Version6.7.0 へのアップグレード

この章では、重要なリリースに固有の情報を提供します。

Firepowerソフトウェアのアップグレードガイドラインについて

便宜上、このリリースノートでは、過去の Firepower ソフトウェアリリースの廃止機能とバージョン固有のアップグレードガイドラインが重複しています。ただし、対象バージョンのリリースノート、およびスキップするその他のメジャーリリースまたはメンテナンスリリースのリリースノートを必ずお読みください。

重要 アップグレードガイドラインは複数の場所に表示できます。このチェックリストを使用して、すべてを確認してください。

表 *1 : Firepower* ソフトウェアのアップグレードガイドラインのインデックス

✓	リソース	詳細
	Version6.7.0のガイドライン （2 ページ）	新規またはこのリリースに固有の重要なアップグレードガイドラインについては、これらを参照してください。
	以前に公開されたガイドライン （3 ページ）	アップグレードでバージョンがスキップされる場合は、これらを参照してください。
	一般的なガイドライン （14 ページ）	ガイドラインが変更されている可能性があるため、アップグレードプロセスに精通している場合でも、これらをお読みください。
	既知の問題	これらを読み、アップグレードに影響するバグを回避する準備を整えます。 アップグレードでバージョンがスキップされる場合は、スキップするメジャーバージョンの既知の問題も参照してください。「Cisco Firepower リリース ノート」を参照してください。
	特長と機能	アップグレードに影響する可能性のあるその他の項目については、これらをお読みください。廃止された機能では、特別にアップグレード前の構成変更が必要になる場合があります。 アップグレードでバージョンがスキップされる場合は、スキップしたバージョンの新機能に関するドキュメントもお読みください。「Cisco Firepower リリース ノート」を参照してください。

Version6.7.0のガイドライン

このチェックリストには、バージョン 6.7.0 の新規または固有のアップグレードガイドラインが含まれています。現在**バージョン 6.3.0 ～ 6.6.x** を実行している場合は、次のガイドラインを確認してください。

表 *2 :* バージョン *6.7.0* 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 スイッチポートでの無効な VLAN ID によるアップグレードの失敗 （3 ページ）	Firepower 1010	6.4.0 ー 6.6.x	6.7.0 以降

Firepower 1010 スイッチポートでの無効な VLAN ID によるアップグレードの失敗

展開：Firepower 1010

アップグレード元：バージョン 6.4.0 ～ 6.6.x

直接アップグレード先：バージョン 6.7.0 以上

Firepower 1010 では、VLAN ID を 3968 ー 4047 の範囲にしてスイッチポートを設定した場合、FTD のバージョン 6.7.0 以上へのアップグレードは失敗します。これらの ID は内部使用専用です。

以前に公開されたガイドライン

このチェックリストには、中間リリースに適用されるアップグレードガイドラインが含まれています。現在バージョン **6.3.0 ～ 6.5.0** を実行している場合は、次のガイドラインを確認してください。

表 *3 :* 以前に公開されたバージョン *6.7.0* 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
	FMCv をアップグレードするには 28 GB の RAM が必要 （4 ページ）	FMCv	6.2.3 ～ 6.5.0.x	6.6.0 +
	FMC のアップグレード後にイベントが一時的に使用できない （5 ページ）	FMC	6.2.3 ～ 6.5.0.x	6.6.0 +
	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 （6 ページ）	Firepower 1000 シリーズ	6.4.0	6.5.0 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
	FTD/FDM アップグレード時に削除される履歴データ （6 ページ）	FDM を使用した FTD	6.2.3 ～ 6.4.0.x	6.5.0 以降
	新しい URL カテゴリとレピュテーション （7 ページ）	任意（Any）	6.2.3 ～ 6.4.0.x	6.5.0 以降
	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（14 ページ）	Firepower 2100 シリーズ Firepower 4100/9300	6.2.3 ～ 6.3.0.x	6.4.0 以降

FMCv をアップグレードするには 28 GB の RAM が必要

展開：FMCv

アップグレード元：バージョン 6.5.0.x

直接アップグレード先：バージョン 6.6.0+

すべての FMCv 実装には同じ RAM 要件が適用され、32 GB が推奨、28 GB が必須となりました（FMCv 300 の場合は 64 GB）。仮想アプライアンスに割り当てられたメモリが 28 GB 未満の場合、バージョン 6.6.0+ へのアップグレードは失敗します。アップグレード後、メモリ割り当てを引き下げると、正常性モニタがアラートを発行します。

これらの新しいメモリ要件は、すべての仮想環境にわたって一貫した要件を適用し、パフォーマンスを向上させ、新しい機能を利用できるようにします。デフォルト設定を引き下げないことをお勧めします。使用可能なリソースによっては、パフォーマンスを向上させるために仮想アプライアンスのメモリと CPU の数を増やすことができます。FMCv のメモリ要件の詳細については、Cisco Firepower Management Center Virtual 入門ガイドを参照してください。

（注） バージョン 6.6.0 リリースの時点で、クラウドベースの FMCv の展開（AWS、Azure）でのメモリ不足インスタンスのタイプが完全に廃止されました。以前の Firepower バージョンであっても、これらを使用して新しい FMCv インスタンスを作成することはできません。既存のインスタンスは引き続き実行できます。

次の表に、メモリが不足している FMCv 展開のアップグレード前の要件を示します。

表 *4 :* バージョン *6.6.0+* にアップグレードする場合の *FMCv* のメモリ要件

プラットフォーム	アップグレード前のアクション	詳細
VMware	28 GB 以上（推奨 32 GB）を割り当てます。	最初に仮想マシンの電源をオフにします。 手順については、VMware のマニュアルを参照してください。
KVM	28 GB 以上（推奨 32 GB）を割り当てます。	手順については、ご使用の KVM 環境のマニュアルを参照してください。
AWS	インスタンスのサイズを変更します。 • c3.xlarge から c3.4xlarge へ。 • c3.2.xlarge から c3.4xlarge へ。 • c4.xlarge から c4.4xlarge へ。 • c4.2xlarge から c4.4xlarge へ。 また、新規展開用に c5.4xlarge インスタンスも用意しています。	サイズを変更する前にインスタンスを停止します。これを行うと、インスタンスストアのボリューム上のデータが失われるため、最初にインスタンスストアによってバックアップされたインスタンスを最初に移行してください。さらに、管理インターフェイスに復元力のある IP アドレスがない場合は、そのパブリック IP アドレスが解放されます。 手順については、Linux インスタンスの AWS ユーザガイドのインスタンスタイプの変更に関するマニュアルを参照してください。
Azure	インスタンスのサイズを変更します。 • Standard_D3_v2 から Standard_D4_v2 へ。	Azure ポータルまたは PowerShell を使用します。サイズを変更する前にインスタンスを停止する必要はありませんが、停止すると追加のサイズが表示される場合があります。サイズ変更により、実行中の仮想マシンが再起動されます。 手順については、Windows VM のサイズ変更に関する Azure のマニュアルを参照してください。

FMC のアップグレード後にイベントが一時的に使用できない

展開：FMC

アップグレード元：バージョン 6.5.0.x

直接アップグレード先：バージョン 6.6.0+

バージョン 6.6.0 では、接続およびセキュリティ インテリジェンス イベントに新しいデータストアを使用します。

アップグレードが完了し、FMC がリブートすると、履歴接続イベントとセキュリティ インテリジェンスイベントがバックグラウンドで移行され、リソースが制限されます。FMC モデル、システム負荷、および保存したイベント数に応じて、数時間から最大で 1 日かかることがあります。

履歴イベントは、経過時間ごとに、最新のイベントが最初に以降されます。移行されていないイベントは、クエリ結果やダッシュボードに表示されません。移行が完了する前に接続イベントデータベースの制限に達した場合（アップグレード後のイベントの場合など）、最も古い履歴イベントは移行されません。

ヒント　メニューバーの [システムステータス（System Status）] アイコンをクリックして、メッセージセンターでイベントの移行の進行状況をモニタします。

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「安全に消去する」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。

FTD/FDM アップグレード時に削除される履歴データ

展開：Firepower Device Manager

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 以降

データベース スキーマの変更により、すべての履歴レポート データがアップグレード中に削除されます。アップグレード後、履歴データをクエリしたり、履歴データをダッシュボードに表示したりすることはできません。

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。カテゴリの変更に関する詳細なリストについては、『Cisco Firepower Release Notes, Version 6.5.0』を参照してください。新しい URL カテゴリの説明については、Talos の「Intelligence Categories」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（Questionable）、ニュートラル（Neutral）、好ましい（Favorable）、信頼されている（Trusted）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、レピュテーションによりさらに制約を追加することはできません。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されていない（Untrusted）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、信頼されていない（Untrusted）レピュテーションの未分類 URL は、「悪意のあるサイト（Malicious Sites）」という新しい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 もカテゴリで制約する必要があります。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 *5:* 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 が若干変更されることがあります。
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 *6:* 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 のリソースにアクセス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特定します（次の項を参照）。 （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 **[Policies]** > **[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（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 7: 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。	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、これらのルールがマークされます。
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。	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。この場合は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。	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（11 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。	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。	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 をレピュテーションでフィルタ処理することも、レピュテーションのない URL をフィルタ処理することもできません。 [未分類（Uncategorized）] カテゴリまたは [すべて（Any）] のレピュテーションでフィルタ処理されるルールが、期待どおりに動作することを確認してください。

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 *8*：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を決定	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。
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。

ガイドライン	詳細
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 *9 :* 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。

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。

一般的なガイドライン

これらの一般的なガイドラインは、すべてのアップグレードに適用されます。

アプライアンスの正常性と通信

アップグレードプロセスの間、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。マイナーな問題がメジャーな問題になる前に解決します。

応答しないアップグレード

アップグレードしているアプライアンスとの間での変更の展開、またはアップグレードしているアプライアンスの手動での再起動やシャットダウンは行わないでください。進行中のアップグレードを再開しないでください。事前のチェック中に、アップグレードプロセスが停止しているように見える場合がありますが、これは想定内の動作です。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合には Cisco TAC にお問い合わせください。

アップグレード前のチェックリスト

このチェックリストは、一般的なアップグレードの問題を回避できるアクションを示しています。 ただし、このリストは包括的なものではありません。詳細な手順については、該当するアップグレードガイド（「アップグレード手順 （30 ページ）」）を参照してください。

表 *10 : Firepower* ソフトウェアのアップグレード前チェックリスト

✓	アクション	詳細
	導入評価。	FirePOWER アプライアンスをアップグレードする前に、展開の現在の状態を判断します。状況を理解することにより、目的を達成する方法を決定します。 少なくとも次の項目に回答できる必要があります。 • どんなアプライアンスがありますか、またどの FirePOWER バージョンを実行していますか。どのバージョンを実行したいですか、またそのバージョンは実行可能ですか。直接アップグレードできますか。FMC 展開では、FMC デバイスの互換性を維持できますか。 • アプライアンスのいずれかで個別のオペレーティングシステムのアップグレードが必要ですか。ホスティング環境のアップグレードを必要とする仮想アプライアンスはありますか。 • ハイアベイラビリティ/スケーラビリティを実現するように設定されていますか。デバイスは、IPS として、ファイアウォールとして、パッシブに展開されていますか。

✓	アクション	詳細
	管理ネットワークの帯域幅を確認します。	Firepowerアプライアンスをアップグレードする（または準備状況チェックを実行する）には、アップグレードパッケージがアプライアンス上に存在する必要があります。Firepowerアップグレードパッケージには、さまざまなサイズがあります。管理ネットワークに大量のデータ転送を実行するための帯域幅があることを確認します。 FMCの展開では、アップグレードパケージをアップグレード時に管理対象デバイスに転送する場合は、帯域幅が不十分だとアップグレード時間が長くなったり、アップグレードがタイムアウトする原因となったりする可能性があります。アップグレードする前に、FMC、またはFTDデバイスの場合は独自の内部Webサーバのいずれかから、管理対象デバイスにFirepowerアップグレードパッケージを手動でプッシュ（コピー）することをお勧めします。 『Firepower Management Centerから管理対象装置へのデータをダウンロードするためのガイドライン』（トラブルシューティングテクニカルノーツ）を参照してください。
	アプライアンスへのアクセスを確認します。	Firepowerデバイスは、（インターフェイス設定に応じて）アップグレード中、またはアップグレードが失敗した場合に、トラフィックを渡すことを停止できます。Firepowerデバイスをアップグレードする前に、ユーザの位置からのトラフィックがデバイスの管理インターフェイスにアクセスするためにデバイス自体を通過する必要がないことを確認してください。FMCの展開では、デバイスを経由せずにFMC管理インターフェイスにアクセスできる必要もあります。
	設定変更を計画します。	主要なアップグレードでは特に、アップグレードの前または後に、アップグレードにより重要な設定変更が発生することがあります。たとえば、廃止されたFlexConfigコマンドは、アップグレード後の展開の問題を引き起こす可能性があります。 「Firepowerソフトウェアのアップグレードガイドラインについて（1ページ）」のチェックリストを使用して、潜在的な問題を特定します。

✓	アクション	詳細
	バックアップを実行します。	アップグレードの前後に Firepower アプライアンスをバックアップします（サポートされている場合）。 • アップグレード前：アップグレードが致命的な失敗であった場合は、再イメージ化を実行し、復元する必要がある場合があります。再イメージ化によって、システムパスワードを含むほとんどの設定が工場出荷時の初期状態に戻ります。最近のバックアップがある場合は、通常の操作にすばやく戻ることができます。 • アップグレード後：これにより、新しくアップグレードされた展開のスナップショットが作成されます。新しいFMCバックアップファイルがデバイスがアップグレードされたことを「認識」するように、管理対象デバイスをアップグレードした後に FMC をバックアップすることをお勧めします。 **注意** Firepower アプライアンスを安全なリモートロケーションにバックアップし、正常に転送が行われることを確認することを強くお勧めします。アプライアンスに残っているバックアップは、手動またはアップグレードプロセスによって削除できます（アップグレードプロセスでは、ローカルに保存されたバックアップが消去される）。特に、バックアップファイルは暗号化されていないため、不正アクセスを許可しないでください。バックアップ ファイルが変更されていると、復元プロセスは失敗します。 バックアップと復元は、複雑なプロセスになる可能性があります。手順をスキップしたり、セキュリティやライセンスの問題を無視しないでください。誤りを避けるには、注意深い計画と準備が役立ちます。バックアップと復元の要件、ガイドライン、制限事項、およびベストプラクティスの詳細については、ご使用の Firepower 製品のコンフィギュレーション ガイドを参照してください。
	準備状況チェックを実行します。	FMC展開では、準備状況チェックをお勧めします。このチェックにより、Firepowerをアップグレードするためのアプライアンスの準備状況を評価できます。このチェックにより、データベース整合性、バージョン不一致、デバイス登録などの問題を識別できます。

✓	アクション	詳細
	アップグレードをスケジュール設定します。1007	アップグレードのスケジュール設定は、中断による展開環境への影響が最も小さい時間に行うことを推奨します。 メンテナンスウィンドウをスケジュールするときは、トラフィックフローおよびインスペクションへの影響と、アップグレードにかかる可能性がある時間を考慮します。また、ウィンドウで実行する必要があるタスクと、事前に実行できるタスクを検討します。慎重な計画と準備で中断を最小限に抑えます。メンテナンスウィンドウがアップグレードパッケージの取得およびプッシュ、準備状況チェックの実行、バックアップの作成などを行うまで待機しないようにします。
	NTP 同期を確認します。	時刻の提供に使用している NTP サーバと Firepower アプライアンスが同期していることを確認します。同期されていないと、アップグレードが失敗する可能性があります。FMC 展開では、時刻のずれが 10 秒を超えている場合、[時刻同期化ステータス（Time Synchronization Status）] ヘルスモジュールからアラートが発行されますが、手動で確認する必要もあります。 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。
	ASA FirePOWER デバイスで ASA REST API を無効化します。	ASA FirePOWER モジュールをアップグレードする前に、ASA REST API を無効にしていることを確認します。無効にしていない場合、アップグレードが失敗することがあります。ASA CLI から：`no rest api agent`。アンインストール後に再度有効にすることができます：`rest-api agent`。
	設定を展開します。	アップグレードする前に古いデバイスに設定を展開すると、失敗する可能性が減少します。 一部の展開では、設定が古い場合、アップグレードがブロックされることがあります。 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。 さらに、いくつかの設定を展開することで Snort が再起動されます。これにより、トラフィックのインスペクションが中断し、デバイスのトラフィックの処理方法によっては、再起動が完了するまでトラフィックが中断する場合があります。詳細については、トラフィック フロー、検査、およびデバイス動作 （22 ページ） を参照してください。

✓	アクション	詳細
	実行中のタスクを確認します。	アップグレードする前に、重要なタスクが完了していることを確認します。アップグレードの開始時に実行中のタスクは停止し、失敗したタスクとなり、再開できません。 また、アップグレード中に実行するようにスケジュールされたタスクを確認し、それらをキャンセルまたは延期することをお勧めします。バージョン 6.7.0 以降の FMC 展開では、アップグレードでスケジュールされたタスクが自動的に延期されるようになりました。アップグレード中に開始するようにスケジュールされたタスクは、アップグレード後の再起動の 5 分後に開始されます。
	ディスク容量を確認します。	最終的なディスク容量のチェックを実行します。空きディスク容量が十分でない場合、アップグレードは失敗します。詳細については、時間テストとディスク容量の要件 （19 ページ）を参照してください。

アップグレードする最小バージョン

次のように Version6.7.0 に直接アップグレードできます。特定のメンテナンスリリースまたはパッチレベルを実行する必要はありません。

表 *11 : Firepower* ソフトウェアをバージョン *6.7* にアップグレードするための最小バージョン。*0*

Platform	最小バージョン
Firepower Management Center	6.3.0
Firepower デバイス	6.3.0 FXOS 2.9.1.131 以降のビルド （Firepower 4100/9300 に必要）。

時間テストとディスク容量の要件

Firepower アプライアンスをアップグレードするには、十分な空きディスク容量が必要です。これがない場合、アップグレードは失敗します。Firepower Management Center を使用して管理対象デバイスをアップグレードする場合、デバイスアップグレードパッケージに対して、FMC は /Volume パーティションに追加のディスク容量を必要とします。また、アップグレードを実行するための十分な時間を確保してください。

参考のために、社内の時間とディスク容量のテストに関するレポートを提供しています。

時間テストについて

ここで指定した時間の値は、社内のテストに基づいています。

（注） 特定のプラットフォーム/シリーズについてテストされたすべてのアップグレードの最も遅い時間を報告していますが、複数の理由により（以下を参照）、報告された時間よりも、アップグレードにかかる時間が長くなることがあります。

テスト条件

- 展開：値は、Firepower Management Center 展開のテストから取得されています。これは、同様の条件の場合、リモートとローカルで管理されているデバイスの raw アップグレード時間が類似しているためです。
- バージョン：メジャー アップグレードの場合、以前のすべての対象メジャー バージョンからのアップグレードをテストします。パッチについては、ベースバージョンからアップグレードをテストします。
- モデル：ほとんどの場合、各シリーズの最もローエンドのモデルでテストし、場合によってはシリーズの複数のモデルでテストします。
- 仮想設定：メモリおよびリソースのデフォルト設定を使用してテストします。
- ハイアベイラビリティと拡張性：スタンドアロンデバイスでテストします。

  ハイアベイラビリティの構成またはクラスタ化された構成では、動作の継続性を保持するため、複数のデバイスは1つずつアップグレードされます。アップグレード中は、各デバイスはメンテナンス モードで動作します。そのため、デバイス ペアまたはクラスタ全体のアップグレードには、スタンドアロンデバイスのアップグレードよりも長い時間がかかります。
- 構成：構成とトラフィック負荷が最小限のアプライアンスでテストします。

  アップグレード時間は、構成の複雑さ、イベントデータベースのサイズ、また、それらがアップグレードから影響を受けるかどうか、受ける場合はどのような影響を受けるかにより、長くなる場合があります。たとえば多くのアクセス制御ルールを使用している場合、アップグレードはこれらのルールの格納方法をバックエンドで変更する必要があるため、アップグレードにはさらに長い時間がかかります。

時間はアップグレードのみを対象

値は、各プラットフォーム上で Firepower アップグレードスクリプトの実行にかかる時間のみを表しています。これらには、次の時間は含まれていません。

- 管理対象デバイスへのアップグレードパッケージの転送（アップグレード前かアップグレード中かにかかわらない）。
- 準備状況チェック。

- VDB と SRU の更新。
- 設定の展開。
- リブート（値が別途に報告される場合がある）。

ディスク容量の要件について

容量の見積もりは、すべてのアップグレードについて報告された最大のものです。2020年前半以降のリリースでは、次のようになります。

- 切り上げなし（1 MB 未満）。
- 次の 1 MB に切り上げ（1 MB ～ 100 MB）。
- 次の 10 MB に切り上げ（100 MB ～ 1 GB）。
- 次の 100 MB に切り上げ（1 GB を超える容量）。

バージョン 6.7.0 の時間とディスク容量

表 *12 :* バージョン *6.7.0* の時間とディスク容量

[Platform]	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リブート時間
FMC	13.6 GB	70 MB	—	46 分	9 分
FMCv：VMware 6.0	15.5 GB	64 MB	—	35 分	8 分
Firepower 1000 シリーズ	430 MB	11 GB	2 GB	17 分	16 分
Firepower 2100 シリーズ	500 MB	11 GB	1.1 GB	15 分	16 分
Firepower 4100 シリーズ	10 MB	10 GB	1.1 GB	10 分	12 分
Firepower 4100 シリーズコンテナインスタンス	8 MB	9.5 GB	1.1 GB	10 分	9 分
Firepower 9300	64 MB	11.1 GB	1.1 GB	13 分	12 分
ASA 5500-X シリーズ with FTD	8.7 GB	96 KB	1.1 GB	26 分	13 分

[Platform]	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リブート時間
FTDv：VMware 6.0	8.1 GB	26 KB	1.1 GB	14 分	18 分
ASA FirePOWER	10.3 GB	64 MB	1.3 GB	62 分	11 分
NGIPSv：VMware 6.0	5.5 GB	54 MB	840 MB	10 分	6 分

トラフィック フロー、検査、およびデバイス動作

アップグレード中に発生するトラフィック フローおよびインスペクションでの潜在的な中断を特定する必要があります。これは、次の場合に発生する可能性があります。

- デバイスが再起動された場合。
- デバイス上でオペレーティング システムまたは仮想ホスティング環境をアップグレードする場合。
- デバイス上で Firepower ソフトウェアをアップグレードするか、パッチをアンインストールする場合。
- アップグレードまたはアンインストール プロセスの一部として設定変更を展開する場合（Snort プロセスが再開します）。

デバイスのタイプ、展開のタイプ（スタンドアロン、ハイアベイラビリティ、クラスタ化）、およびインターフェイスの設定（パッシブ、IPS、ファイアウォールなど）によって中断の性質が決まります。アップグレードまたはアンインストールは、保守期間中に行うか、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。

FTD アップグレード時の動作： Firepower 4100/9300 シャーシ

このセクションでは、FTD を搭載した Firepower 4100/9300 シャーシをアップグレードするときのデバイスとトラフィックの動作を説明します。

Firepower 4100/9300 シャーシ：FXOS のアップグレード

シャーシ間クラスタリングまたはハイアベイラビリティペアの構成がある場合でも、各シャーシの FXOS を個別にアップグレードします。アップグレードの実行方法により、FXOS のアップグレード時にデバイスがトラフィックを処理する方法が決定されます。

表 *13 : FXOS* アップグレード中のトラフィックの動作

導入	メソッド	トラフィックの動作
スタンドアロン	—	廃棄

導入	メソッド	トラフィックの動作
ハイアベイラビリティ	**ベストプラクティス**：スタンバイで FXOS を更新し、アクティブピアを切り替えて新しいスタンバイをアップグレードします。	影響なし。
	スタンバイでアップグレードが終了する前に、アクティブ ピアで FXOS をアップグレードします。	1 つのピアがオンラインになるまでドロップされる。
シャーシ間クラスタ（6.2 以降）	**ベストプラクティス**：少なくとも 1 つのモジュールを常にオンラインにするため、一度に 1 つのシャーシをアップグレードします。	影響なし。
	ある時点ですべてのモジュールを停止するため、シャーシを同時にアップグレードします。	少なくとも 1 つのモジュールがオンラインになるまでドロップされる。
シャーシ内クラスタ（Firepower 9300 のみ）	ハードウェアバイパス有効：[Bypass: Standby] または [Bypass-Force]。（6.1 以降）	検査なしで受け渡される。
	ハードウェアバイパス無効：[Bypass: Disabled]。（6.1 以降）	少なくとも 1 つのモジュールがオンラインになるまでドロップされる。
	ハードウェア バイパス モジュールなし。	少なくとも 1 つのモジュールがオンラインになるまでドロップされる。

スタンドアロン FTD デバイス：Firepower ソフトウェアのアップグレード

アップグレード中、Firepower デバイス/セキュリティモジュールはメンテナンスモードで稼働します。アップグレードの開始時にメンテナンスモードを開始すると、トラフィックインスペクションが 2 ー 3 秒中断します。インターフェイスの構成により、その時点とアップグレード中の両方のスタンドアロンデバイスによるトラフィックの処理方法が決定されます。

表 *14 : Firepower* ソフトウェアアップグレード中のトラフィックの動作：スタンドアロン *FTD* デバイス

インターフェイス コンフィギュレーション	トラフィックの動作
ファイアウォールインターフェイス	EtherChannel、冗長、サブインターフェイスを含むルーテッドまたはスイッチド。 スイッチドインターフェイスは、ブリッジグループまたはトランスペアレントインターフェイスとしても知られています。	廃棄

インターフェイス コンフィギュレーション		トラフィックの動作
IPS のみのインターフェイス	インラインセット、ハードウェアバイパス強制が有効：[Bypass: Force]（6.1 以上）。	ハードウェアバイパスを無効にするか、スタンバイモードに戻すまで、インスペクションなしで合格。
	インラインセット、ハードウェアバイパス スタンバイ モード：[Bypass: Standby]（6.1 以上）。	デバイスがメンテナンスモードの場合、アップグレード中にドロップされます。その後、デバイスがアップグレード後の再起動を完了する間、インスペクションなしで合格します。
	インラインセット、ハードウェアバイパスが無効：[Bypass: Disabled]（6.1 以上）。	廃棄
	インラインセット、ハードウェアバイパス モジュールなし。	廃棄
	インラインセット、タップモード。	パケットをただちに出力、コピーへのインスペクションなし。
	パッシブ、ERSPAN パッシブ。	中断なし、インスペクションなし。

ハイアベイラビリティペア：FirePOWER ソフトウェアアップグレード

ハイ アベイラビリティ ペアのデバイスの FirePOWER ソフトウェアをアップグレードする間に、トラフィック フローまたはインスペクションが中断されることはありません。継続稼働できるように、一度に1つずつアップグレードされます。アップグレード中、デバイスはメンテナンス モードで稼働します。

スタンバイ側のデバイスが最初にアップグレードされます。デバイスの役割が切り替わり、新しくスタンバイになったデバイスがアップグレードされます。アップグレードの完了時には、デバイスの役割は切り替わったままです。アクティブ/スタンバイの役割を維持する場合、アップグレード前に役割を手動で切り替えます。それにより、アップグレードプロセスによって元の役割に切り替わります。

クラスタ：FirePOWER ソフトウェア アップグレード

Firepower Threat Defense クラスタのデバイスで FirePOWER ソフトウェアをアップグレードする間に、トラフィック フローまたはインスペクションが中断されることはありません。継続稼働できるように、一度に 1 つずつアップグレードされます。データ セキュリティ モジュールを最初にアップグレードして、その後コントロールモジュールをアップグレードします。アップグレード中、セキュリティモジュールはメンテナンスモードで稼働します。

コントロール セキュリティ モジュールをアップグレードする間、通常トラフィック インスペクションと処理は続行しますが、システムはロギングイベントを停止します。ロギングダウン

タイム中に処理されるトラフィックのイベントは、アップグレードが完了した後、非同期のタイムスタンプ付きで表示されます。ただし、ロギングダウンタイムが大きい場合、システムはログ記録する前に最も古いイベントをプルーニングすることがあります。

（注） バージョン6.2.0、6.2.0.1、または6.2.0.2からシャーシ間クラスタをアップグレードすると、各モジュールがクラスタから削除されるときに、トラフィック インスペクションで2～3秒のトラフィック中断が発生します。

ハイアベイラビリティとクラスタリング ヒットレス アップグレードの要件

ヒットレスアップグレードの実行には、次の追加要件があります。

フローオフロード：フローオフロード機能でのバグ修正により、FXOSとFTDのいくつかの組み合わせはフローオフロードをサポートしていません。『Cisco Firepower Compatibility Guide』を参照してください。ハイアベイラビリティまたはクラスタ化された展開でヒットレスアップグレードを実行するには、常に互換性のある組み合わせを実行していることを確認する必要があります。

アップグレードパスに FXOS の2.2.2.91、2.3.1.130、またはそれ以降のアップグレード（FXOS 2.4.1. x、2.6.1 などを含む）が含まれている場合、次のパスを使用します。

1. FTD を 6.2.2.2 以降にアップグレードします。

2. FXOS を 2.2.2.91、2.3.1.130、またはそれ以降にアップグレードします。

3. FTD を最終バージョンにアップグレードします。

たとえば、FXOS 2.2.2.17/FTD 6.2.2.0 を実行していて、FXOS 2.6.1/FTD 6.4.0 にアップグレードする場合は、次を実行できます。

1. FTD を 6.2.2.5 にアップグレードします。

2. FXOS を 2.6.1 にアップグレードします。

3. FTD を 6.4.0 にアップグレードします。

バージョン6.1.0へのアップグレード：FTDハイアベイラビリティペアのバージョン6.1.0へのヒットレスアップグレードを実行するには、プレインストールパッケージが必要です。詳細については、『Firepower System Release Notes Version 6.1.0 Preinstallation Package』を参照してください。

展開時のトラフィックの動作

アップグレード プロセス中には、設定を複数回展開します。Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。詳細については、『Firepower Management Center 構成ガイド』の「Configurations that Restart the Snort Process when Deployed or Activated」を参照してください。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、Snortプロセスを再起動すると、HA/スケーラビリティ用に設定されたものを含め、すべての Firepower デバイスでトラフィック インスペクションが中断されます。インターフェイス設定により、中断中にインスペクションせずにトラフィックをドロップするか受け渡すかが決定されます。

表 *15 : FTD* 展開時のトラフィックの動作

インターフェイス コンフィギュレーション		トラフィックの動作
ファイアウォール インターフェイス	EtherChannel、冗長、サブインターフェイスを含むルーテッドまたはスイッチド。 スイッチドインターフェイスは、ブリッジグループまたはトランスペアレントインターフェイスとしても知られています。	廃棄
IPS のみのインターフェイス	インラインセット、[Failsafe] が有効または無効（6.0.1 ～ 6.1）。	検査なしで受け渡される。 [フェールセーフ（Failsafe）] が無効で、Snortがビジーでもダウンしていない場合、いくつかのパケットがドロップすることがあります。
	インラインセット、[Snort Fail Open: Down]：無効（6.2 以降）	廃棄
	インラインセット、[Snort Fail Open: Down]：有効（6.2 以降）	検査なしで受け渡される。
	インラインセット、タップモード。	パケットをただちに出力、コピーへのインスペクションなし。
	パッシブ、ERSPAN パッシブ。	中断なし、インスペクションなし。

FTD アップグレード時の動作：その他のデバイス

このセクションでは、Firepower 1000/2100 シリーズ、ASA 5500-X シリーズ、ISA 3000、および FTDv で Firepower Threat Defense をアップグレードするときのデバイスとトラフィックの動作を説明します。

スタンドアロン FTD デバイス：Firepower ソフトウェアのアップグレード

アップグレード中、Firepower デバイスはメンテナンスモードで稼働します。アップグレードの開始時にメンテナンスモードを開始すると、トラフィック インスペクションが 2 ー 3 秒中断

します。インターフェイスの構成により、その時点とアップグレード中の両方のスタンドアロンデバイスによるトラフィックの処理方法が決定されます。

表 *16 : Firepower* ソフトウェアアップグレード中のトラフィックの動作：スタンドアロン *FTD* デバイス

インターフェイス コンフィギュレーション		トラフィックの動作
ファイアウォールインターフェイス	EtherChannel、冗長、サブインターフェイスを含むルーテッドまたはスイッチド。 スイッチドインターフェイスは、ブリッジグループまたはトランスペアレントインターフェイスとしても知られています。	廃棄
IPS のみのインターフェイス	インラインセット、ハードウェアバイパス強制が有効：[Bypass: Force]（Firepower 2100 シリーズ、6.3 以上）。	ハードウェアバイパスを無効にするか、スタンバイモードに戻すまで、インスペクションなしで合格。
	インラインセット、ハードウェアバイパス スタンバイ モード：[Bypass: Standby]（Firepower 2100 シリーズ、6.3 以上）。	デバイスがメンテナンスモードの場合、アップグレード中にドロップされます。その後、デバイスがアップグレード後の再起動を完了する間、インスペクションなしで合格します。
	インラインセット、ハードウェアバイパスが無効：[Bypass: Disabled]（Firepower 2100 シリーズ、6.3 以上）。	廃棄
	インラインセット、ハードウェアバイパス モジュールなし。	廃棄
	インラインセット、タップモード。	パケットをただちに出力、コピーへのインスペクションなし。
	パッシブ、ERSPAN パッシブ。	中断なし、インスペクションなし。

ハイアベイラビリティペア：FirePOWER ソフトウェアアップグレード

ハイ アベイラビリティ ペアのデバイスの FirePOWER ソフトウェアをアップグレードする間に、トラフィック フローまたはインスペクションが中断されることはありません。継続稼働できるように、一度に 1 つずつアップグレードされます。アップグレード中、デバイスはメンテナンス モードで稼働します。

スタンバイ側のデバイスが最初にアップグレードされます。デバイスの役割が切り替わり、新しくスタンバイになったデバイスがアップグレードされます。アップグレードの完了時には、デバイスの役割は切り替わったままです。アクティブ/スタンバイの役割を維持する場合、アップグレード前に役割を手動で切り替えます。それにより、アップグレードプロセスによって元の役割に切り替わります。

展開時のトラフィックの動作

アップグレード プロセス中には、設定を複数回展開します。Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。詳細については、『Firepower Management Center 構成ガイド』の「Configurations that Restart the Snort Process when Deployed or Activated」を参照してください。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、Snortプロセスを再起動すると、HA/スケーラビリティ用に設定されたものを含め、すべての Firepower デバイスでトラフィック インスペクションが中断されます。インターフェイス設定により、中断中にインスペクションせずにトラフィックをドロップするか受け渡すかが決定されます。

表 *17 : FTD* 展開時のトラフィックの動作

インターフェイス コンフィギュレーション		トラフィックの動作
ファイアウォール インターフェイス	EtherChannel、冗長、サブインターフェイスを含むルーテッドまたはスイッチド。 スイッチドインターフェイスは、ブリッジグループまたはトランスペアレントインターフェイスとしても知られています。	廃棄
IPS のみのインターフェイス	インラインセット、[Failsafe] が有効または無効（6.0.1 ～ 6.1）。	検査なしで受け渡される。 [フェールセーフ（Failsafe）] が無効で、Snortがビジーでもダウンしていない場合、いくつかのパケットがドロップすることがあります。
	インラインセット、[Snort Fail Open: Down]：無効（6.2 以降）	廃棄
	インラインセット、[Snort Fail Open: Down]：有効（6.2 以降）	検査なしで受け渡される。
	インラインセット、タップモード。	パケットをただちに出力、コピーへのインスペクションなし。
	パッシブ、ERSPAN パッシブ。	中断なし、インスペクションなし。

ASA FirePOWER アップグレード時の動作

ASA FirePOWER module にトラフィックをリダイレクトする ASA サービス ポリシーは、Firepower ソフトウェア アップグレードの間（Snort プロセスを再起動する特定の設定を導入するときなど）にモジュールがトラフィックを処理する方法を決定します。

表 *18 : ASA FirePOWER* アップグレード中のトラフィックの動作

トラフィック リダイレクションのポリシー	トラフィックの動作
フェール オープン（**sfr fail-open**）	インスペクションなしで転送
フェール クローズ（**sfr fail-close**）	ドロップされる
モニタのみ（**sfr {fail-close}|{fail-open} monitor-only**）	パケットをただちに出力、コピーへのインスペクションなし

ASA FirePOWER 展開時のトラフィックの動作

Snort プロセスを再起動している間のトラフィックの動作は、ASA FirePOWER module をアップグレードする場合と同じです。

アップグレード プロセス中には、設定を複数回展開します。Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。詳細については、『Firepower Management Center 構成ガイド』の「Configurations that Restart the Snort Process when Deployed or Activated」を参照してください。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。 さらに、Snort プロセスを再起動すると、トラフィック インスペクションが中断されます。サービスポリシーにより、中断中にインスペクションせずにトラフィックをドロップするか通過するかが決定されます。

NGIPSv アップグレード時の動作

このセクションでは、NGIPSvをアップグレードするときのデバイスとトラフィックの動作を説明します。

Firepower ソフトウェア アップグレード

インターフェイスの設定により、アップグレード中に NGIPSv がトラフィックを処理する方法が決定されます。

表 *19 : NGIPSv* アップグレード中のトラフィックの動作

インターフェイス コンフィギュレーション	トラフィックの動作
インライン	切断

インターフェイス コンフィギュレーション	トラフィックの動作
インライン、タップ モード	パケットをただちに出力、コピーへのインスペクションなし
Passive	中断なし、インスペクションなし

展開時のトラフィックの動作

アップグレード プロセス中には、設定を複数回展開します。Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。詳細については、『Firepower Management Center 構成ガイド』の「Configurations that Restart the Snort Process when Deployed or Activated」を参照してください。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。さらに、Snortプロセスを再起動すると、トラフィック インスペクションが中断されます。インターフェイス設定により、中断中にインスペクションせずにトラフィックをドロップするか受け渡すかが決定されます。

表 *20 : NGIPSv* 展開時のトラフィックの動作

インターフェイス コンフィギュレーション	トラフィックの動作
インライン、[フェールセーフ（Failsafe）] が有効または無効	インスペクションなしで転送 [フェールセーフ（Failsafe）] が無効で、Snort がビジーでもダウンしていない場合、いくつかのパケットがドロップすることがあります。
インライン、タップ モード	すぐにパケットを出力し、バイパス Snort をコピーする
Passive	中断なし、インスペクションなし

アップグレード手順

リリース ノートにはアップグレード手順は含まれていません。これらのリリースノートに記載されているガイドラインと警告を読んだ後、次のいずれかのドキュメントを参照してください。

表 *21 : Firepower* アップグレード手順

タスク	ガイド
FMC 展開のアップグレード。	Cisco Firepower Management Center Upgrade Guide

タスク	ガイド
FDM を使用した Firepower Threat Defense ソフトウェアのアップグレード。	Firepower Device Manager 用 Cisco Firepower Threat Defense 構成ガイド アップグレード先のバージョンではなく、現在実行している FTD バージョンのガイドの「システム管理」の章を参照してください。
Firepower 4100/9300 シャーシの FXOS のアップグレード。	Cisco Firepower 4100/9300 Upgrade Guide
ASDM を使用した ASA FirePOWER モジュールのアップグレード。	Cisco ASA Upgrade Guide
での ROMMON イメージのアップグレード。	Cisco ASA and Firepower Threat Defense Reimage Guide 「*Upgrade the ROMMON Image*」のセクションを参照してください。常に最新のイメージがあることを確認してください。

アップグレードパッケージ

アップグレード パッケージは、 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。

- FMCv を含む Firepower Management Center：https://www.cisco.com/go/firepower-software
- Firepower Threat Defense（ISA 3000）： https://www.cisco.com/go/isa3000-software
- Firepower Threat Defense（FTDv を含む他のすべてのモデル）：https://www.cisco.com/go/ftd-software
- ASA with FirePOWER Services（ASA 5500-X シリーズ）： https://www.cisco.com/go/asa-firepower-sw
- ASA with FirePOWER Services（ISA 3000）： https://www.cisco.com/go/isa3000-software
- NGIPSv： https://www.cisco.com/go/ngipsv-software

Firepower ソフトウェア アップグレード パッケージを検索するには、Firepower アプライアンス モデルを選択または検索し、現在のバージョンの Firepower ソフトウェアのダウンロード ページを参照します。使用可能なアップグレード パッケージは、インストール パッケージ、ホットフィックス、およびその他の該当するダウンロードとともに表示されます。

ヒント インターネットにアクセスできる FMC は、手動でダウンロードできるようになってから約 2 週間後に、シスコから Firepower メンテナンスリリース（Version6.7.x3 桁番号のアップグレード）を直接ダウンロードできます。次の場合、シスコからの直接ダウンロードはサポートされていません。

- メジャーリリース。
- バージョン 6.6 以降へのほとんどのパッチ。
- FDM または ASDM 展開。

ファミリまたはシリーズのすべての Firepower モデルに同じアップグレードパッケージを使用します。アップグレードパッケージのファイル名には、プラットフォーム、パッケージタイプ（アップグレード、パッチ、ホットフィックス）、および Firepower のバージョンが反映されています。 メンテナンスリリースでは、アップグレード パッケージ タイプが使用されることに注意してください。

次に例を示します。

- パッケージ：`Cisco_Firepower_Mgmt_Center_Upgrade-6.6.0-90.sh.REL.tar`
- プラットフォーム： Firepower Management Center
- パッケージタイプ：アップグレード
- バージョンおよびビルド：6.6.0-90
- ファイル拡張子：sh.REL.tar

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、アップグレードパッケージとホットフィックスパッケージは署名付きのアーカイブになっています。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。表示を高速化するには、のパッケージが不要になった後、それらのパッケージを削除します。

表 *22 : Firepower* ソフトウェア アップグレード パッケージ

Platform	パッケージ
FMC/FMCv	Cisco_Firepower_Mgmt_Center
Firepower 1000 シリーズ	Cisco_FTD_SSP-FP1K
Firepower 2100 シリーズ	Cisco_FTD_SSP-FP2K

Platform	パッケージ
Firepower 4100/9300 シャーシ	Cisco_FTD_SSP
FTD を搭載した ASA 5500-X シリーズ FTD を搭載した ISA 3000 FTDv	Cisco_FTD
ASA FirePOWER	Cisco_Network_Sensor
NGIPSv	Cisco_Firepower_NGIPS_Virtual

オペレーティングシステムのアップグレードパッケージ

オペレーティングシステムのアップグレードパッケージの詳細については、次のガイドの「アップグレードの計画」の章を参照してください。

- Cisco ASA Upgrade Guide（ASA OS の場合）
- Cisco Firepower 4100/9300 Upgrade Guide（FXOSの場合）