仮想アプライアンスの概要

Cisco FireSIGHT® システムは、検出されたアプリケーション、ユーザ、および URL に基づいてネットワークへのアクセスを制御する機能と、業界トップのネットワーク侵入防御システムのセキュリティを統合したものです。

シスコは、VMware vSphere と VMware vCloud Director のホスティング環境用に 64 ビット仮想防御センターおよびバーチャル デバイスをパッケージ化しています。vCenter または VMware vCloud Director を使用して、64 ビット仮想防御センターと 64 ビット仮想管理対象デバイスを ESXi ホストに展開できます。仮想アプライアンスは e1000（1 Gbit/s）インターフェイスを使用します。また、デフォルトのインターフェイスを vmxnet3（10 Gbit/s）インターフェイスに置き換えることもできます。また、仮想アプライアンスのパフォーマンスと管理を向上させるために VMware ツールを使用することもできます。

防御センターによって、システムの一元管理コンソールとデータベース リポジトリが提供されます。仮想デバイスは次のように、パッシブ展開またはインライン展開の仮想ネットワークまたは物理ネットワークのトラフィックを検査できます。

- パッシブ展開の仮想デバイスは、ネットワーク上を流れるトラフィックを単純に監視します。
- パッシブ センシング インターフェイスはすべてのトラフィックを無条件で受信し、これらのインターフェイスで受信されたトラフィックは再送信されません。
- インライン展開の仮想デバイスでは、ネットワーク上のホストの可用性、整合性、または機密性に影響を及ぼす可能性がある攻撃からネットワークを保護できます。インライン デバイスは単純な侵入防御システムとして展開できます。インライン デバイスを設定して、アクセス制御を実行したり、他の方法でネットワーク トラフィックを管理したりすることができます。
- インライン インターフェイスはすべてのトラフィックを無条件で受信し、展開環境での設定によって明示的に廃棄されている場合を除き、これらのインターフェイスで受信されたトラフィックは再送信されます。

仮想防御センターは物理デバイス、Blue Coat X-Series 向け Cisco NGIPS、および Cisco ASA with FirePOWER Services（ASA FirePOWER）を管理することができ、物理防御センターはバーチャル デバイスを管理できます。ただし、仮想アプライアンスはシステムのハードウェア ベースの機能をサポートしません。仮想防御センターは高可用性をサポートせず、仮想デバイスはクラスタリング、スタッキング、スイッチング、ルーティングなどをサポートしません。物理 FireSIGHT システム アプライアンスの詳細については、『*FireSIGHT System Installation Guide*』を参照してください。

このインストール ガイドは、仮想 FireSIGHT システム アプライアンス（デバイスおよび防御センター）の展開、インストール、セットアップに関する情報を提供します。また、vSphere クライアント、VMware vCloud Director Web ポータル、VMware ツール（オプション）を含む VMware 製品の機能と名称について精通していることを想定しています。

次のトピックで FireSIGHT システム 仮想アプライアンスについて説明します。

- 「FireSIGHT システム 仮想アプライアンス」(P.1-2)
- 「仮想アプライアンスの機能について」(P.1-3)
- 「FireSIGHT システム のコンポーネント」(P.1-7)
- 「仮想アプライアンスのライセンス」(P.1-12)
- 「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」(P.1-14)

FireSIGHT システム 仮想アプライアンス

FireSIGHT システム *仮想アプライアンス*は、トラフィック検知の管理対象 *バーチャル デバイス*か、または管理 *仮想*防御センターのいずれかになります。詳細については、次の項を参照してください。

- 「仮想防御センター」(P.1-2)
- 「仮想管理対象デバイス」(P.1-2)
- 「仮想アプライアンスの機能について」(P.1-3)
- 「動作環境の前提条件」(P.1-6)
- 「仮想アプライアンスのパフォーマンス」(P.1-7)

仮想防御センター

防御センターは、FireSIGHT システム配置環境の集中管理ポイントとイベント データベースを提供します。仮想防御センターは、侵入、ファイル、マルウェア、検出、接続、およびパフォーマンス データを集約し、相互に関連付けます。これには、特定のホストにおけるイベントの影響を評価し、ホストにセキュリティ侵害をマークするタグ付けをすることが含まれます。これにより、デバイス間で交わされる情報の監視、ネットワーク上で発生するアクティビティ全体の評価や制御が可能になります。

仮想防御センターの主な機能は次のとおりです。

- デバイス、ライセンス、およびポリシーの管理
- 表、グラフ、図に表示されるイベント情報と状況情報
- ヘルスとパフォーマンスのモニタリング
- 外部通知とアラート
- リアルタイムに脅威に対処するための関連付け、侵害の痕跡、および修復機能
- カスタムもしくはテンプレートベースのレポート作成

仮想管理対象デバイス

組織内のネットワーク セグメントに展開されたバーチャル デバイスは、分析用にトラフィックをモニタします。パッシブに展開されたバーチャル デバイスは、ネットワーク トラフィック情報を把握するのに役立ちます。インライン展開の場合、仮想デバイスを使用して、複数の基準に基づいてトラフィック フローに影響を与えることができます。各デバイスには、モデルとライセンスに応じて次のような特徴があります。

- 組織のホスト、オペレーティング システム、アプリケーション、ユーザ、ファイル、ネットワーク、および脆弱性に関する詳細情報を収集する

- ネットワークベースのさまざまな基準、およびアプリケーション、ユーザ、URL、IP アドレスの評価、および侵入やマルウェアの調査結果を含めた他の基準によって、ネットワーク トラフィックをブロックまたは許可する

仮想デバイスには Web インターフェイスが**ありません**。仮想デバイスはコンソールとコマンドラインを使用して設定し、防御センターで管理する必要があります。

仮想アプライアンスの機能について

仮想アプライアンスは物理アプライアンスの機能の多くを備えています。

- 仮想防御センターは、仮想防御センターの高可用性ペアを作成できないことを除き、物理防御センターと同じ機能を持っています。FireSIGHT ライセンスがある場合、仮想防御センターは 50,000 件のホストおよびユーザを監視できます。
- 仮想デバイスは物理デバイスのトラフィックおよびブロッキング分析機能を持っています。ただし、スイッチング、ルーティング、VPN、および他のハードウェア ベース、冗長性、およびリソース共有の機能は実行できません。

仮想防御センターの機能について

「表 1-1 仮想防御センターでサポートされる機能」(P.1-3)に、システムの主要な機能と仮想防御センターの比較を示します。ここでは、ユーザがそれらの機能をサポートするデバイスを管理し、適切なライセンスがインストールされ適用されていることを想定しています。

仮想アプライアンスでサポートされる機能およびライセンスの要約については、「FireSIGHT システム のコンポーネント」(P.1-7)および「仮想アプライアンスのライセンス」(P.1-12)を参照してください。

仮想防御センターは、シリーズ 2、シリーズ 3、ASA FirePOWER、およびX-シリーズ デバイスを管理できることに留意しておいてください。同様に、シリーズ 2 およびシリーズ 3 の防御センターは仮想デバイスを管理できます。デバイス ベース機能（スタック構成、スイッチング、ルーティングなど）に関する防御センターの列は、仮想防御センターがそれらの機能を実行するためにデバイスを管理および設定できるかどうかを示します。たとえば、仮想デバイスで VPN の設定はできませんが、仮想防御センターを使用すれば VPN 展開でシリーズ 3 デバイスを管理できます。

表 1-1　　仮想防御センターでサポートされる機能

特徴または機能	仮想防御センター
管理対象デバイスによって報告されるディスカバリ データ（ホスト、アプリケーション、およびユーザ）を収集し、組織のネットワーク マップを作成する	yes
ネットワーク トラフィックの位置情報データを表示する	yes
侵入検知と防御（IPS）の配置を管理する	yes
セキュリティ インテリジェンスのフィルタリングを実行するデバイスを管理する	yes
位置情報ベースのフィルタリングを含む単純なネットワークベース制御を実行するデバイスを管理する	yes
アプリケーション制御を実行するデバイスを管理する	yes
ユーザ制御を実行するデバイスを管理する	yes

表 1-1　仮想防御センターでサポートされる機能（続き）

特徴または機能	仮想防御センター
リテラル URL によってネットワーク トラフィックをフィルタリングするデバイスを管理する	yes
カテゴリおよびレピュテーション別の URL フィルタリングを実行するデバイスを管理する	yes
ファイル タイプによる単純なファイル制御を実行するデバイスを管理する	yes
ネットワークベースの高度なマルウェア対策（AMP）を実行するデバイスを管理する	yes
FireAMP 配置環境からエンドポイントベースのマルウェア（FireAMP）イベントを受信する	yes
デバイスベースのハードウェアベース機能を管理する • 高速パス ルール • 厳密な TCP の適用 • 設定可能バイパス インターフェイス • タップ モード • スイッチングとルーティング • NAT ポリシー • VPN	yes
デバイスベースの冗長性とリソース共有を管理する • デバイス スタック • デバイス クラスタ • Blue Coat X-Series 向け Cisco NGIPSの VAP グループ • クラスタ化スタック	yes
トラフィック チャネルを使用して、内部トラフィックとイベント トラフィックを分離して管理する	yes
複数の管理インターフェイスを使用して、異なるネットワーク上のトラフィックを分離して管理する	yes
ハイ アベイラビリティを確立する	no
マルウェア ストレージ パックをインストールする	no
eStreamer、ホスト入力、またはデータベース クライアントへの接続	yes

仮想管理対象デバイスの機能について

「表 1-2 仮想管理対象デバイスでサポートされる機能」（P.1-5）に、システムの主要な機能と管理対象デバイスの比較を示します。ここでは、管理防御センターから適切なライセンスがインストールされ適用されていることを想定しています。

バージョン 5.4.1 のシステムを実行する防御センターの任意のモデルを使用してバージョン 5.4.1 の仮想デバイスを管理できますが、いくつかのシステム機能は防御センターのモデルによって制限されることに留意してください。たとえば、仮想管理対象デバイスがセキュリティ

インテリジェンス フィルタリング機能をサポートしている場合でも、シリーズ 2 DC500 を使用してその機能を実行する仮想管理対象デバイスを管理することはできません。詳細については、「 仮想防御センターの機能について」(P.1-3)を参照してください。

表 1-2　仮想管理対象デバイスでサポートされる機能

特徴または機能	仮想管理対象デバイス
管理対象デバイスによって報告されるディスカバリ データ(ホスト、アプリケーション、およびユーザ)を収集し、組織のネットワーク マップを作成する	yes
ネットワーク トラフィックの位置情報データを表示する	yes
ネットワーク ディスカバリ:ホスト、アプリケーション、およびユーザ	yes
侵入検知および防御(IPS)	yes
セキュリティ インテリジェンス フィルタリング	yes
アクセス制御:基本的なネットワーク制御	yes
アクセス制御:位置情報ベースのフィルタリング	yes
アクセス制御:アプリケーション制御	yes
アクセス制御:ユーザ制御	yes
アクセス制御:リテラル URL	yes
アクセス制御:カテゴリとレピュテーションによる URL フィルタリング	yes
ファイル制御:ファイル タイプ別	yes
ネットワーク ベースの高度マルウェア防御(AMP)	yes
Automatic Application Bypass	yes
高速パス ルール	no
厳密な TCP の適用	no
設定可能バイパス インターフェイス	no
タップ モード	no
スイッチングとルーティング	no
NAT ポリシー	no
VPN	no
デバイス スタッキング	no
デバイス クラスタリング	no
クラスタ化スタック	no
トラフィック チャネル	no
複数の管理インターフェイス	no
マルウェア ストレージ パック	no
FireSIGHT システム固有のインタラクティブ CLI	yes
eStreamer クライアントへの接続	no

動作環境の前提条件

次のホスティング環境で 64 ビットの仮想アプライアンスをホストできます。

- VMware ESXi 5.5（vSphere 5.5）
- VMware ESXi 5.1（vSphere 5.1）
- VMware vCloud Director 5.1

サポート対象のすべての ESXi バージョンで VMware Tools を有効化できます。VMware Tools のすべての機能については、VMware の Web サイト（http://www.vmware.com/）を参照してください。ホスティング環境の作成については、VMware vCloud Director および VMware vCenter を含む VMwareESXi のマニュアルを参照してください。

仮想アプライアンスは Open Virtual Format（OVF）パッケージを使用します。VMware Workstation、Player、Server、および Fusion は OVF パッケージを認識しないため、サポートされません。また、仮想アプライアンスは、仮想ハードウェアのバージョン 7 の仮想マシンとしてパッケージ化されます。

ESXi ホストとして動作するコンピュータは、次の要件を満たす必要があります。

- 仮想化サポートとして、Intel® Virtualization Technology（VT）または AMD Virtualization™（AMD-V™)テクノロジのいずれかを実現する 64 ビット CPU が必要
- 仮想化は、BIOS 設定で有効化する必要がある
- 仮想デバイスをホストするために、コンピュータには Intel e1000 ドライバと互換性があるネットワーク インターフェイスが必要（PRO 1000MT デュアル ポート サーバ アダプタまたは PRO 1000GT デスクトップ アダプタなど）

詳細については、VMware の Web サイト http://www.vmware.com/resources/guides.html を参照してください。

作成する各仮想アプライアンスでは、ESXi ホストに一定量のメモリ、CPU、およびハードディスク スペースが必要です。デフォルトの設定は、システム ソフトウェアの実行の最小要件であるため、**減らさない**でください。ただし、使用可能なリソースによっては、パフォーマンスを向上させるために仮想アプライアンスのメモリと CPU の数を増やすことができます。次の表に、デフォルトのアプライアンス設定を示します。

表 1-3　　デフォルトの仮想アプライアンス設定

設定	デフォルト	設定調整の可否
メモリ	4 GB	可。仮想デバイスに対して次の量を割り当てる**必要**があります。 • 4 GB 以上 • カテゴリとレピュテーションに基づく URL フィルタリングを使用する場合は 5 GB • 大規模なダイナミック フィードを使用してセキュリティ インテリジェンスのフィルタリングを実行する場合は 6 GB • URL フィルタリングおよびセキュリティ インテリジェンスを実行する場合は 7 GB
仮想 CPU	4	可。最大 8
ハード ディスク プロビジョニング サイズ	40 GB（デバイス） 250 GB（防御センター）	no

仮想アプライアンスのパフォーマンス

仮想アプライアンスのスループットおよび処理能力を正確に予測することは不可能です。次のように、多数の要因がパフォーマンスに大きく影響します。

- ESXi ホストのメモリと CPU の容量
- ESXi ホストで実行されている仮想マシンの総数
- センシング インターフェイスの数、ネットワーク パフォーマンス、およびインターフェイス速度
- 各仮想アプライアンスに割り当てられたリソースの量
- ホストを共有する他の仮想アプライアンスのアクティビティのレベル
- 仮想デバイスに適用されるポリシーの複雑さ

ヒント　VMware は複数のパフォーマンス測定ツールとリソース割り当てツールを備えています。仮想アプライアンスを実行しながら、ESXi ホストでこれらのツールを使用し、トラフィックの監視とスループットの測定を行います。スループットに満足できない場合は、ESXi ホストを共有する仮想アプライアンスに割り当てられたリソースを調整します。

また、仮想アプライアンスのパフォーマンスと管理を向上させるために VMware ツールを有効にできます。あるいは、ホスト上、または仮想パフォーマンスを調べる ESXi ホストの仮想化管理レイヤ（ゲスト レイヤではなく）に、ツール（`esxtop` または VMware/サードパーティのアドオンなど）をインストールできます。VMware ツールを有効にする方法については、『*FireSIGHT System User Guide*』を参照してください。

FireSIGHT システム のコンポーネント

続くセクションでは、組織のセキュリティ、アクセプタブル ユース ポリシー、およびトラフィック管理戦略に貢献する仮想防御センターおよびバーチャル デバイスの主要機能の一部について説明します。シリーズ 2 およびシリーズ 3 アプライアンスでサポートされる追加機能の詳細については、『*FireSIGHT System Installation Guide*』および『*FireSIGHT System User Guide*』を参照してください。

ヒント　仮想アプライアンス機能の多くは、ライセンスとユーザ ロールに依存します。必要に応じて、FireSIGHT システム のマニュアルに機能とタスクごとの要件が記載されています。

以下のトピックでは、組織のセキュリティ、適用可能な使用ポリシー、およびトラフィック管理の戦略に対して有用な FireSIGHT システム の主な機能について説明します。

- 「FireSIGHT」（P.1-8）
- 「アクセス コントロール」（P.1-8）
- 「侵入検知と侵入防御」（P.1-9）
- 「ファイルの追跡、コントロール、マルウェア防御」（P.1-9）
- 「アプリケーション プログラミング インターフェイス」（P.1-10）

FireSIGHT

FireSIGHT™ は、ネットワークの全体像を提供するためにホスト、オペレーティング システム、アプリケーション、ユーザ、ファイル、ネットワーク、位置情報、および脆弱性に関する情報を収集するシスコのディスカバリおよび認識テクノロジーです。

防御センターの Web インターフェイスを使用して、FireSIGHT で収集したデータを表示および分析することができます。また、このデータを使用することで、アクセス コントロールを実施し、侵入ルールの状態を修正できます。また、ホストの相関イベント データに基づいて、ネットワーク上のホストの侵害の痕跡を生成し、追跡できます。

アクセス コントロール

*アクセス制御*はポリシーベースの機能で、ユーザはこれを使用してネットワークを横断できるトラフィックを指定、検査、および記録することが可能です。*アクセス制御ポリシー*は、ネットワーク上のトラフィックをシステムがどのように処理するかを決定します。*アクセス制御ルール*が含まれていないポリシーを使用して、*デフォルト アクション*と呼ばれる以下のいずれかの方法でトラフィックを処理することができます。

- すべてのトラフィックをブロックして、ネットワークに入れない
- すべてのトラフィックを信頼してネットワークに入ることを許可し、検査は行わない
- すべてのトラフィックがネットワークに入ることを許可し、ネットワーク ディスカバリ ポリシーのみを使用してトラフィックを検査する
- すべてのトラフィックがネットワークに入ることを許可し、侵入ポリシーとネットワーク ディスカバリ ポリシーを使用してトラフィックを検査する

アクセス制御ポリシーにアクセス制御ルールを含めて、対象のデバイスがトラフィックをどのように処理するか(簡単な IP アドレスのマッチングから、異なるユーザ、アプリケーション、ポート、および URL が関与する複雑なシナリオまで)、より詳しく定義することができます。それぞれのルールについて、ユーザはルールの *アクション*、つまり侵入またはファイル ポリシーと一致するトラフィックを信頼、監視、ブロック、または検査するかどうかを指定します。

それぞれのアクセス制御ポリシーについてカスタム HTML ページを作成することができます。このページは、システムが HTTP 要求をブロックするときに表示されます。オプションで、ユーザに警告するページを表示することができますが、ユーザはボタンをクリックして最初に要求されたサイトの表示を継続できるようにすることも可能です。

アクセス制御の一部として、セキュリティ インテリジェンス機能により、トラフィックがアクセス制御ルールによって分析される前に特定の IP アドレスをブラックリストに登録(トラフィックの入出を拒否)することができます。システムで地理情報をサポートしている場合は、検出された送信元および宛先の国および大陸に基づいて、トラフィックをフィルタすることもできます。

アクセス制御には、侵入の検知および防御、ファイル コントロール、および高度なマルウェア防御が含まれています。詳細については、次の項を参照してください。

侵入検知と侵入防御

侵入検知および防御により、ユーザはセキュリティ違反のネットワーク トラフィックを監視し、インラインの展開で、悪意のあるトラフィックをブロックまたは改正することができます。

侵入防御はアクセス制御に組み込まれており、ユーザは侵入ポリシーと特定のアクセス制御ルールを関連付けることができます。ネットワーク トラフィックがルールの条件と一致する場合、一致するトラフィックを、侵入ポリシーを使用して分析できます。また、侵入ポリシーをアクセス制御ポリシーのデフォルト アクションに関連付けることもできます。

侵入ポリシーは次のようなさまざまな要素で構成されます。

- プロトコル ヘッダー値、ペイロードの内容、および特定のパケット サイズの特性を検査するルール
- FireSIGHT の推奨事項に基づくルール状態設定
- プリプロセッサやその他の検出およびパフォーマンス機能などの高度な設定
- 関連するプリプロセッサとプリプロセッサ オプション用のイベントを生成可能なプリプロセッサ ルール

ファイルの追跡、コントロール、マルウェア防御

マルウェアの影響を特定し、軽減することを容易にするために、FireSIGHT システム のファイル制御、ネットワーク ファイルのトラジェクトリ、および高度なマルウェア防御のコンポーネントはネットワーク トラフィック内のファイルの伝送を(マルウェア ファイルも含めて)検出、追跡、取得、分析、およびオプションでブロックすることができます。

ファイル制御

*ファイル制御*により、管理対象デバイスは、ユーザが特定のアプリケーション プロトコルを介して特定のタイプのファイルをアップロード(送信)またはダウンロード(受信)するのを検出およびブロックすることができます。ファイル制御は、全体的なアクセス制御設定の一部として設定します。アクセス制御ルールに関連付けられたファイル ポリシーによって、ルールの条件を満たすネットワーク トラフィックが検査されます。

ネットワークベースの高度なマルウェア防御(AMP)

ネットワークベースの*高度なマルウェア対策*(AMP)によって、複数のファイル タイプのマルウェアに関してネットワーク トラフィックを検査できます。バーチャル デバイスは、詳細な分析を行うために、検出されたファイルをハード ドライブに保存できます。

検出されたファイルは、保存済みかどうかに関係なく、ファイルの SHA-256 ハッシュ値を使用して単純な既知の性質の検索を行うために Collective Security Intelligence クラウド に送信できます。また、脅威のスコアを生成する*動的分析*を行うためにファイルを送信することもできます。このコンテキスト情報を使用して、特定のファイルをブロックまたは許可するようにシステムを設定できます。

マルウェア防御をアクセス制御設定全体の一部として設定することができます。アクセス制御ルールに関連付けられているファイル ポリシーは、ルールの条件に一致するネットワーク トラフィックを検査します。

FireAMP の統合

FireAMP はシスコのエンタープライズクラスの高度なマルウェア分析および防御ソリューションで、高度なマルウェアの発生、高度で継続的な脅威、および標的型攻撃を検出、認識、ブロックします。

組織に FireAMP のサブスクリプションがある場合は、個々のユーザが自分のコンピュータやモバイル デバイス（*エンドポイント*とも呼ばれる）に*FireAMP コネクタ*をインストールします。これらの軽量エージェントが Collective Security Intelligence クラウドと通信し、次に Collective Security Intelligence クラウドが防御センターと通信します。

防御センターをクラウドに接続するように設定した後で防御センターの Web インターフェイスを使用して、組織のエンドポイントでのスキャン、検出、および検疫の結果として生成されたエンドポイントベースのマルウェア イベントを表示することができます。また、防御センターは FireAMP のデータを使用して、ホストに対する侵害の痕跡を生成および追跡するとともに、ネットワーク ファイルのトラジェクトリを表示します。

FireAMP 展開を構成するには、*FireAMP* ポータルを使用します。ポータルは、マルウェアをすばやく特定および検疫するうえで有用です。ユーザはマルウェアを発生時に特定し、それらのトラジェクトリを追跡して影響を把握し、正常にリカバリする方法を学習することができます。FireAMP を使用してカスタム保護を作成する、グループ ポリシーに基づいて特定のアプリケーションの実行をブロックする、カスタム ホワイトリストを作成する、といったことも可能です。

詳細については、http://amp.sourcefire.com/を参照してください。

ネットワーク ファイルのトラジェクトリ

ネットワーク ファイル トラジェクトリ機能を使用すれば、ネットワーク全体のファイルの伝送パスを追跡することができます。システムは SHA-256 ハッシュ値を使用してファイルを追跡するため、ファイルを追跡するには、システムで以下のいずれかの処理を行う必要があります。

- ファイルの SHA-256 ハッシュ値を計算し、その値を使用してマルウェアのクラウド ルックアップを実行する
- 防御センターと組織の FireAMP サブスクリプションとの統合を使用して、ファイルについてエンドポイントベースの脅威および検疫データを受け取る

各ファイルには、関連するトラジェクトリ マップが付随しており、これには、一定期間のファイルの転送を視覚的に表したものや、ファイルに関する追加情報が含まれています。

アプリケーション プログラミング インターフェイス

アプリケーション プログラミング インターフェイス（API）を使用してシステムと対話する方法がいくつかあります。詳細については、サポート サイトから追加のドキュメントをダウンロードできます。

eStreamer

Event Streamer（eStreamer）を使用すれば、シスコ アプライアンスからの数種類のイベント データをカスタム開発されたクライアント アプリケーションにストリーム配信できます。クライアント アプリケーションを作成したら、ユーザはそれを eStreamer サーバ（防御センターまたは管理対象デバイス）に接続し、eStreamer サービスを開始して、データのやりとりを始めることができます。

eStreamer の統合ではカスタム プログラミングが必要ですが、これによりユーザはアプライアンスの特定のデータを要求することができます。たとえば、ネットワーク管理アプリケーションの 1 つにネットワーク ホスト データを表示する場合、防御センターからホストの重要度または脆弱性のデータを取得し、その情報を表示に追加するためのプログラムを記述することができます。

外部データベースのアクセス

データベース アクセス機能によって、JDBC SSL 接続をサポートするサードパーティ製クライアントを使用して防御センター上の複数のデータベース テーブルを照会できます。

Crystal Reports、Actuate BIRT、JasperSoft iReport などの業界標準のレポート作成ツールを使用してクエリを作成し、送信することができます。また、独自のカスタム アプリケーションを設定して シスコ データをクエリすることもできます。たとえば、侵入およびディスカバリ イベント データについて定期的にレポートしたり、アラート ダッシュボードをリフレッシュしたりするサーブレットを構築することが可能です。

ホスト入力

ホスト入力機能では、スクリプトまたはコマンドライン ファイルを使用してサードパーティのソースからデータをインポートすることにより、ネットワーク マップの情報を増やすことができます。

Web インターフェイスにもいくつかのホスト入力機能があります。これらの機能では、オペレーティング システムまたはアプリケーション プロトコルの識別情報を変更し、脆弱性を有効化または無効化し、ネットワーク マップからさまざまな項目（クライアントやサーバ ポーとなど）を削除することができます。

修復

システムには、ネットワークの状況が関連する相関ポリシーやコンプライアンス ホワイトリストに違反したときに、防御センターが自動的に起動できる修復の作成を可能にする API が含まれます。これにより、ユーザが攻撃に即時に対処できない場合でも攻撃の影響を自動的に緩和でき、またシステムが組織のセキュリティ ポリシーに準拠し続けるようにすることができます。お客様が作成する修復のほかに、防御センターにはいくつかの事前定義された修復モジュールが付属しています。

複数の管理インターフェイス

シリーズ 3 アプライアンスおよび仮想防御センターで*複数の管理インターフェイス*を使用して、2 つのトラフィック チャネル（デバイス間通信を行う*管理トラフィック チャネル*および Web アクセスなどの外部トラフィックを伝送する*イベント トラフィック チャネル*）にトラフィックを分離することによって、パフォーマンスを向上できます。両方のトラフィック チャネルを同じ管理インターフェイス上で伝送することも、2 つの管理インターフェイスに分割して各インターフェイスで 1 つずつトラフィック チャネルを伝送することもできます。

防御センター上の特定の管理インターフェイスから別のネットワークまでのルートを作成することにより、あるネットワーク上のデバイスからのトラフィックと別のネットワーク上のデバイスからのトラフィックを、防御センターで別々に管理することができます。

追加の管理インターフェイスは、次の例外を除いて、デフォルトの管理インターフェイスと同じように機能（防御センター間でのハイ アベイラビリティを使用など）します。

- DHCP は、デフォルト（`eth0`）管理インターフェイスにのみ設定できます。追加のインターフェイス（`eth1` など）には、固有の静的 IP アドレスとホスト名が必要です。
- デフォルト以外の管理インターフェイスを使用して防御センターと管理対象デバイスを接続する場合、それらのアプライアンスが NAT デバイスによって分離されているならば、同じ管理インタフェースを使用するよう両方のトラフィック チャネルを設定する必要があります。
- 70xx ファミリでは、2 つのチャネルにトラフィックを分離し、それらのチャネルが仮想防御センターの 1 つ以上の管理インターフェイスにトラフィックを送信するように設定できます。ただし、70xx ファミリには 1 つの管理インターフェイスしかないため、デバイスは唯一の管理インターフェイス上で防御センターから送信されたトラフィックを受信します。

アプライアンスを設置した後、Web ブラウザを使用して複数の管理インターフェイスを設定します。管理インターフェイスを仮想防御センターに追加する方法については、「インターフェイスの追加と構成」(P.4-10)を参照してください。詳細については、『*FireSIGHT System User Guide*』の「Multiple Management Interfaces」を参照してください。

仮想アプライアンスのライセンス

組織に対して FireSIGHT システム の最適な展開を実現するために、さまざまな機能についてライセンスを取得することができます。防御センターを使用して、それ自身と管理対象デバイスのライセンスを管理する必要があります。

シスコ は、防御センターの初期設定時に、購入したライセンスを追加することを推奨します。そうしない場合、初期設定時に登録するデバイスは、未ライセンスとして防御センターに追加されます。この場合、初期設定プロセスが終了した後で、各デバイスで個別にライセンスを有効化する必要があります。詳細については、「仮想アプライアンスの設定」(P.5-1)を参照してください。

FireSIGHT ライセンスは、防御センターの各購入に含まれており、ホスト、アプリケーション、およびユーザ ディスカバリを実行するために必要です。防御センター上の FireSIGHT ライセンスにより、防御センターおよびその管理対象デバイスで監視可能なホスト数とユーザ数と、ユーザ制御を許可するユーザ数も決定されます。仮想防御センターの場合、この制限は 50,000 の個別のホストおよびユーザです。

防御センターが以前バージョン 4.10.x を実行していた場合は、FireSIGHT ライセンスの代わりに、従来の RNA ホスト ライセンスと RUA ユーザ ライセンスを使用できる場合があります。詳細については、「ライセンス設定」(P.5-11)を参照してください。

モデル固有ライセンスを追加すれば、管理対象デバイスは、次のように、さまざまな機能を実行できます。

保護

保護ライセンスにより、仮想デバイスは侵入検知と防御、ファイル管理、およびセキュリティ インテリジェンス フィルタリングを実行できます。

Control

Control ライセンスにより、仮想デバイスはユーザおよびアプリケーションの制御を実行できます。仮想デバイスは、Control ライセンスによって シリーズ 2 デバイスおよび シリーズ 3 デバイスに付与されるハードウェア ベースのいずれの機能（スイッチングまたはルーティングなど）もサポートしませんが、仮想防御センターは物理デバイスでそうした機能を管理できます。Control ライセンスには保護ライセンスが必要です。

URL フィルタリング

URL フィルタリング ライセンスにより、仮想デバイスは定期的に更新されるクラウドベースのカテゴリとレピュテーションのデータを使用して、監視対象ホストが要求した URL に基づいて、ネットワークを通過できるトラフィックを判別できます。URL フィルタリング ライセンスには保護ライセンスが必要です。

マルウェア

マルウェア ライセンスにより、仮想デバイスはネットワークベースの高度なマルウェア防御（AMP）を実行できます。これはネットワーク上で転送されるファイルに含まれるマルウェアを検出し、ブロックする機能です。また、ネットワーク上で転送されるファイルを追跡するトラジェクトリを表示することもできます。マルウェア ライセンスには保護ライセンスが必要です。

VPN

VPN ライセンスにより、仮想防御センターを使用して、シリーズ 3 デバイス上の仮想ルータ間、またはシリーズ 3 デバイスからリモート デバイスまたは他のサードパーティ製 VPN エンドポイントへセキュアな VPN トンネルを構築できます。VPN ライセンスには、保護ライセンスとControlライセンスが必要です。

アーキテクチャとリソースの制限により、すべての管理対象デバイスにすべてのライセンスが適用できるわけではありません。一般に、デバイスがサポートしていない機能のライセンスは付与できません。「仮想アプライアンスの機能について」(P.1-3) を参照してください。

次の表に、防御センターに追加して、各デバイス モデルに適用可能なライセンスの概要を示します。防御センターの行(FireSIGHT を除くすべてのライセンス)は、防御センターがそれらのライセンスを使用してデバイスを管理できるかどうかを示します。たとえば、シリーズ 3 デバイスを使用した VPN 展開を構築するために シリーズ 2 DC1000 を使用できますが、カテゴリおよびレピュテーション ベースの URL フィルタリングを実行するために DC500 を使用することはできません(管理されるデバイスとは無関係に)。なお、n/a は、管理対象デバイスとは関係のない防御センター ベースのライセンスを示します。

表 1-4　各モデルによってサポートされるライセンス

モデル	FireSIGHT	保護	Control	URL フィルタリング	マルウェア	VPN
シリーズ 2 デバイス: • 3D500、3D1000、3D2000 • 3D2100、3D2500、3D3500、3D4500 • 3D6500 • 3D9900	n/a	自動、セキュリティ インテリジェンスなし	no	no	no	no
シリーズ 3 デバイス: • 7000 シリーズ • 8000 シリーズ	n/a	yes	yes	yes	yes	yes
仮想デバイス	n/a	yes	はい、ただしハードウェア機能のサポートなし	yes	yes	no
Cisco ASA with FirePOWER Services	n/a	yes	はい、ただしハードウェア機能のサポートなし	yes	yes	no
Blue Coat X-Series 向け Cisco NGIPS	n/a	yes	はい、ただしハードウェア機能のサポートなし	yes	yes	no
シリーズ 2 防御センター: • DC500	yes	はい、ただしセキュリティ インテリジェンスなし	はい、ただしユーザ制御なし	no	no	yes
シリーズ 2 防御センター: • DC1000、DC3000	yes	yes	yes	yes	yes	yes

表 1-4　各モデルによってサポートされるライセンス（続き）

モデル	FireSIGHT	保護	Control	URL フィルタリング	マルウェア	VPN
シリーズ 3 防御センター： • DC750、DC1500、DC3500、DC2000、DC4000	yes	yes	yes	yes	yes	yes
仮想の防御センター	yes	yes	yes	yes	yes	yes

ライセンスの詳細については、『*FireSIGHT System User Guide*』の章「FireSIGHT システム のライセンス」を参照してください。

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防御センターをインストールする必要があります。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。また、防御センターでその他のネットワーク上にあるデバイスからのトラフィックを管理および分離できるように、複数の管理インターフェイスを設定することもできます。

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　Blue Coat X-Series 向け Cisco NGIPS と Cisco ASA with FirePOWER Services を除いて、FireSIGHT システム 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、『*FireSIGHT System User Guide*』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 アクセス要件」（P.1-15）
- 「通信ポートの要件」（P.1-16）

インターネット アクセス要件

仮想防御センターは、デフォルトでオープンしているポート 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に設定されます。バーチャル デバイスでは、マルウェア ライセンスを有効にしている場合のみ、ポート 443 がオープンします。このポートがオープンしていると、デバイスは動的分析のためにファイルを送信できます。詳細については、「通信ポートの要件」（P.1-16）を参照してください。FireSIGHT 仮想アプライアンスはプロキシ サーバの使用をサポートしています。詳細については、『*FireSIGHT System User Guide*』を参照してください。プロキシ サーバは whois アクセスに使用できない点にも注意が必要です。

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 1-5　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 アクセスが必要な動作	アプライアンス
動的分析：照会	動的分析のために、提出済みファイルの脅威スコアを Collective Security Intelligence クラウドに照会します。	防御センター
動的分析：送信	動的分析のためにファイルを Collective Security Intelligence クラウドに提出します。	管理対象デバイス
FireAMP 統合	エンドポイント ベースの（FireAMP）マルウェア イベントを Collective Security Intelligence クラウドから受信します。	防御センター
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
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
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、X-シリーズ、および ASA FirePOWER を除く）
セキュリティ インテリジェンス フィルタリング	FireSIGHT システム インテリジェンス フィードを含む外部ソースからのセキュリティ 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
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、X-シリーズ、および ASA FirePOWER を除く）
URL フィルタリング	クラウドベースの URL カテゴリおよびレピュテーション データをアクセス制御用にダウンロードし、カテゴライズされていない URL に対してルックアップを実行します。	防御センター
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、X-シリーズ、および ASA FirePOWER を除く）

通信ポートの要件

FireSIGHT システム 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、ユーザ エージェントに防御センターを接続するまで、エージェントの通信ポート(3306/tcp)は閉じられたままです。別の例としては、LOM を有効にするまで、シリーズ 3 アプライアンスのポート 623/udp は閉じられたままです。

注意　オープンしているポートを閉じると展開にどのような影響が生じるかを理解するまで、オープンしているポートを閉じないでください。

たとえば、管理デバイスのポート 25/tcp(SMTP)アウトバウンドを閉じると、デバイスによる個々の侵入イベントに関する電子メール通知の送信がブロックされます(『*FireSIGHT System User Guide*』を参照)。別の例としては、ポート 443/tcp(HTTPS)を閉じることによって、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、これにより、デバイスはマルウェアと疑われるファイルを動的分析のために Collective Security Intelligence クラウドに送信することもできなくなります。

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場合に、LDAP および RADIUS 認証用にカスタム ポートを指定できます。『*FireSIGHT System User Guide*』を参照してください。
- 管理ポート(8305/tcp)は変更できます。『*FireSIGHT System User Guide*』を参照してください。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、導入内の相互に通信する必要があるすべてのアプライアンスの管理ポートを変更する必要があります。
- アップグレードした防御センターが Collective Security Intelligence クラウドと通信できるようにするため、ポート 32137/tcp を使用できます。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、『*FireSIGHT System User Guide*』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 1-6　FireSIGHT システムの機能と操作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許可します。
25/tcp	SMTP	発信	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	発信	すべて	DNS を使用します。

表 1-6　FireSIGHT システムの機能と操作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
67/udp 68/udp	DHCP	発信	すべて（X-シリーズ 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	発信	すべて（仮想デバイス、X-シリーズ、および ASA FirePOWER 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	X-シリーズ と ASA FirePOWER を除くすべて	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	発信	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	発信	すべて（仮想デバイスと X-シリーズ を除く）	外部認証用に LDAP サーバと通信します。
389/tcp 636/tcp	LDAP	発信	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	着信	すべて（仮想デバイス、X-シリーズ、および ASA FirePOWER を除く）	アプライアンスの Web インターフェイスへのアクセス。

表 1-6　FireSIGHT システムの機能と操作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） • 共有されたセキュリティ インテリジェンス フィードと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（FireAMP）のマルウェア 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、仮想デバイス、X-シリーズ、および ASA FirePOWER	動的分析のためにファイルを送信します。
514/udp	syslog	発信	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	着信	TCP	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、X-シリーズ、および ASA FirePOWER 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	User Agent	着信	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-シリーズ を除く）	eStreamer クライアントと通信します。
8305/tcp	デバイス管理	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**。
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。