アクティブ スキャンの設定

FireSIGHT システムは、ネットワークのトラフィックをパッシブ分析してネットワーク マップを構築します。しかし、ホストをアクティブにスキャンして、そのホストに関する情報を判別する必要が生じることがあります。たとえば、オープン ポート上で実行中のサーバがホストにあり、システムによるネットワークのモニタリング中にそのサーバがトラフィックを送受信しなかった場合、システムではそのサーバに関する情報をネットワーク マップに追加しません。しかし、アクティブ スキャナを使用して直接そのホストをスキャンすると、サーバの存在を検出できます。

ホストをアクティブにスキャンする場合、ホストに関する情報を取得しようとする際にパケットを送信します。FireSIGHT システムは Nmap™ 6.01 と統合されています。これはネットワークの調査やセキュリティの監査用のオープン ソースのアクティブ スキャナで、ホスト上で実行されているオペレーティング システムやサーバを検出するのに使用できます。Nmap スキャンを使用すると、その結果に基づいて、ホスト上で実行されているオペレーティング システムやサーバに関する詳細情報を調べ、システムの脆弱性に関する報告内容を改善できます。

注 スキャン オプションによっては（ポートスキャンなど）低帯域幅のネットワークに非常に負荷をかけることがあります。この種のスキャンは、必ずネットワーク利用率が低い時間にスケジュールする必要があります。

詳細については、次の項を参照してください。

- 「Nmap スキャンの概要」（P.43-1）
- 「Nmap スキャンのセットアップ」（P.43-10）
- 「Nmap スキャンの管理」（P.43-16）
- 「スキャン ターゲットの管理」（P.43-20）
- 「アクティブ スキャンの結果での作業」（P.43-22）

Nmap スキャンの概要

ライセンス：FireSIGHT

Nmap を使用すると、ネットワーク内のホスト上のポートをアクティブにスキャンして、そのホストのオペレーティング システムやサーバのデータを判別することにより、ネットワーク マップの質を高めたり、スキャン対象のホストにマップされている脆弱性の精度を微調整したりできます。Nmap がホスト プロファイルに結果を追加できるようにするには、その前にホストがネットワーク マップ内になければならないことに注意してください。結果ファイル内でスキャン結果を参照することもできます。

Nmap を使用してホストをスキャンすると、以前に検出されなかったオープン ポート上のサーバが、そのホストに関するホスト プロファイル内の Servers リストに追加されます。ホスト プロファイルの Scan Results セクションには、フィルタ処理されていたり閉じていたりしている TCP ポートや UDP ポート上で検出されたサーバがリストされます。デフォルトでは、Nmap は 1660 を超える TCP ポートをスキャンします。

Nmap はスキャン結果と 1500 を超える既知のオペレーティング システムのフィンガープリントを比較して、オペレーティング システムを判別し、それぞれにスコアを割り当てます。最高スコアのオペレーティング システムのフィンガープリントが、ホストに割り当てられるオペレーティング システムになります。

Nmap スキャンで識別されたサーバがシステムで認識され、対応するサーバ定義がシステムにある場合、システムはそのサーバの脆弱性をホストにマップします。システムは、Nmap で使用されているサーバの名前を対応するシスコのサーバ定義にマップし、システム内で各サーバにマップされた脆弱性を使用します。同様に、システムは Nmap のオペレーティング システム名をシスコのオペレーティング システム定義にマップします。Nmap がホストのオペレーティング システムを検出すると、システムは対応するシスコのオペレーティング システム定義からホストに脆弱性を割り当てます。

スキャンに使用される基礎的な Nmap テクノロジーの詳細については、http://insecure.org にある Nmap のマニュアルを参照してください。

シスコ アプライアンス上の Nmap の詳細については、次のトピックを参照してください。

- 「Nmap 修復の概要」（P.43-2）
- 「Nmap スキャン戦略の作成」（P.43-6）
- 「サンプルの Nmap スキャン プロファイル」（P.43-7）

Nmap 修復の概要

ライセンス：FireSIGHT

Nmap 修復を作成して、Nmap スキャンの設定を定義できます。Nmap 修復は、相関ポリシー内で応答として使用したり、オン デマンドで実行したり、特定の時間に実行するようにスケジュールしたりできます。Nmap スキャンの結果をネットワーク マップ内に表示するには、スキャン対象のホストがネットワーク マップ内にすでに存在していなければなりません。

Nmap により提供されるサーバやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままであることに注意してください。Nmap を使用してホスト内でオペレーティング システムやサーバのデータをスキャンすることを計画している場合は、定期的なスキャンのスケジュールをセットアップして、Nmap によって提供されるオペレーティング システムやサーバのデータを最新に保つこともできます。詳細については、「Nmap スキャンの自動化」（P.49-5）を参照してください。ホストがネットワーク マップから削除されると、そのホストに関する Nmap スキャン結果は破棄されることにも注意してください。

Nmap の機能に関する詳細情報については、http://insecure.org にある Nmap のマニュアルを参照してください。次の表に、FireSIGHT システム上で設定できる Nmap 修復オプションを示します。

表 43-1　Nmap 修復オプション

オプション	説明	対応する Nmap オプション
Scan Which Address(es) From Event?	Nmap スキャンを相関ルールに対する応答として使用する場合、イベント内の送信元ホスト、宛先ホスト、またはその両方のどのアドレスをスキャンするのか制御するオプションを選択します。	該当なし
Scan Types	Nmap がポートをスキャンする方法を選択します。 • [TCP Syn] スキャンは、完全な TCP ハンドシェイクを使用せずに数千のポートにただちに接続します。このオプションを使用すると、TCP 接続が開始されますが完了はしていない状態で、admin アカウントが raw パケット アクセス権を持つホストや IPv6 が実行されていないホスト上でステルス モードでクイック スキャンできます。ホストが TCP Syn スキャンで送信される SYN パケットを確認応答すると、Nmap は接続をリセットします。 • [TCP Connect] スキャンは、connect() システム コールを使用して、ホスト上のオペレーティング システムを介して接続を開きます。TCP Connect スキャンは、防御センター上の admin ユーザや管理対象デバイスがホストに対する raw パケット特権を持っていない場合や、IPv6 ネットワークをスキャンしている場合に使用できます。つまり、このオプションは TCP Syn スキャンを使用できない状況で使用します。 • [TCP ACK] スキャンは、ACK パケットを送信して、ポートがフィルタ処理されているかいないかを検査します。 • [TCP Window] スキャンは、TCP ACK スキャンと同じ機能に加えて、ポートが開いているか閉じているかも判別します。 • [TCP Maimon] スキャンは、FIN/ACK プローブを使用して BSD 派生システムを識別します。	**TCP Syn**：-sS **TCP Connect**：-sT **TCP ACK**：-sA **TCP Window**：-sW **TCP Maimon**：-sM
Scan for UDP ports	TCP ポートに加えて UDP ポートのスキャンも有効にします。UDP ポートのスキャンには時間がかかることがあるので、クイック スキャンする場合はこのオプションを使用しないように注意してください。	-sU
Use Port From Event	相関ポリシー内で応答として修復を使用する計画の場合に、修復によるスキャンの対象として、相関応答をトリガーするイベントで指定されたポートのみを有効にします。 ヒント　Nmap がオペレーティング システムやサーバに関する情報を収集するかどうかも制御できます。新しいサーバに関連付けられたポートをスキャンするには、[Use Port From Event] オプションを有効にします。	該当なし
Scan from reporting detection engine	ホストを報告した検出エンジンがあるアプライアンスからホストへのスキャンを有効にします。	該当なし

表 43-1　Nmap 修復オプション（続き）

オプション	説明	対応する Nmap オプション
Fast Port Scan	スキャン元デバイス上の `/var/sf/nmap/share/nmap/nmap-services` ディレクトリ内にある `nmap-services` ファイルにリストされている TCP ポートのみに対するスキャンを有効にし、その他のポート設定を無視できるようにします。このオプションと [Port Ranges and Scan Order] オプションを併用できないことに注意してください。	`-F`
Port Ranges and Scan Order	Nmap ポート仕様シンタックスを使用して、スキャンする特定のポートを設定し、スキャンする順序も設定します。このオプションと [Fast Port Scan] オプションを併用できないことに注意してください。	`-p`
Probe open ports for vendor and version information	サーバ ベンダーとバージョン情報の検出を有効にします。オープン ポートでサーバ ベンダーとバージョン情報を調査する場合、Nmap はサーバの識別に使用するサーバ データを取得します。次に、シスコのサーバ データをそのサーバに置き換えます。	`-sV`
Service Version Intensity	サービス バージョンに対する Nmap プローブの強度を選択します。サービスの強度の数値が大きいほど、使用されるプローブが多くなり、精度は高くなります。強度の数値が小さいほど、プローブは高速になりますが、取得する情報は少なくなります。	`--version-intensity <intensity>`
Detect Operating System	ホストのオペレーティング システム情報の検出を有効にします。 ホストでのオペレーティング システムの検出を設定した場合、Nmap はホストをスキャンし、その結果を使用してオペレーティング システムごとに評価を作成します。この評価は、ホスト上でそのオペレーティング システムが実行されている可能性を反映します。Nmap で識別されるアイデンティティ データがネットワーク マップに表示される時点とその方法の詳細については、「現在の ID について」（P.42-5）を参照してください。	`-o`
Treat All Hosts As Online	ホスト ディスカバリ プロセスを省略し、ターゲット範囲内のすべてのホスト上でのポート スキャンを有効にします。このオプションを有効にすると、Nmap は [Host Discovery Method] と [Host Discovery Port List] の設定を無視するので注意してください。	`-PN`

表 43-1　Nmap 修復オプション（続き）

オプション	説明	対応する Nmap オプション
Host Discovery Method	ホスト ディスカバリを、ターゲット範囲内のすべてのホストに対して実行するか、[Host Discovery Port List] にリストされているポートを経由して実行するか、または、ポートがリストされていない場合にそのホスト ディスカバリ方式のデフォルト ポートを経由するかを選択します。 ここで、[Treat All Hosts As Online] も有効にすると、[Host Discovery Method] オプションは無効になり、ホスト ディスカバリが実行されないことに注意してください。 ホストが存在していて利用可能であるかどうかを Nmap がテストする際に使用する方式を以下から選択します。 • [TCP SYN] オプションは、SYN フラグが設定された空の TCP パケットを送信し、応答を受信するとホストが利用可能であると認識します。デフォルトでは TCP SYN はポート 80 をスキャンします。TCP SYN スキャンは、ステートフル ファイアウォール ルールが指定されたファイアウォールでブロックされる可能性が低いことに注意してください。 • [TCP ACK] オプションは、ACK フラグが設定された空の TCP パケットを送信し、応答を受信するとホストが利用可能であると認識します。デフォルトでは TCP ACK もポート 80 をスキャンします。TCP ACK スキャンは、ステートレス ファイアウォール ルールが指定されたファイアウォールでブロックされる可能性が低いことに注意してください。 • [UDP] オプションは、UDP パケットを送信し、クローズ ポートからポート到達不能応答が戻されるとホストが利用可能であると想定します。デフォルトでは UDP はポート 40125 をスキャンします。	**TCP SYN**：`-PS` **TCP ACK**：`-PA` **UDP**：`-PU`
Host Discovery Port List	ホスト ディスカバリの実行時にスキャンするポートを、カスタマイズしたカンマ区切りリストで指定します。	ホスト ディスカバリ方式に応じたポート リスト
Default NSE Scripts	ホスト ディスカバリを行い、サーバ、オペレーティング システム、脆弱性を検出する Nmap スクリプトのデフォルト セットを実行できるようにします。デフォルト スクリプトのリストについては、http://nmap.org/nsedoc/categories/default.html を参照してください。	`-sC`
Timing Template	スキャン プロセスのタイミングを選択します。選択する数値が大きいほど、スキャンは高速になり包括的ではなくなります。	**0**：`T0`（paranoid） **1**：`T1`（sneaky） **2**：`T2`（polite） **3**：`T3`（normal） **4**：`T4`（aggressive） **5**：`T5`（insane）

Nmap スキャン戦略の作成

ライセンス：FireSIGHT

アクティブ スキャンにより重要な情報が得られることがありますが、Nmap などのツールを多用すると、ネットワーク リソースに負荷がかかり、重要なホストがクラッシュすることさえあります。アクティブ スキャナを使用する際には、スキャン戦略を作成して、スキャンする必要があるホストとポートのみスキャンするようにしてください。

詳細については、次の項を参照してください。

- 「適切なスキャン ターゲットの選択」（P.43-6）
- 「スキャン対象にする適切なポートの選択」（P.43-7）
- 「ホスト ディスカバリ オプションの設定」（P.43-7）

適切なスキャン ターゲットの選択

ライセンス：FireSIGHT

Nmap を設定する際に、スキャン対象のホストを識別するスキャン ターゲットを作成できます。スキャン ターゲットには 1 つの IP アドレス、IP アドレスの CIDR ブロックまたはオクテット範囲、IP アドレス範囲、スキャンする IP アドレスまたは範囲のリスト、および 1 つ以上のホスト上のポートが含まれます。

次の方法でターゲットを指定できます。

- IPv6 ホストの場合：
- 厳密な IP アドレス（192.168.1.101 など）
- IPv4 ホストの場合：
- 厳密な IP アドレス（192.168.1.101 など）またはカンマかスペースで区切った IP アドレスのリスト
- CIDR 表記を使用した IP アドレス ブロック（たとえば、192.168.1.0/24 は、両端を含めて 192.168.1.1 から 192.168.1.254 の間の 254 個のホストをスキャンします）

  FireSIGHT システムでの CIDR 表記の使用法の詳細については、「IP アドレスの表記法」（P.1-19）を参照してください。
- オクテットの範囲アドレッシングを使用した IP アドレス範囲（たとえば、`192.168.0-255.1-254` は、`192.168.x.x` の範囲内の末尾が .0 と .255 以外のすべてのアドレスをスキャンします）
- ハイフンを使用した IP アドレス範囲（たとえば、192.168.1.1 - 192.168.1.5 は、両端を含めて 192.168.1.1 から 192.168.1.5 の間の 6 つのホストをスキャンします）
- カンマかスペースで区切ったアドレスか範囲のリスト（たとえば、`192.168.1.0/24, 194.168.1.0/24` は、両端を含めて 192.168.1.1 から 192.168.1.254 の間の 254 個のホストと、両端を含めて 194.168.1.1 から 194.168.1.254 の間の 254 個のホストをスキャンします）

理想的な Nmap スキャンのスキャン ターゲットには、システムで識別できないオペレーティング システムがあるホスト、識別されていないサーバがあるホスト、最近ネットワーク上で検出されたホストが含まれます。ネットワーク マップ内にないホストに関する Nmap 結果は、ネットワーク マップに追加できないことに注意してください。

注意　Nmap によって提供されるサーバやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままになります。Nmap を使用したホストのスキャンを計画している場合は、Nmap で提供されるオペレーティング システムやサーバのデータを最新に保つため、定期的なスキャンのスケジュールをセットアップすることもできます。詳細については、「Nmap スキャンの自動化」（P.49-5）を参照してください。ホストがネットワーク マップから削除されると、Nmap スキャン結果は破棄されることにも注意してください。また、ターゲットをスキャンする権限を持っていることを確認してください。Nmap を使用して自分や自社に属さないホストをスキャンすると違法になる場合があります。

スキャン対象にする適切なポートの選択

ライセンス：FireSIGHT

設定するスキャン ターゲットごとに、スキャン対象のポートを選択できます。各ターゲット上でスキャンする必要があるポートのセットを正確に識別するため、個々のポート番号、ポート範囲、または一連のポート番号やポート範囲を指定できます。

デフォルトでは、Nmap は 1 から 1024 までの TCP ポートをスキャンします。相関ポリシー内で応答として修復を使用する計画の場合は、相関応答をトリガーするイベントで指定されたポートのみを修復でスキャンできます。オン デマンドまたはスケジュール済みタスクとして修復を実行する場合、または Use Port From Event を使用しない場合は、その他のポート オプションを使用して、スキャンするポートを決定できます。`nmap-services` ファイルにリストされている TCP ポートのみスキャンし、その他のポート設定を無視するよう選択できます。TCP ポートの他に UDP ポートもスキャンできます。UDP ポートに対するスキャンには時間がかかることがあるので、すばやくスキャンする場合はこのオプションを使用しないように注意してください。スキャン対象として特定のポートかポート範囲を選択するには、Nmap ポート仕様シンタックスを使用してポートを識別します。

ホスト ディスカバリ オプションの設定

ライセンス：FireSIGHT

ホストに対してポート スキャンを始める前にホスト ディスカバリを実行するかどうかを決めるか、またはスキャンを計画しているすべてのホストがオンラインであると想定できます。すべてのホストをオンラインとして扱わないことを選択した場合、使用するホスト ディスカバリ方式を選択でき、必要に応じて、ホスト ディスカバリ時のスキャン対象ポートのリストをカスタマイズできます。ホスト ディスカバリ時には、リストされているポートでオペレーティング システムやサーバの情報は調査されません。特定のポートを経由する応答を使用して、ホストがアクティブで使用可能かどうかのみを判別します。ホスト ディスカバリを実行して、ホストが利用可能でなかった場合には、そのホスト上のポートは Nmap でスキャンされません。

サンプルの Nmap スキャン プロファイル

ライセンス：FireSIGHT

次のシナリオには、ご使用のネットワーク上で Nmap を使用する方法の例が示されています。

- 「例：不明なオペレーティング システムの解決」（P.43-8）
- 「例：新しいホストに対する応答」（P.43-9）

例：不明なオペレーティング システムの解決

ライセンス：FireSIGHT

システムでネットワーク上のホストのオペレーティング システムを判別できない場合、Nmap を使用してホストをアクティブ スキャンできます。Nmap は、スキャンから得られた情報を利用して、使用されている可能性のあるオペレーティング システムを評価します。次に、最高の評価のオペレーティング システムを、ホストのオペレーティング システムを識別したものとして使用します。

Nmap を使用して新しいホストにオペレーティング システムやサーバの情報を要求すると、スキャン対象のホストに対するシステムによるそのデータのモニタリングは非アクティブになります。Nmap を使用してホスト検出を実行し、システムにより不明なオペレーティング システムがあるとマークが付けられたホストのサーバ オペレーティング システムを検出すると、同種のホストのグループを識別できる場合があります。その場合、それらのホストのうちの 1 つに基づいたカスタム フィンガープリントを作成し、システムでそのフィンガープリントを、Nmap スキャンに基づいてそのホスト上で実行されていると判明したオペレーティング システムと関連付けるようにすることができます。可能な限り、Nmap などのサードパーティ製の静的データを入力するよりも、カスタム フィンガープリントを作成してください。カスタム フィンガープリントを使用すると、システムはホストのオペレーティング システムを継続してモニタし、必要に応じて更新できるからです。

Nmap を使用してオペレーティング システムを検出する方法：

アクセス：Admin/Discovery Admin

ステップ 1　Nmap モジュールのスキャン インスタンスを設定します。

詳細については、「Nmap スキャン インスタンスの作成」（P.43-10）を参照してください。

ステップ 2　次の設定を使用して Nmap 修復を作成します。

- [Use Port From Event] を有効にして、新しいサーバに関連付けられたポートをスキャンします。
- [Detect Operating System] を有効にして、ホストのオペレーティング システムの情報を検出します。
- [Probe open ports for vendor and version information] を有効にして、サーバ ベンダーとバージョン情報を検出します。
- ホストが既存であることが判明しているので、[Treat All Hosts as Online] を有効にします。

Nmap 修復の作成の詳細については、「Nmap 修復の作成」（P.43-13）を参照してください。

ステップ 3　システムで不明なオペレーティング システムがあるホストが検出されたときにトリガーされる相関ルールを作成します。

このルールは、**ディスカバリ イベントが発生**し、**ホストの OS 情報が変更**されており、**OS 名が不明**という条件が満たされている場合にトリガーされる必要があります。

相関ルールの作成の詳細については、「相関ポリシーのルールの作成」（P.39-3）を参照してください。

ステップ 4　相関ルールを組み込む相関ポリシーを作成します。

相関ポリシーの作成の詳細については、「相関ポリシーの作成」（P.39-48）を参照してください。

ステップ 5　相関ポリシー内で、ステップ 2 で応答として作成した Nmap 修復をステップ 3 で作成したルールに追加します。

ステップ 6　相関ポリシーをアクティブにします。

ステップ 7　ネットワーク マップ上のホストを消去し、強制的にネットワーク検出が再起動されてネットワーク マップが再構築されるようにします。

ステップ 8　1 日後か 2 日後に、相関ポリシーによって生成されたイベントを検索します。Nmap 結果から、ホスト上で検出されたオペレーティング システムを分析し、システムで認識されない特定のホスト設定がネットワーク上にあるかどうか調べます。

Nmap 結果の分析の詳細については、「スキャン結果の分析」（P.43-24）を参照してください。

ステップ 9　不明なオペレーティング システムがあるホストが複数検出され、Nmap 結果が同一の場合は、それらのホストの 1 つに対してカスタム フィンガープリントを作成し、将来類似のホストを識別する際に使用します。

詳細については、「クライアントのフィンガープリントの作成」（P.42-9）を参照してください。

例：新しいホストに対する応答

ライセンス：FireSIGHT

システムにより、侵入の可能性があるサブネット内で新しいホストが検出された場合、そのホストをスキャンして、そのホストの脆弱性に関する正確な情報を入手できます。

そのためには、このサブネット内に新しいホストが出現した時点で検出し、そのホスト上で Nmap スキャンを実行する修復を起動する相関ポリシーを作成してアクティブにします。

このポリシーをアクティブにした後で、修復状態の表示（[Policy & Response] > [Responses] > [Remediations] > [Status]）を定期的に検査して、修復が起動された時点を調べることができます。修復の動的なスキャン ターゲットには、サーバ検出の結果としてスキャンされたホストの IP アドレスを含める必要があります。これらのホストのホスト プロファイルを調べて、Nmap によって検出されたオペレーティング システムとサーバに基づいて、対処する必要がある脆弱性がホストにあるかどうか確認します。

注意　大規模なネットワークや動的なネットワークがある場合、新しいホストの検出は頻繁に発生するので、スキャンを使用して応答するには不向きな場合があります。リソースの過負荷を避けるために、頻繁に発生するイベントへの応答として Nmap スキャンを使用しないでください。また、Nmap を使用して新しいホストのオペレーティング システムやサーバの情報を要求すると、スキャン対象のホストに対するシスコによるそのデータのモニタリングが非アクティブになることに注意してください。

新しいホストの出現に対する応答としてスキャンする方法：

アクセス：Admin/Discovery Admin

ステップ 1　Nmap モジュールのスキャン インスタンスを設定します。

詳細については、「Nmap スキャン インスタンスの作成」（P.43-10）を参照してください。

ステップ 2　次の設定を使用して Nmap 修復を作成します。

- [Use Port From Event] を有効にして、新しいサーバに関連付けられたポートをスキャンします。
- [Detect Operating System] を有効にして、ホストのオペレーティング システムの情報を検出します。

- [Probe open ports for vendor and version information] を有効にして、サーバ ベンダーとバージョン情報を検出します。
- ホストが既存であることが判明しているので、[Treat All Hosts as Online] を有効にします。

Nmap 修復の作成の詳細については、「Nmap 修復の作成」（P.43-13）を参照してください。

ステップ 3　システムが特定のサブネット上で新しいホストを検出したときにトリガーされる相関ルールを作成します。

このルールは、**ディスカバリ イベントが発生**し、**新しいホストが検出**されたときにトリガーされる必要があります。

相関ルールの作成の詳細については、「相関ポリシーのルールの作成」（P.39-3）を参照してください。

ステップ 4　相関ルールを組み込む相関ポリシーを作成します。

相関ポリシーの作成の詳細については、「相関ポリシーの作成」（P.39-48）を参照してください。

ステップ 5　相関ポリシー内で、ステップで応答として作成した Nmap 修復を、ステップ 3 で作成したルールに追加します。

ステップ 6　相関ポリシーをアクティブにします。

ステップ 7　新しいホストが通知されたら、ホスト プロファイルを調べて Nmap スキャンの結果を確認し、ホストに適用されている脆弱性に対処します。

Nmap スキャンのセットアップ

ライセンス：FireSIGHT

Nmap を使用してスキャンするには、最初にスキャン インスタンスとスキャン修復を設定します。Nmap スキャンをスケジュールする計画の場合は、スキャン ターゲットも定義します。

詳細については、次の項を参照してください。

- 「Nmap スキャン インスタンスの作成」（P.43-10）
- 「Nmap スキャン ターゲットの作成」（P.43-11）
- 「Nmap 修復の作成」（P.43-13）

Nmap スキャン インスタンスの作成

ライセンス：FireSIGHT

脆弱性についてネットワークをスキャンするのに使用する Nmap モジュールごとに別々のスキャン インスタンスをセットアップできます。防御センター上のローカル Nmap モジュールか、リモートでスキャンを実行するために使用するデバイスに対してスキャン インスタンスをセットアップできます。各スキャンの結果は常に防御センターに保存されます。リモート デバイスからスキャンを実行する場合でも、この場所でスキャンを設定できます。ミッション クリティカルなホストへの不慮のスキャンや悪意のあるスキャンを防ぐには、インスタンスのブラックリストを作成し、そのインスタンスで決してスキャンしてはならないホストを指示できます。

既存のスキャン インスタンスと同じ名前のスキャン インスタンスを追加できないことに注意してください。

スキャン インスタンスを作成する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] を選択します。

[Scanners] ページが表示されます。

ステップ 2　[Add Nmap Instance] をクリックします。

[Instance Detail] ページが表示されます。

ステップ 3　[Instance Name] フィールドに、1 文字から 63 文字の英数字の名前を入力します。アンダースコア（_）とハイフン（-）以外の特殊文字およびスペースは使用できません。

ステップ 4　[Description] フィールドに 0 文字から 255 文字の英数字の説明を指定します。スペースや特殊文字を使用できます。

ステップ 5　オプションで、[Black Listed Scan hosts] フィールドで、このスキャン インスタンスがスキャン*しない*ホストまたはネットワークを指定します。

- IPv6 ホストの場合、厳密な IP アドレス（`2001:DB8::fedd:eeff` など）
- IPv4 ホストの場合、厳密な IP アドレス（`192.168.1.101` など）または CIDR 表記を使用した IP アドレス ブロック（たとえば、`192.168.1.0/24` は、両端を含めて `192.168.1.1` から `192.168.1.254` の間の 254 個のホストをスキャンします）
- 感嘆符（!）を使用してアドレス値の否定はできないことに注意してください。

ブラックリストに含まれるネットワーク内のホストをスキャン対象として特定すると、スキャンは実行されません。

ステップ 6　オプションで、防御センターの代わりにリモート デバイスからスキャンを実行するには、そのデバイスの IP アドレスか名前を指定します。この情報は、防御センター Web インターフェイス内のそのデバイスに関する [Information] ページの [Remote Device Name] フィールドに表示されます。

ステップ 7　[Create] をクリックします。

スキャン インスタンスが作成されます。

Nmap スキャン ターゲットの作成

ライセンス：FireSIGHT

特定のホストとポートを識別するスキャン ターゲットを作成して保存できます。その後、オンデマンド スキャンを実行するかスキャンをスケジュールする際に、保存済みのスキャン ターゲットの 1 つを使用できます。

IPv4 アドレスのターゲットをスキャンする場合、1 つの IP アドレス、IP アドレスのリスト、CIDR 表記、または Nmap スキャンのオクテットを使用して、スキャンするホストを選択できます。ハイフンを使用して、アドレスの範囲を指定することもできます。カンマかスペースを使用して、リスト内のアドレスや範囲を区切ります。

IPv6 アドレスのスキャンの場合、1 つの IP アドレスを使用します。範囲指定は入力できません。

Nmap で提供されるサーバやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままであることに注意してください。Nmap を使用したホストのスキャンを計画している場合は、Nmap で提供されるオペレーティング システムやサーバのデータを最新に保つため、定期的なスキャンのスケジュールをセットアップすることもできます。詳細については、「Nmap スキャンの自動化」（P.49-5）を参照してください。ホストがネットワーク マップから削除されると、そのホストに関する Nmap スキャン結果は破棄されることにも注意してください。

スキャン ターゲットを作成する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] を選択します。

[Scanners] ページが表示されます。

ステップ 2　ツールバーで、[Targets] をクリックします。

[Scan Target List] ページが表示されます。

ステップ 3　[Create Scan Target] をクリックします。

[Scan Target] ページが表示されます。

ステップ 4　[Name] フィールドに、このスキャン ターゲットに使用する名前を入力します。

ステップ 5　[IP Range] テキスト ボックスで、次のシンタックスを使用して、スキャンする 1 つ以上のホストを指定します。

- IPv6 ホストの場合、厳密な IP アドレス（`2001:DB8::fedd:eeff` など）
- IPv4 ホストの場合、厳密な IP アドレス（`192.168.1.101` など）または IP アドレスのカンマ区切りリスト
- IPv4 ホストの場合、CIDR 表記を使用した IP アドレス ブロック（たとえば、`192.168.1.0/24` は、両端を含めて 192.168.1.1 から 192.168.1.254 の間の 254 個のホストをスキャンします）

  FireSIGHT システムでの CIDR 表記の使用法の詳細については、「IP アドレスの表記法」（P.1-19）を参照してください。
- IPv4 ホストの場合、オクテットの範囲アドレッシングを使用した IP アドレス範囲（たとえば、`192.168.0-255.1-254`は、`192.168.x.x` の範囲内の末尾が .0 と .255 以外のすべてのアドレスをスキャンします）
- IPv4 ホストの場合、ハイフンを使用した IP アドレス範囲（たとえば、`192.168.1.1-192.168.1.5` は、両端を含めて 192.168.1.1 から 192.168.1.5 の間の 6 つのホストをスキャンします）
- IPv4 ホストの場合、カンマかスペースで区切ったアドレスまたは範囲のリスト（たとえば、`192.168.1.0/24, 194.168.1.0/24` は、両端を含めて 192.168.1.1 から 192.168.1.254 の間の 254 個のホストと、両端を含めて 194.168.1.1 から 194.168.1.254 の間の 254 個のホストをスキャンします）

注　[IP Range] テキスト ボックスには最大 255 文字まで入力できます。また、スキャン ターゲット内の IP アドレスか範囲のリストでカンマを使用した場合、ターゲットを保存する際にカンマはスペースに変換されるので注意してください。

ステップ 6　[Ports] フィールドで、スキャンするポートを指定します。

1 から 65535 までの値を使用して、次のいずれかを入力できます。

- 1 つのポート番号
- カンマで区切ったポートのリスト
- ハイフンで区切ったポート番号の範囲
- ハイフンで区切ったポート番号の複数の範囲をカンマで区切ったもの

ステップ 7　[Save] をクリックします。

スキャン ターゲットが作成されます。

Nmap 修復の作成

ライセンス：FireSIGHT

Nmap 修復を作成して、Nmap スキャンの設定を定義できます。Nmap 修復は、相関ポリシー内で応答として使用したり、オン デマンドで実行したり、特定の時間に実行するようにスケジュールしたりできます。Nmap スキャンの結果をネットワーク マップ内に表示するには、スキャン対象のホストがネットワーク マップ内にすでに存在していなければなりません。

Nmap 修復の具体的な設定について詳しくは、「Nmap 修復の概要」（P.43-2）を参照してください。

Nmap で提供されるサーバやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままであることに注意してください。Nmap を使用してホスト内でオペレーティング システムやサーバのデータをスキャンすることを計画している場合は、定期的なスキャンのスケジュールをセットアップして、Nmap によって提供されるオペレーティング システムやサーバのデータを最新に保つこともできます。詳細については、「Nmap スキャンの自動化」（P.49-5）を参照してください。ホストがネットワーク マップから削除されると、そのホストに関する Nmap スキャン結果は破棄されることにも注意してください。

Nmap の機能に関する一般情報については、http://insecure.org にある Nmap のマニュアルを参照してください。

Nmap 修復を作成する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] を選択します。

[Scanners] ページが表示されます。

ステップ 2　修復を追加するスキャン インスタンスの隣の [Add Remediation] をクリックします。

[Edit Remediation] ページが表示されます。

ステップ 3　[Remediation Name] フィールドに、1 文字から 63 文字の英数字を使用して修復の名前を入力します。アンダースコア（_）とハイフン（-）以外の特殊文字およびスペースは使用できません。

ステップ 4　[Description] フィールドに、0 文字から 255 文字の英数字を使用して修復の説明を入力します。スペースや特殊文字を使用できます。

ステップ 5　侵入イベント、接続イベント、またはユーザ イベントに対してトリガーする相関ルールへの応答としてこの修復を使用する計画の場合は、[Scan Which Address(es) From Event?] オプションを設定します。

- イベントの送信元 IP アドレスと宛先 IP アドレスによって表されるホストをスキャンするには、[Scan Source and Destination Addresses] を選択します。
- イベントの送信元 IP アドレスによって表されるホストをスキャンするには、[Scan Source Address Only] を選択します。
- イベントの宛先 IP アドレスによって表されるホストをスキャンするには、[Scan Destination Address Only] を選択します。

ディスカバリ イベントまたはホスト入力イベントに対してトリガーする相関ルールへの応答としてこの修復を使用する計画の場合は、デフォルトでそのイベントに関連するホストの IP アドレスが修復によってスキャンされます。このオプションを設定する必要はありません。

注　トラフィック プロファイルの変更に対してトリガーする相関ルールへの応答として Nmap 修復を割り当て**ないでください**。

ステップ 6　以下のように [Scan Type] オプションを設定します。

- TCP 接続を開始して完了していない状態で、`admin` アカウントが raw パケット アクセス権を持つホストや IPv6 が実行されていないホスト上でステルス モードですばやくスキャンするには、[TCP Syn Scan] を選択します。
- システム コール `connect()`（防御センター上の `admin` アカウントが raw パケット アクセス権を持っていないホストや IPv6 が実行されているホスト上で使用できる）を使用してスキャンするには、[TCP Connect Scan] を選択します。
- ACK パケット送信して、ポートがフィルタ処理されているかどうか検査するには、[TCP ACK Scan] を選択します。
- ACK パケットを送信して、ポートがフィルタ処理されているかどうか検査し、ポートが開いているか閉じているかも判別するには、[TCP Window Scan] を選択します。
- FIN/ACK プローブを使用して BSD 派生システムを識別するには、[TCP Maimon Scan] を選択します。

ステップ 7　オプションで、TCP ポートに加えて UDP ポートをスキャンするには、[Scan for UDP ports] オプションで [On] を選択します。

ヒント　UDP ポートスキャンは TCP ポートスキャンよりも時間がかかります。スキャン時間を短縮するには、このオプションを無効のままにします。

ステップ 8　相関ポリシー違反への応答としてこの修復を使用する計画の場合は、[Use Port From Event] を以下のように設定します。

- 相関イベント内のポートをスキャンし、ステップ 11 で指定するポートをスキャンしない場合は、[On] を選択します。

  相関イベント内のポートをスキャンする場合は、ステップ 5 で指定した IP アドレス上のポートが修復によりスキャンされることに注意してください。これらのポートも修復の動的スキャンのターゲットに追加されます。
- ステップ 11 で指定するポートのみスキャンするには、[Off] を選択します。

ステップ 9　相関ポリシー違反への応答としてこの修復を使用する計画で、イベントを検出した検出エンジンを実行しているアプライアンスを使用してスキャンを実行するには、[Scan from reporting detection engine] オプションを以下のように設定します。

- レポート検出エンジンを実行しているアプライアンスからスキャンするには、[On] を選択します。
- 修復内で設定されているアプライアンスからスキャンするには、[Off] を選択します。

ステップ 10　[Fast Port Scan] オプションを以下のように設定します。

- スキャン元デバイス上の `/var/sf/nmap/share/nmap/nmap-services` ディレクトリ内の `nmap-services` ファイルにリストされているポートのみスキャンし、その他のポート設定を無視するには、[On] を選択します。
- すべての TCP ポートをスキャンするには、[Off] を選択します。

ステップ 11　[Port Ranges and Scan Order] フィールドで、Nmap のシンタックスを使用して、デフォルトでスキャンするポートを、スキャンする順序で入力します。

1 から 65535 までの値を指定します。ポートを区切るには、カンマかスペースを使用します。ハイフンを使用してポートの範囲を指示することもできます。TCP ポートと UDP ポートの両方ともスキャンする場合は、スキャン対象の TCP ポートのリストの先頭に T を挿入し、UDP ポートのリストの先頭に U を挿入します。たとえば、UDP トラフィックのポート 53 と 111 をスキャンしてから、TCP トラフィックのポート 21 から 25 までスキャンするには、`U:53,111,T:21-25` と入力します。

ステップ 8 で説明されているように、相関ポリシー違反への応答として修復が起動する場合には、[Use Port From Event] オプションによりこの設定が上書きされることに注意してください。

ステップ 12　オープン ポートでサーバ ベンダーとバージョン情報を調査するには、[Probe open ports for vendor and version information] を以下のように設定します。

- ホスト上のオープン ポートでサーバ情報をスキャンして、サーバ ベンダーとバージョンを識別するには、[On] を選択します。
- ホストに関するシスコのサーバ情報を使い続ける場合は、[Off] を選択します。

ステップ 13　オープン ポートの調査を選択する場合は、[Service Version Intensity] ドロップダウン リストから数値を選択して、使用するプローブの数を設定します。

- 選択する数値が大きいほど使用するプローブの数が増えるので、スキャンは長時間になり精度が上がります。
- 選択する数値が小さいほど、使用するプローブの数が減るので、スキャンは高速になり精度が下がります。

ステップ 14　オペレーティング システム情報をスキャンするには、[Detect Operating System] を以下のように設定します。

- ホストに対してオペレーティング システムを識別する情報をスキャンするには、[On] を選択します。
- ホストに関するシスコのオペレーティング システム情報を使い続ける場合は、[Off] を選択します。

ステップ 15　ホスト ディスカバリが行われるかどうか、およびポートのスキャンが使用可能なホストのみに対して実行されるかどうかを決めるには、[Treat All Hosts As Online] を以下のように設定します。

- ホスト ディスカバリ プロセスを省略し、ターゲット範囲内のすべてのホスト上でのポート スキャンを実行するには、[On] を選択します。
- [Host Discovery Method] と [Host Discovery Port List] の設定を使用してホスト ディスカバリを実行し、使用不能なホスト上でのポート スキャンを省略するには、[Off] を選択します。

ステップ 16　Nmap でホストの可用性をテストする場合に使用する方式を以下のように選択します。

- SYN フラグが設定された空の TCP パケットを送信し、使用可能なホスト上のクローズ ポート上の RST 応答かオープン ポート上の SYN/ACK 応答を引き起こすには、[TCP SYN] を選択します。

  このオプションはデフォルトでポート 80 をスキャンすることと、TCP SYN スキャンはステートフル ファイアウォール ルールが指定されたファイアウォールでブロックされる可能性が低いことに注意してください。

- ACK フラグが設定された空の TCP パケットを送信し、使用可能なホスト上の RST 応答を引き起こすには、[TCP ACK] を選択します。

  このオプションはデフォルトでポート 80 をスキャンすることと、TCP ACK スキャンはステートレス ファイアウォール ルールが指定されたファイアウォールでブロックされる可能性が低いことに注意してください。

- UDP パケットを送信し、使用可能なホスト上のクローズ ポートからのポート到達不能応答を引き起こすには、[UDP] を選択します。このオプションは、デフォルトでポート 40125 をスキャンします。

ステップ 17　ホスト ディスカバリ時にポートのカスタム リストをスキャンする場合は、選択したホスト ディスカバリ方式に該当するポートのリストを、[Host Discovery Port List] フィールドにカンマで区切って入力します

ステップ 18　ホスト ディスカバリを行い、サーバ、オペレーティング システム、脆弱性 のディスカバリを行う Nmap スクリプトのデフォルト セットを使用するかどうかを制御するには、[Default NSE Scripts] オプションを以下のように設定します。

- Nmap スクリプトのデフォルト セットを実行するには、[On] を選択します。
- Nmap スクリプトのデフォルト セットを省略するには、[Off] を選択します。

デフォルト スクリプトのリストについては、http://nmap.org/nsedoc/categories/default.html を参照してください。

ステップ 19　スキャン プロセスのタイミングを設定するには、タイミングのテンプレート番号を選択します。選択する数値が大きいほどスキャンは高速で幅が狭くなり、小さいほどスキャンは低速で包括的になります。

ステップ 20　[Save] をクリックし、[Done] をクリックします。

修復が作成されます。

Nmap スキャンの管理

ライセンス：FireSIGHT

必要に応じて、Nmap スキャン インスタンスや修復を変更したり削除したりできます。オンデマンドの Nmap スキャンを実行することもできます。以前のスキャンに関する Nmap 結果を表示したりダウンロードしたりすることもできます。詳細については、次の項を参照してください。

- 「Nmap スキャン インスタンスの管理」（P.43-17）
- 「Nmap 修復の管理」（P.43-18）
- 「オンデマンド Nmap スキャンの実行」（P.43-19）

Nmap スキャン インスタンスの管理

ライセンス：FireSIGHT

Nmap スキャン インスタンスを編集したり削除したりできます。詳細については、次の項を参照してください。

- 「Nmap スキャン インスタンスの編集」（P.43-17）
- 「Nmap スキャン インスタンスの削除」（P.43-17）

Nmap スキャン インスタンスの編集

ライセンス：FireSIGHT

スキャン インスタンスを変更するには、次の手順を使用します。インスタンスを変更する際に、そのインスタンスに関連付けられた修復を表示、追加、削除できることに注意してください。

スキャン インスタンスを編集する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] を選択します。

[Scanners] ページが表示されます。

ステップ 2　編集するインスタンスの横にある [View] をクリックします。

[Instance Detail] ページが表示されます。

ステップ 3　オプションで、表示または編集する修復の横にある [View] をクリックします。

修復の編集の詳細については、「Nmap 修復の編集」（P.43-18）を参照してください。

ステップ 4　オプションで、削除する修復の横にある [Delete] をクリックします。

修復の削除の詳細については、「Nmap 修復の削除」（P.43-19）を参照してください。

ステップ 5　オプションで、[Add] をクリックして、このスキャン インスタンスに新しい修復を追加します。

新しい修復の作成の詳細については、「Nmap 修復の管理」（P.43-18）を参照してください。

ステップ 6　オプションで、スキャン インスタンスの設定に変更を加えてから、[Save] をクリックします。

ステップ 7　**[Done]** をクリックします。

スキャン インスタンスが変更されます。

Nmap スキャン インスタンスの削除

ライセンス：FireSIGHT

インスタンス内でプロファイルが作成された Nmap モジュールを使用しなくなった場合には、Nmap スキャン インスタンスを削除します。スキャン インスタンスを削除すると、そのインスタンスを使用する修復も削除されることに注意してください。

スキャン インスタンスを削除する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] をクリックします。

[Scanners] ページが表示されます。

ステップ 2　削除するスキャン インスタンスの横にある [Delete] をクリックします。

インスタンスが削除されます。

Nmap 修復の管理

ライセンス：FireSIGHT

Nmap 修復を編集したり削除したりできます。詳細については、次の項を参照してください。

- 「Nmap 修復の編集」（P.43-18）
- 「Nmap 修復の削除」（P.43-19）

Nmap 修復の編集

ライセンス：FireSIGHT

Nmap 修復に加えた変更は、進行中のスキャンには影響しません。新しい設定は、次回スキャンが開始されたときに有効になります。

Nmap 修復を編集する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] を選択します。

[Scanners] ページが表示されます。

ステップ 2　編集する修復の横にある [View] をクリックします。

[Remediation Edit] ページが表示されます。

ステップ 3　必要に応じて変更を加えます。

変更できる設定については、「Nmap 修復の作成」（P.43-13）を参照してください。

ステップ 4　[Save] をクリックし、[Done] をクリックします。

修復が変更されます。

Nmap 修復の削除

ライセンス：FireSIGHT

Nmap 修復が不要になったら削除します。

Nmap 修復を削除する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] を選択します。

[Scanners] ページが表示されます。

ステップ 2　削除する修復の横にある [Delete] をクリックします。

ステップ 3　修復を削除することを確認します。

修復が削除されます。

オンデマンド Nmap スキャンの実行

ライセンス：FireSIGHT

必要なときにいつでもオンデマンド Nmap スキャンを起動できます。スキャンする IP アドレスとポートを入力するか、既存のスキャン ターゲットを選択して、オンデマンド スキャンのターゲットを指定できます。

Nmap で提供されるサーバやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままであることに注意してください。Nmap を使用したホストのスキャンを計画している場合は、Nmap で提供されるオペレーティング システムやサーバのデータを最新に保つため、定期的なスキャンのスケジュールをセットアップすることもできます。詳細については、「Nmap スキャンの自動化」（P.49-5）を参照してください。また、ホストがネットワーク マップから削除されると、Nmap スキャン結果は破棄されることにも注意してください。

オンデマンド Nmap スキャンを実行する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] を選択します。

[Scanners] ページが表示されます。

ステップ 2　スキャンの実行時に使用する Nmap 修復の横にある [Scan] をクリックします。

[Nmap Scan Target] ダイアログ ボックスが表示されます。

ステップ 3　オプションで、保存済みのスキャン ターゲットを使用してスキャンするには、[Saved Targets] ドロップダウン リストからターゲットを選択して、[Load] をクリックします。

スキャン ターゲットに関連付けられた IP アドレスおよびポートが、[IP Range(s)] フィールドと [Ports] フィールドに入力されます。

ヒント　スキャン ターゲットを作成するには、[Edit/Add Targets] をクリックします。詳細については、「Nmap スキャン ターゲットの作成」（P.43-11）を参照してください。

ステップ 4　[IP Range(s)] フィールドで、最大 255 文字までで、スキャンするホストの IP アドレスを指定するかロードされたリストを変更します。

IPv4 アドレスのホストの場合、複数の IP アドレスをカンマで区切って指定するか、CIDR 表記を使用できます。感嘆符（!）を前に挿入して IP アドレスを否定することもできます。FireSIGHT システムでの CIDR 表記の使用法の詳細については、「IP アドレスの表記法」（P.1-19）を参照してください。

IPv6 アドレスのホストの場合、厳密な IP アドレスを使用します。範囲指定は入力できません。

ステップ 5　[Ports] フィールドで、スキャンするポートを指定するか、ロードされたリストを変更します。

ポート番号、カンマで区切ったポートのリスト、ハイフンで区切ったポート番号の範囲を入力できます。ポートの入力の詳細については、「検索でのポートの指定」（P.45-7）を参照してください。

ステップ 6　[Scan Now] をクリックします。

Nmap サーバがスキャンを実行します。

Nmap は IP アドレスの範囲を検証し、範囲が無効な場合はエラー メッセージを表示することに注意してください。表示された場合は、[IP Range(s)] フィールドの内容を訂正し、有効な IP アドレス範囲を指定してください。

スキャン ターゲットの管理

ライセンス：FireSIGHT

Nmap モジュールを設定する際にスキャン ターゲットを作成して保存できます。スキャン ターゲットは、オンデマンドまたはスケジュール済みのスキャンの実行時にターゲットにするホストとポートを識別します。これにより、毎回新しいスキャン ターゲットを作成する必要がなくなります。スキャン ターゲットには、スキャンする 1 つの IP アドレスか IP アドレスのブロック、および 1 つ以上のホスト上のポートが含まれます。Nmap ターゲットの場合、Nmap オクテット範囲のアドレッシングや IP アドレスの範囲も使用できます。Nmap オクテットの範囲アドレッシングの詳細については、http://insecure.org にある Nmap のマニュアルを参照してください。

スキャン ターゲットに多数のホストが含まれている場合、スキャンに要する時間が延びる場合があることに注意してください。回避策として、一度にスキャンするホストを減らしてください。

スキャン ターゲットの作成後に変更または削除できます。

詳細については、次の項を参照してください。

- 「Nmap スキャン ターゲットの作成」（P.43-11）
- 「スキャン ターゲットの編集」（P.43-21）
- 「スキャン ターゲットの削除」（P.43-21）

スキャン ターゲットの編集

ライセンス：FireSIGHT

作成したスキャン ターゲットを変更できます。

ヒント　修復を使用して特定の IP アドレスをスキャンするつもりがないのに、修復を起動した相関ポリシー違反にホストが関係していたためにその IP アドレスがターゲットに追加された場合は、修復の動的スキャン ターゲットを編集できます。

既存のスキャン ターゲットを編集する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] を選択します。

[Scanners] ページが表示されます。

ステップ 2　ツールバーで、[Targets] をクリックします。

[Scan Target List] ページが表示されます。

ステップ 3　編集するスキャン ターゲットの横にある [Edit] をクリックします。

[Scan Target] ページが表示されます。

ステップ 4　必要に応じて変更を加え、[Save] をクリックします。

スキャン ターゲットが更新されます。

スキャン ターゲットの削除

ライセンス：FireSIGHT

スキャン ターゲットにリストされているホストをスキャンする必要がなくなった場合は、そのスキャン ターゲットを削除します。

スキャン ターゲットを削除する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] を選択します。

[Scanners] ページが表示されます。

ステップ 2　ツールバーで、[Targets] をクリックします。

[Scan Target List] ページが表示されます。

ステップ 3　削除するスキャン ターゲットの横にある [Delete] をクリックします。

スキャン ターゲットが削除されます。

アクティブ スキャンの結果での作業

ライセンス：FireSIGHT

進行中の Nmap スキャンをモニタする方法、FireSIGHT システムで以前に実行したスキャンからの結果か FireSIGHT システム以外で実行した結果をインポートする方法、およびスキャン結果を表示して分析する方法については、次の項を参照してください。

スキャン結果の表示

ライセンス：FireSIGHT

スキャン結果のテーブルを表示してから、探している情報に応じてイベント表示を操作できます。

スキャン結果にアクセスすると表示されるページは、使用するワークフローに応じて異なります。定義済みのワークフローを使用できます。このワークフローにはスキャン結果のテーブル ビューが含まれます。

特定の必要に合致する情報だけが表示されるカスタム ワークフローを作成することもできます。カスタム ワークフローの作成の詳細については、「カスタム ワークフローの作成」（P.47-45）を参照してください。

次の表で、スキャン結果ワークフローのページで実行できる特定のアクションの一部について説明します。

表 43-2　　スキャン結果テーブルの機能

目的	操作
表の列の内容に関する詳細の参照	詳細については、「スキャン結果テーブルについて」（P.43-24）を参照してください。
スキャン結果の日時範囲の変更	時間範囲のリンクをクリックします。詳細については、「イベント時間の制約の設定」（P.47-27）を参照してください。
スキャン結果のソート	列のタイトルをクリックします。列のタイトルを再度クリックすると、ソート順序が逆になります。
表示される列の制約	非表示にする列見出しのクローズ アイコン（ ✖ ）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、[Apply] をクリックします。 **ヒント**　その他の列を表示するには該当するチェック ボックスを選択し、非表示にするにはクリアしてから、[Apply] をクリックします。無効にした列を再度表示するには、 展開矢印（ ▶ ）をクリックして検索制約を展開してから、[Disabled Columns] の下の列名をクリックします。

表 43-2　スキャン結果テーブルの機能 （続き）

目的	操作
特定の値を制約しながらのワークフロー内の次のページへのドリルダウン	次のいずれかの方法を使用します。 • カスタム ワークフロー内に作成したドリルダウン ページで、行内の値をクリックします。テーブル ビューの行の値をクリックすると、テーブル ビューは制約され、次のページにドリルダウン**しない**ことに注意してください。 • 一部のユーザを制約して次のワークフロー ページにドリルダウンするには、次のワークフローのページで表示するユーザの横のチェック ボックスを選択し、[View] をクリックします。 • 現在の制約を保持しながら次のワークフロー ページにドリルダウンするには、[View All] をクリックします。 **ヒント**　テーブル ビューのページ名には必ず「Table View」が含まれます。 詳細については、「イベントの制約」（P.47-36）を参照してください。
スキャン インスタンスと修復の設定	ツールバーの [Scanners] をクリックします。 詳細については、「Nmap スキャンのセットアップ」（P.43-10）を参照してください。
ワークフローのページ内やページ間の移動	詳細については、「ワークフローのページの使用」（P.47-21）を参照してください。
他のイベント ビューに移動して、関連イベントを確認する	表示するイベント ビューの名前を [Jump to] ドロップダウン リストから選択します。詳細については、「ワークフロー間のナビゲート」（P.47-41）を参照してください。
スキャン結果の検索	[Search] をクリックします。詳細については、「スキャン結果の検索」（P.43-26）を参照してください。

スキャン結果を表示する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] を選択します。

ステップ 2　[Scan Results] をクリックします。

デフォルトのスキャン結果ワークフローの先頭ページが表示されます。カスタム ワークフローなどの別のワークフローを使用するには、ワークフローのタイトルの付近の [(switch workflows)] をクリックします。別のデフォルト ワークフローの指定方法については、「イベント ビュー設定の設定」（P.58-3）を参照してください。

スキャン結果テーブルについて

ライセンス：FireSIGHT

Nmap スキャンを実行すると、防御センターでデータベース内のスキャン結果が収集されます。スキャン結果テーブルのフィールドについて、以下の表で説明します。

表 43-3　スキャン結果のフィールド

フィールド	説明
Start Time	この結果を作成したスキャンの開始日時。
End Time	この結果を作成したスキャンの終了日時。
Scan Target	この結果を作成したスキャンのスキャン ターゲットの IP アドレス（DNS 解決が有効になっている場合はホスト名）。
Scan Type	この結果を作成したスキャンのタイプを示す、Nmap またはサードパーティのスキャナ名。
Scan Mode	この結果を作成したスキャンのモード： • On Demand：オン デマンドで実行されたスキャンからの結果。 • Imported：別のシステムでスキャンされて防御センターにインポートされた結果 • Scheduled：スケジュール済みタスクとして実行されたスキャンからの結果。

スキャン結果の分析

ライセンス：FireSIGHT

ローカル Nmap モジュールを使用して作成したスキャン結果を、レンダリングされたページとしてポップアップ ウィンドウで表示できます。Nmap 結果ファイルを raw XML 形式でダウンロードすることもできます。

Nmap によって検出されたオペレーティング システムやサーバの情報を、ホスト プロファイルやネットワーク マップ内で参照することもできます。ホストのスキャンが生成するサーバ情報がフィルタ除去されているかクローズ状態のポートのサーバに関する情報の場合、または、スキャンが収集した情報がオペレーティング システム情報やサーバのセクションに含めることができない情報の場合、それらの結果は、ホスト プロファイルの Nmap Scan Results セクションに含められます。詳細については、「ホスト プロファイルの表示」（P.37-5）を参照してください。

スキャンのモニタリング

ライセンス：FireSIGHT

Nmap スキャンの進行状況を検査し、現在進行中のスキャン ジョブをキャンセルできます。スキャン結果には各スキャンの開始時刻と終了時刻が示されます。またスキャンの完了後に、スキャン結果をレンダリングされたページとしてポップアップ ウィンドウで表示することもできます。Nmap は、http://insecure.org で入手できる Nmap バージョン 1.01 DTD を使用して、ダウンロードして表示できる結果を生成します。スキャン結果をクリアすることもできます。

スキャンをモニタする方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] を選択します。

ステップ 2　[Scan Results] をクリックします。

デフォルトのスキャン結果ワークフローの先頭ページが表示されます。カスタム ワークフローなどの別のワークフローを使用するには、ワークフローのタイトルの付近の [(switch workflows)] をクリックします。別のデフォルト ワークフローの指定方法については、「イベント ビュー設定の設定」（P.58-3）を参照してください。

ヒント　スキャン結果のテーブル ビューが含まれていないカスタム ワークフローを使用している場合、ワークフローのタイトル付近の [(switch workflows)] をクリックしてから、[Scan Results] を選択します。

ステップ 3　次の操作を実行できます。

- スキャン結果をレンダリングされたページとしてポップアップ ウィンドウで表示するには、スキャン ジョブの横にある [View] をクリックします。
- テキスト エディタで raw XML コードを表示できるようにスキャン結果ファイルのコピーを保存するには、スキャン ジョブの横の [Download] をクリックします。

スキャン結果のインポート

ライセンス：FireSIGHT

FireSIGHT システムの外部で実行された Nmap スキャンによって作成された XML 結果ファイルをインポートできます。以前に FireSIGHT システムからダウンロードした XML 結果ファイルもインポートできます。Nmap スキャン結果をインポートするには、結果ファイルは XML 形式で、Nmap バージョン 1.01 DTD に準拠している必要があります。Nmap 結果の作成と Nmap DTD の詳細については、http://insecure.org にある Nmap のマニュアルを参照してください。FireSIGHT システムからの XML 結果のダウンロードの詳細については、「スキャンのモニタリング」（P.43-24）を参照してください。

Nmap がホスト プロファイルに結果を追加できるようにするには、その前にホストがネットワーク マップ内になければならないことに注意してください。

結果をインポートする方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Scanners] を選択します。

[Scan Instances] ページが表示されます。

ステップ 2　ツールバーで、[Import Results] をクリックします。

[Import Results] ページが表示されます。

ステップ 3　[Browse] をクリックし、結果ファイルに移動します。

ステップ 4　[Import Results] ページに戻ったら、[Import] をクリックして結果をインポートします。

結果ファイルがインポートされます。

スキャン結果の検索

ライセンス：FireSIGHT

FireSIGHT システム内のアプライアンスや管理対象アプライアンスで実行した Nmap またはサードパーティのスキャン結果を検索できます。

表 43-4　スキャン結果の検索条件

フィールド	検索条件ルール
Start Time	この結果を作成したスキャンの開始日時を入力します。 時間入力の構文については、「検索での時間制約の指定」（P.45-5）を参照してください。
End Time	この結果を作成したスキャンの終了日時を入力します。 時間入力の構文については、「検索での時間制約の指定」（P.45-5）を参照してください。
Scan Target	この結果を作成したスキャンのスキャン ターゲットの IP アドレス（DNS 解決が有効になっている場合はホスト名）を入力します。 IP アドレスの範囲を指定するには、特定の IP アドレスか CIDR 表記を使用します。IP アドレスに使用できるシンタックスの完全な説明については、「検索での IP アドレスの指定」（P.45-6）を参照してください。
Scan Type	この結果を作成したスキャンのタイプを示す、`Nmap` またはサードパーティのスキャナ ID を入力します。
Scan Mode	この結果を作成したスキャンのモードを以下のように入力します。 • オン デマンドで実行されたスキャンからの結果を取得するには、`On Demand` と入力します。 • 別のシステムでスキャンされて防御センターにインポートされた結果を取得するには、`Imported` と入力します。 • スケジュール済みタスクとして実行されたスキャンからの結果を取得するには、`Scheduled` と入力します。

保存済み検索のロードおよび削除方法を含む、検索の詳細については、「イベントの検索」（P.45-1）を参照してください。

スキャン結果を検索する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Analysis] > [Search] を選択してから、[Table] ドロップダウン リストから [Scan Results] を選択します。

[Scan Results] 検索ページが表示されます。

ヒント　データベース内で別の種類のイベントを検索するには、[Table] ドロップダウン リストから選択します。

ステップ 2　オプションで、検索を保存する場合は、[Name] フィールドに検索の名前を入力します。

名前を入力しないと、検索を保存する際に防御センターにより自動的に名前が付けられます。

ステップ 3　「スキャン結果の検索条件」の表で説明されているとおりに、該当するフィールドに検索条件を入力します。複数の条件を入力すると、すべての条件に一致するレコードだけが防御センターにより戻されます。

ステップ 4　他のユーザがアクセスできるように検索を保存する場合は、[Save As Private] チェック ボックスをクリアします。それ以外の場合は、このチェック ボックスを選択された状態のままにして、自分だけ使用できるように検索を保存します。

ヒント　制限された特権を持つカスタム ユーザ ロール（または 4.10.1 より前のバージョンから変換された Restricted Event Analysts）に対する制限として検索を保存する場合は、プライベート検索として保存する**必要があります**。

ステップ 5　次の選択肢があります。

- 検索を開始するには、[Search] をクリックします。

  検索結果が表示されます。
- 既存の検索を変更している場合に変更内容を保存するには、[Save] をクリックします。

ステップ 6　[Save as New Search] をクリックすると、検索条件が保存されます。検索が保存され（[Save As Private] を選択した場合はユーザ アカウントに関連付けられ）、後で実行できるようになります。