アップグレードガイドライン

このドキュメントには、バージョン 7.4 の重要なリリース固有のアップグレードガイドラインが記載されていますが、

アップグレードの計画

誤りを避けるには、注意深い計画と準備が役立ちます。この表はアップグレードの計画プロセスを要約したものです。詳細なチェックリストと手順については、該当するアップグレードガイドとコンフィギュレーション ガイド（http://www.cisco.com/go/threatdefense-74-docs）を参照してください。

表 *1:* アップグレードの計画フェーズ

計画フェーズ	次を含む
計画と実現可能性	展開を評価します。 アップグレードパスを計画します。 すべてのアップグレードガイドラインを読み、設定の変更を計画します。 アプライアンスへのアクセスを確認します。 帯域幅を確認します。 メンテナンス時間帯をスケジュールします。
バックアップ	設定およびイベントをバックアップします。 Firepower 4100/9300 および の FXOS をバックアップします。
アップグレードパッケージ	アップグレードパッケージをシスコからダウンロードします。 システムにアップグレードパッケージをアップロードします。
関連するアップグレード	仮想展開内で仮想ホスティングをアップグレードします。 Firepower 4100/9300 のファームウェアをアップグレードします。 Firepower 4100/9300 および の FXOS をアップグレードします。
最終チェック	設定を確認します。 NTP 同期を確認します。 Management Center で変更管理ワークフローを確認します。 設定を展開します。 準備状況チェックを実行します。 ディスク容量を確認します。 実行中のタスクを確認します。 展開の正常性と通信を確認します。

アップグレードする最小バージョン

アップグレードする最小バージョン

次のように、メンテナンスリリースを含むバージョン 7.4 に直接アップグレードできます。

表 *2 :* バージョン *7.4* 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
Management Center	7.0
脅威防御 （GCP 対応 Threat Defense Virtual を除く）	7.0 Firepower 4100/9300 には FXOS 2.14.1.131 が必要です。ほとんどの場合、各メジャーバージョンで最新の FXOS ビルドを使用することを推奨します。判断のヒントについては、Cisco Firepower 4100/9300 FXOS 2.14 リリースノート を参照してください。
GCP 向け Threat Defense Virtual	7.2 バージョン 7.1 以前からバージョン 7.2 以降にアップグレードすることはできないため、新しいインスタンスを展開する必要があります。

バージョン 7.4 のアップグレードガイドライン

以下のチェックリストでは、該当する可能性のある新規アップグレードガイドラインや以前に公開されたアップグレードガイドラインを提供します。

表 *3 : Management Center* を使用した *Threat Defense* のアップグレードガイドラインバージョン *7.4*

✓	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
常にチェック				
	アップグレードする最小バージョン （3 ページ）	いずれか	いずれか	いずれか

✓	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
	Cisco Secure Firewall Management Center の新機能（リリース別）：アップグレードに影響を与える新機能および廃止された機能が記載されています。現在のバージョンと対象バージョンの間にあるすべてのバージョンを確認してください。	いずれか	いずれか	いずれか
	未解決のバグおよび解決されたバグ：アップグレードに影響を与えるバグが記載されています。現在のバージョンと対象バージョン間にあるすべてのバージョンのリリースノートを確認してください。	いずれか	いずれか	いずれか
	クラウド提供型 Firewall Management Center のアップグレードガイドライン （6 ページ）	Threat Defense	いずれか	いずれか
	Firepower 4100/9300 シャーシのアップグレードガイドライン （6 ページ）	Firepower 4100/9300 Secure Firewall 3100/4200	いずれか	いずれか
特定の展開に対するその他のガイドライン				
	大規模構成向けの拡張された、バージョン 7.4.0 へのアップグレード後の展開 （5 ページ）	Management Center	6.6.0 +	7.4.0 のみ

表 *4 : Device Manager* を使用した *Threat Defense* のアップグレードガイドラインバージョン *7.4*

✓	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
常にチェック				
	アップグレードする最小バージョン （3 ページ）	いずれか	いずれか	いずれか

✓	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
	Cisco Secure Firewall デバイスマネージャの新機能（リリース別）：アップグレードに影響を与える新機能および廃止された機能が記載されています。現在のバージョンと対象バージョンの間にあるすべてのバージョンを確認してください。	いずれか	いずれか	いずれか
	未解決のバグおよび解決されたバグ：アップグレードに影響を与えるバグが記載されています。現在のバージョンと対象バージョン間にあるすべてのバージョンのリリースノートを確認してください。	いずれか	いずれか	いずれか
	Firepower 4100/9300 シャーシのアップグレードガイドライン （6 ページ）	Firepower 4100/9300	いずれか	いずれか

特定の展開に対するその他のガイドライン
このリリースに固有の Device Manager に関する追加のアップグレードガイドラインはありません。

大規模構成向けの拡張された、バージョン7.4.0へのアップグレード後の展開

展開：Management Center

アップグレード元：オブジェクト最適化が無効になっている展開。

直接アップグレード先：バージョン 7.4.0 のみ

アクセス コントロール オブジェクトの最適化により、ネットワークが重複するアクセス コントロール ルールがある場合、パフォーマンスが向上し、デバイスリソースの消費が少なくなります。最適化は、Management Center で機能が有効になった後の最初の展開時に管理対象デバイスで行われます（アップグレードで有効になった場合も含む）。ルールの数が多い場合、システムがポリシーを評価してオブジェクトの最適化を実行するのに数分から 1 時間かかることがあります。この間、デバイスの CPU 使用率も高くなることがあります。機能が無効になった後の最初の展開でも同様のことが発生します（アップグレードによって無効になった場合も含む）。この機能が有効または無効になった後は、メンテナンス時間帯やトラフィックの少ない時間帯など、影響が最小限になる時間に展開することを強く推奨します。

計画するには、次の表を使用します。

表 *5*: オブジェクト最適化を使用した *Management Center* のアップグレードの計画

バージョン（Version）	デフォルト/設定の再イメージ	Upgrading	有効化/無効化
7.0.5 以前	サポートされていません（無効）。	—	—
7.0.6 以降のメンテナンスリリース	ディセーブル。	現在の設定が保持されます。	Cisco TAC にお問い合わせください。
7.1.0 ～ 7.2.3	サポートされていません（無効）。	無効。	—
7.2.4 ～ 7.2.5	イネーブル。	有効。	Cisco TAC にお問い合わせください。
7.3.x	サポートされていません（無効）。	無効。	—
7.4.0	イネーブル。	有効。	Cisco TAC にお問い合わせください。
7.4.1 以降	イネーブル。	現在の設定が保持されます。	ユーザー設定可能。

クラウド提供型 Firewall Management Center のアップグレードガイドライン

クラウド提供型 Firewall Management Center はアップグレード対象外です。機能の更新はシスコが行います。クラウド提供型 Firewall Management Center を使用して Threat Defense をアップグレードするには、クラウド提供型 Firewall Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイドを参照してください。

Firepower 4100/9300 シャーシのアップグレードガイドライン

Firepower 4100/9300 の場合、Threat Defense のメジャーアップグレードにはシャーシのアップグレード（FXOS とファームウェア）も必要です。メンテナンスリリースとパッチでアップグレードが必要になることはほとんどありませんが、最新のビルドにアップグレードして、解決済みの問題を活用することもできます。

表 *6 : Firepower 4100/9300* シャーシのアップグレードガイドライン

ガイドライン	詳細
FXOS のアップグレード。	Firepower 4100/9300 で Threat Defense バージョン 7.4 を実行するには、FXOS 2.14.1.131 以降が必要です。 FXOS 2.2.2 から、それ以降の任意の FXOS バージョンにアップグレードできます。重要なリリース固有のアップグレードガイドライン、新機能および廃止された機能、未解決のバグおよび解決済みのバグについては、Cisco Firepower 4100/9300 FXOS リリースノート を参照してください。
ファームウェアのアップグレード。	FXOS 2.14.1 以降のアップグレードにはファームウェアが含まれます。以前の FXOS バージョンにアップグレードする場合は、Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guideを参照してください。
アップグレードの時間。	シャーシのアップグレードには最長 45 分かかり、トラフィックフローやインスペクションに影響を与える場合があります。詳細については、シャーシのアップグレードでのトラフィックフローとインスペクション （8 ページ）を参照してください。

応答しないアップグレード

アップグレード中は、設定の変更の実施または展開を行わないでください。システムが非アクティブに見えても、アップグレード中は手動で再起動またはシャットダウンしないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。

応答しない Management Center

進行中のアップグレードは再開しないでください。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。

応答しない Threat Defense のアップグレード

メジャーアップグレードやメンテナンスアップグレードでは、失敗したアップグレードまたは進行中のアップグレードを手動でキャンセルし、失敗したアップグレードを再試行できます。

- Management Center：[デバイス管理（Device Management）] ページの [アップグレード（Upgrade）] タブ、およびメッセージセンターからアクセスできる [アップグレードステータス（Upgrade Status）] ポップアップを使用します。
- Device Manager ：[システムアップグレード（System Upgrade）] パネルを使用します。

Threat Defense CLI を使用することもできます。

（注） デフォルトでは、Threat Defense はアップグレードが失敗すると自動的にアップグレード前の状態に復元されます（「自動キャンセル」）。失敗したアップグレードを手動でキャンセルまたは再試行できるようにするには、アップグレードを開始するときに自動キャンセルオプションを無効にします。パッチの自動キャンセルはサポートされていません。高可用性または拡張性の展開では、自動キャンセルは各デバイスに個別に適用されます。つまり、1 つのデバイスでアップグレードが失敗した場合、そのデバイスだけが元に戻ります。

この機能は、パッチまたはバージョン 6.6 以前からのアップグレードではサポートされていません。

アップグレードを元に戻すまたはアンインストールする

アップグレードに成功したにもかかわらず、システムが期待どおりに機能しない場合は、復元またはアンインストールが可能な場合があります。

- マネージャにかかわらず、メジャーおよびメンテナンスアップグレードの Threat Defense への復元がサポートされています。
- Management Center を使用した Threat Defense のパッチのアンインストールがサポートされています。Management Center パッチをアンインストールすることもできます。

これが機能せず、以前のバージョンに戻す必要がある場合、イメージを再作成する必要があります。ガイドライン、制限、および手順については、現在実行しているバージョンの Management Center/デバイスマネージャのアップグレードガイドを参照してください。

トラフィック フローとインスペクション

デバイスのアップグレード（ソフトウェアおよびオペレーティングシステム）により、トラフィックフローとインスペクションが影響を受けます。影響が最も少ない時間帯にメンテナンス期間をスケジュールします。

シャーシのアップグレードでのトラフィックフローとインスペクション

FXOS をアップグレードするとシャーシが再起動します。ファームウェアのアップグレードを含むバージョン 2.14.1 以降への FXOS アップグレードの場合、デバイスは 2 回リブートします。1 回は FXOS 用、1 回はファームウェア用です。対象には、 のバージョン 7.4.1 以降のシャーシアップグレードが含まれます。

高可用性またはクラスタ展開の場合でも、各シャーシの FXOS を個別にアップグレードします。中断を最小限に抑えるには、1 つずつシャーシをアップグレードします。

表 *7:* トラフィックフローとインスペクション：*FXOS* のアップグレード

Threat Defense の導入	トラフィックの挙動	メソッド
スタンドアロン	廃棄	—
高可用性	影響なし。	**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。
	1 つのピアがオンラインになるまでドロップされる。	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。
シャーシ間クラスタ	影響なし。	**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。
	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。	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。
シャーシ内クラスタ（FirePOWER 9300 のみ）	検査なしで受け渡される。	ハードウェアバイパス有効：[Bypass: Standby] または [Bypass-Force]。
	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無効：[Bypass: Disabled]。
	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。

Management Center を使用した Threat Defense アップグレードのトラフィックフローとインスペクション

スタンドアロンデバイスでのソフトウェアのアップグレード

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。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 *8:* トラフィックフローとインスペクション：スタンドアロンデバイスでのソフトウェアのアップグレード

インターフェイス コンフィギュレーション		トラフィックの挙動
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 ISA 3000 のブリッジ グループ インターフェイスの場合に限り、FlexConfig ポリシーを使用して、停電時のハードウェアバイパスを設定できます。これにより、ソフトウェアのアップグレード中にトラフィックのドロップが発生しますが、デバイスがアップグレード後の再起動中、インスペクションなしでトラフィックが通過します。
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：[バイパス（Bypass）]：[強制（Force）]	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がスタンバイモード：[バイパス（Bypass）]：[スタンバイ（Standby）]	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：[バイパス（Bypass）]：[無効（Disabled）]	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。

高可用性および拡張性に関するソフトウェアのアップグレード

高可用性デバイスやクラスタ化されたデバイスのアップグレード中に、トラフィックフローや検査が中断されることはありません。高可用性ペアの場合、スタンバイ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。

クラスタの場合、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。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。

シングルユニットのクラスタでは、ヒットレスアップグレードはサポートされないことに注意してください。トラフィックフローと検査の中断は、スタンドアロンデバイスと同様に、アクティブユニットのインターフェイス設定に依存します。

ソフトウェアの復元（メジャーおよびメンテナンスリリース）

たとえ高可用性および拡張性を備えた環境でも、復元時のトラフィックフローとインスペクションの中断を予測する必要があります。これは、すべてのユニットを同時に復元させたほうが、復元がより正常に完了するためです。同時復元とは、すべてのデバイスがスタンドアロンであるかのように、トラフィックフローと検査の中断がインターフェイスの設定のみに依存することを意味します。

ソフトウェアのアンインストール（パッチ）

スタンドアロンデバイスの場合、パッチのアンインストール中のトラフィックフローと検査の中断は、アップグレードの場合と同じになります。高可用性および拡張性の展開では、中断を最小限に抑えるために、アンインストールの順序を明確に計画する必要があります。これは、ユニットとしてアップグレードしたデバイスであっても、デバイスから個別にパッチをアンインストールするためです。

設定変更の導入

Snort プロセスを再起動すると、高可用性/拡張性を備えた構成になっているものを含め、すべてのデバイスでトラフィックフローとインスペクションが一時的に中断されます。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。Snort を再起動せずに展開すると、リソース要求時にいくつかのパケットが検査なしでドロップされることがあります。

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。

表 *9:* トラフィックフローとインスペクション：設定変更の展開

インターフェイス コンフィギュレーション		トラフィックの挙動
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、[フェールセーフ（Failsafe）] が有効または無効。	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フェールオープン：ダウン（Snort Fail Open: Down）]：無効	廃棄
	インライン、[Snortフェールオープン：ダウン（Snort Fail Open: Down）]：有効	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。

Device Manager を使用した Threat Defense アップグレードのトラフィックフローとインスペクション

ソフトウェアのアップグレード

アップグレード中にトラフィックがドロップされます。高可用性の展開では、デバイスを1つずつアップグレードすることで、中断を最小限に抑えることができます。

ISA 3000 の場合にのみ、電源障害に対するハードウェアバイパスを設定すると、トラフィックはアップグレード中にドロップされますが、デバイスのアップグレード後の再起動中に検査なしでトラフィックが渡されます。

ソフトウェアの復元（メジャーおよびメンテナンスリリース）

復元中にトラフィックがドロップされます。高可用性の展開では、両方のユニットを同時に復元すると、復元が成功する可能性が高くなります。最初のユニットがオンラインに戻ると、トラフィックフローとインスペクションが再開されます。

設定変更の導入

Snort プロセスを再起動すると、高可用性を備えた構成になっているものを含め、すべてのデバイスでトラフィックフローとインスペクションが一時的に中断されます。Snort を再起動せずに展開すると、リソース要求時にいくつかのパケットが検査なしでドロップされることがあります。

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。

時間とディスク容量

アップグレードまでの時間

将来のベンチマークとして使用できるように、独自のアップグレード時間を追跡および記録することをお勧めします。次の表に、アップグレード時間に影響を与える可能性のあるいくつかの事項を示します。

注意 アップグレード中は、設定を変更または展開しないでください。システムが非アクティブに見えても、手動で再起動またはシャットダウンしないでください。ほとんどの場合、進行中のアップグレードを再開しないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。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 応答しないアップグレード （7 ページ） を参照してください。

表 *10*：アップグレード時間の考慮事項

考慮事項	詳細（Details）
バージョン	アップグレードでバージョンがスキップされると、通常、アップグレード時間は長くなります。
モデル	通常、ローエンドモデルではアップグレード時間が長くなります。
仮想アプライアンス	仮想展開でのアップグレード時間はハードウェアに大きく依存します。

考慮事項	詳細（**Details**）
高可用性とクラスタリング	高可用性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。
設定	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、それらがアップグレードから影響を受けるかどうか、どのような影響を受けるかによって長くなります。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、アップグレードではそ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、さらに長い時間がかかります。
コンポーネント	オペレーティングシステムまたは仮想ホスティングのアップグレード、アップグレードパッケージの転送、準備状況チェック、VDB と侵入ルール（SRU/LSP）の更新、設定の展開、およびその他の関連タスクを実行するために、追加の時間が必要になる場合があります。

アップグレードするディスク容量

準備状況チェックでは、アップグレードを実行するのに十分なディスク容量があるかどうかが示されます。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。

表 *11*：ディスク容量の確認

プラットフォーム	コマンド
Management Center	**システム**（⚙）>**[モニタリング（Monitoring）]**>**[統計（Statistics）]** を選択し、Management Center を選択します。[ディスク使用率（Disk Usage）] で、[By Partition] の詳細を展開します。
Threat Defense with Management Center	**システム**（⚙）>**[モニタリング（Monitoring）]**>**[統計（Statistics）]** を選択し、確認するデバイスを選択します。[ディスク使用率（Disk Usage）] で、[By Partition] の詳細を展開します。
Threat Defense with Device Manager	**show disk** CLI コマンドを使用します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。