
# Cisco FireSIGHT システムの概要

Cisco FireSIGHT® システムは、専用プラットフォームで展開されるか、ソフトウェア ソリューションとして展開される、ネットワーク セキュリティおよびトラフィック管理製品の統合スイートです。

システムは、組織のセキュリティ ポリシー（ネットワークを保護するためのガイドライン）に準拠する方法でネットワーク トラフィックを処理できるように設計されています。セキュリティ ポリシーにはアクセプタブル ユース ポリシー（AUP）も含まれていることがあります。AUP は、組織のシステムの使用方法に関するガイドラインを従業員に提供します。

一般的な展開では、ネットワーク セグメントにインストールされた複数のトラフィック検知管理対象 *デバイス* が分析対象のトラフィックをモニタし、管理を行う *防御センター*® にレポートします。インライン展開の場合、デバイスがトラフィックのフローに影響を与える場合があります。

ヒント

デバイスおよび 防御センター には複数のモデルがあります。管理対象デバイスには、物理および仮想 FirePOWER アプライアンス、Blue Coat X-Series 向け Cisco NGIPS、Cisco ASA with FirePOWER Services（ASA FirePOWER）が含まれます。防御センター は、物理または仮想アプライアンスとして展開することもできます。必要に応じて、アプライアンス モデルはさらにシリーズおよびファミリに分類されます。通常、システム機能はモデルおよびライセンスによって異なります。

防御センター では、集中管理コンソールの Web インターフェイスを使用して管理、分析、およびレポート タスクを実行できます。物理管理対象デバイスにも、初期セットアップ、基本的な分析と設定タスクを実行するために使用できる Web インターフェイスがあります。仮想管理対象デバイス、Blue Coat X-Series 向け Cisco NGIPS、および ASA FirePOWER デバイスには、FireSIGHT システムの Web インターフェイスがありません。これらのデバイスでは、管理を行う 防御センター を使用して実行できないタスクは CLI を使用して実行する必要があります。

このガイドでは、FireSIGHT システムの特徴と機能について説明します。各章の説明、図、および手順では、ユーザ インターフェイスのナビゲート、システム パフォーマンスの最大化、問題のトラブルシューティングに役に立つ詳細な情報を記載しています。

続く各トピックでは、FireSIGHT システムの概要、主要なコンポーネント、およびこのマニュアルの使用方法について説明しています。

# 管理対象デバイスの概要

ネットワーク セグメントにインストールされている管理対象デバイスは、分析のためにトラフィックを監視します。パッシブな展開の場合、管理対象デバイスは、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、送信されたファイル（マルウェアを含む）、脆弱性など、組織の資産に関する詳細情報を収集します。FireSIGHT システムがこの情報を分析用に関連付けることで、ユーザがアクセスする Web サイトと使用するアプリケーションをモニタし、トラフィック パターンを評価して、侵入や他の攻撃の通知を受信できます。

インラインで展開されたシステムは、*アクセス コントロール*を使用してトラフィックのフローに影響を与えることができ、これによって、ネットワークを出入りしたり通過したりするトラフィックを処理する方法を詳細に指定できます。ネットワーク トラフィックについて収集したデータおよびそのデータから収集したすべての情報は、次に基づいてそのトラフィックのフィルタ処理や制御ができます。

- シンプルで容易に決定されるトランスポート層およびネットワーク層の特性（送信元と宛先、ポート、プロトコルなど）
- レピュテーション、リスク、ビジネスとの関連性、使用されたアプリケーション、または訪問した URL などの特性を含む、トラフィックに関する最新のコンテキスト情報
- 組織の Microsoft Active Directory LDAP ユーザ（ユーザごとに異なるアクセス レベルを付与できます）
- 暗号化されたトラフィックの特性（このトラフィックを復号化してさらに分析することもできます）
- 暗号化されていないトラフィックまたは復号化されたトラフィックに、禁止されているファイル、検出されたマルウェア、または侵入イベントが存在するかどうか

各タイプのトラフィックのインスペクションと制御は、最大限の柔軟性とパフォーマンスを引き出すために最も意味がある局面で実行されます。たとえば、レピュテーション ベースのブラックリスト登録は、単純な送信元と宛先のデータを使用するため、禁止されたトラフィックをプロセスの初期段階でブロックできます。その一方、侵入およびエクスプロイトの検出とブロックは、プロセスの最後の防衛ラインとして実行されます。

アクセス コントロールに加えて、シリーズ 3 デバイスでネットワーク管理機能を使用すると、スイッチドおよびルーテッド環境での対応、ネットワーク アドレス変換（NAT）の実行が可能になります。また、設定した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）トンネルを構築できます。バイパス インターフェイス、集約インターフェイス、高速パス ルール、厳密な TCP の適用を設定することもできます。

詳細については、以下を参照してください。

- シリーズ 2 およびシリーズ 3 管理対象デバイス（1-3 ページ）
- 64 ビット仮想管理対象デバイス（1-3 ページ）
- Blue Coat X-Series 向け Cisco NGIPS（1-4 ページ）
- Cisco ASA with FirePOWER Services（1-4 ページ）
- Snort プロセスを再開する構成（1-8 ページ）
- Snort の再開によるトラフィックへの影響（1-9 ページ）

# シリーズ 2 およびシリーズ 3 管理対象デバイス

Cisco FirePOWER 7000 シリーズおよび 8000 シリーズのすべてのデバイスを含むシリーズ 3 デバイスは、FireSIGHT システム専用の物理デバイスの第 3 シリーズです。シリーズ 3 デバイスのスループットはさまざまですが、多数の同じ機能を共有します。一般に、8000 シリーズ デバイスは 7000 シリーズよりも高性能で、高速パス ルール、リンク集約、およびスタックなどの追加機能もサポートします。

防御センター と シリーズ 3 デバイスは、どちらもブランディング遷移中であることをご了承ください。防御センター は FireSIGHT Management Center とも呼ばれ、シリーズ 3 デバイスは FirePOWER デバイスとも呼ばれます。防御センター の製品識別番号は、DC ではなく FS で始まる場合があります。同様に、シリーズ 3 デバイスの製品識別番号は 3D ではなく FP で始まる場合があります。その他の点ではモデル番号の変更はありません。たとえば、DC4000 および FS4000 は同じ 防御センター を指します。

シリーズ 2 は物理管理対象デバイスの第 2 シリーズです。シリーズ 2 デバイスは、Protection ライセンスに関連する機能のほとんど（侵入検知と防御、ファイル制御、および単純なネットワーク ベースのアクセス制御）を自動的に保有します。

ただしリソースおよびアーキテクチャの制限により、シリーズ 2 デバイスは Protection ライセンスで使用できる機能の一部しかサポートしません。シリーズ 2 デバイスは、アーカイブ ファイル内にネストされたファイルに対して、セキュリティ インテリジェンス フィルタリングおよびファイル制御を実行できません。また、シリーズ 2 デバイスでは、FireSIGHT ライセンス付きの防御センター を使用しても、地理位置情報ベースのアクセス制御を実行することはできません。シリーズ 2 デバイスでライセンスを取得した他の機能を有効にすることは**できません**。

今後、Cisco から新しいシリーズ 2 アプライアンスが出荷されることはありませんが、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 デバイスをバージョン 5.4.1 に更新または再イメージ化することができます。イメージの再作成の結果、アプライアンス上のほとんど**すべて**の設定とイベント データは失われますので注意してください。詳細については、『*FireSIGHT システム Installation Guide*』を参照してください。

ヒント　バージョン 4.10.3 の配置環境からバージョン 5.2 の配置環境に特定の設定とイベント データを移行した後、バージョン 5.4.1 に更新できます。詳細については、バージョン 5.2 の『*FireSIGHT システム Migration Guide*』を参照してください。

# 64 ビット仮想管理対象デバイス

VMware vSphere Hypervisor または VMware vCloud Director 環境を使用して ESXi ホストとして 64 ビット仮想デバイスを展開できます。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。サポートされているバージョンのリストについては、『*FireSIGHT システム Virtual Installation Guide*』を参照してください。VMware ツール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。

仮想アプライアンスでは e1000（1 ギガビット/秒）インターフェイスが使用されますが、VMware vSphere Client を使用してデフォルトのセンシングおよび管理インターフェイスを vmxnet3（10 ギガビット/秒）インターフェイスに置き換えることもできます。また、VMware vSphere Client を使用して、仮想 防御センター で追加の管理インターフェイスを作成できます。詳細については、『*FireSIGHT システム Virtual Installation Guide*』を参照してください。

インストールおよび適用されているライセンスに関係なく、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、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 FireSIGHT システムの Web インターフェイスがありません。

# Blue Coat X-Series 向け Cisco NGIPS

Blue Coat X-Series 向け Cisco NGIPS を Blue Coat X-シリーズ プラットフォームにインストールできます。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ているライセンスに関係なく、Blue Coat X-Series 向け Cisco NGIPS は FireSIGHT システムの次の機能をサポートしません。

- Blue Coat X-Series 向け Cisco NGIPS は、高度なマルウェア対策（AMP）、アプリケーション制御、ユーザ制御、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）を含む、マルウェア または Control ライセンスで使用できる機能をサポートしません。
- Blue Coat X-Series 向け Cisco NGIPS を使用して、暗号化されたトラフィックを復号化または検査（SSL インスペクション）することはできません。
- Blue Coat X-Series 向け Cisco NGIPS を使用して、ネットワーク トラフィックをその発信元または宛先の国または大陸に基づいてフィルタリングすること（地理位置情報に基づくアクセス制御）はできません。
- 防御センター の Web インターフェイスを使用して Blue Coat X-Series 向け Cisco NGIPS の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 Blue Coat X-Series 向け Cisco NGIPS のシャットダウン、再起動、その他の管理を行うことはできません。
- 防御センター を使用して、Blue Coat X-Series 向け Cisco NGIPS のバックアップを作成したり、バックアップからそれを復元したりすることはできません。
- Blue Coat X-Series 向け Cisco NGIPS にヘルス ポリシーまたはシステム ポリシーを適用することはできません。これには時間設定の管理が含まれます。

Blue Coat X-Series 向け Cisco NGIPS に Web インターフェイスはありません。ただし、X-シリーズ 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、システムのインストールや、次のようなプラットフォーム固有の管理タスクを実行します。

- X-シリーズ プラットフォームのロード バランシングと冗長性の利点（Cisco の物理デバイス クラスタリングと同等）を活用できる Virtual Appliance Processor（VAP）グループの作成
- 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単位（MTU）の設定を含む）
- プロセスの管理
- 時間設定の管理（NTP の設定を含む）

# Cisco ASA with FirePOWER Services

Cisco ASA with FirePOWER Services（ASA FirePOWER デバイス）は、管理対象デバイスと同様に機能します。この配置環境では、ASA デバイスは最も重要なシステム ポリシーを提供し、アクセス制御、侵入検知と防御、ディスカバリ、および高度なマルウェア対策のためにトラフィックを FireSIGHT システムに渡します。

インストールおよび適用されているライセンスに関係なく、ASA FirePOWER デバイスは FireSIGHT システムの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、これらの機能は ASA プラットフォームによって提供され、ASA CLI および ASDM を使用して設定できます。詳細については、ASA のマニュアルを参照してください。

- ASA FirePOWER デバイスは SSL インスペクション（検査）をサポートしません。
- 防御センター の Web インターフェイスを使用して ASA FirePOWER の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 のシャットダウン、再起動、その他の管理を行うことはできません。
- 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したり、バックアップからそのデバイスを復元したりすることはできません。
- VLAN タグの条件を使用して、トラフィックを照合するためのアクセス コントロール ルールを記述することはできません。

ASA FirePOWER デバイスに FireSIGHT Web インターフェイスはありません。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。ASA 専用のこれらのツールを使用して、システムのインストールおよびプラットフォーム固有のその他の管理タスクを実行します。詳細については、ASA FirePOWER モジュールのドキュメントを参照してください。

スタンドアロン デバイスまたは管理対象デバイスとして ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X、ASA5516-X、および ISA 3000 デバイスを管理できます。スタンドアロンの ASA FirePOWER モジュールは ASDM の ASA FirePOWER 構成で管理し、管理対象の ASA FirePOWER モジュールは防御センターで管理します。デバイスが防御センターに登録されている場合、ASA FirePOWER モジュールを ASDM で管理することはできません。

ASA FirePOWER デバイスを編集し、マルチ コンテキスト モードからシングル コンテキスト モード（またはその逆）に切り替えると、デバイスによってすべてのインターフェイスの名前が変更されることに注意してください。更新された ASA FirePOWER のインターフェイス名を使用する、すべての FireSIGHT システム セキュリティ ゾーン、相関ルール、および関連する設定の再設定が**必要**です。

（注）　防御センター では、ASA FirePOWER デバイスが SPAN ポート モードで展開されている場合、ASA インターフェイスを表示しません。

# Cisco ISA 3000

Cisco ISA 3000 はファイアウォール、脅威に対する防御、および VPN サービスを提供する、DIN レールに取り付ける高耐久性産業セキュリティ アプライアンスです。これはギガビット イーサネットと専用管理ポートを備えた、低消費電力、ファンなしのデバイスです。次の 2 つの SKU があります。

• Copper SKU（管理ポートの付いた 4x10/100/1000Base-T を装備）

• Fiber SKU（2x1GbE SFP および管理ポートの付いた 2x10/100/1000Base-T を装備）

Cisco ISA 3000 には、業界屈指の脅威と拡張マルウェア保護を組み合わせた Cisco ASA ファイアウォール保護が付属します。Cisco ISA 3000 は Cisco ASA with FirePOWER Services を実行します。詳細については、Cisco ASA with FirePOWER Services（1-4 ページ）を参照してください。

# 管理対象デバイスの各モデルでサポートされる機能の概要

バージョン 5.4.1 を実行している場合、FireSIGHT システム デバイスのスループットと機能はモデルおよびライセンスによって異なります。

防御センター と シリーズ 3 デバイスは、どちらもブランディング遷移中であることをご了承ください。防御センター は FireSIGHT Management Center とも呼ばれ、シリーズ 3 デバイスは FirePOWER デバイスとも呼ばれます。防御センター の製品識別番号は、DC ではなく FS で始まる場合があります。同様に、シリーズ 3 デバイスの製品識別番号は 3D ではなく FP で始まる場合があります。その他の点ではモデル番号の変更はありません。たとえば、DC4000 および FS4000 は同じ 防御センター を指します。

バージョン 5.4.1 デバイスの管理にはどのバージョン 5.4.1 防御センター でも使用できますが、DC500（および範囲がより狭い DC750 まで）がサポートする FireSIGHT システムの機能は制限されています。詳細については、防御センター の各モデルでサポートされる機能の概要（1-11 ページ）を参照してください。

次の表では、システムの主なアクセス制御機能とネットワーク管理機能を、それらの機能をサポートする管理対象デバイスおよび有効にする必要があるライセンスに対応付けています。これらの機能の簡単な説明は、FireSIGHT システム のコンポーネント（1-15 ページ）を参照してください。

*表 1-1　各デバイス モデルでサポートされるアクセス制御機能*

| 機能 | シリーズ 2 デバイス | シリーズ 3 デバイス | ASA FirePOWER デバイス | 仮想デバイス | X-シリーズ デバイス | ライセンス |
|---|---|---|---|---|---|---|
| アクセス制御：基本的なネットワーク制御 | はい | はい | VLAN 制御なし | はい | はい | 任意（Any） |
| アクセス制御：リテラル URL | いいえ | はい | はい | はい | はい | 任意（Any） |
| アクセス制御：SSL インスペクション | いいえ | はい | いいえ | いいえ | いいえ | 任意（Any） |
| ネットワーク検出：ホスト、ユーザ、アプリケーション | はい | はい | はい | はい | はい | FireSIGHT |
| アクセス制御：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 | FireSIGHT |
| 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 | Protection |
| 侵入検知および防御（IPS） | はい | はい | はい | はい | はい | Protection |
| ファイル制御：ファイル タイプ別 | はい | はい | はい | はい | はい | Protection |
| ファイル制御：アーカイブ ファイルのインスペクション | いいえ | はい | はい | はい | はい | Protection |
| 高度なマルウェア防御（AMP） | いいえ | はい | はい | はい | いいえ | マルウェア |
| アクセス制御：アプリケーション制御 | いいえ | はい | はい | はい | いいえ | Control |
| アクセス制御：ユーザ制御 | いいえ | はい | はいはい | はい | いいえ | Control |
| 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 | いいえ | はい | はい | はい | はい | URL Filtering |

*表 1-2　各デバイス モデルでサポートされる管理およびネットワーク管理機能*

| 機能 | シリーズ 2 デバイス | シリーズ 3 デバイス | ASA FirePOWER デバイス | 仮想デバイス | X-シリーズ デバイス | ライセンス |
|---|---|---|---|---|---|---|
| トラフィック チャネル | いいえ | はい | いいえ | いいえ | いいえ | 任意（Any） |
| 複数の管理インターフェイス | いいえ | はい | いいえ | いいえ | いいえ | 任意（Any） |
| リンク集約 | いいえ | はい | いいえ | いいえ | いいえ | 任意（Any） |
| FireSIGHT システム Web インターフェイス | 限定的 | 限定的 | いいえ | いいえ | いいえ | 任意（Any） |
| 制限されたコマンドライン インターフェイス（CLI） | いいえ | はい | はい | はい | いいえ | 任意（Any） |
| 外部認証 | はい | はい | いいえ | いいえ | いいえ | 任意（Any） |
| eStreamer クライアントへの接続 | はい | はい | はい | いいえ | いいえ | 任意（Any） |
| 自動アプリケーション バイパス | はい | はい | はい | はい | いいえ | 任意（Any） |
| タップ モード | いいえ | はい | いいえ | いいえ | いいえ | 任意（Any） |
| 高速パス ルール | いいえ | 8000 シリーズ | いいえ | いいえ | いいえ | 任意（Any） |
| 厳密な TCP の適用 | いいえ | はい | いいえ | いいえ | いいえ | Protection |
| インラインセットのバイパス モード | はい | NetMod/SFP によって異なる | いいえ | いいえ | いいえ | Protection |
| 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 | マルウェア |
| スイッチング、ルーティング、スイッチドおよびルーテッド集約インターフェイス | いいえ | はい | いいえ | いいえ | いいえ | Control |
| NAT ポリシー | いいえ | はい | いいえ | いいえ | いいえ | Control |
| デバイス スタッキング | いいえ | 3D8140<br>82xx ファミリ<br>83xx ファミリ | いいえ | いいえ | いいえ | 任意（Any） |
| デバイス クラスタリング | いいえ | はい | いいえ | いいえ | X-シリーズ ベース | Control（X-シリーズ を除く） |
| クラスタ化スタック | いいえ | 3D8140<br>82xx ファミリ<br>83xx ファミリ | いいえ | いいえ | いいえ | Control |
| VPN | いいえ | はい | いいえ | いいえ | いいえ | VPN |

# Snort プロセスを再開する構成

Snort® プロセスは、下記のいずれかの構成を適用すると、必ず再開されます。

**注意**　構成の一部を適用するときに、Snort プロセスの再開が要求され、これにより一時的にトラフィック検査が中断します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

**アクセス コントロール ポリシー**

- 初めてポリシーを適用する
- アクセス コントロール ルール内の [URL] タブで URL カテゴリおよびレピュテーション条件を追加または削除する
- アクセス コントロール ルール内の [インスペクション（Inspection）] タブで侵入ポリシーまたはファイル ポリシーを関連付ける、または、その後で [なし（None）] を選択することによってポリシーを削除する

**アクセス コントロール ポリシーの詳細設定**

- [一般設定（General Settings）] で [ポリシー適用中のトラフィックの検査（Inspect Traffic During Policy Apply）] を無効にする
- [ファイルとマルウェアの設定（Files and Malware Settings）] で値を変更する
- [SSL ポリティ?設定（SSL Policy Settings）] で SSL ポリシーを関連付ける、または、その後で [なし（None）] を選択することによってポリシーを削除する
- [検出拡張設定（Detection Enhancement Settings）] で適応型プロファイルを有効または無効にする

**セキュリティ インテリジェンス（Security Intelligence）**

- 右クリック メニューで [今すぐホワイトリスト（Whitelist Now）] または [今すぐブラックリスト（Blacklist Now）] オプションを選択する場合を除き、セキュリティ インテリジェンス リストを変更する

**SSL ポリシー**

- SSL ルール内の [カテゴリ（Category）] タブで URL カテゴリおよびレピュテーションを追加または削除する

**ファイル ポリシー**

- アーカイブ ファイル インスペクションを有効または無効にする
- ファイル タイプまたはファイル カテゴリをファイル ルールに追加する、または、その後でルールからそれを削除する
- [ファイルの検出（Detect Files）] または [マルウェアのブロック（Block Malware）] でファイル ルール アクションを変更する
- ファイル ルールで [ファイルの保存（Store Files）] を有効または無効にする

ネットワーク分析ポリシー

- IMAP、POP、または SMTP プリプロセッサの値（[Base64 復号化の深さ（Base64 Decoding Dept）]、[7 ビット/8 ビット/バイナリ復号化の深さ（7-Bit/8-Bit/Binary Decoding Depth）]、[引用符で囲まれた印刷可能な復号化の深さ（Quoted-Printable Decoding Depth）]、または [UNIX 間復号化の深さ（Unix-to-Unix Decoding Depth）]）を変更する

デバイス管理

- ルーティング：シリーズ 3 ルーテッド インターフェイスまたは仮想ルータを追加する
- VPN：VPN を追加または削除する
- MTU：非管理インターフェイスの MTU 値（シリーズ 2）または MTU 最高値（シリーズ 3）を変更する
- デバイス ハイ アベイラビリティ（高可用性）：ハイ アベイラビリティ状態共有オプションを変更する
- AAB：AAB をアクティブにする

（注）　自動アプリケーション バイパス（AAB）は、それが有効化されていて、単一パケットの処理に異常に長い時間がかかっている場合にのみアクティブになります。AAB がアクティブになると、Snort プロセスが再起動します。

更新の事前適用

- 新しい（または更新された）共有オブジェクト ルールを含む侵入ルール更新をインポートした後、アクセス コントロールまたは侵入ポリシーを適用する
- 脆弱性データベース（VDB）更新をインストールした後、アクセス コントロール ポリシーを適用する

システムの更新プログラム

バイナリの変更を含むシステム更新プログラムまたはパッチをインストールします。バイナリの変更には、Snort、プリプロセッサ、脆弱性データベース（VDB）、または共有オブジェクト ルールの変更が含まれることがあります。なお、管理対象デバイスの場合は、バイナリの変更が含まれていないパッチを適用すると Snort の再開が必要になることがあります。

# Snort の再開によるトラフィックへの影響

次の表に示すように、トラフィックに対する Snort の再開（再起動）の影響は、管理対象デバイスのモデル、およびデバイスでのトラフィック処理方法に応じて異なります。

*表 1-3　再開によるトラフィックへの影響（管理対象デバイスのモデル別）*

| モデル | 設定 | 再開中のトラフィック |
|---|---|---|
| シリーズ 2、シリーズ 3、仮想 | インライン、[フェールセーフ（Failsafe）] が有効または無効 | インスペクションなしで受け渡される*（[フェールセーフ（Failsafe）] が無効になっていて、しかも Snort がビジー状態だがダウンしていない場合、いくつかのパケットがドロップすることがあります） |
| | パッシブ | 中断なし、インスペクションなし |

*表 1-3　再開によるトラフィックへの影響（管理対象デバイスのモデル別）（続き）*

| モデル | 設定 | 再開中のトラフィック |
|---|---|---|
| 3D9900、シリーズ 3 | インライン、タップ モード | 中断なし、インスペクションなし* |
| シリーズ 3 | ルーテッド、スイッチド、透過 | ドロップされる |
| ASA FirePOWER | フェールオープン（[トラフィック許可（Permit Traffic）]）状態のルーテッドまたは透過 | インスペクションなしで受け渡される |
| | フェールクローズ（[トラフィッククローズ（Close Traffic）]）状態のルーテッドまたは透過 | ドロップされる |

*シリーズ 2 は、センシング インターフェイスで MTU を変更すると、トラフィックをドロップします。それ以外の場合は、図のようにトラフィックを処理します。

# 防御センター の概要

防御センター は、FireSIGHT システム展開の集中管理コンソールおよびデータベース リポジトリを提供します。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の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、ホストに侵害の痕跡（兆候）タグを付けます。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。防御センター は、デバイスのネットワーク管理機能（スイッチング、ルーティング、NAT、VPN など）も制御します。

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
- 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
- カスタムおよびテンプレートベースのレポート
- 運用の継続性を確保するハイ アベイラビリティ（冗長性）機能

シリーズ 2 およびシリーズ 3 防御センター は、Cisco が提供するフォールトトレラントな専用の物理ネットワーク アプライアンスです。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 を展開することもできます。防御センター は、すべてのタイプ（物理、仮想、Cisco ASA with FirePOWER Services、および Blue Coat X-Series 向け Cisco NGIPS）のデバイスを管理できます。

防御センター は、さまざまなデバイス管理、イベント保存、ホスト モニタリング、およびユーザ モニタリング機能を備えています。リソースおよびアーキテクチャの制限により、DC500（および範囲がより狭い DC750 まで）は FireSIGHT システム機能の一部しかサポートしないことに注意してください。

防御センター と シリーズ 3 デバイスは、どちらもブランディング遷移中であることをご了承ください。防御センター は FireSIGHT Management Center とも呼ばれ、シリーズ 3 デバイスは FirePOWER デバイスとも呼ばれます。防御センター の製品識別番号は、DC ではなく FS で始まる場合があります。同様に、シリーズ 3 デバイスの製品識別番号は 3D ではなく FP で始まる場合があります。その他の点ではモデル番号の変更はありません。たとえば、DC4000 および FS4000 は同じ 防御センター を指します。

(注)　今後、Cisco から新しいシリーズ 2 防御センター が出荷されることはありませんが、バージョン 5.4.1 に更新または再イメージ化することができます。イメージの再作成の結果、アプライアンス上のほとんど**すべて**の設定とイベント データは失われますので注意してください。詳細については、『*FireSIGHT システム Installation Guide*』を参照してください。

# 防御センター の各モデルでサポートされる機能の概要

バージョン 5.4.1 を実行している場合、すべての 防御センター には同様の機能がありますが、容量と速度が主な違いとなります。防御センター のモデルによって、管理できるデバイス数、保存できるイベント数、およびモニタできるホスト数とユーザ数が異なります。詳細については、以下を参照してください。

- デバイスの管理（4-1 ページ）
- データベース イベント制限の設定（63-16 ページ）
- FireSIGHT ホストおよびユーザ ライセンスの制限について（65-9 ページ）

バージョン 5.4.1 デバイスの管理にはどのバージョン 5.4.1 防御センター でも使用できますが、DC500（および範囲がより狭い DC750 まで）がサポートする FireSIGHT システムの機能は制限されています。また、**デバイス**のライセンスおよびモデルによって多くのシステム機能が制限されます。管理対象デバイスの各モデルでサポートされる機能の概要（1-6 ページ）を参照してください。

DC 2000 および DC4000 では、Cisco のユニファイド コンピューティング システム（UCS）プラットフォームが FireSIGHT システムに導入されます。DC2000 および DC4000 は、ベースボード管理コントローラ（BMC）上で UCS Manager やCisco Integrated Management Controller（CIMC）などのツールを使用する Cisco の機能をサポートしないことに注意してください。次の表では、システムのアクセス制御およびネットワーク管理の主な機能に、それらの機能をサポートする 防御センター および有効にする必要があるライセンスを対応付けます。これらの機能の簡単な説明は、FireSIGHT システム のコンポーネント（1-15 ページ）を参照してください。

*表 1-4　防御センター の各モデルでサポートされるアクセス制御機能*

| 機能 | シリーズ 2 防御センター | シリーズ 3 防御センター | 最大で 防御センター | ライセンス |
|---|---|---|---|---|
| 単純なネットワークベースのアクセス制御を実行するデバイスを管理する | はい | はい | はい | 任意（Any） |
| リテラル（手動入力）URL 別の URL 制御を実行するデバイスを管理する | はい | はい | はい | 任意（Any） |
| SSL インスペクションを実行するデバイスを管理する | はい | はい | はい | 任意（Any） |
| 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 | はい | はい | はい | FireSIGHT |
| 地理位置情報（国および大陸）データによる検出を強化し、地理位置情報ベースのアクセス制御を実行するデバイスを管理する | DC1000、DC3000 | はい | はい | FireSIGHT |

*表 1-4　防御センター の各モデルでサポートされるアクセス制御機能（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 | 最大で 防御センター | ライセンス |
|---|---|---|---|---|
| セキュリティ インテリジェンス フィルタリング（ブラックリスト登録）を実行するデバイスを管理する | DC1000、DC3000 | はい | はい | Protection |
| 侵入検知と防御（IPS）の配置を管理する | はい | はい | はい | Protection |
| 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 | はい | はい | はい | Protection |
| アーカイブ ファイルのインスペクションを実行するデバイスを管理する | DC1000、DC3000 | はい | はい | Protection |
| アプリケーション制御を実行するデバイスを管理する | はい | はい | はい | Control |
| ユーザ制御を実行するデバイスを管理する | DC1000、DC3000 | はい | はい | Control |
| 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 | DC1000、DC3000 | はい | はい | URL フィルタリング（URL Filtering） |
| 高度なマルウェア対策（AMP）の展開を管理し、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 | はい | マルウェア |
| 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 | はい | はい | はい | FireAMP サブスクリプション |
| 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 | 任意（Any） |

*表 1-5　防御センター の各モデルでサポートされるネットワーク管理および冗長性機能*

| 機能 | シリーズ 2 防御センター | シリーズ 3 防御センター | 最大で 防御センター | ライセンス |
|---|---|---|---|---|
| トラフィック チャネルを使用して、内部と外部のトラフィックを分離して管理する | いいえ | はい | はい | 任意（Any） |
| 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 | いいえ | はい | はい | 任意（Any） |
| 防御センター の冗長性（ハイ アベイラビリティ）を確立する | DC1000、DC3000 | DC1500、DC2000、DC3500、DC4000 | いいえ | 任意（Any） |

*表 1-5　防御センター の各モデルでサポートされるネットワーク管理および冗長性機能（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 | 最大で 防御センター | ライセンス |
|---|---|---|---|---|
| デバイスベースの冗長性とリソース共有（スタック、クラスタ、およびクラスタ化スタック）を管理する | はい | はい | はい | Control |
| ハードウェア依存のネットワーク管理機能（高速パス ルール、厳密な TCP の適用、バイパス モード、タップ モード、スイッチングおよびルーティング、NAT、VPN）を使用してデバイスを管理する | はい | はい | はい | 機能に応じて異なる |

# バージョン 5.4.X で提供される 防御センター とデバイス

次の表に、Cisco FireSIGHT システム バージョン 5.4.X で提供され 防御センター と管理対象デバイスを示します。

*表 1-6　バージョン 5.4.1 FireSIGHT システムの 防御センター およびデバイス*

| モデル/ファミリ | シリーズ | タイプ | バージョン 5.4.x |
|---|---|---|---|
| 70xx ファミリ：<br>• 3D7010/7020/7030/7050 | シリーズ 3 FirePOWER（7000 シリーズ） | デバイス | バージョン 5.4.0.x |
| 71xx ファミリ：<br>• 3D7110/7120<br>• 3D7115/7125<br>• AMP7150 | シリーズ 3 FirePOWER（7000 シリーズ） | デバイス | バージョン 5.4.0.x |
| 81xx ファミリ：<br>• 3D8120/8130/8140<br>• AMP8150 | シリーズ 3 FirePOWER（8000 シリーズ） | デバイス | バージョン 5.4.0.x |
| 82xx ファミリ：<br>• 3D8250<br>• 3D8260/8270/8290 | シリーズ 3 FirePOWER（8000 シリーズ） | デバイス | バージョン 5.4.0.x |
| 83xx ファミリ：<br>• 3D8350<br>• 3D8360/8370/8390<br>• AMP8350<br>• AMP8360/8370/8390 | シリーズ 3 FirePOWER（8000 シリーズ） | デバイス | バージョン 5.4.0.x |
| 64 ビット仮想デバイス | 適用対象外 | デバイス | バージョン 5.4.0.x |
| Blue Coat X-Series 向け Cisco NGIPS | 適用対象外 | デバイス | バージョン 5.4.0.x |

*表 1-6　バージョン 5.4.1 FireSIGHT システムの 防御センター およびデバイス（続き）*

| モデル/ファミリ | シリーズ | タイプ | バージョン 5.4.x |
|---|---|---|---|
| ASA FirePOWER:<br>• ASA5512-X<br>• ASA5515-X<br>• ASA5525-X<br>• ASA5545-X<br>• ASA5555-X<br>• ASA5585-X-SSP-10<br>• ASA5585-X-SSP-20<br>• ASA5585-X-SSP-40<br>• ASA5585-X-SSP-60 | 適用対象外 | デバイス | バージョン 5.4.0.x |
| ASA FirePOWER:<br>• ASA5506-X<br>• ASA5506H-X<br>• ASA5506W-X<br>• ASA5508-X<br>• ASA5516-X<br>• ISA 3000 | 適用対象外 | デバイス | バージョン 5.4.1.x |
| シリーズ 3 防御センター:<br>• DC750/1500/3500<br>• DC2000/4000 | シリーズ 3 | 防御センター | バージョン 5.4.1.x |
| 64 ビット仮想 防御センター | 適用対象外 | 防御センター | バージョン 5.4.1.x |

防御センター と シリーズ 3 デバイスは、どちらもブランディング遷移中であることをご了承ください。防御センター は FireSIGHT Management Center とも呼ばれ、シリーズ 3 デバイスは FirePOWER デバイスとも呼ばれます。防御センター の製品識別番号は、DC ではなく FS で始まる場合があります。同様に、シリーズ 3 デバイスの製品識別番号は 3D ではなく FP で始まる場合があります。その他の点ではモデル番号の変更はありません。たとえば、DC4000 および FS4000 は同じ 防御センター を指します。

今後、Cisco から新しいシリーズ 2 アプライアンスが出荷されることはありませんが、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 デバイスと 防御センター をバージョン 5.4.1 に更新または再イメージングすることができます。イメージの再作成の結果、アプライアンス上のほとんど**すべて**の設定とイベント データは失われますので注意してください。詳細については、『*FireSIGHT システム Installation Guide*』を参照してください。

**ヒント**　バージョン 4.10.3 の配置環境からバージョン 5.2 の配置環境に特定の設定とイベント データを移行してから、バージョン 5.4.1 に更新できます。詳細については、バージョン 5.2 の『*FireSIGHT システム Migration Guide*』を参照してください。

# FireSIGHT システム のコンポーネント

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。



ヒント　FireSIGHT システムの多くの機能はアプライアンス モデル、ライセンス、およびユーザ ロールによって異なります。このドキュメントには、それぞれの機能用に FireSIGHT システムのどのライセンスとデバイスが必要か、各手順を完了するための権限を持っているのはどのユーザ ロールかについての情報が含まれています。詳細については、表記法（1-21 ページ）を参照してください。

## 冗長性およびリソース共有

FireSIGHT システム の冗長性とリソース共有機能を使用すれば、運用継続性を保証し、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

運用の継続性を確保するには、防御センターの*ハイ アベイラビリティ*機能で、冗長な DC1000、DC1500、DC2000、DC3000、DC3500、または DC4000 防御センター を指定してデバイスを管理できます。イベント データは管理対象デバイスから両方の 防御センター にストリームされ、特定の設定要素が両方の 防御センター で保持されます。一方の 防御センター で障害が発生した場合は、もう一方の 防御センター を使用して中断することなくネットワークをモニタできます。

### デバイス スタッキング

デバイスのスタッキングでは、1 つのスタック構成内で 2 ～ 4 個の物理デバイスを接続することにより、ネットワーク セグメントで検査されるトラフィックの量を増やすことができます。スタック構成を確立するときに、各スタック構成のデバイスのリソースを 1 つの共有構成に統合します。

### デバイス クラスタリング

デバイスのクラスタリング（デバイスの高可用性とも呼ばれる）では、2 つ以上の シリーズ 3 デバイスまたはスタック間でのネットワーキング機能および設定データの冗長性を確立することができます。2 つ以上のピア デバイスまたはスタックをクラスタリングすると、ポリシーの適用、システムの更新、および登録について 1 つの論理システムが生成されます。デバイスのクラスタリングを使用して、システムは手動または自動でフェールオーバーを実現することが可能です。

ほとんどの場合、SFRP を使用することによって、デバイスをクラスタ化せずにレイヤ 3 の冗長性を実現できます。SFRP では、指定した IP アドレスに対する冗長なゲートウェイとしてデバイスを機能させることができます。ネットワークの冗長性では、2 つ以上のデバイスまたはスタックが同じネットワーク接続を提供し、ネットワーク上の他のホストに対する接続性を保証するよう設定することができます。

#### Blue Coat X-Series 向け Cisco NGIPS によるロード バランシング

X-シリーズ プラットフォーム上で複数メンバーからなる VAP グループ内の個々の VAP として Blue Coat X-Series 向け Cisco NGIPS を展開することで、X-シリーズ プラットフォームのロード バランシングと冗長性の利点（Cisco の物理デバイス クラスタリングと同等）を活用できます。その場合は、防御センター を使用してそれらの VAP グループを管理します。詳細については、『*Blue Coat X-Series 向け Cisco NGIPS Installation and Configuration Guide*』を参照してください。

# ネットワーク トラフィックの管理

FireSIGHT システムのネットワーク トラフィック管理機能によって、管理対象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。ユーザは、スイッチド、ルーテッド、または（この両者を組み合わせた）ハイブリッドの環境内で機能するようシリーズ 3 のデバイスを設定し、ネットワーク アドレス変換（NAT）を実行することができます。また、安全な仮想プライベート ネットワーク（VPN）トンネルを構築することができます。

### スイッチング

複数のネットワーク セグメントの間でパケットのスイッチングが可能になるように、レイヤ 2 の展開で FireSIGHT システムを設定することができます。レイヤ 2 の展開では、スタンドアロンのブロードキャスト ドメインとして動作するよう、管理対象デバイス上でスイッチド インターフェイスおよび仮想スイッチを設定します。仮想スイッチは、ホストの MAC アドレスを使用してパケットの送信先を決定します。複数の物理インターフェイスを単一の論理リンクにグループ化することで、ネットワークの 2 つのエンドポイント間でパケット スイッチングが可能になります。エンドポイントは、2 台の FirePOWER 管理対象デバイス、またはサードパーティ アクセス スイッチに接続している 1 台の FirePOWER 管理対象デバイスである場合があります。

### ルーティング

複数のインターフェイス間でトラフィックをルーティングするように、レイヤ 3 の展開で、FireSIGHT システムを設定することができます。レイヤ 3 配置では、トラフィックを受信および転送するため、管理対象デバイスでルーテッド インターフェイスと仮想ルータを設定します。システムは宛先 IP アドレスに従ってパケット転送を決定し、パケットをルーティングします。ルータは転送基準に基づいて発信インターフェイスから宛先を取得し、アクセス コントロール ルールは、適用するセキュリティ ポリシーを指定します。

仮想ルータを設定するときに、スタティック（静的）ルートを定義できます。また、Routing Information Protocol（RIP）および Open Shortest Path First（OSPF）のダイナミック ルーティング プロトコルを設定することができます。スタティック ルートと RIP、またはスタティック ルートと OSPF を組み合わせて設定することもできます。ユーザは、設定するそれぞれの仮想ルータに対して DHCP リレーを設定できます。

Cisco アプライアンスの設定で仮想スイッチと仮想ルータの両方を使用する場合は、それらの 2 つの間でトラフィックをブリッジするように関連付けられているハイブリッド インターフェイスを設定できます。これらのユーティリティはトラフィックを分析し、そのタイプと適切な応答（ルート、スイッチ、またはそれ以外）を判断します。複数の物理インターフェイスを単一の論理リンクにグループ化することで、ネットワークの 2 つのエンドポイント間でトラフィックがルーティングされます。エンドポイントは、2 台の FirePOWER 管理対象デバイス、またはサードパーティ ルータに接続している 1 台の FirePOWER 管理対象デバイスである場合があります。

#### NAT

レイヤ 3 の展開で、ネットワーク アドレス変換（NAT）を設定できます。内部サーバを外部ネットワークに公開することも、内部ホストまたはサーバを外部アプリケーションに接続できるようにすることも可能です。また、IP アドレスのブロックを使用するか、IP アドレスおよびポート変換の制限付きのブロックを使用することにより、外部ネットワークからプライベート ネットワーク アドレスを隠すよう、NAT を設定することもできます。

#### VPN

バーチャル プライベート ネットワーク（VPN）は、インターネットや他のネットワークなどのパブリック ソースを介したエンドポイント間でセキュアなトンネルを確立するネットワーク接続です。シリーズ 3 デバイスの仮想ルータ間で安全な VPN トンネルを構築するよう、FireSIGHT システムを設定することができます。

## FireSIGHT

FireSIGHT™ は Cisco の検出（ディスカバリ）および認識テクノロジーです。ユーザがネットワーク全体を把握できるように、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、地理位置情報、および脆弱性に関する情報を収集します。

防御センター の Web インターフェイスを使用して、収集され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、アクセス制御を実行し、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。

## アクセス制御

*アクセス コントロール*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、および記録できます。*アクセス コントロール ポリシー*は、システムがネットワーク上のトラフィックを処理する方法を決定します。

最も単純なアクセス コントロール ポリシーでは、*デフォルト アクション*を使用してすべてのトラフィックを処理するターゲット デバイスを指定します。追加のインスペクションなしですべてのトラフィックをブロックまたは信頼するか、または侵入および検出データがないかトラフィックを検査するようにこのデフォルト アクションを設定できます。

より複雑なアクセス コントロール ポリシーは、セキュリティ インテリジェンス データに基づいてトラフィックをブラックリスト登録することができます。さらに、*アクセス コントロール ルール*を使用して、ネットワーク トラフィックのロギングおよび処理を細かく制御することができます。これらのルールは単純にすることも複雑にすることもでき、複数の基準を使用してトラフィックを照合および検査します。セキュリティ ゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、およびユーザ別にトラフィックを制御できます。アクセス コントロールの詳細オプションには、復号化、前処理、およびパフォーマンスが含まれます。

各アクセス コントロール ルールには*アクション*も含まれており、一致するトラフィックをモニタ、信頼、ブロック、または許可するかどうかを決定します。トラフィックを許可するときは、システムが侵入ポリシーまたはファイル ポリシーを使用してトラフィックを最初に検査し、アセットに到達したりネットワークを出る前に、エクスプロイト、マルウェア、または禁止されたファイルをブロックするように指定できます。

# SSL インスペクション

SSL インスペクション（検査）はポリシーベースの機能です。暗号化されたトラフィックを復号化せずに処理したり、暗号化されたトラフィックを復号化して詳細なアクセス制御検査を行ったりすることができます。トラフィックの復号化や詳細な分析を行わずに信頼できない暗号化トラフィックの送信元をブロックすることも、暗号化されたトラフィックを復号化する代わりにアクセス制御を使用して検査することもできます。

暗号化トラフィックをさらに調査するために、システムにアップロードされた公開キー証明書とペア化された秘密キーを使用して、ネットワークを通過する暗号化トラフィックを復号化し、非暗号化の場合と同じ方法で復号化トラフィックをアクセス制御によって検査できます。復号されたトラフィックのポスト分析をブロックしない場合、トラフィックは再暗号化されて宛先ホストに渡されます。システムは、暗号化された接続を処理する際にその詳細をログに記録できます。

# 侵入検知と侵入防御

侵入検知および侵入防御は、トラフィックが宛先に許可される前のシステムの最後の防御ラインです。*侵入ポリシー*は、アクセス コントロール ポリシーによって呼び出される侵入検知および侵入防御の設定の定義済みセットです。*侵入ルール*およびその他の設定を使用して、これらのポリシーはセキュリティ違反がないかトラフィックを検査し、インライン展開では、悪意のあるトラフィックをブロックまたは変更できます。

Cisco は、複数の侵入ポリシーを FireSIGHT システムとともに提供します。システム付属のポリシーを使用することで、Cisco 脆弱性調査チーム（VRT）の経験を活用できます。これらのポリシーに対して、VRT は侵入およびプリプロセッサ ルールの状態（有効または無効）を設定し、他の詳細設定の初期設定も行います。ルールを有効にすると、ルールに一致するトラフィックに対して侵入イベントが生成されます（さらに、必要に応じてトラフィックがブロックされます）。

システムが提供するポリシーが組織のセキュリティのニーズに十分に対応していない場合は、カスタム ポリシーを作成することで、環境内のシステムのパフォーマンスを向上させ、ネットワーク上で発生する悪意のあるトラフィックやポリシー違反に焦点を当てたビューを提供できます。設定できるカスタム ポリシーを作成および調整することにより、システムがネットワーク上のトラフィックを処理して侵入の有無について検査する方法を非常にきめ細かく設定できます。

# 高度なマルウェア防御とファイル制御

マルウェアの影響を特定して軽減しやすくするため、FireSIGHT システムのファイル制御、ネットワーク ファイル トラジェクトリ、および高度なマルウェア防御の各コンポーネントによって、ネットワーク トラフィック内のファイル（アーカイブ ファイルの内のマルウェア ファイルとネストされたファイルを含む）の伝送を検出、追跡、キャプチャ、分析、および必要に応じてブロックできます。

### 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 コントロール設定の一部として設定します。アクセス コントロール 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*高度なマルウェア防御*(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。アプライアンスでは、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(一部のモデルで)マルウェア ストレージ パックに保存できます。

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。

マルウェア防御は、総合的なアクセス コントロール設定の一部として設定することができます。アクセス コントロール 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 統合

FireAMP は Cisco 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は Cisco 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。

組織のセキュリティ ポリシーで従来型クラウド サーバ接続の使用が許可されていない場合、Cisco のプライベート オンプレミス クラウド ソリューションである FireAMP プライベート クラウドを入手して設定できます。これは、圧縮された、パブリックの Cisco クラウドのローカル バージョンとして機能する仮想マシンです。

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 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。

FireAMP 展開を設定するには、*FireAMP ポータル*(http://amp.sourcefire.com/)を使用します。このポータルは、マルウェアをすばやく識別し、検疫するのに役立ちます。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 を使用すると、カスタム保護の作成、グループ ポリシーに基づく特定のアプリケーションの実行のブロック、カスタム ホワイトリストの作成も可能です。

### ネットワーク ファイル 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

各ファイルにはトラジェクトリー マップが関連付けられています。このマップには、経時的なファイルの転送を視覚化した情報と、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用意されています。詳細については、次のいずれかのサポート サイトから追加資料をダウンロードできます。

- **シスコ：**（http://www.cisco.com/cisco/web/support/index.html）

### eStreamer

Event Streamer（eStreamer）を使用すると、Cisco 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。作成したクライアント アプリケーションを eStreamer サーバ（防御センター または物理管理対象デバイス）に接続し、eStreamer サービスを起動してデータ交換を開始することができます。

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 アクセス機能により、JDBC SSL 接続をサポートしているサードパーティのクライアントを使用して、防御センター のいくつかのデータベース テーブルに対しクエリを実行できます。

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 Cisco 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 API が含まれており、ユーザはこれを使用して*修復*（修正）を作成することができます。ネットワークの条件が、関連付けられている相関ポリシーまたはコンプライアンス ホワイトリストに違反したときに 防御センター が自動的に修復を起動できます。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。ユーザ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。

# ドキュメント リソース

FireSIGHT システムのドキュメント セットには、オンライン ヘルプと PDF ファイルが含まれています。オンライン ヘルプには、Web インターフェイスから次のようにしてアクセスできます。

- 各ページの状況依存ヘルプ リンクをクリックする
- [ヘルプ（Help）] > [オンライン（Online）] を選択する

オンライン ヘルプには、防御センター またはデバイスの Web インターフェイスを使用して実行できるタスク（システム管理、ポリシー管理、イベント分析を含む）に関する情報が含まれています。

PDF ドキュメントの最新バージョンには、次のいずれかのサポート サイトからアクセスできます。

- **シスコ：**（http://www.cisco.com/cisco/web/support/index.html）

そのようなドキュメントには、次のようなものがあります。

- *FireSIGHT システム ユーザ ガイド*（オンライン ヘルプと同じ内容が含まれていますが、印刷が簡単な形式）
- 『*FireSIGHT システム Installation Guide*』（Cisco のアプライアンスをインストールするための情報、およびハードウェア仕様特有の情報と安全に関する情報が含まれる）
- *FireSIGHT システム Virtual Installation Guide*（仮想デバイスおよび仮想防御センターのインストール、管理、およびトラブルシューティングに関する情報が含まれる）
- *Blue Coat X-Series 向け Cisco NGIPS Installation and Configuration Guide*（Blue Coat X-Series 向け Cisco NGIPS のインストール、管理、およびトラブルシューティングに関する情報が含まれる）
- 各種の API ガイドおよび補足資料

# 表記法

このドキュメントには、それぞれの機能用に FireSIGHT システムのどのライセンスとアプライアンス モデルが必要か、各手順を完了するための権限を持っているのはどのユーザ ロールかについての情報が含まれています。詳細については、次の項を参照してください。

- ライセンスの表記規則（1-21 ページ）
- サポートされるデバイスと 防御センター の表記規則（1-23 ページ）
- アクセスの表記規則（1-23 ページ）

## ライセンスの表記規則

項の先頭に記載されているライセンス文は、その項に記載されている機能を使用するのに必要なライセンスを示しています。具体的なライセンスは次のとおりです。

**FireSIGHT**

FireSIGHT ライセンスは防御センターに含まれており、ホスト、アプリケーション、およびユーザ ディスカバリの実行に必要です。防御センターでの FireSIGHT ライセンスは、防御センターとその管理対象デバイスで監視可能なホストおよびユーザの数、ユーザ制御を実行ために使用可能なユーザの数を決定します。

### Protection

Protection ライセンスでは、管理対象デバイスが侵入の検出および防御、ファイル制御、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できます。このライセンスは、管理対象デバイスの購入時に自動的に付属する保護（TA）サブスクリプションに対応します。

### Control

Control ライセンスでは、管理対象デバイスでユーザおよびアプリケーションの制御を実行することができます。また、デバイスがスイッチングおよびルーティング（DHCP リレーを含む）や NAT を実行したり、デバイスおよびスタックをクラスタ化したりできます。Control ライセンスには Protection ライセンスが必要です。このライセンスは、管理対象デバイスの購入時に自動的に付属します。

### URL Filtering

URL Filtering ライセンスでは、管理対象デバイスが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、ネットワークを通貨できるトラフィックを判別できます。URL Filtering ライセンスには Protection ライセンスが必要です。このライセンスは、保護（TAC または TAMC）と組み合わせたサービス サブスクリプションとして購入できます。また、保護（TA）がすでに有効になっているデバイスの場合は、アドオン サブスクリプション（URL）として購入できます。

### マルウェア

マルウェア ライセンスでは、管理対象デバイスが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、取得、およびブロックし、動的な分析のためにこれらのファイルを送信することができる機能です。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 Protection ライセンスが必要です。マルウェア ライセンスは、保護（TAM または TAMC）と組み合わせたサービス サブスクリプションとして購入できます。また、保護（TA）がすでに有効になっているデバイスの場合は、アドオン サブスクリプション（AMP）として購入できます。

### VPN

VPN ライセンスでは、Cisco の管理対象デバイスの仮想ルータ間で安全な VPN トンネルを構築することができます。VPN ライセンスには、Protection ライセンスと Control ライセンスが必要です。VPN ライセンスを購入するには、販売担当者までお問い合わせください。

ライセンス付きの機能の多くは追加的であるため、このドキュメントでは、各機能で最も必要なライセンスについてのみ記載しています。たとえば、ある機能で FireSIGHT、Protection、および Control のライセンスが必要な場合、Control のみが記載されています。

ライセンス文の「または」という語は、その項に記載されている機能を使用するには特定のライセンスが必要であるが、追加のライセンスで機能を追加できることを示しています。たとえば、あるファイル ポリシー内で、一部のファイル ルール アクションには Protection ライセンスが必要であり、他のファイル ルール アクションには マルウェア ライセンスが必要であるとします。この場合、そのファイル ルールの説明のライセンス文には、「Protection または マルウェア」と示されます。

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ないことに注意してください。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。管理対象デバイスの各モデルでサポートされる機能の概要（1-6 ページ）を参照してください。詳細については、ライセンスについて（65-1 ページ）を参照してください。

# サポートされるデバイスと 防御センター の表記規則

項の先頭に記載されているサポートされるデバイス文は、ある機能が特定のデバイス シリーズ、ファミリ、またはモデルでのみサポートされていることを示しています。たとえば、スタッキングは シリーズ 3 のデバイスでのみサポートされています。項にサポートされるデバイス文が記載されていない場合は、機能がすべてのデバイスでサポートされているか、またはその項が管理対象デバイスに適用されないことを表しています。

このリリースでサポートされているプラットフォームの詳細については、防御センター の概要（1-10 ページ）を参照してください。

# アクセスの表記規則

このドキュメントの各手順の先頭に記載されているアクセス文は、手順の実行に必要な事前定義のユーザ ロールを示しています。複数のロールを区切るスラッシュは、記載されているどのロールでも手順を実行できることを示しています。次の表は、アクセス文で使用される共通の用語について定義しています。

*表 1-7　アクセスの表記規則*

| アクセス用語 | 意味 |
|---|---|
| Access Admin | ユーザは Access Control Admin ロールを持っている必要がある |
| Admin | ユーザは Administrator ロールを持っている必要がある |
| 任意（Any） | ユーザはいずれのロールを持っていてもよい |
| Any/Admin | ユーザはいずれのロールを持っていてもよいが、Administrator ロールのみが無制限のアクセス権を持つ（プライベートとして保存された他のユーザのデータを参照できるなど） |
| Any Security Analyst | ユーザは、Security Analyst または Security Analyst (Read Only) のロールのいずれかを持つことができる |
| データベース | ユーザは External Database ロールを持っている必要がある |
| Discovery Admin | ユーザは Discovery Admin ロールを持っている必要がある |
| Intrusion Admin | ユーザは Intrusion Admin ロールを持っている必要がある |
| Maint | ユーザは Maintenance User ロールを持っている必要がある |
| Network Admin | ユーザは Network Admin ロールを持っている必要がある |
| Security Analyst | ユーザは Security Analyst ロールを持っている必要がある |
| Security Approver | ユーザは Security Approver ロールを持っている必要がある |

カスタム ロールを持っているユーザは、事前定義されたロールとは異なる権限セットを持つことができます。事前定義のロールを使用して、ある手順に対するアクセス要件を示す場合は、類似の権限を持つカスタム ロールもアクセス権限を持っています。カスタム ロールを持っているユーザは、設定ページにアクセスするために使用するメニュー パスが若干異なる場合があります。たとえば、侵入ポリシー権限のみを付与されたカスタム ロールを持つユーザは、アクセス コントロール ポリシーを使用する標準パスではなく侵入ポリシーを経由してネットワーク分析ポリシーにアクセスします。カスタム ユーザ ロールの詳細については、カスタム ユーザ ロールの管理（61-57 ページ）を参照してください。

# IP アドレスの表記規則

IPv4 Classless Inter-Domain Routing（CIDR）の表記、および IPv6 の類似のプレフィックス長の表記を使用して、FireSIGHT システムの多数の場所でアドレス ブロックを定義することができます。

CIDR 表記は、ネットワーク IP アドレスとビット マスクを組み合わせて使用し、指定されたアドレス ブロック内の IP アドレスを定義します。たとえば次の表に、プライベート IPv4 アドレス空間を CIDR 表記で示します。

*表 1-8　CIDR 表記の構文例*

| CIDR ブロック | CIDR ブロックの IP アドレス | サブネット マスク | IP アドレスの数 |
|---|---|---|---|
| 10.0.0.0/8 | 10.0.0.0 ～ 10.255.255.255 | 255.0.0.0 | 16,777,216 |
| 172.16.0.0/12 | 172.16.0.0 ～ 172.31.255.255 | 255.240.0.0 | 1,048,576 |
| 192.168.0.0/16 | 192.168.0.0 ～ 192.168.255.255 | 255.255.0.0 | 65,536 |

同様に、IPv6 はネットワーク IP アドレスとプレフィックス長を組み合わせて使用し、指定されたブロック内の IP アドレスを定義します。たとえば 2001:db8::/32 は、プレフィックス長が 32 ビットの 2001:db8:: ネットワーク内の IPv6 アドレスを表します。つまり、2001:db8:: ～ 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff を表します。

CIDR またはプレフィックス長の表記を使用して IP アドレスのブロックを指定する場合、FireSIGHT システム は、マスクまたはプレフィックス長で指定されたネットワーク IP アドレスの部分**のみ**を使用します。たとえば、10.1.2.3/8 と入力した場合、FireSIGHT システム では 10.0.0.0/8 が使用されます。

つまり Cisco は、CIDR またはプレフィックス長の表記を使用する場合に、ビット境界上でネットワーク IP アドレスを使用する標準の方法を推奨していますが、FireSIGHT システム ではこれは必要ありません。