Management Center のアップグレード

Management Center のアップグレード：スタンドアロン

この手順を使用して、スタンドアロンの Management Center をアップグレードします。

続行すると、Management Center のアップグレードウィザードに、アップグレードに関する基本情報と、現在のアップグレード関連のステータスが表示されます。表示内容には、アップグレードできない理由が含まれます。ウィザードから移動しても進行状況は保持され、他のユーザーは新しいアップグレードワークフローを開始できません（例外：CAC でログインしている場合、ログアウトしてから 24 時間後に進行状況がクリアされます）。ワークフローに戻るには、**システム**（⚙） > **[Product Upgrades]** を選択し、Management Center のシステム概要で [再開（Resume）] をクリックします。

Management Center のアップグレードは、ウィザードを完了して [アップグレード（Upgrade）] をクリックするまで開始されません。アップグレードパッケージのダウンロードや準備状況チェックの実行など、その時点までのすべての手順は、メンテナンスウィンドウ外で実行できます。アップグレード後の最初の展開時におけるトラフィック処理については、設定展開時のトラフィックフローとインスペクションを参照してください。古い ASA FirePOWER または NGIPSv デバイスを管理している場合、トラフィック処理については、Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0を参照ください。

⚠

注意 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、進行中のアップグレードを手動で再起動、シャットダウン、または再起動しないでください。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 Cisco TAC にお問い合わせください。

始める前に

アップグレードの準備が整っていることを確認します。

- ターゲットバージョンを実行できるかどうかを確認します：互換性
- アップグレードパスを計画します：アップグレードパス
- アップグレードのガイドラインを確認します：アップグレードのガイドライン
- インフラストラクチャとネットワークを確認します：インフラストラクチャとネットワークの確認
- 設定、タスク、および展開全体の正常性を確認します：設定と展開の確認
- バックアップを実行します：バックアップ

ステップ 1 Management Center で、**システム**（⚙）> **[Product Upgrades]** を選択します。

ステップ 2 アップグレードパッケージを取得します。

[製品のアップグレード（Product Upgrades）]ページには、現在の展開に適用されるすべてのアップグレードパッケージが、特にマークされた推奨リリースとともに一覧表示されます。ほとんどの場合、必要なアップグレードパッケージまたはバージョンの横にある [ダウンロード（Download）] をクリックするだけで取得できます。

詳細については、Management Center へのアップグレードパッケージのアップロードとダウンロードおよびアップグレードパッケージのトラブルシューティングを参照してください。

ステップ 3 アップグレードウィザードを起動します。

ターゲットバージョンの横にある [アップグレード（Upgrade）] をクリックします。ドロップダウンメニューが表示されたら、[Management Center] を選択します。

Management Center のアップグレードウィザードが表示されます。互換性やその他のクイック事前チェックは自動的に実行されます。たとえば、設定を展開する必要がある場合、すぐにアラートが表示されます。

ステップ 4 [次へ（Next）] をクリックして準備状況チェックを実行します。

[準備状況チェックの実行（Run Readiness Checks）] をクリックします。準備状況チェックの実行中は、手動で再起動またはシャットダウンしないでください。Management Center の場合、準備状況チェックに合格することは必須です。準備状況チェックで不合格になるとアップグレードできません。

ステップ 5 [次へ（Next）] をクリックし、アップグレードの準備ができていることを再確認します。

以前に実行した設定と展開の正常性チェックを再確認することをお勧めします（設定と展開の確認）。

ステップ 6 [アップグレード（Upgrade）] をクリックし、アップグレードして再起動することを確認します。

ログアウトするまで、メッセージセンターで事前チェックの進行状況をモニターできます。

ステップ 7 可能なときに、 に再度ログインします。

- メジャーアップグレードとメンテナンスアップグレード：アップグレードが完了する前にログインできます。アップグレードの進行状況をモニターし、アップグレードログとエラーメッセージを確認するために使用できるページが表示されます。アップグレードが完了し、システムが再起動すると再度ログアウトされます。リブート後に、再ログインしてください。
- パッチとホットフィックス：アップグレードと再起動が完了した後にログインできます。

ステップ 8 アップグレードが成功したことを確認します。

ログイン時にアップグレードの成功メッセージが表示されない場合は、**[ヘルプ（Help）]**（?）>**[バージョン情報（About）]** を選択して、現在のソフトウェアのバージョン情報を表示します。

ステップ 9 侵入ルール（SRU/LSP）および脆弱性データベース（VDB）を更新します。

シスコサポートおよびダウンロードサイトで利用可能なコンポーネントが現在実行中のバージョンより新しい場合は、新しいバージョンをインストールします。侵入ルールを更新する場合、ポリシーを自動的に再適用する必要はありません。後で適用します。

ステップ 10 アップグレード後に必要な構成変更があれば、実行します。

ステップ 11 管理対象デバイスに構成を再展開します。

Management Center のアップグレード：ハイアベイラビリティ

高可用性 Management Center を一度に 1 つずつアップグレードするには、この手順を使用します。ワークフローもアップグレードパッケージも、高可用性 Management Center 間で同期されません。

同期を一時停止して、スタンバイをアップグレードします。アップグレードが完了すると、Management Center がアクティブに戻って稼働し、他の Management Center をアップグレードできるようになります。この一時的なアクティブ-アクティブ状態のことを「スプリットブレイン」と呼び、アップグレード中（およびパッチのアンインストール中）を除き、サポートされていません。 ペアが split-brain の状況で、構成の変更または展開を行わないでください。同期の再開後は変更内容が失われます。

続行すると、Management Center のアップグレードウィザードに、アップグレードに関する基本情報と、現在のアップグレード関連のステータスが表示されます。表示内容には、アップグレードできない理由が含まれます。ウィザードから移動しても進行状況は保持され、他のユーザーは新しいアップグレードワークフローを開始できません（例外：CAC でログインしている場合、ログアウトしてから 24 時間後に進行状況がクリアされます）。ワークフローに戻るには、**システム**（⚙）>**[Product Upgrades]** を選択し、Management Center のシステム概要で [再開（Resume）] をクリックします。

Management Center のアップグレードは、ウィザードを完了し、同期を一時停止して、[アップグレード（Upgrade）] をクリックするまで開始されません。アップグレードパッケージのダウ

ンロードや準備状況チェックの実行など、その時点までのすべての手順は、メンテナンスウィンドウ外で実行できます。アップグレード後の最初の展開時におけるトラフィック処理については、設定展開時のトラフィックフローとインスペクションを参照してください。古い ASA FirePOWER または NGIPSv デバイスを管理している場合、トラフィック処理については、Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0を参照ください。

（注） ホットフィックス リリース ノートに特に記載されていない、または Cisco TAC から指示されていない限り、高可用性 Management Center にホットフィックスをインストールするために同期を一時停止する必要はありません。

注意 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、進行中のアップグレードを手動で再起動、シャットダウン、または再起動しないでください。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 Cisco TAC にお問い合わせください。

始める前に

アップグレードの準備が整っていることを確認します。

- ターゲットバージョンを実行できるかどうかを確認します：互換性
- アップグレードパスを計画します：アップグレードパス
- アップグレードのガイドラインを確認します：アップグレードのガイドライン
- インフラストラクチャとネットワークを確認します：インフラストラクチャとネットワークの確認
- 設定、タスク、および展開全体の正常性を確認します：設定と展開の確認
- バックアップを実行します：バックアップ

両方の Management Center のアップグレードを準備します。

ステップ 1 いずれかの Management Center で、**システム**（⚙）>**[Product Upgrades]** を選択します。

ステップ 2 アップグレードパッケージを取得します。

[製品のアップグレード（Product Upgrades）]ページには、現在の展開に適用されるすべてのアップグレードパッケージが、特にマークされた推奨リリースとともに一覧表示されます。ほとんどの場合、必要なアップグレードパッケージまたはバージョンの横にある [ダウンロード（Download）] をクリックするだけで取得できます。詳細については、Management Center へのアップグレードパッケージのアップロードとダウンロードおよびアップグレードパッケージのトラブルシューティングを参照してください。

これは両方の Management Center で実行する必要があります。アップグレードパッケージは同期されません。

ステップ 3 アップグレードウィザードを起動します。

ターゲットバージョンの横にある [アップグレード（Upgrade）] をクリックします。ドロップダウンメニューが表示されたら、[Management Center] を選択します。

Management Center のアップグレードウィザードが表示されます。互換性やその他のクイック事前チェックは自動的に実行されます。たとえば、設定を展開する必要がある場合、すぐにアラートが表示されます。

ステップ 4 [次へ（Next）] をクリックして準備状況チェックを実行します。

[準備状況チェックの実行（Run Readiness Checks）] をクリックします。準備状況チェックの実行中は、手動で再起動またはシャットダウンしないでください。Management Center の場合、準備状況チェックに合格することは必須です。準備状況チェックで不合格になるとアップグレードできません。

ステップ 5 [次へ（Next）] をクリックし、アップグレードの準備ができていることを再確認します。

以前に実行した設定と展開の正常性チェックを再確認することをお勧めします（設定と展開の確認）。

ステップ 6 他の Management Center について、手順 1 ～ 5 を繰り返します。

同期を一時停止します。

ステップ 7 アクティブ状態の Managagement Center で、同期を一時停止します。

アクティブから一時停止した場合は、どちらからでも再開できます。スタンバイから一時停止した場合は、スタンバイから再開する必要があります。

a) **[統合（Integration）] > [その他の統合（Other Integrations）]** を選択します。
b) [ハイ アベイラビリティ（High Availability）] タブで、[同期の一時停止（Pause Synchronization）] をクリックします。

スタンバイをアップグレードしてから、アクティブをアップグレードします。

ステップ 8 スタンバイ状態の Managagement Center で、[アップグレード（Upgrade）] をクリックし、アップグレードして再起動することを確認します。

ログアウトするまで、メッセージセンターで事前チェックの進行状況をモニターできます。

ステップ 9 可能なときに、 に再度ログインします。

- メジャーアップグレードとメンテナンスアップグレード：アップグレードが完了する前にログインできます。アップグレードの進行状況をモニターし、アップグレードログとエラーメッセージを確認するために使用できるページが表示されます。アップグレードが完了し、システムが再起動すると再度ログアウトされます。リブート後に、再ログインしてください。
- パッチとホットフィックス：アップグレードと再起動が完了した後にログインできます。

ステップ 10 アップグレードが成功したことを確認します。

ログイン時にアップグレードの成功メッセージが表示されない場合は、**[ヘルプ（Help）]**（?）**> [バージョン情報（About）]** を選択して、現在のソフトウェアのバージョン情報を表示します。

ステップ 11 他の Management Center について、手順 8 ～ 10 を繰り返します。

同期を再開し、アップグレード後のタスクを完了します。

ステップ 12 引き続き、古いアクティブ状態の Managagement Center（アップグレードしたばかりの Managagement Center）で、同期を再開します。

a) **[統合（Integration）]** > **[その他の統合（Other Integrations）]** を選択します。

b) [ハイ アベイラビリティ（High Availability）] タブで、[同期の再開（Resume Synchronization）] をクリックします。

ステップ 13 侵入ルール（SRU/LSP）および脆弱性データベース（VDB）を更新します。

シスコ サポートおよびダウンロード サイトで利用可能なコンポーネントが現在実行中のバージョンより新しい場合は、新しいバージョンをインストールします。侵入ルールを更新する場合、ポリシーを自動的に再適用する必要はありません。後で適用します。

ステップ 14 アップグレード後に必要な構成変更があれば、実行します。

ステップ 15 管理対象デバイスに構成を再展開します。

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。