ネットワーク マップの使用

FireSIGHT システムは、ネットワーク上を移動するトラフィックをパッシブに収集し、データを復号化し、設定されたオペレーティング システムおよびフィンガープリントと比較します。この情報から、システムはネットワークの詳細な表現である *ネットワーク マップ*を作成します。

ネットワーク マップでは、Defense Center を使用して、ホストとネットワーク デバイス(ブリッジ、ルータ、NAT デバイス、ロード バランサ)に関するネットワーク トポロジを調べることができます。迅速にネットワークの全体を見るために便利なツールです。ネットワーク マップでは、関連付けられたホスト属性、アプリケーション、クライアント、侵入を受けたホストの痕跡、脆弱性をドリルダウンできます。つまり、実行する分析に合わせて、ネットワーク マップのビューを選択できます。

ホスト入力機能を使用して、サードパーティ製アプリケーションから、オペレーティング システム、アプリケーション、クライアント、プロトコル、またはホスト属性情報を追加して、システムが収集する情報を増やすことができます。また、Nmap を使用してアクティブにネットワーク マップのホストをスキャンして、ネットワーク マップにスキャン結果を追加できます。

ネットワーク マップのビュー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できます。たとえば、組織の各部門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。

詳細については、次の項を参照してください。

ネットワーク マップについて

ライセンス：FireSIGHT

ネットワーク マップの各ビューは、展開可能なカテゴリおよびサブカテゴリの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、展開されて、その下のサブカテゴリが表示されます。実行する分析の種類に応じて、ネットワーク マップの異なるビューを選択できます。

Defense Center は、ディスカバリ ポリシーが適用されているすべてのセキュリティ ゾーン（NetFlow 対応デバイスからのデータを処理するゾーンを含む）からデータを収集します。複数のデバイスが同じネットワーク資産を検出した場合、Defense Center は情報をまとめて資産を複合表示します。

NetFlow 対応デバイスによってエクスポートされるデータを追加するようネットワーク検出ポリシーを設定できますが、これらのホストに関して利用可能な情報は限られています。たとえば、これらのホストのオペレーティング システム データは得られません（ただしホスト入力機能を使って指定する場合を除く）。詳細については、NetFlow と FireSIGHT データの違い（45-19 ページ）を参照してください。

任意のネットワーク マップで任意のホストの*ホスト プロファイル*を参照できます。システムによって収集されたホストのすべての情報の完全なビューを提供します。ホスト プロファイルには、ホスト名、オペレーティング システム、およびすべての関連付けられた IP アドレスといった一般情報と、検出されたプロトコル、アプリケーション、侵入の痕跡、およびホスト上で実行しているクライアントといった固有情報が含まれます。ホスト プロファイルには、ホストと検出された資産に関連付けられた脆弱性に関する情報も含まれます。ホスト プロファイルの詳細については、ホスト プロファイルの使用（49-1 ページ）を参照してください。

調査する必要がなくなった項目はネットワーク マップから削除できます。ネットワーク マップからホストとアプリケーションを削除できます。また、脆弱性を削除または非アクティブ化できます。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検出した場合は、ネットワーク マップにホストを再追加します。同様に、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）を検出すると、アプリケーションのネットワーク マップに再追加されます。システムがホストを脆弱にする変更を検出すると、そのホストの脆弱性は再アクティブ化されます。

また、ネットワーク マップを使用して、ネットワーク全体の脆弱性を非アクティブにできます。これにより、システムが脆弱と判断したホストについて、その特定の攻撃や悪用の心配がないとみなすことになります。

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。モニタリング対象からロード バランサおよび NAT デバイスを除外する必要があることもあります。これらは、過度のイベントおよび誤った結果をもたらすイベントを作成して、データベースを一杯にしたり、Defense Center をオーバーロードさせたりする可能性があります。詳細については、ホスト データ収集について（45-3 ページ）を参照してください。

ホストのネットワーク マップの操作

ライセンス：FireSIGHT

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表示でき、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。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ホスト数を表示します。

NetFlow 対応デバイスによってエクスポートされるデータに基づいてホストをネットワーク マップに追加するようネットワーク検出ポリシーを設定できますが、これらのホストについて利用可能な情報は限られています。たとえば、ホスト入力機能を使用してデータを提供していない限り、NetFlow データでネットワーク マップに追加されたホストのオペレーティング システム データはありません。

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 マップを表示できます。カスタム ネットワーク トポロジの操作（48-11 ページ）を参照してください。

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ネットワーク マップから削除できます。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。詳細については、ネットワーク検出ポリシーの作成（45-25 ページ）を参照してください。

（注） シスコ ネットワーク マップからネットワーク デバイスを削除**しない**ことを**強く**推奨します。システムはその場所を使用してネットワーク トポロジを特定するためです（モニタリング対象ホスト用のネットワーク ホップと TTL 値の生成を含む）。ネットワーク デバイスのネットワーク マップからはネットワーク デバイスを削除できませんが、ホストのネットワーク マップからネットワーク デバイスを削除しないようにしてください。

ホストのネットワーク マップを表示するには、次の手順を実行します。

アクセス：Admin/Any Security Analyst

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

ホストのネットワーク マップが開き、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。

手順 2　調査するホストの特定の IP アドレスまたは MAC アドレスにドリルダウンします。

たとえば、IP アドレス 192.168.40.11 のホストを表示するには、**192**、**192.168**、**192.168.40**、**192.168.40.11** の順にクリックします。**192.168.40.11** をクリックすると、ホスト プロファイルが表示されます。ホスト プロファイルの詳細については、ホスト プロファイルの使用（49-1 ページ）を参照してください。

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。

手順 3　オプションで、サブネット、IP アドレス、または MAC アドレスを削除するには、削除する要素の隣にある削除アイコン( )をクリックし、ホストまたはサブネットを削除することを確認します。

ホストが削除されます。システムはホストを再検出すると、ネットワーク マップにホストを再追加します。

手順 4　オプションで、ホストのネットワーク マップのホスト ビューとトポロジ ビューを切り替えます。

- カスタム トポロジで整理されたホストのネットワーク マップのビューに切り替えるには、ホスト ビュー(デフォルト)で、ネットワーク マップの一番上にある [(トポロジ)((topology))] をクリックします。
- サブネットで整理されたホストのネットワーク マップのビューに切り替えるには、トポロジ ビューで、ネットワーク マップの一番上にある [(ホスト)((hosts))] をクリックします。

カスタム トポロジの設定については、カスタム ネットワーク トポロジの操作(48-11 ページ)を参照してください。

ネットワーク デバイスのネットワーク マップの操作

ライセンス: FireSIGHT

ネットワークのセグメント同士を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、ロード バランサ)を表示するため、またそのネットワーク デバイスのホスト プロファイルにドリルダウンするために、ネットワーク デバイスのネットワーク マップを使用します。ネットワーク デバイスのネットワーク マップは、IP および MAC という 2 つのセクションに分けられます。IP セクションは IP アドレスで識別されたネットワーク デバイスのリストを表示します。MAC セクションは MAC アドレスで識別されるネットワーク デバイスのリストを表示します。また、このネットワーク マップ ビューは、デバイスに 1 つの IP アドレスまたは複数の IP アドレスがあるかに関係なく、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 デバイスの数を表示します。

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たラベルはネットワーク 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 デバイスを区別するためにシステムでは次の方法を使用します。

- Cisco Discovery Protocol(CDP)メッセージの分析。ネットワーク デバイスと種類を特定します(Cisco 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、IP アドレスが 1 つ以上の可能性があります。STP を使用して通信している場合は、MAC アドレスが 1 つのみの可能性があります。

ネットワーク マップからネットワーク デバイスを削除することはできません。システムはその場所を使用してネットワーク トポロジを特定するためです(モニタリング対象ホスト用のネットワーク ホップと TTL 値の生成を含む)。

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、ネットワーク デバイスの背後で検出されたモバイル デバイスのハードウェア プラットフォームを反映する [ハードウェア（Hardware）] 列を含む [システム（Systems）] セクションがあります。[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た場合、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 デバイスにはハードウェア プラットフォームの情報がある場合とない場合がありますが、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。

ネットワーク デバイスのネットワーク マップを表示するには、次の手順を実行します。

アクセス：Admin/Any Security Analyst

手順 1　[分析（Analysis）] > [ホスト（Hosts）] > [ネットワーク マップ（Network Map）] > [ネットワーク デバイス（Network Devices）] を選択します。

ネットワーク デバイスのネットワーク マップが開き、一意のネットワーク デバイスの数と、ネットワーク デバイスの IP アドレスと MAC アドレスのリストを表示します。各アドレスまたはアドレスの一部は、アドレスの次のレベルか、各ホストのホスト プロファイルへのリンクです。

手順 2　調査するネットワーク デバイスの特定の IP アドレスまたは MAC アドレスにドリルダウンします。

ネットワーク デバイスのホスト プロファイルが表示されます。ホスト プロファイルの詳細については、ホスト プロファイルの使用（49-1 ページ）を参照してください。

手順 3　オプションで、IP または MAC アドレスでフィルタリングをするには、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。

侵入の痕跡のネットワーク マップの操作

ライセンス：FireSIGHT

侵入の痕跡（IOC）のネットワーク マップを使用して、ネットワーク上の侵入されたホストを IOC のカテゴリで整理して表示します。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。

システムは、ホストの侵入ステータスを判断するために、侵入イベント、Security Intelligence、FireAMP を含む複数のソースからのデータを使用します。

侵入の痕跡のネットワーク マップから、何らかの侵入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。

侵入の痕跡のネットワーク マップを表示するには、次の手順を実行します。

アクセス：Admin/Any Security Analyst

手順 1　[分析（Analysis）] > [ホスト（Hosts）] > [ネットワーク マップ（Network Map）] > [侵入の痕跡（Indications of Compromise）] を選択します。

侵入の痕跡のネットワーク マップが表示されます。

手順 2　調査する特定の IOC カテゴリをクリックします。

たとえば、マルウェアが検出されたホストを表示するには、[マルウェア検出（Malware Detected）] をクリックします。

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。

手順 3　選択した IOC カテゴリで、特定の IP アドレスへドリルダウンします。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。

侵入を受けたホストのホスト プロファイルが表示され、侵入の痕跡のセクションが展開されます。ホスト プロファイルの IOC セクションの詳細については、ホスト プロファイルでの侵害の兆候の使用（49-9 ページ）を参照してください。

手順 4　オプションで、IOC カテゴリ、侵入を受けたホスト、または侵入を受けたホストのグループを解決済みにするには、解決する要素の隣にある削除アイコン（ ）をクリックし、それを解決することを確認します。

カテゴリまたはホストが解決されます（IOC タグが削除されます）。その IOC が再度トリガーされると、ネットワーク マップに再追加されます。

モバイル デバイスのネットワーク マップの操作

ライセンス：FireSIGHT

ネットワークに接続されたモバイル デバイスを表示するため、またそのデバイスのホスト プロファイルにドリルダウンするために、モバイル デバイスのネットワーク マップを使用します。また、このネットワーク マップ ビューは、デバイスに 1 つの IP アドレスまたは複数の IP アドレスがあるかに関係なく、システムによって検出されたすべての一意のモバイル デバイスの数を表示します。

モバイル デバイスを区別するためにシステムでは次の方法を使用します。

- モバイル デバイスのモバイル ブラウザからの HTTP トラフィックのユーザ エージェント ストリングの分析
- 特定のモバイル アプリケーションの HTTP トラフィックのモニタ

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たラベルはモバイル デバイスのネットワーク マップに表示されます。

モバイル デバイスのネットワーク マップを表示するには、次の手順を実行します。

アクセス：Admin/Any Security Analyst

手順 1　[分析（Analysis）] > [ホスト（Hosts）] > [ネットワーク マップ（Network Map）] を選択し、[モバイル デバイス（Mobile Devices）] タブを選択します。

モバイル デバイスのネットワーク マップが開き、一意のモバイル デバイスの数と、モバイル デバイスの IP アドレスのリストを表示します。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。

手順 2　調査するモバイル デバイスの特定の IP アドレスにドリルダウンします。

たとえば、IP アドレス 10.11.40.11 のデバイスを表示するには、**10**、**10.11**、**10.11.40**、**10.11.40.11** の順にクリックします。**10.11.40.11** をクリックすると、ホスト プロファイルが表示されます。ホスト プロファイルの詳細については、ホスト プロファイルの使用（49-1 ページ）を参照してください。

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。

手順 3　オプションで、サブネットまたは IP アドレスを削除するには、削除する要素の隣にある削除アイコン（ ）をクリックし、デバイスまたはサブネットを削除することを確認します。

デバイスが削除されます。システムはデバイスを再検出すると、ネットワーク マップにデバイスを再追加します。

アプリケーションのネットワーク マップの操作

ライセンス：FireSIGHT

アプリケーションのネットワーク マップを使用して、アプリケーション名、ベンダー、バージョン、さらには各アプリケーションを実行するホストによって階層ツリーに整理された、ネットワークのアプリケーションを表示できます。

システムが検出するアプリケーションは、システム ソフトウェアおよび VDB アップデートによって、およびアドオン 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。ディテクタの全般的な情報を含む最新のリストについては、次のサポート サイトのいずれかを参照してください。

- **シスコ：**（http://www.cisco.com/cisco/web/support/index.html）

アプリケーションのネットワーク マップから、特定のアプリケーションを実行する各ホストのホスト プロファイルを表示できます。また、アプリケーション 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、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 マップから削除できます。

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 カテゴリを削除すると、そのアプリケーション カテゴリはネットワーク マップから削除されます。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] として識別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、またはバージョンを削除すると、影響を受けるアプリケーションは、ネットワーク マップと、それを含むホスト プロファイルから削除されます。

  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 アドレスを削除する場合、IP アドレスはアプリケーション リストから削除され、アプリケーション自体は、選択した IP アドレスのホスト プロファイルから削除されます。

  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。

アプリケーションのネットワーク マップを表示するには、次の手順を実行します。

アクセス：Admin/Any Security Analyst

手順 1　[分析（Analysis）] > [ホスト（Hosts）] > [ネットワーク マップ（Network Map）] > [アプリケーション（Applications）] を選択します。

アプリケーションのネットワーク マップが表示されます。

手順 2　調査する特定のアプリケーションにドリルダウンします。

たとえば、Apache など特定のタイプの Web サーバを表示する場合は、[http] をクリックし、[Apache] をクリックして、表示する Apache Web サーバのバージョンをクリックします。

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。

手順 3　選択したアプリケーションの特定の IP アドレスをクリックします。

アプリケーションを実行しているホストのホスト プロファイルが表示され、アプリケーション セクションが展開されます。ホスト プロファイルのアプリケーション セクションの詳細については、ホスト プロファイルでのサーバの使用（49-17 ページ）を参照してください。

手順 4　オプションで、アプリケーション 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、また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には、削除する要素の隣にある削除アイコン（ ）をクリックし、削除することを確認します。

アプリケーションが削除されます。システムはアプリケーションを再検出すると、ネットワーク マップに再追加します。

脆弱性のネットワーク マップの操作

ライセンス：FireSIGHT

脆弱性のネットワーク マップを使用して、システムがネットワーク上で検出した脆弱性をレガシーの脆弱性 ID（SVID）、Bugtraq ID、CVE ID、または Snort ID 別に整理して表示します。脆弱性は ID 番号によって並べられ、影響を受けるホストが各脆弱性の下にリストされます。

脆弱性のネットワーク マップから、特定の脆弱性の詳細を表示できます。また、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。これは、影響を受ける特定のホストの脆弱性によって生じる脅威を評価するのに役立ちます。

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見なす場合（パッチを適用済みの場合など）、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 マップに表示されますが、これまで影響を受けていたホストの IP アドレスはグレーのイタリック体で表示されます。これらのホストのホスト プロファイルでは、非アクティブ化した脆弱性は無効として表示されますが、個々のホストについて手動で有効にすることができます。詳細については、個々のホストに対する脆弱性の設定（49-33 ページ）を参照してください。

ホスト上のアプリケーションまたはオペレーティング システムのアイデンティティの競合がある場合、システムは候補となるアイデンティティの両方について脆弱性を表示します。アイデンティティの競合が解決した場合、脆弱性は現在のアイデンティティに関連付けされたままになります。詳細については、現在の ID について（46-5 ページ）およびID の競合について（46-7 ページ）を参照してください。

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およびバージョンが含まれていた場合にのみ、検出されたアプリケーションの脆弱性が脆弱性のネットワーク マップに表示されます。ただし、システム ポリシー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、ベンダーおよび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。アプリケーションの脆弱性マッピングの設定の詳細については、サーバの脆弱性のマッピング（63-33 ページ）を参照してください。

脆弱性 ID（または脆弱性 ID の範囲）の隣の数字は、次の 2 つの数を示します。

- 最初の数字は、1 つまたは複数の脆弱性の影響を受ける、一意でないホストの数です。ホストが複数の脆弱性の影響を受ける場合、複数回カウントされます。したがって、この数字がネットワーク上のホスト数を上回ることもあります。脆弱性を非アクティブ化すると、その脆弱性の影響を受ける可能性のあるホスト数の分、この数が減ります。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、この数は表示されません。
- 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、一意でないホストの総数とほぼ同じ数です。

脆弱性を非アクティブ化すると、ユーザが指定したホストについてのみ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。その後でシステムが非アクティブ化されていないホストに脆弱性を検出すると（たとえば、ネットワーク マップの新しいホスト）、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、非アクティブ化されている関連付けられた脆弱性を再アクティブ化することがあります。

脆弱性のネットワーク マップを表示するには、次の手順を実行します。

アクセス：Admin/Any Security Analyst

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

脆弱性のネットワーク マップが表示されます。

手順 2　[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。デフォルトでは、脆弱性はレガシーの脆弱性 ID（SVID）ごとに表示されます。

手順 3　調査する特定の脆弱性にドリルダウンします。

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。

脆弱性の詳細が表示されます。表示される情報の詳細については、脆弱性の詳細の表示（49-30 ページ）を参照してください。

さらにネットワーク マップでは、影響を受けるホストの IP アドレスが Defense Center によって表示されます。任意の IP アドレスをクリックして、そのホストのホスト プロファイルを表示できます。

手順 4　オプションで、脆弱性を非アクティブ化します。

- 脆弱性の影響を受けるすべてのホストの脆弱性を非アクティブ化するには、脆弱性番号の隣にある削除アイコン（ ）をクリックします。
- 個々のホストの脆弱性を非アクティブ化するには、ホストの IP アドレスの隣にある削除アイコン（ ）をクリックします。

脆弱性が非アクティブになります。該当するホストの IP アドレスは、ネットワーク マップにグレーの斜体で表示されます。さらに、こ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を無効として表示します。

ヒント　脆弱性の再アクティブ化の詳細については、個々のホストに対する脆弱性の設定（49-33 ページ）を参照してください。

ホスト属性のネットワーク マップの操作

ライセンス：FireSIGHT

ホスト属性のネットワーク マップを使用して、ネットワーク上のホストをホスト属性で整理して表示します。ホストを整理するために使用するホスト属性を選択すると、Defense 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。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。

ホスト属性のネットワーク マップでは、ユーザ定義のホスト属性に基づいてホストを整理できます。これらの属性について、ネットワーク マップは値が Unassigned として割り当てられていないホストを表示します。

詳細については、ユーザ定義のホスト属性の使用（49-35 ページ）を参照してください。

さらに、ホスト属性のネットワーク マップは、ユーザが作成したコンプライアンス ホワイト リストに対応するホスト属性に基づいてホストを整理できます。ユーザが作成するコンプライアンス ホワイト リストごとに、各ホワイト リストと同じ名前でホスト属性が自動的に作成されます。

ホワイト リストのホスト属性がとり得る値は次の通りです。

- `Compliant` は、ホワイト リストに準拠しているホスト
- `Non-Compliant` は、ホワイト リストに違反しているホスト
- `Not Evaluated` は、ホワイトリストの有効な対象でないか、または何らかの理由で評価されていないホスト

コンプライアンス ホワイト リストの詳細については、FireSIGHT システムのコンプライアンス ツールとしての使用（52-1 ページ）を参照してください。

（注） ホスト属性のネットワーク マップでは、事前定義されたホスト属性（ホストの重要度など）を使用して、ホストを整理することはできません。

ホスト属性のネットワーク マップを表示するには、次の手順を実行します。

アクセス：Admin/Any Security Analyst

手順 1　[分析（Analysis）] > [ホスト（Hosts）] > [ネットワーク マップ（Network Map）] > [ホスト属性（Host Attributes）] を選択します。

ホスト属性のネットワーク マップが表示されます。

手順 2　[属性（Attribute）] ドロップダウン リストから、ホスト属性を選択します。

Defense Center はホスト属性の値をリストし、その値が割り当てられたホストの数を括弧内に表示します。

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。

手順 3　ホスト属性値をクリックすると、その値が割り当てられたホストが表示されます。

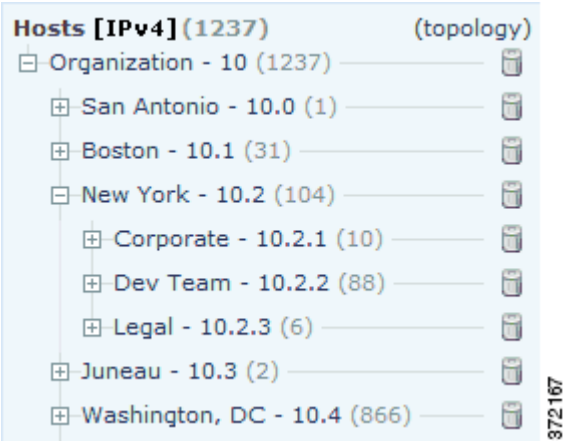
手順 4　ホストの IP アドレスをクリックすると、そのホストのホスト プロファイルが表示されます。

カスタム ネットワーク トポロジの操作

ライセンス：FireSIGHT

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、組織内の各部門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。こうすることで、ホストまたはネットワーク デバイスのネットワーク マップを表示する際に、サブネットに割り当てたラベルが次の図のように表示されます。



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。

ホストおよびネットワーク デバイスのネットワーク マップの詳細については、ホストのネットワーク マップの操作（48-3 ページ）およびネットワーク デバイスのネットワーク マップの操作（48-4 ページ）を参照してください。

詳細については、次の項を参照してください。

- カスタム トポロジの作成（48-12 ページ）
- カスタム トポロジの管理（48-17 ページ）

カスタム トポロジの作成

ライセンス：FireSIGHT

カスタム トポロジを作成するには、ネットワークを指定する必要があります。これには、次の 3 つの方法のいずれかまたはすべてを使用します。

- シスコが検出したトポロジのインポート。システムによって検出されたホストとネットワーク デバイスに基づいて推測した、最も正確と考えられるネットワークの展開を使用して、ネットワークを追加します。
- 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。ネットワーク検出ポリシーで、FireSIGHT システムのモニタリング対象として設定したネットワークを追加します。

- トポロジへのネットワークの手動追加。他の 2 つの方法で作成される展開の表現が、不正確または不完全な場合に使用します。

トポロジをネットワーク マップで使用するには、トポロジを保存してアクティブ化する必要があります。

カスタム トポロジを作成するには、次の手順を実行します。

アクセス：Admin/Discovery Admin

手順 1　[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）] を選択し、[カスタム トポロジ（Custom Topology）] を選択します。

[カスタム トポロジ（Custom Topology）] ページが表示されます。

手順 2　[トポロジの作成（Create Topology）] をクリックします。

[トポロジの作成（Create Topology）] ページが表示されます。

手順 3　トポロジ名や説明など、基本的なトポロジ情報を入力します。

基本的なトポロジ情報の入力（48-14 ページ）を参照してください。

手順 4　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。

- シスコが検出したトポロジをインポートしてネットワークをトポロジに追加する場合は、検出されたトポロジのインポート（48-14 ページ）の手順に従います。
- ネットワーク検出ポリシーからインポートすることで、トポロジにネットワークを追加するには、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（48-15 ページ）の手順を参照してください。
- トポロジにネットワークを手動で追加するには、手動によるカスタム トポロジへのネットワークの追加（48-16 ページ）の手順に従います。

手順 5　トポロジを修正するには、次の手順を実行します。

- カスタム トポロジからネットワークを削除するには、削除するネットワークの隣にある [削除（Delete）] をクリックします。
- ネットワークを名称変更するには、ネットワークの隣にある [名称変更（Rename）] をクリックします。表示されるポップアップ ウィンドウで、[名前（Name）] フィールドに新しい名前を入力し、[名称変更（Rename）] をクリックします。この名前のラベルが、ネットワーク マップのネットワークに付けられます。

手順 6　[保存（Save）] をクリックします。

トポロジが保存されます。

（注）　ネットワーク マップでこのトポロジを使用するには、アクティブ化する必要があります。詳細については、カスタム トポロジの管理（48-17 ページ）を参照してください。

基本的なトポロジ情報の入力

ライセンス：FireSIGHT

各カスタム トポロジに、名前と、必要に応じて簡単な説明を入力します。

基本的なトポロジ情報を入力するには、次の手順を実行します。

アクセス：Admin

手順 1　[トポロジの編集（Edit Topology）] ページで、[名前（Name）] フィールドにトポロジの名前を入力します。

手順 2　オプションで、[説明（Description）] フィールドにトポロジの説明を入力します。

手順 3　オプションで、カスタム トポロジをどのように構築するかに応じて、以降のセクションの手順に進みます。

- 検出されたトポロジのインポート（48-14 ページ）
- 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（48-15 ページ）
- 手動によるカスタム トポロジへのネットワークの追加（48-16 ページ）

検出されたトポロジのインポート

ライセンス：FireSIGHT

カスタム トポロジにネットワークを追加する方法の 1 つは、FireSIGHT システムによって検出されたトポロジをインポートすることです。この検出されたトポロジは、検出されたホストとネットワーク デバイスに基づいてシステムが推測した、最も正確と考えられるネットワークの展開です。

検出されたトポロジをインポートするには、次の手順を実行します。

アクセス：Admin

手順 1　[トポロジの編集（Edit Topology）] ページで、[検出されたトポロジのインポート（Import Discovered Topology）] をクリックします。

手順 2　検出されたネットワークがページに示されます。

手順 3　オプションで、カスタム トポロジをどのように構築するかに応じて、以降のセクションの手順に進みます。

- 検出されたトポロジのインポート（48-14 ページ）
- 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（48-15 ページ）
- 手動によるカスタム トポロジへのネットワークの追加（48-16 ページ）

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

ライセンス：FireSIGHT

カスタム トポロジにネットワークを追加する方法の 1 つは、ネットワーク検出ポリシーで FireSIGHT システムのモニタリング対象として設定したネットワークをインポートすることです。ネットワーク検出ポリシーの作成（45-25 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ネットワークをインポートするには、次の手順を実行します。

アクセス：Admin

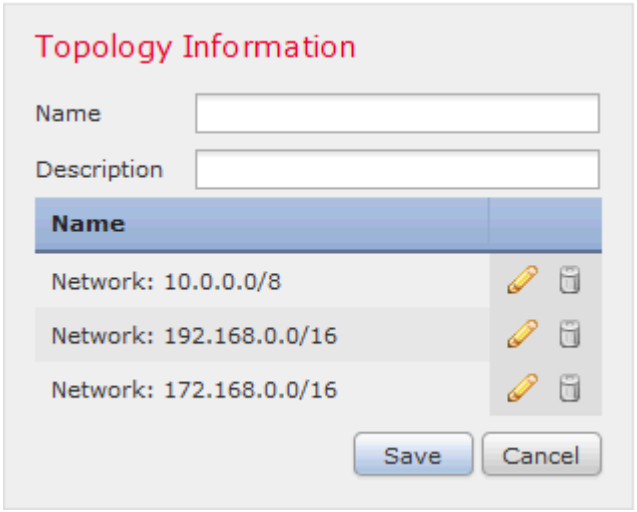
手順 1　[トポロジの編集（Edit Topology）] ページで、[ポリシー ネットワークのインポート（Import Policy Networks）] をクリックします。

ポップアップ ウィンドウが表示されます。

手順 2　ドロップダウン リストから、使用するネットワーク検出ポリシーを選択し、[ロード（Load）] をクリックします。

手順 3　ネットワーク検出ポリシーのモニタリング対象ネットワークがページに示されます。

たとえば、10.0.0.0/8、192.168.0.0/16、172.12.0.0/16 のネットワークをモニタリングするようにネットワーク検出ポリシーを設定すると、そのネットワークがページに表示されます。



手順 4　別のネットワーク検出ポリシーからネットワークを追加するには、手順 1 と 2 を繰り返します。

手順 5　オプションで、カスタム トポロジをどのように構築するかに応じて、以降のセクションの手順を実行します。

- 検出されたトポロジのインポート（48-14 ページ）
- 手動によるカスタム トポロジへのネットワークの追加（48-16 ページ）

手動によるカスタム トポロジへのネットワークの追加

ライセンス：FireSIGHT

シスコが検出したトポロジのインポートや、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によって、ネットワーク配置が不正確または不完全に表示される場合は、カスタム トポロジにネットワークを手動で追加できます。

ネットワークをカスタム トポロジに手動で追加するには、次の手順を実行します。

アクセス：Admin

手順 1　[トポロジの編集（Edit Topology）] ページで、[ネットワークの追加（Add Network）] をクリックします。

ポップアップ ウィンドウが表示されます。

手順 2　オプションで、[名前（Name）] フィールドに名前を入力してネットワークに名前を付けます。

この名前のラベルが、トポロジをアクティブ化した後で、ホストおよびネットワーク デバイスのネットワーク マップのネットワークに付けられます。

詳細については、ホストのネットワーク マップの操作（48-3 ページ）およびネットワーク デバイスのネットワーク マップの操作（48-4 ページ）を参照してください。

手順 3　[IP アドレス（IP Address）] フィールドと [ネットマスク（Netmask）] フィールドに、トポロジに追加するネットワークを表す IP アドレスとネットワーク マスク（CIDR 表記）を入力します。

FireSIGHT システムでの CIDR 表記の使用法の詳細については、IP アドレスの表記規則（1-24 ページ）を参照してください。

手順 4　[追加（Add）] をクリックします。

ネットワークがトポロジに追加されます。

手順 5　トポロジにさらにネットワークを追加するには、手順 1 ～ 4 を繰り返します。

ヒント　トポロジからネットワークを削除するには、削除するネットワークの隣にある [削除（Delete）] をクリックし、ネットワークと、ネットワークへのすべてのリンクを削除することを確認します。

手順 6　オプションで、カスタム トポロジをどのように構築するかに応じて、以降のセクションの手順を実行します。

- 検出されたトポロジのインポート（48-14 ページ）
- 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（48-15 ページ）

カスタム トポロジの管理

ライセンス：FireSIGHT

カスタム トポロジの管理には [カスタム トポロジ（Custom Topology）] ページを使用します。トポロジを作成、変更、削除できます。

トポロジの状態が名前とともに表示されます。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。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。

次の手順を使用して、カスタム トポロジのアクティブ化または非アクティブ化、トポロジの変更、またはトポロジの削除を行います。

アクティブなトポロジを削除すると、その変更はただちに有効になります。つまり、ネットワーク マップにはカスタム トポロジが表示されなくなります。

カスタム トポロジをアクティブ化または非アクティブ化するには、次の手順を実行します。

アクセス：Admin

手順 1　[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）] > [カスタム トポロジ（Custom Topology）] を選択します。

[カスタム トポロジ（Custom Topology）] ページが表示されます。

手順 2　以下の 2 つの対処法があります。

- トポロジを**アクティブ化する**には、ポリシーの隣にある [アクティブ化（Activate）] をクリックします。
- トポロジを**非アクティブ化する**には、ポリシーの隣にある [非アクティブ化（Deactivate）] をクリックします。

カスタム トポロジを変更するには、次の手順を実行します。

アクセス：Admin

手順 1　[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）] > [カスタム トポロジ（Custom Topology）] を選択します。

[カスタム トポロジ（Custom Topology）] ページが表示されます。

手順 2　編集するトポロジの隣にある編集アイコン（ ）をクリックします。

[トポロジの編集（Edit Topology）] ページが表示されます。変更可能なさまざまな設定の詳細については、カスタム トポロジの作成（48-12 ページ）を参照してください。

手順 3　必要な変更を行い、[保存（Save）] をクリックします。

トポロジが変更されます。トポロジがアクティブな場合は、ネットワーク マップに行った変更は即時に有効になります。

カスタム トポロジを削除するには、次の手順を実行します。

アクセス：Admin

手順 1　[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）] > [カスタム トポロジ（Custom Topology）] を選択します。

[カスタム トポロジ（Custom Topology）] ページが表示されます。

手順 2　削除するトポロジの隣にある [削除（Delete）] をクリックします。トポロジがアクティブな場合は、削除することを確認します。

トポロジが削除されます。