FireSIGHT システム リリース ノート

バージョン 5.3.1
初版：2014 年 7 月 17 日
最終更新日：2015 年 1 月 21 日

更新プロセスについて精通しているとしても、必ずこれらのリリース ノートをよく読んで理解してください。ここでは、サポートされているプラットフォーム、新規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 ブラウザの適合性について説明しています。また、これらのリリース ノートには、次のアプライアンスの前提条件、警告、および特別なインストールについての指示が記載されています。

- シリーズ 2 およびシリーズ 3 の防御センター（DC500、DC750、DC1000、DC1500、DC3000、および DC3500）
- 64 ビットの仮想防御センター

注 この更新は、防御センター **のみ**を対象としています。物理的または仮想的な管理対象デバイスや、Sourcefire Software for X-Series ではサポート**されていません**。

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

これらのリリース ノートは、FireSIGHT システムのバージョン 5.3.1 で有効です。バージョン 5.3.0.1 以上の FireSIGHT システムを実行しているアプライアンスをバージョン 5.3.1 へ更新することができます。

詳細については、次のセクションを参照してください。

Cisco Systems, Inc.
www.cisco.com

新しい機能

リリース ノートのこのセクションでは、新機能や更新された機能、および FireSIGHT システムのバージョン 5.3.1 に含まれる機能について概説しています。

詳細については、『*FireSIGHT システム User Guide*』、『*FireSIGHT システム Installation Guide*』、および『*FireSIGHT システム Virtual Installation Guide*』を参照してください。

Cisco ASA with FirePOWER Services の管理

バージョン 5.3.1 では、FireSIGHT 防御センターを使用して Cisco ASA with FirePOWER Services（ASA FirePOWER デバイス）を管理する機能が導入されています。バージョン 5.3.1 を実行している 防御センターは、次の ASA デバイス上で ASA FirePOWER モジュールを管理することができます。

- 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

バージョン 5.3.1 を実行している防御センターによって管理するためには、ASA FirePOWER モジュールはバージョン 5.3.1 を実行している**必要があります**。ASA FirePOWER モジュールは、ASA ソフトウェアのバージョン 9.2.2 以降を実行している前述のプラットフォームに**のみ**インストールすることができます。

Cisco ASA with FirePOWER Services の機能制限

防御センターを使用して Cisco ASA with FirePOWER Services デバイスを管理する場合は、ASA FirePOWER モジュールが最も重要なシステム ポリシーを提供し、アクセス制御、侵入検知と防御、ディスカバリ、および高度なマルウェア対策のためにトラフィックを FireSIGHT システムへ渡します。

インストールおよび適用されているライセンスに関係なく、ASA FirePOWER デバイスは FireSIGHT システム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、仮想プライベート ネットワーク（VPN）、ネットワーク アドレス変換（NAT）など）をサポート**しません**。

注 ASA プラットフォームにはこれらの機能が用意されており、ASA コマンドライン インターフェイス（CLI）、および Adaptive Security Device Manager（ASDM）を使用して設定されます。詳細については、ASA FirePOWER モジュールのドキュメントを参照してください。

- 防御センターの 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、再開、または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 デバイスに対してバックアップを作成したり、バックアップを復元したりすることは**できません**。
- VLAN タグの条件を使用して、トラフィックを照合するためのアクセス コントロール ルールを記述することは**できません**。

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

注 ASA FirePOWER デバイスが SPAN ポート モードで導入されている場合には、防御センターには ASA インターフェイスが表示**されません**。

用語

バージョン 5.3.1 では、FireSIGHT 防御センターを使用して Cisco ASA with FirePOWER Services を管理する機能が導入されています。バージョン 5.3 または バージョン 5.3.0.1 のドキュメントを参照している場合は、バージョン 5.3.1 のドキュメントと用語が異なることにお気付きになるかもしれません。

表 1　　用語の変更

バージョン 5.3.1 の用語	説明
シスコ	以前の *Sourcefire*
FireSIGHT システム	以前の *Sourcefire 3D System*
防御センター FireSIGHT 防御センター シスコ FireSIGHT 管理センター	以前の *Sourcefire 防御センター*
管理対象デバイス	以前の *Sourcefire 管理対象デバイス*
FireSIGHT 管理対象デバイス	FireSIGHT 防御センターによって管理されるすべてのデバイス（管理対象デバイスおよび ASA デバイス）
Cisco Adaptive Security Appliance（ASA） ASA デバイス	シスコ ASA ハードウェア

表 1　　用語の変更

バージョン 5.3.1 の用語	説明
Cisco ASA with FirePOWER Services	ASA FirePOWER モジュールがインストールされた ASA デバイス
ASA FirePOWER モジュール	適合する ASA デバイスにインストールされているハードウェアとソフトウェア
ASA ソフトウェア	Cisco ASA デバイスにインストールされているベース ソフトウェア

ヒント　シスコのドキュメントでは、防御センターのことを FireSIGHT 管理センターということがあります。防御センターと FireSIGHT 管理センターは同じアプライアンスです。

ドキュメントの最新情報

サポート サイトから、更新されたすべてのドキュメントをダウンロードすることができます。バージョン 5.3.1 では、新機能および変更された機能を反映し、ドキュメントについて報告された問題点を解決するために、次のドキュメントが更新されました。

- FireSIGHT System *Online Help*
- *FireSIGHT System User Guide*
- *FireSIGHT System Installation Guide*
- *FireSIGHT System Virtual Installation Guide*
- *FireSIGHT System eStreamer Integration Guide*
- *FireSIGHT System Database Access Guide*

バージョン 5.3.1 について更新されたドキュメントには次のエラーが含まれています。

- ドキュメントでは、スタック内のデバイスに関して、誤って次のように記載されています。

  ```
  If a secondary device fails, the primary device continues to sense traffic, generate alerts, and send traffic to all secondary devices.On failed secondary devices, traffic is dropped.A health alert is generated indicating loss of link.
  ```

  ドキュメントでは、スタック内のセカンダリ デバイスが失敗した場合、デフォルトでは、設定可能なバイパスが有効になっているインライン セットが、プライマリ デバイス上でバイパス モードになることを明記する必要があります。それ以外のすべての設定では、システムは、失敗したセカンダリ デバイスへ継続してトラフィックをロード バランシングします。いずれの場合も、リンクが失われたことを示すためのヘルス アラートが生成されます。（122708、123380、138433）
- ドキュメントには、ASA デバイス セキュリティ コンテキストを修正して、シングル コンテキスト モードからマルチ コンテキスト モードへ（またはその逆へ）切り替えるときに、セキュリティ ゾーンの設定からインターフェイスが削除されることが反映されていません。（141050、141064）

はじめる前に：更新と適合性に関する重要な注意事項

バージョン 5.3.1 の更新プロセスを開始する前に、更新プロセス中のシステムの動作について、および互換性の問題や、更新前や更新後に必要となる設定変更について理解しておく必要があります。

注意 シスコでは、保守作業用の時間帯、または導入によるサービスの中断が及ぼす影響が最も少ない時間帯に更新を行うことを強く推奨しています。

詳細については、次のセクションを参照してください。

設定およびイベントのバックアップのガイドライン

シスコでは更新を始める前に、アプライアンス上に存在するすべてのバックアップ ファイルを削除または移動してから、現行のイベントおよび設定データを外部の場所へバックアップすることを強く推奨しています。

防御センターを使用して、イベントおよび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、『*FireSIGHT システム User Guide*』を参照してください。

注 防御センターは、以前の更新によってローカルに保存されているバックアップを消去します。アーカイブされたバックアップを保持しておくには、バックアップを外部に保存します。

更新中の監査ロギング

Web インターフェイスを備えているアプライアンスを更新する場合は、システムで更新前タスクが完了し、最新の更新インターフェイス ページが表示された後でも、更新プロセスが完了しアプライアンスがリブートされるまでアプライアンスへのログイン試行は監査ログに反映されません。

バージョン 5.3.1 へ更新するためのバージョン要件

バージョン 5.3.1 へ更新するには、防御センターはバージョン 5.3.0.1 以上を実行している必要があります。それより前のバージョンを実行している場合は、サポート サイトから更新を取得できます。

注 この更新は、管理対象デバイス、またはSourcefire Software for X-Seriesではサポートされていません。

アプライアンスの現在のバージョンがこのリリースのバージョン（バージョン 5.3.1）に近いほど、更新にかかる時間が短くなります。

バージョン 5.3.1 へ更新するための時間およびディスク領域の要件

次の表は、バージョン 5.3.1 への更新についてのディスク領域と時間のガイドラインを示しています。防御センターを使用して管理対象デバイスを更新する場合には、防御センターで、/Volume パーティションについて追加のディスク領域が必要になることに注意してください。

注意 更新プロセス中は、どのタイミングにおいてもアプライアンスの更新の再開、またはリブートを**行わないで**ください。シスコは、参考用に時間の見積を提示しますが、実際の更新時間は、アプライアンス モデル、導入、および設定によって異なります。更新の事前チェック、およびリブートの後はシステムが稼働していないように見えることがあるので注意してください。これは予想される動作です。

更新によるリブートでは、データベースのチェックが行われます。データベースのチェックでエラーが見つかった場合は、更新が完了するまでの時間が長くなります。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の間は実行されません。

更新中に問題が発生した場合は、サポートに連絡してください。

表 2　時間とディスク領域の要件

アプライアンス	領域	ボリュームごとの領域	マネージャ上のボリュームごとの領域	時間
シリーズ 2 の防御センター	0 MB	2.16 GB	n/a	55 ～ 70 分
シリーズ 3 の防御センター	0 MB	2.2 GB	n/a	50 ～ 65 分
仮想の防御センター	0 MB	2.2 GB	n/a	ハードウェアに依存

バージョン 5.3.1 へ更新した後の製品の適合性

バージョン 5.3.1 を実行している防御センターは、管理対象デバイス、および ASA デバイス上にインストールされているASA FirePOWER モジュールを管理することができます。防御センターで管理できるようにするには、デバイスは、次の表に記載されているバージョンを実行している必要があります。

表 3　　管理対象のバージョン要件

アプライアンス	バージョン 5.3.1 を実行している防御センターで管理するための最小バージョン
物理的および仮想的な管理対象デバイス	バージョン 5.2 の FireSIGHT システム
Sourcefire Software for X-Series	バージョン 5.3 の FireSIGHT システム
ASA FirePOWER モジュール	バージョン 5.3.1 の FireSIGHT システム

オペレーティング システムの適合性

次のホスティング環境で 64 ビットの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

次の ASA プラットフォームでバージョン 9.2.2 以降を実行しているものについて、ASA FirePOWER モジュールをインストールできます。

- 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

詳細については、『*FireSIGHT システム Installation Guide*』または『*FireSIGHT システム Virtual Installation Guide*』を参照してください。

Web ブラウザの適合性

FireSIGHT システムの Web インターフェイス バージョン 5.3.1 は、次の表に記載されているブラウザについてテストされています。

表 4　　サポートされる Web ブラウザ

ブラウザ	有効にする必要があるオプションと必要な設定
Chrome 34	JavaScript、Cookie
Firefox 29	JavaScript、Cookie、Secure Sockets Layer（SSL）v3
Microsoft Internet Explorer 9、10、および 11	JavaScript、Cookie、Secure Sockets Layer（SSL）v3、128 ビットの暗号化、**アクティブ スクリプティング** セキュリティ設定、互換性ビュー、[Check for newer versions of stored pages] を [Automatically] に設定する

画面解像度の適合性

シスコでは、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解像度で使用できますが、高解像度にすると表示が最適化されます。

前のバージョンへ戻す

何らかの理由で、アプライアンスを FireSIGHT システムの以前のリリースに戻さなければならない場合は、サポートに詳細を問い合わせてください。

更新のインストール

更新を始める前に、これらのリリース ノート（具体的には「はじめる前に：更新と適合性に関する重要な注意事項」（P.5））をよく読んで理解しておく必要があります。

FireSIGHT システムのバージョン 5.3.0.1 以上を実行しているアプライアンスをバージョン 5.3.1 へ更新するには、ガイドライン、および以下の手順を参照してください。

- 「防御センターの更新」（P.10）
- 「シェルを使用した更新の実行」（P.12）

注　この更新は、物理的または仮想的な管理対象デバイスや、Sourcefire Software for X-Series ではサポート**されていません**。

注意　更新中は、ログイン プロンプトが表示されるまでアプライアンスをリブートまたはシャットダウン**しないで**ください。更新の事前チェックでシステムが稼働していないように見えることがありますが、これは予想される動作で、アプライアンスをリブートまたはシャットダウンする必要はありません。

更新のタイミング

更新プロセスはトラフィック インスペクション、トラフィック フロー、およびリンク ステートに影響を及ぼす可能性があるため、シスコでは更新を保守作業用の時間帯、または導入によるサービスの中断が及ぼす影響が少ない時間帯に更新を行うことを**強く**推奨しています。

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。

ペアリングされた防御センターでの更新のインストール

ハイ アベイラビリティ ペアの 1 つの防御センターの更新を開始すると、ペアリングされている他方の防御センターが、まだプライマリになっていない場合はプライマリになります。また、ペアリングされている防御センターは設定情報の共有を停止します。ペアリングされている防御センターは、通常の同期プロセスの一部としてソフトウェアの更新を受け取り**ません**。

操作の継続性を保証するために、ペアリングされている防御センターを同時に更新**しないで**ください。最初に、セカンダリ防御センターの更新手順を完了し、次にプライマリ防御センターを更新してください。

インストール後

防御センターで更新を実行した後で、デバイスの設定およびアクセス コントロール ポリシーを再適用する**必要があります**。アクセス コントロール ポリシーを適用すると、トラフィック フローおよび処理が一時的に停止することがあります。また、一部のパケットが検査されずに通過する可能性もあります。詳細については、『*FireSIGHT システム User Guide*』を参照してください。

導入が正常に稼働していることを確認するために、更新後にいくつかの追加手順を実行する必要があります。次の作業を行います。

- 更新が正常に終了したことを確認する
- 導入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
- バージョン 5.3.1 の最新のパッチに更新し、可能な場合は最新の拡張機能とセキュリティ修正パッチを使用する
- オプションとして、侵入ルールおよび脆弱性データベース（VDB）を更新し、アクセス コントロール ポリシーを再適用する
- 「新しい機能」（P.2）の情報に基づいて、必要な設定変更を行う

次のセクションには、更新を行うため手順に加えて、更新後の手順を実行する方法の詳細が含まれています。ここに記載されている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

仮想防御センターも含めて、防御センターを更新するには、このセクションの手順を使用します。バージョン 5.3.1 の更新では、防御センターがリブートされます。

注意 更新中は、ログイン プロンプトが表示されるまでアプライアンスをリブートまたはシャットダウン**しないで**ください。更新の事前チェックでシステムが稼働していないように見えることがありますが、これは予想される動作で、アプライアンスをリブートまたはシャットダウンする必要はありません。

注 防御センターをバージョン 5.3.1 に更新すると、アプライアンスから既存のアンインストーラが削除されます。

防御センターを更新する方法

ステップ 1 これらのリリース ノートを読んで、更新前の必要なタスクを完了します。

詳細については、「はじめる前に：更新と適合性に関する重要な注意事項」（P.5）を参照してください。

ステップ 2 サポート サイトから更新をダウンロードします。

- シリーズ 2 の防御センター：

  `Sourcefire_3D_Defense_Center_Patch-5.3.1-152.sh`
- シリーズ 3 および仮想防御センター：

  `Sourcefire_3D_Defense_Center_S3_Patch-5.3.1-152.sh`

注 更新はサポート サイトから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。

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

更新が防御センターへアップロードされます。Web インターフェイスには、アップロードした更新のタイプ、バージョン番号、および更新が生成された日時が表示されます。

ステップ 4 導入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。

ステップ 5 タスク キューを参照（[System] > [Monitoring] > [Task Status]）して、実行中のタスクがないことを確認します。

更新を開始したときに実行中であったタスクは停止し、失敗します。これらのタスクは再開できません。更新が完了した後でタスク 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。実行時間の長いタスクがある場合、更新を開始する前に、完了するのを待機する**必要があります**。

ステップ 6 [System] > [Updates] を選択します。

[Product Updates] タブが表示されます。

ステップ 7 アップロードした更新の隣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。

ステップ 8 防御センターを選択して [Install] をクリックします。更新をインストールして防御センターをリブート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、更新の進行状況の監視を開始することができます。ただし、防御センターが更新後に必要なチェックを完了したら、ログアウトします。ログインすると、[Upgrade Status] ページが表示されます。[Upgrade Status] ページには進捗バーが表示され、実行中のスクリプトに関する詳細な情報が示されます。

更新が何らかの理由で失敗すると、ページにはエラー メッセージが表示され、失敗の日時、更新が失敗したときに実行されていたスクリプト、およびサポートへ連絡するための指示が示されます。更新は再開**しないで**ください。

注意 更新で、（[Update Status] ページを手動でリフレッシュしたら、数分たっても進捗が表示されない、などの）その他の問題が発生した場合は、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。

更新が完了すると、防御センターに正常終了のメッセージが表示され、リブートします。

ステップ 9 更新が終了した後で、ブラウザ キャッシュを削除し、ブラウザを強制的にリロードします。このようにしない場合、ユーザ インターフェイスは予期しない動作をすることがあります。

ステップ 10 防御センターにログインします。

ステップ 11 エンド ユーザ ライセンス契約書（EULA）を確認し、承認します。EULA を承認しない場合、アプライアンスからログアウトされることに注意してください。

ステップ 12 [Help] > [About] を選択し、ソフトウェアのバージョンが正しくバージョン 5.3.1 と示されていることを確認します。また、防御センターのルール更新と VDB のバージョンを記録しておいてください。この情報は後で必要になります。

ステップ 13 導入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。

ステップ 14 サポート サイトで利用できるルール更新が、防御センター上のルールよりも新しい場合は、新しいルールをインポートします。

ルールの更新の詳細については、『*FireSIGHT システム User Guide*』を参照してください。

ステップ 15 サポート サイトで利用できる VDB が防御センター上の VDB よりも新しい場合は、最新の VDB をインストールします。

VDB の更新をインストールすると、トラフィック フローおよび処理が一時的に停止することがあります。また、一部のパケットが検査されずに通過する可能性もあります。詳細については、『*FireSIGHT システム User Guide*』を参照してください。

ステップ 16 すべての管理対象デバイスに、デバイスの設定を再適用します。

グレー表示されている [Apply] ボタンをもう一度アクティブにするには、デバイスの設定でいずれかのインターフェイスを編集し、変更を行わずに [Save] をクリックします。

ステップ 17 すべての管理対象デバイスに、アクセス コントロール ポリシーを再適用します。

注意 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 コントロール ポリシーを完全に再適用する必要があります。

アクセス コントロール ポリシーを適用すると、トラフィック フローおよび処理が一時的に停止することがあります。また、一部のパケットが検査されずに通過する可能性もあります。詳細については、『*FireSIGHT システム User Guide*』を参照してください。

ステップ 18 サポート サイトでバージョン 5.3.1 用のパッチを入手できる場合は、*FireSIGHT システム リリース ノート* で該当のバージョンについて記載されているとおりに、最新のパッチを適用します。最新の拡張機能とセキュリティ修正パッチを利用するには、最新のパッチに更新**する必要があります**。

注 防御センターでバージョン 5.3 からバージョン 5.3.1 に更新する際に FSIC 障害が発生した場合は、バージョン 5.3.1 に更新する前にバージョン 5.3.0.2 をインストールします。

シェルを使用した更新の実行

シスコでは防御センターで Web インターフェイスを使用して更新を行うことを推奨していますが、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珍しいケースもあります。

バージョン 5.3.1 の更新では、すべてのアプライアンスをリブートします。詳細については、「更新中の監査ロギング」（P.5）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方法：

ステップ 1 これらのリリース ノートを読んで、更新前の必要なタスクを完了します。

詳細については、「はじめる前に：更新と適合性に関する重要な注意事項」（P.5）を参照してください。

ステップ 2 サポート サイトから適切な更新をダウンロードします。

- シリーズ 2 の防御センター：

  `Sourcefire_3D_Defense_Center_Patch-5.3.1-152.sh`
- シリーズ 3 および仮想防御センター：

  `Sourcefire_3D_Defense_Center_S3_Patch-5.3.1-152.sh`

注 更新はサポート サイトから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。

ステップ 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のシェルにログインします。

仮想アプライアンスの場合は、仮想コンソールを使用して VMware vSphere クライアントにログインします。

ステップ 4 プロンプトで、要求されるパスワードを入力して、root ユーザとして更新プログラムを実行します。

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

update_name は、以前にダウンロードした更新のファイル名です。

更新プロセスが開始されます。

ステップ 5 更新が完了すると、アプライアンスがリブートします。更新を監視し、次のセクションの説明に従って更新後の手順を実行できます。

- 「防御センターの更新」（P.10）

注 防御センターでバージョン 5.3 からバージョン 5.3.1 に更新する際に FSIC 障害が発生した場合は、バージョン 5.3.1 に更新する前にバージョン 5.3.0.2 をインストールします。

解決済みの問題

次のセクションでは、バージョン 5.3.1 の更新で解決された問題をリストします。

バージョン 5.3.1 で解決された問題

- 侵入イベントのパケットのビューに、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場合がある問題を解決しました。（138208）
- カスタム変数を参照する侵入ルールをインポートできない問題を解決しました。（138211）
- Cisco IOS ヌル ルート修復モジュールで Telnet を有効にして、Cisco IOS ルータで既定で有効になるように Cisco IOS インスタンスのユーザ名を設定すると、Cisco IOS ヌル ルート修復が防御センターで失敗する問題を解決しました。（139506）
- すべての（any）ネットワークを除外する除外ネットワーク値を使用したネットワーク変数の作成を、システムが回避しなかった問題を解決しました。（139510）

既知の問題

バージョン 5.3.1 では、次の問題が既知の問題として報告されています。

- データベースのチェックのために、バージョン 5.3 以降を実行しているアプライアンスや ASA FirePOWER モジュールをリブートするための時間が追加で必要となります。データベースのチェック中にエラーが検出された場合、リブートには、データベースを修復するための追加の時間が必要となります。（135564、136439）
- GRE 47 ポート条件によってアクセス コントロール規則を作成することはできません。（140642、140644、140646、140648、140650）
- 防御センターから管理対象デバイスを削除して、別のデバイスを追加し、デフォルト アクションに関連付けられた侵入ポリシーと共にアクセス制御ポリシーを再適用した場合、システムは、防御センターが現在管理しているデバイスよりも多くのデバイスで侵入ポリシーが期限切れであることを示します。（140705）
- デバイスのグループにデバイス スタックを追加し、適用されるアクセス制御ポリシーを編集すると、ポリシーからすべての対象デバイスが削除され、新しいデバイスの追加ができなくなり、ポリシー名が破損されます。回避策として、デバイス グループからデバイス スタックを削除し、ターゲットのスタンドアロン デバイス、デバイス スタック、およびデバイス グループを個別に削除します。（140710）
- 防御センターにプロキシとシングルサインオン（SSO）の両方を設定したときに、プロキシが Cisco セキュリティ マネージャ（CSM）のサーバに接続できない場合、SSO はタイムアウトして失敗します。（140897）
- 単一の正常性ポリシーを 100 以上の管理対象デバイス システムに適用しようとすると、まれに問題が発生する場合があります。回避策として、正常性ポリシーを適用する管理対象デバイスの数を減らします。（140977）
- [Product Updates] ページ（[System] > [Updates]）で [Download Updates] をクリックして更新パッチを自動的にダウンロードしようとすると、防御センターが不正なパッチをダウンロードする場合があります。回避策として、[Product Updates] ページで [Upload Update] をクリックし、更新パッチを手動でダウンロードします。（141056）

- 事前に Web インターフェイスを使用して ASA デバイスを防御センターに登録していないと、防御センターの Web インターフェイスを使用してシングル サインオン（SSO）を設定することはできません。防御センターの SSO をハイ アベイラビリティ（HA）ペアに設定する場合、シスコは ASA デバイスを両方の防御センターに登録し、プライマリの防御センターから SSO を設定することを推奨します。（141150）
- 侵入イベントの通知として送信される syslog アラートに、正しくない侵入ルールの分類データが含まれる場合があります。（141213、141216、141220）
- eStreamer が多数のファイル イベントを取得すると、システムでメモリの問題が発生します。（141222）
- 適応型プロファイルを設定するとき、**ネットワーク**値としてネットワーク変数を使用すると、適応型プロファイルは失敗します。回避策として、明示的に IP アドレスまたはアドレス ブロックを指定します。（141225）
- トラフィックをブロックするアクセス制御ルールや侵入ルールを作成して、それらを、インラインのインターフェイス セットを使用する仮想管理対象デバイスに適用する場合、アプライアンスを再起動するまでトラフィックの中断が発生します。（141230）
- 設定のみのバックアップを作成する場合、バックアップ ファイルに余分なディスカバリ イベント データが含まれます。（141246）
- VLAN タグ オブジェクトを使用する保存済み検索設定を作成する場合、システムは、VLAN タグのオブジェクトを使用したフィールドの値を `0` にして検索設定を保存します。（141330）
- 多数のページを持つカスタム ワークフローを作成した場合、ページの右上部分にある時間ウィンドウによって、ワークフローの最後のページへのリンクが見えなくなる可能性があります。（141336）
- まれなケースとして、セキュリティ ゾーンに複数のパッシブ インターフェイスを追加した後に、管理対象デバイスの設定でセキュリティ ゾーンを参照した場合、設定の適用が失敗して、システムで検出の中断が発生します。（141625、141628）
- 1 つ以上の検出リソースが管理対象デバイスで応答しない場合、脆弱性データベース（VDB）の更新をインストールすると、システムに問題が発生する場合があります。（141758）
- まれなケースとして、多数のアクセス制御ポリシーの適用を完了した場合に、システムでメモリの問題が発生し、**アンマネージド ディスクの使用率が高い**ことを示す複数のヘルス アラートが生成される場合があります。（141830）

次の既知の問題は、以前のリリースで報告されたものです。

- [Destination Port/ICMP Code] が「0」の侵入イベントをシステムが生成した場合、[Intrusion Event Statistics] ページ（[Overview] > [Summary] > [Intrusion Event Statistics]）の [Top 10 Destination Ports] セクションでは、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]）は、ハイ アベイラビリティ ピア間で同期**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、変更を編集して適用する必要があります。（130612、130652）
- システムのプルーニングが開始する前にディスク領域の使用量がディスク領域のしきい値を超えた場合に、大規模なシステム バックアップが失敗する場合があります。（132501）
- RunQuery ツールを使用して `SHOW TABLES` コマンドを実行すると、クエリが失敗する場合があります。クエリの失敗を回避するには、RunQuery アプリケーションだけを使用してこのクエリを対話形式で実行します。（132685）
- 以前にインポートしたローカルの侵入ルールを削除した場合、その削除されたルールを再インポートできません。（132865）

- まれなケースとして、侵入ルールの 141：7 や 142：7 に対してシステムがイベントを生成しないことがあります。（132973）
- 管理対象デバイスのリモート バックアップに無関係な統合ファイルが含められ、防御センターで大規模なバックアップ ファイルが生成される場合があります。（133040）
- アプライアンスの CLI またはシェルを使用して、防御センターまたは管理対象デバイスの最大伝送ユニット（MTU）を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 MTU を編集することはできません。（133802）
- URL にアスタリスク（*）が含まれる URL オブジェクトを作成すると、システムは、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ション処理されたルールの警告を生成しません。URL オブジェクトの URL には、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 オプションの有効な侵入ポリシーによって生成された侵入イベントの 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` **アラート**です。（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、システムは、侵入イベントのテーブル ビューにセキュリティ ゾーン データを表示しません。（134402）
- [Fast Port Scan] オプションを有効にして Nmap スキャン修復を設定すると、Nmap の修復が失敗します。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場合、そのテーブルのレポートにはデータが取り込まれません。（134541）
- 同時システム バックアップのタスクをスケジュールして実行すると、システム パフォーマンスを低下させます。回避策として、スケジュール設定するタスクに時差を付けて、一度に 1 つのバックアップだけ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制御パラメータが有効な事前設定された LDAP 接続を編集する場合、[Fetch Groups] をクリックしても [Available Groups] ボックスに値が表示されません。使用可能なグループを取得するには、LDAP 接続を編集するとき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] を有効にすると、ダッシュボードまたはイベント ビューで IPv6 アドレスに関連付けられたホスト名が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際には、[Base Filter] フィールドに 450 文字を超えて入力することはできません。（135314）
- 夏時間（DST）の期間中にタスクをスケジュールすると、DST 以外の期間中はそのタスクが実行されない場合があります。回避策として、[Time Zone Preference] ページ（[Admin] > [User Preferences]）のローカル タイム ゾーンとして [Europe, London] を選択し、DST 以外の期間中にタスクを再作成します。（135480）
- SSH プリプロセッサ ルール 128：1 で、システムが誤検出を発生させることがあります。（135567）
- HTTP プリプロセッサ オプション [Extract Original Client IP Address] が有効なルールを含む侵入ポリシーを適用すると、トラフィックが専用プロキシ サーバを通過する場合に、侵入イベントの [Original Client IP] フィールドにシステムが正しくないデータを取り込むことがあります。（135651）
- ジョブ タイプとして [Report] を指定したタスクをスケジュールした場合、システムは、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を添付しません。（136026）

- 複数のデバイスにアクセス制御ポリシーを適用する場合、防御センターは、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、異なるタスク状態を表示します。[Device Management] ページ（[Devices] > [Device Management]）に表示されるものが正しい状態です。（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、防御センターはイベント ビューアに矛盾するデータを表示します。（136419）
- カスタムの侵入ルールを `.rtf` ファイルとしてインポートした場合、システムは、`.rtf` ファイル タイプがサポートされていないことを警告しません。（136500）
- セキュリティ インテリジェンス フィードを設定して、Windows オペレーティング システムが稼働するコンピュータで作成された**フィード URL** を指定した場合、システムは、送信された IP アドレスの数を [Security Intelligence] タブのツールチップに正しく表示しません。回避策として、`dos2unix` コマンドを使用してファイルを Windows のエンコーディングから UNIX のエンコーディングに変換し、[Security Intelligence] ページの [Update Feeds] をクリックします。（136557）
- 物理インターフェイスを無効にすると、それに関連付けらた論理インターフェイスも無効になりますが、その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）
- キャプチャされたファイル テーブルに基づいてカスタム テーブルを作成すると、システムがエラー メッセージを生成します。システムは、キャプチャされたファイル テーブルに基づいたカスタム テーブルの作成をサポートしていません。（136844）
- 40 文字を超えるホスト名で管理対象デバイスを登録すると、デバイスの登録が失敗します。（137235）
- フィルタ基準に次のいずれかの特殊文字を含めると、システムによるオブジェクト マネージャでのオブジェクトのフィルタ処理が予期したものになりません。ドル記号（`$`）、キャレット（`^`）、アスタリスク（`*`）、ブラケット（`[]`）、縦棒（`|`）、スラッシュ（`\`）、ピリオド（`.`）、疑問符（`?`）。（137493）
- システム ポリシーで Simple Network Management Protocol（SNMP）のポーリングを有効にした場合、いずれかのクラスタ化管理対象デバイスでハイ アベイラビリティ（HA）リンク インターフェイス設定を変更すると、システムが不正確な SNMP ポーリング要求を生成する場合があります。（137546）
- 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 サーバのログ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します。（137952）
- システムが DNS または NTP パケットを正しくない順序で受け取った場合、オペレーティング システムの概要（Operating System Summary）ワークフローに不正確な DNS サーバ数、NTP サーバ数、DNS ポート数が表示されます。（138047）
- ファイル イベントのテーブル ビューでは、不適格なファイル イベントのファイル履歴の表示をサポートしているように見えます。計算された SHA-256 値のあるファイルのファイル履歴だけを表示できます。（138155）
- X 軸が**ファイル名**のグラフを含む HTML または PDF 形式のレポートを生成すると、システムは、x 軸のファイル名に UTF-8 文字を表示しません。（138297）
- まれなケースとして、複数のデバイスを管理するために防御センターを使用したことがある場合、システムはダッシュボードに不正確なの侵入イベント数を表示します。（138298）
- まれなケースとして、侵入ポリシーの編集と再適用を何百回も行うと、侵入ルールの更新とシステムの更新が完了するまで 24 時間以上が必要になります。（138333）
- 位置情報データベース（GeoDB）の最新バージョンが防御センターにインストールされていて、同じバージョンの GeoDB に更新しようとすると、システムはエラー メッセージを生成します。（138348）

- Syslog や SNMP トラップ サーバのログに記録された接続イベントは、**URL レピュテーション**値が不正確な場合があります。（138504、139466）
- 導入内で複数のアクセス制御ポリシーを適用した場合、特定のアクセス制御ルールに一致する侵入イベントや接続イベントを検索すると（[Analysis] > [Search]）、他のポリシー内の無関係なルールによって生成されたイベントを取得することがあります。（138542）
- アクセス制御ルールを 1 つのポリシーから別のポリシーにカット アンド ペーストすることはできません。（138713）
- Security Intelligence Source/Destination メタデータ（rec_type:281）で、eStreamer サーバが送信元を宛先として、宛先を送信元として識別します。（138740）
- アクセス制御ポリシーで、システムは特定の信頼ルールをポリシーのセキュリティ インテリジェンス ブラックリストよりも前に処理します。最初のモニタ ルールの前、またはアプリケーション、URL、ユーザ、位置情報ベースのネットワーク状態のあるルールの前に配置された信頼ルールは、ブラックリストよりも前に処理されます。つまり、アクセス制御ポリシーの上部付近にある信頼ルール（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により、ブラックリストに登録される必要のあるトラフィックが、代わりに無検査で通過できるようになります。（138743、139017）
- 侵入ポリシーで [Drop When Inline] を無効にすると、インライン正規化はトラフィックで変更されたパケットの表示を停止し、システムはどのトラフィックが変更されたかを示しません。[Drop When Inline] を再度有効にした後に、ネットワーク上の他のデバイスやアプリケーションが同じように動作しなくなる場合があります。（139174、139177）
- セキュリティ上の既知の問題Sourcefireは、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）規格（CVE-2013-4786）の脆弱性を認識しています。アプライアンスで Lights-Out Management（LOM）を有効にすると、この脆弱性のリスクが顕在化します。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導入します。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）
- まれなケースとして、[Task Status] ページ（[System] > [Monitoring] > [Task Status]）が、失敗したシステム ポリシーの適用を成功していると誤って報告することがあります。（139428）
- 基本ポリシーによって互いを参照する 3 つ以上の侵入ポリシーを設定して保存すると、システムは [Intrusion Policy] ページ（[Policies] > [Intrusion] > [Intrusion Policy]）のすべてのポリシーの最終変更日を更新しません。回避策として、5 から 10 分間待機し、[Intrusion Policy] ページを更新します。（139647）
- 夏時間（DST）の適用期間から DST の非適用期間に移行する日が時間帯に含まれるレポートを設定して保存した場合、システムは指定時刻よりも 1 時間前に時間帯を開始するように調整します。回避策として、時間帯を 1 時間遅く開始するように設定します。（139713）
- 防御センター Web インターフェイスの [Object Manager] ページを介してグローバル ホワイトリストから IP アドレスを削除した場合、防御センターのコマンドライン インターフェイス（CLI）は変更されません。（139784）

支援が必要な場合

FireSIGHT システムをお選びいただき、ありがとうございます。

Sourcefire サポート

新しいお客様の場合、https://support.sourcefire.com/ にアクセスして「Sourcefire Support Welcome Kit」をダウンロードしてください。これは、Sourcefire の概要を理解して Customer Center のアカウントをセットアップするために役立つドキュメントです。

ご質問がある場合、更新された資料をダウンロードする場合、Sourcefire防御センターに関する支援が必要な場合は、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/。
- Sourcefire サポートの電子メール アドレス：support@sourcefire.com。
- Sourcefire サポートの電話番号：410-423-1901 または 1-800-917-4134。

シスコ サポート

マニュアルの入手方法、シスコ Bug Search Tool（BST）の使用方法、サービス要求の送信方法、シスコ ASA デバイスに関する追加情報の入手方法については、『*What's New in Cisco Product Documentation*』（http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html）を参照してください。

『*What's New in Cisco Product Documentation*』は、シスコの新規および改訂版の技術マニュアルの一覧も示し、RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツをデスクトップに配信することもできます。RSS フィードは無料のサービスです。

シスコ ASA デバイスに関してご質問がある場合や支援が必要な場合は、以下のシスコ サポートに連絡してください。

- シスコ サポート サイト：http://support.cisco.com/。
- シスコ サポートの電子メール アドレス：tac@cisco.com。
- シスコ サポートの電話番号：1-408-526-7209 または 1-800-553-2447。