SOURCEFIRE 3D SYSTEM リリース ノート

バージョン 5.3.0.1

初版：2014 年 4 月 21 日
最終更新日：2015 年 3 月 18 日

このリリース ノートは、Sourcefire 3D System バージョン 5.3.0.1 に適用されます。更新プロセスについて理解している場合でも、これらのリリース ノートをよく読み理解してください。リリース ノートには、サポートされているプラットフォーム、新機能および変更された機能、既知の問題と解決済みの問題、製品と Web ブラウザの互換性について説明されています。また、次のアプライアンスの前提条件、警告、および特定のインストールおよびアンインストール手順の詳細も含まれています。

- シリーズ 2 および シリーズ 3 防御センター（DC500、DC750、DC1000、DC1500、DC3000 および DC3500）
- シリーズ 2 および シリーズ 3 管理対象デバイス（3D500、3D1000、3D2000、3D2100、3D2500、3D3500、3D4500、3D6500、7000 Series、8000 Series、3D9900、AMP7150 および AMP8150）
- Sourcefire Software for X-Series
- 64 ビット仮想防御センターおよび管理対象デバイス

ヒント Sourcefire 3D System の詳細については、オンライン ヘルプを参照するか、サポート サイトから『*Sourcefire 3D System User Guide*』をダウンロードしてください。

Sourcefire 3D System のバージョン 5.3 以上を実行しているアプライアンスをバージョン 5.3.0.1 に更新するには、「アプライアンスの更新」（P.6）で説明する手順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。

- 「変更された機能」（P.2）
- 「Sourcefire マニュアルの更新」（P.2）
- 「はじめに：重要な更新と互換性に関する注意事項」（P.3）
- 「アプライアンスの更新」（P.6）
- 「更新のアンインストール」（P.18）
- 「バージョン 5.3.0.1 で解決された問題」（P.25）
- 「既知の問題」（P.31）
- 「以前のバージョンで導入された機能」（P.37）
- 「サポート」（P.46）

変更された機能

次のリストで、Sourcefire 3D System の既存の機能に対する変更点を説明します。

- バージョン 5.3.0.1 では、LDAP ユーザ名の大文字と小文字が区別されません。バージョン 5.3 では、ユーザ名の大文字と小文字が区別されていました。
- データベースに対するクエリの実行時に、`application_host_map` 表の `application_tag_id` フィールドを使用した結合は実行できなくなりました。

Sourcefire マニュアルの更新

バージョン 5.3.0.1 では次のマニュアルが更新され、新機能の追加と変更された機能を反映し、報告されているマニュアルの問題に対応しました。

- *Sourcefire 3D System User Guide*
- *Sourcefire 3D System Online Help*
- *Sourcefire 3D System Installation Guide*
- *Sourcefire 3D System Virtual Installation Guide*
- *Sourcefire Software for X-Series Installation and Configuration Guide*
- *Sourcefire 3D System eStreamer Integration Guide*
- *Sourcefire 3D System Qualys Connector Guide*
- *Sourcefire 3D System Database Access Guide*
- *Sourcefire 3D System Host Input API Guide*

- *Sourcefire DC750 Quick Start Guide*
- *Sourcefire DC1500 Quick Start Guide*
- *Sourcefire DC3500 Quick Start Guide*
- *Sourcefire 7000 Series Devices Quick Start Guide*
- *Sourcefire 8000 Series Devices Quick Start Guide*

最新のマニュアルはすべて Sourcefire サポート サイトからダウンロードできます。

はじめに：重要な更新と互換性に関する注意事項

バージョン 5.3.0.1 の更新プロセスを開始する前に、更新プロセスの実行中および実行後のシステムの動作、互換性の問題、および更新前および更新後に行う必要がある設定の変更を理解しておいてください。

警告　Sourcefire では、更新を保守期間中に行うか、または中断による展開環境への影響が最も小さい時点で行うことを**強く**推奨します。

詳細については、次の項を参照してください。

- 「設定とイベントのバックアップのガイドライン」（P.3）
- 「更新中のトラフィック フローとトラフィック検査」（P.4）
- 「製品互換性」（P.5）

設定とイベントのバックアップのガイドライン

Sourcefire は、更新を開始する前に、現行のイベントおよび設定データを外部ロケーションにバックアップすることを**強く**推奨します。これらのデータは、更新プロセスの一部としてバックアップ**されません**。

防御センターを使用して、それ自体のイベント データと設定データ、および管理対象デバイスのイベント データと設定データをバックアップします。バックアップおよび復元機能の詳細については、『*Sourcefire 3D System User Guide*』を参照してください。

重要　防御センターは以前の更新で作成したバックアップを消去破棄します。保存されたバックアップを保持するには、そのバックアップを外部に保存します。

更新中のトラフィック フローとトラフィック検査

更新プロセス（および更新のアンインストール）により、管理対象デバイスは再起動します。デバイスの設定方法と展開方法に応じて、次の機能に影響が及びます。

- トラフィック検査（アプリケーションの認知と制御、URL フィルタリング、セキュリティ インテリジェンス、侵入検出および防御、接続のロギングを含む）
- トラフィック フロー（スイッチング、ルーティング、NAT、VPN、関連機能を含む）
- リンク ステート

クラスタ デバイスを更新する際、システムはトラフィックの中断を避けるために一度に 1 台のデバイスの更新を実行することに注意してください。

トラフィック検査およびリンク ステート

インライン展開では、管理対象デバイス（モデルによって異なる）がアプリケーション制御、ユーザ制御、URL フィルタリング、セキュリティ インテリジェンス、侵入防御、スイッチング、ルーティング、NAT、および VPN を介してトラフィック フローに影響を与えることがあります。パッシブ展開では、ネットワーク トラフィック フローに影響を与えることなく侵入検出を実行し、ディスカバリ データを収集できます。アプライアンスの機能の詳細については、『*Sourcefire 3D System Installation Guide*』を参照してください。

次の表に、トラフィック フロー、トラフィック検査、リンク ステートが、展開に応じて更新中にどのような影響を受けるかの詳細を示します。インライン設定方法に関係なく、スイッチング、ルーティング、NAT、および VPN は、更新プロセス中に実行**されない**ことに注意してください。

ネットワーク トラフィックの中断

展開	ネットワーク トラフィックが中断されたか
設定可能なバイパスを持つインライン （インライン設定に対して有効にされた**設定可能なバイパス**オプション）	ネットワーク トラフィックは、更新時に 2 つの時点で中断されます。 • 更新プロセスの開始時に、リンクがダウンしてから復旧（フラップ）し、ネットワーク カードがハードウェア バイパスに切り替わる間にトラフィックが一時的に中断します。トラフィックは、ハードウェア バイパスでは検査されません。 • 更新が終了すると、リンク フラップとネットワーク カードがバイパスから切り替わる間にトラフィックが再度一時的に中断されます。エンドポイントがセンサのインターフェイスに再接続し、リンクが再確立された後、トラフィックは再度検査されます。 **重要**：設定可能なバイパス オプションは、仮想デバイス、Sourcefire Software for X-Series デバイスの非バイパス NetMod、または 8000 Series デバイスの SFP トランシーバではサポートされて**いません**。
インライン	ネットワーク トラフィック更新中にわたってブロックされます。
パッシブ	ネットワーク トラフィックは更新時に中断されませんが、検査もされません。

スイッチングおよびルーティング

管理対象デバイスは、更新時にスイッチング、ルーティング、NAT、VPN、または関連機能を実行**しません**。スイッチングとルーティングのみを実行するようにデバイスを設定した場合、ネットワーク トラフィックは更新中常にブロックされます。

製品互換性

バージョン 5.3.0.1 を実行するデバイスを管理するには、防御センターのバージョン 5.3 以上を使用する必要があります。

バージョン 5.3.0.1 を実行している防御センターは、バージョン 5.2.0.4 以上を実行している物理デバイスと仮想デバイスおよびバージョン 5.3 以上を実行している Sourcefire Software for X-Series を管理できます。

Web ブラウザの互換性

Sourcefire 3D System 用の Web インターフェイスのバージョン 5.3.0.1 は、次の表に示すブラウザでテスト済みです。

Web ブラウザの互換性

ブラウザ	必須の有効化オプションと設定
Chrome 33	JavaScript、Cookie
Firefox 27.0.1	JavaScript、cookies、Secure Sockets Layer（SSL）v3
Microsoft Internet Explorer 9 および 10	JavaScript、cookies、Secure Sockets Layer（SSL）v3、128 ビット暗号、[Active scripting] のセキュリティ設定、互換性表示、[Check for newer versions of stored pages] を [Automatically] に設定

画面解像度の互換性

Sourcefire では幅が 1280 ピクセル以上の画面解像度を選択することを推奨しています。ユーザ インターフェイスは低い解像度と互換性がありますが、より高い解像度により、表示が最適化されます。

アプライアンスの更新

Sourcefire 3D System のバージョン 5.3 以上を実行しているアプライアンスをバージョン 5.3.0.1 に更新するには、以下で説明する手順を参照してください。以下の各項で、バージョン 5.3.0.1 の更新の準備とインストールができます。

- 「更新の計画」（P.7）
- 「防御センターの更新」（P.11）
- 「管理対象デバイスおよび Sourcefire Software for X-Series の更新」（P.13）
- 「更新の実行にシェルを使用する」（P.16）

警告　ログイン プロンプトが表示されるまでは、更新中にアプライアンスを再起動したりシャット ダウンしたり**しないでください**。システムは更新の事前チェックの部分では機能していないように見えることがありますが、これは予期された動作で、アプライアンスを再起動したり、シャット ダウンしたりする必要はありません。

更新の計画

更新を始める前に、これらのリリース ノート、特に「はじめに：重要な更新と互換性に関する注意事項」（P.3）を精読し、理解する必要があります。問題なく更新プロセスを実行するためには、以下の各項も一読する必要があります。

Sourcefire 3D System バージョン要件

バージョン 5.3.0.1 に更新するには、アプライアンスがバージョン 5.3 以上を実行している必要があります。それより前のバージョンが実行されている場合、Sourcefire サポート サイトから更新を取得できます

防御センターがその管理対象デバイスをバージョン 5.3.0.1 に更新するには、バージョン 5.3.0.1 以上を実行している必要があります。

オペレーティング システムの要件

次のホスティング環境で 64 ビット仮想 Sourcefire 仮想アプライアンスをホストできます。

- VMware vSphere Hypervisor/VMware ESXi 5.0
- VMware vSphere Hypervisor/VMware ESXi 5.1
- VMware vCloud Director 5.1

詳細については、『*Sourcefire 3D System Virtual Installation Guide*』を参照してください。

XOS バージョン 9.7.2 以降およびバージョン 10.0 以降が稼働する X-Series アプライアンスで Sourcefire Software for X-Series を実行できます。詳細については、『*Sourcefire Software for X-Series Installation and Configuration Guide*』を参照してください。

時間とディスク スペース要件

次の表に、バージョン 5.3.0.1 更新のディスク容量と時間の目安を示します。管理対象デバイスを更新するために防御センターを使用するときには、防御センターの `/Volume` パーティションに追加のディスク容量が必要であることに注意してください。

更新プロセス中のどの時点でも、更新を再開始したりアプライアンスを再起動したり**しないで**ください。Sourcefire では目安として時間の見積りを提供していますが、実際の更新時間はアプライアンスのモデル、展開、および設定によって異なります。システムは更新の事前チェック部分および再起動後に機能していないように見えることがありますが、これは予期された動作です。

ヒント 更新での再起動の部分にはデータベースのチェックが含まれます。データベースのチェック中にエラーが検出された場合、更新が完了するためにはさらに時間が必要です。データベースと対話するシステム デーモンは、データベースのチェックおよび修復中は動作**しません**。

更新の進行状況で問題が発生した場合は、Sourcefire サポートに連絡してください。

時間とディスク スペース要件

アプライアンス	必要容量	ボリュームの容量	マネージャのボリューム当たりの容量	時間
シリーズ 2 防御センター	1 MB	714 MB	n/a	32 分
シリーズ 2 管理対象デバイス	1 MB	507 MB	56 MB	17 分
シリーズ 3 防御センター	1 MB	736 MB	n/a	27 分
シリーズ 3 管理対象デバイス	1 MB	863 MB	142 MB	37 分
3D9900 管理対象デバイス	1 MB	516 MB	50 MB	25 分
Sourcefire Software for X-Series	56 MB	1 MB（/分/アプリケーションのローカル ディスク）	20 MB	11 分
仮想防御センター	1 MB	736 MB	n/a	ハードウェアによって異なる
仮想管理対象デバイス	1 MB	199 MB	19 MB	ハードウェアによって異なる

設定とイベントのバックアップのガイドライン

Sourcefire は、更新を開始する前に、現行のイベントおよび設定データを外部ロケーションにバックアップすることを**強く**推奨します。これらのデータは、更新プロセスの一部としてバックアップ**されません**。

防御センターを使用して、そのイベント データと設定データ、および管理しているデバイスのイベント データと設定データをバックアップできます。バックアップおよび復元機能の詳細については、『*Sourcefire 3D System User Guide*』を参照してください。

更新を実行するタイミング

更新プロセスはトラフィック検査、トラフィック フロー、リンク ステートに影響を与える可能性があるため、Sourcefire では更新を保守期間に、または中断が展開に及ぼす影響が最小のときに実行することを**強く**推奨します。

インストール方法

更新を実行するには防御センターの Web インターフェイスを使用します。まず防御センターを更新してから、それを使用して、管理するデバイスを更新します。

インストールの順序

その管理対象デバイスを更新する前に、防御センターを更新します。

ペアの防御センターに対する更新のインストール

高可用性ペアの片方の防御センターの更新を開始すると、もう一方の防御センターがプライマリになります（まだプライマリになっていなかった場合）。また、ペアの防御センターは設定情報の共有を止めます。ペアの防御センターは、定期的な同期プロセスの一部としてソフトウェア アップデートを受信**しません**。

運用の継続性を保証するには、ペアの 防御センター を同時に更新**しないでください**。まず、セカンダリ防御センターの更新手続きを完了してから、プライマリ防御センターを更新します。

クラスタ型デバイスに対する更新のインストール

クラスタ型デバイスに更新をインストールする場合、システムは一度に 1 台のデバイスに対して更新を実行します。更新が始まると、システムはまずそれをセカンダリ デバイスに適用し、必要なすべてのプロセスが再起動してデバイスがトラフィックを再び処理するまで、そのデバイスは保守モードになります。システムは次に更新をプライマリ デバイスに適用し、プライマリ デバイスも同じプロセスをたどります。

スタック型デバイスに対する更新のインストール

スタック型デバイスで更新をインストールする場合、システムは更新を同時に実行します。各デバイスは、更新が完了すると通常の動作を再開します。次の点に注意してください。

- すべてのセカンダリ デバイスの更新が完了する*前に*プライマリ デバイスの更新が完了すると、すべてのデバイスで更新が完了するまでスタックは限定的な、バージョンが混在している状態で動作します。
- すべてのセカンダリ デバイスの更新が完了した*後に*プライマリ デバイスの更新が完了した場合、プライマリ デバイスで更新が完了した時点でスタックは通常の動作を再開します。

X-Series デバイスへの更新のインストール

バージョン 5.3.0.1 に更新するには、Sourcefire Software for X-Series でバージョン 5.3 以上を実行している必要があります。

バージョン 4.10.x を実行している Sourcefire Software for X-Series をバージョン 5.3.0.1 に更新することは**できません**。代わりに、以前のバージョンをアンインストールし、バージョン 5.3 をインストールしてからバージョン 5.3.0.1 をインストールする必要があります。詳細については、『*Sourcefire Software for X-Series Installation and Configuration Guide*』を参照してください。

Sourcefire Software for X-Series を更新すると、影響を受ける VAP がリロードされます。Sourcefire Software for X-Series がインライン展開され、複数メンバーの VAP グループを使用している場合、Sourcefire では VAP を 1 つずつ更新することを推奨しています。これにより、更新中の VAP のリロード中に、グループ内の他の VAP がネットワーク トラフィックを検査できます。インライン展開で単一 VAP の VAP グループを使用している場合、VAP をリロードするとネットワーク トラフィックが中断されます。更新は保守期間に、または更新が展開に及ぼす影響が最小のときに計画してください。

インストール後

防御センターまたは管理対象デバイスのいずれかの更新を実行した後に、デバイス設定とアクセス制御ポリシーを再適用する**必要があります**。アクセス制御ポリシーを適用すると、トラフィック フローとトラフィック処理で一時的に停止が発生したり、一部のパケットが検査なしで通過することがあります。詳細については、『*Sourcefire 3D System User Guide*』を参照してください。

環境が正常に動作していることを保証するために、ユーザが実行しなければならないいくつか追加の更新後の手順があります。次の作業を行います。

- 更新が成功したことの検証
- 環境のすべてのアプライアンスが正常に通信していることの確認
- 侵入ルールと脆弱性データベース（VDB）の更新（必要に応じて）

次の各項では、更新の実行と更新後の手順の完了に関する詳細情報を示します。これらすべてのタスクを完了してください。

防御センターの更新

仮想防御センターを含む、ご使用の防御センターを更新するには、この項の手順を使用します。バージョン 5.3.0.1 の更新では、防御センター が再起動します。

警告　防御センターを更新する前に、すべての管理対象デバイスにアクセス制御ポリシーを再適用します。そうしない場合、管理対象デバイスの最終的な更新が失敗することがあります。

警告　ログイン プロンプトが表示されるまでは、更新中にアプライアンスを再起動したりシャット ダウンしたり**しないでください**。システムは更新の事前チェックの部分では機能していないように見えることがありますが、これは予期された動作で、アプライアンスを再起動したり、シャット ダウンしたりする必要はありません。

防御センターを更新するには、次の手順に従います。

1. このリリース ノートを参照し、必要な更新前処理タスクを完了します。

   詳細については、「はじめに：重要な更新と互換性に関する注意事項」（P.3）および「更新の計画」（P.7）を参照してください。

2. 次の更新を Sourcefire サポート サイトからダウンロードします。
   - シリーズ 2 防御センターの場合：
     `Sourcefire_3D_Defense_Center_Patch-5.3.0.1-66.sh`
   - シリーズ 3 および仮想防御センターの場合：
     `Sourcefire_3D_Defense_Center_S3_Patch-5.3.0.1-66.sh`

   重要　サポート サイトから更新を直接ダウンロードします。電子メールで更新ファイルを転送すると、破損する可能性があります。

3. [System] > [Updates] を選択し、次に [Product Updates] タブで [Upload Update] をクリックして、防御センターに更新をアップロードします。更新を参照し、[Upload] をクリックします。

   更新が防御センターにアップロード されます。

4. 環境内のアプライアンスが正常に通信していること、およびヘルス モニタによって報告された問題がないことを確認します。

5. タスク キューを調べ（[System] > [Monitoring] > [Task Status]）、進行中のタスクがないことを確認します。

   更新の開始時に実行中のタスクは停止され、失敗したタスクとなり、再開できません。これらは更新が完了した後にタスク キューから手動で削除する必要があります。タスク キューは 10 秒ごとに自動的にリフレッシュされます。更新を始める前に、実行時間の長いタスクが完了するまで待つ**必要があります**。

6. [System] > [Updates] を選択します。

   [Product Updates] タブが表示されます。

7. アップロードした更新の横にあるインストール アイコンをクリックします。

   [Install Update] ページが表示されます。

8. 防御センターを選択し、[Install] をクリックします。更新をインストールすること、および防御センターを再起動することを確認します。

   更新プロセスが開始されます。タスク キュー（[System] > [Monitoring] > [Task Status]）で更新の進行状況を監視できます。

   警告　更新が完了し、防御センターが再起動するまでは、Web インターフェイスを使用して別のタスクを実行**しないでください**。更新が完了する前に、Web インターフェイスが利用できなくなり、ユーザが防御センターによりログアウトされる場合があります。これは予期される動作です。再度ログインしてタスク キューを表示してください。更新がまだ実行中の場合は、更新が完了するまで Web インターフェイスを使用**しないでください**。更新時に問題が発生した場合は（タスク キューが更新の失敗を示している、タスク キューを手動でリフレッシュしても数分間にわたって進行状況が表示されない、など）、更新を再開**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。

9. 更新が終了したら、ブラウザ キャッシュをクリアし、ブラウザでリロードを強制します。そうしない場合、ユーザ インターフェイスが予期しない動作を示すことがあります。

10. 防御センターにログインします。

11. [Help] > [About] を選択し、ソフトウェアのバージョンが正しく表示される（バージョン 5.3.0.1）ことを確認してください。また、防御センターのルール更新と VDB のバージョンもメモしてください。この情報は後で必要になります。

12. 環境内のアプライアンスが正常に通信していること、およびヘルス モニタによって報告された問題がないことを確認します。

13. サポート サイトで利用可能なルール更新が、ご使用の防御センターのルールより新しい場合は、新しいルールをインポートします。

    ルール更新の詳細については、『*Sourcefire 3D System User Guide*』を参照してください。

14. サポート サイトで利用可能な VDB が、ご使用の防御センターの VDB より新しい場合は、最新の VDB をインストールします。

    VDB 更新をインストールすると、トラフィック フローとトラフィック処理で一時的に停止が発生し、一部のパケットが検査なしで通過することがあります。詳細については、『*Sourcefire 3D System User Guide*』を参照してください。

15. すべての管理対象デバイスにデバイス設定を再適用します。

    ヒント グレーアウトされた [Apply] 再度有効にするには、デバイス設定でいずれかのインターフェイスを編集してから変更を適用せずに、[Save] をクリックしします。

16. すべての管理対象デバイスにアクセス制御ポリシーを再適用します。

    警告 侵入ポリシーは個別に再適用**しないでください**。すべてのアクセス制御ポリシーを完全に再適用する必要があります。

    アクセス制御ポリシーを適用すると、トラフィック フローとトラフィック処理で一時的に停止が発生したり、一部のパケットが検査なしで通過することがあります。詳細については、『*Sourcefire 3D System User Guide*』を参照してください。

管理対象デバイスおよび Sourcefire Software for X-Series の更新

防御センターを バージョン 5.3.0.1 に更新したら、それらを使用して、管理するデバイスを更新します。

防御センターがその管理対象デバイスをバージョン 5.3.0.1 に更新するには、バージョン 5.3.0.1 以上を実行している必要があります。Web インターフェイスがないため、Sourcefire Software for X-Series と仮想管理対象デバイスを更新するには防御センターを使用する必要があります。

管理対象デバイスの更新は、2 段階のプロセスです。まず、サポート サイトから更新をダウンロードして、管理元の防御センターにアップロードします。次に、ソフトウェアをインストールします。同じ更新ファイルを使用する場合に限り、複数のデバイスを同時に更新できます。

バージョン 5.3.0.1 の更新では、すべてのデバイスが再起動し、Sourcefire Software for X-Series VAP グループがリロードします。管理対象デバイスは、更

新時にトラフィック検査、スイッチング、ルーティング、NAT、VPN、または関連機能を実行**しません**。デバイスの設定および展開方法に応じて、更新プロセスはトラフィック フローおよびリンク ステートにも影響する場合があります。詳細については、「更新中のトラフィック フローとトラフィック検査」（P.4）を参照してください。

警告　管理対象デバイスを更新する前に、その管理元の防御センターを使用して、管理対象デバイスに適切なアクセス制御ポリシーを再適用します。そうしない場合、管理対象デバイスの更新が失敗することがあります。

警告　ログイン プロンプトが表示されるまでは、更新中にアプライアンスを再起動したりシャット ダウンしたり**しないでください**。システムは更新の事前チェックの部分では機能していないように見えることがありますが、これは予期された動作で、アプライアンスを再起動したり、シャット ダウンしたりする必要はありません。

ヒント　Sourcefire Software for X-Series がインライン展開され、複数メンバーの VAP グループを使用している場合、Sourcefire では VAP を 1 つずつ更新することを推奨しています。これにより、更新中の VAP のリロード中に、グループ内の他の VAP がネットワーク トラフィックを検査できます。インライン展開で単一 VAP の VAP グループを使用している場合、VAP をリロードするとネットワーク トラフィックが中断されます。更新は保守期間に、または更新が展開に及ぼす影響が最小のときに計画してください。

管理対象デバイスを更新するには、次の手順を実行します。

1. このリリース ノートを参照し、必要な更新前処理タスクを完了します。

   詳細については、「はじめに：重要な更新と互換性に関する注意事項」（P.3）および「更新の計画」（P.7）を参照してください。

2. デバイスの管理元の防御センターで Sourcefire ソフトウェアを更新します。「防御センターの更新」（P.11）を参照してください。

3. 次の更新を Sourcefire サポート サイトからダウンロードします。

   - シリーズ 2 管理対象デバイスの場合：
     `Sourcefire_3D_Device_Patch-5.3.0.1-66.sh`
   - シリーズ 3 管理対象デバイスの場合：
     `Sourcefire_3D_Device_S3_Patch-5.3.0.1-66.sh`

- 3D9900 管理対象デバイスの場合：
  `Sourcefire_3D_Device_x900_Patch-5.3.0.1-66.sh`
- 仮想管理対象デバイスの場合：
  `Sourcefire_3D_Device_Virtual64_VMware_Patch-5.3.0.1-66.sh`
- Sourcefire Software for X-Series の場合：
  `Sourcefire_3D_XOS_Device_Patch-5.3.0.1-66.sh`

重要 サポート サイトから更新を直接ダウンロードします。電子メールで更新ファイルを転送すると、破損する可能性があります。

4. [System] > [Updates] を選択し、次に [Product Updates] タブで [Upload Update] をクリックして、防御センターに更新をアップロードします。更新を参照し、[Upload] をクリックします。

   更新が防御センターにアップロードされます。

5. 環境内のアプライアンスが正常に通信していること、およびヘルス モニタによって報告された問題がないことを確認します。

6. インストール中の更新の横にあるインストール アイコンをクリックします。

   [Install Update] ページが表示されます。

7. 更新をインストールするデバイスを選択します。

   スタック型のペアを更新する場合は、ペアの一方のメンバーを選択すると、自動的に他方が選択されます。スタック型ペアのメンバーは一緒に更新する必要があります。

8. [Install] をクリックします。更新をインストールしてデバイスを再起動することを確認します。

   更新プロセスが開始されます。防御センターのタスク キュー（[System] > [Monitoring] > [Task Status]）で更新の進行状況を監視できます。

   管理対象デバイスは更新時に 2 回再起動することがありますが、これは予期される動作です。

   インライン展開された Sourcefire Software for X-Series の場合、VAP のリロード中はトラフィックが中断されます。

警告 更新時に問題が発生した場合は（タスク キューが更新の失敗を示している、タスク キューを手動でリフレッシュしても数分間にわたって進行状況が表示されない、など）、更新を再開**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。

9. [Devices] > [Device Management] を選択し、更新したデバイスが正しいソフトウェア バージョン（バージョン 5.3.0.1）であることを確認します。

10. 環境内のアプライアンスが正常に通信していること、およびヘルス モニタによって報告された問題がないことを確認します。
11. すべての管理対象デバイスにデバイス設定を再適用します。

> **ヒント** グレーアウトされた [Apply] 再度有効にするには、デバイス設定でいずれかのインターフェイスを編集してから変更を適用せずに、[Save] をクリックしします。

12. すべての管理対象デバイスにアクセス制御ポリシーを再適用します。

    アクセス制御ポリシーを適用すると、トラフィック フローとトラフィック処理で一時的に停止が発生したり、一部のパケットが検査なしで通過することがあります。詳細については、『*Sourcefire 3D System User Guide*』を参照してください。

更新の実行にシェルを使用する

Sourcefire では更新を実行するのに、防御センターの Web インターフェイスを使用することを推奨しますが、bash シェルを使用してアプライアンスを更新しなければならない状況がまれに存在することがあります。

重要 Sourcefire 3D System の新しい未構成の（バージョン 5.3）インストールを更新する場合は、シェルを使用**しないでください**。シェルを使用してアプライアンスを更新する前に、Web インターフェイスを使用して初期設定を完了してください。

重要 Sourcefire Software for X-Series を更新する場合は、シェルを使用**しないでください**。代わりに、管理元の防御センター（「管理対象デバイスおよび Sourcefire Software for X-Series の更新」（P.13）を参照）を使用してください。

バージョン 5.3.0.1 の更新では、すべてのアプライアンスが再起動します。管理対象デバイスは、更新時にトラフィック検査、スイッチング、ルーティング、NAT、VPN、または関連機能を実行**しません**。デバイスの設定および展開方法に応じて、更新プロセスはトラフィック フローおよびリンク ステートにも影響する場合があります。詳細については、「更新中のトラフィック フローとトラフィック検査」（P.4）を参照してください。

シェルを使用して更新をインストールするには：

1. このリリース ノートを参照し、必要な更新前処理タスクを完了します。

   詳細については、「はじめに：重要な更新と互換性に関する注意事項」（P.3）および「更新の計画」（P.7）を参照してください。

2. 適切な更新を Sourcefire サポートサイトからダウンロードします。
   - シリーズ 2 防御センターの場合：
     `Sourcefire_3D_Defense_Center_Patch-5.3.0.1-66.sh`
   - シリーズ 3 および仮想防御センターの場合：
     `Sourcefire_3D_Defense_Center_S3_Patch-5.3.0.1-66.sh`
   - シリーズ 2 管理対象デバイスの場合：
     `Sourcefire_3D_Device_Patch-5.3.0.1-66.sh`
   - シリーズ 3 管理対象デバイスの場合：
     `Sourcefire_3D_Device_S3_Patch-5.3.0.1-66.sh`
   - 3D9900 管理対象デバイスの場合：
     `Sourcefire_3D_Device_x900_Patch-5.3.0.1-66.sh`
   - 仮想管理対象デバイスの場合：
     `Sourcefire_3D_Device_Virtual64_VMware_Patch-5.3.0.1-66.sh`

   重要 サポート サイトから更新を直接ダウンロードします。電子メールで更新ファイルを転送すると、破損する可能性があります。

3. 管理者権限を持つアカウントを使用してアプライアンス シェルにログインします。

   仮想アプライアンスの場合は、VMware vSphere Client で仮想コンソールを使用してログインします。シリーズ 3 または仮想管理対象デバイスでは、シェル プロンプトを表示するのに `expert` と入力する必要があることに注意してください。

4. プロンプトで、root ユーザとして次のパスワードを入力し、更新を実行します。

   `sudo install_update.pl /var/sf/updates/`*`update_name`*

   ここで、*`update_name`* は先にダウンロードした更新ファイル名です。

   更新プロセスが開始されます。

5. 更新が完了すると、アプライアンスが再起動します。更新を監視し、次の各項で説明するように更新後の手順を完了できます。
   - 「防御センターの更新」（P.11）
   - 「管理対象デバイスおよび Sourcefire Software for X-Series の更新」（P.13）

更新のアンインストール

次の各項を参照して、ご使用のアプライアンスからバージョン 5.3.0.1 の更新をアンインストールできます。

- 「アンインストールの計画」（P.18）
- 「管理対象デバイスからの更新のアンインストール」（P.20）
- 「仮想管理対象デバイスからの更新のアンインストール」（P.21）
- 「Sourcefire Software for X-Series からの更新のアンインストール」（P.22）
- 「防御センターからの更新のアンインストール」（P.23）

アンインストールの計画

更新をアンインストールする前に、次のすべての項を精読し、理解する必要があります。

アンインストールの方法

更新はローカルでアンインストールする必要があります。防御センターを使用して管理対象デバイスから更新をアンインストールすることは**できません**。

すべての物理アプライアンスおよび仮想防御センターに対し、ローカル Web インターフェイスを使用して更新をアンインストールします。仮想管理対象デバイスとSourcefire Software for X-Series には Web インターフェイスがないため、bash シェルを使用して更新をアンインストールする必要があります。

アンインストールの順序

更新は、インストールの逆の順序でアンインストールします。つまり、最初に管理対象デバイスから更新をアンインストールし、その後に防御センターからアンインストールします。

クラスタ アプライアンスまたはペア アプライアンスからの更新のアンインストール

高可用性ペアのクラスタ デバイスおよび防御センターは、同じバージョンの Sourcefire 3D System を実行する必要があります。アンインストール プロセスは自動フェールオーバーをトリガーしますが、不一致のペアまたはクラスタのアプライアンスは、設定情報を共有せず、同期の一部として更新をインストールまたはアンインストールすることもありません。冗長アプライアンスから更新をアンインストールする必要がある場合は、即時および連続的にアンインストールを実行するように計画します。

運用の継続性を保証するには、クラスタ デバイスとペア防御センターから更新を 1 つずつアンインストールします。まず、セカンダリ アプライアンスから更新をアンインストールします。アンインストール プロセスが完了するまで待ってから、すぐにプライマリ アプライアンスから更新をアンインストールします。

警告　クラスタ デバイスまたはペア防御センターからのアンインストール プロセスが失敗した場合は、アンインストールを再開したり、ピアの設定を変更したり**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。

スタック デバイスからの更新のアンインストール

スタック内のすべてのデバイスが、同じバージョンの Sourcefire 3D System を実行する必要があります。スタック デバイスのいずれかから更新をアンインストールすると、そのスタックではデバイスが限定的な、バージョンが混在する状態になります。

展開への影響を最小にするために、Sourcefire ではスタック デバイスから更新を同時にアンインストールすることを推奨しています。スタックはアンインストールがスタック内のすべてのデバイスで完了すると、通常の動作を再開します。

インライン展開されたデバイスからの更新のアンインストール

更新のアンインストール中、管理対象デバイスはトラフィック検査、スイッチング、ルーティング、または関連機能を実行**しません**。デバイスの設定および展開方法に応じて、アンインストール プロセスはトラフィック フローおよびリンク ステートにも影響する場合があります。詳細については、「更新中のトラフィック フローとトラフィック検査」（P.4）を参照してください。

Sourcefire Software for X-Series からの更新のアンインストール

Sourcefire Software for X-Series から更新を完全にアンインストールするため、各 VAP グループから個別に更新をアンインストールする必要があります。Sourcefire 3D System のバージョン 5.3.0.1 の更新をアンインストールすると、影響を受ける VAP がリロードされます。Sourcefire Software for X-Series がインライン展開され、複数メンバーの VAP グループを使用している場合、Sourcefire では任意の VAP から更新をアンインストールした後、他の VAP から更新をアンインストールする前に、その VAP がリロードできるようにすることを推奨します。

これにより、影響を受ける VAP のリロード中に、グループ内の他の VAP がネットワーク トラフィックを検査できます。インライン展開で単一 VAP の VAP グループを使用している場合、VAP をリロードするとネットワーク トラフィックが中断されます。アンインストールは保守期間に、またはアンインストールが展開に及ぼす影響が最小のときに計画してください。

アンインストール後

更新をアンインストールした後、展開環境が正しく動作していることを保証するために、いくつかの手順を実行する必要があります。これらはアンインストールが成功したこと、および展開環境のすべてのアプライアンスが正常に通信していることを確認することが含まれます。

次の各項では、更新の実行と更新後の手順の完了に関する詳細情報を示します。これらすべてのタスクを完了してください。

管理対象デバイスからの更新のアンインストール

次の手順では、ローカルの Web インターフェイスを使用して管理対象デバイスからバージョン 5.3.0.1 の更新をアンインストールする方法について説明します。防御センターを使用して管理対象デバイスから更新をアンインストールすることは**できません**。

バージョン 5.3.0.1 の更新をアンインストールすると、デバイスはバージョン 5.3 を実行するようになります。以前のバージョンのアンインストールの詳細については、該当するバージョンのリリース ノートを参照してください。

バージョン 5.3.0.1 の更新をアンインストールすると、デバイスが再起動します。管理対象デバイスは、更新時にトラフィック 検査、スイッチング、ルーティング、または関連機能を実行**しません**。デバイスの設定および展開方法に応じて、更新プロセスはトラフィック フローおよびリンク ステートにも影響する場合があります。詳細については、「更新中のトラフィック フローとトラフィック検査」（P.4）を参照してください。

更新をアンインストールするには、次の手順を実行します。

1. 「アンインストールの計画」（P.18）を読み、理解します。
2. 管理元の防御センターで、展開環境内のアプライアンスが正常に通信していること、およびヘルス モニタによって報告された問題がないことを確認します。
3. 管理対象デバイスでタスク キューを調べ（[System] > [Monitoring] > [Task Status]）、進行中のタスクがないことを確認します。

   実行中でアンインストールが開始されるときに停止されたタスクは失敗したタスクとなり、再開できません。これらはアンインストールが完了した後にタスク キューから手動で削除する必要があります。タスク キューは 10 秒ごとに自動的にリフレッシュされます。アンインストールを始める前に、実行時間の長いタスクが完了するまで待つ**必要があります**。
4. [System] > [Updates] を選択します。

   [Product Updates] タブが表示されます。

5. 削除する更新と一致するアンインストーラの横にあるインストール アイコンをクリックしてから、更新をアンインストールすること、およびデバイスを再起動することを確認します。

   アンインストールのプロセスが開始されます。タスク キュー（[System] > [Monitoring] > [Task Status]）でアンインストールの進行状況を監視できます。

   警告　アンインストールが完了し、デバイスが再起動するまでは、Web インターフェイスを使用して別のタスクを実行**しないでください**。アンインストールが完了する前に、Web インターフェイスが利用できなくなり、ユーザがデバイスによりログアウトされる可能性があります。これは予期される動作です。再度ログインしてタスク キューを表示してください。アンインストールが実行中の場合は、完了するまで Web インターフェイスを使用**しないでください**。アンインストール時に問題が発生した場合は（タスク キューが更新の失敗を示している、タスク キューを手動でリフレッシュしても数分間にわたって進行状況が表示されない、など）、アンインストールを再開始**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。

6. アンインストールが終了したら、ブラウザ キャッシュをクリアし、ブラウザでリロードを強制します。そうしない場合、ユーザ インターフェイスが予期しない動作を示すことがあります。
7. デバイスにログインします。
8. [Help] > [About] を選択し、ソフトウェアのバージョンが正しく表示される（バージョン 5.3）ことを確認してください。
9. 管理元の防御センターで、展開環境内のアプライアンスが正常に通信していること、およびヘルス モニタによって報告された問題がないことを確認します。

仮想管理対象デバイスからの更新のアンインストール

次の手順は、仮想管理対象デバイスからバージョン 5.3.0.1 の更新をアンインストールする方法について説明します。防御センターを使用して管理対象デバイスから更新をアンインストールすることは**できません**。

バージョン 5.3.0.1 の更新をアンインストールすると、デバイスはバージョン 5.3 を実行するようになります。以前のバージョンのアンインストールの詳細については、該当するバージョンのリリース ノートを参照してください。

バージョン 5.3.0.1 の更新をアンインストールすると、デバイスが再起動します。仮想管理対象デバイスは、更新時にトラフィックの検査や関連機能を実行**しません**。デバイスの設定および展開方法に応じて、更新プロセスはトラフィック フローにも影響する場合があります。詳細については、「更新中のトラフィック フローとトラフィック検査」（P.4）を参照してください。

更新をアンインストールするには、次の手順を実行します。

1. 「アンインストールの計画」（P.18）を読み、理解します。
2. admin として、SSH を介してまたは仮想コンソールを介してデバイスにログインします。
3. CLI プロンプトで、expert と入力して bash シェルにアクセスします。
4. bash シェル プロンプトで、sudo su - と入力します。
5. admin パスワードを入力して、root 権限でプロセスを続行します。
6. プロンプトで、以下を 1 行で入力します。

   ```
   install_update.pl /var/sf/updates/Sourcefire_3D_
   Device_Virtual64_VMware_Patch_Uninstaller-5.3.0.1-66.sh
   ```

   アンインストールのプロセスが開始されます。

   警告　アンインストールで問題が発生した場合は、アンインストールを再開始**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。

7. アンインストールの完了後に、管理元の防御センターにログインし、[Devices] > [Device Management] を選択します。更新をアンインストールしたデバイスが正しいソフトウェア バージョンになっている（バージョン 5.3）ことを確認します。
8. 環境内のアプライアンスが正常に通信していること、およびヘルス モニタによって報告された問題がないことを確認します。

Sourcefire Software for X-Series からの更新のアンインストール

次の手順は、バージョン 5.3.0.1 の更新を Sourcefire Software for X-Series からアンインストールする方法について説明します。防御センターを使用して更新をアンインストールすることはできません。Sourcefire Software for X-Series から更新を完全にアンインストールするため、各 VAP グループから個別に次の手順を実行する必要があります。

バージョン 5.3.0.1 の更新をアンインストールすると、Sourcefire Software for X-Series でバージョン 5.3 が実行されるようになります。

更新をアンインストールするには、次の手順を実行します。

1. 「アンインストールの計画」（P.18）を読み、理解します。
2. 更新をアンインストールする VAP にログインします。

   たとえば、侵入 VAP グループの最初の VAP にログインするには、次のように入力します。

   ```
   CBS# unix su
   [root@machine admin]# rsh intrusion_1
   ```
3. プロンプトで、Sourcefire スクリプトを実行するようにセッション環境を設定するため、次のコマンドを実行します。

   ```
   source /opt/sf/profile
   ```
4. プロンプトで、以下を 1 行で入力し、**Enter** キーを押します。

   ```
   install_update.pl
   /var/sf/updates/Sourcefire_3D_XOS_Device_Patch_Uninstaller-
   5.3.0.1-66.sh
   ```

   更新が削除され、VAP がリロードします。Sourcefire Software for X-Series がインライン展開されている場合、VAP のリロード中にその VAP へのトラフィックが中断されます。ただし、VAP グループに他の VAP がある場合、他の VAP 間でトラフィックが負荷分散されることに注意してください。
5. 管理元の防御センターで [Devices] > [Device Management] を選択し、ソフトウェアのバージョンが正しく表示される（バージョン 5.3）ことを確認してください。
6. Sourcefire Software for X-Series が防御センターと正常に通信していることを確認します。
7. VAP グループ内の VAP ごとにステップ 1 ～ 6 を繰り返します。

防御センターからの更新のアンインストール

バージョン 5.3.0.1 の更新を防御センターおよび仮想防御センターからアンインストールするには、次の手順を使用します。アンインストール プロセスにより、防御センターが再起動されることに注意してください。

バージョン 5.3.0.1 の更新をアンインストールすると、防御センターはバージョン 5.3 を実行するようになります。以前のバージョンのアンインストールの詳細については、該当するバージョンのリリース ノートを参照してください。

更新をアンインストールするには、次の手順を実行します。

1. 「アンインストールの計画」（P.18）を読み、理解します。
2. 環境内のアプライアンスが正常に通信していること、およびヘルス モニタによって報告された問題がないことを確認します。

3. タスク キューを調べ（[System] > [Monitoring] > [Task Status]）、進行中のタスクがないことを確認します。

   実行中でアンインストールが開始されるときに停止されたタスクは失敗したタスクとなり、再開できません。これらはアンインストールが完了した後にタスク キューから手動で削除する必要があります。タスク キューは 10 秒ごとに自動的にリフレッシュされます。アンインストールを始める前に、実行時間の長いタスクが完了するまで待つ**必要があります**。

4. [System] > [Updates] を選択します。

   [Product Updates] タブが表示されます。

5. 削除する更新と一致するアンインストーラの横にあるインストール アイコンをクリックします。

   [Install Update] ページが表示されます。

6. 防御センターを選択し、[Install] をクリックしてから、更新をアンインストールすること、およびデバイスを再起動することを確認します。

   アンインストールのプロセスが開始されます。タスク キュー（[System] > [Monitoring] > [Task Status]）でアンインストールの進行状況を監視できます。

   警告 アンインストールが完了し、防御センターが再起動するまでは、Web インターフェイスを使用して別のタスクを実行**しないでください**。アンインストールが完了する前に、Web インターフェイスが利用できなくなり、ユーザが 防御センター によりログアウトされる可能性があります。これは予期される動作です。再度ログインしてタスク キューを表示してください。アンインストールが実行中の場合は、完了するまで Web インターフェイスを使用**しないでください**。アンインストール時に問題が発生した場合は（タスク キューが更新の失敗を示している、タスク キューを手動でリフレッシュしても数分間にわたって進行状況が表示されない、など）、アンインストールを再開始**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。

7. アンインストールが終了したら、ブラウザ キャッシュをクリアし、ブラウザでリロードを強制します。そうしない場合、ユーザ インターフェイスが予期しない動作を示すことがあります。

8. 防御センターにログインします。

9. [Help] > [About] を選択し、ソフトウェアのバージョンが正しく表示される（バージョン 5.3）ことを確認してください。

10. 環境内のアプライアンスが正常に通信していること、およびヘルス モニタによって報告された問題がないことを確認します。

バージョン 5.3.0.1 で解決された問題

バージョン 5.3.0.1 で解決された問題を以下に示します。

- セキュリティ問題複数のクロスサイト スクリプティング（XSS）の脆弱性が解決されました。
- セキュリティ問題複数のクロスサイト リクエスト フォージェリ（CSRF）の脆弱性が解決されました。
- セキュリティ問題複数のインジェクションの脆弱性（HTML インジェクション、コマンド ライン インジェクションなど）の脆弱性が解決されました。
- セキュリティ問題 Linux、MySql、および stronSwan での複数の脆弱性の問題が解決されました。これには CVE-2013-2237 および CVE-2013-2338 で説明されている問題が含まれます。
- まれに、別の侵入ポリシーと共有されているレイヤでローカル侵入ルールを含む侵入ポリシーを設定すると、侵入ポリシーのエクスポートが失敗することがあるという問題が解決されました。（132312）
- まれに、侵入ルールのいずれかに機密データ（sdf）ルール分類が含まれている場合に、Snort がパケット処理を停止することがあるという問題が解決されました。（132600）
- まれに、極端に大きなポート範囲を指定し、他のルール条件（これにより、防御センターがそれらをデバイスに拡大形式で送信することになる）を含むルールを使用してアクセス制御ポリシーを作成および適用した場合に、Snort によりシステム リソースが枯渇するという問題が解決されました。（132998）
- アクセス制御ポリシーの [Security Intelligence] ページで、100 を超える使用可能なセキュリティ ゾーンを表示できないという問題が解決されました。（133418）
- ユーザ名および Message Digest 5（MD5）パスワード暗号化を使用して認証するようにプロキシ サーバを設定すると、防御センターとの通信で問題が発生するという問題が解決されました。（133727、135041）
- 高可用性設定で防御センターのペアに管理対象デバイスを登録するときに、コマンド ライン インターフェイス（CLI）を使用できないという問題が解決されました。（133825）
- システムが [Intrusion Event Performance] グラフのデータを省略する管理対象デバイスのメモリの問題が解決しました。（133944）
- [Total Packets Received] Snort リアルタイム統計で異常に大きなカウントが生成されるという問題が解決されました。（134036）

- システムで、侵入ポリシーのいずれかを、単一の管理対象デバイスに合計 4096 回以上再適用する（個別に再適用するか、またはアクセス制御ポリシーの一部として再適用する）ことができないという問題が解決されました。（134231）
- まれに、無関係な [Module Disk Usage: Frequent drain of Connection Events] ヘルス アラートがシステムにより生成されるという問題が解決されました。（134355）
- 脆弱性データベース（VDB）通知に示されている FireSight Detector Update に関連するアプリケーション ディテクタがアクセス制御ポリシーに含まれている場合、新しいバージョンの VDB の適用後にアクセス制御ポリシーが [out-of-date] としてマークされないという問題が解決されました。（134458）
- グリニッジ標準時（GMT：UTC とも呼ばれます）がローカル時間帯ではない場合に、スケジュール済みの位置情報更新が失敗する場合があるという問題が解決されました。（134742）
- セキュリティ問題アプリケーション検出、アクセス制御、および相関ルール管理における複数のクロスサイト スクリプティング（XSS）の脆弱性が解決されました。（135011、135629、135632）
- アクセス制御ルールに URL 条件が含まれている場合の Snort の安定性が向上しました。（135071、136833）
- バージョン 5.1.1.x で導入された管理対象デバイスをバージョン 5.2.x に更新し、その後バージョン 5.3 に更新すると、[high unmanaged disk usage] についての無関係なヘルス アラートが生成されるという問題が解決されました。（135689）
- バージョン 5.2.x からバージョン 5.3 にアプライアンスを更新し、後でバックアップを作成した場合、バージョン 5.3 のイメージを再作成した防御センターでバックアップを復元することができないという問題が解決されました。（135869）
- 1 つの IP アドレスを共有する複数の固有ホストが、ホスト プロファイルで複数の実 MAC アドレスを持つ 1 つのホストとして表示されるという問題が解決されました。（135956、135992）
- 物理的な管理対象デバイスで [User Management] ページ（[System] > [Local] > [User Management]）へのアクセスが制限されるという問題が解決されました。（136079）
- セキュリティ問題侵入ルール エディタ ページでの XSS 脆弱性（CVE-2014-2012）が除去されました。この脆弱性により、攻撃者が情報にアクセスしてその情報を公開したり、ユーザ アクションと要求を偽装したり、または任意の JavaScript を実行したりできる可能性がありました。この問題をご報告いただいた Liad Mizrachi Check Point Security Research Team に対し、謝意を表します。（136542）

- セキュリティ問題 [User Configuration] ページでのクロスサイト リクエスト フォージェリ（CSRF）の脆弱性（CVE-2014-2011）が除去されました。この脆弱性により、攻撃者がユーザ アカウントを追加、編集できる可能性がありました。この問題をご報告いただいた Liad Mizrachi Check Point Security Research Team に対し、謝意を表します。（136911）
- セキュリティ問題 [User Management] ページでの CSRF 脆弱性（CVE-2014-2028）が除去されました。この脆弱性により、攻撃者がユーザ アカウントをアクティブ化、非アクティブ化、編集、削除できる可能性がありました。この問題をご報告いただいた Liad Mizrachi Check Point Security Research Team に対し、謝意を表します。（136914）
- システムが、4GB 以上の速度のファイバ インターフェイスについて誤った速度データを示すという問題が解決されました。（137484）
- セキュリティ問題 [Scheduling] ページ、[Health Monitor] ページ、およびイベント ビューアでの XSS 脆弱性（CVE-2014-2275）が除去されました。この脆弱性により、攻撃者が情報にアクセスしてその情報を公開したり、ユーザ アクションと要求を偽装したり、または任意の JavaScript を実行したりできる可能性がありました。この問題をご報告いただいた Adi Volkovitz Check Point Security Research Team に対し、謝意を表します。（137850、137853、137856）
- シリーズ 3 管理対象デバイスのファイバ インターフェイスの接続を切断してから再接続しても、システムがネットワーク接続を再確立しないという問題が解決されました。（138099）

以前の更新で解決された問題

バージョン 5.3 からバージョン 5.3.0.1 にアプライアンスを更新できるため、この更新には、バージョン 5.3 での変更も含まれます。以前に解決された問題をバージョン別に示します。

バージョン 5.3

- セキュリティ問題複数のクロスサイト スクリプティング（XSS）の脆弱性が解決されました。
- セキュリティ問題複数のクロスサイト リクエスト フォージェリ（CSRF）の脆弱性が解決されました。

- セキュリティ問題複数のインジェクションの脆弱性（HTML インジェクション、コマンド ライン インジェクションなど）の脆弱性が解決されました。
- セキュリティ問題 cURL、Linux、MySQL、strongSwan、および Wireshark での複数の脆弱性の問題が解決されました。これには CVE-2013-1944、CVE-2013-3783CVE-2013-5718、CVE-2013-5719、CVE-2013-5720、CVE-2013-5721、CVE-2013-5722 で説明されている問題が含まれます。
- VPN のパフォーマンスと安定性が向上しました。（116996、119698、123636）
- クラスタ化したスタックでデバイス設定を変更し、変更をただちに適用すると、適用が失敗し、システムによりタスク ステータス キューにエラー メッセージが表示される問題が解決されました。（121625）
- 新しい侵入ルールの更新をインストールすると、相関ルールによって参照されるカスタム侵入ルールの分類が、事前定義された分類に戻ってしまうことがある問題が解決されました。（122163）
- 異なるホスト、ユーザ、およびアプリケーションの組み合わせを検出するように設定された、同じゾーンとネットワークにより制約を受ける 2 つ以上のネットワーク ディスカバリ ルールを適用した場合に、ネットワーク ディスカバリ ポリシーが予期したとおりに機能しない場合がある問題が解決されました。（122853）
- LDAP サーバのホスト名と IP アドレスのネットワーク環境の DNS エントリが一致しなかった場合に LDAP 認証に失敗する可能性がある問題が解決されました。（123447）
- シリーズ 3 アプライアンス で Sourcefire 3D System の更新に 3 時間以上必要であった問題が解決されました。（124148）
- 非アクティブな管理対象デバイスが含まれているときに、デバイス グループを編集できない場合がある問題が解決されました。（124286）
- システムがすでに Sourcefire 3D System の更新を実行中にユーザが侵入ルールの更新をインストールしようとすると、エラー メッセージが生成されるようになりました。（124290）
- まれに、防御センターがリモート ストレージにイベントをバックアップしなかった問題が解決されました。（124350）
- システムが誤った「**Please wait, loading...**」メッセージを表示する場合がある問題が解決されました。（124918）
- Nmap スキャンのパフォーマンスが改善されました。（124999）
- 失敗した侵入ルールの更新をシステムが未完了で終了していた問題が解決されました。（125368）

- SMTP プリプロセッサ ルールの 124:1、124:3、または 124:10 で、システムが誤検出アラートを生成する問題が解決されました。（125449）
- セキュリティ問題複数のパケットの表示問題が解決されました。（125531、132258）
- 機密データの分析のパフォーマンスが改善されました。（125588、126167）
- [Scan from reporting device] が無効になっている修正を使用しても、システムがデバイスから Nmap スキャンを実行してしまう問題が解決されました。（125608）
- 自動検出 DCE/RPC プリプロセッサ オプションのいずれかを有効にした場合に、システムがトラフィック再構成時に誤検出アラートを生成する問題が修正されました。（125737）
- 新しい侵入ルールの更新をインポートした後に、侵入ポリシー内のインポート済みルールの数がインポート ログにあるルールの数と一致しない問題が修正されました。（125900）
- セキュリティ問題システムが一部のユーザ ロールのユーザに不正なアクセス権限を付与していた問題が解決されました。（126016、127428、127779）
- クラスタ構成、スタック構成、およびクラスタかつスタック構成において管理対象デバイス上の複数の同期問題が解決されました。（126106、128724）
- 接続イベントを syslog に送信するときの syslog アラート応答の安定性が向上しました。（127682）
- TCP ストリーム プリプロセッサ オプションの [Require TCP 3-Way Handshake] を有効にし、レート ベースの攻撃防御プリプロセッサが過剰な同時接続を制限するように設定した場合に、不完全（SYN のみ）な接続に対する侵入ルール 135:2 でシステムがイベントを生成する問題が解決されました。（127803）
- 標準偏差 2 以上のトラフィック スパイクでトリガーするようにトラフィック プロファイルおよび相関ルールを設定した場合に、システムが相関イベントを生成しなかった問題が解決されました。（128107）
- 侵入ルール 1:24490 でシステムが誤検出アラートを生成していた問題が解決されました。（128304）
- まれに、3D8120、3D8130、3D8140、および 3D8250 でシステムの問題が発生し、再起動が必要だったハードウェアの問題が解決されました。（128689）
- ネットワーク検出ポリシーを使用して LDAP トラフィックのユーザ検出を無効にした場合に、防御センターがユーザ エージェントのログイン データのロギングを停止する問題が解決されました。（128741）
- 自動 LDAP ユーザ データ取得をスケジュールした場合に、オンデマンドのユーザ データの取得とダウンロードを実行できない場合がある問題が解決されました。（128962）

- セキュリティ問題オブジェクト マネージャおよびルール エディタの複数の XSS の脆弱性が解決されました。（129052、132023）
- 確認した侵入イベントをユーザが表示し、パケット ビューまでドリルダウンした場合に、表示されるイベントがなく、確認された制約が削除される場合がある問題が解決されました。（129257）
- SMTP サーバが接続エラーに応答した場合に、システムが誤って SMTP トラフィックを識別し、存在しないアプリケーション情報により接続イベントを生成する場合がある問題が解決されました。（130085）
- 高可用性構成の防御センターでのアクセス制御ポリシーの同期問題が解決されました。（130475）
- まれに、解釈できないメッセージを含む重大なヘルス アラート メールをシステムが生成する問題が解決されました。（130518）
- オブジェクト マネージャのセキュリティ ゾーン ページの複数の表示問題が解決されました。（130569、130631、130632）
- カスタム ワークフローのドリルダウンにより、ユーザが侵入イベントの不正なパケット ビュー ページにリダイレクトされる問題が解決されました。（130620）
- リモート コンソール アクセス オプションとして [Physical Serial Port] を選択しても、システムの復元起動オプションが管理対象デバイスのシリアル ポートに出力されない場合がある問題が解決されました。（130772）
- ハードウェア障害の後のフェールオーバー時における、クラスタ化された管理対象デバイスの安定性が向上しました。（130811、130812、131031、133088、130602）
- クラスタ化された管理対象デバイスのフェールオーバーの同期問題が解決されました。（130829）
- ファイル転送プロトコル（FTP）トラフィックを処理する場合に、システムのマルウェア分析機能とブロッキング機能が向上しました。（130888、133134）
- まれに、侵入ポリシー ページが表示されない問題が解決されました。（131181）
- まれに、サーバのテーブル ビュー（[Analysis] > [Hosts] > [Servers]）でサーバが複製され、誤ったサーバ数が作成されることがある問題が修正されました。（131329）
- サポート技術情報の記事 000001950 で説明されているようにスタティック ルートを設定し、ネットワーク設定にその後の変更を行った場合に、システムが次のシステムの再起動後までスタティック ルートをドロップする場合がある問題が解決されました。（131646）
- 3 スタックで 3 台の管理対象デバイスをスタックする場合の安定性が向上しました。（131836、131896）

- システムが Sourcefire 3D System のメジャー バージョンに更新した後に、ユーザ アカウントのホーム ディレクトリ ファイルを誤った場所に置く問題が解決されました。（132503）
- 侵入ポリシーの [Quoted-Printable Decoding Depth] 詳細オプションを無効にしても、システムが侵入ルール 124:11 でイベントを生成してしまう問題が解決されました。（132538）
- [Correlation Events] テーブルおよび [Applications] テーブルからのデータが読み込まれたカスタム テーブルを設定し、次に共通フィールドとして [Source IP] を選択すると、バージョン 5.3 への更新が失敗する問題が解決しました。（135735）
- 監視ルール（接続終了のロギングを強制する）および [Log at Beginning of Connection] を有効にした信頼ルールを含むアクセス制御ポリシーを設定すると、SSH 暗号化トラフィックと照合するための接続終了イベントが生成されない場合がある問題が解決されました。（135952）

既知の問題

バージョン 5.3.0.1 で報告されている既知の問題を以下に示します。

- 8000 Series 管理対象デバイスの最大伝送単位（MTU）設定によって IP データグラム フラグメンテーションがトリガーされると、システムで NMSB 接続の問題が発生する可能性があります。（135731）
- セキュリティ インテリジェンス フィードを設定し、Windows オペレーティング システムが稼働するコンピュータ上に作成された**フィード URL** を指定する場合、[Security Intelligence] タブのツールチップには、送信された IP アドレスの正確な数が表示されません。回避策として、`dos2unix` コマンドを使用してファイルを Windows エンコードから Unix エンコードに変換し、[Security Intelligence] ページの [Update Feeds] をクリックします。（136557）
- [Captured Files] テーブルに基づいてカスタム テーブルを作成すると、システムによりエラー メッセージが生成されます。システムでは、[Captured Files] テーブルに基づくカスタム テーブルの作成がサポートされていません。（136844）
- 40 文字を超える長さのホスト名を持つ管理対象デバイスを登録しようとすると、デバイス登録が失敗します。（137235）
- 場合によっては、ドル記号（$）、キャラット（^）、アスタリスク（*）、大カッコ（[ ]）、縦棒（|）、スラッシュ（\）、ピリオド（.）、疑問符（?）のいずれかの特殊文字をフィルタ条件に指定すると、オブジェクト マネージャでのオブジェクトのフィルタリングが予期されているとおりに実行されないことがあります。（137493）

- 場合によっては、システム ポリシーで 簡易ネットワーク管理プロトコル（SNMP）ポーリングを有効にしている場合に、クラスタ構成管理対象デバイスの 1 つで高可用性（HA）リンク インターフェイス設定を変更すると、正しくない SNMP ポーリング要求が生成されることがあります。（137546）
- 場合によっては、ブラックリストに登録されている接続を Syslog または SNMP トラップ サーバに記録するようにアクセス制御ポリシーを設定すると、システムの問題が発生することがあります。（137952）
- 場合によっては、侵入イベント パケット ビューに、イベントを生成したルールと一致しないルール メッセージが表示されることがあります。（138011）
- 場合によっては、システムが DNS または NTP パケットを受信する順序が正しくないと、[Operating System Summary] ワークフローに表示される DNS サーバ数、NTP サーバ数、および DNS ポート数が誤っていることがあります。（138047）
- カスタム変数を参照する侵入ルールをインポートできません。回避策として、ルールをインポートし、インポートしたルールを編集してカスタム変数を再度追加する前に、侵入ルールからカスタム変数を削除します。（138077）
- バックアップの実行中に防御センターとその管理対象デバイスの間の接続がシステムにより解除されると、管理対象デバイスが完了したバックアップ ファイルを防御センターに送信せず、[Task Status] ページ（[System] > [Monitoring] > [Task Status]）にバックアップがまだ進行中であることが報告されます。この状況が発生した場合は、管理対象デバイスから直接バックアップをダウンロードしてください。（138102）
- ファイル イベントのテーブル ビューで、対象外のファイル イベントのファイル トラジェクトリの表示がサポートされているように見えます。算出された SHA-256 値を持つファイルのファイル トラジェクトリのみを表示できます。（138155）
- X 軸として [File Name] を使用したグラフを含む HTML 形式または PDF 形式のレポートを生成すると、X 軸のファイル名の UTF-8 文字が表示されません。（138297）
- まれに、以前に防御センターを使用して複数のデバイスを管理したことがある場合、ダッシュボードに誤った侵入イベント数が表示されることがあります。（138298）
- まれに、侵入ポリシーの変更と再適用を数百回行うと、侵入ルールの更新とシステムの更新が完了するまでに 24 時間以上を要することがあります。（138333）
- 最新バージョンの位置情報データベース（GeoDB）が防御センターにインストールされており、同じバージョンでこの GeoDB を更新しようとすると、システムによりエラー メッセージが生成されます。（138348）

- 複数のアクセス制御ポリシーを展開環境全体に適用する場合、特定のアクセス制御ルールに一致する侵入イベントまたは接続イベントを検索すると（[Analysis] > [Search]）、その他のポリシー内の無関係のルールによって生成されたイベントが取得されることがあります。（138542）
- まれに、シリーズ 3 管理対象デバイスのダッシュボードとイベント ビューに、誤ったパケット数（非常に多数のパケット数）が表示されることがあります。（138608）
- 場合によっては、システムの更新が失敗した後で シリーズ 3 管理対象デバイスを再起動すると、ハードウェアの問題が発生することがあります。システムの更新が失敗した場合は、アプライアンスを再起動**せずに**、サポートに連絡してください。（138684）
- ポリシー間ではアクセス制御ルールをカット アンド ペーストできません。（138713）
- Cisco IOS Null Route 修復モジュールで Telnet を有効にし、Cisco IOS ルータ上でデフォルトで有効にする Cisco IOS インスタンスのユーザ名を設定すると、Cisco IOS Null Route 修復が防御センターで失敗します。（139387）
- 変数セットのネットワーク変数の 1 つで、:: または ::0 アドレスが除外されており、アクセス制御ポリシーでこの変数セットを参照している場合、アクセス制御ポリシー（またはアクセス制御ポリシーで参照される侵入ポリシー）の適用が失敗します。:: または ::0 を除外ネットワーク リストに追加しないでください。（139406）
- まれに、[Task Status] ページ（[System] > [Monitoring] > [Task Status]）に、失敗したシステム ポリシー適用が正常に完了したものとして報告されることがあります。（139428）
- 基本ポリシーを介して相互参照する 3 つ以上の侵入ポリシーを設定して保存すると、[Intrusion Policy] ページ（[Policies] > [Intrusion] > [Intrusion Policy]）のすべてのポリシーの [Last Modified] の日付が更新されません。回避策として、5 ～ 10 分間待ってから [Intrusion Policy] ページを更新します。（139647）
- 場合によっては、夏時間（DST）対応から DST 非対応への移行日を含む時間枠を使用してレポートを設定して保存すると、システムではその時間枠が指定よりも 1 時間早く開始するように調整されることがあります。回避策として、1 時間遅れて開始するように時間枠を設定します。（139713）

- 防御センター Web インターフェイスの [Object Manager] ページでグローバル ホワイトリストから IP アドレスを削除すると、防御センターのコマンド ライン インターフェイス（CLI）でこの変更が反映されません。（139784）
- 70xx ファミリの管理対象デバイスでネットワーク アドレス変換（NAT）ポリシーを作成し、宛先ポート範囲を指定するダイナミック NAT ルールを配置した後で、1 番目の範囲に含まれる宛先ポートを指定する 2 番目のダイナミック NAT ルールを指定すると、1 番目のダイナミック ルールに一致しないトラフィックは、2 番目のダイナミック ルールと照合されません。（140216、140307）

以前のリリースで報告されている既知の問題

以下は Sourcefire 3D System の旧リリースで報告された既知の問題のリストです。

- [Destination Port/ICMP Code] が [0] のときにシステムが侵入イベントを生成した場合に、[Intrusion Event Statistics] ページの [Top 10 Destination Ports] セクション（[Overview] > [Summary] > [Intrusion Event Statistics]）で表示からポート番号が省略されます。（125581）
- 防御センターのローカル設定（[System] > [Local] > [Configuration]）が高可用性ピアの間で同期**されません**。プライマリだけではなく、すべての防御センターで変更を編集し、適用する必要があります。（130612、130652）
- システムがプルーニングを開始する前にディスク容量の使用率がディスク容量のしきい値を超えると、場合によっては、大規模なシステム バックアップが失敗する可能性があります。（132501）
- 場合によっては、RunQuery ツールを使用して `SHOW TABLES` コマンドを実行するとをクエリが失敗することがあります。クエリーの失敗を回避するには、必ずこのクエリーを RunQuery アプリケーションを使用して対話形式で実行します。（132685）
- Sourcefire 3D System の更新が失敗した後に シリーズ 3 管理対象デバイスを再起動すると、それ以降の更新が元の問題を解決した後でも失敗する可能性があります。（132700）
- 以前にインポートしたローカル侵入ルールを削除すると、削除したルールを再インポートできません。（132865）
- まれに、システムが侵入ルール 141:7 または 142:7 に対するイベントを生成しない場合があります。（132973）
- 管理対象デバイスのリモート バックアップに余分な統合ファイルが含まれ、防御センターにサイズの大きいバックアップ ファイルが生成される場合があります。（133040）

- 防御センターまたは管理対象デバイスの最大伝送単位（MTU）は、アプライアンスの CLI またはシェルを使用して編集する必要があります。ユーザインターフェイスを使用して防御センターまたは管理対象デバイスの MTU を編集することはできません。（133802）
- アスタリスク（*）の付いた URL オブジェクトを URL に作成すると、そのオブジェクトを参照するルールを含むアクセス制御ポリシー用のプリエンプト ルールの警告が生成されません。URL オブジェクト URL にアスタリスク（*）を使用**しないでください**。（134095、134097）
- 侵入イベントの syslog アラートを生成するように侵入ポリシーを設定する場合、プリプロセッサ オプションが有効になっている侵入ルールにより生成される侵入イベントの syslog アラート メッセージは、カスタマイズされたメッセージではなく「`Snort Aleat`」になります。（134270）
- スタックのセカンダリ デバイスが侵入イベントを生成すると、侵入イベントのテーブル ビューにセキュリティ ゾーンのデータが表示されません。（134402）
- [Fast Port Scan] オプションを有効にして Nmap スキャン修正を設定すると、Nmap 修正が失敗します。回避策として、[Fast Port Scan] オプションを無効にします。（134499）
- 接続イベント テーブルに保存された検索条件に基づいて接続イベントのサマリー データを含むレポートを生成すると、そのテーブルのレポートにデータが取り込まれません。（134541）
- 同時システム バックアップ タスクを計画し、実行すると、システム パフォーマンスが低下します。回避策として、スケジュールされたタスクを調整して、一度に 1 回のバックアップのみが実行されるようにします。（134575）
- ユーザおよびグループのアクセス コントロール パラメータが有効になっている、以前に設定した LDAP 接続を編集する場合、[Fetch Groups] をクリックしても [Available Groups] ボックスにデータが取り込まれません。使用可能なグループを取得するには、LDAP 接続の編集時にパスワードを再入力する必要があります。（134872）
- [Event View Settings] ページの [Event Preferences] セクションで [Resolve IP Addresses] を有効にした場合に、IPv6 アドレスに関連付けられたホスト名がダッシュボードまたはイベント ビューで正しく解決されない場合があります。（135182）
- LDAP 認証オブジェクトを作成する場合、[Base Filter] フィールドに 450 文字以上入力することができません。（135314）

- 夏時間（DST）の実施中にタスクをスケジュールした場合、DST を実施していない期間にはそのタスクが実行されないことがあります。回避策として、[Time Zone Preference] ページ（[Admin] > [User Preferences]）で [Europe, London] をローカルの時間帯として選択し、DST を実施していないときにタスクを再作成します。（135480）
- システムには、データベースのチェックのため、バージョン 5.3 以降が実行されているアプライアンスを再起動するのに追加の時間が必要です。データベースのチェック中にエラーが検出された場合は、データベースを修復するために再起動にさらに時間が必要です。（135564、136439）
- システムが SSH プリプロセッサ ルール 128:1 に対して誤検出を生成する場合があります。（135567）
- [Extract Original Client IP Address] HTTP プリプロセッサ オプションを有効にしたルールが含まれる侵入ポリシーを適用すると、トラフィックが専用のプロキシ サーバを通過した場合に、不正なデータを持つ侵入イベントが [Original Client IP] フィールドに読み込まれることがあります。（135651）
- 8000 Series 管理対象デバイスの最大伝送単位（MTU）設定によって IP データグラム フラグメンテーションがトリガーされると、システムで NMSB 接続の問題が発生する可能性があります。（135731）
- ジョブのタイプとして [Report] を指定してタスクをスケジュールした場合に、電子メールで送信されるステータス レポートにレポートが添付されません。（136026）
- アクセス制御ポリシーを複数のデバイスに適用すると、防御センターでは Web インターフェイスの [Task Status] ページ、[Access Control policy] ページ、および [Device Management] ページでタスク ステータスが異なる表示になります。[Device Management] ページ（[Devices] > [Device Management]）のステータスが正しい表示です。（136364、136614 ）
- ヘルス イベント テーブルに基づいてカスタム ワークフローを作成すると、防御センターによりイベント ビューアに競合データが表示される場合があります。（136419）
- カスタム侵入ルールを `.rtf` ファイルとしてインポートした場合、`rtf` ファイル タイプはサポートされていないという警告が出ません。（136500）
- 物理インターフェイスを無効にすると、それに関連付けられる論理インターフェイスは無効になりますが、管理対象デバイスのアプライアンス エディタの [Interfaces] タブでは緑色のままです。（136560）
- syslog または SNMP トラップ サーバに記録された接続イベントが、誤った [URL Reputation] 値を持つ場合があります。（138504、139466）
- セキュリティ インテリジェンス ソース/宛先メタデータ（rec_type:281）で、eStreamer サーバがソースを宛先として認識し、宛先をソースとして認識します。（138740）

- アクセス制御ポリシーでは、ポリシーのセキュリティ インテリジェンス ブラックリストの前にシステムは特定の信頼ルールを処理します。最初の監視ルールの前、またはアプリケーション、URL、ユーザ、または位置情報に基づくネットワーク条件を持つルールの前に置かれた信頼ルールは、ブラックリストの前に処理されます。つまり、アクセス制御ポリシーの最上位に近い信頼ルール（最も小さい番号のルール）または単純なポリシーで使用される信頼ルールでは、ブラックリストに登録されるべきトラフィックが登録されず、無検査で通過することを許可します。（138743、139017）
- 侵入ポリシーの [Drop When Inline] を無効にすると、トラフィックで検知されたパケットのインライン正規化による変更が停止し、どのようなトラフィックが変更されるかが示されません。場合によっては、[Drop When Inline] を再度有効にした後、ネットワークの他のデバイスやアプリケーションも同じように動作しないことがあります。（139174、139177）
- セキュリティ問題 Sourcefire は Intelligent Platform Management Interface（IPMI）標準（CVE-2013-4786）に内在する脆弱性を認識しています。アプライアンスの Lights-Out-Management（LOM）を有効にすると、この脆弱性にさらされます。脆弱性を軽減するには、信頼されるユーザのみがアクセス可能なセキュアな管理ネットワークにアプライアンスを展開し、複雑で、辞書に載っていない単語からなる 20 バイトのパスワードを使用します。この脆弱性を回避せず、LOM を有効にする場合は、3 か月ごとに複雑なパスワードを変更してください。この脆弱性のリスクを回避するには、LOM を有効にしないでください。（139286、140954）

以前のバージョンで導入された機能

以前のバージョンで説明された機能は、他の新機能に取って代わったり、解決済みの問題によって更新されることがあります。

5.3

次の機能は、バージョン 5.3 で導入されました。

ファイルのキャプチャと保存

ライセンス：マルウェア
サポートされるデバイス：シリーズ 3、仮想、X-Series
サポートされる防御センター：任意（DC500 を除く）

ファイル キャプチャ機能はファイル タイプまたはファイル配置に基づいて、ネットワーク トラフィックから目的のファイルを自動的に分割する機能を提供します。一度キャプチャされると、ファイルはローカルで FirePOWER アプライアンスに保存されるか、Sourcefire のクラウドベースのサンドボックス テクノロジーである動態分析を使用した、追加のマルウェア分析のために自動的に送信できます。

ファイル キャプチャはファイル ポリシーの一部として設定されます。ファイルを一意に識別し、ファイル ストレージでの重複を減らすために、ファイルごとに SHA-256 が計算されています。キャプチャされたファイルは FirePOWER アプライアンスのプライマリ ハード ドライブに保存されます。

キャプチャされたファイルは動態分析のために手動で送信するか、または、イベント テーブル ビュー、ネットワーク ファイルの File Trajectory 機能、およびキャプチャ ファイルのテーブル ビューを使って FirePOWER アプライアンスからダウンロードできます。

動態分析、脅威スコア、および要約レポート

ライセンス：マルウェア
サポートされるデバイス：シリーズ 3、仮想、X-Series
サポートされる防御センター：任意（DC500 を除く）

バージョン 5.3 では、クラウド ベースのテクノロジーを使用することにより、ネットワークの新しいゼロデイの悪意のある動作を迅速に特定する機能を最大化する、動態分析が導入されています。この機能を設定した場合、未知の場所にある以前には検知できなかったファイルを Sourcefire クラウドに送信し、ファイルの動作を掘り下げて分析することができます。その動作に基づいて脅威スコアが判定され、防御センターに通知されます。脅威スコアが高いほど、ファイルが悪意のあるものである可能性が高く、脅威スコアのレベルに基づいて対応策を実行できます。

Sourcefire はまた、分析に関する詳細と、なぜ脅威スコアがファイルに割り当てられたかを示す、関連する動態分析要約レポートも提供します。この追加情報はマルウェアの識別と検出機能の最適化に役立ちます。

自動的にファイルをキャプチャし、動態分析のために送信するようにシステムを設定することも、分析のためにファイルをオンデマンドで送信することもできます。

カスタム検出

ライセンス：マルウェア
サポートされるデバイス：シリーズ 3、仮想、X-Series
サポートされる防御センター：任意（DC500 を除く）

カスタム ファイル検出は、Sourcefire がファイルを悪意があると識別しなかった場合でも、ネットワークを移動する任意のファイルを識別し、ブロックするために使用できます。これらの探索の実行にはクラウド接続を必要としないため、カスタム ファイル検出は任意の種類のプライベートなインテリジェンス データに対して使用する場合に最適です。

悪意のあるファイルを特定した場合、そのファイル固有の SHA-256 値をカスタム ファイル検出リストに追加することで、自動的にそのファイルをブロックできます。カスタム検出リストをクリーン リスト（特定のファイルをクリーンであるとマークできる）と組み合わせて使用できます。

カスタム ファイル検出リストとクリーン リストを併用することで、ユーザ個々の環境に対するマルウェア保護対策をカスタマイズできます。カスタム ファイル検出リストとクリーン リストは、各ファイル ポリシーにデフォルトで含まれており、ポリシーごとにいずれかのリスト、または両方のリストを使用しないことを選択できます。

Spero エンジン

ライセンス：マルウェア
サポートされるデバイス：シリーズ 3、仮想、X-Series
サポートされる防御センター：任意（DC500 を除く）

Spero エンジン機能はビッグ データを使用して、実行可能ファイル内の疑わしいマルウェアや潜在的な新しいマルウェアを検出するための、新たなクラウドベースの方法を提供します。Spero は実行可能ファイルの構造情報、参照されるダイナミック リンク ライブラリ（DLL）、および移植可能な実行可能ファイル（PE）ヘッダーのメタデータに基づき、実行可能ファイルのシグニチャを作成します。その後に、この機能は機械学習データ ツリーを分析し、ファイルにマルウェアが含まれているかどうかを判定します。Spero 分析結果はファイルの配置と共に考慮され、実行可能ファイルの最終的な配置を生成します。

SMB ファイルの検出

ライセンス：保護
サポートされるデバイス：機能に依存
サポートされる防御センター：機能に依存

バージョン 5.3 では、サーバ メッセージ ブロック（SMB）経由で転送されたファイルを含む、NetBIOS-ssn（NetBIOS Send-Sequence-Number）トラフィックで転送されるファイルを検出、検査、ブロックできるようになりました。

AMP クラウド接続

ライセンス：マルウェア、URL フィルタリング
サポートされる防御センター：任意（DC500 を除く）

バージョン 5.3 以前は、Sourcefire クラウドに接続するには TCP ポート 32137 および防御センターからクラウドへの直接接続を使用しなければなりませんでした。

バージョン 5.3 では、マルウェアの検出と動態分析を行うための Sourcefire クラウドへの接続に、プロキシのサポートが導入されました。以前は、TCP ポート 32137 を使用しなければなりませんでしたが、現在ではデフォルトで TCP ポート 443 を介して接続されるため、より多くの組織が接続して Sourcefire の高度なマルウェア インテリジェンスを利用できるようになっています。ポート 32137 の使用はまだサポートされていますが、もうデフォルト設定ではありません。

以前のバージョンの Sourcefire 3D System からバージョン 5.3 に更新すると、レガシー ポート 32137 の使用はデフォルトで有効になっていることに注意してください。更新後にポート 443 を介して接続する場合は、[Cloud Services] ページ（[System] > [Local] > [Configuration] > [Cloud Services]）のチェックボックスをオフにします。

ホストとイベントの相関 IOC 形式（セキュリティ侵害の表示）

ライセンス：FireSIGHT + 保護または FireAMP サブスクリプション
サポートされるデバイス：機能に依存
サポートされる防御センター：機能に依存

ホストとイベントを相関させることにより、攻撃によってセキュリティが侵害された可能性のあるネットワークのホストを特定することができるようになります。ホストとイベントの相関は、侵入イベント、接続イベント、セキュリティ インテリジェンス イベント、および FireAMP イベントからのデータを集計することにより、ネットワークのセキュリティ違反を迅速に診断し、これを阻止します。

この機能は、システムが特定の種類のセキュリティ侵害に対して侵害の痕跡（IOC）イベントを生成するかどうか、そしてそれらのイベントを当該ホストと相関させるかどうかをユーザが制御できる、Sourcefire 提供の IOC ルールを導入します。イベント生成時に、システムはその IOC イベントの影響を受けるホストに IOC タグを設定します。固有の検出ソースから最も多くの IOC イベントを関連付けられたホストは、セキュリティ侵害の可能性が一番高いホストです。違反が解決されると、IOC タグは削除されます。IOC イベントおよびホストのタグはホスト プロファイル、ネットワーク マップ、コンテキスト エクスプローラ、ダッシュボード、およびイベント ビューアで表示できます。

拡張セキュリティ インテリジェンスのイベント ストレージおよびビュー

ライセンス：保護
サポートされるデバイス：シリーズ 3、仮想、X-Series
サポートされる防御センター：任意（DC500 を除く）

システムがセキュリティ インテリジェンス データに基づきトラフィックをブラックリストに登録する、またはブラックリストに登録されたトラフィックを監視するように設定されている場合、ダッシュボードとコンテキスト エクスプローラでセキュリティ インテリジェンス イベントを表示できるようになりました。セキュリティ インテリジェンス イベントは、接続イベントと似ていますが、別々に保存、切り分けられ、独自のイベント ビュー、ワークフロー、カスタム分析ダッシュボード ウィジェットのプリセットを持っています。

簡素化された侵入ポリシーの変数管理

ライセンス：保護
サポートされるデバイス：任意
サポートされる防御センター：任意

変数セットの追加はオブジェクト マネージャでの変数管理を簡素化し、一元化します。カスタム変数セットを作成し、ネットワーク環境に合わせてデフォルトの変数セットをカスタマイズします。デフォルトの変数セットは、Sourcefire の提供するデフォルト変数とユーザが作成したカスタム変数の両方を含むマスターキーとして機能し、カスタム変数セットを自動入力するために使用できます。このセットの変数をカスタマイズすると、その変数を含む他のすべての変数セットに変更が伝播されます。

バージョン 5.2 からバージョン 5.3 への更新では既存の変数が変数セットに自動的に移行します。システム レベルの既存の変数はデフォルト変数セット内でカスタム変数になります。侵入ポリシー レベルで設定されたカスタム変数は、侵入ポリシーにより新しいカスタム変数セットにグループ化されます。

位置情報とアクセス制御

ライセンス：FireSIGHT
サポートされるデバイス：シリーズ 3、仮想
サポートされる防御センター：任意（DC500 を除く）

バージョン 5.3 では、アクセス制御ポリシー内の送信元または宛先の国に基づいてトラフィックをフィルタリングする機能が導入されました。位置情報フィルタを使用するには、個々の国を指定するか、またはアクセス制御ポリシー ルールで位置情報オブジェクトを参照します。

位置情報オブジェクトはオブジェクト マネージャで設定され、システムが監視対象ネットワークのトラフィックで特定した 1 つ以上の国を表します。国のカスタム グループを保存および編成するため、位置情報オブジェクトを作成します。

URL フィルタリング ライセンスの変更

ライセンス：保護 + URL フィルタリング
サポートされるデバイス：シリーズ 3、仮想、X-Series
サポートされる防御センター：任意（DC500 を除く）

Sourcefire では URL フィルタリングを有効にする制御ライセンスが不要になりました。保護ライセンスのみが必要です。URL フィルタリング ライセンスを初めて追加すると、防御センターは URL フィルタリングおよび自動更新を自動的に有効にします。

シリーズ 3 FirePOWER アプライアンスの 8300 ファミリ

サポートされるデバイス：3D8350、3D8360、3D8370、3D8390

バージョン 5.3 には シリーズ 3 FirePOWER 管理対象デバイスの強力な 8300 ファミリが導入されています。8300 ファミリは既存の シリーズ 3 8000 Series の管理対象デバイスのスタッキング、クラスタリング、既存のすべての NetMod、およびその他のすべての機能をサポートしています。さらに、3D8350 では 15Gbps、3D8360 では 30Gbps、3D8370 では 45Gbps、3D8390 では 60Gbps の、より速い接続スピードを実現する機能強化が行われています。

専用の AMP アプライアンス

サポートされるデバイス：AMP7150 および AMP8150

また、バージョン 5.3 には、Sourcefire の AMP 機能のパフォーマンスを最大化する追加処理能力を備えて設計された 2 つの新しい シリーズ 3 FirePower 管理対象デバイスも取り入れられています。AMP7150 は 32GB の RAM と 120GB のハード ドライブを備え、Small Form-Factor Pluggable（SFP）トランシーバをサポートする 71xx ファミリのデバイスです。AMP8150 は 96GB の RAM、2 つの CPU、24 のコア、および 400 GB のハード ドライブを搭載した 81xx ファミリのデバイスです。

ディスク マネージャの機能強化

ライセンス：任意
サポートされるデバイス：シリーズ 2、シリーズ 3、X-Series
サポートされる防御センター：シリーズ 2、シリーズ 3

バージョン 5.3 では Sourcefire により、すべてのアプライアンスにおいてディスク容量の管理とファイル プルーニングが改善されました。これらの機能強化はファイルのキャプチャ機能をサポートし、全体的なパフォーマンスを向上させます。

マルウェア ストレージ パック

サポートされるデバイス：8000 Series

Sourcefire では、キャプチャ ファイル用のローカル ストレージと、イベントおよび設定ストレージ用にメイン ハード ドライブ上の空きスペースを提供する、Sourcefire 付属のセカンド ハード ドライブ、すなわち *マルウェア ストレージ パック*の取り付けがサポートされるようになりました。すべての 8000 Series 管理対象デバイスにマルウェア ストレージ パックを追加できます（追加ストレージが付属して出荷される AMP8150 を除く）。マルウェア ストレージ パックはスタック型またはクラスタ型 8000 Series デバイスでもサポートされています（AMP8150 を除く）。

マルウェア ストレージ パックが追加された場合、互換性のある管理対象デバイスはこれを検出し、既存のファイル キャプチャを追加されたドライブに自動転送して、メイン ドライブの容量を空けます。

警告　サードパーティのハード ドライブは**取り付けないでください**。サポートされていないハード ドライブを取り付けると、デバイスが破損する可能性があります。

Sourcefire Software for X-Series

サポートされるデバイス：X-Series

バージョン 5.3 の Sourcefire 3D System は、X-Series オペレーティング システム（XOS）バージョン 9.7.2（以降）とバージョン 10.0（以降）を実行する X-Series アプライアンスでサポートされるようになりました。以前のバージョンの XOS を使用している場合は、Blue Coat システム サポートにお問い合わせください。X-Series の詳細については、『*Sourcefire Software for X-Series Installation and Configuration Guide*』を参照してください。

仮想アプライアンスの初期設定の改善

ライセンス：任意
サポートされるデバイス：仮想、X-Series
サポートされる防御センター：仮想

バージョン 5.3 では、vSphere ハイパーバイザまたは vCloud Director を使用して、vCloud のワークフローを離れることなく、仮想デバイスの初期設定を行うことができます。初期設定時のデフォルト パスワードの変更やネットワーキングの設定、初期検出モードの設定、管理元の防御センターの設定のために、仮想デバイスのコンソールに接続する必要がなくなりました。これらの設定手順は、vCloud 展開ワークフロー中にすべて実行できます。ESXi を使用して展開することも可能ですが、それには VMware コンソールで追加の設定が必要なことに注意してください。

変更された機能

- 実行時間の長いクエリの検索と停止に、シェル ベースのクエリ管理ツールを使用できるようになりました。クエリ管理ツールでは指定した分数よりも実行時間が長いクエリを検索し、それらのクエリを停止することができます。ユーザがクエリを停止すると、このツールにより監査ログと syslog にイベントが記録されます。

  このツールにアクセスできるのは、防御センターのシェル アクセス権限を持つ管理ユーザだけであることに注意してください。詳細については、防御センターのシェルで `query_manager -h` を入力するか、または『*Sourcefire 3D System User Guide*』の「Stopping Long-Running Queries」を参照してください。
- バージョン 5.3 以降、Sourcefire では、Web サーバにより参照されたトラフィックを、参照された接続の Web アプリケーションとして識別するようになりました。たとえば、advertising.com を介してアクセスされたアドバタイズメントが実際は CNN.com から参照されている場合、Sourcefire は CNN.com を Web アプリケーションとして識別します。
- 次のいずれかのポート条件を含むアクセス制御ルールは設定できなくなりました：`IP 0`、`IP-ENCAP 4`、`IPv6 41`、`IPv6-ROUTE 43`、`IPv6-FRAG 44`、`GRE 47`、または `IPv6-OPTS 60`。

  以前のバージョンの Sourcefire 3D System から更新すると、アクセス制御ポリシー ルール エディタが警告を付けて無効な規則をマークし、オブジェクト マネージャが無効なポート オブジェクトの値を TCP にリセットします。バグ 140709 についてコメントアウト
- スタックまたはクラスタを解除した場合、デバイスがプライマリ デバイス グループに留まるようになりました。バージョン 5.3 以前では、デバイスがスタックまたはクラスタに追加される前に属していたグループにデバイスが戻されました。
- NetFlow データ収集とログ作成のパフォーマンスと安定性が向上しました。Sourcefire はまた、NetFlow を有効にしたデバイスによりエクスポートされた接続のために、次の新しいフィールドを追加しました。[NetFlow Destination/Source Autonomous System]、[NetFlow Destination/Source Prefix]、[NetFlow Destination/Source TOS]、および [NetFlow SNMP Input/Output]。
- バージョン 5.3 以降、認証オブジェクトの作成に IPv6 アドレスを使用できるようになりました。シェル アカウントの認証には IPv6 アドレスによる認証オブジェクトを使用できないことに注意してください。
- バージョン 5.3 以降、シリーズ 3 管理対象デバイスで IPv6 高速パス ルールを作成する際に、固有の**イニシエータ** IP アドレスと**レスポンダ** IP アドレスを指定できるようになりました。バージョン 5.3 以前では、フィールドは固定され、[Any] に設定されていました。

- バージョン 5.3 を シリーズ 3 管理対象デバイスに新規にインストールする場合、Automatic Application Bypass（AAB）機能はデフォルトで有効になっています。以前のバージョンの Sourcefire 3D System から更新した場合は、AAB の設定は影響を受けません。単一パケットの処理に事前設定した時間が経過した場合にだけ、AAB が有効になることに注意してください。AAB が有効な場合、影響を受ける Snort プロセスはシステムにより強制終了されます。
- バージョン 5.3 への更新時に、システムは現在適用されているアクセス制御ポリシーと、最大 10 個の保存されているが適用されていないアクセス制御ポリシーに対するリビジョンを、変更を保ちながら保存できるようになりました。
- 複数のレポート生成タスクを同時にスケジュールした場合、システムはタスクを待ち行列に入れます。それらは [Task Status] ページ（[System] > [Monitoring] > [Task Status]）で表示できます。
- ポンド記号（#）を使用してセキュリティ ゾーン オブジェクトを指定することはできません。
- バージョン 5.3 以降、侵入ルールの `icode` 引数範囲で、-1 を最小値として使用できるようになりました。最小値として -1 を選択すると、範囲に ICMP コード 0 を含めることができます。
- Cyrus SASL 認証に対する攻撃を検出する、新規の SMTP プリプロセッサ アラートが追加されました。
- バージョン 5.3 以降、タイプ 502 侵入イベントに関するファイル ポリシー UUID メタデータがシステムに含まれるようになりました。
- ファイルの性質 [Neutral] は [Unknown] になりました。性質が [Unknown] のファイルは、クラウドが性質を割り当てる前にマルウェア クラウド検索が実行されたことを示します。
- 不正な認証ヘッダーを含むパケットを識別する複数の新しい Snort デコーダ ルールが追加されました。
- 接続サマリー テーブルの [Ingress Interface]、[Ingress Security Zone]、[Egress Interface]、または [Egress Security Zone] フィールドに基づくカスタム分析ダッシュボード ウィジェットは設定できなくなりました。
- バージョン 5.3 以降、すでにシステムにインストールされているバージョンの Sourcefire 位置情報データベース（GeoDB）をインストールしようとすると、システムがアラートを発行するようになりました。
- バージョン 5.3 以降、[Application Protocol Category]、[Client Category]、および [Web Application Category] の各条件を使用して相関ルールを作成できるようになりました。

サポート

Sourcefire をご購入いただき、ありがとうございました。https://support.sourcefire.com/ にアクセスし、『Sourcefire Support Welcome Kit』をダウンロードしてください。このサポート キットは、お客様による Sourcefire サポートの利用と、カスタマー センターのアカウントの設定をお手伝いします。

Sourcefire 防御センターまたは管理対象デバイスについての質問やサポートが必要な場合は、Sourcefire サポートにお問い合わせください。

- Sourcefire サポート サイト：https://support.sourcefire.com/
- 電子メールによる Sourcefire サポートへのお問い合わせ：support@sourcefire.com
- 電話による Sourcefire サポートへのお問い合わせ：410.423.1901 または 1.800.917.4134

X-Series プラットフォームに関する質問がある場合、またはサポートが必要な場合は、Blue Coat サポート サイトをご覧ください。https://www.bluecoat.com/support/contactsupport/。

Sourcefire 製品をご利用いただきありがとうございました。

特記事項

本書のいかなる部分もシスコの明確な書面による事前の許可なく、編集することはできず、また、その他別の著作物や任意のドキュメント、ユーザ マニュアルに加えることも、派生的な著作物の作成に使用することもできません。シスコは条件を随時変更する権利を留保し、本書の継続的な使用はこれらの条項に同意したものと見なされます。

免責事項

本書およびそこから入手できるすべての情報には正確ではないものや誤植が含まれていることがあります。シスコは随時本書を変更できます。シスコが管理するすべての Web サイト、ドキュメント、および/またはすべての製品情報の正確性や的確性について、シスコは一切の表明または保証を行いません。シスコが管理する Web サイト、ドキュメント、およびすべての製品情報は「現状のまま」提供され、シスコはすべての明示および暗黙の保証を否認します。これには権原の保証および特定目的に対する商品性および/または適合性が含まれますが、これらに限定されるものではありません。シスコはいかなる場合でも、シスコが管理する Web サイトまたは文書から発生、またはそれらに関連した任意の方法において生じた、直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、または結果的損害（代替商品または代替サービスの調達、データの損失、利益の損失、および/または事業の中断を含むが、これらに限定されない）に対して、それがどのように発生したか、あるいは契約、厳密な法的責任、過失あるいはその他の行為またはその他の任意の法的責任の理論に基づくものであるか否かにかかわらず、かつ、シスコがそうした損害の可能性を通知されていたとしても、一切責任を負いません。州または司法管轄区域によっては、結果的または偶発的な損害の制限または除外が許可されていないため、お客様に上記の制限が適用されない場合があります。