CHAPTER 2
SOURCEFIRE 3D SYSTEM の概要

Sourcefire 3D® システムは、業界トップ レベルのネットワーク侵入防御システムのセキュリティに、検出されたアプリケーション、ユーザ、および URL に基づいてネットワークへのアクセスを制御する機能を組み合わせたものです。ユーザは Sourcefire のアプライアンスを、スイッチド、ルーテッド、または（この両者を組み合わせた）ハイブリッドの環境内で使用することで、ネットワーク アドレス変換（NAT）を実行することができます。また、管理対象デバイスの Sourcefire の仮想ルータ間で安全な仮想プライベート ネットワーク（VPN）トンネルを構築することができます。

Sourcefire 防御センター® は、Sourcefire 3D System に集中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 セグメントにインストールされている管理対象デバイスは、分析用のトラフィックを監視します。

パッシブな展開のデバイスは、ネットワークを流れるトラフィックを、スイッチ SPAN、仮想スイッチ、ミラー ポートなどを使用して監視します。パッシブ センシング インターフェイスはすべてのトラフィックを無条件で受信し、これらのインターフェイスで受信されたトラフィックは再送信されません。

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

物理アプライアンスのほかに、ソフトウェア ベースの以下の Sourcefire アプライアンスを展開することができます。

- 64 ビット仮想防御センター®（VMware ESXi および VMware VMware vCloud Director ホスティング環境用）
- 同じ VMware 環境を使用した 64 ビットの仮想デバイス、および Crossbeam プラットフォーム上のホスティング X-シリーズの Sourcefire ソフトウェア

このガイドでは、Sourcefire 3D System の機能に関する情報を提供します。各章の説明、図、および手順には、ユーザ インターフェイスをナビゲートする、システム パフォーマンスを最大にする、問題をトラブルシューティングする、といったことに役に立つ詳細な情報が記載されています。

以下のトピックでは Sourcefire 3D System の概要、主なコンポーネント、Sourcefire アプライアンスに対するログインとログアウトの方法について説明します。また、システムの Web インターフェイスの使用に関する基本的な情報が含まれており、このガイドの使用法について理解するうえで有用です。

- 「Sourcefire 3D System のアプライアンス」（P.14）
- 「Sourcefire 3D System のコンポーネント」（P.22）
- 「セキュリティ、インターネット アクセス、および通信ポート」（P.29）
- 「ドキュメント リソース」（P.34）
- 「ドキュメントの表記規則」（P.35）
- 「IP アドレスの表記規則」（P.38）
- 「アプライアンスへのログイン」（P.40）
- 「アプライアンスにログインしてアカウントを設定する」（P.42）
- 「アプライアンスからのログアウト」（P.44）
- 「コンテキスト メニューの使用」（P.45）

Sourcefire 3D System のアプライアンス

Sourcefire *アプライアンス*は、トラフィック検知の管理対象の *デバイス*または管理を実行する*防御センター*のいずれかです。

物理的なデバイスはフォールトトレラントで、特定の目的に特化したネットワーク アプライアンスであり、ある範囲のスループットおよび機能で使用することができます。防御センターはこれらのデバイスの集中管理ポイントとして機能し、生成されたイベントを自動的に集約し、関連付けます。それぞれの物理アプライアンスのタイプには、いくつかの *モデル*があります。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。

また、64 ビットの仮想防御センターとデバイスを、VMware ESXi および VMware vCloud Director ホスティング環境でホストすることもできます。仮想防御センターは物理デバイスを管理することが可能で、物理防御センターは仮想デバイスを管理することが可能です。また、X-シリーズの Sourcefire ソフトウェアを Crossbeam プラットフォームでホストすることができます。

Sourcefire 3D System の多くの機能は、アプライアンスによって異なります。詳細については、次の項を参照してください。

- 「防御センター」（P.15）
- 「管理対象デバイス」（P.15）
- 「アプライアンスのシリーズ、モデル、および機能について」（P.16）

防御センター

防御センターは Sourcefire 3D System 展開環境に集中管理ポイントとイベントデータベースを提供します。（物理および仮想両方の）防御センターは侵入、ファイル、マルウェア、ディスカバリ、接続、およびパフォーマンスのデータを集約して関連付け、特定のホストにおけるイベントの影響を評価し、ホストに侵害の痕跡のタグを付けます。これにより、デバイス間で交わされる情報の監視、ネットワーク上で発生するアクティビティ全体の評価や制御が可能になります。

防御センターの主な機能は次のとおりです。

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

多くの物理防御センターでは、高可用性（冗長）機能により操作の継続性が保証されています。

管理対象デバイス

物理 Sourcefire デバイスはフォールトトレラントで、特定の目的に特化したネットワークアプライアンスであり、ある範囲のスループットで使用することができます。仮想デバイスまたは X-シリーズの Sourcefire ソフトウェア をホストすることもできます。パッシブに展開されたデバイスは、ネットワーク トラフィックについて理解するうえで有用です。インラインで展開されている場合は、Sourcefire デバイスを使用し、複数の基準に基づいてトラフィックのフローに影響を及ぼすことができます。防御センターを使用して Sourcefire デバイスを管理する必要があります。

モデルおよびライセンスによって、管理対象デバイスの機能は次のように異なります。

- 組織のホスト、オペレーティング システム、アプリケーション、ユーザ、ファイル、ネットワーク、および脆弱性に関する詳細情報を収集する
- ネットワークベースのさまざまな基準、およびアプリケーション、ユーザ、URL、IP アドレスの評価、および侵入やマルウェアの調査結果を含めた他の基準によって、ネットワーク トラフィックをブロックまたは許可する
- 設定可能なバイパス インターフェイス、高速パス ルール、および厳密な TCP の適用の他に、スイッチング、ルーティング、DHCP、NAT、VPN の機能を備えている
- クラスタリング（冗長性）により操作の継続性を保証する、スタッキングにより複数のデバイスのリソースを組み合わせることができる

アプライアンスのシリーズ、モデル、および機能について

Sourcefire 3D System のバージョン 5.3 は、物理アプライアンスの 2 つのシリーズ、および仮想アプライアンスと X-シリーズの Sourcefire ソフトウェア で使用することができます。Sourcefire 3D System の多くの機能は、アプライアンスによって異なります。詳細については、以下を参照してください。

- 「シリーズ 2 のアプライアンス」（P.16）
- 「シリーズ 3 のアプライアンス」（P.17）
- 「仮想アプライアンス」（P.17）
- 「X-シリーズの Sourcefire ソフトウェア」（P.17）
- 「バージョン 5.3 で配布されるアプライアンス」（P.18）
- 「アプライアンスのモデル別のサポートされる機能」（P.19）

シリーズ 2 のアプライアンス

シリーズ 2 は Sourcefire 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 のデバイスは、Sourcefire 3D System の一部の機能セットしかサポートしていません。

Sourcefire では新しい シリーズ 2 のアプライアンスを出荷していませんが、シリーズ 2 デバイスおよび防御センターをバージョン 5.3 に再イメージングすることができます。再イメージングを実行すると、アプライアンス上の**すべての**設定およびイベント データが失われます。詳細については、『*Sourcefire 3D System Installation Guide*』を参照してください。

警告! また、防御センター バージョン 4.10.3 または 3D Sensor の特定の設定とイベント データを、防御センター バージョン 5.2 へ移行し、その後でバージョン 5.3 にアップグレードすることができます。詳細については、『*Sourcefire 3D System Migration Guide*』でバージョン 5.2 を参照してください。

バージョン 5.3 を実行している場合、シリーズ 2 のデバイスは 保護ライセンスに関連付けられているほとんどの機能（侵入検知および防御、ファイル制御、基本的なアクセス制御など）を自動的に備えています。ただし、シリーズ 2 の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、高度なアクセス制御、または高度なマルウェア対策は実行できません。また、シリーズ 2 のデバイスでライセンスを取得した他の機能を有効にすることもできません。高速パス ルール、スタッキング、およびタップ モードをサポートしている 3D9900 を除いて、シリーズ 2 のデバイスは、シリーズ 3 のデバイスに関連付けられてい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）をサポートしていません。

バージョン 5.3、DC1000、および DC3000 シリーズ 2 防御センターは、Sourcefire 3D System のすべての機能をサポートしていますが、DC500 には、制限された機能のみ付随しています。

シリーズ 3 のアプライアンス

シリーズ 3 はSourcefire の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 および8000 シリーズ のデバイスはシリーズ 3 のアプライアンスです。8000 シリーズ のデバイスはより強力で、7000 シリーズ のデバイスがサポートしていない機能をサポートしています。

仮想アプライアンス

64 ビットの仮想防御センターとデバイスを、VMware ESXi および VMware vCloud Director ホスティング環境でホストすることができます。仮想防御センターは最大 25 個の物理または仮想デバイスを管理することが可能で、物理防御センターは仮想デバイスを管理することが可能です。

インストールおよび適用されているライセンスに関係なく、仮想アプライアンスはシステムのハードウェアベースの機能（冗長性、リソース共有、スイッチング、ルーティングなど）をサポートしません。また、仮想デバイスには Web インターフェイスがありません。

X-シリーズの Sourcefire ソフトウェア

Crossbeam プラットフォーム上でソフトウェアベースの X-シリーズの Sourcefire ソフトウェア をホストすることができます。これは仮想デバイスと類似の機能を備えています。仮想デバイスと同様に、X-シリーズの Sourcefire ソフトウェアには Web インターフェイスがありません。

インストールおよび適用されているライセンスに関係なく、X-シリーズの Sourcefire ソフトウェア はハードウェアベースの機能（冗長性、リソースの共有、スタッキング、クラスタリング、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。

Sourcefire 3D System を使用して冗長性を設定することはできませんが、X-シリーズの Sourcefire ソフトウェアのパッケージをインストールするときに冗長性を設定することができます。詳細については、『*Sourcefire Software for X-Series Installation Guide*』を参照してください。

バージョン 5.3 で配布されるアプライアンス

以下の表は、Sourcefire が Sourcefire 3D System のバージョン 5.3 で配布するアプライアンスについて示しています。

バージョン 5.3 の Sourcefire アプライアンス

モデル/ファミリ	シリーズ	タイプ
70xx ファミリ： • 3D7010/7020/7030	シリーズ 3（7000 シリーズ）	デバイス
71xx ファミリ： • 3D7110/7120 • 3D7115/7125 • AMP7150	シリーズ 3（7000 シリーズ）	デバイス
81xx ファミリ： • 3D8120/8130/8140 • AMP8150	シリーズ 3（8000 シリーズ）	デバイス
82xx ファミリ： • 3D8250 • 3D8260/8270/8290	シリーズ 3（8000 シリーズ）	デバイス
83xx ファミリ： • 3D8350 • 3D8360/8370/8390	シリーズ 3（8000 シリーズ）	デバイス

バージョン 5.3 の Sourcefire アプライアンス（続き）

モデル/ファミリ	シリーズ	タイプ
仮想デバイス	n/a	デバイス
X-シリーズの Sourcefire ソフトウェア	n/a	デバイス
シリーズ 3 防御センター： • DC750/1500/3500	シリーズ 3	防御センター
仮想防御センター	n/a	防御センター

Sourcefire では新しい シリーズ 2 のアプライアンスを出荷していませんが、シリーズ 2 デバイスおよび防御センターをバージョン 5.3 に再イメージングすることができます。再イメージングを実行すると、アプライアンス上のすべての設定およびイベント データが失われます。詳細については、『*Sourcefire 3D System Installation Guide*』を参照してください。

防御センター バージョン 4.10.3 または 3D Sensor の特定の設定とイベント データを、防御センター バージョン 5.2 へ移行し、その後でバージョン 5.3 にアップグレードすることができます。詳細については、『*Sourcefire 3D System Migration Guide*』でバージョン 5.2 を参照してください。ガイドおよび移行スクリプトの入手については、Sourcefire のサポートへお問い合わせください。

アプライアンスのモデル別のサポートされる機能

Sourcefire 3D System の多くの機能は、アプライアンスによって異なります。次の表は、正しいライセンスがインストールおよび適用されている場合の、システムの主な機能と、それらの機能をサポートするアプライアンスを対応付けたものです。

デバイスベースの機能（スタッキング、スイッチング、ルーティングなど）の防御センターの列は、防御センターがこれらの機能を実行するためにデバイスを管理および設定できるかどうかを示しています。たとえば、シリーズ 2 DC1000 を使用して、シリーズ 3 のデバイス上で NAT を管理することができます。

アプライアンスのモデル別のサポートされる機能

機能	シリーズ 2 のデバイス	シリーズ 2 防御センター	シリーズ 3 のデバイス	シリーズ 3 防御センター	仮想デバイス	仮想防御センター	X-シリーズ
ネットワーク ディスカバリ：ホスト、アプリケーション、およびユーザ	可	可	可	可	可	可	可
地理情報データ	可	DC1000 DC3000	可	可	可	可	可
侵入検知および防御（IPS）	可	可	可	可	可	可	可
セキュリティ インテリジェンス フィルタリング	不可	DC1000、DC3000	可	可	可	可	可
アクセス制御：基本的なネットワーク制御	可	可	可	可	可	可	可
アクセス制御：アプリケーション	不可	可	可	可	可	可	可
アクセス制御：ユーザ	不可	DC1000、DC3000	可	可	可	可	可
アクセス制御：リテラル URL	不可	可	可	可	可	可	可
アクセス制御：カテゴリおよびレピュテーションによる URL のフィルタリング	不可	DC1000、DC3000	可	可	可	可	可
ファイルの制御：ファイル タイプによる	可	可	可	可	可	可	可
ネットワークベースの高度なマルウェア防御（AMP）	不可	DC1000、DC3000	可	可	可	可	可
FireAMP の統合	n/a	可	n/a	可	n/a	可	n/a

アプライアンスのモデル別のサポートされる機能（続き）

機能	シリーズ 2 のデバイス	シリーズ 2 防御センター	シリーズ 3 のデバイス	シリーズ 3 防御センター	仮想デバイス	仮想防御センター	X-シリーズ
高速パス ルール	3D9900	可	8000 シリーズ	可	不可	可	不可
厳密な TCP の適用	不可	可	可	可	不可	可	不可
設定可能なバイパス インターフェイス	可	可	ハードウェアが制限されている場合を除く	可	不可	可	不可
タップ モード	3D9900	可	可	可	不可	可	不可
スイッチングおよびルーティング	不可	可	可	可	不可	可	不可
NAT ポリシー	不可	可	可	可	不可	可	不可
VPN	不可	可	可	可	不可	可	不可
高可用性	n/a	DC1000、DC3000	n/a	DC1500、DC3500	n/a	不可	n/a
デバイスのスタッキング	3D9900	可	3D8140、82xx ファミリ、83xx ファミリ	可	不可	可	不可
デバイスのクラスタリング	不可	可	可	可	不可	可	不可
クラスタ化されたスタック	不可	可	3D8140、82xx ファミリ、83xx ファミリ	可	不可	可	不可
マルウェア ストレージ パック	不可	DC1000、DC3000	可	可	不可	不可	不可
インタラクティブ CLI	不可	不可	可	不可	可	不可	不可

X-シリーズの Sourcefire ソフトウェア には、Crossbeam プラットフォームに固有のコマンド ライン インターフェイスがあります。ユーザはこれを使用して冗長性やロードバランシング、あるいはその両方を設定することができます。詳細については、『*Sourcefire Software for X-Series Installation Guide*』を参照してください。

Sourcefire 3D System のコンポーネント

以下のトピックでは、組織のセキュリティ、適用可能な使用ポリシー、およびトラフィック管理の戦略に対して有用な Sourcefire 3D System の主な機能について説明します。

- 「冗長性およびリソース共有」（P.22）
- 「ネットワーク トラフィックの管理」（P.23）
- 「FireSIGHT」（P.25）
- 「アクセス制御」（P.25）
- 「侵入検知と侵入防御」（P.26）
- 「ファイルの追跡、コントロール、マルウェア防御」（P.26）
- 「アプリケーション プログラミング インターフェース」（P.28）

ヒント! Sourcefire 3D System の多くの機能はアプライアンス モデル、ライセンス、およびユーザ ロールによって異なります。このドキュメントには、各機能に対して Sourcefire 3D System のどのライセンスとデバイスが必要か、各手順を完了するための権限を持っているのはどのユーザ ロールかについての情報が含まれています。詳細については、「ドキュメントの表記規則」（P.35）を参照してください。

冗長性およびリソース共有

Sourcefire 3D System の冗長性およびリソース共有の機能により、操作の継続性が保証され、複数の物理デバイスのリソースの処理を組み合わせることが可能になります。

防御センター高可用性

操作の継続性を確保するために、防御センターの*高可用性*機能を使用して、冗長な DC1000、DC1500、DC3000、または DC3500 の防御センターでデバイスを管理するよう指定することができます。イベント データは、管理対象デバイスから両方の防御センターへストリームされます。いくつかの設定要素は、両方の防御センターで保持されます。一方の防御センターで障害が発生した場合、他方の防御センターの使用を中断せずにネットワークを監視することができます。

デバイスのスタッキング

*デバイスのスタッキング*では、1 つのスタック構成内で 2 ～ 4 個の物理デバイスを接続することにより、ネットワーク セグメントで検査されるトラフィックの量を増やすことができます。スタック型の構成を確立する場合は、スタックされている各デバイスのリソースを、共有している 1 つの構成に統合します。

デバイスのクラスタリング

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

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

X-シリーズの Sourcefire ソフトウェア の冗長性

Sourcefire 3D System を使用して X-シリーズの Sourcefire ソフトウェア をクラスタ化することはできませんが、X-シリーズの Sourcefire ソフトウェア パッケージをインストールするときに冗長性を設定することができます。詳細については、『*Sourcefire Software for X-Series Installation Guide*』を参照してください。

ネットワーク トラフィックの管理

Sourcefire 3D System のネットワーク トラフィック管理機能では、管理対象デバイスを組織のネットワーク インフラストラクチャの一部として機能させることができます。ユーザは、スイッチド、ルーテッド、または（この両者を組み合わせた）ハイブリッドの環境内で機能するよう シリーズ 3 のデバイスを設定し、ネットワーク アドレス変換（NAT）を実行することができます。また、安全な仮想プライベート ネットワーク（VPN）トンネルを構築することができます。

スイッチング

複数のネットワーク セグメントの間でパケットのスイッチングが可能になるように、レイヤ 2 の展開で Sourcefire 3D System を設定することができます。レイヤ 2 の展開では、スタンドアロンのブロードキャスト ドメインとして動作するよう、管理対象デバイス上でスイッチド インターフェイスおよび仮想スイッチを設定します。仮想スイッチは、ホストの MAC アドレスを使用してパケットの送信先を決定します。

ルーティング

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

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

Sourcefire アプライアンスの設定で仮想スイッチと仮想ルータの両方を使用する場合は、それらの 2 つの間でトラフィックをブリッジするように関連付けられているハイブリッド インターフェイスを設定できます。これらのユーティリティはトラフィックを分析し、そのタイプと適切な応答（ルート、スイッチ、またはそれ以外）を判断します。

NAT

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

VPN

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

FireSIGHT

FireSIGHT™ は Sourcefire のディスカバリおよび認識テクノロジーで、ユーザがネットワークの全容を理解できるようにするために、ホスト、オペレーティング システム、アプリケーション、ユーザ、ファイル、ネットワーク、地理情報、および脆弱性に関する情報を収集します。

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

アクセス制御

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

- すべてのトラフィックをネットワークに入ることができないようにブロックする
- ネットワークに入るすべてのトラフィックを詳細な検査なしで信頼する
- すべてのトラフィックがネットワークに入ることを許可し、ネットワーク ディスカバリ ポリシーのみを使用してトラフィックを検査する
- すべてのトラフィックがネットワークに入ることを許可し、侵入およびネットワーク ディスカバリ ポリシーを使用してトラフィックを検査する

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

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

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

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

侵入検知と侵入防御

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

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

侵入ポリシーには、次のようなさまざまなコンポーネントが含まれています。

- プロトコル ヘッダー値、ペイロードの内容、特定のパケット サイズの特性を検査するルール
- FireSIGHT の推奨事項に基づいたルール状態の設定
- プリプロセッサやその他の検出、パフォーマンス機能などの詳細設定
- プリプロセッサのルール（これにより、関連付けられているプリプロセッサおよびプリプロセッサのオプションについてイベントを生成できる）

ファイルの追跡、コントロール、マルウェア防御

マルウェアの影響を特定し、軽減することを容易にするために、Sourcefire 3D System のファイル制御、ネットワーク ファイルのトラジェクトリ、および高度なマルウェア防御のコンポーネントはネットワーク トラフィック内のファイルの伝送を（マルウェア ファイルも含めて）検出、追跡、取得、分析、およびオプションでブロックすることができます。

ファイル制御

*ファイル制御*により、管理対象デバイスは、ユーザが特定のアプリケーション プロトコルを介して特定のタイプのファイルをアップロード（送信）またはダウンロード（受信）するのを検出およびブロックすることができます。ファイル制御をアクセス制御設定全体の一部として設定することができます。アクセス制御ルールに関連付けられているファイル ポリシーは、ルールの条件に一致するネットワーク トラフィックを検査します。

ネットワークベースの高度なマルウェア防御（AMP）

ネットワークベースの*高度なマルウェア防御*（AMP）を使用して、システムはネットワーク トラフィックでいくつかのファイル タイプ（PDF、Microsoft Office の多数のドキュメント、その他のタイプなど）でマルウェアを検査することができます。マルウェアが検出されると、管理対象デバイスはこれらのファイルを手動で分析するためにハード ドライブまたはマルウェアのストレージ パックに保存することができます。デバイスがファイルを保存するかどうかに関係なく、デバイスは*動的分析*のためにファイルを Sourcefire のクラウドへ送信することが可能です。また、防御センターは以下の結果に基づいて、ファイルの性質を割り当てます。

- マルウェアのクラウド ルックアップ、または*動的分析*の結果（脅威スコア）
- ファイルの*クリーン リスト*
- ファイルの*カスタム検出リスト*

管理対象デバイスはこの情報を使用してファイルをブロックまたは許可します。

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

FireAMP の統合

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

組織に FireAMP のサブスクリプションがある場合は、個々のユーザが自身のコンピュータおよびモバイル 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。これらの軽量なエージェントは Sourcefire クラウドと通信し、これが防御センターと通信します。防御センターをクラウドに接続するように設定した後で防御センターの Web インターフェイスを使用して、組織のエンドポイントでのスキャン、検出、および検疫の結果として生成されたエンドポイントベースのマルウェア イベントを表示することができます。

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

ネットワーク ファイルのトラジェクトリ

ネットワーク ファイルのトラジェクトリ機能により、ネットワークにおけるファイルの伝送経路を追跡することができます。システムは SHA-256 ハッシュ値を使用してファイルを追跡するため、ファイルを追跡するには、システムで以下のいずれかの処理を行う必要があります。

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

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

アプリケーション プログラミング インターフェース

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

eStreamer

Event Streamer（eStreamer）では、Sourcefire のアプライアンスからカスタム開発のクライアント アプリケーションへ、いくつかの種類のイベント データをストリームすることができます。クライアント アプリケーションを作成したら、ユーザはそれを eStreamer サーバ（防御センターまたは管理対象デバイス）に接続し、eStreamer サービスを開始して、データのやりとりを始めることができます。

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

外部データベースのアクセス

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

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

ホスト入力

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

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

修復

システムには API が含まれており、ユーザはこれを使用して*修復*を作成することができます。ネットワークの条件が、関連付けられている相関ポリシーまたはコンプライアンス ホワイトリストに違反したときに防御センターが自動的に修復を起動できます。これにより、ユーザが攻撃に即時に対処できない場合でも攻撃の影響を自動的に緩和でき、またシステムが組織のセキュリティ ポリシーに準拠し続けるようにすることができます。ユーザが作成する修復のほかに、防御センターにはいくつかの事前定義された修復モジュールが付属しています。

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ためには、保護された内部ネットワークに防御センターをインストールする必要があります。防御センターは、使用可能なサービスとポートのうち必要なもののみを持つように設定されていますが、攻撃がファイアウォールの外から侵入して、ここまで到達できないことを確認する必要があります。

防御センターと管理対象デバイスが同じネットワーク上に存在している場合は、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することができます。これにより、ユーザは防御センターからデバイスを安全に制御し、管理対象デバイスのネットワーク セグメント上で生成されたイベント データを集約することができます。防御センターのフィルタリング機能を使用して、ネットワーク全体で攻撃のデータを分析して相関付け、セキュリティ ポリシーが適切に実装されているかを評価することができます。

ただし、Sourcefire 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に設定されていることに注意してください。Sourcefire 3D System の機能には、この直接接続が必要なものと、プロキシ サーバの使用をサポートするものとがあります。またシステムでは、アプライアンスの Web インターフェイスにアクセスできるようにするため、および基本的なアプライアンス内通信のために、特定のポートをオープンなままにしておく必要があります。デフォルトでは、システムが追加の機能を利用できるようにするために、他のいくつかのポートがオープンになっています。

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.30）
- 「オープンな通信ポートの要件」（P.32）

インターネット アクセスの要件

デフォルトでは、Sourcefire 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に設定されています。Sourcefire 3D System の一部の機能では、この直接接続が必要です。ただし、このような機能はすべてプロキシ サーバの使用をサポートしています。『*Sourcefire 3D SystemUser Guide*』の「Configuring Network Setting」を参照してください。

ヒント! ユーザは、システム ソフトウェア、侵入ルール、GeoDB、VDB の更新をアプライアンスへ手動でアップロードすることができます。

操作の継続性を確保するために、高可用性ペアの両方の防御センターがインターネットにアクセスできる必要があります。特定の機能については、プライマリ防御センターがインターネットにアクセスし、同期プロセスでセカンダリと情報を共有します。このためプライマリで障害が発生した場合は、『*Sourcefire 3D System User Guide*』の「Monitoring and Changing High Availability Status」に記載されているように、セカンダリをプライマリにプロモートする必要があります。

次の表では、Sourcefire 3D System のインターネット アクセスの要件について説明します。

Sourcefire 3D System インターネット アクセスの要件

対象	インターネット アクセスの目的	高可用性の考慮事項	プロキシを使用するか
RSS フィードのダッシュボード ウィジェット	Sourcefire などの外部のソースから RSS フィード データをダウンロードする。	フィード データは同期されない。	はい
セキュリティ インテリジェンスのフィード	Sourcefire Intelligence Feed などの外部ソースから、セキュリティ インテリジェンスのフィード データをダウンロードする。	プライマリ防御センターはフィード データをダウンロードして、セカンダリと共有する。プライマリに障害が発生した場合はロールを切り替える必要がある。	はい
URL フィルタリング データ	クラウドベースの URL カテゴリおよびレピュテーション データをアクセス制御用にダウンロードし、カテゴライズされていない URL に対してルックアップを実行する。	プライマリ防御センターは URL フィルタリング データをダウンロードして、セカンダリと共有する。プライマリに障害が発生した場合はロールを切り替える必要がある。	はい
マルウェアのクラウド ルックアップ（マルウェア ライセンス取得済み）	クラウド ルックアップを実行して、ネットワーク トラフィックで検出されたファイルにマルウェアが含まれているかどうかを判断する。	ペアの防御センターはクラウド ルックアップを個別に実行するが、ファイル ポリシーは同期化されている。	はい
動的分析	マルウェア分析のためにクラウドへファイルを送信する。	ファイル ポリシーは同期化されているが、ペアの防御センターは、クラウドに対してマルウェア分析のために送信されたファイルを個別に問い合わせする。	はい

Sourcefire 3D System インターネット アクセスの要件（続き）

対象	インターネット アクセスの目的	高可用性の考慮事項	プロキシを使用するか
FireAMP の統合（FireAMP のサブスクリプション）	Sourcefire のクラウドからエンドポイントベースのマルウェア イベントを受信する。	クラウドの接続は同期されない。両方の防御センターでクラウド接続を設定する。	はい
システム、侵入ルール、GeoDB および VDB の更新	侵入ルール、GeoDB、VDB、またはシステムの更新をアプライアンスへ直接ダウンロードするか、またはダウンロードをスケジュールする。	ルール、GeoDB および VDB の更新は同期化されているが、システムの更新は同期化されていない。更新をダウンロードするすべてのアプライアンスは、インターネットにアクセスできる必要がある。	はい
IP アドレスのコンテキスト メニューを使用した whois 情報の取得	whois 情報を取得する。	whois 情報を要求するすべてのアプライアンスがインターネットにアクセスできる必要がある。	はい

オープンな通信ポートの要件

Sourcefire 3D System では、ユーザがアプライアンスの Web インターフェイスへアクセスできるようにするため、および基本的なアプライアンス内通信のためにポート 443（受信）および 8305（受信および送信）をオープンにしておく必要があります。

デフォルトでは、システムが追加の機能を利用できるようにするために、他のいくつかのポートがオープンになっています。次の表に、これらのポートを示します。ポート 67 と 68 では DHCP がデフォルトで無効になっていることに注意してください。

Sourcefire 3D System のオープンな通信ポートの要件

ポート	説明	プロトコル	方向	ポートをオープンにする目的
22	SSH/SSL	TCP	双方向	アプライアンスに対するセキュアなリモート接続を可能にする。
25	SMTP	TCP	発信	アプライアンスから電子メール通知とアラートを送信する。
53	DNS	TCP	発信	DNS を使用する。
67、68	DHCP	UDP	発信	DHCP を使用する。**デフォルトでは無効です。**

Sourcefire 3D System のオープンな通信ポートの要件（続き）

ポート	説明	プロトコル	方向	ポートをオープンにする目的
80	HTTP	TCP	送信または双方向	RSS Feed ダッシュボード ウィジェットがリモート Web サーバ（発信）に接続できるようにする。 受信アクセスを追加することにより、防御センターは HTTP を介してカスタムおよびサードパーティのセキュリティ インテリジェンス フィードを更新し、URL のフィルタリング情報をダウンロードできるようにする。
161、162	SNMP	UDP	双方向（161）、送信（162）	SNMP ポーリング（受信）および SNMP トラップ（送信）を有効にした場合に、アクセスを提供する。
389、636	LDAP	TCP	発信	認証のためにユーザ アクティビティを追跡する。
443	HTTPS/AMQP、クラウド ルックアップ	TCP	受信または双方向	アプライアンスにアクセスする。**必須**。 送信アクセスを追加することにより、防御センターでソフトウェアの更新、VDB および GeoDB の更新、URL のフィルタリング情報、安全なセキュリティ インテリジェンス フィード、およびエンドポイントベースの（FireAMP の）マルウェア イベントをダウンロードまたは受信できるようにする。 ポート 443 を介した接続により、防御センターはクラウド ルックアップを実行して、ネットワーク トラフィックで検出されたファイルにマルウェアが含まれているかを判断する、クラウドに対して動的な分析情報を問い合わせる、ファイルのトラジェクトリを追跡する、などの処理を実行できる。 ポート 443 を介した接続により、管理対象デバイスが動的な分析のためにクラウドへファイルを送信できるようにする。
514	syslog	UDP	発信	リモート syslog サーバへアラートを送信する。
623	SOL/LOM	UDP	双方向	シリーズ 3 のアプライアンス上で Serial Over LAN（SOL）接続を使用して Lights-Out Management（LOM）を実行できるようにする。
1500、2000	データベース アクセス	TCP	受信	外部データベースへのアクセスが有効になっている場合に防御センターにアクセスする。

Sourcefire 3D System のオープンな通信ポートの要件（続き）

ポート	説明	プロトコル	方向	ポートをオープンにする目的
1812、1813	RADIUS	UDP	送信または双方向	RADIUS を使用する。受信アクセスを追加することにより、RADIUS の認証およびアカウンティングが正しく機能することが保証される。 ポート 1812 および 1813 はデフォルトであるが、他のポートを使用するよう RADIUS を設定することができる。『*Sourcefire 3D System User Guide*』の「Configuring RADIUS Connection Setting」を参照。
3306	Sourcefire ユーザ エージェント	TCP	受信	防御センターと Sourcefire ユーザ エージェント間の通信を可能にする。
8302	eStreamer	TCP	双方向	eStreamer クライアントを使用する。
8305	デバイス管理	TCP	双方向	防御センターと管理対象デバイス間で通信する。**必須**。
8307	ホスト入力クライアント	TCP	双方向	防御センターとホスト入力クライアント間の通信を可能にする。
32137	マルウェアのクラウド ルックアップ（レガシー、オプション）	TCP	双方向	防御センターでクラウド ルックアップを実行して、ネットワーク トラフィックで検出されたファイルにマルウェアが含まれているかどうかを判断し、ファイルのトラジェクトリを追跡することができるようにする。

ドキュメント リソース

Sourcefire 3D System のドキュメント セットには、オンライン ヘルプと PDF ファイルが含まれています。ユーザは次の 2 つの方法でオンライン ヘルプを使用できます。

- 各ページで状況依存ヘルプのリンクをクリックする
- [Help] > [Online] を選択する

オンライン ヘルプには、Web インターフェイスで完了できるタスクに関する情報（ユーザ管理、システム管理、イベント分析の手順や概念的な情報など）が含まれています。

ドキュメントの CD には、以下の内容の PDF が含まれています。

- *Sourcefire 3D System User Guide*（オンライン ヘルプと同じ内容が含まれていますが、印刷が簡単な形式）
- *Sourcefire 3D System Installation Guide*（Sourcefire のアプライアンスをインストールするための情報、およびハードウェア仕様特有の情報と安全に関する情報が含まれる）
- *Sourcefire 3D システム仮想インストール ガイド*（仮想デバイスおよび仮想防御センターのインストール、管理、およびトラブルシューティングに関する情報が含まれる）
- *Sourcefire Software for X-Series Installation Guide*（X-シリーズの Sourcefire ソフトウェア のインストール、管理、およびトラブルシューティングに関する情報が含まれる）
- 各種の API ガイドおよび補足資料

Sourcefire のサポート サイト（https://support.sourcefire.com/）で PDF ドキュメントマニュアルの最新バージョンを入手できます。

ドキュメントの表記規則

このドキュメントには、各機能に対して Sourcefire 3D System のどのライセンスとアプライアンス モデルが必要か、各手順を完了するための権限を持っているのはどのユーザ ロールかについての情報が含まれています。詳細については、次の項を参照してください。

- 「ライセンスの表記規則」（P.35）
- 「サポートされるデバイスと防御センターの表記規則」（P.37）
- 「アクセスの表記規則」（P.37）

ライセンスの表記規則

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

FireSIGHT

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

防御センターが以前にバージョン 4.10.x を実行していた場合は、FireSIGHT ライセンスの代わりに古い RNA Host および RUA User ライセンスを使用できる可能性があります。

保護

保護ライセンスでは、管理対象デバイスで侵入の検出および防御、ファイル制御、セキュリティ インテリジェンスのフィルタリングを実行することができます。

制御

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

URL フィルタリング

URL フィルタリング ライセンスでは、管理対象デバイスが定期的に更新されるクラウドベースのカテゴリおよびレピュテーション データを使用して、監視対象ホストが要求した URL に基づいて、ネットワークを通貨できるトラフィックを判別できます。URL フィルタリング ライセンスには保護ライセンスが必要です。

マルウェア

マルウェア ライセンスでは、管理対象デバイスがネットワークベースの高度なマルウェア防御（AMP）を実行できます。これは、ネットワーク上で転送されるファイルに含まれるマルウェアを検出、取得、およびブロックし、動的な分析のためにこれらのファイルを送信することができる機能です。また、ネットワーク上で転送されるファイルを追跡するトラジェクトリを表示することもできます。マルウェア ライセンスには保護ライセンスが必要です。

VPN

VPN ライセンスでは、Sourcefire の管理対象デバイスの仮想ルータ間で安全な VPN トンネルを構築することができます。VPN ライセンスには保護および制御ライセンスが必要です。

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

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

アーキテクチャとリソースの制限により、すべての管理対象デバイスにすべてのライセンスが適用できるわけではないことに注意してください。一般に、デバイスがサポートしていない機能のライセンスは付与できません。「アプライアンスのモデル別のサポートされる機能」（P.19）を参照してください。ユーザが使用できる機能に対してライセンスがどのような影響を与えるかについて、および古い RNA Host および RUA User ライセンスの使用についての詳細は、『*Sourcefire 3D System User Guide*』の「Understanding Licensing」を参照してください。

サポートされるデバイスと防御センターの表記規則

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

このリリースでサポートされているプラットフォームの詳細については、「アプライアンスのシリーズ、モデル、および機能について」（P.16）を参照してください。

アクセスの表記規則

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

アクセスの表記規則

アクセスの用語	意味
Access Admin	ユーザは Access Control Admin ロールを持っている必要がある
Admin	ユーザは Administrator ロールを持っている必要がある
Any	ユーザはいずれのロールを持っていてもよい

アクセスの表記規則（続き）

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

カスタム ロールを持っているユーザは、事前定義されたロールとは異なる権限セットを持つことができます。事前定義のロールを使用して、ある手順に対するアクセス要件を示す場合は、類似の権限を持つカスタム ロールもアクセス権限を持っています。カスタム ユーザ ロールの詳細については、『*Sourcefire 3D System User Guide*』の「Managing Custom User roles」を参照してください。

IP アドレスの表記規則

IPv4 Classless Inter-Domain Routing（CIDR）の表記、および IPv6 の類似のプレフィックス長の表記を使用して、Sourcefire 3D System の多数の個所におけるアドレス ブロックを定義することができます。

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

CIDR 表記の構文例

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

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

CIDR またはプレフィックス長の表記を使用して IP アドレスのブロックを指定する場合、Sourcefire 3D System は、マスクまたはプレフィックス長で指定されたネットワーク IP アドレスの部分**のみ**を使用します。たとえば、10.1.2.3/8 と入力した場合、Sourcefire 3D System では 10.0.0.0/8 が使用されます。

つまり Sourcefire は、CIDR またはプレフィックス長の表記を使用する場合に、ビット境界上でネットワーク IP アドレスを使用する標準の方法を推奨していますが、Sourcefire 3D System ではこれは必要ありません。

アプライアンスへのログイン

ライセンス: 任意

防御センターには Web ベースのインターフェイスが用意されており、これを使用して管理および分析のタスクを実行することができます。物理管理対象デバイスは Web ベースの制限されたインターフェイスを備えており、これによって、初期設定および基本的な分析と設定のタスクを実行できます。仮想管理対象デバイスおよび X-シリーズの Sourcefire ソフトウェア には Web インターフェイスがありません。ユーザは Web ブラウザを使用してアプライアンスにログインして、Web インターフェイスにアクセスすることができます。ブラウザ要件の詳細については、リリース ノートで Sourcefire 3D System のこのバージョンについて参照してください。

インストール後にアプライアンスに最初にログインするユーザは、管理ユーザ アカウント（`admin`）を使用してログインし、初期設定プロセスを完了する必要があります。これについては、『*Sourcefire 3D System Installation Guide*』に記載されています。『*Sourcefire 3D System User Guide*』の「Adding New User Accounts」に記載されているとおりに他のユーザ アカウントを作成した後は、自分自身と他のユーザはこれらのアカウントを使用して Web インターフェイスにログインする必要があります。

重要! Sourcefire のアプライアンスはユーザ アカウントに基づいてユーザ アクティビティを監査するため、ユーザが正しいアカウントでシステムにログインしていることが保証されます。

アプライアンスにログインすると、ユーザがアクセスできる機能は、対象のユーザ アカウントに付与されている権限によって制御されます。ただし、アプライアンスに対するログインおよびログアウトの手順は変わりません。ログイン時に組織で SecurID® トークンを使用している場合は、SecurID PIN にトークンが付加され、ログインするためのパスワードとして使用されます。たとえば、PIN が `1111` で SecurID トークンが `222222` の場合は、`1111222222` と入力します。

警告! 誤った資格情報を複数回指定すると、シェルのアクセス アカウントがロックされることがあります。アカウントがロックされている場合でも、資格情報を再度入力するよう促されます。正しい資格情報を入力しているのにログインが拒否される場合は、ログインを繰り返さずに、システム管理者に連絡してください。

Web セッションでアプライアンスのホーム ページに初めてアクセスするユーザは、そのアプライアンスの最後のログイン セッション情報を表示することができます。最後のログインについて、次の情報を表示できます。

- ログインの年、月、日、曜日
- ログイン時のアプライアンスのローカル時間（24 時間表記）
- アプライアンスにアクセスするために最後に使用されたホストとドメイン名

デフォルトでは、ユーザがセッションからタイムアウトされないと設定されていない限り、非活動の状態が 1 時間経過した後で、自動的にセッションからユーザがログアウトされます。Administrator ロールを持つユーザは、システム ポリシーでセッションのタイムアウト間隔を変更できます。詳細については、『*Sourcefire 3D System User Guide*』の「Managing User Login Settings and Configuring User Interface Settings」を参照してください。

プロセスの中には長時間かかるものがあります。このため、Web ブラウザで、スクリプトが応答しなくなっていることを示すメッセージが表示されることがあります。このような場合は、プロセスが完了してからスクリプトを続行するようにしてください。

Web インターフェイスを使用してアプライアンスにログインするには：

アクセス： Any

1. ブラウザで `https://`*`hostname`*`/` にアクセスします。ここで *`hostname`* はアプライアンスのホスト名を表します。

   ログイン ページが表示されます。

2. [Username] および [Password] フィールドで、ユーザ名とパスワードを入力します。ユーザ名では、大文字と小文字が区別されます。

   企業で SecurID を使用している場合、SecurID トークンが SecurID PIN の末尾に付加され、ログイン時にパスワードとして使用されます。Sourcefire 3D System にログインする前に、自身の SecurID PIN を生成しておく必要があります。

3. [Login] をクリックします。

   デフォルトの開始ページが表示されます。ユーザ アカウントに対して新しいホーム ページを選択した場合は、代わりにそのページが表示されます。詳細については、『*Sourcefire 3D System User Guide*』の「Specifying Your Home Page」を参照してください。

   ページの上部に表示されるメニューおよびメニュー オプションは、ユーザ アカウントの権限によって異なります。ただし、デフォルト ホームページのリンクには、ユーザ アカウントの権限の範囲に対応するオプションが含まれています。アカウントに付与されている権限とは異なる権限が必要なリンクをクリックすると、次の警告メッセージが表示されます。

```
You are attempting to view an unauthorized page.This
activity has been logged.
```

提供されるメニューから別のオプションを選択するか、またはブラウザ ウィンドウで [Back] をクリックします。

コマンド ラインを介して シリーズ 3 または仮想デバイスにログインするには：

アクセス： CLI の基本設定

1. *`hostname`* でアプライアンスに対する SSH 接続を開きます。ここで *`hostname`* はアプライアンスのホスト名を表します。

   `login as:` コマンド プロンプトが表示されます。

2. ユーザ名を入力して Enter キーを押します。

   [Password:] プロンプトが表示されます。

3. パスワードを入力して Enter キーを押します。

   ログイン バナーが表示され、その後に **>** プロンプトが示されます。

   コマンド ライン アクセスのレベルで許可されている任意のコマンドを使用できます。使用できる CLI コマンドの詳細については、『*Sourcefire 3D System User Guide*』の「Command Line Reference」を参照してください。

アプライアンスにログインしてアカウントを設定する

ライセンス: Any

ユーザ アカウントの中には、外部の認証サーバを介して認証されるものもあります。LDAP または RADIUS 資格情報を使用して Sourcefire 3D System にログオンすることを組織で許可している場合、外部のユーザ資格情報を使用してアプライアンスに初めてログインすると、アプライアンスではローカル ユーザ レコードを作成し、これらの資格情報を権限セットに関連付けます。ローカル ユーザ レコードの権限は、以下のようにグループまたはリストのメンバーシップ全体に付与されている場合を除いて、変更することができます。

- 外部認証されているユーザ アカウントのデフォルト ロールが特定のアクセス ロールに設定されている場合、ユーザは（システム管理者による追加の設定なしで）外部のアカウント資格情報を使用してアプライアンスにログインすることができます。
- アカウントが外部で認証されており、デフォルトではアクセス権が付与されない場合、ログインはできますが機能にはアクセスできません。ユーザ（またはシステム管理者）は、ユーザ機能へ適切なアクセス権を付与する権限を変更することができます。

シェル アクセス ユーザの場合、システムはアプライアンス上にローカル ユーザ アカウントを作成しません。シェル アクセスは、シェル アクセス フィルタ、または LDAP サーバに設定されている PAM ログイン属性、あるいは RADIUS サーバ上のシェル アクセスリストによってすべて制御されます。

シェル ユーザは、小文字、大文字、または小文字と大文字が混在するユーザ名を使用してログインすることができます。シェルのログイン認証では大文字と小文字が区別されます。LDAP ユーザ名には、下線（_）、ピリオド（.）、ハイフン（-）を使用することができますが、それ以外では英数字しかサポートされていません。

ログイン時に組織で SecurID トークンを使用している場合は、SecurID PIN にトークンが付加され、ログインするためのパスワードとして使用されます。たとえば、PIN が `1111` で SecurID トークンが `222222` の場合は、`1111222222` と入力します。

重要! Web インターフェイスにアクセスする権限を持っていない場合は、システム管理者に連絡してアカウントの権限を変更してもらうか、Administrator のアクセス権を持つユーザとしてログインし、対象のアカウントの権限を変更します。詳細については、『*Sourcefire 3D System User Guide*』の「Modifying User Privileges and Options」を参照してください。

外部で認証されたアカウントをアプライアンスに作成するには：

アクセス： Any

1. ブラウザで `https://`*`hostname`*`/` にアクセスします。ここで *`hostname`* はアプライアンスのホスト名を表します。

   ログイン ページが表示されます。

2. [Username] と [Password] のフィールドに値を入力します。

   重要! 企業で SecurID を使用している場合、SecurID トークンが SecurID PIN に付加され、ログイン時にパスワードとして使用されます。

3. [Login] をクリックします。

   表示されるページは、外部認証のデフォルト アクセス ロールによって異なります。

   - 認証オブジェクトまたはシステム ポリシーでデフォルトのアクセス ロールを選択した場合は、デフォルトの開始ページが表示されます。ユーザ アカウントに対して新しいホーム ページを選択した場合は、代わりにそのページが表示されます。詳細については、『*Sourcefire 3D System User Guide*』の「Specifying Your Home Page」を参照してください。

     ページの上部に表示される使用可能なメニューおよびメニュー オプションは、ユーザ アカウントの権限によって異なります。ただし、デフォルト ホームページのリンクには、ユーザ アカウントの権限の範囲に対応するオプションが含まれています。アカウントに付与されている権限とは異なる権限が必要なリンクをクリックすると、次の警告メッセージが表示されます。

     ```
     You are attempting to view an unauthorized page. This
     activity has been logged.
     ```

     提供されるメニューから別のオプションを選択するか、またはブラウザ ウィンドウで [Back] をクリックします。

   - デフォルトのアクセス ロールを選択していない場合は、[Login] ページが再表示され、次のエラー メッセージが示されます。

     ```
     Unable to authorize access. If you continue to have
     difficulty accessing this device, please contact the system
     administrator.
     ```

   認証方法として、属性の一致を使用する RADIUS サーバを使用する場合、ユーザ アカウントが作成されているため、最初のログインは拒否されます。もう一度ログインする必要があります。

アプライアンスからのログアウト

ライセンス: Any

Web インターフェイスをアクティブに使用しなくなった場合、Sourcefire では、少しの間 Web ブラウザから離れるだけであっても、ログアウトすることを推奨しています。ログアウトによって Web セッションが終了し、自分の資格情報を使用して他のユーザがアプライアンスを使用できないようになります。

デフォルトでは、ユーザがセッションからタイムアウトされないと設定されていない限り、非活動の状態が 1 時間経過した後で、自動的にセッションからユーザがログアウトされます。Administrator ロールを持つユーザは、システム ポリシーでセッションのタイムアウト間隔を変更できます。詳細については、『*Sourcefire 3D System User Guide*』の「Managing User Login Settings and Configuring User Interface Settings」を参照してください。

アプライアンスからログアウトするには：

アクセス： Any

▶ ツールバーの [Logout] をクリックします。

コンテキスト メニューの使用

ライセンス: 機能によって異なる

操作の利便性を高めるため、Web インターフェイスのいくつかのページではポップアップ コンテキスト メニューをサポートしています。これを使用して、Sourcefire 3D System の他の機能へショートカットでアクセスすることができます。メニューの内容は*ホットスポット*によって異なり、ユーザはページだけでなく特定のデータにアクセスすることもできます。

たとえば、イベント ビューの *IP アドレス ホットスポット*、侵入イベントのパケット ビュー、ダッシュボード、および Context Explorer には追加のオプションがあります。アドレスに関連付けられているホストの詳細（使用可能な whois やホスト プロファイルの情報など）を知るには、ホットスポットを右クリックして [IP address] コンテキスト メニューを使用します。（セキュリティ インテリジェンスのフィルタリングをサポートしていない）DC500 防御センターを除いては、セキュリティ インテリジェンスのグローバル ホワイトリストまたはブラックリストに個別の IP アドレスを追加することもできます。

別の例として、イベント ビューおよびダッシュボードの *SHA-256 値のホットスポット*では、ファイルの SHA-256 ハッシュ値をクリーン リストまたはカスタム検出リストに追加したり、コピーするためにハッシュ値全体を表示したりできます。この機能は、DC500 防御センターではサポートされていないことに注意してください。

次の一覧では、Web インターフェイスのさまざまなページのコンテキスト メニューで使用できるオプションについて説明しています。Sourcefire コンテキスト メニューがサポートされていないページまたは場所では、ブラウザの標準のコンテキスト メニューが表示されます。

アクセス制御ポリシー エディタ

アクセス制御ポリシー エディタには、各アクセス制御ルールのホットスポットが含まれます。コンテキスト メニューを使用して、新しいルールとカテゴリの挿入、ルールのカット、コピー、および貼り付け、ルール状態の設定、およびルールの編集を行うことができます。

NAT ポリシー エディタ

NAT ポリシー エディタには、各 NAT ルールのホットスポットが含まれます。コンテキスト メニューを使用して、新しいルールの挿入、ルールのカット、コピー、および貼り付け、ルール状態の設定、およびルールの編集を行うことができます。

侵入ルール エディタ

侵入ルール エディタには、各侵入ルールのホットスポットが含まれます。コンテキスト メニューを使用して、ルールの編集、ルール状態の設定（ルールの無効化を含む）、しきい値と抑制のオプションの設定、およびルールのドキュメントの表示を行うことができます。

イベント ビューア

イベント ページ（ドリルダウン ページとテーブル ビュー）には、各イベント、IP アドレス、および特定の検出ファイルの SHA-256 ハッシュ値のホットスポットが含まれます。ほとんどのイベント タイプでは、コンテキスト メニューを使用して、Context Explorer で関連情報を表示したり、イベントの情報について新しいウィンドウでドリルダウンしたりできます。ファイルの SHA-256 ハッシュ値、脆弱性の説明、URL などの、イベント フィールドに含まれているテキストが長すぎて、イベント ビューですべて表示できない場合、コンテキスト メニューを使用してテキスト全体を表示することができます。

取得されたファイル、ファイル イベント、およびマルウェア イベントに対して、コンテキスト メニューを使用してファイルをクリーン リストまたはカスタム検出リストに追加する、クリーン リストまたはカスタム検出リストからファイルを削除する、ファイルのコピーをダウンロードする、動的分析のためにファイルをクラウドへ送信する、などの処理を実行できます。

侵入イベントに対しても、コンテキスト メニューを使用して、侵入ルール エディタまたは侵入ポリシーで実行できるものと類似のタスクを実行できます。これには、ルール状態を設定する（ルールの無効化を含む）、しきい値と抑制のオプションを設定する、ルールのドキュメントを表示するなどのタスクがあります。

パケット ビュー

侵入イベントのパケット ビューには、IP アドレスのホットスポットが含まれます。パケット ビューでは、右クリック メニューではなく、左クリックのコンテキスト メニューを使用することに注意してください。

ダッシュボード

多くのダッシュボード ウィジェットには、関連する情報を Context Explorer で表示するためのホットスポットが含まれます。ダッシュボード ウィジェットには、IP アドレスと SHA-256 の値のホットスポットを含めることができます。

Context Explorer

Context Explorer には、図、表、およびグラフのホットスポットが含まれます。Context Explorer よりも詳細なグラフまたはリストのデータを調べたい場合は、関連するデータのテーブル ビューにドリルダウンすることができます。また、関連するホスト、ユーザ、アプリケーション、ファイル、および侵入ルールの情報を表示できます。

Context Explorer でも左クリックのコンテキスト メニューを使用することに注意してください。これには、Context Explorer に特有のフィルタリングおよび他のオプションも含まれています。詳細については、『*Sourcefire 3D System User Guide*』の「Drilling Down on Context Explorer Data」を参照してください。

コンテキスト メニューにアクセスするには：

アクセス： Any

1. Web インターフェイスのホットスポット対応ページで、ポインタをホットスポットに合わせます。

   Context Explorer を除いて、「`Right-click for menu`」というメッセージが表示されます。

2. コンテキスト メニューを起動します。
   - Context Explorer またはパケット ビューでは、ポインティング デバイスを左クリックします。
   - ホットスポット対応の他のすべてのページでは、ポインティング デバイスを右クリックします。

   ポップアップ コンテキスト メニューが表示され、ホットスポットに適したオプションが示されます。

3. オプションの名前を左クリックして、いずれかのオプションを選択します。

   アクセス制御ポリシー エディタまたは NAT ポリシー エディタを使用している場合は、ルールが変更されます。それ以外の場合は、選択したオプションに基づいて新しいブラウザ ウィンドウが開きます。