] にエンドポイントの値を入力します。
バルク（**Bulk**）	1. [Download .csv Template] オプションをクリックして、.csvテンプレートをダウンロードします。

オプション	手順
	2. ダウンロードした .csv ファイルに、登録する必要がある各エンドポイントの詳細を入力します。具体的には、MACアドレス、エンドポイントタイプ、ハードウェアモデル、およびハードウェア製造元です。このファイルを保存します。 **3.** [Choose a File] オプションを使用して .csv ファイルをアップロードします。 [Bulk] オプションを使用すると、一度に最大 500 個のエンドポイントを登録できます。

ステップ 3 [Next] をクリックします。

ステップ 4 [Review Endpoint] ウィンドウでエンドポイントの詳細を確認します。変更が必要な場合は、エンドポイントの詳細を編集することもできます。

（注） 既存のエンドポイントの登録中は、エンドポイントのプロファイルラベルの変更が紫色で反映され、編集できます。

ステップ 5 [Next] をクリックして、登録プロセスを続行します。

ステップ 6 [登録（Register）] をクリックします。

登録済みのエンドポイントの編集

登録済みのエンドポイントのプロファイリング情報は、[Endpoint Inventory] ウィンドウから更新できます。

ステップ 1 編集するエンドポイントの MAC アドレスの横にあるチェックボックスをオンにします。

ステップ 2 [Actions] をクリックします。

ステップ 3 [Edit Endpoint] をクリックします。

ステップ 4 [Endpoint Type]、[Hardware Model]、[Hardware Manufacturer] に詳細を入力します。

ステップ 5 [Save] をクリックします。

登録済みのエンドポイントの削除

登録済みのエンドポイントがネットワークの一部ではなくなった場合は、Cisco AI エンドポイント分析から削除できます。

ステップ 1 削除するエンドポイントの MAC アドレスの横にあるチェックボックスをオンにします。

ステップ 2 [Actions] をクリックします。

ステップ 3 [Delete Endpoint] をクリックします。

次のメッセージが表示されます。

「Do you really want to delete the selected endpoint(s)?」

ステップ 4 [Yes] をクリックして、Cisco AI エンドポイント分析からエンドポイントを完全に削除します。

プロファイリングルール

Cisco AI エンドポイント分析のプロファイリングルールを使用すると、共通の属性を組み合わせてエンドポイントをグループ化できます。これらの属性により、エンドポイントタイプ、OS タイプ、ハードウェアモデル、およびハードウェア製造元でエンドポイントを識別できます。プロファイリングルールを使用すると、多くのエンドポイントを簡単に管理できます。

Cisco AI エンドポイント分析は、DPI、メディアプロトコル、医療業界のプロトコルなどを介してネットワークデバイスからプロファイリングデータを受信します。Cisco ISE からのプロファイリングデータは、pxGrid を介して通信されます。これらのプロファイリング属性をデバイスディクショナリで使用してプロファイルルールを作成できます。

プロファイリングルールは、Cisco AI エンドポイント分析の [Profiling Rules] タブで確認できます。このタブの下に表示されるテーブルで、[Rule Name] エントリをクリックすると、割り当てられたプロファイルと使用される属性が表示されます。

Cisco AI エンドポイント分析でエンドポイントをプロファイリングするために使用されるプロファイリングルールは次のとおりです。

- システムルール
- シスコの規則
- Cisco AI ルール

ルールの優先順位付け

Cisco AI エンドポイント分析のプロファイリングルールには優先順位があります。プロファイリングルールの実行は、このルールの優先順位に従って、精度の高いエンドポイントをプロファイリングします。

Cisco AI エンドポイント分析ではユーザー入力がプライマリであるため、プロファイリングルールの優先順位は次のようになります。

- 管理者が作成した静的プロファイル（たとえば、[Register Endpoints] オプションを使用して追加したプロファイル）。
- 管理者が作成したカスタムルール。
- デフォルトで使用可能なシスコ提供のシステムルール。

- 機械学習対応のスマートグループ化ワークフローによって自動生成されたルール。

ルールに設定された優先順位を表示するには、[Profiling Rules] ウィンドウで [Rule priorityitization] をクリックします。

登録済みのエンドポイントは、さまざまなプロファイリングラベルの複数の Cisco AI エンドポイント分析ルールによってプロファイリングできます。次の表に、2 つのエンドポイントに対するプロファイリングルールの設計を示します。

エンドポイント 1	エンドポイント 2
システムルールによってプロファイリングされたハードウェアモデル	システムルールによってプロファイリングされたハードウェアモデル
Cisco AI ルールによってプロファイリングされた OS タイプ	カスタムルールによってプロファイリングされたハードウェアモデル
カスタムルールによってプロファイリングされたハードウェア製造元	Cisco AI ルールによってプロファイリングされたハードウェアモデル

エンドポイント 2 のルール優先順位では、カスタムルールが他のルールよりも優先されます。エンドポイント 2 のハードウェアモデルラベルは、カスタムルールによってプロファイリングされます。

エンドポイント 1 の場合、ルールごとに異なるプロファイルラベルが定義され、それに応じて各ラベルがプロファイリングされます。

プロファイリングルールのフィルタ処理

ステップ 1 [Profiling Rules] ウィンドウで、[Filter] をクリックします。

ステップ 2 [Rule Name] フィールドに、名前を入力します。

ステップ 3 対応するドロップダウンリストからエンドポイント属性の値を選択して、一連のエンドポイントをフィルタ処理します。

ステップ 4 [Apply] をクリックします。

更新されたプロファイリングルールの表示

ステップ 1 [Endpoint Inventory] ウィンドウに移動します。

ステップ 2 エンドポイントの MAC アドレスの横にあるチェックボックスをクリックして、エンドポイントのプロファイリングの詳細を表示します。

ステップ 3 プロファイルラベルの横にある情報アイコンをクリックし、ルール名をクリックして、割り当てられたプロファイルと属性の詳細を表示します。

システムルール

Cisco AI エンドポイント分析には、エンドポイントをプロファイリングするためのシステムルールと呼ばれる事前定義済みのルールが用意されています。Cisco AI エンドポイント分析を導入すると、特定のルールを設定することなく、エンドポイントのゼロデイ可視性を実現できます。

新しくオンボーディングされたエンドポイントは、デフォルトでシステムルールを使用してプロファイリングされます。

ネットワークデバイスは、Cisco DNA Center の **[Provision]** > **[Network Devices]** > **[Inventory]** ウィンドウで管理されます。

これらのネットワークデバイスは、システムルールによってプロファイリングされ、Cisco AI エンドポイント分析の [Endpoint Inventory] ウィンドウには表示されません。ただし、カスタムルールでプロファイリングされたエンドポイントは、カスタムルールがネットワークデバイスを [Device Type] として作成されるため表示できます。

シスコの規則

システムルールのほかに、エンドポイント属性を組み合わせて、エンドポイントをプロファイリングするためのカスタムルールを作成することもできます。カスタムルールは、Cisco AI エンドポイント分析の他のエンドポイント プロファイリング ルールよりも優先されます。

プロファイリングルールの論理と条件

[Endpoint Inventory] ウィンドウでカスタム プロファイリング ルールを作成できます。カスタム プロファイリング ルールを作成するには、エンドポイントの属性と値に基づいて論理条件を作成する必要があります。これらの属性は、ネットワークプローブデータから収集され、[Attribute Glossary] ウィンドウで使用できる分類属性とは異なります。

値は、エンドポイントグループを一意に識別するユーザー入力です。次の演算子を使用して、属性と値から正規表現が作成されます。

演算子	説明
次の文字列を含む	属性は、選択した値を持ちます。
イコール	属性は、選択した値に厳密にマッピングされます。
一致する	属性は、選択した値の正規表現パターンと一致する必要があります。
Starts With	属性は、選択した値で始まる必要があります。

（注） Contains、Equals、および Starts With は、大文字と小文字を区別する演算子です。大文字と小文字を区別しない値の場合は、Matches 演算子を使用します。

論理（[AND] および [OR]）によってこれらの条件をさらに組み合わせて、ネストされたルールを作成できます。

論理条件の作成と編集

論理条件を作成するには、次の手順に従います。

ステップ 1 [Choose Attribute Conditions] ウィンドウで、更新する [Attribute] の横にあるチェックボックスをオンにします。

ステップ 2 [Operator] ドロップダウンリストからオプションを選択します。

ステップ 3 [Value] フィールドに値を入力します。

ステップ 4 [Next] をクリックします。

ステップ 5 表示される [Add Logic to Conditions] ウィンドウで、条件間の [AND] ロジックまたは [OR] ロジックをドラッグアンドドロップして、カスタムルールの条件の論理シーケンスを作成します。

（注） 条件の横にある垂直省略記号を使用して、[Add Logical Conditions] ウィンドウで属性条件を追加または編集することもできます。

ステップ 6 [Next] をクリックします。

カスタムルールの作成

ステップ 1 [Endpoint Inventory] ウィンドウで、プロファイリングするエンドポイントの MAC アドレスの横にあるチェックボックスをオンにします。

ステップ 2 [Actions] をクリックし、[Profile with Custom Rules] を選択します。

ステップ 3 表示される [Name Rule and Type] ウィンドウの [Rule Name] フィールドにルールの名前を入力し、[Profile Label] ドロップダウンリストからラベルを選択します。

[Profile Label] ドロップダウンリストから選択した内容に応じて、対応するフィールドが表示され、その名前は動的に更新されます。たとえば、[Endpoint Type] を選択すると、[Endpoint Type] フィールドが表示されます。

ステップ 4 表示される新しいフィールドに値を入力します。情報の入力を開始すると、一致するオプションが表示されます。要件に一致するオプションがあれば、そのオプションを選択します。なければ、タイプ名全体を入力します。

ステップ 5 [Next] をクリックします。

ステップ 6 表示される [Choose Attribute Conditions] ウィンドウで、論理条件を作成します。

詳細については、「プロファイリングルールの論理と条件」を参照してください。

ステップ 7 [Review Rule] ウィンドウで、このカスタムルールでプロファイリングされるエンドポイントのリストを確認します。

ステップ 8 [Next] をクリックします。

ステップ 9 [Profiles] をクリックします。

カスタムルールの編集

ステップ 1 [Profiling Rules] ウィンドウで、編集する管理ルールの横にあるチェックボックスをオンにします。

ステップ 2 [Actions] をクリックし、[Edit] を選択します。

ステップ 3 表示される [Edit] ウィンドウの [Rule Name] フィールドにルールの名前を入力し、ルールの作成時に選択した [Profile Label] に基づいてプロファイルの詳細を選択または入力します。

ステップ 4 [Logic and Conditions] セクションで、垂直省略記号をクリックし、[Edit] を選択して、プロファイリングルールの論理と条件を更新します。詳細については、「プロファイリングルールの論理と条件」を参照してください。

ステップ 5 **[次へ (Next)]** をクリックします。

ステップ 6 **[適用 (Apply)]** をクリックします。
既存のルールが新しいプロファイリングの詳細で更新されると、そのルールでプロファイリングされたエンドポイントが新しいプロファイリングの詳細で更新されます。

カスタムルールの削除

ステップ 1 [Profiling Rules] ウィンドウで、削除するルールの横にあるチェックボックスをオンにします。

ステップ 2 [Actions] をクリックし、[Delete] を選択します。

次のメッセージが表示されます。

「Do you really want to delete the selected Rule(s)?」

ステップ 3 [Yes] をクリックして、Cisco AI エンドポイント分析からルールを完全に削除します。

カスタムルールが削除されると、このルールでプロファイリングされたエンドポイントがシステムルールで更新されます。

Cisco AI ルールまたはスマートグループ化

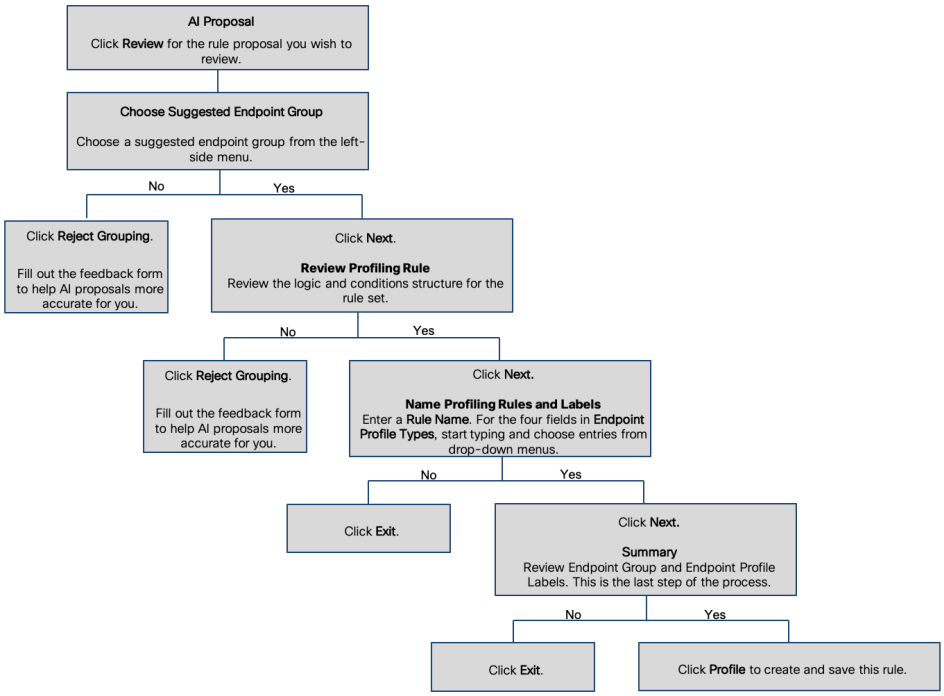
Cisco AI エンドポイント分析は、ML クラウドを使用して、ネットワーク上の不明なエンドポイントを動的にグループ化します。また、不明なエンドポイントのグループにカスタムラベル

を割り当てることもできます。クラスタを確認し、示されたプロファイリング提案を承認または拒否できます。

プロファイリング提案を承認すると、選択したエンドポイントをプロファイリングして、今後ネットワークに参加する同様のエンドポイントをプロファイリングするためのプロファイリングルールが自動的に作成されます。

プロファイリングルール提案の変更

[Endpoint Analytics] ホームページの [AI Proposal] ダッシュレットには、スマートグループ化によって生成されたエンドポイントクラスタに基づいてルール提案が表示されます。AI 提案を表示するには、対応する提案タイプの横にある [Review] をクリックし、次の決定表に従って進みます。



プロファイリングルールのインポート

カスタムプロファイリングルールと Cisco AI ルールを移行するには、.json ファイルをインポートします。

ステップ 1 [Profiling Rule] ウィンドウで、[Actions] をクリックします。

ステップ 2 [Import Profiling Rules] を選択します。

ステップ 3 [Choose a file] をクリックし、システムの .json ファイルを参照します。

ステップ 4 [OK] をクリックします。

プロファイリングルールのエクスポート

Cisco AI エンドポイント分析からカスタムルールおよび Cisco AI プロファイリングルールをエクスポートしてバックアップできます。[Export Profiling Rules] オプションは、使用可能なすべてのカスタムルールと Cisco AI プロファイリングルールをエクスポートします。ルールを選択してエクスポートすることはできません。

ステップ 1 [Profiling Rules] ウィンドウで、[Actions] をクリックします。

ステップ 2 [Export Profiling Rules] を選択します。

ステップ 3 [Yes] をクリックして、すべてのカスタムルールと ML プロファイリングルールをエクスポートします。終了するには、[No] をクリックします。

（注） 同じファイルを Cisco AI エンドポイント分析に再度インポートできます。

階層

Cisco AI エンドポイント分析階層は、エンドポイントタイプに基づいてエンドポイントの論理グループを作成するのに役立ちます。エンドポイントのカテゴリとサブカテゴリを作成すると、エンドポイントの可視性に焦点が当てられ、許可プロセスが簡素化されます。

デフォルトの [All Endpoints] 親カテゴリからカテゴリを作成できます。エンドポイントの総数、エンドポイントタイプ、サブカテゴリなどのカテゴリの詳細が [Hierarchy] ウィンドウの個々のボックス内に表示されます。

カテゴリを作成、編集、および削除して、階層を並べ替えることができます。

カテゴリとサブカテゴリの作成

ステップ 1 [Hierarchy] ウィンドウで、親カテゴリの水平省略記号をクリックします。

ステップ 2 [Create Category] をクリックします。

ステップ 3 カテゴリ名を入力します。

ステップ 4 Enter キーを押します。

次のタスク

カテゴリを作成したら、[Endpoint Type] ウィンドウからエンドポイントタイプをドラッグアンドドロップするか、カテゴリを編集してエンドポイントを追加できます。

カテゴリまたはサブカテゴリの編集

ステップ 1 [Hierarchy] ウィンドウで、カテゴリの水平省略記号をクリックします。
ステップ 2 [Edit] をクリックします。
ステップ 3 表示される [Edit] ウィンドウで、[Category Name] に値を入力します。
ステップ 4 カテゴリを再割り当てする場合は、ドロップダウンメニューから [Parent Category] を入力します。
ステップ 5 [Endpoint Type] タブをクリックします。
ステップ 6 [Actions] をクリックし、[Add Endpoint Type] を選択します。
ステップ 7 [Search Dropdown] リストからエンドポイントタイプを選択します。
ステップ 8 **[保存（Save）]** をクリックします。

次のタスク

[Endpoint Type] ウィンドウで、[All]、[Available]、および [Assigned] でエンドポイントタイプをフィルタ処理できます。

カテゴリからのエンドポイントタイプの削除

ステップ 1 [Hierarchy] ウィンドウで、削除するカテゴリの水平省略記号をクリックします。
ステップ 2 [Edit] をクリックします。
ステップ 3 [Edit] ウィンドウで、[Endpoint Type] タブをクリックします。
ステップ 4 削除するエンドポイントタイプの横にあるチェックボックスをオンにします。
ステップ 5 [Actions] をクリックし、[Remove From Category] を選択します。

次のメッセージが表示されます。

「Are you sure you want to delete this category?」

ステップ 6 カテゴリからエンドポイントを削除するには、[Yes] をクリックします。終了するには、[No] をクリックします。

カテゴリからのエンドポイントタイプの再割り当て

ステップ 1 [Hierarchy] ウィンドウで、カテゴリの水平省略記号をクリックします。

ステップ 2 [Edit] をクリックします。

ステップ 3 [Edit] ウィンドウで、[Endpoint Type] タブをクリックします。

ステップ 4 再割り当てするエンドポイントタイプの横にあるチェックボックスをオンにします。

ステップ 5 [Actions] をクリックし、[Re-assign to existing category] または [Re-assign to a new category] を選択します。

オプション	手順
既存のカテゴリへの再割り当て	1. [Reassign] ウィンドウで、[Category] ドロップダウンリストから既存のカテゴリを選択します。 2. **[保存（Save）]** をクリックします。
新しいカテゴリへの再割り当て	1. [Reassign] ウィンドウで、[Category] ドロップダウンリストから [New Category] を選択します。 2. [Parent Category] ドロップダウンリストから親カテゴリを選択します。 3. [New Category] フィールドにカテゴリ名を入力します。 4. [Save（保存）] をクリックします。

カテゴリの削除

始める前に

親カテゴリを削除する前に、そのサブカテゴリを確認します。サブカテゴリを別の既存のカテゴリまたは新しいカテゴリに再割り当てできます。そうしないと、すべてのサブカテゴリが親カテゴリとともに削除されます。カテゴリの削除中にサブカテゴリを再割り当てすることもできます。

ステップ 1 [Hierarchy] ウィンドウで、カテゴリの水平省略記号をクリックします。

ステップ 2 [削除（Delete）] をクリックします。

サブカテゴリが割り当てられているカテゴリを削除する場合には、[Reassign Relationships] ダイアログボックスが表示されます。次のオプションのいずれかを選択します。

オプション	条件	手順
既存のカテゴリへの再割り当て	既存のカテゴリにサブカテゴリを再割り当てします。	**1.** [Category] ドロップダウンリストからカテゴリを選択します。 **2.** [Reassign] をクリックします。 親カテゴリが削除され、選択したカテゴリにサブカテゴリが再割り当てされます。
新しいカテゴリへの再割り当て	既存のカテゴリにサブカテゴリを再割り当てします。	**1.** [Parent Category] ドロップダウンリストからカテゴリを選択します。 **2.** [New Category] フィールドにカテゴリ名を入力します。 **3.** [Reassign] をクリックします。 親カテゴリが削除され、新しいカテゴリにサブカテゴリが再割り当てされます。
カテゴリからの削除	親カテゴリとともにサブカテゴリを削除します。	[Reassign] をクリックします。 親カテゴリとそのサブカテゴリが削除されます。

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。