



## 第 1 章 STM タスク フローの概要

この章では、MARS を Security Threat Mitigation (STM) システムとしてネットワークに配置する場合に従う必要があるプロジェクトフェーズおよびタスク フローについて説明します。ただし、その前に、セキュリティ対策を実施可能にする一連のポリシーを作成する必要があります。

セキュリティ ポリシーでは、次の事項を決定する必要があります。

- ・ ユーザが属する組織のセキュリティ目標
- ・ 保護するリソース
- ・ 最新のマップおよびインベントリを含むネットワーク インフラストラクチャ
- ・ より多くの保護を必要とする重要なリソース(研究開発、財務、人事など)

モニタリング ポリシーでは、次の事項を決定する必要があります。

- ・ ユーザ、送信元、宛先、サービス、稼働時間を含む、ネットワーク上の管理トラフィック フローの予測量
- ・ ユーザ、送信元、宛先、サービス、稼働時間を含む、セキュリティ プローブおよび脆弱性テストのためのネットワーク トラフィックの予測量
- ・ 「ネットワーク プロキシミティ」から重要なリソースに監査データを配信できるネットワーク インフラストラクチャ
- ・ ネットワーク インフラストラクチャ内のデバイスおよびホストで使用可能なさまざまなイベント ログイング レベル
- ・ 調査に使用するデバイスおよび技術

軽減ポリシーでは、次の事項を決定する必要があります。

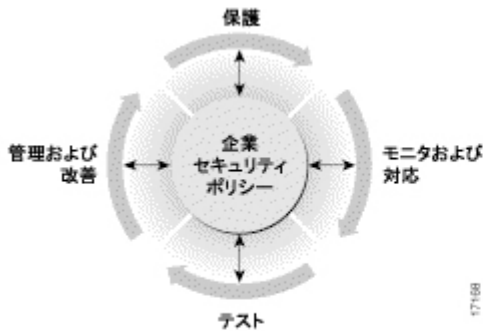
- ・ 重要なリソースに対するネットワーク上のチョーク ポイント
- ・ レイヤ 2 およびレイヤ 3 デバイスで軽減された攻撃を記述するためのプロセスの定義
- ・ ホストおよびアプリケーション レイヤで軽減された攻撃を記述するためのプロセスの定義
- ・ ネットワーク運用、セキュリティ運用、ホスト所有者、および共有ホストのアプリケーション所有者など、企業の所有権に関する問題の解決
- ・ セキュリティ対策チームおよび復旧チームに通知するためのポリシー
- ・ IOS IPS Dynamic Attack Mitigation (DAM) など、ベンダー検出ツールのプライオリティ付けのプロセス
- ・ 検出された攻撃のブロック方法(一時的あるいは永久的にブロックするのか、MARS で生成された規則を使用するのか、セキュリティ運用チームが定義したカスタム規則を使用するのか、など)

復旧ポリシーでは、次の事項を決定する必要があります。

- ・ ネットワーク内のノード タイプごとの、検出されたにもかかわらず軽減されていない攻撃への対応方法
- ・ ホストおよびアプリケーションを適切に復旧するためのツール ベンダー更新ポリシー
- ・ 復旧オプションを使用できない、感染したレガシー ホストを隔離するためのポリシーおよび手順。これらの手順には、バックアップからの復元またはネットワークの隔離が含まれることがあります。

作成したポリシーは、シスコ セキュリティ ホイールのハブになります(図 1-1)。

図 1-1 シスコ セキュリティ ホイール



ネットワーク セキュリティを表すシスコ セキュリティ ホイールのスポークは、次の 4 つのステップで構成される連続したプロセスです。

1. システムを保護します。
2. ネットワーク内でセキュリティ ポリシーに対する違反や攻撃をモニタし、対応します。
3. セキュリティ セーフガードの有効性をテストします。
4. 企業セキュリティを管理し、改善します。

4 つのすべてのステップは連続して行う必要があります。企業のセキュリティ ポリシーを作成および更新する場合は、各ステップを考慮する必要があります。

ここでは、次のプロジェクト フェーズに伴う推奨タスク フローについて詳細に説明します。

- ・ プロビジョニング(「プロビジョニング フェーズのチェックリスト」を参照)
- ・ モニタリング(「モニタリング フェーズのチェックリスト」を参照)

## プロビジョニング フェーズのチェックリスト

プロビジョニングでは、ハードウェア、ソフトウェア、およびネットワークの計画、セットアップ、および設定を行います。これにより、MARS アプライアンスのデータおよびネットワーク リソースに実際にアクセスできるようになります。このフェーズは、インストールが正常に完了したあとに実行します。インストール手順については、『*Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*』を参照してください。

次のチェックリストに、意思決定プロセスを理解するために必要なタスク、および MARS を最も効率的な方法でプロビジョニングするのに必要な基本フローを示します。各ステップには複数のサブステップが含まれることがあります。これらのステップとサブステップは順番どおりに実行する必要があります。チェックリストでは、各タスクを実行するための具体的手順の参照先も示しています。

✓	タスク
□	<p><b>1. インベントリおよびレビュー可能なレポート デバイス、軽減デバイス、およびサポート デバイス</b></p> <p>レポート デバイスは、ユーザとネットワークのアクティビティ、およびデバイスのステータスと設定に関するログを提供します。軽減デバイスは、検出された攻撃に対処する際に使用することができ、また、レポート デバイスとしても機能します。サポート デバイスは、レポート デバイス、軽減デバイス、または MARS アプライアンスにネットワーク サービスを提供します。</p> <p>ネットワーク上のどのデバイスをモニタするかについては、複数の要因が関係します。たとえば、デバイスの配置、同じネットワーク セグメント上のその他のデバイスと比較した場合のレポート機能、および MARS アプライアンスで実現する必要のある動作レベルなどです。</p> <p>どのデバイスをレポート デバイスおよび軽減デバイスにするかを検討する場合は、これらのデバイスから MARS に提供されるデータを把握する必要があります。有効なすべてのデバイスを追加しただけでは、最適なモニタリングおよび軽減方針とはいえません。慎重に検討してデバイスを選択することにより、MARS のワークロードを削減して、検出時間および軽減時間を短縮し、フォールス ポジティブ検出を改善することができます。</p> <p>MARS が処理するのはモニタ対象デバイスのみであるため、モニタするデバイスは慎重に決定する必要があります。次に、デバイスを決定する場合の考慮事項の例を 2 つだけ示します。</p> <ul style="list-style-type: none"> <li>・ 特定のネットワーク セグメントのレポート デバイスで使用可能なログおよびデータ タイプを考慮して、ネットワークのアクティビティの全体像が最もよくわかるログを選択します。</li> <li>・ ネットワーク内の各セグメントの本来のチョークポイントにある軽減デバイスを特定します。これらの軽減デバイスを</li> </ul>

	<p>MARS の処理対象にすると、攻撃を止める可能性が高まります。MARS は攻撃を識別すると、ネットワークポロジを調べて、最適なチョークポイントを特定します。ただし、MARS が調査するのは、モニタ対象デバイスのみです。</p> <p>サポート デバイスは STM システムの運用に重要な役割を果たすことがあります。したがって、ネットワーク上のサポート デバイスのインベントリを作成し、検討する必要があります。対象となるデバイスは、電子メール サーバ、AAA(認証、許可、アカウントिंग)サーバ、DNS サーバ、Syslog サーバ など、想定される STM システムで特定の役割を果たすデバイスです。</p> <p><b>結果:</b> モニタするデバイス リストが完成します。各デバイスの詳細には、デバイス名、レポート IP アドレス、管理 IP アドレス、管理プロトコル、管理アカウント情報、およびイネーブルにするロギング機能、レベル、プロトコルが含まれます。</p> <p>詳細については、以下を参照してください。</p> <ul style="list-style-type: none"> <li>・ 「モニタ対象デバイスの選択」</li> <li>・ 「動作レベル」</li> <li>・ 『<i>Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System</i>』の『<a href="#">Deployment Planning Guidelines</a>』(p.2-1)</li> <li>・ 「デバイス インベントリ ワークシート」</li> </ul>
□	<p><b>2. 必要なすべてのトラフィック フローを特定し、イネーブルにします。</b></p> <p>対象デバイスを決定したら、管理、報告、および通知に使用するネットワーク サービスが、目的のトラフィック フローに対して許可されていることを確認する必要があります。ステップ 1 で作成した詳細な <i>デバイス インベントリ ワークシート</i> を参照して、MARS アプライアンスと各サポート デバイス、レポート デバイス、軽減デバイスとの間の管理、ロギング、および通知トラフィックが中間ゲートウェイで許可されていることを確認します。</p> <p>さらに、DNS、電子メール、AAA、および NTP サーバなどのサポート デバイスのネットワーク サービスが、ネットワーク上の MARS アプライアンス、サポート デバイス、レポート デバイス、および軽減デバイスを通してできるように許可する必要があります。</p> <p><b>ヒント</b> MARS アプライアンスを含むすべてのデバイスは、同じ時刻に同期させることを推奨します。MARS アプライアンスは HTTPS サーバであるため、ここで使用される証明書では、時刻、日付、およびタイム ゾーンが適切に設定されている必要があります。これらが適切に設定されていないと、セッションおよびインシデントのタイム スタンプが不正確になり、HTML インターフェイスにアクセスする際に「タイムアウト」エラーが発生することがあります。</p> <p>トラブルシューティングしなければならない事態を制限するには、送信元ネットワーク セグメントから宛先セグメントへの各トラフィック フローをテストする必要があります。できれば、プロトコルごとに、デバイス間のすべてのフローをテストして、さまざまなゲートウェイ ACL(アクセス制御リスト)の最適な一致と最初の一致のセマンティックによって、目的のトラフィック フローが妨げられないことを確認します。ネットワーク上のすべてのセキュリティ デバイスの場合と同じように、イネーブル化されたトラフィック フローの対象を、目的のプロトコル、ポート、および送信元/宛先ペアに限定する必要があります。</p> <p><b>結果:</b> すべての中間ゲートウェイで、デバイスと MARS アプライアンス間のログ、管理、および通知トラフィックが許可されていることが確認されます。</p> <p>詳細については、以下を参照してください。</p> <ul style="list-style-type: none"> <li>・ 『<i>Top Issues for the Cisco Security Monitoring, Analysis, and Response System</i>』の『<a href="#">Event Timestamps and Processing</a>』</li> <li>・ 『<i>Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System</i>』の『<a href="#">Deployment Planning Guidelines</a>』(p.2-1)</li> <li>・ 『<i>Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System</i>』の『<a href="#">Supporting Devices</a>』(p.2-1)</li> <li>・ 『<i>Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System</i>』の『<a href="#">Required Traffic Flows</a>』(p.2-3)</li> <li>・ 『<i>Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System</i>』の『<a href="#">Specify the Time Settings</a>』(p.5-10)</li> <li>・ 「デバイス インベントリ ワークシート」</li> </ul>

□	<p><b>3. レポート デバイス、軽減デバイス、およびサポート デバイスをブートストラップします。</b></p> <p><u>デバイス インベントリ ワークシート</u>で決定したデバイスごとにブートストラップを行って、MARS との間に必要な通信が発生するように設定します。デバイスのブートストラップでは、STM システム内の役割によって決定する値を、デバイスの設定値にします。デバイス タイプおよび役割に応じて、次のブートストラップ タスクを実行します。</p> <ul style="list-style-type: none"> <li>・ MARS アプライアンスが軽減およびアクセスのために実行するデバイス管理をイネーブルにする。</li> <li>・ MARS アプライアンスのために正しいログを収集するエージェントをインストールする。</li> <li>・ 正しいロギング レベルおよびロギング サービスをイネーブルにする。</li> <li>・ MARS アプライアンスにログを転送するか、これらのログを必要に応じて受信またはプルするアプライアンスを決定する。</li> <li>・ デバイス設定の検出をイネーブルにする。</li> <li>・ デバイスが MARS アプライアンスから通知を受信できるように設定する。</li> </ul> <p>STM システムで想定された役割を割り当てるための設定は、デバイスごとに異なります。デバイスについて検討する場合は、STM システム内で想定される役割と、上記タスクの設定を直接、関連付けます。さらに、MARS によって課せられる制限を把握します。たとえば、特定のデバイス タイプを検出する場合、サポート対象プロトコルに制限があることがあります。</p> <p><b>結果:</b> レポート デバイスおよび軽減デバイスで、正しいロギング レベルがイネーブルになります。MARS アプライアンスはこれらのデバイスから必要なすべてのログを受信またはプルすることができます。また、設定値を取得したり、サポート対象の軽減デバイスに ACLS をプッシュすることができます。検出済み攻撃の通知が必要なデバイスは、MARS アプライアンスからこのような通知を受信するように設定できます。MARS アプライアンスは、受信したイベントを取得して格納しますが、これらを検査するには、レポート デバイスおよび軽減デバイスを HTML インターフェイスで定義して、アクティブにする必要があります。</p> <p><b>ヒント</b> HTML インターフェイスにデバイスを追加してアクティブにする前に、デバイスから MARS にパブリッシュされたイベントを問い合わせるには、デバイスの報告 IP アドレスを一致基準として使用します。この方法は、デバイスが適切にブートストラップされていることを確認する場合に便利です。</p> <p>詳細については、以下を参照してください。</p> <ul style="list-style-type: none"> <li>・ 「デバイス インベントリ ワークシート」</li> <li>・ <a href="#">「Supported Reporting and Mitigation Devices」</a></li> <li>・ 「ブートストラップの概要」</li> <li>・ レポート デバイスおよび軽減デバイスのログ設定に関するユーザ ガイドの項</li> </ul>
□	<p><b>4. MARS にデバイスを定義します。</b></p> <p>レポート デバイスおよび軽減デバイスを決定したうえでブートストラップして、必要なトラフィック フローをイネーブルにしたら、これらのデバイスを MARS に定義する必要があります。MARS は、この情報を使用してデバイスと通信します。定義するためには、HTML インターフェイスに各デバイスを追加するか、CSV (カンマ区切りベクトル) ファイルをインポートします。CSV ファイルは、基本的なデバイス タイプに必要な設定を定義し、より複雑なデバイスを定義するための起点となります。また、トポロジー検出を使用して、レポート デバイスおよび軽減デバイスを自動的に検出してから、前の手順に戻って、詳細を追加指定することができます。</p> <p>ほとんどのデバイス タイプに対し、デバイス検出に使用するアクセス プロトコルを決定する必要があります。選択したプロトコルによって、検出できるデータ タイプ、および軽減の実行の可否が決まります。これらのオプションを理解すると、企業のポリシーに適合する一貫した方法を見つけることができます。</p> <p>デバイスの追加方法は、ネットワーク上のデバイス数と、追加するデバイスの CSV デバイス キーワードの有無によって異なります。また、エージェント、モジュール、またはセンサを使用するデバイス タイプを定義する場合は、ベースとなるホストまたはデバイスを定義してから、モジュール、センサ、およびエージェントをベース デバイスに追加するなど、複数のステップが必要です。たとえば、Cisco ASA デバイスに IPS モジュールを追加する場合は、Cisco ASA デバイスを定義してから、このデバイスのコンポーネントとして IPS モジュールを定義する必要があります。また、専用アプライアンスでない多くのアプリケーションでは、アプリケーションが稼働するホスト (汎用、Windows、UNIX、または Linux) を定義してから、アプリケーションとホストを関連付ける必要があります。</p> <p>デバイスを追加したら、HTML インターフェイスの各ページにある Activate をクリックして、追加したデバイスをアクティブにする必要があります。</p> <p><b>結果:</b> すべてのレポート デバイスおよび軽減デバイスが、MARS 内に定義され、アクティブになります。デバイスが MARS</p>

内でブートストラップおよび定義されると、MARS はデバイスから受信したログの検査を開始します。MARS はデバイスが追加されるまで、受信したイベントの取得および格納だけを行い、検査は実行しません。

詳細については、以下を参照してください。

- ・ 「デバイス インベントリ ワークシート」
- ・ 「アクセス タイプの選択」
- ・ 「レポート デバイスおよび軽減デバイスの個別の追加」
- ・ 「シード ファイルを使用した複数のレポート デバイスおよび軽減デバイスの追加」
- ・ 「自動トポロジー検出を使用したレポート デバイスおよび軽減デバイスの追加」
- ・ [「Supported Reporting and Mitigation Devices」](#) (p.2) (CSV Keyword カラム)
- ・ 「レポート デバイスおよび軽減デバイスとの接続の確認」
- ・ 「レポート デバイスおよび軽減デバイスのアクティブ化」

## 5. MARS のグローバル データ収集の設定値およびスケジュールを設定します。

デバイスを追加したら、次に示す MARS の豊富なデータ収集機能をイネーブルにできます。

- ・ **動的な脆弱性スキャン** — MARS は攻撃を検出したときに、ネットワークをプローブして、攻撃の成功の可能性および重大度を判定することができます。検出された攻撃に応じてデータ収集を実行するには、この機能をイネーブルにして、分析するネットワークを指定する必要があります。
- ・ **NetFlow データ収集** — NetFlow データを使用すると、MARS はネットワーク内の一般的なデータ フローをプロファイリングして異常を識別し、ワームの急増を含む Day Zero 攻撃を検出することができます。統計的プロファイリングには、4 日間 ~ 2 週間かかります。プロファイルが作成されると、MARS は異常なトラフィック フローの検出を開始し、これらのフローに応じたインシデントを作成します。NetFlow データ収集を設定するには、NetFlow トラフィックを生成できるデバイスを設定し、共有コミュニティ スtring を待ち受けるように MARS を設定する必要があります。
- ・ **レイヤ 3 トポロジー検出** — レイヤ 3 ネットワーク デバイス (IP レイヤで動作するデバイス) を検出する、プロセス中心の処理。このレイヤ 3 データは、攻撃パス ベクトルを判別し、トポロジー グラフを読み込む場合に使用します。この情報の更新スケジュールは定義することができます。
- ・ **レイヤ 2 デバイス検出** — この機能を使用すると、MARS は攻撃パス ベクトルを判別したり、MAC (メディア アクセス制御) アドレスによって攻撃元ホストおよびターゲットを識別したりすることにより、IP アドレスのスプーフィング攻撃による混乱を回避できます。この機能は通常、スイッチを追加したり、軽減機能をイネーブルにしたりするときに設定します。

MARS が定期的にデータをプルするデバイスには、複数のタイプがあります。これらのデバイスに対し、イベント ログを取得して処理するためのインターバルを定義できます。これらの更新機能は、次のとおりです。

- ・ **Distributed Threat Mitigation (DTM) デバイスの更新** — DTM サービスは Cisco IPS および Cisco IDS デバイスをポーリングして、すべてのレポート デバイスにわたって最上位の起動シグニチャを判別します。MARS はこの情報に基づいて、ネットワークで起動したシグニチャの最上位リストを生成します。これにより、DTM フィーチャ セットを実行している Cisco IOS ルータは、実行する必要のあるシグニチャリストを MARS に問い合わせることができます。
- ・ **Windows イベント ログ** — MARS が Windows ホストおよびサーバから監査追跡レコードをプルする頻度を設定できます。この設定はこのようなすべてのホストでグローバルです。デフォルト値は 5 分です。
- ・ **Oracle イベント ログ** — MARS が Oracle データベース サーバから監査追跡レコードをプルする頻度を設定できます。この設定はこのようなすべてのサーバでグローバルです。デフォルト値は 5 分です。
- ・ **モニタ対象デバイスの更新スケジューラ** — MARS が Qualys QualysGuard、Foundstone Foundscan、eEye REM などの特定のレポート デバイスからデータをプルする頻度を設定できます。スケジュールは IP アドレス単位で設定します。

設定を定義したら、HTML インターフェイスの各ページにある Activate をクリックして、定義をアクティブにする必要があります。

	<p>ます。</p> <p><b>結果:</b> レポート デバイス、軽減デバイス、およびサポート デバイスからプルされたキャッシュ済みデータの更新スケジュールが MARS 内に定義され、アクティブになります。これらの設定を定義すると、MARS はネットワークをプローブしたり、レポート デバイス、軽減デバイス、およびサポート デバイスからアップデートをプルしたりすることができます。</p> <p>詳細については、以下を参照してください。</p> <ul style="list-style-type: none"> <li>・ 「データ イネーブル化機能」</li> <li>・ Windows イベント ログのプル時間間隔</li> <li>・ 「レイヤ 2 検出および軽減機能」</li> <li>・ 「Oracle イベント ログのプル インターバルの設定」</li> <li>・ 「動的な脆弱性スキャン用ネットワーク」</li> <li>・ 「NetFlow 異常検出の概要」</li> <li>・ 「レイヤ 3 トポロジー検出の設定」</li> <li>・ 「DTM の設定」</li> <li>・ 「トポロジー更新のスケジュール」</li> </ul>
	<p><b>6. サポート デバイスおよびネットワーク資産に関する脆弱性評価情報を読み込みます。</b></p> <p>脆弱性評価情報の対象は、ネットワークの特定のホストです。ホストがレポート デバイスであるか、軽減デバイスであるか、またはネットワーク上の重要な資産であるかに関係なく、すべてのホストについて詳細な情報を取得できます。</p> <p>この情報には、ホストで稼働するオペレーティング システム、パッチ レベル、およびネットワーク サービスが含まれます。ホストを定義したら、HTML インターフェイスの各ページにある Activate をクリックして、ホストをアクティブにする必要があります。</p> <p><b>結果:</b> MARS はネットワーク上のホスト、および稼働しているサービスについての詳細情報を取得します。</p> <p>詳細については、以下を参照してください。</p> <ul style="list-style-type: none"> <li>・ 「ホストとデバイスの ID および詳細に関する方針」</li> <li>・ 「デバイス インベントリ ワークシート」</li> <li>・ 「IP 管理」</li> <li>・ 「サービス管理」</li> </ul>
<input type="checkbox"/>	<p><b>7. イベント生成および処理をモニタおよび調整します。</b></p> <p>モニタリング アプリケーションの場合と同様に、技術上の精度およびパフォーマンスを高めるには、ログ生成およびイベント処理を調整することが重要です。MARS でどのイベントを処理するかを調整する方法は、次の 2 つです。</p> <ul style="list-style-type: none"> <li>・ <b>デバイス側の調整</b> — この方法では、デバイス レベルでイベント生成を制限します。MARS は、セキュリティまたはデバイス ステータスに関連しないイベントは受信しません。この方法では、ネットワークの複数のデバイスから報告された疑わしい重複データの除去と、トラフィック サマリー Syslog など、MARS 内でレポートやクエリーによって複製される可能性のあるイベントの除去も行われます。</li> <li>・ <b>アプライアンス側の調整</b> — この方法では、MARS アプライアンスで受信したイベントのうち、通常のネットワーク アクティビティまたは計画済みのネットワーク アクティビティを表すものを特定します。MARS がこのようなイベントを疑わしいセキュリティ インシデントとして処理しないようにするために、廃棄規則を定義します。このような廃棄規則を定義する場合は、できるだけ細かく定義する必要があります。たとえば、予測期間内に特定の IP アドレスで発生すると想定される ping スニップの送信元を特定します。この場合は、ネットワークおよび管理方法に関する情報を明示的に指定する必要があるため、スプーフィングはより困難になります。さらに 7 つの条件を組み合わせ、規則を限定することができます。7 つの条件とは、送信元、宛先、サービス タイプ、イベント タイプ、時間範囲、レポート デバイス、およびイベントの重大度です。イベント全体を廃棄するのか、またはイベントを廃棄してデータベースに記録して、クエリーやレポートに使用できるようにするのかを選択する必要があります。</li> </ul> <p>調整は、攻撃の識別能力、真に疑わしいアクティビティに関するレポートの品質、および STM ソリューションの全体的なパ</p>

パフォーマンスや精度を改善するために継続的に行うタスクです。調整タスクではトラフィックを詳細に調査します。調査を行ったり精度を上げたりするには、アプライアンスに着信するイベントをデバイス単位で評価します。

**ヒント** ラボ ネットワーク環境では、MARS アプライアンスを使用して、生成されたイベントおよび調整オプションをデバイス タイプごとに調査します。制御された環境では、要件を文書化しておくことにより、デバイス側の重要な調整基準をモニタリング デバイス タイプごとに確立して、運用ネットワークの調整作業を大幅に削減できます。

**結果:** STM システムにとって価値のあるイベントのみが、MARS アプライアンスによって処理されるようになります。

詳細については、以下を参照してください。

- ・ 「アプライアンス側の調整に関する注意事項」

## モニタリング フェーズのチェックリスト

プロビジョニング フェーズを完了したら、セキュリティに関するより広範な目標および要件を実現できるように MARS を設定する必要があります。モニタリング フェーズの主な目標は、モニタリング、軽減機能、および復旧ポリシーを効率的に実現することです。このフェーズでは、この目標の達成に必要な戦略、規則、レポート、およびその他の設定を定義します。



**注:** 検出された攻撃に対応する準備をするため、トラフィック フローのモニタリングを開始する前に、企業のセキュリティ ポリシーに厳密に適合するように、MARS を設定しておく必要があります。

次のチェックリストに、意思決定プロセスを理解するために必要なタスク、および MARS を最も効率的に運用するために必要な基本フローを示します。各ステップには複数のサブステップが含まれることがあります。これらのステップとサブステップは順番どおりに実行する必要があります。チェックリストには、各タスクを実行するための具体的手順の参照先も示されています。

✓	タスク
□	<p><b>1. モニタリング、通知、軽減機能、復旧、および監査に関する方針を決定します。</b></p> <p>これらの方針で重要となるのは、目的のトラフィック フローや生成されたイベントでなく、MARS アプライアンスがこのデータを処理したあとに何を実行するかです。MARS によるネットワークの保護方法、および進行中の攻撃を停止して感染したホストを復旧させる方法を、モニタリングおよび鑑識分析の短期および長期の要件を考慮して決定する場合は、これらの方針が重要となります。これらの方針には、MARS へのユーザ介入の予測だけでなく、レポート デバイスに関する予測も含まれます。基本的には、予想される役割、タスク、およびデータ要件がこれらの方針によって決定するため、イベント、規則、クエリ、およびレポートを、特定のタスクに必要なデータを提供する役割に対応付けることができます。</p> <p>すべてのセキュリティ システムの場合と同様に、ジョブの実行に最低限必要な権限をユーザに割り当てることを推奨します。管理レベルの権限は、MARS アプライアンスの管理者のみに限る必要があります。</p> <p><b>結果:</b> 検出された攻撃およびデバイス問題に効果的に対応するために必要なユーザおよび役割が決定されます。通知に回答するための明確なガイダンスが定義され、このような通知の情報に関する要件、および予測される使用方法と配信方式が決定されます。</p> <p>詳細については、以下を参照してください。</p> <ul style="list-style-type: none"> <li>・ 「モニタリング、通知、軽減、復旧、および監査に関する方針」</li> <li>・ <a href="#">「ケース管理」</a></li> <li>・ <a href="#">「ユーザ管理」</a></li> <li>・ <a href="#">「Management タブの概要」</a></li> <li>・ 「ユーザ役割ワークシート」</li> </ul>
□	<p><b>2. 通知サービスを定義します。</b></p> <p>このタスクでは、軽減および復旧担当者に通知し、必要なその他のアクションを実行するように、MARS の通知サービスを準備します。MARS では、通知サービスは次の 3 つのブロックで構成されます。</p> <ul style="list-style-type: none"> <li>・ <b>ユーザ アカウント</b> — レポートまたは通知を受け取るユーザ、またはモニタリングや軽減措置のために HTML イン</li> </ul>

ターフェイスにアクセスするユーザ。ユーザは、電子メール、ページャ メッセージ、または Short Message Service (SMS) メッセージの形式で通知を受けることができます。ユーザは、Admin、Security Analyst、Operator、Notification Only の 4 つの役割のいずれかに割り当てられ、これによって HTML インターフェイスのアクセス権限が決定します。

- ・ **デバイス** — 通知を SNMP (簡易ネットワーク管理プロトコル) メッセージ、Syslog メッセージ、または (IOS IPS デバイスの場合は) DAM メッセージ (遮断と同等) の形式で受信するデバイス。デバイスの定義の詳細については、「プロビジョニング フェーズのチェックリスト」を参照してください。
- ・ **アクション** — インспекション規則内で定義される通知アクション。通知対象がユーザかデバイスかに応じて、スタッフにガイダンスを表示したり、デバイスに攻撃を記録またはブロックしたりするように指示できます。

MARS では、通知を受信すると想定されるユーザまたはデバイスをシステムで識別する必要があります。したがって、最初に、特定のイベント設定に基づいて通知する必要があるユーザまたはグループに対応付けるユーザ アカウントを定義します (「ユーザ役割ワークシート」を参照)。また、通知される必要があるデバイス、または何らかのアクションを実行する必要があるデバイスを指定する必要があります (「デバイス インベントリ ワークシート」を参照)。

次に、通知サービス設定 (アクション) として、電子メール、ページ、SMS、SNMP、Syslog、DAM から、1 つまたは複数選択します。これらの設定にはそれぞれ、各通知タイプごとに定義可能な連絡先情報およびメッセージが含まれます。

これらの設定を定義する独立したインターフェイスはありません。通知サービス設定を定義するには、既存のインспекション規則を編集し、新しいアクション定義を追加する必要があります。これらの設定を定義すると、すべてのインспекション規則で使用できるようになります。

**結果:** 必要なすべてのユーザが MARS で識別され、正しいユーザに通知されるように規則およびレポートをカスタマイズできるようになります。

詳細については、以下を参照してください。

- ・ [「ユーザ管理」](#)
- ・ [「ユーザ グループに対するユーザの追加または削除」](#)
- ・ [「IP 管理」](#)
- ・ 「レポート デバイスおよび軽減デバイスの追加」
- ・ 「サードパーティ製 Syslog および SNMP サーバへのアラート データの転送」
- ・ 「MARS MIB のフォーマット」
- ・ [「インспекション規則」](#)
- ・ [「システムおよびユーザ インспекション規則の処理」](#)
- ・ [「アラートの設定」](#)
- ・ [「アラートの送信」](#)



### 3. カスタム インспекション規則を定義し、システム インспекション規則を調整します。

インспекション規則によって、異種デバイスからのイベントを、攻撃またはその他のネットワーク セッションのエンドツーエンド アクティビティが反映された重要なセッションに関連付けます。MARS は攻撃をエンドツーエンドで識別するため、ネットワークの軽減ポイントを確実に判別することができます。ただし、異なる目標を実現するためにインспекション規則を定義することもできます。攻撃の識別は実現可能な目標の 1 つにすぎません。その他の目標の例としては、重要な資産の使用の特定、ネットワーク ヘルス、使用率分析に基づくネットワーク設定の調整などがあります。

MARS には 100 を超えるインспекション規則が組み込まれていますが、ユーザが属する企業のポリシーにとって重要なセッションを識別できないことがあります。たとえば、カスタム アプリケーションまたはサポート対象外アプリケーションの使用をモニタする場合は、選択された送信元と宛先間のトラフィックを、既知のプロトコルとポートのペアを使用してモニタするインспекション規則を新規に定義できます。または、該当するアプリケーションによって生成されたイベントを独自に処理するカスタム ログ パーサーを定義して、追跡するイベント内のデータを調べることができます。既知のプロトコルとポートのペアをモニタすると、セッション数などのサマリー データを取得することができます。一方カスタム ログ パーサーは、リソース利用率や失敗したログインなどのトラフィックの特徴を詳細に検査することができます。カスタム パーサーを定義するには、アプライアンスで使用されるメッセージ フォーマットを調べ、クリア テキスト形式で MARS にパブリッシュする必要があります。

作成した規則を意味のあるグループに編成すると、目的を明確にしたり、システムの学習能力を改善したりすることができます。具体的な目標について検討する場合は、規則グループ(および対応するレポートグループ)を定義して、ステップ 1 で決定した方針を調整する必要があります。規則は複数のグループに属することができるため、同じ問題を解決するための同じ規則を何度も作成する必要はありません。グループ化の目的は、単に作業をまとめて、一度に 1 つの方針を処理できるようにすることです。

**結果:** 企業ポリシーに適合する適切な通知を送信するように、カスタム インспекション規則がすべて作成され、既存のインспекション規則が設定されます。カスタム ログ パーサーおよびインспекション規則がすべて定義され、ユーザ ネットワーク内で発生したトラフィック フローまたはサポート対象外のアプリケーションやプロトコルを監査できるようになります。

詳細については、以下を参照してください。

- ・ [「規則およびレポートグループ」](#)
- ・ [「イベント管理」](#)
- ・ [「IP 管理」](#)
- ・ [「サービス管理」](#)
- ・ [「ユーザ管理」](#)
- ・ 「ユーザ定義のログ パーサー テンプレートの追加」
- ・ [「インспекション規則」](#)
- ・ [「システムおよびユーザ インспекションの処理」](#)
- ・ [「アラートの設定」](#)
- ・ [「アラートの送信」](#)

#### 4. カスタム クエリーおよびレポートを定義します。

クエリーおよびレポートは鑑識分析を行うためのツールです。このツールを使用すると、履歴データを分析し、MARS のリアルタイム モニタリング機能では知り得ない長期的な傾向を特定することができます。本来、クエリーはレポート テンプレートの定義に従ってデータをオンデマンドで詳細に検査するために実行します。それに対してレポートは、定期的に行われるようにスケジュールするものであり、継続的に検査する期間および頻度を定義できます。クエリーを使用すると、検索基準をフィルタリングして、レポート テンプレートに基づいて検索範囲を狭めたり、広げることができます。MARS には定義済みレポート テンプレートが多数用意されているため、ポリシーの実現にとって重要なインシデントおよびイベントに重点を置いた新しいレポート テンプレートを定義できます。この機能は、特に適合レポート要件に従う場合に役立ちます。レポートを定義し、生成スケジュールを立てて、結果を監査レコードの一部として格納できるためです。

アクセス全体と同様、レポートおよびクエリーの実行または表示機能は、ユーザ役割に基づいて制限することができます。このようなセーフガード機能により、システムの他のユーザがレポートのスケジュールを誤って変更するような事態を回避できます。また、ユーザにレポートが通知されるようにレポート テンプレートを設定することもできます。通常、レポートの通知には電子メールがよく使用されますが、すべての通知方法がサポートされています。

**結果:** 鑑識分析および監査の目標を実現するために必要なレポート テンプレートが定義され、最小権限ポリシーに従ってユーザ役割に割り当てられます。レポートのアクセスまたは分配と、スタッフ間の問い合わせに役立つレポートグループが定義されます。

詳細については、以下を参照してください。

- ・ [「クエリーおよびレポート」](#)
- ・ [「Query ページ」](#)
- ・ [「レポートを使用した長期クエリーの実行」](#)
- ・ [「バッチ クエリーの実行」](#)
- ・ [「Reports ページ」](#)
- ・ [「レポートの作成」](#)

## 5. ネットワークおよびセキュリティ アクティビティをモニタします。

このタスクには、ネットワーク内で攻撃または問題点をモニタして、対応する作業が含まれます。MARS へのユーザの介入方法は、ユーザの役割および運用ガイドラインによって異なります。ユーザが HTML インターフェイスを使用してほぼリアルタイムでトラフィックをモニタする場合は、疑わしい動作や異常な動作への対処時期や対処方法だけでなく、表示された関連データに関する詳しい知識が必要です。

MARS にはネットワークとセキュリティ アクティビティに対する 2 つのインターフェイスがあります。1 つは Summary タブで、もう 1 つは Query/Reports タブです。各インターフェイスには、ネットワークの現状の把握に役立つさまざまなビューおよびツールが用意されています。

Summary タブにはイベントがほぼリアルタイムで表示され、Query/Reports タブには主に過去の鑑識分析が表示されます (ステップ 4 を参照)。Summary タブにはネットワーク アクティビティの主な状況として、ホットスポット図、最新イベント、インシデントチャート、およびトポロジー図が表示されるため、最新のアクティビティを確認できます。

さらに調査や軽減が必要なインシデントを指定する際には、インシデントを調査してフォールス ポジティブであるかどうかを判断したり、MARS を使用して攻撃をブロックしたりすることができます。レイヤ 2 で動作するチョークポイント (プライマリスイッチ) が存在する場合、MARS は適切なデバイスを特定して、推奨される CLI 変更を行い、これらの変更をユーザがデバイスにプッシュできるようにします。チョークポイントがレイヤ 3 デバイスの場合、MARS は、特定されたチョークポイントとの管理セッションにコピー アンド ペーストできる CLI 変更を推奨します。

このような方法により、ユーザはネットワーク内の疑わしい動作をモニタし、検出内容に対応することができます。

**結果:** ネットワーク上の攻撃をモニタ、表示、および軽減するために必要なビューおよびツールについて理解しました。

詳細については、以下を参照してください。

- ・ [「ネットワークの概要」](#)
- ・ [「インシデントの調査」](#)
- ・ [「軽減」](#)
- ・ [「規則およびレポートグループ」](#)
- ・ [「イベントグループ」](#)
- ・ [「ケース管理」](#)
- ・ [「False Positive ページ」](#)
- ・ [「未加工メッセージの取得」](#)

## 6. システムおよびネットワーク ヘルスをモニタします。

STM システムは MARS アプライアンスだけを示すのではなく、すべてのレポート デバイスや軽減デバイス、およびすべての MARS アプライアンスが含まれます。システムのヘルスを評価する場合は、これらのデバイスのヘルスをそれぞれモニタする必要があります。異常な動作に関する通知を生成するインスペクション規則を使用したり、システム ヘルスに関するクエリーおよびレポートを生成したり、MARS のシステム ログを手動で表示したりすることにより、システム ヘルスをモニタします。

MARS では、CPU、帯域幅、メモリなど一般的なリソースの使用に関するレポートを作成できます。システム ヘルスのモニタリングを簡素化するために、レポート グループを定義して、これらのレポートを意味のあるグループにまとめることができます。特定のユーザ役割に限って、レポートおよびクエリーを表示できるようにすることも可能です。

レポートはスケジュール可能であるため、レポートが更新されるたびに該当するユーザに知らせることができます。

**ヒント** レポート デバイスのリソース使用率を表示できない場合は、Admin > System Configuration > Security and Monitored Devices でデバイスを定義する際に、Monitor Resource Usage オプションがイネーブルになっていることを確認してください。このデータを提供するように設定できるデバイスのリストについては、「リソース使用率データの設定」を参照してください。

MARS にはアプライアンス自体のステータスに関する詳細ログや、アプライアンスのヘルスに関するステータスを表示するコマンドライン ユーティリティがいくつか組み込まれています。

**結果:** システムおよびネットワーク ヘルスのモニタを行うために MARS に用意されているツールおよびレポートについて理解しました。

詳細については、以下を参照してください。

- ・ [「規則およびレポートグループ」](#)
- ・ [「規則およびレポートグループの概要」](#)
- ・ 「リソース使用率データの設定」
- ・ [\[pnstatus\] \(A-21 ページ\)](#)
- ・ [「pnlog」 \(A-16 ページ\)](#)
- ・ [「実行時ロギング レベルの設定」](#)
- ・ [「アプライアンスのログ ファイルの表示」](#)
- ・ [「監査追跡の表示」](#)
- ・ [「未加工メッセージの取得」](#)



### 7. MARS の処理を調整します。

モニタリング アプリケーションに関する継続的な作業である調整には、イベント処理方法の感度および精度を調整する作業が含まれます。MARS では、次のようなさまざまな方法で変更を行うことができます。

- ・ 廃棄規則を使用して、MARS によるイベント処理をイネーブルまたはディセーブルにします。
- ・ デバイスでイベント生成をオンまたはオフにします。
- ・ 選択したインシデントをフォールス ポジティブとして識別します。
- ・ 特定のネットワーク、ホスト、サービス、レポート デバイス、またはトラフィック フローを追加または除外することにより、インスペクション規則を調整します。
- ・ IPS や IDS などのデバイス タイプ別にトラフィックのインスペクションを調整し、イベント生成に使用される規則セットを改良します。
- ・ レポート デバイスを追加または削除することにより、報告イベント セットの変更や、フォールス ポジティブ、OS フィンガープリント、脆弱性評価などの MARS の自己調整機能を改善するために使用できる補助データの提供が行われます。
- ・ 資産、サービス、および脆弱性評価情報を記述して、ネットワーク上で予測される動作を示します。ネットワークの詳細な情報が MARS に集まるにつれて、着信イベントに対する MARS の評価精度も高まります。

**結果:** MARS アプライアンスによって処理されるイベントの範囲が、STM システムに最も価値のあるイベントに限定されるか、またはこのようなイベントを含むように拡張されます。

詳細については、以下を参照してください。

- ・ 「アプライアンス側の調整に関する注意事項」
- ・ [「廃棄規則の作業」](#)
- ・ [「フォールス ポジティブの確認」](#)
- ・ 「モニタ対象デバイスの選択」

## モニタリング、通知、軽減、復旧、および監査に関する方針

STM で企業のセキュリティ ポリシーをサポートするには、複数の方針を緊密に調整する必要があります。

- ・ モニタリングでは、ネットワーク アクティビティおよびデバイスのステータスを調査して、異常なアクティビティまたは動作を識別します。
- ・ 通知では、検出された異常に対応する担当者に警告し、対処に必要な情報を提供します。

- ・ 軽減では、疑わしいアクティビティに対応して、ネットワークへの拡散を防止します。
- ・ 復旧では、正常な対処を行って、ネットワークの感染ホストを浄化します。
- ・ 監査では、その他のタスク中に発生したアクティビティを記録して、報告します。監査の目的は、適合性の監査や傾向分析をサポートするためのアクティビティおよび対処法をアカウントに提供することです。

最初に決定しなければならないのは、選択されたチョークポイントでの軽減に対する責任を持つ担当者です。通常、企業内では、各部門にわたるコア ネットワーク インフラストラクチャ デバイスから専用のセキュリティ デバイスを分離しています。たとえば、2 つの独立したチーム(セキュリティ運用チームとネットワーク運用チーム)は、共有デバイス上で、異なるネットワーク コンポーネントまたはポリシーに責任を持ちます。ネットワークで MARS を展開する前に、企業ポリシーに従って、軽減方針の責任者を明確に定義する必要があります。

軽減方針には、2 つの選択肢があります。

- ・ MARS を利用して、チョークポイントを判別し、推奨された CLI 変更を受け入れます。これによって、検出された攻撃をブロックすることができます。
- ・ MARS の推奨事項を評価できる担当者に通知し、インシデントの詳細を送信します。ただし、検出された攻撃を停止させる場所および方法についての最終判断は、その担当者が行います。

どちらの方法を選択しても、攻撃のブロック期間、正常化のために必要な内部攻撃調査の方法、必要な隔離期間後にポリシーを更新する担当者、および監査に適合するために、このようなイベントレコードを保持する方法(MARS のケース管理機能がチケット統合システムと連携しているかどうかなど)について、ガイドラインを作成する必要があります。

次に、実行しなければならないモニタリングタイプを明確にする必要があります。つまり、システムモニタリングとセキュリティモニタリングを区別します。システムモニタリングでは、MARS アプライアンスのステータスだけでなく、MARS によって管理されるレポートデバイスおよび軽減デバイスのヘルスやステータスもモニタします。セキュリティモニタリングでは、ネットワークおよびセキュリティに関するアクティビティを重点的にモニタします。

どちらのタイプのモニタリングを行う場合でも、定義済みおよびカスタムのクエリーやレポートの中で必要なもの、これらによって取得されるデータを評価して対応するプロセス、および MARS のケース管理機能を使用して応答を管理し、変更を追跡するためのガイドラインを決定する必要があります。

最終フェーズでは、特定のインシデントが検出された場合に通知するユーザを決定します。たとえば、デバイスステータスに関するインシデントを通知するユーザと、セキュリティに関するインシデントを通知するユーザなどです。軽減および復旧の担当者とはモニタリング(必要な場合は部門にまたがるモニタリング)を実行する担当者、および通知の生成方法と形式を決定します。この作業では、SMS、ページアラート、電子メールなどから方法を選択し、インシデント、クエリー、またはレポートのどれに基づいて通知を生成するかを決定します。

## アプライアンス側の調整に関する注意事項

MARS アプライアンスを調整する場合、レポートデバイスから着信したトラフィックの検査は重要ではありません。アプライアンス側で調整する場合は、主に次の 2 つの方法を使用します。

- ・ **廃棄規則** — レポートデバイスから受信した特定の基準と一致するすべてのイベントを廃棄します。この方法は高速で、最も調整が少なくすみます。廃棄規則を定義するときに、イベントログを維持するのか、または単に廃棄するのかを指定することもできます。廃棄規則の利点は、イベントがインスペクション規則で処理されないため、発生する可能性のあるワークロードが削減されて、アプライアンスの処理が高速になることです。
- ・ **インスペクションからのデバイスの削除** — インスペクション規則からデバイスを削除します。この方法は、特定のタイプのアラームをトリガーするイベントのみが対象になります。レポートデバイスから受信した特定の基準と一致するイベントがまったく破棄されないのがこの方法の利点です。つまり、この方法で重要になるのは、起動したすべてのインシデントを削除するのではなく、イベントに基づいて、特定のフォールス ポジティブを削減することです。また、クエリーおよびレポートを使用してイベントを確認できるように、イベントが記録されます。

どちらの方法を使用する場合も、規則を追加または変更したときには、Activate をクリックして変更を有効にする必要があります。

## デバイス インベントリ ワークシート

デバイス インベントリ ワークシートを使用すると、ネットワーク上のデバイスに関して必要な情報を収集できます。収集する情報は次のとおりです。

- ・ **デバイス名** — デバイスの既知の名前。通常は、デバイスの DNS 名になります。MARS のトポロジー グラフ、レポート、およびイベントに、この名前が使用されます。
- ・ **レポート IP アドレス** — MARS に対してイベントを送信するネットワーク インターフェイスに割り当てられた IP アドレス。MARS はこのアドレスを使用してデバイス名に対応付けて、デバイスから送信されたメッセージおよびイベントを一意に識別します。



