配置プランニングのガイドライン

この章では、1 台または複数の MARS アプライアンスの配置に関する情報について説明します。ここで説明する内容は、次のとおりです。

MARS のコンポーネント

配置をプランニングする場合、ネットワーク上のレポーティング デバイスから送信されるトラフィック量を処理できるように、MARS アプライアンスの容量を考慮する必要があります。購入するモデルおよびネットワーク上での配置場所は、ネットワークまたはセグメント上で予測される持続的な Events per Second（EPS）および NetFlow Flows per Second（FPS）によって異なります。

各モデルでサポートされる EPS および FPS レートの詳細は、*Cisco Security Monitoring, Analysis and Response System:Data Sheet* を参照してください。また、このデータシートには、フォーム ファクタ、消費電力要件、ディスク タイプなど、各アプライアンス モデルの詳細な技術仕様が記載されています。

サポート装置

*サポート装置*とは、MARS が使用するネットワーク サービスを提供するネットワーク装置またはホストのことです。表 2-1 に、配置プランニングに役立つように、任意および必須のサポート装置を示します。

表 2-1　サポート装置とその役割

サポート装置のタイプ	必要性	説明
E メール サーバ	必要	MARS は、E メール サーバを使用して、管理レポートおよび通知を配信します。
NTP サーバ	単一装置の配置には不要 Global Controller を含む配置には必要	すべてのアプライアンス上にタイムゾーンおよび UTC を設定する必要があります。受信メッセージのタイムスタンプは、正確なインシデントの相関性を把握するうえで重要です。
DNS サーバ	必要	MARS は、DNS を使用してモニタ対象デバイスのホスト名を解決します。これにより、レポートおよびクエリーを判読しやすくなります。
Internal Upgrade Server	不要	これらのサーバの設定および使用方法の詳細は、アプライアンス ソフトウェアのアップグレードのチェックリスト（p.6-8）を参照してください。
GUI クライアント	必要	アプライアンスを管理するための GUI を実行するホストです。

必要なトラフィック フロー

*必要なトラフィック フロー*は、ゲートウェイにより MARS アプライアンスがレポーティング デバイス、脅威軽減デバイス、または（サポート装置にリストされている）サポート装置から分離された場合、ゲートウェイにより許可する必要があるトラフィックを識別します。また、Global Controller と、モニタ対象の Local Controller 間のトラフィック フローも許可する必要があります。

次の表に、トラフィック フローのカテゴリ、必要なプロトコル、および必要な許可期間を示します。

表 2-2　必要なトラフィック フローおよびポート

カテゴリ	プロトコル	許可の必要性	説明
管理 GUI	HTTPS/SSL（TCP ポート 443）	必須	アプライアンスを効率的に使用して、GUI ベースの管理トラフィックをブロックすることはできません。このトラフィックは、Global Controller から Local Controller に対して、また MARS アプライアンスからアプライアンスを管理するコンピュータに対して、必ずイネーブルでなければなりません。
管理 CLI	SSH（TCP 22）	必要に応じて許可	—
サポート サーバおよびサービス	DNS（TCP および UDP ポート 53） NTP（TCP/UDP ポート 123） SMTP（TCP ポート 25） ICMP（IP レベル サービス） NFS		SMTP は、発信メール サービスに使用されます。ICMP は、診断およびトラブルシューティングに役立ち、ダイナミックな脆弱性スキャナに必要です。NFS は、MARS のデータ アーカイブを保持するために、Network Attached Storage（NAS）サーバにより使用されます。NFS ポートはネゴシエートされるので、NAS サーバは MARS アプライアンスと同じネットワーク セグメント上に配置することを推奨します。
GUI からのアップグレード	HTTPS または FTP（TCP ポート 20 および 21）	必要に応じて許可	任意に GUI から実行する場合に必要です。
CLI からのアップグレード	HTTPS、HTTP（TCP ポート 80）、または FTP	必要に応じて許可	コマンドラインでは、DVD ドライブからのアップグレードも可能です。この場合、追加のオープン ポートは不要です。
レポーティング デバイスまたは脅威軽減デバイスの検出	Telnet（TCP ポート 23） SSH FTP SNMP（TCP 161）	必須	MARS アプライアンスは、動作確認のためにデバイスに定期的に通信します。

表 2-2　必要なトラフィック フローおよびポート（続き）

カテゴリ	プロトコル	許可の必要性	説明
レポーティング デバイスまたは脅威軽減デバイスのモニタ	HTTPS SSH SNMP Telnet FTP PostOffice（UDP ポート 45000） RDEP（SSL） SDEE（SSL） Syslog（UDP ポート 514）	必須	
Grobal Controller および Local Controller のデータ同期	プロプライエタリ（ポート 8444）	必須	このポートは、Grobal Controller で正確なデータ相関性を保持するために、外部インターフェイスおよび内部インターフェイスで持続的にオープンしておく必要があります。
	NetFlow（TCP ポート 2055）		スイッチ（コアではなく、分散スイッチおよびアクセス スイッチ）間のスパニング ツリーをイネーブルにする必要があります。 Admin > NetFlow Config ページで、NetFlow トラフィックを待ち受けるアプライアンス上のポートを変更できます。
	OPSEC-LEA（TCP ポート 18184） OPSEC-CA（TCP 18210） SSLCA（TCP ポート 18184） OPSEC-CPMI（TCP ポート 18190）		Check Point デバイスのみで使用されます。 CA は、OPSEC アプリケーションの証明書の抽出に使用されます。
	Oracle Database Listener（TCP ポート 1521）		Oracle のみで使用されます。
	MS SQL（TCP ポート 1433）		FoundStone および eEye で使用されます。