セキュリティ、インターネット アクセス、および通信ポート

防御センターを保護するには、保護された内部ネットワークにそれをインストールしてください。防御センターは必要なサービスとポートだけを使用するよう設定されますが、ファイアウォール外部からの攻撃がそこまで（または管理対象デバイスまで）決して到達できないようにする必要があります。

防御センターとその管理対象デバイスが同じネットワーク上に存在する場合は、デバイス上の管理インターフェイスを、防御センターと同じ保護された内部ネットワークに接続できます。これにより、防御センターからデバイスを安全に制御することができます。

アプライアンスの展開方法とは無関係に、アプライアンス間通信は暗号化されます。それでも、分散型サービス拒否（DDoS）や中間者攻撃などの手段でシスコ アプライアンス間の通信が中断、ブロック、または改ざんされないよう何らかの対策を講じる必要があります。

また、FireSIGHT システムの機能によってはインターネット接続が必要となることにも注意してください。デフォルトで、すべてのシスコ アプライアンスはインターネットに直接接続するよう設定されます。加えて、システムで特定のポートを開いたままにしておく必要があります。その目的は基本的なアプライアンス間通信、セキュアなアプライアンス アクセス、および特定のシステム機能を正しく動作させるために必要なローカル / インターネット リソースへのアクセスを可能にすることです。

ヒント

Sourcefire Software for X-Series を除いて、シスコ アプライアンスではプロキシ サーバを使用できます。詳細については、「ネットワーク設定の構成」（P.51-9）および「http-proxy」（P.D-32）を参照してください。

詳細については、以下を参照してください。

- 「インターネット アクセスの要件」（P.E-1）
- 「通信ポートの要件」（P.E-3）

インターネット アクセスの要件

デフォルトで、シスコ アプライアンスはポート 443/tcp（HTTPS）および 80/tcp（HTTP）でインターネットに直接接続するよう設定されます。これらのポートは、すべてのシスコ アプライアンス上でデフォルトでオープンになっています（「通信ポートの要件」（P.E-3）を参照）。ほとんどのシスコ アプライアンスではプロキシ サーバを使用できることに注意してください（「ネットワーク設定の構成」（P.51-9）を参照）。

継続的な運用を維持するには、ハイ アベイラビリティ ペアの両方の防御センターがインターネット アクセスを備えている必要があります。機能によっては、プライマリ防御センターがインターネットに接続した後、同期プロセス中にセカンダリと情報を共有します。このため、プライマリで障害が発生した場合は、「ハイ アベイラビリティ ステータスのモニタリングおよび変更」（P.6-11）に記載されているように、セカンダリをアクティブに昇格させる必要があります。

次の表に、FireSIGHT システムの特定の機能におけるインターネット アクセス要件を示します。

表 E-1　FireSIGHT システム機能のインターネット アクセス要件

機能	インターネット アクセスの目的	アプライアンス	ハイ アベイラビリティの考慮事項
動的分析：照会	動的分析のために、送信済みファイルの脅威スコアをクラウドに照会します。	防御センター	ペア化された防御センターは、個別に脅威スコアをクラウドに照会します。
動的分析：送信	動的分析用にファイルをクラウドに送信します。	管理対象デバイス（X-Series を含む）	n/a
FireAMP 統合	シスコからエンドポイント ベースの（FireAMP）マルウェア イベントを受信します。	防御センター	クラウド接続は同期されません。両方の防御センターで設定してください。
侵入ルール、VDB、および GeoDB の更新	侵入ルール、GeoDB、または VDB の更新をアプライアンスに直接ダウンロードするか、ダウンロードをスケジュールします。	防御センター	侵入ルール、GeoDB、および VDB の更新は同期されます。
ネットワークベースの AMP	マルウェア クラウド検索を実行します。	防御センター	ペア化された防御センターは、個別にクラウド検索を実行します。
RSS フィード ダッシュボード ウィジェット	シスコを含む外部ソースから RSS フィード データをダウンロードします。	すべて（仮想デバイスと X-Series を除く）	フィード データは同期されません。
セキュリティ インテリジェンス フィルタリング	シスコ インテリジェンス フィードを含む外部ソースから、セキュリティ インテリジェンス フィード データをダウンロードします。	防御センター	プライマリ防御センターがフィード データをダウンロードして、セカンダリと共有します。プライマリに障害が発生した場合は、セカンダリをアクティブに昇格させてください。
システム ソフトウェアの更新	システム更新をアプライアンスに直接ダウンロードするか、ダウンロードをスケジュールします。	すべて（仮想デバイスと X-Series を除く）	システム更新は同期されません。

表 E-1　FireSIGHT システム機能のインターネット アクセス要件 （続き）

機能	インターネット アクセスの目的	アプライアンス	ハイ アベイラビリティの考慮事項
URL フィルタリング	アクセス コントロール用にクラウド ベースの URL カテゴリおよびレピュテーション データをダウンロードし、未分類 URL の検索を実行します。	防御センター	プライマリ防御センターは URL フィルタリング データをダウンロードして、セカンダリと共有します。プライマリに障害が発生した場合は、セカンダリをアクティブに昇格させてください。
whois	外部ホストの whois 情報を要求します。	すべて（仮想デバイスと X-Series を除く）	whois 情報を要求するアプライアンスは、インターネット アクセスを備えている必要があります。

通信ポートの要件

Sourcefire 3D System アプライアンスは、（デフォルトでポート 8305/tcp を使用する）双方向 SSL 暗号化通信チャネルを使って通信します。基本的なアプライアンス間通信用にこのポートを開いたままにする**必要があります**。他のオープン ポートの役割は次のとおりです：

- アプライアンスの Web インターフェイスにアクセスする
- アプライアンスへのリモート接続を保護する
- 特定のシステム機能を正しく動作させるために必要なローカル / インターネット リソースへのアクセスを可能にする

一般に、機能関連のポートは、該当する機能を有効化または設定する時点まで、閉じたままになります。たとえば、防御センターをユーザ エージェントに接続するまでは、エージェント通信ポート（3306/tcp）は閉じたままになります。別の例として、LOM を有効にするまでは、シリーズ 3 アプライアンス上のポート 623/udp が閉じたままになります。

注意　開いたポートを閉じると展開にどのような影響が及ぶか理解するまでは、開いたポートを**閉じないでください**。

たとえば、管理デバイス上のポート 25/tcp（SMTP）アウトバウンドを閉じた場合、個別の侵入イベントに関する電子メール通知をデバイスから送信できなくなります（『「侵入ルールの外部アラートの設定」（P.31-1）』を参照）。別の例として、ポート 443/tcp（HTTPS）を閉じることにより物理管理対象デバイスの Web インターフェイスへのアクセスを無効にできますが、それと同時に、動的分析のためにデバイスから疑わしいマルウェア ファイルをクラウドに送信できなくなります。

次のように、システムのいくつかの通信ポートを変更できることに注意してください。

- システムと認証サーバの間の接続を設定するときに、LDAP および RADIUS 認証用のカスタム ポートを指定できます（「LDAP 認証サーバの指定」（P.48-17）および「RADIUS 接続の設定」（P.48-34）を参照）。
- 管理ポート（8305/tcp）を変更できます（「ネットワーク設定の構成」（P.51-9）を参照）。ただし、シスコでは、デフォルト設定を維持することを**強く**推奨しています。管理ポートを変更する場合は、相互に通信する必要のある展開内のすべてのアプライアンスでそれを変更する必要があります。

- ポート 32137/tcp を使用して、アップグレード対象の防御センターと シスコの通信を可能にすることができます。ただし、シスコでは、バージョン 5.3 以降の新規インストールのデフォルトであるポート 443 に切り替えることを推奨しています。詳細については、「クラウド通信の有効化」（P.51-27）を参照してください。

次の表は、FireSIGHT システムの機能を最大限に活用できるように、各アプライアンス タイプで必要なオープン ポートを示しています。

表 E-2　FireSIGHT システムの機能と運用のためのデフォルト通信ポート

ポート	説明	方向	開いているアプライアンス	目的
22/tcp	SSH/SSL	双方向	すべて	アプライアンスへのセキュアなリモート接続を可能にします。
25/tcp	SMTP	アウトバウンド	すべて	アプライアンスから電子メール通知とアラートを送信します。
53/tcp	DNS	アウトバウンド	すべて	DNS を使用します。
67/udp 68/udp	DHCP	アウトバウンド	すべて（X-Series を除く）	DHCP を使用します。 (注)　これらのポートはデフォルトで**閉じられています**。
80/tcp	HTTP	アウトバウンド	すべて（仮想デバイスと X-Series を除く）	RSS フィード ダッシュボード ウィジェットからリモート Web サーバに接続できるようにします。
		双方向	防御センター	HTTP 経由でカスタムおよびサードパーティのセキュリティ インテリジェンス フィードを更新します。 URL カテゴリおよびレピュテーション データをダウンロードします（さらにポート 443 も必要）。
161/udp	SNMP	双方向	すべて（X-Series を除く）	SNMP ポーリング経由でアプライアンスの MIB にアクセスできるようにします。
162/udp	SNMP	アウトバウンド	すべて	リモート トラップ サーバに SNMP アラートを送信します。
389/tcp 636/tcp	LDAP	アウトバウンド	すべて（仮想デバイスと X-Series を除く）	外部認証用に LDAP サーバと通信します。
389/tcp 636/tcp	LDAP	アウトバウンド	防御センター	検出された LDAP ユーザに関するメタデータを取得します。
443/tcp	HTTPS	インバウンド	すべて（仮想デバイスと X-Series を除く）	アプライアンスの Web インターフェイスにアクセスします。

表 E-2　FireSIGHT システムの機能と運用のためのデフォルト通信ポート （続き）

ポート	説明	方向	開いているアプライアンス	目的
443/tcp	HTTPS AMQP クラウド通信	双方向	防御センター	次のものを取得します： • ソフトウェア、侵入ルール、VDB、および GeoDB の更新 • URL カテゴリおよびレピュテーション データ（さらにポート 80 も必要） • シスコ インテリジェンス フィードおよび他のセキュアなセキュリティ インテリジェンス フィード • エンドポイント ベースの（FireAMP）マルウェア イベント • ファイルに関してネットワーク トラフィックで検出されたマルウェアの性質 • 送信されたファイルに関する動的分析情報
			シリーズ 2デバイスと シリーズ 3 デバイス	デバイスのローカル Web インターフェイスを使用してソフトウェア更新をダウンロードします。
			シリーズ 3および仮想デバイス、X-Series	動的分析のためにファイルを送信します。
514/udp	syslog	アウトバウンド	すべて	リモート syslog サーバにアラートを送信します。
623/udp	SOL/LOM	双方向	シリーズ 3	Serial Over LAN（SOL）接続を使用して Lights-Out Management を実行できるようにします。
1500/tcp 2000/tcp	データベース アクセス	インバウンド	防御センター	サードパーティ クライアントによるデータベースへの読み取り専用アクセスを可能にします。
1812/udp 1813/udp	RADIUS	双方向	すべて（仮想デバイスと X-Series を除く）	外部認証とアカウンティングのために RADIUS サーバと通信します。
3306/tcp	ユーザ エージェント	インバウンド	防御センター	ユーザ エージェントと通信します。
8302/tcp	eStreamer	双方向	すべて（仮想デバイスと X-Series を除く）	eStreamer クライアントと通信します。
8305/tcp	アプライアンス通信	双方向	すべて	展開におけるアプライアンス間で安全に通信します。**必須です。**

表 E-2　FireSIGHT システムの機能と運用のためのデフォルト通信ポート （続き）

ポート	説明	方向	開いているアプライアンス	目的
8307/tcp	ホスト入力クライアント	双方向	防御センター	ホスト入力クライアントと通信します。
32137/tcp	クラウド通信	双方向	防御センター	アップグレード対象の防御センターと Collective Security Intelligence クラウド クラウドの通信を可能にします。