バージョン 6.5.0 へのアップグレード

この章では、バージョン 6.5.0 の重要なリリースに固有の情報を提供します。

また、新機能、廃止された機能とプラットフォーム、メニューと用語の変更、ブラックリストに登録された FlexConfig コマンドなどの情報に関して「特長と機能」に目を通す必要があります。

に関するガイドラインと警告 バージョン 6.5.0

このチェックリストには、バージョン 6.5.0 に関する新しい重要なアップグレード ガイドラインと警告が含まれています。「以前に公開されたガイドラインと警告 （22 ページ）」および「一般的なガイドラインと警告 （28 ページ）」も確認する必要があります。

表 *1* : 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 （2 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 での出力最適化の無効化 （2 ページ）	FTD	6.2.3 ～ 6.4.0.x	6.5.0 のみ

✓	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
	アップグレードによって北米の Cisco Cloud に展開が割り当てられる （3 ページ）	任意（Any）	6.2.3 ～ 6.4.0.x	6.5.0 以降
	Cisco 脅威インテリジェンスダイレクタ（TID） 動作の変更 （3 ページ）	FMC	6.2.3 ～ 6.4.0.x	6.5.0 以降
	FTD/FDM アップグレード時に削除される履歴データ （4 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 （4 ページ）	任意（Any）	6.2.3 ～ 6.4.0.x	6.5.0 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「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。

バージョン 6.5.0 での出力最適化の無効化

展開：FTD

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 のみ

CSCvq34340 を軽減するため、FTD デバイスをバージョン 6.4.0.7+ または バージョン 6.5.0.2+ にパッチすると、出力最適化処理がオフになります。これは、出力最適化機能が有効になっているか、無効になっているかに関係なく発生します。

バージョン 6.5.0 へのアップグレード：

- バージョン 6.2.3.x から：出力最適化を有効にしてオンにします。

- バージョン 6.3.0.x から：出力最適化を有効にしてオンにします。
- バージョン 6.4.0.x から：現在の設定を使用します。ただし、バージョン 6.4.0.x パッチにより出力最適化がオフになっても機能が引き続き有効になっている場合は、バージョン 6.5.0 へのアップグレードにより再度オンになります。

（注） バージョン 6.5.0.2+ にパッチを適用するか、またはバージョン 6.6.0 にアップグレードことをお勧めします。バージョン 6.5.0 または 6.5.0.1 のままの場合は、FTD CLI から **no asp inspect-dp egress-optimization** を実行して出力最適化を手動で無効にする必要があります。

この問題は、出力最適化が想定のとおりに動作するバージョン 6.6.0 で修正されました。詳細については、ソフトウェアアドバイザリ『FTD traffic outage due to 9344 block size depletion caused by the egress optimization feature』を参照してください。

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+

シスコ クラウド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。

FDM を使用した FTD の場合は、スマートライセンスに登録するときにリージョンを選択します。登録済みデバイスをアップグレードすると、米国（北米）リージョンに割り当てられます。リージョンを変更するには、Cisco Smart Software Manager（CSSM）で登録解除して再登録する必要があります。

Cisco 脅威インテリジェンスダイレクタ（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。以前にブロックされ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。

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。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 *2:* 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。 カテゴリの変更に関する詳細なリストについては、「URL カテゴリの変更 （12 ページ）」を参照してください。
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 *3:* 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 4: 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（16 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。 リスト：新しいカテゴリ （15 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。 リスト：マージされたカテゴリ （17 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（9 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 （18 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（20 ページ）および変更されていないカテゴリ （21 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 *5*：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 *6 :* 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 7: 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 （17 ページ）		[軍（Military）]	変更されていないカテゴリ （21 ページ）
乱用薬物	マージされたカテゴリ （17 ページ）		自動車	カテゴリの名前変更 （20 ページ）
アダルトとポルノ	カテゴリの分割（18 ページ）		Music	カテゴリの名前変更 （20 ページ）
アルコールとタバコ	カテゴリの分割（18 ページ）		ニュースとメディア	カテゴリの名前変更 （20 ページ）
ボットネット	カテゴリの名前変更 （20 ページ）		Nudity	カテゴリの名前変更 （20 ページ）
ビジネスと経済	カテゴリの分割（18 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 （20 ページ）
不正	カテゴリの名前変更 （20 ページ）		オープン HTTP プロキシ	カテゴリの名前変更 （20 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（18 ページ）		パーク ドメイン（Parked Domains）	変更されていないカテゴリ （21 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（18 ページ）		サーフへの支払い	マージされたカテゴリ （17 ページ）
確認済みのスパム送信元	マージされたカテゴリ （17 ページ）		ピアツーピア	カテゴリの名前変更 （20 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 （17 ページ）		個人のサイトやブログ	カテゴリの分割（18 ページ）
カルトとオカルト	カテゴリの分割（18 ページ）		個人ストレージ	カテゴリの分割（18 ページ）
出会い系（Dating）	変更されていないカテゴリ （21 ページ）		哲学と政治的主張	カテゴリの名前変更 （20 ページ）
休止サイト	カテゴリの名前変更 （20 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 （20 ページ）
動的生成コンテンツ	マージされたカテゴリ （17 ページ）		プライベート IP アドレス	廃止されたカテゴリ （16 ページ）
Educational Institutions	マージされたカテゴリ （17 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 （20 ページ）
エンターテイメントとアート	カテゴリの分割（18 ページ）		要検討	カテゴリの名前変更 （20 ページ）
ファッションと美容	カテゴリの名前変更 （20 ページ）		不動産（Real Estate）	変更されていないカテゴリ （21 ページ）
金融サービス	カテゴリの名前変更 （20 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 （17 ページ）
食品と食事	カテゴリの名前変更 （20 ページ）		参照および調査	カテゴリの分割（18 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（Gambling）	カテゴリの分割（18 ページ）		宗教（Religion）	変更されていないカテゴリ（21 ページ）
ゲーム（Games）	変更されていないカテゴリ（21 ページ）		Search Engines	マージされたカテゴリ（17 ページ）
政府/自治体	マージされたカテゴリ（17 ページ）		性教育（Sex Education）	マージされたカテゴリ（17 ページ）
総額	マージされたカテゴリ（17 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（20 ページ）
ハッキング（Hacking）	マージされたカテゴリ（17 ページ）		ショッピング（Shopping）	変更されていないカテゴリ（21 ページ）
中傷と人種差別	カテゴリの名前変更（20 ページ）		ソーシャル ネットワーク（Social Network）	カテゴリの分割（18 ページ）
健康と薬	カテゴリの名前変更（20 ページ）		社会	カテゴリの分割（18 ページ）
ホームとガーデン	カテゴリの分割（18 ページ）		スパム URL	マージされたカテゴリ（17 ページ）
狩猟と釣り	カテゴリの名前変更（20 ページ）		Sports	マージされたカテゴリ（17 ページ）
法律違反	カテゴリの分割（18 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（21 ページ）
画像とビデオ検索	カテゴリの名前変更（20 ページ）		ストリーミング メディア	カテゴリの名前変更（20 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（20 ページ）		水着と肌着	カテゴリの名前変更（20 ページ）

古いカテゴリ	変更内容		古いカテゴリ	変更内容
インターネット通信	カテゴリの分割（18 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 （17 ページ）
インターネットポータル	マージされたカテゴリ （17 ページ）		旅行（Travel）	変更されていないカテゴリ （21 ページ）
求職（Job Search）	変更されていないカテゴリ （21 ページ）		未分類	廃止されたカテゴリ （16 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 （17 ページ）		未確認のスパム送信元	マージされたカテゴリ （17 ページ）
こども用品	カテゴリの名前変更 （20 ページ）		暴力	マージされたカテゴリ （17 ページ）
リーガル	マージされたカテゴリ （17 ページ）		武器（Weapons）	変更されていないカテゴリ （21 ページ）
ローカル情報	カテゴリの名前変更 （20 ページ）		Web 広告	マージされたカテゴリ （17 ページ）
マルウェア サイト（Malware Sites）	変更されていないカテゴリ （21 ページ）		Web ベースの電子メール	カテゴリの分割（18 ページ）
マリファナ	マージされたカテゴリ （17 ページ）		Web ホスティング サイト	カテゴリの名前変更 （20 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 *8*: 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 *9*: 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 *10* : 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 （9 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 *11* : 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	

古いカテゴリ	新しくマージされたカテゴリ
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	
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 *12 :* 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（Pornography）
	アダルト（Adult）
アルコールとタバコ	アルコール（Alcohol）
	タバコ（Tobacco）
ビジネスと経済	ビジネスおよび産業（Business and Industry）
	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（Software Updates）
	コンピュータおよびインターネット（Computers and Internet）
	SaaS および B2B（SaaS and B2B）
	オンライン会議（Online Meetings）

古い単一カテゴリ	新しいカテゴリの分割
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（Computer Security）
	パーソナル VPN（Personal VPN）
カルトとオカルト	超常現象（Paranormal）
	占星術（Astrology）
エンターテイメントとアート	芸術（Arts）
	エンターテイメント（Entertainment）
ギャンブル（Gambling）	ギャンブル（Gambling）
	宝くじ（Lotteries）
ホームとガーデン	自然（Nature）
	DIY プロジェクト（DIY Projects）
法律違反	違法行為（Illegal Activities）
	児童虐待コンテンツ（Child Abuse Content）
	違法ダウンロード（Illegal Downloads）
インターネット通信	インターネット電話（Internet Telephony）
	チャットおよびインスタントメッセージ（Chat and Instant Messaging）
個人のサイトやブログ	個人サイト（Personal Sites）
	オンライン コミュニティ（Online Communities）
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（Online Storage and Backup）
	ファイル転送サービス（File Transfer Services）
参照および調査	科学技術（Science and Technology）
	社会科学（Social Science）

古い単一カテゴリ	新しいカテゴリの分割
ソーシャル ネットワーク（Social Network）	ソーシャル ネットワーキング（Social Networking）
	プロフェッショナル ネットワーキング（Professional Networking）
社会	社会および文化（Society and Culture）
	非政府組織
Web ベースの電子メール	Web-based Email
	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 *13 :* 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

古いカテゴリ名	新しいカテゴリ名
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）
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 *14* : 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（Dating）
ゲーム（Games）
求職（Job Search）
[軍（Military）]
パーク ドメイン（Parked Domains）

変更されていないカテゴリ
不動産（Real Estate）
宗教（Religion）
ショッピング（Shopping）
旅行（Travel）
武器（Weapons）

表 *15* : 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）

以前に公開されたガイドラインと警告

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。いくつかの以前のメジャー バージョンからバージョン 6.5.0 にアップグレードできます。アップグレードする最小バージョン （31 ページ）を参照してください。

表 *16* : 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（23 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 （24 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（24 ページ）	任意	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、NGIPSv で準備状況チェックに失敗する可能性（25 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（25 ページ）	FMC を使用した FTD	6.2.0 ～ 6.2.3.x	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（26 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（26 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（27 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（27 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（28 ページ）	FMC	6.1.0 ～ 6.2.3.x	6.3.0 以降

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。

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。

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、NGIPSv で準備状況チェックに失敗する可能性

展開：FMC、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 *17* : 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。

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。`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 [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（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。

一般的なガイドラインと警告

これらの重要なガイドラインと警告は、すべてのアップグレードに適用されます。ただし、このリストは包括的なものではありません。アップグレードパスの計画、OS のアップグレード、準備状況チェック、バックアップ、メンテナンス期間など、アップグレードプロセスに関するその他の重要な情報へのリンクについては、「アップグレード手順 （43 ページ）」を参照してください。

イベントデータと設定データのバックアップ

サポートされている場合は、アップグレードの前後にバックアップすることをお勧めします。

- アップグレード前：アップグレードが致命的なレベルで失敗した場合は、再イメージ化と復元が必要になることがあります。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。

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必要があります。アップグレードによって、ローカルに保存されたバックアップは消去されます。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。

バックアップの最初のステップとして、アプライアンスモデルとバージョンを、パッチレベルを含めて書き留めておいてください。 FMC の場合は、VDB のバージョンを書き留めておきます。 Firepower 4100/9300 シャーシの場合は、FXOS のバージョンを書き留めておきます。. 新しいアプライアンスや再イメージ化したアプライアンスにバックアップを復元する必要がある場合は、新しいアプライアンスを最初に更新する必要がある場合があるため、これは重要です。

（注） 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、セキュリティ上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。

NTP 同期の確認

アップグレードする前に、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。

帯域幅の確認

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る可能性があります。アップグレードする前に、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。詳細については、『Guidelines for Downloading Data from the Firepower Management Center to Managed Devices』（トラブルシューティングのテクニカルノート）を参照してください。

アプライアンスアクセス

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。Firepower Management Center 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。

署名付きのアップグレードパッケージ

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、署名付き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。

ASA FirePOWER デバイスでの ASA REST API の無効化

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`。

シスコとのデータの共有

一部の機能にシスコとのデータ共有が含まれます。

6.2.3+ では、*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。アップグレード中に、参加を承諾するか、辞退するかを尋ねられます。また、いつでもオプトインまたはオプトアウトできます。

バージョン 6.2.3+ では、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。現在の設定でオプトアウトが選択されている場合でも、メジャーアップグレードによって Web 分析トラッキングが有効になります。このデータの収集を拒否する場合は、各メジャーアップグレードの後にオプトアウトしてください。

6.5.0+ では、*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。アップグレード中に、参加を承諾するか、辞退するかを尋ねられます。また、いつでもオプトインまたはオプトアウトできます。

アップグレードにより侵入ルールをインポートして自動的に有効化できます。

現在の Firepower バージョンでサポートされていないキーワードが新しい侵入ルールで使用されている場合、侵入ルールデータベース（SRU）を更新しても、そのルールはインポートされません。

Firepower ソフトウェアをアップグレードし、これらのキーワードがサポートされると、新しい侵入ルールがインポートされ、IPS の設定に応じて自動的に有効化できるため、イベントの生成とトラフィックフローへの影響を開始できます。

サポートされているキーワードは、Firepower ソフトウェアに含まれている Snort のバージョンによって異なります。

- FMC：[ヘルプ（Help）] > [About（バージョン情報）] を選択します。
- FDM を使用した FTD：**show summary** CLI コマンドを使用します。
- ASDM を使用した ASA FirePOWER：[ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [システム情報（System Information）] を選択します。

また、『Cisco Firepower Compatibility Guide』の「*Bundled Components*」の項で Snort バージョンを確認することもできます。

Snort リリースノートには、新しいキーワードの詳細が含まれています。https://www.snort.org/downloads でSnort ダウンロードページのリリースノートを参照できます。

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。

アップグレードする最小バージョン

いくつかの以前のメジャー バージョン シーケンスからバージョン 6.5.0 に直接アップグレードできます。アップグレードするために、以前のバージョンの最新のパッチを実行する必要はありません。

表 *18 : Firepower* ソフトウェアをバージョン *6.5.0* にアップグレードするための最小バージョン

プラットフォーム	最小バージョン
Firepower Management Center Firepower 4100/9300 シリーズを除く、FMC 展開のすべての管理対象デバイス。	6.2.3

プラットフォーム	最小バージョン
FMC を使用した Firepower 4100/9300 上の Firepower Threat Defense	FXOS 2.7.1.92+ を搭載した 6.2.3
FDM を使用した Firepower Threat Defense（すべてのプラットフォーム）	6.2.3
ASDM を使用した ASA FirePOWER	6.2.3

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 6.5.0 の時間とディスク容量

表 *19 :* バージョン *6.5.0* の時間とディスク容量

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	時間
FMC	18.6 GB	24 MB	—	47 分
FMCv：VMware 6.0	18.7 GB	30 MB	—	35 分
Firepower 1000 シリーズ	1 GB	11.3 GB	1.1 GB	10 分
Firepower 2100 シリーズ	1.1 GB	12.3 GB	1 GB	12 分
Firepower 4100 シリーズ	20 MB	10.8 GB	990 MB	8 分
Firepower 9300	23 MB	10.9 GB	990 MB	8 分
ASA 5500-X シリーズ with FTD	10.4 GB	120 KB	1.1 GB	17 分
FTDv：VMware 6.0	10 GB	120 KB	1.1 GB	10 分
ASA FirePOWER	12.2 GB	26 MB	1.3 GB	81 分
NGIPSv：VMware 6.0	6.6 GB	22 MB	870 MB	9 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 Chassis

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 Chassis：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 *20 : FXOS* アップグレード中のトラフィックの動作

展開	方法	トラフィックの動作
スタンドアロン	—	ドロップされる
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）	Fail-to-wire 有効：[バイパス：スタンバイ（Bypass: Standby）] または [バイパス：強制（Bypass-Force）]（6.1 以降）	インスペクションなしで転送
	Fail-to-wire 無効：[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
	fail-to-wire 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

インターフェイスの設定により、アップグレード中にスタンドアロン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 *21 : 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

インターフェイスの設定		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。	ドロップされる
IPS のみのインターフェイス	インラインセット、fail-to-wire が有効：[バイパス：スタンバイ（Bypass: Standby）] または [バイパス：強制（Bypass-Force）]（6.1 以降）	次のいずれかを行います。 • ドロップ（6.1 から 6.2.2.x） • インスペクションなしで転送（6.2.3 以降）
	インラインセット、fail-to-wire が無効：[バイパス：無効（Bypass: Disabled）]（6.1 以降）	ドロップされる
	インラインセット、fail-to-wire モジュールなし	ドロップされる
	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

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。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。

スレーブ セキュリティ モジュールを最初にアップグレードして、その後マスター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。

マスター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。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、デバイスがトラフィックを処理する方法に応じて異なります。

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 Configuration Guide』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 *22 : FTD* 展開時のトラフィックの動作

インターフェイスの設定		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。	ドロップされる

インターフェイスの設定		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、[フェールセーフ（Failsafe）] が有効または無効（6.0.1 ～ 6.1.0.x）	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。
	インラインセット、[Snort フェールオープン：ダウン（Snort Fail Open: Down）]：無効（6.2 以降）	ドロップされる
	インラインセット、[Snort フェールオープン：ダウン（Snort Fail Open: Down）]：有効（6.2+）	インスペクションなしで転送
	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

インターフェイスの設定により、アップグレード中にスタンドアロン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 *23 : 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

インターフェイスの設定		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。	ドロップされる

インターフェイスの設定		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、fail-to-wire が有効：[バイパス：スタンバイ（Bypass: Standby）] または [バイパス：強制（Bypass-Force）]（6.1 以降）	次のいずれかを行います。 • ドロップ（6.1 から 6.2.2.x） • インスペクションなしで転送（6.2.3 以降）
	インラインセット、fail-to-wire が無効：[バイパス：無効（Bypass: Disabled）]（6.1 以降）	ドロップされる
	インラインセット、fail-to-wire モジュールなし	ドロップされる
	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

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 Configuration Guide』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 *24 : FTD* 展開時のトラフィックの動作

インターフェイスの設定		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。	ドロップされる
IPS のみのインターフェイス	インラインセット、[フェールセーフ（Failsafe）]が有効または無効（6.0.1 ～ 6.1.0.x）	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。
	インラインセット、[Snortフェールオープン：ダウン（Snort Fail Open: Down）]：無効（6.2 以降）	ドロップされる
	インラインセット、[Snortフェールオープン：ダウン（Snort Fail Open: Down）]：有効（6.2+）	インスペクションなしで転送
	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

Snort プロセスを再起動する特定の設定を展開する場合を含め、モジュールが FirePOWER ソフトウェア アップグレード中にトラフィックを処理する方法を決定する、ASA FirePOWER module へのトラフィック リダイレクトに関する ASA サービス ポリシーです。

表 *25 : 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 リダイレクト 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 プロセスが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 Configuration Guide』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 *26 : NGIPSv* アップグレード中のトラフィックの動作

インターフェイスの設定	トラフィックの動作
インライン	ドロップされる
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
パッシブ	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 Configuration Guide』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 *27 : NGIPSv* 展開時のトラフィックの動作

インターフェイスの設定	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
パッシブ	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、次のいずれかを参照してください。

- Cisco Firepower Management Center Upgrade Guide：管理対象デバイスや付随するオペレーティング システムを含む、FMC 展開のアップグレード
- Cisco ASA Upgrade Guide：ASDM を使用した ASA FirePOWER moduleのアップグレード
- Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager：FDM を使用した FTD のアップグレード

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

署名付きの（.tar）パッケージは解凍しないでください。

表 *28 :* のアップグレード パッケージ バージョン *6.5.0*

プラットフォーム	パッケージ
FMC/FMCv	Cisco_Firepower_Mgmt_Center_Upgrade-*version-build*.sh.REL.tar
Firepower 1000 シリーズ	Cisco_FTD_SSP_FP1K_Upgrade-*version-build*.sh.REL.tar
Firepower 2100 シリーズ	Cisco_FTD_SSP_FP2K_Upgrade-*version-build*.sh.REL.tar
Firepower 4100/9300 シャーシ	Cisco_FTD_SSP_Upgrade-*version-build*.sh.REL.tar
FTD を搭載した ASA 5500-X シリーズ FTD を搭載した ISA 3000 Firepower Threat Defense 仮想	Cisco_FTD_Upgrade-*version-build*.sh.REL.tar
ASA FirePOWER	Cisco_Network_Sensor_Upgrade-*version-build*.sh.REL.tar
NGIPSv	Cisco_Firepower_NGIPS_Virtual_Upgrade-*version-build*.sh.REL.tar