FireSIGHT システム インストレーション ガイド

バージョン 5.3.1
14/07/17

Cisco Systems, Inc.
www.cisco.com
シスコは世界各国 200 箇所にオフィスを開設しています。
住所、電話番号、FAX 番号は
以下のシスコ Web サイトをご覧ください。
www.cisco.com/go/offices。

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

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.1-5）
- 「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.1-8）
- 「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.1-8）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.1-17）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.1-20）

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.1-20）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。

展開について

固有なネットワーク アーキテクチャごとのニーズに対応するように、FireSIGHT システムを展開できます。防御センターは、FireSIGHT システムのための一元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。デバイスは、分析のためにトラフィック接続を収集するように、ネットワーク セグメントにインストールされます。

パッシブ展開に含まれるデバイスにより、スイッチの SPAN、仮想スイッチ、またはミラー ポートを使用してネットワークを通過するトラフィックを監視して、ネットワークを横断するトラフィックの特性に関するデータを収集できます。インライン展開に含まれるデバイスにより、ネットワーク上のホストの可用性、整合性、機密性に影響を及ぼす可能性のある攻撃を見つけるために、ネットワークを監視できます。デバイスは、インライン、スイッチド、ルーテッド、またはハイブリッド (レイヤ 2/レイヤ 3) 環境に展開できます。

（注） ASA FirePOWER のデバイスの展開シナリオについて詳しくは、ASA のマニュアルを参照してください。

展開オプションについて詳しくは、以下の項を参照してください。

- 「展開のオプションについて」（P.2-2）では、展開を設計する際に考慮する必要のある要素について説明します。
- 「インターフェイスについて」（P.2-2）では、さまざまなインターフェイスの相違点と、それらが展開内でどのように機能するかについて説明します。
- 「ネットワークへのデバイスの接続」（P.2-6）では、ハブ、スパン、およびネットワーク タップを展開内で使用する方法について説明します。
- 「展開のオプション」（P.2-10）では、基本的な展開について説明し、その中にある主な機能場所を示します。
- 「アクセス制御による展開」（P.2-15）では、インライン展開でアクセス コントロールを使用する利点について説明します。
- 「複数ポートの管理対象デバイスの使用」（P.2-20）では、複数のネットワーク用に、またはネットワーク展開で仮想ルータや仮想スイッチとして利用するために、管理対象デバイスを使用する方法について説明します。
- 「複雑なネットワークの展開」（P.2-22）では、VPN を使用したり複数のエントリ ポイントが存在したりするような、高度な展開シナリオについて説明します。

展開について詳しくは、シスコ の営業部門から入手可能な『*Best Practices Guide*』を参照してください。

展開のオプションについて

の展開に関する決定は、さまざまな要素に基づいて行います。以下の質問に答えることにより、ネットワークの脆弱なエリアを理解し、侵入検知と侵入防御のニーズを明確にすることができます。

- パッシブまたはインラインのどちらのインターフェイスで管理対象デバイスを展開しますか。デバイスはパッシブと他のインラインが混在しているインターフェイスをサポートしますか。詳細については、「インターフェイスについて」（P.2-2）を参照してください。
- どのようにして管理対象デバイスをネットワークに接続しますか。ハブを使用しますか。タップを使用しますか。スイッチのスパニング ポートを使用しますか。仮想スイッチを使用しますか。詳細については、「ネットワークへのデバイスの接続」（P.2-6）を参照してください。
- ネットワーク上のすべての攻撃を検出しますか、またはファイアウォールを通過する攻撃だけを検出しますか。特殊なセキュリティ ポリシーを必要とする、財務、会計、人事記録、生産コード、その他の機密性の高い保護された情報など、特定の資産がネットワーク上に存在しますかか。詳細については、「展開のオプション」（P.2-10）を参照してください。
- 管理対象デバイスの複数のポートを、ネットワーク タップからのさまざまな接続を再結合するために使用しますか、またはさまざまなネットワークからのトラフィックをキャプチャして評価するために使用しますか。複数のポートを、仮想ルータまたは仮想スイッチのどちらとして機能するように使用しますか。詳細については、「複数ポートの管理対象デバイスの使用」（P.2-20）を参照してください。
- リモート ワーカーには、VPN またはモデムアクセスのどちらを提供しますか。侵入防御の展開を必要とするリモート オフィスがありますか。請負業者その他の臨時スタッフを雇用していますか。それらのスタッフは、特定のネットワーク セグメントにアクセスが制限されていますか。ネットワークを顧客、サプライヤ、ビジネス パートナーなど他の組織のネットワークと統合しますか。詳細については、「複雑なネットワークの展開」（P.2-22）を参照してください。

インターフェイスについて

以下の項では、さまざまなインターフェイスが FireSIGHT システムの機能に与える影響について説明します。パッシブおよびインライン インターフェイスに加えて、ルーテッド、スイッチド、ハイブリッドの各インターフェイスもあります。詳細については、次の項を参照してください。

パッシブ インターフェイス

ライセンス：すべて

サポートされるデバイス：すべて

スイッチの SPAN、仮想スイッチ、またはミラー ポートを使用して、ネットワークで送られるトラフィックを監視するパッシブ展開を設定し、スイッチ上の他のポートからトラフィックをコピーできるようにすることができます。パッシブ インターフェイスを使用すると、ネットワーク トラフィックのフローに含まれていなくても、ネットワーク内のトラフィックを検査できます。パッシブ展開で設定されている場合、システムはトラフィックのブロッキングやシェーピングなど、特定のアクションを実行できません。パッシブ 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、受信したトラフィックを再送信しません。

管理対象デバイスの一つ以上の物理ポートをパッシブ インターフェイスとして設定できます。詳細については、「ネットワークへのデバイスの接続」（P.2-6）を参照してください。パッシブ モードの ASA FirePOWER デバイスを設定する方法について詳しくは、ASA のマニュアルを参照してください。

インライン インターフェイス

ライセンス：すべて

サポートされるデバイス：すべて

2 つのポートを一緒にバインドすることで、インライン構成をネットワーク セグメントにトランスペアレントに設定します。インライン インターフェイスを使用すると、隣接するネットワーク デバイスを設定しなくても、デバイスを任意のネットワーク設定でインストールできます。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に受信します。その後、明示的にドロップされたものを除いて、それらのインターフェイスで受信されたすべてのトラフィックが再送信されます。

管理対象デバイスの一つ以上の物理ポートをインライン インターフェイスとして設定できます。インライン展開でトラフィックを処理するには、その前に、インライン セットにインライン インターフェイスのペアを割り当てる必要があります。

（注） インターフェイスをインライン インターフェイスとして設定する場合、NetMod での隣接ポートも自動的にインライン インターフェイスとなり、ペアが完成します。

設定可能なバイパスのインライン セットによって、ハードウェアに重大な障害（デバイスへの電力供給の停止など）が生じた場合に、トラフィックを処理する方法を選択できます。あるネットワーク セグメントでは接続性が重要であると判断し、別のネットワーク セグメントでは未検査のトラフィックを許可できないと判断する場合があります。設定可能なバイパスのインライン セットを使用すると、ネットワーク トラフィックのトラフィック フローを次のいずれかの方法で管理できます。

- *バイパス*：バイパスに設定されたインターフェイス ペアでは、デバイスに障害が生じた場合に、すべてのトラフィックのフローが続行します。トラフィックは、デバイスをバイパスし、そのデバイスによるインスペクションや他の処理をバイパスします。バイパスでは、インスペクションが行われないトラフィックがネットワーク セグメント間を通過する可能性がありますが、ネットワークの接続性は保持されます。
- *非バイパス*：非バイパスの設定されたインターフェイス ペアでは、デバイスに障害が生じた場合に、すべてのトラフィックが停止します。障害が発生しているデバイスに到達したトラフィックは、そのデバイスに入れられません。非バイパスでは、インスペクションが

行われずにトラフィックが通過することはありませんが、デバイスに障害が生じた場合に、ネットワーク セグメントの接続性が失われます。展開の状態として、トラフィックを失うことよりもネットワーク セキュリティの方が重要な場合は、非バイパス インターフェイスを使用します。

デバイスに障害が生じた場合にトラフィック のフローが続行するようにするには、インライン セットをバイパスとして設定します。デバイスに障害が生じた場合にトラフィック を停止させるには、インライン セットを非バイパスとして設定します。再イメージングを行うと、バイパス モードのアプライアンスが非バイパス設定にリセットされて、バイパス モードに再設定されるまではネットワークのトラフィックが中断されることに注意してください。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。

すべてのアプライアンスに、設定可能なバイパス インターフェイスを含めることができます。8000 シリーズ のアプライアンスには、バイパスに設定できないインターフェイスを持つ NetMods を含めることもできます。NetMods の詳細については、「8000 シリーズ モジュール」（P.6-46）を参照してください。

[Advanced] オプションはアプライアンスによって異なり、タップ モード、伝播リンク ステート、トランスペアレント インライン モード、厳格な TCP モードが含まれることがあります。インライン インターフェイス セットを設定する方法について詳しくは、『*FireSIGHT System User Guide*』の「インライン セットの設定」を参照してください。インライン インターフェイスの使用方法について詳しくは、「ネットワークへのデバイスの接続」（P.2-6）を参照してください。

FireSIGHT システムを使用して ASA FirePOWER デバイスのバイパス インターフェイスを設定することはできません。インライン モードの ASA FirePOWER デバイスを設定する方法について詳しくは、ASA のドキュメントを参照してください。

スイッチド インターフェイス

ライセンス：制御

サポートされるデバイス：シリーズ 3

レイヤ 2 展開の管理対象デバイスのスイッチド インターフェイスを設定して、複数のネットワーク間のパケット スイッチングを提供できます。また、管理対象デバイスに仮想スイッチを設定して、ネットワークを論理セグメントに分割する、スタンドアロンのブロードキャスト ドメインとして機能させることができます。仮想スイッチは、ホストからの Media Access Control（MAC）のアドレスを使用して、パケットの送信先を判別します。

スイッチド インターフェイスには、物理設定または論理設定を使用できます。

- *物理スイッチド インターフェイス*は、スイッチングが設定された物理インターフェイスです。タグなし VLAN トラフィックを処理するために物理スイッチド インターフェイスを使用します。
- *論理スイッチド インターフェイス*は、物理インターフェイスと VLAN タグを関連付けます。VLAN タグが指定されたトラフィックを処理するために論理インターフェイスを使用します。

仮想スイッチは、ネットワークを論理セグメントに分割する、スタンドアロンのブロードキャスト ドメインとして機能させることができます 仮想スイッチは、ホストからの Media Access Control（MAC）のアドレスを使用して、パケットの送信先を判別します。仮想スイッチを設定すると、そのスイッチは最初、スイッチ内にある使用可能なすべてのポートを介してパケットをブロードキャストします。時間の経過と共に、スイッチはタグの付けられたリターン トラフィックを使用して、各ポートに接続されたネットワークにどのホストが存在するかを学習します。

デバイスを仮想スイッチとして設定し、残りのインターフェイスを使用して監視対象のネットワーク セグメントに接続できます。デバイスで仮想スイッチを使用するには、物理スイッチドインターフェイスを作成し、『*FireSIGHT System User Guide*』の「仮想スイッチのセットアップ」の手順に従ってください。

ルーテッド インターフェイス

ライセンス：制御

サポートされるデバイス：シリーズ 3

ルーテッド インターフェイスをレイヤ 3 展開の管理対象デバイスに設定して、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できます。トラフィックをルーティングするには、各インターフェイスに IP アドレスを割り当て、インターフェイスを仮想ルータに割り当てる必要があります。

ゲートウェイのバーチャル プライベート ネットワーク（ゲートウェイ VPN）または Network Address Translation（NAT）と共に使用するための、ルーテッド インターフェイスを設定できます。詳細については、「ゲートウェイ VPN の展開」（P.2-14）および「ポリシーベース NAT による展開」（P.2-15）を参照してください。

また、宛先アドレスに基づいてパケット転送の決定を行ってパケットをルーティングするように、システムを設定できます。ルーテッド インターフェイスとして設定されるインターフェイスは、レイヤ 3 トラフィックを受信および転送します。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、適用されるセキュリティ ポリシーがアクセス コントロール規則によって指定されます。

ルーテッド インターフェイスには、物理設定または論理設定を使用できます。

- *物理ルーテッド インターフェイス*は、ルーティングが設定された物理インターフェイスです。タグなし VLAN トラフィックを処理するために物理ルーテッド インターフェイスを使用します。
- *論理スイッチド インターフェイス*は、物理インターフェイスと VLAN タグを関連付けます。VLAN タグが指定されたトラフィックを処理するために論理インターフェイスを使用します。

レイヤ 3 展開でルーテッド インターフェイスを使用するには、仮想ルータを設定し、それらにルーテッド インターフェイスを割り当てる必要があります。仮想ルータは、レイヤ 3 トラフィックをルーティングするルーテッド インターフェイスのグループです。

デバイスを仮想ルータとして設定し、残りのインターフェイスを使用して監視対象のネットワーク セグメントに接続できます。また、TCP のセキュリティを最大にするために、厳格な TCP を適用することもできます。デバイスで仮想ルータを使用するには、デバイス上に物理ルーテッド インターフェイスを作成し、『*FireSIGHT System User Guide*』の「仮想ルータのセットアップ」の手順に従ってください。

ハイブリッド インターフェイス

ライセンス：制御

サポートされるデバイス：シリーズ 3

FireSIGHT システムが仮想ルータと仮想スイッチ間のトラフィックをブリッジングできるようにする論理ハイブリッド インターフェイスを、管理対象デバイスに設定できます。仮想スイッチのインターフェイスで受信した IP トラフィックが、関連付けられているハイブリッド論理インターフェイスの MAC アドレスにアドレス指定されている場合、システムはそれをレイヤ 3 トラフィックとして処理して、送信先 IP アドレスに応じてトラフィックをルーティングするかまたはトラフィックに応答します。他のトラフィックを受信した場合、システムはそれをレイヤ 2 トラフィックとして扱い、適切にスイッチングします。

ハイブリッド インターフェイスを作成するには、まず仮想スイッチと仮想ルータを設定してから、仮想スイッチと仮想ルータをハイブリッド インターフェイスに追加します。仮想スイッチと仮想ルータの両方に関連付けられていないハイブリッド インターフェイスは、ルーティング用に使用することができず、トラフィックの生成やトラフィックへの応答は行いません。

Network Address Translation (NAT) とのハイブリッド インターフェイスを設定して、ネットワーク間でトラフィックを渡すことができます。詳細については、「ポリシーベース NAT による展開」（P.2-15）を参照してください。

デバイスでハイブリッド インターフェイスを使用する場合、デバイスにハイブリッド インターフェイスを定義してから、『*FireSIGHT System User Guide*』の「ハイブリッド インターフェイスのセットアップ」に示された手順に従います。

ネットワークへのデバイスの接続

管理対象デバイスを複数の方法でネットワークに接続できます。パッシブまたはインライン インターフェイスを使用してハブまたはネットワーク タップを設定するか、またはパッシブ インターフェイスを使用して Span ポートを設定します。以下の項では、サポートされている接続方法およびケーブル配線に関する考慮事項について説明します。

ハブの使用

イーサネット ハブは、管理対象デバイスがネットワーク セグメント上のすべてのトラフィックを確実に認識できるようにするシンプルな方法です。このタイプのほとんどのハブは、セグメント上のいずれかのホストの IP トラフィックを受け取って、ハブに接続されたすべてのデバイスにブロードキャストします。ハブに設定されたインターフェイスを接続して、セグメント上のすべての入力および出力トラフィックを監視します。ハブを使用しても、パケット衝突が生じる可能性があるため、検出エンジンが大量のネットワーク上のパケットをすべて認識できるとは限りません。トラフィックの少ないシンプルなネットワークでは、このことはほとんど問題になりません。トラフィックの多いネットワークでは、別のオプションによって結果が改

善されることがあります。ハブに障害が発生したり、電源が失われた場合は、ネットワーク接続が切断されることに注意してください。シンプルなネットワークでは、そのネットワークが停止します。

一部のデバイスは、ハブとして販売されていても実際にはスイッチとして機能するものであり、各パケットをすべてのポートに伝送しません。ハブに管理対象デバイスを接続しても、すべてのトラフィックが認識されないときには、別のハブを購入するか、または SPAN ポートを持つスイッチを使用しなければならない場合があります。

SPAN ポートの使用

多くのネットワーク スイッチには、1 つ以上のポートからのトラフィックをミラーイングする SPAN ポートが含まれています。SPAN ポートに設定されたインターフェイスを接続することにより、すべてのポートから混合トラフィック（通常は入力および出力）を監視できます。この機能を含むスイッチがネットワーク上の適切な場所にすでに存在する場合は、管理対象デバイスのコスト以外には追加の機器コストをほとんどかけずに、複数セグメントでの検出を展開できます。トラフィックの多いネットワークの場合、このソリューションには制限があります。SPAN ポートが 200Mbps を処理することができ、3 つのミラー対象ポートのそれぞれが 100Mbps まで処理できる場合、SPAN ポートはオーバーサブスクライブされてパケットをドロップするようになり、管理対象デバイスの効率が減少する可能性があります。

ネットワーク タップの使用

ネットワーク タップにより、ネットワーク フローを中断したりネットワーク トポロジを変更しなくても、トラフィックをパッシブに監視できます。さまざまな帯域幅に対応したタップをすぐに使用できるので、ネットワーク セグメントの着信パケットと発信パケットの両方を分析できます。ほとんどのタップでは 1 つのネットワーク セグメントだけを監視できるため、スイッチ上に 8 つあるポートの内の 2 つでトラフィックを監視するには得策ではありません。代わりに、ルータとスイッチの間にタップを設置すれば、スイッチへの IP ストリーム全体にアクセスすることができます。

設計上、ネットワーク タップは入力トラフィックと出力トラフィックを、2 つの異なるケーブルでの 2 つの異なるストリームに分割します。管理対象デバイスは、通信の 2 つの部分を再結合する複数ポートのオプションを提供し、トラフィック ストリーム全体がデコーダ、プリプロセッサ、および検出エンジンによって評価されるようにします。

銅線インターフェイスのインライン展開のケーブル配線

ネットワークにデバイスをインラインで展開し、デバイスのバイパス機能を使用してデバイスの障害時にネットワーク接続が維持されるようにする場合は、接続箇所をケーブル配線する方法に特別な注意を払ってください。

光ファイバ バイパス ケーブル インターフェイスによってデバイスを展開する場合は、接続箇所が確実に結合され、ケーブルがよじれていないことを確認する以外に、特別なケーブル配線の問題はありません。ただし、光ファイバ ネットワーク インターフェースではなく銅線を使用してデバイスを展開している場合は、デバイス モデルが異なれば使用するネットワーク カードも異なるので、使用するデバイス モデルに注意する必要があります。一部の 8000 シリーズ NetMods では、バイパス設定が許可されないことに注意してください。

デバイスのネットワーク インターフェイス カード（NIC）は、自動メディア依存インターフェイス クロスオーバー（Auto-MDI-X）と呼ばれる機能をサポートします。この機能により、ネットワーク インターフェイスは、ストレートまたはクロスのどちらのイーサネット ケーブ

ルを使用して別のネットワーク デバイスに接続するかを自動的に設定できます。次の表は、さまざまなデバイスと、それらがストレートまたはクロスのどちらの接続によってバイパスするかをリストしています。

表 2-1　　デバイスとバイパス特性

デバイス	フェール オープンの形式
3D500、3D1000、3D2000	ストレート
7000 シリーズ	クロス
8000 シリーズ	クロス

ストレート接続でバイパスする管理対象デバイスでは、ネットワーク上で稼働しているデバイスに対して通常行うのと同じ方法で、デバイスを配線します。ほとんどの場合、1 本のストレート ケーブルと 1 本のクロス ケーブルを使用して、デバイスを 2 つのエンドポイントに接続する必要があります。

図 2-1　　ストレート線のバイパス接続のケーブル配線

クロス接続でバイパスする管理対象デバイスでは、配置されたデバイスがない場合に通常行うのと同じ方法で、デバイスを配線します。デバイスへの電源供給が失われても、リンクは機能する必要があります。ほとんどの場合、2 本のストレート ケーブルを使用して、デバイスを 2 つのエンドポイントに接続する必要があります。

図 2-2　　クロス線のバイパス接続のケーブル配線

次の表は、ハードウェア バイパス設定で、クロス ケーブルまたはストレート ケーブルを使用するケースを示しています。レイヤ 2 ポートは展開のストレート（MDI）エンドポイントとして機能し、レイヤ 3 ポートは展開のクロス（MDIX）エンドポイントとして機能することに注意してください。バイパスが正常に機能するためには、クロスの合計（ケーブルとアプライアンス）が奇数であることが必要です。

表 2-2　　ハードウェア バイパスの有効な設定

エンドポイント 1	ケーブル	管理対象デバイス	ケーブル	エンドポイント 2
MDIX	ストレート	ストレート	ストレート	MDI
MDI	クロス	ストレート	ストレート	MDI
MDI	ストレート	ストレート	クロス	MDI
MDI	ストレート	ストレート	ストレート	MDIX
MDIX	ストレート	クロス	ストレート	MDIX

表 2-2　　ハードウェア バイパスの有効な設定 （続き）

エンドポイント 1	ケーブル	管理対象デバイス	ケーブル	エンドポイント 2
MDI	ストレート	クロス	ストレート	MDI
MDI	クロス	クロス	クロス	MDI
MDIX	クロス	クロス	ストレート	MDI

すべてのネットワーク環境は固有のものであり、さまざまな組み合わせで Auto-MDI-X をサポートするエンドポイントを持っている可能性があることに注意してください。正しいケーブル配線によってデバイスを設置していることを確認する最も簡単な方法は、デバイスの電源を落とした状態で、まず 1 本のクロス ケーブルと 1 本のストレート ケーブルを使用してデバイスを 2 つのエンドポイントに接続することです。2 つのエンドポイントが通信可能であることを確認します。それらが通信できない場合は、いずれかのケーブルのタイプが正しくありません。いずれかのケーブル（1 本のみ）を他のタイプ（ストレートまたはクロス）に切り替えてください。

インライン デバイスの電源を落とした状態で 2 つのエンドポイントが正常に通信可能になった後に、デバイスの電源を入れます。Auto-MDI-X 機能は、2 つのエンドポイントが通信を続行するようにします。インライン デバイスを交換する必要がある場合は、元のデバイスとそれに代わるデバイスとでバイパス特性が異なる場合に備えて、新しいデバイスの電源を落とし、その新しいデバイスとエンドポイントとが通信できるようにする手順を繰り返す必要があります。

Auto-MDI-X 設定は、ネットワーク インターフェイスの自動ネゴシエーションを許可した場合にのみ正しく機能します。ネットワーク環境で [Network Interface] ページの [Auto Negotiate] オプションを無効にすることが必要な場合は、インライン ネットワーク インターフェイス用に正しい MDI/MDIX オプションを指定します。詳しくは、『*FireSIGHT System User Guide*』の「インライン インターフェイスの設定」を参照してください。

特別な場合

8000 シリーズ デバイスの接続

8000 シリーズの管理対象デバイスを防御センターに登録するときは、接続の両側で自動ネゴシエーションを使用するか、またはその両側を同じ固定速度に設定して、ネットワーク リンクが安定したものとなるようにする必要があります。8000 シリーズの管理対象デバイスは、半二重ネットワーク リンクをサポートしません。また、接続の反対側での速度の違いやデュプレックス設定をサポートしません。

リモート コンソールの変更

70xx ファミリ のデバイスで、リモート コンソールを物理シリアル ポートから Lights-Out Management に、または Lights-Out Management から物理シリアル ポートに変更する際に、予想される LILO のブートのプロンプトが表示されるようにアプライアンスを 2 回リブートしなければならないことがあります。

展開のオプション

ネットワーク セグメントに管理対象デバイスを展開すると、侵入検知システムを使用してトラフィックを監視したり、侵入防止システムを使用してネットワークを脅威から保護することができます。

また、仮想スイッチ、仮想ルータ、またはゲートウェイ VPN として動作するように管理対象デバイスを配置することもできます。さらに、ポリシーを使用して、ネットワークのトラフィックをルーティングしたり、トラフィックへのアクセスを制御することができます。詳細については、次の項を参照してください。

- 「仮想スイッチを使用した展開」（P.2-10）
- 「仮想ルータの展開」（P.2-11）
- 「ハイブリッド インターフェイスによる展開」（P.2-13）
- 「ゲートウェイ VPN の展開」（P.2-14）
- 「ポリシーベース NAT による展開」（P.2-15）
- 「アクセス制御による展開」（P.2-15）

仮想スイッチを使用した展開

ライセンス：制御

サポートされるデバイス：シリーズ 3

インライン インターフェイスをスイッチド インターフェイスとして設定することにより、管理対象デバイスに*仮想スイッチ*を作成できます。仮想スイッチは、展開にレイヤ 2 パケット スイッチングを提供します。[Advanced] オプションには、スタティック MAC アドレスの設定、スパニング ツリー プロトコルの有効化、厳密な TCP の適用、およびドメイン レベルでのブリッジ プロトコル データ ユニット（BPDU）のドロップが含まれます。スイッチド インターフェイスについて詳しくは、「スイッチド インターフェイス」（P.2-4）を参照してください。

仮想スイッチには、トラフィックを処理するために複数のスイッチド インターフェイスを含める必要があります。それぞれの仮想スイッチで、システムは、スイッチド インターフェイスとして設定されたポートのセットに対してのみトラフィックをスイッチングします。たとえば、4 つのスイッチド インターフェイスのある仮想スイッチを設定した場合、システムが 1 つのポートを介してトラフィック パケットを受信すると、それらのパケットはスイッチ上の残りの 3 つのポートだけにブロードキャストされます。

トラフィックを許可するように仮想スイッチを設定するには、物理ポートに複数のスイッチド インターフェイスを設定し、仮想スイッチを追加して設定してから、仮想スイッチをスイッチド インターフェイスに割り当てます。システムは、外部物理インターフェイスで受信される、待機するスイッチド インターフェイスのないトラフィックをドロップします。システムが VLAN タグのないパケットを受信し、そのポートの物理スイッチド インターフェイスが設定されていない場合、そのパケットはドロップされます。システムが VLAN タグのあるパケットを受信し、論理スイッチド インターフェイスが設定されていない場合も、そのパケットはドロップされます。

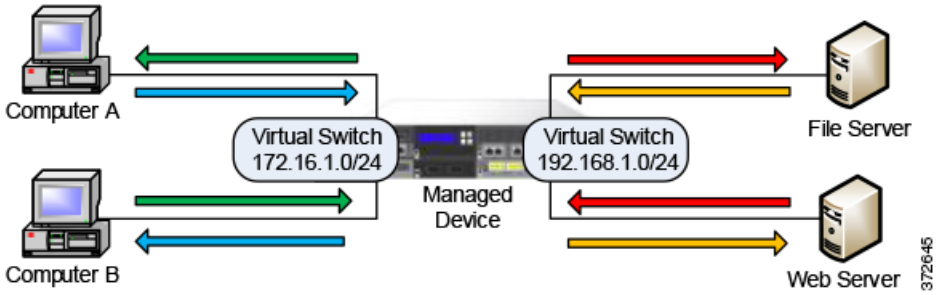
必要に応じて追加の論理スイッチド インターフェイスを物理ポートに定義できますが、トラフィックを処理するために、論理スイッチド インターフェイスを仮想スイッチに割り当てる必要があります。

仮想スイッチには、拡張性の利点があります。物理スイッチを使用する場合、スイッチ上の使用可能なポートの数によって制限されます。物理スイッチを仮想スイッチに置き換える場合は、使用する帯域幅と、展開に導入する複雑さのレベルによってのみ制限されます。

ワークグループ接続やネットワーク セグメントなど、レイヤ 2 スイッチを使う場合、仮想スイッチを使用します。作業者が大半の時間をローカル セグメントで費やす場合、レイヤ 2 スイッチは特に効果的です。大規模な展開（たとえば、ブロードキャスト トラフィック、Voice-over-IP、複数ネットワークを含む展開など）では、仮想スイッチを、展開の小規模なネットワーク セグメントで使用できます。

複数の仮想スイッチを同じ管理対象デバイスに展開する場合、各ネットワークの必要に応じて、さまざまなレベルのセキュリティを維持できます。

図 2-3　　管理対象デバイスの仮想スイッチ



この例では、管理対象デバイスが、2 つの別個のネットワーク（172.16.1.0/20 と 192.168.1.0/24）からのトラフィックを監視します。どちらのネットワークも同じ管理対象デバイスによって監視されますが、仮想スイッチは、同じネットワーク上にあるコンピュータやサーバにのみトラフィックを渡します。トラフィックは、172.16.1.0/24 仮想スイッチを介してコンピュータ A からコンピュータ B に（青色の線で示されているように）渡し、同じ仮想スイッチを介してとコンピュータ B からコンピュータから A に（緑色の線で示されているように）渡すことができます。同様に、トラフィックは、192.168.1.0/24 仮想スイッチを介してファイルと Web サーバ間で（赤色の線とオレンジ色の線で示されているように）受け渡すことができます。ただし、コンピュータがサーバと同じ仮想スイッチ上にないため、そのコンピュータと Web またはファイル サーバ間でトラフィックを受け渡すことができません。

スイッチド インターフェイスおよび仮想スイッチの設定について詳しくは、『*FireSIGHT System User Guide*』の「仮想スイッチのセットアップ」を参照してください。

仮想ルータの展開

ライセンス：制御

サポートされるデバイス：シリーズ 3

管理対象デバイスに*仮想ルータ*を作成して、複数のネットワーク間のトラフィックをルーティングしたり、プライベート ネットワークをパブリック ネットワーク（インターネットなど）に接続することができます。仮想ルータは、2 つのルーテッド インターフェイスを接続して、展開のために、宛先アドレスに応じたレイヤ 3 パケット転送の決定を提供します。必要に応じて、仮想ルータでの厳密な TCP 適用を有効にすることができます。ルーテッド インターフェイスの詳細については、「ルーテッド インターフェイス」（P.2-5）を参照してください。ゲートウェイ VPN と共に仮想ルータを使用する必要があります。詳細については、「ゲートウェイ VPN の展開」（P.2-14）を参照してください。

仮想ルータには、同じブロードキャスト ドメイン内にある 1 つ以上の個別のデバイスから、物理的または論理的にルーティングされた設定を含めることができます。VLAN タグを持つ物理インターフェイスで受信されたトラフィックを処理するためには、各論理インターフェイスをその特定のタグに関連付ける必要があります。トラフィックをルーティングするには、論理ルーテッド インターフェイスを仮想ルータに割り当てる必要があります。

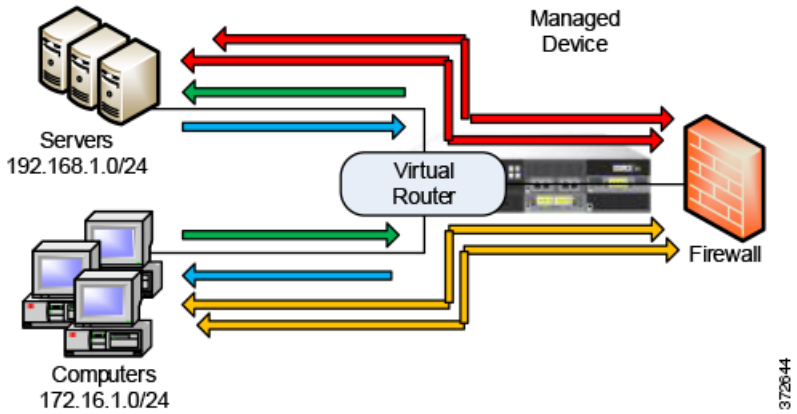
仮想ルータを設定するには、物理設定または論理設定によってルーテッド インターフェイスを設定します。タグのない VLAN のトラフィックを処理するために、物理ルーテッド インターフェイスを設定できます。また、指定の VLAN タグのあるトラフィックを処理するために、論理ルーテッド インターフェイスを作成することもできます。システムは、外部物理インターフェイスで受信される、待機するルーテッド インターフェイスのないトラフィックをドロップします。システムが VLAN タグのないパケットを受信し、そのポートの物理ルーテッド インターフェイスが設定されていない場合、そのパケットはドロップされます。システムが VLAN タグのあるパケットを受信し、論理ルーテッド インターフェイスが設定されていない場合も、そのパケットはドロップされます。

仮想ルータには、拡張性の利点があります。物理ルータによって接続可能なネットワークの数が制限されるときには、複数の仮想ルータを同じ管理対象デバイスに設定できます。同じデバイスにルータを配置すると、展開の物理的な複雑さが軽減され、1 つのデバイスから複数のルータを監視および管理できます。

レイヤ 3 物理ルータを使用して、展開内の複数のネットワーク間でトラフィックを転送したり、プライベート ネットワークをパブリック ネットワークに接続する場合、仮想ルータを使用します。仮想ルータは、さまざまなセキュリティ要件を持つ多数のネットワークまたはネットワーク セグメントを含む大規模な展開で、特に効果的です。

管理対象デバイスに仮想ルータを展開する場合、1 つのアプライアンスを使用して、複数のネットワークを相互に接続したり、インターネットに接続したりできます。

図 2-4　　管理対象デバイスの仮想ルータ



この例では、トラフィックがネットワーク 172.16.1.0/20 上のコンピュータとネットワーク 192.168.1.0/24 上のサーバ間（青と緑の線で示されている）を移動できるように、管理対象デバイスに仮想ルータが含まれます。仮想ルータの 3 番目のインターフェイスにより、各ネットワークからのトラフィックを、ファイアウォールとの間で受け渡す（赤色とオレンジ色の線で示されている）ことができます。

詳しくは、『*FireSIGHT System User Guide*』の「仮想ルータのセットアップ」を参照してください。

ハイブリッド インターフェイスによる展開

ライセンス：制御

サポートされるデバイス：シリーズ 3

仮想スイッチと仮想ルータを使用して、レイヤ 2 とレイヤ 3 ネットワーク間でトラフィックをルーティングするために、管理対象デバイスに*ハイブリッド インターフェイス*を作成できます。これにより、スイッチ上でローカル トラフィックをルーティングしたり、外部ネットワークとの間でトラフィックをルーティングできる、1 つのインターフェイスが提供されます。最適な結果を得るために、このインターフェイスでポリシーベースの NAT を設定して、ハイブリッド インターフェイスでのネットワーク アドレス変換を提供します。「ポリシーベース NAT による展開」（P.2-15）を参照してください。

ハイブリッド インターフェイスには、1 つ以上のスイッチド インターフェイスと 1 つ以上のルーテッド インターフェイスを含める必要があります。共通展開は 2 つのスイッチド インターフェイスで構成されています。それらは、プライベートまたはパブリックで、トラフィックをローカル ネットワークに渡すための仮想スイッチ、およびネットワークにトラフィックをルーティングするための仮想ルータとして設定されています。

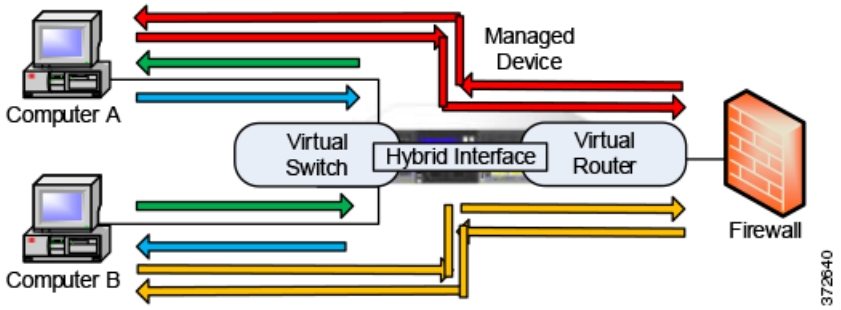
ハイブリッド インターフェイスを作成するには、まず仮想スイッチと仮想ルータを設定してから、仮想スイッチと仮想ルータをハイブリッド インターフェイスに追加します。仮想スイッチと仮想ルータの両方に関連付けられていないハイブリッド インターフェイスは、ルーティング用に使用することができず、トラフィックの生成やトラフィックへの応答は行いません。

ハイブリッド インターフェイスは、コンパクトであり、拡張性に優れているという利点があります。単一のハイブリッド インターフェイスを使用すると、レイヤ 2 とレイヤ 3 の両方のトラフィック ルーティング機能が結合して 1 つのインターフェイスとなって、展開内の物理アプライアンスの数が減り、トラフィックのための単一の管理インタフェースが提供されます。

レイヤ 2 とレイヤ 3 の両方のルーティング機能が必要な場合、ハイブリッド インターフェイスを使用します。この展開は、スペースやリソースが限られている展開での小さなセグメントに最適です。

ハイブリッド インターフェイスを展開すると、トラフィックをローカル ネットワークから外部またはパブリック ネットワーク（インターネットなど）に渡すことができるとともに、ハイブリッド インターフェイスでの仮想スイッチと仮想ルータに関する個別のセキュリティ上の考慮事項に対応することができます。

図 2-5　　管理対象デバイスのハイブリッド インターフェイス



この例では、コンピュータ A と コンピュータ B は同じネットワーク上に存在し、管理対象デバイスに設定されたレイヤ 2 の仮想スイッチを使用して通信します（青と緑の線で示されています）。管理対象デバイス上で設定されている仮想ルータは、ファイアウォールへのレイヤ 3 アクセスを提供します。ハイブリッド インターフェイスは、仮想スイッチと仮想ルータのレイヤ 2 およびレイヤ 3 機能を結合して、各コンピュータからハイブリッド インターフェイスを介してファイアウォールに（赤色とオレンジ色の線で示されているように）トラフィックを渡すことができるようにします。

詳しくは、『*FireSIGHT System User Guide*』の「ハイブリッド インターフェイスのセットアップ」を参照してください。

ゲートウェイ VPN の展開

ライセンス：VPN

サポートされるデバイス：シリーズ 3

ローカル ゲートウェイとリモート ゲートウェイ間のセキュアなトンネルを確立するために、*ゲートウェイ バーチャル プライベート ネットワーク*（ゲートウェイVPN）接続を作成できます。ゲートウェイ間のセキュアなトンネルは、それらの間の通信を保護します。

FireSIGHT システムを設定して、Internet Protocol Security（IPSec）プロトコル スイートを使用する、シスコの管理対象デバイスの仮想ルータからリモート デバイスや他のサードパーティの VPN エンドポイントへのセキュアな VPN トンネルを構築します。VPN 接続が確立されると、ローカル ゲートウェイの背後にあるホストは、セキュアな VPN トンネルを介してリモート ゲートウェイの背後にあるホストに接続できます。VPN エンドポイントは、トンネルのセキュリティ アソシエーションを作成するために、Internet Key Exchange（IKE）のバージョン 1 またはバージョン 2 のプロトコルを使用して相互に認証を行います。システムは、IPsec 認証ヘッダー（AH）モードまたは IPsec カプセル化セキュリティ ペイロード（ESP）モードで稼動します。AH と ESP はどちらも認証を提供し、ESP は暗号化も提供します。

ゲートウェイ VPN は、ポイントツーポイント、スター、またはメッシュの展開で使用できます。

- ポイントツーポイント展開は、2 つのエンドポイントを直接的な 1 対 1 の関係で相互に接続します。両方のエンドポイントがピア デバイスとして設定され、どちらのデバイスもセキュアな接続を開始できます。少なくとも 1 台のデバイスは、VPN 対応の管理対象デバイスであることが必要です。

  遠隔地のホストがパブリック ネットワークを使用してユーザーのネットワーク内のホストに接続する際のネットワーク セキュリティを維持するためには、ポイントツーポイント展開を使用します。

- スター展開は、ハブと複数のリモート エンドポイント（リーフ ノード）間のセキュアな接続を確立します。ハブ ノードと個々のリーフ ノード間の接続は、それぞれ別個の VPN トンネルです。通常、ハブ ノードは本社にある VPN 対応の管理対象デバイスです。リーフ ノードは支店に配置し、大半のトラフィックを開始します。

  インターネットまたは他のサードパーティのネットワークを介したセキュアな接続を使用して、組織の本社と支店を接続し、すべての社員に組織のネットワークに対する制御されたアクセス権を付与するには、スター展開を使用します。

- メッシュ展開は、VPN トンネルによってすべてのエンドポイントをまとめて接続します。これにより、1 つのエンドポイントに障害が発生しても残りのエンドポイントは相互の通信を続行できるので、冗長性が提供されます。

  分散した支店のグループを接続して、1 つまたは複数の VPN トンネルで障害が発生してもトラフィックが続行できるようにするには、メッシュ展開を使用します。この設定で展開する VPN 対応の管理対象デバイスの数により、冗長性のレベルが制御されます。

ゲートウェイ VPN の設定および展開について詳しくは、『*FireSIGHT System User Guide*』の「ゲートウェイ VPN」を参照してください。

ポリシーベース NAT による展開

ライセンス：制御

サポートされるデバイス：Any（ASA FirePOWER を除く）

ポリシーベースのネットワーク アドレス変換（NAT）を使用して、NAT をどのように実行するかを指定するポリシーを定義できます。単一のインターフェイス、1 つ以上のデバイス、またはネットワーク全体をポリシーのターゲットにすることができます。

静的な変換（1 対 1）または動的な変換（1 対多）を設定できます。動的な変換は、最初に一致したルールが適用されるまでルールが順番に検索される、順序に依存したものであることに注意してください。

ポリシーベースの NAT は通常、以下の展開で機能します。

- プライベート ネットワーク アドレスを非表示にする。

  プライベート ネットワークからパブリック ネットワークにアクセスするとき、NAT はプライベート ネットワーク アドレスをパブリック ネットワーク アドレスに変換します。ユーザーの特定のプライベート ネットワーク アドレスは、パブリック ネットワークで非表示になります。

- プライベート ネットワーク サービスへのアクセスを許可する。

  パブリック ネットワークがプライベート ネットワークにアクセスするとき、NAT はパブリック アドレスをプライベート ネットワーク アドレスに変換します。パブリック ネットワークは、ユーザーの特定のプライベート ネットワーク アドレスにアクセスできます。

- 複数のプライベート ネットワーク間でトラフィックをリダイレクトする。

  プライベート ネットワークのサーバが接続先のプライベート ネットワークのサーバにアクセスするとき、プライベート アドレスが重複しないようにするため、そしてトラフィックがそれらのサーバ間を移動できるようにするために、NAT は 2 つのプライベート ネットワーク間でプライベート アドレスを変換します。

ポリシーベースの NAT を使用すると、追加のハードウェアの必要がなくなり、侵入検知システムまたは侵入防御システムの設定と NAT が 1 つのユーザー インターフェースに統合されます。詳しくは、『*FireSIGHT System User Guide*』の「NAT ポリシーの使用」を参照してください。

アクセス制御による展開

ライセンス：すべて

サポートされるデバイス：すべて

アクセス制御は、ネットワークに出入りしたりネットワーク内を移動したりできるトラフィックに対して、指定、検査、およびログ記録を行えるようにするポリシーベースの機能です。以下の項では、アクセス制御が展開でどのように機能するかを説明します。この機能について詳しくは、『*FireSIGHT System User Guide*』を参照してください。

アクセス制御ポリシーは、システムがネットワークのトラフィックを処理する方法を指定します。アクセス制御ルールをポリシーに追加して、ネットワーク トラフィックの処理とログ記録の方法をより詳細に制御することができます。

アクセス制御ルールを含まないアクセス制御ポリシーは、以下のデフォルト アクションの 1 つを使用してトラフィックを処理します。

- ネットワークに入らないようにすべてのトラフィックをブロックする
- ネットワークに入るすべてのトラフィックを信頼して受け入れ、それ以上の検査は行わない

- ネットワークに入るすべてのトラフィックを許可して受け入れ、ネットワーク検出ポリシーによるトラフィックの検査だけを実行する
- ネットワークに入るすべてのトラフィックを許可して受け入れ、侵入ポリシーとネットワーク検出ポリシーによるトラフィックの検査を実行する

アクセス制御ルールはさらに、ターゲットのデバイスがトラフィックを処理する方法を定義します。これには、簡単な IP アドレス マッチングから、さまざまなユーザー、アプリケーション、ポート、および URL が関係する複雑なシナリオまで含まれます。各ルールに対して、ルール アクション（つまり、侵入ポリシーやファイル ポリシーに基づいて、一致するトラフィックに対して信頼、監視、ブロック、検査のどれを行うか）を指定します。

アクセス制御は、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フィルタリングできます。これは、送信元または宛先 IP アドレスに基づいて、アクセス制御ポリシーごとに、ネットワークを通過できるトラフィックを指定する機能です。この機能により、トラフィックがブロックされて検査されない、拒否される IP アドレスのブラックリストを作成できます。

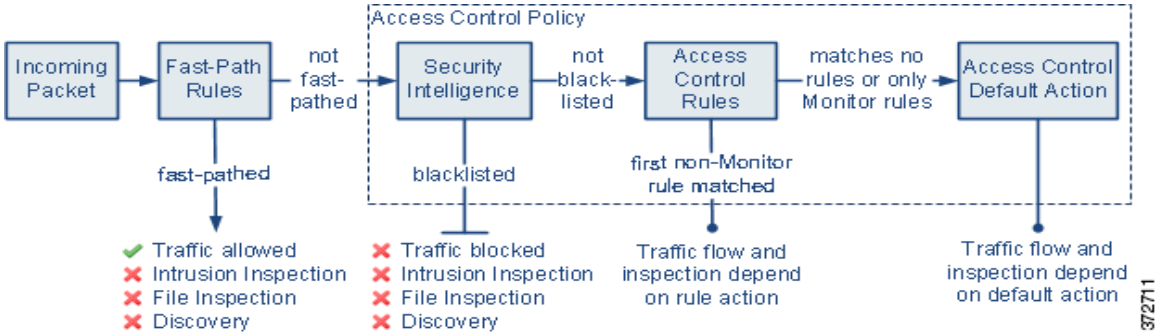
サンプルの展開では、一般的なネットワーク セグメントを例示しています。これらの場所のそれぞれに管理対象デバイスを展開すると、さまざまな目的のために役立ちます。以下の項では、一般的な場所についての推奨事項を説明します。

- 「ファイアウォールの内側」（P.2-16）では、アクセス制御がファイアウォールを通過するトラフィックに対してどのように機能するかを説明します。
- 「DMZ 上」（P.2-17）では、DMZ 内のアクセス制御が外向きのサーバをどのように保護するかを説明します。
- 「内部ネットワーク上」（P.2-18）では、アクセス制御が意図的または偶発的な攻撃から内部ネットワークをどのように保護するかを説明します。
- 「コア ネットワーク上」（P.2-19）では、厳密なルールのアクセス制御ポリシーが重要な資産をどのように保護するかを説明します。
- 「リモートまたはモバイル ネットワーク上」（P.2-19）では、アクセス制御がリモート ロケーションやモバイル デバイス上のトラフィックから、ネットワークをどのように監視し保護するかを説明します。

ファイアウォールの内側

ファイアウォールの内側の管理対象デバイスは、ファイアウォールによって許可された着信トラフィックや、誤った設定のためにファイアウォールを通過したトラフィックを監視します。一般的なネットワーク セグメントには、DMZ、内部ネットワーク、コア、モバイル アクセス、リモート ネットワークなどがあります。

次の図は、FireSIGHT システムを通過するトラフィック フローを例示して、そのトラフィックに実行される検査のタイプを詳しく示しています。システムは、高速処理されるトラフィックやブラックリストに記載されたトラフィックを検査しないことに注意してください。アクセス制御ルールやデフォルト アクションによって処理されるトラフィックの場合、フローと検査はルール アクションによって異なります。分かりやすくするために、ルール アクションは図に示されていませんが、システムは信頼されるトラフィックやブロックされたトラフィックに対してどのような検査も実行しません。また、デフォルト アクションではファイル検査がサポートされていません。



着信パケットは、まず高速処理のルールと突き合わせて検査されます。一致が見つかった場合、トラフィックは高速処理されます。一致しない場合、セキュリティ インテリジェンスベースのフィルタリングにより、パケットがブラックリストに含まれているかどうかを判別します。含まれていない場合は、アクセス制御ルールが適用されます。パケットがルールの条件を満たす場合、トラフィック フローと検査はルール アクションによって決まります。パケットがルールに一致しない場合、トラフィック フローと検査はデフォルト ポリシー アクションによって決まります。（モニタ ルールでは例外が生じ、トラフィックの評価が続行します。）各アクセス制御ポリシーのデフォルト アクションは、高速処理されず、ブラックリストに含まれていない、さらには監視以外のルールと一致しないトラフィックを管理します。高速処理は、8000 シリーズと 3D9900 デバイスでのみ使用可能であることに注意してください。

アクセス制御ルールを作成して、ネットワーク トラフィックの処理とログ記録の方法をより詳細に制御することができます。ルールごとに、特定の条件に一致するトラフィックに適用するアクション（信頼する、監視する、ブロックする、または検査する）を指定します。

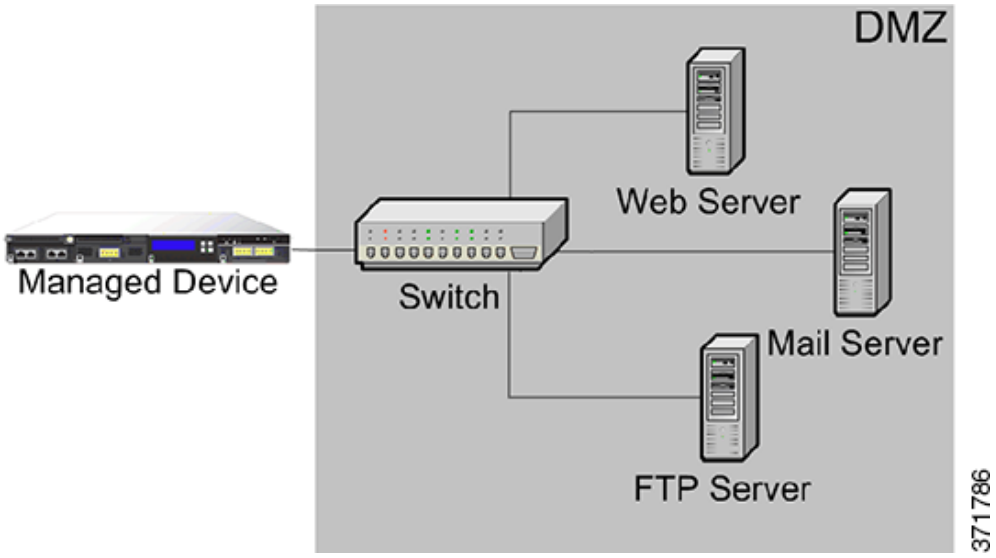
DMZ 上

DMZ は外向きのサーバ（Web、FTP、DNS、メールなど）を含んでおり、内部ネットワークのユーザに対して、メール リレーや Web プロキシなどのサービスを提供することもあります。

DMZ に保存されるコンテンツは静的なものであり、変更が計画されて実行される場合には、明確な連絡と事前の通知が行われます。DMZ 内のサーバに生じる変更は計画されているものだけなので、このセグメントでの攻撃は通常はインバウンドで、すぐに明らかになります。このセグメントのための有効なアクセス制御ポリシーは、サービスへのアクセスを厳格に制御し、新しいネットワーク イベントを検索します。

DMZ 内のサーバには、DMZ がネットワークを介して照会できるデータベースを含めることができます。DMZ と同様に予期しない変更が生じることはありませんが、データベースのコンテンツはより機密性が高く、Web サイトや他の DMZ サービスよりも強力な保護を必要とします。DMZ のアクセス制御ポリシーに加えて強力な侵入ポリシーを設定することは、効果的な戦略となります。

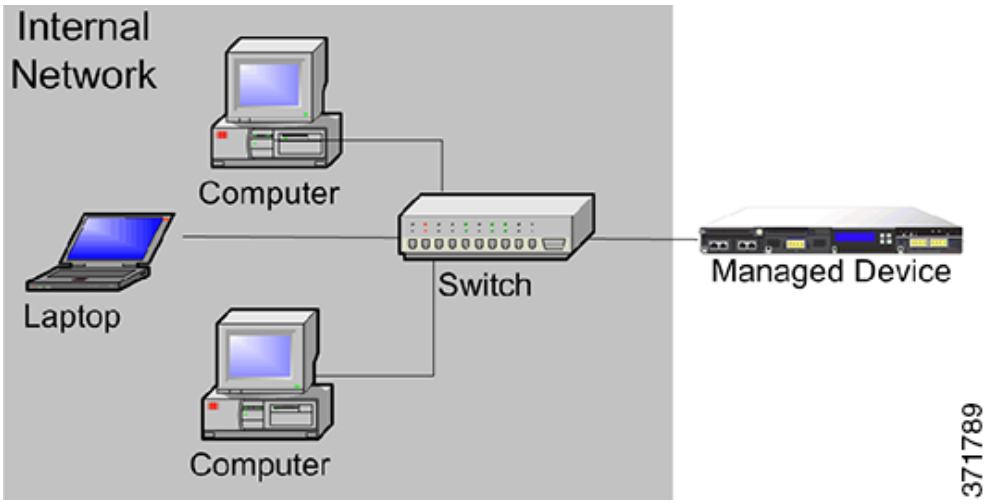
このセグメントに展開された管理対象デバイスは、DMZ 内の侵害されたサーバから発信される、インターネットに対する攻撃を検出できます。ネットワーク ディスカバリを使用してネットワーク トラフィックの監視を行うと、それらの公開されているサーバで変更点（予期されないサービスが突然現れるなど）を監視して、DMZ 内の侵害されたサーバを発見するために役立ちます。



内部ネットワーク上

悪意のある攻撃は内部ネットワーク上のコンピュータから生じることがあります。これは、明確な行為（未知のコンピュータが不意にネットワークに出現するなど）または偶発的な感染（オフサイトで感染した作業用ラップトップがネットワークに接続してウイルスを拡散するなど）である可能性があります。内部ネットワークでのリスクはアウトバウンドである可能性もあります（コンピュータが疑わしい外部 IP アドレスに情報を送信するなど）。

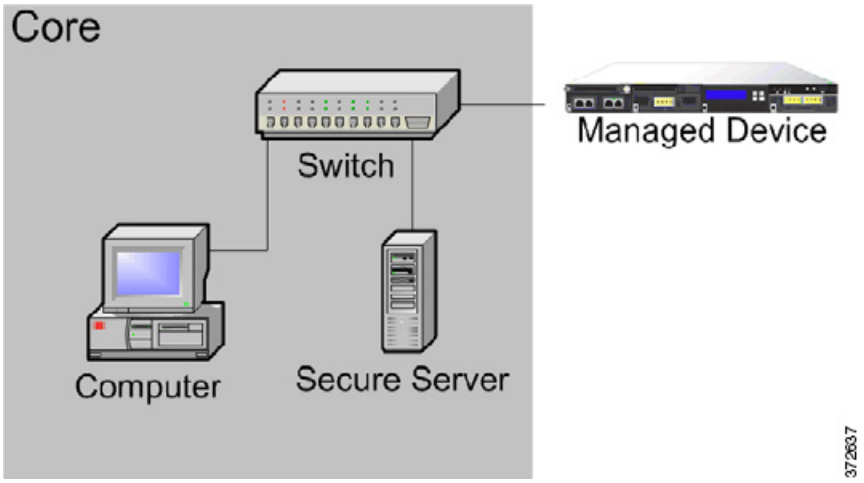
このダイナミック ネットワークでは、アウトバウンド トラフィックに加えてすべての内部トラフィックにも、厳密なアクセス制御ポリシーが必要です。ユーザとアプリケーション間のトラフィックを厳密に制御する、アクセス制御ルールを追加します。



コア ネットワーク上

コア資産は、あらゆるコストを払ってでも保護する必要がある、ビジネスの成功に不可欠な資産です。コア資産はビジネスの性質によって異なりますが、典型的なコア資産には、財務センターや管理センター、さらには知的財産のリポジトリが含まれます。コア資産のセキュリティが侵犯された場合、ビジネスが破たんする可能性があります。

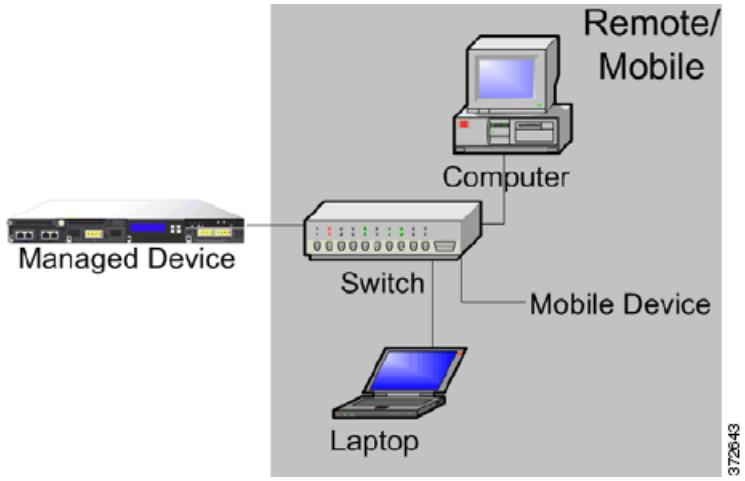
ビジネスが機能するためには、このセグメントが容易に使用可能でなければならないものの、厳密に制限され制御される必要もあります。アクセス制御では、リスクが最も高いネットワーク セグメント（リモート ネットワークやモバイル デバイスなど）が、それらの資産にアクセスできないようにする必要があります。このセグメントでは、ユーザやアプリケーションのアクセスに厳密なルールを適用して、最も積極的な制御を使用します。



リモートまたはモバイル ネットワーク上

オフサイトにあるリモート ネットワークは通常、仮想プライベート ネットワーク（VPN）を使用してプライマリ ネットワークにアクセスできるようにします。モバイル デバイスやパーソナル デバイスの業務目的での使用（「スマートフォン」を使用して社内電子メールにアクセスする、など）は、ますます一般的になっています。

これらのネットワークは、迅速かつ継続的に変更される、非常に動的な環境となることがあります。専用のモバイルまたはリモート ネットワークに管理対象デバイスを展開すると、不明な外部ソースに出入りするトラフィックを監視および管理するための、厳格なアクセス コントロール ポリシーを作成することができます。ポリシーは、ユーザ、ネットワーク、およびアプリケーションがコア リソースにアクセスする方法を厳密に制限して、リスクを軽減できます。



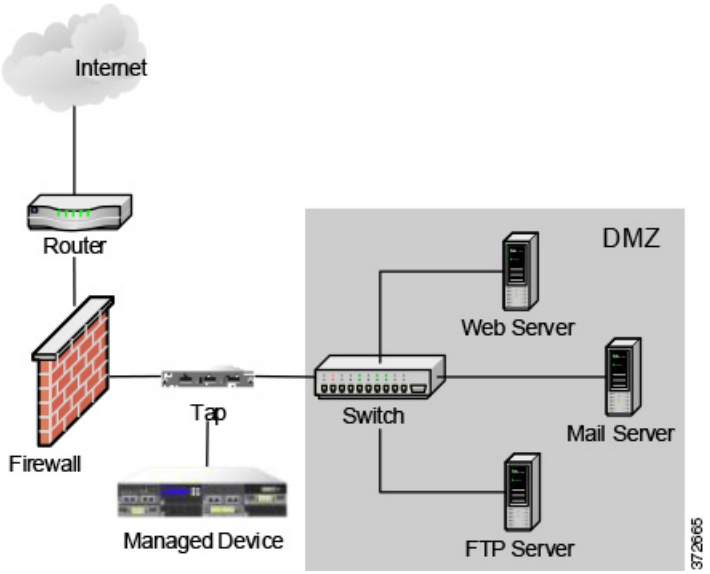
複数ポートの管理対象デバイスの使用

管理対象デバイスは、ネットワーク モジュールに、複数のセンシング ポートを提供します。以下の目的で、複数ポートの管理対象デバイスを使用できます。

- ネットワーク タップから個々の接続を再結合する
- さまざまなネットワークからのトラフィックを検知して評価する
- 仮想ルータとして実行する
- 仮想スイッチとして実行する

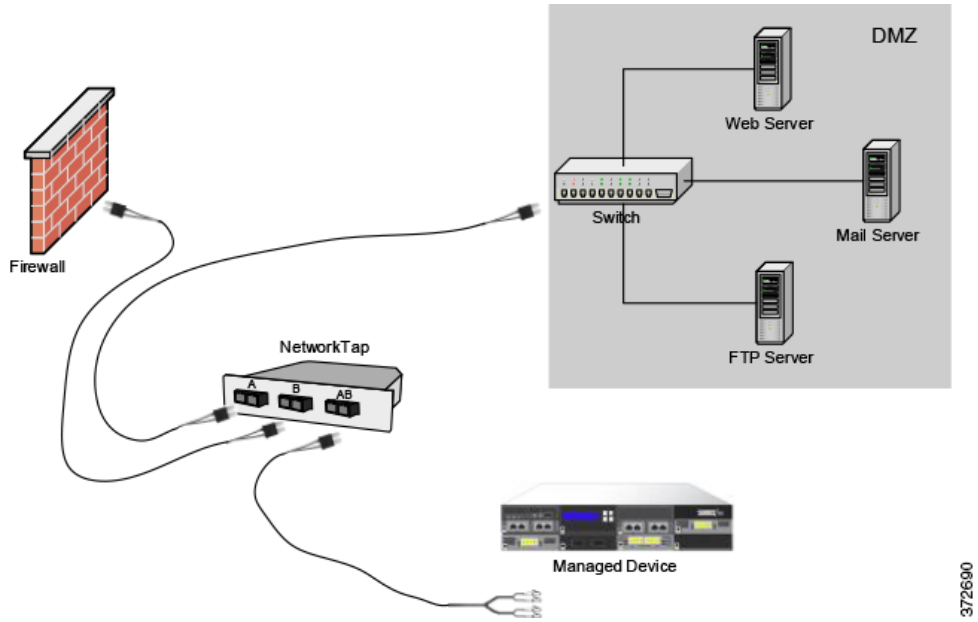
（注）　各ポートは、デバイスの評価対象となる完全なスループットを受信できますが、管理対象デバイスでの合計トラフィックが帯域幅の評価を超えるとパケットの消失が発生します。

ネットワーク タップのある複数ポートの管理対象デバイスを展開することは、簡単な処理です。次の図は、トラフィックの多いネットワーク セグメントに設置されたネットワーク タップを示しています。

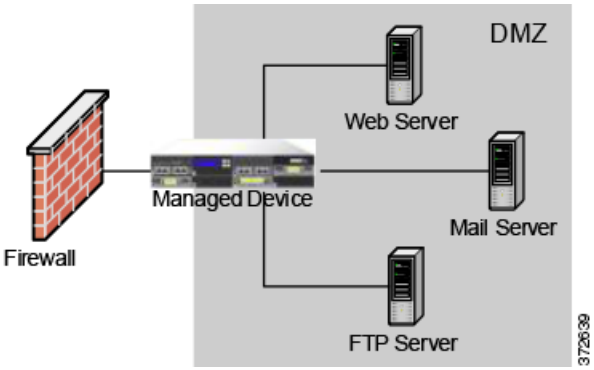


このシナリオでは、タップが別個のポートを介して着信および発信トラフィックを伝送します。管理対象デバイス上の複数ポートのインターフェイス アダプタ カードをタップに接続すると、管理対象デバイスはトラフィックを単一のデータ ストリームに組み合わせて、分析可能にすることができます。

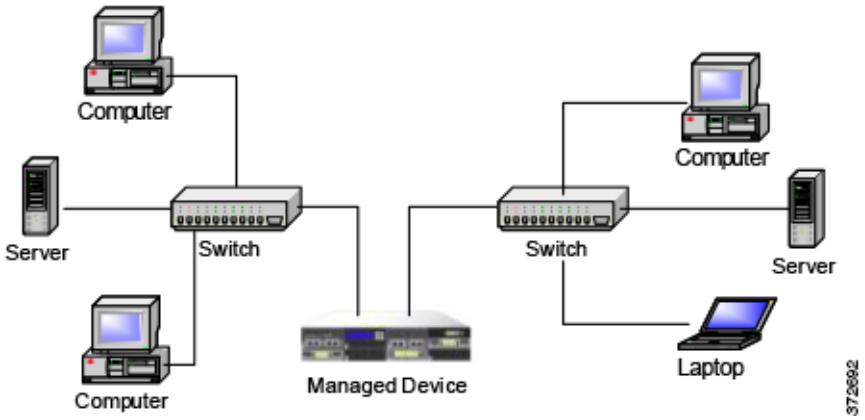
以下の図に示すようなギガビット光学タップでは、管理対象デバイス上にあるポートのセットは、どちらもタップからのコネクタによって使用されることに注意してください。



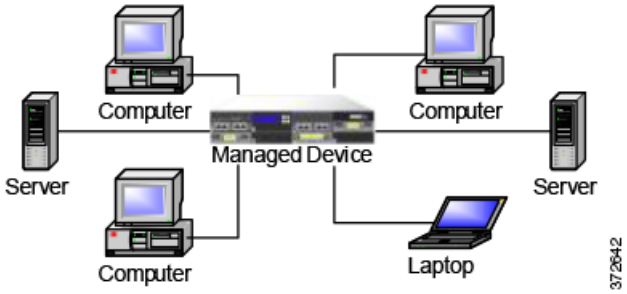
仮想スイッチを使用して、展開のタップとスイッチの両方を置き換えることができます。タップを仮想スイッチに置き換える場合は、タップのパケット配信保証を失うことに注意してください。



さまざまなネットワークからのデータを取得するインターフェイスを作成することもできます。次の図は、デュアルポートのアダプタがある単一のデバイスと、2 つのネットワークに接続された 2 つのインターフェイスを示しています。



1 つのデバイスを使用して両方のネットワーク セグメントを監視することに加えて、デバイスの仮想スイッチの機能を使用して、展開にある両方のスイッチを置き換えることができます。



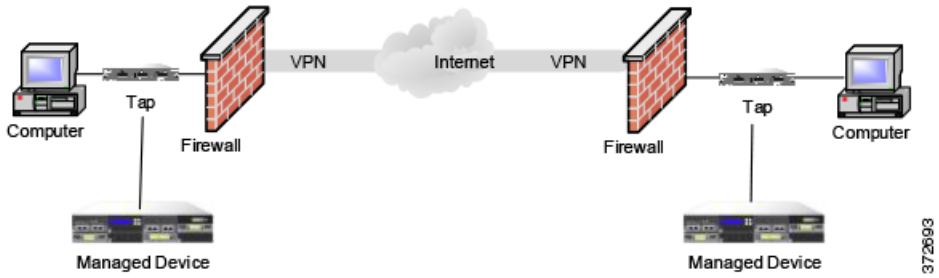
複雑なネットワークの展開

エンタープライズのネットワークは、VPN などのリモート アクセスを必要とする場合や、ビジネス パートナーやバンキング接続などの複数のエントリー ポイントを持つ場合があります。以下の項では、これらの展開に関係する問題の一部について説明します。

VPN との統合

バーチャル プライベート ネットワーク（VPN）は、IP トンネリング技術を使用して、ローカル ネットワークのセキュリティをインターネット上のリモート ユーザに提供します。一般に、VPN ソリューションは IP パケット内のデータ ペイロードを暗号化します。IP ヘッダーは暗号化されていないので、そのパケットを他のパケットと同様にパブリック ネットワーク経由で送信することができます。パケットが宛先ネットワークに到達すると、ペイロードが復号化されて、パケットは適切なホストに送られます。

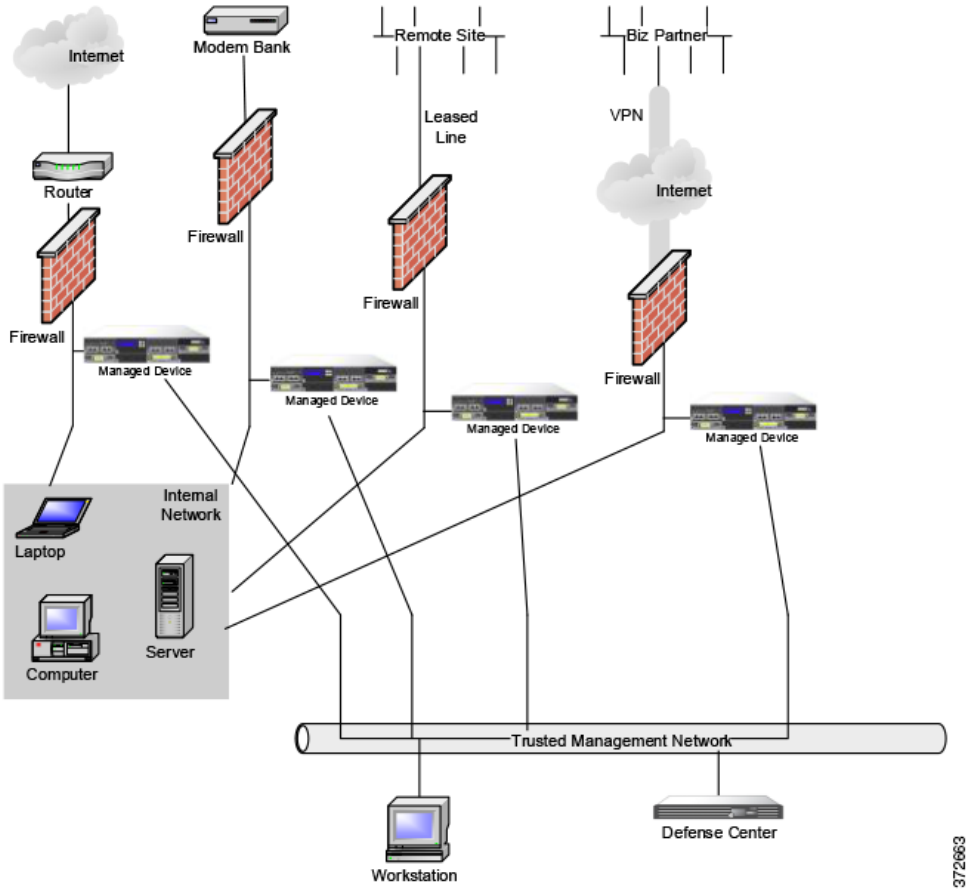
ネットワーク アプライアンスは VPN パケットの暗号化されたペイロードを分析できないため、管理対象デバイスを VPN 接続の終端エンドポイントの外部に配置すると、すべてのパケット情報にアクセスできるようになります。次の図は、管理対象デバイスを VPN 環境に展開する方法を例示しています。



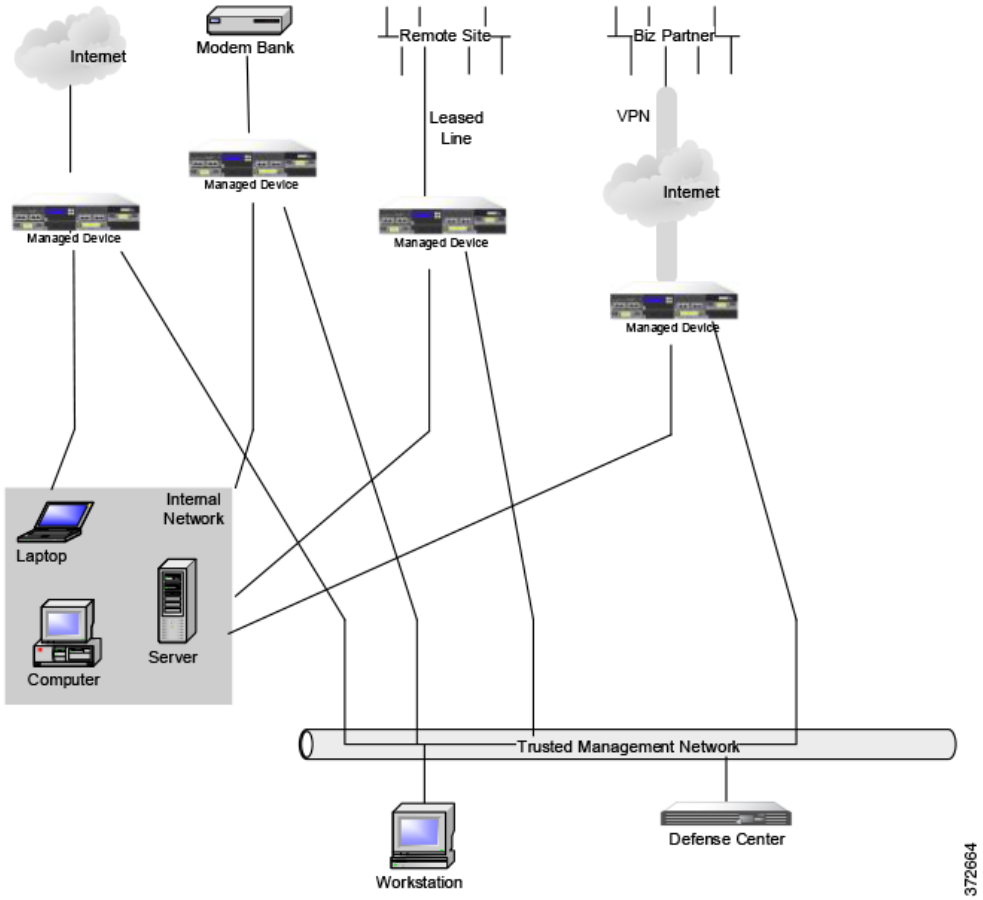
管理対象デバイスとの VPN 接続の両側で、ファイアウォールとタップを置き換えることができます。タップを管理対象デバイスに置き換える場合は、タップのパケット配信保証を失うことに注意してください。

他のエントリ ポイントでの侵入検知

多くのネットワークには、複数のアクセス ポイントが含まれています。インターネットに接続する単一の境界ルータの代わりに、一部の企業は、インターネット、モデム バンク、およびビジネス パートナーのネットワークへの直接リンクの組み合わせを使用します。一般に、管理対象デバイスは、ファイアウォールの近く（ファイアウォールの内部、ファイアウォールの外部、または両方）に、そしてビジネス データの整合性と機密性のために重要なネットワーク セグメントに展開する必要があります。次の図は、管理対象デバイスを、複数のエントリ ポイントが存在する複雑なネットワークの主な場所に設置する方法を示しています。

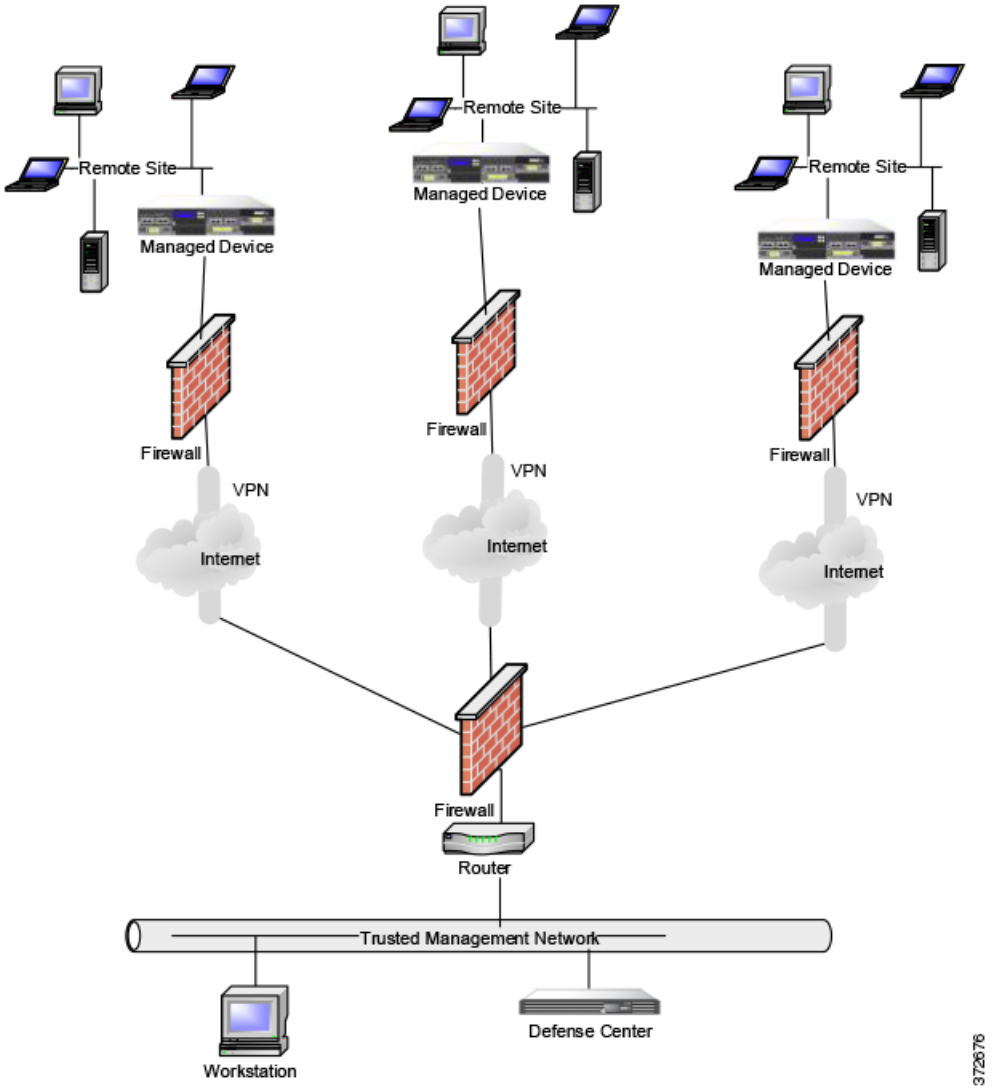


ファイアウォールとルータを、そのネットワーク セグメントに展開された管理対象デバイスに置き換えることができます。

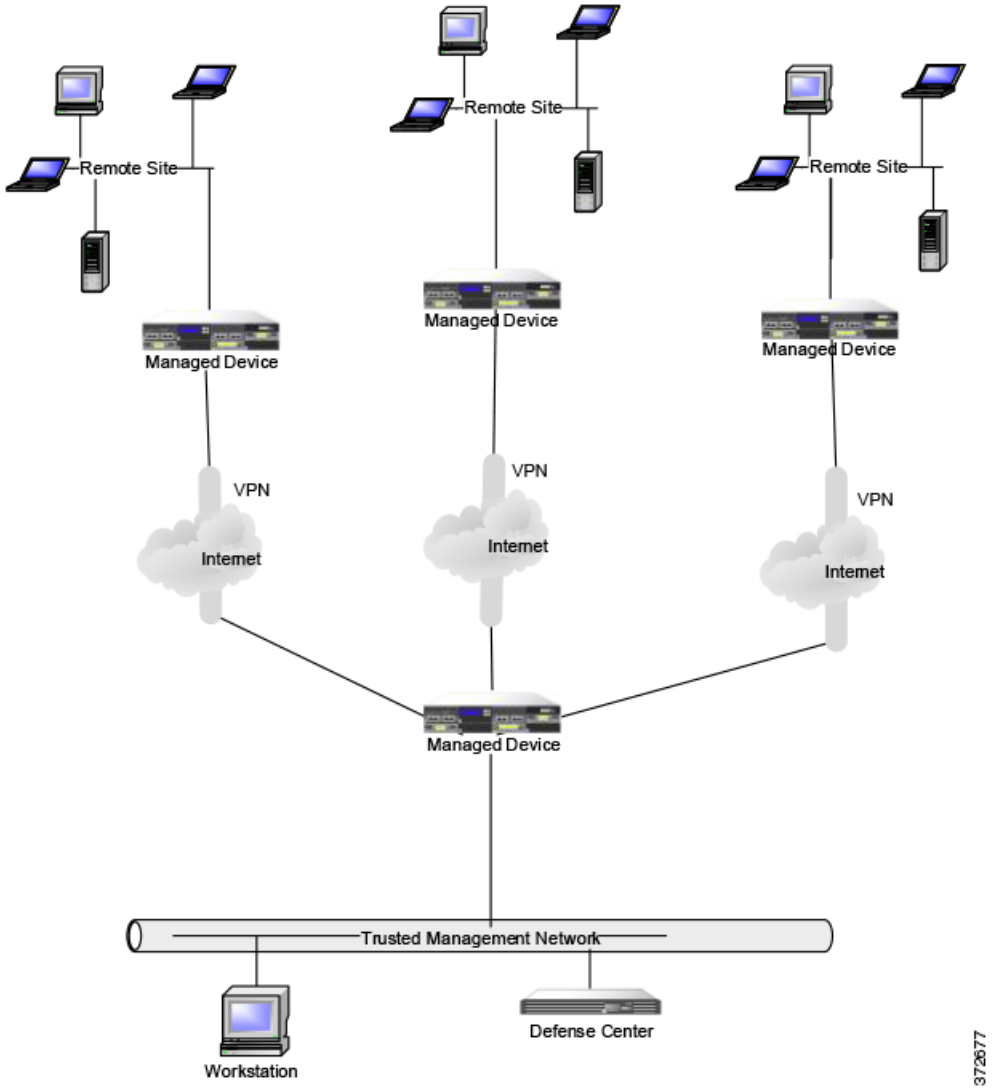


複数サイト環境での展開

多くの組織では、地理的に分散している企業全体で侵入検知を展開し、1 か所からすべてのデータを分析することを望んでいます。FireSIGHT システムは、組織の多数の場所に展開された管理対象デバイスからのイベントを集約して関連付けする防御センターを提供して、これをサポートします。同じネットワーク上の同じ地理的な場所に複数の管理対象デバイスと防御センターを展開するのとは異なり、さまざまな地理的な場所に管理対象デバイスを展開する際には、管理対象デバイスとデータ ストリームのセキュリティを確保するために対策を講じる必要があります。データを保護するために、保護されていないネットワークから管理対象デバイスと防御センターを隔離する必要があります。これは、VPN を介した管理対象デバイスからのデータ ストリームを送信することによって、または次の図のように他のセキュアなトンネリング プロトコルによって実行できます。



ファイアウォールとルータを、各ネットワーク セグメントに展開された管理対象デバイスに置き換えることができます。



複雑なネットワーク内の管理対象デバイスの統合

単純な複数セクター ネットワークよりも複雑なネットワーク トポロジに、管理対象デバイスを展開できます。この項では、FireSIGHT 防御センターを使用した複数の管理対象デバイスの管理や、複数サイト環境での管理対象デバイスの展開と管理についての情報に加えて、プロキシ サーバ、NAT デバイス、および VPN が存在する環境に展開する際のネットワーク ディスカバリと脆弱性分析に関連した問題について説明します。

プロキシ サーバと NAT との統合

ネットワーク アドレス変換（NAT）のデバイスやソフトウェアがファイアウォールの外側に配置されており、ファイアウォールの内側に内部ホストの IP アドレスが効果的に隠されている場合があります。管理対象デバイスがこれらのデバイスやソフトウェアと監視されるホストの間に配置されている場合は、システムがプロキシや NAT デバイスの背後にあるホストを正確に識別しない可能性があります。このような場合、シスコでは、ホストが正しく検出されるように、プロキシまたは NAT デバイスで保護されているネットワーク セグメント内に管理対象デバイスを配置するように推奨しています。

ロード バランシング方式との統合

一部のネットワーク環境では、Web ホスティングや FTP ストレージ サイトなどのサービスに対してネットワーク ロード バランシングを実行するために、「サーバ ファーム」設定が使用されます。ロード バランシング環境では、IP アドレスが、固有のオペレーティング システムの複数のホスト間で共有されます。この場合、システムはオペレーティング システムの変更を検出するので、高い信頼値を持つ静的なオペレーティング システム ID を提供できません。影響を受けるホストにある別個のオペレーティング システムの数に応じて、システムは、多数のオペレーティング システムの変更イベントを生成するか、またはより低い信頼値を持つ静的なオペレーティング システム ID を示します。

検出に関するその他の考慮事項

識別されているホストの TCP/IP スタックに変更が生じた場合は、システムがホストのオペレーティング システムを正確に識別できないことがあります。場合によっては、パフォーマンスを向上させるためにこれを行うことがあります。たとえば、インターネット インフォメーション サービス（IIS）の Web サーバを実行する Windows ホストの管理者は、TCP ウィンドウ サイズを大きくして受信するデータの量を増やし、パフォーマンスを向上させるように勧められています。別の例として、TCP/IP スタックの変更によって本当のオペレーティング システムを不明瞭にして、正確に識別できないようにし、攻撃対象とならないようにする場合があります。この対処方法が用いられるシナリオとして考えられるのは、攻撃者がネットワークの偵察スキャンを実施して特定のオペレーティング システムを持つホストを識別してから、そのオペレーティング システムに合った手段を使用して、それらのホストを対象にした攻撃を行うことです。

FireSIGHT システム アプライアンスの設置

大規模な FireSIGHT システム展開の一部として、ネットワーク上に FireSIGHT システム アプライアンスを容易に設置できます。ネットワークのセグメントにデバイスを設置し、トラフィックを検査して、適用される侵入ポリシーに基づいて侵入イベントを生成します。このデータの送信先となる防御センターでは、展開全体のデータを相互に関連付け、セキュリティ上の脅威を総合的に調整して対処するために 1 つ以上のデバイスを管理します。

別々の展開場所で使用される複数のアプライアンスを 1 か所で事前設定できます。事前設定のガイダンスについては、「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。

（注） ASA FirePOWER デバイスの設置方法については、ASA のマニュアルを参照してください。

FireSIGHT システム アプライアンスの詳しい設置方法については、以下の項を参照してください。

同梱品目

FireSIGHT システム アプライアンスに付属のコンポーネントを以下に示します。システムおよび関連するアクセサリを開梱するときには、次のように、パッケージの中身が全て揃っていることを確認してください。

- FireSIGHT システム アプライアンス × 1
- 電源コード（2 本の電源コードが、冗長電源を含むアプライアンスに付属しています）
- カテゴリ 5e イーサネット ストレート ケーブル：防御センター用と管理対象デバイス用にそれぞれ 1 本ずつ
- ラックマウント キット（3D7010、3D7020、および 3D7030 で別々に使用するために必要なトレイとラックマウント キット）× 1

セキュリティ上の考慮事項

アプライアンスを設置する前に、次の点を考慮することをシスコでは推奨しています。

- 無許可ユーザが立ち入ることのできない安全な場所にあるロック付きラックに FireSIGHT システム アプライアンスを配置します。
- 訓練を受け、資格要件を満たしている人物にのみ、FireSIGHT システム アプライアンスの設置、交換、管理、または修理を許可します。
- 無許可アクセスから保護された安全な内部管理ネットワークに、管理インターフェイスを必ず接続します。
- アプライアンスへのアクセスを許可される具体的なワークステーションの IP アドレスを特定します。アプライアンスのシステム ポリシー内でアクセス リストを使用して、それらの特定のホストに対してのみアプライアンスへのアクセスを限定的に許可します。詳細については、『*FireSIGHT System User Guide*』を参照してください。

管理インターフェイスの識別

管理インターフェイスを使用して、展開内の各アプライアンスをネットワークに接続します。これにより、防御センターは管理対象デバイスと通信してそれらを管理することができます。

FireSIGHT システム アプライアンスは、さまざまなハードウェア プラットフォームで提供されています。設置手順を進めるときには、該当するアプライアンスに応じて正しい図を参照してください。

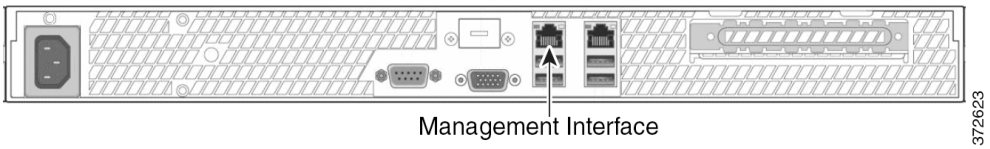
- 「FireSIGHT 防御センター 750」（P.3-2）
- 「FireSIGHT 防御センター 1500」（P.3-3）
- 「FireSIGHT 防御センター 3500」（P.3-3）
- 「FireSIGHT 7000 シリーズ」（P.3-3）
- 「FireSIGHT 8000 シリーズ」（P.3-4）

FireSIGHT 防御センター 750

DC750 を 1 U アプライアンスとして使用できます。

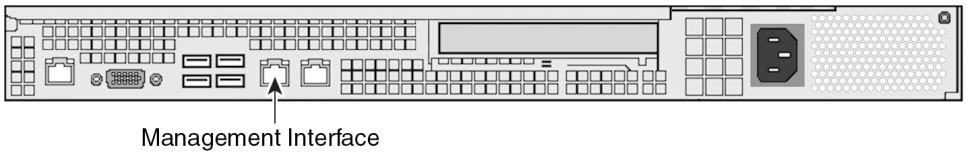
次のシャーシ背面図に、DC750 の管理インターフェイスの位置を示します。

図 3-1　　DC750



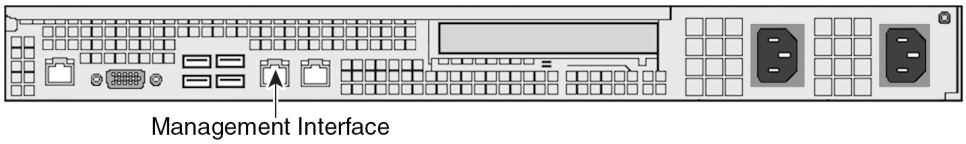
FireSIGHT 防御センター 1500

DC1500 を 1 U アプライアンスとして使用できます。次のシャーシ背面図に、管理インターフェイスの位置を示します。



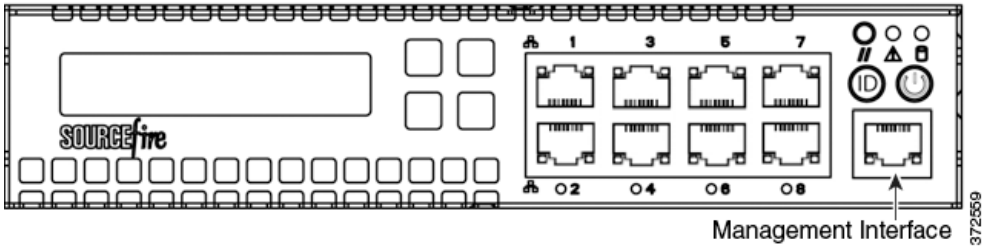
FireSIGHT 防御センター 3500

DC3500 を 1 U アプライアンスとして使用できます。次のシャーシ背面図に、管理インターフェイスの位置を示します。

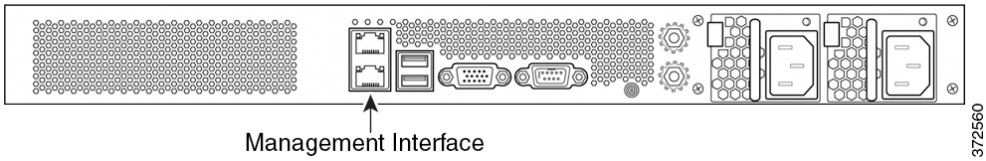


FireSIGHT 7000 シリーズ

3D7010、3D7020、および 3D7030 はシャーシ トレイ幅の半分の 1 U アプライアンスです。次のシャーシ前面図に、管理インターフェイスを示します。

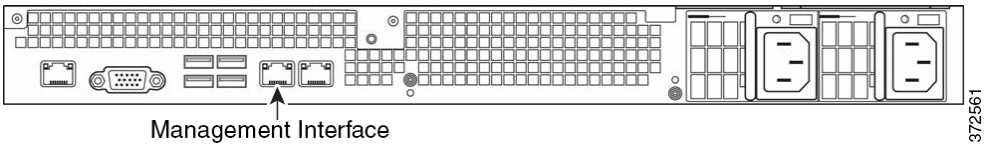


3D7110/7120、3D7115/7125、および AMP7150 を 1 U アプライアンスとして使用できます。次のシャーシ背面図に、管理インターフェイスの位置を示します。

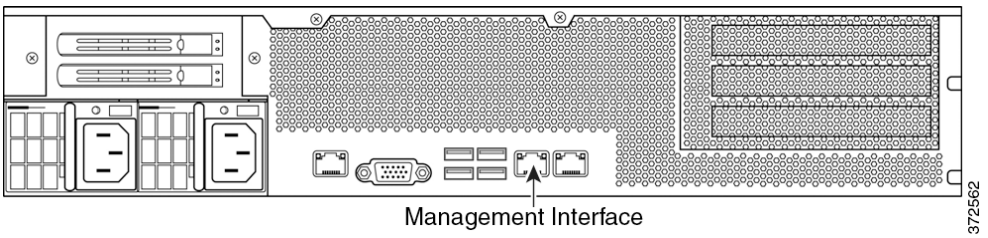


FireSIGHT 8000 シリーズ

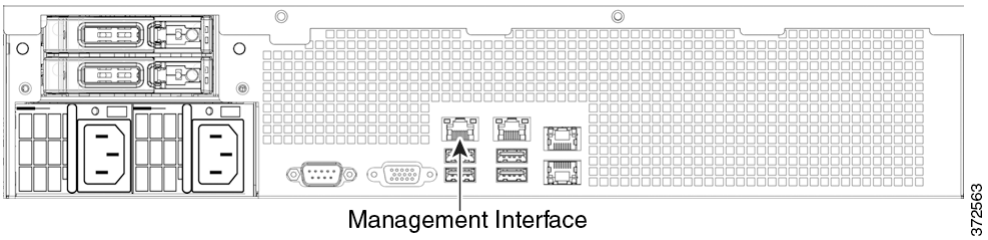
3D8120、3D8130、3D8140、および AMP8150 を 1 U アプライアンスとして使用できます。次のシャーシ背面図に、管理インターフェイスの位置を示します。



3D8250 を 2 U アプライアンスとして使用できます。3D8260、3D8270、および 3D8290 は、1 つ、2 つ、または 3 つのセカンダリ 2 U アプライアンスが付属する 2 U アプライアンスとして使用可能です。次のシャーシ背面図に、2 U アプライアンスごとの管理インターフェイスの位置を示します。



3D8350 を 2 U アプライアンスとして使用できます。3D8360、3D8370、および 3D8390 は、1 つ、2 つ、または 3 つのセカンダリ 2 U アプライアンスが付属する 2 U アプライアンスとして使用可能です。次のシャーシ背面図に、2 U アプライアンスごとの管理インターフェイスの位置を示します。



センシング インターフェイスの識別

管理対象デバイスは、センシング インターフェイスを使用してネットワーク セグメントに接続します。各デバイスでモニター可能なセグメントの数は、デバイス上のセンシング インターフェイスの数と、ネットワーク セグメント上で使用する接続タイプ（パッシブ、インライン、ルーテッド、またはスイッチド）に応じて異なります。

以下の項では、各管理対象デバイスのセンシング インターフェイスについて説明します。

- 7000 シリーズ 上のセンシング インターフェイスを特定するには、「FirePOWER 7000 シリーズ」（P.3-5）を参照してください。
- 8000 シリーズ上のモジュール スロットを特定するには、「FirePOWER 8000 シリーズ」（P.3-8）を参照してください。
- 8000 シリーズ NetMod 上のセンシング インターフェイスを特定するには、「8000 シリーズ モジュール」（P.3-10）を参照してください。

接続タイプについては、「インターフェイスについて」（P.2-2）を参照してください。

FirePOWER 7000 シリーズ

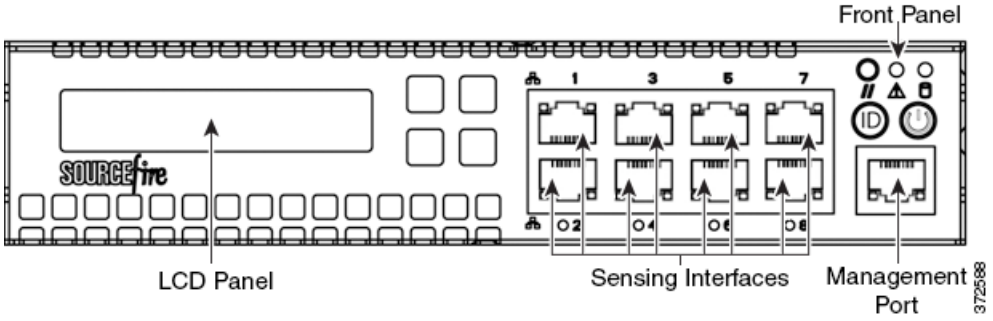
次の設定で、7000 シリーズを使用することができます。

- それぞれ設定可能なバイパス機能を持つ 8 つの銅線インターフェイスを、ラック トレイ幅の半分の 1 U デバイス
- それぞれ設定可能なバイパス機能を持つ 8 つの銅線インターフェイスまたは 8 つの光ファイバ インターフェイスを備えた 1 U デバイス
- 設定可能なバイパス機能を持つ 4 つの銅線インターフェイスと、バイパス機能のない 8 つの Small Form-Factor Pluggable（SFP）ポートを備えた 1 U デバイス

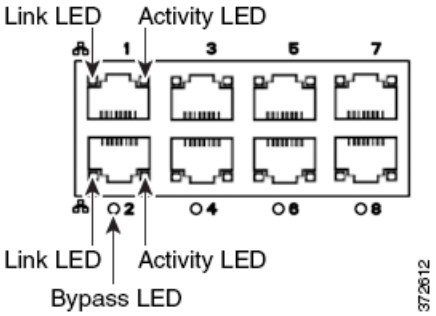
3D7010、3D7020、および 3D7030

3D7010、3D7020、および 3D7030 には、それぞれ設定可能なバイパス機能を持つ 8 つの銅線ポート センシング インターフェイスが付属しています。次のシャーシ前面図に、センシング インターフェイスの位置を示します。

図 3-2　　8 ポート 1000BASE-T 設定可能バイパス インターフェイス（銅線）



これらの接続を使用して、最大 8 つの別個のネットワーク セグメントを受動的にモニタリングできます。また、インライン（またはバイパス モードのインライン）でペア化されたインターフェイスを使用して、デバイスを侵入防御システムとして最大 4 つのネットワーク上に展開できます。



デバイスの自動バイパス機能を利用するためには、2 つのインターフェイスを垂直にネットワーク セグメントに接続する必要があります（インターフェイス 1 と 2、3 と 4、5 と 6、または 7 と 8）。自動バイパス機能を使用すると、デバイスで障害が発生した場合や電源を消失した場合でもトラフィックが流れることができます。インターフェイスを配線した後、Web インターフェイスを使用して、インターフェイスのペアをインライン セットとして設定し、そのインライン セットでバイパス モードを有効にします。

3D7110 と 3D7120

3D7110 と 3D7120 には、8 つの銅線ポート センシング インターフェイスまたは 8 つの光ファイバ ポート センシング インターフェイスが付属しており、それぞれバイパス機能を設定できます。次のシャーシ前面図に、センシング インターフェイスの位置を示します。

図 3-3　　3D7110 と 3D7120 銅線インターフェイス

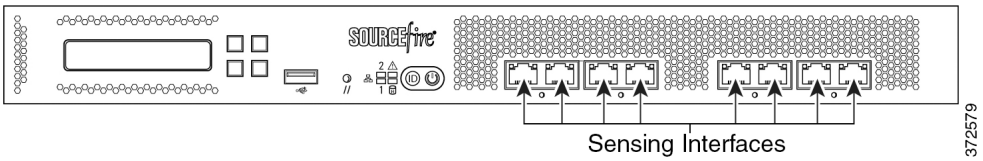
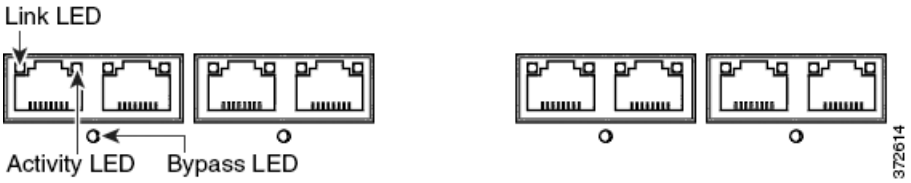


図 3-4　　8 ポート 1000BASE-T 銅線インターフェイス



これらの接続を使用して、最大 8 つの別個のネットワーク セグメントを受動的にモニタリングできます。また、インライン（またはバイパス モードのインライン）でペア化されたインターフェイスを使用して、デバイスを侵入防御システムとして最大 4 つのネットワーク上に展開できます。

デバイスの自動バイパス機能を利用するためには、左側にある 2 つのインターフェイスあるいは右側にある 2 つのインターフェイスをネットワーク セグメントに接続する必要があります。自動バイパス機能を使用すると、デバイスで障害が発生した場合や電源を消失した場合でもトラフィックが流れることができます。インターフェイスを配線した後、Web インターフェイスを使用して、インターフェイスのペアをインライン セットとして設定し、そのインライン セットでパイパス モードを有効にします。

図 3-5　　3D7110 と 3D7120 の光ファイバ インターフェイス

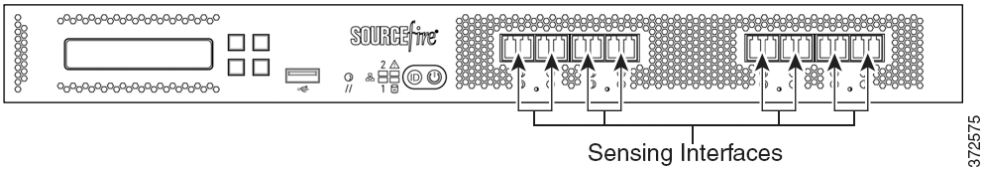


図 3-6　　8 ポート 1000BASE-SX 設定可能バイパス（光ファイバ）

8 ポート 1000BASE-SX 光ファイバ設定可能バイパスの設定では、LC タイプ（ローカル コネクタ）光トランシーバが使用されます。

これらの接続を使用して、最大 8 つの別個のネットワーク セグメントを受動的にモニタリングできます。また、インライン（またはバイパス モードのインライン）でペア化されたインターフェイスを使用して、デバイスを侵入防御システムとして最大 4 つのネットワーク上に展開できます。

ヒント　最高のパフォーマンスを得るには、インターフェイス セットを連続的に使用してください。いずれかのインターフェイスをスキップすると、パフォーマンスが低下する可能性があります。

デバイスの自動バイパス機能を利用するためには、左側にある 2 つのインターフェイスあるいは右側にある 2 つのインターフェイスをネットワーク セグメントに接続する必要があります。自動バイパス機能を使用すると、デバイスで障害が発生した場合や電源を消失した場合でもトラフィックが流れることができます。インターフェイスを配線した後、Web インターフェイスを使用して、インターフェイスのペアをインライン セットとして設定し、そのインライン セットでパイパス モードを有効にします。

3D7115、3D7125、および AMP7150

3D7115、3D7125、および AMP7150 デバイスには、設定可能なバイパス機能を持つ 4 ポート銅線インターフェイスと、バイパス機能のない 8 つのホットスワップ可能 Small Form-Factor Pluggable（SFP）ポートが付属しています。次のシャーシ前面図に、センシング インターフェイスの位置を示します。

図 3-7　　3D7115 と 3D7125 の銅線インターフェイスと SFP インターフェイス

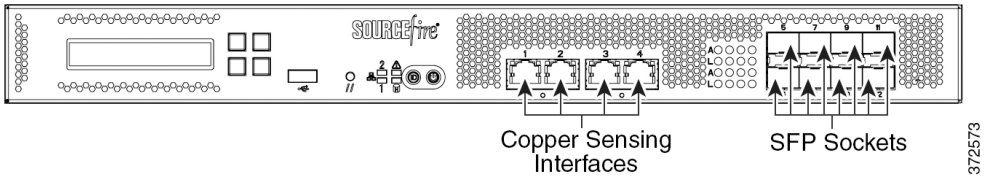
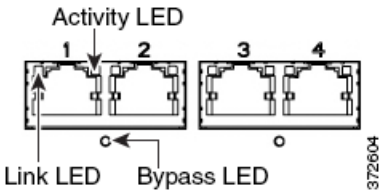


図 3-8　　4 つの 1000BASE-T 銅線インターフェイス



銅線インターフェイスを使用して、最大 4 つの別個のネットワーク セグメントを受動的にモニタリングできます。また、インライン（またはバイパス モードのインライン）でペア化されたインターフェイスを使用して、デバイスを侵入防御システムとして最大 2 つのネットワーク上に展開できます。

デバイスの自動バイパス機能を利用するためには、左側にある 2 つのインターフェイスあるいは右側にある 2 つのインターフェイスをネットワーク セグメントに接続する必要があります。自動バイパス機能を使用すると、デバイスで障害が発生した場合や電源を消失した場合でもトラフィックが流れることができます。インターフェイスを配線した後、Web インターフェイスを使用して、インターフェイスのペアをインライン セットとして設定し、そのインライン セットでパイパス モードを有効にします。

SFP インターフェイス

シスコ SFP トランシーバを SFP ソケットに取り付けると、最大 8 つの別個のネットワーク セグメントを受動的にモニタリングできます。また、インライン（非バイパス モード）でペア化されたインターフェイスを使用して、デバイスを侵入検知システムとして最大 4 つのネットワーク上に展開できます。

シスコ SFP トランシーバは、1G 銅線、1G 短距離光ファイバ、または 1G 長距離光ファイバで使用され、ホットスワップ可能です。パッシブ設定またはインライン設定で、銅線または光ファイバ トランシーバを任意に組み合わせてデバイスで使用できます。なお、SFP トランシーバはバイパス機能を備えていないため、侵入防御展開でこれらを使用するのは不適切です。互換性を維持するために、シスコから入手可能な SFP トランシーバだけを使用してください。詳細については、「3D71x5 および AMP7150 デバイスでの SFP トランシーバの使用」（P.B-1）を参照してください。

図 3-9　サンプルの SFP トランシーバ

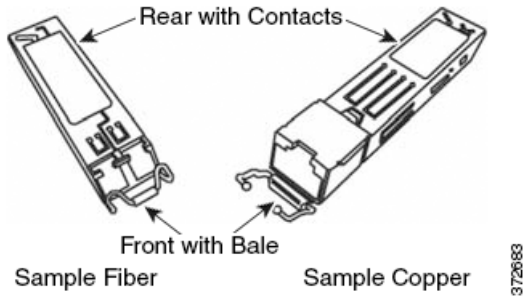
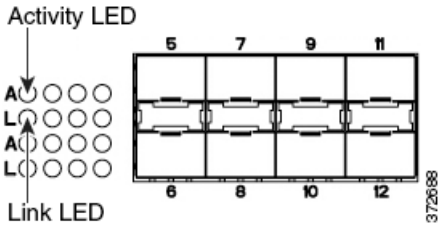


図 3-10　SFP ソケット



FirePOWER 8000 シリーズ

8000 シリーズ は、10G ネットワーク スイッチを備えた 1 U デバイス、または 10G と 40G のどちらかのネットワーク スイッチを備えた 2 U デバイスとして使用可能です。このデバイスは完全に組み立てられた状態で出荷されることもありますが、センシング インターフェイスを含むネットワーク モジュール（NetMod）を取り付けることもできます。

（注） デバイス上の非互換スロットに NetMod を取り付けた場合（たとえば 3D8250 または 3D8350 のスロット 1 と 4 に 40G NetMod を挿入した場合）、または他の何らかの形で NetMod とシステムの互換性がない場合は、NetMod を設定しようとすると、管理している防御センターの Web インターフェイスにエラーまたは警告メッセージが表示されます。支援が必要な場合は、サポートに連絡してください。

次のモジュールには、設定可能なバイパス センシング インターフェイスがあります。

- 設定可能なバイパス機能を持つクワッドポート 1000BASE-T 銅線インターフェイス
- 設定可能なバイパス機能を持つクワッドポート 1000BASE-SX 光ファイバ インターフェイス
- 設定可能なバイパス機能を持つデュアルポート 10GBASE（MMSR または SMLR）光ファイバ インターフェイス
- 設定可能なバイパス機能を持つデュアルポート 40GBASE-SR4 光ファイバ インターフェイス（2 U デバイスのみ）

次のモジュールには、非バイパス センシング インターフェイスがあります。

- バイパス機能のないクワッドポート 1000BASE-T 銅線インターフェイス
- バイパス機能のないクワッドポート 1000BASE-SX 光ファイバ インターフェイス
- バイパス機能のないデュアルポート 10GBASE（MMSR または SMLR）光ファイバ インターフェイス

加えて、スタッキング モジュールは、同じ方法で設定された複数のアプライアンスのリソースを統合します。スタッキング モジュールは、3D8140、3D8250、および 3D8350 ではオプションであり、3D8260、3D8270、3D8290 と 3D8360、3D8370、3D8390 のスタック構成では標準搭載です。

注意　このモジュールはホットスワップ可能では**ありません**。詳細については、「8000 シリーズ モジュールの取り付けと取り外し」（P.C-1）を参照してください。

次のシャーシ前面図に、センシング インターフェイスを含むモジュール スロットの位置を示します。

図 3-11　81xx ファミリ のシャーシ前面図

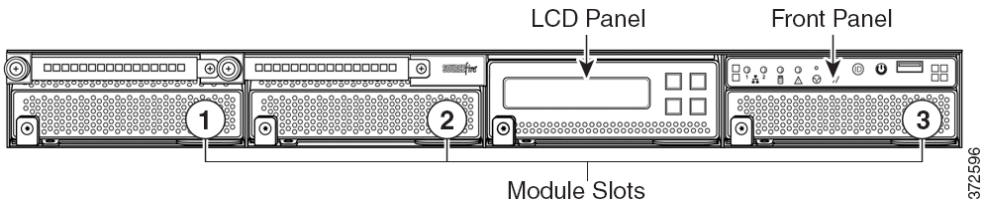
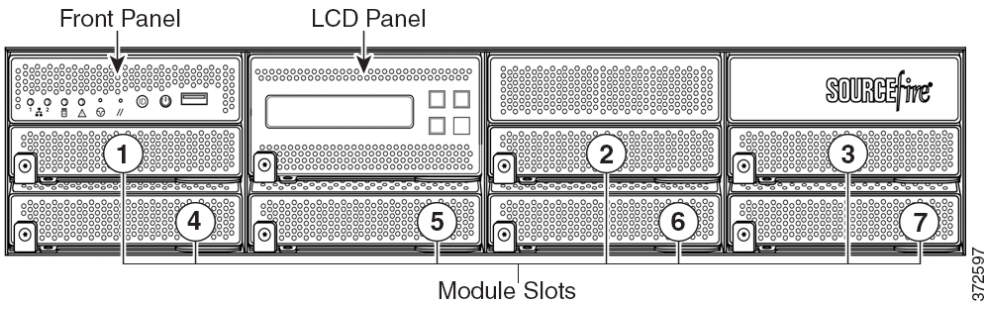


図 3-12　82xx ファミリ および 83xx ファミリ のシャーシ前面図



8000 シリーズ モジュール

8000 シリーズ は、設定可能なバイパス機能を持つ次のモジュールと一緒に出荷されることがあります。

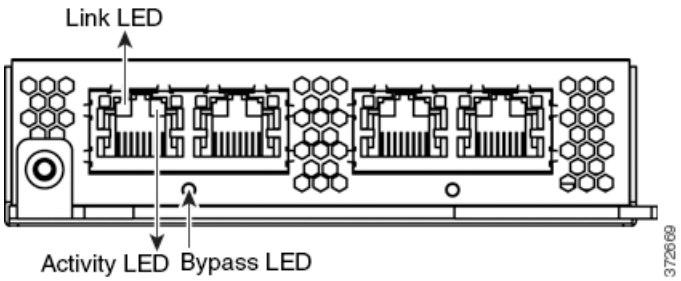
- 設定可能なバイパス機能を持つクワッドポート 1000BASE-T 銅線インターフェイス 詳細については、「図 3-13クワッドポート 1000BASE-T（銅線）設定可能バイパス NetMod」（P.3-10）を参照してください。
- 設定可能バイパス機能を持つクワッドポート 1000BASE-SX 光ファイバ インターフェイス。詳細については、「図 3-14クワッドポート 1000BASE-SX（光ファイバ）設定可能バイパス NetMod」（P.3-11）を参照してください。
- 設定可能なバイパス機能を持つデュアルポート 10GBASE（MMSR または SMLR）光ファイバ インターフェイス。詳細については、「図 3-15デュアルポート 10GBASE（MMSR または SMLR）光ファイバの設定可能バイパス NetMod」（P.3-11）を参照してください。
- 設定可能なバイパス機能を持つデュアルポート 40GBASE-SR4 光ファイバ インターフェイス。詳細については、「図 3-16デュアルポート 40GBASE-SR4（光ファイバ）設定可能バイパス NetMod」（P.3-12）を参照してください。

8000 シリーズ は、設定可能なバイパス機能のない次のモジュールと一緒に出荷されることがあります。

- バイパス機能のないクワッドポート 1000BASE-T 銅線インターフェイス。詳細については、「図 3-18クワッドポート 1000BASE-T（銅線）非バイパス NetMod」（P.3-13）を参照してください。
- バイパス機能のないクワッドポート 1000BASE-SX 光ファイバ インターフェイス。詳細については、「図 3-19クワッドポート 1000BASE-SX（光ファイバ）の非バイパス NetMod」（P.3-13）を参照してください。
- バイパス機能のないクワッドポート 10GBASE（MMSR または SMLR）光ファイバ インターフェイス。詳細については、「図 3-20クワッドポート 10GBASE（MMSR または SMLR）光ファイバ非バイパス NetMod」（P.3-13）を参照してください。

スタッキング モジュールは 3D8140、3D8250、および 3D8350 ではオプションであり、3D8260、3D8270、3D8290 と 3D8360、3D8370、3D8390 のスタック構成では標準搭載です。詳細については、「8000 シリーズ スタッキング モジュール」（P.3-14）を参照してください。

図 3-13　　クワッドポート 1000BASE-T（銅線）設定可能バイパス NetMod

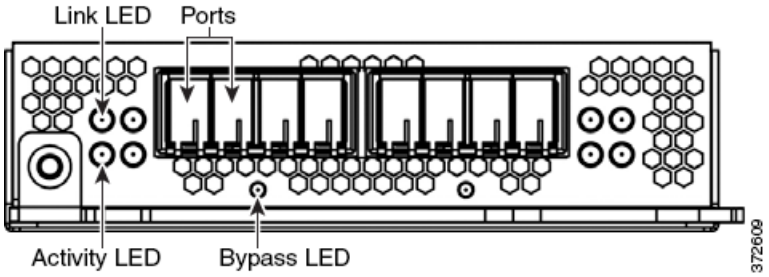


これらの接続を使用して、最大 4 つの別個のネットワーク セグメントを受動的にモニタリングできます。また、インライン（またはバイパス モードのインライン）でペア化されたインターフェイスを使用すると、デバイスを侵入防御システムとして最大 2 つのネットワーク上に展開できます。

デバイスの自動バイパス機能を利用するためには、左側にある 2 つのインターフェイスあるいは右側にある 2 つのインターフェイスをネットワーク セグメントに接続する必要があります。これにより、デバイスで障害が発生した場合や電源を消失した場合でもトラフィックが流れる

ことができます。また、Web インターフェイスを使用して、インターフェイスのペアをインライン セットとして設定し、そのインライン セットでパイパス モードを有効にする必要もあります。

図 3-14　クワッドポート 1000BASE-SX（光ファイバ）設定可能バイパス NetMod



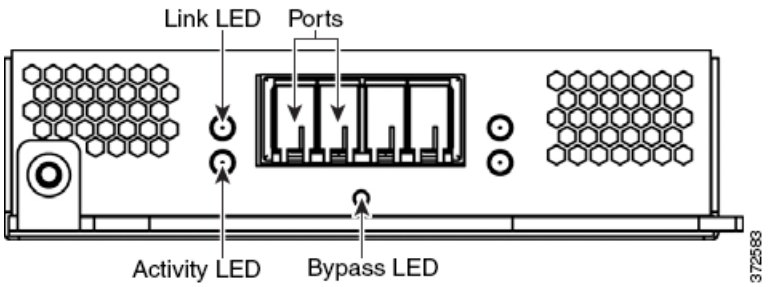
クワッドポート 1000BASE-SX 光ファイバ設定可能バイパスの設定では、LC タイプ（ローカル コネクタ）光トランシーバが使用されます。

この設定を使用して、最大 4 つの別個のネットワーク セグメントを受動的にモニタリングできます。また、インライン（またはバイパス モードのインライン）でペア化されたインターフェイスを使用すると、管理対象デバイスを侵入防御システムとして最大 2 つの別個のネットワーク上に展開できます。

ヒント　最高のパフォーマンスを得るには、インターフェイス セットを連続的に使用してください。インターフェイスをスキップすると、パフォーマンスが低下する可能性があります。

デバイスの自動バイパス機能を利用するためには、左側にある 2 つのインターフェイス、または右側にある 2 つのインターフェイスをネットワーク セグメントに接続する必要があります。これにより、デバイスで障害が発生した場合や電源を消失した場合でもトラフィックが流れることができます。また、Web インターフェイスを使用して、インターフェイスのペアをインライン セットとして設定し、そのインライン セットでパイパス モードを有効にする必要もあります。

図 3-15　デュアルポート 10GBASE（MMSR または SMLR）光ファイバの設定可能バイパス NetMod



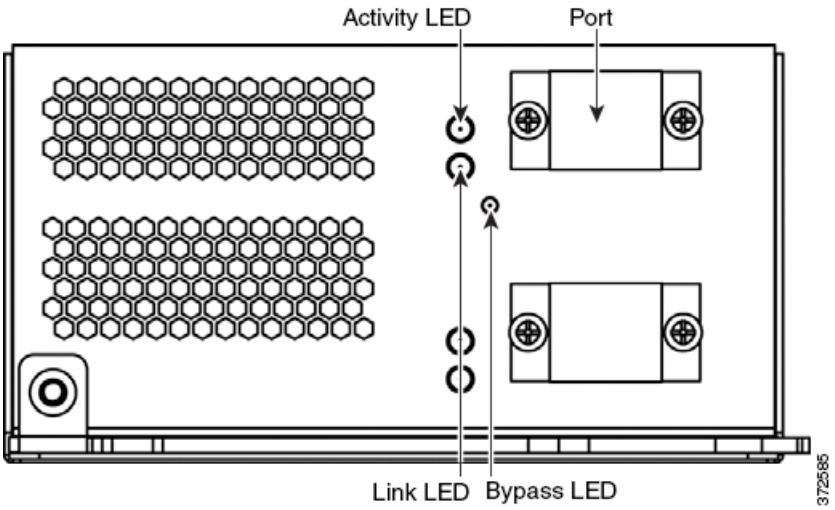
デュアルポート 10GBASE 光ファイバ設定可能バイパスの設定では、LC タイプ（ローカル コネクタ）光トランシーバが使用されます。MMSR インターフェイスあるいは SMLR インターフェイスが可能であることに注意してください。

この設定を使用して、最大 2 つの別個のネットワーク セグメントを受動的にモニタリングできます。また、インライン（またはバイパス モードのインライン）でペア化されたインターフェイスを使用すると、管理対象デバイスを侵入防御システムとして単一のネットワーク上に展開できます。

ヒント　最高のパフォーマンスを得るには、インターフェイス セットを連続的に使用してください。インターフェイスをスキップすると、パフォーマンスが低下する可能性があります。

デバイスの自動バイパス機能を利用するためには、2 つのインターフェイスをネットワーク セグメントに接続する必要があります。これにより、デバイスで障害が発生した場合や電源を消失した場合でもトラフィックが流れることができます。また、Web インターフェイスを使用して、インターフェイスのペアをインライン セットとして設定し、そのインライン セットでバイパス モードを有効にする必要もあります。

図 3-16　デュアルポート 40GBASE-SR4（光ファイバ）設定可能バイパス NetMod



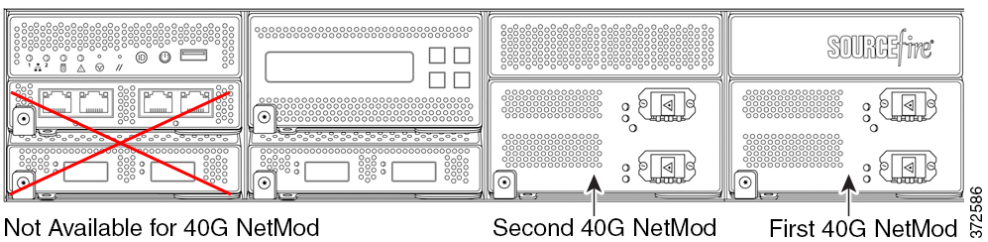
デュアルポート 40GBASE-SR4 光ファイバ設定可能バイパスの設定では、MPO（マルチファイバ プッシュ オン）コネクタ光トランシーバが使用されます。

40G NetMod は、3D8270、3D8290、3D8360、3D8370、および 3D8390、または 40G 対応の 3D8250、3D8260、および 3D8350 でのみ使用可能です。40G 非対応のデバイスに 40G インターフェイスを作成しようとすると、管理する防御センター Web インターフェイスの 40G インターフェイス画面は赤く表示されます。40G 対応 3D8250 の LCD パネルには「3D 8250-40G」と表示され、40G 対応 3D8350 の LCD パネルには「3D 8350-40G」と表示されます。

この設定を使用して、最大 2 つの別個のネットワーク セグメントを受動的にモニタリングできます。また、インライン（またはバイパス モードのインライン）でペア化されたインターフェイスを使用すると、デバイスを侵入防御システムとして 1 つのネットワーク上に展開できます。

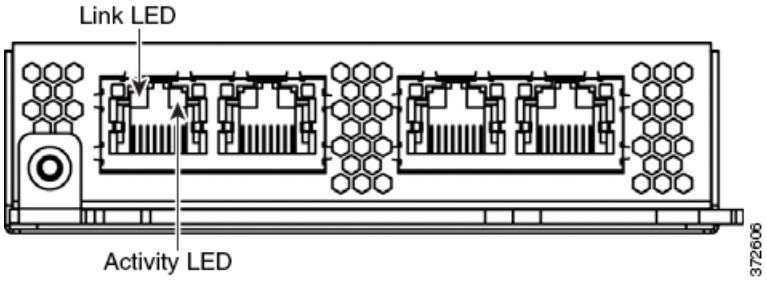
最大で 2 つの 40G NetMod を使用できます。1 番目の 40G NetMod をスロット 3 と 7 に、2 番目をスロット 2 と 6 に取り付けます。スロット 1 と 4 で 40G NetMod を使用することはできません。

図 3-17　40G NetMod の配置



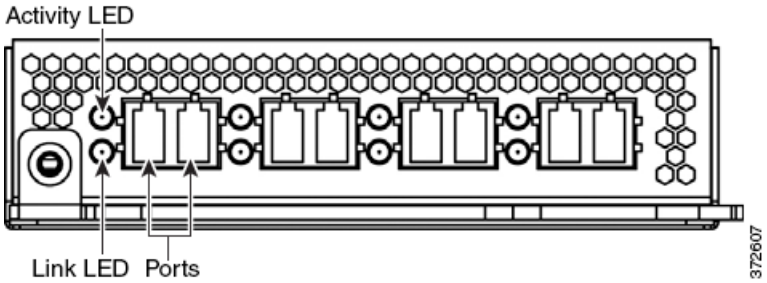
デバイスの自動バイパス機能を利用するためには、Web インターフェイスを使用して、インターフェイスのペアをインライン セットとして設定し、そのインライン セットでバイパス モードを有効にする必要があります。

図 3-18　クワッドポート 1000BASE-T（銅線）非バイパス NetMod



これらの接続を使用して、最大 4 つの別個のネットワーク セグメントを受動的にモニタリングできます。また、インライン設定でペア化されたインターフェイスを、最大 2 つのネットワーク セグメントで使用することもできます。

図 3-19　クワッドポート 1000BASE-SX（光ファイバ）の非バイパス NetMod

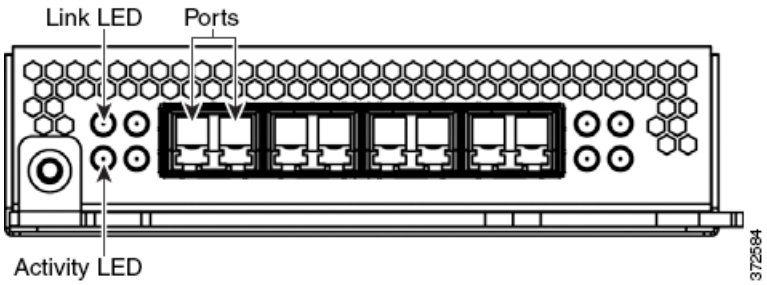


クワッドポート 1000BASE-SX 光ファイバ非バイパス設定では、LC タイプ（ローカル コネクタ）光トランシーバが使用されます。

これらの接続を使用して、最大 4 つの別個のネットワーク セグメントを受動的にモニタリングできます。また、インライン設定でペア化されたインターフェイスを、最大 2 つのネットワーク セグメントで使用することもできます。

ヒント　最高のパフォーマンスを得るには、インターフェイス セットを連続的に使用してください。インターフェイスをスキップすると、パフォーマンスが低下する可能性があります。

図 3-20　クワッドポート 10GBASE（MMSR または SMLR）光ファイバ非バイパス NetMod



クワッドポート 10GBASE 光ファイバ非バイパス設定では、MMSR インターフェイスまたは SMLR インターフェイスを備えた LC タイプ（ローカル コネクタ）光トランシーバが使用されます。

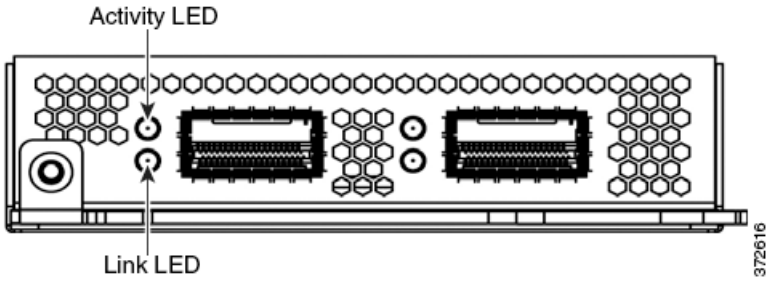
注意　クワッドポート 10GBASE 非バイパス NetMod には、取り外し不可能な Small Form-Factor Pluggable（SFP）トランシーバが実装されています。SFP を取り外そうとすると、モジュールが破損する可能性があります。

これらの接続を使用して、最大 4 つの別個のネットワーク セグメントを受動的にモニタリングできます。また、インライン設定でペア化されたインターフェイスを、最大 2 つのネットワーク セグメントで使用することもできます。

ヒント　最高のパフォーマンスを得るには、インターフェイス セットを連続的に使用してください。インターフェイスをスキップすると、パフォーマンスが低下する可能性があります。

8000 シリーズ スタッキング モジュール

スタッキング モジュールは、同じ方法で設定された複数のアプライアンスのリソースを統合します。スタッキング モジュールは 3D8140、3D8250、および 3D8350 ではオプションであり、3D8260、3D8270、3D8290 と 3D8360、3D8370、3D8390 のスタック構成では標準搭載です。



スタッキング モジュールを使用すると、2 つのデバイスのリソースを統合して、1 つをプライマリ デバイス、もう 1 つをセカンダリ デバイスとして使用できます。プライマリ デバイスにのみ、センシング インターフェイスがあります。次のデバイスでスタッキング モジュールを使用できます。

- 3D8140、3D8250、および 3D8350 はスタッキング モジュール付きで出荷可能です。
- 3D8260 と 3D8360 では、プライマリ デバイスに 1 つのスタッキング モジュールが、セカンダリ デバイスに 1 つのスタッキング モジュールが付属しています。
- 3D8270 と 3D8370 では、プライマリ デバイスに 2 つのスタッキング モジュールが、2 台のセカンダリ デバイスそれぞれに 1 つのスタッキング モジュールが付属しています。
- 3D8290 と 3D8390 では、プライマリ デバイスに 3 つのスタッキング モジュールが、3 台のセカンダリ デバイスそれぞれに 1 つのスタッキング モジュールが付属しています。

スタック済みデバイスの詳しい使用方法については、スタック構成でのデバイスの使用を参照してください。

スタック構成でのデバイスの使用

スタック構成では、同じ方法で設定されたデバイスのリソースを統合することにより、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。1 つのデバイスがプライマリ デバイスとして指定され、ネットワーク セグメントに接続されます。他のすべてのデバイスはセカンダリ デバイスとして指定され、プライマリ デバイスに追加のリソースを提供するためにそれらが使用されます。防御センターはスタック構成を作成、編集、および管理します。

プライマリ デバイスには、センシング インターフェイスと、接続されているセカンダリ デバイスごとに 1 つのスタッキング インターフェイス セットが含まれています。プライマリ デバイス上のセンシング インターフェイスを、非スタック デバイスと同じ方法で、モニタ対象のネットワーク セグメントに接続します。スタッキング ケーブルを使用して、プライマリ デバイス上のスタッキング インターフェイスをセカンダリ デバイス上のスタッキング インターフェイスに接続します。それぞれのセカンダリ デバイスは、スタッキング インターフェイスを使用してプライマリ デバイスに直接接続されます。セカンダリ デバイスにセンシング インターフェイスが含まれる場合、それらは使用されません。

次の設定で、デバイスをスタックできます。

- 2 つの 3D8140
- 最大で 4 つの 3D8250
- 1 つの 3D8260（1 つの 10G 対応プライマリ デバイスと 1 つのセカンダリ デバイス）
- 1 つの 3D8270（1 つの 40G 対応プライマリ デバイスと 2 つのセカンダリ デバイス）
- 1 つの 3D8290（1 つの 40G 対応プライマリ デバイスと 3 つのセカンダリ デバイス）
- 最大で 4 つの 3D8350
- 1 つの 3D8360（1 つの 40G 対応プライマリ デバイスと 1 つのセカンダリ デバイス）
- 1 つの 3D8370（1 つの 40G 対応プライマリ デバイスと 2 つのセカンダリ デバイス）
- 1 つの 3D8390（1 つの 40G 対応プライマリ デバイスと 3 つのセカンダリ デバイス）

3D8260、3D8270、3D8360、および 3D8370 では、追加のデバイスをスタックして、合計 4 デバイスからなるスタックにすることができます。

1 つのデバイスがプライマリ デバイスとして指定され、プライマリ ロール付きで防御センターの Web インターフェイスに表示されます。スタック構成内の他のすべてのデバイスはセカンダリであり、Web インターフェイスでセカンダリ ロールとして表示されます。スタック済みデバイスからの情報を表示する場合を除き、統合されたリソースは 1 つのエンティティとして扱われます。

単一の 3D8140、3D8250、または 3D8350 を接続する場合と同じ方法で、分析対象のネットワーク セグメントにプライマリ デバイスを接続します。スタック配線図に示すように、セカンダリ デバイスをプライマリ デバイスに接続します。

ネットワーク セグメントおよび他のデバイスとの間の物理接続が完了した後、防御センターを使用してスタックを設定し、管理します。

以下の項では、スタック構成デバイスを接続して管理する方法について詳しく説明します。

- 「3D8140 の接続」（P.3-16）
- 「82xx ファミリ と 83xx ファミリ の接続」（P.3-16）
- 「8000 シリーズ スタッキング ケーブルの使用」（P.3-19）
- 「スタック構成デバイスの管理」（P.3-20）

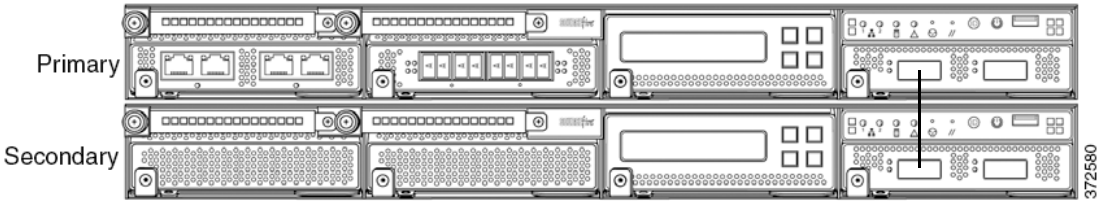
3D8140 の接続

2 つの 3D8140 をスタック構成で接続できます。1 本の 8000 シリーズ スタッキング ケーブルを使用して、プライマリ デバイスとセカンダリ デバイスの間の物理接続を確立する必要があります。スタッキング ケーブルの使用方法については、「8000 シリーズ スタッキング ケーブルの使用」（P.3-19）を参照してください。

スタッキング モジュール間をケーブルで容易に接続できるように、各デバイスをラックに設置します。プライマリ デバイスの上または下にセカンダリ デバイスを設置できます。

単一の 3D8140 を接続する場合と同じ方法で、分析対象のネットワーク セグメントにプライマリ デバイスを接続します。セカンダリ デバイスをプライマリ デバイスに直接接続します。

下の図に、プライマリ デバイスの下にセカンダリ デバイスを設置した状態を示します。



3D8140 セカンダリ デバイスを接続する方法：

ステップ 1　8000 シリーズ スタッキング ケーブルを使用して、プライマリ デバイス上の左側のスタッキング インターフェイスを、セカンダリ デバイス上の左側のスタッキング インターフェイスに接続します。その後、デバイスを管理する防御センターを使用して、システム内のスタック構成デバイスの関係を構築します。右側のスタッキング インターフェイスが接続されていないことに注意してください。「スタック構成デバイスの管理」（P.3-20）を参照してください。

82xx ファミリ と 83xx ファミリ の接続

次に示すいずれかの構成で接続することができます。

- 最大で 4 つの 3D8250 または 3D8350
- 1 つの 3D8260（1 つの 10G 対応プライマリ デバイスと 1 つのセカンダリ デバイス）
- 1 つの 3D8360（1 つの 40G 対応プライマリ デバイスと 1 つのセカンダリ デバイス）
- 1 つの 3D8270 または 3D8370（1 つの 40G 対応プライマリ デバイスと 2 つのセカンダリ デバイス）
- 1 つの 3D8290 または 3D8390（1 つの 40G 対応プライマリ デバイスと 3 つのセカンダリ デバイス）

3D8260、3D8270、3D8360、および 3D8370 では、追加のデバイスをスタックして、合計 4 デバイスからなるスタックにすることができます。

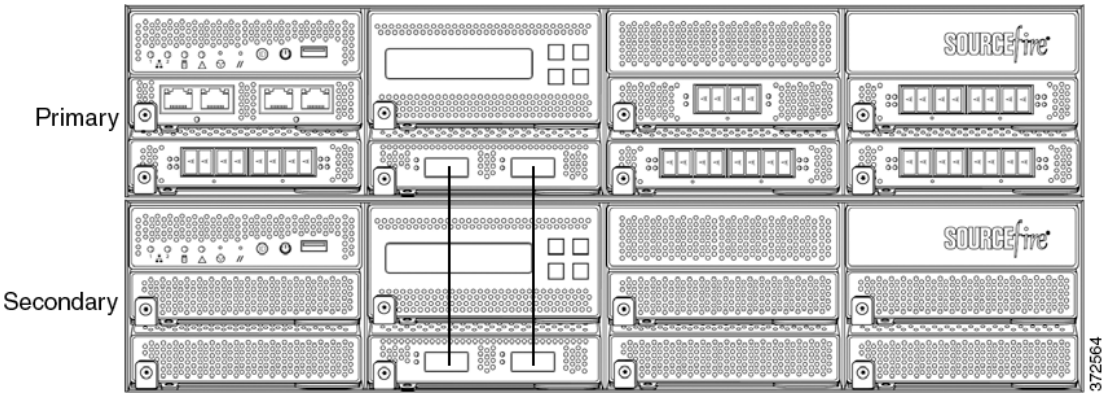
プライマリ デバイスに接続するセカンダリ デバイスごとに、2 本ずつの 8000 シリーズ スタッキング ケーブルを使用する必要があります。スタッキング ケーブルの使用方法については、「8000 シリーズ スタッキング ケーブルの使用」（P.3-19）を参照してください。

スタッキング モジュール間をケーブルで容易に接続できるように、各デバイスをラックの中に設置します。プライマリ デバイスの上または下に、セカンダリ デバイスを設置できます。

単一の 3D8250 または 3D8350 を接続する場合と同じ方法で、分析対象のネットワーク セグメントにプライマリ デバイスを接続します。設定で必要とされるセカンダリ デバイスの数に応じて、それぞれをプライマリ デバイスに直接接続します。

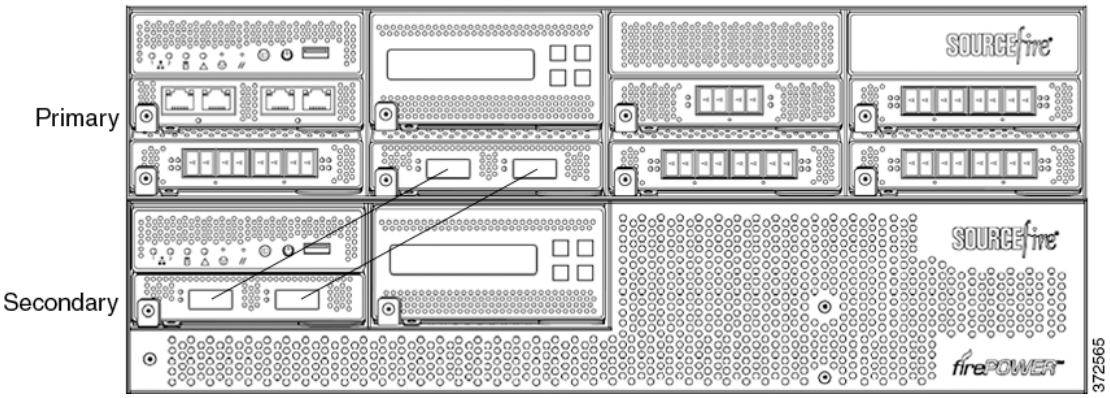
3D8250 または 3D8350 プライマリ デバイスと 1 つのセカンダリ デバイス

次に、3D8250 または 3D8350 プライマリ デバイスと 1 つのセカンダリ デバイスの例を示します。セカンダリ デバイスがプライマリ デバイスの下に設置されています。セカンダリ デバイスにはセンシング インターフェイスが含まれていないことに注意してください。



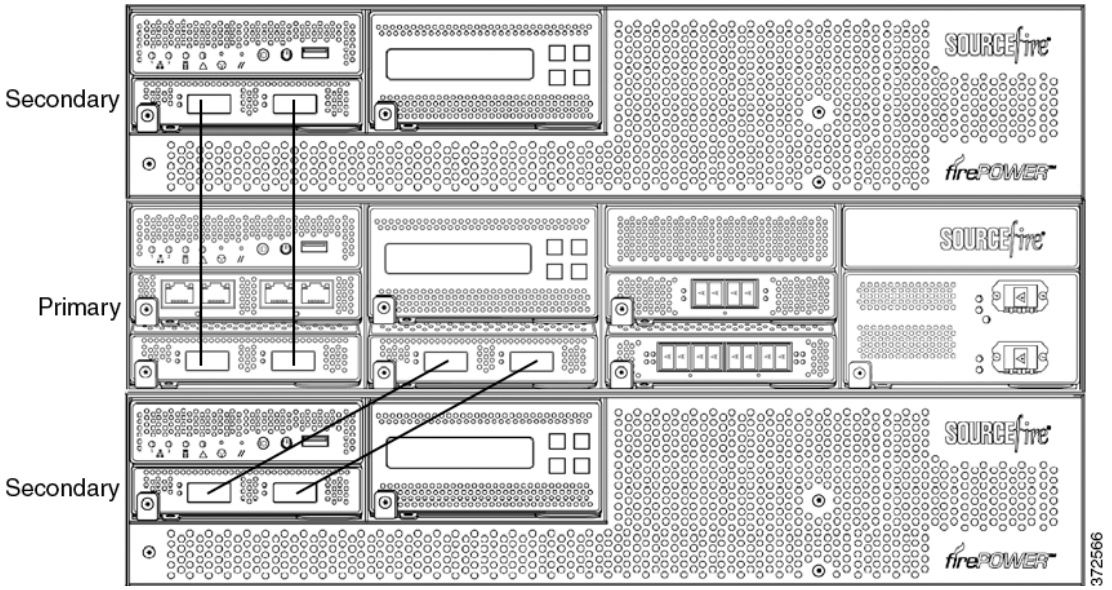
3D8260 または 3D8360 プライマリ デバイスと 1 つのセカンダリ デバイス

次に、3D8260 または 3D8360 の設定例を示します。3D8260 には 10G 対応 3D8250 プライマリ デバイスと 1 つの専用セカンダリ デバイスが含まれています。3D8360 には 40G 対応 3D8350 プライマリ デバイスと 1 つの専用セカンダリ デバイスが含まれています。両方の設定（3D8260 または 3D8360）で、セカンダリ デバイスがプライマリ デバイスの下に設置されます。



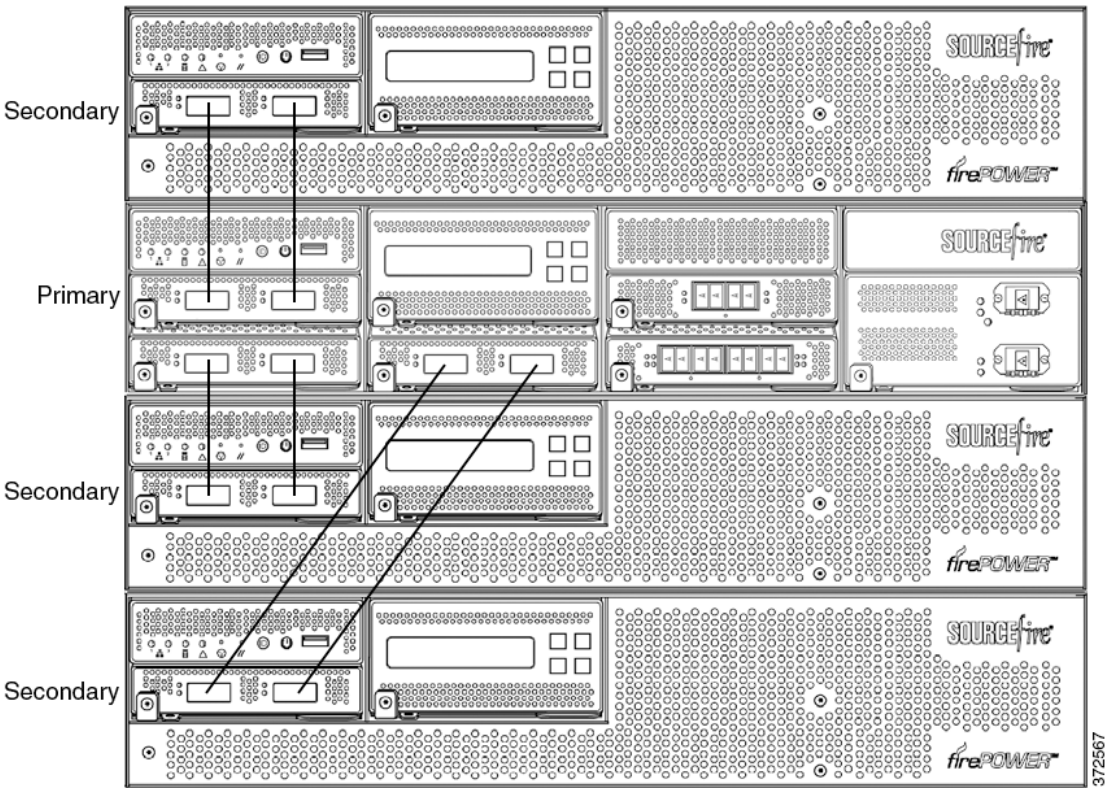
3D8270 または 3D8370 プライマリ デバイス（40G）と 2 つのセカンダリ デバイス

次に、3D8270 または 3D8370 の設定例を示します。3D8270 には 40G 対応 3D8250 プライマリ デバイスと 2 つの専用セカンダリ デバイスが含まれています。3D8370 には 40G 対応 3D8350 プライマリ デバイスと 2 つの専用セカンダリ デバイスが含まれています。両方の設定（3D8270 または 3D8370）で、1 つのセカンダリ デバイスがプライマリ デバイスの上に設置され、他のセカンダリ デバイスがプライマリ デバイスの下に設置されます。



3D8290 または 3D8390 プライマリ デバイス（40G）と 3 つのセカンダリ デバイス

次に、3D8290 または 3D8390 の設定例を示します。3D8290 には 40G 対応 3D8250 プライマリ デバイスと 3 つの専用セカンダリ デバイスが含まれています。3D8370 には 40G 対応 3D8350 プライマリ デバイスと 2 つの専用セカンダリ デバイスが含まれています。両方の設定（3D8290 または 3D8390）で、1 つのセカンダリ デバイスがプライマリ デバイスの上に設置され、2 つのセカンダリ デバイスがプライマリ デバイスの下に設置されます。



3D8250 または 3D8350 セカンダリ デバイスを接続する方法：

ステップ 1　8000 シリーズ スタッキング ケーブルを使用して、プライマリ デバイス上のスタッキング モジュールの左側のインターフェイスを、セカンダリ デバイス上のスタッキング モジュールの左側のインターフェイスに接続します。

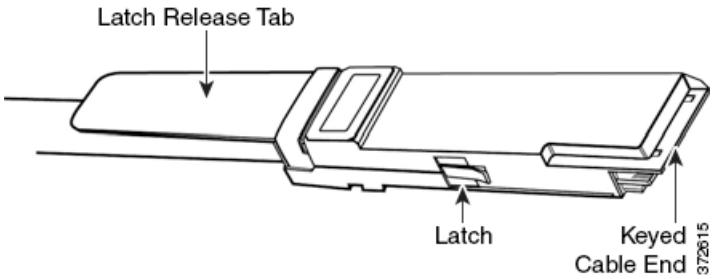
ステップ 2　2 本目の 8000 シリーズ スタッキング ケーブルを使用して、プライマリ デバイス上のスタッキング モジュールの右側のインターフェイスを、セカンダリ デバイス上のスタッキング モジュールの右側のインターフェイスに接続します。

ステップ 3　接続するセカンダリ デバイスごとにステップ 1 と 2 を繰り返します。

ステップ 4　デバイスを管理する防御センターを使用して、スタック構成デバイスの関係を構築し、統合リソースを管理します。「スタック構成デバイスの管理」（P.3-20）を参照してください。

8000 シリーズ スタッキング ケーブルの使用

8000 シリーズ スタッキング ケーブルは両方の先端が同じ鍵型になっており、デバイスにケーブルを固定するためのラッチとラッチ解放つまみがそれぞれ付いています。



8000 シリーズ スタッキング ケーブルを使用して、以下に示すデバイス設定の必要に応じて、プライマリ デバイスと各セカンダリ デバイスの間の物理接続を確立します。

- 3D8250、3D8260、3D8270、および 3D8290 では接続ごとに 2 本ずつケーブルが必要です
- 3D8350、3D8360、3D8370、および 3D8390 では接続ごとに 2 本ずつケーブルが必要です
- 3D8140 では 1 本のケーブルが必要です

スタッキング ケーブルの取り付けまたは取り外し時にデバイスの電源をオフにする必要はありません。

注意　デバイスを配線するときには、シスコ 8000 シリーズ スタッキング ケーブルだけを使用してください。サポートされていないケーブルを使用すると予期しないエラーが発生する可能性があります。

デバイスを物理的に接続したら、防御センターを使用して、スタック済みデバイスを管理します。

8000 シリーズ スタッキング ケーブルを挿入する方法：

ステップ 1　ケーブルを挿入するには、解放つまみを上にした状態でケーブル先端を持ち、鍵型の先端部分をスタッキング モジュール上のポートに差し込んで、ラッチがカチッと鳴るまで押し込みます。

8000 シリーズ スタッキング ケーブルを取り外す方法：

ステップ 1　ケーブルを取り外すには、解放つまみを引っ張ってラッチを解放した後、ケーブルの先端を引き抜きます。

スタック構成デバイスの管理

防御センターはデバイス間のスタック関係を構築し、プライマリ デバイスのインターフェイス セットを制御し、スタック内の統合リソースを管理します。スタック済みデバイスのローカル Web インターフェイス上でインターフェイス セットを管理することはできません。

スタック関係が構築されると、すべてのデバイスは単一の、共有される検出設定を使ってトラフィックを個別に検査します。プライマリ デバイスで障害が発生した場合は、プライマリ デバイスの設定に従って（つまりスタック関係が存在しない場合と同じ方法で）トラフィックが処理されます。セカンダリ デバイスで障害が発生した場合、プライマリ デバイスは引き続きトラフィックを検知し、アラートを生成して、障害発生中のセカンダリ デバイスにトラフィックを送り、そこでトラフィックが破棄されます。

スタック済みデバイスを構築および管理する方法については、『*FireSIGHT System User Guide*』の「スタック デバイスの管理」を参照してください。

ラックへのアプライアンスの取り付け

FireSIGHT システム は、さまざまなハードウェア プラットフォームで出荷されます。すべての FireSIGHT システム アプライアンスをラックマウントできます（3D7010、3D7020、および 3D7030 用の 1 U 取り付けキットを購入した場合）。また、アプライアンスを設置したときには、アプライアンスのコンソールにアクセスできることを確認する必要もあります。初期セットアップ用にコンソールにアクセスするには、次のいずれかの方法で 1 つの FireSIGHT システム アプライアンスに接続します。

キーボードとモニタ/KVM

USB キーボードと VGA モニタを任意の FireSIGHT システム アプライアンスに接続できます。キーボード、ビデオ、およびマウス（KVM）スイッチに接続されたアプライアンスをラックマウントするには、これが便利です。

注意　アプライアンスは大容量ストレージ デバイスをブート デバイスとして使用する可能性があるため、初期セットアップのためにアプライアンスにアクセスするときには、KVM コンソールと一緒に USB 大容量ストレージを**使用しない**でください。

管理インターフェイスへのイーサネット接続

次のネットワーク設定を使用して、インターネットに接続してはならないローカル コンピュータを設定します。

- IP アドレス：`192.168.45.2`
- ネットマスク：`255.255.255.0`

- デフォルト ゲートウェイ：192.168.45.1

  イーサネット ケーブルを使用して、ローカル コンピュータのネットワーク インターフェイスをアプライアンス上の管理インターフェイスに接続します。アプライアンスとの対話には、HyperTerminal や Xmodem などのターミナル エミュレーション ソフトウェアを使用します。このソフトウェア用の設定は次のとおりです。

- 9600 ボー
- 8 データ ビット
- パリティ チェックなし
- 1 ストップ ビット
- フロー制御なし

  物理 FireSIGHT システム アプライアンス上の管理インターフェイスは、デフォルト IPv4 アドレスで事前設定されていることに注意してください。ただし、セットアップ手順の一部として、管理インターフェイスを IPv6 アドレスで再設定できます。

初期セットアップ後に、次に示す追加の方法でコンソールにアクセスできます。

シリアル接続/ラップトップ

物理シリアル ポートを使用して、コンピュータを（3D2100/2500/3500/4500 デバイス以外の）任意の FireSIGHT システム アプライアンスに接続できます。適切なロールオーバー シリアル ケーブル（ヌル モデム ケーブルまたはシスコ コンソール ケーブルとも呼ばれる）を常に接続した状態で、デフォルト VGA 出力をシリアル ポートにリダイレクトするようリモート管理コンソールを設定してください。アプライアンスと対話するには、上記のとおり端末エミュレーション ソフトウェアを使用します。

シリアル ポートには、アプライアンスによって RJ-45 接続と DB-9 接続のどちらかが実装されています。アプライアンス別のコネクタについては、次の表を参照してください。

表 3-1　　モデル別のシリアル コネクタ

アプライアンス	コネクタ
3D500/1000/2000	DB-9（メス）
3D6500	RJ-45
シリーズ 3 の防御センター	RJ-45
3D70xx ファミリ	RJ-45
3D71xx ファミリ	DB-9（メス）
3D8000 シリーズ	RJ-45
3D9900	RJ-45

適切なロールオーバー ケーブルをデバイスに接続した後、「コンソール出力のリダイレクト」（P.3-23）に記載されているようにコンソール出力をリダイレクトします。各アプライアンスのシリアル ポートを特定するには、「ハードウェア仕様」（P.6-1）の図を使用してください。

Serial over LAN（SOL）を使用する Lights-Out Management（LOM）

LOM 機能を使用すると、SOL 接続を通して シリーズ 3 アプライアンスに対して限定的なアクション セットを実行できます。LOM に対応したアプライアンスを出荷時の初期状態に復元する必要があり、そのアプライアンスに物理的にアクセスできない場合は、LOM を使用して復元プロセスを実行できます。LOM を使用してアプライアンスに接続した後、物理シリアル接続を使用する場合と同じ方法で、復元ユーティリティにコマンドを発行します。詳細については、「Lights-Out Management の設定」（P.7-20）を参照してください。

LOM を使用してアプライアンスを工場出荷時設定に復元するには、ネットワーク設定を削除**しないでください**。ネットワーク設定を削除すると、LOM 接続もドロップされます。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。

アプライアンスを設置する方法：

ステップ 1　取り付けキットと付属の手順書を使用して、アプライアンスをラックに取り付けます。

ステップ 2　キーボードとモニタまたはイーサネット接続を使用してアプライアンスに接続します。

ステップ 3　キーボードとモニタを使用してアプライアンスをセットアップしている場合は、ここでイーサネット ケーブルを使用して、保護されるネットワーク セグメントに管理インターフェイスを接続します。

コンピュータをアプライアンスの物理管理インターフェイスに直接接続することによって初期セットアップ手順を実行する予定の場合は、セットアップの完了時点で、保護されるネットワークに管理インターフェイスを接続します。

ステップ 4　管理対象デバイスの場合は、インターフェイスに合わせて適切なケーブルを使用して、分析対象のネットワーク セグメントにセンシング インターフェイスを接続します。

- 銅線センシング インターフェイス：デバイスに銅線センシング インターフェイスが含まれている場合は、必ず適切なケーブルを使用してネットワークに接続します（「銅線インターフェイスのインライン展開のケーブル配線」（P.2-7）を参照）。
- 光ファイバ アダプタ カード：光ファイバ アダプタ カードが実装されたデバイスの場合は、オプションのマルチモード ファイバ ケーブルの LC コネクタをアダプタ カード上の 2 つのポートに任意の順序で接続します。分析対象のネットワーク セグメントに SC プラグを接続します。
- ファイバ タップ：オプションの光ファイバ タップが実装されたデバイスを展開している場合は、オプションのマルチモード ファイバ ケーブルの SC プラグを、タップ上の「analyzer」ポートに接続します。分析対象のネットワーク セグメントにタップを接続します。
- 銅線タップ：オプションの銅線タップが実装されたデバイスを展開している場合は、タップの左側にある A ポートと B ポートを、分析対象のネットワーク セグメントに接続します。タップの右側にある A ポートと B ポート（「analyzer」ポート）をアダプタ カード上の 2 つの銅線ポートに接続します。

  管理対象デバイスを展開するときのオプションの詳細については、「展開について」（P.2-1）を参照してください。

  バイパス インターフェイスが実装されたデバイスを展開している場合は、デバイスで障害が発生してもネットワーク接続を維持できるデバイス機能を活用できます。設置と遅延のテストについては、「インライン バイパス インターフェイス設置のテスト」（P.3-24）を参照してください。

ステップ 5　電源コードをアプライアンスに接続し、電力源に差し込みます。

アプライアンスに冗長電源がある場合は、電源コードを両方の電源に接続し、それを別々の電力源に差し込みます。

ステップ 6　アプライアンスの電源をオンにします。

直接イーサネット接続を使用してアプライアンスをセットアップする場合は、ローカル コンピュータ上のネットワーク インターフェイスとアプライアンス上の管理インターフェイスの両方のリンク LED が点灯していることを確認してください。管理インターフェイスとネットワーク インターフェイスの LED が点灯していない場合は、クロス ケーブルを使用してみてください。詳細については、「銅線インターフェイスのインライン展開のケーブル配線」（P.2-7）を参照してください。

ステップ 7　次の章（「FireSIGHT システム アプライアンスのセットアップ」（P.4-1））に進みます。

コンソール出力のリダイレクト

デフォルトで、FireSIGHT システム アプライアンスは初期化ステータス *init* メッセージを VGA ポートに出力します。アプライアンスを工場出荷時設定に復元し、そのライセンスとネットワークの設定を削除すると、コンソール出力も復元ユーティリティによって VGA にリセットされます。物理シリアル ポートまたは SOL を使用してコンソールにアクセスする必要がある場合、初期セットアップの完了後にコンソール出力をシリアル ポートにリダイレクトすることをシスコでは推奨しています。

シェルを使用してコンソール出力をリダイレクトするには、アプライアンスのシェルからスクリプトを実行します。次の表に、アプライアンスへのアクセス方法に応じて使用すべきコンソール設定を一覧表示します。

表 3-2　　コンソール リダイレクト オプション

オプション	設定
VGA（デフォルト）	`tty0`
物理シリアル	`ttyS0`
SOL を介した LOM	`ttyS0`

すべての シリーズ 3 アプライアンスが LOM をサポートしますが、7000 シリーズ デバイスは LOM と物理シリアル アクセスを同時にサポートしないことに注意してください。ただし、どちらを使用してもコンソール設定は同じです。

シェルを使用してコンソール出力をリダイレクトする方法：

アクセス：Admin

ステップ 1　キーボード/モニタまたはシリアル接続を使用し、管理者特権を持つアカウントでアプライアンスのシェルにログインします。パスワードは、アプライアンスの Web インターフェイスのパスワードと同じです。

シリーズ 3 または仮想管理対象デバイス上では、「`expert`」と入力してシェル プロンプトを表示させる必要があることに注意してください。

アプライアンスのプロンプトが表示されます。

ステップ 2　プロンプトで、次のコマンドを入力して root ユーザとしてコンソール出力を設定します。

```
sudo /usr/local/sf/bin/set_console.sh -c console_value
```

ここで、*`console_value`* は表 3-2（P.3-23）に記載されているように、アプライアンスへのアクセス方法を示す設定値です。

ステップ 3　変更を反映させるには、「`sudo reboot`」と入力してアプライアンスをリブートします。

アプライアンスがリブートします。

インライン バイパス インターフェイス設置のテスト

バイパス インターフェイスを備えた管理対象デバイスは、デバイスが電源オフまたは動作不能な状態になってもネットワーク接続を維持できます。このようなデバイスを必ず適切に設置し、設置により生じた遅延を計測することが重要です。

（注）　スイッチのスパニング ツリー ディスカバリ プロトコルは 30 秒のトラフィック遅延を引き起こす可能性があります。シスコでは、次の手順でスパニング ツリーを無効にすることを推奨します。

銅線インターフェイスにのみ適用される次の手順では、インライン バイパス インターフェイスの設置と ping 遅延をテストする方法について説明します。ping テストを実行するためにネットワークに接続し、管理対象デバイス コンソールに接続する必要があります。

インライン バイパス インターフェイスが設置されたデバイスをテストする方法：

アクセス：Admin

ステップ 1　アプライアンスのインターフェイス セット タイプがインライン バイパス モード用に設定されていることを確認します。

インターフェイス セットをインライン バイパス モード用に設定する手順については、『*FireSIGHT System User Guide*』の「インライン セットの設定」を参照してください。

ステップ 2　スイッチ上のすべてのインターフェイス、ファイアウォール、およびデバイスのセンシング インターフェイスを自動ネゴシエーションに設定します。

（注）　シスコ デバイスでは、自動 MDIX を使用する場合に自動ネゴシエーションが必要です。

ステップ 3　デバイスの電源をオフにして、すべてのネットワーク ケーブルを外します。

デバイスを再接続して、適切なネットワーク接続が存在することを確認します。デバイスからスイッチおよびファイアウォールへのクロスオーバー ケーブルとストレート ケーブルの配線手順をチェックします（「銅線インターフェイスのインライン展開のケーブル配線」（P.2-7）を参照）。

ステップ 4　デバイスの電源をオフにして、ファイアウォールからデバイス経由でスイッチに ping できることを確認します。

ping が失敗した場合は、ネットワーク配線を修正します。

ステップ 5　ステップ 10 が完了するまで、継続的に ping を実行します。

ステップ 6　デバイスの電源を再びオンにします。

ステップ 7　キーボード/モニタまたはシリアル接続を使用し、管理者特権を持つアカウントでデバイスにログインします。パスワードは、デバイスの Web インターフェイスのパスワードと同じです。

デバイスのプロンプトが表示されます。

ステップ 8　「`system shutdown`」と入力して、デバイスをシャットダウンします。

また、Web インターフェイスを使用してデバイスをシャットダウンすることもできます。『*FireSIGHT System User Guide*』の「デバイスの管理」の章を参照してください。ほとんどのデバイスで電源をオフにすると、カチッという音がします。この音は、リレーが切り替わって、デバイスがハードウェア バイパスに移行した音です。

ステップ 9　30 秒間待機します。

ping トラフィックが再開したことを確認します。

ステップ 10　デバイスの電源を再びオンにして、ping トラフィックが継続的に通過していることを確認します。

ステップ 11　タップ モードをサポートするアプライアンスの場合は、次の条件下で ping 遅延結果をテストして記録できます。

- デバイスの電源がオフ
- デバイスの電源がオン、ポリシーにルールが適用されていない、インライン侵入ポリシー保護モード
- デバイスの電源がオン、ポリシーにルールが適用されていない、インライン侵入ポリシー保護タップ モード
- デバイスの電源がオン、ポリシーに調整済みルールが適用されている、インライン侵入ポリシー保護モード

遅延時間が設置における許容範囲内であることを確認します。過剰な遅延が発生する問題の解決方法については、『*FireSIGHT System User Guide*』の「パケット遅延しきい値の設定」および「ルール遅延しきい値について」を参照してください。

FireSIGHT システム アプライアンスのセットアップ

アプライアンスを展開して設置した後、信頼された管理ネットワーク上で新しいアプライアンスが通信できるよう、セットアップ手順を実行する必要があります。また、管理者パスワードを変更し、エンド ユーザ ライセンス契約書（EULA）に同意する必要もあります。

さらにセットアップ手順では、時刻の設定、デバイスの登録とライセンス認証、更新のスケジューリングなど、さまざまな初期管理レベルのタスクも実行できます。セットアップと登録の時点で選択したオプションにより、システムで作成/適用されるデフォルト インターフェイス、インライン セット、ゾーン、およびポリシーが決定されます。

これらの初期設定とポリシーの目的は、オプションを制限することではなく、アウトオブザボックス エクスペリエンスを提供し、展開のセットアップ時間を短縮することです。デバイスがどのように初期設定されるかとは無関係に、防御センターを使用してデバイスの設定をいつでも変更できます。つまり、セットアップ時にたとえば検出モードやアクセス コントロール ポリシーを選択した場合でも、特定のデバイス、ゾーン、ポリシー設定に固定されることはありません。

（注） ASA FirePOWER デバイスのセットアップ方法については、ASA マニュアルを参照してください。

初期セットアップ手順の各ステップの詳細については、以下の項を参照してください。

- 「セットアップ手順について」（P.4-2）ではセットアップ手順の概要について説明します。これは、アプライアンスのモデルと、アプライアンスに物理的にアクセスできるかどうかによって異なります。

（注） セットアップ手順をまだ理解していない場合、シスコはこの項を最初に読むことを**強く**推奨します。

- 「スクリプトを使用したネットワークの設定」（P.4-4）では、スクリプトを使用することで、新しいアプライアンスを管理ネットワーク上で通信可能にするためのネットワーク設定の指定方法について説明します。キーボードとモニタを使ってアクセスするすべての防御センターに関して、このステップを行う必要があります。
- 「CLI を使用して シリーズ 3 デバイスで初期セットアップを実行する」（P.4-6）では、対話形式のコマンドライン インターフェイス（CLI）を使用して、シリーズ 3 デバイス上でセットアップ手順を実行する方法について説明します。
- 「初期セットアップ ページ：デバイス」（P.4-8）では、デバイスの Web インターフェイスを使用して、その初期セットアップを完了する方法について説明します。

- 「初期セットアップ ページ：防御センター」（P.4-12）では、防御センターの Web インターフェイスを使用して、その初期セットアップを完了する方法について説明します。
- 「次の手順」（P.4-17）には、FireSIGHT システム展開のセットアップ時に実行することのできるセットアップ後タスクについてのガイダンスを示します。

注意 この章の手順では、アプライアンスの電源をオフにせずにセットアップする方法について説明します。ただし、何らかの理由で電源をオフにする必要がある場合は、『*FireSIGHT System User Guide*』の「デバイスの管理」の章に記載された手順、シリーズ 3 デバイス上の CLI での `system shutdown` コマンド、あるいはアプライアンスのシェル（エキスパート モードとも呼ばれる）での `shutdown -h now` コマンドを使用してください。

セットアップ手順について

これまでの章の説明に従って新しい FireSIGHT システム アプライアンスを展開して設置した後、セットアップ手順を実行する必要があります。セットアップを開始する前に、次の要件が満たされていることを確認してください。

アプライアンス モデル

どのアプライアンスをセットアップするか理解している必要があります。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*、または管理する側の *防御センター* のどちらかです。アプライアンス タイプごとに複数の *モデル* が存在し、これらのモデルはさらに *シリーズ* と *ファミリ* にグループ分けされます。詳細については、「FireSIGHT システム アプライアンス」（P.1-2）を参照してください。

アクセス

新しいアプライアンスをセットアップするには、キーボードとモニタ/KVM（キーボード、ビデオ、マウス）、または直接イーサネット接続を使用してアプライアンスの管理インターフェイスに接続する必要があります。初期セットアップ後に、アプライアンスをシリアル アクセス用に設定できます。詳細については、「ラックへのアプライアンスの取り付け」（P.3-20）を参照してください。

（注） アプライアンスは大容量ストレージ デバイスをブート デバイスとして使用する可能性があるため、初期セットアップのためにアプライアンスにアクセスするときには、KVM コンソールと一緒に USB 大容量ストレージを**使用しない**でください。

情報

アプライアンスが管理ネットワーク上で通信できるようになるために必要な最低限の情報は、IPv4 または IPv6 管理 IP アドレス、ネットマスクまたはプレフィクス長、およびデフォルト ゲートウェイです。

アプライアンスの展開方法がわかっている場合、セットアップ手順は、さまざまな初期管理レベルのタスク（登録とライセンス認証など）を実行する良い機会にもなります。

ヒント 複数のアプライアンスを展開する場合は、まずデバイスをセットアップした後で、それらを管理する防御センターをセットアップします。デバイスの初期セットアップ手順では、デバイスを防御センターに事前登録できます。防御センターのセットアップ手順では、事前登録した管理対象デバイスを追加してライセンス認証できます。

セットアップが完了したら、防御センターの Web インターフェイスを使用して、展開用のほとんどの管理タスクと分析タスクを実行します。管理対象の物理デバイスに備わっている制限付き Web インターフェイスを使用すると、基本的な管理だけを実行できます。詳細については、「次の手順」（P.4-17）を参照してください。

アプライアンス タイプごとのセットアップ方法については、詳しくは以下を参照してください。

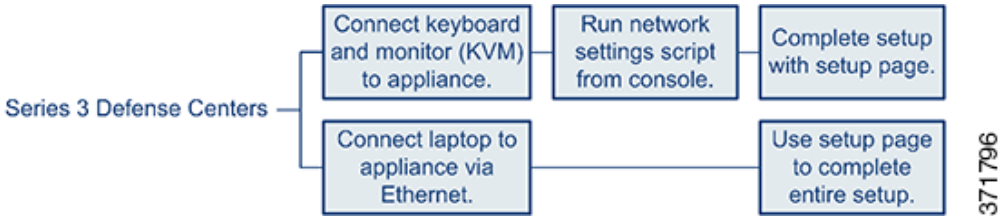
- 「シリーズ 3 防御センターのセットアップ」（P.4-3）
- 「シリーズ 3 デバイスのセットアップ」（P.4-4）

ヒント　工場出荷時設定に復元された後のアプライアンスをセットアップしている場合（「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）、アプライアンスのライセンスとネットワーク設定がまだ削除済みでなければ、管理ネットワーク上のコンピュータを使ってアプライアンスの Web インターフェイスを直接参照し、セットアップを実行できます。「初期セットアップ ページ：デバイス」（P.4-8）、または「初期セットアップ ページ：防御センター」（P.4-12）に進んでください。

シリーズ 3 防御センターのセットアップ

サポートされる防御センター：シリーズ 3

次の図は、シリーズ 3 防御センターをセットアップするときの選択肢を示しています。



シリーズ 3 防御センターをセットアップする方法：

アクセス：Admin

ステップ 1　キーボードとモニタを使用している場合は、アプライアンスを管理ネットワーク上で通信可能にするための設定を容易にするスクリプトを実行します（「スクリプトを使用したネットワークの設定」（P.4-4）を参照）。

再イメージングしたアプライアンスをセットアップするときに、復元手順の一部としてネットワーク設定が維持されている場合、または、直接イーサネット接続でアプライアンスにアクセスする場合は、次の手順に進みます。

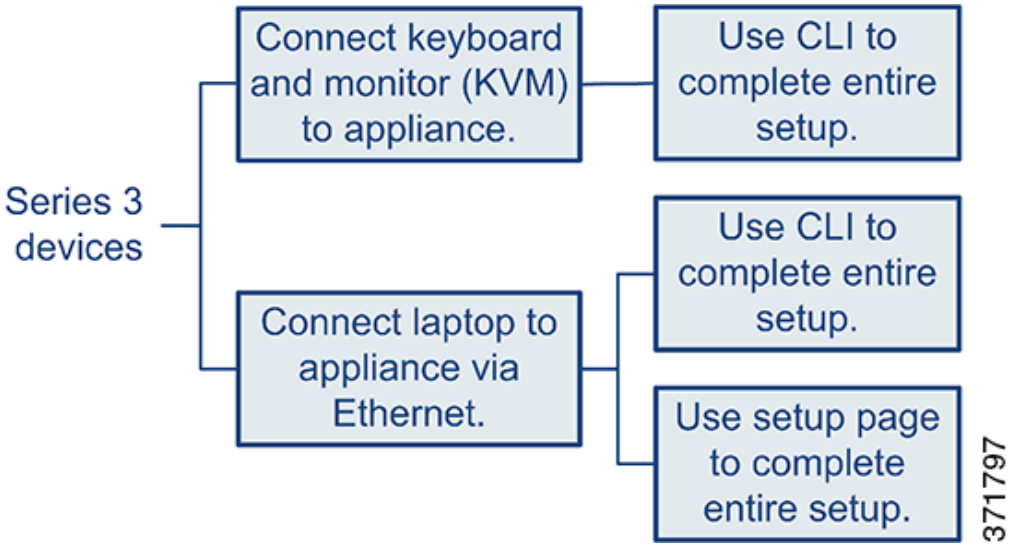
ステップ 2　管理ネットワーク上のコンピュータからアプライアンスの Web インターフェイスを参照することにより、セットアップ手順を完了します。

- 管理対象デバイスの Web インターフェイスを使用して、そのデバイスのセットアップを完了するには、「初期セットアップ ページ：デバイス」（P.4-8）を参照してください。
- 防御センターの Web インターフェイスを使用して、そのセットアップを完了するには、「初期セットアップ ページ：防御センター」（P.4-12）を参照してください。

シリーズ 3 デバイスのセットアップ

サポートされるデバイス：シリーズ 3

次の図は、シリーズ 3 デバイスをセットアップするときの選択肢を示しています。



シリーズ 3 デバイスへのアクセス方法により、そのセットアップ方法が決まります。次の選択肢があります。

- デバイスへの接続方法とは無関係に、CLI を使用してデバイスをセットアップできます（「CLI を使用して シリーズ 3 デバイスで初期セットアップを実行する」（P.4-6）を参照）。
- 直接イーサネット接続でアプライアンスにアクセスする場合は、ローカル コンピュータからアプライアンスの Web インターフェイスを参照できます（「初期セットアップ ページ：デバイス」（P.4-8）を参照）。

再イメージングしたデバイスをセットアップするときに、復元手順の一部としてネットワーク設定が維持されている場合は、SSH または Lights-Out Management（LOM）接続で CLI にアクセスできます。また、管理ネットワーク上のコンピュータからデバイスの Web インターフェイスを参照することもできます。

スクリプトを使用したネットワークの設定

サポートされるデバイス：シリーズ 2

新しい防御センターまたは シリーズ 2 のデバイスを設置した後、または再イメージングの一部としてネットワーク設定を削除した後には、管理ネットワーク上で通信できるようにアプライアンスを設定する必要があります。コンソールでスクリプトを実行することにより、このステップが完了します。

FireSIGHT システムでは、IPv4 と IPv6 の両方の管理環境のためのデュアルスタック実装が提供されています。スクリプトは、まず IPv4 管理を設定（または無効化）するよう要求して、その後に IPv6 の設定を要求します。IPv6 展開の場合は、ローカル ルータから設定値を取得できます。IPv4 または IPv6 管理 IP アドレス、ネットマスクまたはプレフィックス長、およびデフォルト ゲートウェイを指定する必要があります。

スクリプトのプロンプトに従って操作するとき、多岐選択方式の質問に対する選択肢は (y/n) のようにカッコ内に表示されます。デフォルトは [y] のように大カッコ内に表示されます。Enter キーを押すと選択が確定します。

なお、スクリプトでは、アプライアンスのセットアップ Web ページとほぼ同じセットアップ情報が要求されます。詳細については、「ネットワーク設定」（P.4-9）（デバイス）および「ネットワーク設定」（P.4-14）（防御センター）を参照してください。

スクリプトを使用してネットワークを設定する方法：

アクセス：Admin

ステップ 1　コンソールで、アプライアンスにログインします。ユーザ名として admin、パスワードとしてシスコ を使用します。

シリーズ 3 または仮想管理対象デバイス上では、「expert」と入力してシェル プロンプトを表示させる必要があることに注意してください。

ステップ 2　admin プロンプトで、次のスクリプトを実行します。

```
sudo /usr/local/sf/bin/configure-network
```

ステップ 3　スクリプトのプロンプトに従ってください。

最初に IPv4 管理を設定（または無効化）してから、IPv6 の設定に移ります。ネットワーク設定を手動で指定する場合は、以下の手順を実行する必要があります。

- ネットマスクを含む IPv4 アドレスを、ドット付き 10 進数形式で入力します。たとえば 255.255.0.0 というネットマスクを指定できます。
- IPv6 アドレスを、コロン区切りの 16 進数形式で入力します。IPv6 プレフィックスの場合、ビット数を指定します（たとえば 112 のプレフィックス長）。

ステップ 4　設定が正しいことを確認します。

設定を誤って入力した場合は、プロンプトで「n」と入力して Enter キーを押します。その後、正しい情報を入力できます。設定が実装されるときに、コンソールにメッセージが表示される場合があります。

ステップ 5　アプライアンスからログアウトします。

ステップ 6　次のステップは、アプライアンスによって以下のように異なります。

- 管理対象デバイスの Web インターフェイスを使用して、そのデバイスのセットアップを完了するには、「初期セットアップ ページ：デバイス」（P.4-8）に進みます。
- 防御センターの Web インターフェイスを使用して、そのセットアップを完了するには、「初期セットアップ ページ：防御センター」（P.4-12）に進みます。

CLI を使用して シリーズ 3 デバイスで初期セットアップを実行する

サポートされるデバイス：シリーズ 3

オプションで、デバイスの Web インターフェイスを使用する代わりに、CLI を使って シリーズ 3 デバイスを設定できます。新しく設定するデバイスに、CLI を使って初めてログインするときには、EULA を読んでそれに同意する必要があります。その後、セットアップ プロンプトに従って管理パスワードを変更し、デバイスのネットワーク設定と検出モードを設定します。最後に、デバイスを管理する防御センターにデバイスを登録します。

セットアップ プロンプトに従って操作するとき、オプションは `(y/n)` のようにカッコ内に表示されます。デフォルトは `[y]` のように大カッコ内に表示されます。Enter キーを押すと選択が確定します。

なお、CLI では、デバイスのセットアップ Web ページとほぼ同じセットアップ情報が要求されます。これらのオプションの詳細については、「初期セットアップ ページ：デバイス」（P.4-8）を参照してください。

CLI を使用して シリーズ 3 デバイスで初期セットアップを完了する方法：

アクセス：Admin

ステップ 1　デバイスにログインします。ユーザ名として `admin`、パスワードとして シスコ を使用します。

- キーボードとモニタが接続された シリーズ 3 デバイスの場合は、コンソールからログインします。
- イーサネット ケーブルを使用して シリーズ 3 デバイスの管理インターフェイスにコンピュータを接続した場合は、インターフェイスのデフォルト IPv4 アドレス（192.168.45.45）に SSH します。

  ただちに、EULA を読むようデバイスから要求されます。

ステップ 2　EULA を読んでそれに同意します。

ステップ 3　`admin` アカウントのパスワードを変更します。このアカウントには管理者特権が付与されているため、削除できません。

このパスワードを使用すると、`admin` ユーザはデバイスの Web インターフェイスとその CLI にログインできます。`admin` ユーザにはコンフィギュレーション CLI アクセス権が付与されます。アプライアンス Web インターフェイス用のいずれかのユーザ パスワードを変更すると、CLI のパスワードも変更されます（その逆も同様です）。

シスコが推奨する強力なパスワードは、大文字/小文字が混在し、少なくとも 1 つの数字を含む 8 文字以上の英数字からなるパスワードです。辞書に記載されている単語の使用を避けてください。詳細については、「パスワードの変更」（P.4-9）を参照してください。

ステップ 4　デバイスのネットワーク設定を行います。

最初に IPv4 管理を設定（または無効化）してから、IPv6 の設定に移ります。ネットワーク設定を手動で指定する場合は、以下の手順を実行する必要があります。

- ネットマスクを含む IPv4 アドレスを、ドット付き 10 進数形式で入力します。たとえば 255.255.0.0 というネットマスクを指定できます。
- IPv6 アドレスを、コロン区切りの 16 進数形式で入力します。IPv6 プレフィックスの場合、ビット数を指定します（たとえば 112 のプレフィックス長）。

詳細については、「ネットワーク設定」（P.4-9）を参照してください。設定が実装されるときに、コンソールにメッセージが表示される場合があります。

ステップ 5　LCD パネルを使用してデバイスのネットワーク設定を変更できるようにするかどうかを選択します。

注意　このオプションを有効にすると、セキュリティ リスクが生じる可能性があります。LCD パネルを使用してネットワーク設定を行うには、物理アクセスのみが必要であり、認証は不要です。詳細については、「シリーズ 3 デバイスでの LCD パネルの使用」（P.5-1）を参照してください。

ステップ 6　デバイスを展開した方法に基づいて検出モードを指定します。

詳細については、「検出モード」（P.4-11）を参照してください。設定が実装されるときに、コンソールにメッセージが表示される場合があります。完了すると、このデバイスを防御センターに登録するよう通知され、CLI プロンプトが表示されます。

ステップ 7　CLI を使用して、デバイスを管理する防御センターにデバイスを登録するには、次の項（CLI を使用して シリーズ 3 デバイスを防御センターに登録する）に進みます。

防御センターを使用してデバイスを管理する必要があります。今すぐデバイスを登録しない場合、後でデバイスを防御センターに追加するには、その前にデバイスにログインして登録する必要があります。

ステップ 8　アプライアンスからログアウトします。

CLI を使用して シリーズ 3 デバイスを防御センターに登録する

サポートされるデバイス：シリーズ 3

CLI を使用して シリーズ 3 デバイスを設定した場合、セットアップ スクリプトの終わりに CLI を使用してデバイスを防御センターに登録することを シスコ はお勧めします。すでにデバイスの CLI にログインしているため、初期セットアップ手順中にデバイスを防御センターに登録するのが最も簡単です。

デバイスを登録するには、`configure manager add` コマンドを使用します。デバイスを防御センターに登録するにはは、英数字からなる一意の登録キーが常に必要となります。これは、37 文字以下で指定する、ライセンス キーとは異なる単純なキーです。

ほとんどの場合、次のように、防御センターのホスト名または IP アドレスを登録キーと一緒に指定する必要があります。

```
configure manager add DC.example.com my_reg_key
```

ただし、デバイスと防御センターが NAT デバイスで分離されている場合は、次のように、一意の NAT ID を登録キーと一緒に入力して、ホスト名の代わりに `DONTRESOLVE` を指定します。

```
configure manager add DONTRESOLVE my_reg_key my_nat_id
```

デバイスを防御センターに登録する方法：

アクセス：コンフィギュレーション CLI

ステップ 1　コンフィギュレーション CLI アクセス レベルを持つユーザとしてデバイスにログインします。

- コンソールから初期セットアップを実行している場合は、必要なアクセス レベルを持つ `admin` ユーザとしてすでにログイン済みです。
- そうでない場合は、デバイスの管理 IP アドレスまたはホスト名に SSH します。

ステップ 2　プロンプトで、`configure manager add` コマンドを使ってデバイスを防御センターに登録します。構文は次のとおりです。

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} reg_key
[nat_id]
```

ここで、

- `{hostname | IPv4_address | IPv6_address | DONTRESOLVE}` は、防御センターの完全修飾ホスト名と IP アドレスのどちらかを指定します。防御センターを直接アドレス指定できない場合は、`DONTRESOLVE` を使用します。
- *reg_key* は、デバイスを防御センターに登録するために必要な 37 文字以下の英数字からなる一意の登録キーです。
- *nat_id* は、防御センターとデバイスの間の登録プロセスで使用されるオプションの英数字文字列です。ホスト名が `DONTRESOLVE` に設定されている場合は、必須です。

ステップ 3　アプライアンスからログアウトします。

デバイスを防御センターに追加する準備が整いました。

初期セットアップ ページ：デバイス

すべての管理対象デバイス（CLI を使って設定された シリーズ 3 デバイスを除く：「CLI を使用して シリーズ 3 デバイスで初期セットアップを実行する」（P.4-6）を参照）に対して、デバイスの Web インターフェイスにログインし、セットアップ ページで初期設定オプションを指定することによって、セットアップ手順を実行する必要があります。

管理者パスワードを変更し、（未設定であれば）ネットワーク設定を指定し、EULA に同意する必要があります。また、デバイスを防御センターに事前登録して検出モードを指定することもできます。登録時に選択された検出モードその他のオプションは、システムが作成するデフォルト インターフェイス、インライン セット、ゾーンに加えて、管理対象デバイスに最初に適用されるポリシーを決定します。

管理対象の物理デバイスの Web インターフェイスを使用して、そのデバイスの初期セットアップを完了する方法：

アクセス：Admin

ステップ 1　ブラウザで `https://mgmt_ip/` を参照します。ここで、*mgmt_ip* はデバイスの管理インターフェイスの IP アドレスです。

- イーサネット ケーブルでコンピュータに接続されたデバイスの場合は、そのコンピュータ上のブラウザで、デフォルト管理インターフェイスの IPv4 アドレス（`https://192.168.45.45/`）を参照します。
- ネットワーク設定がすでに完了しているデバイスの場合は、管理ネットワーク上のコンピュータを使用して、そのデバイスの管理インターフェイスの IP アドレスを参照します。

ログイン ページが表示されます。

ステップ 2　ユーザ名として `admin`、パスワードとして `Sourcefire` を使用してログインします。

セットアップ ページが表示されます。セットアップを完了する方法については、以下の項を参照してください。

- 「パスワードの変更」（P.4-9）
- 「ネットワーク設定」（P.4-9）

- 「シリーズ 3 デバイスの LCD パネルの設定」（P.4-10）
- 「リモート管理」（P.4-10）
- 「時刻の設定」（P.4-10）
- 「検出モード」（P.4-11）
- 「自動バックアップ」（P.4-12）
- 「エンド ユーザ ライセンス契約書（EULA）」（P.4-12）

ステップ 3　完了したら、[Apply] をクリックします。

選択内容に従ってデバイスが設定されます。中間ページが表示された後、管理者ロールを持つ admin ユーザとして Web インターフェイスにログインされます。

ステップ 4　デバイスからログアウトします。

デバイスを防御センターに追加する準備が整いました。

（注）　イーサネット ケーブルを使ってデバイスに直接接続した場合は、コンピュータを切断して、デバイスの管理インターフェイスを管理ネットワークに接続します。デバイスの Web インターフェイスに任意の時点でアクセスする必要がある場合は、管理ネットワーク上のコンピュータのブラウザで、セットアップ時に設定した IP アドレスまたはホスト名を参照します。

パスワードの変更

admin アカウントのパスワードを変更する必要があります。このアカウントには管理者特権が付与されているため、削除できません。

このパスワードを使用すると、admin ユーザはデバイスの Web インターフェイスとその CLI にログインできます。admin ユーザにはコンフィギュレーション CLI アクセス権が付与されます。アプライアンス Web インターフェイス用のいずれかのユーザ パスワードを変更すると、CLI のパスワードも変更されます（その逆も同様です）。

シスコが推奨する強力なパスワードは、大文字/小文字が混在し、少なくとも 1 つの数字を含む 8 文字以上の英数字からなるパスワードです。辞書に記載されている単語の使用を避けてください。

ネットワーク設定

デバイスのネットワーク設定を使用すると、デバイスは管理ネットワーク上で通信を行うことができます。すでにデバイスのネットワークが設定済みの場合は、ページのこのセクションに事前にいくつかの値が入力されます。

FireSIGHT システムでは、IPv4 と IPv6 の両方の管理環境のためのデュアルスタック実装が提供されています。管理ネットワーク プロトコル（**IPv4**、**IPv6**、または**両方**）を指定する必要があります。選択内容に応じてセットアップ ページにさまざまなフィールドが表示され、そこで IPv4 または IPv6 管理 IP アドレス、ネットマスクまたはプレフィックス長、およびデフォルト ゲートウェイを設定する必要があります。

- IPv4 の場合は、アドレスとネットマスクをドット付き 10 進数形式で設定する必要があります（例：ネットマスク 255.255.0.0）。

- IPv6 ネットワークの場合は、[Assign the IPv6 address using router autoconfiguration] チェックボックスをオンにして、自動的に IPv6 ネットワーク設定を割り当てることができます。そうでない場合は、コロン区切りの 16 進数形式のアドレスおよびプレフィックス内のビット数を設定する必要があります（例：プレフィックス長 112）。

また、最大で 3 つの DNS サーバ、およびデバイスのホスト名とドメインを指定することもできます。

シリーズ 3 デバイスの LCD パネルの設定

サポートされるデバイス：シリーズ 3

シリーズ 3 デバイスを設定する場合は、LCD パネルを使用してデバイスのネットワーク設定を変更できるようにするかどうかを選択します。

注意　このオプションを有効にすると、セキュリティ上のリスクが生じる可能性があります。LCD パネルを使用してネットワーク設定を行うには、物理アクセスのみが必要であり、認証は不要です。詳細については、「シリーズ 3 デバイスでの LCD パネルの使用」（P.5-1）を参照してください。

リモート管理

防御センターを使用して、シスコ デバイスを管理する必要があります。2 段階からなるこのプロセスでは、まずデバイス上でリモート管理を設定した後、デバイスを防御センターに追加します。便宜上、セットアップ ページでは、デバイスを管理する防御センターにデバイスを事前登録できます。

[Register This Device Now] チェックボックスをオンにしたまま、管理する防御センターの IP アドレスまたは完全修飾ドメイン名を [Management Host] として指定します。また、後でデバイスを防御センターに登録するときに使用する英数字の [Registration Key] を入力します。これは、37 文字以下で指定する、ライセンス キーとは異なる単純なキーであることに注意してください。

（注）　デバイスと防御センターがネットワーク アドレス変換（NAT）デバイスで分離されている場合は、初期セットアップの完了後までデバイス登録を延期してください。詳細については、*FireSIGHT System User Guide* の「デバイスの管理」の章を参照してください。

時刻の設定

デバイスの時刻を手動で設定することも、ネットワーク タイム プロトコル（NTP）を介して（防御センターを含む）NTP サーバを使って設定することもできます。シスコは、管理対象デバイス用の NTP サーバとして防御センターを使用することを推奨します。

また、`admin` アカウント用のローカル Web インターフェイスで使用されるタイム ゾーンを指定することもできます。現在のタイム ゾーンをクリックし、ポップアップ ウィンドウを使って変更できます。

検出モード

デバイスに関して選択された検出モードは、システムでデバイスのインターフェイスが初期設定される方法と、それらのインターフェイスがインライン セットまたはセキュリティ ゾーンのどちらに属するかを決定します。

検出モードの設定を後で変更することはできません。これは、システムによるデバイス初期設定の調整を容易にするために、セットアップ中にユーザが選択するオプションに過ぎません。一般的に、デバイスの展開方法に基づいて検出モードを次のように選択する必要があります。

パッシブ

デバイスが侵入検知システム（IDS）として受動的に（パッシブに）展開されている場合、このモードを選択します。パッシブ展開では、ファイルとマルウェアの検出、セキュリティ インテリジェンス モニタリング、およびネットワーク検出を実行できます。

インライン

デバイスが侵入防御システムとしてインラインで展開されている場合、このモードを選択します。通常、侵入防御システムは *Fail Open* 型であり、一致しないトラフィックが*許可*されます。

また、インライン展開では、ネットワーク ベースの高度なマルウェア防御（AMP）、ファイル制御、セキュリティ インテリジェンス フィルタリング、およびネットワーク検出を実行することもできます。

任意のデバイスに関してインライン モードを選択できますが、次のインターフェイスを使用するインライン セットにはバイパス機能が欠如していることに注意してください。

- 8000 シリーズ デバイス上の非バイパス NetMod
- 71xx ファミリ デバイス上の SFP トランシーバ

（注）　再イメージングにより、インライン展開のデバイスは非バイパス設定にリセットされます。このため、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。

アクセス コントロール

このモードを選択するのは、デバイスがアクセス コントロール展開の一部としてインラインで展開されている場合、つまりアプリケーション、ユーザ、および URL の制御を実行する場合です。アクセス コントロールを実行するよう設定されたデバイスは通常、*Fail Close* 型であり、一致しないトラフィックを*ブロック*します。ルールでは、通過させるトラフィックを明示的に指定します。

さらに、クラスタリング、厳密な TCP 強制、ファストパス ルール、スイッチング、ルーティング、DHCP、NAT、VPN など、（モデルによって異なる）デバイス固有のハードウェア ベース機能を利用する場合にも、このモードを選択してください。

また、アクセス コントロール展開では、マルウェア防御、ファイル制御、セキュリティ インテリジェンス フィルタリング、およびネットワーク検出を実行することもできます。

ネットワーク検出

デバイスが受動的に展開されている場合、ホスト、アプリケーション、およびユーザ検出のみを実行するには、このモードを選択します。

次の表は、選択した検出モードに基づいて作成されるインターフェイス、インライン セット、およびゾーンを示しています。

表 4-1　検出モードに基づく初期設定

検出モード	セキュリティ ゾーン	インライン セット	インターフェイス
インライン	内部および外部	デフォルト インライン セット	デフォルト インライン セットに追加される最初のペア：内部ゾーンと外部ゾーンに 1 つずつ
パッシブ	パッシブ	なし	パッシブ ゾーンに割り当てられる最初のペア
アクセス コントロール	なし	なし	なし
ネットワーク検出	パッシブ	なし	パッシブ ゾーンに割り当てられる最初のペア

セキュリティ ゾーンは防御センター レベルの設定であり、デバイスを実際に防御センターに登録するまでは作成されないことに注意してください。登録時に、適切なゾーン（内部、外部、またはパッシブ）がすでに防御センターに存在する場合は、一覧表示されたインターフェイスが登録プロセスで既存のゾーンに追加されます。ゾーンが存在しない場合は、システムがそれを作成し、インターフェイスを追加します。インターフェイス、インライン セット、およびセキュリティ ゾーンの詳細については、『*FireSIGHT System User Guide*』を参照してください。

自動バックアップ

デバイスには、データをアーカイブするメカニズムが備わっているため、障害発生時に設定とイベント データを復元できます。初期セットアップの一部として、[Enable Automatic Backups] を設定することができます。

この設定を有効にすると、デバイス上の設定の週次バックアップを作成するスケジュール済みタスクが作成されます。

エンド ユーザ ライセンス契約書（EULA）

EULA を注意深く読んで、その条項に従うことに同意する場合は、このチェックボックスをオンにします。入力したすべての情報が正しいことを確認し、[Apply] をクリックします。選択内容に従ってデバイスが設定され、それを管理する防御センターに追加できる状態になります。

初期セットアップ ページ：防御センター

すべての防御センターに対してセットアップ手順を完了する必要があります。その際、防御センターの Web インターフェイスにログインし、セットアップ ページで初期設定オプションを指定します。管理者パスワードを変更し、（未設定であれば）ネットワーク設定を指定して、EULA に同意する必要があります。

また、セットアップ手順では、デバイスを登録してライセンス認証することもできます。デバイスを登録するには、その前にデバイス自体のセットアップ手順を完了することに加えて、防御センターをリモート マネージャとして追加する必要があります。そうしないと登録が失敗します。

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）および「FireSIGHT システムのライセンス」（P.1-14）を参照してください。

防御センター上で Web インターフェイスを使用して初期セットアップを完了する方法：

アクセス：Admin

ステップ 1　ブラウザで `https://mgmt_ip/` を参照します。ここで、*mgmt_ip* は防御センターの管理インターフェイスの IP アドレスです。

- イーサネット ケーブルでコンピュータに接続された防御センターの場合は、そのコンピュータ上のブラウザで、デフォルト管理インターフェイスの IPv4 アドレス（`https://192.168.45.45/`）を参照します。
- ネットワーク設定がすでに完了している防御センターの場合は、管理ネットワーク上のコンピュータを使用して、その防御センターの管理インターフェイスの IP アドレスを参照します。

ログイン ページが表示されます。

ステップ 2　ユーザ名として `admin`、パスワードとして `Sourcefire` を使用してログインします。

セットアップ ページが表示されます。セットアップを完了する方法については、以下の項を参照してください。

- 「パスワードの変更」（P.4-14）
- 「ネットワーク設定」（P.4-14）
- 「時刻の設定」（P.4-14）
- 「ルール更新の継続的インポート」（P.4-14）
- 「継続的なAdmin位置情報の更新」（P.4-15）
- 「自動バックアップ」（P.4-15）
- 「ライセンスの設定」（P.4-15）
- 「デバイス登録」（P.4-16）
- 「エンド ユーザ ライセンス契約書（EULA）」（P.4-17）

ステップ 3　完了したら、[Apply] をクリックします。

選択内容に従って防御センターが設定されます。中間ページが表示された後、管理者ロールを持つ `admin` ユーザとして Web インターフェイスにログインされます。

（注）　イーサネット ケーブルを使ってデバイスに直接接続した場合は、コンピュータを切断して、防御センターの管理インターフェイスを管理ネットワークに接続します。管理ネットワーク上のコンピュータのブラウザを使用して、設定済みのホスト名または IP アドレスで防御センターにアクセスし、このガイドの残りの手順を完了します。

ステップ 4　[Task Status] ページ（[System] > [Monitoring] > [Task Status]）を使用して、初期セットアップが正常に行われたことを確認します。

このページは 10 秒ごとに自動更新されます。初期デバイス登録タスクとポリシー適用タスクのステータスが [Completed] になるまでページを監視します。また、セットアップの一部として、侵入ルールまたは位置情報の更新を設定した場合は、それらのタスクも監視できます。

防御センターを使用する準備が整いました。展開の詳しい設定方法については、『*FireSIGHT System User Guide*』を参照してください。

ステップ 5　「次の手順」（P.4-17）に進みます。

パスワードの変更

admin アカウントのパスワードを変更する必要があります。このアカウントには管理者特権が付与されているため、削除できません。

シスコが推奨する強力なパスワードは、大文字/小文字が混在し、少なくとも 1 つの数字を含む 8 文字以上の英数字からなるパスワードです。辞書に記載されている単語の使用を避けてください。

ネットワーク設定

防御センターのネットワーク設定を使用すると、管理ネットワーク上で通信を行うことができます。すでにネットワークが設定済みの場合は、ページのこのセクションに事前にいくつかの値が入力されます。

FireSIGHT システムでは、IPv4 と IPv6 の両方の管理環境のためのデュアルスタック実装が提供されています。管理ネットワーク プロトコル（**IPv4**、**IPv6**、または**両方**）を指定する必要があります。選択内容に応じてセットアップ ページにさまざまなフィールドが表示され、そこで IPv4 または IPv6 管理 IP アドレス、ネットマスクまたはプレフィックス長、およびデフォルト ゲートウェイを設定する必要があります。

- IPv4 の場合は、アドレスとネットマスクをドット付き 10 進数形式で設定する必要があります（例：ネットマスク 255.255.0.0）。
- IPv6 ネットワークの場合は、[Assign the IPv6 address using router autoconfiguration] チェックボックスをオンにして、自動的に IPv6 ネットワーク設定を割り当てることができます。そうでない場合は、コロン区切りの 16 進数形式のアドレスおよびプレフィックス内のビット数を設定する必要があります（例：プレフィックス長 112）。

また、最大で 3 つの DNS サーバ、およびデバイスのホスト名とドメインを指定することもできます。

時刻の設定

防御センターの時刻を手動で設定することも、ネットワーク タイム プロトコル（NTP）を介して NTP サーバを使って設定することもできます。

また、admin アカウント用のローカル Web インターフェイスで使用されるタイム ゾーンを指定することもできます。現在のタイム ゾーンをクリックし、ポップアップ ウィンドウを使って変更できます。

ルール更新の継続的インポート

ライセンス：保護

新しい脆弱性が発見されると、脆弱性調査チーム（VRT）は侵入ルールの更新をリリースします。ルール更新には、新しい（または更新された）侵入ルールとプリプロセッサ ルール、既存のルールの状態変更、およびデフォルト侵入ポリシー設定の変更が含まれています。また、ルール更新ではルールが削除されたり、新しいルール カテゴリとシステム変数が提供されたりすることもあります。

展開で侵入検知および防御を実行する予定の場合、[Enable Recurring Rule Update Imports] を有効にして継続的にインポートすることをシスコでは推奨しています。

[Import Frequency] で頻度を指定できることに加えて、ルールが更新されるたびに侵入ポリシーを再適用（[Policy Reapply]）するようシステムを設定できます。初期設定プロセスの一部としてルール更新を実行するには、[Install Now] を選択します。

（注）　ルール更新には、新しいバイナリが含まれることがあります。ルール更新をダウンロードしてインストールする手順が組織のセキュリティ ポリシーに準拠していることを確認してください。加えて、ルール更新の容量が大きい場合があるため、ネットワーク使用率の低い時間帯にルールをインポートするようにしてください。

継続的なAdmin位置情報の更新

サポートされる防御センター：（DC500 以外）

ほとんどの防御センターでは、システムによって生成されたイベントに関連付けられたAdmin ルーテッド IP アドレスに関する地理情報を表示したり、ダッシュボードと Context Explorer で位置情報統計を監視したりできます。

防御センターの位置情報データベース（GeoDB）には、IP アドレスに関連するインターネット サービス プロバイダー（ISP）、接続タイプ、プロキシ情報、正確な位置などの情報が含まれています。定期的な GeoDB 更新を有効にすると、システムは常に最新の位置情報を使用できます。展開で位置情報関連の分析を実行する予定の場合、[Enable Recurring Weekly Updates] を有効にして定期更新することをシスコでは推奨しています。

GeoDB の週次更新の頻度を指定できます。タイム ゾーンをクリックし、ポップアップ ウィンドウを使って変更できます。初期設定プロセスの一部としてこのデータベースをダウンロードするには、[Install Now] を選択します。

（注）　GeoDB 更新は容量が大きくなる場合があり、ダウンロード後のインストールに最大 45 分かかることがあります。ネットワーク使用率が低い時間帯に GeoDB を更新してください。

自動バックアップ

防御センターには、データをアーカイブするメカニズムが備わっているため、障害発生時に設定を復元できます。初期セットアップの一部として、[Enable Automatic Backups] を設定することができます。

この設定を有効にすると、防御センターの設定の週次バックアップを作成するスケジュール済みタスクが作成されます。

ライセンスの設定

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。ホスト、アプリケーション、およびユーザ検出を実行するには、防御センター上の FireSIGHT ライセンスが必要です。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さまざまな機能を実行できます。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。「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）および「FireSIGHT システムのライセンス」（P.1-14）を参照してください。

初期セットアップ ページを使用して、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。今すぐライセンスを追加しない場合、初期セットアップ時に登録したデバイスはすべて「ライセンスなし」として防御センターに追加されます。初期セットアップ プロセスが完了した後で、それぞれを個別にライセンス認証する必要があります。なお、再イメージングしたアプライアンスをセットアップするときに、復元手順の一部としてライセンス設定が維持されている場合は、このセクションに事前に入力される可能性があります。

まだライセンスを取得していない場合は、https://keyserver.sourcefire.com/ に移動するリンクをクリックして、画面上の指示に従います。（初期セットアップ ページに表示される）ライセンス キーの他に、サポート契約で設定された連絡先に事前に電子メールで送信されたアクティベーション キーも必要です。

ライセンスをテキスト ボックスの中に貼り付けて、[Add/Verify] をクリックすることにより、ライセンスを追加します。有効なライセンスを追加すると、ページが更新され、追加済みのライセンスを確認できまか。ライセンスは一度に 1 つずつ追加してください。

デバイス登録

防御センターでは、FireSIGHT システム で現在サポートされている任意のデバイス（物理または仮想）を管理できます。

（注）　デバイスを防御センターに登録するには、その前に、デバイスにリモート管理を設定する必要があります。

初期セットアップ手順では、事前に登録されたデバイスのほとんどを防御センターに追加できます（「リモート管理」（P.4-10）を参照）。ただし、デバイスと防御センターが NAT デバイスによって分離されている場合は、セットアップ手順の完了後にそれを追加する必要があります。

デバイスの登録時に、アクセス コントロール ポリシーをデバイスに自動的に適用するにはは、[Apply Default Access Control Policies] チェックボックスをオンのままにします。ここでは単にポリシーを適用するかどうかを設定することに注意してください。防御センターが各デバイスにどのポリシーを適用するか選択することはできません。各デバイスに適用されるポリシーは、デバイスの設定時に選択される検出モード（「検出モード」（P.4-11）を参照）によって異なります。次の表にそれを示します。

表 4-2　検出モードごとに適用されるデフォルト アクセス コントロール ポリシー

検出モード	デフォルト アクセス コントロール ポリシー
インライン	デフォルト侵入防御
パッシブ	デフォルト侵入防御
アクセス コントロール	デフォルト アクセス コントロール
ネットワーク検出	デフォルト ネットワーク検出

以前に防御センターで管理していたデバイスの初期インターフェイス設定を変更した場合には、例外が発生します。この場合、この新しい防御センター ページによって適用されるポリシーは、変更後の（現在の）デバイス設定によって異なります。インターフェイスが設定されている場合、防御センターはデフォルト侵入防御ポリシーを適用します。そうでない場合、防御センターはデフォルト アクセス コントロール ポリシーを適用します。

デバイスを追加するには、その**ホスト名**または **IP アドレス**に加えて、デバイス登録時に指定した**登録キー**も入力します。これは、37 文字以下ですでに指定した、ライセンス キーとは異なる単純なキーです。

その後、チェックボックスを使用して、ライセンス付与された機能をデバイスに追加します。防御センターにすでに追加されたライセンスだけを選択できます（「ライセンスの設定」（P.4-15）を参照）。

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。ただし、セットアップ ページでは、管理対象デバイスでサポートされないライセンスを有効にしたり、モデル固有のライセンスがない機能を有効にしたり**できます**。このように動作する理由は、後にならないと防御センターがデバイス モデルを特定しないためです。システムは無効なライセンスをイネーブル化できません。無効なライセンスをイネーブル化しようとしても、使用可能なライセンス数は減少しません。

（どの防御センターを使用して各ライセンスを各デバイス モデルに適用できるかなど）ライセンス認証の詳細については、「防御センター モデル別にサポートされる機能」（P.1-8）および「FireSIGHT システムのライセンス」（P.1-14）を参照してください。

（注） [Apply Default Access Control Policies] をオンにした場合は、**インライン**または**パッシブ**検出モードを選択したデバイス上で保護 ライセンスを有効にする必要があります。また、インターフェイスがすでに設定された管理対象デバイス上で保護を有効にする必要もあります。そうしないと、（この場合に保護を必要とする）デフォルト ポリシーの適用が失敗します。

ライセンスを有効にした後、[Add] をクリックしてデバイスの登録設定を保存し、オプションで、新しいデバイスを追加します。間違ったオプションを選択した場合、またはデバイス名を誤って入力した場合は、[Delete] をクリックしてそれを削除します。その後、デバイスを再び追加できます。

エンド ユーザ ライセンス契約書（EULA）

EULA を注意深く読んで、その条項に従うことに同意する場合は、このチェックボックスをオンにします。入力したすべての情報が正しいことを確認し、[Apply] をクリックします。

選択内容に従って防御センターが設定されます。中間ページが表示された後、管理者ロールを持つ `admin` ユーザとして Web インターフェイスにログインされます。「初期セットアップ ページ：防御センター」（P.4-12）のステップ 3 に進んで、防御センターの初期セットアップを完了します。

次の手順

アプライアンスの初期セットアップ手順が完了し、正常にセットアップされたことを確認したら、展開の管理を容易にするためのさまざまな管理タスクを実行することをシスコでは推奨しています。また、初期セットアップ時に省略したタスク（デバイス登録やライセンス認証など）があれば、それも実行してください。以降のセクションで説明するタスクの詳細について、および展開の設定を始める方法については、『*FireSIGHT System User Guide*』を参照してください。

ヒント シリアルまたは LOM/SOL 接続を使用してアプライアンスのコンソールにアクセスするためには、コンソール出力をリダイレクトする必要があります（「インライン バイパス インターフェイス設置のテスト」（P.3-24）を参照）。とくに LOM を使用する場合には、この機能に加えて、1 人以上の LOM ユーザも有効にする必要があります（「LOM と LOM ユーザを有効にする」（P.7-21）を参照）。

個別のユーザ アカウント

初期セットアップが完了した時点で、システム上の唯一のユーザは、管理者ロールとアクセス権を持つ admin ユーザです。このロールを持つユーザは、シェルまたは CLI 経由を含め、システムのメニューと設定に対するフル アクセスが可能です。セキュリティおよび監査上の理由で、admin アカウント（および管理者ロール）の使用を制限することを シスコでは推奨しています。

システムを使用するユーザごとに別々のアカウントを作成すると、組織で各ユーザのアクションや変更を監査できるだけでなく、各ユーザに関連付けられたユーザ アクセス ロールを制限することもできます。これは、ほとんどの設定タスクと分析タスクを実行する場所である防御センターではとくに重要です。たとえば、アナリストはネットワーク セキュリティを分析するためにイベント データにアクセスする必要がありますが、展開の管理機能にアクセスする必要はないでしょう。

システムには、さまざまな管理者やアナリストのために事前定義された 10 個のユーザー ロールが含まれています。また、特殊なアクセス特権を持つカスタム ユーザ ロールを作成することもできます。

ヘルス ポリシーとシステム ポリシー

デフォルトで、すべてのアプライアンスに初期システム ポリシーが適用されます。システム ポリシーは、メール中継ホスト プリファレンスや時刻同期設定など、展開内の多数のアプライアンス間で類似することの多い設定を管理します。防御センターを使用して、それ自体およびすべての管理対象デバイスに同じシステム ポリシーを適用することを シスコでは推奨しています。

デフォルトで、防御センターにはヘルス ポリシーも適用されます。ヘルス モニタリング機能の一部であるヘルス ポリシーは、展開内のアプライアンスのパフォーマンスを継続的に監視するシステム向けの基準を提供します。防御センターを使用してヘルス ポリシーをすべての管理対象デバイスに適用することを シスコでは推奨しています。

ソフトウェアとデータベースの更新

展開を開始する前に、アプライアンス上でシステム ソフトウェアを更新してください。展開内のすべてのアプライアンスで FireSIGHT システムの最新バージョンを実行することを シスコでは推奨しています。また、侵入ルール更新、VDB、および GeoDB が展開で使用されている場合、それらの最新バージョンをインストールしてください。

注意　FireSIGHT システム を何らかの形で更新する前には、更新に付随するリリース ノートまたは注意書を読む**必要**があります。リリース ノートには、サポートされるプラットフォーム、互換性、前提条件、警告、特定のインストール/アンインストール手順などの重要情報が含まれています。

シリーズ 3 デバイスでの LCD パネルの使用

シリーズ 3 デバイスでは、システムの Web インターフェイスの代わりにデバイス前面の LCD パネルを使用して、デバイス情報を表示したり特定の設定値を設定したりすることができます。

LCD パネルには、ディスプレイと 4 つの多機能キーがあり、デバイスの状態に応じて異なる情報を表示し、異なる設定を可能にする、複数のモードで動作します。

詳細については、次の項を参照してください。

- 「LCD パネルのコンポーネントについて」（P.5-2）は、LCD パネルのコンポーネントを識別し、パネルのメイン メニューを表示する方法について説明します。
- 「LCD 多機能キーの使用」（P.5-3）は、LCD パネルの多機能キーを使用する方法について説明します。
- 「[Idle Display] モード」（P.5-4）は、デバイスがアイドル状態のときに、どのように LCD パネルがさまざまなシステム情報を表示するかについて説明します。
- 「[Network Configuration] モード」（P.5-4）は、LCD パネルを使用してデバイスの管理インターフェイスのネットワーク構成（IPv4 または IPv6 アドレス、サブネット マスクまたはプレフィックス、およびデフォルト ゲートウェイ）を設定する方法について説明します。

注意 LCD パネルを使用して再設定できるようにすると、セキュリティ リスクが生じる可能性があります。LCD パネルを使用して設定を行うために必要なのは、物理的なアクセスだけであり、認証は必要ありません。

- 「[System Status] モード」（P.5-7）は、監視対象システムの情報（リンク ステート伝播、バイパス ステータス、システム リソースなど）を表示する方法、および LCD パネルの明るさやコントラストを変更する方法について説明します。
- 「[Information] モード」（P.5-8）は、デバイスのシャーシ シリアル番号、IP アドレス、モデル、ソフトウェアとファームウェアのバージョンなど、システムの識別情報を表示する方法について説明します。
- 「[Error Alert] モード」（P.5-9）は、バイパス、ファン ステータス、ハードウェア アラートなど、LCD パネルがエラー状態や障害状態を通知する方法について説明します。

（注） LCD パネルを使用するには、デバイスの電源がオンになっている必要があります。デバイスの電源をオンにする方法やデバイスをシャット ダウンする方法について詳しくは、『*FireSIGHT System User Guide*』の「デバイスの管理」の章を参照してください。

LCD パネルのコンポーネントについて

シリーズ 3 デバイス前面の LCD パネルには、ディスプレイと 4 つの多機能キーがあります。

- ディスプレイには、2 行のテキスト（それぞれ最大 17 文字まで）と多機能キーのマップが示されています。マップは、記号を使用して、対応する多機能キーで実行可能な操作を示しています。
- 多機能キーを使用することにより、システム情報を確認し、LCD パネルのモードによって異なる、基本的な設定タスクを行うことができます。詳細については、「LCD 多機能キーの使用」（P.5-3）を参照してください。

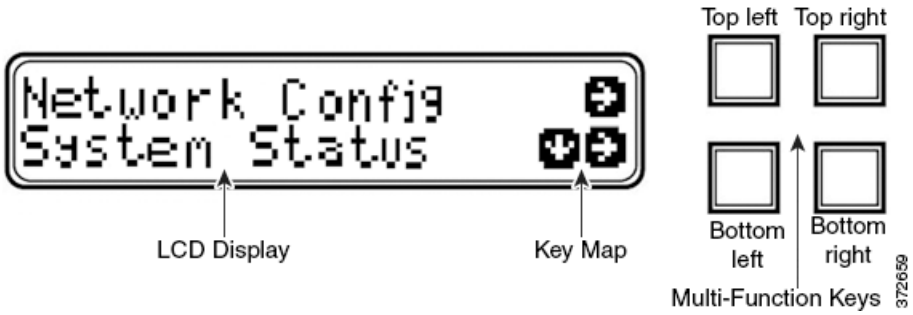
次の図は、パネルのデフォルトの [Idle Display] モードを示しています。ここではキー マップは示されません。

図 5-1　　LCD パネル、[Idle Display] モード

[Idle Display] モードでは、CPU 使用率と使用可能な空きメモリ、およびシャーシのシリアル番号がパネルに交互に表示されます。任意のキーを押すと [Idle Display] モードは中断し、[Network Configuration]、[System Status]、および [Information] モードにアクセスできる LCD パネルのメイン メニューが表示されます。

次の図は、4 つの多機能キー（左上、右上、左下、右下）に対応するキー マップがあるメイン メニューを示しています。

図 5-2　　LCD パネル、メイン メニュー



メイン メニューにアクセスするには、次の手順に従います。

ステップ 1　[Idle Display] モードで、任意の多機能キーを押します。

メイン メニューが表示されます。

- デバイスのネットワーク設定を変更するには、「[Network Configuration] モード」（P.5-4）を参照してください。
- 監視対象のシステム情報を参照する方法や LCD パネルの明るさとコントラストを調整する方法については、「[System Status] モード」（P.5-7）を参照してください。

- システムの識別情報を表示するには、「[Information] モード」（P.5-8）を参照してください。

（注） LCD パネルが [Idle Display] モードに切り替わるときに多機能キーを押すと、予期されないメニューがパネルに表示される可能性があります。

LCD 多機能キーの使用

4 つの多機能キーにより、シリーズ 3 デバイスの LCD パネルでメニューやオプションの間を移動できます。ディスプレイにキー マップが表示されたら、多機能キーを使用できます。マップでの記号の位置は、機能およびその機能を実行するために使用するキーの位置に対応します。記号が表示されていない場合、対応するキーには機能がありません。

ヒント 記号の機能（さらにはキー マップ）は、LCD パネルのモードに応じて異なります。予期した結果が生じない場合は、LCD パネルのモードを確認してください。

次の表は、多機能キーの機能について説明しています。

表 5-1　LCD パネルの多機能キー

記号	説明	機能
↑	上矢印	現在のメニュー オプションのリストを上にスクロールします。
↓	下矢印	現在のメニュー オプションのリストを下にスクロールします。
←	左矢印	以下のいずれかのアクションを実行します。 • アクションは実行しないで、LCD パネル メニューを表示します。 • カーソルを左に移動します。 • 編集を再び有効にします。
→	右矢印	以下のいずれかのアクションを実行します。 • その行に示されているメニュー オプションを表示します。 • カーソルを右に移動します。 • スクロールして続きのテキストを表示します。
X	取り消し	アクションを取り消します。
+	追加	選択された桁の数字を 1 つ増やします。
-	削減	選択された桁の数字を 1 つ小さくします。
✓	チェック マーク	そのアクションを受け入れます。

[Idle Display] モード

LCD パネルは、非アクティブ（どの多機能キーも押されていない）でエラーの検出されない状態が 60 秒間続いた後に [Idle Display] モードになります。システムでエラーが検出されると、そのエラーが解決されるまで、パネルは [Error Alert] モードになります（「[Error Alert] モード」（P.5-9）を参照してください）。ネットワーク設定の編集中や診断の実行中も、[Idle Display] モードが無効になります。

[Idle Display] モードでは、CPU 使用率と使用可能な空きメモリ、およびシャーシのシリアル番号がパネルに交互に（5 秒間隔で）表示されます。

各ディスプレイのサンプルを以下に示します。

```
CPU: 50%
FREE MEM: 1024 MB
```

または

```
Serial Number:
3D99-101089108-BA0Z
```

[Idle Display] モードでは、任意の多機能キーを押すとメイン メニューが表示されます。「LCD パネルのコンポーネントについて」（P.5-2）を参照してください。

（注） LCD パネルが [Idle Display] モードに切り替わるときに多機能キーを押すと、予期されないメニューがパネルに表示される可能性があります。

[Network Configuration] モード

FireSIGHT システムでは、IPv4 と IPv6 の両方の管理環境のためのデュアルスタック実装が提供されています。[Network Configuration] モードでは、LCD パネルを使用して、シリーズ 3 デバイスの管理インターフェイスのネットワーク設定（IP アドレス、サブネット マスクまたはプレフィックス、デフォルト ゲートウェイ）を設定できます。

デフォルトでは、LCD パネルを使用してネットワーク設定を変更する機能は無効になっています。これは初期セットアップ プロセスで有効にするか、またはデバイスの Web インターフェイスを使用して有効にすることができます。詳細については、「LCD パネルを使用したネットワーク再設定の許可」（P.5-6）を参照してください。

注意 このオプションを有効にすると、セキュリティ リスクが生じる可能性があります。LCD パネルを使用してネットワーク設定を行うには、物理アクセスのみが必要であり、認証は不要です。

[Network Configuration] モードを使用してネットワーク設定を行うには、以下を行います。

ステップ 1　[Idle Display] モードで任意の多機能キーを押して、メイン メニューを表示します。

メイン メニューが表示されます。

```
Network Config          →
System Status        ↓ →
```

ステップ 2　[Network Configuration] モードにアクセスするには、一番上の行の右矢印（à）キーを押します。

LCD パネルには、以下が表示されます。

```
IPv4                 ↓ →
IPv6                   →
```

ステップ 3　右矢印キーを押して、設定する IP アドレスを選択します。

- IPv4 の場合、LCD パネルには以下のように表示されます。

```
IPv4 set to DHCP.   ←
Enable Manual?      →
```

- IPv6 の場合、LCD パネルには以下のように表示されます。

```
IPv6 Disabled.      ←
Enable Manual?      →
```

ステップ 4　手動でネットワークを設定するには、右矢印キーを押します。

- IPv4 の場合、LCD パネルに IPv4 アドレスが表示されます。次に例を示します。

```
IPv4 Address:     - +
194.170.001.001   X →
```

- IPv6 の場合、LCD パネルにブランクの IPv6 アドレスが表示されます。次に例を示します。

```
IPv6 Address:     - +
0000:0000:0000:00 X →
```

パネルの最初の行は、IPv4 または IPv6 のどちらのアドレスを編集しているかを示します。2 番目の行は、編集する IP アドレスを示します。カーソルは最初の桁を下線で強調表示して、編集中の桁であることを表します。2 つの記号は、各行の右にある多機能キーに対応しています。

IPv6 のアドレスは、ディスプレイに全体が収まらないことに注意してください。数字を編集してカーソルを右に移動させると、IPv6 アドレスが右にスクロールします。

ステップ 5　必要に応じて、カーソルのある下線で強調表示された桁を編集し、IP アドレスの次の桁に移動します。

- 桁を編集するには、上の行のマイナス（-）キーまたはプラス（+）キーを押して、桁の数字を 1 つずつ減少または増加させます。
- IP アドレスの次の桁に移動するには、下の行の右矢印キーを押して、カーソルを右にある次の桁に移動します。

カーソルが最初の桁にあるとき、LCD パネルには、IP アドレスの末尾にキャンセルの記号と右矢印の記号が表示されます。カーソルが他のいずれかの桁にあるとき、LCD パネルには、左矢印と右矢印の記号が表示されます。

ステップ 6　IPv4 または IPv6 アドレスの編集を終了したら、右矢印キーをもう一度押して、変更を受け入れるためのチェック マーク（✓）キーを表示します。

右矢印キーを押す前に、ディスプレイの機能記号は次の例のようになります。

```
IPv4 Address:     - +
194.170.001.001   X →
```

右矢印キーを押した後に、ディスプレイの機能記号は次の例のようになります。

```
IPv4 Address:     X ✓
194.170.001.001   ←
```

ステップ 7　チェック マーク キーを押して、IP アドレスの変更を受け入れます。

IPv4 の場合、LCD パネルに以下が表示されます。

```
Subnet Mask:      - +
000.000.000.000   X →
```

IPv6 の場合、LCD パネルに以下が表示されます。

```
Prefix:           - +
000.000.000.000   X →
```

ステップ 8　IP アドレスを編集したときと同様にサブネット マスクやプレフィクスを編集して、チェック マーク キーを押し、変更を受け入れます。

LCD パネルには、以下が表示されます。

```
Default Gateway    - +
000.000.000.000    X →
```

ステップ 9　IP アドレスを編集したときと同様にデフォルト ゲートウェイを編集して、チェック マーク キーを押し、変更を受け入れます。

LCD パネルには、以下が表示されます。

```
Save?              ✓
                   X
```

ステップ 10　チェック マーク キーを押して、変更を保存します。

LCD パネルを使用したネットワーク再設定の許可

セキュリティ リスクが生じるため、LCD パネルを使用してネットワーク設定を変更する機能は、デフォルトでは無効になっています。これは初期セットアップ プロセスで有効にするか（「シリーズ 3 デバイスのセットアップ」（P.4-4）を参照）、または以下の手順でデバイスの Web インターフェイスを使用して有効にできます。

デバイスの LCD パネルを使用してネットワークの再設定を許可するには、以下のようにします。

アクセス：Admin

ステップ 1　デバイスの初期設定を完了したら、管理者権限のあるアカウントを使用してデバイスの Web インターフェイスにログインします。

ステップ 2　[System] > [Local] > [Configuration] を選択します。

[Information] ページが表示されます。

ステップ 3　[Network] をクリックします。

[Network Settings] ページが表示されます。

ステップ 4　[LCD Panel] の下にある [Allow reconfiguration of network configuration] チェック ボックスを選択します。セキュリティ警告が表示されたら、このオプションを有効にすることを確認します。

ヒント　このページで示される他のオプションについて詳しくは、『*FireSIGHT System User Guide*』を参照してください。

ステップ 5　[Save] をクリックします。

ネットワーク設定が変更されます。

[System Status] モード

LCD パネルの [System Status] モードでは、リンク ステートの伝播、バイパスのステータス、システム リソースなど、監視対象システム情報が表示されます。[System Status] モードでは、LCD パネルの明るさとコントラストも変更できます。

次の表には、このモードで使用できる情報とオプションが示されています。

表 5-2　[System Status] モードの オプション

オプション	説明
Resources	CPU 使用率と使用可能な空きメモリが表示されます。[Display] モードでも、この情報が示されることに注意してください。

Link State	現在使用中のインライン セットと、そのセットのリンク状態ステータスのリストを表示します。最初の行はインライン セットを示し、2 番目の行はそのステータスを示します（normal または tripped）。次に例を示します。
	`eth2-eth3:`
	`normal`

Fail Open	使用中のバイパスのインライン セット、およびそれらのペアのステータス（normal または in bypass）のリストを表示します。
Fan Status	デバイスのファンのリストとステータスを表示します。
Diagnostics	サポートから使用可能な特定のキー シーケンスを押した後にアクセス可能になります。 ⚠ **注意**　サポートの指示がない限り、診断メニューにアクセス**しない**でください。サポートからの特定の指示なしで診断メニューにアクセスすると、システムが破損することがあります。
LCD Brightness	LCD ディスプレイの明るさを調整できます。
LCD Contrast	LCD ディスプレイのコントラストを調整できます。

[System Status] モードにして、監視対象のシステムの情報を表示するには、以下の手順を行います。

ステップ 1　[Idle Display] モードで任意の多機能キーを押して、メイン メニューを表示します。

メイン メニューが表示されます。

```
Network Config        →
System Status       ↓ →
```

ステップ 2　[System Status] モードにアクセスするには、一番下の行の右矢印（→）キーを押します。

LCD パネルには、以下が表示されます。

```
Resources           ↓ →
Link State          ↓ →
```

ステップ 3　下矢印（â）キーを押して、オプションをスクロールします。表示するステータスの横にある行で右矢印キーを押します。

選択したオプションに応じて、表 5-2（P.5-7）にリストされた情報が LCD パネルに表示されます。LCD パネルの明るさやコントラストを変更する方法については、次の手順を参照してください。

LCD パネルの明るさやコントラストを変更するには、以下のようにします。

ステップ 1　[System Status] モードで、LCD パネルに [LCD Brightness] および [LCD Contrast] オプションが表示されるまで、下矢印（â）キーを押してオプションをスクロールします。

```
LCD Brightness      ↓ →
LCD Contrast        ↓ →
```

ステップ 2　調整する LCD ディスプレイ機能（明るさまたはコントラスト）の横にある行の右矢印キーを押します。

LCD パネルには、以下が表示されます。

```
Increase              →
Decrease            ↓ →
```

ステップ 3　選択したディスプレイ機能を増加または減少させるためには、右矢印キーを押します。

それらのキーを押すと、LCD ディスプレイが変化します。

ステップ 4　[Exit] オプションを表示するには、下矢印を押します。

```
Decrease            ↓ →
Exit                  →
```

ステップ 5　設定を保存してメイン メニューに戻るには、[Exit] 行の右矢印キーを押します。

[Information] モード

LCD パネルの [Information] モードには、デバイスのシャーシのシリアル番号、IP アドレス、モデル、ソフトウェアとファームウェアのバージョンなど、システムの識別情報が表示されます。サポートに支援を要請する場合に、この情報が必要になることがあります。

次の表は、このモードで参照可能な情報を示しています。

表 5-3　[Information] モードのオプション

オプション	説明
IP address	デバイス管理インターフェイスの IP アドレスを表示します。
Model	デバイスのモデルを表示します。
Serial number	デバイスのシャーシのシリアル番号を表示します。
Versions	デバイスのシステム ソフトウェアとファームウェアのバージョンを表示します。多機能のキーを使用して、次の情報をスクロールします。 • Product version • NFE version • Micro Engine version • Flash version • GerChr version

[Information] モードにして、システムの識別情報を表示するには、以下を行いますす。

ステップ 1　[Idle Display] モードで任意の多機能キーを押して、メイン メニューを表示します。

メイン メニューが表示されます。

```
Network Config          →
System Status       ↓ →
```

ステップ 2　LCD パネルに [Information] モードが表示されるまで、下矢印（â）キーを押してモードをスクロールします。

```
System Status       ↓ →
Information         ↓ →
```

ステップ 3　[Information] モードにアクセスするには、一番下の行の右矢印（→）キーを押します。

ステップ 4　下矢印（â）キーを押して、オプションをスクロールします。表示する情報の横にある行で右矢印キーを押します。

選択したオプションに応じて、表 5-3（P.5-8）にリストされた情報が LCD パネルに表示されます。

[Error Alert] モード

ハードウェア エラーや障害状態が発生した場合、[Idle Display] モードは中断されて [Error Alert] モードになります。[Error Alert] モードでは、LCD ディスプレイが点滅し、次の表にリストされたエラーの 1 つまたは複数が表示されます。

表 5-4　　LCD パネルのエラー アラート

エラー	説明
Hardware alarm	ハードウェア アラームに関するアラート
Link state propagation	ペアになっているインターフェイスのリンク状態を表示します。
Bypass	バイパス モードで設定されたインライン セットのステータスを表示します。
Fan status	ファンがクリティカル状態に達した場合のアラート

ハードウェア エラーのアラートが発生すると、LCD ディスプレイにハードウェア アラートのメイン メニューが次のように表示されます。

```
HARDWARE ERROR!         →
Exit                    →
```

多機能キーを使用して、エラー アラートのリストをスクロールしたり、[Error Alert] モードを終了したりできます。注意すべき点として、すべてのエラー状態が解決されるまで LCD ディスプレイは点滅し、アラート メッセージを表示します。

LCD パネルでは、常にプラットフォーム デーモン エラー メッセージが最初に表示され、それに続いて他のハードウェア エラー メッセージのリストが表示されます。次の表には、シリーズ 3 デバイスのエラー メッセージに関する基本情報が示されています。ここで、*x* はアラートを生成する NFE アクセラレータ カート（0 または 1）を示します。

表 5-5　ハードウェア アラームのエラー メッセージ

エラー メッセージ	監視対象の条件	説明
NFE_platformd*X*	プラットフォーム デーモン	プラットフォーム デーモンが失敗したときにアラートを出します。
NFE_temp*X*	温度ステータス	アクセラレータ カードの温度が許容範囲を超えたときにアラートを出します。 • WARNING：80°C/176°F（7000 シリーズ）または 97°C/206°F（8000 シリーズ）より大きい。 • CRITICAL：90°C/194°F（7000 シリーズ）または 102°C/215°F（8000 シリーズ）より大きい。
HeartBeat*X*	ハートビート	システムがハートビートを検出できないときにアラートを出します。
frag*X*	nfe_ipfragd（ホスト フラグ）デーモン	ipfragd デーモンが失敗したときにアラートを出します。
rules*X*	Rulesd（ホストのルール）デーモン	Rulesd デーモンが失敗したときにアラートを出します。
TCAM*X*	TCAM デーモン	TCAM デーモンが失敗したときにアラートを出します。
NFEMessD*X*	メッセージ デーモン	メッセージ デーモンが失敗したときにアラートを出します。
NFEHardware	ハードウェア ステータス	1 つ以上のアクセラレータ カードが通信していないときにアラートを出します。
NFEcount	検出されたカード	デバイスで検出されたアクセラレータ カード数がプラットフォームの予想アクセラレータ カード数に一致しないときにアラートを表示します。
7000 シリーズ のみ：GerChr_comm 7000 シリーズ のみ：NMSB_comm	通信	メディア アセンブリが存在しない場合や通信していない場合にアラートを出します。
7000 シリーズ のみ：gerd 8000 シリーズ のみ：scmd	scmd デーモンのステータス	scmd デーモンが失敗したときにアラートを出します。
7000 シリーズ のみ：gpsl 8000 シリーズ のみ：psls	psls デーモンのステータス	psls デーモンが失敗したときにアラートを出します。
7000 シリーズ のみ：gftw 8000 シリーズ のみ：ftwo	ftwo デーモンのステータス	ftwo デーモンが失敗したときにアラートを出します。

表 5-5　ハードウェア アラームのエラー メッセージ （続き）

エラー メッセージ	監視対象の条件	説明
NFE_port18 NFE_port19 NFE_port20 NFE_port21	内部リンクのステータス	ネットワーク モジュールのスイッチ ボードとアクセラレータ カードの間のリンクが失敗したときにアラートを出します： • 7000 シリーズ すべてのファミリ：NFE_port18 のみ • 8000 シリーズ 81xx ファミリ：NFE_port18 および NFE_port19 のみ 82xx ファミリ および 83xx ファミリ：NFE_port18、NFE_port19、NFE_port20、および NFE_port21

LCD ディスプレイにハードウェア アラートのエラー メッセージを表示するには、次の手順に従います。

ハードウェア アラートのエラー メッセージを確認するには、以下のようにします。

ステップ 1　[Error Alert] モードで、[HARDWARE ERROR!] 行にある右矢印（→）キーを押して、[Error Alert] モードをトリガーしたハードウェア エラーを表示させます。

LCD パネルに、NFE platform デーモンの障害から始まるエラー アラート メッセージがリストされ、それに続いてエラー メッセージのリストが表示されます。

```
NFEplatformd X
NFEtemp X          ↓
```

ここで、*x* はアラートを生成したアクセラレータ カード（0 または 1）です。

ステップ 2　エラーをさらに表示するには、エラー メッセージの行にある下矢印（â）キーを押します。その他のエラーがない場合、[Exit] 行が表示されます。

```
Exit               →
```

ステップ 3　[Error Alert] モードを終了するには、右矢印（→）キーを押します。

アラートをトリガーしたエラーを解決する前に [Error Alert] モードを終了した場合、LCD パネルは [Error Alert] モードに戻ります。支援が必要な場合は、サポートに連絡してください。

ハードウェア仕様

FireSIGHT システムはさまざまなアプライアンスに提供されており、組織のニーズを満たします。アプライアンスをラックに設置する方法の詳細については、「ラックとキャビネットの取り付けオプション」（P.6-1）を参照してください。

（注） ASA FirePOWER デバイスのハードウェア仕様については、ASA のマニュアルを参照してください。

各アプライアンスのハードウェア仕様は次のセクションで説明します。

ラックとキャビネットの取り付けオプション

FireSIGHT システム アプライアンスは、ラックとサーバのキャビネットに配置できます。3D7010、3D7020、および 3D7030 を除くアプライアンスには、ラックマウント キットが同梱されています。ラックにアプライアンスを取り付ける方法については、ラックマウント キットとともに提供された手順を参照してください。

3D7010、3D7020、および 3D7030 にはトレイとラックマウント キットが必要です。これは別個に入手できます。他のアプライアンスのラックおよびキャビネット マウント キットは別に購入できます。

防御センター

防御センターの詳細情報については、以下を参照してください。

DC750

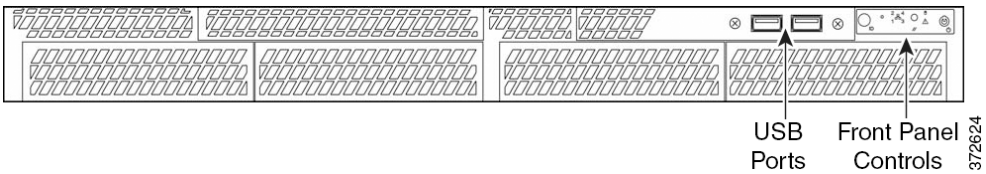
DC750 は、1 U アプライアンスです。アプライアンスの詳細情報については、以下を参照してください。

- 「DC750 シャーシ前面図」（P.6-2）
- 「DC750 シャーシ背面図」（P.6-4）
- 「DC750 の物理パラメータおよび環境パラメータ」（P.6-5）

DC750 シャーシ前面図

DC750 シャーシの前面には前面パネル コントロールがあります。

図 6-1　　DC750



次の図に、DC750 の前面パネルのコントロールと LED を示します。ハードディスク ドライブとシステムのステータス アイコン、NIC の番号（1、2、3、4）とアクティビティ ステータス、および電源ボタンも LED です。

図 6-2　　DC750

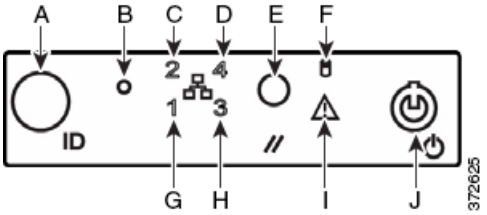


表 6-1　　前面パネルのコンポーネント

A	ID LED 付き ID ボタン	F	ハード ディスク ドライブのステータス LED
B	マスク不能割り込みボタン	G	NIC 1 のアクティビティ ステータス LED
C	NIC 2 のアクティビティ ステータス LED	H	NIC 3 のアクティビティ ステータス LED
D	NIC 4 のアクティビティ ステータス LED	I	システム ステータス LED
E	リセット ボタン	J	電源 LED 付き電源ボタン

シャーシの前面パネルは、システムの動作状態を表示するため、ユーザが確認できる 5 個の LED を備えています。次の表に、前面パネルの LED の説明を示します。

表 6-2　DC750 前面パネル LED

LED	説明
システム ステータス	以下のようにシステム ステータスを示します。 • 緑のライトはシステムが正常に動作していることを示します。 • 緑のライトの点滅はシステムが Degraded 状態で動作していることを示します。 詳細については、表 6-3（P.6-3）を参照してください。
電源	システムに電力が供給されているか、スリープ状態かを示します。 • 緑のライトはシステムが正常に動作していることを示します。 • ライトが消灯している場合、システムはオフです。 • 緑のライトの点滅はシステムがスリープ状態にあることを示します。 スリープ表示の間は、チップセットによってスタンバイ状態が維持されます。BIOS を経由せずに電源がオフになった場合、BIOS によって状態がクリアされるまでは、システムの電源を投入すると、電源がオフのときに有効であった状態に復元されます。システムが正常に電源オフにならなかった場合、電源ライトが点滅すると同時にシステム ステータス ライトがオフになる場合があります。これは、障害または設定変更により BIOS を実行できないためです。
ハードドライブ アクティビティ	ハード ドライブ アクティビティを示します。 • 緑のライトの点滅は固定ディスク ドライブがアクティブであることを示します。 • ライトが消灯している場合、ドライブ アクティビティがないか、またはシステムの電源がオフかスリープ状態です。 ドライブ アクティビティは、オンボード ハード ディスク コントローラによって決定されます。サーバのボードからも、アドイン コントローラがこのライトにアクセスするヘッダーが提供されます。
NIC アクティビティ	システムとネットワークの間のアクティビティを示します。 • 緑のライトの点滅はアクティビティがあることを示します。 • ライトが消灯している場合、アクティビティはありません。

次の表に、システム ステータス LED が点灯する可能性がある条件について示します。

表 6-3　DC750 システム ステータス

条件	説明
Critical	次のイベントに関連する、重大またはリカバリ不能なしきい値を超過した。 • 温度、電圧、またはファンの重大なしきい値を超過した • 電源サブシステムの障害 • プロセッサが正しく取り付けられていない、またはプロセッサが非互換のため、システムの電源をオンにできない • 重大なイベント ロギング エラー。システム メモリの修正不能な ECC エラーや、PCI SERR および PERR など致命的/修正不可能なバス エラーなど

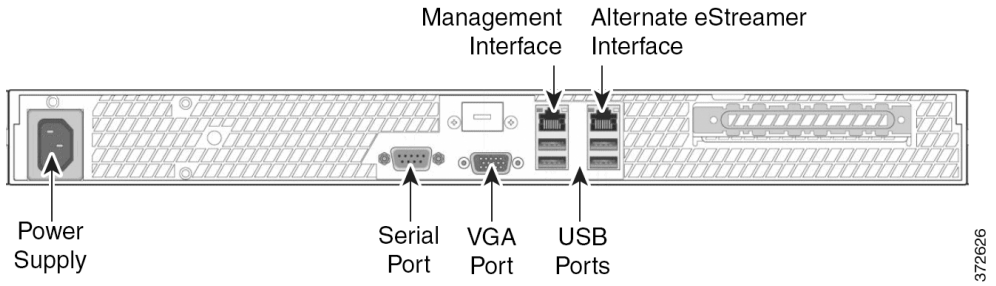
表 6-3　DC750 システム ステータス （続き）

条件	説明
Non-critical	Non-critical 状態は、次のイベントに関連するしきい値を超過した。 • 温度、電圧、またはファンの重大ではないしきい値を超過した • シャーシのトレスパス • システム BIOS の Set Fault Indication コマンド。BIOS は、システム メモリや CPU の設定変更など、ほかの重大でない状態を示すため、このコマンドを使用する場合があります。
Degraded	Degraded 状態は次のイベントに関連付けられています。 • 1 つ以上のプロセッサが Fault Resilient Boot（FRB）または BIOS により無効になっている • BIOS により、システム メモリの一部がディセーブルにされたか、またはマップアウトした

DC750 シャーシ背面図

シャーシの背面には、DC750 の電源と接続ポートがあります。

図 6-3　DC750



次の表に、アプライアンスの背面にある機能について示します。

表 6-4　DC750 システム コンポーネント：背面図

機能	説明
電源モジュール	AC 電源からの電力を防御センターに供給します。
シリアル ポート、 VGA ポート USB ポート	デバイスにモニタ、キーボード、およびマウスを接続するために使用します。
10/100/1000 Mbps イーサネット管理インターフェイス	アウトオブバンド管理ネットワーク接続を提供します。管理インターフェイスは、メンテナンスおよび設定の目的**のみ**で使用します。サービス トラフィックを伝送することは意図されていません。
代替 eStreamer インターフェイス	eStreamer クライアントに代替インターフェイスを提供します。

10/100/1000 Mbps 管理インターフェイスは、アプライアンスの背面にあります。次の表に、管理インターフェイスに関連付けられた LED の説明を示します。

表 6-5　DC750 管理インターフェイスの LED

LED	説明
左（リンク）	リンクが動作しているかどうかを示します。 • ライトが点灯している場合、リンクは動作中です。 • ライトが消灯している場合、リンクはありません。
右（アクティビティ）	ポートのアクティビティを示します。 • ライトの点滅はアクティビティを示します。 • ライトが消灯している場合、リンクはありません。

DC750 の物理パラメータおよび環境パラメータ

次の表に、アプライアンスの物理的な属性と環境パラメータを示します。

表 6-6　DC750 の物理パラメータおよび環境パラメータ

パラメータ	DC750
フォーム ファクタ	1 U
寸法（奥行 x 幅 x 高さ）	21.8 インチ x 17.25 インチ x 1.67 インチ （55.37 cm x 43.82 cm x 4.24 cm）
最大重量	33 ポンド （15 kg）
電源モジュール	120 VAC 用 250 W 電源モジュール 110 V、50/60 Hz で最大 6.0 A 220 V、50/60 Hz で最大 3.0 A
動作温度	50 ˚F ～ 95 ˚F（10 ˚C ～ 35 ˚C）。最大温度変化が 1 時間あたり 18 ˚F（10 ˚C）を超えないこと
非動作時温度	-40 ˚F ～ +158 ˚F（-40 ˚C ～ +70 ˚C）
非動作時湿度	90 %。95 ˚F（35 ˚C）で結露しないこと
音響ノイズ	一般的なオフィスの周囲温度（23 +/- 2 ˚C、73 +/- 4 ˚F）でアイドル状態時に 7.0 dBA
耐衝撃性	2 G の 1/2 正弦衝撃（11 ミリ秒）でエラーなし
パッケージ状態での耐衝撃性	24 インチ （60 cm）の自由落下の後、表面に損傷があったとしても動作可能。 シャーシ重量 40 ～ 80 ポンド （18 ～ 36 kg）
ESD	大気放電で +/-12 kV、接触放電で 8 K
エアーフロー	前面から背面
システム冷却要件	1660 BTU/時

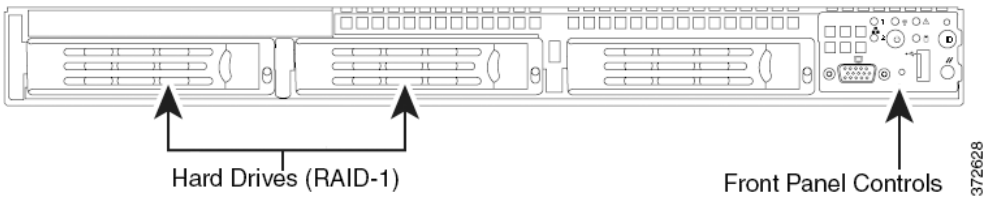
DC1500

DC 1500 は、1 U アプライアンスです。アプライアンスの詳細情報については、以下を参照してください。

- 「DC1500 シャーシ前面図」（P.6-6）
- 「DC1500 シャーシの背面図」（P.6-8）
- 「DC1500 の物理パラメータおよび環境パラメータ」（P.6-9）

DC1500 シャーシ前面図

シャーシの前面には、ハード ドライブおよび前面パネル コントロールがあります。



次の図に、前面パネルのコントロールおよび LED を示します。

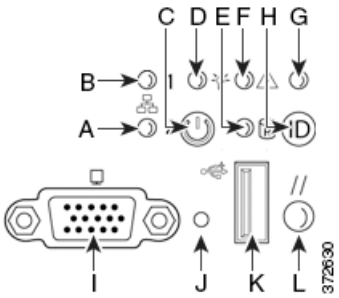


表 6-7　前面パネルのコンポーネント

A	NIC 2 のアクティビティ LED	G	ID LED
B	NIC 1 アクティビティ LED	H	ID ボタン
C	電源ボタン	I	ビデオ コネクタ（使用不可）
D	電源/スリープ LED	J	マスク不能割り込みボタン
E	固定ディスク ドライブのステータス	K	USB 2.0 コネクタ
F	システム ステータス LED	L	リセット ボタン

シャーシの前面パネルは、システムの動作状態を表示するため、ユーザが確認できる前面ベゼル付きまたはベゼルなしの 6 個の LED を備えています。次の表に、前面パネルの LED の説明を示します。

表 6-8　DC1500 前面パネル LED

LED	説明
NIC 1 アクティビティ NIC 2 アクティビティ	システムとネットワークの間のアクティビティを示します。 • 緑のライトの点滅はアクティビティを示します。 • ライトが消灯している場合、アクティビティはありません。
電源/スリープ	システムに電力が供給されているか、スリープ状態かを示します。 • 緑のライトはシステムが正常に動作していることを示します。 • 緑のライトの点滅はシステムがスリープ状態にあることを示します。 • ライトが消灯している場合、システムに電力が供給されていないことを示します。 スリープ表示の間は、チップセットによってスタンバイ状態が維持されます。BIOS を経由せずに電源がオフになった場合、BIOS によって状態がクリアされるまでは、システムの電源を投入すると、電源がオフのときに有効であった状態に復元されます。システムが正常に電源オフにならなかった場合、電源ライトが点滅すると同時にシステム ステータス ライトがオフになる場合があります。これは、障害または設定変更により BIOS を実行できないためです。
ハード ドライブ アクティビティ	ハード ドライブ アクティビティを示します。 • 緑のライトの点滅は固定ディスク ドライブがアクティブであることを示します。 • オレンジのライトは固定ディスク ドライブに障害があることを示します。 • ライトが消灯している場合、ドライブ アクティビティがないか、またはシステムの電源がオフかスリープ状態です。 ドライブ アクティビティは、オンボード ハード ディスク コントローラによって決定されます。サーバのボードからも、アドイン コントローラがこのライトにアクセスするヘッダーが提供されます。
システム ステータス	以下のようにシステム ステータスを示します。 • 緑のライトはシステムが正常に動作していることを示します。 • 緑のライトの点滅はシステムが Degraded 状態で動作していることを示します。 • オレンジのライトは、システムが重大またはリカバリ不能な状態にあることを示します。 • オレンジのライトの点滅は、システムが Non-critical な状態であることを示します。 • ライトが消灯している場合、パワーオン セルフテスト（POST）処理中、またはシステムが停止していることを示します。 **（注）** オレンジのステータス ライトの方が緑のステータス ライトよりも優先されます。オレンジのライトが点灯または点滅している場合、緑のライトは消灯します。 詳細については、表 6-3（P.6-3）を参照してください。
システム ID	高密度ラックに設置するシステムを他の類似したシステムと区別して特定します。 • 青いライトは ID ボタンが押されたことを示します。青いライトはアプライアンスの背面にあります。 • ライトが消灯している場合、ID ボタンは押されていません。

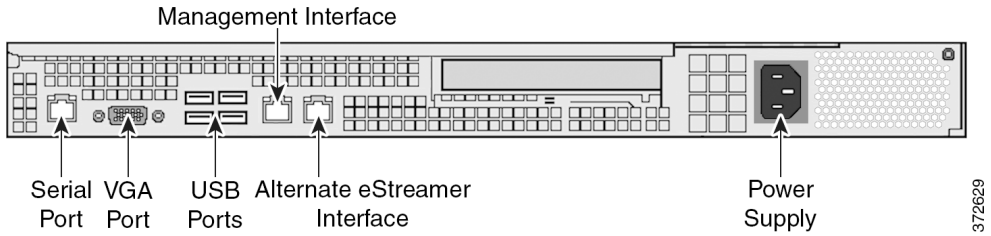
次の表に、システム ステータス LED が点灯する可能性がある条件について示します。

表 6-9　DC1500 システム ステータス

条件	説明
Critical	次のイベントに関連する、重大またはリカバリ不能なしきい値を超過した。 • 温度、電圧、またはファンの重大なしきい値を超過した • 電源サブシステムの障害 • プロセッサが正しく取り付けられていない、またはプロセッサが非互換のため、システムの電源をオンにできない • 重大なイベント ロギング エラー。システム メモリの修正不能な ECC エラーや、PCI SERR および PERR など致命的/修正不可能なバス エラーなど
Non-critical	Non-critical 状態は、次のイベントに関連するしきい値を超過した。 • 温度、電圧、またはファンの重大ではないしきい値を超過した • シャーシのトレスパス • システム BIOS の Set Fault Indication コマンド。BIOS は、システム メモリや CPU の設定変更など、ほかの重大でない状態を示すため、このコマンドを使用する場合があります。
Degraded	Degraded 状態は次のイベントに関連付けられています。 • 1 つ以上のプロセッサが Fault Resilient Boot（FRB）または BIOS により無効になっている • BIOS により、システム メモリの一部がディセーブルにされたか、またはマップアウトした

DC1500 シャーシの背面図

シャーシの背面には、接続ポートと電源があります。



次の表に、アプライアンスの背面にある機能について示します。

表 6-10　DC1500 システム コンポーネント：背面図

機能	説明
電源モジュール	AC 電源からの電力を防御センターに供給します。
VGA ポート USB ポート	防御センター にモニタ、キーボード、およびマウスを接続するために使用します。
10/100/1000 Mbps イーサネット管理インターフェイス	アウトオブバンド管理ネットワーク接続を提供します。管理インターフェイスは、メンテナンスおよび設定の目的**のみ**で使用します。サービス トラフィックを伝送することは意図されていません。

表 6-10　DC1500 システム コンポーネント：背面図 （続き）

機能	説明
代替 eStreamer インターフェイス	eStreamer クライアントに代替インターフェイスを提供します。
RJ45 シリアル ポート	アプライアンスのすべての管理サービスにダイレクト アクセスするため、ワークステーションとアプライアンスの直接接続（RJ45 を使用して DB-9 アダプタへ）を確立できるようにします。RJ45 シリアル ポートは、メンテナンスおよび設定目的**のみ**で使用します。サービス トラフィックを伝送することは意図されていません。 **（注）** 前面パネルと背面パネルの両方のシリアル ポートを同時に使用することはできません。

10/100/1000 Mbps 管理インターフェイスは、アプライアンスの背面にあります。次の表に、管理インターフェイスに関連付けられた LED の説明を示します。

表 6-11　DC1500 管理インターフェイスの LED

LED	説明
左（リンク）	リンクが動作しているかどうかを示します。 • ライトが点灯している場合、リンクは動作中です。 • ライトが消灯している場合、リンクはありません。
右（アクティビティ）	ポートのアクティビティを示します。 • ライトの点滅はアクティビティを示します。 • ライトが消灯している場合、アクティビティはありません。

DC1500 の物理パラメータおよび環境パラメータ

次の表に、アプライアンスの物理的な属性と環境パラメータを示します。

表 6-12　DC1500 の物理パラメータおよび環境パラメータ

パラメータ	説明
フォーム ファクタ	1 U
寸法（奥行 x 幅 x 高さ）	27.2 インチ x 16.93 インチ x 1.7 インチ （69.1 cm x 43.0 cm x 4.3 cm）
最大重量	34 ポンド （15.4 kg）
電源モジュール	120 VAC 用 600 W 電源モジュール 110 V、50/60 Hz で最大 9.5 A 220 V、50/60 Hz で最大 4.75 A
動作温度	50 ˚F ～ 95 ˚F（10 ˚C ～ 35 ˚C）
非動作時温度	-40 ˚F ～ +158 ˚F（-40 ˚C ～ +70 ˚C）
非動作時湿度	90 %。82.4 ˚F（28 ˚C）で結露しないこと
音響ノイズ	一般的なオフィスの周囲温度でアイドル状態時に 7.0 dBA 未満（ラックマウント）
耐衝撃性	2 G の 1/2 正弦衝撃（11 ミリ秒）でエラーなし

表 6-12　DC1500 の物理パラメータおよび環境パラメータ （続き）

パラメータ	説明
パッケージ状態での耐衝撃性	24 インチ （60 cm）の自由落下の後、表面に損傷があったとしても動作可能。 シャーシ重量 40 ～ 80 ポンド （18 ～ 36 kg）
ESD	Intel 環境テスト仕様で +/- 15 kV（I/O ポート +/- 8 KV）
エアーフロー	前面から背面
システム冷却要件	2550 BTU/時

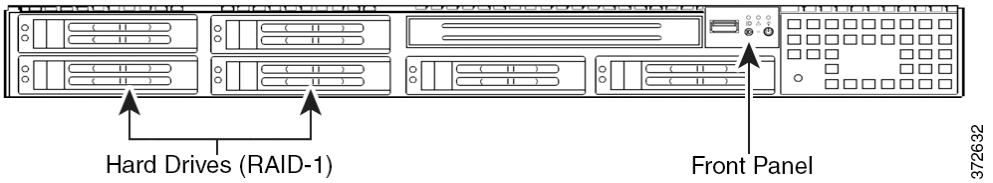
DC3500

DC3500 は、1 U アプライアンスです。アプライアンスの詳細情報については、以下を参照してください。

- 「DC3500 シャーシ前面図」（P.6-10）
- 「DC3500 シャーシの背面図」（P.6-12）
- 「DC3500 の物理パラメータおよび環境パラメータ」（P.6-14）

DC3500 シャーシ前面図

シャーシの前面には、ハード ドライブおよび前面パネルがあります。



アプライアンスの前面には、前面パネル用のコントロールと LED 表示があります。

次の図に、前面パネルのコントロールおよび LED を示します。

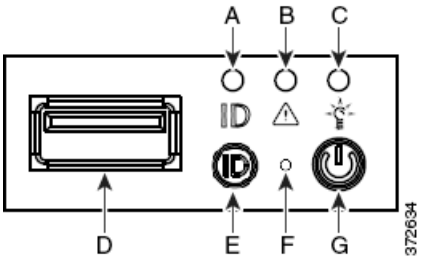


表 6-13　前面パネルのコンポーネント

A	ID LED	E	ID ボタン
B	システム ステータス LED	F	リセット ボタン
C	電源 LED	G	電源ボタン
D	USB ポート		

シャーシの前面パネルは、システムの動作状態を示す 3 個の LED を備えています。次の表に、前面パネルの LED の説明を示します。

表 6-14　DC3500 前面パネル LED

LED	説明
電源	システムに電力が供給されているかどうかを示します。 • 緑のライトはシステムに電力が供給されていることを示します。 • ライトが消灯している場合、システムに電力が供給されていないことを示します。
システム ステータス	システム ステータスを示します。 • 緑のライトはシステムが正常に動作していることを示します。 • 緑のライトの点滅はシステムが Degraded 状態で動作していることを示します。 • オレンジのライトの点滅は、システムが Non-critical な状態であることを示します。 • オレンジのライトは、システムが重大またはリカバリ不能な状態にあることを示します。 • ライトが消灯している場合、システムが起動処理中またはオフであることを示します。 **（注）** オレンジのステータス ライトの方が緑のステータス ライトよりも優先されます。オレンジのライトが点灯または点滅している場合、緑のライトは消灯します。 詳細については、「表 6-15（P.6-12）」を参照してください。
ハード ドライブ アクティビティ	ハード ドライブ ステータスを示します。 • 緑のライトの点滅は固定ディスク ドライブがアクティブであることを示します。 • オレンジのライトは固定ディスク ドライブに障害があることを示します。 • ライトが消灯している場合、ドライブ アクティビティがないか、またはシステムの電源がオフです。
NIC アクティビティ	ネットワーク アクティビティがあるかどうかを示します。 • 緑のライトの点滅はネットワーク アクティビティがあることを示します。 • ライトが消灯している場合、ネットワーク アクティビティはありません。
システム ID	高密度ラックに設置するシステムを他の類似したシステムと区別して特定します。 • 青いライトは ID ボタンが押されたことを示します。青いライトはアプライアンスの背面にあります。 • ライトが消灯している場合、ID ボタンは押されていません。

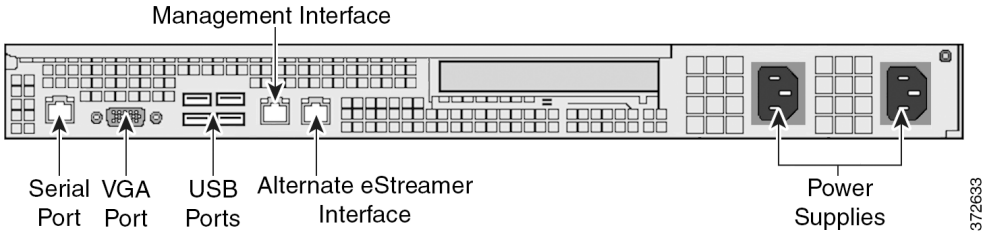
次の表に、システム ステータス LED が点灯する可能性がある条件について示します。

表 6-15　DC3500 システム ステータス

条件	説明
Critical	次のイベントに関連する、重大またはリカバリ不能なしきい値を超過した。 • 温度、電圧、またはファンの重大なしきい値を超過した • 電源サブシステムの障害 • プロセッサが正しく取り付けられていない、またはプロセッサが非互換のため、システムの電源をオンにできない • 重大なイベント ロギング エラー。システム メモリの修正不能な ECC エラーや、PCI SERR および PERR など致命的/修正不可能なバス エラーなど
Non-critical	Non-critical 状態は、次のイベントに関連するしきい値を超過した。 • 温度、電圧、またはファンの重大ではないしきい値を超過した • シャーシのトレスパス • システム BIOS の Set Fault Indication コマンド。BIOS は、システム メモリや CPU の設定変更など、ほかの重大でない状態を示すため、このコマンドを使用する場合があります。
Degraded	Degraded 状態は次のイベントに関連付けられています。 • 1 つ以上のプロセッサが Fault Resilient Boot（FRB）または BIOS により無効になっている • BIOS により、システム メモリの一部がディセーブルにされたか、またはマップアウトした • 電源の 1 つのケーブルが外れているか、または機能していない **ヒント** Degraded 状態の表示を確認するには、まず電源の接続を確認します。アプライアンスの電源をオフにし、両方の電源コードを外し、電源コードを再接続し、アプライアンスを再起動します。 ⚠ **注意** 安全に電源をオフにするには、『*FireSIGHT System User Guide*』の「デバイスの管理」の章に示された手順を使用するか、または防御センターのシェルから `shutdown -h now` コマンドを使用します。

DC3500 シャーシの背面図

シャーシの背面には、接続ポートと電源があります。



次の表に、アプライアンスの背面にある機能について示します。

表 6-16　DC3500 システム コンポーネント：背面図

機能	説明
PS/2 マウス コネクタ PS/2 キーボード コネクタ VGA ポート USB ポート	ワークステーションとアプライアンスの直接接続を確立するため、RJ45 シリアル ポートを使用するか代わりに、モニタ、キーボード、およびマウスをアプライアンスに接続できるようにします。また、アプライアンスに同梱されたサム ドライブを使用して、工場出荷時の初期状態に戻すためにも USB ポートを使用します。
RJ45 シリアル ポート	アプライアンスのすべての管理サービスにダイレクト アクセスするため、ワークステーションとアプライアンスの直接接続（RJ45 を使用して DB-9 アダプタへ）を確立できるようにします。RJ45 シリアル ポートは、メンテナンスおよび設定目的**のみ**で使用します。サービス トラフィックを伝送することは意図されていません。 **（注）** 前面パネルと背面パネルの両方のシリアル ポートを同時に使用することはできません。
10/100/1000 Mbps イーサネット管理インターフェイス	アウトオブバンド管理ネットワーク接続を提供します。管理インターフェイスは、メンテナンスおよび設定の目的**のみ**で使用します。サービス トラフィックを伝送することは意図されていません。
代替 eStreamer インターフェイス	eStreamer クライアントに代替インターフェイスを提供します。
冗長電源	AC 電源からの電力をアプライアンスに供給します。

10/100/1000 Mbps 管理インターフェイスは、アプライアンスの背面にあります。次の表に、管理インターフェイスに関連付けられた LED の説明を示します。

表 6-17　DC3500 管理インターフェイスの LED

LED	説明
左（アクティビティ）	ポートのアクティビティを示します。 • ライトの点滅はアクティビティを示します。 • ライトが消灯している場合、アクティビティはありません。
右（リンク）	リンクが動作しているかどうかを示します。 • ライトはリンクが動作していることを示します。 • ライトが消灯している場合、リンクはありません。

電源モジュールは、アプライアンスの背面にあります。次の表に、デュアル電源に関連する LED の説明を示します。

表 6-18　DC3500 電源 LED

LED	説明
消灯	電源が接続されていない。
オレンジ	このモジュールに電力が供給されていない。 または モジュール障害、ヒューズ切れ、ファンの障害などの電源の重大なイベントがあり、電源がシャット ダウンされている。

表 6-18　DC3500 電源 LED （続き）

LED	説明
オレンジに点滅	高温またはファン速度低下などの電源の警告イベントが発生した。電源は動作を続行。
緑色に点滅	AC 入力があり、電圧はスタンバイ状態、電源スイッチはオフ。
グリーン	電源が接続され、オンになっている。

DC3500 の物理パラメータおよび環境パラメータ

次の表に、アプライアンスの物理的な属性と環境パラメータを示します。

表 6-19　DC3500 の物理パラメータおよび環境パラメータ

パラメータ	説明
フォーム ファクタ	1 U
寸法（奥行 x 幅 x 高さ）	26.2 インチ x 16.93 インチ x 1.7 インチ （66.5 cm x 43.0 cm x 4.3 cm）
重量	38 ポンド （17.2 kg）
電源モジュール	120 VAC でデュアル 650 W 冗長電源 110 V、50/60 Hz で最大 8.5 A 220 V、50/60 Hz で最大 4.2 A
動作温度	50 ˚F ～ 95 ˚F（10 ˚C ～ 35 ˚C）
非動作時温度	-40 ˚F ～ 158 ˚F（-40 ˚C ～ 70 ˚C）
湿度（動作時）	5 % ～ 85 %
非動作時湿度	90 %。95 ˚F（35 ˚C）で結露しないこと
音響ノイズ	一般的なオフィスの周囲温度でアイドル状態時に 7.0 dBA 未満（ラックマウント）
耐衝撃性	2 G の 1/2 正弦衝撃（11 ミリ秒 ）でエラーなし
パッケージ状態での耐衝撃性	24 インチ （60 cm）の自由落下の後、表面に損傷があったとしても動作可能。 シャーシ重量 40 ～ 80 ポンド （18 ～ 36 kg）
ESD	Intel 環境テスト仕様で +/- 15 kV（I/O ポート +/- 8 KV）
エアーフロー	前面から背面
システム冷却要件	2550 BTU/時
RoHS	RoHS 指令 2002/95/EC 準拠

7000 シリーズ デバイス

すべての 7000 シリーズ デバイスには、アプライアンス前面に LCD パネルがあり、このパネルでアプライアンスの設定の表示、およびイネーブルにされている場合は設定ができます。

各デバイスの詳細情報については、以下を参照してください。

- 「3D7010、3D7020、および 3D7030」（P.6-15）
- 「3D7110 および 3D7120」（P.6-20）
- 「3D7115、3D7125、および AMP7150」（P.6-27）

3D7010、3D7020、および 3D7030

3D7010、3D7020、および 3D7030 デバイスも、70xx ファミリ と呼ばれ、1 U アプライアンスでラック トレイの 2 分の 1 幅であり、それぞれ設定可能なバイパス機能を持つ 8 個の銅線インターフェイスが装備されています。70xx ファミリアプライアンスの安全上の考慮事項については、『*Regulatory Compliance and Safety Information for FirePOWER and FireSIGHT Appliances*』を参照してください。

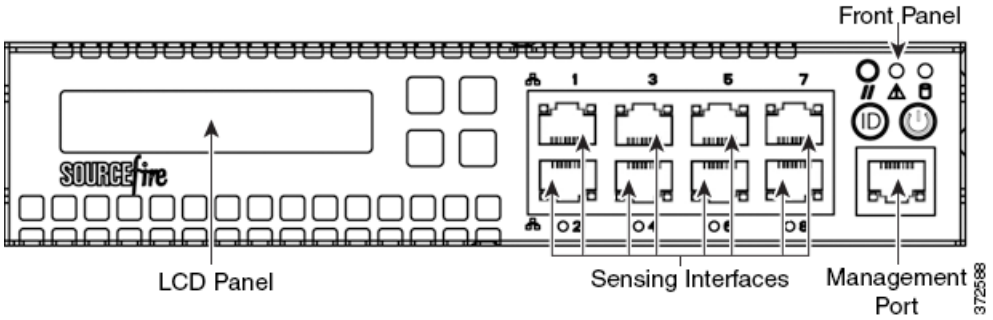
詳細については、次の項を参照してください。

- 「70xx ファミリ 前面図」（P.6-15）
- 「70xx ファミリ 背面図」（P.6-19）
- 「70xx ファミリ の物理パラメータおよび環境パラメータ」（P.6-19）

70xx ファミリ 前面図

シャーシの前面には、LCD パネル、センシング インターフェイス、前面パネル、および管理インターフェイスがあります。

図 6-4　70xx ファミリ（シャーシ：CHRY-1U-AC）前面図



次の表に、アプライアンスの前面にある機能について示します。

表 6-20　70xx ファミリ システム コンポーネント：前面図

機能	説明
LCD パネル	複数のモードで動作し、デバイスの設定、エラー メッセージの表示、システム ステータスの表示を行います。詳細については、「シリーズ 3 デバイスでの LCD パネルの使用」（P.5-1）を参照してください。
センシング インターフェイス	ネットワークに接続するセンシング インターフェイスです。詳細については、「センシング インターフェイス」（P.6-17）を参照してください。
10/100/1000 イーサネット管理インターフェイス	アウトオブバンド管理ネットワーク接続を提供します。管理インターフェイスは、メンテナンスおよび設定の目的**のみ**で使用します。サービス トラフィックを伝送することは意図されていません。
前面パネル	システムの動作状態、および電源ボタンなどのさまざまなコントロールを示す LED を備えています。詳細については、「表 6-303D7110 および 3D7120 前面パネル コンポーネント」（P.6-22）を参照してください。

図 6-5　70xx ファミリ の前面パネル

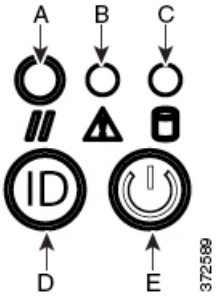


表 6-21　前面パネルのコンポーネント

A	リセット ボタン	D	システム ID ボタン
B	システム ステータス LED	E	電源ボタンおよび LED
C	ハード ドライブ アクティビティ LED		

シャーシの前面パネルは、システムの動作状態を示す LED を備えています。次の表に、前面パネルの LED の説明を示します。

表 6-22　70xx ファミリ前面パネル LED

LED	説明
リセット ボタン	電源を外さずにアプライアンスをリブートするために使用します。
システム ステータス	システム ステータスを示します。 • 緑のライトはシステムに電力が供給され正常に動作しているか、または電力が供給されていないが AC 電源に接続されていることを示します。 • オレンジのライトはシステム障害を示します。 詳細については、「表 6-23（P.6-17）」を参照してください。
ハード ドライブ アクティビティ	ハード ドライブ ステータスを示します。 • 緑のライトの点滅は固定ディスク ドライブがアクティブであることを示します。 • ライトが消灯している場合、ドライブ アクティビティがないか、システムの電源がオフになっています。
システム ID	押されたとき、ID ボタンには青いライトが表示されます。青いライトはシャーシの背面で確認できます。
電源ボタンおよび LED	アプライアンスに電力が供給されているかどうかを示します。 • 緑のライトはアプライアンスに電源が供給されていて、システムがオンであることを示します。 • ライトが消灯している場合、システムがシャット ダウンされているか、電力が供給されていません。

次の表に、システム ステータス LED が点灯する可能性がある条件について示します。

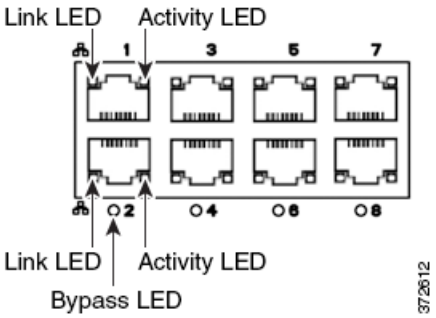
表 6-23　　70xx ファミリ システム ステータス

条件	説明
Critical	次のイベントに関連する、重大またはリカバリ不能なしきい値を超過した。 • 温度、電圧、またはファンの重大なしきい値を超過した • 電源サブシステムの障害 • プロセッサが正しく取り付けられていない、またはプロセッサが非互換のため、システムの電源をオンにできない • 重大なイベント ロギング エラー。システム メモリの修正不能な ECC エラーや、PCI SERR および PERR など致命的/修正不可能なバス エラーなど
Non-critical	Non-critical 状態は、次のイベントに関連するしきい値を超過した。 • 温度、電圧、またはファンの重大ではないしきい値を超過した • システム BIOS の Set Fault Indication コマンド。BIOS は、システム メモリや CPU の設定変更など、ほかの重大でない状態を示すため、このコマンドを使用する場合があります。
Degraded	Degraded 状態は次のイベントに関連付けられています。 • 1 つ以上のプロセッサが Fault Resilient Boot（FRB）または BIOS により無効になっている • BIOS により、システム メモリの一部がディセーブルにされたか、またはマップアウトした • 電源の 1 つのケーブルが外れているか、または機能していない

センシング インターフェイス

70xx ファミリ アプライアンスには、それぞれ設定可能なバイパス機能を持つ 8 個の銅線インターフェイスが装備されています。

図 6-6　　8 ポート 1000BASE-T 銅線インターフェイス



次の表に、銅線インターフェイスのアクティビティ LED とリンク LED の説明を示します。

表 6-24　70xx ファミリ 銅線リンク/アクティビティ LED

ステータス	説明
両方の LED がオフ	インターフェイスにリンクがない。
リンクがオレンジ	インターフェイスのトラフィック速度が 10 Mb または 100 Mb。
リンクが緑	インターフェイスのトラフィック速度が 1 Gb。
アクティビティが緑に点滅	インターフェイスにリンクがあり、トラフィックが通過中。

次の表に、銅線インターフェイスのバイパス LED の説明を示します。

表 6-25　70xx ファミリ 銅線のバイパス LED

ステータス	説明
消灯	インターフェイス ペアは、バイパス モードでないか、電力が供給されていない。
緑色で点灯	インターフェイス ペアは、バイパス モード開始可能。
黄色で点灯	インターフェイス ペアはバイパス モードになり、トラフィックを検査していない。
オレンジに点滅	インターフェイス ペアはバイパス モード、すなわちフェール オープンされている。

10/100/1000 管理インターフェイスは、アプライアンスの前面にあります。次の表に、管理インターフェイスに関連付けられた LED の説明を示します。

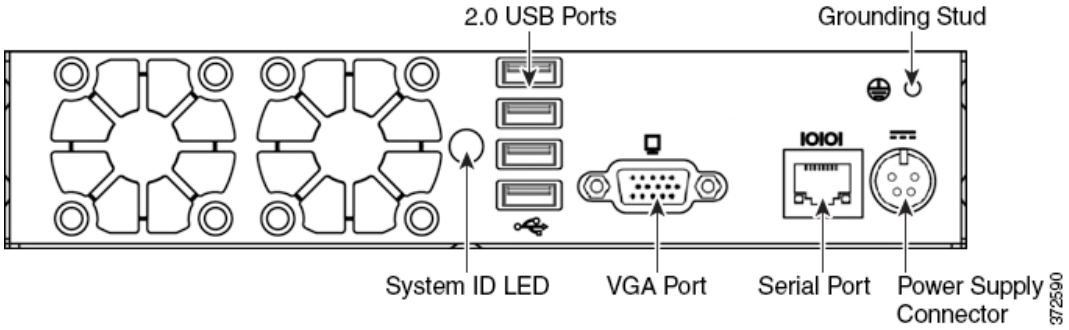
表 6-26　70xx ファミリ 管理インターフェイス LED

LED	説明
左（リンク）	リンクが動作しているかどうかを示します。ライトが点灯している場合、リンクは動作中です。ライトが消灯している場合、リンクはありません。
右（アクティビティ）	ポートのアクティビティを示します。ライトが点滅している場合、アクティビティがあります。ライトが消灯している場合、リンクはありません。

70xx ファミリ 背面図

シャーシの背面には、システム ID LED、接続ポート、接地スタッド、および電源コネクタがあります。

図 6-7　　70xx ファミリ（シャーシ：CHRY-1U-AC）背面図



次の表に、アプライアンスの背面にある機能について示します。

表 6-27　　70xx ファミリ システム コンポーネント：背面図

機能	説明
システム ID LED	高密度ラックに設置するシステムを他の類似したシステムと区別して特定します。青い LED は ID ボタンが押されたことを示します。
USB 2.0 ポート VGA ポート シリアル ポート	ワークステーションとアプライアンスの直接接続を確立するため、RJ45 シリアル ポートの代わりとして、デバイスにモニタ、キーボード、およびマウスを接続できるようにします。
アース スタッド	共通ボンディング網にアプライアンスを接続するために使用します。詳細については、「FirePOWER デバイスの所要電力」（P.A-1）を参照してください。
12 V 電源コネクタ	AC 電源からデバイスへの電源接続を提供します。

70xx ファミリ の物理パラメータおよび環境パラメータ

次の表に、アプライアンスの物理的な属性と環境パラメータを示します。

表 6-28　　70xx ファミリ の物理パラメータおよび環境パラメータ

パラメータ	説明
フォーム ファクタ	1 U、ラック ハーフ幅
寸法（奥行 x 幅 x 高さ）	単一シャーシ：12.49 インチ x 7.89 インチ x 1.66 インチ（31.74 cm x 20.04 cm x 4.21 cm） 2 シャーシ トレイ：25.05 インチ x 17.24 インチ x 1.73 インチ （63.62 cm × 43.8 cm × 4.44 cm）
シャーシの重量 最大搭載量	シャーシ：7 ポンド （3.17 kg） 単一シャーシ、トレイに電源：17.7 ポンド （8.03 kg） シャーシ 2 台、単一トレイに電源：24.7 ポンド （11.2 kg）
銅線 1000BASE-T	ペア設定のギガビット銅線イーサネット バイパス可能インターフェイス ケーブルおよび距離：Cat5E、50 m

表 6-28　70xx ファミリ の物理パラメータおよび環境パラメータ （続き）

パラメータ	説明
電源モジュール	200W AC 電源 電圧：公称 100 VAC ～ 240 VAC（最大 90 VAC ～ 264 VAC） 電流：全範囲で最大 2 A 周波数範囲：公称 50/60 Hz（最大 47 Hz ～ 63 Hz）
動作温度	0 ˚C ～ 40 ˚C（32 ˚F ～ 104 ˚F）
非動作時温度	-20 ˚C ～ 70 ˚C（-29 ˚F ～ 158 ˚F）
湿度（動作時）	5 ～ 95 %、結露しないこと これらの制限を超えた動作は保証されず、推奨されません。
非動作時湿度	0 ～ 95 %、結露しないこと 装置は、相対湿度 95% 未満の結露しない環境で保管してください。装置を稼働させる前に、少なくとも 48 時間、最大動作湿度未満で慣らし運転してください。
高度	海抜 0 ～ 5905 フィート（0 ～ 1800 m）
冷却要件	682 BTU/時 必要な動作温度範囲内にアプライアンスを維持するための十分な冷却機能を提供します。これに失敗すると、アプライアンスに誤動作や損傷が発生することがあります。
音響ノイズ	アイドル時 53 dBA。プロセッサ最大負荷時 62 dBA。
耐衝撃性	5 G の 1/2 正弦衝撃（11 ミリ秒）でエラーなし
エアーフロー	1 分あたり 20 立方フィート（570 リットル） アプライアンスを通過するエアーフローは、前面から入って背面から出ます。側面への換気はありません。

3D7110 および 3D7120

71xx ファミリ に属する 3D7110 および 3D7120 デバイスは 1 U アプライアンスで、それぞれ設定可能なバイパス機能を持つ 8 個の銅線インターフェイスまたは 8 個の光ファイバ インターフェイスが装備されています。71xx ファミリアプライアンスの安全上の考慮事項については、『*Regulatory Compliance and Safety Information for FirePOWER and FireSIGHT Appliances*』を参照してください。

詳細については、次の項を参照してください。

- 「3D7110 および 3D7120 シャーシ前面図」（P.6-21）
- 「3D7110 および 3D7120 シャーシ背面図」（P.6-25）
- 「3D7110 および 3D7120 の物理パラメータおよび環境パラメータ」（P.6-26）

3D7110 および 3D7120 シャーシ前面図

シャーシの前面には、LCD パネル、USB ポート、前面パネル、および銅線または光ファイバのセンシング インターフェイスがあります。

図 6-8　銅線インターフェイスを備えた 3D7110 および 3D7120（シャーシ：GERY-1U-8-C-AC）

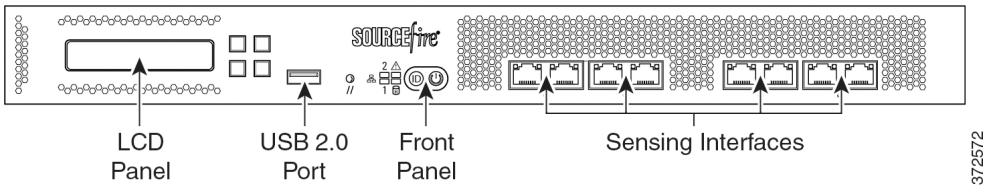
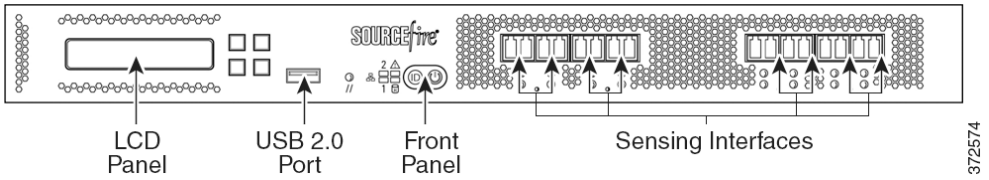


図 6-9　光ファイバ インターフェイスを備えた 3D7110 および 3D7120（シャーシ：GERY-1U-8-FM-AC）



次の表に、アプライアンスの前面にある機能について示します。

表 6-29　3D7110 および 3D7120 システム コンポーネント：前面図

機能	説明
LCD パネル	複数のモードで動作し、デバイスの設定、エラー メッセージの表示、システム ステータスの表示を行います。詳細については、「シリーズ 3 デバイスでの LCD パネルの使用」（P.5-1）を参照してください。
前面パネルの USB 2.0 ポート	デバイスにキーボードを接続するために使用します。
前面パネル	システムの動作状態、および電源ボタンなどのさまざまなコントロールを示す LED を備えています。詳細については、「図 6-103D7110 および 3D7120 前面パネル」（P.6-21）を参照してください。
センシング インターフェイス	ネットワークに接続するセンシング インターフェイスです。詳細については、「3D7110 および 3D7120 センシング インターフェイス」（P.6-23）を参照してください。

図 6-10　3D7110 および 3D7120 前面パネル

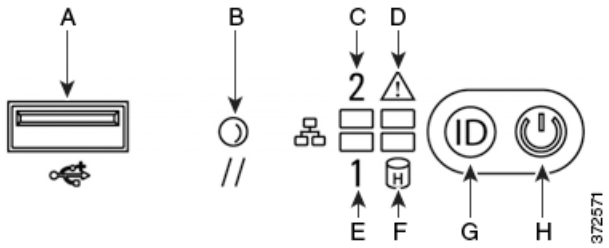


表 6-30　3D7110 および 3D7120 前面パネル コンポーネント

A	USB 2.0 コネクタ	E	NIC 1 アクティビティ LED
B	リセット ボタン	F	ハード ドライブ アクティビティ LED
C	NIC 2 アクティビティ LED	G	ID ボタン
D	システム ステータス LED	H	電源ボタンおよび LED

シャーシの前面パネルは、システムの動作状態を示す LED を備えています。次の表に、前面パネルの LED の説明を示します。

表 6-31　3D7110 および 3D7120 前面パネル LED

LED	説明
NIC アクティビティ（1 および 2）	ネットワーク アクティビティがあるかどうかを示します。 • 緑のライトの点滅はネットワーク アクティビティがあることを示します。 • ライトが消灯している場合、ネットワーク アクティビティはありません。
システム ステータス	システム ステータスを示します。 • ライトが消灯している場合、システムが正常に動作しているか、電源がオフです。 • 赤のライトは、システム エラーを示します。 詳細については、「表 6-323D7110 および 3D7120 システム ステータス」（P.6-23）を参照してください。
リセット ボタン	電源を外さずにアプライアンスをリブートするために使用します。
ハード ドライブ アクティビティ	ハード ドライブ ステータスを示します。 • 緑のライトの点滅は固定ディスク ドライブがアクティブであることを示します。 • オレンジのライトは固定ディスク ドライブに障害があることを示します。 • ライトが消灯している場合、ドライブ アクティビティがないか、システムの電源がオフになっています。
システム ID	高密度ラックに設置するシステムを他の類似したシステムと区別して特定します。 • 青いライトは ID ボタンが押されたことを示します。青いライトはアプライアンスの背面にあります。 • ライトが消灯している場合、ID ボタンは押されていません。
電源ボタンおよび LED	アプライアンスに電力が供給されているかどうかを示します。 • 緑のライトはアプライアンスに電源が供給されていて、システムがオンであることを示します。 • 緑のライトの点滅は、アプライアンスに電源が供給されていて、シャット ダウンされていることを示します。 • ライトが消灯している場合、システムに電源が供給されていません。

次の表に、システム ステータス LED が点灯する可能性がある条件について示します。

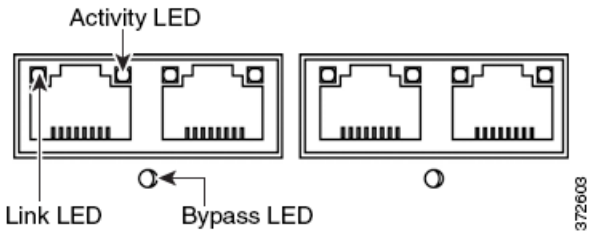
表 6-32　3D7110 および 3D7120 システム ステータス

条件	説明
Critical	次のイベントに関連する、重大またはリカバリ不能なしきい値を超過した。 • 温度、電圧、またはファンの重大なしきい値を超過した • 電源サブシステムの障害 • プロセッサが正しく取り付けられていない、またはプロセッサが非互換のため、システムの電源をオンにできない • 重大なイベント ロギング エラー。システム メモリの修正不能な ECC エラーや、PCI SERR および PERR など致命的/修正不可能なバス エラーなど
Non-critical	Non-critical 状態は、次のイベントに関連するしきい値を超過した。 • 温度、電圧、またはファンの重大ではないしきい値を超過した • シャーシのトレスパス • システム BIOS の Set Fault Indication コマンド。BIOS は、システム メモリや CPU の設定変更などの追加の、非クリティカルな状態を示すため、このコマンドを使用する場合があります。
Degraded	Degraded 状態は次のイベントに関連付けられています。 • 1 つ以上のプロセッサが Fault Resilient Boot（FRB）または BIOS により無効になっている • BIOS により、システム メモリの一部がディセーブルにされたか、またはマップアウトした • 電源の 1 つのケーブルが外れているか、または機能していない **ヒント** Degraded 状態の表示を確認するには、まず電源の接続を確認します。デバイスの電源をオフにし、両方の電源コードを外し、電源コードを再接続し、デバイスを再起動します。 ⚠ **注意** 安全に電源をオフにするには、『*FireSIGHT System User Guide*』の「デバイスの管理」の章に示された手順を使用するか、または CLI から `system shutdown` コマンドを使用します。

3D7110 および 3D7120 センシング インターフェイス

3D7110 および 3D7120 デバイスは、それぞれ設定可能なバイパス機能を持つ 8 ポート銅線インターフェイスまたは 8 ポート光ファイバ インターフェイスが装備されています。

図 6-11　8 ポート 1000BASE-T 銅線インターフェイス



次の表に、銅線インターフェイスのアクティビティ LED とリンク LED の説明を示します。

表 6-33　3D7110 および 3D7120 銅線リンク/アクティビティ LED

ステータス	説明
両方の LED がオフ	インターフェイスにリンクがない。
リンクがオレンジ	インターフェイスのトラフィック速度が 10 Mb または 100 Mb。
リンクが緑	インターフェイスのトラフィック速度が 1 Gb。
アクティビティが緑に点滅	インターフェイスにリンクがあり、トラフィックが通過中。

次の表に、銅線インターフェイスのバイパス LED の説明を示します。

表 6-34　3D7110 および 3D7120 銅線のバイパス LED

ステータス	説明
消灯	インターフェイス ペアは、バイパス モードでないか、電力が供給されていない。
緑色で点灯	インターフェイス ペアは、バイパス モード開始可能。
黄色で点灯	インターフェイス ペアはバイパス モードになり、トラフィックを検査していない。
オレンジに点滅	インターフェイス ペアはバイパス モード、すなわちフェール オープンされている。

図 6-12　8 ポート 1000BASE-SX 光ファイバの設定可能バイパス インターフェイス

次の表に、光ファイバ インターフェイスのリンク LED とアクティビティ LED の説明を示します。

表 6-35　3D7110 および 3D7120 光ファイバ リンク/アクティビティ LED

ステータス	説明
上（アクティビティ）	インライン インターフェイスの場合：インターフェイスにアクティビティがある場合、ライトが点灯します。消灯時は、アクティビティがありません。 パッシブ インターフェイスの場合：ライトは機能しません。
下（リンク）	インライン インターフェイスまたはパッシブ インターフェイスの場合：インターフェイスにリンクがある場合、ライトが点灯します。消灯時は、リンクがありません。

次の表に、光ファイバ インターフェイスのアクティビティ LED とリンク LED の説明を示します。

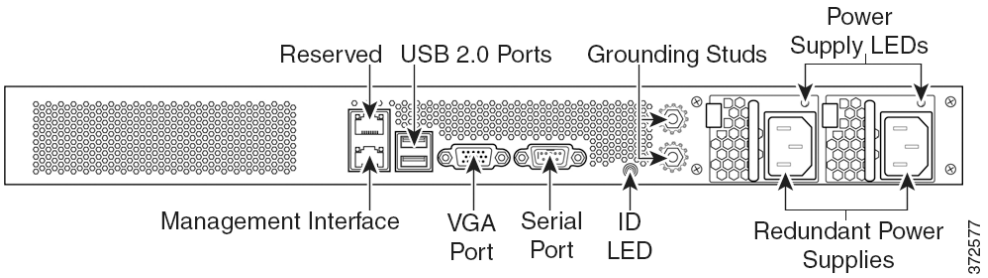
表 6-36　3D7110 および 3D7120 光ファイバのバイパス LED

ステータス	説明
消灯	インターフェイス ペアは、バイパス モードでないか、電力が供給されていない。
緑色で点灯	インターフェイス ペアは、バイパス モード開始可能。
黄色で点灯	インターフェイス ペアはバイパス モードになり、トラフィックを検査していない。
オレンジに点滅	インターフェイス ペアはバイパス モード、すなわちフェール オープンされている。

3D7110 および 3D7120 シャーシ背面図

シャーシの背面には、管理インターフェイス、接続ポート、接地スタッド、および電源があります。

図 6-13　3D7110 および 3D7120（シャーシ：GERY-1U-8-C-AC または GERY-1U-8-FM-AC）背面図



次の表に、アプライアンスの背面にある機能について示します。

表 6-37　3D7110 および 3D7120 システム コンポーネント：背面図

機能	説明
VGA ポート USB ポート	ワークステーションとアプライアンスの直接接続を確立するため、デバイスにモニタ、キーボード、およびマウスを接続できるようにします。
10/100/1000 イーサネット管理インターフェイス	アウトオブバンド管理ネットワーク接続を提供します。管理インターフェイスは、メンテナンスおよび設定目的**のみ**で使用します。サービス トラフィックを伝送することは意図されていません。
システム ID LED	高密度ラックに設置するシステムを他の類似したシステムと区別して特定します。青いライトは ID ボタンが押されたことを示します。
接地スタッド	共通ボンディング網にアプライアンスを接続するために使用します。詳細については、「FirePOWER デバイスの所要電力」（P.A-1）を参照してください。
冗長電源	AC 電源からの電力をデバイスに供給します。シャーシの背面から見て、電源 #1 は左側にあり、電源 #2 は右にあります。
電源装置の LED	電源の状態を示します。「表 6-393D7110 および 3D7120 電源 LED」（P.6-26）を参照してください。

10/100/1000 管理インターフェイスは、アプライアンスの背面にあります。次の表に、管理インターフェイスに関連付けられた LED の説明を示します。

表 6-38　3D7110 および 3D7120 管理インターフェイス LED

LED	説明
左（アクティビティ）	ポートのアクティビティを示します。 • ライトの点滅はアクティビティを示します。 • ライトが消灯している場合、アクティビティはありません。
右（リンク）	リンクが動作しているかどうかを示します。 • ライトはリンクが動作していることを示します。 • ライトが消灯している場合、リンクはありません。

電源モジュールは、アプライアンスの背面にあります。次の表に、電源に関連付けられた LED の説明を示します。

表 6-39　3D7110 および 3D7120 電源 LED

LED	説明
消灯	電源コードが接続されていない。
赤	このモジュールに電力が供給されていない。 または モジュール障害、ヒューズ切れ、ファンの障害などの電源の重要なイベントがあり、電源がシャット ダウン。
赤色に点滅	高温またはファン速度低下などの電源の警告イベントが発生した。電源は動作を続行。
緑色に点滅	AC 入力があり、電圧はスタンバイ状態、電源スイッチはオフ。
グリーン	電源が接続され、オンになっている。

3D7110 および 3D7120 の物理パラメータおよび環境パラメータ

次の表に、アプライアンスの物理的な属性と環境パラメータを示します。

表 6-40　3D7110 および 3D7120 の物理パラメータおよび環境パラメータ

パラメータ	説明
フォーム ファクタ	1 U
寸法（奥行 x 幅 x 高さ）	21.6 インチ x 19.0 インチ x 1.73 インチ （54.9 cm x 48.3 cm x 4.4 cm）
重量 最大搭載量	27.5 ポンド （12.5 kg）
銅線 1000BASE-T	ペア設定のギガビット銅線イーサネット バイパス可能インターフェイス ケーブルおよび距離：Cat5E、50 m
光ファイバ 1000BASE-SX	光ファイバのバイパス可能インターフェイス LC コネクタ付き ケーブルおよび距離：SX はマルチモード ファイバ（850 nm）、550 m（標準）

表 6-40　3D7110 および 3D7120 の物理パラメータおよび環境パラメータ （続き）

パラメータ	説明
電源モジュール	450 W デュアル冗長（1+1）AC 電源 電圧：公称 100 VAC ～ 240 VAC（最大 85 VAC ～ 264 VAC） 電流：電源ごとに、90 VAC ～ 132 VAC で最大 3 A 電源ごとに、187 VAC ～ 264 VAC で最大 1.5 A 周波数範囲：47 Hz ～ 63 Hz
動作温度	5 ˚C ～ 40 ˚C（41 ˚F ～ 104 ˚F）
非動作時温度	-20 ˚C ～ 70 ˚C（-29 ˚F ～ 158 ˚F）
湿度（動作時）	5 % ～ 85 %（結露しないこと）
非動作時湿度	5 % ～ 90%、結露しないこと、最大湿球温度 28 ˚C（82 ˚F）温度 25 ˚C ～ 35 ˚C（77 ˚F ～ 95 ˚F） 装置は、相対湿度 95% 未満の結露しない環境で保管してください。装置を稼働させる前に、少なくとも 48 時間、最大動作湿度未満で慣らし運転してください。
高度	海抜 0 フィート～ 5905 フィート （0 ～ 1800 m）
冷却要件	900 BTU/時 必要な動作温度範囲内にアプライアンスを維持するための十分な冷却機能を提供します。これに失敗すると、アプライアンスに誤動作や損傷が発生することがあります。
音響ノイズ	プロセッサ最大負荷、ファン正常動作時 64 dBA GR-63-CORE 4.6 準拠の音響ノイズ
耐衝撃性	Bellecore GR-63-CORE 標準準拠
エアーフロー	1 分あたり 140 立方フィート （3900 リットル） アプライアンスを通過するエアーフローは、前面から入って背面から出ます。側面への換気はありません。

3D7115、3D7125、および AMP7150

71xx ファミリ に属する 3D7115、3D7125、および AMP7150 デバイスには、設定可能なバイパス機能を持つ 4 ポート銅線インターフェイス、およびバイパス機能のない 8 個のホットスワップ可能な Small Form-Factor Pluggable（SFP）ポートが装備されています。互換性を保証するため、シスコ SFP トランシーバだけを使用してください。71xx ファミリアプライアンスの安全上の考慮事項については、『*Regulatory Compliance and Safety Information for FirePOWER and FireSIGHT Appliances*』を参照してください。

（注） FirePOWER AMP7150 には 3D7115 および 3D7125 と共通のフォーム ファクタが少なからずありますが、FireSIGHT システム のネットワーク ベースの高度なマルウェア対策（AMP）機能を利用するために最適化されています。

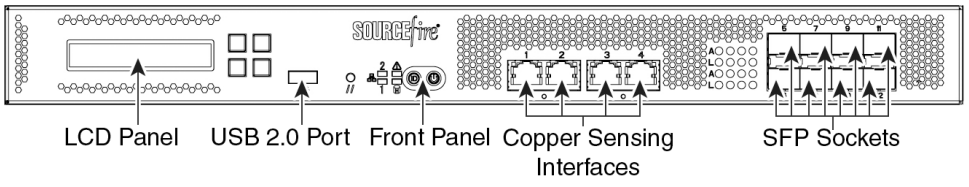
詳細については、次の項を参照してください。

- 「3D7115、3D7125、および AMP7150 シャーシ前面図」（P.6-28）
- 「3D7115、3D7125、および AMP7150 シャーシ背面図」（P.6-33）
- 「3D7115、3D7125、および AMP7150 の物理パラメータおよび環境パラメータ」（P.6-34）

3D7115、3D7125、および AMP7150 シャーシ前面図

シャーシの前面には、LCD パネル、USB ポート、前面パネル、および銅線センシング インターフェイス、および SFP ソケットがあります。

図 6-14　　3D7115、3D7125、および AMP7150（シャーシ：GERY-1U-8-4C8S-AC）前面図



次の表に、アプライアンスの前面にある機能について示します。

表 6-41　　3D7115、3D7125 および AMP7150 システム コンポーネント：前面図

機能	説明
LCD パネル	複数のモードで動作し、デバイスの設定、エラー メッセージの表示、システム ステータスの表示を行います。詳細については、「シリーズ 3 デバイスでの LCD パネルの使用」（P.5-1）を参照してください。
前面パネルの USB 2.0 ポート	デバイスにキーボードを接続するために使用します。
前面パネル	システムの動作状態、および電源ボタンなどのさまざまなコントロールを示す LED を備えています。詳細については、「図 6-153D7115、3D7125 および AMP7150 前面パネル」（P.6-28）を参照してください。
センシング インターフェイス	ネットワークに接続するセンシング インターフェイスです。詳細については、「3D7115、3D7125、および AMP7150 センシング インターフェイス」（P.6-30）を参照してください。

図 6-15　　3D7115、3D7125 および AMP7150 前面パネル

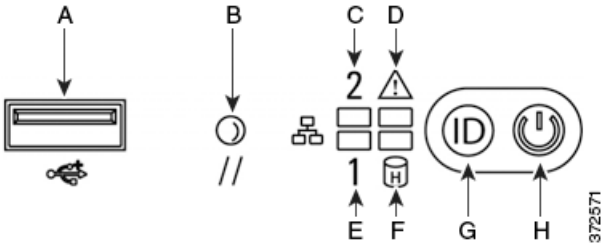


表 6-42　　3D7115、3D7125、および AMP7150 前面パネル コンポーネント

A	USB 2.0 コネクタ	E	NIC 1 アクティビティ LED
B	リセット ボタン	F	ハード ドライブ アクティビティ LED
C	NIC 2 アクティビティ LED	G	ID ボタン
D	システム ステータス LED	H	電源ボタンおよび LED

シャーシの前面パネルは、システムの動作状態を示す LED を備えています。次の表に、前面パネルの LED の説明を示します。

表 6-43　3D7115、3D7125、および AMP7150 前面パネル LED

LED	説明
NIC アクティビティ（1 および 2）	ネットワーク アクティビティがあるかどうかを示します。 • 緑のライトの点滅はネットワーク アクティビティがあることを示します。 • ライトが消灯している場合、ネットワーク アクティビティはありません。
システム ステータス	システム ステータスを示します。 • ライトが消灯している場合、システムが正常に動作しているか、電源がオフです。 • 赤のライトは、システム エラーを示します。 詳細については、「表 6-43D7115、3D7125、および AMP7150 システム ステータス」（P.6-30）を参照してください。
リセット ボタン	電源を外さずにアプライアンスをリブートするために使用します。
ハード ドライブ アクティビティ	ハード ドライブ ステータスを示します。 • 緑のライトの点滅は固定ディスク ドライブがアクティブであることを示します。 • オレンジのライトは固定ディスク ドライブに障害があることを示します。 • ライトが消灯している場合、ドライブ アクティビティがないか、システムの電源がオフになっています。
システム ID	高密度ラックに設置するシステムを他の類似したシステムと区別して特定します。 • 青いライトは ID ボタンが押されたことを示します。青いライトはアプライアンスの背面にあります。 • ライトが消灯している場合、ID ボタンは押されていません。
電源ボタンおよび LED	アプライアンスに電力が供給されているかどうかを示します。 • 緑のライトはアプライアンスに電源が供給されていて、システムがオンであることを示します。 • 緑のライトの点滅は、アプライアンスに電源が供給されていて、シャット ダウンされていることを示します。 • ライトが消灯している場合、システムに電力が供給されていないことを示します。

次の表に、システム ステータス LED が点灯する可能性がある条件について示します。

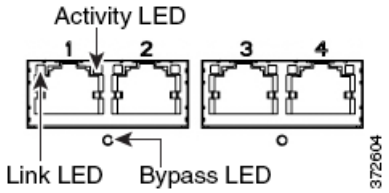
表 6-44　3D7115、3D7125、および AMP7150 システム ステータス

条件	説明
Critical	次のイベントに関連する、重大またはリカバリ不能なしきい値を超過した。 • 温度、電圧、またはファンの重大なしきい値を超過した • 電源サブシステムの障害 • プロセッサが正しく取り付けられていない、またはプロセッサが非互換のため、システムの電源をオンにできない • 重大なイベント ロギング エラー。システム メモリの修正不能な ECC エラーや、PCI SERR および PERR など致命的/修正不可能なバス エラーなど
Non-critical	Non-critical 状態は、次のイベントに関連するしきい値を超過した。 • 温度、電圧、またはファンの重大ではないしきい値を超過した • シャーシのトレスパス • システム BIOS の Set Fault Indication コマンド。BIOS は、システム メモリや CPU の設定変更などの追加の、非クリティカルな状態を示すため、このコマンドを使用する場合があります。
Degraded	Degraded 状態は次のイベントに関連付けられています。 • 1 つ以上のプロセッサが Fault Resilient Boot（FRB）または BIOS により無効になっている • BIOS により、システム メモリの一部がディセーブルにされたか、またはマップアウトした • 電源の 1 つのケーブルが外れているか、または機能していない **ヒント** Degraded 状態の表示を確認するには、まず電源の接続を確認します。デバイスの電源をオフにし、両方の電源コードを外し、電源コードを再接続し、デバイスを再起動します。 ⚠ **注意** 安全に電源をオフにするには、『*FireSIGHT System User Guide*』の「デバイスの管理」の章に示された手順を使用するか、または CLI から `system shutdown` コマンドを使用します。

3D7115、3D7125、および AMP7150 センシング インターフェイス

3D7115、3D7125、および AMP7150 デバイスには、設定可能なバイパス機能を持つ 4 ポート銅線インターフェイスと、バイパス機能のない 8 つのホットスワップ可能 Small Form-Factor Pluggable（SFP）ポートが付属しています。

図 6-16　4 つの 1000BASE-T 銅線インターフェイス



次の表に、銅線インターフェイスのリンク LED とアクティビティ LED の説明を示します。

表 6-45　3D7115、3D7125、および AMP7150 銅線リンク/アクティビティ LED

ステータス	説明
両方の LED がオフ	インターフェイスにリンクがない。
リンクがオレンジ	インターフェイスのトラフィック速度が 10 Mb または 100 Mb。
リンクが緑	インターフェイスのトラフィック速度が 1 Gb。
アクティビティが緑に点滅	インターフェイスにリンクがあり、トラフィックが通過中。

次の表に、銅線インターフェイスのバイパス LED の説明を示します。

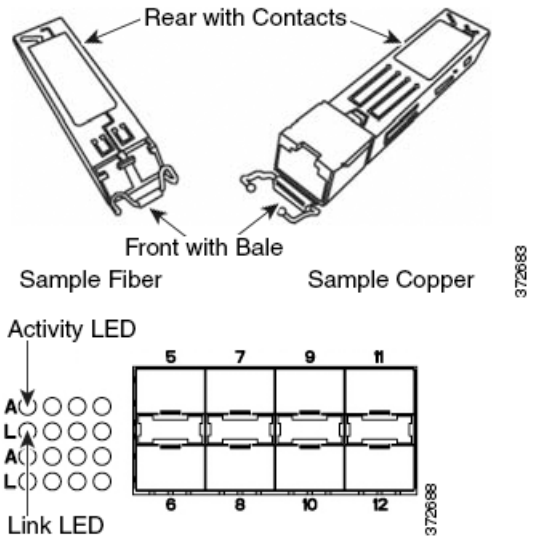
表 6-46　3D7115、3D7125、および AMP7150 銅線のバイパス LED

ステータス	説明
消灯	インターフェイス ペアは、バイパス モードでないか、電力が供給されていない。
緑色で点灯	インターフェイス ペアは、バイパス モード開始可能。
黄色で点灯	インターフェイス ペアはバイパス モードになり、トラフィックを検査していない。
オレンジに点滅	インターフェイス ペアはバイパス モード、すなわちフェール オープンされている。

SFP インターフェイス

8 個のホットスワップ可能 シスコ SFP トランシーバを設置でき、1 G 銅線、1 G 短距離光ファイバ、または 1 G 長距離光ファイバを使用可能です。SFP トランシーバにバイパス機能はありません。侵入防御の配置に使用しないでください。詳細については、「3D71x5 および AMP7150 デバイスでの SFP トランシーバの使用」（P.B-1）を参照してください。

図 6-17　サンプルの SFP トランシーバ



次の表に、光ファイバ LED の説明を示します。

表 6-47　3D7115、3D7125、および AMP7150 SFP ソケット アクティビティ / リンク LED

ステータス	説明
上（アクティビティ）	インライン インターフェイスの場合：インターフェイスにアクティビティがある場合、ライトが点灯します。消灯時は、アクティビティがありません。 パッシブ インターフェイスの場合：ライトは機能しません。
下（リンク）	インライン インターフェイスまたはパッシブ インターフェイスの場合：インターフェイスにリンクがある場合、ライトが点灯します。消灯時は、リンクがありません。

次の表に、SFP 光トランシーバの仕様の説明を示します。

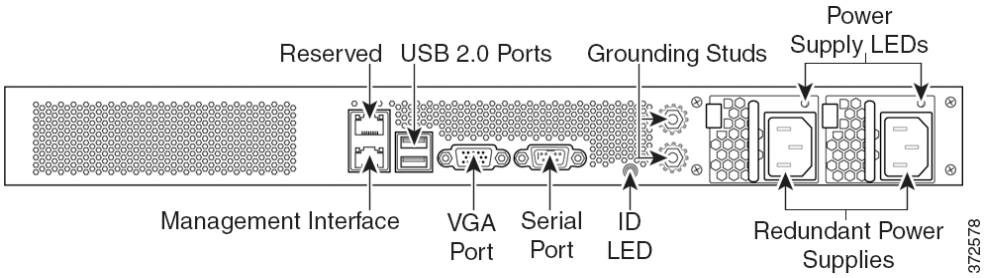
表 6-48　3D7115、3D7125、および AMP7150 SFP 光パラメータ

パラメータ	1000BASE-SX	1000BASE-LX
光コネクタ	LC デュプレックス	LC デュプレックス
ビット レート	1000 Mbps	1000 Mbps
ボー レート/エンコーディング/許容度	1250 Mbps/ 8b/10b エンコーディング	1250 Mbps/ 8b/10b エンコーディング
光インターフェイス	マルチモード	シングル モードのみ
動作距離	200 m（656 フィート） （62.5 μm/125 μm 光ファイバの場合） 500 m（1640 フィート） （50 μm/125 μm 光ファイバの場合）	10 km（6.2 マイル） （9 μm/125 μm 光ファイバの場合）
トランスミッタの波長	770 - 860 nm （通常 850 nm）	1270 ～ 1355 nm （通常 1310 nm）
最大平均起動電力	0 dBm	-3 dBm
最小平均起動電力	-9.5 dBm	-11.5 dBm
レシーバでの最大平均電力	0 dBm	-3 dBm
レシーバ感度	-17 dBm	-19 dBm

3D7115、3D7125、および AMP7150 シャーシ背面図

シャーシの背面には、管理インターフェイス、接続ポート、接地スタッド、および電源があります。

図 6-18　　3D7115、3D7125、および AMP7150（シャーシ：GERY-1U-8-4C8S-AC）背面図



次の表に、アプライアンスの背面にある機能について示します。

表 6-49　　3D7115、3D7125 および AMP7150 システム コンポーネント：背面図

機能	説明
VGA ポート USB ポート	ワークステーションとアプライアンスの直接接続を確立するため、デバイスにモニタ、キーボード、およびマウスを接続できるようにします。
10/100/1000 イーサネット管理インターフェイス	アウトオブバンド管理ネットワーク接続を提供します。管理インターフェイスは、メンテナンスおよび設定目的**のみ**で使用します。サービス トラフィックを伝送することは意図されていません。
システム ID LED	高密度ラックに設置するシステムを他の類似したシステムと区別して特定します。青いライトは ID ボタンが押されたことを示します。
接地スタッド	共通ボンディング網にアプライアンスを接続するために使用します。詳細については、「FirePOWER デバイスの所要電力」（P.A-1）を参照してください。
冗長電源	AC 電源からの電力をデバイスに供給します。シャーシの背面から見て、電源 #1 は左側にあり、電源 #2 は右にあります。
電源装置の LED	電源の状態を示します。「表 6-513D7115、3D7125、および AMP7150 電源 LED」（P.6-34）を参照してください。

10/100/1000 管理インターフェイスは、アプライアンスの背面にあります。次の表に、管理インターフェイスに関連付けられた LED の説明を示します。

表 6-50　　3D7115、3D7125、および AMP7150 管理インターフェイス LED

LED	説明
左（アクティビティ）	ポートのアクティビティを示します。 • ライトの点滅はアクティビティを示します。 • ライトが消灯している場合、アクティビティはありません。
右（リンク）	リンクが動作しているかどうかを示します。 • ライトはリンクが動作していることを示します。 • ライトが消灯している場合、リンクはありません。

電源モジュールは、アプライアンスの背面にあります。次の表に、電源に関連付けられた LED の説明を示します。

表 6-51　3D7115、3D7125、および AMP7150 電源 LED

LED	説明
消灯	電源コードが接続されていない。
赤	このモジュールに電力が供給されていない。 または モジュール障害、ヒューズ切れ、ファンの障害などの電源の重要なイベントがあり、電源がシャット ダウン。
赤色に点滅	高温またはファン速度低下などの電源の警告イベントが発生した。電源は動作を続行。
緑色に点滅	AC 入力があり、電圧はスタンバイ状態、電源スイッチはオフ。
グリーン	電源が接続され、オンになっている。

3D7115、3D7125、および AMP7150 の物理パラメータおよび環境パラメータ

次の表に、アプライアンスの物理的な属性と環境パラメータを示します。

表 6-52　3D7115、3D7125、および AMP7150 の物理パラメータおよび環境パラメータ

パラメータ	説明
フォーム ファクタ	1 U
寸法（奥行 x 幅 x 高さ）	21.6 インチ x 19.0 インチ x 1.73 インチ （54.9 cm x 48.3 cm x 4.4 cm）
重量 最大搭載量	29.0 ポンド （13.2 kg）
銅線 1000BASE-T	ペア設定のギガビット銅線イーサネット バイパス可能インターフェイス ケーブルおよび距離：Cat5E、50 m
銅線 1000BASE-T SFP	ペア設定のギガビット銅線イーサネット非バイパス インターフェイス ケーブルおよび距離：Cat5E、50 m
光ファイバ 1000BASE-SX SFP	光ファイバの非バイパス インターフェイス LC コネクタ付き ケーブルおよび距離：SX はマルチモード ファイバ（850 nm）、550 m（標準） 62.5 μm/125 μm の光ファイバで 200 m（656 フィート） 50 μm/125 μm の光ファイバで 500 m（1640 フィート）
光ファイバ 1000BASE-LX SFP	光ファイバの非バイパス インターフェイス LC コネクタ付き ケーブルおよび距離：LX はシングルモード光ファイバ（1310 nm）、10 km （9 μm/125 μm 光ファイバ（標準）の場合）
電源モジュール	450 W デュアル冗長（1+1）AC 電源 電圧：公称 100 VAC ～ 240 VAC（最大 85 VAC ～ 264 VAC） 電流：電源ごとに、90 VAC ～ 132 VAC で最大 3 A 電源ごとに、187 VAC ～ 264 VAC で最大 1.5 A 周波数範囲：47 Hz ～ 63 Hz
動作温度	5 ˚C ～ 40 ˚C（41 ˚F ～ 104 ˚F）
非動作時温度	-20 ˚C ～ 70 ˚C（-29 ˚F ～ 158 ˚F）

表 6-52　3D7115、3D7125、および AMP7150 の物理パラメータおよび環境パラメータ （続き）

パラメータ	説明
湿度（動作時）	5 % ～ 85 %（結露しないこと）
非動作時湿度	5 % ～ 90%、結露しないこと、最大湿球温度 28 ˚C（82 ˚F）温度 25 ˚C ～ 35 ˚C（77 ˚F ～ 95 ˚F） 装置は、相対湿度 95% 未満の結露しない環境で保管してください。装置を稼働させる前に、少なくとも 48 時間、最大動作湿度未満で慣らし運転してください。
高度	海抜 0 フィート～ 5905 フィート （0 ～ 1800 m）
冷却要件	900 BTU/時 必要な動作温度範囲内にアプライアンスを維持するための十分な冷却機能を提供します。これに失敗すると、アプライアンスに誤動作や損傷が発生することがあります。
音響ノイズ	プロセッサ最大負荷、ファン正常動作時 64 dBA GR-63-CORE 4.6 準拠の音響ノイズ
耐衝撃性	Bellecore GR-63-CORE 標準準拠
エアーフロー	1 分あたり 140 立方フィート（3900 リットル） アプライアンスを通過するエアーフローは、前面から入って背面から出ます。側面への換気はありません。

8000 シリーズ デバイス

8000 シリーズ デバイスは、銅線または光ファイバのセンシング インターフェイスを含むネットワーク モジュール（NetMods）を使用します。デバイスは出荷時に完全構成状態とすることも、自分でモジュールを設置することもできます。FireSIGHT システムをインストールする前にデバイスを組み立てます。モジュールに付属の組立手順を参照してください。

一部の 8000 シリーズ デバイスは、システムの機能を拡張するためスタックできます。スタック構成キットごとに、NetMod をスタック モジュールに交換し、8000 シリーズ スタック構成ケーブルを使用してデバイスをまとめてケーブル接続します。詳細については、「スタック構成でのデバイスの使用」（P.3-15）を参照してください。

8000 シリーズ デバイスはさまざまなシャーシに設置できます。

- 3D8120、3D8130、3D8140、および AMP8150 は 81xx ファミリ とも呼ばれ、1 U シャーシで、最大 3 個のモジュールを搭載できます。3D8140 のみ、合計 2 U 構成のスタック構成キットを追加できます。

  （注） FirePOWER AMP8150 には 3D8130 と共通のフォーム ファクタが少なからずありますが、FireSIGHT システム のネットワーク ベースの高度なマルウェア対策（AMP）機能を利用するために最適化されています。

- 82xx ファミリ に属する 3D8250 は 2 U シャーシで、最大 7 個のモジュールを搭載できます。合計 8 U の構成にするため最大 3 個のスタック構成キットを追加できます。
- 82xx ファミリ に属する 3D8260 は、2 台の 2 U シャーシによる 4 U 構成です。プライマリ シャーシは、1 台のスタック モジュールと 6 台のセンシング モジュールを収納します。セカンダリ シャーシは、1 台のスタック モジュールを収納します。合計 8 U の構成にするため最大 2 個のスタック構成キットを追加できます。

- 82xx ファミリ に属する 3D8270 は、3 台の 2 U シャーシによる 6 U 構成です。プライマリ シャーシは、2 台のスタック モジュールと最大 5 台のセンシング モジュールを収納します。セカンダリ シャーシは、それぞれ 1 台のスタック モジュールを収納します。合計 8 U の構成にするため 1 個のスタック構成キットを追加できます。
- 82xx ファミリ に属する 3D8290 は、4 台の 2 U シャーシによる 8 U 構成です。プライマリ シャーシは、3 台のスタック モジュールと最大 4 台のセンシング モジュールを収納します。セカンダリ シャーシは、それぞれ 1 台のスタック モジュールを収納します。このモデルは完全に構成済みで、スタック構成キットは使用できません。
- 83xx ファミリ に属する 3D8350 は 2 U シャーシで、最大 7 個のモジュールを搭載できます。合計 8 U の構成にするため最大 3 個のスタック構成キットを追加できます。
- 83xx ファミリ に属する 3D8360 は、2 台の 2 U シャーシによる 4 U 構成です。プライマリ シャーシは、1 台のスタック モジュールと 6 台のセンシング モジュールを収納します。セカンダリ シャーシは、1 台のスタック モジュールを収納します。合計 8 U の構成にするため最大 2 個のスタック構成キットを追加できます。
- 83xx ファミリ に属する 3D8370 は、3 台の 2 U シャーシによる 6 U 構成です。プライマリ シャーシは、2 台のスタック モジュールと最大 5 台のセンシング モジュールを収納します。セカンダリ シャーシは、それぞれ 1 台のスタック モジュールを収納します。合計 8 U の構成にするため 1 個のスタック構成キットを追加できます。
- 83xx ファミリ に属する 3D8390 は、4 台の 2 U シャーシによる 8 U 構成です。プライマリ シャーシは、3 台のスタック モジュールと最大 4 台のセンシング モジュールを収納します。セカンダリ シャーシは、それぞれ 1 台のスタック モジュールを収納します。このモデルは完全に構成済みで、スタック構成キットは使用できません。

詳細については、次の項を参照してください。

- 「8000 シリーズ シャーシ前面図」（P.6-36）
- 「8000 シリーズ シャーシ背面図」（P.6-40）
- 「8000 シリーズ の物理パラメータおよび環境パラメータ」（P.6-43）
- 「8000 シリーズ モジュール」（P.6-46）

8000 シリーズ シャーシ前面図

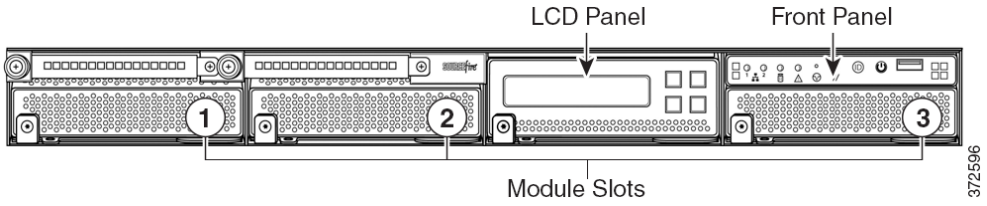
8000 シリーズ シャーシは、81xx ファミリ、82xx ファミリ、または 83xx ファミリ です。

81xx ファミリ、82xx ファミリ、および 83xx ファミリ ア プライアンスの安全上の考慮事項については、『*Regulatory Compliance and Safety Information for FirePOWER and FireSIGHT Appliances*』を参照してください。

81xx ファミリ シャーシ前面図

シャーシの前面図には、LCD パネル、前面パネル、および 3 つのモジュール スロットが示されています。

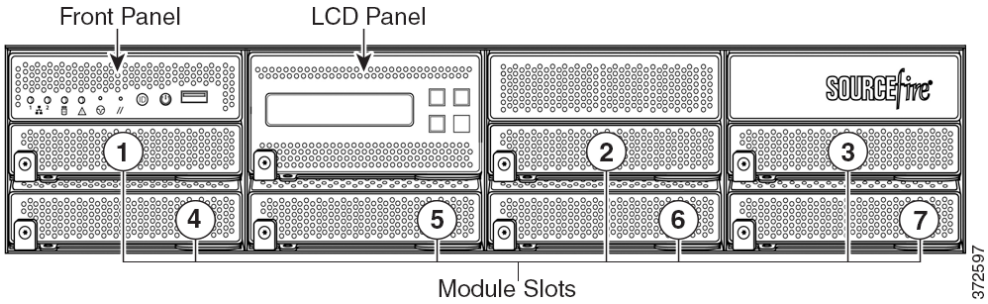
図 6-19　81xx ファミリ（シャーシ：CHAS-1U-AC/DC）前面図



82xx ファミリ および 83xx ファミリ シャーシ前面図

シャーシの前面図には、LCD パネル、前面パネル、および 7 つのモジュール スロットが示されています。

図 6-20　82xx ファミリ（シャーシ：CHAS-2U-AC/DC）および83xx ファミリPG35-2U-AC/DC）前面図



次の表に、アプライアンスの前面にある機能について示します。

表 6-53　8000 シリーズ システム コンポーネント：前面図

機能	説明
モジュール スロット	モジュールを収納します。利用可能なモジュールの詳細については、「8000 シリーズ モジュール」（P.6-46）を参照してください。
LCD パネル	複数のモードで動作し、デバイスの設定、エラー メッセージの表示、システム ステータスの表示を行います。詳細については、「シリーズ 3 デバイスでの LCD パネルの使用」（P.5-1）を参照してください。
前面パネル コントロール	システムの動作状態、および電源ボタンなどのさまざまなコントロールを示す LED を備えています。詳細については、「図 6-2282xx ファミリ および 83xx ファミリの前面パネル」（P.6-38）を参照してください。
前面パネルの USB ポート	USB 2.0 ポートを使用して、デバイスにキーボードを接続できます。

詳細については、次の項を参照してください。

- 「8000 シリーズ の前面パネル」（P.6-38）
- 「8000 シリーズ シャーシ背面図」（P.6-40）

8000 シリーズ の前面パネル

81xx ファミリ、82xx ファミリ、および 83xx ファミリ の前面パネルには、同じコンポーネントを収納できます。

図 6-21　　81xx ファミリ の前面パネル

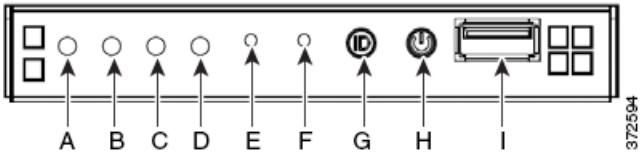


図 6-22　　82xx ファミリ および 83xx ファミリの前面パネル

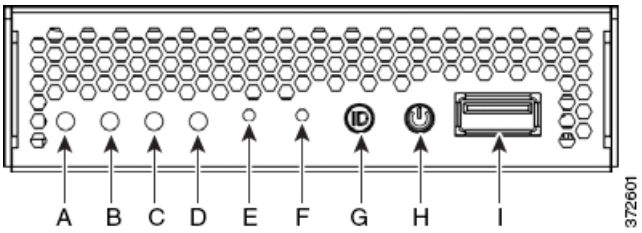


表 6-54　　8000 シリーズの前面パネルのコンポーネント

A	NIC アクティビティ LED	F	リセット ボタン
B	予約済み	G	ID ボタン
C	ハード ドライブ アクティビティ LED	H	電源ボタンおよび LED
D	システム ステータス LED	I	USB 2.0 コネクタ
E	マスク不能割り込みボタン		

シャーシの前面パネルは、システムの動作状態を示す LED を備えています。次の表に、前面パネルの LED の説明を示します。

表 6-55　　8000 シリーズ前面パネル LED

LED	説明
NIC アクティビティ	ネットワーク アクティビティがあるかどうかを示します。 • 緑はネットワーク アクティビティがあることを示します。 • ライトが消灯している場合、ネットワーク アクティビティはありません。
ハード ドライブ アクティビティ	ハード ドライブ ステータスを示します。 • 緑の点滅は固定ディスク ドライブがアクティブであることを示します。 • オレンジは固定ディスク ドライブのエラーを示します。 • ライトが消灯している場合、ドライブ アクティビティがないか、システムの電源がオフになっています。

表 6-55　8000 シリーズ前面パネル LED （続き）

LED	説明
システム ステータス	システム ステータスを示します。 • 緑はシステムが正常に動作していることを示します。 • 緑の点滅はシステムが Degraded 状態で動作していることを示します。 • オレンジの点滅は、システムが Non-critical 状態であることを示します。 • オレンジはシステムが重大またはリカバリ不能な状態にあるか、システムが起動処理中であることを示します。 • ライトがオフの場合、システムは起動処理中またはオフです。 **（注）** オレンジのステータス ライトの方が緑のステータス ライトよりも優先されます。オレンジのライトが点灯または点滅している場合、緑のライトは消灯します。 詳細については、「表 6-56（P.6-39）」を参照してください。
システム ID	高密度ラックに設置するシステムを他の類似したシステムと区別して特定します。 • 青いライトは ID ボタンが押されたことを示します。青いライトはアプライアンスの背面にあります。 • ライトが消灯している場合、ID ボタンは押されていません。
電源ボタンおよび LED	システムに電力が供給されているかどうかを示します。 • 緑は、システムに電力が供給されていることを示します。 • ライトが消灯している場合、システムに電源が供給されていません。

次の表に、システム ステータス LED が点灯する可能性がある条件について示します。

表 6-56　8000 シリーズ システム ステータス

条件	説明
Critical	次のイベントに関連する、重大またはリカバリ不能なしきい値を超過した。 • 温度、電圧、またはファンの重大なしきい値を超過した • 電源サブシステムの障害 • プロセッサが正しく取り付けられていない、またはプロセッサが非互換のため、システムの電源をオンにできない • 重大なイベント ロギング エラー。システム メモリの修正不能な ECC エラーや、PCI SERR および PERR など致命的/修正不可能なバス エラーなど
Non-critical	Non-critical 状態は、次のイベントに関連するしきい値を超過した。 • 温度、電圧、またはファンの重大ではないしきい値を超過した • シャーシのトレスパス • システム BIOS の Set Fault Indication コマンド。BIOS は、システム メモリや CPU の設定変更など、ほかの重大でない状態を示すため、このコマンドを使用する場合があります。

表 6-56　　8000 シリーズ システム ステータス （続き）

条件	説明
Degraded	Degraded 状態は次のイベントに関連付けられています。 • 1 つ以上のプロセッサが Fault Resilient Boot（FRB）または BIOS により無効になっている • BIOS により、システム メモリの一部がディセーブルにされたか、またはマップアウトした • 電源の 1 つのケーブルが外れているか、または機能していない **ヒント** Degraded 状態の表示を確認するには、まず電源の接続を確認します。デバイスの電源をオフにし、両方の電源コードを外し、電源コードを再接続し、デバイスを再起動します。 ⚠ **注意** 安全に電源をオフにするには、『*FireSIGHT System User Guide*』の「デバイスの管理」の章に示された手順を使用するか、または CLI から `system shutdown` コマンドを使用します。

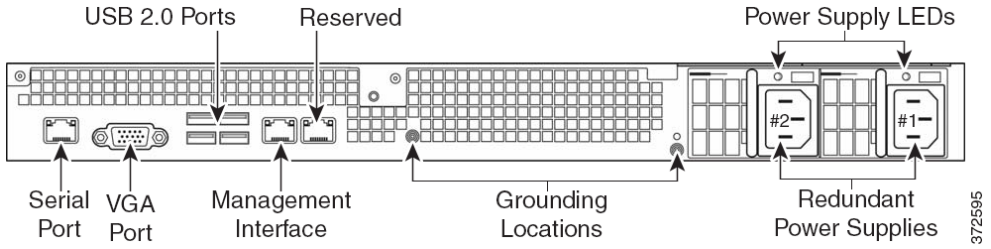
8000 シリーズ シャーシ背面図

8000 シリーズ シャーシは、81xx ファミリ、82xx ファミリ、または 83xx ファミリ です。

81xx ファミリ シャーシ背面図

シャーシ背面図には、接続ポート、管理インターフェイス、および電源が示されています。

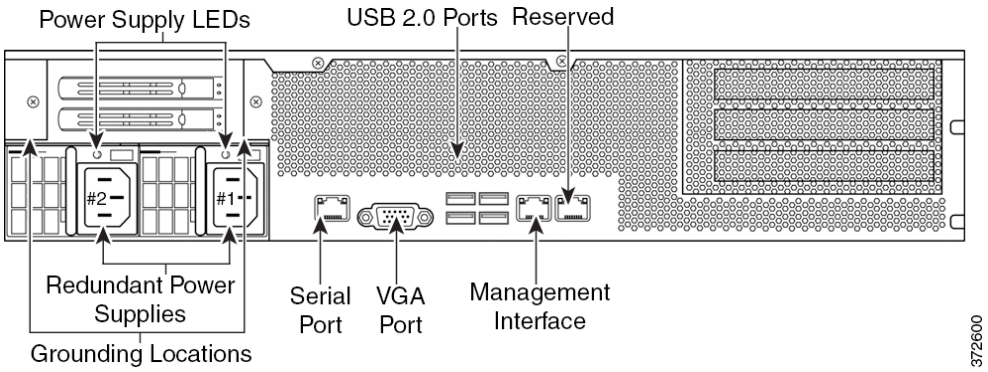
図 6-23　　81xx ファミリ（シャーシ：CHAS-1U-AC/DC）背面図



82xx ファミリ シャーシ背面図

シャーシの背面図には、電源、接続ポート、および管理インターフェイスが示されています。

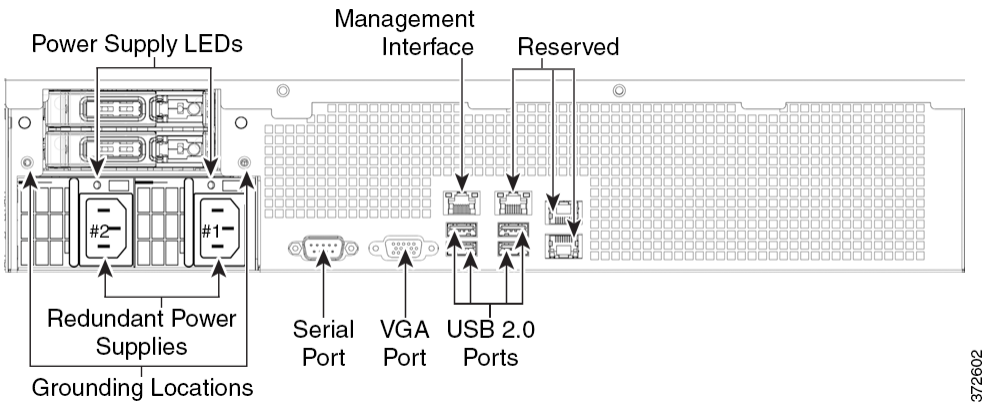
図 6-24　82xx ファミリ（シャーシ：CHAS-2U-AC/DC）背面図



83xx ファミリ シャーシ背面図

シャーシの背面図には、電源、接続ポート、および管理インターフェイスが示されています。

図 6-25　83xx ファミリ（シャーシ：PG35-2U-AC/DC）背面図



次の表に、アプライアンスの背面にある機能について示します。

表 6-57　8000 シリーズ システム コンポーネント：背面図

機能	説明
VGA ポート USB 2.0 ポート	ワークステーションとアプライアンスの直接接続を確立するため、シリアル ポートの代わりとして、デバイスにモニタ、キーボード、およびマウスを接続できるようにします。
RJ45 シリアル ポート（81xx ファミリ および 82xx ファミリ）	デバイスのすべての管理サービスにダイレクト アクセスするため、ワークステーションとアプライアンスの直接接続（RJ45 を使用して DB-9 アダプタへ）を確立できるようにします。RJ45 シリアル ポートは、メンテナンスおよび設定目的**のみ**で使用します。サービス トラフィックを伝送することは意図されていません。

表 6-57　8000 シリーズ システム コンポーネント：背面図（続き）

機能	説明
RS232 シリアル ポート（83xx ファミリ）。	デバイスのすべての管理サービスにダイレクト アクセスするため、ワークステーションとアプライアンスの直接接続を確立できるようにします。RS232 シリアル ポートは、メンテナンスおよび設定目的**のみ**で使用します。サービス トラフィックを伝送することは意図されていません。
10/100/1000 イーサネット管理インターフェイス	アウトオブバンド管理ネットワーク接続を提供します。管理インターフェイスは、メンテナンスおよび設定の目的**のみ**で使用します。サービス トラフィックを伝送することは意図されていません。
冗長電源	AC 電源からの電力をデバイスに供給します。シャーシの背面から見て、電源 #1 は右側にあり、電源 #2 は左にあります。
接地場所	共通ボンディング網にアプライアンスを接続するために使用します。詳細については、「FirePOWER デバイスの所要電力」（P.A-1）を参照してください。

10/100/1000 管理インターフェイスは、アプライアンスの背面にあります。次の表に、管理インターフェイスに関連付けられた LED の説明を示します。

表 6-58　8000 シリーズ 管理インターフェイス LED

LED	説明
左（アクティビティ）	ポートのアクティビティを示します。 • ライトの点滅はアクティビティを示します。 • ライトが消灯している場合、アクティビティはありません。
右（リンク）	リンクが動作しているかどうかを示します。 • ライトはリンクが動作していることを示します。 • ライトが消灯している場合、リンクはありません。

電源モジュールは、アプライアンスの背面にあります。次の表に、管理インターフェイスに関連付けられた LED の説明を示します。

表 6-59　8000 シリーズ 電源の LED

LED	説明
消灯	電源が接続されていない。
オレンジ	このモジュールに電力が供給されていない。 または モジュール障害、ヒューズ切れ、ファンの障害などの電源の重大なイベントがあり、電源がシャット ダウンされている。
オレンジに点滅	高温またはファン速度低下などの電源の警告イベントが発生した。電源は動作を続行。
緑色に点滅	AC 入力があり、電圧はスタンバイ状態、電源スイッチはオフ。
グリーン	電源が接続され、オンになっている。

8000 シリーズの物理パラメータおよび環境パラメータ

次の表に、81xx ファミリ デバイスの物理的な属性と環境パラメータを示します。

表 6-60　81xx ファミリの物理パラメータおよび環境パラメータ

パラメータ	説明
フォーム ファクタ	1 U
寸法 （奥行 x 幅 x 高さ）	28.7 インチ x 17.2 インチ x 1.73 インチ（72.8 cm x 43.3 cm x 4.4 cm）
重量 最大搭載量	43.5 ポンド（19.8 kg）
銅線 1000BASE-T の設定可能バイパス NetMod	ペア設定のクワッドポート ギガビット銅線イーサネット設定可能バイパス インターフェイス ケーブルおよび距離：Cat5E、50 m
光ファイバ 10GBASE の設定可能バイパス MMSR または SMLR NetMod	デュアルポート光ファイバの設定可能バイパス インターフェイス LC コネクタ付き ケーブルおよび距離： LR はシングルモード、5000 m（使用可能） SR はマルチモード ファイバ（850 nm）、550 m（標準）
光ファイバ 1000BASE-SX の設定可能バイパス NetMod	クワッドポート光ファイバの設定可能バイパス インターフェイス 1000BASE-SX LC コネクタ付き ケーブルおよび距離：SX はマルチモード ファイバ（850 nm）、550 m（標準）
銅線 1000BASE-T の非バイパス NetMod	ペア設定のクワッドポート ギガビット銅線イーサネットの非バイパス インターフェイス ケーブルおよび距離：Cat5E、50 m
光ファイバ 10GBASE、非バイパス MMSR または SMLR NetMod	クワッドポート光ファイバの非バイパス インターフェイス LC コネクタ付き ケーブルおよび距離： LR はシングルモード、5000 m（使用可能） SR はマルチモード ファイバ（850 nm）、550 m（標準）
光ファイバ 1000BASE-SX の非バイパス NetMod	クワッドポート光ファイバの非バイパス インターフェイス 1000BASE-SX LC コネクタ付き ケーブルおよび距離：SX はマルチモード ファイバ（850 nm）、550 m（標準）
電源モジュール	AC または DC 用に設計されたデュアル 650 W 冗長電源。 AC 電圧：公称 100 VAC ～ 240 VAC（最大 85 VAC ～ 264 VAC） AC 電流：電源ごとに全範囲で最大 5.2 A 電源ごとに、187 VAC ～ 264 VAC で最大 2.6 A AC 周波数範囲：47 Hz ～ 63 Hz DC 電圧：公称 -48 VDC RTN 参照 最大 -40 VDC ～ -72 VDC DC 電流：電源ごとに最大 11 A
動作温度	10 ～ 35 °C（50 ～ 95 °F）
非動作時温度	-20 ˚C ～ 70 ˚C（-29 ˚F ～ 158 ˚F）
湿度（動作時）	5 % ～ 85 %（結露しないこと）
非動作時湿度	5 % ～ 90 %、結露しないこと、最大湿球温度 28 ˚C、温度 25 ˚C ～ 35 ˚C
高度	海抜 0 フィート～ 6000 フィート（0 ～ 1800 m）

表 6-60　81xx ファミリ の物理パラメータおよび環境パラメータ （続き）

パラメータ	説明
冷却要件	1725 BTU/時 必要な動作温度範囲内にアプライアンスを維持するための十分な冷却機能を提供します。これに失敗すると、アプライアンスに誤動作や損傷が発生することがあります。
音響ノイズ	最大正常動作ノイズは 87.6 dB LWAd（高温） 一般的な正常動作ノイズは 80 dB LWAd。
耐衝撃性	2 G の 1/2 正弦衝撃（11 ミリ秒 ）でエラーなし
エアーフロー	1 分あたり 160 立方フィート（4500 リットル） 周囲温度が動作範囲にあっても、前面または背面を遮断したり、十分なスペースのないキャビネットに装置を入れたりして、エアーフローを制限すると、装置が過熱状態になる可能性があります。 アプライアンスを通過するエアーフローは、前面から入って背面から出ます。前面および背面の最小推奨スペースは 7.9 インチ（20 cm）です。この最小値は、アプライアンスの前面に低温の通気の供給が保証できる場合のみ使用できます。

次の表に、82xx ファミリ および 83xx ファミリ デバイスの物理的な属性と環境パラメータを示します。

表 6-61　82xx ファミリ および 83xx ファミリ の物理パラメータと環境パラメータ

パラメータ	説明	
フォーム ファクタ	2 U	
寸法（奥行 x 幅 x 高さ）	29.0 インチ x 17.2 インチ x 3.48 インチ（73.5 cm x 43.3 cm x 88.2 cm）	
最大搭載重量	82xx ファミリ：	58 ポンド （25.3 kg）
	83xx ファミリ：	67 ポンド （30.5 kg）
銅線 1000BASE-T の設定可能バイパス NetMod	ペア設定のクワッドポート ギガビット銅線イーサネット設定可能バイパス インターフェイス ケーブルおよび距離：Cat5E、50 m	
光ファイバ 10GBASE MMSR または SMLR の設定可能バイパス NetMod	デュアルポート光ファイバの設定可能バイパス インターフェイス LC コネクタ付き ケーブルおよび距離： LR はシングルモード、5000 m（使用可能） SR はマルチモード ファイバ（850 nm）、550 m（標準）	
光ファイバ 1000BASE-SX の設定可能バイパス NetMod	クワッドポート光ファイバの設定可能バイパス インターフェイス 1000BASE-SX LC コネクタ付き ケーブルおよび距離：SX はマルチモード ファイバ（850 nm）、550 m（標準）	
光ファイバ 40GBASE-SR4 の設定可能バイパス NetMod	デュアルポート光ファイバの設定可能バイパス インターフェイス OTP/MTP コネクタ付き ケーブルおよび距離： OM3：850 nm マルチモードで 100 m OM4：850 nm マルチモードで 150 m	
銅線 1000BASE-T の非バイパス NetMod	ペア設定のクワッドポート ギガビット銅線イーサネットの非バイパス インターフェイス ケーブルおよび距離：Cat5E、50 m	

表 6-61　82xx ファミリ および 83xx ファミリ の物理パラメータと環境パラメータ （続き）

パラメータ	説明	
光ファイバ 10GBASE、非バイパス MMSR または SMLR NetMod	クワッドポート光ファイバの非バイパス インターフェイス LC コネクタ付き ケーブルおよび距離： LR はシングルモード、5000 m（使用可能） SR はマルチモード ファイバ（850 nm）、550 m（標準）	
光ファイバ 1000BASE-SX の非バイパス NetMod	クワッドポート光ファイバの非バイパス インターフェイス 1000BASE-SX LC コネクタ付き ケーブルおよび距離： SX はマルチモード ファイバ（850 nm）、550 m（標準）	
電源モジュール	82xx ファミリ：	AC または DC 用に設計されたデュアル 750 W 冗長電源。 AC 電圧：公称 100 VAC ～ 240 VAC（最大 85 VAC ～ 264 VAC） AC 電流：電源ごとに全範囲で最大 8 A 電源ごとに、187 VAC ～ 264 VAC で最大 4A AC 周波数範囲：47 Hz ～ 63 Hz DC 電圧：公称 -48 VDC RTN 参照 最大 -40 VDC ～ -72 VDC DC 電流：電源ごとに最大 18 A
	83xx ファミリ：	AC または DC 用に設計されたデュアル 1000 W 冗長電源。 AC 電圧：公称 100 VAC ～ 240 VAC（最大 85 VAC ～ 264 VAC） AC 電流：電源ごとに全範囲で最大 11 A 電源ごとに、187 VAC ～ 264 VAC で最大 5.5 A AC 周波数範囲：47 Hz ～ 63 Hz DC 電圧：公称 -48 VDC RTN 参照 最大 -40 VDC ～ -72 VDC DC 電流：電源ごとに最大 25 A
動作温度	82xx ファミリ：10 ˚C ～ 35 ˚C（50 ˚F ～ 95 ˚F）	
	83xx ファミリ：	5 ˚C ～ 40 ˚C（41 ˚F ～ 104 ˚F）
非動作時温度	-20 ˚C ～ 70 ˚C（-29 ˚F ～ 158 ˚F）	
湿度（動作時）	5 % ～ 85 %（結露しないこと）	
非動作時湿度	5 % ～ 90 %、結露しないこと、最大湿球温度 28 ˚C、温度 25 ˚C ～ 35 ˚C	
高度	海抜 0 フィート～ 6000 フィート（0 ～ 1800 m）	
冷却要件	最大 2900 BTU/時 必要な動作温度範囲内にアプライアンスを維持するための十分な冷却機能を提供します。これに失敗すると、アプライアンスに誤動作や損傷が発生することがあります。	
音響ノイズ	最大正常動作ノイズは 81.6 dB LWAd（高温） 一般的な正常動作ノイズは 81.4 dB LWAd。	

表 6-61　82xx ファミリ および 83xx ファミリ の物理パラメータと環境パラメータ （続き）

パラメータ	説明
耐衝撃性	2 G の 1/2 正弦衝撃（11 ミリ秒 ）でエラーなし
エアーフロー	前面から背面へ 1 分あたり 210 立方フィート（6000 リットル） 周囲温度が動作範囲にあっても、前面または背面を遮断したり、十分なスペースのないキャビネットに装置を入れたりして、エアーフローを制限すると、装置が過熱状態になる可能性があります。 アプライアンスを通過するエアーフローは、前面から入って背面から出ます。前面および背面の最小推奨スペースは 7.9 インチ（20 cm）。この最小値は、アプライアンスの前面に低温の通気の供給が保証できる場合のみ使用できます。

8000 シリーズ モジュール

銅線インターフェイスまたは光ファイバ インターフェイスで 8000 シリーズ アプライアンスのセンシング インターフェイスを実現できます。

注意　このモジュールはホットスワップ可能では**ありません**。詳細については、「8000 シリーズ モジュールの取り付けと取り外し」（P.C-1）を参照してください。

次のモジュールには、設定可能なバイパス センシング インターフェイスがあります。

- 設定可能なバイパス機能を持つクワッドポート 1000BASE-T 銅線インターフェイス。「クワッドポート 1000BASE-T（銅線）設定可能バイパス NetMod」（P.6-47）を参照してください。
- 設定可能なバイパス機能を持つクワッドポート 1000BASE-SX 光ファイバ インターフェイス。詳細については、「クワッドポート 1000BASE-SX（光ファイバ）設定可能バイパス NetMod」（P.6-47）を参照してください。
- 設定可能なバイパス機能を持つデュアルポート 10GBASE（MMSR または SMLR）光ファイバ インターフェイス。詳細については、「デュアルポート 10GBASE（MMSR または SMLR）光ファイバの設定可能バイパス NetMod」（P.6-49）を参照してください。
- 設定可能なバイパス機能（2 U デバイスのみ）を持つデュアルポート 40GBASE-SR4 光ファイバ インターフェイス。詳細については、「デュアルポート 40GBASE-SR4（光ファイバ）設定可能バイパス NetMod」（P.6-50）を参照してください。

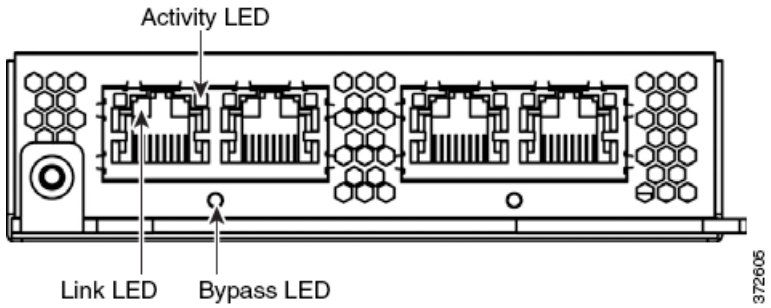
次のモジュールには、非バイパス センシング インターフェイスがあります。

- バイパス機能のないクワッドポート 1000BASE-T 銅線インターフェイス。詳細については、「クワッドポート 1000BASE-T（銅線）非バイパス NetMod」（P.6-52）を参照してください。
- バイパス機能のないクワッドポート 1000BASE-SX 光ファイバ インターフェイス。詳細については、「クワッドポート 1000BASE-SX（光ファイバ）の非バイパス NetMod」（P.6-52）を参照してください。
- バイパス機能のないクワッドポート 10GBASE（MMSR または SMLR）光ファイバ インターフェイス。詳細については、「クワッドポート 10GBASE（MMSR または SMLR）光ファイバ非バイパス NetMod」（P.6-53）を参照してください。

さらに、2 台の 3D8140、最大 4 台の 3D8250、または 4 台の 3D8350 デバイスを接続して、処理能力を組み合わせてスループットを向上させるために、スタック モジュールを使用できます。詳細については、「スタック モジュール」（P.6-55）を参照してください。

クワッドポート 1000BASE-T（銅線）設定可能バイパス NetMod

クワッドポート 1000BASE-T 銅線の設定可能なバイパス NetMod には、4 つの銅線ポートとリンク、アクティビティ、およびバイパスの LED があります。



次の表に、銅線インターフェイスのリンク LED とアクティビティ LED の説明を示します。

表 6-62　銅線リンク/アクティビティ LED

ステータス	説明
両方の LED がオフ	インターフェイスにリンクはなく、バイパス モードではない。
リンクがオレンジ	インターフェイスのトラフィック速度が 10 Mb または 100 Mb。
リンクが緑	インターフェイスのトラフィック速度が 1 Gb。
アクティビティが緑に点滅	インターフェイスにリンクがあり、トラフィックが通過中。

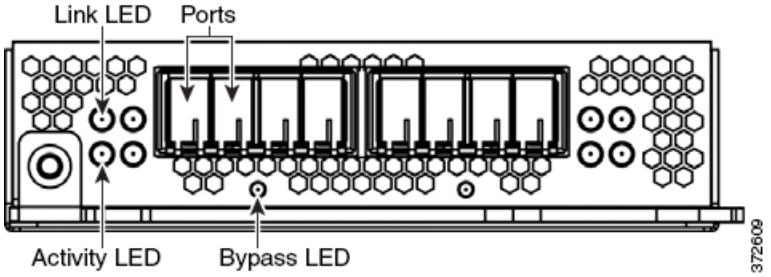
次の表に、銅線インターフェイスのバイパス LED の説明を示します。

表 6-63　銅線のバイパス LED

ステータス	説明
消灯	インターフェイスにリンクはなく、バイパス モードではない。
緑色で点灯	インターフェイスにリンクがあり、トラフィックが通過中。
黄色で点灯	インターフェイスは意図的に停止されました。
オレンジに点滅	インターフェイスはバイパス モード、すなわちフェール オープンされている。

クワッドポート 1000BASE-SX（光ファイバ）設定可能バイパス NetMod

クワッドポート 1000BASE-SX 光ファイバの設定可能なバイパス NetMod には、4 つの光ファイバ ポートとリンク、アクティビティ、およびバイパスの LED があります。



次の表に、光ファイバ インターフェイスのリンク LED とアクティビティ LED の説明を示します。

表 6-64　光ファイバ リンク/アクティビティ LED

ステータス	説明
上	インライン インターフェイスまたはパッシブ インターフェイスの場合： • ライトの点滅はインターフェイスにアクティビティがあることを示します。 • ライトが消灯している場合、アクティビティはありません。
下	インライン インターフェイスの場合： • ライトはインターフェイスにアクティビティがあることを示します。 • ライトが消灯している場合、アクティビティはありません。 パッシブ インターフェイスの場合、ライトは常時点灯します。

次の表に、光ファイバ インターフェイスのバイパス LED の説明を示します。

表 6-65　光ファイバのバイパス LED

ステータス	説明
消灯	インターフェイスにリンクはなく、バイパス モードではない。
緑色で点灯	インターフェイスにリンクがあり、トラフィックが通過中。
黄色で点灯	インターフェイスは意図的に停止されました。
オレンジに点滅	インターフェイスはバイパス モード、すなわちフェール オープンされている。

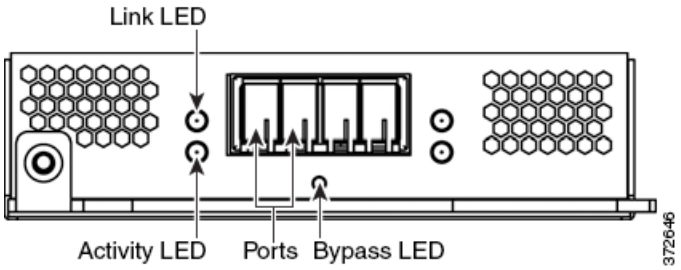
次の表に、光ファイバ インターフェイスの光仕様の説明を示します。

表 6-66　1000BASE-SX NetMod の光パラメータ

パラメータ	1000BASE-SX
光コネクタ	LC デュプレックス
ビット レート	1000 Mbps
ボー レート/エンコーディング/許容度	1250 Mbps/8b/10b エンコーディング
光インターフェイス	マルチモード
動作距離	62.5 μm/125 μm の光ファイバで 200 m（656 フィート） 50 μm/125 μm の光ファイバで 500 m（1640 フィート）
トランスミッタの波長	770 ～ 860 nm（通常 850 nm）
最大平均起動電力	0 dBm
最小平均起動電力	-9.5 dBm
レシーバでの最大平均電力	0 dBm
レシーバ感度	-17 dBm

デュアルポート 10GBASE（MMSR または SMLR）光ファイバの設定可能バイパス NetMod

デュアルポート 10GBASE（MMSR または SMLR）光ファイバの設定可能バイパス NetMod には 2 個の光ファイバ ポート、リンク、アクティビティ、バイパスの LED があります。



次の表に、光ファイバ インターフェイスのリンク LED とアクティビティ LED の説明を示します。

表 6-67　光ファイバ リンク/アクティビティ LED

ステータス	説明
上	インライン インターフェイスまたはパッシブ インターフェイスの場合: • ライトの点滅はインターフェイスにアクティビティがあることを示します。 • ライトが消灯している場合、アクティビティはありません。
下	インライン インターフェイスの場合： • ライトはインターフェイスにアクティビティがあることを示します。 • ライトが消灯している場合、アクティビティはありません。 パッシブ インターフェイスの場合、ライトは常時点灯します。

次の表に、光ファイバ インターフェイスのバイパス LED の説明を示します。

表 6-68　光ファイバのバイパス LED

ステータス	説明
消灯	インターフェイスにリンクはなく、バイパス モードではない。
緑色で点灯	インターフェイスにリンクがあり、トラフィックが通過中。
黄色で点灯	インターフェイスは意図的に停止されました。
オレンジに点滅	インターフェイスはバイパス モード、すなわちフェール オープンされている。

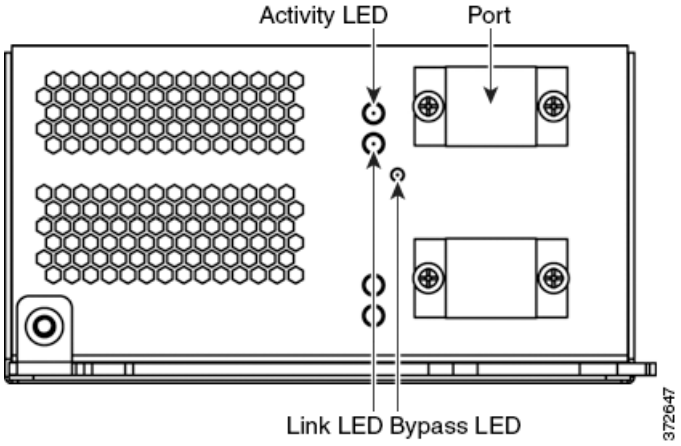
次の表に、光ファイバ インターフェイスの光パラメータの説明を示します。

表 6-69　10GBASE MMSR および SMLR NetMod 光パラメータ

パラメータ	10GBASE MMSR	10GBASE SMLR
光コネクタ	LC デュプレックス	LC デュプレックス
ビット レート	10.000 Gbps	10.000 Gbps
ボー レート/ エンコーディング/許容度	10.3125 Gbps/ 64/66b エンコーディング/ +/- 100 ppm	10.3125 Gbps/ 64/166b エンコーディング/ +/- 100 ppm
光インターフェイス	マルチモード	シングル モードのみ
動作距離	840 ～ 860 nm （通常 850 nm） 26 m（85 フィート）～ 33 m（108 フィート）62.5 μm/125 μm 光ファイバ（モーダル BW それぞれ 160 ～ 200） 66 m（216 フィート）～ 82 m（269 フィート）50 μm/125 μm 光ファイバ（モーダル BW それぞれ 400 ～ 500） 300 m（980 フィート）までの距離では、高品質（OM3）光ファイバが利用できます。 最短距離（すべて）: 2 m（6 フィート）	1270 ～ 1355 nm （通常 1310 nm） 2 m ～ 10 km（6 フィート ～ 6.2 マイル）用 （9 μm/125 μm 光ファイバの場合）
トランスミッタの波長	840 ～ 860 nm （通常 850 nm）	1270 ～ 1355 nm （通常 1310 nm）
最大平均起動電力	-1 dBm	-0.5 dBm
最小平均起動電力	-7.3 dBm	-8.2 dBm
レシーバでの最大平均電力	-1 dBm	-0.5 dBm
レシーバ感度	-9.9 dBm	-14.4 dBm

デュアルポート 40GBASE-SR4（光ファイバ）設定可能バイパス NetMod

デュアルポート 40GBASE-SR4 光ファイバの設定可能なバイパス NetMod には、2 つの光ファイバ ポートとリンク、アクティビティ、およびバイパスの LED があります。



3D8270、3D8290、3D8360、3D8370 および 3D8390 だけで、または 40G 対応 3D8250、3D8260 および 3D8350 で 40G NetMod を使用できます。40G 非対応のデバイスに 40G インターフェイスを作成しようとすると、管理する防御センター Web インターフェイスの 40G インターフェイス画面は赤く表示されます。40G 対応 3D8250 の LCD パネルには「3D 8250-40G」と表示され、40G 対応 3D8350 の LCD パネルには「3D 8350-40G」と表示されます。配置の詳細については、「8000 シリーズ モジュール」（P.3-10）を参照してください。

次の表に、光ファイバ インターフェイスのリンク LED とアクティビティ LED の説明を示します。

表 6-70　光ファイバ リンク/アクティビティ LED

ステータス	説明
上（アクティビティ）	インターフェイスにアクティビティが発生すると、ライトが点滅します。消灯時は、アクティビティがありません。
下（リンク）	インターフェイスにリンクがある場合、ライトが点灯します。消灯時は、リンクがありません。

次の表に、光ファイバ インターフェイスのバイパス LED の説明を示します。

表 6-71　光ファイバのバイパス LED

ステータス	説明
消灯	インターフェイス ペアにリンクがなく、バイパス モードではない。または、電源が供給されていない。
緑色で点灯	インターフェイス ペアにリンクがあり、トラフィックが通過中。
黄色で点灯	インターフェイスは意図的に停止されました。
オレンジに点滅	インターフェイスはバイパス モード、すなわちフェール オープンされている。

次の表に、光ファイバ インターフェイスの光パラメータの説明を示します。

表 6-72　40GBASE-SR4 NetMod の光パラメータ

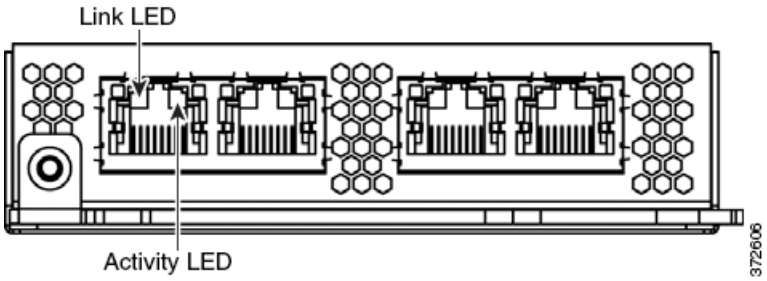
パラメータ	40GBASE-SR4
光コネクタ	OTP/MTP 1 列構成、光ファイバ ポジション 12 個。外側の 8 個の光ファイバのみ使用されます。
ビット レート	40.000 Gbps
ボー レート/エンコーディング/許容度	10.3125 Gbps/ 64/66b エンコーディング /+/- 100 ppm
光インターフェイス	マルチモード
動作距離	100 m（320 フィート） （50 μm/125 μm 光ファイバ（OM3）の場合） 最短距離：0.5 m（2 フィート） 40G 光信号は、MPO コネクタを使用して 8 本の光ファイバ ケーブルで伝送されます。
トランスミッタの波長	840 ～ 860 nm（通常 850 nm）

表 6-72　40GBASE-SR4 NetMod の光パラメータ （続き）

パラメータ	40GBASE-SR4
最大平均起動電力	2.4 dBm
最小平均起動電力	-7.8 dBm
レシーバでの最大平均電力	2.4 dBm
レシーバ感度	-9.5 dBm

クワッドポート 1000BASE-T（銅線）非バイパス NetMod

クワッドポート 1000BASE-T 銅線の非バイパス NetMod には、4 つの銅線ポートと、リンクおよびアクティビティの LED があります。



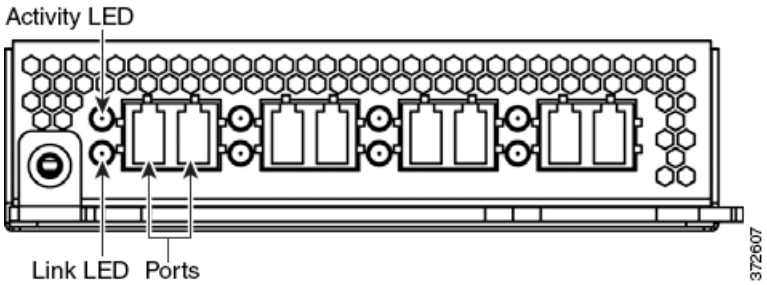
次の表に、銅線 LED の説明を示します。

表 6-73　非バイパス銅線リンク/アクティビティ LED

ステータス	説明
両方の LED がオフ	インターフェイスにリンクがない。
リンクがオレンジ	インターフェイスのトラフィック速度が 10 Mb または 100 Mb。
リンクが緑	インターフェイスのトラフィック速度が 1 Gb。
アクティビティが緑に点滅	インターフェイスにリンクがあり、トラフィックが通過中。

クワッドポート 1000BASE-SX（光ファイバ）の非バイパス NetMod

クワッドポート 1000BASE-SX 光ファイバの非バイパス NetMod には、4 つの光ファイバ ポートと、リンクおよびアクティビティの LED があります。



次の表に、光ファイバ インターフェイスのリンク LED とアクティビティ LED の説明を示します。

表 6-74　非バイパス光ファイバ リンク/アクティビティ LED

ステータス	説明
上 （アクティビティ）	インライン インターフェイスまたはパッシブ インターフェイスの場合：インターフェイスにアクティビティがある場合、ライトが点滅します。消灯時は、アクティビティがありません。
下 （リンク）	インライン インターフェイスの場合：インターフェイスにリンクがある場合、ライトが点灯します。消灯時は、リンクがありません。 パッシブ インターフェイスの場合：ライトは常時点灯します。

次の表に、光ファイバ インターフェイスの光パラメータの説明を示します。

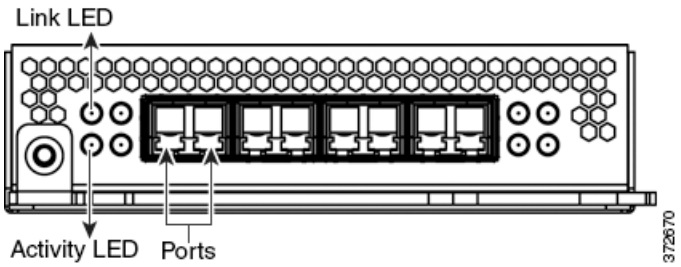
表 6-75　1000BASE-SX NetMod の光パラメータ

パラメータ	1000BASE-SX
光コネクタ	LC デュプレックス
ビット レート	1000 Mbps
ボー レート/エンコーディング/許容度	1250 Mbps/8b/10b エンコーディング
光インターフェイス	マルチモード
動作距離	62.5 μm/125 μm の光ファイバで 200 m（656 フィート） 50 μm/125 μm の光ファイバで 500 m（1640 フィート）
トランスミッタの波長	770 ～ 860 nm（通常 850 nm）
最大平均起動電力	0 dBm
最小平均起動電力	-9.5 dBm
レシーバでの最大平均電力	0 dBm
レシーバ感度	-17 dBm

クワッドポート 10GBASE（MMSR または SMLR）光ファイバ非バイパス NetMod

クワッドポート 10GBASE（MMSR または SMLR）光ファイバの非バイパス NetMod には、4 つの光ファイバ ポートと、リンクおよびアクティビティの LED があります。

注意　クワッドポート 10GBASE の非バイパス NetMod には取り外せない SFP があります。SFP を取り外そうとすると、モジュールが破損することがあります。



次の表に、光ファイバ インターフェイスのリンク LED とアクティビティ LED の説明を示します。

表 6-76　光ファイバ リンク/アクティビティ LED

ステータス	説明
上	インライン インターフェイスまたはパッシブ インターフェイスの場合：インターフェイスにアクティビティがある場合、ライトが点滅します。消灯時は、アクティビティがありません。
下	インライン インターフェイスの場合：インターフェイスにリンクがある場合、ライトが点灯します。消灯時は、リンクがありません。 パッシブ インターフェイスの場合：ライトは常時点灯します。

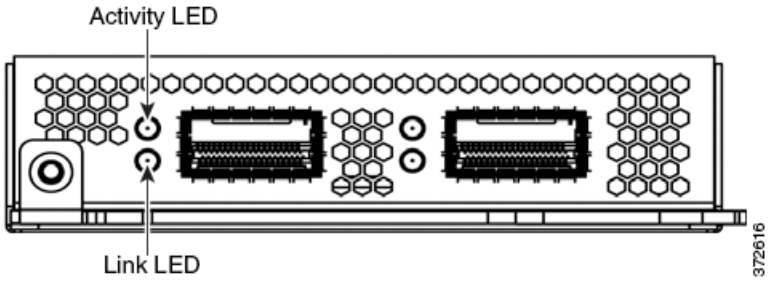
次の表に、光ファイバ インターフェイスの光パラメータの説明を示します。

表 6-77　10GBASE MMSR および SMLR NetMod 光パラメータ

パラメータ	10GBASE MMSR	10GBASE SMLR
光コネクタ	LC デュプレックス	LC デュプレックス
ビット レート	10.000 Gbps	10.000 Gbps
ボー レート/ エンコーディング/許容度	10.3125 Gbps/ 64/66b エンコーディング/ +/- 100 ppm	10.3125 Gbps/ 64/66b エンコーディング/ +/- 100 ppm
光インターフェイス	マルチモード	シングル モードのみ
動作距離	840 ～ 860 nm （通常 850 nm） 26 m（85 フィート）～ 33 m（108 フィート） 62.5 μm/125 μm 光ファイバ（モーダル BW それぞれ 160 ～ 200） 66 m（216 フィート）～ 82 m（269 フィート） 50 μm/125 μm 光ファイバ（モーダル BW それぞれ 400 ～ 500） 300 m（980 フィート）までの距離では、高品質（OM3）光ファイバが利用できます。 最短距離（すべて）： 2 m（6 フィート）	1270 ～ 1355 nm （通常 1310 nm） 2 m ～ 10 km（6 フィートから 6.2 マイル） （9 μm/125 μm 光ファイバの場合）
トランスミッタの波長	840 ～ 860 nm （通常 850 nm）	1270 ～ 1355 nm （通常 1310 nm）
最大平均起動電力	-1 dBm	-0.5 dBm
最小平均起動電力	-7.3 dBm	-8.2 dBm
レシーバでの最大平均電力	-1 dBm	-0.5 dBm
レシーバ感度	-9.9 dBm	-14.4 dBm

スタック モジュール

スタック モジュールには、8000 シリーズ スタック構成ケーブル用の 2 個の接続ポート、アクティビティおよびリンクの LED があります。



次の表に、スタック構成 LED の説明を示します。（注）スタック モジュールは 3D8140、3D8250、および 3D8350 で利用可能であり、3D8260/3D8270/3D8290 および 3D8360/3D8370/3D8390 に組み込まれています。

表 6-78　　スタック構成 LED

ステータス	説明
上	インターフェイスのアクティビティを示します。 • ライトの点滅はインターフェイスにアクティビティがあることを示します。 • ライトが消灯している場合、アクティビティはありません。
下	インターフェイスにリンクがあるかどうかを示します。 • ライトはインターフェイスにリンクがあることを示します。 • ライトが消灯している場合、リンクはありません。

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

シスコは、防御センターや管理対象デバイスを工場出荷時の初期設定に復元または再イメージングできるように、サポート サイトに ISO イメージを提供しています。

（注） ASA FirePOWER デバイスを復元または再イメージングする方法の詳細については、ASA のマニュアルを参照してください。

詳細については、次の項を参照してください。

はじめる前に

出荷時の初期状態にアプライアンスを復元し始める前に、復元プロセス中に予期されるシステムの動作について理解しておく必要があります。

設定とイベントのバックアップのガイドライン

復元プロセスを開始する前に、アプライアンス上に存在するバックアップ ファイルを削除または移動してから、現在のイベントおよび設定データを外部の場所にバックアップすることをシスコは推奨します。

アプライアンスを出荷時の初期状態に復元すると、アプライアンス上のほとんど**すべて**の設定とイベント データが失われます。復元ユーティリティはアプライアンスのライセンス、ネットワーク、コンソール、および Lights-Out Management（LOM）の設定を保持できますが、その他のすべてのセットアップ作業は、復元プロセスの完了後に実行する必要があります。

復元プロセスの間のトラフィック フロー

ネットワークでのトラフィック フローの中断を回避するために、アプライアンスの復元はメンテナンス期間中に行うか、または中断によって展開が受ける影響が最小となるときに行うことをシスコは推奨します。

インラインで展開された管理対象デバイスを復元すると、デバイスが非バイパス（フェール クローズ）の設定にリセットされるので、ネットワークのトラフィックは中断します。トラフィックは、デバイスにバイパス対応のインライン セットを設定するまでブロックされています。

デバイス設定を編集してバイパスを設定する方法の詳細については、『*FireSIGHT System User Guide*』の「デバイスの管理」の章を参照してください。

復元プロセスについて

FireSIGHT システム *アプライアンス*は、トラフィック検知を行う管理対象*デバイス*または管理*防御センター*です。各アプライアンス タイプには複数の*モデル*があります。それらのモデルはさらに、*シリーズ*と*ファミリ*にグループ化されます。詳細については、「FireSIGHT システム アプライアンス」（P.1-2）を参照してください。

アプライアンスを復元するための詳細な手順は、アプライアンスのモデル、およびアプライアンスに物理的にアクセスできるかどうかによって異なりますが、一般的なプロセスは同じです。

（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。再イメージングを行うと、バイパス モードのアプライアンスが非バイパス設定にリセットされて、バイパス モードに再設定されるまではネットワーク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。

FireSIGHT システムのアプライアンスを復元する方法：

アクセス：Admin

ステップ 1　復元するアプライアンス（デバイスまたは防御センター）のモデルを判別します。

ステップ 2　サポート サイトから正しい復元 ISO イメージを取得します。

ステップ 3　適切なストレージ メディアにイメージをコピーします。

ステップ 4　アプライアンスに接続します。

ステップ 5　アプライアンスをリブートして、復元ユーティリティを起動します。

ステップ 6　ISO イメージをインストールします。

ユーザに便利なように、ほとんどのアプライアンスで、復元プロセスの一部としてシステム ソフトウェアおよび侵入ルールのアップデートをインストールできます。

次の表は、FireSIGHT システムのアプライアンスのさまざまなモデルを復元する方法を要約しています。

表 7-1　アプライアンスの各モデルでサポートされる復元方式

モデル	復元方式	物理アクセスは必要か。	復元中にアップデートするか。
DC1000 DC3000	シスコが提供する ISO イメージのプリロードされた CD-ROM を使用するか、または独自の CD を作成します。	CD をロードするには [yes] を選択します。	いいえ
DC500 すべてのシリーズ 2 のデバイス（3D9900 を除く）	シスコ提供の外部 USB ドライブから起動し、インタラクティブ メニューを使用して ISO イメージをアプライアンスにダウンロードおよびインストールします。	USB ドライブを挿入するには [yes] を選択します。	はい
3D9900 シリーズ 3 アプライアンス	アプライアンスの内部フラッシュ ドライブから起動し、インタラクティブ メニューを使用してアプライアンスに ISO イメージをダウンロードおよびインストールします。	いいえ。リモート KVM スイッチ（すべて）または LOM（シリーズ 3）により、遠隔で復元できます	はい

Web インターフェイスを使用してアプライアンスを復元**できない**ことに注意してください。アプライアンスを復元するには、以下のいずれかの方法でそれに接続します。

キーボードとモニタ/KVM

USB キーボードと VGA モニタを任意の FireSIGHT システム アプライアンスに接続できます。これは、KVM（キーボード、ビデオ、マウス）スイッチに接続されたラックマウント型のアプライアンスで役立ちます。リモート アクセス可能な KVM がある場合は、物理的にアクセスできなくても、シリーズ 3 アプライアンスと 3D9900 を復元できます。

シリアル接続/ラップトップ

3D2100/2500/3500/4500 デバイス以外のFireSIGHT システムアプライアンスにコンピュータを接続するために、ロールオーバー シリアル ケーブル（別名 ヌル モデム ケーブルまたは Cisco コンソール ケーブル）を使用できます。シリアル ポートの場所は、アプライアンスのハードウェア仕様を参照してください。アプライアンスとの対話には、HyperTerminal や Xmodem などのターミナル エミュレーション ソフトウェアを使用します。各アプライアンスのシリアル ポート コネクタの表など、詳細については「シリアル接続/ラップトップ」（P.3-21）を参照してください。

Serial over LAN（SOL）を使用する Lights-Out Management（LOM）

Serial over LAN（SoL）接続による Lights-Out Management（LOM）を使用して、限定されたアクションのセットを シリーズ 3 アプライアンス上で実行できます。LOM に対応したアプライアンスを出荷時の初期状態に復元する必要があり、そのアプライアンスに物理的にアクセスできない場合は、LOM を使用して復元プロセスを実行できます。LOM を使用してアプライアンスに接続した後、物理シリアル接続を使用する場合と同じ方法で、復元ユーティリティにコマンドを発行します。詳細については、「Lights-Out Management の設定」（P.7-20）を参照してください。

復元 ISO とアップデート ファイルの取得

シスコは、アプライアンスを工場出荷時の初期設定に復元できるように ISO イメージを提供しています。アプライアンスを復元する前に、サポート サイトから正しい ISO イメージを取得してください。

アプライアンスの復元に使用する ISO イメージは、そのアプライアンス モデルのサポートをシスコがいつ導入したかによって異なります。新しいアプライアンス モデルに対応するためにマイナー バージョンと共に ISO イメージがリリースされる場合を除いて、通常 ISO イメージはシステム ソフトウェアのメジャー バージョン（5.2 や 5.3 など）に関連付けられます。互換性のないシステムのバージョンをインストールしないように、常にアプライアンスで使用可能な最新の ISO イメージを使用することをシスコは推奨します。

ほとんどのアプライアンスは、外部 USB または内部フラッシュ ドライブを使用してアプライアンスを起動するため、復元ユーティリティを実行できます。ただし、DC1000 および DC3000 防御センターでは、復元 ISO の CD が必要です。DC1000 または DC3000 を使用している場合は、アプライアンスの購入時にシスコが CD-ROM で ISO イメージを提供しています。異なるバージョンにアプライアンスを復元する場合は、該当する ISO イメージをダウンロードして、新しい（データのない）復元 ISO CD を作成してから、それを使用してアプライアンスを復元できます。

シスコはまた、常にアプライアンスでサポートされるシステム ソフトウェアの最新バージョンを実行することも推奨します。サポートされる最新のメジャー バージョンにアプライアンスを復元した後に、システム ソフトウェア、侵入ルール、および脆弱性データベース（VDB）を更新する必要があります。詳細については、適用するアップデートのリリース ノート、および『*FireSIGHT System User Guide*』の「システム ソフトウェアの更新」の章を参照してください。

ユーザに便利なように、ほとんどのアプライアンスで、復元プロセスの一部としてシステム ソフトウェアおよび侵入ルールのアップデートをインストールできます。たとえば、デバイスをバージョン 5.3 に復元し、そのプロセスの一部としてデバイスをバージョン 5.3.0.1 にアップデートすることができます。ルールの更新が必要なのは防御センターだけであることに注意してください。

DC1000 および DC3000 防御センターの復元には CD を使用するため、それらのアプライアンスでは、復元プロセスの一部としてアップデートをインストールすることはできないことに注意してください。代わりに、後でアプライアンスをアップデートしてください。

復元 ISO や他のアップデート ファイルを取得する方法：

アクセス：Any

ステップ 1　サポート アカウントのユーザ名とパスワードを使用して、サポート サイト（https://support.sourcefire.com/）にログインします。

ステップ 2　[Downloads] をクリックし、表示されるページで [3D System] タブを選択して、インストールするシステム ソフトウェアのメジャー バージョンをクリックします。

たとえば、バージョン 5.3 またはバージョン 5.3.1 の ISO イメージをダウンロードするには、[Downloads] > [3D System] > [5.3] をクリックします。

ステップ 3　ダウンロードするイメージ（ISO イメージ）を見つけます。

ページの左側にあるいずれかのリンクをクリックして、ページの該当するセクションを表示することができます。たとえば、[5.3.1 Images] をクリックすると、FireSIGHT システムのバージョン 5.3.1 のイメージとリリース ノートが表示されます。

ステップ 4　ダウンロードする ISO イメージをクリックします。

ファイルのダウンロードが開始されます。

ステップ 5　オプションで、システム ソフトウェアおよび侵入ルールのアップデートをダウンロードします。

- システム ソフトウェアのアップデートは、サポート サイトの ISO イメージと同じページにあります。ページの左側にあるいずれかのリンクをクリックして、ページの該当するセクションを表示することができます。たとえば、[5.3.1] をクリックすると、FireSIGHT システムのバージョン 5.3.1 のアップデートとリリース ノートが表示されます。
- ルールのアップデートをダウンロードするには、[Downloads] > [Rules] & [VDB] > [Rules] を選択します。ルールの最新のアップデートがページ上部に表示されます。

DC1000 または DC3000 を復元するときは、復元プロセスの完了後に更新をインストールする必要があることに注意してください。

ステップ 6　どのようにアプライアンスを復元しますか。

- ほとんどのアプライアンス（USB や内部フラッシュ ドライブ によって復元するもの）では、アプライアンスが管理ネットワークでアクセスできる HTTP（Web）サーバ、FTP サーバ、または SCP 対応ホストにファイルをコピーします。
- DC1000 および DC3000 では、ISO イメージを使用して復元用 CD を作成します。

注意　ISO やアップデート ファイルを電子メールで転送**しない**でください。ファイルが破損することがあります。また、ファイルの名前を変更**しない**でください。復元ユーティリティは、ファイルの名前がサポート サイトでの名前と同じであることを必要とします。

復元プロセスの開始

サポートされるデバイス：すべて

サポートされる防御センター：DC1000 と DC3000 を除くすべて

DC1000 および DC3000 防御センターを除くすべてのアプライアンスでは、外部 USB または内部フラッシュ ドライブからアプライアンスを起動して復元プロセスを開始します。表 7-1（P.7-3）をしてください。

アプライアンスへのアクセスと接続が適切なレベルであること、および ISO イメージが正しいことを確認した後に、以下のいずれかの手順によってアプライアンスを復元します。

- 「KVM または物理シリアル ポートを使用する復元ユーティリティの起動」（P.7-6）では、アプライアンスが LOM をサポートしない場合や LOM にアクセスできない場合に、復元プロセスを開始する方法について説明します。この方式は、DC1000 と DC3000 防御センターを除くすべてのアプライアンスの復元に使用できます。
- 「Lights-Out Management を使用する復元ユーティリティの開始」（P.7-7）では、LOM を使用して SoL 接続経由で シリーズ 3 アプライアンスの復元プロセスを開始する方法について説明します。
- 「CD を使用する DC1000 または DC3000 の復元」（P.7-18）では、CD を使用して、DC1000 または DC3000 防御センターを復元する方法について説明します。

注意　この章で示す手順は、電源をオフにしないでアプライアンスを復元する方法について説明します。ただし、何らかの理由で電源をオフにする必要がある場合は、『*FireSIGHT System User Guide*』の「デバイスの管理」の章に示された手順を使用するか、シリーズ 3 デバイスの CLI で `system shutdown` コマンドを使用するか、またはアプライアンスのシェル（エキスパート モードと呼ばれます）から `shutdown -h now` コマンドを使用します。

KVM または物理シリアル ポートを使用する復元ユーティリティの起動

サポートされるデバイス：すべて

サポートされる防御センター：DC1000 と DC3000 を除くすべて

DC1000 および DC3000 防御センターを除くすべてのアプライアンスでは、シスコはアプライアンス モデルに応じて外部 USB または内部フラッシュ ドライブに復元ユーティリティを提供しています。表 7-1（P.7-3）を参照してください。

（注） アプライアンスは大容量ストレージ デバイスをブート デバイスとして使用する可能性があるため、初期セットアップのためにアプライアンスにアクセスするときには、KVM コンソールと一緒に USB 大容量ストレージを使用**しない**でください。

シリーズ 3 アプライアンスを出荷時の初期状態に復元する必要があり、そのアプライアンスに物理的にアクセスできない場合は、LOM を使用して復元プロセスを実行できます。「Lights-Out Management を使用する復元ユーティリティの開始」（P.7-7）を参照してください。

復元ユーティリティを起動する方法：

アクセス：Admin

ステップ 1　DC500 やシリーズ 2 デバイス（ただし 3D9900 は除く）の復元に USB ドライブを使用する場合は、アプライアンスの使用可能な USB ポートに USB ドライブを挿入します。

それ以外の場合は、次のステップに進みます。

ステップ 2　キーボード/モニタまたはシリアル接続を使用して、管理者権限を持つアカウントでアプライアンスにログインします。パスワードは、アプライアンスの Web インターフェイスのパスワードと同じです。

アプライアンスのプロンプトが表示されます。

ステップ 3　アプライアンスをリブートします。

- 防御センターまたはシリーズ 2 管理対象デバイスでは、`sudo reboot` と入力します。
- シリーズ 3 管理対象デバイスでは、`system reboot` と入力します。

アプライアンスがリブートします。DC500 防御センターまたは 3D500/1000/2000 デバイスでは、スプラッシュ画面が表示されます。

ステップ 4　再起動の状態をモニタします。

- システムがデータベースの検査を実行している場合、次のメッセージが表示されることがあります。`The system is not operational yet.Checking and repairing database are in progress.This may take a long time to finish.`
- DC500 防御センターまたは 3D500/1000/2000 デバイスで、スプラッシュ画面が表示されたら Ctrl + U をゆっくりと繰り返し押します。
- キーボードとモニタの接続を使用する他のすべてのアプライアンスでは、赤い LILO のブート メニューが表示されます。すぐにいずれかの矢印キーを押して、アプライアンスが現在インストールされているシステムのバージョンが起動されないようにします。

- シリアル接続を使用する他のすべてのアプライアンスでは、BIOS のブート オプションが表示されたときに、Tab キーをゆっくりと繰り返し押します（これにより、アプライアンスが現在インストールされているシステムのバージョンを起動しないようにします）。以下の LILO のブート プロンプトが表示されます。

```
LILO 22.8 boot:
3D-5.3 System_Restore
```

ステップ 5　以下のようにして、システムの復元を指示します。

- DC500 防御センターまたは 3D500/1000/2000 デバイスでは、Enter キーを押します。
- キーボードとモニタの接続を使用する他のすべてのアプライアンスでは、矢印キーを使用して [System_Restore] を選択し、Enter キーを押します。
- シリアル接続を使用する他のすべてのアプライアンスでは、プロンプトで `System_Restore` と入力し、Enter キーを押します。

以下の選択項目に続いて `boot` プロンプトが表示されます。

```
0. Load with standard console
1. Load with serial console
```

ステップ 6　復元ユーティリティの対話型メニューの表示モードを選択します。

- キーボードとモニタ接続の場合は、`0` と入力して Enter キーを押します。
- シリアル接続の場合は、`1` と入力して Enter キーを押します。

表示モードを選ばない場合、復元ユーティリティは 30 秒後にデフォルトの標準コンソールを表示します。

アプライアンスをこのメジャー バージョンに初めて復元する場合を除いて、ユーティリティは、最後に使用した復元設定を自動的にロードします。一連のページで設定を確認して、続行します。

復元ユーティリティの著作権情報が表示されます。

ステップ 7　Enter キーを押して著作権表示を確認し、「対話型メニューを使用するアプライアンスの復元」（P.7-9）の手順を続行します。

Lights-Out Management を使用する復元ユーティリティの開始

サポートされるデバイス：シリーズ 3

サポートされる防御センター：シリーズ 3

シリーズ 3 アプライアンスを出荷時の初期状態に復元する必要があり、そのアプライアンスに物理的にアクセスできない場合は、LOM を使用して復元プロセスを実行できます。初期設定を行うために LOM を使用する場合は、初期設定時にネットワーク設定を保持する**必要がある**ことに注意してください。

（注）　LOM を使用してアプライアンスを復元するには、その前にその機能を有効にする必要があります。「Lights-Out Management の設定」（P.7-20）を参照してください。

Lights-Out Management を使用して復元ユーティリティを開始する方法：

アクセス：Admin

ステップ 1　コンピュータのコマンド プロンプトで、IPMI コマンドを入力して SoL セッションを開始します。

- IPMItool の場合は、次のように入力します。

```
sudo ipmitool -I lanplus -H IP_address -U username sol activate
```

- ipmiutil の場合は、次のように入力します。

```
sudo ipmiutil sol -a -V4 -J3 -N IP_address -U username -P password
```

ここで、*IP_address* はアプライアンスの管理インターフェイスの IP アドレス、*username* は承認 LOM アカウントのユーザ名、*password* はそのアカウントのパスワードです。`sol activate` コマンドを発行した後に、IPMItool はパスワードの入力を要求することに注意してください。

シリーズ 3 または仮想管理対象デバイスを使用している場合は、`expert` と入力してシェル プロンプトを表示します。

ステップ 2　root ユーザとしてアプライアンスをリブートします。

- 防御センターの場合は、`sudo reboot` と入力します。
- シリーズ 3 デバイスの場合は、`system reboot` と入力します。

アプライアンスがリブートします。

ステップ 3　再起動の状態をモニタします。

システムがデータベースの検査を実行している場合、次のメッセージが表示されることがあります。`The system is not operational yet.Checking and repairing database are in progress.This may take a long time to finish.`

シリアル接続を使用する他のすべてのアプライアンスでは、BIOS のブート オプションが表示されたときに、Tab キーをゆっくりと繰り返し押します（これにより、アプライアンスが現在インストールされているシステムのバージョンを起動しないようにします）。以下のような LILO のブート プロンプトが表示されるまで続けてください。

```
LILO 22.8 boot:
3D-5.3 System_Restore
```

ステップ 4　`boot` プロンプトに `System_Restore` と入力して、復元ユーティリティを開始します。

以下の選択項目に続いて `boot` プロンプトが表示されます。

```
0. Load with standard console
1. Load with serial console
```

ステップ 5　`1` を入力して Enter キーを押すと、アプライアンスのシリアル接続を介して対話式の復元メニューがロードされます。

（注）　表示モードを選ばない場合、復元ユーティリティは 10 秒後にデフォルトの標準コンソールを表示します。

アプライアンスをこのメジャー バージョンに初めて復元する場合を除いて、ユーティリティは、最後に使用した復元設定を自動的にロードします。一連のページで設定を確認して、続行します。

復元ユーティリティの著作権情報が表示されます。

ステップ 6　Enter キーを押して著作権表示を確認し、「対話型メニューを使用するアプライアンスの復元」（P.7-9）の手順を続行します。

対話型メニューを使用するアプライアンスの復元

サポートされるデバイス：すべて

サポートされる防御センター：DC1000/3000 を除くすべて

ほとんどの FireSIGHT システム アプライアンスの復元ユーティリティは、対話式メニューを使用して復元プロセスをガイドします。

ヒント　CD を使用して DC1000 または DC3000 を復元する場合は、「CD を使用する DC1000 または DC3000 の復元」（P.7-18）に進んでください。

（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。再イメージングを行うと、バイパス モードのアプライアンスが非バイパス設定にリセットされて、バイパス モードに再設定されるまではネットワーク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。

メニューには、次の表にリストされたオプションが表示されます。

表 7-2　復元メニューのオプション

オプション	説明	参照先
1 IP Configuration	復元するアプライアンスの管理インターフェイスに関するネットワーク情報を指定して、アプライアンスが、ISO や他のアップデート ファイルの置かれたサーバと通信できるようにします。	「アプライアンスの管理インターフェイスの識別」（P.7-11）
2 Choose the transport protocol	アプライアンスの復元に使用する ISO イメージの場所、およびアプライアンスがファイルをダウンロードするために必要な資格情報を指定します。	「ISO イメージの場所および転送方式の指定」（P.7-11）
3 Select Patches/Rule Updates	アプライアンスを ISO イメージのベース バージョンに復元した後に適用する、システム ソフトウェアおよび侵入ルールのアップデートを指定します。	「復元中のシステム ソフトウェアと侵入ルールのアップデート」（P.7-13）
4 Download and Mount ISO	適切な ISO イメージ、およびシステム ソフトウェアや侵入ルールのアップデートをダウンロードします。ISO イメージをマウントします。	「ISO とアップデート ファイルのダウンロード、およびイメージのマウント」（P.7-14）
5 Run the Install	復元プロセスを起動します。	「復元プロセスの起動」（P.7-14）
6 Save Configuration 7 Load Configuration	復元設定のセットを後で使用するために保存するか、または保存されたセットをロードします。	「復元設定の保存とロード」（P.7-17）
8 Wipe Contents of Disk	ハード ドライブを安全にスクラビング処理を行って、その内容にアクセスできないようにします。	「ハード ドライブのスクラビング」（P.D-1）

メニュー内の移動には矢印キーを使用します。メニュー オプションを選択するには、上向きまたは下向きの矢印を使用します。ページの下部にある [OK] ボタンと [Cancel] ボタンを切り替えるには、左右の矢印キーを使用します。

メニューには、2 つの異なる種類のオプションが表示されます。

- 番号の付いたオプションを選択するには、最初に適切なオプションを上下の矢印を使用して強調表示してから、ページの下部にある [OK] ボタンが強調表示されているときに。Enter キーを押します。
- 複数選択（オプション ボタン）オプションを選択するには、まず該当するオプションを上下の矢印を使用して強調表示してから、スペース バーを使用してそのオプションに x のマークを付けます。選択を確定するには、[OK] ボタンが強調表示されているときに Enter キーを押します。

ほとんどの場合は、メニュー オプションの [1]、[2]、[4]、および [5] を順番に実行します。任意選択で、メニュー オプションの [3] を追加して、システム ソフトウェアと侵入ルールのアップデートを復元プロセス中にインストールできます。

アプライアンスに現在インストールされているバージョンから別のメジャー バージョンにアプライアンスを復元する場合、2 つのパスの復元プロセスが必要となります。最初のパスでオペレーティング システムをアップデートし、2 番目のパスでシステム ソフトウェアの新しいバージョンをインストールします。

現在 2 番目のパスを実行中の場合、または使用する復元設定が復元ユーティリティによって自動的にロードされた場合は、メニュー オプション [4] の「ISO とアップデート ファイルのダウンロード、およびイメージのマウント」（P.7-14）から開始できます。どちらにしても、シスコは、続行する前に復元設定の値をダブルチェックすることをお勧めします。

ヒント　事前に保存されている設定を使用するには、メニュー オプション [6] の「復元設定の保存とロード」（P.7-17）から開始します。設定をロードした後は、メニュー オプション [4] の「ISO とアップデート ファイルのダウンロード、およびイメージのマウント」（P.7-14）に移動します。

対話型メニューを使用してアプライアンスを復元するには、以下の手順に従います。

ステップ 1　**1 IP Configuration**：「アプライアンスの管理インターフェイスの識別」（P.7-11）を参照してください。

ステップ 2　**2 Choose the transport protocol**：「ISO イメージの場所および転送方式の指定」（P.7-11）を参照してください。

ステップ 3　**3 Select Patches/Rule Updates（オプション）**：「復元中のシステム ソフトウェアと侵入ルールのアップデート」（P.7-13）。

ステップ 4　**4 Download and Mount ISO**：「ISO とアップデート ファイルのダウンロード、およびイメージのマウント」（P.7-14）を参照してください。

ステップ 5　**5 Run the Install**：「復元プロセスの起動」（P.7-14）を参照してください。

アプライアンスの管理インターフェイスの識別

サポートされるデバイス：すべて

サポートされる防御センター：DC1000/3000 を除くすべて

復元ユーティリティを実行する際の最初の手順は、復元するアプライアンスの管理インターフェイスを識別して、アプライアンスが ISO やアップデート ファイルのコピー先サーバと通信できるようにすることです。LOM を使用する場合は、アプライアンスの管理 IP アドレスが LOM の IP アドレスでは**ない**ことに注意してください。

アプライアンスの管理インターフェイスを識別する方法：

アクセス：Admin

ステップ 1　メイン メニューで、[1 IP Configuration] を選択します。

[Pick Device] ページが表示されます。

ステップ 2　アプライアンスの管理インターフェイス（通常は [eth0]）を選択します。

[IP Configuration] ページが表示されます。

ステップ 3　ネットワーク管理に使用するプロトコルとして [IPv4] または [IPv6] を選択します。

管理インターフェイスに IP アドレスを割り当てるためのオプションが表示されます。

ステップ 4　管理インターフェイスに IP アドレスを割り当てる方法として [Static] または [DHCP] を選択します。

- [Static] を選択した場合は、一連のページで、管理インターフェイスの IP アドレス、ネットワーク マスクまたはプレフィックス長、およびデフォルト ゲートウェイを手動で入力するように求められます。
- [DHCP] を選択した場合は、アプライアンスによって管理インターフェイスの IP アドレス、ネットワーク マスクまたはプレフィックス長、およびとデフォルト ゲートウェイが自動的に検出されて、IP アドレスが表示されます。

ステップ 5　プロンプトが出されたら、設定を確認します。

アプライアンスの管理インターフェイスに割り当てられた IP アドレスについてプロンプトが出された場合、確認します。メイン メニューが再表示されます。

ステップ 6　次のセクションISO イメージの場所および転送方式の指定に進みます。

ISO イメージの場所および転送方式の指定

サポートされるデバイス：すべて

サポートされる防御センター：DC1000/3000 を除くすべて

復元プロセスで必要なファイルのダウンロードに使用される管理 IP アドレスを設定した後に、アプライアンスの復元に使用する ISO イメージを識別する必要があります。これは、サポート サイト（「復元 ISO とアップデート ファイルの取得」（P.7-4）を参照）からダウンロードして、Web サーバ、FTP サーバ、または SCP 対応ホストに保存した ISO イメージです。

対話型メニューは、次の表にリストされているように、ダウンロードの実行に必要な情報を入力するためのプロンプトを出します。

表 7-3　復元ファイルのダウンロードに必要な情報

使用する機能	入力する情報
HTTP	• Web サーバの IP アドレス • ISO イメージのディレクトリへのフル パス（たとえば、`/downloads/ISOs/`）
FTP	• FTP サーバの IP アドレス • 使用する資格情報が属するユーザのホーム ディレクトリからの相対で示した、ISO イメージのディレクトリへのパス（たとえば、`mydownloads/ISOs/`） • FTP サーバの承認ユーザ名とパスワード
SCP	• SCP サーバの IP アドレス • SCP サーバの承認ユーザ名 • ISO イメージのディレクトリへのフル パス • 以前に入力したユーザ名に対するパスワード パスワードを入力する前に、アプライアンスから、信頼できるホストのリストに SCP サーバを追加するように求められる場合があることに注意してください。続行するためには、それを受け入れる必要があります。

復元ユーティリティは、ISO イメージ ディレクトリ内でアップデート ファイルを検索することにも注意してください。

復元ファイルの場所および転送方式を指定する方法：

アクセス：Admin

ステップ 1　メイン メニューで、[2 Choose the transport protocol] を選択します。

ステップ 2　表示されるページで [HTTP]、[FTP]、または [SCP] を選択します。

ステップ 3　表 7-3（P.7-12）で説明されているように、選択したプロトコルに必要な情報は、復元ユーティリティで表示される一連のページを使用して入力します。

指定した情報が正しければ、アプライアンスはサーバに接続して、指定した場所にシスコの ISO イメージのリストを表示します。

ステップ 4　使用する ISO イメージを選択します。

ステップ 5　プロンプトが出されたら、設定を確認します。

メイン メニューが再表示されます。

ステップ 6　復元プロセスの一部として、システム ソフトウェアや侵入ルールのアップデートをインストールしますか。

- インストールする場合は、次のセクション復元中のシステム ソフトウェアと侵入ルールのアップデートに進みます。
- インストールしない場合は、「ISO とアップデート ファイルのダウンロード、およびイメージのマウント」（P.7-14）に進みます。復元プロセスの完了後に、システムの Web インターフェイスを使用してアップデートを手動でインストールできることに注意してください。

復元中のシステム ソフトウェアと侵入ルールのアップデート

サポートされるデバイス：すべて

サポートされる防御センター：DC1000/3000 を除くすべて

任意選択で、アプライアンスを ISO イメージのベース バージョンに復元した後、復元ユーティリティを使用してシステム ソフトウェアと侵入ルールをアップデートできます。ルールの更新が必要なのは防御センターだけであることに注意してください。

復元ユーティリティは、1 つのシステム ソフトウェアのアップデートと 1 つのルールのアップデートだけを使用できます。ただし、システムのアップデートは最新のメジャー バージョンからの累積であり、ルールのアップデートも累積です。シスコは、アプライアンスで使用可能な最新のアップデートを取得することを推奨します。「復元 ISO とアップデート ファイルの取得」（P.7-4）を参照してください。

復元プロセス中にアプライアンスをアップデートしないことを選択した場合、システムの Web インターフェイスを使用して後で更新できます。詳細については、インストールするアップデートのリリース ノート、および『*FireSIGHT System User Guide*』の「システム ソフトウェアの更新」の章を参照してください。

復元プロセスの一部としてアップデートをインストールする方法：

アクセス：Admin

ステップ 1　メイン メニューで、[3 Select Patches/Rule Updates] を選択します。

復元ユーティリティは、前の手順（「ISO イメージの場所および転送方式の指定」（P.7-11）を参照）で指定した場所とプロトコルを使用して、その場所にあるシステム ソフトウェア アップデート ファイルのリストを取得して表示します。SCP を使用する場合、アップデート ファイルのリストを表示するは、プロンプトが出されたときにパスワードを入力します。

ステップ 2　使用するシステム ソフトウェアのアップデート（存在する場合）を選択します。

アップデートを選択する必要はありません。アップデートを選択しないで続行するには Enter キーを押します。該当する場所にシステム ソフトウェアのアップデートがない場合は、Enter キーを押して続行するように促すプロンプトがシステムから出されます。

復元ユーティリティは、ルールのアップデート ファイルのリストを取得して表示します。SCP を使用する場合、リストを表示するには、プロンプトが出されたときにパスワードを入力します。

ステップ 3　使用するルールのアップデート（存在する場合）を選択します。

アップデートを選択する必要はありません。アップデートを選択しないで続行するには Enter キーを押します。該当する場所にルールのアップデートがない場合は、Enter キーを押して続行するように促すプロンプトがシステムから出されます。

選択内容が保存されて、メイン メニューが再表示されます。

ステップ 4　次のセクションISO とアップデート ファイルのダウンロード、およびイメージのマウントに進みます。

ISO とアップデート ファイルのダウンロード、およびイメージのマウント

サポートされるデバイス：すべて

サポートされる防御センター：DC1000 と DC3000 を除くすべて

復元プロセスを起動する前の最後の手順は、必要なファイルをダウンロードし、ISO イメージをマウントすることです。

ヒント　この手順を開始する前に、復元設定を後で使用できるように保存することもできます。詳細については、「復元設定の保存とロード」（P.7-17）を参照してください。

ISO イメージをダウンロードしてマウントする方法：

アクセス：Admin

ステップ 1　メイン メニューで、[4 Download and Mount ISO] を選択します。

ステップ 2　プロンプトが出されたら、選択内容を確認します。SCP サーバからダウンロードする場合は、プロンプトが出されたらパスワードを入力します。

適切なファイルがダウンロードされ、マウントされます。メイン メニューが再表示されます。

ステップ 3　次のセクション復元プロセスの起動に進みます。

復元プロセスの起動

サポートされるデバイス：すべて

サポートされる防御センター：DC1000 と DC3000 を除くすべて

ISO イメージをダウンロードしてマウントすれば、復元プロセスを起動する準備が整います。アプライアンスに現在インストールされているバージョンから別のメジャー バージョンにアプライアンスを復元する場合、2 つのパスの復元プロセスが必要となります。最初のパスでオペレーティング システムをアップデートし、2 番目のパスでシステム ソフトウェアの新しいバージョンをインストールします。

2 パスの 1 番目（メジャー バージョンのみの変更）

アプライアンスを別のメジャー バージョンに復元する場合、復元ユーティリティでの最初のパスでは、アプライアンスのオペレーティング システムと、必要な場合は復元ユーティリティ自体を更新します。

（注）　アプライアンスを同じメジャー バージョンに復元する場合、またはプロセスでの 2 番目のパスを実行している場合は、次の手順「2 番目または唯一のパス」（P.7-16）に進みます。

2 パス復元プロセスの 1 番目のパスを実行する方法：

アクセス：Admin

ステップ 1　メイン メニューで、[5 Run the Install] を選択します。

ステップ 2　アプライアンスのリブートするプロンプトが 2 回出されるので確認します。

（注）　外部 USB ドライブを使用して復元するアプライアンスで、システムの異なるバージョンに関連付けられた復元ユーティリティがドライブに存在する場合、続行するにはドライブのユーティリティをアップデートする必要があります。プロンプトが出されたら、ユーティリティの更新（および、保存されている復元設定の削除）のため、`yes` と入力します。その後、更新されたドライブのリブートを確認します。USB ドライブを更新しない場合は、アプライアンスがリブートします。このドライブを使用してアプライアンスを復元することはできません。

ステップ 3　リブートをモニタし、以下のように復元プロセスを再度起動します。

- システムがデータベースの検査を実行している場合、次のメッセージが表示されることがあります。`The system is not operational yet.Checking and repairing database are in progress.This may take a long time to finish.`
- キーボードとモニタの接続では、赤い LILO のブート メニューが表示されます。すぐにいずれかの矢印キーを押して、アプライアンスが現在インストールされているシステムのバージョンが起動されないようにします。
- シリアルまたは SoL/LOM 接続では、BIOS のブート オプションが表示されたとき、次のような LILO のブート プロンプトが表示されるまで、Tab キーをゆっくりと繰り返し押します。

```
LILO 22.8 boot:
3D-5.3 System_Restore
```

ステップ 4　以下のようにして、システムの復元を指示します。

- キーボードとモニタの接続では、矢印キーを使用して [System_Restore] を選択し、Enter キーを押します。
- シリアルまたは SoL/LOM 接続では、プロンプトに `System_Restore` と入力して Enter キーを押します。

いずれの場合も、以下の選択項目に続いて `boot` プロンプトが表示されます。

```
0. Load with standard console
1. Load with serial console
```

ステップ 5　復元ユーティリティの対話型メニューの表示モードを選択します。

- キーボードとモニタ接続の場合は、`0` と入力して Enter キーを押します。
- シリアルまたは SoL/LOM 接続の場合は、`1` と入力して Enter キーを押します。

表示モードを選ばない場合、復元ユーティリティは 10 秒後にデフォルトの標準コンソールを表示します。

アプライアンスをこのメジャー バージョンに初めて復元する場合を除いて、ユーティリティは、最後に使用した復元設定を自動的にロードします。一連のページで設定を確認して、続行します。

復元ユーティリティの著作権情報が表示されます。

ステップ 6　Enter キーを押して著作権表示を確認してから、プロセスの 2 番目のパスを「対話型メニューを使用するアプライアンスの復元」（P.7-9）から開始します。

2 番目または唯一のパス

復元プロセスの 2 番目または唯一のパスを実行するには、次の手順に従います。

復元プロセスの 2 番目または唯一のパスを実行する方法：

アクセス：Admin

ステップ 1　メイン メニューで、[5 Run the Install] を選択します。

ステップ 2　アプライアンスを復元することを確認して、次の手順に進みます。

ステップ 3　アプライアンスのライセンスとネットワーク設定を削除するかどうかを選択します。これらの設定を削除すると、ディスプレイ（コンソール）の設定もリセットされ、シリーズ 3 アプライアンスの場合は LOM もリセットされます。

ほとんどの場合、初期設定プロセスが短縮されるので、これらの設定は削除しません。多くの場合、復元とその後の初期設定を行ってから設定を変更した方が、すぐにリセットするより少ない時間ですみます。詳細については、「次の手順」（P.7-19）を参照してください。

注意　LOM 接続を使用してアプライアンスを復元する場合には、ネットワーク設定を削除**しない**でください。アプライアンスをリブートした後は、LOM 経由で再接続できません。

ステップ 4　アプライアンスの復元に USB ドライブを使用する場合は、アプライアンスを復元する最終確認の入力を求めるプロンプトが復元ユーティリティによって出されたときに、そのドライブを取り外します。

ステップ 5　アプライアンスを復元する最終確認を入力します。

復元プロセスの最終段階が開始します。完了してプロンプトが出されたら、アプライアンスのリブートを確認します。

注意　復元プロセスが完了するまで、十分な時間を確保しておいてください。内部フラッシュ ドライブを備えたアプライアンスでは、フラッシュ ドライブがユーティリティによってまず更新され、その後に他の復元作業の実行に使用されます。フラッシュの更新中に（たとえば Ctrl + C を押すことにより）終了した場合、回復不能なエラーが発生する可能性があります。復元に時間がかかりすぎていると思える場合や、プロセスで他の問題が発生した場合でも、終了**しない**でください。代わりに、サポートに連絡してください。

（注）　再イメージングを行うと、バイパス モードのアプライアンスが非バイパス設定にリセットされて、バイパス モードに再設定されるまではネットワーク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。

ステップ 6　「次の手順」（P.7-19）に進みます。

復元設定の保存とロード

サポートされるデバイス：すべて

サポートされる防御センター：DC1000 と DC3000 を除くすべて

ほとんどのアプライアンスでは、復元ユーティリティを使用して、アプライアンスを復元する必要が生じた場合に使用する復元設定を保存できます。復元ユーティリティは最後に使用された設定を自動的に保存しますが、次の複数の設定を保存することもできます。

- アプライアンスの管理インターフェイスに関するネットワーク情報。「アプライアンスの管理インターフェイスの識別」（P.7-11）を参照してください。
- 復元 ISO イメージの場所、およびアプライアンスがファイルをダウンロードする際に必要な転送プロトコルと資格情報。「ISO イメージの場所および転送方式の指定」（P.7-11）を参照してください。
- アプライアンスを ISO イメージのベース バージョンに復元した後に適用する、システム ソフトウェアおよび侵入ルールのアップデート（存在する場合）。「復元中のシステム ソフトウェアと侵入ルールのアップデート」（P.7-13）を参照してください。

SCP パスワードは保存されません。ユーティリティが SCP を使用して ISO や他のファイルをアプライアンスに転送する必要のあることが設定で指定されている場合、復元プロセスを完了するには、サーバに再認証する必要があります。

復元設定を保存するための最適なタイミングは、上記にリストされた情報を入力した後で、ISO イメージをダウンロードしてマウントする前です。システムの別のメジャー バージョンと互換性を持つように復元 USB ドライブを更新した場合は、保存されている復元設定が失われることに注意してください。

復元設定を保存する方法：

アクセス：Admin

ステップ 1　復元ユーティリティのメイン メニューから、[6 Save Configuration] を選択します。

ユーティリティは保存する設定の値を表示します。

ステップ 2　プロンプトが出されたら、設定を保存することを確認します。

ステップ 3　プロンプトが出されたら、設定の名前を入力します。

設定が保存されて、メイン メニューが再表示されます。

ステップ 4　直前に保存した設定を使用してアプライアンスを復元する場合は、「ISO とアップデート ファイルのダウンロード、およびイメージのマウント」（P.7-14）に進んでください。

保存された復元設定をロードする方法：

アクセス：Admin

ステップ 1　メイン メニューで、[7 Load Configuration] を選択します。

ユーティリティは、保存した復元設定のリストを表示します。最初のオプションの [default_config] は、アプライアンスの復元に最後に使用した設定です。その他のオプションは、保存した復元設定です。

ステップ 2　使用する設定を選択します。

ユーティリティはロードする設定を表示します。

ステップ 3　プロンプトが出されたら、設定をロードすることを確認します。

設定がロードされます。アプライアンスの管理インターフェイスに割り当てられた IP アドレスについてプロンプトが出された場合、確認します。メイン メニューが再表示されます。

ステップ 4　直前にロードした設定を使用してアプライアンスを復元する場合は、「ISO とアップデート ファイルのダウンロード、およびイメージのマウント」（P.7-14）に進んでください。

CD を使用する DC1000 または DC3000 の復元

サポートされるデバイス：なし

サポートされる防御センター：DC1000、DC3000

CD-ROM ドライブを備えた DC1000 および DC3000 防御センターでは、アプライアンスの購入時に復元 CD がシスコにより提供されています。異なるバージョンにアプライアンスを復元する場合は、該当する ISO イメージをダウンロードして、新しい（データのない）復元 ISO CD を作成してから、それを使用してアプライアンスを復元できます。「復元 ISO とアップデート ファイルの取得」（P.7-4）を参照してください。

これらの防御センターの復元には CD を使用するため、それらのアプライアンスでは、復元プロセスの一部としてアップデートをインストールすることはできないことに注意してください。代わりに、後でアプライアンスをアップデートしてください。

CD を使用して、DC1000 または DC3000 を復元する方法：

アクセス：Admin

ステップ 1　防御センターの CD トレイに復元 CD を挿入します。

アプライアンスの電源がオフの場合は、オンにしてトレイを開きます。

ステップ 2　キーボード/モニタまたはシリアル接続を使用して、管理者権限を持つアカウントで防御センターにログインします。パスワードは、防御センターの Web インターフェイスのパスワードと同じです。

防御センターのプロンプトが表示されます。

ステップ 3　プロンプトで、`sudo reboot` と入力して、防御センターを root ユーザとしてリブートします。

CD から防御センターが起動されます。これには数分かかることがあります。

ステップ 4　プロンプトが出されたら、防御センターを復元することを確認します。

ステップ 5　アプライアンスのライセンスとネットワーク設定を削除するかどうかを選択します。これらの設定を削除すると、ディスプレイ（コンソール）設定もリセットされます。

ほとんどの場合、初期設定プロセスが短縮されるので、これらの設定は削除しません。多くの場合、復元とその後の初期設定を行ってから設定を変更した方が、すぐにリセットするより少ない時間ですみます。詳細については、「次の手順」（P.7-19）を参照してください。

ステップ 6　アプライアンスを復元する最終確認を入力します。

復元プロセスが開始して、画面に進行状況が示されます。

注意　復元プロセスが完了するまで、十分な時間を確保しておいてください。まれなケースとして、（たとえば Ctrl + C を押すことやアプライアンスの電源を切ることにより）終了した場合、回復不能なエラーが発生する可能性があります。復元に時間がかかりすぎていると思える場合や、プロセスで他の問題が発生した場合でも、終了**しないでください**。代わりに、サポートに連絡してください。

ステップ 7　プロンプトが表示されたら、Enter を押して続行します。

防御センターは CD を排出します。CD を取り出して、トレイを閉じます。

ステップ 8　プロンプトが再度出されたら、Enter キーを押して、復元が完了したこととアプライアンスをリブートすることを確認します。

アプライアンスがリブートします。

ステップ 9　次の手順に進みます。

次の手順

アプライアンスを工場出荷時設定に復元すると、インライン展開されたデバイスのバイパス設定など、アプライアンスにあるほとんど**すべて**の設定とイベント データが失われます、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。

アプライアンスを復元した後、初期設定プロセスを完了する必要があります。

- アプライアンスのライセンスとネットワーク設定を削除していない場合は、管理ネットワーク上のコンピュータを使用してアプライアンスの Web インターフェイスを直接参照して、セットアップを実行できます。詳細については、「初期セットアップ ページ：デバイス」（P.4-8）および「初期セットアップ ページ：防御センター」（P.4-12）を参照してください。
- ライセンスとネットワーク設定を削除した場合は、管理ネットワークと通信するように設定することから始めて、アプライアンスを新規の場合と同様に設定する必要があります。「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。

ライセンスとネットワーク設定を削除すると、ディスプレイ（コンソール）設定もリセットされ、シリーズ 3 アプライアンスでは LOM の設定もリセットされることに注意してください。初期設定プロセスを完了した後、次を実行します。

- シリアルまたは SoL/LOM 接続を使用してアプライアンスのコンソールにアクセスするする場合、コンソールの出力をリダイレクトする必要があります。「インライン バイパス インターフェイス設置のテスト」（P.3-24）を参照してください。
- LOM を使用する場合は、その機能を再度有効にすること、および少なくとも 1 人の LOM ユーザを有効にする必要があります。「LOM と LOM ユーザを有効にする」（P.7-21）を参照してください。

Lights-Out Management の設定

サポートされるデバイス：シリーズ 3

サポートされる防御センター：シリーズ 3

シリーズ 3 アプライアンスを出荷時の初期状態に復元する必要があり、そのアプライアンスに物理的にアクセスできない場合は、Lights-Out Management（LOM）を使用して復元プロセスを実行できます。LOM を使用して シリーズ 2 アプライアンスを復元することは**できません**。シリーズ 3 アプライアンスだけが LOM をサポートします。

LOM 機能により、Serial over LAN（SoL）の接続設定を使用して、シリーズ 3 防御センターまたは管理対象デバイスに対して限定されたアクションのセットを実行できます。LOM では、アウトオブバンド管理接続のコマンドライン インターフェイスを使用して、シャーシのシリアル番号の表示、ファンの速度や温度などの状態のモニタなどのタスクを実行できます。

LOM コマンドのシンタックスは使用しているユーティリティによって異なりますが、通常 LOM コマンドには次の表にリストされた要素が含まれます。

表 7-4　　LOM コマンドのシンタックス

IPMItool（Linux/Mac）	ipmiutil（Windows）	説明
`ipmitool`	`ipmiutil`	IPMI ユーティリティを起動します。
該当なし	`-V4`	ipmiutil のみ：LOM セッションの管理者権限を有効にします。
`-I lanplus`	`-J3`	LOM セッションの暗号化を有効にします。
`-H` *`IP_address`*	`-N` *`IP_address`*	アプライアンスの管理インターフェイスの IP アドレスを指定します。
`-U` *`username`*	`-U` *`username`*	承認 LOM アカウントのユーザ名を指定します。
該当なし（ログイン時にプロンプトが出されます）	-P *`password`*	ipmiutil のみ：承認 LOM アカウントのパスワードを指定します。
`command`	*`command`*	アプライアンスに対して発行するコマンド。コマンドを発行する場所は、以下のようにユーティリティによって異なることに注意してください。 • IPMItool の場合、コマンドを最後に入力します。 • ipmiutil の場合、コマンドを最初に入力します。

そのため、IPMItool の場合は次のようになります。

```
ipmitool -I lanplus -H IP_address -U username command
```

または、ipmiutil の場合は次のようになります。

```
ipmiutil command -V4 -J3 -N IP_address -U username -P password
```

`chassis power off` コマンドと `chassis power cycle` コマンドは 70xx ファミリ アプライアンスでは無効であることに注意してください。FireSIGHT システムでサポートされる LOM コマンドの完全なリストについては、『*FireSIGHT System User Guide*』の「アプライアンス設定の構成」の章を参照してください。

（注）　SoL を使用して 7000 シリーズ デバイスに接続するには、その前に、デバイスの管理インターフェイスに接続されたサードパーティのスイッチング装置のスパニング ツリー プロトコル（STP）を無効にする必要があります。

LOM を使用してアプライアンスを復元するには、その前に、アプライアンスと復元を実行するユーザの両方の LOM を有効にする必要があります。次に、サードパーティのインテリジェント プラットフォーム管理インターフェイス（IPMI）ユーティリティを使用してアプライアンスにアクセスします。また、アプライアンスのコンソール出力をシリアル ポートにリダイレクトしていることを確認する必要もあります。

詳細については、次の項を参照してください。

- 「LOM と LOM ユーザを有効にする」（P.7-21）
- 「IPMI ユーティリティのインストール」（P.7-22）

LOM と LOM ユーザを有効にする

サポートされるデバイス：シリーズ 3

サポートされる防御センター：シリーズ 3

LOM を使用してアプライアンスを復元するには、その前にその機能を有効にして設定する必要があります。また、この機能を使用するユーザに明示的に LOM 権限を付与する必要もあります。

LOM と LOM ユーザの設定は、各アプライアンスのローカル Web インターフェイスを使用して、アプライアンスごとに行います。つまり、防御センターを使用して管理対象デバイスの LOM を設定することはできません。同様に、ユーザはアプライアンスごとに個別に管理されるため、防御センターで LOM 対応ユーザを有効にしたり作成したりしても、その機能は管理対象デバイスのユーザに転送されません。

LOM ユーザには、次の制限もあります。

- ユーザには管理者ロールを割り当てる必要があります。
- ユーザ名は最大で英数字 16 文字まで使用できます。ハイフンやそれより長いユーザ名は LOM ユーザではサポートされていません。
- パスワードは最大で英数字 20 文字まで使用できます。それより長いパスワードは LOM ユーザではサポートされていません。ユーザの LOM パスワードはそのユーザのシステム パスワードと同じです。
- シリーズ 3 防御センターおよび 8000 シリーズ デバイスは最大 13 の LOM ユーザを設定できます。7000 シリーズ デバイスは最大 8 の LOM ユーザを設定できます。

ヒント　以下の作業の詳細については、『*FireSIGHT System User Guide*』の「アプライアンス 設定の構成」の章を参照してください。

LOM を有効にする方法：

アクセス：Admin

ステップ 1　[System] > [Local] > [Configuration] を選択してから、[Console Configuration] をクリックします。

ステップ 2　次に行う手順は、使用するアプライアンスのモデルによって以下のように異なります。

- 防御センターと 8000 シリーズ デバイスで LOM を有効にするには、**物理シリアル ポート**を使用してリモート アクセスを有効にする必要があります。その後、LOM の IP アドレス、ネットマスク、およびデフォルト ゲートウェイを指定できます（または DHCP を使用してこれらの値が自動的に割り当てられるようにします）。
- 7000 シリーズ デバイスで、[Lights Out Management] を選択して LOM 設定を行います。7000 シリーズ デバイスは、LOM と物理シリアル アクセスを同時にはサポートしません。

（注）　LOM の IP アドレスは、アプライアンスの管理インターフェイスの IP アドレスとは異なる必要があります。

FireSIGHT システム ユーザ用に LOM の機能を有効にする方法：

アクセス：Admin

ステップ 1　[System] > [Local] > [User Management] を選択してから、既存のユーザを編集して LOM 権限を追加するか、またはアプライアンスへの LOM アクセスに使用する新しいユーザを作成します。

ステップ 2　[User Configuration] ページで、すでに有効になっていなければ **Administrator** ロールを有効にします。

ステップ 3　[Allow Lights-Out Management Access] チェック ボックスをオンにして、変更を保存します。

IPMI ユーティリティのインストール

コンピュータ上のサードパーティ IPMI ユーティリティを使用して、アプライアンスへの SoL 接続を作成します。

コンピュータが Linux または Mac OS を実行している場合、IPMItool を使用します。多くの Linux ディストリビューションでは IPMItool が標準装備されていますが、Mac では IPMItool をインストールする必要があります。まず、Mac に Apple の xCode Developer Tools パッケージがインストールされていることを確認します。また、コマンドラインの開発用オプション コンポーネントがインストールされていることを確認します（新バージョンの「UNIX Development」と「System Tools」、または旧バージョンの「Command Line Support」）。最後に、MacPorts と IPMItool をインストールします。詳細については、任意の検索エンジンを使用するか、または以下のサイトを参照してください。

```
https://developer.apple.com/technologies/tools/
http://www.macports.org/
```

Windows 環境では、ipmiutil を使用します。これはユーザ自身でコンパイルする必要があります。コンパイラへのアクセス権がない場合は、コンパイルするために ipmiutil 自体を使用できます。詳細については、任意の検索エンジンを使用するか、または以下のサイトを参照してください。

```
http://ipmiutil.sourceforge.net/
```

FirePOWER デバイスの所要電力

この項では、ここでは、FirePOWER デバイスの所要電力および関連情報について説明します。

（注） ASA FirePOWER デバイスの所要電力について詳しくは、ASA のマニュアルを参照してください。

警告と注意

このドキュメントには、警告と注意の両方が含まれています。警告は、安全に関するものです。警告に従わないと、けがや機器の損傷が生じる可能性があります。注意は、正常に機能するための要件です。注意に従わないと、正常に機能しないことがあります。

注意 機器またはサブアセンブリの屋内ポートは、建物内配線や露出配線、またはケーブル配線だけの接続に適しています。建物内部の装置ポートまたはサブアセンブリは工場外設備（OSP）またはその配線に接続しているインターフェイスに金属的に接続**しないでください**。これらのインターフェイスは、屋内インターフェイス専用（GR-1089-CORE Issue 4 に記載されたタイプ 2 ポートまたはタイプ 4 ポート）に設計されており、屋外用の OSP ケーブルと区別する必要があります。これらのインターフェイスを金属的に OSP 配線と接続する場合、プライマリ プロテクタを追加するだけでは、十分に保護されません。

静電気制御

注意 接地されたリスト ストラップや静電放電作業台の使用などの静電放電の制御手順は、アプライアンスを開梱、インストール、または移動する前に実施されている必要があります。過剰な静電放電により、アプライアンスが損傷したり、意図しない処理が発生したりする可能性があります。

70xx ファミリのアプライアンス

この項では、以下のシスコ デバイスの所要電力について説明します。

- 3D7010、3D7020、および 3D7030（CHRY-1U-AC）

これらのシスコ デバイスは、National Electric Code が適用されるネットワーク通信施設や地域で専門の担当者が設置するのに適しています。各デバイスは AC アプライアンスとしてのみ使用可能であることに注意してください。

シスコは、返品が必要となる場合に備えて梱包材を保管しておくことをお勧めします。

詳細については、次の項を参照してください。

- 回路の設置、電圧、電流、周波数範囲、および電源コードについて詳しくは、「設置」（P.A-2）を参照してください。
- ボンディング箇所、推奨端子、およびアース線の要件について詳しくは、「接地の要件」（P.A-3）を参照してください。

設置

FireSIGHT システムのアプライアンスは、NFPA 70 の 250 条、National Electric Code（NEC）ハンドブック、および地域の電気規格の要件に従って設置する必要があります。

アプライアンスは、単一の電源装置を使用します。FireSIGHT システムを設置するネットワーク機器の入力場所に、外部電力サージ保護デバイスを使用する必要があります。

電源回路の定格は、アプライアンス全体の定格に対応している必要があります。

電圧

電源は、公称電圧 100 VAC から 240 VAC（最大電圧 90 VAC から 264 VAC）に対応しています。この範囲外の電圧を使用すると、アプライアンスが損傷することがあります。

電流

表示された定格電流は全範囲で最大 2 A です。出火の危険を小さくするために、適切な導線とブレーカーを使用する必要があります。

周波数範囲

AC 電源の周波数範囲は 47 Hz から 63 Hz です。この範囲外の周波数では、アプライアンスが動作しないか、不適正に動作する可能性があります。

電源コード

電源装置の電源接続は IEC C14 コネクタで、IEC C13 コネクタを接続できます。UL 認定電源コードを使用する必要があります。最小ワイヤ ゲージは 16 AWG です。アプライアンスに付属のコードは 16 AWG の NEMA 515P プラグ付きの UL 認定コードです。他の電源コードについては、工場にお問い合わせください。

（注）　電源のコードは切断しないでください。

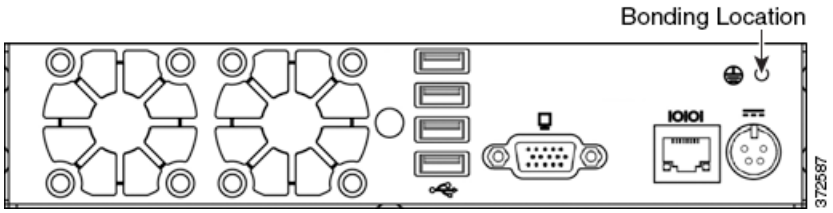
接地の要件

アプライアンスは、共通ボンディング網に接地する必要があります。

ボンディング箇所

接地のボンディング箇所は、シャーシの背面にあります。M4 スタッドが備わっています。リング端子を接続するために、外向き歯付きのロック ワッシャが備わっています。各スタッドの横に標準の接地記号があります。

次の図は、シャーシ上のボンディング箇所を示しています。



推奨端子

アース接続のためには、UL 認定端子を使用する必要があります。#6（M3.5）スタッド用のクリアランスホール付きリング端子を使用できます。16 AWG 線には、AMP/Tyco 36151 が推奨されます。これは、#6 スタッド用の穴付き UL 認定リング端子です。

アース線の要件

アース線は、単一故障が生じた場合に回路電流を十分に処理できるサイズであることが必要です。アース線のサイズは、回路を保護するために使用されるブレーカーの電流と同じにします。「電流」（P.A-2）を参照してください。

露出した導体は、圧着接続を行う前に、腐食防止剤でコーティングする必要があります。接地のために使用できるのは銅線のケーブルだけです。

71xx ファミリのアプライアンス

この項では、以下のシスコ デバイスの所要電力について説明します。

- 3D7110 および 3D7120（GERY-1U-8-AC）
- 3D7115 および 3D7125（GERY-1U-4C8S-AC）

これらのシスコ デバイスは、National Electric Code が適用されるネットワーク通信施設や地域で専門の担当者が設置するのに適しています。各デバイスは AC アプライアンスとしてのみ使用可能であることに注意してください。

シスコは、返品が必要となる場合に備えて梱包材を保管しておくことをお勧めします。

詳細については、次の項を参照してください。

- 回路の設置、電圧、電流、周波数範囲、および電源コードについて詳しくは、「設置」（P.A-4）を参照してください。
- ボンディング箇所、推奨端子、およびアース線の要件について詳しくは、「接地の要件」（P.A-5）を参照してください。

設置

FireSIGHT システム は、NFPA 70 の 250 条、National Electric Code（NEC）ハンドブック、および地域の電気規格の要件に従って設置する必要があります。

冗長電源を作成するためには、別の回路が必要です。電源状態の問題や入力ラインの電力異常による電力損失を防ぐために、無停電電源またはバッテリ保護電源を使用します。

アプライアンス全体を稼働させるために十分な電力を、各電源に供給します。各電源の電圧と電流の定格は、アプライアンスのラベルに記載されています。

FireSIGHT システムを設置するネットワーク機器の入力場所には、外部電力サージ保護デバイスを使用します。

別個の回路の設置

複数の異なる回路を使用する場合は、それぞれの回路の定格がアプライアンス全体の定格に対応している必要があります。この設定により、回路の障害と電源の障害から保護されます。

例: 各電源が別々の 220 V 回路に接続しています。ラベルに記載されているように、各回路には 5 A を供給できることが必要です。

同じ回路の設置

同じ回路を使用して両方の電力を供給する場合、1 つの電源装置の電力定格がボックス全体に適用されます。この設定では、電源の障害からのみ保護されます。

例: どちらの電源装置も同じ 220 V 回路に接続されています。この回路から得られる最大電流は、ラベルに示されているとおり 5 A です。

電圧

電源装置は次の電圧に対応しています: 公称 100 VAC から 240 VAC（最大 85 VAC から 264 VAC）。この範囲外の電圧を使用すると、アプライアンスが損傷することがあります。

電流

ラベルに示された各電源装置の定格電流は、範囲全体では装置あたり最大 10 A、187 VAC から 264 VAC では装置あたり最大 5 A です。出火の危険を小さくするために、適切な導線とブレーカーを使用する必要があります。

周波数範囲

AC 電源の周波数範囲は 47 Hz から 63 Hz です。この範囲外の周波数では、アプライアンスが動作しないか、不適正に動作する可能性があります。

電源コード

電源装置の電源接続は IEC C14 コネクタで、IEC C13 コネクタを接続できます。UL 認定電源コードを使用する必要があります。最小ワイヤ ゲージは 16 AWG です。アプライアンスに付属のコードは 16 AWG の NEMA 515P プラグ付きの UL 認定コードです。他の電源コードについては、工場にお問い合わせください。

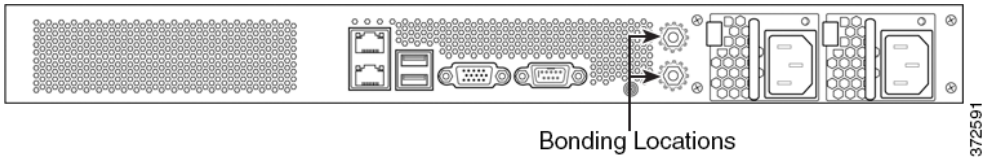
接地の要件

FireSIGHT システムは、共通ボンディング網に接地する必要があります。

ボンディング箇所

接地のボンディング箇所は、シャーシの背面にあります。M4 スタッドが備わっています。リング端子を接続するために、外向き歯付きのロック ワッシャが備わっています。各スタッドの横に標準の接地記号があります。

次の図は、シャーシ上のボンディング箇所を示しています。



推奨端子

アース接続には UL 認定端子を使用する必要があります。4 mm または #8 スタッド用のクリアランスホール付きリング端子を使用できます 10-12 AWG 線には、Tyco 34853 が推奨されます。これは、#8 スタッド用の穴付き UL 認定リング端子です。

アース線の要件

アース線は、単一故障が生じた場合に回路電流を十分に処理できるサイズであることが必要です。アース線のサイズは、回路を保護するために使用されるブレーカーの電流と同じにします。「電流」（P.A-4）を参照してください。

露出した導体は、圧着接続を行う前に、腐食防止剤でコーティングする必要があります。接地のために使用できるのは銅線のケーブルだけです。

81xx ファミリのアプライアンス

この項では、以下のシスコ デバイスの所要電力について説明します。

- 3D8120、3D8130、および 3D8140（CHAS-1U-AC、CHAS-1U-DC、または CHAS-1U-AC/DC）

これらのシスコ デバイスは、National Electric Code が適用されるネットワーク通信施設や地域で専門の担当者が設置するのに適しています。

シスコは、返品が必要となる場合に備えて梱包材を保管しておくことをお勧めします。

詳細については、次の項を参照してください。

- 回路の設置、電圧、電流、周波数範囲、および電源コードについて詳しくは、「AC の設置」（P.A-6）を参照してください。
- 回路の設置、電圧、電流、接地基準、端子、ブレーカー要件、および配線の最小サイズについて詳しくは、「DC の設置」（P.A-7）を参照してください。
- ボンディング箇所、推奨端子、アース線の要件、および DC 電源について詳しくは、「接地の要件」（P.A-9）を参照してください。

AC の設置

FireSIGHT システム は、NFPA 70 の 250 条、National Electric Code（NEC）ハンドブック、および地域の電気規格の要件に従って設置する必要があります。

注意　AC 電源に DC 電力を接続**しないでください**。

冗長電源を作成するためには、別の回路が必要です。電源状態の問題や入力ラインの電力異常による電力損失を防ぐために、無停電電源またはバッテリ保護電源を使用します。

アプライアンス全体を稼働させるために十分な電力を、各電源に供給します。各電源の電圧と電流の定格は、アプライアンスのラベルに記載されています。

FireSIGHT システムを設置するネットワーク機器の入力場所には、外部電力サージ保護デバイスを使用します。

別個の回路の設置

複数の異なる回路を使用する場合は、それぞれの回路の定格がアプライアンス全体の定格に対応している必要があります。この設定により、回路の障害と電源の障害から保護されます。

例: 各電源が別々の 220 V 回路に接続しています。ラベルに記載されているように、各回路には 5 A を供給できることが必要です。

同じ回路の設置

同じ回路を使用して両方の電力を供給する場合、1 つの電源装置の電力定格がボックス全体に適用されます。この設定では、電源の障害からのみ保護されます。

例: どちらの電源装置も同じ 220 V 回路に接続されています。この回路から得られる最大電流は、ラベルに示されているとおり 5 A です。

AC 電圧

電源装置は次の電圧に対応しています: 公称 100 VAC から 240 VAC（最大 85 VAC から 264 VAC）。この範囲外の電圧を使用すると、アプライアンスが損傷することがあります。

AC 電流

ラベルに示された各電源装置の定格電流は、範囲全体では装置あたり最大 5.2 A、187 VAC から 264 VAC では装置あたり最大 2.6A です。出火の危険を小さくするために、適切な導線とブレーカーを使用する必要があります。

周波数範囲

AC 電源の周波数範囲は 47 Hz から 63 Hz です。この範囲外の周波数では、アプライアンスが動作しないか、不適正に動作する可能性があります。

電源コード

電源装置の電源接続は IEC C14 コネクタで、IEC C13 コネクタを接続できます。UL 認定電源コードを使用する必要があります。最小ワイヤ ゲージは 16 AWG です。アプライアンスに付属のコードは 16 AWG の NEMA 515P プラグ付きの UL 認定コードです。他の電源コードについては、工場にお問い合わせください。

DC の設置

冗長電源を作成するためには、別の回路が必要です。電源状態の問題や入力ラインの電力異常による電力損失を防ぐために、無停電電源またはバッテリ保護電源を使用します。

注意　DC 電源に AC 電力を接続**しないでください**。

アプライアンス全体を稼働させるために十分な電力を、各電源に供給します。各電源の電圧と電流の定格は、アプライアンスのラベルに記載されています。

FireSIGHT システムを設置するネットワーク機器の入力場所には、外部電力サージ保護デバイスを使用します。

別個の回路の設置

複数の異なる回路を使用する場合は、それぞれの回路の定格がアプライアンス全体の定格に対応している必要があります。この設定により、回路の障害と電源の障害から保護されます。

例: 各電源が別々の-48 VDC 回路に接続されています。ラベルに記載されているように、各回路には 20 A を供給できることが必要です。

同じ回路の設置

同じ回路を使用して両方の電力を供給する場合、1 つの電源装置の電力定格がボックス全体に適用されます。この設定では、電源の障害からのみ保護されます。

例: どちらの電源装置も同じ –48 VDC 回路に接続されています。この回路から得られる最大電流は、ラベルに示されているとおり 20 A です。

注意　この最適化を使用するには、電源コードの定格が各電源装置の全体の定格に対応している必要があります。

DC 電圧

電源装置は、以下の電圧に対応しています。

- RTN を基準として公称 -48 V。
- -40 VDC から最大 -72 VDC

この範囲外の電圧を使用すると、アプライアンスが損傷することがあります。

DC 電流

装置あたり最大 11 A。

接地基準

DC 電源装置は、接地基準から完全に分離されます。

推奨端子

電源はネジ端子によって DC 電源に接続されます。端子は UL 認定のものであることが必要です。端子には M4（#8）ネジに対応した穴が必要です。端子の最大幅は 8.1 mm（0.320 インチ）です。10 - 12 ゲージの導線用の代表的なスペード端子は Tyco 325197 です。

ブレーカー要件

定格電圧で定格電流を流せる容量のブレーカーを設置する必要があります。回路ブレーカーは次の要件を満たす必要があります。

- UL 認定品
- CSA 認定（推奨）
- VDE 認定（推奨）
- 最大負荷（20 A）のサポート
- 設置電圧（電源装置の要件に応じて -40 V から -72 VDC）のサポート
- DC 使用に適した定格

推奨されるブレーカーは、Airpax IELK1-1-72-20.0-01-V です。使用される端子オプションは設置環境によって異なります。このブレーカーは、DC 定格が 80 V の単極 20 A ブレーカーです。これは*長遅延型*としてリストされています。このブレーカーについて詳しくは、http://www.airpax.net/site/utilities/eliterature/pdfs/ial.pdf を参照してください。

配線サイズの最小要件

レースウェイあたり 3 本の導線（1 回路）がある電源フィードは、12 AWG 線を使用できます。レースウェイあたり複数の回路がある電源フィードは、10 AWG 線を使用する必要があります。冗長電源装置用の 2 つの異なるフィードは 2 つの回路であり、10 AWG 線を使用する必要があることに注意してください。

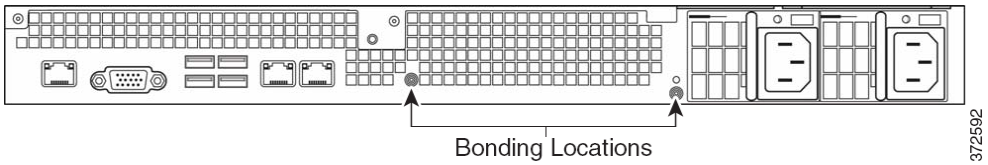
接地の要件

FireSIGHT システムは、共通ボンディング網に接地する必要があります。

ボンディング箇所

接地のボンディング箇所は、シャーシの背面にあります。M4 スタッドが備わっています。リング端子を接続するために、外向き歯付きのロック ワッシャが備わっています。各スタッドの横に標準の接地記号があります。

次の図は、1 U シャーシ上のボンディング箇所を示しています。



推奨端子

アース接続には UL 認定端子を使用する必要があります。4 mm または #8 スタッド用のクリアランスホール付きリング端子を使用できます 10-12 AWG 線には、Tyco 34853 が推奨されます。これは、#8 スタッド用の穴付き UL 認定リング端子です。

アース線の要件

アース線は、単一故障が生じた場合に回路電流を十分に処理できるサイズであることが必要です。アース線のサイズは、回路を保護するために使用されるブレーカーの電流と同じにします。AC 回路については、「AC 電流」（P.A-6）を参照してください。DC 回路については、「DC 電流」（P.A-8）を参照してください。

露出した導体は、圧着接続を行う前に、腐食防止剤でコーティングする必要があります。接地のために使用できるのは銅線のケーブルだけです。

DC 電源装置

DC 電源装置には、電源ごとの追加のアース接続があります。これにより、ホットスワップ可能な電源装置を電力、リターン、およびアースに接続して、安全に挿入できるようにします。アース ラグを接続する必要があります。

これは外向き歯付きのロック ワッシャがある M4 ネジです。

アース線は、回路ブレーカーに適合するサイズにする必要があります。

82xx ファミリのアプライアンス

この項では、以下のシスコ デバイスの所要電力について説明します。

- 3D8250、3D8260、3D8270、および 3D8290（CHAS-2U-AC、CHAS-2U-DC、または CHAS-2U-AC/DC）

これらのシスコ デバイスは、National Electric Code が適用されるネットワーク通信施設や地域で専門の担当者が設置するのに適しています。

シスコは、返品が必要となる場合に備えて梱包材を保管しておくことをお勧めします。

詳細については、次の項を参照してください。

- 回路の設置、電圧、電流、周波数範囲、および電源コードについて詳しくは、「AC の設置」（P.A-10）を参照してください。
- 回路の設置、電圧、電流、接地基準、端子、ブレーカー要件、および配線の最小サイズについて詳しくは、「DC の設置」（P.A-11）を参照してください。
- ボンディング箇所、推奨端子、アース線の要件、および DC 電源について詳しくは、「接地の要件」（P.A-13）を参照してください。

AC の設置

FireSIGHT システム は、NFPA 70 の 250 条、National Electric Code（NEC）ハンドブック、および地域の電気規格の要件に従って設置する必要があります。

注意　AC 電源に DC 電力を接続**しないでください**。

冗長電源を作成するためには、別の回路が必要です。電源状態の問題や入力ラインの電力異常による電力損失を防ぐために、無停電電源またはバッテリ保護電源を使用します。

アプライアンス全体を稼働させるために十分な電力を、各電源に供給します。各電源の電圧と電流の定格は、アプライアンスのラベルに記載されています。

FireSIGHT システムを設置するネットワーク機器の入力場所には、外部電力サージ保護デバイスを使用します。

別個の回路の設置

複数の異なる回路を使用する場合は、それぞれの回路の定格がアプライアンス全体の定格に対応している必要があります。この設定により、回路の障害と電源の障害から保護されます。

例: 各電源が別々の 220 V 回路に接続しています。ラベルに記載されているように、各回路には 5 A を供給できることが必要です。

同じ回路の設置

同じ回路を使用して両方の電力を供給する場合、1 つの電源装置の電力定格がボックス全体に適用されます。この設定では、電源の障害からのみ保護されます。

例: どちらの電源装置も同じ 220 V 回路に接続されています。この回路から得られる最大電流は、ラベルに示されているとおり 5 A です。

AC 電圧

電源装置は次の電圧に対応しています: 公称 100 VAC から 240 VAC（最大 85 VAC から 264 VAC）。この範囲外の電圧を使用すると、アプライアンスが損傷することがあります。

AC 電流

ラベルに示された各電源装置の定格電流は、範囲全体では装置あたり最大 8 A、187 VAC から 264 VAC では装置あたり最大 4A です。出火の危険を小さくするために、適切な導線とブレーカーを使用する必要があります。

周波数範囲

AC 電源の周波数範囲は 47 Hz から 63 Hz です。この範囲外の周波数では、アプライアンスが動作しないか、不適正に動作する可能性があります。

電源コード

電源装置の電源接続は IEC C14 コネクタで、IEC C13 コネクタを接続できます。UL 認定電源コードを使用する必要があります。最小ワイヤ ゲージは 16 AWG です。アプライアンスに付属のコードは 16 AWG の NEMA 515P プラグ付きの UL 認定コードです。他の電源コードについては、工場にお問い合わせください。

DC の設置

冗長電源を作成するためには、別の回路が必要です。電源状態の問題や入力ラインの電力異常による電力損失を防ぐために、無停電電源またはバッテリ保護電源を使用します。

注意　DC 電源に AC 電力を接続**しない**でください。

アプライアンス全体を稼働させるために十分な電力を、各電源に供給します。各電源の電圧と電流の定格は、アプライアンスのラベルに記載されています。

FireSIGHT システムを設置するネットワーク機器の入力場所には、外部電力サージ保護デバイスを使用します。

別個の回路の設置

複数の異なる回路を使用する場合は、それぞれの回路の定格がアプライアンス全体の定格に対応している必要があります。この設定により、回路の障害と電源の障害から保護されます。

例: 各電源が別々の-48 VDC 回路に接続されています。ラベルに記載されているように、各回路には 20 A を供給できることが必要です。

同じ回路の設置

同じ回路を使用して両方の電力を供給する場合、1 つの電源装置の電力定格がボックス全体に適用されます。この設定では、電源の障害からのみ保護されます。

例: どちらの電源装置も同じ –48 VDC 回路に接続されています。この回路から得られる最大電流は、ラベルに示されているとおり 20 A です。

注意　この最適化を使用するには、電源コードの定格が各電源装置の全体の定格に対応している必要があります。

DC 電圧

電源装置は、以下の電圧に対応しています。

- RTN を基準として公称 -48 V。
- -40 VDC から最大 -72 VDC

この範囲外の電圧を使用すると、アプライアンスが損傷することがあります。

DC 電流

装置あたり最大 18 A。

接地基準

DC 電源装置は、接地基準から完全に分離されます。

推奨端子

電源はネジ端子によって DC 電源に接続されます。端子は UL 認定のものであることが必要です。端子には M4（#8）ネジに対応した穴が必要です。端子の最大幅は 8.1 mm（0.320 インチ）です。10 - 12 ゲージの導線用の代表的なスペード端子は Tyco 325197 です。

ブレーカー要件

定格電圧で定格電流を流せる容量のブレーカーを設置する必要があります。回路ブレーカーは次の要件を満たす必要があります。

- UL 認定品
- CSA 認定（推奨）
- VDE 認定（推奨）
- 最大負荷（20 A）のサポート
- 設置電圧（電源装置の要件に応じて -40 V から -72 VDC）のサポート
- DC 使用に適した定格

推奨されるブレーカーは、Airpax IELK1-1-72-20.0-01-V です。使用される端子オプションは設置環境によって異なります。このブレーカーは、DC 定格が 80 V の単極 20 A ブレーカーです。これは*長遅延型*としてリストされています。このブレーカーについて詳しくは、http://www.airpax.net/site/utilities/eliterature/pdfs/ial.pdf を参照してください。

配線サイズの最小要件

レースウェイあたり 3 本の導線（1 回路）がある電源フィードは、12 AWG 線を使用できます。レースウェイあたり複数の回路がある電源フィードは、10 AWG 線を使用する必要があります。冗長電源装置用の 2 つの異なるフィードは 2 つの回路であり、10 AWG 線を使用する必要があることに注意してください。

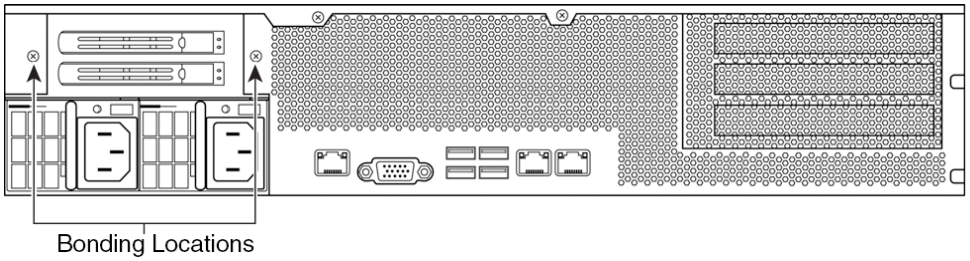
接地の要件

FireSIGHT システムは、共通ボンディング網に接地する必要があります。

ボンディング箇所

接地のボンディング箇所は、シャーシの背面にあります。M4 スタッドが備わっています。リング端子を接続するために、外向き歯付きのロック ワッシャが備わっています。各スタッドの横に標準の接地記号があります。

次の図は、2 U シャーシ上の接合箇所を示しています。



推奨端子

アース接続には UL 認定端子を使用する必要があります。4 mm または #8 スタッド用のクリアランスホール付きリング端子を使用できます 10-12 AWG 線には、Tyco 34853 が推奨されます。これは、#8 スタッド用の穴付き UL 認定リング端子です。

アース線の要件

アース線は、単一故障が生じた場合に回路電流を十分に処理できるサイズであることが必要です。アース線のサイズは、回路を保護するために使用されるブレーカーの電流と同じにします。AC 回路については、「AC 電流」（P.A-6）を参照してください。DC 回路については、「DC 電流」（P.A-8）を参照してください。

露出した導体は、圧着接続を行う前に、腐食防止剤でコーティングする必要があります。接地のために使用できるのは銅線のケーブルだけです。

DC 電源装置

DC 電源装置には、電源ごとの追加のアース接続があります。これにより、ホットスワップ可能な電源装置を電力、リターン、およびアースに接続して、安全に挿入できるようにします。アース ラグを接続する必要があります。

これは外向き歯付きのロック ワッシャがある M4 ネジです。

アース線は、回路ブレーカーに適合するサイズにする必要があります。

83xx ファミリのアプライアンス

この項では、以下のシスコ デバイスの所要電力について説明します。

- 3D8350、3D8360、3D8370、および 3D8390（PG35-2U-AC/DC）

これらのシスコ デバイスは、National Electric Code が適用されるネットワーク通信施設や地域で専門の担当者が設置するのに適しています。

シスコは、返品が必要となる場合に備えて梱包材を保管しておくことをお勧めします。

詳細については、次の項を参照してください。

- 回路の設置、電圧、電流、周波数範囲、および電源コードについて詳しくは、「AC の設置」（P.A-14）を参照してください。
- 回路の設置、電圧、電流、接地基準、端子、ブレーカー要件、および配線の最小サイズについて詳しくは、「DC の設置」（P.A-15）を参照してください。
- ボンディング箇所、推奨端子、アース線の要件、および DC 電源について詳しくは、「接地の要件」（P.A-17）を参照してください。

AC の設置

FireSIGHT システム は、NFPA 70 の 250 条、National Electric Code（NEC）ハンドブック、および地域の電気規格の要件に従って設置する必要があります。

注意　AC 電源に DC 電力を接続**しない**でください。

冗長電源を作成するためには、別の回路が必要です。電源状態の問題や入力ラインの電力異常による電力損失を防ぐために、無停電電源またはバッテリ保護電源を使用します。

アプライアンス全体を稼働させるために十分な電力を、各電源に供給します。各電源の電圧と電流の定格は、アプライアンスのラベルに記載されています。

FireSIGHT システムを設置するネットワーク機器の入力場所には、外部電力サージ保護デバイスを使用します。

別個の回路の設置

複数の異なる回路を使用する場合は、それぞれの回路の定格がアプライアンス全体の定格に対応している必要があります。この設定により、回路の障害と電源の障害から保護されます。

例: 各電源が別々の 220 V 回路に接続しています。ラベルに記載されているように、各回路には 10 A を供給できることが必要です。

同じ回路の設置

同じ回路を使用して両方の電力を供給する場合、1 つの電源装置の電力定格がボックス全体に適用されます。この設定では、電源の障害からのみ保護されます。

例: どちらの電源装置も同じ 220 V 回路に接続されています。この回路から得られる最大電流は、ラベルに示されているとおり 10 A です。

AC 電圧

電源装置は次の電圧に対応しています: 公称 100 VAC から 240 VAC（最大 85 VAC から 264 VAC）。この範囲外の電圧を使用すると、アプライアンスが損傷することがあります。

AC 電流

ラベルに示された各電源装置の定格電流は、範囲全体では装置あたり最大 11 A、187 VAC から 264 VAC では装置あたり最大 5.5 A です。出火の危険を小さくするために、適切な導線とブレーカーを使用する必要があります。

周波数範囲

AC 電源の周波数範囲は 47 Hz から 63 Hz です。この範囲外の周波数では、アプライアンスが動作しないか、不適正に動作する可能性があります。

電源コード

電源装置の電源接続は IEC C14 コネクタで、IEC C13 コネクタを接続できます。UL 認定電源コードを使用する必要があります。最小ワイヤ ゲージは 16 AWG です。アプライアンスに付属のコードは 16 AWG の NEMA 515P プラグ付きの UL 認定コードです。他の電源コードについては、工場にお問い合わせください。

DC の設置

冗長電源を作成するためには、別の回路が必要です。電源状態の問題や入力ラインの電力異常による電力損失を防ぐために、無停電電源またはバッテリ保護電源を使用します。

注意　DC 電源に AC 電力を接続**しない**でください。

アプライアンス全体を稼働させるために十分な電力を、各電源に供給します。各電源の電圧と電流の定格は、アプライアンスのラベルに記載されています。

FireSIGHT システムを設置するネットワーク機器の入力場所には、外部電力サージ保護デバイスを使用します。

別個の回路の設置

複数の異なる回路を使用する場合は、それぞれの回路の定格がアプライアンス全体の定格に対応している必要があります。この設定により、回路の障害と電源の障害から保護されます。

例: 各電源が別々の-48 VDC 回路に接続されています。ラベルに記載されているように、各回路には 25 A を供給できることが必要です。

同じ回路の設置

同じ回路を使用して両方の電力を供給する場合、1 つの電源装置の電力定格がボックス全体に適用されます。この設定では、電源の障害からのみ保護されます。

例: どちらの電源装置も同じ –48 VDC 回路に接続されています。この回路から得られる最大電流は、ラベルに示されているとおり 25 A です。

注意　この最適化を使用するには、電源コードの定格が各電源装置の全体の定格に対応している必要があります。

DC 電圧

電源装置は、以下の電圧に対応しています。

- RTN を基準として公称 -48 V。
- -40 VDC から最大 -72 VDC

この範囲外の電圧を使用すると、アプライアンスが損傷することがあります。

DC 電流

装置あたり最大 25 A。

接地基準

DC 電源装置は、接地基準から完全に分離されます。

推奨端子

電源はネジ端子によって DC 電源に接続されます。端子は UL 認定のものであることが必要です。端子には M4（#8）ネジに対応した穴が必要です。端子の最大幅は 8.1 mm（0.320 インチ）です。10 - 12 ゲージの導線用の代表的なスペード端子は Tyco 325197 です。

ブレーカー要件

定格電圧で定格電流を流せる容量のブレーカーを設置する必要があります。回路ブレーカーは次の要件を満たす必要があります。

- UL 認定品
- CSA 認定（推奨）
- VDE 認定（推奨）
- 最大負荷（20 A）のサポート
- 設置電圧（電源装置の要件に応じて -40 V から -72 VDC）のサポート
- DC 使用に適した定格

推奨されるブレーカーは、Airpax IELK1-1-72-20.0-01-V です。使用される端子オプションは設置環境によって異なります。このブレーカーは、DC 定格が 80 V の単極 20 A ブレーカーです。これは*長遅延型*としてリストされています。このブレーカーについて詳しくは、http://www.airpax.net/site/utilities/eliterature/pdfs/ial.pdf を参照してください。

配線サイズの最小要件

レースウェイあたり 3 本の導線（1 回路）がある電源フィードは、12 AWG 線を使用できます。レースウェイあたり複数の回路がある電源フィードは、10 AWG 線を使用する必要があります。冗長電源装置用の 2 つの異なるフィードは 2 つの回路であり、10 AWG 線を使用する必要があることに注意してください。

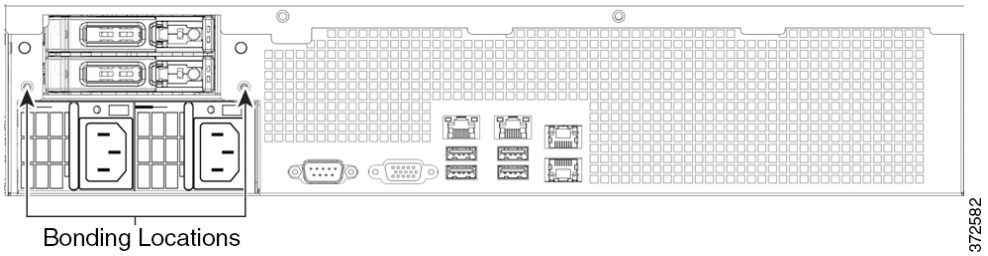
接地の要件

FireSIGHT システムは、共通ボンディング網に接地する必要があります。

ボンディング箇所

接地のボンディング箇所は、シャーシの背面にあります。M4 スタッドが備わっています。リング端子を接続するために、外向き歯付きのロック ワッシャが備わっています。各スタッドの横に標準の接地記号があります。

次の図は、83xx ファミリ 2 U シャーシ上のボンディング箇所を示しています。



推奨端子

アース接続には UL 認定端子を使用する必要があります。4 mm または #8 スタッド用のクリアランスホール付きリング端子を使用できます 10-12 AWG 線には、Tyco 34853 が推奨されます。これは、#8 スタッド用の穴付き UL 認定リング端子です。

アース線の要件

アース線は、単一故障が生じた場合に回路電流を十分に処理できるサイズであることが必要です。アース線のサイズは、回路を保護するために使用されるブレーカーの電流と同じにします。AC 回路については、「AC 電流」（P.A-15）を参照してください。DC 回路については、「DC 電流」（P.A-16）を参照してください。

露出した導体は、圧着接続を行う前に、腐食防止剤でコーティングする必要があります。接地のために使用できるのは銅線のケーブルだけです。

DC 電源装置

DC 電源装置には、電源ごとの追加のアース接続があります。これにより、ホットスワップ可能な電源装置を電力、リターン、およびアースに接続して、安全に挿入できるようにします。アース ラグを接続する必要があります。

これは外向き歯付きのロック ワッシャがある M4 ネジです。

アース線は、回路ブレーカーに適合するサイズにする必要があります。

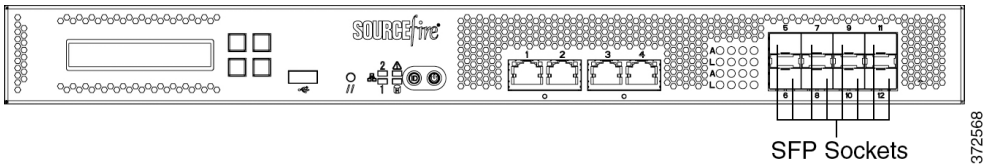
3D71x5 および AMP7150 デバイスでの SFP トランシーバの使用

以下のセクションでは、3D7115 と 3D7125（総称で 3D71x5）および AMP7150 で、Small Form-Factor Pluggable（SFP）のソケットとトランシーバを使用する方法について詳しく説明します。

3D71x5 と AMP7150 SFP のソケットおよびトランシーバ

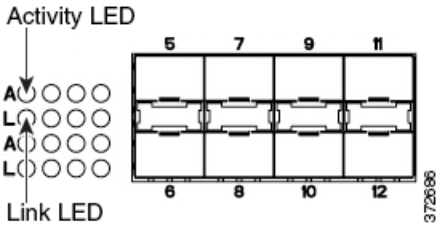
3D71x5 と AMP7150 のアプライアンスには、8 つの Small Form-Factor Pluggable（SFP）のソケットが含まれていて、最大 8 つの SFP トランシーバを含めることができます。

図 B-1　　3D71x5 および AMP7150 の正面図



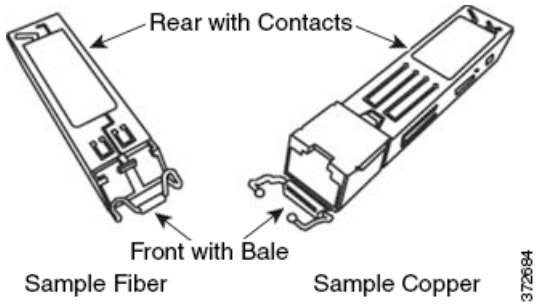
3D71x5 および AMP7150 SFP のソケット

8 つの SFP ソケットには、垂直パターンで 5 から 12 までの番号が付けられ、中央を基準とした配置（上の段は上向き、下の段は下向き）になっています。



ソケットの左側に付属する LED には、各インターフェイスのアクティビティとリンクに関する情報が表示されます。詳細については、「表 6-473D7115、3D7125、および AMP7150 SFP ソケット アクティビティ /リンク LED」（P.6-32）を参照してください。

サンプルの SFP トランシーバ



3D71x5 および AMP7150 は、以下の 3 つの形式を任意に組み合わせた、最大 8 つの SFP トランシーバをサポートできます。

- SFP-C-1: 銅線のトランシーバ
- SFP-F-1-SR: ショート レンジの光ファイバのトランシーバ
- SFP-F-1-LR: ロング レンジの光ファイバのトランシーバ

3D71x5 と AMP7150 では、シスコ SFP トランシーバだけを使用してください。非 シスコ の SFP トランシーバは、ソケット内で機能しなくなることがあり、トランシーバ、シャーシ、またはその両方に永続的な損害を与える可能性があります。

デバイスが機能している間は、トランシーバを取り付けたり取り外したりすることができます。設定の変更を確認するには、防御センターのユーザ インターフェイスを更新します。

SFP トランシーバにバイパス機能はありません。これらのトランシーバは、デバイスに障害が発生したり電源が切断された場合にデバイスがすべてのトラフィックを停止する必要がある、パッシブ配置やインライン配置で使用します（たとえば、仮想スイッチ、仮想ルータ、一部のアクセス制御ポリシーなど）。

パッシブ展開の場合、最大 8 つのソケットで任意の組み合わせのトランシーバを使用することにより、最大 8 つのネットワーク セグメントをモニタできます。インライン展開の場合、垂直方向に連続するソケット（5 と 6、7 と 8、9 と 10、または 11 と 12）でトランシーバの任意の組み合わせ（銅線、光ファイバ、または混合）を使用して、最大 4 つのネットワーク セグメントをモニタできます。

デバイスを管理する防御センターを使用して、トランシーバのポートを設定します。

SFP トランシーバの取り付け

トランシーバを取り付ける際には、適切な静電放電（ESD）の手順に従ってください。背面の接続部品に触れることは避け、接続部品やポートにほこりや汚れが付かないようにします。

注意　トランシーバをソケットに無理に押し込むことは、トランシーバが機能しなくなり、トランシーバ、シャーシ、またはその両方に永続的な損害を与える可能性があるため、行わないでください。

SFP トランシーバを取り付ける方法は、以下のとおりです。

ステップ 1　背面の接続部品に触れないように注意しながら、ベールの両端を指で持ち、トランシーバの背面をスライドさせてシャーシのソケットに入れます。上の段のソケットは上向きになり、下の段のソケットは下向きになることに注意してください。

ステップ 2　ベールをトランシーバに対して慎重に押し込み、ベールを閉じてロック機能を作動させ、トランシーバを固定します。

ステップ 3　「FireSIGHT システム アプライアンスの設置」（P.3-1）の手順に従って、トランシーバのポートを構成します。

現在稼動中のデバイスにトランシーバを取り付ける場合、変更を確認するには、防御センターのユーザ インターフェイスを更新する必要があることに注意してください。

SFP トランシーバの取り外し

トランシーバを取り外す際には、適切な静電放電（ESD）の手順に従ってください。背面の接続部品に触れることは避け、接続部品やポートにほこりや汚れが付かないようにします。

SFP トランシーバを取り外す方法：

ステップ 1　デバイスから取り外すトランシーバからすべてのケーブルを取り外します。

ステップ 2　指でトランシーバのベールをシャーシから慎重に引き出し、接続機能を解除します。

上の段のトランシーバは引き下げます。下の段のトランシーバは持ち上げます。

ステップ 3　指でベールの両端を持ち、トランシーバの背面の接続部品に触れないように注意しながら、ベールを取っ手にしてトランシーバをシャーシから慎重に引き出します。

8000 シリーズ モジュールの取り付けと取り外し

8000 シリーズ アプライアンスでは、モジュラの配置を柔軟に行うことができます。以下の操作を行うには、この項の手順を実行します。

- アプライアンスに新しいモジュールを取り付ける
- アプライアンスに取り付けられているモジュールを取り外したり交換したりする

以下の項では、8000 シリーズ モジュールの取り付け、取り外し、または交換のための方法を説明します。

8000 シリーズ アプライアンスのモジュール スロット

8000 シリーズ アプライアンスは、次のスロットのモジュールを使用できます。

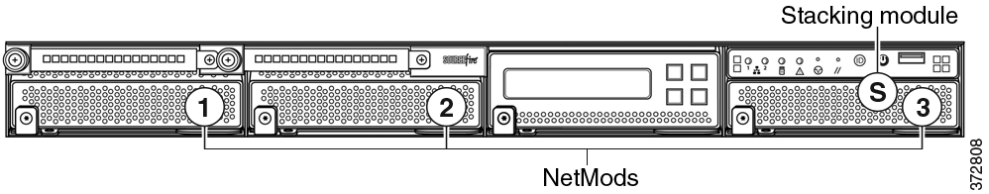
アプライアンスにモジュールを取り付けた後、以下のセクションを参照して、モジュールの詳細な使用方法を確認してください。

- センシング インターフェイスの設定方法について詳しくは、「センシング インターフェイスの識別」（P.3-4）を参照してください。
- スタック モジュールの使用方法について詳しくは、「スタック構成でのデバイスの使用」（P.3-15）を参照してください。

81xx ファミリ

81xx ファミリ アプライアンスは、次のスロットのモジュールを使用できます。

図 C-1　　81xx ファミリのプライマリ デバイス



スタック構成に関する考慮事項

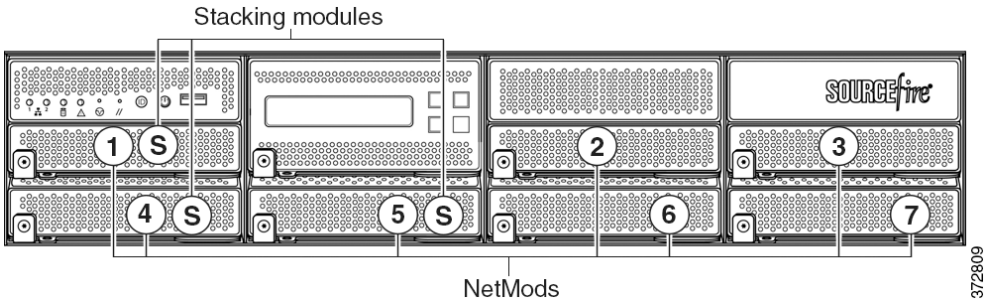
スタック デバイスについては、以下のようにモジュールを構成します。

- プライマリ デバイスだけにネットワーク モジュール（NetMod）を取り付けます。
- プライマリ デバイスに 1 つのスタック モジュール、およびセカンダリ デバイスに 1 つのスタック モジュールを取り付けます。

82xx ファミリおよび 83xx ファミリ

82xx ファミリと83xx ファミリのアプライアンスは、以下のスロットでモジュールを使用できます。

図 C-2　　82xx ファミリと83xx ファミリのプライマリ デバイス

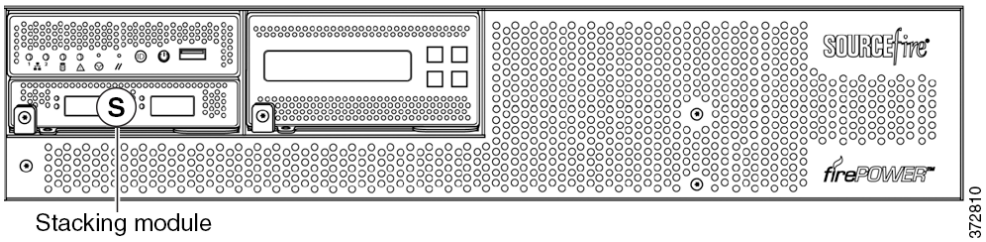


スタック構成に関する考慮事項

スタック デバイスについては、以下のようにモジュールを構成します。

- プライマリ デバイスだけにネットワーク モジュール（NetMod）を取り付けます。
- スタックされたセカンダリ デバイスごとに 1 つのスタック モジュールをプライマリ デバイスに取り付け、各セカンダリ デバイスに 1 つのスタック モジュールを取り付けます。

図 C-3　　82xx ファミリと83xx ファミリのセカンダリ デバイス



同梱品目

モジュール アセンブリ キットには、T8 トルクス ドライバ、および以下の 1 つ以上のモジュールが含まれています。

- クワッドポート 1000BASE-T の銅線の設定可能なバイパス NetMod。詳細については、「クワッドポート 1000BASE-T（銅線）設定可能バイパス NetMod」（P.6-47）を参照してください。
- クワッドポート 1000BASE-SX の光ファイバの設定可能なバイパス NetMod。詳細については、「クワッドポート 1000BASE-SX（光ファイバ）設定可能バイパス NetMod」（P.6-47）を参照してください。
- デュアルポート 10GBASE（MMSR または SMLR）の光ファイバの設定可能なバイパス NetMod。詳細については、「デュアルポート 10GBASE（MMSR または SMLR）光ファイバの設定可能バイパス NetMod」（P.6-49）を参照してください。
- デュアルポート 40GBASE-SR4 の光ファイバの設定可能なバイパス NetMod。詳細については、「デュアルポート 40GBASE-SR4（光ファイバ）設定可能バイパス NetMod」（P.6-50）を参照してください。

（注） このデュアルスロット NetMod は、40G 容量の 3D8250 または 3D8350 でのみ使用します。アプライアンスをアップグレードする必要がある場合は、『*Cisco 8000 Series Device 40G Capacity Upgrade Guide*』を参照してください。

- クワッドポート 1000BASE-T の銅線接続の非バイパス NetMod。詳細については、「クワッドポート 1000BASE-T（銅線）非バイパス NetMod」（P.6-52）を参照してください。
- クワッドポート 1000BASE-SX の光ファイバ接続の非バイパス NetMod。クワッドポート 1000BASE-SX の光ファイバ接続の非バイパス NetMod。詳細については、「クワッドポート 1000BASE-SX（光ファイバ）の非バイパス NetMod」（P.6-52）を参照してください。
- クワッドポート 10GBASE（MMSR または SMLR）の光ファイバ接続の非バイパス NetMod。詳細については、「クワッドポート 10GBASE（MMSR または SMLR）光ファイバ非バイパス NetMod」（P.6-53）を参照してください。

注意 クワッドポート 10GBASE の光ファイバ接続の非バイパス NetMod には、取り外しのできない Small Form-factor Pluggable（SFP）トランシーバが含まれています。SFP を取り外そうとすると、モジュールが破損する可能性があります。

- スタック モジュール。詳細については、「スタック モジュール」（P.6-55）を参照してください。

アプライアンス上の互換性がないスロットに NetMod を取り付ける場合、または NetMod が他の点でシステムと互換性がない場合は、NetMod を設定しようとすると、管理している防御センターの Web インターフェイスにエラーまたは警告メッセージが表示されます。支援が必要な場合は、サポートに連絡してください。

（注） NetMod を交換すると、完全に設定済みの韓国認証（KCC マーク）アプライアンスの設定が変更されることがあります。詳しくは、アプライアンスの元のコンフィギュレーション マニュアル、および『*Regulatory Compliance and Safety Information for FirePOWER and FireSIGHT Appliances*』マニュアルを参照してください。

モジュール パーツの特定

すべてのモジュールには、モジュールのセンシング インターフェイス、速度、サイズに関係なく、同じパーツが含まれています。

図 C-4　　モジュールまたはスロット カバーの例（開いている状態）

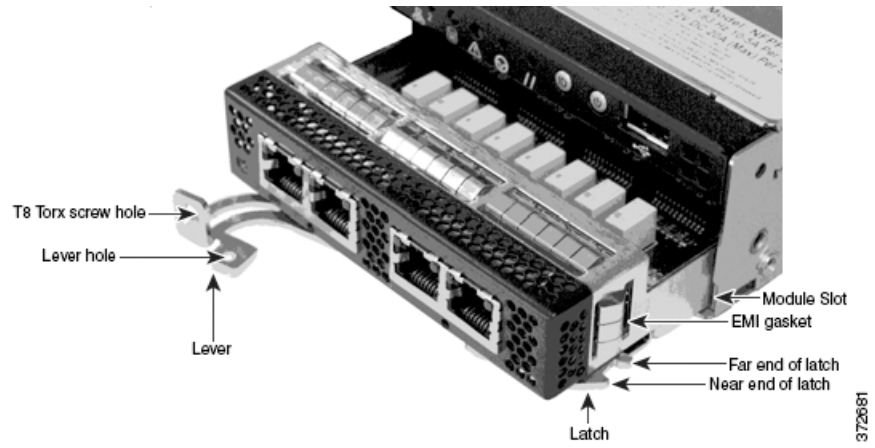
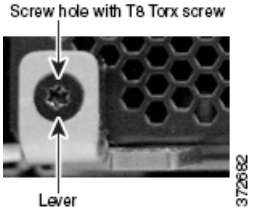


図 C-5　　モジュール レバーの例（閉じられてネジで固定されている状態）



はじめる前に

以下のガイドラインを参考にして、モジュールの取り付けまたは取り外しの準備をしてください。

- すべてのアプライアンスおよびモジュールを確認します。
- NetMod を取り付けるスロットを特定します。

ヒント　NetMod は、利用可能な互換性のあるすべてのスロットに挿入できます。

- スタック モジュールに適切なスロットを特定します。「スタック構成でのデバイスの使用」（P.3-15）を参照してください。
- 3D8140：スロット 3
- 3D8250、3D8260 および 3D8350、3D8360 プライマリ スロット：スロット 5
- 3D8270 および 3D8370 プライマリ スロット：スロット 5 および 1
- 3D8290 および 3D8390 プライマリ スロット：スロット 5、1、および 4
- 3D82xx および 3D83xx セカンダリ：スロット S
- EMI ガスケットが設置されていることを確認します。
- アプライアンスからすべての電源コードのプラグを抜きます。

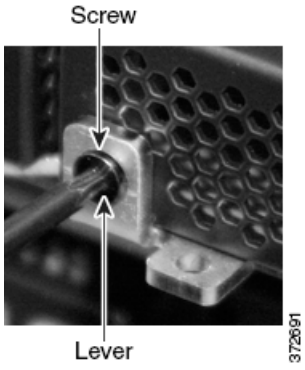
注意　モジュールはホットスワップ**できません**。モジュールを取り付けるまたは取り外す前に、電源を切り、アプライアンスから**すべての**電源コードのプラグを抜く必要があります。

モジュールまたはスロット カバーの取り外し

モジュールを取り扱う際には、リスト ストラップの着用や静電気防止用の作業台の使用など、適切な静電気防止（ESD）の推奨事項に従ってください。未使用のモジュールは、損傷を防ぐために静電気防止用の袋またはボックスに入れて保管します。

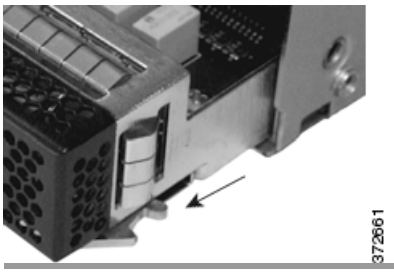
モジュールやスロット カバーを取り外す方法は、次のとおりです。

ステップ 1　付属のドライバを使用して、モジュールのレバーから T8 トルクス ネジを取り外して保管しておきます。



ステップ 2　モジュールからレバーを引き出して、ラッチを解放します。

ステップ 3　モジュールをスロットから取り出します。

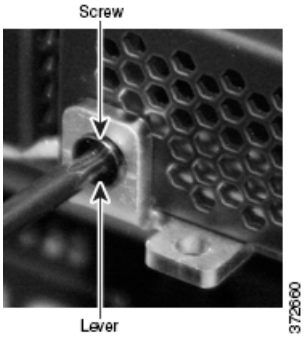


モジュールまたはスロット カバーの取り付け

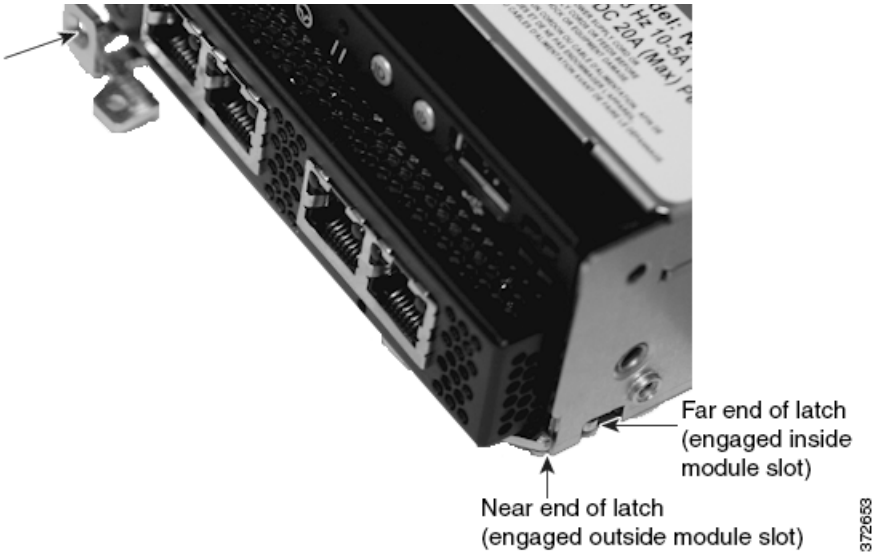
既存のモジュールやスロット カバーを取り外して、新しいモジュール用のスロットを準備します。詳細については、「モジュールまたはスロット カバーの取り外し」（P.C-5）を参照してください。

モジュールやスロット カバーを取り付ける方法は、次のとおりです。

ステップ 1　付属のドライバを使用して、モジュールのレバーから T8 トルクス ネジを取り外して保管しておきます。

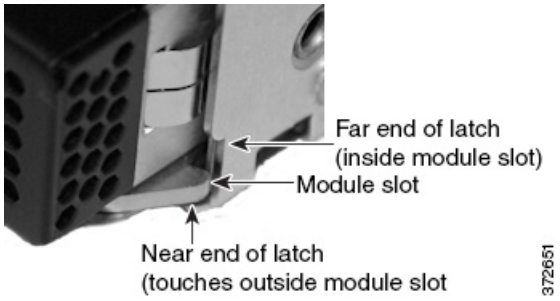


ステップ 2　モジュールからレバーを引き出して、ラッチを開きます。ラッチの手前の端は見えています。ラッチの奥の端はモジュール内にあります。

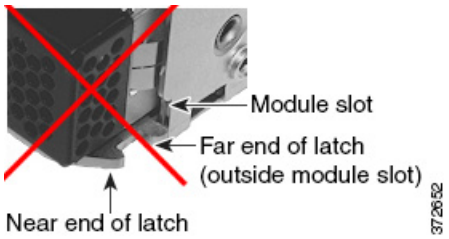


ステップ 3　ラッチの奥の端がスロット内に入り、ラッチの近端がモジュール スロットの外側に接触するまで、モジュールをスロットに挿入します。

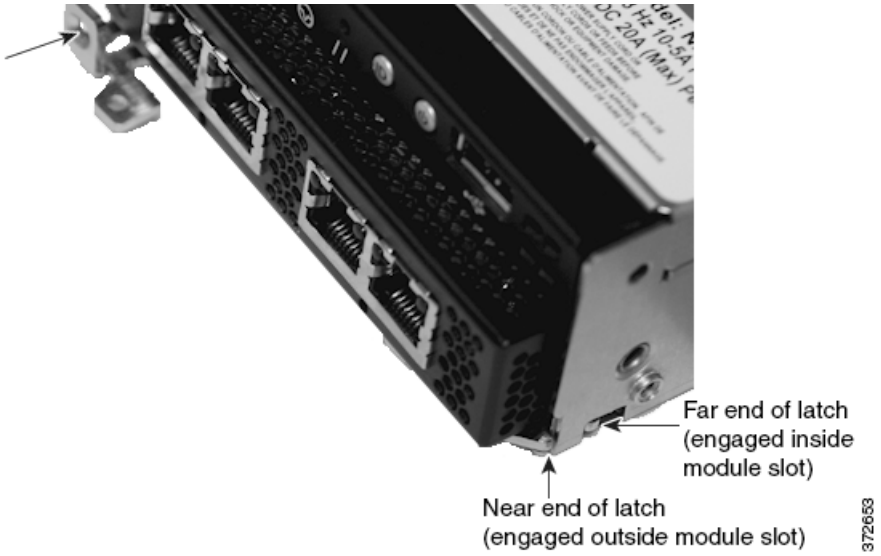
正しいモジュールの位置



正しくないモジュールの位置

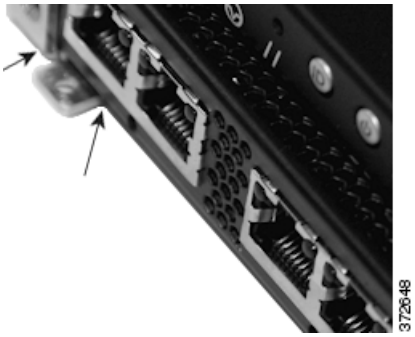


ステップ 4　レバーをモジュールに向けて押し、ラッチが連動して、モジュールがスロット内に挿入されるようにします。

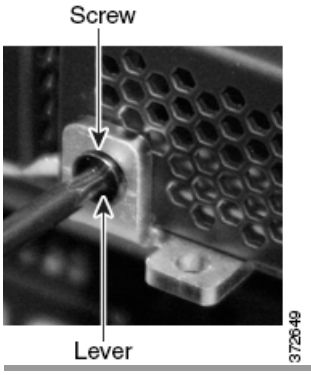


注意　力を**入れすぎない**ようにしてください。ラッチが連動しない場合は、モジュールを取り外して位置を再調整してから再試行します。

ステップ 5　ネジ穴にしっかりと押し込んで、レバーをモジュールに十分に押し付け、ラッチを固定します。レバーがモジュールにしっかりと向き合い、モジュールがシャーシと揃うようにします。



ステップ 6　保管しておいた T8 トルクス ネジをレバーに挿入して締め付けます。



ハード ドライブのスクラビング

ほとんどの防御センターと管理対象デバイスのハード ドライブを安全にスクラビングして、その内容にアクセスできないようにすることができます。たとえば、機密データを含む故障したアプライアンスを返送する必要がある場合は、この機能を使用してデータを上書きできます。

ハード ドライブの内容のスクラビング

サポートされるデバイス：すべて

サポートされる防御センター：DC1000 と DC3000 を除くすべて

このモードでのディスクのスクラビングは、米国国防総省による以下の規格を満たしています。

規格

DoD のスクラビング シーケンスは、リムーバルおよび非リムーバルのリジッド ディスクのサニタイズについて DoD 5220.22-M に準拠しています。この手順では、アドレス指定可能なすべての領域をある文字で上書きしてから、その補数で上書きし、さらにランダムな文字で上書きし、検証します。その他の制約事項については、DoD のマニュアルを参照してください。

注意 ハード ドライブをスクラビングすると、アプライアンス上の**すべての**データが消失して、アプライアンスは操作不能になります。

ハード ドライブのスクラビングは、「対話型メニューを使用するアプライアンスの復元」（P.7-9）で説明されているインタラクティブ メニューのオプションを使用して行います。

ハード ドライブをスクラビングする方法：

アクセス：Admin

ステップ 1 アプライアンスにアクセスしている方法に応じて、以下のいずれかのセクションにある指示に従い、復元ユーティリティのインタラクティブ メニューを表示します。

- 「KVM または物理シリアル ポートを使用する復元ユーティリティの起動」（P.7-6）
- 「Lights-Out Management を使用する復元ユーティリティの開始」（P.7-7）

DC1000 および DC3000 では、この機能がサポートされていないことに注意してください。

ステップ 2 メイン メニューで、[8 Wipe Contents of Disk] を選択します。

ステップ 3　プロンプトが表示されたら、ハード ドライブのスクラビングを実行することを確認します。

ハード ドライブがスクラビングされます。スクラブ プロセスは、完了までに数時間かかる場合があります。大容量ドライブにはより多くの時間がかかります。

FireSIGHT システム アプライアンスの事前設定

ステージング ロケーション（複数のアプライアンスを事前設定またはステージングするための中央の場所）で、ターゲット ロケーション（ステージング ロケーション以外の任意のロケーション）に展開するアプライアンス（防御センターまたはデバイス）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してターゲット ロケーションに展開するには、以下の手順に従います。

- ステージング ロケーションのデバイスにシステムをインストールします。
- オプションで、デバイスを防御センターに登録します。
- オプションで、管理防御センターからデバイスに更新をプッシュします。
- オプションで、防御センターからデバイスの登録を解除します。
- シャット ダウンして、ターゲット ロケーションにアプライアンスを発送します。
- ターゲット ロケーションにアプライアンスを展開します。

詳細については、次の項を参照してください。

- 「はじめる前に」（P.E-2）
- 「システムのインストール」（P.E-3）
- 「デバイスの登録」（P.E-4）
- 「アプライアンスの発送の準備」（P.E-4）
- 「アプライアンスの事前設定のトラブルシューティング」（P.E-7）

ヒント 梱包材はすべて保管しておき、アプライアンスを再梱包する際にすべての参考資料と電源コードを含めるようにします。

はじめる前に

アプライアンスを事前設定する前に、ステージング ロケーションとターゲット ロケーションのネットワーク設定情報、ライセンス情報、その他の関連情報を収集します。

ヒント　ステージング ロケーションとターゲット ロケーションのこの情報を管理するためのスプレッドシートを作成すると便利でしょう。

初期設定の際は、アプライアンスをネットワークに接続してシステムをインストールするための十分な情報を使用して、アプライアンスを設定します。オプションで、デバイスを防御センターに接続し、防御センターからデバイスに更新をプッシュすることができます。初期設定のために必要ではなくても、事前設定に役立つ可能性のある機能が他にあればそれらもイネーブルにすることができます。詳細については、次の項を参照してください。

- 「必須の事前設定の情報」（P.E-2）
- 「オプションの事前設定情報」（P.E-2）
- 「時間管理の事前設定」（P.E-3）

必須の事前設定の情報

アプライアンスを事前設定するには、最低でも以下の情報が必要です。

- 新しいパスワード（初期設定にはパスワードの変更が必要）
- アプライアンスのホスト名
- アプライアンスのドメイン名
- アプライアンスの IP 管理アドレス
- ターゲット ロケーションでのアプライアンスのネットワーク マスク
- ターゲット ロケーションでのアプライアンスのデフォルト ゲートウェイ
- ステージング ロケーション（またはアクセス可能な場合にはターゲット ロケーション）での DNS サーバの IP アドレス
- ステージング ロケーション（またはアクセス可能な場合にはターゲット ロケーション）での NTP サーバの IP アドレス
- ターゲット ロケーションの検出モード

オプションの事前設定情報

次のように、一部のデフォルト設定を変更することができます。

- デバイス（シリーズ 3 の管理対象デバイスのみ）を設定するために LCD パネルにアクセスすることを許可する
- 手動でアプライアンスの時間を設定する場合に、時間帯を設定する。
- 自動バックアップのためのリモート ストレージの場所を設定する
- デバイスの LOM をイネーブルにするために、シリーズ 3 デバイスの Lights-Out 管理（LOM）の IP アドレスを設定する

デバイスを防御センターに登録する場合は、以下の情報が必要になります。

- 管理対象デバイスの名前または IP アドレス
- 管理ホスト名（防御センター）
- 登録キー（最大 37 文字の個人的に作成された固有な英数字のキー）

時間管理の事前設定

次の考慮事項に注意します。

- シスコは、物理的な NTP サーバと時刻を同期することを推奨します。仮想防御センターに管理対象デバイスを同期しないでください。仮想アプライアンスでのパフォーマンス最適化は、リアルタイム クロックに影響を与える場合があります。
- ステージング ロケーションのネットワークがターゲット ロケーションの DNS サーバおよび NTP サーバにアクセスできる場合は、ターゲット ロケーションの DNS サーバおよび NTP サーバの IP アドレスを使用します。そうでない場合は、ステージング ロケーションの情報を使用して、ターゲット ロケーションでリセットします。
- NTP を使用する代わりに、アプライアンスの時刻を手動に設定した場合は、ターゲットの展開のタイムゾーンを使用します。「時刻の設定」（P.4-10）を参照してください。

システムのインストール

「FireSIGHT システム アプライアンスの設置」（P.3-1）および「FireSIGHT システム アプライアンスのセットアップ」（P.4-1）にあるインストール手順を使用します。システムを事前設定する際には、以下に注意してください。

- シリーズ 3 デバイスでは、LCD パネルを使用してデバイスのネットワーク設定にアクセスすることを許可すると、デバイスに物理的にアクセスすることによって不正な変更を行うことができる、というセキュリティ リスクが発生します。「シリーズ 3 デバイスの LCD パネルの設定」（P.4-10）を参照してください。
- ターゲット展開で、防御センターのホスト名または IP アドレスを使用してデバイスを事前登録します。後に登録を完了するときのために、登録キーを記録しておいてください。「リモート管理」（P.4-10）を参照してください。
- デフォルトの検出モードを変更する場合は、ターゲットの展開の担当者に通知してください。検出モードとは異なる方法でインターフェイスを設定すると、システムが正しくインターフェイスを割り当てなくなることがあります。「検出モード」（P.4-11）を参照してください。
- デバイス用に Network Address Translation（NAT）を設定する必要がある場合は、デバイスの CLI（シリーズ 3 デバイスの場合のみ）または管理防御センターの Web インターフェイスを使用してデバイスを登録する際に、デバイスの NAT ID を指定します。「CLI を使用して シリーズ 3 デバイスを防御センターに登録する」（P.4-7）および『*FireSIGHT System User Guide*』の「NAT 環境での作業」を参照してください。
- 初期設定時にライセンスを追加します。その時点でライセンスを追加しない場合は、初期設定時に登録するすべてのデバイスがライセンスなしで防御センターに追加されます。初期設定プロセスの完了後に、それらに個別にライセンスを付与する必要があります。「ライセンスの設定」（P.4-15）を参照してください。

デバイスの登録

防御センターでデバイスのソフトウェア バージョン以上のソフトウェア バージョンを実行している場合は、デバイスを防御センターに登録して、ポリシーや更新を管理対象デバイスにプッシュできます。

（注） 防御センターとその管理対象デバイスを、異なるターゲット ロケーションに展開する場合は、そのデバイスを防御センターから削除した後で、アプライアンスをシャット ダウンする必要があります。「防御センターからのデバイスの削除」（P.E-5）を参照してください。

デバイスを防御センターに登録する方法：

ステップ 1　デバイスで、ターゲットの展開の防御センターのホスト名または IP アドレスを使用して、リモート管理を設定します。後に登録を完了する際に使用できるように、登録キーを記録しておいてください。「リモート管理」（P.4-10）を参照してください。

（注） デバイスを防御センターに登録するには、その前に、デバイスにリモート管理を設定する必要があります。

ステップ 2　防御センターで、リモート管理設定の登録情報を使用してデバイスを登録します。「デバイス登録」（P.4-16）を参照してください。

アプライアンスの発送の準備

アプライアンスの発送の準備をするには、安全に電源を切って、アプライアンスを再梱包する必要があります。

- ターゲット ロケーションで防御センターと管理対象デバイスが同じ設定で使用されない場合は、防御センターからデバイスを削除してから、電源を切ってアプライアンスを再梱包する必要があります。「防御センターからのデバイスの削除」（P.E-5）を参照してください。
- 安全にアプライアンスの電源を切る方法については、「アプライアンスの電源を切る」（P.E-6）を参照してください。
- アプライアンスの発送のための準備を安全に行うために、「発送に関する考慮事項」（P.E-6）を参照してください。

防御センターからのデバイスの削除

防御センターと管理対象デバイスを同じターゲット ロケーションに展開しない場合は、防御センターからデバイスを削除する必要があります。こうすることで、ターゲット ロケーションでデバイスを異なる防御センターに登録するとき、そのデバイスが元の防御センターの UUID を探そうとすることはなくなります。

デバイスを防御センターから削除する方法：

ステップ 1　防御センターで、[Devices] > [Device Management] と選択します。

[Device Management] ページが表示されます。

ステップ 2　除去するデバイスの横にある削除アイコン（ ）をクリックします。

プロンプトが出されたら、デバイスを削除することを確認します。デバイスと防御センターの間の通信が切断されて、デバイスが [Device Management] ページから削除されます。デバイスに、防御センターから NTP 経由で時刻を受信させるシステム ポリシーがある場合、デバイスはローカルの時間管理に戻ります。

デバイスを防御センターから削除した後に、デバイスが防御センターによってリモート管理されていないことを確認してください。

デバイスが防御センターによって管理されていないことを確認する方法：

ステップ 1　管理対象デバイスで、Web インターフェイスまたは CLI を使用して、以下のいずれかを行います。

- 管理対象デバイスの Web インターフェイスで、[System] > [Local] > [Registration] > [Remote Management] に移動し、[Remote Management] 画面のホスト リストが空であることを確認します。
- 管理対象デバイスの CLI で、コマンド `show manager` を実行し、ホストが表示されないことを確認します。

防御センターからのライセンスの削除

何らかの理由でライセンスを削除する必要がある場合は、次の手順に従います。シスコ は防御センターの固有のライセンス キーに基づいてライセンスを生成するため、ある防御センターから削除したライセンスを別の防御センターで再利用することはできないことに注意してください。詳しくは、『*FireSIGHT System User Guide*』の「FireSIGHT システム のライセンス」を参照してください。

ライセンスを削除する方法：

ステップ 1　[Systems] > [Licenses] を選択します。

[License] ページが表示されます。

ステップ 2　削除するライセンスの横にある削除アイコン（ ）をクリックします。

ライセンスを削除すると、そのライセンスを使用するすべてのデバイスからライセンス機能が削除されます。たとえば、有効な保護のライセンスが 100 台の管理対象デバイスに対してイネーブルになっている場合、そのライセンスを削除すると、100 台のデバイスすべてから保護機能が削除されます。

ステップ 3　ライセンスを削除することを確認します。

ライセンスが削除されます。

アプライアンスの電源を切る

電源を抜く前に、アプライアンスの電源を安全に切るには、次の手順に従います。

防御センターの電源を切る方法：

ステップ 1　防御センターのコマンド ラインに以下を入力します。

```
sudo shutdown -h now
```

防御センターが安全にシャット ダウンします。

管理対象デバイスの電源を切る方法：

ステップ 1　デバイスのコマンド ラインに以下を入力します。

```
system shutdown
```

デバイスが安全にシャット ダウンします。

発送に関する考慮事項

ターゲット ロケーションにアプライアンスを発送する準備を行うには、安全に電源を切って、アプライアンスを再梱包する必要があります。次の考慮事項に注意します。

- 元の梱包材を使用してアプライアンスを再梱包します。
- アプライアンスと共にすべての参考資料と電源コードを含めます。
- 不適切な取り扱いや過度の負荷により損傷することがないよう NetMod および SFP を保護します。
- ターゲット ロケーションに、新しいパスワードや検出モードといったすべての設定情報を提供します。

アプライアンスの事前設定のトラブルシューティング

アプライアンスがターゲットでの配布用に適切に設定されている場合、そのアプライアンスは追加の設定なしでインストールして配布できます。

アプライアンスへのログインに問題がある場合、事前設定にエラーがある可能性があります。次のトラブルシューティング手順を試行してください。

- すべての電源ケーブルや通信ケーブルがアプライアンスに正しく接続されていることを確認します。
- アプライアンスの現在のパスワードを知っていることを確認します。ステージング ロケーションでの初期設定の際、パスワードの変更を求めるプロンプトが出されます。新しいパスワードについては、ステージング ロケーションから提供された設定情報を参照してください。
- ネットワーク設定が正しいことを確認します。「初期セットアップ ページ：デバイス」（P.4-8）および「初期セットアップ ページ：防御センター」（P.4-12）を参照してください。
- 正しい通信ポートが適切に機能していることを確認します。ファイアウォール ポートの管理方法については、ファイアウォールのマニュアルを参照してください。必須のオープン ポートについては、「通信ポートの要件」（P.1-20）を参照してください。
- 展開でネットワーク アドレス変換（NAT）のアプライアンスを使用する場合は、NAT が正しく設定されていることを確認してください。『*FireSIGHT System User Guide*』の「NAT 環境での作業」を参照してください。

問題が引き続き発生する場合は、IT 部門に連絡してください。

用 語 集

7000 シリーズ

シリーズ 3 FirePOWER 管理対象デバイスのグループ。このシリーズのデバイスには、70xx ファミリ（3D7010、3D7020、3D7030 モデル）と 71xx ファミリ（3D7110、3D7115、3D7120、3D7125、AMP7150 モデル）が含まれます。

8000 シリーズ

シリーズ 3 FirePOWER 管理対象デバイスのグループ。このシリーズのデバイスには、81xx ファミリ（3D8120、3D8130、3D8140、AMP8150 モデル）、82xx ファミリ（3D8250、3D8260、3D8270、3D8290 モデル）、および 83xx ファミリ（3D8350、3D8360、3D8370、3D8390 モデル）が含まれます。8000 シリーズ デバイスは、一般的に、7000 シリーズ デバイスより強力です。

ASA FirePOWER

Cisco ASA with FirePOWER Services の省略名。

Cisco ASA with FirePOWER Services

Cisco Adaptive Security Appliance（ASA）管理対象デバイスのグループ。このシリーズのデバイスには、ASA5512-X、ASA5515-X、ASA5525-X、ASA5545-X、ASA5555-X、ASA5585-X-SSP-10、ASA5585-X-SSP-20、ASA5585-X-SSP-40、および ASA5585-X-SSP-60 の各モデルが含まれます。

CLI

コマンドライン インターフェイスを参照してください。

Context Explorer

侵入、接続、ファイル、ジオロケーション、マルウェア、およびディスカバリ ポリシーを使用して、モニタ対象ネットワークに関する詳細でインタラクティブなグラフィカル情報を表示するページ。それぞれのセクションに、詳細なリストを伴う、鮮明な折れ線グラフ、棒グラフ、円グラフ、およびドーナツ グラフの形式で情報が表示されます。分析を微調整するためのカスタム フィルタの作成と適用を容易に行うことができ、また、グラフ領域をクリックするか、その上にマウス カーソルを移動することにより、データ セクションをより詳細に調査できます。高度にカスタマイズ可能で、区分化され、リアルタイムで更新されるダッシュボードに比べて、Context Explorer は、手動で更新され、そのデータの広範なコンテキストを提供するように設計され、アクティブ ユーザ調査用に設計された単一の一貫性のあるレイアウトで構成されています。

Control ライセンス

ユーザとアプリケーションの条件をアクセス コントロール ルールに追加することによって、ユーザ制御とアプリケーション制御の実装を可能にするライセンス。また、スイッチングとルーティング（DHCP リレーと NAT を含む）を実行するように管理対象デバイスを設定したり、管理対象デバイスのクラスタリングを設定したりすることもできます。

eStreamer

イベント データを防御センターまたは管理対象デバイスから外部のクライアント アプリケーションにストリーム配信するための FireSIGHT システム コンポーネント。

Event Streamer

eStreamer を参照してください。

FireAMP Connector

サブスクリプション ベースの FireAMP 展開内のユーザがコンピュータやモバイル デバイスなどのエンドポイント上にインストールする軽量エージェント。このコネクタは、シスコ クラウドと通信しながら、組織全体のマルウェアをすばやく特定して検疫するための情報を交換します。

FireAMP サブスクリプション

組織で FireAMP を高度なマルウェア対策（AMP）ソリューションとして使用するための別途購入されるサブスクリプション。管理対象デバイスでネットワークベースの AMP を実行するためのマルウェア ライセンスと比較してください。

FireAMP ポータル

組織のサブスクリプション ベースの FireAMP 展開を設定するための Web サイト（http://amp.sourcefire.com/）。

FireAMP

マルウェアの発生、持続的脅威、および標的型攻撃を検出、把握、およびブロックするシスコのエンタープライズクラスでエンドポイント ベースの高度なマルウェア分析および保護ソリューション。組織で FireAMP サブスクリプションが使用されている場合は、個別のユーザがエンドポイント（コンピュータ、モバイル デバイス）上で軽量の FireAMP Connector をインストールしてから、シスコ クラウドと通信します。これにより、マルウェアをすばやく特定して検疫するだけでなく、それらの発生を検出して、それらのトラジェクトリを追跡し、それらの影響を把握して、効果的な回復方法を習得することができます。FireAMP ポータルは、カスタム保護を構築したり、特定のアプリケーションの実行をブロックしたり、カスタム ホワイトリストを作成したりするためにも使用できます。ネットワークベースの高度なマルウェア対策と比較してください。

FireSIGHT ライセンス

ユーザが、ホスト、アプリケーション、およびユーザ検出を実行するための 防御センター 上のデフォルト ライセンス。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用してモニタ可能な個別のホストとユーザの数だけでなく、アクセス コントロール ルールでユーザ制御を実行するために使用可能なアクセス制御ユーザの数も決定します。

GeoDB

ジオロケーション データベースを参照してください。

LDAP 認証

Lightweight Directory Access Protocol（LDAP）ディレクトリ サーバに保存された LDAP ディレクトリと比較することによって、ユーザ クレデンシャルを確認する外部認証の形式。

Lights-Out Management（LOM）

アウトオブバンド Serial over LAN（SoL）管理接続を使用して、アプライアンスの Web インターフェイスにログインせずに、アプライアンスをリモートでモニタまたは管理可能なシリーズ 3 の機能。シャーシのシリアル番号の表示やファンの速度や温度などの状態のモニタなど、限られたタスクを実行できます。

NAT ポリシー

NAT によるルーティングを実行するための NAT ルールを使用するポリシー。

NAT

ネットワーク アドレス変換。プライベート ネットワーク上の複数のホスト間で単一のインターネット接続を共有するために最もよく使用される機能。ディスカバリを使用すれば、システムはネットワーク デバイスを論理インターフェイスとして識別できます。加えて、FireSIGHT システムのレイヤ 3 展開では、NAT ポリシーを使用して NAT によるルーティングを設定できます。

NetMod

管理対象デバイス用のセンシング インターフェイスを含むそのデバイスのシャーシ内に設置するモジュール。

Protection ライセンス

侵入検知および防御、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するためのシリーズ 3 とバーチャル デバイス用のライセンス。ライセンスがない場合は、シリーズ 2 デバイスがセキュリティ インテリジェンスを除く Protection 機能を自動的に使用します。

RADIUS 認証

Remote Authentication Dial In User Service。ネットワーク リソースへのユーザ アクセスの認証、許可、およびアカウンティングのために使用されるサービス。FireSIGHT システム ユーザが RADIUS サーバ経由で認証できるようにするための外部認証オブジェクトを作成できます。

SFP モジュール

71xx ファミリ デバイス上のネットワーク モジュールに挿入された Small Form-factor Pluggable トランシーバ。SFP モジュール上のセンシング インターフェイスは設定可能なバイパスを許可しません。

URL カテゴリ

マルウェアやソーシャル ネットワーキングなどの URL の一般的な分類。

URL フィルタリング ライセンス

URL カテゴリと URL レピュテーション情報に基づいて URL フィルタリングを実行可能なライセンス。URL フィルタリング ライセンスは期限切れになる場合があります。

URL フィルタリング

防御センターによってシスコ クラウドから取得された URL の URL カテゴリと URL レピュテーション情報と相関がある、モニタ対象ホストから要求された URL に基づいてネットワーク上を伝送可能なトラフィックを決定するアクセス コントロール ルールを作成するための機能。許可またはブロックする URL を個別にまたはグループで指定することによって、Web トラフィックに対するきめ細かなカスタム制御を実現することもできます。

UTC 時間

協定世界時。UTC はグリニッジ標準時（GMT）とも呼ばれ、世界中のあらゆる場所に共通の標準時間です。FireSIGHT システムは UTC を使用しますが、タイム ゾーン機能を使用して現地時刻を設定できます。

VDB

脆弱性データベースを参照してください。

VLAN

仮想ローカル エリア ネットワーク。VLAN は、地理的場所ではなく、部門や主な用途など、その他の基準でホストをマップします。モニタ対象ホストのホスト プロファイルには、そのホストに関連付けられたすべての VLAN 情報が表示されます。VLAN 情報は、イベントをトリガーしたパケット内の最も内側の VLAN タグとして、侵入イベントにも含まれています。侵入ポリシーとターゲット コンプライアンス ホワイト リストを VLAN でフィルタ処理することができます。レイヤ 2 展開とレイヤ 3 展開では、管理対象デバイス上の仮想スイッチと仮想ルータを VLAN タグ付きトラフィックを適切に処理するように設定できます。

VPN

シスコ 管理対象デバイス上の仮想ルータ間または管理対象デバイスからリモート デバイスや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 トンネルを構築するための機能。

VPN ライセンス

シスコ 管理対象デバイス上の仮想ルータ間または管理対象デバイスからリモート デバイスや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 トンネルを構築するためのライセンス。

VRT

シスコ VRT を参照してください。

Web アプリケーション

HTTP トラフィックの内容または HTTP トラフィックに対して要求された URL を表すアプリケーションの一種。

zone

セキュリティ ゾーンを参照してください。

アクセス コントロール ポリシー

管理対象デバイスでモニタするネットワーク トラフィックのアクセス制御を実行するためにそれらのデバイスに適用するポリシー。アクセス コントロール ポリシーには、複数のアクセス コントロール ルールを含めることができます。また、これらのルールの条件を満たさないトラフィックの処理とロギングを決定するデフォルト アクションも指定します。アクセス コントロール ポリシーは、HTTP 応答ページ、セキュリティ インテリジェンス、およびその他の詳細設定を指定することもできます。

アクセス コントロール ルール

FireSIGHT システム がモニタ対象ネットワーク トラフィックを検査するために使用し、きめ細かなアクセス制御を可能にするための一連の条件。アクセス コントロール ルールはアクセス コントロール ポリシーを設定し、単純な IP アドレス マッチングの実行、または複数のユーザ、アプリケーション、ポート、または URL が関係する複雑な接続の特性を決定することができます。アクセス コントロール ルール アクションによって、ルールの条件を満たすトラフィックをシステムがどのように処理するかが決定されます。その他のルール設定によって、接続をログに記録する方法（および記録するかどうか）と、一致するトラフィックを侵入ポリシーとファイル ポリシーのどちらで検査するかが決定されます。

アクセス リスト

システム ポリシーで設定された IP アドレスのリスト。アプライアンスにアクセス可能なホストを表します。デフォルトでは、すべての人がポート 443（HTTPS）を使用してアプライアンスの Web インターフェイスにアクセスし、ポート 22（SSH）を使用してコマンド ラインにアクセスすることができます。また、ポート 161 を使用して SNMP アクセスを追加することもできます。

アクセス制御

ネットワークを通過可能なトラフィックを指定、検査、およびログに記録するための FireSIGHT システム の機能。アクセス制御は、侵入検知および防御、ファイル制御、および高度なマルウェア対策の各機能を含み、ディスカバリ機能で検査可能なトラフィックも特定します。

アプライアンス

防御センターまたは管理対象デバイス。アプライアンスは物理にも仮想にもすることができます。

アプリケーション プロトコル

サーバとホスト上のクライアント アプリケーション間の通信中に検出されたアプリケーション プロトコル トラフィック（SSH や HTTP など）を表すアプリケーションの種類。

アプリケーション

検出済みのネットワーク アセット、通信手段、または HTTP コンテンツ。これに対するアクセス コントロール ルールを作成できます。システムは、アプリケーション プロトコル、クライアント アプリケーション、および Web アプリケーションという 3 種類のアプリケーションを検出します。

アプリケーション制御

アクセス制御の一部として、ネットワークを通過可能なアプリケーション トラフィックを指定するための機能。

アラート

システムが特定のイベントを生成したことを示す通知。アラートは、特定のアクセス コントロール ルールによってログに記録された侵入イベント（影響フラグを含む）、検出イベント、マルウェア イベント、相関ポリシー違反、ヘルス ステータスの変化、および接続に基づいて通知できます。アラートはほとんどの場合、電子メール、Syslog、または SNMP トラップ経由で通知できます。

イベント ビューア

イベントを表示して操作するためのシステム コンポーネント。イベント ビューアは、ワークフローを使用して、広範なイベント ビューを表示してから、興味のあるイベントだけを含む絞り込まれたイベント ビューを表示します。イベント ビューでは、ワークフローをドリルダウンしたり、検索を使用したりすることによって、イベントを制限できます。

イベント

イベント ビューアでワークフローを使用して表示可能な特定の出来事に関する詳細情報のコレクション。イベントは、ネットワークに対する攻撃、検出されたネットワーク アセットの変化、組織のセキュリティ ポリシーやネットワーク利用ポリシーの違反などを表すことができます。システムは、変わりやすいアプライアンスのヘルス ステータス、Web インターフェイスの使用状況、ルール更新、および起動された修復に関する情報を含むイベントも生成します。最後に、システムは、これらの「イベント」が特定の出来事を表していない場合でも、その他の特定の情報をイベントとして表示します。たとえば、イベント ビューアを使用して、検出されたホスト、アプリケーション、およびそれらの脆弱性に関する詳細情報を表示できます。

インポート

アプライアンス間でさまざまな設定を転送するために使用可能な手段。同じタイプの別のアプライアンスからエクスポートした設定をインポートすることができます。

インライン インターフェイス

インライン展開でトラフィックを処理するように設定されたセンシング インターフェイス。ペア内のインライン セットにインライン インターフェイスを追加する必要があります。

インライン セット

インライン インターフェイスの 1 つ以上のペア。

インライン展開

管理対象デバイスがネットワーク上にインラインで配置される FireSIGHT システム の展開。この設定では、デバイスがスイッチング、ルーティング、アクセス制御、および侵入検知および防御を使用してネットワーク トラフィック フローに影響を与える場合があります。

ウィジェット

ダッシュボード ウィジェットを参照してください。

エンドポイント

ユーザが組織の高度なマルウェア対策戦略の一部として FireAMP Connector をインストールするコンピュータまたはモバイル デバイス。

カスタム ユーザ ロール

特殊なアクセス権限を持つユーザ ロール。カスタム ユーザ ロールは、メニュー ベースのアクセス許可とシステム アクセス許可のセットを有し、完全にオリジナルにすることも、事前定義されたユーザ ロールに基づくこともできます。

仮想スイッチ

ネットワーク経由で着信トラフィックと発信トラフィックを処理するスイッチド インターフェイスのグループ。レイヤ 2 展開では、管理対象デバイス上に仮想スイッチを設定して、ネットワークを論理セグメントに分割しながらスタンドアロン ブロードキャスト ドメインとして動作させることができます。仮想スイッチは、ホストからの Media Access Control（MAC）アドレスを使用してパケットの送信先を決定します。

仮想防御センター

仮想ホスティング環境内の独自の設備に展開可能な防御センター。

仮想ルータ

レイヤ 3 トラフィックをルーティングするルーテッド インターフェイスのグループ。レイヤ 3 展開では、宛先 IP アドレスに基づいてパケット転送を決定することにより、パケットをルーティングするように仮想ルータを設定できます。静的ルートを定義したり、Routing Information Protocol（RIP）および Open Shortest Path First（OSPF）ダイナミック ルーティング プロトコルを設定したり、ネットワーク アドレス変換（NAT）を実装したりできます。

管理インターフェイス

FireSIGHT システム アプライアンスの管理に使用するネットワーク インターフェイス。ほとんどの展開において、管理インターフェイスは内部の保護されたネットワークに接続されます。センシング インターフェイスと比較してください。

管理対象デバイス

デバイスを参照してください。

クライアント アプリケーション

クライアントを参照してください。

クライアント

クライアント アプリケーションとも呼ばれる。あるホスト上で動作しながら、特定の処理を別のホスト（サーバ）に依存するアプリケーション。たとえば、電子メール クライアントを使用すれば、電子メールを送受信することができます。あるホスト上のユーザが特定のクライアントを使用して別のホストにアクセスしていることをシステムが検出すると、そのクライアントの名前とバージョン（入手可能な場合）を含む情報をホスト プロファイルとネットワーク マップで報告します。

クラスタリング

2 つのピア シリーズ 3 デバイスまたはスタック間のネットワーキング機能と構成データの冗長性を実現可能にする機能。クラスタリングは、ポリシー適用、システム更新、および登録のための単一の論理システムを提供します。冗長な防御センターを設定可能なハイ アベイラビリティと比較してください。

高度なマルウェア対策

略して AMP。FireSIGHT システムのネットワークベースのマルウェア検出機能とマルウェア クラウド検索機能。この機能を FireAMP サブスクリプションが必要なシスコのエンドポイント ベースの AMP ツールである FireAMP と比較してください。

コマンドライン インターフェイス

シリーズ 3 と仮想デバイス上の制限付きテキスト ベース インターフェイス。CLI ユーザが実行可能なコマンドは、そのユーザに割り当てられたアクセス レベルによって異なります。

コンテキスト メニュー

Web インターフェイス上のさまざまなページで利用可能なポップアップ メニュー。FireSIGHT システム の他の機能にアクセスするためのショートカットとして使用できます。メニューの内容は、表示しているページ、調査している特定のデータ、割り当てられたユーザ ロールなどさまざまな要素によって異なります。コンテキスト メニュー オプションには、侵入ルール、イベント、およびホスト情報へのリンク、さまざまな侵入ルール設定、Context Explorer へのクイック リンク、IP アドレスによるセキュリティ インテリジェンス グローバル ブラックリストまたはグローバル ホワイトリストをホストに追加するためのオプション、およびグローバル ホワイトリストに SHA-256 ハッシュ値を使用してファイルを追加するためのオプションがあります。

サーバ

アプリケーション プロトコル トラフィックによって識別される、ホスト上にインストールされたサーバ アプリケーション（クライアント アプリケーションと比較してください）。

ジオロケーション データベース

ルーティング可能な IP アドレスに関連付けられた既知のジオロケーション データの定期更新データベース（GeoDB とも呼ばれる）。

ジオロケーション

接続タイプやインターネット サービス プロバイダーなどのモニタ対象ネットワーク上のトラフィック内で検出されたルーティング可能な IP アドレスの地理的発生源に関するデータを提供する機能。ジオロケーション データベース、接続イベント、侵入イベント、ファイル イベント、およびマルウェア イベントだけでなく、ホスト プロファイルに保存されたジオロケーション情報も表示できます。

シスコ VRT

シスコの脆弱性調査チーム。

シスコ インテリジェンス フィード

レピュテーションを下げるためにシスコ VRT によって決定される IP アドレスの定期更新リストのコレクション。フィード内の各リストは、特定のカテゴリ（オープン リレー、既知の攻撃者、偽の IP アドレス（bogon）など）を表します。アクセス コントロール ポリシーでは、セキュリティ インテリジェンスを使用していずれかのカテゴリまたはすべてのカテゴリをブラックリストに追加できます。インテリジェンス フィードは定期的に更新されるため、それを使用することにより、システムは確実に最新情報を使用してネットワーク トラフィックをフィルタ処理できます。

シスコ クラウド

防御センターがマルウェア、セキュリティ インテリジェンス、URL フィルタリング データなどの最新の関連情報を入手可能な、*クラウド サービス*とも呼ばれる、シスコ ホステッド外部サーバ。マルウェア クラウド検索も参照してください。

システム ポリシー

メール中継ホスト プリファレンスや時刻同期設定などの、1 つの展開内の複数のアプライアンスと同様の設定。防御センターを使用して、システム ポリシーをそれ自体とその管理対象デバイスに適用します。

修復

システムに対する攻撃の可能性を軽減するアクション。修復を設定し、それらを相関ポリシー内で相関ルールとコンプライアンス ホワイト リストに関連付けることによって、トリガーされたときに防御センターで修復が起動されるようにできます。これにより、その場で解決できない攻撃を自動的に軽減するだけでなく、システムが組織のセキュリティ ポリシーに準拠していることを保証することもできます。防御センターには事前に定義された修復が付属していますが、柔軟な API を使用してカスタム修復を作成することもできます。

詳細設定

設定に特定の専門知識が必要なプリプロセッサ機能またはその他の侵入ポリシー機能。通常、詳細設定は、ほとんどまたはまったく変更を必要とせず、すべての展開に共通ではありません。

シリーズ 2

シスコ アプライアンス モデルの第 2 シリーズ。リソース、アーキテクチャ、およびライセンスの制限により、シリーズ 2 アプライアンスは、FireSIGHT システム機能の一部しかサポートしません。シリーズ 2 デバイスには、3D500、3D1000、3D2000、3D2100、3D2500、3D3500、3D4500、3D6500、および 3D9900 が含まれます。シリーズ 2 防御センターには、DC500、DC 1000、および DC 3000 が含まれます。

シリーズ 3

シスコ アプライアンス モデルの第 3 シリーズ。シリーズ 3 アプライアンスには、7000 シリーズと 8000 シリーズのデバイスだけでなく、DC750、DC1500、および DC3500 防御センターも含まれます。

侵入

ネットワーク上で発生したセキュリティ違反、攻撃、または悪用。

侵入イベント

侵入ポリシー違反を記録するイベント。侵入イベント データには、悪用の日付、時刻、および種類だけでなく、攻撃とそのターゲットに関するその他のコンテキスト情報も含まれます。

侵入検知および防御

ネットワーク トラフィックのセキュリティ ポリシー違反のモニタリングとインライン展開における悪意のあるトラフィックをブロックまたは変更できる能力。FireSIGHT システムでは、侵入ポリシーとアクセス コントロール ルールまたはデフォルト アクションを関連付けるときに侵入検知および防御を実行します。

侵入ポリシー

ネットワーク トラフィックの侵入とセキュリティ ポリシー違反を検査するように設定可能なさまざまなコンポーネント。これらのコンポーネントには、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侵入ルール、侵入ルールでよく使用される変数、FireSIGHT の推奨ルール設定、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詳細設定、および関連するプリプロセッサ オプション用のイベントを生成可能なプリプロセッサ ルールが含まれます。ネットワーク トラフィックがアクセス コントロール ルールの条件を満たしている場合は、侵入ポリシーを使用してそのトラフィックを検査できます。侵入ポリシーとデフォルト アクションを関連付けることもできます。

侵入ルール

モニタ対象ネットワーク トラフィックに適用された場合に、潜在的な侵入、セキュリティ ポリシー違反、およびセキュリティ違反を特定するキーワードと引数のセット。システムはルール条件に基づいてパケットを比較します。パケット データが条件と一致すると、ルールがトリガーされ、侵入イベントが生成されます。侵入ルールにはドロップ ルールとパス ルールが含まれています。

スイッチド インターフェイス

レイヤ 2 展開でトラフィックを切り替えるために使用するインターフェイス。タグなし VLAN トラフィックを処理する物理スイッチド インターフェイスをセットアップすることも、VLAN タグが指定されたトラフィックを処理する論理スイッチド インターフェイスをセットアップすることもできます。

スイッチ

マルチポート ブリッジとして機能するネットワーク デバイス。ネットワーク検出を使用すれば、システムでスイッチがブリッジとして識別されます。加えて、管理対象デバイスを複数のネットワーク間でパケット スイッチングを実行する仮想スイッチとして設定できます。

スケジュールされたタスク

一度だけ実行するように、または、定期的に実行するようにスケジュール可能な管理タスク。

スタック構成

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 セグメント上で検査するトラフィック量を増やすための機能。スタック構成を設定するときに、スタックする各デバイスのリソースを単一の共有構成に統合します。

スタック

検出リソースを共有する 2 ～ 4 つの接続されたデバイス。

脆弱性

ホストが被る可能性のある特定の侵害を指す表現。防御センターは、脆弱性がある各ホストの脆弱性に関する情報をホスト プロファイルで提供します。加えて、脆弱性ネットワーク マップを使用して、システムがモニタ対象ネットワーク全体で検出した脆弱性の全体図を入手できます。ホストが特定の侵害に対して脆弱ではなくなったと判断した場合は、特定の脆弱性を非アクティブにすることも、無効としてマークすることもできます。

脆弱性データベース

VDB とも呼ばれる、ホストが影響を受ける可能性のある既知の脆弱性のデータベース。システムは、各ホストで検出されたオペレーティング システム、アプリケーション プロトコル、およびクライアントと VDB を相互に関連づけることによって、特定のホストでネットワーク侵害のリスクが増大するかどうかを判断しやすくします。VDB 更新には、新しい脆弱性と更新された脆弱性だけでなく、新しいアプリケーション ディテクタと更新されたアプリケーション ディテクタも含まれます。

セキュリティ インテリジェンス フィード

システムが設定された間隔で定期的にダウンロードする IP アドレスの動的コレクションであるセキュリティ インテリジェンス オブジェクトの一種。フィードは定期的に更新されるため、それらを使用することにより、セキュリティ インテリジェンス機能で最新の情報を使用してネットワーク トラフィックがフィルタ処理されることが保証されます。シスコ インテリジェンス フィードも参照してください。

セキュリティ インテリジェンス リスト

セキュリティ インテリジェンス オブジェクトとして防御センターに手動でアップロードする IP アドレスの単純な静的コレクション。このリストは、セキュリティ インテリジェンス フィードだけでなく、グローバル ブラックリストとグローバル ホワイトリストも拡張または最適化するために使用します。

セキュリティ インテリジェンス

ソース IP アドレスまたは宛先 IP アドレスに基づいて、アクセス コントロール ポリシー単位でネットワークを通過可能なトラフィックを指定するための機能。これは、トラフィックがアクセス コントロール 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追加する（そのアドレスからのまたはそのアドレスへのトラフィックを拒否する）場合に特に便利です。オプションで、セキュリティ インテリジェンス フィルタリング用のモニタ設定を使用できます。これにより、システムでブラックリストに追加された接続を分析できるようになりますが、ブラックリストと一致したものがログに記録されます。

セキュリティ ゾーン

さまざまなポリシーと設定でトラフィック フローを管理および分類するために使用可能な 1 つ以上のインライン、パッシブ、スイッチド、またはルーテッド インターフェイスのグループ分け。単一のゾーン内のインターフェイスで複数のデバイスをカバーできます。単一のデバイスに複数のセキュリティ ゾーンを設定することもできます。トラフィックを処理する前に、設定するそれぞれのインターフェイスをセキュリティ ゾーンに割り当てる必要があります。すべてのインターフェイスを 1 つのセキュリティ ゾーンに所属させることもできます。

セキュリティ ポリシー

ネットワークを保護するための組織のガイドライン。たとえば、セキュリティ ポリシーで、ワイヤレス アクセス ポイントの使用を禁止します。セキュリティ ポリシーにアクセプタブル ユース ポリシー（AUP）を含めることもできます。これにより、組織のシステムの使用方法に関するガイドラインが従業員に提供されます。

セキュリティ ポリシー違反

ネットワークのセキュリティ違反、攻撃、悪用、またはその他の不正使用。

接続

2 つのホスト間のモニタ対象セッション。アクセス コントロール ポリシー内の管理対象デバイスによって検出された接続をログに記録できます。ネットワーク検出ポリシーで NetMod 接続ロギングを設定します。

設定可能なバイパス

バイパス モードを設定可能なインライン セットの特性。

センシング インターフェイス

ネットワーク セグメントのモニタに使用されるデバイス上のネットワーク インターフェイス。管理インターフェイスと比較してください。

相関

ネットワーク上の脅威にリアルタイムに対処する相関ポリシーの作成に使用可能な機能。相関の修復コンポーネントは、ポリシー違反に対処するための独自のカスタム修復モジュールを作成してアップロードできる柔軟な API を提供します。

タスク キュー

アプライアンスが実行する必要のあるジョブのキュー。ポリシーを適用したり、ソフトウェア アップデートをインストールしたり、その他の長時間ジョブを実行したりすると、ジョブがキューに入れられ、そのステータスが [Task Status] ページに表示されます。[Task Status] ページには、ジョブの詳細なリストが表示され、10 秒ごとに再描画され、そのステータスが更新されます。

ダッシュボード ウィジェット

FireSIGHT システムの側面に対する理解を促す小型の自己完結型ダッシュボード コンポーネント。

ダッシュボード

システムによって収集または生成されたイベントに関するデータを含む、現在のシステム ステータスを一目で確認できるようにする表示。システムに付属のダッシュボードを増強するために、選択したダッシュボード ウィジェットにデータを設定したさまざまなカスタム ダッシュボードを作成できます。モニタ対象ネットワークの外観や動作に関する広範で簡略化されたカラフルな画像を提供する Context Explorer と比較してください。

タップ モード

各パケットのコピーが分析され、ネットワーク トラフィック フローはデバイスをパススルーせず妨害されない 3D9900 とシリーズ 3 デバイス上で使用可能な高度なインライン セット オプション。パケットそのものではなく、パケットのコピーが処理されるため、デバイスは、アクセス コントロール ポリシーと侵入ポリシーがトラフィックをドロップ、変更、またはブロックするように設定されていてもパケット ストリームに影響を与えることはできません。

データベース アクセス

サードパーティ製クライアントによる防御センター データベースへの読み取り専用アクセスを可能にする機能。

テーブル ビュー

イベント情報をデータベース テーブル内のフィールドごとに 1 列ずつ表示するワークフロー ページの一種。イベント分析を実行するときに、ドリルダウン ページを使用して調査するイベントを絞り込んでから、興味のあるイベントの詳細が表示されたテーブル ビューに移動することができます。テーブル ビューの多くは、システムに付属のワークフロー内の最後から 2 つ目のページです。

ディスカバリ ポリシー

ネットワーク検出ポリシーを参照してください。

ディスカバリ

管理対象デバイスを使用してネットワークをモニタし、ネットワークの完全で永続的なビューを提供する FireSIGHT システムのコンポーネント。ネットワーク検出によって、ネットワーク上のホスト（ネットワーク デバイスとモバイル デバイスを含む）の台数や種類だけでなく、それらのホスト上のオペレーティング システム、アクティブ アプリケーション、およびオープン ポートに関する情報も特定されます。また、ネットワーク上のユーザ アクティビティをモニタするようにシスコ管理対象デバイスを設定して、ポリシー違反、攻撃、またはネットワークの脆弱性の原因を特定できるようにすることもできます。

適用

ポリシーまたはそれに対する変更を有効にするために実行するアクション。ほとんどのポリシーは防御センター から管理対象デバイスに適用されます。ただし、相関ポリシーは管理対象デバイスの設定への変更に関与しないため、ユーザがアクティブ化または非アクティブ化します。

デコーダ

スニファで取り込んだパケットをプリプロセッサによって理解可能な形式に置き換える侵入検知および防御のコンポーネント。

デバイス クラスタリング

クラスタリングを参照してください。

デバイス スタッキング

スタック構成を参照してください。

デバイス

さまざまなスループットで使用可能な、フォールトトレラント設計で特定用途向けのアプライアンス。デバイス上で有効にされたライセンス対象機能に応じて、それらを利用し、受動的にトラフィックをモニタしてネットワーク アセット、アプリケーション トラフィック、およびユーザ アクティビティの包括的マップを作成したり、侵入検知および防御を実行したり、アクセス制御を実行したり、スイッチングとルーティングを設定したりできます。防御センターを使用してデバイスを管理する必要があります。

デフォルト アクション

アクセス コントロール ポリシーの一部として、ポリシー内のルールの条件を満たさないトラフィックの処理方法を決定します。アクセス コントロール ルールもセキュリティ インテリジェンス設定も含まないアクセス コントロール ポリシーを適用した場合は、デフォルト ポリシー アクションによってネットワーク上の非ファストパス トラフィックの処理方法が決定されます。デフォルト アクションは、余分な検査を行わずにトラフィックをブロックまたは信頼するように設定したり、ネットワーク検出ポリシーまたは侵入ポリシーを使用してトラフィックを検査したりするように設定できます。

トランスペアレント インライン モード

デバイスを「Bump In The Wire」として機能させ、送信元と宛先に関係なく、それが認識するすべてのネットワーク トラフィックを転送可能にするための高度なインライン セット オプション。

ネットワーク デバイス

FireSIGHT システムで、ブリッジ、ルータ、NAT デバイス、または論理インターフェイスとして特定されたホスト。

ネットワーク ファイル トラジェクトリ

ホストがネットワーク経由でファイルを転送する場合のファイルのパスの視覚的表現。SHA-256 ハッシュ値が関連付けられたファイルの場合は、トラジェクトリ マップに、ファイルを転送したすべてのホストの IP アドレス、ファイルが検出された時刻、ファイルのマルウェア処理、関連するファイル イベント、マルウェア イベントなどが表示されます。

ネットワーク マップ

ネットワークの詳細な表現。ネットワーク マップを使用すれば、ネットワーク上で実行中のホスト、モバイル デバイス、およびネットワーク デバイスの観点だけでなく、関連するホスト属性、アプリケーション プロトコル、および脆弱性の観点でもネットワーク トポロジを表示できます。

ネットワーク検出

ディスカバリを参照してください。

ネットワーク検出ポリシー

NetMod 対応デバイスによってモニタされたネットワークを含む特定のネットワーク セグメントに対してシステムが収集するディスカバリ ポリシーの種類（ホスト、ユーザ、およびアプリケーション データなど）を指定するポリシー。ネットワーク検出ポリシーは、インポート解決プリファレンスとアクティブ検出ソース プライオリティも管理します。

バーチャル デバイス

仮想ホスティング環境内の独自の設備に展開可能な管理対象デバイス。バーチャル デバイスを仮想スイッチまたは仮想ルータとして設定することはできません。

ハイ アベイラビリティ

デバイスのグループを管理するように冗長な物理 防御センター を設定するための機能。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 に流れ、ほとんどの設定要素が両方の 防御センター 上で維持されます。プライマリ 防御センター で障害が発生した場合は、セカ

ンダリ 防御センター を使用して中断せずにネットワークをモニタできます。冗長なデバイスを指定可能なクラスタリングと比較してください。

バイパス モード

何らかの理由でセット内のセンシング インターフェイスで障害が発生した場合にトラフィックの流れを維持できるようにするインライン セットの特性。

ハイブリッド インターフェイス

システムで仮想ルータと仮想スイッチ間のトラフィックをブリッジするための管理対象デバイス上の論理インターフェイス。

パッシブ インターフェイス

パッシブ展開でトラフィックを分析するように設定されたセンシング インターフェイス。

パッシブ検出

管理対象デバイスによって受動的に収集されたトラフィックの分析を通したディスカバリ ポリシーのコレクション。アクティブ検出と比較してください。

非バイパス モード

何らかの理由でセット内のセンシング インターフェイスで障害が発生した場合にトラフィックをブロックするインライン セットの特性。

ファイル タイプ

PDF、EXE、MP3 などのファイル形式の特定の種類。

ファイル トラジェクトリ

ネットワーク ファイル トラジェクトリを参照してください。

ファイル ポリシー

システムがファイル制御と高度なマルウェア対策を実行するために使用するポリシー。ファイル ルールによって生成されたファイル ポリシーは、アクセス コントロール ポリシー内のアクセス コントロール ルールから呼び出されます。

ファイル制御

アクセス制御の一部として、ネットワークを通過可能なファイルの種類を指定してログに記録するための機能。

ファストパス ルール

分析する必要のないトラフィックに処理のバイパスを許可するため、限定的な条件を使用して、デバイスのハードウェア レベルで設定するルール。

フィード

セキュリティ インテリジェンス フィードを参照してください。

物理インターフェイス

NetMod 上の物理ポートを表すインターフェイス。

プリプロセッサ ルール

プリプロセッサまたはポートスキャン フロー ディテクタに関連付けられた侵入ルール。プリプロセッサ ルールでイベントを生成する場合は、そのルールを有効にする必要があります。プリプロセッサ ルールには、プリプロセッサ固有の GID（ジェネレータ ID）が割り当てられます。

プリプロセッサ

侵入ポリシーによって検査されるトラフィックを正規化し、不適切なヘッダー オプションの識別、IP データグラムの最適化、TCP ステートフル インスペクションとストリーム リアセンブルの提供、およびチェックサムの確認によるネットワーク層とトランスポート層のプロトコル異常の特定を支援する機能。プリプロセッサは、特定の種類のパケット データをシステムで分析可能な形式で表現できます。このようなプリプロセッサは、データ正規化プリプロセッサまたはアプリケーション層プロトコル プリプロセッサと呼ばれます。アプリケーション層プロトコルのエンコーディングを正規化すれば、データが別の方法で表現されるパケットに同じコンテンツ関連侵入ルールを効率的に適用し、意味のある結果を得ることができます。プリプロセッサは、パケットが設定されたプリプロセッサ オプションをトリガーするたびにプリプロセッサ ルールを生成します。

ヘルス ポリシー

展開内のアプライアンスのヘルスをチェックするときに使用される基準。ヘルス ポリシーは、ヘルス モジュールを使用して、FireSIGHT システム のハードウェアとソフトウェアが正しく動作しているかどうかを示します。デフォルトのヘルス ポリシーを使用することも、独自のものを作成することもできます。

ヘルス モジュール

展開内のアプライアンスの CPU 使用率や空きディスク領域などの特定の性能的側面のテスト。ユーザがヘルス ポリシーで有効にするヘルス モジュールは、モニタしている性能的側面が特定のレベルに達したときにヘルス イベントを生成します。

ヘルス モニタ

展開内のアプライアンスのパフォーマンスを継続的にモニタする機能。ヘルス モニタは、適用されたヘルス ポリシー内のヘルス モジュールを使用してアプライアンスをテストします。

防御センター

デバイスを管理し、それらが生成したイベントを自動的に集約して関連付けるための集中管理点。

保護されたネットワーク

ファイアウォールなどのデバイスによって他のネットワーク ユーザから保護された組織の内部ネットワーク。FireSIGHT システムを使用して配信される侵入ルールの多くは、保護されたネットワークと保護されていない（または外部の）ネットワークを定義する変数を使用します。

ホスト

ネットワークに接続され、一意の IP アドレスが割り当てられたデバイス。FireSIGHT システムにとって、ホストは、モバイル デバイス、ブリッジ、ルータ、NAT デバイス、または論理インターフェイスとして分類されない特定のホストです。

ホスト入力

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 ソースからデータをインポートしてネットワーク マップ内の情報を拡張するための機能。この Web インターフェイスはいくつかのホスト入力機能も提供します。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 ID を変更したり、脆弱性を有効または無効にしたり、クライアント ポートとサーバ ポートを含むネットワーク マップからさまざまな項目を削除したりできます。

ポリシー

アプライアンスに最も頻繁に設定を適用するためのメカニズム。アクセス コントロール ポリシー、相関ポリシー、ファイル ポリシー、ヘルス ポリシー、侵入ポリシー、ネットワーク検出ポリシー、およびシステム ポリシーを参照してください。

マルウェア イベント

シスコの高度なマルウェア対策ソリューションのいずれかによって生成されるイベント。ネットワークベースのマルウェア イベントは、シスコ クラウドがネットワーク トラフィック内で検出されたファイルのマルウェア処理を戻したときに生成されます。その処理が変化すると、遡及的なマルウェア イベントが生成されます。展開された FireAMP Connector が脅威を検出したり、マルウェアの実行をブロックしたり、マルウェアを検疫したり、マルウェアの検疫に失敗したりした場合に生成されるエンドポイント ベースのマルウェア イベントと比較してください。

マルウェア クラウド検索

防御センターがシスコ クラウドと通信して、ファイルの SHA-256 ハッシュ値に基づいてネットワーク トラフィック内で検出されたファイルのマルウェア処理を決定するプロセス。

マルウェア ブロッキング

シスコのネットワークベースの高度なマルウェア対策（AMP）ソリューションのコンポーネント。マルウェア検出 が検出されたファイルのマルウェア処理を完了したら、そのファイルをブロックすることも、そのアップロードまたはダウンロードを許可することもできます。この機能を FireAMP サブスクリプションが必要なシスコのエンドポイント ベースの AMP ツールである FireAMP と比較してください。

マルウェア ライセンス

ネットワーク トラフィック内の高度なマルウェア対策（AMP）を実行するためのライセンス。ファイル ポリシーを使用すれば、管理対象デバイスによって検出された特定のファイル タイプに対してマルウェア クラウド検索を実行するようにシステムを設定できます。FireAMP サブスクリプションと比較してください。

マルウェア対策

高度なマルウェア対策を参照してください。

マルウェア検出

シスコのネットワークベースの高度なマルウェア対策（AMP）ソリューションのコンポーネント。ネットワーク トラフィックを検査する全体的なアクセス制御設定の一部として管理対象デバイスに適用されるファイル ポリシー。その後で、防御センターは検出された特定のファイル タイプのマルウェア クラウド検索を実行し、ファイルのマルウェア処理をユーザに警告するイベントを生成します。続けて AMP マルウェア ブロッキングが実行されて、ファイルをブロックするか、そのアップロードまたはダウンロードを許可します。この機能を FireAMP サブスクリプションが必要なシスコのエンドポイント ベースの AMP ツールである FireAMP と比較してください。

モニタ

アクセス コントロール ポリシーで、セキュリティ インテリジェンス ブラックリストまたはアクセス コントロール ルールと一致するトラフィックをログに記録するが、システムにはトラフィックを即座に許可またはブロックするのではなく、評価を継続させる方法。

モバイル デバイス

FireSIGHT システムで、ディスカバリ機能によって可搬型のハンドヘルド デバイス（携帯電話やタブレットなど）として特定されたホスト。多くの場合、システムは、モバイル デバイスがジェイルブレイクされているかどうかを検出できます。

ユーザ アクティビティ

システムがユーザ ログイン（オプションで、失敗したログイン試行を含む）または防御センター データベースに対するユーザ レコードの追加または削除を検出したときに生成されるイベント。

ユーザ エージェント

ユーザがネットワークにログインするとき、または、その他の理由で Active Directory クレデンシャルに対して認証されるときにそのユーザをモニタするため、サーバにインストールするエージェント。アクセス制御ユーザのユーザ アクティビティは、ユーザ エージェントから報告されるときにだけアクセス制御に使用されます。

ユーザ ロール

FireSIGHT システムのユーザに付与されるアクセス レベル。たとえば、イベント アナリスト、FireSIGHT システムを管理している管理者、サードパーティ製ツールを使用して防御センター データベースにアクセスしているユーザなどのための Web インターフェイスにさまざまなアクセス権限を付与することができます。特殊なアクセス権限を持つカスタム ロールを作成することもできます。

ユーザ

ネットワーク アクティビティが管理対象デバイスまたはユーザ エージェントによって検出されたユーザ。

ユーザ認識

組織で脅威、エンドポイント、およびネットワーク インテリジェンスをユーザ ID 情報に関連付けたり、ユーザにユーザ制御の実行を許可したりするための機能。

ユーザ制御

アクセス制御の一部として、ネットワークに出入りしたり、ネットワーク内部を移動したりするユーザ関連トラフィックを指定してログに記録するための機能。

リスト

セキュリティ インテリジェンス リストを参照してください。

リンク ステート伝達

インライン セット内のどちらかのインターフェイスがダウンしたときに自動的にペア内の 2 つ目のインターフェイスをダウンさせるバイパス モードのインライン セットのオプション。ダウンしたインターフェイスが復旧すると、2 つ目のインターフェイスも自動的に復旧します。つまり、ペア化されたインターフェイスのリンク ステートが変化すると、それに合わせてもう一方のインターフェイスのリンク ステートが自動的に変化します。

ルータ

ネットワーク間でパケットを転送する、ゲートウェイに配置されたネットワーク デバイス。ネットワーク検出を使用すれば、システムでルータを識別できます。加えて、管理対象デバイスを、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仮想ルータとして設定できます。

ルーテッド インターフェイス

レイヤ 3 展開でトラフィックをルーティングするインターフェイス。タグなし VLAN トラフィックを処理する物理ルーテッド インターフェイスをセットアップすることも、VLAN タグが指定されたトラフィックを処理する論理ルーテッド インターフェイスをセットアップすることもできます。また、静的なアドレス解決プロトコル（ARP）エントリをルーテッド インターフェイスに追加することもできます。

ルール アクション

ルールの条件を満たすネットワーク トラフィックの処理方法を指定した設定。アクセス コントロール ルール アクションとファイル ルール アクションを参照してください。

ルール

ネットワーク トラフィックの検査基準を提供する、通常はポリシー内にある構造。

ルール更新

必要に応じて、新しいまたは更新された標準テキストのルール、共有オブジェクトのルール、およびプリプロセッサ ルールを含む侵入ルールの更新。ルール更新では、ルールの削除、デフォルト侵入ポリシー設定の変更、およびシステム変数とルール カテゴリの追加または削除が行われる場合があります。

ルール状態

侵入ポリシー内の侵入ルールが有効になっている（[Generate Events] または [Drop and Generate Events] に設定されている）か、無効になっている（[Disable] に設定されている）か。ルールを有効にした場合は、ネットワーク トラフィックの評価に使用されます。ルールを無効にした場合は、使用されません。

レイヤ

侵入ポリシー内の侵入ルール、プリプロセッサ ルール、および詳細設定構成の完全なセット。ポリシー内の組み込みレイヤにカスタム ユーザ レイヤを追加できます。侵入ポリシー内の上位レイヤの設定が下位レイヤの設定より優先されます。

レピュテーション（IP アドレス）

セキュリティ インテリジェンスを参照してください。

論理インターフェイス

タグ付きトラフィックが物理インターフェイスを通過したときに特定の VLAN タグ付きトラフィックを処理するように定義された仮想サブインターフェイス。