バージョン別アップグレードのガイドラインと警告

この章では、Firepower ソフトウェアのアップグレードに関する重要なリリースに固有の情報を提供します。

アップグレードパッチで1つ以上のメジャーバージョンがスキップされた場合（つまり、最後のメジャーバージョンまたはそのパッチの 1 つからアップグレードしない場合）、中間バージョンの警告とガイドラインも確認する必要があります。その情報は、この章およびFirepower リリースノートに記載されています。

- 廃止された機能 （2 ページ）
- 廃止された FlexConfig コマンド （9 ページ）
- 複数のバージョンに関するガイドライン （10 ページ）
- バージョン 6.5.0 のガイドライン （13 ページ）
- バージョン 6.4.0.x ガイドライン （35 ページ）
- バージョン 6.4.0 のガイドライン （35 ページ）
- バージョン 6.3.0.x のガイドライン （39 ページ）
- バージョン 6.3.0 のガイドライン （39 ページ）
- バージョン 6.2.3.x ガイドライン （50 ページ）
- バージョン 6.2.3 ガイドライン （52 ページ）
- バージョン 6.2.2.x のガイドライン （55 ページ）
- バージョン 6.2.2 ガイドライン （56 ページ）
- バージョン 6.2.0.x のガイドライン （57 ページ）
- バージョン 6.2.0 ガイドライン （58 ページ）
- バージョン 6.1.0 ガイドライン （61 ページ）
- バージョン 6.0.0 ガイドライン （62 ページ）

廃止された機能

バージョン 6.5.0 で廃止された機能

これらの機能はバージョン 6.5.0 で廃止されました。

（注） バージョン 6.5.0 ではサポートされていますが、Cisco Firepower User Agent ソフトウェアとアイデンティティソースを使用したユーザ制御についてはサポートの終了が予定されています。今すぐ Cisco Identity Services Engine/Passive Identity Connector（ISE/ISE-PIC）に切り替えることを強くお勧めします。これにより、ユーザエージェントで使用できない機能も利用できるようになります。詳細については、Cisco Firepower Management Center コンフィギュレーション ガイドのページでご使用のバージョンの *Cisco Firepower* ユーザ エージェント コンフィギュレーション ガイド を参照してください。

表 *1*：バージョン *6.5.0* で廃止された機能

機能	説明
FMC CLI を無効にする機能	バージョン 6.3.0 では、明示的に有効にする必要がある FMC CLI が導入されました。バージョン 6.5.0 では、新しい展開とアップグレードされた展開の両方に対して、FMC CLI が自動的に有効になります。Linux シェル（エキスパートモードとも呼ばれる）にアクセスする場合は、CLI にログインしてから、**expert** コマンドを使用する必要があります。 **注意** Cisco TAC の指示に従って操作する場合を除き、シェルを使用して Firepower アプライアンスにアクセスしないよう強くお勧めします。 廃止されたオプション：**[システム（System）] > [設定（Configuration）] > [コンソール設定（Console Configuration）] > [CLIアクセスの有効化（Enable CLI Access）] チェックボックス**
TLS 1.0 および 1.1	セキュリティを強化するには： • キャプティブポータル（アクティブ認証）では、TLS 1.0 のサポートが廃止されました。 • ホスト入力で TLS 1.0 および TLS 1.1 のサポートが廃止されました。 クライアントが Firepower アプライアンスとの接続に失敗した場合は、TLS 1.2 をサポートするようにクライアントをアップグレードすることをお勧めします。

機能	説明
Firepower 4100/9300 用の TLS crypto アクセラレーション FXOS CLI コマンド	Firepower 4100/9300 の複数のコンテナインスタンスに対して TLS crypto アクセラレーションを許可する一環として、次の FXOS CLI コマンドを削除しました。 • **show hwCrypto** • **config hwCrypto** および、この FTD CLI コマンドを削除しました。 • **show crypto accelerator status** 代替手段の詳細については、新しい機能のマニュアルを参照してください。
Cisco Security Packet Analyzer の統合	バージョン 6.5.0 では、FMC と Cisco Security Packet Analyzer の統合のサポートを終了します。 廃止された画面/オプション： • **[システム（System）] > [統合（Integration）] > [パケットアナライザ（Packet Analyzer）]** • **[分析（Analysis）] > [詳細（Advanced）] > [パケットアナライザのクエリ（Packet Analyzer Queries）]** • ダッシュボードまたはイベントビューアでイベントを右クリックしたときの [クエリパケットアナライザ（Query Packet Analyzer）]
Firepower Management Center モデル MC750、1500、および 3500	MC750、MC1500、および MC3500 モデルでは、Firepower Management Center ソフトウェアをバージョン 6.5.0 以降にアップグレードしたり、このバージョンを新規インストールしたりできません。これらの FMC を使用してバージョン 6.5.0 以降のデバイスを管理することはできません。
Firepower ソフトウェアを搭載した ASA 5515-X および ASA 5585-X シリーズ デバイス	これらのモデルでは、Firepower ソフトウェア（FTD と ASA FirePOWER の両方）をバージョン 6.5.0+ にアップグレードしたり、このバージョンを新規インストールしたりできません。 • ASA 5515-X • ASA 5585-X-SSP-10、-20、-40、-60 ただし、バージョン 6.5.0 の FMC を使用して、古いデバイス（バージョン 6.2.3 ～ 6.4.x）を管理できます。

機能	説明
Firepower 7000/8000 シリーズデバイス	AMP モデルを含む、Firepower 7000/8000 シリーズデバイスでは、Firepower ソフトウェアをバージョン 6.5.0 以降にアップグレードしたり、このバージョンを新規インストールしたりできません。ただし、バージョン 6.5.0 の FMC を使用して、古いデバイス（バージョン 6.2.3 ～ 6.4.x）を管理できます。

バージョン 6.4.0 で廃止された機能

これらの機能はバージョン 6.4.0 で廃止されました。

表 *2:* バージョン *6.4.0* で廃止された機能

機能	説明
SSL ハードウェア アクセラレーション FTD CLI コマンド	TLS crypto アクセラレーション機能の一部として、次の FTD CLI コマンドを削除しました。 • **system support ssl-hw-accel enable** • **system support ssl-hw-accel disable** • **system support ssl-hw-status** 代替手段の詳細については、新しい機能のマニュアルを参照してください。

バージョン 6.3.0 で廃止された機能

これらの機能はバージョン 6.3.0 で廃止されました。

表 *3* : バージョン *6.3.0* で廃止された機能

機能	説明
復号化のためのEMS拡張機能のサポート（6.3.0 のみ）	バージョン 6.3.0 では、バージョン 6.2.3.8/6.2.3.9 で導入された EMS 拡張機能のサポートが中止されます。つまり、[復号 - 再署名（Decrypt-Resign）] と [復号 - 既知のキー（Decrypt-Known Key）] の両方の SSL ポリシーアクションが、ClientHello ネゴシエーション時に EMS 拡張機能をサポート（よりセキュアな通信が可能）しなくなります。EMS 拡張機能は、 RFC 7627 によって定義されています。 FMC 展開では、この機能は、デバイスのバージョンによって異なります。FMC をバージョン 6.3.0 にアップグレードしても、サポートされるバージョンがデバイスで実行されていれば、サポートは中止されません。ただし、デバイスをバージョン 6.3.0 にデバイスをアップグレードすると、サポートは中止されます。 サポートはバージョン 6.3.0.1 で再導入されています。
パッシブおよびインラインタップ インターフェイスの復号化	バージョン 6.3.0 では、パッシブモードまたはインラインタップモードのインターフェイスでの復号化トラフィックは、GUI を介して設定することはできますが、サポートされなくなりました。暗号化されたトラフィックのインスペクションは必然的に制限されます。
VMware 5.5 のホスティング	バージョン 6.3.0 以降の仮想展開は VMware vSphere/VMware ESXi 5.5 でテストされていません。Firepower ソフトウェアをアップグレードする前に、ホスティング環境をアップグレードすることをお勧めします。
Firepower ソフトウェアを搭載した ASA 5506-X シリーズおよび ASA 5512-X デバイス	これらのモデルでは、Firepower ソフトウェア（FTD と ASA FirePOWER の両方）のバージョン 6.3.0 以降へのアップグレードまたは新規インストールはできません。 • ASA 5506-X、5506H-X、5506W-X • ASA 5512-X ただし、バージョン 6.3.0 の FMC を使用して、古いデバイス（バージョン 6.1.0 ～ 6.2.3.x）を管理できます。

バージョン 6.2.3.x で廃止された機能

これらの機能はバージョン 6.2.3.x で廃止されました。

表 *4:* バージョン *6.2.3.x* で廃止された機能

機能	説明
バージョン 6.2.3.8 は使用不可	バージョン 6.2.3.8 は 2019 年 1 月 7 日にシスコサポートおよびダウンロードサイトから削除されました。このバージョンは、バージョン6.2.3.9に置き換えられます。バージョン6.2.3.8を実行している場合は、アップグレードすることを強くお勧めします。バージョン 6.2.3.8 を実行しているデバイスは、一定時間後にトラフィックの送受信を停止する可能性があります。 バージョン 6.2.3.8 から以降のパッチにアップグレードしてから、そのパッチをアンインストールすると、バージョン6.2.3.8に戻ることに注意してください。その時点で、ただちにアップグレードするか、バージョン 6.2.3.8 をアンインストールする必要があります。バージョン 6.2.3.8 のままにしないでください。

バージョン 6.2.1 で廃止された機能

これらの機能はバージョン 6.2.1 で廃止されました。

表 *5:* バージョン *6.2.1* で廃止された機能

機能	説明
バージョン 6.2.1 は使用不可	バージョン 6.2.1 は 2017 年 11 月 17 日にシスコサポートおよびダウンロードサイトから削除されました。このバージョンは、バージョン6.2.2に置き換えられました。バージョン6.2.2は同じ機能を提供し、すべてのFirepowerプラットフォームをサポートします。バージョン 6.2.1 を実行している場合は、アップグレードすることを強くお勧めします。

バージョン 6.2.0 で廃止された機能

これらの機能はバージョン 6.2.0 で廃止されました。

表 *6 :* バージョン *6.2.0* で廃止された機能

機能	説明
ネストされた相関ルール	

機能	説明
	バージョン 6.2.0 では、ネストされた相関ルールのサポートが終了します。ある相関ルールが別の相関ルールのトリガーとなっている場合、その相関ルールはネストされています。 たとえば、どちらも侵入イベントのトリガーであるルール A とルール B を作成する場合、「ルール A は true」をルール B の制約として使用できます。この設定では、ルール A はルール B 内にネストされています。 **自動設定の変更** アップグレードプロセスは、ネストされたルール（ルール A）からネストされたルール（ルール B）へ設定をコピーしてネストされたルールを削除することで、特定のネストされた相関ルールを「フラット化」します。また、アップグレードは、ホストプロファイル/ユーザ資格とスヌーズ/非アクティブ期間を、ネストされたルールからネストルールへコピーします。 非アクティブ期間を除いて、これらのすべての設定について、設定がネストルールに存在しない場合にのみ、システムはネストされたルールからネストルールへ設定をコピーできます。システムがネストされたルールからネストルールへ非アクティブ期間をコピーするときは、結果として生じるルールがネスト構成にもともと含まれる両方のルールの設定を使用するように、ネストルールの非アクティブ期間を保持します。 **アップグレードの失敗の回避** アップグレードする前に、ネストされた相関ルールを「フラット化」できることを確認してください。そうなっていなければ、アップグレードは失敗します。ネストされたルールとネストルールに特定の競合がある場合は、アップグレードによりネストされたルールをフラット化できないことに注意してください。アップグレードの失敗を回避するには、アップグレードの前に、以下のように相関ルールを変更します。 • ネストされた構成内で 1 つのルールだけがこれらの設定を指定するように、ホストプロファイル資格、ユーザ資格、スヌーズ期間の設定をネストされたルールまたはネストルールから削除します。 • 接続トラッカーを任意のネストされたルールから削除します。 • ホストプロファイル資格、ユーザ資格、スヌーズ期間、非アクティブ期間を、true にする必要がないネストされたルールから削除します。つまり、ネストルール内の OR 演算子を使用して他のルールの条件にリンクされているネストされたルールから、これらの要素を削除します。

廃止された FlexConfig コマンド

いくつかの Firepower Threat Defense の機能は、ASA 設定コマンドを使用して設定されます。バージョン 6.2（FMC 展開）以降では、Smart CLI または FlexConfig を使用して、他の方法では Web インターフェイスでサポートされないさまざまな ASA 機能を手動で設定できます。

FTD アップグレードにより、以前に FlexConfig を使用して設定した機能について、GUI またはスマート CLI のサポートが追加されることがあります。これにより、現在使用している FlexConfig コマンドが廃止される可能性があります。既存の設定は引き続き動作し、展開も可能ですが、新しく廃止されたコマンドを使用して FlexConfig オブジェクトを割り当てたり作成したりすることはできなくなります。

アップグレード後、FlexConfig ポリシーおよび FlexConfig オブジェクトを確認してください。廃止されたコマンドが含まれている場合、メッセージは問題を示します。設定をやり直すことをお勧めします。新しい設定を確認したら、問題のある FlexConfig オブジェクトまたは FlexConfig コマンドを削除できます。

Firepower Management Center を使用した FTD

次の表に、廃止された FlexConfig オブジェクトとそれらに関連付けられているテキスト オブジェクトを示します。事前定義されたオブジェクトの完全なリストについては、『Firepower Management Center Configuration Guide』を参照してください。

表 *7 : FMC* を使用した *FTD*：廃止された *FlexConfig* オブジェクト

非推奨メソッド	オブジェクト	詳細	新しいロケーション
6.3.0 以降	FlexConfig オブジェクト： • Default_DNS_Configure 関連するテキストオブジェクト： • defaultDNSNameServerList • defaultDNSParameters	デフォルト DNS グループを設定します。デフォルト DNS グループでは、データインターフェイスの完全修飾ドメイン名を解決する際に使用できる DNS サーバを定義します。これにより、IP アドレスではなくホスト名を使用して、CLI で **ping** などのコマンドを使用することができます。	FTD プラットフォーム設定ポリシーで、データインターフェイスの DNS を設定します。

非推奨メソッド	オブジェクト	詳細	新しいロケーション
6.3.0 以降	FlexConfig オブジェクト： • TCP_Embryonic_Conn_Limit • TCP_Embryonic_Conn_Timeout 関連するテキストオブジェクト： • tcp_conn_misc • tcp_conn_limit • tcp_conn_timeout	初期接続制限およびタイムアウトを設定してSYNフラッドサービス妨害（DoS）攻撃から保護します。	これらの機能は、FTDサービスポリシーで設定します。ポリシーは、デバイスに割り当てられているアクセス制御ポリシーの [詳細設定（Advanced）] タブで確認できます。

次の表に、バージョン 6.2.3+ で、FDM を使用した FTD で新たに廃止された CLI コマンドの一覧を示します。機能がバージョン 6.2.0 に導入されたときに廃止されたコマンドを含む、廃止されたコマンドの完全なリストについては、『Firepower Management Center Configuration Guide』を参照してください。

表 *8*：*FMC* を使用した *FTD*：廃止された *CLI* コマンド

非推奨メソッド	コマンド	詳細
6.2.3 以降	**pager**	設定がブロックされます。

複数のバージョンに関するガイドライン

これらの重要なガイドラインと警告は、複数の Firepower メジャーバージョン、またはメジャーバージョンと複数のパッチに適用されます。

表 *9*：複数のバージョンに関するガイドライン

✓	ガイドライン	プラットフォーム	影響を受けるバージョン
	Firepower 1010 デバイス上の EtherChannel で出力トラフィックがブラックホール化される場合がある （11 ページ）	Firepower 1010	6.4.0 ～ 6.4.0.4
	アップグレードの失敗：コンテナインスタンスのディスク容量不足（11 ページ）	Firepower 4100/9300	6.3.0.1 ～ 6.5.0

✓	ガイドライン	プラットフォーム	影響を受けるバージョン
	動的分析 CA 証明書のパッチ/ホットフィックス （11 ページ）	任意	6.0.0 ～ 6.2.3.x

Firepower 1010 デバイス上の EtherChannel で出力トラフィックがブラックホール化される場合がある

展開：FTD を搭載した Firepower 1010

影響を受けるバージョン：バージョン 6.4.0 ～ 6.4.0.5

関連するバグ：CSCvq81354

FTD バージョン 6.4.0 ～ 6.4.0.5 を実行している Firepower 1010 デバイスでは EtherChannel を設定しないことを強くお勧めします（バージョン 6.4.0.1 および 6.4.0.2 はこのモデルではサポートされていないことに注意してください）。

内部トラフィックハッシュの問題により、Firepower 1010 デバイス上の EtherChannel では出力トラフィックがブラックホール化されることがあります。ハッシュは送信元 IP アドレスと宛先 IP アドレスに基づくため、特定の送信元 IP と宛先 IP のペアで一貫性のある動作になります。つまり、一部のトラフィックは常に機能し、一部のトラフィックは常に失敗します。

この問題は、次回の 6.4.0.x パッチで修正される予定です。また、バージョン 6.5.0 でも修正されます。

アップグレードの失敗：コンテナインスタンスのディスク容量不足

展開：FTD を搭載した Firepower 4100/9300

アップグレード元：バージョン 6.3.0 ～ 6.4.0.x

直接アップグレード先：バージョン 6.3.0.1 ～ 6.5.0

多くの場合はメジャーアップグレード時に（場合によってはパッチ適用時に）、コンテナインスタンスを使用して設定された FTD デバイスが、ディスク容量不足のエラーにより事前チェック段階で失敗することがあります。

この問題が発生した場合には、空きディスク容量を増やしてみてください。それでも解決しない場合は、Cisco TAC にお問い合わせください。

動的分析 CA 証明書のパッチ/ホットフィックス

展開：動的分析のためにファイルを送信する AMP for Networks（マルウェア検出）展開

影響を受けるバージョン：バージョン 6.0+

解決：CSCvj07038

2018 年 6 月 15 日、一部の Firepower 展開では、動的分析のためにファイルを送信できなくなりました。これは、AMP Threat Grid クラウドとの通信に必要だった CA 証明書が期限切れになったために発生しました。バージョン6.3.0は、新しい証明書を使用する最初のメジャーバージョンです。

（注） バージョン6.3.0+にアップグレードしない場合は、新しい証明書を取得して動的分析を再度有効にするために、パッチまたはホットフィックスを適用する必要があります。ただし、その後、パッチまたはホットフィックスが適用された展開をバージョン6.2.0またはバージョン6.2.3にアップグレードすると、古い証明書に戻るため、パッチまたはホットフィックスを再度適用する必要があります。

パッチまたはホットフィックスを初めてインストールする場合は、ファイアウォールで、FMC とその管理対象デバイスの両方から `fmc.api.threatgrid.com`（`panacea.threatgrid.com` を置き換える）へのアウトバウンド接続が許可されていることを確認してください。管理対象デバイスは、動的分析のためにファイルをクラウドに送信します。FMC は結果を照会します。

次の表に、メジャー バージョン シーケンスとプラットフォームごとに、古い証明書を使用するバージョンと、新しい証明書を使用するパッチおよびホットフィックスを示します。パッチおよびホットフィックスは、シスコサポートおよびダウンロードサイトで入手できます。リリースノートについては、Firepower リリースノートを参照してください。

表 *10*：新しい *CA* 証明書を使用するパッチとホットフィックス

古い証明書を使用するバージョン	新しい証明書を使用する最初のパッチ	新しい証明書を使用するホットフィックス	
6.2.3 ～ 6.2.3.3	6.2.3.4	ホットフィックス G	FTD デバイス
		ホットフィックス H	FMC、NGIPS デバイス
6.2.2 ～ 6.2.2.3	6.2.2.4	ホットフィックス BN	すべてのプラットフォーム
6.2.1	なし。アップグレードが必要です。	なし。アップグレードが必要です。	
6.2.0 ～ 6.2.0.5	6.2.0.6	ホットフィックス BX	FTD デバイス
		ホットフィックス BW	FMC、NGIPS デバイス

古い証明書を使用するバージョン	新しい証明書を使用する最初のパッチ	新しい証明書を使用するホットフィックス	
6.1.0 ～ 6.1.0.6	6.1.0.7	ホットフィックス EM	すべてのプラットフォーム
6.0.x	なし。アップグレードが必要です。	なし。アップグレードが必要です。	

バージョン 6.5.0 のガイドライン

表 *11* : バージョン *6.5.0* の新しいガイドライン

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	Firepower 1000 シリーズ デバイスではアップグレード後に電源の再投入が必要 （15 ページ）	Firepower 1000 シリーズ	6.4.0	6.5.0 以降
	バージョン 6.5.0-120 を使用したマルチドメイン FMC のアップグレード （15 ページ）	FMC	6.2.3 ～ 6.4.0.x	6.5.0 のみ
	アップグレードの失敗：NTP が同期していないアプライアンス （16 ページ）	任意（Any）	6.2.3 ~ 6.4.0	6.5.0 のみ
	アップグレードによって北米の Cisco Cloud に展開が割り当てられる （16 ページ）	任意（Any）	6.2.3 ~ 6.4.0	6.5.0 以降
	Cisco Threat Intelligence Director （TID） 動作の変更 （16 ページ）	FMC	6.2.3 ~ 6.4.0	6.5.0 以降
	新しい URL カテゴリとレピュテーション （17 ページ）	任意（Any）	6.2.3 ~ 6.4.0	6.5.0 以降

これらの事前に公開されたガイドラインと警告は、中間リリースに適用されます。アップグレードパスでメジャーバージョンがスキップされる場合は、このチェックリストを確認してください。

表 *12 :* 以前に公開されたバージョン *6.5.0* のガイドライン

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	アップグレードの失敗：コンテナインスタンスのディスク容量不足（11 ページ）	Firepower 4100/9300	6.3.0 ～ 6.4.0.x	6.3.0.1 ～ 6.5.0
	TLS 暗号化アクセラレーションの有効化/無効にすることは不可 （38 ページ）	Firepower 2100 シリーズ Firepower 4100/9300	6.2.3 ～ 6.3.0.x	6.4.0 以降
	URL フィルタリングキャッシュのタイムアウトが変更される可能性（43 ページ）	任意（Any）	6.2.3.x	6.3.0 以降
	FMC、7000/8000 シリーズ、NGIPSv で準備状況チェックに失敗する可能性 （44 ページ）	FMC Firepower 7000/8000 シリーズ NGIPSv	6.1.0 ～ 6.1.0.6 6.2.0 ～ 6.2.0.6 6.2.1 6.2.2 ～ 6.2.2.4 6.2.3 ～ 6.2.3.4	6.3.0 以降
	リモートアクセス VPN のデフォルト設定の変更によって VPN トラフィックがブロックされる可能性（44 ページ）	FMC を使用した FTD	6.2.0 ～ 6.2.3.x	6.3.0 以降
	FMC 1000/2500/4500 にはアップグレード前のホットフィックスが必要な場合がある （45 ページ）	MC1000、2500、および 4500	6.2.0 ～ 6.2.3.7	6.3.0 以降
	アプライアンスへのアクセスの更新されたセキュリティ （47 ページ）	任意（Any）	6.1.0 ～ 6.2.3.x	6.3.0 以降
	セキュリティインテリジェンスによって可能になるアプリケーションの識別 （47 ページ）	FMC の展開	6.1.0 ～ 6.2.3.x	6.3.0 以降
	アップグレード後に VDB を更新して CIP 検出を有効化 （48 ページ）	任意（Any）	6.1.0 ～ 6.2.3.x	6.3.0 以降
	無効な侵入変数セットによって展開に失敗する可能性 （48 ページ）	任意（Any）	6.1.0 ～ 6.2.3.x	6.3.0 以降

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	接続イベントと侵入イベントに関する Syslog の動作の変更 （49 ページ）	FMC	6.1.0 ～ 6.2.3.x	6.3.0 以降

Firepower 1000 シリーズ デバイスではアップグレード後に電源の再投入が必要

展開：Firepower 1000 シリーズ デバイス

アップグレード元：バージョン 6.4.0.x

直接アップグレード先：バージョン 6.5.0+

バージョン 6.5.0 では、Firepower 1000/2100 および Firepower 4100/9300 シリーズデバイス向けの FXOS CLI の「secure erase」機能が導入されています。

Firepower 1000 シリーズデバイスでは、この機能を適切に動作させるには、バージョン 6.5.0+ にアップグレードした後にデバイスの電源を再投入する必要があります。自動リブートでは十分ではありません。サポートされているその他のデバイスでは、電源の再投入は必要ありません。

バージョン 6.5.0-120 を使用したマルチドメイン FMC のアップグレード

展開：FMC

アップグレード元：バージョン 6.2.3 ～ 6.4.x

直接アップグレード先：バージョン 6.5.0 のみ

関連するバグ：CSCvr47499

導入環境でドメイン（マルチテナンシー）が使用されている場合に、子ドメインのアクセスコントロールポリシーで、デフォルトの NAP として子ドメインで作成されたカスタムネットワーク分析ポリシーを使用すると、FMC のバージョン 6.5.0-**115**（2019 年 9 月 26 日リリース）へのアップグレードに失敗します。

次の場合、アップグレードは失敗しません。

- 子ドメインのアクセス コントロール ポリシーで、デフォルトの NAP としてグローバルドメインで作成されたカスタムネットワーク分析ポリシーを使用する場合。
- 子ドメインのアクセス コントロール ポリシーで、NAP ルールにおいてカスタム NAP を使用する場合。

マルチドメイン展開では、バージョン 6.5.0-**120**（2019 年 10 月 8 日リリース）アップグレードパッケージを使用してください。

（注） 誤ってバージョン6.5.0-115を使用してアップグレードに失敗した場合は、問題を修正してアップグレードを再開する手順について Cisco TAC にお問い合わせください。

アップグレードの失敗：NTP が同期していないアプライアンス

展開：すべて

アップグレード元：バージョン 6.2.3 ～ 6.4.x

直接アップグレード先：バージョン 6.5.0 のみ

バージョン6.5.0にアップグレードする前に、時刻の取得に使用しているNTPサーバとFirepowerアプライアンスが同期されていることを確認する必要があります。同期されていないと、アップグレードに失敗する可能性があります。

FMC展開では、クロックの同期のずれが10秒を超えている場合に[時刻同期ステータス（Time Synchronization Status）]ヘルスモジュールによってアラートが表示されますが、手動でも確認してください。

時刻を確認するには、次の手順を実行します。

- FMC：[システム（System）] > [設定（Configuration）] > [時刻（Time）] を選択します。
- デバイス：**show time** CLI コマンドを使用します。

アップグレードによって北米の Cisco Cloud に展開が割り当てられる

展開：すべて

アップグレード元：バージョン 6.2.3 ～ 6.4.x

直接アップグレード先：バージョン 6.5.0+

Cisco Cloudサービスの「リージョン」が導入されました。導入環境の地域別クラウドは、Cisco Defense Orchestrator、Cisco Threat Response、Cisco Success Network、および Cisco Support Diagnostics の各機能に使用されます。

FMC 展開の場合、デフォルトでは、アップグレードによって米国（北米）リージョンに割り当てられます。リージョンは [システム（System）] > [統合（Integration）] > [クラウドサービス（Cloud Services）] ページで変更できます。

Cisco Threat Intelligence Director（TID） 動作の変更

展開：FMC

アップグレード元：バージョン 6.2.3 ～ 6.4.0.x

直接アップグレード先：バージョン 6.5.0+

バージョン 6.5.0+ では、TID ブロッキングおよびモニタリング監視可能アクションが、セキュリティ インテリジェンス ブラックリストを使用したブロッキングおよびモニタリングよりも優先されるようになりました。

[ブロック（Block）] TID 監視可能アクションを設定した場合は、トラフィックが [ブロック（Block）] に設定されたセキュリティ インテリジェンス ブラックリストにも一致していても、次のようになります。

- 接続イベントのセキュリティ インテリジェンス カテゴリは [TIDブロック（TID Block）] のバリアントになります。
- システムは、[ブロック済み（Blocked）] のアクション実施を伴う TID インシデントを生成します。

[モニタ（Monitor）] TID 監視可能アクションを設定した場合は、トラフィックが [モニタ（Monitor）] に設定されたセキュリティ インテリジェンス ブラックリストにも一致していても、次のようになります。

- 接続イベントのセキュリティ インテリジェンス カテゴリは [TIDモニタ（TID Monitor）] のバリアントになります。
- システムは、[モニタ済み（Monitored）] のアクション実施を伴う TID インシデントを生成します。

以前は、どちらの場合も、システムではカテゴリが分析別に報告され、TIDインシデントは生成されませんでした。

（注） システムは引き続き、トラフィックを以前と同様に効果的に処理します。以前ブロックされていたトラフィックは引き続きブロックされ、モニタ対象トラフィックは引き続きモニタされます。単に、どのコンポーネントが「クレジット」を取得するかが変更されます。また、生成される TID インシデントが増える場合もあります。

セキュリティ インテリジェンスと TID の両方を有効にした場合のシステム動作の詳細については、『Firepower Management Center Configuration Guide』の「TID-Firepower Management Center Action Prioritization」の情報を参照してください。

新しい URL カテゴリとレピュテーション

展開：すべて

アップグレード元：バージョン 6.2.3 ～ 6.4.0.x

直接アップグレード先：バージョン 6.5.0+

Cisco Talos Intelligence Group（Talos） は、URL の分類およびフィルタ処理のために、新しいカテゴリを導入し、レピュテーションの名前を変更しました。新しいURLカテゴリについては、Talos Intelligence Categories のサイトを参照してください。

また、ルール設定オプションは同じままですが、未分類およびレピュテーションのない URL の概念が新しくなっています。

- 未分類の URL は、疑わしい、ニュートラル、好ましい、または信頼できるというレピュテーションのいずれかになります。

  [未分類（Uncategorized）] の URL はフィルタ処理できますが、レピュテーションでさらに絞り込むことはできません。これらのルールは、レピュテーションに関係なく、すべての未分類 URL と一致します。

  カテゴリのない信頼できないルールのような設定は存在しないことに注意してください。それ以外の場合、信頼できないレピュテーションの未分類 URL は、新しい悪意のあるサイト脅威カテゴリに自動的に割り当てられます。

- レピュテーションのない URL は任意のカテゴリに属することができます。

  レピュテーションのない URL をフィルタ処理することはできません。「レピュテーションなし」に対応するオプションはルールエディタにありません。ただし、レピュテーションに [すべて（Any）] を指定して URL をフィルタ処理することは可能で、その場合はレピュテーションのない URL が含まれます。これらの URL もカテゴリで絞り込む必要があります。Any/Any ルールに対するユーティリティはありません。

次の表に、アップグレードでの変更点の概要を示します。これらの変更は、ほとんどのお客様にとって最小限の影響で済むように設計されており、アップグレード後の展開を妨げることもありませんが、これらのリリースノートおよび現在の URL フィルタリングの設定を確認することを強くお勧めします。慎重な計画と準備は、誤った手順を回避することに加えて、アップグレード後のトラブルシューティングにかかる時間を短縮するのに役立ちます。

表 *13*：アップグレード時の展開の変更

変更内容	詳細
URL ルールのカテゴリが変更されます。	アップグレードにより、次のポリシーで、新しいカテゴリセットのほぼ同等のルールが使用されるように URL ルールが変更されます。 • アクセスコントロール • SSL • QoS（FMC のみ） • 相関（FMC のみ） これらの変更により、余分なルールや無効になったルールが生じ、パフォーマンスが低下する可能性があります。マージされたカテゴリが設定に含まれている場合、許可またはブロックされる URL が若干変更される可能性があります。 カテゴリの変更に関する詳細については、「URL カテゴリの変更 （25 ページ）」を参照してください。

変更内容	詳細
URL ルールのレピュテーションの名前が変更されます。	アップグレードにより、新しいレピュテーション名を使用するように URL ルールが変更されます。 **1.** 信頼されていない（「高リスク」だった） **2.** 疑わしい（「疑わしいサイト」だった） **3.** ニュートラル（「セキュリティリスクのある無害なサイト」だった） **4.** 好ましい（「無害なサイト」だった） **5.** 信頼されている（「十分に既知」だった）
URL キャッシュをクリアします。	アップグレードによって URL キャッシュがクリアされます。このキャッシュには、システムが以前にクラウドで検索した結果が含まれています。ローカルデータセットに含まれていない URL については、アクセス時間が一時的に少し長くなることがあります。
「レガシー」イベントにラベルを付けます。	すでにログに記録されているイベントの場合、アップグレードにより、関連する URL のカテゴリおよびレピュテーション情報が「レガシー」としてラベル付けされます。これらのレガシーイベントは時間の経過とともにデータベースからエージアウトします。

URL カテゴリおよびレピュテーションのアップグレード前のアクション

アップグレードする前に、次のアクションを実行します。

表 *14:* アップグレード前のアクション

アクション	詳細
アプライアンスが Talos のリソースに到達できることを確認します。	アップグレード後、システムは次のシスコのリソースと通信できる必要があります。 • https://regsvc.sco.cisco.com/ - 登録 • https://est.sco.cisco.com/ - セキュア通信のための証明書を取得 • https://updates-talos.sco.cisco.com/ - クライアント/サーバマニフェストを取得 • http://updates.ironport.com/ - データベースのダウンロード（注：ポート 80 を使用） • https://v3.sds.cisco.com/ - クラウドクエリ クラウドクエリサービスは、次の IP アドレスブロックも使用します。 • IPv4 クラウドクエリ： • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 • IPv6 クラウドクエリ： • 2a04:e4c7:ffff::/48 • 2a04: e4c7: fffe::/48
潜在的なルールの問題を特定します。	今後の変更点を理解します。現在の URL フィルタリング設定を調べて、アップグレード後に実行する必要があるアクションを決定します（次のセクションを参照）。 （注） 廃止されたカテゴリを使用する URL ルールをこの時点で変更することができます。そうしない場合、それらを使用するルールによってアップグレード後の展開が妨げられます。 FMC 展開では、アクセスコントロールのルールや下位ポリシー（SSL など）のルールを含む、ポリシーの現在の保存されている設定に関する詳細情報を提供する、アクセスコントロール ポリシー レポートを生成することを推奨します。URL ルールごとに、現在のカテゴリ、レピュテーション、関連付けられているルールアクションが表示されます。FMC で **[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]** を選択し、該当するポリシーの横にあるレポートアイコン（ ）をクリックします。

URL カテゴリおよびレピュテーションのアップグレード後のアクション

アップグレード後に URL フィルタリング設定を再確認し、できるだけ早く次のアクションを実行する必要があります。展開のタイプとアップグレードによって行われた変更に応じて、一部の（すべてではない）の問題が GUI でマークされることがあります。たとえば、FMC/FDM のアクセスコントロール ポリシーでは、[警告の表示（Show Warnings）]（FMC）または [問題ルールの表示（Show Problem Rules）] (FDM) をクリックできます。

表 *15*：アップグレード後の操作

アクション	詳細
廃止されたカテゴリをルールから削除します。必須。 リスト：廃止されたカテゴリ（29 ページ）。	アップグレードでは、廃止されたカテゴリを使用する URL ルールは変更されません。これらを使用するルールは展開を阻止します。 FMC では、これらのルールにマークされます。
新しいカテゴリを含めるルールを作成または変更します。 リスト：新しいカテゴリ （28 ページ）。	ほとんどの新しいカテゴリは脅威を特定します。これらのカテゴリを使用することを強くお勧めします。 FMC では、この新しいカテゴリはこのアップグレード後にマークされませんが、今後、Talos によってカテゴリが追加される場合があります。これが行われる場合、新しいカテゴリがマークされます。
マージされたカテゴリの結果として変更されたルールを評価します。 リスト：マージされたカテゴリ （30 ページ）。	影響を受けたカテゴリのいずれかが含まれている各ルールに影響を受けたすべてのルールが含まれるようになります。元のカテゴリが異なるレピュテーションに関連付けられていた場合、新しいルールはさらに広い、より包含的なレピュテーションに関連付けられます。以前と同様に URL をフィルタリングするには、いくつかの設定を変更する必要があります。「マージされた URL カテゴリを持つルールのガイドライン（22 ページ）」を参照してください。 変更内容とプラットフォームがルールの警告を処理する方法に応じて、変更がマークされることがあります。たとえば、FMC は完全に冗長および完全にプリエンプション処理されたルールをマークしますが、部分的に重複したルールはマークしません。
分割されたカテゴリの結果として変更されたルールを評価します。 リスト：カテゴリの分割 （31 ページ）。	アップグレードにより、URL ルール内の古い単一のカテゴリが新しいカテゴリすべてに置き換えられ、新しいカテゴリは古いカテゴリにマッピングされます。これにより URL のフィルタリング方法は変更されませんが、影響を受けるルールを変更して、新しい精度を活用することができます。 これらの変更はマークされません。

アクション	詳細
名前が変更されたカテゴリまたは**変更されていない**カテゴリを把握します。 リスト：カテゴリの名前変更（33 ページ）および変更されていないカテゴリ （34 ページ）。	特に対処の必要はありませんが、これらの変更に注意する必要があります。 これらの変更はマークされません。
未分類およびレピュテーションのない URL の処理方法を評価します。	未分類の URL とレピュテーションのない URL を使用できるようになりましたが、未分類の URL を評価してフィルタリングすることも、レピュテーションのない URL をフィルタリングすることもできません。 未分類のカテゴリによってフィルタリングされるルール、または任意のレピュテーションが、期待どおりに動作するかどうか確認してください。

マージされた URL カテゴリを持つルールのガイドライン

アップグレード前に URL フィルタリング設定を確認する場合は、次のシナリオとガイドラインのどちらが適用されるかを決定します。これにより、アップグレード後の設定が予想どおりに実行され、問題を解決するためのクイックアクションを実行できるようになります。

表 *16*：マージされた *URL* カテゴリを持つルールのガイドライン

ガイドライン	詳細
ルールの順序によって、トラフィックに一致するルールが決定されます。	同じカテゴリを含むルールを検討する場合は、トラフィックが、その条件を含むリスト内の最初のルールと一致することに注意してください。
同じルール内のカテゴリと異なるルール内のカテゴリ	単一のルール内でカテゴリをマージすると、ルール内の単一のカテゴリにマージされます。たとえば、カテゴリ A とカテゴリ B がマージされてカテゴリ AB になり、カテゴリ A とカテゴリ B を持つルールがある場合、マージ後にルールは単一のカテゴリ AB を保持します。 異なるルールのカテゴリをマージすると、マージ後に各ルールで同じカテゴリを持つルールが個別に生成されます。たとえば、カテゴリ A とカテゴリ B がマージされてカテゴリ AB になり、カテゴリ A を持つルール 1 とカテゴリ B を持つルール 2 がある場合、マージ後にルール 1 とルール 2 にはカテゴリ AB がそれぞれ含まれます。この状況を解決する方法は、ルールの順序、ルールに関連付けられたアクションとレピュテーションレベル、ルールに含まれる他の URL カテゴリ、およびルールに含まれる非 URL 条件によって異なります。

ガイドライン	詳細
関連付けられたアクション	異なるルールのマージされたカテゴリが異なるアクションに関連付けられている場合、マージ後に、同じカテゴリに対して異なるアクションを持つ 2 つ以上のルールが生成される場合があります。
関連付けられているレピュテーションレベル	マージの前に異なるレピュテーションレベルに関連付けられたカテゴリが単一のルールに含まれている場合、マージされたカテゴリは、より包括的なレピュテーションレベルに関連付けられます。たとえば、カテゴリ A が特定のルールで [すべてのレピュテーション（Any reputation）] に関連付けられており、カテゴリ B が同じルールでレピュテーションレベル [3 - セキュリティリスクのある無害なサイト（3 - Benign sites with security risks）] に関連付けられている場合、マージ後に、そのルール内のカテゴリ AB は [すべてのレピュテーション（Any reputation）] に関連付けられます。
重複および冗長カテゴリとルール	マージ後、異なるルールには、異なるアクションとレピュテーションレベルに関連付けられている同じカテゴリが含まれる場合があります。 冗長ルールは完全に重複しているとは限りませんが、ルール順序が前にある別のルールが一致する場合、トラフィックに一致しなくなる可能性があります。たとえば、ルール 1 とカテゴリ A（[すべてのレピュテーション（Any Reputation）] に適用される）を事前マージし、ルール 2 とカテゴリ B（レピュテーション 1-3 のみに適用される）を事前マージする場合、マージ後に、ルール 1 とルール 2 の両方にカテゴリ AB が含まれるようになるが、ルール順序でルール 1 の順序が前にあると、ルール 2 が一致することはありません。 FMC において、同一のカテゴリとレピュテーションを持つルールでは警告が表示されます。ただし、これらの警告は、含まれているカテゴリが同じですが、レピュテーションが異なるルールを示すことはありません。 注意：重複または冗長カテゴリを解決する方法を決定する際には、ルールのすべての条件を考慮してください。
ルール内の他の URL カテゴリ	マージされた URL を含むルールには、他の URL カテゴリも含まれている場合があります。したがって、マージ後に特定のカテゴリが複製された場合は、これらのルールを削除するのではなく、変更する必要があることがあります。
ルール内の非 URL 条件	マージされた URL カテゴリを含むルールには、アプリケーション条件などの他のルール条件も含まれている場合があります。したがって、マージ後に特定のカテゴリが複製された場合は、これらのルールを削除するのではなく、変更する必要があることがあります。

次の表の例ではカテゴリ A とカテゴリ B を使用しています。現在はカテゴリ AB にマージされています。2 つのルールの例では、ルール 1 はルール 2 よりも前に表示されます。

表 *17:* マージされた *URL* カテゴリを持つルールの例

シナリオ	アップグレード前	アップグレード後
同じルール内のマージされたカテゴリ	ルール 1 にはカテゴリ A とカテゴリ B が含まれる。	ルール 1 にはカテゴリ AB が含まれる。
異なるルール内でマージされたカテゴリ	ルール 1 にはカテゴリ A が含まれる。 ルール 2 にはカテゴリ B が含まれる。	ルール 1 にはカテゴリ AB が含まれる。 ルール 2 にはカテゴリ AB が含まれる。 具体的な結果は、リスト内のルールの順序、レピュテーションレベル、および関連付けられたアクションによって異なります。また、冗長性を解決する方法を決定する際に、ルール内の他のすべての条件も考慮する必要があります。
異なるルール内でマージされたカテゴリには異なるアクションが含まれる （レピュテーションは同じ）	ルール 1 には [許可（Allow）] に設定されたカテゴリ A が含まれる。 ルール 2 には [ブロック（Block）] に設定されたカテゴリ B が含まれる。 （レピュテーションは同じ）	ルール 1 には [許可（Allow）] に設定されたカテゴリ AB が含まれる。 ルール 2 には [ブロック（Block）] に設定されたカテゴリ AB が含まれる。 ルール 1 は、このカテゴリのすべてのトラフィックに一致します。 ルール 2 がトラフィックに一致することはなく、カテゴリとレピュテーションの両方が同じであるため、マージ後に警告を表示した場合は、警告インジケータが表示されます。
同じルール内でマージされたカテゴリには異なるレピュテーションレベルが含まれる	ルール 1 には次が含まれます。 レピュテーション Any のカテゴリ A レピュテーション 1-3 のカテゴリ B	ルール 1 にはレピュテーション Any のカテゴリ AB が含まれる。

シナリオ	アップグレード前	アップグレード後
異なるルール内でマージされたカテゴリには異なるレピュテーションレベルが含まれる	ルール 1 にはレピュテーション Any のカテゴリ A が含まれる。 ルール 2 にはレピュテーション 1-3 のカテゴリ B が含まれる。	ルール 1 にはレピュテーション Any のカテゴリ AB が含まれる。 ルール 2 にはレピュテーション 1-3 のカテゴリ AB が含まれる。 ルール 1 は、このカテゴリのすべてのトラフィックに一致します。 ルール 2 がトラフィックに一致することはありませんが、レピュテーションが同一でないため、警告インジケータは表示されません。

URL カテゴリの変更

このテーブルを使用して、URL カテゴリの変更方法を判定します。

表 *18*：古い *URL* カテゴリのインデックス

古いカテゴリ	変更内容		古いカテゴリ	変更内容
妊娠中絶	マージされたカテゴリ （30 ページ）		軍	変更されていないカテゴリ （34 ページ）
乱用薬物	マージされたカテゴリ （30 ページ）		自動車	カテゴリの名前変更 （33 ページ）
アダルトとポルノ	カテゴリの分割 （31 ページ）		音楽	カテゴリの名前変更 （33 ページ）
アルコールとタバコ	カテゴリの分割 （31 ページ）		ニュースとメディア	カテゴリの名前変更 （33 ページ）
ボットネット	カテゴリの名前変更 （33 ページ）		ヌード	カテゴリの名前変更 （33 ページ）
ビジネスと経済	カテゴリの分割 （31 ページ）		オンライン グリーティング カード	カテゴリの名前変更 （33 ページ）
不正	カテゴリの名前変更 （33 ページ）		オープン HTTP プロキシ	カテゴリの名前変更 （33 ページ）

古いカテゴリ	変更内容		古いカテゴリ	変更内容
コンピュータとインターネット情報	カテゴリの分割 （31 ページ）		パークドメイン	変更されていないカテゴリ （34 ページ）
コンピュータとインターネットセキュリティ	カテゴリの分割 （31 ページ）		サーフへの支払い	マージされたカテゴリ （30 ページ）
確認済みのスパム送信元	マージされたカテゴリ （30 ページ）		ピアツーピア	カテゴリの名前変更 （33 ページ）
コンテンツ配信ネットワーク	マージされたカテゴリ （30 ページ）		個人のサイトやブログ	カテゴリの分割 （31 ページ）
カルトとオカルト	カテゴリの分割 （31 ページ）		個人ストレージ	カテゴリの分割 （31 ページ）
出会い系	変更されていないカテゴリ （34 ページ）		哲学と政治的主張	カテゴリの名前変更 （33 ページ）
休止サイト	カテゴリの名前変更 （33 ページ）		フィッシングとその他の不正行為	カテゴリの名前変更 （33 ページ）
動的生成コンテンツ	マージされたカテゴリ （30 ページ）		プライベート IP アドレス	廃止されたカテゴリ （29 ページ）
教育機関	マージされたカテゴリ （30 ページ）		プロキシ回避とアノニマイザー	カテゴリの名前変更 （33 ページ）
エンターテイメントとアート	カテゴリの分割 （31 ページ）		要検討	カテゴリの名前変更 （33 ページ）
ファッションと美容	カテゴリの名前変更 （33 ページ）		不動産	変更されていないカテゴリ （34 ページ）
金融サービス	カテゴリの名前変更 （33 ページ）		レクリエーションおよび趣味	マージされたカテゴリ （30 ページ）
食品と食事	カテゴリの名前変更 （33 ページ）		参照および調査	カテゴリの分割 （31 ページ）

古いカテゴリ	変更内容		古いカテゴリ	変更内容
ギャンブル	カテゴリの分割（31 ページ）		宗教	変更されていないカテゴリ （34 ページ）
ゲーム	変更されていないカテゴリ （34 ページ）		検索エンジン	マージされたカテゴリ （30 ページ）
政府/自治体	マージされたカテゴリ （30 ページ）		性教育	マージされたカテゴリ （30 ページ）
総額	マージされたカテゴリ （30 ページ）		シェアウェアとフリーウェア	カテゴリの名前変更 （33 ページ）
ハッキング	マージされたカテゴリ （30 ページ）		ショッピング	変更されていないカテゴリ （34 ページ）
中傷と人種差別	カテゴリの名前変更 （33 ページ）		ソーシャルネットワーク	カテゴリの分割（31 ページ）
健康と薬	カテゴリの名前変更 （33 ページ）		社会	カテゴリの分割（31 ページ）
ホームとガーデン	カテゴリの分割（31 ページ）		スパム URL	マージされたカテゴリ （30 ページ）
狩猟と釣り	カテゴリの名前変更 （33 ページ）		Sports	マージされたカテゴリ （30 ページ）
法律違反	カテゴリの分割（31 ページ）		スパイウェアとアドウェア	変更されていないカテゴリ （34 ページ）
画像とビデオ検索	カテゴリの名前変更 （33 ページ）		ストリーミングメディア	カテゴリの名前変更 （33 ページ）
個人向け株式アドバイスとツール	カテゴリの名前変更 （33 ページ）		水着と肌着	カテゴリの名前変更 （33 ページ）
インターネット通信	カテゴリの分割（31 ページ）		トレーニングおよびツール	マージされたカテゴリ （30 ページ）

古いカテゴリ	変更内容		古いカテゴリ	変更内容
インターネットポータル	マージされたカテゴリ （30 ページ）		旅行	変更されていないカテゴリ （34 ページ）
求職	変更されていないカテゴリ （34 ページ）		未分類	廃止されたカテゴリ （29 ページ）
キーロガーとモニタリング	マージされたカテゴリ （30 ページ）		未確認のスパム送信元	マージされたカテゴリ （30 ページ）
こども用品	カテゴリの名前変更 （33 ページ）		暴力	マージされたカテゴリ （30 ページ）
リーガル	マージされたカテゴリ （30 ページ）		武器	変更されていないカテゴリ （34 ページ）
ローカル情報	カテゴリの名前変更 （33 ページ）		Web 広告	マージされたカテゴリ （30 ページ）
マルウェアサイト	変更されていないカテゴリ （34 ページ）		Web ベースの電子メール	カテゴリの分割 （31 ページ）
マリファナ	マージされたカテゴリ （30 ページ）		Web ホスティングサイト	カテゴリの名前変更 （33 ページ）

新しいカテゴリ

これらのテーブルには、完全に新しい URL カテゴリがリストされています。ほとんどの URL カテゴリでは脅威が特定されます。URL ルールを作成または変更して、新しい脅威カテゴリを含めることを強くお勧めします。既存の一部の URL カテゴリでは脅威が特定されることに注意してください。これらの URL カテゴリも含めることをお勧めします。脅威カテゴリのリストについては、Talos Intellience Categories のサイトを参照してください。

表 *19*：新しいカテゴリ

新しいカテゴリ
ダイナミックおよびレジデンシャル

表 *20* : 新しい脅威カテゴリ

新しい脅威カテゴリ
Bogon
クリプトジャッキング
DNS トンネリング
ドメイン生成アルゴリズム
ダイナミック DNS
電子バンキング詐欺
エクスプロイト
高リスクサイトおよびロケーション
侵害の兆候（IOC）
リンク共有
悪意のあるサイト
モバイルの脅威
新しく発見されたドメイン
第三者中継
P2P マルウェアノード
潜在的な DNS 再バインド
TOR exit ノード

廃止されたカテゴリ

アップグレードでは、廃止されたカテゴリを使用する URL ルールは変更されません。これらのルールによって展開が防止されるため、削除または変更する必要があります。

表 *21* : 廃止されたカテゴリ

廃止されたカテゴリ
未分類
プライベート IP アドレス

マージされたカテゴリ

影響を受けたカテゴリのいずれかが含まれている各ルールに影響を受けたすべてのルールが含まれるようになります。元のカテゴリが異なるレピュテーションに関連付けられていた場合、新しいルールはさらに広い、より包含的なレピュテーションに関連付けられます。以前と同様に URL をフィルタリングするには、いくつかの設定を変更する必要があります。「マージされた URL カテゴリを持つルールのガイドライン （22 ページ）」を参照してください。

URL ルールを作成または変更して、新しい脅威カテゴリ（スパム）を含めることを強くお勧めします。

表 *22*：マージされたカテゴリ

古いカテゴリ	新しくマージされたカテゴリ
Web 広告	アドバタイズメント
サーフへの支払い	
教育機関	教育
トレーニングおよびツール	
暴力	最高
総額	
政府/自治体	政府および法律
リーガル	
乱用薬物	違法ドラッグ
マリファナ	
動的生成コンテンツ	インフラストラクチャ
コンテンツ配信ネットワーク	
ハッキング	ハッキング
キーロガーとモニタリング	
検索エンジン	検索エンジンおよびポータル
インターネットポータル	
性教育	性教育
妊娠中絶	

古いカテゴリ	新しくマージされたカテゴリ
確認済みのスパム送信元	スパム（脅威カテゴリ）
スパム URL	
未確認のスパム送信元	
レクリエーションおよび趣味	スポーツおよびレクリエーション
スポーツ	

カテゴリの分割

アップグレードにより、URLルール内の古い単一のカテゴリが新しいカテゴリすべてに置き換えられ、新しいカテゴリは古いカテゴリにマッピングされます。アップグレード後、影響を受けるルールを変更して、新しい精度を活用することができます。

表 *23*：カテゴリの分割

古い単一カテゴリ	新しいカテゴリの分割
アダルトとポルノ	ポルノ
	アダルト
アルコールとタバコ	アルコール
	タバコ
ビジネスと経済	ビジネスおよび産業
	携帯電話（Mobile Phones）
コンピュータとインターネット情報	ソフトウェアアップデート
	コンピュータおよびインターネット
	SaaS および B2B
	オンライン会議
コンピュータとインターネットセキュリティ	コンピュータセキュリティ
	パーソナル VPN
カルトとオカルト	超常現象
	占星術

古い単一カテゴリ	新しいカテゴリの分割
エンターテイメントとアート	芸術
	エンターテイメント
ギャンブル	ギャンブル
	宝くじ
ホームとガーデン	自然
	DIY プロジェクト
法律違反	違法行為
	児童虐待コンテンツ
	違法ダウンロード
インターネット通信	インターネット電話
	チャットおよびインスタントメッセージ
個人のサイトやブログ	個人サイト
	オンラインコミュニティ
個人ストレージ	オンラインストレージおよびバックアップ
	ファイル転送サービス
参照および調査	科学技術
	社会科学
ソーシャルネットワーク	ソーシャルネットワーキング
	プロフェッショナル ネットワーキング
社会	社会および文化
	非政府組織
Web ベースの電子メール	Web ベースの電子メール
	組織の電子メール

カテゴリの名前変更

特に対処の必要はありませんが、これらの変更に注意する必要があります。URLルールを作成または変更して、新しい脅威カテゴリ（ボットネット、オープンHTTPプロキシ、フィッシング）を含めることを強くお勧めします。

表 *24*：カテゴリの名前変更

古いカテゴリ名	新しいカテゴリ名
ボットネット	ボットネット（脅威カテゴリ）
不正	不正および盗用
休止サイト	非実用的
ファッションと美容	ファッション
金融サービス	金融
食品と食事	飲食
中傷と人種差別	ヘイトスピーチ
健康と薬	健康および栄養
狩猟と釣り	ハンティング
画像とビデオ検索	写真検索と画像
個人向け株式アドバイスとツール	オンライントレード
子供用品	子供向け
ローカル情報	参考資料
自動車	乗り物
音楽	ストリーミングオーディオ
ニュースとメディア	ニュース
ヌード	性的でないヌード
オンライン グリーティング カード	デジタルポストカード
オープン HTTP プロキシ	オープン HTTP プロキシ（脅威カテゴリ）
ピアツーピア	ピアファイル転送
哲学と政治的主張	政治
フィッシングとその他の不正行為	フィッシング（脅威カテゴリ）

古いカテゴリ名	新しいカテゴリ名
プロキシ回避とアノニマイザー	フィルタリング回避
要検討	ユーモア
シェアウェアとフリーウェア	フリーウェアおよびシェアウェア
ストリーミングメディア	ストリーミング ビデオ
水着と肌着	下着および水着
Web ホスティングサイト	Web ホスティング

変更されていないカテゴリ

特に対処の必要はありませんが、これらの変更に注意する必要があります。URL ルールを作成または変更して、新しい脅威カテゴリ（マルウェアサイト、スパイウェア、アドウェア）を含めることを強くお勧めします。

表 *25 :* 変更されていないカテゴリ

変更されていないカテゴリ
出会い系
ゲーム
求職
軍
パークドメイン
不動産
宗教
ショッピング
旅行
武器

表 *26 :* 変更されていない脅威カテゴリ

変更されていない脅威カテゴリ
マルウェアサイト（脅威カテゴリ）
スパイウェアとアドウェア（脅威カテゴリ）

バージョン 6.4.0.x ガイドライン

表 *27* : バージョン *6.4.0.x* ガイドライン

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	アップグレードの失敗：コンテナインスタンスのディスク容量不足 （11 ページ）	Firepower 4100/9300	6.4.0	以降のパッチ 6.5.0
	Firepower 1010 デバイス上の EtherChannel で出力トラフィックがブラックホール化される場合がある （11 ページ）	Firepower 1010	6.4.0 のみ	6.4.0.3 ～ 6.4.0.5
	Firepower 1000 シリーズではバージョン 6.4.0.1 および 6.4.0.2 はサポート対象外 （35 ページ）	Firepower 1000 シリーズ	6.4.0 のみ	6.4.0.1 または 6.4.0.2

Firepower 1000 シリーズではバージョン 6.4.0.1 および 6.4.0.2 はサポート対象外

展開：Firepower 1000 シリーズ デバイス

アップグレード元：バージョン 6.4.0

直接アップグレード先：バージョン 6.4.0.1 または 6.4.0.2

Firepower 1000 シリーズ デバイスをバージョン 6.4.0.1 または 6.4.0.2 にアップグレードすることはできません。

バージョン 6.4.0 のガイドライン

表 *28* : バージョン *6.4.0* の新しいガイドライン

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	Firepower 1010 デバイス上の EtherChannel で出力トラフィックがブラックホール化される場合がある （11 ページ）	Firepower 1010	6.4.0	6.4.0.3 ～ 6.4.0.5

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	アップグレードの失敗：コンテナインスタンスのディスク容量不足（11 ページ）	Firepower 4100/9300	6.3.0 ～ 6.4.0.x	6.3.0.1 ～ 6.5.0
	アップグレードの失敗：以前のバージョンが 6.2.3.12 の NGIPS デバイス （37 ページ）	Firepower 7000/8000 シリーズ ASA FirePOWER NGIPSv	6.2.3 ～ 6.3.0.x	6.4.0 のみ
	TLS 暗号化アクセラレーションの有効化/無効にすることは不可（38 ページ）	Firepower 2100 シリーズ Firepower 4100/9300	6.1.0 ～ 6.3.0.x	6.4.0 以降
	Firepower 4100/9300 のアップグレードにはバージョン 6.2.0 が必要 （38 ページ）	Firepower 4100/9300	6.1.0.x	6.4.0 のみ

これらの事前に公開されたガイドラインと警告は、中間リリースに適用されます。アップグレードパスでメジャーバージョンがスキップされる場合は、このチェックリストを確認してください。

表 *29* : 以前に公開されたバージョン *6.4.0* のガイドライン

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	URL フィルタリングキャッシュのタイムアウトが変更される可能性（43 ページ）	任意（Any）	6.2.3.x	6.3.0 以降
	FMC、7000/8000 シリーズ、NGIPSv で準備状況チェックに失敗する可能性 （44 ページ）	FMC Firepower 7000/8000 シリーズ NGIPSv	6.1.0 ～ 6.1.0.6 6.2.0 ～ 6.2.0.6 6.2.1 6.2.2 ～ 6.2.2.4 6.2.3 ～ 6.2.3.4	6.3.0 以降
	リモートアクセス VPN のデフォルト設定の変更によって VPN トラフィックがブロックされる可能性（44 ページ）	FMC を使用した FTD	6.2.0 ～ 6.2.3.x	6.3.0 以降

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	FMC 1000/2500/4500 にはアップグレード前のホットフィックスが必要な場合がある （45 ページ）	MC1000、2500、および 4500	6.2.0 ～ 6.2.3.7	6.3.0 以降
	アプライアンスへのアクセスの更新されたセキュリティ （47 ページ）	任意（Any）	6.1.0 ～ 6.2.3.x	6.3.0 以降
	セキュリティ インテリジェンスによって可能になるアプリケーションの識別 （47 ページ）	FMC の展開	6.1.0 ～ 6.2.3.x	6.3.0 以降
	アップグレード後に VDB を更新して CIP 検出を有効化 （48 ページ）	任意（Any）	6.1.0 ～ 6.2.3.x	6.3.0 以降
	無効な侵入変数セットによって展開に失敗する可能性 （48 ページ）	任意（Any）	6.1.0 ～ 6.2.3.x	6.3.0 以降
	接続イベントと侵入イベントに関する Syslog の動作の変更 （49 ページ）	FMC	6.1.0 ～ 6.2.3.x	6.3.0 以降
	レポートの結果の制限の変更 （54 ページ）	FMC	6.1.0 ～ 6.2.2.x	6.2.3 ～ 6.4.0
	アップグレードの前にバージョン 6.1.x FTD クラスタからサイト ID を削除 （54 ページ）	FTD クラスタ	6.1.0.x	6.2.3 ～ 6.4.0
	アクセスコントロールでは SRU から遅延ベースのパフォーマンス設定を取得可能 （58 ページ）	FMC	6.1.0.x	6.2.0 ～ 6.4.0
	FTD での「フェールセーフ」から「Snort フェール オープン」への置き換え （59 ページ）	FMC を使用した FTD	6.1.0.x	6.2.0 ～ 6.4.0

アップグレードの失敗：以前のバージョンが 6.2.3.12 の NGIPS デバイス

展開：7000/8000 シリーズ、ASA FirePOWER、NGIPSv

関連するバグ：CSCvp42398

アップグレード元：バージョン 6.2.3 ～ 6.3.0.x

直接アップグレード先：バージョン 6.4.0 のみ

次の場合、NGIPS デバイスをバージョン 6.4.0 にアップグレードすることはできません。

- デバイスが以前にバージョン 6.2.3.12 を実行していて、その後、次を実行した。
- バージョン 6.2.3.12 パッチをアンインストールしたか、バージョン 6.3.0.x にアップグレードした。

  これには、バージョン 6.2.3.12 パッチをアンインストールしてから、バージョン 6.3.0.x にアップグレードしたシナリオも含まれています。

上記が現在の状況である場合は、Cisco TAC にお問い合わせください。

TLS 暗号化アクセラレーションの有効化/無効にすることは不可

展開：Firepower 2100 シリーズ、Firepower 4100/9300 シャーシ

アップグレード元：バージョン 6.1.0 ～ 6.3.x

直接アップグレード先：バージョン 6.4.0 以降

SSL ハードウェア アクセラレーションは、*TLS* 暗号化アクセラレーションに名前が変更されました。

デバイスによっては、TLS 暗号化アクセラレーションがソフトウェアまたはハードウェアで実行される場合があります。アップグレードでは、この機能を手動で無効にした場合でも、すべての対象デバイスでアクセラレーションが自動的に有効になります。ほとんどの場合、この機能を設定することはできません。この機能は自動的に有効になり、無効にすることはできません。

バージョン *6.4.0* へのアップグレード： Firepower 4100/9300 シャーシのマルチインスタンス機能を使用している場合は、FXOS CLI を使用して、モジュール/セキュリティエンジンごとに、*1* つのコンテナインスタンスに対して TLS 暗号アクセラレーションを有効にすることができます。他のコンテナインスタンスに対してアクセラレーションは無効になっていますが、ネイティブインスタンスには有効になっています。

バージョン *6.5.0* 以降へのアップグレード：Firepower 4100/9300 シャーシのマルチインスタンス機能を使用している場合は、FXOS CLI を使用して、Firepower 4100/9300 シャーシ上の複数のコンテナインスタンス（最大 16 個）に対して TLS 暗号アクセラレーションを有効にすることができます。新しいインスタンスでは、この機能がデフォルトで有効になっています。ただし、アップグレードによって既存のインスタンスのアクセラレーションが有効になることはありません。代わりに、 **config hwCrypto enable** CLI コマンドを使用してください。

Firepower 4100/9300 のアップグレードにはバージョン 6.2.0 が必要

展開：FTD を搭載した Firepower 4100/9300

アップグレード元：バージョン 6.1.x

直接アップグレード先：バージョン 6.4.0 のみ

他の FMC 管理対象デバイスとは異なり、Firepower 4100/9300 シリーズデバイスでは、Firepower Threat Defense ソフトウェアをバージョン 6.1 から 6.4 に直接アップグレードすることはできません。これは、FXOS 2.6.1 は FTD バージョン 6.1 と互換性がないが、バージョン 6.4 では必要であるからです。

FXOS 2.3.1 では中間バージョンとしてバージョン 6.2.3 を使用することを推奨します。FXOS を最初にアップグレードする必要があることに注意してください。バージョン6.3を中間リリースとして使用しないでください。『Firepower Release Notes, Version 6.3.0』のガイドラインと警告を参照してください。

バージョン 6.3.0.x のガイドライン

表 *30* : バージョン *6.3.0.x* のガイドライン

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	アップグレードの失敗：コンテナインスタンスのディスク容量不足（11 ページ）	Firepower 4100/9300	6.3.0.x	以降のパッチ 6.4.0 および 6.5.0

バージョン 6.3.0 のガイドライン

表 *31* : バージョン *6.3.0* の新しいガイドライン

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	名前が変更されたアップグレードとインストールパッケージ （41 ページ）	FMC Firepower 7000/8000 シリーズ NGIPSv	任意	6.3.0 以降
	バージョン 6.3+ に再イメージ化するとほとんどのアプライアンスで LOM が無効になる （43 ページ）	FMC（物理） Firepower 7000/8000 シリーズ	の新しいガイドライン	6.3.0 以降
	URL フィルタリングキャッシュのタイムアウトが変更される可能性（43 ページ）	の新しいガイドライン	6.2.3.x	6.3.0 以降

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	FMC、7000/8000 シリーズ、NGIPSv で準備状況チェックに失敗する可能性 （44 ページ）	FMC Firepower 7000/8000 シリーズ NGIPSv	6.2.3 ～ 6.2.3.4 6.2.2 ～ 6.2.2.4 6.2.1 6.2.0 ～ 6.2.0.6 6.1.0 ～ 6.1.0.6	6.3.0 以降
	リモートアクセス VPN のデフォルト設定の変更によって VPN トラフィックがブロックされる可能性 （44 ページ）	FMC を使用した FTD	6.2.0 ～ 6.2.3.x	6.3.0 以降
	FMC 1000/2500/4500 にはアップグレード前のホットフィックスが必要な場合がある （45 ページ）	MC1000、2500、および 4500	6.2.0 ～ 6.2.3.7	6.3.0 以降
	アップグレードでの TLS/SSL ハードウェア アクセラレーションの有効化 （46 ページ）	Firepower 2100 シリーズ Firepower 4100/9300	6.1.0 ～ 6.2.3.x	6.3.0 のみ
	アップグレードの失敗：FMC および ASA FirePOWER へのバージョン 6.3.0-83 アップグレード （47 ページ）	FMC ASDM を使用した ASA FirePOWER	6.1.0 ～ 6.2.3.x	6.3.0 のみ
	アプライアンスへのアクセスの更新されたセキュリティ （47 ページ）	任意	6.1.0 ～ 6.2.3.x	6.3.0 以降
	セキュリティ インテリジェンスによって可能になるアプリケーションの識別 （47 ページ）	FMC の展開	6.1.0 ～ 6.2.3.x	6.3.0 以降
	アップグレード後に VDB を更新して CIP 検出を有効化 （48 ページ）	任意	6.1.0 ～ 6.2.3.x	6.3.0 以降
	無効な侵入変数セットによって展開に失敗する可能性 （48 ページ）	任意	6.1.0 ～ 6.2.3.x	6.3.0 以降
	接続イベントと侵入イベントに関する Syslog の動作の変更 （49 ページ）	FMC	6.1.0 ～ 6.2.3.x	6.3.0 以降

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	Firepower 4100/9300 では FXOS のアップグレードの前に FTD プッシュが必要 （49 ページ）	Firepower 4100/9300	6.1.0.x	6.3.0 のみ

これらの事前に公開されたガイドラインと警告は、中間リリースに適用されます。アップグレードパスでメジャーバージョンがスキップされる場合は、このチェックリストを確認してください。

表 *32 :* 以前に公開されたバージョン *6.3.0* のガイドライン

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	レポートの結果の制限の変更 （54 ページ）	FMC	6.1.0 ～ 6.2.2.x	6.2.3 ～ 6.4.0
	アップグレードの前にバージョン 6.1.x FTD クラスタからサイト ID を削除 （54 ページ）	FTD クラスタ	6.1.0.x	6.2.3 ～ 6.4.0
	アクセスコントロールでは SRU から遅延ベースのパフォーマンス設定を取得可能 （58 ページ）	FMC	6.1.0.x	6.2.0 ～ 6.4.0
	FTD での「フェールセーフ」から「Snort フェール オープン」への置き換え （59 ページ）	FMC を使用した FTD	6.1.0.x	6.2.0 ～ 6.4.0

名前が変更されたアップグレードとインストールパッケージ

展開： FMC、7000/8000 シリーズ、NGIPSv

アップグレード元：バージョン 6.1.0 ～ 6.2.3.x

直接アップグレード先：バージョン 6.3 +

アップグレード、パッチ、ホットフィックス、およびインストールパッケージの命名スキーム（名前の最初の部分）は、当該プラットフォーム上で「Version 6.3.0」で始まるように変更されました。

（注） この変更により、古い物理アプライアンス（DC750、1500、2000、3500、4000のほか、7000/8000シリーズ デバイスと AMP モデル）の再イメージ化に関する問題が発生します。バージョン 5.x を現在実行していて、これらのアプライアンスのいずれかにバージョン 6.3.0 または 6.4.0 を新規インストールする必要がある場合は、シスコサポートおよびダウンロードサイトからインストールパッケージをダウンロードした後、その名前を「古い」名前に変更します。これらのアプライアンスをバージョン 6.5+ に再イメージ化することはできません。

表 ***33 :*** 命名スキーム：アップグレード、パッチ、およびホットフィックスパッケージ

プラットフォーム	命名方式
FMC	新： Cisco_Firepower_Mgmt_Center 旧： Sourcefire_3D_Defense_Center_S3
Firepower 7000/8000 シリーズ	新： Cisco_Firepower_NGIPS_Appliance 旧： Sourcefire_3D_Device_S3
NGIPSv	新： Cisco_Firepower_NGIPS_Virtual 旧： Sourcefire_3D_Device_VMware 旧： Sourcefire_3D_Device_Virtual64_VMware

表 ***34 :*** 命名スキーム：インストールパッケージ

プラットフォーム	命名方式
FMC （物理）	新： Cisco_Firepower_Mgmt_Center 旧： Sourcefire_Defense_Center_M4 旧： Sourcefire_Defense_Center_S3
FMCv: VMware	新： Cisco_Firepower_Mgmt_Center_Virtual_VMware 旧： Cisco_Firepower_Management_Center_Virtual_VMware
FMCv: KVM	新： Cisco_Firepower_Mgmt_Center_Virtual_KVM 旧： Cisco_Firepower_Management_Center_Virtual
Firepower 7000/8000 シリーズ	新： Cisco_Firepower_NGIPS_Appliance 旧： Sourcefire_3D_Device_S3
NGIPSv	新： Cisco_Firepower_NGIPSv_VMware 旧： Cisco_Firepower_NGIPS_VMware

バージョン 6.3+ に再イメージ化するとほとんどのアプライアンスで LOM が無効になる

展開：物理 FMC、7000/8000 シリーズ デバイス

再イメージ化元：バージョン 6.0+

直接アップグレード先：バージョン 6.3 +

バージョン 6.3+ を新規インストールすると、セキュリティ上の理由から、ほとんどのアプライアンスの Lights-Out 管理（LOM）設定が自動的に削除されます。いくつかの古い FMC モデルでは、管理ネットワーク設定とともにLOM設定を保持するオプションが用意されています。

バージョン 6.3+ の再イメージ化中にネットワーク設定を削除する場合は、初期設定を実行するためにアプライアンスに物理的にアクセスできることを確認する必要があります。LOM を使用することはできません。初期設定を実行した後、LOM とLOMユーザを再度有効にすることができます。

表 *35 : LOM* 設定への再イメージ化の影響

プラットフォーム	バージョン6.2.3以前への再イメージ化	バージョン6.3+への再イメージ化
MC1600、2600、4600 MC1000、2500、4500 MC2000、4000	削除されない	常に削除される
MC750、1500、3500	ネットワーク設定を削除すると削除される	ネットワーク設定を削除すると削除される
7000/8000 シリーズ	常に削除される	常に削除される

URL フィルタリングキャッシュのタイムアウトが変更される可能性

展開：すべて

アップグレード元：バージョン 6.2.3.x

直接アップグレード先：バージョン 6.3.0+

バージョン 6.3.0 の新機能として、GUI で URL フィルタリングキャッシュのタイムアウト値を設定できます。古いデータと一致するURLのインスタンスを最小限に抑えるため、キャッシュ内の URL を期限切れに設定できます。Cisco TAC と連携して URL フィルタリングキャッシュのタイムアウト値を変更している場合、アップグレードによってその値が変更される可能性があります。

アップグレード完了後、

- FMC：**[システム（System）] > [統合（Integration）]** を選択し、[Cisco CSI] タブをクリックして、[キャッシュされたURLの期限切れ（Cached URLs Expire）] 設定を確認します。
- FDM：**[システム設定（System Settings）] > [トラフィック設定（Traffic Settings）] > [URL フィルタリングの設定（URL Filtering Preferences）]** を選択し、[URL存続可能時間（URL Time to Live）] 設定を確認します。

FMC、7000/8000シリーズ、NGIPSvで準備状況チェックに失敗する可能性

展開：FMC、7000/8000 シリーズ デバイス、NGIPSv

アップグレード元：バージョン 6.1.0 ～ 6.1.0.6、バージョン 6.2.0 ～ 6.2.0.6、バージョン 6.2.1、バージョン 6.2.2 ～ 6.2.2.4、およびバージョン 6.2.3 ～ 6.2.3.4

直接アップグレード先：バージョン 6.3.0+

次に示すバージョンの Firepower のいずれかからアップグレードする場合は、そこに示されているモデルで準備状態チェックを実行できません。これは、準備状況チェックプロセスが新しいアップグレードパッケージに対して互換性を持たないためです。

表 *36 :* バージョン *6.3.0* 以降用の準備状況チェックを備えたパッチ

準備完了チェックがサポートされない	修正された最初のパッチ
6.1.0 ～ 6.1.0.6	6.1.0.7
6.2.0 ～ 6.2.0.6	6.2.0.7
6.2.1	なし。バージョン 6.2.3.5+ にアップグレードしてください。
6.2.2 ～ 6.2.2.4	6.2.2.5
6.2.3 ～ 6.2.3.4	6.2.3.5

リモートアクセス VPN のデフォルト設定の変更によって VPN トラフィックがブロックされる可能性

展開：**リモートアクセス VPN 用に設定された** Firepower Threat Defense

アップグレード元：バージョン 6.2.x

直接アップグレード先：バージョン 6.3 +

バージョン6.3では非表示オプションの **sysopt connection permit-vpn** のデフォルト設定が変更されています。アップグレードすると、リモートアクセス VPN がトラフィックを渡さなくなる可能性があります。この場合は、次のいずれかの手法を使用してください。

- **sysopt connection permit-vpn** コマンドを設定する FlexConfig オブジェクトを作成します。このコマンドの新しいデフォルトは **no sysopt connection permit-vpn** です。

  これは、外部ユーザがリモートアクセス VPN アドレスプール内の IP アドレスになりすますことができないため、VPN でトラフィックを許可するよりも安全な方法です。欠点は VPN トラフィックが検査されないことです。つまり、侵入とファイルの保護、URL フィルタリング、その他の高度な機能がトラフィックに適用されません。

- リモートアクセス VPN アドレスプールからの接続を許可するアクセス制御ルールを作成します。

  この方法では、VPN トラフィックが確実に検査され、高度なサービスを接続に適用できます。欠点は、外部のユーザが IP アドレスをスプーフィングして、内部ネットワークにアクセスしやすくなることです。

FMC 1000/2500/4500 にはアップグレード前のホットフィックスが必要な場合がある

展開： Firepower Management Center モデル FMC 1000、2500、および 4500

アップグレード元：バージョン 6.2.0 ～ 6.2.3.7

直接アップグレード先：バージョン 6.3.0+

FMC 1000、MC2500、または MC4500 をバージョン 6.2.0 ～ 6.2.3.7 からバージョン 6.3.0+ にアップグレードする前に、プレインストールホットフィックスの適用が必要になる場合があります。または、バージョン 6.2.3.8 + にアップグレードすることもできます。他の FMC モデルまたはバージョンにホットフィックスを適用しないでください。

このホットフィックス（またはパッチ）により、RAID コントローラのファームウェアがバージョン 24.12.1-0411 に更新されます。ホットフィックスを更新しないと、バージョン 6.3.0+ を実行しているアップグレード済み FMC でパフォーマンス上の問題が発生する可能性があります。

（注） 影響を受けるバージョンを実行している場合でも、ファームウェアがすでに最新の状態になっていることもあります。この状況では、ホットフィックスはエラーで失敗します。「イメージファイルのバージョンがコントローラ上のものと同じか、それより古いバージョンです。コントローラはフラッシュされていません。（`The image file has older version thanor same as that on the controller. The controller is not flashed.`）」このメッセージが表示された場合は、ホットフィックスなしでも安全にアップグレードできます。

ホットフィックスを適用する前にファームウェアのバージョンを再確認するには、FMC で Linux シェル（エキスパートモードとも呼ばれます）にアクセスし、**`sudo storcli /c0 show | grep "FW Version"`** コマンドを実行します。

ホットフィックスは シスコサポートおよびダウンロードサイト で入手可能であり、お使いの現在のメジャーバージョンのアップグレードパッケージおよびインストールパッケージと同じ場所にあります。ホットフィックスを適用するには、通常のアップグレードページ（**[システム（System）] > [更新（Updates）]**）を使用します。

表 *37:* プレインストール ホットフィックス パッケージ

現在のバージョン	ホットフィックス	パッケージ
6.3.0 以降	—	ホットフィックスまたはパッチを適用せずに 6.3.0+ にアップグレードした場合は、Cisco TAC に連絡してください。
6.2.3.8 以降のパッチ	—	正常にアップグレードします。ホットフィックスは必要ありません。
6.2.3 ～ 6.2.3.7	ホットフィックス AJ	Sourcefire_3D_Defense_Center_S3_Hotfix_AJ-6.2.3.999-5.sh.REL.tar
6.2.2.x	ホットフィックス BY	Sourcefire_3D_Defense_Center_S3_Hotfix_BY-6.2.2.999-1.sh.REL.tar
6.2.1	—	バージョン 6.2.3 にアップグレードし、ホットフィックス AJ またはパッチのいずれかを 6.2.3.8+ に適用します。
6.2.0.x	—	バージョン 6.2.3 にアップグレードし、ホットフィックス AJ またはパッチのいずれかを 6.2.3.8+ に適用します。

アップグレードでの TLS/SSL ハードウェア アクセラレーションの有効化

展開：Firepower 2100 シリーズ、Firepower 4100/9300 シャーシ

アップグレード元：バージョン 6.1.0 ～ 6.2.3.x

直接アップグレード先：バージョン 6.3.0 のみ

アップグレードプロセスにより、対象デバイスの TLS/SSL ハードウェア アクセラレーション（*TLS* 暗号化アクセラレーションと呼ばれる場合もあります）が自動的に有効になります。この機能は、導入されたバージョン 6.2.3 では Firepower 4100/9300 シャーシ 上でデフォルトで無効になっており、Firepower 2100 シリーズのデバイスでは利用できませんでした。

トラフィックを復号しない管理対象デバイスで TLS/SSL ハードウェア アクセラレーション を使用すると、パフォーマンスに影響を与えることがあります。トラフィックを復号しないデバイスではこの機能を無効にすることをお勧めします。

無効にするには、次の CLI コマンドを使用します。

```
system support ssl-hw-offload disable
```

アップグレードの失敗：FMC および ASA FirePOWER へのバージョン 6.3.0-83 アップグレード

展開： Firepower Management Center、ASA FirePOWER（ローカル管理）

アップグレード元：バージョン 6.1.0 ～ 6.2.3.x

直接アップグレード先：バージョン 6.3.0-83

一部の Firepower Management Center およびローカル（ASDM）管理された ASA FirePOWER モジュールでは、バージョン 6.3.0、ビルド 83 でのアップグレードに失敗していました。この問題は、バージョン 5.4.x からアップグレードした一部のお客様に限られていました。詳細については、Cisco Bug Search Tool で CSCvn62123 を参照してください。

新しいアップグレードパッケージが利用可能になりました。バージョン 6.3.0-83 アップグレードパッケージをダウンロードした場合は、使用しないでください。この問題のためにすでにアップグレードに失敗した場合は、Cisco TAC に連絡してください。

アプライアンスへのアクセスの更新されたセキュリティ

展開：すべて

アップグレード元：バージョン 6.1 ～ 6.2.3.x

直接アップグレード先：バージョン 6.3 +

セキュリティを強化するために、バージョン 6.3 では、セキュア SSH アクセスのためにサポートされる暗号と暗号化アルゴリズムのリストが更新されました。暗号エラーのために SSH クライアントが Firepower アプライアンスとの接続に失敗する場合は、クライアントを最新バージョンに更新してください。

セキュリティインテリジェンスによって可能になるアプリケーションの識別

展開：Firepower Management Center

アップグレード元：バージョン 6.1 ～ 6.2.3.x

直接アップグレード先：バージョン 6.3 +

バージョン 6.3 では、セキュリティ インテリジェンスの設定によりアプリケーションの検出と識別が可能になります。現在の展開で検出を無効にした場合は、アップグレードプロセスによって再び検出が有効になる可能性があります。必要がない場合（たとえば、IPS のみの展開など）に検出を無効にするとパフォーマンスが向上する可能性があります。

検出を無効にするには、次の手順を実行する必要があります。

- ネットワーク検出ポリシーからすべてのルールを削除します。

- 単純なネットワークベースの条件（ゾーン、IPアドレス、VLANタグ、およびポート）のみを使用してアクセス制御を実行します。どんな種類のアプリケーション、ユーザ、URL、または地理位置情報の制御も行わないでください。
- **（新規）**デフォルトのグローバルリストなど、アクセス コントロール ポリシーのセキュリティインテリジェンス設定からすべてのホワイトリストとブラックリストを削除することで、ネットワークと URL ベースのセキュリティ インテリジェンスを無効にします。
- **（新規）**DNSのデフォルトのグローバルホワイトリストやDNSルールのグローバルブラックリストなど、関連付けられている DNS ポリシー内のすべてのルールを削除または無効にすることで、DNS ベースのセキュリティ インテリジェンスを無効にします。

アップグレード後に VDB を更新して CIP 検出を有効化

展開：すべて

アップグレード元：バージョン 6.1.0 ～ 6.2.3.x、VDB 299+ 搭載

直接アップグレード先：バージョン 6.3.0+

脆弱性データベース（VDB）299以降を使用しているときにアップグレードする場合、アップグレードプロセスの問題により、アップグレード後のCIP検出を使用できなくなります。これには、2018 年 6 月から現在までにリリースされたすべての VDB に加えて、最新の VDB も含まれます。

アップグレード後は常に脆弱性データベース（VDB）を最新バージョンに更新することを推奨しますが、この場合は特に重要です。

この問題の影響を受けるかどうかを確認するには、CIP ベースアプリケーションの条件を使用して、アクセス制御ルールを設定してみてください。ルールエディタでCIPアプリケーションが見つからない場合は、手動で VDB を更新します。

無効な侵入変数セットによって展開に失敗する可能性

展開：すべて

アップグレード元：バージョン 6.1 ～ 6.2.3.x

直接アップグレード先：バージョン 6.3.0+

侵入変数セット内のネットワーク変数については、除外する IP アドレスが、含める IP アドレスのサブセットである必要があります。次の表に、有効な設定と無効な設定の例を示します。

有効	無効
含める：10.0.0.0/8 除外する：10.1.0.0/16	含める：10.1.0.0/16 除外する：172.16.0.0/12 除外する：10.0.0.0/8

バージョン 6.3.0 より前のバージョンでは、このタイプの無効な設定でネットワーク変数を正常に保存できました。現在のバージョンでは、これらの設定によって展開がブロックされ、次のエラーが表示されます。「変数セットに無効な除外値が含まれています。（`Variable set has invalid excluded values.`）」

この場合は、正しく設定されていない変数セットを識別して編集してから展開しなおしてください。変数セットによって参照されているネットワークオブジェクトおよびグループの編集が必要である場合もあることに注意してください。

接続イベントと侵入イベントに関する Syslog の動作の変更

展開：Firepower Management Center

アップグレード元：バージョン 6.1.0 ～ 6.2.3.x

直接アップグレード先：バージョン 6.3.0+

バージョン 6.3.0 では、システムが Syslog を介して接続イベントと侵入イベントをログに記録する方法が変更され、一元化されています。アクセス コントロール ポリシーの新しい [ロギング（Logging）] タブでこれらの設定にアクセスできます。

アップグレードによって接続イベントログの既存の設定が変更されることはありません。ただし、Syslog 経由では「期待されなかった」侵入イベントの受信が突然開始される可能性があります。これは、バージョン 6.3.0+ にアップグレードすると、侵入ポリシーによって、Syslog イベントが新しい [ロギング（Logging）] タブ上の宛先に送信されるためです（バージョン 6.3.0 以前では、外部ホストではなく、管理対象デバイス自体の Syslog にイベントを送信するように侵入ポリシーで Syslog アラートを設定できました）。

また、NGIPS デバイス（7000/8000 シリーズ、ASA FirePOWER、NGIPSv）から送信されるメッセージで、RFC 5425 で指定されている ISO 8601 タイムスタンプ形式が使用されるようになりました。

Firepower 4100/9300 では FXOS のアップグレードの前に FTD プッシュが必要

展開：FTD を搭載した Firepower 4100/9300

アップグレード元：FXOS 2.0.1、2.1.1、または 2.3.1 上のバージョン 6.1.x

直接アップグレード先：FXOS 2.4.1 上のバージョン 6.3.0

Firepower Management Center がバージョン 6.2.3+ を実行している場合は、アップグレードの前に Firepower アップグレードパッケージを管理対象デバイスにプッシュ（コピー）することを強くお勧めします。これにより、アップグレード メンテナンス ウィンドウの長さを縮小できます。

FTD を搭載した Firepower 4100/9300 の場合、必要な付属する FXOS のアップグレードを開始する前にプッシュすることをお勧めします。また、バージョン 6.1 からバージョン 6.3+ に直接

アップグレードする場合は、このプッシュが必須です。FXOS をアップグレードする前にプッシュする必要があります。

これは、Firepower 6.1 を実行したまま FXOS をバージョン 2.4.1 にアップグレードすると、デバイス管理ポートがフラップする（そのため、デバイスと FMC の間で断続的な通信上の問題が発生する）ためです。「sftunnel daemon exited」というアラームが表示される可能性があり、長時間の通信をともなうタスク（大規模なアップグレードパッケージのプッシュなど）が失敗する可能性があります。

FTD を搭載した Firepower 4100/9300 をアップグレードするには、必ず次の手順に従ってください。

1. FMC をターゲットバージョンにアップグレードします。
2. シスコサポートおよびダウンロードサイト からデバイス アップグレード パッケージを取得し、それを FMC にアップロードします。
3. FMC を使用してアップグレードパッケージをデバイスにプッシュします。
4. プッシュが完了したら、FXOS をターゲットバージョンにアップグレードします。
5. すぐに、FMC を使用してデバイス上の Firepower ソフトウェアをアップグレードします。

   Firepower ソフトウェアをアップグレードするまでは、管理ポートのフラップが発生する可能性があることに注意してください。

バージョン 6.2.3.x ガイドライン

表 *38* : バージョン *6.2.3.x* ガイドライン

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	動的分析 CA 証明書のパッチ/ホットフィックス （11 ページ）	任意	6.2.3.x	以降のパッチ
	CC モードが有効になっているバージョン 6.2.3.10 FTD にアップグレードすると FSIC 障害が発生 （51 ページ）	FTD	6.2.3 ～ 6.2.3.9	6.2.3.10 のみ
	バージョン 6.2.3.3 FTD デバイスをローカル管理に切り替えることは不可 （51 ページ）	FMC を使用した FTD	6.2.3 ～ 6.2.3.2	6.2.3.3
	バージョン 6.2.3 ～ 88 FMC をアップグレードする前のホットフィックス （52 ページ）	FMC	6.2.3-88	6.2.3.1 ～ 6.2.3.3

CC モードが有効になっているバージョン 6.2.3.10 FTD にアップグレードすると FSIC 障害が発生

展開： Firepower Threat Defense

アップグレード元：バージョン 6.2.3 ～ 6.2.3.9

直接アップグレード先：バージョン 6.2.3.10 のみ

既知の問題：CSCvo39052

CC モードを有効にして FTD デバイスをバージョン6.2.3.10 にアップグレードすると、デバイスの再起動時に FSIC（ファイルシステム整合性チェック）が失敗します。

⚠

注意 セキュリティ認定準拠が有効な場合に FSIC が失敗すると、Firepower ソフトウェアは起動せず、リモート SSH アクセスが無効になり、ローカルコンソールを介してのみアプライアンスにアクセスできます。この問題が発生した場合は、Cisco TAC にお問い合わせください。

FTD の展開にセキュリティ認定コンプライアンス（CC モード）が必要な場合は、バージョン 6.2.3.13 以降に直接アップグレードすることをお勧めします。Firepower 4100/9300 デバイスの場合は、FXOS 2.3.1.130+ にアップグレードすることも推奨します。

バージョン 6.2.3.3 FTD デバイスをローカル管理に切り替えることは不可

展開：FMC を使用した FTD

アップグレード元：バージョン 6.2.3 ～ 6.2.3.2

直接アップグレード先：バージョン 6.2.3.3 のみ

バージョン 6.2.3.3 では、Firepower Threat Defense デバイスの管理を FMC から FDM に切り替えることはできません。この問題は、バージョン 6.2.3.3 パッチをアンインストールしても発生します。この時点でローカル管理に切り替える場合は、バージョン 6.2.3 を新しくインストールするか、Cisco TAC にお問い合わせください。

この問題を回避するには、6.2.3.3 のバージョンにアップグレードする前に管理を切り替えます。または、最新パッチにアップグレードします。管理を切り替えると、デバイス構成は失われます。

バージョン 6.2.3.3 では、FDM から FMC への管理の切り替えが可能であることに注意してください。

バージョン 6.2.3 ～ 88 FMC をアップグレードする前のホットフィックス

展開：FMC

アップグレード元：バージョン 6.2.3 ～ 88

直接アップグレード先：バージョン 6.2.3.1、バージョン 6.2.3.2、またはバージョン 6.2.3.3

シスコは、Firepower のアップグレードパッケージの更新版ビルドを適宜リリースしています。バージョン 6.2.3 ～ 88 は、それ以降のビルドに置き換えられています。バージョン 6.2.3 ～ 88 を実行している FMC をバージョン 6.2.3.1、バージョン 6.2.3.2、またはバージョン 6.2.3.3 にアップグレードすると、SSE クラウド接続が継続的にドロップし、エラーが生成されます。パッチをアンインストールしても、この問題は解決しません。

バージョン 6.2.3 ～ 88 を実行している場合は、アップグレードの前にホットフィックス T をインストールします。

バージョン 6.2.3 ガイドライン

表 *39* : バージョン *6.2.3* の新しいガイドライン

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	シスコとのデータの共有 （53 ページ）	任意	任意	6.2.3 以降
	アップグレード後にアクセス コントロール ポリシーを編集/再保存する （53 ページ）	任意	6.1.0 ～ 6.2.2.x	6.2.3 のみ
	レポートの結果の制限の変更 （54 ページ）	FMC	6.1.0 ～ 6.2.2.x	6.2.3 ～ 6.4.0
	アップグレードの前にバージョン 6.1.x FTD クラスタからサイト ID を削除 （54 ページ）	FTD クラスタ	6.1.0.x	6.2.3 ～ 6.4.0

これらの事前に公開されたガイドラインと警告は、中間リリースに適用されます。アップグレードパスでメジャーバージョンがスキップされる場合は、このチェックリストを確認してください。

表 *40* : 以前に公開されたバージョン *6.2.3* のガイドライン

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	アクセスコントロールではSRUから遅延ベースのパフォーマンス設定を取得可能 （58 ページ）	FMC	6.1.0.x	6.2.0 ～ 6.4.0
	FTD での「フェールセーフ」から「Snort フェール オープン」への置き換え （59 ページ）	FMC を使用した FTD	6.1.0.x	6.2.0 ～ 6.4.0
	動的分析 CA 証明書のパッチ/ホットフィックス （11 ページ）	任意（Any）	6.1.0 ～ 6.2.3	以降のバージョン

シスコとのデータの共有

展開：すべて

アップグレード元：バージョン 6.1.0+

直接アップグレード先：バージョン 6.2.3+

さまざまな機能にシスコとのデータ共有が含まれます。

- 6.2.3+ の場合、 *Cisco Success Network* は、テクニカルサポートを提供するために不可欠な使用状況に関する情報と統計情報をシスコに送信します。
- 6.2.3+ の場合、 *Web* 分析のトラッキングは、これに限定されませんが、ページでの操作、ブラウザのバージョン、製品のバージョン、ユーザの場所、FMC の管理 IP アドレスまたはホスト名を含む、個人を特定できない使用状況データをシスコに送信します。
- 6.5.0+ の場合、 *Cisco Support Diagnostics*（「シスコのプロアクティブサポート」とも呼ばれる）は、設定および運用上の健全性データをシスコに送信し、自動化された問題検出システムを通じてそのデータを処理して問題をプロアクティブに通知できるようにします。また、この機能により、Cisco TAC は TAC ケースの過程でデバイスから必要な情報を収集することもできます。

これらの機能は自動的に有効になる場合があります。参加の許可または拒否の詳細については、設定ガイドを参照してください。

アップグレード後にアクセス コントロール ポリシーを編集/再保存する

展開：すべて

アップグレード元：バージョン 6.1 ～ 6.2.2.x

直接アップグレード先：バージョン 6.2.3 のみ

侵入ポリシーの変数セットでのみ使用されるネットワークまたはポートオブジェクトを設定している場合、アップグレード後にアクセス コントロール ポリシーに関連付けられている展開が失敗します。これが発生する場合、アクセス コントロール ポリシーを編集し、（説明の編集などの）変更、保存、および再展開を行います。

レポートの結果の制限の変更

展開：Firepower Management Center

アップグレード元：バージョン 6.1.0 ～ 6.2.2.x

直接アップグレード先：バージョン 6.2.3 ～ 6.4.0

バージョン 6.2.3 では、次のように、使用できる結果の数、またはレポートのセクションに含めることができる結果の数が制限されています。テーブルおよび詳細ビューでは、PDF レポートに HTML または CSV レポートよりも少ないレコードを含めることができます。

表 *41 :* レポートの結果の新しい制限

レポートセクションタイプ	最大レコード数：**HTML** または **CSV** レポートセクション	最大レコード数：**PDF** レポートセクション
棒グラフ 円グラフ	100（上位または下位）	100（上位または下位）
テーブルビュー	400,000	100,000
詳細ビュー	1,000	500

Firepower Management Center をアップグレードする前に、レポートテンプレート内のセクションで最大 HTML または CSV よりも大きい結果数を指定する場合は、アップグレードプロセスが設定を新しい最大値に下げます。

PDF レポートを生成するレポートテンプレートの場合、テンプレートセクションの PDF の制限を超えると、アップグレードプロセスは出力形式を HTML に変更します。PDF の生成を続行するには、結果数を PDF の最大に下げます。アップグレード後にこれを行った場合、出力形式の設定を PDF に戻します。

アップグレードの前にバージョン 6.1.x FTD クラスタからサイト ID を削除

展開： Firepower Threat Defenseクラスタ

アップグレード元：バージョン 6.1.x

直接アップグレード先：バージョン 6.2.3 ～ 6.4.0

Firepower Threat Defense バージョン 6.1.x クラスタは、サイト間クラスタリングをサポートしていません（バージョン 6.2.0 以降では FlexConfig を使用してサイト間機能を設定できます）。

FXOS 2.1.1 でバージョン 6.1.x クラスタを展開または再展開している場合、（サポートされていない）サイト ID の値を入力しているときは、アップグレードする前に、FXOS の各ユニットでサイト ID を削除（0 に設定）する必要があります。そうしないと、アップグレード後、ユニットがクラスタに再度参加できなくなります。

すでにアップグレード済みの場合は、サイト ID を各ユニットから削除してからクラスタを再確立します。サイト ID を表示または変更するには、『Cisco FXOS CLI Configuration Guide』を参照してください。

バージョン 6.2.2.x のガイドライン

表 *42* : バージョン *6.2.2.x* のガイドライン

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	動的分析 CA 証明書のパッチ/ホットフィックス （11 ページ）	任意	6.2.2.x	以降のパッチ
	Firepower 2100 シリーズ HA ペアはバージョン 6.2.2 から6.2.2.4 にアップグレードできない （55 ページ）	Firepower 2100 シリーズ HA ペア	6.2.2 のみ	6.2.2.4 のみ

Firepower 2100 シリーズ HA ペアはバージョン 6.2.2 から6.2.2.4 にアップグレードできない

展開：FTD ハイアベイラビリティペアとして設定された Firepower 2100 シリーズ デバイス

アップグレード元：バージョン 6.2.2 のみ

直接アップグレード先：バージョン 6.2.2.4 のみ

ハイアベイラビリティの Firepower 2100 デバイスでは、バージョン 6.2.2 からバージョン 6.2.2.4 へのアップグレードに失敗します。バージョン 6.2.2 を実行していて、バージョン 6.2.2.4 が実際に必要な場合は、最初にバージョン 6.2.2.1 にアップグレードします。それ以外の場合は、このバージョンをスキップすることをお勧めします。

すでにアップグレードを開始していて、アップグレードが失敗した場合は、再イメージ化することをお勧めします。

バージョン 6.2.2 ガイドライン

表 *43 :* バージョン *6.2.2* の新しいガイドライン

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	セキュリティ強化：署名付きのアップグレードパッケージ （56 ページ）	任意	任意	6.2.2 以降
	8000 シリーズのセキュリティ認定コンプライアンスのためにバージョン 6.2.2.1+ が必要 （56 ページ）	Firepower 8000 シリーズ	6.2.0.x	6.2.2 のみ

セキュリティ強化：署名付きのアップグレードパッケージ

展開：すべて

アップグレード元：バージョン 6.2.1+

直接アップグレード先：バージョン 6.2.2+

Firepowerでは、正しいファイルを使用していることを確認できるようにするために、バージョン6.2.1+からのアップグレードパッケージ（およびバージョン6.2.1+へのホットフィックス）は、署名付きの tar アーカイブ（.tar）になっています。以前のバージョンからのアップグレードでは、引き続き未署名のパッケージが使用されます。

シスコサポートおよびダウンロードサイトからアップグレードパッケージを手動でダウンロードする場合（たとえば、メジャーアップグレードやエアギャップ展開のために）、正しいパッケージをダウンロードしていることを確認してください。 署名付きの（.tar）パッケージは解凍しないでください。

（注） 署名付きのアップグレードパッケージをアップロードした後、システムがパッケージを確認する際に、GUIのロードに数分かかることがあります。表示を高速化する必要がなくなった後、署名付きのパッケージを削除します。

8000 シリーズのセキュリティ認定コンプライアンスのためにバージョン 6.2.2.1+ が必要

展開：Firepower 8000 シリーズ デバイス

アップグレード元：バージョン 6.2.0.x

直接のアップグレード先：バージョン 6.2.2 のみ

バージョン 6.2.2 を実行している 8000 シリーズデバイスでセキュリティ認定コンプライアンス（CC/UCAPL モード）を有効にすると、FSIC（ファイルシステム整合性チェック）の障害が発生する可能性があります。その前に、デバイスをバージョン 6.2.2.1+ にアップグレードしてください。

⚠

注意 FSIC が失敗したため、Firepower ソフトウェアは起動せず、リモート SSH アクセスが無効になり、ローカルコンソールを介してのみアプライアンスにアクセスできます。この問題が発生した場合は、Cisco TACにお問い合わせください。

バージョン 6.2.0.x のガイドライン

表 *44* : バージョン *6.2.0.x* のガイドライン

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	動的分析 CA 証明書のパッチ/ホットフィックス （11 ページ）	任意	6.2.0.x	以降のパッチ
	バージョン 6.2.0.3 FMC へのホットフィックス BH の適用 （57 ページ）	FMC	6.2.0 ～ 6.2.0.2	6.2.0.3 のみ

バージョン 6.2.0.3 FMC へのホットフィックス BH の適用

展開：FMC

アップグレード元：バージョン 6.2 ～ 6.2.0.2

直接アップグレード先：バージョン 6.2.0.3 のみ

解決：CSCvg32885

バージョン 6.2.0.3 にアップグレードした後、ホットフィックス BH を適用する必要があります。ホットフィックス BH を適用しない場合、アクセスコントロールルールを編集したり、設定の変更を展開したりできません。

詳細については、『Firepower Hotfix Release Notes』を参照してください。

バージョン 6.2.0 ガイドライン

表 *45* : バージョン *6.2.0* の新しいガイドライン

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	アクセスコントロールではSRUから遅延ベースのパフォーマンス設定を取得可能 （58 ページ）	FMC	6.1.0.x	6.2.0 ～ 6.4.0
	FTD での「フェールセーフ」から「Snort フェール オープン」への置き換え （59 ページ）	FMC を使用した FTD	6.1.0.x	6.2.0 ～ 6.4.0
	アップグレード時に IAB の [すべてのアプリケーション（All Applications）] オプションが削除される （60 ページ）	FMC ASDM を使用した ASA FirePOWER	6.1.0.3 以降のパッチ	6.2.0 のみ
	アップグレード時に無効化される低メモリデバイスの URL フィルタリングのサブサイトルックアップ （61 ページ）	任意	6.1.0.1 以降のパッチ	6.2.0 のみ

アクセスコントロールではSRUから遅延ベースのパフォーマンス設定を取得可能

展開：FMC

アップグレード元：6.1.x

直接アップグレード先：6.2.0+

バージョン 6.2.0+ の新しいアクセス コントロール ポリシーでは、デフォルトで、最新の侵入ルール更新（SRU）から遅延ベースのパフォーマンス設定が取得されます。この動作は、新しい [設定の適用元（Apply Settings From）] オプションによって制御されます。このオプションを設定するには、アクセス コントロール ポリシーを編集または作成して、[詳細（Advanced）] をクリックし、遅延ベースのパフォーマンス設定を編集します。

バージョン 6.2.0+ にアップグレードすると、現在（バージョン 6.1.x）の設定に従って新しいオプションが設定されます。現在の設定が次の場合、新しいオプションは次のように設定されます。

- [デフォルト（Default）] : 新しいオプションは、[インストールされたルールの更新（Installed Rule Update）] に設定されます。アップグレードしてから展開すると、最新の SRU からの

遅延ベースのパフォーマンス設定が使用されます。最新のSRUが指定する内容によって、トラフィックの処理が変更される可能性があります。

- [カスタム（Custom）]：新しいオプションは、[カスタム（Custom）] に設定されます。システムは現在のパフォーマンス設定を保持します。このオプションによって動作が変更されることはありません。

アップグレードする前に設定を確認することをお勧めします。前述したように、バージョン 6.1.x の FMC Web インターフェイスから、ポリシーの遅延ベースのパフォーマンス設定を表示し、[デフォルトに戻す（Revert To Defaults）] ボタンがグレー表示されているかどうかを確認します。ボタンがグレー表示されている場合は、デフォルト設定が使用されています。ボタンがアクティブになっている場合は、カスタム設定が設定されています。

FTDでの「フェールセーフ」から「Snortフェールオープン」への置き換え

展開：FMC を使用した FTD

アップグレード元：バージョン 6.1.x

直接アップグレード先：バージョン 6.2+

バージョン 6.2 では、Snort フェール オープン設定により、FMC によって管理される Firepower Threat Defense デバイスのフェールセーフオプションが置き換えられます。フェールセーフでは、Snort がビジー状態のときにトラフィックをドロップすることができますが、Snort がダウンしている場合、トラフィックはインスペクションなしで自動的に通過します。Snort フェール オープンでは、このトラフィックをドロップすることができます。

FTD デバイスをアップグレードすると、その新しい Snort フェールオープン設定は、以下のように、古いフェールセーフ設定に依存します。新しい設定ではトラフィックの処理が変更されることはありませんが、アップグレードの前にフェールセーフを有効または無効にするかどうかを検討してください。

表 *46 :* フェールセーフの *Snort* フェールオープンへの移行

バージョン 6.1 のフェールセーフ	バージョン 6.2 の Snort フェールオープン	動作
無効（デフォルトの動作）	[ビジー（Busy）]：無効 [ダウン（Down）]：有効	Snort プロセスがビジー状態の場合は、新規および既存の接続をドロップし、Snort プロセスがダウンしている場合は、接続をインスペクションなしで通過します。
有効	[ビジー（Busy）]：有効 [ダウン（Down）]：有効	Snort プロセスがビジー状態またはダウンしている場合、新規または既存の接続をインスペクションなしで通過します。

Snort フェールオープンでは、デバイスにバージョン 6.2 が必要であることに注意してください。バージョン 6.1.x のデバイスを管理している場合、FMC Web インターフェイスにフェールセーフオプションが表示されます。

アップグレード時に IAB の [すべてのアプリケーション（All Applications）] オプションが削除される

展開：FMC、ASDM を使用した ASA FirePOWER

アップグレード元：6.1.0.3 以降のパッチ

直接アップグレード先：6.2.0 のみ

インテリジェント アプリケーション バイパス（IAB）のオプション [未確認アプリケーションを含むすべてのアプリケーション（All applications including unidentified applications）] は、いずれかの IAB インスペクション パフォーマンスしきい値が満たされると、アプリケーションのタイプに関係なく、フローバイパスしきい値を超過するアプリケーションを信頼します。このオプションは、次のバージョンで使用できます。

- バージョン 6.0.1.4 以降のパッチ
- バージョン 6.1.0.3 以降のパッチ
- バージョン 6.2.0.1 以降のパッチ
- バージョン 6.2.2 以降のすべてのパッチとメジャーバージョン

このオプションがサポートされているバージョンからサポートされていないバージョンにアップグレードすると、オプションは削除されます。また、このオプションを実際に有効にしていて、アクセス コントロール ポリシーに IAB バイパス可能なアプリケーションとフィルタの設定が含まれていない場合は、アップグレードされたユーザインターフェイスでは次の予期しない動作が実行されます。

- IAB は有効になっているが、[未確認アプリケーションを含むすべてのアプリケーション（All applications including unidentified applications）] オプションが表示されなくなる。
- [IABの設定（IAB configuration）] ページに [1アプリケーション/フィルタ（1 Applications/Filters）] が表示され、1 つのアプリケーションまたはフィルタが設定されていると誤って示す。
- アプリケーションおよびフィルタエディタの [選択されたアプリケーションとフィルタ（Selected Applications and Filters）] ウィンドウに、[削除済み（FMC）（deleted(FMC)）] または [任意のアプリケーション（ASDM）（Any Application(ASDM)）] が表示される。この選択を削除することをお勧めします。

オプションを復元するには、任意のバージョンの 6.2.0.x パッチを適用するか、バージョン 6.2.2+（推奨）にアップグレードします。

アップグレード時に無効化される低メモリデバイスの URL フィルタリングのサブサイトルックアップ

展開：URL フィルタリングを実行する低メモリデバイス

アップグレード元：バージョン 6.1.0.3 以降のパッチ

直接アップグレード先：バージョン 6.2.0 のみ

メモリの制約上、一部のモデルでは、カテゴリとレピュテーションの小さなデータベースによって URL フィルタリングが実行されます。これは、URL のサブサイトに親サイトとは異なる URL カテゴリとレピュテーションがあるが、デバイスには親サイトのデータのみがある場合に問題になる可能性があります。

バージョン 6.1.0.3 では、システムの動作を変更することにより、親 URL のカテゴリとレピュテーションに依存せずに、デバイスがこれらのサブサイトには「不明」のカテゴリとレピュテーションがあると認識するようにしました。これにより、デバイスがサブサイトのデータのクラウドルックアップを実行するように強制されます（次回にその結果をキャッシュします）。

バージョン 6.2.0 では、これらのサブサイトのクラウドルックアップのサポートが廃止されています。影響を受けるデバイスは次のとおりです。

- Firepower 7010、7020、および 7030
- ASA 5506-X シリーズ、5508-X、5516-X
- ASA 5512-X、5515-X、5525-X

サポートはバージョン 6.2.0.1 で再導入されています。

バージョン 6.1.0 ガイドライン

これらの重要な警告はバージョン 6.1.0 に適用されます。

ASA FirePOWER モジュールをアップグレードする前に ASA REST API を無効にする

展開：ASA FirePOWER

（注） この警告は、今後のすべてのリリースに適用されます。 このステップは現在、アップグレード手順に明示的に含まれています。

ASA FirePOWER モジュールをアップグレードする前に、次の ASA CLI を使用して ASA REST API を無効にします。

no rest-api agent

REST API を無効にしない場合、アップグレードは失敗します。次のコマンドを実行して、アップグレード後に REST API を再度有効にすることができます。

rest-api agent

ASA FirePOWER モジュールのバージョン 6.0 以降も実行している場合、ASA 5506-X シリーズのデバイスでは ASA REST API はサポートされません。

STIG モードから UCAPL モードに変更

展開：Firepower Management Center

バージョン6.1 では、セキュリティ技術導入ガイド（STIG）モードとして知られているセキュリティ認定準拠モードは、統合機能認定製品リスト（UCAPL）モードに名前が変更されます。アップグレード後、STIG モードであった FirePOWER アプライアンスは UCAPL モードになります。UCAPL モードに関連するシステム機能のすべての制限と変更が有効になります。

UCAPL 準拠のためのシステム強化に関する情報を含め、詳細については、『*Firepower Management Center Configuration Guide*』の「Security Certifications Compliance」の章、および認定エンティティが提供するこの製品のガイドラインを参照してください。

アップグレード後に従来のライセンスを復元する

展開：Firepower Management Center

Firepower Management Center をバージョン 6.1 にアップグレードすると、管理対象の NGIPSv、ASA FirePOWER、7000 シリーズ、8000 シリーズのデバイスの従来のライセンスが削除されるまたは無効になることがあります更新を開始する前に、この問題を回避するために実行できるスクリプトについて Cisco TAC へお問い合わせください。

更新後にアップグレード前スクリプトを実行しない場合：

- 削除されたライセンスを確認し、再インストールします。**[システム（System）]**>**[ライセンス（Licenses）]** > **[従来のライセンス（Classic Licenses）]** の順に選択します。
- 影響を受けるデバイスを編集し、ライセンスを再有効化します。**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択します。

バージョン 6.0.0 ガイドライン

これらの重要な警告はバージョン 6.0.0 に適用されます。

用語とブランディング

バージョン 6.0 には、以下を含む用語とブランディングのメジャーな変更があります。

- FireSIGHT システム → Firepower
- FireSIGHT Defense Center → Firepower Management Center（FMC）
- シリーズ 3 デバイス → 7000 シリーズ デバイスまたは 8000 シリーズ デバイス
- 仮想管理対象デバイス → NGIPSv

詳細については、『Cisco Firepower Terminology Guide』を参照してください。

バージョン 6.0 のプレインストールパッケージ

バージョン5.4.xからバージョン6.0へのアップグレードの場合、シスコではアップグレードを最適化するプレインストールパッケージを提供しています。

一部のケースでは、次の表に記載されている、プレインストールパッケージを使用する必要があります。必須ではない場合でも、アップグレードパスでバージョン6.0プレインストールパッケージを追加して使用することを強くお勧めします。詳細については、『FireSIGHT System Release Notes Version 6.0.0 Preinstallation』を参照してください。

プラットフォーム	アップグレードする最低バージョン	必要なパッケージ	推奨されるパッケージ
FireSIGHT Defense Center（FMC）	5.4.1.1	5.4.1.1 ～ 5.4.1.5	5.4.1.6+
7000/8000 シリーズ	5.4.0.2	5.4.0.2 ～ 5.4.0.6	5.4.0.7+
NGIPSv	5.4.0.2	5.4.0.2 ～ 5.4.0.6	5.4.0.7+
ASA FirePOWER: 5.4.1.x	5.4.1.1	5.4.1.1 ～ 5.4.1.5	5.4.1.6+
ASA FirePOWER: 5.4.0.x	5.4.0.2	5.4.0.2 ～ 5.4.0.6	5.4.0.7+

DC750、DC1500、DC3500 および Virtual Defense Center のメモリをアップグレードする

次の FireSIGHT Defense Center モデルでは、バージョン 6.0 を実行するために追加のメモリが必要です。

- DC750
- DC1500
- DC3500
- 仮想防御センター

メモリの増加はシスコの製品要件によって決定されるため、シスコでは、認定の DC750 または DC1500 でバージョン 6.0 を実行する権限があるお客様に、無償で利用できるメモリアップグレードキットを作成しています。

- キットを注文する：Field Notice: FN - 64077 - Cisco FireSIGHT and Sourcefire Defense Center Management Appliances - Memory Upgrade Required for FirePOWER Software V6.0 and Later を参照してください。
- メモリをアップグレードする：『*Firepower Management Center Installation Guide*』の「Memory Upgrade Instructions for Firepower Management Centers」を参照してください。

Defense Center のハイアベイラビリティペアを中断する

バージョン 6.0.x では、Firepower Management Center のハイアベイラビリティをサポートしていません。

Defense Center のバージョン 5.4.x ハイアベイラビリティペアを Firepower Management Center のバージョン 6.0 ハイアベイラビリティペアにアップグレードすることはできません。ペアを中断し、各 Defense Center を個別にアップグレードする必要があります。ハイアベイラビリティをバージョン 6.1 で再確立できます。

[URLキャッシュミスルックアップの再試行（Retry URL Cache Miss Lookup）] オプションを無効にする

バージョン 5.4.0.6、バージョン 5.4.1.5 またはそれ以前を実行しているデバイスを管理している場合、Firepower Management Center をバージョン 6.0 にアップグレードすると、トラフィックの停止やシステムの問題を引き起こす可能性があります。

Defense Center をアップグレードする前に、デバイスに展開するアクセス コントロール ポリシーの [詳細（Advanced）] タブで設定する [URLキャッシュミスルックアップの再試行（Retry URL Cache Miss Lookup）] オプション無効にします。その後、再配置します。管理対象デバイスをバージョン 5.4.0.7+ またはバージョン 5.4.1.6+（またはバージョン 6.0）にアップグレードした後に、オプションを再度有効にできます。

Defense Center HTTPS 証明書を更新する

これらの HTTPS 証明書のいずれかを使用しているバージョン 5.4.x Defense Center をバージョン 6.0 の Firepower Management Center にアップグレードする場合、ログインできなくなるため、Cisco TAC に連絡する必要があります。

- RSASSA-PSS 署名アルゴリズムで生成される証明書。

  アップグレードする前に、sha1WithRSAEncryption アルゴリズムまたは sha256WithRSAEncryption アルゴリズムで生成された証明書、あるいは Defense Center のデフォルト証明書に置き換えます。リブートします。

- 2048 ビットよりも大きい公開サーバキーを使用して生成された証明書。

  アップグレードする前に、サーバ証明書要求（CSR）で生成された証明書に置き換えます。リブートします。

また、アップグレード後に、これらのタイプの証明書のいずれかをアップロードしないでください。 バージョン 5.4.x アプライアンスで証明書を生成するには、『*FireSIGHT System User Guide*』、バージョン 5.4.1 の「Using Custom HTTPS Certificates」を参照してください。

プライベート AMP クラウドのサポートなし

バージョン 6.0 は、プライベート AMP クラウドで Firepower 署名ルックアップの AMP をサポートしません。バージョン 6.0 では、システムは自動的にパブリック AMP クラウドに SHA-256 署名を送信します。プライベート AMP クラウドがあり、エンドポイントからのイベントを受

信している場合、バージョン 6.0 の Defense Center は、構成への追加変更なく、これらのイベントの受信を続行します。