ネットワーク マップの使用

ここでは、ネットワーク マップの使用方法について説明します。

ネットワーク マップ

Firepower システムは、ネットワークを通じて送信されるトラフィックをモニタし、トラフィック データを復号化してから、設定されているオペレーティング システムおよびフィンガープリント とそのデータを比較します。このシステムでは、次にそのデータを使用して、ネットワーク マップというネットワークの詳細な表示を生成します。マルチドメイン展開では、システムはリーフ ドメインごとの個々のネットワーク マップを生成します。

システムは、ネットワーク検出ポリシーのモニタリングで特定された管理対象デバイスからデータを収集します。管理対象デバイスでは、モニタされたトラフィックから直接ネットワーク アセットを検出したり、処理された NetFlow レコードから間接的にネットワーク アセットを検出したりします。複数のデバイスで同じネットワーク アセットを検出した場合、システムではそれらの情報をまとめてそのアセットの複合表示を生成します。

受動的に検出されるデータを補完するには、次のようにします。

- オープンソースの Nmap™ スキャナを使用してホストをアクティブにスキャンして、そのスキャン結果をネットワーク マップに追加します。
- ホスト入力機能を使用して、サードパーティ製のアプリケーションからホストデータを手動で追加できます。

ネットワークマップには、検出されたホストとネットワークデバイスの観点から見たネットワーク トポロジが表示されます。

ネットワーク マップを使用すれば、次のことを行えます。

- ネットワークの全体的なビューを即座に入手できます。

- 実行する分析に適したさまざまなビューを選択できます。ネットワーク マップの各ビューの形式は、展開可能なカテゴリおよびサブカテゴリを持つ階層ツリーからなる、同一の形式です。カテゴリをクリックすると、展開して、その下のサブカテゴリが表示されます。
- カスタム トポロジ機能を使用してサブネットを整理して識別できます。たとえば、組織の各部署が異なるサブネットを使用している場合、カスタム トポロジ機能を使用して、それらのサブネットに分かりやすいラベルを割り当てることができます。
- 任意のモニタ対象ホストのホスト プロファイルにドリルダウンすれば、詳細情報を表示できます。
- アセットの調査が不要になった場合は、そのアセットを削除できます。

（注） システムは、ネットワーク マップから削除されたホストに関連付けられているアクティビティを検出した場合、そのホストをネットワーク マップに再度追加します。同様に、削除されたアプリケーションは、システムでアプリケーションの変更（たとえば、Apache Web サーバが新しいバージョンにアップグレードされた場合）を検出すると、ネットワーク マップに再度追加されます。システムが特定のホストを脆弱にする変更を検出した場合、それらのホストの脆弱性が再びアクティブにされます。

ヒント ネットワーク マップからホストまたはサブネットを永続的に除外するには、ネットワーク検出ポリシーを変更します。ロード バランサおよび NAT デバイスで過剰なイベントまたは無関係なイベントを生成していることが判明した場合は、それらのデバイスをモニタリングから除外することができます。

関連トピック

ネットワーク検出ポリシーの設定

ホストのネットワーク マップ

[ホスト（Hosts）] タブのネットワーク マップには、ホスト数と、ホストの IP アドレスと MAC アドレスのリストが表示されます。各アドレスまたはアドレスの一部は、次のレベルへのリンクです。このネットワーク マップ ビューは、ホストに 1 つの IP アドレスまたは複数の IP アドレスがあるかを問わず、システムによって検出されたすべての一意のホスト数を表示します。

ホストのネットワーク マップを使用して、サブネットによって階層ツリーに整理されたネットワークのホストを参照でき、特定のホストのホスト プロファイルにドリルダウンできます。

システムは、ホストをエクスポートされた NetFlow レコードからネットワーク マップに追加できますが、これらのホストに使用できる情報は限られます（NetFlowデータと管理対象デバイスデータの違い を参照）。

ネットワークのカスタム トポロジを作成して、サブネットに意味のあるラベル（部門名など）を割り当てることができます。これはホストのネットワーク マップで表示されます。また、カスタム トポロジで指定した組織に基づいてホストのネットワーク マップを表示することもできます。

ホストのネットワーク マップからネットワーク全体、サブネット、または個々のホストを削除できます。ホストがネットワークに接続されていないことがわかっている場合など、分析を効率化するために削除できます。システムは削除されたホストに関連付けられたアクティビティを後で検出すると、ネットワーク マップにホストを再追加します。ネットワーク マップからホストまたはサブネットを永続的に除外するには、ネットワーク検出ポリシーを変更します。

注意 ネットワーク デバイスをネットワーク マップから削除しないでください。システムがネットワーク トポロジを判断するために必要です。

ネットワーク デバイスのネットワーク マップ

[ネットワーク デバイス（Network Devices）] タブのネットワーク マップには、ネットワークの 1 つのセグメントを別のセグメントに接続するネットワーク デバイス（ブリッジ、ルータ、NAT デバイス、およびロード バランサ）が表示されます。このマップには、IP アドレスで特定されたデバイスと、MAC アドレスで特定されたデバイスがリストされる 2 つのセクションがあります。

また、このマップには、デバイスに保持されている IP アドレスが 1 つか複数かに関係なく、システムによって検出されたすべての一意のネットワーク デバイスの数も表示されます。

ネットワークのカスタム トポロジを作成した場合、サブネットに割り当てられているラベルがネットワーク デバイスのネットワーク マップに表示されます。

ネットワーク デバイスを識別するためにシステムで使用される方法には、次のものがあります。

- Cisco Discovery Protocol（CDP）メッセージの分析。ネットワーク デバイスとそれらのタイプを識別できます（シスコ デバイスのみ）。
- スパニング ツリー プロトコル（STP）の検出。デバイスをスイッチまたはブリッジとして識別します。
- 同じ MAC アドレスを使用している複数のホストの検出。MAC アドレスを、ルータに属しているものとして識別します。
- クライアント側からの TTL 値の変更、または通常のブート時間よりも頻繁に変更されている TTL 値の検出。この検出では、NAT デバイスとロード バランサを識別します。

ネットワーク デバイスが CDP を使用して通信している場合、1 つ以上の IP アドレスを保持している可能性があります。ネットワーク デバイスが STP を使用して通信している場合は、1 つの MAC アドレスのみを保持している可能性があります。

ネットワーク デバイスをネットワーク マップから削除することはできません。これは、システムでそれらの場所を使用してネットワーク トポロジを判断するためです。

ネットワーク デバイスのホスト プロファイルには、[オペレーティング システム（Operating Systems）] セクションではなく [システム（Systems）] セクションがあります。このセクションに

は、ネットワーク デバイスの背後で検出されたモバイル デバイスすべてのハードウェア プラットフォームが反映された[ハードウェア（Hardware）]列が含まれています。[システム（Systems）]の下にハードウェアプラットフォームの値が表示され場合、システムは、ネットワークデバイスの背後で 1 つ以上のモバイル デバイスが検出されたことを示しています。モバイル デバイスはハードウェア プラットフォームの情報を持っていることも、持っていないこともありますが、モバイルデバイスではないシステムではハードウェアプラットフォーム情報は検出されないことに注意してください。

モバイル デバイスのネットワーク マップ

[モバイル デバイス（Mobile Devices）] タブのネットワーク マップには、ネットワークに接続されているモバイルデバイスが表示されます。また、このネットワークマップには、デバイスに設定されている IP アドレスが 1 つか複数かに関係なく、システムによって検出されたすべての一意のモバイル デバイスの数も表示されます。

各アドレスまたはアドレスの一部分は、次のレベルへのリンクです。また、サブネットまたは IP アドレスを削除することもできます。そして、システムでそのデバイスを再検出すると、そのデバイスをネットワーク マップに再度追加します。

さらに、ドリルダウンしてモバイルデバイスのホストプロファイルを表示することもできます。

モバイル デバイスを特定するために、システムでは次のことを行います。

- モバイル デバイスのモバイル ブラウザからの HTTP トラフィック内のユーザ エージェントの文字列を分析します。
- 特定のモバイル アプリケーションの HTTP トラフィックをモニタします。

ネットワークのカスタム トポロジを作成した場合、サブネットに割り当てられているラベルがモバイル デバイスのネットワーク マップに表示されます。

侵害の兆候のネットワーク マップ

[侵害の兆候（Indications of Compromise）] タブのネットワーク マップには、ネットワーク上で侵害されたホストが IOS カテゴリ別に編成されて表示されます。影響を受けているホストは各カテゴリの下に表示されます。各アドレスまたはアドレスの一部は、次のレベルへのリンクです。

システムは、ホストのセキュリティ侵害のステータスを判断するために、侵入イベント、セキュリティ インテリジェンス、Cisco Advanced Malware Protection（AMP）を含む複数のソースからのデータを使用します。

[侵害の兆候（Indications of Compromise）] タブのネットワーク マップから、何らかのセキュリティ侵害を受けたと判断される各ホストのホスト プロファイルを表示できます。さらに、IOC カテゴリまたは特定のホストを削除でき（解決済みにする）、これによって当該ホストから IOC タグが削除されます。たとえば、問題が対応済みで、繰り返し発生する可能性が低いと判断した場合に、IOC カテゴリをネットワーク マップから削除できます。

ネットワーク マップのホストやIOCカテゴリを解決済みにしても、ネットワークからは削除されません。システムがその IOC をトリガーする情報を新たに検出すると、解決済みのホストまたは IOC カテゴリはネットワーク マップに再表示されます。

アプリケーション プロトコルのネットワーク マップ

[アプリケーション プロトコル（Application Protocols）] タブのネットワーク マップには、ネットワークで稼働しているアプリケーションが、アプリケーション名、ベンダー、バージョン、各アプリケーションを実行しているホストを基準とした階層ツリー形式で表示されます。

システムが検出するアプリケーションは、システム ソフトウェアや VDB が更新された場合や、アドオンディテクタをインポートした場合に変わることがあります。各システムまたはVDBアップデートのリリース ノートまたはアドバイザリテキストには、新規および更新されたディテクタの情報が含まれています。ディテクタを網羅した最新のリストについては、Cisco のサポート サイト（http://www.cisco.com/cisco/web/support/index.html）を参照してください。

このネットワーク マップから、特定のアプリケーションを実行している各ホストのホスト プロファイルを確認できます。

また、アプリケーションのカテゴリ、すべてのホストで実行されているアプリケーション、あるいは特定のホストで実行されているアプリケーションを削除することもできます。たとえば、あるアプリケーションがホスト上で無効化されているとわかっており、システムによる影響レベルの認定で使用されないようにする場合は、そのアプリケーションをネットワーク マップから削除します。

ネットワーク マップからアプリケーションを削除しても、ネットワークからは削除されません。削除したアプリケーションは、システムがアプリケーションの変更（たとえばApache Web サーバが新しいバージョンにアップグレードされた）を検出するか、ユーザがシステムの検出機能を再起動すると、ネットワーク マップに再表示されます。

何を削除するかによって、動作は次のように異なります。

- アプリケーション カテゴリ：アプリケーション カテゴリを削除すると、そのアプリケーション カテゴリがネットワーク マップから除去されます。削除したカテゴリの下にあるすべてのアプリケーションは、そのアプリケーションを含むすべてのホストプロファイルから削除されます。

  たとえば、[http] を削除した場合、[http] として示されるすべてのアプリケーションがすべてのホストプロファイルから削除され、[http]はネットワーク マップのアプリケーション ビューに表示されなくなります。

- 特定のアプリケーション、ベンダー、バージョン：これらの要素を削除すると、関連するアプリケーションがネットワーク マップから除去され、そのアプリケーションを含むホスト プロファイルからもアプリケーションが除去されます。

  たとえば、[http] カテゴリを展開し、[Apache] を削除すると、[Apache] としてリストされているすべてのアプリケーションは、[Apache] の下にリストされているバージョンを問わず、それらを含むホストプロファイルから削除されます。同様に、[Apache] を削除する代わりに、特定のバージョン（[1.3.17] など）を削除すると、影響を受けるホスト プロファイルから、選択されたバージョンだけが削除されます。

- 特定の IP アドレス：IP アドレスを削除すると、その IP アドレスがアプリケーション リストから除去され、選択した IP アドレスのホスト プロファイルからアプリケーション自体が除去されます。

  たとえば、[http]、[Apache]、[1.3.17 (Win32)] の順に展開し、[172.16.1.50:80/tcp] を削除すると、Apache 1.3.17（Win32）アプリケーションは IP アドレス 172.16.1.50 のホスト プロファイルから削除されます。

[脆弱性（Vulnerabilities）] のネットワーク マップ

[脆弱性（Vulnerabilities）] タブのネットワーク マップには、システムによってネットワークで検出された脆弱性がレガシーの脆弱性 ID（SVID）、Bugtraq ID、CVE ID、または Snort ID ごとに編成されて表示されます。脆弱性は、デフォルトでは SVID ごとに表示されます。脆弱性は ID 番号順に並べられ、影響を受けるホストが各脆弱性の下にリストされます。

このネットワーク マップから、特定の脆弱性の詳細、および特定の脆弱性の影響を受けるホストのホスト プロファイルを表示できます。この情報は、影響を受ける特定のホストに対するその脆弱性によって生じる脅威を評価するために役立ちます。

特定の脆弱性がネットワーク上のホストに該当しないと判断した場合（たとえば、パッチの適用が完了した場合）、その脆弱性を非アクティブ化できます。非アクティブ化された脆弱性はネットワーク マップに表示され続けますが、これまで影響を受けていたそれらのホストのIPアドレスはグレーのイタリック体で表示されます。それらのホストのホスト プロファイルには、非アクティブ化された脆弱性は無効と表示されますが、個々のホストについて手動で有効とマークすることができます。

ホスト上のアプリケーションまたはオペレーティング システムにアイデンティティの競合がある場合、システムは可能性のあるアイデンティティの両方について脆弱性をリスト表示します。アイデンティティの競合が解決された場合、その脆弱性は現在のアイデンティティに関連付けられたままになります。

ネットワーク マップには、デフォルトではパケットにアプリケーションのベンダーとバージョンが含まれている場合にのみ、検出されたアプリケーションの脆弱性が表示されます。ただし、Firepower Management Center の構成でアプリケーションの脆弱性マッピングの設定を有効化することで、ベンダーとバージョンのデータがないアプリケーションの脆弱性をリストするようにシステムを設定できます。

脆弱性 ID（または脆弱性 ID の範囲）の隣の数字は、次の 2 つのカウントを表しています。

影響を受けるホスト数

最初の数字は、1 つまたは複数の脆弱性の影響を受ける 1 台とは限らないホストのカウントです。1 台のホストが複数の脆弱性の影響を受ける場合、このカウントは複数回数えられます。このため、このカウントがネットワーク上のホスト数を上回ることがありえます。脆弱性を非アクティブ化すると、このカウントはその脆弱性の影響を受ける可能性のあるホスト数の分減少します。1 つまたは複数の脆弱性の影響を受ける可能性のあるホストについて、脆弱性を 1 つも非アクティブ化していない場合、このカウントは表示されません。

影響を受ける可能性のあるホスト数

2 番目の数字は、1 つまたは複数の脆弱性の影響を受ける可能性があるとシステムが判断した 1 台とは限らないホストの総数のカウントです。

脆弱性を非アクティブ化すると、指定したホストについてのみ脆弱性が非アクティブになります。脆弱と判断されたすべてのホストか、指定した個々の脆弱なホストの脆弱性を非アクティブ化することができます。脆弱性が非アクティブ化されると、該当するホストの IP アドレスはネットワーク マップにグレーのイタリック体で表示されます。また、それらのホストのホストプロファイルでは、非アクティブ化された脆弱性が無効と表示されます。

その後でシステムが脆弱性が非アクティブ化されていないホストに（たとえば、ネットワーク マップ内の新しいホストに）その脆弱性を検出すると、システムはそのホストの脆弱性をアクティブ化します。新たに検出された脆弱性は明示的に非アクティブ化する必要があります。また、システムでは、ホストのオペレーティング システムまたはアプリケーションの変更を検出すると、関連付けられている非アクティブ化された脆弱性を再度アクティブ化することがあります。

ホスト属性のネットワーク マップ

[ホスト属性（Host Attributes）] タブのネットワーク マップには、ネットワーク上のホストがユーザ定義ホスト属性またはコンプライアンス ホワイトリスト ホスト属性のいずれかを基準に編成されて表示されます。この表示では、定義済みホスト属性を使用してホストを編成することはできません。

ホストを編成するために使用するホスト属性を選択すると、Firepower Management Center はネットワーク マップで使用可能なその属性の値をリストし、割り当てられた値に基づいてホストをグループ化します。たとえば、ホワイトリスト ホスト属性でホストを編成することにすると、システムは [準拠（Compliant）]、[非準拠（Non-Compliant）]、[評価されていない（Not Evaluated）] カテゴリでホストを表示します。

また、特定のホスト属性値が割り当てられた任意のホストのホスト プロファイルを表示することもできます。

関連トピック

ホスト プロファイル内のホスト属性

ネットワーク マップの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Any Security Analyst

手順

ステップ 1 [分析（Analysis）] > [ホスト（Hosts）] > [ネットワーク マップ（Network Map）]を選択します。

ステップ 2 表示するネットワーク マップのタブをクリックします。

ステップ 3 必要に応じて、以下の操作を続行します。

- ドメインの選択：マルチドメイン展開では、[ドメイン（Domain）] ドロップダウン リストからリーフ ドメインを選択します。
- ホストのフィルタリング：IP または MAC アドレスでフィルタリングするには、検索フィールドにアドレスを入力します。検索をクリアするには、クリアアイコン（  ）をクリックします。
- ドリル ダウン：カテゴリまたはホスト プロファイルを調べる場合、マップのカテゴリまたはサブネットからドリルダウンします。カスタム トポロジを定義した場合、[ホスト（host）] タブから [(トポロジ)（(topology)）] をクリックしてそのトポロジを表示し、デフォルトのビューに戻したい場合は、[(ホスト)（(hosts)）] をクリックします。
- 削除：該当する要素の横にある削除アイコン（  ）をクリックし、以下のことを行います。
  - [ホスト（Hosts）]、[ネットワーク デバイス（Network Devices）]、[モバイル デバイス（Mobile Devices）]、[アプリケーション プロトコル（Application Protocols）] タブのマップから要素を削除する。
  - [侵害の兆候（Indications of Compromise）] タブで IOC カテゴリ、侵害されたホスト、侵害されたホストのグループを解決済みとしてマークを付ける。
  - [脆弱性（Vulnerabilities）] タブですべてのホストまたは単一ホストの脆弱性を非アクティブ化する。
- 脆弱性クラスの指定：[脆弱性（Vulnerabilities）] タブで、[タイプ（Type）] ドロップダウン リストから、表示する脆弱性のクラスを選択します。
- 組織属性の指定：[ホスト属性（Host Attributes）] タブで、[属性（Attribute）] ドロップダウン リストから属性を選択します。

関連トピック

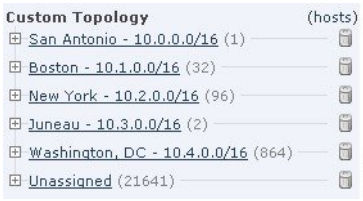
カスタム ネットワーク トポロジ, （9 ページ）
ホスト プロファイル

カスタム ネットワーク トポロジ

ホストおよびネットワークデバイスのネットワークマップでサブネットを整理および識別するために、カスタム トポロジ機能を使用します。

たとえば、部門内の各部署が異なるサブネットを使用している場合、カスタム トポロジ機能を使用して、これらのサブネットにラベルを付けられます。

また、カスタム トポロジで指定した部門に基づいてホストのネットワークマップを表示することもできます。



次のいずれかまたはすべての方法でカスタム トポロジのネットワークを指定できます。

- ネットワーク検出ポリシーからネットワークをインポートして、システムでモニタするように設定したネットワークをトポロジに追加します。
- 手動でネットワークをトポロジに追加します。

[カスタム トポロジ（Custom Topology）]ページにカスタム トポロジと各トポロジのステータスが一覧表示されます。ポリシー名の隣の電球アイコンが点灯している場合、そのトポロジはアクティブで、ネットワーク マップに影響します。消灯している場合、トポロジは非アクティブです。

関連トピック

ホストのネットワーク マップ，（2 ページ）
ネットワーク デバイスのネットワーク マップ，（3 ページ）

カスタム トポロジの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 ツールバーで [カスタム トポロジ（Custom Topology）] をクリックします。

ステップ 3 [トポロジの作成（Create Topology）] をクリックします。

ステップ 4 名前を入力します。

ステップ 5 必要に応じて、[説明（Description）] を入力します。

ステップ 6 トポロジにネットワークを追加します。次の方法のいずれかまたはすべてを使用できます。

- ネットワーク検出ポリシーからのネットワークのインポート, （10 ページ）の説明に従って、ネットワーク検出ポリシーからネットワークをインポートします。
- 手動によるカスタム トポロジへのネットワークの追加, （11 ページ）の説明に従って、手動でネットワークを追加します。

ステップ 7 [保存（Save）] をクリックします。

次の作業

- トポロジをアクティブ化します。詳細については、カスタムトポロジのアクティブおよび非アクティブの設定, （12 ページ）を参照してください。

ネットワーク検出ポリシーからのネットワークのインポート

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

手順

ステップ 1 ネットワークをインポートするカスタム トポロジにアクセスします。

- カスタム トポロジを作成します。カスタム トポロジの作成, （9 ページ）を参照してください。

- 既存のカスタム トポロジを編集します。カスタム トポロジの編集, （13 ページ）を参照してください。

ステップ 2 [ポリシー ネットワークのインポート（Import Policy Networks）] をクリックします。

ステップ 3 [ロード（Load）] をクリックします。システムにより、ネットワーク検出ポリシーのトポロジ情報が表示されます。

ステップ 4 トポロジを修正するには、次の手順を実行します。

- トポロジ内のネットワーク名を変更するには、ネットワークの横にある編集アイコン（）をクリックし、名前を入力してから [名前の変更（Rename）] をクリックします。
- トポロジからネットワークを削除するには、削除アイコン（）をクリックしてから [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックします。

次の作業

- トポロジをアクティブ化します。詳細については、カスタムトポロジのアクティブおよび非アクティブの設定, （12 ページ）を参照してください。

手動によるカスタム トポロジへのネットワークの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

手順

ステップ 1 ネットワークを追加するカスタム トポロジにアクセスします。

- カスタム トポロジを作成します。カスタム トポロジの作成, （9 ページ）を参照してください。

- 既存のカスタム トポロジを編集します。カスタム トポロジの編集, （13 ページ）を参照してください。

ステップ 2 [ネットワークの追加（Add Network）] をクリックします。

ステップ 3 ホストとネットワーク デバイスのネットワーク マップでネットワークのカスタム ラベルを追加するには、[名前（Name）] を入力します。

ステップ 4 追加するネットワークを表す [IP アドレス（IP Address）] と [ネットマスク（Netmask）]（IPv4）を入力します。

ステップ 5 [追加（Add）] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

次の作業

- トポロジをアクティブ化します。詳細については、カスタムトポロジのアクティブおよび非アクティブの設定, （12 ページ）を参照してください。

関連トピック

Firepower システムの IP アドレス表記法

カスタムトポロジのアクティブおよび非アクティブの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

（注） 常に 1 つのカスタム トポロジのみアクティブにできます。複数のトポロジを作成した場合、1 つをアクティブ化すると、自動的に現在アクティブなトポロジが非アクティブになります。

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [カスタムトポロジ（Custom Topology）] を選択します。

ステップ 3 アクティブまたは非アクティブにするトポロジの横にあるスライダをクリックします。

カスタム トポロジの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

アクティブ トポロジに加える変更はただちに有効になります。

手順

ステップ 1 [ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]を選択します。
マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [カスタム トポロジ（Custom Topology）] をクリックします。

ステップ 3 編集するトポロジの横にある編集アイコン（  ）をクリックします。

ステップ 4 カスタム トポロジの作成, （9 ページ）の説明に従って、トポロジを編集します。

ステップ 5 [保存（Save）] をクリックします。