



はじめに

概要

Local Controller (軽減および応答システム) Security Threat Mitigation (STM; セキュリティ脅威軽減) アプライアンスをお買い上げいただき、ありがとうございます。このマニュアルでは、MARS アプライアンスの最も有効な利用法について説明します。



注 このマニュアルに記載された「MARS アプライアンス」に関する情報は、Global Controller アーキテクチャの Local Controller として使用される MARS にも適用されます。

MARS アプライアンス

Cisco Security Monitoring, Analysis, and Response System アプライアンス (MARS アプライアンス) は、STM アプライアンスです (MARS 20、MARS 50、MARS 100、および MARS 200)。ネットワーク内にあるレポート デバイスの「目」および「耳」を通して認識されるネットワークの状態に関して、広範な情報を提供します。レポート デバイスから未処理イベントをすべて取得し、デバイス間でセッション化すると、インシデントのデフォルト規則を起動して、フォールス ポジティブを判別し、図、チャート、クエリー、レポート、規則によって統合情報を提供します。

MARS はネットワーク デバイスに関して提供される情報量に基づいて、異なる複数のレベルで動作します。最も基本的なレベルでは、MARS は Syslog サーバとして機能します。レポート デバイスに関する情報を追加すると、MARS はセッション化を開始します。MARS は完全にイネーブル化されると ネットワークの概略を示し、そこから特定の MAC (メディア アクセス制御) アドレスをすばやくドリルダウンして表示できます。

MARS HTML インターフェイス

MARS ユーザ インターフェイスには、タブやハイパーリンクが配置されたブラウザベースのインターフェイスが採用されています。Web を使用したことがあるユーザは、類似した Web ページの使用経験を活かすことができます。



注 MARS ユーザ インターフェイスを使用している場合は、ブラウザの Back および Forward ボタンを使用しないでください。これらのボタンを使用すると、予期しない動作が発生する可能性があります。

マニュアルの内容

このマニュアルでは、Local Controller の機能について説明します。このマニュアルの構成は次のとおりです。

- 第 1 章「STM タスク フローの概要」 - STM システムの計画と導入に関するタスクフローを示します。企業のセキュリティ ポリシーと組み合わせて、プロビジョニングおよびモニタリングの 2 つのフェーズに基づいて、構造配置および設定方針を示します。

パート I: プロビジョニング フェーズ - ここでは、MARS と通信するためのネットワーク デバイスのプロビジョニングについて詳しく説明します。デバイス インベントリの実行、MARS アプライアンスと通信するためのレポート デバイスや軽減 デバイスのブートストラップ および設定、およびデバイス側での調整について説明します。

- 第 2 章「レポート デバイスおよび軽減デバイスの概要」 - MARS を正常に配置するために重要な概念を示します。これらの概念には、ネットワークのデバイスの選択、動作レベルの概要のほか、データ プル スケジュールなど多数のデバイスに関連するタスクの実行などが含まれます。
- 第 3 章「ルータおよびスイッチ デバイスの設定」
- 第 4 章「ファイアウォール デバイスの設定」
- 第 5 章「VPN デバイスの設定」
- 第 6 章「ネットワークベース IDS および IPS デバイスの設定」
- 第 7 章「ホストベース IDS および IPS デバイスの設定」
- 第 8 章「アンチウィルス デバイスの設定」
- 第 9 章「脆弱性評価デバイスの設定」
- 第 10 章「汎用、Solaris、Linux、および Windows アプリケーション ホストの設定」
- 第 11 章「データベース アプリケーションの設定」
- 第 12 章「Web サーバ デバイスの設定」
- 第 13 章「Web プロキシ デバイスの設定」
- 第 14 章「AAA デバイスの設定」
- 第 15 章「カスタム デバイスの設定」

パート II: モニタリング フェーズ - ここでは、MARS を正しく使用してネットワークをモニタするために重要な概念を示します。これらの概念にはインスペクション規則の定義や、インシデントの調査などが含まれます。

- 第 16 章「ネットワークの概要」 - Dashboard、Network Status、および My Reports ページなどの Summary ページについて説明します。
- 第 17 章「ケース管理」 - ケースを使用してアカウントビリティを実現し、ワークフローを改善する方法を示します。
- 第 18 章「インシデントの調査」 - インシデントおよびフォールス ポジティブについて説明します。
- 第 19 章「規則」 - MARS 規則の処理方法を示します。
- 第 20 章「Management タブの概要」 - イベント、ネットワーク、変数、ホスト、サービス、および MARS ユーザの管理方法を示します。
- 第 21 章「システム メンテナンス」 - MARS のメンテナンス作業の一部を示します。

次の付録もあります。

- 付録 A 「アラートの送信」 - アラートを送信するように MARS を設定する方法について説明します。
- 付録 B 「クエリーの作成」 - MARS の長期クエリーを表示および作成する方法について説明します。
- 付録 C 「レイヤ 2 パスおよび軽減機能の設定」 - MARS と連携するようにレイヤ 2 パスおよび軽減機能を設定する方法を示します。
- 付録 D 「正規表現リファレンス」 - PCRE でサポートされている正規表現の構文および意味を示します。
- 付録 E 「日付/時刻フォーマットの仕様」 - 日付/時刻フィールドの解析は、Unix strtptime() 標準 C ライブラリ関数を使用してサポートされています。
- 用語集 - MARS に関連する用語集です。

マニュアルの入手方法

シスコ製品のマニュアルおよびその他の資料は、Cisco.com で入手することができます。また、テクニカル サポートおよびその他のテクニカル リソースは、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法について説明します。

Cisco.com

シスコの最新のマニュアルは、次の URL からアクセスしてください。

<http://www.cisco.com/univercd/home/home.htm>

シスコの Web サイトには、次の URL からアクセスしてください。

<http://www.cisco.com>
<http://www.cisco.com/jp>

シスコの Web サイトの各国語版へは、次の URL からアクセスしてください。

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

シスコ製品のマニュアルおよびその他の資料は、製品に付属の Documentation DVD パッケージでご利用いただけます。Documentation DVD は定期的に更新されるので、印刷資料よりも新しい情報が得られます。この DVD パッケージは、単独で入手することができます。

Cisco.com (Cisco Direct Customers) に登録されている場合、Ordering ツールまたは Cisco Marketplace から Cisco Documentation DVD (Customer Order Number DOC-DOCDVD=) を発注できます。

Cisco Ordering ツール:

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

マニュアルの発注方法

マニュアルの発注方法については、次の URL にアクセスしてください。

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

シスコ製品のマニュアルは、次の方法でご発注いただけます。

- ・ Cisco.com (Cisco Direct Customers) に登録されている場合、Ordering ツールからシスコ製品のマニュアルを発注できます。次の URL にアクセスしてください。

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- ・ Cisco.com に登録されていない場合、製品を購入された代理店へお問い合わせください。

シスコ製品のセキュリティ

シスコでは、無償の Security Vulnerability Policy ポータルを次の URL で提供しています。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このサイトから、以下のタスクを実行できます。

- ・ シスコ製品における脆弱性を報告する。
- ・ シスコ製品のセキュリティ問題に対する支援を受ける。
- ・ シスコからのセキュリティ情報を入手するために登録を行う。

シスコ製品に関するセキュリティ勧告および注意のリストが以下の URL で確認できます。

<http://www.cisco.com/go/psirt>

勧告および注意事項が変更された際に、リアルタイムで確認したい場合は、以下の URL から Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) にアクセスできます。

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

シスコ製品のセキュリティ問題の報告

シスコでは、安全な製品を提供することを目指しています。製品のリリース前に社内でテストを実施し、すべての脆弱性を迅速に修正するように努めております。お客様がシスコ製品の脆弱性を発見したと思われる場合は、次の PSIRT にご連絡ください。

- ・ 緊急度の高い問題—security-alert@cisco.com
- ・ 緊急度の低い問題—psirt@cisco.com



ヒント お客様が第三者に知られたくない情報をシスコに送信する場合、Pretty Good Privacy (PGP) または PGP と互換性のある製品を使用して情報を暗号化することを推奨します。PSIRT は、PGP バージョン 2.x ~ 8.x と互換性のある暗号化情報を取り扱うことができます。

無効な暗号鍵または失効した暗号鍵は使用しないでください。PSIRT と通信する際は、次の公開鍵サーバの一覧に記載されている有効な公開鍵を使用してください。

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

緊急度の高い問題の場合、次の電話番号で PSIRT に問い合わせることができます。

- ・ 1 877 228-7302
- ・ 1 408 525-6532

テクニカル サポート

Cisco Technical Support では、シスコシステムズとサービス契約を結んでいるお客様、パートナー、リセラー、販売店を対象として、評価の高い 24 時間体制のテクニカル サポートを提供しています。Cisco.com の Cisco Technical Support Web サイトでは、広範囲にわたるオンラインでのサポートリソースを提供しています。さらに、Technical Assistance Center (TAC) では、電話でのサポートも提供しています。シスコシステムズとサービス契約を結んでいない場合は、リセラーにお問い合わせください。

Cisco Technical Support Web サイト

Cisco Technical Support Web サイトでは、オンラインで資料やツールを利用して、トラブルシューティングやシスコ製品およびテクノロジーに関する技術上の問題の解決に役立てることができます。Cisco Technical Support Web サイトは、1 年中いつでも利用することができます。次の URL にアクセスしてください。

<http://www.cisco.com/techsupport>

Cisco Technical Support Web サイト上のツールにアクセスする際は、いずれも Cisco.com のログイン ID およびパスワードが必要です。サービス契約が有効で、ログイン ID またはパスワードを取得していない場合は、次の URL で登録手続きを行ってください。

<http://tools.cisco.com/RPF/register/register.do>



注 テクニカル サポートにお問い合わせいただく前に、Cisco Product Identification (CPI) ツールを使用して、製品のシリアル番号をご確認ください。CPI ツールへは、Documentation & Tools の下にある **Tools & Resources** リンクをクリックして、Cisco Technical Support Web サイトからアクセスできます。Alphabetical Index ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下にある **Cisco Product Identification Tool** リンクをクリックしてください。CPI ツールは、製品 ID またはモデル名、ツリー表示、または特定の製品に対する **show** コマンド出力のコピー & ペーストによる 3 つの検索オプションを提供します。検索結果には、シリアル番号のラベルの場所がハイライトされた製品の説明図が表示されます。テクニカル サポートにお問い合わせいただく前に、製品のシリアル番号のラベルを確認し、メモなどに控えておいてください。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト (<http://www.cisco.com/tac>) のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

<http://www.cisco.com/jp/go/tac>

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。

Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

<http://www.cisco.com/jp/register>

Service Request ツールの使用

オンラインの TAC Service Request ツールを使えば、S3 および S4 の問題について最も迅速にテクニカル サポートを受けられます (ネットワークの障害が軽微である場合、あるいは製品情報が必要な場合)。状況をご説明いただくと、TAC Service Request ツールが推奨される解決方法を提供します。これらの推奨リソースを使用しても問題が解決しない場合は、TAC の技術者が対応します。TAC Service Request ツールは次の URL からアクセスできます。

<http://www.cisco.com/techsupport/servicerequest>

問題が S1 または S2 であるか、インターネットにアクセスできない場合は、電話で TAC にご連絡ください (運用中のネットワークがダウンした場合、あるいは重大な障害が発生した場合)。S1 および S2 の問題には TAC の技術者がただちに対応し、業務を円滑に運営できるよう支援します。

電話でテクニカル サポートを受ける際は、次の番号のいずれかをご使用ください。

アジア太平洋: +61 2 8446 7411 (オーストラリア: 1 800 805 227)

EMEA: +32 2 704 55 55

米国: 1 800 553-2447

TAC の連絡先一覧については、次の URL にアクセスしてください。

<http://www.cisco.com/techsupport/contacts>

問題の重大度の定義

すべての問題を標準形式で報告するために、問題の重大度を定義しました。

重大度 1 (S1) — ネットワークがダウンし、業務に致命的な損害が発生する場合。24 時間体制であらゆる手段を使用して問題の解決にあたります。

重大度 2 (S2) — ネットワークのパフォーマンスが著しく低下、またはシスコ製品のパフォーマンス低下により業務に重大な影響がある場合。通常の業務時間内にフルタイムで問題の解決にあたります。

重大度 3 (S3) — ネットワークのパフォーマンスが低下しているが、ほとんどの業務運用が機能している場合。通常の業務時間内にサービスの復旧を行います。

重大度 4 (S4) — シスコ製品の機能、インストレーション、基本的なコンフィギュレーションについて、情報または支援が必要で、業務への影響がほとんどまたはまったくない場合。

その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワークソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手することができます。

- ・ Cisco Marketplace では、さまざまなシスコの書籍、参考資料、およびロゴ入り商品を提供しています。Cisco Marketplace には、次の URL からアクセスしてください。

<http://www.cisco.com/go/marketplace/>

- ・ Cisco Press では、ネットワーク、トレーニング、認定関連の出版物を幅広く発行しています。初心者から上級者まで、さまざまな読者向けの出版物があります。Cisco Press の最新の出版情報などについては、次の URL からアクセスしてください。

<http://www.ciscopress.com/>

- ・ 『Packet』は、シスコシステムズが発行するテクニカル ユーザ向けの季刊誌で、インターネットやネットワークへの投資を最大限に活用するのに役立ちます。『Packet』には、ネットワーク分野の最新動向、テクノロジーの進展、およびシスコの製品やソリューションに関する記事をはじめ、ネットワークの配置やトラブルシューティングのヒント、設定例、お客様の事例研究、認定やトレーニングに関する情報、および多数の詳細なオンライン リソースへのリンクが盛り込まれています。『Packet』には、次の URL からアクセスしてください。

<http://www.cisco.com/packet>

- ・ 『iQ Magazine』は、シスコのテクノロジーを使って収益の増加、ビジネス効率の向上、およびサービスの拡大を図る方法について学ぶことを目的とした、シスコシステムズが発行する成長企業向けの季刊誌です。この季刊誌は、実際の事例研究や事業戦略を用いて、これら企業が直面するさまざまな課題や、問題解決の糸口となるテクノロジーを明確化し、テクノロジーの投資に関して読者が正しい決断を行う手助けをします。『iQ Magazine』には、次の URL からアクセスしてください。

<http://www.cisco.com/go/iqmagazine>

- ・ 『Internet Protocol Journal』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコシステムズが発行する季刊誌です。『Internet Protocol Journal』には、次の URL からアクセスしてください。

<http://www.cisco.com/ipj>

- ・ シスコシステムズは最高水準のネットワーク関連のトレーニングを実施しています。トレーニングの最新情報については、次の URL からアクセスしてください。

<http://www.cisco.com/en/US/learning/index.html>