FireSIGHT システムの概要

シスコ FireSIGHT® システムは、業界をリードするネットワーク侵入防御システムのセキュリティと、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 アクセスを制御する能力を兼ね備えています。また、FireSIGHT システム アプライアンスを使用して、スイッチド、ルーテッド、またはハイブリッド（スイッチド兼ルーテッド）環境でサービスを提供したり、ネットワーク アドレス変換（NAT）を実行したり、FirePOWER 管理対象デバイスの仮想ルータ間でセキュアなバーチャル プライベート ネットワーク（VPN）トンネルを構築したりすることもできます。

FireSIGHT 防御センター ® は、FireSIGHT システム用の集中型管理コンソールとデータベース リポジトリを提供します。ネットワーク セグメント上に設置された管理対象デバイスが、分析対象となるトラフィックを監視します。

パッシブ展開内のデバイスは、スイッチ SPAN、仮想スイッチ、ミラー ポートなどを使用して、ネットワーク上のトラフィック フローを監視します。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ます。このインターフェイスで受信されたトラフィックは再送されません。

インライン展開内のデバイスを使用すると、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のある攻撃からネットワークを保護できます。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ます。展開内の何らかの設定によって明示的にドロップされない限り、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されます。単純な侵入防御システムとして、インライン デバイスを展開することができます。さらに、アクセス コントロールを実行したり、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ためにインライン デバイスを設定できます。

このインストレーション ガイドでは、FireSIGHT システム アプライアンス（デバイスと防御センター）の展開、設置、およびセットアップに関する情報を提供します。また、FireSIGHT システム アプライアンスのハードウェア仕様と安全性および規制に関する情報も含まれています。

ヒント 仮想防御センターおよびデバイスをホストすることができます。これらは物理アプライアンスを管理したり、物理アプライアンスによる管理対象になったりします。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（冗長性、スイッチング、ルーティングなど）をサポートしません。詳細については、『*FireSIGHT System Virtual Installation Guide*』を参照してください。

以降のトピックでは、FireSIGHT システムを紹介し、その主要コンポーネントについて説明します。

FireSIGHT システム アプライアンス

FireSIGHT システム *アプライアンス* とは、トラフィックを検知する管理対象 *デバイス*、またはそれらを管理する *防御センター* のいずれかを意味します。

物理デバイスは、さまざまなスループットと機能を備えたフォールト トレラントな専用のネットワーク アプライアンスです。防御センターは、これらのデバイスの中央管理点として機能し、デバイスが生成したイベントを自動的に集約して相互に関連付けます。物理アプライアンスのタイプごとに複数の *モデル* が存在します。これらのモデルはさらに *シリーズ* と *ファミリ* に分類されます。FireSIGHT システムの多くの機能は、アプライアンスによって異なります。

防御センターについて

防御センターは、FireSIGHT システム展開における集中管理点およびイベント データベースとしての機能を提供します。また、防御センターは、侵入、ファイル、マルウェア、ディスカバリ、接続、およびパフォーマンスに関するデータを集約して相互に関連付け、特定のホストに対するイベントの影響を評価し、侵害を示すタグをホストに付けます。これにより、相互に関連するデバイスから報告される情報を監視し、ネットワークで発生するアクティビティ全体を評価して制御できます。

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
- テーブル、グラフ、およびチャートを使用したイベントとコンテキスト情報の表示
- 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
- リアルタイムで脅威に対処するための相関、侵害の通知、および修復機能
- カスタムとテンプレート ベースのレポート機能

多くの物理的な防御センターにおいて、ハイ アベイラビリティ（冗長性）機能は継続的な運用を支援します。

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デバイスは、分析対象のトラフィックを監視します。受動的（パッシブ）に展開されたデバイスは、ネットワーク トラフィックの状態を深く理解するうえで役立ちます。インライン展開された FirePOWER デバイスを使用すると、さまざまな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。モデルとライセンスに応じて、デバイスには次のような機能があります。

- 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します。
- さまざまなネットワーク ベースの基準に加えて、（アプリケーション、ユーザ、URL、IP アドレス レピュテーション、侵入/マルウェア インスペクションの結果など）他の基準に基づいて、ネットワーク トラフィックをブロックまたは許可します。
- スイッチング、ルーティング、DHCP、NAT、および VPN 機能に加えて、設定可能バイパス インターフェイス、ファストパス ルール、および厳密な TCP 強制も備えています。

- 継続的な運用に役立つクラスタリング（冗長性）と、複数のデバイスのリソースを統合するスタッキングを備えています。

FirePOWER デバイスを管理するには、防御センターを使用する**必要**があります。

アプライアンスの種類

FireSIGHT システムは、シスコから入手可能なフォールト トレラントな専用の*物理* ネットワーク アプライアンス上で動作します。それぞれの防御センターと管理対象デバイスごとに、複数の*モデル*が存在します。これらのモデルはさらに*シリーズ*と*ファミリ*に分類されます。

管理対象の物理デバイスは、さまざまなスループットと機能を備えています。物理的な防御センターは、デバイス管理、イベント保存、およびホスト/ユーザのモニタリングに関するさまざまな機能を備えています。

また、次に示すソフトウェア ベースのアプライアンスを展開することもできます。

- VMware vSphere Hypervisor または VMware vCloud Director 環境を使用して ESXi ホストとして 64 ビット*仮想*防御センターおよび*仮想*管理対象デバイスを展開できます。
- X-Series の Sourcefire ソフトウェア を Blue Coat X-Series プラットフォーム上に展開できます。これは管理対象デバイスとして機能します。

どちらのタイプ（物理または仮想）の防御センターも、任意のデバイス タイプ（物理、仮想、Cisco ASA with FirePOWER Services、および X-Series の Sourcefire ソフトウェア）を管理できます。ただし、FireSIGHT システムの多くの機能はアプライアンスによって異なることに注意してください。

サポートされている機能を含む FireSIGHT システム アプライアンスの詳細については、以下を参照してください。

- 「シリーズ 2 アプライアンス」（P.1-3）
- 「シリーズ 3 アプライアンス」（P.1-4）
- 「仮想アプライアンス」（P.1-4）
- 「X-Series の Sourcefire ソフトウェア」（P.1-4）
- 「Cisco ASA with FirePOWER Services」（P.1-5）
- 「バージョン 5.3.1 に付属のアプライアンス」（P.1-6）
- 「防御センター モデル別にサポートされる機能」（P.1-7）
- 「管理対象デバイス モデル別にサポートされる機能」（P.1-9）

シリーズ 2 アプライアンス

シリーズ 2 は、従来の物理アプライアンスの 2 番目のシリーズです。リソースとアーキテクチャの制限により、シリーズ 2 デバイスは、FireSIGHT システムの一部の機能ほ限定的にサポートします。

シスコでは、今後新しいシリーズ 2 アプライアンスを出荷する予定はありませんが、以前のバージョンのシステムを実行しているシリーズ 2 防御センターをバージョン 5.3.1 に更新または再イメージングすることができます。シリーズ 2 デバイスをバージョン 5.3.1 に更新または再イメージングすることはできませんが、5.3.1 の防御センターでバージョン 5.2 または 5.3 のデバイスを管理できます。再イメージングすると、アプライアンスに関するほとんど**すべての**設定とイベント データが失われることに注意してください。詳細については、「出荷時の初期状態に FireSIGHT システム アプライアンスを復元する」（P.7-1）を参照してください。

ヒント　特定の設定とイベント データをバージョン 4.10.3 展開からバージョン 5.2 展開に移行した後、バージョン 5.3.1 に更新することができます。詳細については、バージョン 5.2 の『*Cisco FireSIGHT System Migration Guide*』を参照してください。

シリーズ 2 デバイスは、保護ライセンスに関連付けられたほとんどの機能（侵入検知と防御、ファイル制御、および基本的なアクセス コントロール）を自動的に実装します。ただし、シリーズ 2 デバイスは、セキュリティ インテリジェンス フィルタリング、高度なアクセス コントロール、高度なマルウェア防御を実行できません。また、シリーズ 2 デバイス上で他のライセンス付き機能を有効にすることはできません。ファストパス ルール、スタッキング、およびタップ モードをサポートする 3D9900 を除いて、シリーズ 2 デバイスは、シリーズ 3 デバイスに関連するハードウェア ベースの機能（スイッチング、ルーティング、NAT など）をサポートしません。

バージョン 5.3.1 を実行中の DC1000 および DC3000 シリーズ 2 防御センターは、FireSIGHT システムのすべての機能をサポートします。DC 500 の機能はより限定的です。

シリーズ 3 アプライアンス

シリーズ 3 は、FirePOWER 物理アプライアンスの 3 番目のシリーズです。すべての 7000 シリーズ デバイスと 8000 シリーズ デバイスは、シリーズ 3 アプライアンスです。8000 シリーズ デバイスは、より強力で、7000 シリーズ デバイスでサポートされないいくつかの機能をサポートします。

注意　シリーズ 3 デバイスをバージョン 5.3.1 に更新/再イメージングすることはできませんが、5.3.1 防御センターはこれらのデバイスのバージョン 5.2 または 5.3 を管理できます。

仮想アプライアンス

VMware vSphere Hypervisor または VMware vCloud Director 環境を使用して ESXi ホストとして 64 ビット仮想防御センターおよび管理対象デバイスを展開できます。

インストールされて適用されたライセンスとは無関係に、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（冗長性とリソース共有、スイッチング、ルーティングなど）をサポートしません。また、仮想デバイスには Web インターフェイスがありません。仮想アプライアンスの詳細については、『*FireSIGHT System Virtual Installation Guide*』を参照してください。

注意　仮想デバイスをバージョン 5.3.1 に更新/再イメージングすることはできませんが、5.3.1 防御センターはこれらのデバイスのバージョン 5.2 または 5.3 を管理できます。

X-Series の Sourcefire ソフトウェア

X-Series の Sourcefire ソフトウェア を Blue Coat X-Series プラットフォーム上にインストールすることができます。このソフトウェア ベースのアプライアンスは、仮想管理対象デバイスと同じように機能します。インストールおよび適用されたライセンスとは無関係に、X-Series の Sourcefire ソフトウェア は次の機能をサポートしません。

- X-Series の Sourcefire ソフトウェア は、システムのハードウェア ベースの機能（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、VPN、NAT など）をサポートしません。
- X-Series の Sourcefire ソフトウェア を使用して、発信元または宛先の国や大陸に基づいてネットワーク トラフィックをフィルタ処理すること（位置情報ベースのアクセス コントロール）はできません。
- 防御センター Web インターフェイスを使用して、X-Series の Sourcefire ソフトウェア インターフェイスを設定することはできません。
- 防御センターを使用して、X-Series の Sourcefire ソフトウェア プロセスをシャットダウン、再起動、その他の方法で管理することはできません。
- 防御センターを使用して、X-Series の Sourcefire ソフトウェア のバックアップを作成/復元することはできません。
- X-Series の Sourcefire ソフトウェア にヘルス ポリシーやシステム ポリシーを適用することはできません。これには時刻設定の管理が含まれます。

X-Series の Sourcefire ソフトウェア には Web インターフェイスがありません。ただし、X-Series プラットフォームに固有のコマンド ライン インターフェイス（CLI）があります。この CLI を使用して、システムをインストールしたり、次のようなプラットフォーム固有の管理タスクを実行することができます。

- Virtual Appliance Processor（VAP）グループの作成。これにより、X-Series プラットフォームのロード バランシングと冗長性（シスコの物理デバイス クラスタリングと同等）を活用できます。
- パッシブおよびインライン センシング インターフェイスの設定。インターフェイスの最大伝送ユニット（MTU）の設定を含みます。
- プロセスの管理
- NTP 設定を含む時刻設定の管理

注意　X-Series デバイスをバージョン 5.3.1 に更新/再イメージングすることはできませんが、5.3.1 防御センターはこれらのデバイスのバージョン 5.2 または 5.3 を管理できます。

Cisco ASA with FirePOWER Services

防御センターを使用して、Cisco ASA with FirePOWER Services（ASA FirePOWER）デバイスを管理できます。この展開では、ASA デバイスが第一線のシステム ポリシーを提供し、アクセス コントロール、侵入検知と防御、ディスカバリ、および高度なマルウェア防御のためにトラフィックを FireSIGHT システムに渡します。サポートされている ASA モデルのリストについては、「バージョン 5.3.1 FireSIGHT システム アプライアンス」の表を参照してください。

インストールおよび適用されたライセンスとは無関係に、ASA FirePOWER デバイスは FireSIGHT システムを介して次の機能をサポートしません。

- ASA FirePOWER デバイスは、FireSIGHT システムのハードウェア ベースの機能（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、VPN、NAT など）をサポートしません。ただし、ASA プラットフォームにはこれらの機能が備わっており、ASA CLI と ASDM を使ってこれらを設定できます。詳細については、ASA のマニュアルを参照してください。
- 防御センター Web インターフェイスを使用して、ASA FirePOWER インターフェイスを設定することはできません。
- 防御センターを使用して、ASA FirePOWER プロセスをシャットダウン、再起動、その他の方法で管理することはできません。
- 防御センターを使用して、ASA FirePOWER デバイスのバックアップを作成/復元することはできません。
- VLAN タグ条件を使用してトラフィックを照合するアクセス コントロール ルールを作成することはできません。

ASA FirePOWER デバイスには、FireSIGHT Web インターフェイスがありません。ただし、ASA プラットフォームに固有のソフトウェアとコマンド ライン インターフェイス（CLI）があります。これらの ASA 固有のツールを使用して、システムをインストールしたり、プラットフォーム固有の他の管理タスクを実行したりすることができます。詳細については、ASA FirePOWER モジュール のマニュアルを参照してください。

また、ASA FirePOWER モジュールには FirePOWER アプライアンス用の CLI も含まれています。CLI を使用して、FireSIGHT システムを表示、設定、およびトラブルシューティングすることができます。詳細については、『*FireSIGHT System User Guide*』を参照してください。

バージョン 5.3.1 に付属のアプライアンス

次の表に、FireSIGHT システム バージョン 5.3.1 と一緒にシスコから提供されるアプライアンスを示します。

注意　以前のバージョンのシステムを実行している シリーズ 2、シリーズ 3、および仮想防御センターをバージョン 5.3.1 に更新または再イメージングできます。シリーズ 2、シリーズ 3、仮想、または X-Series デバイスをバージョン 5.3.1 に更新/再イメージングすることはできませんが、5.3.1 防御センターはこれらのデバイスのバージョン 5.2 または 5.3 を管理できます。

表 1-1　バージョン 5.3.1 FireSIGHT システム アプライアンス

モデル/ファミリ	シリーズ	フォーム	タイプ
70xx ファミリ： • 3D7010/3D7020/3D7030	シリーズ 3 （7000 シリーズ）	ハードウェア	デバイス
71xx ファミリ： • 3D7110/3D7120 • 3D7115/3D7125 • AMP7150	シリーズ 3 （7000 シリーズ）	ハードウェア	デバイス

表 1-1　バージョン 5.3.1 FireSIGHT システム アプライアンス （続き）

モデル/ファミリ	シリーズ	フォーム	タイプ
81xx ファミリ： • 3D8120/3D8130/3D8140 • AMP8150	シリーズ 3（8000 シリーズ）	ハードウェア	デバイス
82xx ファミリ： • 3D8250 • 3D8260/3D8270/3D8290	シリーズ 3（8000 シリーズ）	ハードウェア	デバイス
83xx ファミリ： • 3D8350 • 3D8360/3D8370/3D8390	シリーズ 3（8000 シリーズ）	ハードウェア	デバイス
64 ビット仮想デバイス	n/a	ソフトウェア	デバイス
X-Series の Sourcefire ソフトウェア	n/a	ソフトウェア	デバイス
ASA FirePOWER： • ASA5585-X-SSP-10、ASA5585-X-SSP-20、ASA5585-X-SSP-40、ASA5585-X-SSP-60	n/a	ハードウェア	デバイス
ASA FirePOWER： • ASA5512-X、ASA5515-X、ASA5525-X、ASA5545-X、ASA5555-X	n/a	ソフトウェア	デバイス
シリーズ 3 防御センター： • DC750/DC1500/DC3500	シリーズ 3	ハードウェア	防御センター
64 ビット仮想防御センター	n/a	ソフトウェア	防御センター

シスコでは、今後新しいシリーズ 2 アプライアンスを出荷する予定はありませんが、以前のバージョンのシステムを実行しているシリーズ 2 防御センターをバージョン 5.3.1 に更新または再イメージングすることができます。シリーズ 2 デバイスをバージョン 5.3.1 に更新/再イメージングすることはできませんが、5.3.1 防御センターは 5.3 デバイスを管理できます。再イメージングすると、アプライアンスに関するほとんど**すべての**設定とイベント データが失われることに注意してください。詳細については、「出荷時の初期状態に FireSIGHT システム アプライアンスを復元する」（P.7-1）を参照してください。

ヒント　特定の設定とイベント データをバージョン 4.10.3 展開からバージョン 5.2 展開に移行した後、バージョン 5.3.1 に更新することができます。詳細については、バージョン 5.2 の『*FireSIGHT System Migration Guide*』を参照してください。

防御センター モデル別にサポートされる機能

バージョン 5.3.1 を実行しているすべての防御センターは、モデルに応じて多少の制限があることを除き、ほぼ同じ機能を備えています。次の表は、システムの主な機能と、これらの機能をサポートする防御センターを示しています（これらの機能をサポートするデバイスを管理しており、適切なライセンスがインストール/適用済みであることを想定しています）。

この表に示す機能に加えて、防御センター モデルに応じて、管理可能なデバイス数、保存可能なイベント数、および監視可能なホスト数とユーザ数が異なります。詳細については、*FireSIGHT System User Guide* を参照してください。

また、バージョン 5.3.1 のシステムを実行している防御センターの任意のモデルを使用して任意のバージョン 5.3 またはバージョン 5.3.1 デバイスを管理できますが、デバイス モデルによってシステム機能の多くが制限されることに留意してください。たとえば、シリーズ 3 防御センターを使用している場合でも、展開にシリーズ 3 デバイスが含まれていない場合は VPN を実装できません。詳細については、「管理対象デバイス モデル別にサポートされる機能」（P.1-9）を参照してください。

表 1-2　防御センター モデル別にサポートされる機能

機能	シリーズ 2 防御センター	シリーズ 3 防御センター	仮想防御センター
管理対象デバイスから報告された検出データ（ホスト、アプリケーション、およびユーザ）を収集して、組織のネットワーク マップを作成する	はい	はい	はい
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	DC1000、DC3000	はい	はい
侵入検知および防御（IPS）展開を管理する	はい	はい	はい
セキュリティ インテリジェンス フィルタリングを実行しているデバイスを管理する	DC1000、DC3000	はい	はい
位置情報に基づくフィルタリングを含む、単純なネットワーク ベースの制御を実行しているデバイスを管理する	はい	はい	はい
アプリケーション制御を実行しているデバイスを管理する	はい	はい	はい
ユーザ制御を実行しているデバイスを管理する	DC1000、DC3000	はい	はい
リテラル URL でネットワーク トラフィックをフィルタ処理するデバイスを管理する	はい	はい	はい
カテゴリとレピュテーションによる URL フィルタリングを実行しているデバイスを管理する	DC1000、DC3000	はい	はい
ファイル タイプによる単純なファイル制御を実行しているデバイスを管理する	はい	はい	はい
ネットワーク ベースの高度なマルウェア防御（AMP）を実行しているデバイスを管理する	DC1000、DC3000	はい	はい
FireAMP 展開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	はい	はい	はい

表 1-2　防御センター モデル別にサポートされる機能 （続き）

機能	シリーズ 2 防御センター	シリーズ 3 防御センター	仮想防御センター
デバイス ベースでハードウェア ベースの機能を管理する： • ファストパス ルール • 厳密な TCP 強制 • 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	はい	はい	はい
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 • X-Series の Sourcefire ソフトウェア VAP グループ • クラスタ化スタック	はい	はい	はい
ハイ アベイラビリティを確立する	DC1000、DC3000	DC1500、DC3500	いいえ
マルウェア ストレージ パックをインストールする	DC1000、DC3000	はい	いいえ
eStreamer、ホスト入力、またはデータベース クライアントに接続する	はい	はい	はい

管理対象デバイス モデル別にサポートされる機能

デバイスはネットワーク トラフィックを処理するアプライアンスです。そのため、FireSIGHT システムの機能の多くは、管理対象デバイスのモデルによって異なります。

次の表は、システムの主な機能と、これらの機能をサポートするデバイスを示しています（管理を行う防御センターから適切なライセンスがインストール/適用済みであることを想定しています）。

バージョン 5.3.1 のシステムを実行している防御センターの任意のモデルを使用して任意のバージョン 5.3 またはバージョン 5.3.1 デバイスを管理できますが、防御センター モデルによっていくつかのシステム機能が制限されることに留意してください。たとえば、セキュリティ インテリジェンス フィルタリングを実行しているデバイスを管理するために、シリーズ 2 DC500 を使用することはできません（デバイスでこの機能がサポートされる場合でも）。詳細については、「防御センター モデル別にサポートされる機能」（P.1-7）を参照してください。

表 1-3　管理対象デバイス モデル別にサポートされる機能

機能	シリーズ 2 デバイス	シリーズ 3 デバイス	ASA FirePOWER	仮想デバイス	X-Series
ネットワーク検出：ホスト、アプリケーション、およびユーザ	はい	はい	はい	はい	はい
侵入検知および防御（IPS）	はい	はい	はい	はい	はい

表 1-3　管理対象デバイス モデル別にサポートされる機能 （続き）

機能	シリーズ 2 デバイス	シリーズ 3 デバイス	ASA FirePOWER	仮想デバイス	X-Series
セキュリティ インテリジェンス フィルタリング	いいえ	はい	はい	はい	はい
アクセス コントロール：基本的なネットワーク制御	はい	はい	はい	はい	はい
アクセス コントロール：位置情報ベースのフィルタリング	いいえ	はい	はい	はい	いいえ
アクセス コントロール：アプリケーション制御	いいえ	はい	はい	はい	はい
アクセス コントロール：ユーザ制御	いいえ	はい	はい	はい	はい
アクセス コントロール：リテラル URL	いいえ	はい	はい	はい	はい
アクセス コントロール：カテゴリとレピュテーションによる URL フィルタリング	いいえ	はい	はい	はい	はい
ファイル制御：ファイル タイプ別	はい	はい	はい	はい	はい
ネットワーク ベースの高度なマルウェア防御（AMP）	いいえ	はい	はい	はい	はい
自動アプリケーション バイパス	はい	はい	いいえ	はい	いいえ
ファストパス ルール	3D9900	8000 シリーズ	いいえ	いいえ	いいえ
厳密な TCP 強制	いいえ	はい	いいえ	いいえ	いいえ
設定可能バイパス インターフェイス	はい	ハードウェア制限される場合を除く	いいえ	いいえ	いいえ
タップ モード	3D9900	はい	いいえ	いいえ	いいえ
スイッチングとルーティング	いいえ	はい	いいえ	いいえ	いいえ
NAT ポリシー	いいえ	はい	いいえ	いいえ	いいえ
VPN	いいえ	はい	いいえ	いいえ	いいえ
デバイス スタッキング	3D9900	3D8140 82xx ファミリ 83xx ファミリ	いいえ	いいえ	いいえ
デバイス クラスタリング	いいえ	はい	いいえ	いいえ	いいえ
クラスタ化スタック	いいえ	3D8140 82xx ファミリ 83xx ファミリ	いいえ	いいえ	いいえ
マルウェア ストレージ パック	いいえ	はい	いいえ	いいえ	いいえ
制限付きコマンド ライン インターフェイス（CLI）	いいえ	はい	はい	はい	いいえ
外部認証	はい	はい	いいえ	いいえ	いいえ
eStreamer クライアントへの接続	はい	はい	はい	いいえ	いいえ

シリーズ 3 デバイス シャーシの指定

ここでは、7000 シリーズ デバイス、8000 シリーズ デバイス、およびそれぞれのシャーシ ハードウェア コードを示します。シャーシ コードは、シャーシ外側の規制ラベルに表示されている、ハードウェアの認定および安全性に関する公式な参照コードです。

7000 シリーズ シャーシの指定

次の表に、全世界で使用される 7000 シリーズ モデルのシャーシ指定を示します。

表 1-4　7000 シリーズ シャーシ モデル

3D デバイス モデル	ハードウェア シャーシ コード
3D7010、3D7020、3D7030	CHRY-1U-AC
3D7110、3D7120（銅線）	GERY-1U-8-C-AC
3D7110、3D7120（光ファイバ）	GERY-1U-8-C-AC
3D7115、3D7125、AMP7150	GERY-1U-4C8S-AC

8000 シリーズ シャーシの指定

次の表に、全世界で使用される シリーズ 3 モデルのシャーシ指定を示します。

表 1-5　8000 シリーズ シャーシ モデル

3D デバイス モデル	ハードウェア シャーシ コード
3D8120、3D8130、3D8140、AMP8150（AC 電源）	CHAS-1U-AC
3D8120、3D8130、3D8140、AMP8150（DC 電源）	CHAS-1U-DC
3D8250、3D8260、3D8270、3D8290（AC 電源）	CHAS-2U-AC
3D8250、3D8260、3D8270、3D8290（DC 電源）	CHAS-2U-DC
3D8350、3D8360、3D8370、3D8390（AC/DC 電源）	PG35-2U-AC/DC

FireSIGHT システム コンポーネント

ここでは、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役立つ FireSIGHT システムの主な機能をいくつか示します。

ヒント　FireSIGHT システムの機能多くは、アプライアンス モデル、ライセンス、およびユーザ ロールに応じて異なります。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。

冗長性とリソース共有

FireSIGHT システムの冗長性とリソース共有機能を使用すると、継続的な運用が可能になり、複数の物理デバイスの処理リソースを統合することができます。

- 防御センター ハイ アベイラビリティ機能を使用すると、デバイス管理用の冗長 DC1000、DC1500、DC3000、または DC3500 防御センターを指定することができます。
- デバイス スタッキングを使用すると、2 ～ 4 つの物理デバイスをスタック構成で接続することにより、ネットワーク セグメントで検査対象となるトラフィックの量を増やすことができます。
- デバイス クラスタリングを使用すると、複数のシリーズ 3 デバイスまたはスタックの間のネットワーキング機能と設定データの冗長性を構築することができます。

ネットワーク トラフィック管理

FireSIGHT システムのネットワーク トラフィック管理機能を使用すると、シリーズ 3 デバイスを組織のネットワーク インフラストラクチャの一部として機能させることができます。次の作業を実行できます。

- 複数のネットワーク セグメント間でパケット スイッチングを実行できるようにレイヤ 2 展開を設定する
- 複数インターフェイス間のトラフィックをルーティングするようにレイヤ 3 展開を設定する
- ネットワーク アドレス変換（NAT）を実行する
- 管理対象デバイス上の仮想ルータからリモート デバイスまたは他のサードパーティ製 VPN エンドポイントへのセキュアな VPN トンネルを構築する

FireSIGHT

シスコのディスカバリ/認識テクノロジである FireSIGHT™ は、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してネットワークの全体像を提供します。

防御センターの Web インターフェイスを使用すると、FireSIGHT によって収集されたデータを表示および分析できます。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。加えて、ホストに関する相関イベント データに基づいて、ネットワーク上のホストへの侵害の兆候を生成し、追跡できます。

アクセス コントロール

ポリシー ベースの機能であるアクセス コントロールを使用すると、ネットワークを通過するトラフィックを指定、検査、および記録することができます。アクセス コントロールの一部であるセキュリティ インテリジェンス機能を使用すると、トラフィックをより詳しく分析する前に、特定の IP アドレスをブラックリストに追加する（そのアドレスへのトラフックとそのアドレスからのトラフィックを拒否する）ことができます。

セキュリティ インテリジェンス フィルタリングの実行後、どのトラフィックをどのように対象デバイスで処理するかを定義できます。その際、単純な IP アドレス照合から、さまざまなユーザー /アプリケーション/ポート/URL を扱う複雑なシナリオに至るまで幅広く使用できます。トラフィックを信頼、監視（モニタリング）、またはブロックできることに加えて、次のような追加の分析も可能です。

- 侵入検知および防御
- ファイル制御
- ファイル トラッキングとネットワークに基づく高度なマルウェア防御（AMP）

侵入検知および防御

侵入検知および防御は、アクセス コントロールの中に統合されたポリシー ベースの機能です。この機能を使用すると、ネットワーク トラフィックのセキュリティ違反を監視したり、インライン展開によって有害なトラフィックをブロック/変更したりできます。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 の推奨に基づくルール状態設定
- 高度な設定（たとえばプリプロセッサその他の検出/パフォーマンス機能）
- 関連するプリプロセッサとプリプロセッサ オプションに関するイベントを生成できるプリプロセッサ ルール

ファイル トラッキング、制御、およびネットワーク ベースの高度なマルウェア防御（AMP）

FireSIGHT システムの構成要素であるファイル制御、ネットワーク ファイル トラジェクトリ（感染経路追跡）、および高度なマルウェア防御は、ネットワーク トラフィック内の（マルウェア ファイルを含む）ファイル転送を検出、追跡、収集、分析し、オプションでブロックできます。これはマルウェアの影響を特定し、軽減するうえで役立ちます。

ファイル制御はアクセス コントロールの中に統合されたポリシー ベースの機能です。この機能を使用すると、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種類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）しようとすると、管理対象デバイスでそれを検出してブロックできます。

ネットワーク ベースの*高度なマルウェア防御*（AMP）を使用すると、システムはネットワークを検査して、いくつかの種類のファイルに含まれるマルウェアを検出できます。アプライアンスは、検出されたファイルをさらに分析するために、ハード ドライブまたは（モデルによっては）マルウェア ストレージ パックに保存することができます。

検出されたファイルを手元に保存するかどうかに関わらず、ファイルの SHA-256 ハッシュ値を使用して単純な既知ディスポジション ルックアップ用にシスコ クラウドにそれを送信することができます。また、脅威スコアを算出する*動的分析*用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システムを設定できます。

FireAMP は、シスコが提供するエンタープライズ向けの高度なマルウェア分析/防御ソリューションです。高度なマルウェアの発生、高度な持続的脅威、および標的を絞った攻撃を検出、把握、ブロックします。組織で FireAMP サブスクリプションを利用している場合は、個別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 Connector をインストールします。これらの軽量エージェントはシスコ クラウドと通信し、さらにクラウドが防御センターと通信します。

クラウドに接続するよう防御センターを設定した後、防御センター Web インターフェイスを使用すると、組織内のエンドポイントのスキャン、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 イベントを表示できます。また、防御センターは FireAMP データを使用してホスト侵害の兆候を生成および追跡することに加えて、ネットワーク ファイル トラジェクトリを表示します。

ネットワーク ファイル トラジェクトリ機能を使用すると、ネットワークにおける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 ハッシュ値を使ってファイルを追跡します。各ファイルには、経時的なファイル転送を視覚化するトラジェクトリ マップが関連付けられ、ファイルに関する追加の情報も含まれています。

アプリケーション プログラミング インターフェース

アプリケーション プログラミング インターフェース（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。

- Event Streamer（eStreamer）を使用すると、FireSIGHT システム 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。
- データベース アクセス機能を使用すると、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、防御センター上のいくつかのデータベース テーブルを照会することができます。
- ホスト入力機能を使用すると、スクリプトまたはコマンドライン ファイルを使ってサードパーティ 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 マップ内の情報を補強できます。
- 修復機能は、ネットワークで特定の条件が満たされたときに防御センターによって自動的に起動される一連のプログラムです。この機能は、担当者がただちに対応できる状態でなくても自動的に攻撃を減退させるだけでなく、システムを組織のセキュリティ ポリシーに常に適合させます。

FireSIGHT システムのライセンス

組織に最適な FireSIGHT システム展開を構築するために、さまざまな機能のライセンスを有効にすることができます。防御センターを使用して、それ自体のライセンスとそれが管理するデバイスのライセンスを管理する必要があります。

防御センターの初期セットアップ時に、組織で購入済みのライセンスを追加することをシスコでは推奨しています。そうしない場合、初期セットアップ時に登録されるデバイスは「ライセンスなし」として防御センターに追加されます。その後、初期セットアップ手順が完了したら、各デバイスで個別にライセンスを有効にする必要があります。詳細については、「FireSIGHT システム アプライアンスのセットアップ」（P.4-1）を参照してください。

ご購入いただいたそれぞれの防御センターに FireSIGHT ライセンスが含まれており、ホスト、アプリケーション、およびユーザの検出を実行するにはこれが必要です。また、防御センター上の FireSIGHT ライセンスは、防御センターとその管理対象デバイスを使って監視できる個別のホスト数とユーザ数、およびユーザ制御に使用できるユーザ数を決定します。次の表に示すように、FireSIGHT のホストおよびユーザ ライセンス制限はモデルにより異なります。

表 1-6　防御センター モデル別の FireSIGHT の制限

防御センターのモデル	FireSIGHT のホスト/ユーザ制限
DC500	1000（ユーザ制御なし）
DC750	2000
DC1000	20,000
DC1500	50,000
DC3000	100,000
DC3500	300,000

以前に防御センターでバージョン 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可能性があります。詳細については、「従来の RNA ホストおよび RUA ユーザ ライセンスの使用」（P.1-16）を参照してください。

さらに、モデル固有のライセンスを使用すると、管理対象デバイスで次のようなさまざまな機能を実行できます。

保護

保護ライセンスを使用すると、管理対象デバイスで侵入検知と防御、ファイル制御、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。

制御

制御ライセンスを使用すると、管理対象デバイスでユーザ制御とアプリケーション制御を実行できます。また、デバイスでスイッチングとルーティング（DHCP リレーを含む）および NAT を実行し、デバイスとスタックをクラスタ化することもできます。制御ライセンスを使用するには、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 ライセンスを使用すると、管理対象デバイスは、定期的に更新されるクラウド ベースのカテゴリおよびレピュテーション データを使用し、監視対象ホストから要求される 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決定できます。URL フィルタリング ライセンスを使用するには、保護ライセンスが必要です。

マルウェア

マルウェア ライセンスを使用すると、管理対象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。つまり、ネットワーク経由で伝送されるファイル内のマルウェアを検出してブロックすることができます。また、ネットワーク経由で伝送された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 ライセンスを使用するには、保護ライセンスが必要です。

VPN

VPN ライセンスを使用すると、シスコの管理対象デバイス上の仮想ルータ間、あるいは管理対象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 エンドポイントまでのセキュアな VPN トンネルを構築できます。VPN ライセンスを使用するには、保護ライセンスおよび制御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のために、すべてのライセンスをすべての管理対象デバイスに適用できるわけではありません。一般に、デバイスでサポートされない機能のライセンスを有効にすることはできません（「管理対象デバイス モデル別にサポートされる機能」（P.1-9）を参照）。

次の表は、防御センターに追加して各デバイス モデルに適用できるライセンスの概要を示しています。（FireSIGHT を除くすべてのライセンスで）防御センターの行は、ライセンスを使用してその防御センターが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 1-7　サポートされるライセンス（モデル別）

モデル	FireSIGHT	保護	制御	URL フィルタリング	マルウェア	VPN
シリーズ 2 デバイス： • 3D500/1000/2000 • 3D2100/2500/3500/4500 • 3D6500 • 3D9900	n/a	自動、セキュリティ インテリジェンスなし	いいえ	いいえ	いいえ	いいえ
シリーズ 3 デバイス： • 7000 シリーズ • 8000 シリーズ	n/a	はい	はい	はい	はい	はい
仮想デバイス	n/a	はい	はい、ただしハードウェア機能のサポートなし	はい	はい	いいえ
Cisco ASA with FirePOWER Services	n/a	はい	はい、ただしハードウェア機能のサポートなし	はい	はい	いいえ
X-Series の Sourcefire ソフトウェア	n/a	はい	はい、ただしハードウェア機能のサポートなし	はい	はい	いいえ
DC500 シリーズ 2 防御センター	はい	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	いいえ	いいえ	はい
DC1000/3000 シリーズ 2 防御センター	はい	はい	はい	はい	はい	はい
DC750/1500/3500 シリーズ 3 防御センター	はい	はい	はい	はい	はい	はい
仮想防御センター	はい	はい	はい	はい	はい	はい

この表の情報に加えて、次の点にも注意してください。

- シリーズ 2 デバイスは、セキュリティ インテリジェンス フィルタリングを除く保護機能を自動的に取得します。
- 仮想デバイス上の制御ライセンスを有効にできますが、仮想デバイスはそのライセンスによって付与されるハードウェア ベースの機能（スイッチングやルーティングなど）をサポートしません。
- DC500 は保護および制御のライセンスでデバイスを管理できますが、セキュリティ インテリジェンス フィルタリングとユーザ制御を実行することはできません。

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

従来の RNA ホストおよび RUA ユーザ ライセンスの使用

FireSIGHT システム バージョン 4.10.x では、RNA ホストおよび RUA ユーザ機能のライセンスによって、監視対象のホストとユーザの制限が決定されました。以前に防御センターでバージョン 4.10.x を実行していた場合は、FireSIGHT ライセンスの代わりに、従来のホスト ライセンスとユーザ ライセンスを使用できます。

従来のライセンスを使用するバージョン 5.3.1 防御センターは、FireSIGHT ホスト制限として RNA ホスト制限を使用し、FireSIGHT ユーザおよびアクセス制御対象ユーザの両方の制限として RUA ユーザ制限を使用します。FireSIGHT ホスト ライセンス制限ヘルス モジュールはライセンス制限に適した警告を発行します。

RNA ホスト制限と RUA ユーザ制限は累積的であることに注意してください。つまり、各タイプの複数のライセンスを防御センターに追加することにより、ライセンスによって許可されるホストまたはユーザの総数を監視できます。

あとで FireSIGHT ライセンスを追加した場合、防御センターはより高い制限を使用します。たとえば、DC1500 上の FireSIGHT ライセンスは、最大で 50,000 のホストとユーザをサポートします。バージョン 4.10.x DC1500 上の RNA ホスト制限が 50,000 を超えていた場合は、バージョン 5.3.1 を実行している同じ防御センター上でその従来のホスト ライセンスを使用すると、より高い制限を使用できます。便宜上、Web インターフェイスには、より高い制限を示すライセンスだけが表示されます。

(注)　FireSIGHT ライセンス制限は防御センターのハードウェア機能に対応しているため、従来のライセンスを使用する場合はこの制限を**超えない**ようにすることをシスコでは推奨しています。ガイダンスについては、サポート担当にお問い合わせください。

バージョン 4.10.x からバージョン 5.3.1 への更新パスが存在しないため、ISO イメージを使用して防御センターを「復元する」必要があります。再イメージングすると、アプライアンスに関する**すべての**設定とイベント データが失われることに注意してください。再イメージング後に、このデータをアプライアンスにインポートすることは**できません**。詳細については、「出荷時の初期状態に FireSIGHT システム アプライアンスを復元する」（P.7-1）を参照してください。

(注)　アプライアンスの再イメージングは、メンテナンス期間中にのみ行ってください。再イメージングにより、インライン展開のデバイスが非バイパス設定にリセットされるため、バイパス モードを再設定するまではネットワーク上のトラフィックが中断されます。詳細については、「復元プロセスの間のトラフィック フロー」（P.7-2）を参照してください。

復元プロセスでは、ライセンスとネットワークの設定を削除するように促されます。これらの設定をそのまま保持してください。ただし誤って削除しても、後から追加し直すことができます。バージョン 5.3.1 防御センターは、バージョン 4.10.x デバイスを管理できないことに注意してください。ただし、サポートされているバージョン 4.10.x デバイスを復元して最新バージョンに更新することができます。詳細については、「出荷時の初期状態に FireSIGHT システム アプライアンスを復元する」（P.7-1）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　X-Series の Sourcefire ソフトウェア 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 アクセスの要件」（P.1-18）
- 「通信ポートの要件」（P.1-19）

インターネット アクセスの要件

FireSIGHT システム アプライアンスは、デフォルトで開かれるポート 443/tcp（HTTPS）とポート 80/tcp（HTTP）を介して、インターネットに直接接続するよう設定されます（「通信ポートの要件」（P.1-19）を参照）。ほとんどの FireSIGHT システム アプライアンスでプロキシ サーバを使用できることに注意してください（『*FireSIGHT System User Guide*』の「Configuring Network Settings」の章を参照してください）。

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。そのため、『*FireSIGHT System User Guide*』の「デバイスの管理」の章に記載されているように、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 1-8　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、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	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	n/a
FireAMP 統合	Collective Security Intelligence クラウド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、X-Series、および ASA FirePOWER 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	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、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、X-Series、および ASA FirePOWER を除く）	システム更新は同期されません。
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が 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、X-Series、および ASA FirePOWER 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

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、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ると、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（『*FireSIGHT System User Guide*』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（『*FireSIGHT System User Guide*』を参照）。
- 管理ポート（8305/tcp）を変更できます（『*FireSIGHT System User Guide*』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 Collective Security Intelligence クラウド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 5.3.1 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 1-9　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。

表 1-9　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
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、X-Series、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 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（仮想デバイス、X-Series、および ASA FirePOWER 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、X-Series、および ASA FirePOWER を除く）	アプライアンスの Web インターフェイスにアクセスします。

表 1-9　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 • ネットワーク トラフィックで検出されたファイルに関するマルウェア ディスポジション • 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-Series、および ASA FirePOWER	動的分析用にファイルをシスコ クラウドに送信します。
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、X-Series、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	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。**
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 とシスコ クラウドの通信を可能にします。

アプライアンスの事前設定

あとで他のサイトに展開するために、1 つの場所で一元的に複数のデバイスと防御センターを事前設定することができます。アプライアンスを事前設定するときの考慮事項については、「FireSIGHT システム アプライアンスの事前設定」（P.E-1）を参照してください。