Cisco HX Data Platform リリース 3.5 のリリース ノート

初版：2018 年 10 月 16 日

最終更新：2020 年 8 月 11 日

はじめに

Cisco HyperFlex システムは、ハイパーコンバージド システムのデザインが持つ力を最大限に活用できます。ソフトウェア デファインド インフラをベースとするこのシステムでは、Cisco Unified Computing System（Cisco UCS）サーバによるソフトウェア デファインドのコンピューティング、強力な Cisco HX Data Platform を利用したソフトウェア デファインド ストレージ、Cisco UCS ファブリックによるソフトウェア デファインドネットワーキングが一元化されています。こうしたテクノロジーにより接続とハードウェア管理を一元化することで、統合されたリソース プールをビジネス ニーズに合わせて提供できる、適応性の高い統合クラスタが実現します。

これらのリリース ノートは、Cisco HX Data Platform リリース 3.5 に関連しており、Cisco HX Data Platform の機能、制限事項、および問題について説明しています。

マニュアルの変更履歴

リリース	日付	説明
3.5 (2h)	2020 年 8 月 11 日	• M4/M5 認定 FI /サーバ ファームウェアの列を追加。HX 3.5 (2h) 認定済みとして USCM 4.1 (2a) を一覧表示。 • HX 3.5(2h)、3.5(2g)、3.5(2f)、3.5(2e)、3.5(2d)、3.5(2c)、3.5(2b)、3.5(2a)、3.5(1a) の未解決の警告の一覧に CSCvv21905 を追加。

リリース	日付	説明
3.5 (2g)	2020 年 7 月 23 日	HyperFlex ソフトウェアのバージョン。Cisco UCS Manager 4.0 (4i) および4.1 (1d) の認定の追加。
3.5 (2h)	2020 年 7 月 16 日	HX 3.5 (2h)、HX 3.5 (2g)、HX 3.5 (2f)、および HX 3.5 (2e) の解決済みの警告を追加。
3.5(1a)	2020 年 5 月 15 日	HX 3.5(1a) - サポート終了
3.5 (2h)	2020 年 5 月 4 日	• M5 向けのホスト アップグレード ユーティリティ (HUU) を、HX 3.5(2h) に合わせて UCS 4.0(4k) にアップデートしました。 • HX REST API アクセス トークン管理についての説明を、「注意事項と制約事項」のセクションに追加しました。
3.5 (2h)	2020 年 3 月 30 日	M4 および M5 推奨 FI/サーバ ファームウェアを、HX 3.5(2g) に合わせて UCS 4.0(4h) にアップデートしました。
3.5 (2h)	2020 年 3 月 24 日	M4 および M5 推奨 FI/サーバ ファームウェアを、HX 3.5(2h) に合わせて UCS 4.0(4h) にアップデートしました。HX 3.5(1a) をサポート対象外に指定しました。HX 3.5(2b) の未解決の問題リストに CSCvs08218 を追加しました。
3.5 (2h)	2020 年 3 月 5 日	HyperFlex バージョン 3.0(1x) および 3.5(1x) のアップグレードのリマインダを追加しました。これらのバージョンはサポート終了であると告知され、サポート対象外となったためです。HX 3.0 の要件に対する参照を削除しました。

リリース	日付	説明
3.5 (2h)	2020 年 1 月 28 日	HX 3.5(2h) の解決済みの問題の一覧に CSCvs47419 を追加しました。
3.5 (2h)	2020 年 1 月 21 日	Cisco HX Data Platform ソフトウェア リリース 3.5(2h) のリリース ノートを作成しました。
3.5 (2c)	2020 年 1 月 14 日	延期されている Cisco HyperFlex リリース HX 3.5(2c) のリリース ノートを更新しました。
3.5 (2g)	2020 年 1 月 10 日	HX 3.5(2g) の未解決の警告の一覧に CSCvs35307 を追加しました。
3.5 (2g)	2019 年 12 月 23 日	HX 3.5(2f)、3.5(2e)、3.5(2d) の場合、M4 および M5 推奨 FI/サーバ ファームウェアを UCS 4.0(4e) に更新しました。
3.5 (2g)	2019 年 12 月 13 日	HX 3.5(2g)、3.5(2f)、3.5(2e) の解決済み警告のリストに CSCvs28167 を追加しました。HX 3.5(2d)、3.5(2c)、3.5(2b)、3.5(2a)、3.5(1a) の未解決の警告の一覧に CSCvs28167 を追加しました。
3.5 (2g)	2019 年 11 月 25 日	未解決の問題リストに CSCvs02466 が追加されました。
3.5 (2g)	2019 年 11 月 19 日	「アップグレード ガイドライン」の項の情報が更新されました。
3.5 (2g)	2019 年 11 月 7 日	3.x 展開セクションの HyperFlex Edge およびファームウェア互換性マトリックスを更新しました。

リリース	日付	説明
3.5 (2g)	2019 年 10 月 25 日	セキュリティ修正の一覧に CSCvj95606 および CSCvq24176 を追加しました。
3.5 (2g)	2019 年 10 月 21 日	Cisco HX Data Platform ソフトウェア リリース 3.5(2g) のリリース ノートを作成しました。
3.5 (2f)	2019 年 9 月 17 日	「関連する問題」の新しいセクションに CSCvq41985 が追加されました。
3.5 (2f)	2019 年 9 月 10 日	3.x 展開向け HyperFlex Edge およびファームウェア互換性マトリックスの HUU/CIMC 情報を更新しました。
3.5 (2f)	2019 年 9 月 6 日	Cisco HX Data Platform ソフトウェア リリース 3.5(2f) のリリース ノートを作成しました。
3.5 (2f)	2019 年 9 月 6 日	HyperFlex リリース 3.5 (2e) および 3.5 (2d) の HUU/CIMC 推奨ファームウェア バージョンが更新されました。
3.5(2e)	2019 年 8 月 23 日	HyperFlex リリース 3.5 (2e) および 3.5 (2d) の推奨 FI/サーバ ファームウェア バージョンが更新されました。
3.5(2e)	2019 年 8 月 21 日	3.x 展開向け HyperFlex Edge およびファームウェア互換性マトリックスに、Cisco IMC バージョン サポート情報が追加されました。
3.5(2e)	2019 年 8 月 8 日	「アップグレード ガイドライン」セクションの「サポートされていない Cisco HX リリースの Cisco HyperFlex システム アップグレード ガイド」を説明する箇条書きを追加しました。

リリース	日付	説明
3.5(2e)	2019 年 8 月 2 日	HyperFlex が UCS server ファームウェア 4.0 (4a)、4.0 (4b)、および 4.0 (4c) をサポートしていないことを説明した重要な注意事項が追加されました。
3.5(2e)	2019 年 7 月 22 日	Cisco HX Data Platform ソフトウェア リリース 3.5(2e) のリリース ノートを作成しました。
3.5 (2d)	2019 年 7 月 15 日	• 「サポートされているバージョンとシステム要件」セクションで、SED ベース HyperFlex システムの UCS Manager の相互運用性が更新されました。 • 「サポートされている VMware vSphere バージョンおよびエディション」の ESXi 6.7 U2 のリリース 3.5 (2b) サポートが更新されました。
3.5(2d)	2019 年 6 月	HyperFlex Edge およびファームウェアの互換性の表を追加しました。
3.5 (2d)	2019 年 6 月 19 日	• 「リリース 3.5 (2d) で解決済みの問題」リストに CSCvp40474 が追加されました。 • 「リリース 3.5 (2b) で未解決の問題」リストに記載されている CSCvp40474 の回避策に関する情報を更新しました。
3.5 (2d)	2019 年 6 月 11 日	Cisco HX Data Platform ソフトウェア リリース 3.5(2d) のリリース ノートを作成しました。

リリース	日付	説明
3.5 (2c)	2019 年 5 月 31 日	CSCvo36198 を、「リリース 3.5 (2c) の解決済みの問題」リストに移動しました。
3.5 (2c)	2019 年 5 月 29 日	• ストレッチ クラスタでリリース 3.5 (2c) を使用していないことに関する重要な注意事項が追加されました。 • 「リリース 3.5 (2c) の未解決の問題リスト」セクションに CSCvp90129 が追加されました。
3.5 (2c)	2019 年 5 月 21 日	• UCS/UCSM のインストールの問題 CSCvo13678 を説明するメモを追加しました。 • 「リリース 3.5 (2c) の解決済みの問題」セクションに関して、CSCvo75522 のストレッチ クラスタ ガイドへの参照が追加されました。 • 「アップグレードのガイドライン」セクションの Hypercheck TechNote の記事へのリンクが更新されました。 • 「リリース 3.5 (2b) で未解決の問題の CSCvo7」セクション CSCvo70723 が更新されました。
3.5 (2c)	2019 年 5 月 20 日	Cisco HX Data Platform ソフトウェア リリース 3.5(2c) のリリース ノートを作成しました。

リリース	日付	説明
3.5 (2b)	2019 年 5 月 16 日	「リリース 3.5 (2b) で未解決の問題」リストに CSCvp58804 が追加されました。
3.5 (2b)	2019 年 5 月 2 日	「リリース 3.5 (2b) で解決済みの警告」リストに CSCvk38003 が追加されました。
3.5 (2b)	2019 年 3 月 22 日	Cisco HX Data Platform ソフトウェア リリース 3.5(2b) のリリース ノートを作成しました。
3.5(2a)	2019 年 1 月 8 日	Cisco HX Data Platform ソフトウェア リリース 3.5(2a) のリリース ノートを作成しました。
3.5(1a)	2018 年 11 月 21 日	「Cisco HX Data Platform ストレージ クラスタの仕様」セクションの形式を改定しました。
3.5(1a)	2018 年 11 月 6 日	• 「サポートされている vSphere バージョン」セクションに vCenter バージョン 6.7 U1 が追加されました。 • 「サポートされている vSphere バージョン」の表から、廃止されたリリース-1.8、2.0、2.1、2.5 を削除しました。 • 「リリース 3.5 (1a) で未解決の問題」リストに CSCvn07634 が追加されました。
3.5(1a)	2018 年 10 月 16 日	Cisco HX Data Platform ソフトウェア リリース 3.5(1a) のリリース ノートを作成しました。

新機能

リリース 3.5 (2h) の新機能

- **新しい 375G Intel Optane 高パフォーマンス キャッシュ ドライブ (PID: HX-NVMI375) のサポートが追加されました。**このドライブは、HXDP 4.0 リリースで導入されたものです。

リリース 3.5 (2g) の新機能

- **第 2 世代 intel® Xeon® スケーラブル プロセッサ更新のサポート**: このリリースには、第 2 世代 Intel® Xeon® スケーラブル プロセッサ リフレッシュ (以前の Cascade Lake) のサポートが含まれています。
- **新しい FIPS 準拠 SED SSD ドライブ HX のサポート**: このドライブは、オーダーできなくなった古いキャッシングドライブ (HX SD800GBENK9) を置き換えます。拡張または交換のために新しいドライブを使用するには、クラスタを HX リリース 3.5 (2g) 以降にアップグレードする必要があります。
- **Edge 向け 1.6TB キャッシュ ドライブ HX-SD16T123X-EP (サーバ PID: HXAF-E-220M5SX) のサポート**: このドライブは、オーダーできなくなった古いキャッシュ ドライブ オプション HX SD400G12TX を置き換えます。新しいドライブ PID を利用するには、HX Edge クラスタを HX リリース 3.5 (2g) とともにインストールする必要があることに注意してください。また、RMA のシナリオでは、HX Edge クラスタを HX リリース 3.5 (2g) 以降にアップグレードする必要があります。

リリース 3.5 (2f) の新機能

（注） Cisco HyperFlex リリース 3.5 (2f) では、ストレッチ クラスタで監視 VM をバージョン1.0.6 以降にアップグレードする必要があります。監視 VM のアップグレード方法の詳細については、「監視 VM のアップグレード」を参照してください。

（注） ストレッチ クラスタを使用した暗号化と SED ドライブの有効な設定はサポートされていません。

リリース 3.5(2e) の新機能

- **次のサーバ設定 HXAF220C-M5SX および HXAF240C-M5SX 向け 1.6TB キャッシュ ドライブ HX-SD16T123X-EP のサポート**: このドライブは、オーダーできなくなった古いキャッシュ ドライブ オプション HX SD400G12TX を置き換えます。新しいドライブ PID を利用するには、クラスタを 3.5 (2g) とともにインストールする必要があることに注意してください。また、新しいドライブを含むノードまたは障害が発生したドライブを交換するとき

に既存のクラスタ (HX SD400G12TX-EP キャッシュ ドライブを使用) を拡張するには、クラスタを 3.5 (2g) 以降にアップグレードする必要があります。

リリース 3.5 (2d) の新機能

- このリリースでは、新しいソフトウェア機能はありません。

リリース 3.5 (2c) の新機能

- このリリースは延期されています。

警告

Cisco HyperFlex Data Platform リリース 3.5(2c) は、ダウンロードできなくなりました。Cisco ソフトウェア ダウンロード サイトで、HX 3.5(2g) または最新の推奨リリースにアップグレードすることをお勧めします。詳細については、『CSCvp90129 のソフトウェア延期通知』および『CSCvp90129 のソフトウェア アドバイザリ: 障害が発生するストレッチ クラスタ ノードが利用不可能になる場合がある』を参照してください。

リリース 3.5 (2b) の新機能

- **EMC RecoverPoint**: Cisco HX Data Platform リリース 3.5 (2b) 以降では、VM の RecoverPoint のサポートが RP4VMs バージョン 5.2. P1 と組み合わせて開始します。VM の RecoverPoint の同期複製機能はサポートされていません。

リリース 3.5 (2a) の新機能

- **HyperFlex ハードウェア アクセラレーション エンジン**: 新しい専用の PCIe ハードウェア アクセラレーション カード (HX)。圧縮効率を高め、速度を向上させ、ストレージ容量を増やすことができます。これらのカードは、現在 HX240 M5 (すべてのフラッシュ/ハイブリッド) ノードで使用可能であり、HX Data Platform エンタープライズ ライセンスが必要です。詳細については、『VMware ESXi 用 Cisco HyperFlex システム リリース 3.5 インストール ガイド』を参照してください。
- **Microsoft Hyper-V の機能拡張**: Cisco HX Data Platform リリース 3.5 (2a) 以降では、Hyper-V コンピューティング専用ノードのクラスタ拡張がサポートされています。詳細については、『Microsoft Hyper-V 用 Cisco HyperFlex システム リリース 3.5 インストール ガイド』を参照してください。
- **Citrix クラウド サービス**: Citrix のワークスペースおよび Citrix 仮想アプリやデスクトップ サービス (以前の XenApp および XenDesktop サービス) などの関連付けられている Citrix クラウド サブスクリプションサービスに接続する新機能です。詳細については、『Citrix ワークスペース アプライアンス向け Cisco HyperFlex リリース 3.5 システム管理ガイド』を参照してください。

- **VMware ESXi 6.7 U1 のサポート**: 詳細については、『Cisco HyperFlex Systems: ネットワーキング トポロジ』および『VMware ESXi 用 Cisco HyperFlex システム インストール ガイド リリース 3.5』を参照してください。
- **HX クラスタを使用した UCS 6454 ファブリック インターコネクト (6454 HX) のサポート**: 詳細については、『Cisco HyperFlex システム: ネットワーキング トポロジ』を参照してください。

リリース 3.5 (1a) の新機能

- **ネイティブ ディザスタ リカバリの機能拡張**： シンプルな「移行計画ワークフロー」を使用して、ディザスタ リカバリ、VM の移行、レプリケーションの再開を簡単に実行できます。また、Stretched Cluster の導入でレプリケーション、計画的移行、ディザスタ リカバリがネイティブでサポートされます。詳細については、『Cisco HyperFlex System 管理ガイド リリース 3.5』を参照してください。
- **HX Data Platform インストーラの機能拡張**：新しい拡張機能として、HX データ プラットフォーム インストーラの強化と信頼性向上が図られています。
  - Hyper-V コンバージド ノードのクラスタ拡張。
  - Stretched Cluster コンピューティング専用ノードおよびコンバージド ノードのクラスタ拡張。
  - クラスタ作成ワークフローの一部として Hyper-V および Windows Server OS のベア メタル インストールが追加されています。
- **ネットワーキングの機能拡張**：HX コンバージドおよびコンピューティング専用ノードでマルチ VIC ネットワーク設計とサードパーティ製 NIC がサポートされます。詳細については、Cisco HyperFlex システム：ネットワーク トポロジを参照してください。
- **アップグレードの機能拡張**：ESXi ハイパーバイザの協調アップグレードをサポートします。HX Data Platform とサーバ ファームウェアについての既存のアップグレードに加えて、今回のリリースでは、HX Connect を介してすべてが協調して動作するシームレスなフル スタック アップグレードの機能が提供されています。

  Cisco HX Data Platform リリース 3.5(1a) 以降では、今後のすべてのアップグレードを HX Connect の UI で完了できます。今後のすべてのアップグレードについて、この機能はリリース 3.5 のすべてのクラスタで有効になります。古いバージョンからリリース 3.5 にアップグレードする場合は、引き続きドキュメントに記載されているブートストラップ スクリプトを実行してください。今回の新しいエンドツーエンドの UI ベースアップグレード機能は、今後のすべてのアップグレードで利用します。詳細については、『Cisco HyperFlex システム リリース 3.5 アップグレード ガイド』を参照してください。
- **ESXi ロックダウン モード**：ホストに許可するアクセスを制限することにより、VMware ESXi のロックダウン モードをサポートし、ESXi ホストのセキュリティを強化します。このモードを有効にすると、ESXi ホストには vCenter Server またはダイレクト コンソール ユーザ インターフェイス（DCUI）からのみアクセスできます。詳細については、『Cisco HyperFlex システム リリース 3.5 インストール ガイド』を参照してください。

- **HX Edge 10GbE エッジ ネットワーク オプション**：新しい 10GbE エッジのサポートにより、HyperFlex Edge クラスタ向けに完全に冗長な高速接続オプションが追加提供されます。詳細については、『Cisco HyperFlex システム リリース 3.5 エッジ導入ガイド』を参照してください。
- **Cisco Container Platform（CCP）と Open Shift Platform（OpenShift）の統合**：Kubernetes とのストレージ統合により、HyperFlex の動的な（オンデマンドの）永続的ボリュームが使用できます。この機能は OpenShift（バージョン 3.10）と Cisco Container Platform（CCP）でサポートされます。詳細については、『Cisco HyperFlex Systems Kubernetes リリース 3.5 アドミニストレーション ガイド』を参照してください。
- **NVIDIA V100 GPU での人工知能および機械学習（AI/ML）ワークロード**：HyperFlex ノード内で NVIDIA Tesla V100 GPU の統合を使用して AI/ML のアプリケーションを作成できます。詳細については、Cisco HyperFlex HX シリーズ スペック シートを参照してください。
- **Permanent License Reservation (PLR)**：この機能は、高度なセキュリティで保護されたインテリジェンス、エアギャップ環境、軍用環境など、外部との通信が制限される状況を対象としています。詳細については、『Cisco HyperFlex システム注文およびライセンス ガイド』を参照してください。
- **DISA の共存の自動化**: 防衛情報システムエージェンシー (disa) の推奨されるセキュリティ技術実装ガイド (stig) の実装を自動化することにより、hyperflex の統合およびコンピューティング専用ノードのセキュリティを強化します。VMware vSphere に関連
- **テクニカル サポート モード**：テクニカル サポート モードを無効にして HyperFlex コンバージド ノードのセキュリティ ポスチャを強化します。これにより、SSH 経由でのコントローラ VM へのリモート アクセスが無効になります。

サポート対象バージョンおよびシステム要件

Cisco HX Data Platform を正常にインストールするには、特定のソフトウェアおよびハードウェアのバージョン、ネットワーク設定が必要です。

すべての要件については、以下を参照してください。

- VMware ESXi の Cisco HyperFlex システム インストール ガイド または
- Cisco HyperFlex Systems インストール ガイド（Microsoft Hyper-V 用）

ハードウェアおよびソフトウェアの相互運用性

ハードウェアとソフトウェアの相互依存関係の一覧については、それぞれの Cisco UCS Manager リリース バージョンの Cisco HyperFlex HX シリーズにおけるハードウェアおよびソフトウェアの相互運用性 [英語] を参照してください。

HyperFlex ソフトウェアのバージョン

Cisco HX Data Platform インストーラ、Cisco HX Data Platform、および Cisco UCS ファームウェアといった HX のコンポーネントは、さまざまなサーバにインストールされます。HX Storage Cluster とともに（またはその内部で）使用される各サーバの各コンポーネントに互換性があることを確認します。

- HyperFlex は、UCS Manager および UCS Server Firmware バージョン 4.0(4a)、4.0(4b)、4.0(4c) をサポートしていません。

  重要 これらのファームウェア バージョンにアップグレードしないでください。

  これらの UCS Manager のバージョンにアップグレードしないでください。

- 事前設定された HX サーバと、インストールされている Cisco UCS サーバ ファームウェアのバージョンが同じであることを確認します。Cisco UCS ファブリック インターコネクト（FI）のファームウェア バージョンが異なる場合は、ファームウェアのバージョンを調整する手順について、『*Cisco HyperFlex Systems Upgrade Guide*』を参照してください。
  - **M4**:新しいハイブリッドまたはオール フラッシュ (Cisco HyperFlex HX240c M4 または HX220c M4)の導入の場合は、 Cisco UCS Manager 3.1(3k)、3.2(3i)、または 4.0(2d) がインストールされていることを確認してください。
  - **M5**: 新しいハイブリッドまたはすべてのフラッシュ（Cisco HyperFlex HX240c M5 または HX220c M5）を展開する場合は、推奨される UCS ファームウェア バージョンがインストールされていることを確認してください。

    重要 複数の Nvidia GPU が存在する場合に Cisco UCS Manager 4.0 (2a) または 4.0 (2b) をアップグレードする場合は、GPU を削除してから、アップグレードと再インストールを実行してください。詳細については、 CSCvo13678を参照してください。

    重要 SED ベース HyperFlex システムについては、A（インフラストラクチャ）、B（ブレードサーバ）および C（ラック サーバ）バンドルが、すべての SED M4/M5 システムに対して Cisco UCS Manager バージョン 4.0(2b) 以降です。詳細については、CSCvh04307 を参照してください。SED ベース HyperFlex システムでは、すべてのクラスタが HyperFlex リリース 3.5(2b) 以降であることも確認します。詳細については、**Field Notice (70234)** および CSCvk17250 を参照してください。

- HX サーバを再インストールするには、サポートされている互換性のあるソフトウェアのバージョンをダウンロードします。要件と手順については『VMware ESXi 向け *Cisco HyperFlex* システム インストール ガイド』を参照してください。
- 推奨される FI/サーバ ファームウェアのリリース ノートを確認してください。

表 *1 : M4/M5* サーバ *(SED* 以外*)* の *HyperFlex* のソフトウェア バージョン

HyperFlex リリース	M4 推奨 FI/サーバ ファームウェア *(上記の重要な注意事項を必ず確認してください)	M5 推奨 FI/サーバ ファームウェア *(上記の重要な注意事項を必ず確認してください)
3.5 (2h)	4.0 (4h)	4.0 (4h)
3.5 (2g)	4.0 (4h)	4.0 (4h)
3.5(2f)	4.0 (4e)	4.0 (4e)
3.5(2e)	4.0 (4e)	4.0 (4e)
3.5 (2d)	4.0 (4e)	4.0 (4e)
3.5 (2c)	リリースの延期	
3.5 (2b)	4.0 (2d)、3.2 (3i)、3.1 (3k)	4.0(2d)
3.5(2a)	4.0(1c)、3.2(3i)、3.1(3k)	4.0(1c)
3.5(1a) - サポートされていない	4.0(1b)、3.2(3h)、3.1(3j)	4.0(1a)

3.x 展開向けHyperFlex Edge およびファームウェア互換性マトリックス

Cisco HX データ プラットフォーム リリース 3.x に基づく導入

サーバのコンポーネント ファームウェアが、次の表に示されている最小バージョン以上であることを確認します。

重要 **HyperFlex Edge は、Cisco IMC バージョン 4.0 (4a)、4.0 (4b)、4.0 (4c)、4.0 (4d)、および 4.0 (4e) をサポートしていません。**

表 *2 : HX220c M4/HXAF220c M4* クラスタ

コンポーネント	ファームウェアの最小バージョン - **HXDP 3.x** *** (上記の重要な注意事項を必ず確認してください)**	ファームウェアの推奨バージョン ***(上記の重要な注意事項を必ず確認してください)**
Cisco Integrated Management Controller（CIMC）	3.0(3f)	4.0 (2f)
Host Upgrade Utility（HUU）ダウンロード リンク	3.0(3f) ソフトウェアのダウンロード	4.0 (2f) ソフトウェアのダウンロード

表 *3 : HX220c M5/HXAF220c M5* クラスタ

コンポーネント	ファームウェアの最小バージョン - **HXDP 3.x** *** (上記の重要な注意事項を必ず確認してください)**	ファームウェアの推奨バージョン *** (上記の重要な注意事項を必ず確認してください)**
Cisco Integrated Management Controller（CIMC）	3.1(2d)	4.0(4k)
Host Upgrade Utility（HUU）ダウンロード リンク	3.1(2d) ソフトウェアのダウンロード	4.0(4k) ソフトウェアのダウンロード

HyperFlex のライセンス

バージョン 2.6(1a) の時点で、HyperFlex は VMware PAC のライセンスをサポートしています。既存 VMware 組み込みライセンスは常にサポートされます。

バージョン 2.5(1a) の時点で、HyperFlex ではスマート ライセンス メカニズムを使用してライセンスを適用するようになっています。詳細と手順については『*VMware ESXi* 向け *Cisco HyperFlex* システム インストール ガイド』を参照してください。

VMware vSphere のライセンス要件

vSphere ライセンスを HyperFlex システムに適用する方法は、そのライセンスの購入方法に応じて変わります。

- **HyperFlex 付きの vSphere ライセンスを購入した場合**

  各 HyperFlex サーバはいずれも、出荷時に Enterprise または Enterprise Plus エディションがプレインストールされています。

（注）

- HX ノードには、プレインストール OEM ライセンスがあります。HX サーバを受け取った後、ブート ドライバのコンテンツを削除または上書きすると、プレインストールされたライセンスも削除されます。
- OEM ライセンス キーは、新しい VMware vCenter 6.0 U1b 機能です。以前のバージョンは OEM ライセンスをサポートしていません。
- プレインストールされた HX ノードはすべて同じ OEM ライセンス キーを共有します。vSphere OEM キーを使用すると、[Usage (使用状況)] の数が [Capacity (容量)] の値を超えることができます。
- **[Assign license (ライセンスの割り当て)]** セクションの **[Add Host (ホストの追加)]** ウィザードで vCenter に HX ホストを追加する場合は、**[OEM license (OEM ライセンス)]** を選択してください。

  実際の vSphere OEM ライセンス キーは難読化されています（例：0N085-XXXXX-XXXXX-XXXXX-10LHH）。
- Standard、Essentials Plus、ROBO エディションは、HX サーバにプレインストールされていません。

- **HyperFlex 付きの vSphere ライセンスを購入しなかった場合**

  HX ノードには、vSphere の基本ライセンスがプレインストールされています。初期設定後、ライセンスをサポートされている vSphere のバージョンに適用できます。

- **vSphere PAC ライセンスを購入した場合**

  VMwareからのPACライセンスレターの指示に従ってライセンスを MY VMware アカウントに追加し、次に指示に従って HX ホストを vCenter に追加して PAC ライセンスを割り当てます。

HyperFlex 補助ノードの HX データ プラットフォーム ソフトウェア バージョン

HyperFlex リリース	補助ノードのバージョン
3.5 (2h)	1.0.8
3.5 (2g)	1.0.6 以降
3.5(2f)	1.0.6 以降
3.5(2e)	1.0.4

HyperFlex リリース	補助ノードのバージョン
3.5 (2d)	1.0.3
3.5 (2c)	リリースの延期
3.5 (2b)	1.0.3
3.5(2a)	1.0.3
3.5(1a) - サポートされていない	1.0.2

（注） Cisco HyperFlex リリース 3.5 (2f) では、ストレッチ クラスタで監視 VM をバージョン1.0.6 以降にアップグレードする必要があります。監視 VM のアップグレード方法の詳細については、「監視 VM のアップグレード」を参照してください。

（注） 旧バージョンのVMは、最新のHXDPバージョンにクラスタがアップグレードされるとサポートされます。

VMware ESXi のソフトウェア要件

ソフトウェア要件には、互換性のある Cisco HyperFlex Systems（HX）、VMware vSphere および、VMware vCenter、および VMware ESXi コンポーネントのバージョンを使用していることを確認するための検証が含まれています。

- すべての HX サーバに、互換性のある vSphere のバージョンがプレインストールされていることを確認します。
- vCenter のバージョンが ESXi のバージョンと同じ、またはそれ以降であることを確認します。
- VMware Product Interoperability Matrix を参照して、vCenter と ESXi のバージョンに互換性があることを確認してください。次の表で ESXi と vCenter の両方がサポートされている限り、新しいバージョンの vCenter を古いバージョンの ESXi とともに使用することができます。
- ルートレベルの権限および関連パスワードが付与された vCenter 管理者アカウントがあることを確認します。

次の表は、VMware vSphere の Enterprise、Enterprise Plus、Standard、Essentials Plus, ROBO エディションに適用されます。

表 *4 : VMware ESXi* のソフトウェア要件

HyperFlex のバージョン（Cisco Unified Communications Manager Version）	VMware ESXi のバージョン	VMware vCenter バージョン
3.5 (2h)	6.0 U3、6.5 U3、6.7 U3	6.0 U3、6.5 U3、6.7 U3
3.5 (2g)	6.0 U3、6.5 U3、6.7 U3	6.0 U3、6.5 U3、6.7 U3
3.5 (2f)	6.0 U3、6.5 U2、6.7 U2[1]	6.0 U3、6.5 の U2 6.7 U1
3.5(2e)	6.0 U3、6.5 U2、6.7 U2[2]	6.0 U3、6.5 の U2 6.7 U1
3.5 (2d)	6.0 U3、6.5 U2、6.7 U2[3]	6.0 U3、6.5 の U2 6.7 U1
3.5 (2c)	リリースの延期	
3.5 (2b)	6.0 U3、6.5 U2、6.7 U1[4]、6.7 U2[5][6]	6.0 U3, 6. 5U2、6.7 U1、6.7 U2
3.5(2a)	6.0 U3、6.5 U2、6.7 U1[7]	6.0 U3、6.5 の U2 6.7 U1
3.5(1a) - サポートされていない	6.0 U3、6.5 U1、6.5 U2	6.0 U3、6.5 U1、6.5 U2、6.7 U1 [8]

1 6.7 U2 の使用は推奨されていません。詳細については、『CSCvq06952 および CSCvp88515 のソフトウェア アドバイザリ』を参照してください。

2 6.7 U2 の使用は推奨されていません。詳細については、『CSCvq06952 および CSCvp88515 のソフトウェア アドバイザリ』を参照してください。

3 6.7 U2 の使用は推奨されていません。詳細については、『CSCvq06952 および CSCvp88515 のソフトウェア アドバイザリ』を参照してください。

4 6.7 U1 の使用は推奨されていません。詳細については、『CSCvo56350 のソフトウェア アドバイザリ』を参照してください。

5 3.5(2b) リリースの場合、クラスタ インストールは最初に 6.0 U3 または 6.5 U2 で実行する必要があります。クラスタを展開した後に、Cisco.comからダウンロード可能な Zip バンドルを使用して、6.7 U2 にアップグレードできます。ESXi の詳細なアップグレードの手順については、『アップグレード ガイド』を参照してください。3.5 (2b) にアップグレードされた既存のクラスタは、いつでも 6.7 U2 に ESXi をアップグレードできます。

6 6.7 U2 の使用は推奨されていません。詳細については、『CSCvq06952 および CSCvp88515 のソフトウェア アドバイザリ』を参照してください。

7 6.7 U1 の使用は推奨されていません。詳細については、『CSCvo56350 のソフトウェア アドバイザリ』を参照してください。

8 3.5（1a）リリースでは、vCenter 6.7U1 の使用は、記載されている ESXi 6.0 および 6.5 のバージョンでのみサポートされています。

（注） vSphere 6.0 ユーザの場合。VMware の vSphere 6.0 の一般サポートは、2020 年 3 月 12 日に終了日を迎えました。HXDP は引き続き、vSphere 6.0 U3 の 3.5(2) および 4.0(2) 長期リリースの両方をサポートします。ただし、サポート終了日を過ぎたため、VMware も Cisco も、今後 ESXi のバグまたはセキュリティ フィックスを提供しません。Cisco TAC は引き続き、すでにリリースされている ESXi 6.0 ビルドを最大限活用できるよう、お客様をサポートします。CIsco では、サポートされている VMware vSphere 6.5 または6.7 リリースにできるだけ早くアップグレードし、『Cisco HyperFlex HX Data Platform Software Releases - for Cisco HyperFlex HX-Series Systems (推奨される Cisco HyperFlex HX データ プラットフォーム ソフトウェアリリース-Cisco HperFlex HX シリーズ システム)』て説明されている Cisco の推奨事項に従うことを強く推奨します。

Microsoft Hyper-V のソフトウェア要件

ソフトウェア要件には、互換性のある Cisco HyperFlex Systems（HX）コンポーネントおよび Microsoft Hyper-V (Hyper-V) コンポーネントのバージョンを使用していることを確認するための検証が含まれています。

HyperFlex ソフトウェアのバージョン

HX コンポーネント（Cisco HX Data Platform インストーラ、Cisco HX Data Platform、および Cisco UCS ファームウェア）は、別個のサーバにインストールされます。HX ストレージ クラスタ内で使用される各サーバの各コンポーネントに互換性があることを確認します。

- **Cisco HyperFlex M5 コンバージド ノード**: ハイブリッド (Cisco HyperFlex HX240c M5、HX220c M5) およびすべてのフラッシュ (Cisco HyperFlex HXAF240c M5、HXAF220c m5) について、Cisco UCS Manager 4.0 (2b) がインストールされていることを確認します。インストール要件および手順に関する詳細は、『*Microsoft Hyper-V* の *Cisco HyperFlex* システム インストール ガイド』を参照してください。

表 *5*: サポートされている *Hyper-V* 上の *M5* サーバ *HyperFlex* ソフトウェアのバージョン

HyperFlex リリース	M5 推奨サーバ ファームウェア
3.5 (2h)	4.0 (4h)
3.5 (2g)	4.0 (4h)
3.5(2f)	4.0 (4e)
3.5(2e)	4.0 (4e)
3.5 (2d)	4.0 (4e)
3.5 (2c)	リリースの延期
3.5 (2b)	4.0(2b)
3.5(2a)	4.0(1d)

HyperFlex リリース	M5 推奨サーバ ファームウェア
3.5(1a) - サポートされていない	4.0(1a)

表 *6 :* サポートされる *Microsoft* ソフトウェア バージョン

Microsoft コンポーネント	バージョン
Windows オペレーティング システム（Windows OS）	Windows サーバ 2016 コアおよびデスクトップ エクスペリエンス。 **注:** Windows Server 2016 Datacenter Core & Desktop Experience では、Windows 2016 ISO イメージは少なくとも Update Build Revision (UBR) 1884である必要があります。 ISO および Retail ISO をアクティベートした OEM は現在サポートされていません。Windows 2012r2 などの Windows サーバの以前のバージョンはサポートされていません。 ISO の英語以外のバージョンは現在サポートされていません。
Active Directory	Windows 2012 以降のドメインおよびフォレスト機能レベル

サポートされている Microsoft ライセンス エディション

1 個以上の HyperFlex ホストにインストールされている Microsoft Windows サーバのバージョンは、『Microsoft ライセンス取得』に記載されている Microsoft ライセンス要件に従ってライセンスが取得されている必要があります。

ブラウザの推奨事項 - 3.5(x) リリース

リストされている HyperFlex コンポーネントを実行するには、次のいずれかのブラウザを使用します。これらのブラウザはテストおよび承認済みです。他のブラウザでも動作する可能性はありますが、すべての機能をテストし、確認しているわけではありません。

表 *7 :* 対応ブラウザ

ブラウザ	Cisco UCS Manager	HX Data Platform インストーラ	HX Connect
Microsoft Internet Explorer	9 以上	11 以上	11 以上
Google Chrome	14 以上	56 以上	56 以上

ブラウザ	Cisco UCS Manager	HX Data Platform インストーラ	HX Connect
Mozilla Firefox	7 以上	52 以上	52 以上

注

- **Cisco HyperFlex Connect**:

  推奨される最小解像度は 1024 x 768 です。

- **Cisco HX Data Platform プラグイン**:

  Cisco HX Data Platform プラグイン は vSphere 内で動作します。VMware ホストのクライアントシステムブラウザの要件については、VMwareのマニュアルを参照してください。

  Cisco HX Data Platform プラグインは vCenter HTML クライアントには表示されません。vCenter フラッシュ クライアントを使用する必要があります。

- **Cisco UCS Manager**:

  ブラウザで次のものがサポートされている必要があります。

  - Java Runtime Environment 1.6 以降。
  - 一部の機能には、Adobe Flash Player 10 以降が必要です。

  Cisco UCS Manager に関するブラウザの最新情報については、最新の『Cisco UCS Manager スタートアップ ガイド』を参照してください。

Cisco HX Data Platform ストレージ クラスタの仕様

クラスタの制限

- Cisco HX Data Platform は、VMware の最大設定に従って、vCenter ごとに管理される最大 100 のクラスタをサポートします。
- Cisco HX Data Platform は、1 つの FI ドメインで任意の数のクラスタをサポートします。各 HX コンバージド ノードは、FEX を使用せずにファブリック A とファブリック B の専用 FI ポートに直接接続する必要があります。C シリーズのコンピューティング専用ノードも、両方の FI に直接接続する必要があります。B シリーズのコンピューティング専用ノードは、シャーシ I/O モジュールを介して両方のファブリックに接続されます。最終的に、FI 上の物理ポートの数により、UCS ドメインでサポートされる最大クラスタ サイズおよび個別のクラスタの最大数が決定します。

次の表では、Cisco HX Data Platform ストレージ クラスタの仕様を示しています。

	VMware ESXi			Microsoft Hyper-V		ストレッチ クラスタ*	
HX サーバ	HX220c M4 HX220c M5 HX240c M4 HX240c M5 HX220c M4 HX220c AF M5 HX240c M4 HX240c M5	HX240c-M5L	HX220c M5 Edge HX220c M4 Edge	HX220c M5 HX240c M5 HX220c AF M5 HX240c M5	HX240c-M5L	HX220c M5 HX240c M5 HX220c AF M5 HX240c M5	HX240c-M5L
UCS B シリーズ/C シリーズ ラック サーバ	B200 M3/M4、B260 M4、B420 M4、B460 M4、B480 M5、C240 M3/M4、C220 M3/M4、C480 M5、C460 M4、B200 M5、C220 m5、および C240 M5	B200 M3/M4、B260 M4、B420 M4、B460 M4、B480 M5、C240 M3/M4、C220 M3/M4、C480 M5、C460 M4、B200 M5、C220 m5、および C240 M5	—	B200 M4、B200 M5	B200 M4、B200 M5	B200 M3/M4、B260 M4、B420 M4、B460 M4、B480 M5、C240 M3/M4、C220 M3/M4、C480 M5、C460 M4、B200 M5、C220 m5、および C240 M5	B200 M3/M4、B260 M4、B420 M4、B460 M4、B480 M5、C240 M3/M4、C220 M3/M4、C480 M5、C460 M4、B200 M5、C220 m5、および C240 M5
サポートされるノード	コンバージドおよびコンピューティング専用ノード	コンバージドおよびコンピューティング専用ノード	コンバージド ノードのみ	コンバージドおよびコンピューティング専用ノード	コンバージドおよびコンピューティング専用ノード	コンバージドおよびコンピューティング専用ノード	コンバージドおよびコンピューティング専用ノード

	VMware ESXi			Microsoft Hyper-V		ストレッチ クラスタ*	
HXDP-S ライセンスされたノードの制限 **コンピューティング専用喉に対して 1:1 比の HXDP-S** **MinMax**	コンバージド ノード: 3 ~ 32 コンピューティング専用ノード: 0 ～ 32	コンバージド ノード: 3 ~ 16 コンピューティング専用ノード:0 ～ 16	コンバージド ノード: 3 (HXDP-E ライセンスが必要)	コンバージド ノード: 3 ~ 16 コンピューティング専用ノード: 0 ～ 16	コンバージド ノード: 3 ~ 16 コンピューティング専用ノード: 0 ～ 16	コンバージド ノード: サイトごとに 2 ～ 16 コンピューティング専用ノード: サイトごとに 0 ～ 16 **注:**HXDP-P ライセンスが必要です	コンバージド ノード: サイトごとに 2 ～ 8 コンピューティング専用ノード: サイトごとに 0 ～ 8 **注:**HXDP-P ライセンスが必要です
HXDP-P ライセンスされたノードの制限 **コンピューティング専用喉に対して 1:2 比の HXDP-P** **MinMax**	コンバージド ノード: 3 ~ 32 コンピューティング専用ノード: 0 ～ 32 (クラスタの最大サイズ)	コンバージド ノード: 3 ~ 16 コンピューティング専用ノード:0 ～ 32	コンバージド ノード: 3 (HXDP-E ライセンスが必要)	コンバージド ノード: 3 ~ 16 コンピューティング専用ノード: 0 ～ 16	コンバージド ノード: 3 ~ 16 コンピューティング専用ノード: 0 ～ 16	コンバージド ノード: サイトごとに 2 ～ 16 コンピューティング専用ノード: サイトごとに0～21 (クラスタの最大サイズ)	コンバージド ノード: サイトごとに 2 ～ 8 コンピューティング専用ノード: サイトごとに 0 ～ 16 (クラスタの最大サイズ)
クラスタの最大サイズ	64	48	3	32	32	サイトあたり 32/クラスタあたり 64	サイトあたり 32/クラスタあたり 64

	VMware ESXi			Microsoft Hyper-V		ストレッチ クラスタ*	
コンピューティングからコンバージドへの最大比率	2:1 *	2:1 *	—	1:1	1:1	2:1 *	2:1 *
説明	✓	✓	非対応	✓	✓	✓**	✓**

*エンタープライズ ライセンスが必要

**両方のサイトで同一の拡張を行う必要があります

注意事項と制約事項

- **HX REST API アクセストークン管理**: HX REST API を利用するアプリケーションは、API コールを行うときにアクセス トークンを再使用する必要があります。AAA 取得アクセス トークン API を使用して取得すると、アクセス トークンは18日間 (1,555,200 秒) 有効です。15分のウィンドウでは、/auth は最大5回呼び出せます(正常に呼び出せた場合)。ユーザは最大8個の失効トークンを作成できます。詳細については、『Cisco HyperFlex Systems REST API Reference（Cisco HyperFlex System REST API リファレンス』ガイドを参照してください。

アップグレードのガイドライン

次のリストは、HyperFlex システムのアップグレードを実行する際の重要な基準を記載します。

すべての HXDP 3.5 のアップグレードのガイドライン

- **Hypercheck ヘルス チェック ユーティリティ**: アップグレードする前に、Hypercheck クラスタでこの予防的ヘルス チェック ユーティリティを実行することを推奨します。これらのチェックにより、注意が必要なエリアがすぐに見やすくなり、シームレスなアップグレード エクスペリエンスを保証します。Hypercheck のインストールと実行方法の完全な手順の詳細については、『HyperFlex 健全性および事前アップグレード チェック ツール』を参照してください。
- **第1世代の Intel Xeon スケーラブルプロセッサから第2世代の Intel Xeon スケーラブルプロセッサへの CPU アップグレードはサポートされていません。**
- —HX コンバージド ノードでは、取り付けられている第 1 世代の Intel Xeon スケーラブル プロセッサから第 2 世代の Intel Xeon スケーラブル プロセッサへの CPU アップグレードまたは交換 (例えば、HX-CPU-6148 から HX-CPU-I6248 へ) はサポートされていません。
- **HX Release 3.5(2a) 以降のクラスタ準備状況**: HX 3.5(2a) 以降のアップグレードは、HX Connect UI を使用して自動的にブートストラップされます。詳細については、『 Cisco HyperFlex Systems Upgrade Guide』を参照してください。

- **ストレッチ クラスタのみの最新の監視 VM へのアップグレード**: Cisco HX Data Platform リリース 3.5 (2f) のストレッチ クラスタを実装するお客様の場合は、最新の監視 VM 1.0.6 以降へのアップグレードが必須です。
- **必要な vCenter のアップグレード**：セキュリティを強化するために、Cisco HX Data Platform リリース 3.5(1a) 以降では TLS 1.2 を使用する必要があります。そのため、HX3.5 にアップグレードする前に、vCenter 6.0 U3f 以降にアップグレードする必要があります。さらに、HX Data Platform の互換性要件を満たすために、ESXi を必要に応じてアップグレードする必要があります。
- **アップグレードの完了—**アップグレード ウィンドウでは、一時的に自己修復 (または再調整) が無効になっています。アップグレードが失敗する場合、できるだけ早くアップグレードを完了する必要があります。
- **サポートされていない自己暗号化ドライブ (SEDs)**: 新しいバージョンの HX Data Platform で最近認定された自己暗号化ドライブ (SEDs) を追加または交換する場合は、HX Data Platform にアップグレードした後にのみ、新しいドライブを互換性のあるバージョンに挿入してください
- メンテナンス時間枠：HX Data Platform と UCS ファームウェアの両方をアップグレードする場合、メンテナンス時間枠の大きさに応じて、vSphere HX Data Platform Plug-inを介したコンバインドアップグレードまたは分割アップグレードのいずれかを選択できます。Cisco UCS Manager インフラストラクチャ アップグレードでは、AutoInstall の使用のみをサポートしており、直接のサーバ ファームウェア アップグレードは、HX Data Platform Plug-in から提供されているアップグレード オーケストレーション フレームワークでのみ実行する必要があります。
- M4 サーバのファームウェアのアップグレード：円滑な動作を確実にして、既知の問題を修正するには、サーバファームウェアをアップグレードする必要があります。特に、長期間にわたる安定性を確保するために、このリリースで使用可能になった新しい SAS HBA ファームウェアを推奨します。

（注）
- 可能な場合は常に、リリース 3.1(3c) 以降の C バンドルにアップグレードするようにしてください。
- 3.1(2f) より前のバージョンの C バンドルを使用している場合は、UCS サーバファームウェア（C バンドル）のコンバインドアップグレードを行って、サーバファームウェアを 3.1(3c) 以降に、HX Data Platform を 2.5 にアップグレードする必要があります。これらのアップグレードを 2 つの別々の操作に分割しないでください。
- クラスタがすでに 3.1(2f) 以降の C バンドルで稼働している場合、必要に応じて HX Data Platform のみのアップグレードまたはコンバインド アップグレードを実行できます。

- **M5サーバ ファームウェアのアップグレード**：M5 世代のサーバでは、ファームウェア バージョン 3.2(2d) 以降を実行する必要があります。
- **ファームウェア ダウングレード** — HX-installer から UCSM のダウングレードはサポートされていません。

サポートされていない HX リリースの HXDP 3.5 へのアップグレードに関する追加のガイドライン

- **バージョン 3.0(1x) または 3.5(1x) を実行している HyperFlex クラスタのアップグレードのリマインダ**: HyperFlex バージョン 3.0(1x) および 3.5(1x) はサポートされていません。サポート終了の通知に記載されているように、サポートが終了したことを宣言しています。詳細については、CSCvt22244 のソフトウェア アドバイザリを参照してください。
- **アップグレード対象の最小 HXDP バージョン**：vCenter プラグインを使用して、2.1(1x) 以降を実行中の HX Data Platform クラスタは、3.5 に直接アップグレードできます。
- **アップグレードの開始**: 2.5(1a) 以降のリリースからアップグレードする場合は、HX Connect UI または CLI の `stcli` コマンドを使用してください。2.5(1a) より前のリリースからアップグレードする場合は、CLI `stcli` コマンドまたはvSphere Web ClientのHX Data Platform Plug-inを使用します。vCenter プラグインは、2.5(1a) リリース以降のアップグレードには使用しないでください。
- **アップグレード対象の最小 HXDP バージョン**：1.8(1f) 以降を実行中の HX Data Platform クラスタは、3.0 に直接アップグレードできます。
- **HX Data Platform 1.7.x、1.8.x、2.0、2.1x クラスタ**—2.6(1a) 以前のバージョンからのユーザーは、3.5x またはそれ以降のリリースにアップグレードする前に、中間バージョンを通過する必要があります。サポートを終了した Cisco HyperFlex HX Data Platform ソフトウェア リリースから、Cisco ソフトウェア ダウンロード サイトの最新の提案されたリリースにアップグレードする必要がある場合、『サポートされていない Cisco HX リリースの Cisco HyperFlex システム アップグレード ガイド』を参照してください。詳細については、『Software Advisory for CSCvq66867 のソフトウェア アドバイザリ: 警告: HXDP 1.8(1a)-1.8(1e) からアップグレードする場合は HXDP 2.6(1e) アップグレード パッケージのみ使用する』を参照してください。
- **HX Data Platform 2.6(1x) および 3.5(2x) クラスタ: 3.5(2x) への直接アップグレードはサポートされていません**—2.6(1x) 以前のバージョンからのユーザーは、3.5(2x) またはそれ以降のリリースにアップグレードする前に、中間バージョンを経過する必要があります。サポートを終了した Cisco HyperFlex HX Data Platform ソフトウェア リリースから、Cisco ソフトウェア ダウンロード サイトの最新の提案されたリリースにアップグレードする必要がある場合、『サポートされていない Cisco HX リリースの Cisco HyperFlex システム アップグレード ガイド』を参照してください。詳細については、『Software Advisory for CSCvq66867 のソフトウェア アドバイザリ: 警告: HXDP 1.8(1a)-1.8(1e) からアップグレードする場合は HXDP 2.6(1e) アップグレード パッケージのみ使用する』を参照してください。
- **必要な vCenter のアップグレード**：セキュリティを強化するために、Cisco HX Data Platform リリース 3.0(1a) 以降では TLS 1.2 を使用する必要があります。そのため、Cisco HX Data

Platform リリース 3.0 にアップグレードする前に、vCenter を 6.0 U3c 以降にアップグレードする必要があります。さらに、HX Data Platform の互換性要件を満たすために、ESXi を必要に応じてアップグレードする必要があります。

- **クラスタの対応状況**：アップグレードを進める前に、クラスタが適切にブートストラップされて、更新済みプラグインがロードされていることを確認します。3.5(1a) よりも前の HX リリースでは、手動クラスタブートストラップが必要です。詳細については、「手動ブートストラップによるアップグレード プロセス」(『VMware ESXi の Cisco HyperFlex システム アップグレード ガイド』)を参照してください。HX リリース 3.5(1a) までのすべてのバージョンでは、アップグレードで必要なため、このクラスタ ブートストラップの手順はスキップしないでください。自動ブートストラップは、HX リリース 3.5(1a) 以降でサポートされています。詳細については、「自動ブートストラップによるアップグレード プロセス」(『VMware ESXi の Cisco HyperFlex システム アップグレード ガイド』)を参照してください。

- **vSphere 5.5 のアップグレード**：vSphere 5.5 を使用している場合、HX Data Platformのアップグレードを開始する前に 6.0 U3/6.5 U1 にアップグレードする必要があります。vSphere 5.5 のサポートはHX Data Platform 2.5(1a) で廃止されたため、アップグレードしようとしても失敗します。

  - HX220 で 5.5 を実行している場合は、TAC に連絡してアップグレードの支援を求めてください。

  - HX240 で 5.5 を実行している場合は、次の順序でコンポーネントをアップグレードします。

    1. vCenter を 6.0 U3f またはそれ以降にアップグレードします。6.5 にアップグレードする場合は、vCenter のインプレース アップグレードが必要です。5.5 から移行する場合、新しい vCenter 6.5 の使用はサポートされません。
    2. オフライン zip バンドルを使用して ESXi を 6.0/6.5 にアップグレードします。

    （注） ESXi のアップグレードが完了してホストが再起動した後、vCenter で手動で ESXi ホストに再接続しなければならない場合があります。

    3. HX Data Platform を（必要に応じて UCS ファームウェアも）アップグレードします。

  - vSphere 6.5 にアップグレードする場合：

    - 特定のクラスタ機能（ネイティブ/スケジュール スナップショット、ReadyClones、HX メンテナンス モードの開始/終了など）は、アップグレードの開始時から 3.5 以降への HX Data Platform のアップグレードが完了するまで動作しません。

    - オフライン zip バンドルを使用して ESXi をアップグレードした後、ESX の [Exit Maintenance Mode] オプションを使用します。HX Data Platform のアップグレード

が完了するまでは、vSphere Web クライアント内で ESX の [メンテナンス モードの終了（Exit Maintenance Mode）] オプションは動作しません。

- vSphere 6.0 のアップグレード：vSphere 6.0 を 6.5 に移行する場合は、次の順序でコンポーネントをアップグレードします。
  1. HX Data Platform と UCS ファームウェアをアップグレードします。
  2. HX Data Platformと ESXi をアップグレード。
  3. HX Data Platform のみを最初にアップグレードし、次に ESXi および/または UCS ファームウェアをアップグレードするか、両方アップグレードします。

- M4/M5 の混在ドメイン：既存の M4 クラスタが含まれる UCS ドメインに新しい別個の M5 クラスタをインストールすると、同じドメインに M4 と M5 が混在することになります。このような場合、オーケストレーションされた UCS サーバファームウェアのアップグレードは、M4 クラスタに Cisco HX Data Platform リリース 2.6 以降がインストールされるまで動作しません。したがって、最初に UCS サーバ ファームウェアを最新の 3.1(3) または 3.2(2) パッチ リリースにアップグレードしてから、既存の USC ドメインに新しい M5 クラスタを追加することがベスト プラクティスです。さらに、新しい M5 クラスタを 1.7 HX Data Platform クラスタと同じドメインに追加する場合は常に、1.7 HX Data Platform クラスタを最初にアップグレードする必要があります。

- **自己暗号ドライブ (SED) を使用した HX Data Platform 2.1(1b)**2.1 を：実行している自己暗号化ドライブ (SEDs) 対応のシステムをアップグレードする場合は、UCS インフラストラクチャとサーバ ファームウェアのアップグレードが必要です。詳細については、**Field Notice (70234)** および CSCvk17250 を参照してください。

- **管理者ユーザアカウント**: 最初に Cisco HX Data Platform、リリース1.7 で展開したクラスタからアップグレードする場合、または展開後にパスワードを手動で変更した場合は、クラスタ管理者パスワードをリセットする必要があります。詳細については、『Cisco HyperFlex Systems Upgrade Guide』を参照してください。

混合クラスタ展開のガイドライン

- M5 コンバージド ノードを持つ既存の M4 クラスタの展開がサポートされています。
- M4 コンバージド ノードを持つ既存の M5 クラスタの展開がサポートされています。
- M4 または M5 コンバージド ノードを持つ既存の混合 M4/M5 クラスタの展開がサポートされています。
- サポートされているコンピューティング専用ノードを追加することは、HX Data Platform 2.6 またはそれ以降のインストーラを使用した M4、M5、混合 M4/M5 クラスタすべてで許可されています。いくつかの例となる組み合わせがここにリストされています。その他多くの組み合わせが可能です。

```
Example combinations:
Expand mixed M4/M5 cluster with compute-only B200, C220, C240 M4/M5
Expand M4 cluster with compute-only B200 M5, C220 M5, C240M5
```

- 混合クラスタを作成するには、展開ワークフローのみがサポートされています。混合 M4/M5 サーバを持つ最初のクラスタ作成はサポートされていません。
- すべての M5 サーバは、既存の M4 サーバのフォーム ファクタ（220/240）、タイプ（Hybrid/AF）、セキュリティ機能（非 SED のみ）およびディスク設定（数量、容量、非 SED）と一致する必要があります。ドライブの互換性については、『Cisco Hyperflex Drive Compatibility』ドキュメントを参照してください。
  - HX220-M4 と組み合わせるとき、HX220-M5 は最大 6 の容量ディスク（2 ディスク スロットは空のまま）を使用します。
- HX Edge、SED、LFF、Hyper-v、およびストレッチ クラスタは、混合 M4 および M5 クラスタをサポートしていません。

リリース 3.5 向け混合クラスタ拡張のガイドライン

混合クラスタは、同じストレージ クラスタ内の M4 および M5 HX コンバージド ノードの両方を持つことで定義されます。混合クラスタを設定するとき、以下のガイドラインが適用されます。

- M5 コンバージド ノードを持つ既存の M4 クラスタの展開がサポートされています。
- M4 コンバージド ノードを持つ既存の M5 クラスタの展開がサポートされています。
- M4 または M5 コンバージド ノードを持つ既存の混合 M4/M5 クラスタの展開がサポートされています。
- サポートされているコンピューティング専用ノードを追加することは、HX Data Platform 2.6 またはそれ以降のインストーラを使用した M4、M5、混合 M4/M5 クラスタすべてで許可されています。いくつかの例となる組み合わせがここにリストされています。その他多くの組み合わせが可能です。

```
Example combinations:
Expand mixed M4/M5 cluster with compute-only B200, C220, C240 M4/M5
Expand M4 cluster with compute-only B200 M5, C220 M5, C240M5
```

- 混合クラスタを作成するには、展開ワークフローのみがサポートされています。混合 M4/M5 サーバを持つ最初のクラスタ作成はサポートされていません。
- すべての M5 サーバは、既存の M4 サーバのフォーム ファクタ（220/240）、タイプ（Hybrid/AF）、セキュリティ機能（非 SED のみ）およびディスク設定（数量、容量、非 SED）と一致する必要があります。
  - HX220-M4 と組み合わせるとき、HX220-M5 は最大 6 の容量ディスク（2 ディスク スロットは空のまま）を使用します。
- HyperFlex Edge は混合クラスタをサポートしません。
- SED SKU は混合クラスタをサポートしません。

セキュリティ修正

次のセキュリティ上の問題が解決されます。

リリース	不具合 ID	CVE	説明
3.5 (2h)	CSCvs06094	CVE-2015-9383 CVE-2018-14498 CVE-2018-20406 CVE-2018-20852 CVE-2019-10160 CVE-2019-13117 CVE-2019-13118 CVE-2019-14287 CVE-2019-14973 CVE-2019-15903 CVE-2019-17546 CVE-2019-18197 CVE-2019-18218 CVE-2019-5010 CVE-2019-5094 CVE-2019-5481CVE-2019-5482 CVE-2019-9636 CVE-2019-9740 CVE-2019-9947 CVE-2019-9948	このバグは、Tenable スキャンの脆弱性に対処するためのものです。
3.5 (2g)	CSCvr20154	CVE-2019-10086	commons beanutils commons-beanutils の複数の脆弱性。
3.5 (2g)	CSCvj95584	CVE-2019-12620	Cisco HyperFlex ソフトウェアの統計情報収集サービスの脆弱性により、認証されていないリモートの攻撃者が該当デバイスに任意の値を入力する可能性があります。 この脆弱性は、統計情報収集サービスの認証が不十分であることに起因します。攻撃者は、影響を受けるデバイスの統計情報収集サービスに適切にフォーマット化されたデータ値を送信することで、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者は Web インターフェイス統計情報で、ユーザーに無効なデータを提示する可能性があります。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。

リリース	不具合 ID	CVE	説明
3.5 (2g)	CSCvo98516	CVE-2019-1975	Cisco HyperFlex ソフトウェアの web ベースインターフェイスの脆弱性により、認証されていないリモートの攻撃者が、該当デバイスでクロスフレームスクリプティング (XFS) 攻撃を実行する可能性があります。 この脆弱性は、HTML iframe 保護が不十分であることに起因します。攻撃者は、悪意のある HTML iframe を含む攻撃者制御の web ページにユーザを誘導することで、この脆弱性をエクスプロイトする可能性があります。不正利用が成功すると、攻撃者はクリックジャックやその他クライアント側のブラウザ攻撃を行うことができます。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。

リリース	不具合 ID	CVE	説明
3.5 (2g)	CSCvr03322		定期的なスキャンによって識別されるオープン ソース ソフトウェア コンポーネントの脆弱性。

リリース	不具合 ID	CVE	説明
		CVE-2014-9092、 CVE-2015-9262、 CVE-2016-10087、 CVE-2016-10165、 CVE-2016-10708、 CVE-2016-10713、 CVE-2016-3616、 CVE-2016-9318、 CVE-2017-10053、 CVE-2017-10067、 CVE-2017-10074、 CVE-2017-10078、 CVE-2017-10081、 CVE-2017-10087、 CVE-2017-10089CVE-2017-10090、 CVE-2017-10096、 CVE-2017-10101、 CVE-2017-10102、 CVE-2017-10107、 CVE-2017-10108、 CVE-2017-10109、 CVE-2017-10110、 CVE-2017-10111、 CVE-2017-10115、 CVE-2017-10116、 CVE-2017-10118、 CVE-2017-10135、 CVE-2017-10176、 CVE-2017-10193CVE-2017-10198、 CVE-2017-10243、 CVE-2017-10274、 CVE-2017-10281、 CVE-2017-10285、 CVE-2017-10295、 CVE-2017-10345、 CVE-2017-10346、 CVE-2017-10347、 CVE-2017-10348、 CVE-2017-10349、 CVE-2017-10350、 CVE-2017-10355、 CVE-2017-10388、	

リリース	不具合 ID	CVE	説明
		CVE-2017-15232CVE-2017-16932、 CVE-2017-17512、 CVE-2017-18258、 CVE-2017-3509、 CVE-2017-3511、 CVE-2017-3526、 CVE-2017-3533、 CVE-2017-3544、 CVE-2018-0734、 CVE-2018-0735、 CVE-2018-0737、 CVE-2018-1000030、 CVE-2018-1000156、 CVE-2018-1000802、 CVE-2018-1000807CVE-2018-1000808、 CVE-2018-1060、 CVE-2018-1061、 CVE-2018-10916、 CVE-2018-10963、 CVE-2018-11212、 CVE-2018-11214、 CVE-2018-1152、 CVE-2018-11574、 CVE-2018-12384、 CVE-2018-12404、 CVE-2018-13785、 CVE-2018-14404、 CVE-2018-14567、 CVE-2018-14647CVE-2018-15473、 CVE-2018-16428、 CVE-2018-16429、 CVE-2018-16435、 CVE-2018-16890、 CVE-2018-17100、 CVE-2018-17101、 CVE-2018-18311、 CVE-2018-18312、 CVE-2018-18313、 CVE-2018-18314、 CVE-2018-18557、 CVE-2018-18585、 CVE-2018-18661、	

リリース	不具合 ID	CVE	説明
		CVE-2018-2579CVE-2018-2588、 CVE-2018-2599、 CVE-2018-2602、 CVE-2018-2603、 CVE-2018-2618、 CVE-2018-2633、 CVE-2018-2634、 CVE-2018-2637、 CVE-2018-2641、 CVE-2018-2663、 CVE-2018-2677、 CVE-2018-2678、 CVE-2018-2783、 CVE-2018-2794、 CVE-2018-2795、 CVE-2018-2796、CVE-、 CVE-CVE-2018-2797、 CVE-2018-2798、 CVE-2018-2799、 CVE-2018-2800、 CVE-2018-2814、 CVE-2018-2815、 CVE-2018-2952、 CVE-2018-3149、 CVE-2018-3150、 CVE-2018-3169、 CVE-2018-3180、 CVE-2018-3183、 CVE-2018-3214、 CVE-2018-6594、 CVE-2018-6951、 CVE-2018-7456、CVE-、 CVE-CVE-2018-8905、 CVE-2019-2422、 CVE-2019-3462、 CVE-2019-3822、 CVE-2019-3823、 CVE-2019-6109、CVE-2019-6111	

リリース	不具合 ID	CVE	説明
3.5 (2g)	CSCvq24176	CVE-2018-15380	Cisco HyperFlex のクラスタ サービス マネージャの脆弱性により、認証されていない隣接する攻撃者がルート ユーザーとしてコマンドを実行する可能性があります。 この脆弱性は、入力に対する不十分な検証に起因します。攻撃者はクラスタ サービス マネージャに接続し、バインドされたプロセスにコマンドを挿入することにより、この脆弱性を悪用する可能性があります。悪用が成功すると、攻撃者は影響を受けるホスト上でルート ユーザーとしてコマンドを実行する可能性があります。 この脆弱性に対処するソフトウェア アップデートは、すでに Cisco からリリースされています。脆弱性に対処する回避策があります。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。

リリース	不具合 ID	CVE	説明
3.5 (2g)	CSCvj95606	CVE-2018-15380	Cisco HyperFlex のクラスタ サービス マネージャの脆弱性により、認証されていない隣接する攻撃者がルート ユーザーとしてコマンド挿入を実行する可能性があります。 この脆弱性は、保護されていないリスニング インターフェイスが原因で発生します。攻撃者は、リッスンしているインターフェイスに接続し、バインドされたプロセスにコマンドを挿入することにより、この脆弱性を悪用する可能性があります。悪用により、攻撃者は影響を受けるホスト上でルート ユーザーとしてコマンドを実行する可能性があります。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。

リリース	不具合 ID	CVE	説明
3.5 (2g)	CSCvo88997		JVM 1.8 U121 で確認された脆弱性は、VC アラーム中にメモリ漏えいとなります(REST API を使用した同時 40 通話)。

リリース	不具合 ID	CVE	説明
		CVE-2017-10053、 CVE-2017-10067、 CVE-2017-10074、 CVE-2017-10078、 CVE-2017-10081、 CVE-2017-10087、 CVE-2017-10089、 CVE-2017-10090、 CVE-2017-10096、 CVE-2017-10101、 CVE-2017-10102、 CVE-2017-10107、 CVE-2017-10108、 CVE-2017-10109、 CVE-2017-10110CVE-2017-10111、 CVE-2017-10115、 CVE-2017-10116、 CVE-2017-10118、 CVE-2017-10135、 CVE-2017-10176、 CVE-2017-10193、 CVE-2017-10198、 CVE-2017-10243、 CVE-2017-10274、 CVE-2017-10281、 CVE-2017-10285、 CVE-2017-10295、 CVE-2017-10345、 CVE-2017-10346CVE-2017-10347、 CVE-2017-10348、 CVE-2017-10349、 CVE-2017-10350、 CVE-2017-10355、 CVE-2017-10356、 CVE-2017-10357、 CVE-2017-10388、 CVE-2017-3509、 CVE-2017-3511、 CVE-2017-3526、 CVE-2017-3533、 CVE-2017-3539、 CVE-2017-3544、	

リリース	不具合 ID	CVE	説明
		CVE-2018-2579CVE-2018-2582、 CVE-2018-2588、 CVE-2018-2599、 CVE-2018-2602、 CVE-2018-2603、 CVE-2018-2618、 CVE-2018-2629、 CVE-2018-2633、 CVE-2018-2634、 CVE-2018-2637、 CVE-2018-2641、 CVE-2018-2663、 CVE-2018-2677、 CVE-2018-2678、 CVE-2018-2783、 CVE-2018-2790、CVE-、 CVE-CVE-2018-2794、 CVE-2018-2795、 CVE-2018-2796、 CVE-2018-2797、 CVE-2018-2798、 CVE-2018-2799、 CVE-2018-2800、 CVE-2018-2814、 CVE-2018-2815、 CVE-2018-2952、 CVE-2018-3136、 CVE-2018-3139、 CVE-2018-3149、 CVE-2018-3150、 CVE-2018-3169、 CVE-2018-3180、CVE-、 CVE-CVE-2018-3183、 CVE-2018-3214、CVE-2019-2422	
3.5(2a)	CSCvn22303	CVE-2016-1000031	**Apache Struts Commons FileUpload RCE** に含まれている、サードパーティ ソフトウェアに関連した脆弱性。

リリース	不具合 ID	CVE	説明
3.5(2a)	CSCvm93059	CVE-2018-18074	**Python package**、**Ubuntu** カーネルに含まれているソフトウェア パッケージのバージョンに関連付けられている脆弱性。
3.5(2a)	CSCvk59165	CVE-2019-1665	認証されていないリモート攻撃者がクロスサイト スクリプティング (XSS) 攻撃を実施可能になる Cisco HyperFlex ソフトウェアの Web ベースの管理インターフェイスに関連する脆弱性。
3.5(2a)	CSCvm53149	CVE-2018-1092 CVE-2018-7492 CVE-2018-8087 CVE-2018-1068 CVE-2018-8781	**Linux kernel for Ubuntu 17.10** に関連付けられている脆弱性。
3.5(2a)	CSCvm53142	CVE-2018-14598 CVE-2018-14599 CVE-2018-14600	**libx11** に関連付けられている脆弱性。
3.5(2a)	CSCvm53132	CVE-2018-14622	**libtirpc**に関連付けられている脆弱性。
3.5(2a)	CSCvm34693	CVE-2018-1060	**Python pop3lib apop() Method Denial of Service**に含まれるソフトウェア バージョンに関連付けられている脆弱性。
3.5(2a)	CSCvm02920	CVE-2018-3615 CVE-2018-3620 CVE-2018-3646	**August CPU Side-Channel Information Disclosure** に関連付けられている脆弱性。
3.5(2a)	CSCvk31047	CVE-2019-1664	Cisco HX Data Platform に含まれている **hxterm** サービスのバージョンに関連付けられている脆弱性。
3.5(2a)	CSCvj08921	CVE-2018-7750	**Paramiko transport.py Authentication Bypass** に含まれているソフトウェア バージョンに関連付けられている脆弱性。

リリース	不具合 ID	CVE	説明
3.5(1a)	CSCvm29418	CVE-2017-18342	**PyYAML** に含まれている、サードパーティ製ソフトウェアに関連付けられている脆弱性。
3.5(1a)	CSCvm20484	CVE-2018-14682 CVE-2018-14679 CVE-2018-14680 CVE-2018-14681	Cisco HX Data Platform に含まれている **libmspack** ソフトウェアパッケージのバージョンに関連付けられている脆弱性。
3.5(1a)	CSCvm15800	CVE-2018-5391	Cisco HyperFlex System には、サービス妨害 (Dos) 脆弱性の IP フラグメントの再構成によって影響を受ける Linux カーネルのバージョンが含まれています。
3.5(1a)	CSCvm10159	CVE-2015-9262	Cisco HX Data Platform に含まれている **libXcursor** に関連付けられている脆弱性。
3.5(1a)	CSCvk59406	—	Cisco HyperFlex ソフトウェアのインストールプロセスの脆弱性により、認証されたローカルの攻撃者が機密情報を読み取ることが可能になる可能性があります。
3.5(1a)	CSCvk32464	—	Cisco HyperFlex ソフトウェアのファイル権限の脆弱性により、認証されたローカルの攻撃者が機密ファイルを読み取る可能性があります。
3.5(1a)	CSCvk22858	—	Cisco HyperFlex ソフトウェアの脆弱性により、認証されていないリモートの攻撃者が署名付きセッショントークンを生成する可能性があります。
3.5(1a)	CSCvk09234	CVE-2018-1092、CVE-2018-7492 CVE-2018-8087、CVE-2018-1068 CVE-2018-8781	Cisco HX Data Platform に含まれている Ubuntu Linux バージョンに関連付けられている脆弱性。

リリース	不具合 ID	CVE	説明
3.5(1a)	CSCvk05700	CVE-2018-12015	Cisco HX Data Platform に含まれている **perl** ソフトウェア パッケージのバージョンに関連付けられている脆弱性。
3.5(1a)	CSCvk05679	CVE-2014-9620 CVE-2014-9653 CVE-2015-8865 CVE-2018-10360 CVE-2014-9621	Cisco HX Data Platform に含まれている **file** ソフトウェア パッケージのバージョンに関連付けられている脆弱性。
3.5(1a)	CSCvk00405	CVE-2016-6796 CVE-2017-12615 CVE-2017-7674 CVE-2016-0762 CVE-2016-6797 CVE-2017-12616 CVE-2018-1304 CVE-2016-5018 CVE-2016-6816 CVE-2017-12617 CVE-2017-5647 CVE-2016-6794 CVE-2016-8735	Cisco HX Data Platform に含まれている **Apache Tomcat** ソフトウェア パッケージのバージョンに関連付けられている脆弱性。
3.5(1a)	CSCvj95590	CVE-2019-1667	Cisco HX Data Platform に含まれている **Graphite** インターフェイスのバージョンに関連付けられている脆弱性。
3.5(1a)	CSCvj95580	CVE-2019-1666	Cisco HX Data Platform に含まれている **Graphite** サービスのバージョンに関連付けられている脆弱性。

リリース	不具合 ID	CVE	説明
3.5(1a)	CSCvj95644	—	Cisco HyperFlex ソフトウェアの Web インターフェイスの脆弱性により、認証されていないリモート攻撃者が、クリックジャック攻撃でデバイスの整合性に影響を与える可能性があります。

リリース	不具合 ID	CVE	説明
3.5(1a)	CSCvj81584		Cisco HX Data Platform に含まれている **Apache Tomcat 7.x** バージョンに関連付けられている脆弱性。

リリース	不具合 ID	CVE	説明
		CVE-2010-4172、CVE-2011-1088 CVE-2011-1582、CVE-2009-0783 CVE-2011-5062、CVE-2013-4590 CVE-2016-0762、CVE-2017-5648 CVE-2012-2733、CVE-2014-0099 CVE-2016-5018、CVE-2018-1304 CVE-2014-0230、CVE-2016-6816 CVE-2011-2729、CVE-2013-2071 CVE-2015-5346、CVE-2017-12616 CVE-2009-3555、CVE-2010-4476 CVE-2011-1183、CVE-2011-2204 CVE-2011-3190、CVE-2013-4286 CVE-2015-5351、CVE-2017-12617 CVE-2011-5063、CVE-2014-0050 CVE-2016-0763、CVE-2017-5664 CVE-2012-3439、CVE-2014-0119 CVE-2016-6794、CVE-2018-1305 CVE-2012-4534、CVE-2014-7810 CVE-2016-8735、CVE-2011-2481 CVE-2010-2227、CVE-2011-0013 CVE-2011-1184、CVE-2012-5568 CVE-2015-5174、CVE-2016-8745 CVE-2011-3375、CVE-2013-4322 CVE-2016-0706、CVE-2017-15706 CVE-2011-5064、CVE-2014-0075 CVE-2016-3092、CVE-2017-6056 CVE-2012-3544、CVE-2014-0160 CVE-2016-6796、CVE-2018-8014 CVE-2011-1475、CVE-2005-2090 CVE-2012-4431、CVE-2010-3718	

リリース	不具合 ID	CVE	説明
		CVE-2011-0534、CVE-2012-3546 CVE-2014-0227、CVE-2016-6797 CVE-2011-2526、CVE-2013-2067 CVE-2015-5345、CVE-2017-12615 CVE-2011-3376、CVE-2013-4444 CVE-2016-0714、CVE-2017-5647 CVE-2012-0022、CVE-2014-0096 CVE-2016-3427、CVE-2017-7674	
3.5(1a)	CSCvj99081	CVE-2017-16612 CVE-2018-8012 CVE-2018-10237	Cisco HX Data Platform に含まれている **Apache zookeeper** バージョンに関連付けられている脆弱性。
3.5(1a)	CSCvj95632	CVE-2018-15382	Cisco HyperFlex の脆弱性により、認証されていないリモートの攻撃者が署名付きセッション トークンを生成する可能性があります。
3.5(1a)	CSCvj08923	CVE-2018-6594	Cisco HX Data Platform に含まれている **El Gamal implementation in PyCrypto** に関連する脆弱性。
3.5(1a)	CSCvj08160	CVE-2017-5715 CVE-2017-5753 CVE-2017-5754	Microsoft Hyper-V を使用した Windows Server の HyperFlex コントローラ VM ソフトウェアに関連付けられている脆弱性。
3.5(1a)	CSCvj63266	CVE-2018-1000300 CVE-2018-1000301 CVE-2018-1000303	Cisco HX Data Platform に含まれている **CURL** ソフトウェア パッケージのバージョンに関連付けられている脆弱性。
3.5(1a)	CSCvj61269	CVE-2018-0494	Cisco HX Data Platform に含まれている **GNU Wget** バージョンに関連付けられている脆弱性。
3.5(1a)	CSCvj55521	CVE-2018-8897、CVE-2018-1087 CVE-2018-1000199	Cisco HX Data Platform に含まれている Linux kernel バージョンに関連付けられている脆弱性。

リリース	不具合 ID	CVE	説明
3.5(1a)	CSCvj59134	CVE-2015-9262 CVE-2018-3639 CVE-2017-3640	Cisco HX Data Platform に影響を与える可能性のある **May CPU Side-Channel** に関連付けられている脆弱性。
3.5(1a)	CSCvj42966	—	Data Protection clone api の戻り値に関連付けられている脆弱性。
3.5(1a)	CSCvi88567	CVE-2017-16995 CVE-2017-0861 CVE-2017-1000407 CVE-2017-11472 CVE-2017-15129 CVE-2017-16528	Cisco HX Data Platform に含まれている **Linux kernel** バージョンに関連付けられている脆弱性。
3.5(1a)	CSCvi60720	—	これは、Cisco HyperFlex HX Data Platform のセキュリティの状況と復元力を強化するために、新しいセキュアなコード ベスト プラクティスを採用するための製品の修正です。
3.5(1a)	CSCvi48372	—	Cisco HyperFlex HX Data Platform ソフトウェアの Web ベースの UI の脆弱性により、認証されていないリモートの攻撃者が該当システムの機密情報にアクセスできる可能性があります。
3.5(1a)	CSCvi46951	CVE-2017-7529	Cisco HX Data Platform に含まれている **nginx** ソフトウェア パッケージのバージョンに関連付けられている脆弱性。
3.5(1a)	CSCvi47250	CVE-2011-3389	Cisco HX Data Platform に含まれている **OpenSSL Protocol** ソフトウェア パッケージのバージョンに関連付けられている脆弱性。
3.5(1a)	CSCvi26246	CVE-2016-3092 CVE-2013-0248 CVE-2014-0050	Cisco UCS に含まれる**Apache commons ファイルのアップロード** バージョンに関連付けられている脆弱性。

リリース	不具合 ID	CVE	説明
3.5(1a)	CSCvi50910	CVE-2016-2183	Cisco HX Data Platform に含まれている DES および Triple DES ciphers ソフトウェア パッケージのバージョンに関連付けられている脆弱性。

リリース 3.5(2h) で解決済みの問題

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
HX Connect			
CSCvq89852	HX Connect は、オフラインからオンライン状態に移行した後、標準クラスタとしてストレッチクラスタを報告します。	3.5(2d)	3.5 (2h)
管理			
CSCvs47419	新しい SSL 証明書を再生成し、vCenter で再登録を実行すると、フィンガープリントの不一致が発生する	3.5 (2g)	3.5 (2h)
CSCvr15546	古い HX ソフトウェアでは、自己署名証明書の有効期限は、使用されている証明書 SHA1 で 2019 年 12 月です。これは、クラスタに対する機能上の影響はありません。	3.5 (2g)	3.5 (2h)
CSCvr92004	HXconnect にログインできません。ログイン中にユーザーに認証失敗のエラー メッセージが表示されます。	3.5 (2g)	3.5 (2h)
CSCvs18117	HX Connect ログインでは、レプリケーション情報を取得するときに「アクセス トークンが無効」になると報告しています。	3.5 (2h)	3.5 (2h)
CSCvq65056	アップグレードされたクラスタを 2.6 クラスタから HX 4.0 (1b) に拡張した後、拡張されたノード間で試行されたときに vMotion が失敗します。	3.5 (2g)	3.5 (2h)
CSCvr37488	**ダウングレード エラーが発生**した最後のノードでは、事前アップグレードが失敗します。	3.5 (2g)	3.5 (2h)
CSCvr75305	ノードの追加は断続的にハングします。	3.5(2e)	3.5 (2h)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvs04926	HX 3.5 (2g) クラスタでは、HX Connect を介して UCS サーバ ファームウェアをアップグレードするときに、次のいずれかのエラーが表示されます。 • **getUcsAvailablePackagesLocalizableMessage(Operation did not complete in expected time and maybe executing in the background.,None,None,Operation did not complete in expected time and maybe executing in the background.,ArrayBuffer())** • **getUcsHfpVersionsLocalizableMessage(Operation did not complete in expected time and maybe executing in the background.,None,None,Operation did not complete in expected time and maybe executing in the background.,ArrayBuffer()** このエラーは、4 個以上のノード クラスタで発生する可能性があります。	3.5 (2g)	3.5 (2h)
CSCvr67532	HX240C M5L 仕様シートには、HXDP 4.0 (1a) 以降で PID HX HD12T7KL4KN がサポートされていることが示されています。検証エラーはトリガーされません。「クラスタの作成」の手順で、「Disk prepare failed magnetic disk /dev/sdX"」というエラーが発生して失敗し、ディスクがブラックリスト登録になります。	3.5(2e)	3.5 (2h)
CSCvk25616	ホストが再起動した後、Vcenter/ESXi にデータストアが設置されません。	2.6(1d)	3.5 (2h)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvn07634	クラスタの展開を試行した後、以前に作成されたすべての HX サービス プロファイルとテンプレートには、次の障害が発生します。 説明: ポリシー参照 vconProfileName HyperFlex は名前の付けられたポリシーを解決しません ID: 435052 タイプ: サーバ 原因: named-policy-unresolved 作成日時: 2018-10-28T19:23:20Z コード: F4526901 発生回数 元の重大度 以前の重大度: 警告 最高重大度 さらに、展開前に作成された既存のサービス プロファイルは、保留中の確認応答状態になる可能性があります。	3.5(1a)	3.5 (2h)

リリース 3.5(2g) で解決済みの問題

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvq09098	この障害により、アップグレードまたは HX メンテナンス モードでの操作が失敗することは非常にまれです。この障害は、監視 VM が誤って異なるストレッチ クラスタ間で共有されているか、誤って設定されている (たとえば、IP 再利用/競合) 場合に発生します。	3.5(2f)	3.5 (2g)
CSCvn16282	vCenter サーバがオフラインの場合、HX Connect 経由でストレッチ クラスタにアクセスできません。	3.5(2e)	3.5 (2g)
CSCvq18999	ストレッチ クラスタのフェールオーバー中に、ファイル書き込みエラーが原因でクラスタ リソース マネージャ コンポーネントがダオフラインになることがあります。	3.5 (2d)	3.5 (2g)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvq94105	クラスタがシャットダウンされると、HX-Connect に誤ったステータスが表示されます。	3.5(2f)	3.5 (2g)
CSCvq84869	大規模なクラスタでは、HX Connect でエラー メッセージ「サーバの呼び出しに失敗しました。」が表示されます。。	3.5 (2g)	3.5 (2g)
CSCvq96428	電源がオフになっている監視ノードでは、HX Connect は引き続き監視ノードをオンラインとして表示します。	3.5(2f)	3.5 (2g)
CSCvq06642	ストレッチクラスタで、クラスタ管理 IP がダウンした後、新しいクラスタ管理 IP にアクセスできるようになるまで 10 分以上かかります	3.5(2f)	3.5 (2g)
CSCvq92858	ノードに SED ドライブがある場合、ストレッチクラスタを展開できません。	3.5(2f)	3.5 (2g)
CSCvq94105	クラスタがシャットダウンされると、ストレッチ クラスタのステータスが失われます。クラスタがオンラインに戻るまで、クラスタの状態は正常です。	3.5(2f)	3.5 (2g)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvs28167		3.5(1a)	3.5 (2g)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
	Cisco HyperFlex でノード置換をインストールまたは完了するため、顧客は HX インストーラ OVA（オープン仮想アプライアンス）ファイルをダウンロードする必要があります。ストレッチ クラスタを展開するには、顧客はさらに Witness OVA をダウンロードする必要があります。リリース HX 3.5(2g) の登校前に CCO で投稿されたすべてのコードは、2019 年 11 月 26 日に期限切れになっている証明書を検出しました。Cisco は更新された証明書で、HX リリース 3.5(2e)、3.5.2(f)、3.5.2(g)、4.0(1a)、4.0(1b) に関連付けられている OVA ファイルを再署名および再投稿しました。その他のリリースについては、期限切れの OVA を持つ OVF テンプレートを展開しようとすると、次のエラーメッセージ「OVAパッケージは無効な証明書で署名されています」で失敗します。 **条件**： 顧客は HX 3.5(2e)、3.5.2(f)、3.5.2(g)、4.0(1a) または 4.0(1b) を展開している場合、Cisco は OVA ファイルに再署名して再投稿しており、パッチが適用されたOVAファイルを使用している場合この問題は発生しません。OVA ファイルが修正されたことを示す OVA ファイル名の「p1」サフィックスを探します。 ファイル名の例： Cisco HyperFlex Data Platform ストレッチ クラスタ監視 の HX 3.5(2g) パッチ OVA ファイル: `HyperFlex-Witness-1.0.6 以降 p1 ova` 他の HX リリースで OVA ファイルを使用しているお客様は、次の回避策を参照してください。 **回避策** 影響を受ける OVA ファイルでの展開が失敗した後、続行するには 2 つのオプションがあります（インストーラおよびOVAファイルに適用）。 オプション A：ローカル マニフェスト ファイルを削除します。 マニフェストファイルを検出可能なため、vCenter は証明書の有効性を確認します。 **1.** OVA ファイルをローカル ディレクトリにダウンロードして展開します。 **2.** .mf ファイルを削除します		

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
	3. 残りのファイルを新しいアーカイブに追加して、「.tar」から「.ova」にファイルの拡張子を変更します。 **4.** vCenter で「OVF テンプレートで展開」を使用して新しく OVA ファイルを作成する展開を続行します。vCenter は証明書を所持していないためファイルを表示します。これは予想された動作で、展開は問題なく続行します。 オプション B - ローカル マニフェスト ファイルを削除します。 ovftool で手動展開：VMware の ovftool を使用して、証明書確認をバイパス中に OVA を展開します。ovftool はダウンロードして顧客のコンピュータで実行可能です。ovftool も HX コントローラ VM で事前インストールされます。これはノード交換とクラスタ拡張にも役立ちます。		

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み

	1. skipManifestcheck スイッチを発生させている間、ovftool を使用して OVA ファイルをデータストアに展開します。次に例を示します。
	`root@SpringpathControllerABCDEFGH:~# ovftool --skipManifestCheck -ds=datastore http://<path to ova>/Cisco-HX-Data-Platform-Installer-v3.5.2c-31725-esx.ova vi://root@<IP of management ESX host>/`
	2. OVA を展開し、以前指定した ESXi ホストの vCenter に存在している必要があります。
	3. VM とコンソールの電源をオンにします
	4. root / Cisco123 のユーザー名/パスワードのデフォルトの組み合わせで VM にログインします
	5. **vi /etc/network/eth0.interface** を発行して VM の IP を静的に設定します
	6. 「iface eth0 inet dhcp」を「iface eth0 inet static」に変更します。次のいずれかが独自のラインと指定したタブで必要になります
	`address <desired ip address of installer>`
	`netmask X.X.X.X`
	`gateway X.X.X.X`
	`<esc> :wq`
	7. ファイルを確認および保存後、VM が再起動します。VM は現在希望している IP アドレスでブートされる必要があります
	8. WebGUI 経由での最初のログイン（引き続きデフォルトのユーザー名/パスワードの組み合わせ）は、ユーザーがパスワードを変更します。
	9. パスワードの変更後、ユーザーは希望のインストール/拡大/ノードの交換アクティビティを開始できます。		

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvp86555	3Node と FI で管理される UCS/HX クラスタの間で HyperFlex をインストールする場合。「実行中」と表示されている手順の 1 つは、「監視ノードの IP 到達可能性チェック」です。 理想的には、これはストレッチ クラスタである場合を除き表示されません。一部はスキップされることもありますが、HXインストールのすべてのタスクが表示されます、	3.5 (2g)	3.5 (2g)
CSCvn23213	クラスタのシャットダウン、storfs パニックが検出されました。	3.0(1b)	3.5 (2g)
CSCvp64440	クラスタの作成中に、インストーラで次のエラーが発生します。「クラスタ作成プロセス中に障害が発生しました。ダウンストリームにコンテンツを送信できません」。	3.5 (2f)、4.0 (1a)	3.5 (2g)
CSCvq01556	2.5 より前のリリースから 2.5 リリースへのオンライン アップグレード プロセスでは、メタデータ形式が変更されています。[アップグレード(upgrade)] ウィンドウで切り捨てられたファイルのメタデータは正しく設定されていないため、クラスタがダウンしてしまう可能性があります。	2.1(1b)	3.5 (2g)
CSCvq00899	この障害により、アップグレードまたは HX メンテナンス モードでの操作が失敗することは非常にまれです。この障害は、監視 VM が誤って異なるストレッチ クラスタ間で共有されているか、誤って設定されている (たとえば、IP 再利用/競合) 場合に発生します。	3.5(2f)	3.5 (2g)
CSCvi08375	3 番目のノードのメンテナンス中に、2 つのノードのメモリが不足しています。	3.5 (2b)	3.5 (2g)
CSCvk12766	ホストが再起動した後、Vcenter/ESXi にデータストアが設置されません。	2.6(1d)	3.5 (2g)
CSCvr06389	Stcli コマンドを使用してタイムゾーンを変更した後、日付は常に UTC (デフォルト) になります。	3.5 (2a)、4.0 (1a)	3.5 (2g)
CSCvo38822	コントローラ VM でパッケージを更新する際に、まれなケースでアップグレードが失敗することがあります。	3.5 (2g)、4.0 (1a)	3.5 (2g)
CSCvp17427	Stcli クラスタのストレージ サマリーは、1 つのノードが再起動したときに 16 個以上のノード クラスタに戻るまでに時間がかかります。	3.5 (1a)、4.0 (1a)	3.5 (2g)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvq[illegible]025	HX リリース 3.5 (2b) インストーラは、エラーが表示されないハイパーバイザ設定手順では失敗します。UCSM の設定は完了しますが、ハイパーバイザの設定は開始されないようです。	3.5(2a)	3.5 (2g)
CSCvq[illegible]587	クラスタの拡張が次のエラーで失敗しました。「SP template org-root/hx-cluster/ls-compute-nodes-m5 is not exist」	3.5 (2b)	3.5 (2g)
CSCvq[illegible]383	カーボン キャッシュによるメモリ使用量。	3.5 (2b)	3.5 (2g)
CSCvq[illegible]782	ユーザーは、iscsi などの外部ストレージ用の 5 番目のオクテットで b1 を使用した macpool を作成し、ドキュメントに従って提案された macpool 設定ではない b1 に vmnic9 が割り当てられました。これにより、アップグレードの一環としてカーネル移行手順を実行する際の設定中、管理用に A1 と B1 mac を選択し、サポート対象外になりました。これにより、HX のアップグレードが中断されます。 ドキュメントリンクに従って、外部ストレージのユーザーは、00:25: B5: XX:01:01-63 を使用して macpool を作成するように推奨します。これにより、問題が回避されます。	3.5 (2d)	3.5 (2g)
CSCvq[illegible]706	LAZ は以前は無効になりましたが、停止から回復した後に再度有効になりました。	3.5 (2d)、4.0 (1b)	3.5 (2g)
CSCvq[illegible]825	クラスタの展開中に、次のエラーが表示されて検証に失敗することがあります:「hw_data_disk_same_size。hw_data_disk_same_size_fail」。これは、サイズが変わる UCS のディスク検出 (たとえば、1～500 Mb) が原因で発生します。この差異は、異なるベンダーまたは同じベンダーのディスク間で発生します。	3.5(2e)	3.5 (2g)
CSCvq[illegible]291	lsass がコントローラをドメインに参加させる際にエラーが発生しました。	3.5 (2e)、4.0 (1b)	3.5 (2g)
CSCvr[illegible]429	1 つ以上のノードで、以前の 3.5 (2d) から 3.5 (2d) へのアップグレード中に storfs が開始されない	3.5(2f)	3.5 (2g)
CSCvq[illegible]652	ICMP リダイレクトが有効です	3.5(1a)	3.5 (2g)
CSCvq[illegible]666	アクティビティ下の HX Connect では、ジョブタイプ: encryptionLocal * はステータス:「成功」ですが、ジョブがまだ実行中であるかのように表示されます。進行中のスピン中のアイコンは、その横に RunStep: が表示されます。	3.5(2a)	3.5 (2g)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvq38358	コマンド「asupcli: all post--type alert」および「asupcli--all ping」を実行中の「内部エラー」	3.0(1b)	3.5 (2g)
CSCvq64028	電源がオフになっている監視ノードでは、HX Connect は引き続き監視ノードをオンラインとして表示します。	3.5(2f)	3.5 (2g)
CSCvn23023	レプリケーション ステータスの更新時のセグメンテーション障害による storfs ノード パニック	3.0(1b)	3.5 (2g)
CSCvn44257	一部の API のタイムアウトは、データ サイズが原因で 40 秒以上かかります。	3.5(1a)	3.5 (2g)
CSCvn77294	クラスタのアップグレード中に、「失敗したアップグレードの検証: vCenter 設定の確認」というエラーが表示されます。理由: アップグレードの検証に失敗しました。DRS 障害: 設定されたフェールオーバーを満たすリソースが不足しています。	2.6 (1e)、3.5 (1a)、3.0 (1a)、4.0 (1a)	3.5 (2g)
CSCvn07364	クラスタの展開を試行した後、以前に HX サービス プロファイルとテンプレートを作成した場合は、次の障害が発生します。 説明: ポリシー参照 vconProfileName HyperFlex は名前の付けられたポリシーを解決しません ID: 435052 タイプ: サーバ 原因: named-policy-unresolved 作成日時: 2018-10-28T19:23:20Z コード: F4526901 発生回数 元の重大度 以前の重大度: 警告 最高重大度 さらに、展開前に作成された既存のサービス プロファイルは、保留中の確認応答状態になる可能性があります。	3.5(1a)	3.5 (2g)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvp63828	HX 複製のクリーンアップが次のエラーで失敗しました: 「情報:DR の状態がクリーンではありません」。	3.5(2a)	3.5 (2g)
CSCvq69225	HX クラスタがリリース 3.5 (1a) より前にアップグレードされ、クラスタ展開がそのシーケンスで行われる場合、既存の UCS サーバは「再起動を保留中」になります。これは UCS Manager で表示されます。	3.5 (2d)	3.5 (2g)
CSCvq96605	クラスタの拡張後、一部のデータストアはマウントに失敗し、HX Connect を使用して手動でマウントする必要がありました。	3.5 (2d)	3.5 (2g)
CSCvk13704	ユーザー名に「.」が使用されているため、コンピュータ アカウントの設定に失敗しました。	3.0(1d)	3.5 (2g)
CSCvp48879	HX のインストール/アップグレードの検証は、SAS コントローラがファームウェア 09.00.00.06 上にあるため失敗します。	3.5 (2c)、4.0 (1a)	3.5 (2g)
CSCvp68523	HyperFlex クラスタが ACI ファブリックに展開され、同じブリッジドメイン内に HX 管理および HX ストレージがある場合、誤った HX ストレージ コントローラ インターフェイスからの ARP 応答が表示され、誤った ARP 学習が発生します。ACI ファブリックでは、HX IP の MAC 移動が表示されます。	3.0 (1j)、4.0 (1a)	3.5 (2g)
CSCvq06652	CBT が有効になっている VM でのスナップショットの作成が失敗し、「vmreparent vmkfstools clone1 でエラーが発生しました」というエラーが表示されます。	3.5 (2c)、4.0 (1a)	3.5 (2g)
CSCvn28282	HyperFlex のコントローラ VM は、デフォルトの出荷証明書ではなく、HTTPS 通信用の CA 署名付き証明書を持つように設定できます。ただしアップグレード中は、CA 署名付き証明書がデフォルトの証明書によって上書きされ、ユーザーは CA 署名付き証明書を再度設定するように求められます。	3.5(2a)	3.5 (2g)
CSCvn28207	サポート バンドルは /var/support/ZKTxnlog からファイルを接続しません。	4.0(1a)	3.5 (2g)
CSCvn65578	ノードを削除する手順を実行すると、vCenter の stcli クラスタの再登録は失敗します。	3.5(2a)	3.5 (2g)
CSCvi28305	HX Connect 内のジョブ ([アクティビティ]) を表示するときに Tomcat / HTTP 500 エラーが発生します。	3.5 (2b)	3.5 (2g)

リリース 3.5(2f) で解決済みの問題

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
ストレッチ クラスタ			
CSCvq53058	監視 VM でストレッチ クラスタ サイトのいずれかから高い RTT 時間 (> 50ms) を持つ場合、クラスタがフェールオーバーまたはフェールバック時間回数が非常に多くなる可能性がある大幅なトランザクション負荷が発生する可能性があります。	3.5(1a)	3.5 (2f)
CSCvq58829	サイトのフェイルオーバーの際、クラスタのメタデータのレプリケーションからの応答が遅いため、クラスタで APD が発生します。	3.5(1a)	3.5 (2f)
CSCvq17778	1 つのサイトでバックツーバック フェールオーバーが発生すると、クラスタが障害を検出するため zookeepr がオフラインになります。	3.5(2d)	3.5 (2f)
CSCvr92004	HX Connect にログインできません。ログイン中にユーザーに認証失敗のエラー メッセージが表示されます。	3.5 (2f)	3.5 (2f)
CSCvq89852	HX Connect は、オフラインからオンライン状態に移行した後、標準クラスタとしてストレッチ クラスタを報告します。	3.5(2a)	3.5 (2f)
管理			

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvs28167		3.5(1a)	3.5 (2f)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み

	Cisco HyperFlex でノード交換をインストールまたは完了するため、顧客はHXインストーラOVA（オープン仮想アプライアンス）ファイルをダウンロードする必要があります。ストレッチ クラスタを展開するには、顧客はさらに Witness OVA をダウンロードする必要があります。リリース HX 3.5(2g) の登校前に CCO で投稿されたすべてのコードは、2019 年 11 月 26 日に期限切れになっている証明書を検出しました。Cisco は更新された証明書で、HX リリース 3.5(2e)、3.5.2(f)、3.5.2(g)、4.0(1a)、4.0(1b) に関連付けられている OVA ファイルを再署名および再投稿しました。その他のリリースについては、期限切れの OVA を持つ OVF テンプレートを展開しようとすると、次のエラー メッセージ「OVA パッケージは無効な証明書で署名されています」で失敗します。
	条件：
	顧客は HX 3.5(2e)、3.5.2(f)、3.5.2(g)、4.0(1a) または 4.0(1b) を展開している場合、Cisco は OVA ファイルに再署名して再投稿しており、パッチが適用された OVA ファイルを使用している場合この問題は発生しません。OVA ファイルが修正されたことを示す OVA ファイル名の「p1」サフィックスを探します。
	ファイル名の例：
	VMware ESXi 用 Cisco HyperFlex Data Platform インストーラ用の HX 3.5(2f) パッチ OVA ファイル:
	`Cisco-hx-data-platform-installer-v1.7.1-14786.ova 3.5.2 f-31787p1-esx`
	Cisco HyperFlex Data Platform ストレッチ クラスタ Witness：
	`HyperFlex-Witness-1.0.6 以降 p1 ova`
	他の HX リリースで OVA ファイルを使用しているお客様は、次の回避策を参照してください。
	回避策
	影響を受ける OVA ファイルでの展開が失敗した		

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
	後、続行するには 2 つのオプションがあります（インストーラおよびOVA ファイルに適用）。 オプション A：ローカル マニフェスト ファイルを削除します。 マニフェストファイルを検出可能なため、vCenter は証明書の有効性を確認します。 **1.** OVA ファイルをローカル ディレクトリにダウンロードして展開します。 **2.** .mf ファイルを削除します **3.** 残りのファイルを新しいアーカイブに追加して、「.tar」から「.ova」にファイルの拡張子を変更します。 **4.** vCenter で「OVF テンプレートで展開」を使用して新しく OVA ファイルを作成する展開を続行します。vCenter は証明書を所持していないためファイルを表示します。これは予想された動作で、展開は問題なく続行します。 オプション B - ローカル マニフェスト ファイルを削除します。 ovftool で手動展開：VMware の ovftool を使用して、証明書確認をバイパス中に OVA を展開します。ovftoolはダウンロードして顧客のコンピュータで実行可能です。ovftool も HX コントローラ VM で事前インストールされます。これはノード交換とクラスタ拡張にも役立ちます。		

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み

	1. skipManifestcheck スイッチを発生させている間、ovftool を使用して OVA ファイルをデータストアに展開します。次に例を示します。
	`root@SpringpathControllerABCDEFGH:~# ovftool --skipManifestCheck -ds=datastore http://<path to ova>/Cisco-HX-Data-Platform-Installer-v3.5.2c-31725-esx.ova vi://root@<IP of management ESX host>/`
	2. OVA を展開し、以前指定した ESXi ホストの vCenter に存在している必要があります。
	3. VM とコンソールの電源をオンにします
	4. root / Cisco123 のユーザー名/パスワードのデフォルトの組み合わせで VM にログインします
	5. **vi /etc/network/eth0.interface** を発行して VM の IP を静的に設定します
	6. 「iface eth0 inet dhcp」を「iface eth0 inet static」に変更します。次のいずれかが独自のラインと指定したタブで必要になります
	`address <desired ip address of installer>`
	`netmask X.X.X.X`
	`gateway X.X.X.X`
	`<esc> :wq`
	7. ファイルを確認および保存後、VM が再起動します。VM は現在希望している IP アドレスでブートされる必要があります
	8. WebGUI 経由での最初のログイン（引き続きデフォルトのユーザー名/パスワードの組み合わせ）は、ユーザーがパスワードを変更します。
	9. パスワードの変更後、ユーザーは希望のインストール/拡大/ノードの交換アクティビティを開始できます。		

CSCvo39912	UCSM のみのアップグレードは、HX のアップグレードの一環として停止します。	3.5(2d)	3.5 (2f)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvq91142	Hyper-V: クラスタがオフライン/APD を示します。NS マスター所有権の転送中のセグメント障害。	3.5(2e)	3.5 (2f)
CSCvn67512	SED データ SSD は、ファームウェアのアップグレード後に電源がオフになることがあります。	3.0(1d)	3.5 (2f)
CSCvq17778	1 つのサイトでバックツーバック フェールオーバーが発生すると、クラスタが障害を検出するため zookeepr がダウンします。	3.5(2d)	3.5 (2f)
CSCvq89852	HX Connect は、オフラインからオンライン状態に移行した後、標準クラスタとしてストレッチクラスタを報告します。	3.5(2a)	3.5 (2f)
CSCvq53058, CSCvq58829	ストレッチ クラスタ サイトのいずれかに対して高い RTT 時間 (> 50ms) を持つ監視 VM の場合、フェールオーバーまたはフェールバックが影響を受ける可能性がある大幅なトランザクション負荷が発生する可能性があります。	3.0(1i) 3.5(1a)	3.5 (2f)

リリース 3.5(2e) で解決済みの問題

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
ストレッチ クラスタ			
CSCvq18919	ストレッチ クラスタのフェールオーバー中に、ファイル書き込みエラーが原因でクラスタ リソース マネージャ コンポーネントがダウンすることがあります。	3.5 (2d)	3.5(2e)
管理			

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvs28167		3.5(1a)	3.5(2e)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み

	Cisco HyperFlex でノード交換をインストールまたは完了するため、顧客はHXインストーラOVA（オープン仮想アプライアンス）ファイルをダウンロードする必要があります。ストレッチ クラスタを展開するには、顧客はさらに Witness OVA をダウンロードする必要があります。リリース HX 3.5(2g) の登校前に CCO で投稿されたすべてのコードは、2019 年 11 月 26 日に期限切れになっている証明書を検出しました。Cisco は更新された証明書で、HX リリース 3.5(2e)、3.5.2(f)、3.5.2(g)、4.0(1a)、4.0(1b) に関連付けられている OVA ファイルを再署名および再投稿しました。その他のリリースについては、期限切れの OVA を持つ OVF テンプレートを展開しようとすると、次のエラー メッセージ「OVA パッケージは無効な証明書で署名されています」で失敗します。
	条件：
	顧客は HX 3.5(2e)、3.5.2(f)、3.5.2(g)、4.0(1a) または 4.0(1b) を展開している場合、Cisco は OVA ファイルに再署名して再投稿しており、パッチが適用された OVA ファイルを使用している場合この問題は発生しません。OVA ファイルが修正されたことを示す OVA ファイル名の「p1」サフィックスを探します。
	ファイル名の例：
	VMware ESXi 用 Cisco HyperFlex Data Platform インストーラ用の HX 3.5(2e) パッチ OVA ファイル:
	`Cisco-hx-data-platform-installer-v1.7.1-14786.ova 3.5.2 e-31762p1-esx`
	Cisco HyperFlex Data Platform ストレッチ クラスタ Witness：
	`HyperFlex-Witness-1.0.4 p1 ova`
	他の HX リリースで OVA ファイルを使用しているお客様は、次の回避策を参照してください。
	回避策
	影響を受ける OVA ファイルでの展開が失敗した		

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
	後、続行するには 2 つのオプションがあります（インストーラおよびOVA ファイルに適用）。 オプション A：ローカル マニフェスト ファイルを削除します。 マニフェストファイルを検出可能なため、vCenter は証明書の有効性を確認します。 **1.** OVA ファイルをローカル ディレクトリにダウンロードして展開します。 **2.** .mf ファイルを削除します **3.** 残りのファイルを新しいアーカイブに追加して、「.tar」から「.ova」にファイルの拡張子を変更します。 **4.** vCenter で「OVF テンプレートで展開」を使用して新しく OVA ファイルを作成する展開を続行します。vCenter は証明書を所持していないためファイルを表示します。これは予想された動作で、展開は問題なく続行します。 オプション B - ローカル マニフェスト ファイルを削除します。 ovftool で手動展開：VMware の ovftool を使用して、証明書確認をバイパス中に OVA を展開します。ovftoolはダウンロードして顧客のコンピュータで実行可能です。ovftool も HX コントローラ VM で事前インストールされます。これはノード交換とクラスタ拡張にも役立ちます。		

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み

	1. skipManifestcheck スイッチを発生させている間、ovftool を使用して OVA ファイルをデータストアに展開します。次に例を示します。
	`root@SpringpathControllerABCDEFGH:~# ovftool --skipManifestCheck -ds=datastore http://<path to ova>/Cisco-HX-Data-Platform-Installer-v3.5.2c-31725-esx.ova vi://root@<IP of management ESX host>/`
	2. OVA を展開し、以前指定した ESXi ホストの vCenter に存在している必要があります。
	3. VM とコンソールの電源をオンにします
	4. root / Cisco123 のユーザー名/パスワードのデフォルトの組み合わせで VM にログインします
	5. **vi /etc/network/eth0.interface** を発行して VM の IP を静的に設定します
	6. 「iface eth0 inet dhcp」を「iface eth0 inet static」に変更します。次のいずれかが独自のラインと指定したタブで必要になります
	`address <desired ip address of installer>`
	`netmask X.X.X.X`
	`gateway X.X.X.X`
	`<esc> :wq`
	7. ファイルを確認および保存後、VM が再起動します。VM は現在希望している IP アドレスでブートされる必要があります
	8. WebGUI 経由での最初のログイン（引き続きデフォルトのユーザー名/パスワードの組み合わせ）は、ユーザーがパスワードを変更します。
	9. パスワードの変更後、ユーザーは希望のインストール/拡大/ノードの交換アクティビティを開始できます。		

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvq18771 CSCvq02860	HX SD16T123X-EP キャッシング ドライブには永続化ロールが割り当てられ、HX SD960G61X-EV はキャッシュ ドライブとして認識されます。	3.5 (2c)	3.5(2e)
CSCvc38351	インストーラで誤った MTU サイズが選択されているため、クラスタの拡張に失敗しました。	1.8(1c)	3.5(2e)
CSCvq18919	ストレッチ クラスタのフェールオーバー中は、エポック ファイルの書き込みエラーが原因で zookeeper がダウンします。	3.5 (2d)	3.5(2e)
CSCvp29431	リリース 3.0 (1c) を実行している HX クラスタでは、すべてのパスがダウン (APD) 状態になり、VM にアクセスできなくなりました	3.0(1c)	3.5(2e)
CSCvq13099	HyperFlex post_install .py スクリプトが、実行中のヘルス チェック手順で間違ったメッセージを生成します。	3.5 (2d)	3.5(2e)

リリース 3.5(2d) で解決済みの問題

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
管理			
CSCvp40474	クラスタが正常な場合でも、複数の Hyper-V Hyperflex ホストがデータストアにアクセスできません。	3.5(2a)	3.5 (2d)
CSCvp90129	ストレッチ クラスタでは、クラスタで障害が発生した場合、または再調整が発生してメンテナンス ウィンドウが表示された場合に、一部のノードでパニックが発生する可能性があります。	3.5 (2c)	3.5 (2d)
CSCvm58031	Tomcat および Nginx ログは、リリース 3.5 の HX Connect を介して生成されたサポート バンドルでは収集されません。	3.5(1a)	3.5 (2d)

リリース 3.5(2c) で解決済みの問題

HX 3.5 (2c) は延期されていることに注意してください。

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
管理			
CSCvo36198	アラーム、仮想マシン、またはイベントのリストを取得すると、「仮想センター到達不能」または「リソース情報を更新できません」というメッセージが断続的に表示されます。	3.5(1a)	3.5 (2c)
CSCvp58804	HX Connect からサポート バンドルを生成すると、メモリのリークが発生し、メモリ不足の問題によりクラスタの健全性が低下する可能性があります。	3.5(2a)	3.5 (2c)
CSCvo75522	1 つのサイトでデータ ネットワークを失うと、クラスタ全体にアクセスできなくなります。詳細については、『*Cisco HyperFlex Systems* ストレッチ クラスタ ガイド リリース*3.5*』の「インストール前チェック リスト」および「サイト間フェールオーバーのトラブルシューティング」の項を参照してください。	3.5(2a)	3.5 (2c)
CSCvp32000	ノードの電源停止時には、キャッシュの再配布が最適に実行される可能性があります。	3.5(1a)	3.5 (2c)
CSCvk46364	ディスク ロールは、HyperFlex リリース 2.6 (1b) のキャッシュ ディスクと容量ディスク間で交換されました。	2.6(1b)	3.5 (2c)
CSCvo67207	一部の VM の HA は、サイト間のネットワーク条件では最適でない場合があります。	3.5(2a)	3.5 (2c)
CSCvp42925	HX インストーラからの変更により、すべての HX vNIC で LLDP が無効になる原因となっています。	3.5(1a)	3.5 (2c)
CSCvp41404	ストレッチ クラスタ展開でのノード障害およびサイト障害に関する不適切な領域レポート。	3.5 (2c)	3.5 (2c)

リリース 3.5(2b) で解決済みの問題

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
ESXi、インストール、アップグレード、展開、管理			

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvh08977	HX Connect または外部バックアップ ベンダーを介して、Quiesced オプションで HX スナップショットが取得されると、仮想センター VM スナップショット マネージャにはスナップショットが休止中として表示されません。Hyperflex の実装では、VMware API で認識されていないアウトオブバンド休止が使用されます。HX スナップショット API 要求が成功した場合は、スナップショットが正常に停止していると考えるのが妥当です。 HX 休止スナップショットに依存している場合は、バックアップベンダーに確認してください。	3.0(1c)	3.5 (2b)
CSCvn59619	HX Quiesced スナップショットが取得されると、返されるスナップショットの ID が特定の状況下で正しくない場合があり、バックアップベンダーと HX スナップショットの統合に影響を与える可能性があります。 HX 休止スナップショットに依存している場合は、バックアップベンダーに確認してください。	3.0(1c)	3.5 (2b)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvk17250	HX ドライブ PID HX には、異なるセクター サイズ (8K と 4K) を持つ 2 つの異なるモデルがあります。リリース 3.5.2a またはそれ以下で異なるドライブ バージョンが一緒に使用されると、Hyperflex ノードでパニックが発生する可能性があります。 /Var/log/springpath/debug-storfs.log には次のエラーメッセージが表示されます。 `storfs[1437:1538]: SUPPORT: PANIC: PANIC ON CONDITION (trustSegmentMetaData == true && CError_Ok(err) == false): PackingError at file /opt/git/cypress/src/modules/kvstore/kvindex.c line 1265` これにより、クラスタが回復不能になる可能性があります。 上記のドライブを使用する設定の HXDP の最小バージョンは 3.5 (2b) 以降です。既存のクラスタに新しいノードを追加するか、既存のクラスターに新しいドライブを追加する前に、このドライブで稼働している既存のクラスタを HXDP バージョン 3.5 (2b) 以降にアップグレードする必要があります。	3.0(1d)	3.5 (2b) 以降
CSCvn73127	ローカルデータストアが ESXi で検索されると、Kernel の移行に失敗します。	3.0(1d)	3.5 (2b)
CSCvn37805	HX 複製クリーンアップが完了できず、Zookeeper の複製設定が古くなっています。	2.5(1a)	3.5 (2b)

CSCvn17787	クラスタの作成/クラスタの拡張ワークフローは、検証手順で次のエラー メッセージが表示され停止します。
	`FIRMWARE-Check UCSC-SAS-M5HD`
	`FIRMWARE-Check UCSC-SAS-M5HD : Required: 00.00.00.29,00.00.00.32,00.00.00.35,00.00.00.50, Found: 00.00.00.58;`
	必要なアクション: 必須バージョンにコントローラ ファームウェアを更新する
		3.5(2a)	3.5 (2b)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvm53972	障害が発生したディスクの自動ソフトウェア修復中に、リリース 2.6 (1x) で実行されているクラスタではすべてのパスがダウンしている可能性があります。	2.6(1b)	3.5 (2b)
Hyper-V			
CSCvn28721	クラスタ拡張は、エラーコード「500-操作のタイムアウト」で失敗する可能性があります。	3.5(2a)	3.5 (2b)
CSCvh80044	HX Connect UI を使用すると、異なる場合に限り、可能性のある既存のデータストア名を複製することで、データストアを作成できます。たとえば、Ds3、ds3、dS3 は有効なデータストアとして許可されます。	3.0(1a)	3.5 (2b)
CSCvn60486	Hyper-V クラスタをアップグレードするとき、**stUpgradeService** および Zookeeper サーバ間でレアな競合状態のアカウント上では、アップグレード オーケストレーションはアップグレード検証エラーをスローし、アップグレード プロセスが中断します。	3.5(2a)	3.5 (2b)
CSCvn54300	アップグレード時に、ユーザーの vSwitch に作成されたチームで VLAN を削除します。 新規インストール時には、複数の Vlan が入力されていても、1つの VLAN タグだけが vSwitch とチームに設定されます。	3.5(2a)	3.5 (2b)

リリース 3.5(2a) で解決済みの問題

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvn59508	以前のリリースからリリース 3.5 (1a) にアップグレードすると、ノード サイト マップに関連する CRM エントリが欠落しているためクラスタの拡張が失敗することがあります。	3.5(1a)	3.5(2a)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvn52412	HX 用 Kubernetes を導入する場合、ユーザーがすべてのノードを有効にすると (**[Settings (設定)]** > **[Integrations (統合)]** > **[Kubernetes]** > **[Enable all nodes (すべてのノードを有効化)]**] を選択)、ESXi ホストは次の条件下でデータストアにアクセスできません。 • HX クラスタは、Intersight を使用して展開された場合。または、 • HX クラスタは、すべての ESXi ホスト iscsi vmk に設定されたストレージ CMIP 値を使用して手動で展開されます。	3.5(1a)	3.5(2a)
CSCvn07634	最初にリリース 3.5 (1a) より前に最初に展開されたクラスタで、リリース 3.5 (1a) ノード展開を試行すると、vCON ポリシーの参照エラーがトリガされます。さらに、展開前に作成された既存のサービス プロファイルは、保留中の確認応答状態になる可能性があります。	3.5(1a)	3.5(2a)
CSCvm97558	メモリ不足状態が原因で、コントローラ VM が再起動します。	3.0(1c)	3.5(2a)
CSCvm66552	ドライブ ファームウェアのバグが原因で、複数の 3.8 TB SED SSD ドライブに障害が発生すると、HX クラスタがオフラインになる可能性があります。詳細については、関連するソフトウェア アドバイザリを参照してください。	3.0(1c)	3.5(2a)
CSCvm53972	障害が発生したディスクの自動ソフトウェア修復中に、I/IO サブシステムでディスクに対する書き込みコマンドがハングします。これにより、他のノードが数分間このノードと通信できなくなります。	2.6(1b)	3.5(2a)
CSCvk46364	容量ディスクが最初に挿入され、キャッシングディスクが次に挿入される場合、2 個のディスクが交換されると (キャッシングディスクおよび別の容量ディスク)、ノードがシャットダウンします。	2.6(1b)	3.5(2a)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvk46179, CSCvm47257	大規模なクラスタでは、「サーバ コーるに失敗しました」というエラーが HX Connect に表示されることがあります。	3.5(1a)	3.5(2a)
CSCvk09073	リリース 2.x から 3.x へのアップグレード中に、アップグレードで障害が発生した場合は、クラスタ管理 IP アドレスに到達不能になる可能性があります(コントローラ VM のいずれにも存在しません)。	3.0(1a)	3.5(2a)
CSCvh04307	ストレージ コントローラ VM へのソフトウェア パッケージのインストールは、次のエラーで失敗します。 システムにロックされたドライブがあります。ロック解除して再度展開してください。 さらに、リリース 2.6 (1e) から 3.0 (1c) にアップグレードすると、次の条件が表示されます。 • アップグレードは、クラスタの準備状況を確認するときに長時間スタックします。 • Stcli クラスタ情報は SED ディスクが使用不可であることを示しているため、クラスタは正常な状態に回復できません。	3.0(1a)	3.5(2a)
Hyper-V			
CSCvm59573	場合によっては、インストール プロセスでハイパーバイザの設定中に Hyper-v OS のインストールが失敗することがあります。	3.5(1a)	3.5(2a)

リリース 3.5(1a) で解決済みの問題

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
ESXi、インストール、アップグレード、展開、管理			

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvk62990	ESXi バージョン 6.0 を搭載した M5 サーバでの HX 展開入では、インストールまたはアップグレードのワークフロー中に PSOD が発生する可能性があります。	2.6(1a)	3.5(1a)
CSCvk39622	HX Connect では、「クラスタ内の 1 個以上のモードでロックダウンモードが有効になっています」メッセージが表示されたアラームが表示されます。さらに、アラームは手動で緑色にリセットされます。	3.0(1d)	3.5(1a)
CSCvj90575	Smartmons ツールは、Samsung SATA ドライブに **Reallocated_Sector_Ct**) 値をレポートします (ディスク モデル **MZ7LM480HMHQ**)。	3.0(1a)	3.5(1a)
CSCvi34303	HX Connect UI は、表が **.csv** 形式でエクスポートされ、Excel で開いたときにエラーを表示します。	3.0(1a)	3.5(1a)
Hyper-V			
CSCvm53679	HX インストーラが失敗し、**HXBootstrap.log** には次のメッセージが含まれています。 **「Active Directory Web サービスが実行されているデフォルト サーバを見つけることができません。」**	3.0(1e)	3.5(1a)
CSCvm42278	データストア アクセスは、頻繁なアラートにつながります。さらに、SMB SCVM クライアントのログ ファイル (/var/log/springpath/debug-smbscvmclient.log) には、そのコントローラがホストされているホストのホスト データ IP アドレスに関する次のようなメッセージが表示されます。	3.0(1e)	3.5(1a)
CSCvk18743	ストレージ コントローラ VM は長時間にわたってダウンしているため、VM の電源がオフになる可能性があります。	3.0(1b)	3.5(1a)

リリース 3.5(2h) で未解決の問題

不具合 ID	症状	回避策	リリースで検出された障害

CSCvv21905	HX Connect UI の暗号化ページに UCSM 読み取り専用ユーザーが存在しないというエラーが発生します。その後、クレデンシャルを使用して UCSM を認証するときに、無効な CSRF トークンのエラーがスローされます。	次のコマンドを実行します。
		`stcli security encryption ucsm-ro-user create --hostname <FI-IP> --username <FI-user-name> --password <FI-password>`
		`stcli security encryption ucsm-ro-user show`
			3.5(1a)

リリース 3.5(2g) で未解決の問題

不具合 ID	症状	回避策	リリースで検出された障害

CSCvv21905	HX Connect UI の暗号化ページに UCSM 読み取り専用ユーザーが存在しないというエラーが発生しました。その後、クレデンシャルを使用して UCSM を認証すると、無効な CSRF トークンのエラーがスローされます。	次のコマンドを実行します。
		`stcli security encryption ucsm-ro-user create --hostname <FI-IP> --username <FI-user-name> --password <FI-password>`
		`stcli security encryption ucsm-ro-user show`
			3.5(1a)

CSCvs35307	HX 2.1 x 以下から HX 3.5 (2g) へのブートストラップに失敗し、互換性のない Java バージョンがあります。	修正を実行するためのサービス リクエストを作成してから、HX 3.5 (2f) にアップグレードしてください。	3.5 (2g)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvs02466	サーバー ファームウェア 4.0(4e) へのアップグレード後、M.2 ブート ディスクがサーバー インベントリに表示されません。その結果、サーバは M.2 ディスクにインストールされている OS で起動できません。この問題は、サーバーの再認識およびコミッション解除と再受信確認後も発生します。	1. サーバーをコミッション解除する 2. サーバーの電源ドレイン-サーバー背面にある両方の電源コードを 10 秒間取り外してから、電源コードを再挿入します。 3. サーバーを再コミッションします。	4.0 (4e)
CSCvq38279	Hyper-V: 複製した DC が使用されたとき、インストール時に Windows フェールオーバー クラスタが正常に作成されませんでした。	クラスタをクリーンアップして、フェールオーバー クラスタを再作成します。HX ストレージ クラスタに触れる必要はありません。	3.5(2e)
CSCvq65830	Hyper-V: あるホストから別のホストに移行した後、VM が破損しています。	NA	3.5(2e)

リリース 3.5(2f) で未解決の問題

不具合 ID	症状	回避策	リリースで検出された障害

CSCvv21905	HX Connect UI の暗号化ページに UCSM 読み取り専用ユーザーが存在しないというエラーが発生しました。その後、クレデンシャルを使用して UCSM を認証すると、無効な CSRF トークンのエラーがスローされます。	次のコマンドを実行します。
		`stcli security encryption ucsm-ro-user create --hostname <FI-IP> --username <FI-user-name> --password <FI-password>`
		`stcli security encryption ucsm-ro-user show`
			3.5(1a)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvq64208	電源がオフになっている監視ノードでは、HX Connect は引き続き監視ノードをオンラインとして表示します。	ログアウトしてから再度ログインし、最新の監視ステータスを取得します。	3.5 (2f)
CSCvq94462	複数の DNS サーバによって拡張検証エラーが発生しました。stcli を検証します。	NA	3.5(2d)
CSCvq96085	クラスタの拡張後、一部のデータストアはマウントに失敗し、HX Connect を使用して手動でマウントする必要がありました。	マウントに失敗したデータストアを手動でマウントします。	3.5 (2d)

リリース 3.5(2e) で未解決の問題

不具合 ID	症状	回避策	リリースで検出された障害

CSCvv21905	HX Connect UI の暗号化ページに UCSM 読み取り専用ユーザーが存在しないというエラーが発生しました。その後、クレデンシャルを使用して UCSM を認証すると、無効な CSRF トークンのエラーがスローされます。	次のコマンドを実行します。
		`stcli security encryption ucsm-ro-user create --hostname <FI-IP> --username <FI-user-name> --password <FI-password>`
		`stcli security encryption ucsm-ro-user show`
			3.5(1a)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvq60925	拡張によってリリース3.5より前の HyperFlex リリースから、リリース3.5またはそれ以降にアップグレードすると、サーバのリブートがトリガされます。	この問題には複数の回避策があります。次のいずれかを実行できます。 1. HyperFlex リリース 3.0 または 2.6 ～ HX Connect から 3.5 への結合アップグレード (HXDP + サーバ ファームウェア更新) を実行します。 2. HXDP を 3.5 リリースにアップグレードした後、HX Connect から UCS サーバファームウェアのアップグレードを実行します。 3. UCS Manager から、サーバのローリング リブートを実行します。各サーバをリブートする前に、HX Connect からクラスタが正常であることを確認してください。	3.5(2e) 3.5 (2d)
CSCvq49412	クラスタでは、使用されているストレージ容量と、監視ノードへのリンクの遅延によって、サイトのフェールオーバー中に一時的なすべてのパスダウン (APD) 状態を確認できるがあります。	リリース 3.5 (2e) ではなし。ただし APD が発生した場合、状態が回復し、しばらくしてから IO が再開されます。APD を回避するための修正は、今後のリリースで利用可能になります。	3.5(2a)
CSCvq54992	EMC リカバリ ポイントの HXDP サポート: 手動による回避が必要です。	Scvmclient VIB を手動でインストール/アップグレードし、それが現在の HX Data Platform バージョンと一致していることを確認します。	3.5 (2b)
CSCvm99150	1 個の ESX ノードで MTU を 9000 から 1500 に変更すると、すべてのノードで storfs プロセスが再起動します。	**1.** 実行中のクラスタでは、ESX レベルで MTU を変更しないでください。 **2.** 元の値に戻します。	3.5(1a) 3.5(2a)
CSCvq17778	複数のサイトのフェールオーバーが発生するまれなケースでは、CRM リーダーの選出が失敗します。	すべてのコントローラを再起動して回復します。	3.5 (2d)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvn73383	クラスタがメンテナンスのためにシャットダウンされています。ただし、ノードが再起動されたとき、既存の障害が原因で、1 個のノードのディスクがパブリッシュされませんでした。クラスタはオンラインに復帰できませんでした。	この回避策は、すべてのディスクがパブリッシュされ、再びクラスタを再起動するように、そのノードのディスク障害を修正することです。	3.0(1c)
CSCvo70650	DR 複製が設定されているノードでは、クラスタの展開が失敗します。DR 複製が設定されている HX クラスタが展開されている場合は、管理 VLAN 情報ではなく、複製 VLAN 情報でインストーラ UI がプルされます。その情報を正しい管理 VLAN id と名前に変更しても、ESXi の複製 VLAN の VLAN でノードが設定されているため、機能しないように見えます。これにより、ホスト到達不能エラーによるノード追加の障害が発生します。	複製 VLAN が使用されていることを確認する必要があります。KVM にログインし、管理 VLAN を正しい VLAN ID に更新して、クラスタの展開を再試行します。	3.5(2a)
CSCvq11456	HyperFlex stcli クラスタ情報に UCSM VIP アドレスが表示されません。	NA	3.5(2d)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvq22844	保留中のアクティビティを確認せず、UCSM でサーバが再起動し、HX Connect進捗フローにメッセージを追加します。 HX Connect は、制御されたローリング サーバのアップグレードをバックグラウンドで実行しています。	NA	3.5(2d)
CSCvn11045	ノードを再起動すると、HX ノードはクラッシュし続けます。	次のコマンドを実行して、インターフェイスがアップしているかどうか、およびループバックインターフェイスに ping を実行できるかどうかを確認します。 **ifconfig –a** **ping 127.0.0.1** : ループバック インターフェイスの起動 **ip link set lo up** : サービスが実行中かどうかをチェック **status scvmclient** **status storfs** - 下のサービスの開始 **start scvmclient** **start storfs**	3.5(1a) 3.0(1e)

リリース 3.5(2d) で未解決の問題

不具合 ID	症状	回避策	リリースで検出された障害

CSCvv21905	HX Connect UI の暗号化ページに UCSM 読み取り専用ユーザーが存在しないというエラーが発生しました。その後、クレデンシャルを使用して UCSM を認証すると、無効な CSRF トークンのエラーがスローされます。	次のコマンドを実行します。
		`stcli security encryption ucsm-ro-user create --hostname <FI-IP> --username <FI-user-name> --password <FI-password>`
		`stcli security encryption ucsm-ro-user show`
			3.5(1a)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvs28167			2.6(1e)

不具合 ID	症状	回避策	リリースで検出された障害
	Cisco HyperFlex でノード置換をインストールまたは完了するため、顧客は HX インストーラ OVA（オープン仮想アプライアンス）ファイルをダウンロードする必要があります。ストレッチクラスタを展開するには、顧客はさらに Witness OVA をダウンロードする必要があります。リリース HX 3.5(2g) の登校前に CCO で投稿されたすべてのコードは、2019 年 11 月 26 日に期限切れになっている証明書を検出しました。Cisco は更新された証明書で、HX リリース 3.5(2e)、3.5.2(f)、3.5.2(g)、4.0(1a)、4.0(1b) に関連付けられている OVA ファイルを再署名および再投稿しました。その他のリリースについては、期限	影響を受ける OVA ファイルでの展開が失敗した後、続行するには2つのオプションがあります（インストーラおよび OVA ファイルに適用）。 オプション A：ローカル マニフェスト ファイルを削除します。 マニフェスト ファイルを検出可能なため、vCenter は証明書の有効性を確認します。 1. OVA ファイルをローカル ディレクトリにダウンロードして展開します。 2. .mf ファイルを削除します 3. 残りのファイルを新しいアーカイブに追加して、「.tar」から「.ova」にファイルの拡張子を変更します。 4. vCenter で「OVF テンプレートで展開」を使用して新しく OVA ファイルを作成する展開を続行します。vCenter は証明書を所持していないためファイルを表示します。これは予想された動作で、展開は問題なく続行します。 オプション B - ローカル マニフェスト ファイルを削除します。 ovftool で手動展開：VMware の ovftool を使用して、証明書確認をバイパス中に OVA を展開します。ovftool はダウンロードして顧客のコンピュータで実行可能です。ovftool も HX コントローラ VM で事前インストールされます。これはノード交換とクラスタ拡張にも役立ちます。 1. skipManifestcheck スイッチを発生させている間、ovftool を使用して OVA ファイルをデータストアに展開します。次に例を示します。 `root@SpringpathControllerABCDEFGH:~# ovftool --skipManifestCheck -ds=datastore http://<path to ova>/Cisco-HX-Data-Platform-Installer-v3.5.2c-31725-esx.ova vi://root@<IP of management ESX`	

不具合 ID	症状	回避策	リリースで検出された障害

	切れの OVA を持つ OVF テンプレートを展開しようとすると、次のエラーメッセージ「OVA パッケージは無効な証明書で署名されています」で失敗します。	host>/
		2. OVA を展開し、以前指定した ESXi ホストの vCenter に存在している必要があります。
		3. VM とコンソールの電源をオンにします
		4. root / Cisco123 のユーザー名/パスワードのデフォルトの組み合わせで VM にログインします
		5. **vi /etc/network/eth0.interface** を発行して VM の IP を静的に設定します
		6. 「iface eth0 inet dhcp」を「iface eth0 inet static」に変更します。次のいずれかが独自のラインと指定したタブで必要になります
		`address <desired ip address of installer>`
		`netmask X.X.X.X`
		`gateway X.X.X.X`
		`<esc> :wq`
		7. ファイルを確認および保存後、VM が再起動します。VM は現在希望している IP アドレスでブートされる必要があります
		8. WebGUI 経由での最初のログイン（引き続きデフォルトのユーザー名/パスワードの組み合わせ）は、ユーザーがパスワードを変更します。
		9. パスワードの変更後、ユーザーは希望のインストール/拡大/ノードの交換アクティビティを開始できます。	

CSCvp78288	クラスタ I/O へディスクを追加するときに 96 秒間凍結する場合。	介入は必要ありません。クラスタは自身で回復します。	3.5 (1i)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvp88990	HyperFlex のアップグレードは、SCVM が ESXi にログインできないために失敗します。	ESXi ホスト上の承認済みキーファイルに SSH 公開キーをコピーします。 SCVM の場合: **cat/etc/ssh/ssh_host_rsa_key.pub** ** 単一の行のすべての出力をコピーします。ターミナル ウィンドウで新しい行にホスト名が出力されていない場合でも、キーの末尾を超えるものはコピーしないでください。 前の出力から ESXi の承認済みキー ファイルにキーを入力します。 **vi/etc/ssh/keys-root/authorized_keys** * 上記の出力のみをファイルに入力した後、ファイルを終了して保存します。 これで、SCVM から ESXi に SSH で接続しようとすると、パスワードを要求することなく許可する必要があります。アップグレードを続行してください。アップグレードが引き続き失敗する場合は、Cisco TAC にお問い合わせください。	3.0(1i)
CSCvp89523	HyperFlex クラスタが ACI ファブリックに展開され、同じブリッジ ドメイン内に HX 管理および HX ストレージがある場合、誤った HX ストレージ コントローラ インターフェイスからの ARP 応答が表示され、誤った ARP 学習が発生します。	HX の管理および HX ストレージは、別々のブリッジ ドメインに存在する必要があります。次の CVD の表 21 を参照してください。 https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/hx3_vsi_2_0.html	3.5 (1j)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvp93442	storfs (fileAIOPanicOnStuckIO) でクラッシュ: IO 要求タイマーが期限切れになりました。	NA	3.5 (2b)
CSCvp96650	UCSM の設定手順で、クラスタの展開中にサブ組織フィールドのエントリが取得されません。UCSM ページのサブ組織入力フィールドが空欄のまま表示されます。	JSON 構成ファイルで、サブ組織名を入力し、その構成をエクスポートします。そうすると、検証が失敗しません。 インポート json 構成ファイル機能を使用して適切なサブ組織名の詳細を持つ json をインポートすることで、検証中に値がピックアップされ、失敗しません。	3.5 (2b)
CSCvp98910	2 ノード ネットワーク パーティションの修復後、分離ノードのデータストアは 15 分間使用できません。	次の 2 つのオプションがあります。 **1.** ARP エントリがタイムアウトするまで 15 ～ 20 分間待機してから、データストアが再びマウントされるようになります。 **2.** ARP エントリを手動でリセットするには、次の手順を実行します。 現在の eth1: 0 を確認します。HyperFlex コントローラ VM とノードの両方から IP/Mac への MAC アドレス。コントローラ VM のシェルから **ifconfig eth1: 0** を実行します。データストアが使用できないノードで、次のコマンド (**esxcli network IP neighbor list**) を使用して、ESXi ARP キャッシュ内の上記の IP アドレスの MAC アドレス エントリを確認します。IP アドレスが誤った MAC アドレスに割り当てられている場合は、次に示すように ARP テーブルからエントリを消去します。 `esxcli network ip neighbor remove -a <IP_address> -v 4`	4.0(1a)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvo86431	ノードがメンテナンスモードの場合、ノードがメンテナンスモードから復帰した後にのみ、ディスクの削除または交換がUIに反映されます。これは、メンテナンス中にstorfsがノード上で実行されておらず、MMから復帰するまでディスク アクティビティを検出できないためです。	ノードをメンテナンス モードにします。	3.5(2a)
CSCvp79511	HX アップグレードリリース 2.1 (1c) > 3.0 (1i) は、ESXi/vCenter が 6.0 u3 以降ではない場合に許可されました。	アップグレードを試行する前に、ESXi および vCenter を 6.0 u3 にアップグレードします。	3.0(1i)

リリース 3.5(2c) で未解決の問題

不具合 ID	症状	回避策	リリースで検出された障害
インストール、アップグレード、展開			

不具合 ID	症状	回避策	リリースで検出された障害

CSCvv21905	HX Connect UI の暗号化ページに UCSM 読み取り専用ユーザーが存在しないというエラーが発生しました。その後、クレデンシャルを使用して UCSM を認証すると、無効な CSRF トークンのエラーがスローされます。	次のコマンドを実行します。
		`stcli security encryption ucsm-ro-user create --hostname <FI-IP> --username <FI-user-name> --password <FI-password>`
		`stcli security encryption ucsm-ro-user show`
			3.5(1a)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvs28167			2.6(1e)

不具合 ID	症状	回避策	リリースで検出された障害
	Cisco HyperFlex でノード置換をインストールまたは完了するため、顧客は HX インストーラ OVA（オープン仮想アプライアンス）ファイルをダウンロードする必要があります。ストレッチクラスタを展開するには、顧客はさらに Witness OVA をダウンロードする必要があります。リリース HX 3.5(2g) の登校前に CCO で投稿されたすべてのコードは、2019 年 11 月 26 日に期限切れになっている証明書を検出しました。Cisco は更新された証明書で、HX リリース 3.5(2e)、3.5.2(f)、3.5.2(g)、4.0(1a)、4.0(1b) に関連付けられている OVA ファイルを再署名および再投稿しました。その他のリリースについては、期限	影響を受ける OVA ファイルでの展開が失敗した後、続行するには2つのオプションがあります（インストーラおよび OVA ファイルに適用）。 オプション A：ローカル マニフェスト ファイルを削除します。 マニフェスト ファイルを検出可能なため、vCenter は証明書の有効性を確認します。 **1.** OVA ファイルをローカル ディレクトリにダウンロードして展開します。 **2.** .mf ファイルを削除します **3.** 残りのファイルを新しいアーカイブに追加して、「.tar」から「.ova」にファイルの拡張子を変更します。 **4.** vCenter で「OVF テンプレートで展開」を使用して新しく OVA ファイルを作成する展開を続行します。vCenter は証明書を所持していないためファイルを表示します。これは予想された動作で、展開は問題なく続行します。 オプション B - ローカル マニフェスト ファイルを削除します。 ovftool で手動展開：VMware の ovftool を使用して、証明書確認をバイパス中に OVA を展開します。ovftool はダウンロードして顧客のコンピュータで実行可能です。ovftool も HX コントローラ VM で事前インストールされます。これはノード交換とクラスタ拡張にも役立ちます。 **1.** skipManifestcheck スイッチを発生させている間、ovftool を使用して OVA ファイルをデータストアに展開します。次に例を示します。 `root@SpringpathControllerABCDEFGH:~# ovftool --skipManifestCheck -ds=datastore http://<path to ova>/Cisco-HX-Data-Platform-Installer-v3.5.2c-31725-esx.ova vi://root@<IP of management ESX`	

不具合 ID	症状	回避策	リリースで検出された障害

	切れの OVA を持つ OVF テンプレートを展開しようとすると、次のエラーメッセージ「OVA パッケージは無効な証明書で署名されています」で失敗します。	host>/
		2. OVA を展開し、以前指定した ESXi ホストの vCenter に存在している必要があります。
		3. VM とコンソールの電源をオンにします
		4. root / Cisco123 のユーザー名/パスワードのデフォルトの組み合わせで VM にログインします
		5. **vi /etc/network/eth0.interface** を発行して VM の IP を静的に設定します
		6. 「iface eth0 inet dhcp」を「iface eth0 inet static」に変更します。次のいずれかが独自のラインと指定したタブで必要になります
		`address <desired ip address of installer>`
		`netmask X.X.X.X`
		`gateway X.X.X.X`
		`<esc> :wq`
		7. ファイルを確認および保存後、VM が再起動します。VM は現在希望している IP アドレスでブートされる必要があります
		8. WebGUI 経由での最初のログイン（引き続きデフォルトのユーザー名/パスワードの組み合わせ）は、ユーザーがパスワードを変更します。
		9. パスワードの変更後、ユーザーは希望のインストール/拡大/ノードの交換アクティビティを開始できます。	

不具合 ID	症状	回避策	リリースで検出された障害
CSCvp90129	ストレッチクラスタでは、クラスタにノードまたはディスクの追加、障害、または再調整が発生したメンテナンスウィンドウが表示された場合、クラスタ内の一部のノードが使用できなくなる可能性があります。	ストレッチ クラスタでは HyperFlex リリース 3.5 (2c) を使用しないでください。ストレッチクラスタ設定ですでにインストールされているか、リリース 3.5 (2c) にアップグレードされている場合は、TAC にお問い合わせください。	3.5 (2c)
CSCvp52171, CSCvm60845	ノード ID オプションを指定して **stcli node remove** を使用しましたが、ノードは削除されませんでした。	1. ノード (削除する) を MM (すでに顧客の場合) ユニットに配置します。 2. クラスタをシャットダウンします。 3. いずれかのノードで「storfs」を開始します (クラスタの一部になります)。 4. ノードを取り外します。 5. 開始したノードで storfs を停止します。 6. クラスタを開始します。 7. zk エントリのクリーンアップ。 8. DS、VM を確認します。	3.0(1i)
CSCvp58739	stcli クラスタの作成は、最新の SAS ファームウェアバージョンでは失敗します。	NA	3.5 (2c)
CSCvj22992	VM は複数のノードに表示されます。	VM を回復するには、データディスクをコピーして新しい VM に接続します。	3.0(1b)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvn67512	ファームウェアアップグレード後の SED ドライブの電源切断	ディスクが表示されるまで、リブートして電源を入れます。	3.0(1d)
CSCvn76916	HX データストアの使用率は、データストア上で VM の組み合わせを使用する場合よりも高くなります。	NA	3.5(1a)
CSCvn99088	Shavlik スナップショットにより、保護された VM が保護されない状態になります。	Shavlik スナップショットを削除します。	3.0(1a)
CSCvo19250	クラスタの容量が 70% を超えると、警告またはアラートは生成されません。	ストレージ容量を増やすか (新しいノードまたはディスク)、またはストレージ使用量を削減します (未使用の VM とスナップショットを削除します)。	3.0(1i)
CSCvo56350	ESXi 6.7 EP06 にアップグレードすると、再起動後に PSOD が検出されます。	ESXi 6.7 Express Patch 08 にアップグレードします。	4.0(1a)
CSCvo62867	EAM エラーが原因でノード交換スクリプトが失敗します。	更新されたスクリプトで問題を解決します。	3.0(1i)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvo79760	クラスタ (HX リリース > = 3.5) とクラスタ (HX リリース < 3.5) のペアリング中に、クラスタでリモート複製ネットワークテストが失敗します (HX リリース < 3.5)。	すべてのワークフローは、3.5 より前の HX リリースを使用してクラスタから実行できます。	3.5(1a)
CSCvo83276	VM のバックアップは、バックアップ VM のスナップショット中にオフになります。	スナップショットを再度取得します。	3.5(1a)
CSCvo93017	クラスタが「失敗」状態になっている状態で、stcli ノードの削除が試行された場合、クラスタからノードを削除できなかった場合でも、出力は正常に表示されます。	TAC に存在するスクリプトを使用して、クラスタの状態をオンラインに更新してからノードの削除を実行すると、ノードが正常に削除されます。	3.5 (1i)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvp12241	2 個のノードの HyperFlex Edge クラスタが正常にフェールバックされず、正常に復帰しない可能性があります。Intersight への接続がまったく機能しない場合に、発生する場合があります (例: トランザクションの遅延が 100 ミリ秒を超える場合など)。	両方のノードがアップ状態で実行中であり、回避策を試行する前に回復する時間を与えていることを確認します (数時間)。回復を与えておらずフェールバックしている場合、両方のコントローラ VM (両方のノードで同時に実行することを推奨) で次のコマンドを実行して再起動します。**restart hxRoboController**.	4.0(1a)
CSCvp19670	クラスタの管理 IP は、クラスタのシャットダウン後には復帰しません。	各ストレージコントローラ VM で cip モニタを開始します。 手動でデータストアをマウントします。	3.5(2a)
CSCvp20230	**クラスタの無効状態**が原因で、ストレッチクラスタのアップグレードがランダムに失敗します。	1. 次のコマンドを実行します。**stcli cluster upgrade --components hxdp --clean** 2. HX アップグレードを再度実行します。 3. 必要に応じて手順 1 および 2 を繰り返します。	3.5 (2b) 3.5(1a)

不具合 ID	症状	回避策	リリースで検出された障害

CSCvp23718	2分 I/O ストール: SSD、HDD またはノードの再起動後、16 ノード、8 TB の LFF クラスタ。	インストール後 (新規展開の場合)、またはリリース 4.0 (1a) へのアップグレード後 (既存の展開の場合) は、すべてのコントローラ VM に次の調整変更を適用します。
		(すべてのコントローラ VM 上の) 次の調整ファイルを編集します。
		`/opt/springpath/config/lff.tunes`
		`/opt/springpath/config/vsi_1.6tb.tunes`
		`cleanerEnableSegSummaryCleaning` は「false」に設定する必要があります
		上記の調整ファイルを編集した後、次の手順を実行します。
		1. すべてのコントローラ VM に SSH でログインします。
		2. 「`Storfstool---z`」を実行します。
		3. 次のコマンドを実行して、値を確認します。調整値は「true」にする必要があります
		`# cat/tmp/stprocfs/system/tune/cleanerEnableSegSummaryCleaning`
		`cleanerEnableSegSummaryCleaning = true`
		4. 次のコマンドを入力し、調整の変更を動的に適用します。
		`# echo false >/tmp/stprocfs/system/tune/cleanerEnableSegSummaryCleaning`
		5. 調整値が変更されていることを確認します。次のコマンドを実行します。値は「false」にする必要があります。
		`# cat /tmp/stprocfs/system/tune/cleanerEnableSegSummaryCleaning`
		`cleanerEnableSegSummaryCleaning = false`
		`f. umount/tmp/stprocfs`
			4.0(1a)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvp26319	リリース 3.5(2b) FlexVol から 4.0 CSI へのアップグレードは機能しません。FlexVol は引き続き動作します。	1. 設定ファイルを手動で更新して、リンク ローカル アドレスを * に変更します。 2. コントローラと ESX で scvmclient を再起動します。	4.0(1a)
CSCvp31021	HyperFlex クラスタのアップグレードは、検証中に「DRS 検証が失敗しました」というエラーで失敗する場合があります。	1. 次のファイルを編集します。 /usr/share/springpath/storfs-validation/workflow-scripts/pre_upgrade_cluster_drs_check.xml 次のファイルを編集し**ないでください**。/pre_upgrade_cluster_drs_check.xml 2. 次のセクションを検索します。 <validator type="vcenter-validate-failover" description="Validate DRS Failover"> <argument name="vcenter-url" ref="vcenter-url"/> <argument name="vcenter-user" ref="vcenter-user"/> <argument name="vcenter-password" ref="vcenter-password"/> <argument name="vcenter-datacenter" ref="vcenter-datacenter"/> <argument name="ip-address-list" ref="ip-address-list"/> <argument name="skip" ref="......."/> </validator> 3. 変更 <argument name="skip" ref="....."/> to <argument name="skip" value="true"/> または、セクション全体をコメント アウトします。	3.5(1a)
CSCvp36364	Apache tomcat の複数の脆弱性。	NA	4.0(1a)

不具合 ID	症状	回避策	リリースで検出された障害

CSCvp37536	HX ストレッチクラスタ監視 VM は、リブート時に DHCP に戻ります。	次のファイルを編集します。
		`vi/etc/network/eth0.interface`
		`自動 eth0`
		`iface eth0 inet static`
		`address x.x.x.x`
		`netmask x.x.x.x`
		`gateway x.x.x.x`
		保存したら、監視 VM を再起動します。IP アドレスが適用されますが、設定ファイルは DHCP にリセットされるため、さらに RCA と解決が検出されるまで、再起動ごとにまた実行する必要があります。
			3.5 (1b)

CSCvp41241	データの再同期中の RF 2 クラスタのシャットダウン。ノード障害後 (非 storfs)。その後、複数のディスク読み取り障害が発生します。ハードブラックリストに登録されています。	障害が発生したディスクをシャーシから取り外し、再度挿入します。 クラスタを再起動します。	3.0(1e)
CSCvp49720	2 ノードの ROBO セットアップでzk リーダーを MM に設定する場合の APD。	ノードの zookeper を停止し、zookeeper データベースのコピーを作成し、データベース ディレクトリ内のファイルを削除して、zookeeper を再起動します。	4.0(1a)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvp60476	ノードの展開後、zookeeper データベースがノード情報で更新されず、「stcli cluster info」の「Node IP Settings」に拡張ノードの情報が表示されません。	root ユーザー名で SSH から CIP に「`# Stcli node add--node-ips--esx--esx--esx`」を実行します。	3.5(2a)

CSCvm77294	次のエラーでリリース 3.x の検証へのアップグレードに失敗します。DRS 障害–不正なアドミッション コントロール設定	1. 許可設定の確認または無効化 (vSphere クラスタ > HA 設定)
		2. 次のファイルを編集します。
		~~/usr/share/springpath/storfs-validation/workflow-scripts/pre_upgrade_cluster_drs_check.xml~~
		次のファイルを編集**しないでください**:
		`/pre_upgrade_cluster_drs_check.xml`
		3. 次のセクションを検索します。
		`<validator type="vcenter-validate-failover" description="Validate DRS Failover">`
		`<argument name="vcenter-url" ref="vcenter-url"/>`
		`<argument name="vcenter-user" ref="vcenter-user"/>`
		`<argument name="vcenter-password" ref="vcenter-password"/>`
		`<argument name="vcenter-datacenter" ref="vcenter-datacenter"/>`
		`<argument name="ip-address-list" ref="ip-address-list"/>`
		`<argument name="skip" ref="......."/>`
		`</validator>`
		4. 変更
		`<argument name="skip" ref="......"/>`
		to
		`<argument name="skip" value="true"/>`
		または、セクション全体をコメント アウトします。
			2.6(1e)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvp36220		該当なし。コールはバックグラウンドで実行され最終的に成功しますが、15 分よりも長くかかる場合があります。	3.5(2a)

不具合 ID	症状	回避策	リリースで検出された障害
	「stcli node add」を実行して15分を超えると、「ノードの追加に失敗しました」と「タイムアウト」を示すメッセージが表示されます。次に例を示します。 root@SpringpathControllerFWNS2M# stcli node add --node-ips 10.6.76.15 --esx-username root -f コントローラのルートパスワードの追加を入力します。 ESX ホストルートパスワードを入力します。 ノードの追加に失敗しました。<<< addNodeUnicastMessageOperation did not complete in expected time and maybe executing in the background,NoneNoneOperation did not complete in expected time and maybe executing in the background,ArrayBuffer() root@SpringpathControllerFWNS2M ~# クラスタ追加が		

不具合 ID	症状	回避策	リリースで検出された障害
	引き続きバックグラウンドで実行されている場合は、タイムアウト時間を長くして、ノードの追加に失敗しないようにより直感的なメッセージをスローして、バックグラウンドで実行している必要があります。 上記の例では、ノードの追加が正常に完了しましたが 15 分を超えていました。		
CSCvp42679	HyperFlex: 現在および必要なファームウェアが同一の場合、キュー状態の UCSM アップグレード。	アップグレードを強制的にクリアする必要があります。次のコマンドを実行します。 `# stcli cluster upgrade: clean: components ucs-fw--ucsm-host 14.39.51.225`	3.5 (2b)
CSCvp46539	HyperFlex 拡張ワークフローでは、VLAN 名が正しくプルされません。	拡張 UI を使用し、手動で VLAN の名前を修正します。	4.0(1a)
CSCvp55109	ノード拡張後に、vm-network で MTU が1500 に変更され、9000 以前に設定されていました。	NA	3.5(2a)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvp62167	電源が停止したクラスタによるパニック	NA	3.5(2a)
CSCvp63635	アップグレード後に SSH を再度有効にすることはできません。	NA	3.5(1a)
CSCvp63958	HX 複製のクリーンアップが次のエラーで失敗しました: 情報:DR の状態がクリーンではありません。	NA	3.5(2a)
CSCvp65649	管理ユーザーとしてアクセスが制限されます。	NA	3.5(2a)
CSCvp65824	リリース 3.5 (2b) から 4.0 (1a) へのアップグレード中に、ノードのステータスが正しくありません。	NA	4.0(1a)
管理			
CSCvp09978	クラスタ情報は、Smart call home が無効になっているにも関わらず、有効になっていることを示しています。	代わりに、 **stcli services sch show**コマンドを使用します。	3.5 (2b)

リリース 3.5(2b) で未解決の問題

不具合 ID	症状	回避策	リリースで検出された障害

CSCvv21905	HX Connect UI の暗号化ページに UCSM 読み取り専用ユーザーが存在しないというエラーが発生しました。その後、クレデンシャルを使用して UCSM を認証すると、無効な CSRF トークンのエラーがスローされます。	次のコマンドを実行します。
		`stcli security encryption ucsm-ro-user create --hostname <FI-IP> --username <FI-user-name> --password <FI-password>`
		`stcli security encryption ucsm-ro-user show`
			3.5(1a)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvs08218		1. Commvault を使用して別のスナップショットを取得します。このエラーメッセージは消えます。 2. sentinel スナップショットを削除して、再度作成します (VM が応答しなくなる可能性があります)。 3. vCenter でアラートを無視/抑制します。	3.5 (2b)

不具合 ID	症状	回避策	リリースで検出された障害
	HyperFlex クラスタ内で実行されている仮想マシンを Commvault がバックアップすると、ネイティブの HyperFlex スナップショットが取得され、完了時に削除されます。ただし、vCenter は vSphere 内で「VM ディスク統合が必須(VM disk consolidation is required)」とレポートします。このアラートは、定期的に更新されない既存の sentinel スナップショットに対してスローされます。Commvault がネイティブ HX スナップショットを取得するには、sentinel スナップショットが存在する必要があります。 また Commvault は、データエージングジョブの一部として、「HX はスナップショットの削		

不具合 ID	症状	回避策	リリースで検出された障害
	除に失敗しました (HX Failed to delete Snap)」というエラーを報告します。エラーメッセージ -「スナップショットスナップショット-100 の削除がエンティティ vm-xx で失敗しました (Delete snapshot snapshot-100 failed for entity vm-xx)」このエンティティでは、以前に発行されたスナップショットのタスクが進行中です。 この問題の修正は、Hotfix Pack SP16.36 で利用できます。		

不具合 ID	症状	回避策	リリースで検出された障害
CSCvs28167			2.6(1e)

不具合 ID	症状	回避策	リリースで検出された障害
	Cisco HyperFlex でノード置換をインストールまたは完了するため、顧客は HX インストーラ OVA（オープン仮想アプライアンス）ファイルをダウンロードする必要があります。ストレッチクラスタを展開するには、顧客はさらに Witness OVA をダウンロードする必要があります。リリース HX 3.5(2g) の登校前に CCO で投稿されたすべてのコードは、2019 年 11 月 26 日に期限切れになっている証明書を検出しました。Cisco は更新された証明書で、HX リリース 3.5(2e)、3.5.2(f)、3.5.2(g)、4.0(1a)、4.0(1b) に関連付けられている OVA ファイルを再署名および再投稿しました。その他のリリースについては、期限	影響を受ける OVA ファイルでの展開が失敗した後、続行するには2つのオプションがあります（インストーラおよび OVA ファイルに適用）。 オプション A：ローカル マニフェスト ファイルを削除します。 マニフェスト ファイルを検出可能なため、vCenter は証明書の有効性を確認します。 1. OVA ファイルをローカル ディレクトリにダウンロードして展開します。 2. .mf ファイルを削除します 3. 残りのファイルを新しいアーカイブに追加して、「.tar」から「.ova」にファイルの拡張子を変更します。 4. vCenter で「OVF テンプレートで展開」を使用して新しく OVA ファイルを作成する展開を続行します。vCenter は証明書を所持していないためファイルを表示します。これは予想された動作で、展開は問題なく続行します。 オプション B - ローカル マニフェスト ファイルを削除します。 ovftool で手動展開：VMware の ovftool を使用して、証明書確認をバイパス中に OVA を展開します。ovftool はダウンロードして顧客のコンピュータで実行可能です。ovftool も HX コントローラ VM で事前インストールされます。これはノード交換とクラスタ拡張にも役立ちます。 1. skipManifestcheck スイッチを発生させている間、ovftool を使用して OVA ファイルをデータストアに展開します。次に例を示します。 `root@SpringpathControllerABCDEFGH:~# ovftool --skipManifestCheck -ds=datastore http://<path to ova>/Cisco-HX-Data-Platform-Installer-v3.5.2c-31725-esx.ova vi://root@<IP of management ESX`	

不具合 ID	症状	回避策	リリースで検出された障害

	切れの OVA を持つ OVF テンプレートを展開しようとすると、次のエラーメッセージ「OVA パッケージは無効な証明書で署名されています」で失敗します。	host>/
		2. OVA を展開し、以前指定した ESXi ホストの vCenter に存在している必要があります。
		3. VM とコンソールの電源をオンにします
		4. root / Cisco123 のユーザー名/パスワードのデフォルトの組み合わせで VM にログインします
		5. **vi /etc/network/eth0.interface** を発行して VM の IP を静的に設定します
		6. 「iface eth0 inet dhcp」を「iface eth0 inet static」に変更します。次のいずれかが独自のラインと指定したタブで必要になります
		`address <desired ip address of installer>`
		`netmask X.X.X.X`
		`gateway X.X.X.X`
		`<esc> :wq`
		7. ファイルを確認および保存後、VM が再起動します。VM は現在希望している IP アドレスでブートされる必要があります
		8. WebGUI 経由での最初のログイン（引き続きデフォルトのユーザー名/パスワードの組み合わせ）は、ユーザーがパスワードを変更します。
		9. パスワードの変更後、ユーザーは希望のインストール/拡大/ノードの交換アクティビティを開始できます。	

CSCvp40474	クラスタが正常な場合でも、複数の Hyper-V HyperFlex ホストがデータストアにアクセスできません。	リリース 3.5 (2d) で修正。	3.5(2a)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvp66679	Hyperflex に、次の Common Vulnerabilities および Exposures によって識別される脆弱性の影響を受けるバージョンの OpenSSL が含まれています。 CVE-2018-0495	NA	3.5(1a)
CSCvp78288	クラスタ I/O へディスクを追加するときに 96 秒間凍結する場合。	介入は必要ありません。クラスタは自身で回復します。	3.5(2a)
CSCvp88990	HX のアップグレードは、SCVM が ESXi にログインできないという問題が発生します。	ESXi ホスト上の承認済みキーファイルに SSH 公開キーをコピーします。 SCVM の場合: `cat/etc/ssh/ssh_host_rsa_key.pub` ** 単一の行のすべての出力をコピーします。ターミナル ウィンドウで新しい行にホスト名が出力されていない場合でも、キーの末尾を超えるものはコピーしないでください。 前の出力から ESXi の承認済みキー ファイルにキーを入力します。 **vi/etc/ssh/keys-root/authorized_keys** * 上記の出力のみをファイルに入力した後、ファイルを終了して保存します。 これで、SCVM から ESXi に SSH で接続しようとすると、パスワードを要求することなく許可する必要があります。アップグレードを続行してください。アップグレードが引き続き失敗する場合は、Cisco TAC にお問い合わせください。	3.0(1i)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvp89523	HyperFlex クラスタが ACI ファブリックに展開され、同じブリッジドメイン内に HX 管理および HX ストレージがある場合、誤った HX ストレージコントローラ インターフェイスからの ARP 応答が表示され、誤った ARP 学習が発生します。ACI ファブリックでは、HX IP の MAC 移動が表示されます。	HX の管理および HX ストレージは、別々のブリッジ ドメインに存在する必要があります。次の CVD の表 21 を参照してください: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/hx30_vsi_32.html	3.0(1i)
CSCvp93442	storfs (fileAIOPanicOnStuckIO) でクラッシュ: IO 要求タイマーが期限切れになりました。	TAC に連絡します。	3.5 (2b)
CSCvp96650	UCSM の設定手順で、クラスタの展開中にサブ組織フィールドのエントリが取得されません。UCSM ページのサブ組織入力フィールドが空欄のまま表示されます。	JSON 構成ファイルで、サブ組織名を入力し、その構成をエクスポートします。そうすると、検証が失敗しません。 インポート json 構成ファイル機能を使用して適切なサブ組織名の詳細を持つ json をインポートすることで、検証中に値がピックアップされ、失敗しません。	3.5 (2b)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvp98910	2 ノード ネットワーク パーティションの修復後、分離ノードのデータストアは 15 分間使用できません。	次の 2 つのオプションがあります。 A) ARP エントリがタイムアウトするまで 15 ～ 20 分間待機してから、データストアが再びマウントされるようになります。 B) ARP エントリを手動でリセットするには、次の手順を実行します。 1. 現在の eth1: 0 を確認します。HyperFlex コントローラ VM とノードの両方から IP/Mac への MAC アドレス。 コントローラ VM のシェルから ifconfig eth1: 0 を実行します。 2. データストアが使用できないノードで、次のコマンドを使用して、ESXi ARP キャッシュ内の上記の IP アドレスの MAC アドレス エントリを確認します。 **"esxcli network ip neighbor list"** 3. IP アドレスが誤った MAC アドレスに割り当てられている場合は、次に示すように ARP テーブルからエントリを消去します。 **esxcli network ip neighbor remove -a <IP_address> -v 4**	4.0(1a)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvo86431	ノードがメンテナンスモードの場合、ノードがメンテナンスモードから復帰した後にのみ、ディスクの削除または交換が UI に反映されます。これは、メンテナンス中に storfs がノード上で実行されておらず、MM から復帰するまでディスクアクティビティを検出できないためです。	ノードをメンテナンス モードにします。	3.5(2a)
CSCvp79511	リリース 3.0 (1i) への HX のアップグレードは、vCenter および ESXi がバージョン 6.0u2 の両方で許可されていますが、バージョン6.0u3ではバージョンチェックが必要です。	アップグレードを試行する前に、ESXi および vCenter を 6.0 u3 にアップグレードします。	3.0(1i)
CSCvp86483	既存のパスワードを知らなくても、HyperFlex ルートまたは管理者パスワードをリセットすることはできません。	TAC に連絡します。	4.0(1a)

リリース 3.5(2a) で未解決の問題

不具合 ID	症状	回避策	リリースで検出された障害
インストール、アップグレード、展開			

CSCvv21905	HX Connect UI の暗号化ページに UCSM 読み取り専用ユーザーが存在しないというエラーが発生しました。その後、クレデンシャルを使用して UCSM を認証すると、無効な CSRF トークンのエラーがスローされます。	次のコマンドを実行します。
		`stcli security encryption ucsm-ro-user create --hostname <FI-IP> --username <FI-user-name> --password <FI-password>`
		`stcli security encryption ucsm-ro-user show`
			3.5(1a)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvs28167	Cisco HyperFlex でノード置換をインストールまたは完了するため、顧客は HX インストーラ OVA（オープン仮想アプライアンス）ファイルをダウンロードする必要があります。ストレッチ クラスタを展開するには、顧客はさらに Witness OVA をダウンロードする必要があります。リリース HX 3.5(2g) の登校前に CCO で投稿されたすべてのコードは、2019 年 11 月 26 日に期限切れになっている証明書を検出しました。Cisco は更新された証明書で、HX リリース 3.5(2e)、3.5.2(f)、3.5.2(g)、4.0(1a)、4.0(1b) に関連付けられている OVA ファイルを再署名および再投稿しました。その他のリリースについては、期限切れの OVA を持つ OVF テンプレートを展開しようとすると、次のエラーメッセージ「OVA パッケージは無効な証明書で署名されています」で失敗します。		2.6(1e)

不具合 ID	症状	回避策	リリースで検出された障害
		影響を受ける OVA ファイルでの展開が失敗した後、続行するには2つのオプションがあります（インストーラおよび OVA ファイルに適用）。 オプション A：ローカルマニフェストファイルを削除します。 マニフェストファイルを検出可能なため、vCenter は証明書の有効性を確認します。 1. OVA ファイルをローカル ディレクトリにダウンロードして展開します。 2. .mf ファイルを削除します 3. 残りのファイルを新しいアーカイブに追加して、「.tar」から「.ova」にファイルの拡張子を変更します。 4. vCenter で「OVF テンプレートで展開」を使用して新しく OVA ファイルを作成する展開を続行します。vCenter は証明書を所持していないためファイルを表示します。これは予想された動作で、展開は問題なく続行します。 オプション B - ローカルマニフェストファイルを削除します。 ovftool で手動展開：VMware の ovftool を使用して、証明書確認をバイパス中に OVA を展開します。ovftool はダウンロードして顧客のコンピュータで実行可能です。ovftool も HX コントローラ VM で事前インストールされます。これはノード交換とクラスタ拡張にも役立ちます。 1. skipManifestcheck スイッチを発生させている間、ovftool を使用して OVA ファイルをデータストアに展開します。次に例を示します。 `root@SpringpathControllerABCDEFGH:~# ovftool --skipManifestCheck -ds=datastore http://<path to ova>/Cisco-HX-Data-Platform-Installer-v3.5.2c-31725-esx.ova`	

不具合 ID	症状	回避策	リリースで検出された障害
		vi://root@<IP of management ESX host>/ 2. OVA を展開し、以前指定した ESXi ホストの vCenter に存在している必要があります。 3. VM とコンソールの電源をオンにします 4. root / Cisco123 のユーザー名/パスワードのデフォルトの組み合わせで VM にログインします 5. **vi /etc/network/eth0.interface** を発行して VM の IP を静的に設定します 6. 「iface eth0 inet dhcp」を「iface eth0 inet static」に変更します。次のいずれかが独自のラインと指定したタブで必要になります address <desired ip address of installer> netmask X.X.X.X gateway X.X.X.X <esc> :wq 7. ファイルを確認および保存後、VM が再起動します。VM は現在希望している IP アドレスでブートされる必要があります 8. WebGUI 経由での最初のログイン（引き続きデフォルトのユーザー名/パスワードの組み合わせ）は、ユーザーがパスワードを変更します。 9. パスワードの変更後、ユーザーは希望のインストール/拡大/ノードの交換アクティビティを開始できます。	

不具合 ID	症状	回避策	リリースで検出された障害
CSCvn89717	リリース 3.5 (1a) から 3.5 (2a) へのアップグレード中に競合状態が発生すると、競合状態が原因で M5 SED クラスタの USB インターフェイスが使用できなくなります。	HyperFlex コントローラの USB デバイスは、CIMC によって公開されているホスト接続された USB です。一部のケースでは、デバイスが完全に初期化されておらず、USB デバイスが検出されていません。この USB デバイスは、CIMC から重要な SED 関連情報を通信するために使用されます。USB デバイスが存在しない場合、ドライブはロックされます。 この問題が発生した場合は、vCenter を介してデバイスを手動で追加し、CIMC との通信を確立し、ドライブのロックを解除します。 （注） この問題は、セキュリティが有効になっている HyperFlex クラスタのアップグレード中にのみ発生する可能性があります。	3.5(2a)
CSCvn51562	Cisco HX Data Platform プラグインは、Windows vCenter Web クライアント 6.7 U1 にロードできません。この問題は VMware VCSA では表示されません。	この問題が発生した場合は、次の手順を実行します。 1. **[管理 (Administration)]** > **[クライアント プラグイン (Client Plugins)]** > **[Springpath]** からプラグインを無効にします。 2. ログアウトしてから、ログインします。 3. **[Administration (管理)]** > **[Client Plugins (クライアント プラグイン)]** > **[Springpath]** からプラグインを有効にします。 4. ログアウトしてから、ログインします。	3.5(2a)

不具合 ID	症状	回避策	リリースで検出された障害

CSCvn17787	クラスタの作成/クラスタの拡張ワークフローは、検証手順で次のエラー メッセージが表示され停止します。
	`FIRMWARE-Check UCSC-SAS-M5HD`
	`FIRMWARE-Check UCSC-SAS-M5HD : Required: 00.00.00.29, 00.00.00.32, 00.00.00.35, 00.00.00.51, Found: 00.00.00.58;`
	必要なアクション: 必須バージョンにコントローラファームウェアを更新する
		これは警告メッセージであり、無視しても問題ありません。**[Skip Create Validation (作成の検証をスキップする)]** をクリックして、クラスタの作成を続行します。この回避策は、クラスタ拡張ワークフローにも適用されます。	3.5(2a)

CSCvm53972	障害が発生したディスクの自動ソフトウェア修復中に、リリース 2.6 (1x) で実行されているクラスタではすべてのパスがダウンしている可能性があります。	この問題が発生した場合は、次の手順を実行します。 • すべてのハードディスクを、ブラックリスト カウント 5 よりも大きい値に置換します。 すべてのノードで **`Maxdiskblacklistccount`** を 10 から 5 に下げます。これにより、別の障害が発生したディスクでこの問題が発生する可能性が低くなります。	2.6(1b)
CSCvh09129	クラスタ拡張: ノードをクラスタに追加する前に、検証(十分な DR IP アドレス) が必要です。	クラスタの新しいノードに割り当てるため、十分な複製 IP アドレスがあることを確認します。必要な場合、複製ネットワーク設定を変更して、追加 IP 範囲を含みます。	2.6(1a)

不具合 ID	症状	回避策	リリースで検出された障害
CSCve73004	2.1 (1b) から2.5 へのファームウェア アップグレードが HX Data Platformによって開始された場合、UCS Manager はディスクファームウェアのステータスを更新しません。	ソフト リセットを実行します。 # `CIMC-soft-rest`	2.5(1a)
CSCvc62266	オフライン アップグレード後、VMware EAM の問題により、一部のコントローラ VM が再起動しないことがあります。`stcli start cluster` コマンドが「ノードは使用できません」というエラーを返します。	コントローラ VM の電源を手動でオンにして、クラスタを開始します。 **1.** コントローラ VM の電源を手動でオンにします。 • vSphere Web クライアントにログインします。 • 電源がオンになっていないコントローラ VM を見つけ出します。vCenter ナビゲータで **[Inventory Lists (インベントリ リスト)]** > **[Virtual Machines (仮想マシン)]** > **[vm]** を選択します。ストレージコントローラ VM の名前には、`stCtlVM` というプレフィックスが付きます。 • [Actions (アクション)] メニューから、**[Power (電源)]** > **[Power On (電源オン)]** を選択します。 **2.** ストレージクラスタを再起動します。 • 任意のコントローラ VM のコマンド ラインにログインします。 • コマンドを実行します。 `# stcli cluster start`	2.0(1a)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvb94112	HX インストーラは、クラスタ拡張プロセス中に、クラスタ拡張検証画面でスタックする可能性があります。	1. ログを確認して、拡張ワークフローがハングしていることを確認します。 2. ブラウザに *http://ip_of_installer/api/reset* と入力して、ワークフローを再起動します。	1.8(1c)
Hyper-V			
CSCvn54300	アップグレード時に、ユーザーの vSwitch に作成されたチームで VLAN を削除します。 新規インストール時には、複数の Vlan が入力されていても、1つの VLAN タグだけが vSwitch とチームに設定されます。	この問題が発生した場合は、ユーザー vSwitch の下でチームに割り当てられた VLAN タグを削除します。	3.5(2a)
CSCvn28721	クラスタ拡張は、エラーコード「500-操作のタイムアウト」で失敗する可能性があります。	Hyper-v フェールオーバー クラスタへの特定のステータス クエリ コールに 40秒 以上かかる場合があるため、まれなケースでこの問題が発生します。これは通常、大規模なクラスタ (>8 ノード) で発生します。 次の手順に従って API タイムアウト値を増価し、サービスを再起動して、操作を再試行してください。 1. HX Installer VM にログインします。 2. 次のコマンドを使用して、ファイル `application.conf` を編集します。 **vi /opt/springpath/storfs-mgmt/stDeploy-1.0/conf/application.conf** 3. `Requesttimeout` を 120 秒に変更します。 4. ファイルを保存します。 5. `Restart stDeploy` を使用してサービスを再起動します。 拡張操作をやり直します。	3.5(2a)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvm05523	まれに、VM のライブ移行がエラー コード 0x138D で失敗する場合があります。	Microsoft から次の回避策を参照し、操作を再試行してください。 • サーバ 2016 S2D クラスタはドレインロールを実行できません • ライブ移行は、クラスタ認識更新からのドレイン中に失敗します • Windows Server 2012 で計画されたメンテナンスのためのノードのドレイン	3.0(1e)
CSCvk37044	ユーザー アカウント内のユーザー名にピリオド(".")が含まれている場合、展開は失敗します。	この問題を回避するには、ユーザー名にピリオド(「.」)は使用しないでください。	3.0(1e)
CSCvi56910	データストアの作成後すぐに、ディレクトリのリストはエラー「別の目的のために使用されているため、プロセスがファイル \\xyz.cloud.local\\ds1 にアクセスできません」で失敗する可能性があります。"	データストアの作成後数分待機して、コマンドを再試行してください。	3.0(1a)
CSCvi16323	HX がグレーアウト表示されているため、Hyper-V Manager (Remote) の特定の HX に移動できない場合があり、**[Inspect Disk (ディスクの検査)]** オプションは使用できません。	これは既知の問題です。	3.0(1a)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvi59119	大文字小文字の場合にのみ異なる既存のデータストア名を複製すると、不明な動作が発生する可能性があります。	これは既知の制限です。大文字小文字での区別は現在サポートされておらず、今後のリリースで対処されます。	3.0(1a)
CSCvh80044	HX Connect UI を使用すると、異なる場合に限り、可能性のある既存のデータストア名を複製することで、データストアを作成できます。たとえば、Ds3、ds3、dS3 は有効なデータストアとして許可されます。	これは既知の制限です。大文字小文字での区別は現在サポートされておらず、今後のリリースで対処されます。	3.0(1a)
CSCvh25238	HX Data Platform 展開中に、DNS に 1 個以上の IP アドレスを追加する場合、コントローラ VM は 1 個の DNS アドレスのみ割り当て可能です。	通常、プライマリ DNS は、HX コントローラ VM が動作するのに十分です。追加の DNS が必要な場合、コントローラ VM の eth0 インターフェイス ファイルを編集し、追加の DNS を追加します。	3.0(1a)
管理			
CSCvf90091	間違ったゲートウェイが提供されると、クラスタやクラスタ作成後にエラーが表示されます。	コントローラ VM にログインして、ゲートウェイを修正します。	2.5(1c)
Replication			

不具合 ID	症状	回避策	リリースで検出された障害
CSCvf29202	仮想マシンが保護されているため、復元にはデータストア上の同じフォルダにないディスクを含まない可能性があります。	仮想マシン ディスクが同じフォルダ以外にあり、保護された仮想マシンのデータストアが存在する場合: 1. ディスクをデータストアの同じフォルダに移動します。 2. 仮想マシンにディスクを追加 (再度追加) します。 これにより、保護と復元作業が正常に行われていることを確認します。	2.5(1a)
暗号化			
CSCvf17183	`Modify security` コマンドの実行中に CIMC がリブートし、サーバがローカル キー管理で保護されている場合、サーバが使用する正しいキーを認識していないため、後続の `disable-security` コマンドが失敗することがあります。	`modify-security` コマンドが進行中だった場合、CIMC がリブートしました。 コントローラ VM にログインし、sed-client を使用して、物理ドライブ キーを更新してサーバのキーに一致させます。	2.5(1a)
CSCvf06510	UCS Manager は、部分的に無効になっている暗号化セキュリティを示している可能性があります。	対処不要です。これはレポート インターフェイス間の同期問題です。 HX Connect から確認するには、**[System Information (システム情報)]** > **[Disks (ディスク)]** > **[Security (セキュリティ)]** を選択します。すべてのディスクおよびコントローラ VM は、セキュリティの無効化を示す必要があります。	2.5(1a)

リリース 3.5(1a) の未解決の問題

不具合 ID	症状	回避策	リリースで検出された障害
インストール、アップグレード、展開			

不具合 ID	症状	回避策	リリースで検出された障害

CSCvv21905	HX Connect UI の暗号化ページに UCSM 読み取り専用ユーザーが存在しないというエラーが発生しました。その後、クレデンシャルを使用して UCSM を認証すると、無効な CSRF トークンのエラーがスローされます。	次のコマンドを実行します。
		`stcli security encryption ucsm-ro-user create --hostname <FI-IP> --username <FI-user-name> --password <FI-password>`
		`stcli security encryption ucsm-ro-user show`
			3.5(1a)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvs28167	Cisco HyperFlex でノード置換をインストールまたは完了するため、顧客は HX インストーラ OVA（オープン仮想アプライアンス）ファイルをダウンロードする必要があります。ストレッチ クラスタを展開するには、顧客はさらに Witness OVA をダウンロードする必要があります。リリース HX 3.5(2g) の登校前に CCO で投稿されたすべてのコードは、2019 年 11 月 26 日に期限切れになっている証明書を検出しました。Cisco は更新された証明書で、HX リリース 3.5(2e)、3.5.2(f)、3.5.2(g)、4.0(1a)、4.0(1b) に関連付けられている OVA ファイルを再署名および再投稿しました。その他のリリースについては、期限切れの OVA を持つ OVF テンプレートを展開しようとすると、次のエラー メッセージ「OVA パッケージは無効な証明書で署名されています」で失敗します。		2.6(1e)

不具合 ID	症状	回避策	リリースで検出された障害
		影響を受けるOVAファイルでの展開が失敗した後、続行するには2つのオプションがあります（インストーラおよびOVAファイルに適用）。 オプション A：ローカル マニフェスト ファイルを削除します。 マニフェストファイルを検出可能なため、vCenterは証明書の有効性を確認します。 **1.** OVA ファイルをローカル ディレクトリにダウンロードして展開します。 **2.** .mf ファイルを削除します **3.** 残りのファイルを新しいアーカイブに追加して、「.tar」から「.ova」にファイルの拡張子を変更します。 **4.** vCenter で「OVF テンプレートで展開」を使用して新しくOVAファイルを作成する展開を続行します。vCenterは証明書を所持していないためファイルを表示します。これは予想された動作で、展開は問題なく続行します。 オプション B - ローカル マニフェスト ファイルを削除します。 ovftool で手動展開：VMware の ovftool を使用して、証明書確認をバイパス中にOVAを展開します。ovftool はダウンロードして顧客のコンピュータで実行可能です。ovftool も HX コントロー	

不具合 ID	症状	回避策	リリースで検出された障害
		ラ VM で事前インストールされます。これはノード交換とクラスタ拡張にも役立ちます。	

不具合 ID	症状	回避策	リリースで検出された障害

		1. skipManifestcheck スイッチを発生させている間、ovftool を使用して OVA ファイルをデータストアに展開します。次に例を示します。
		`root@SpringpathControllerABCDEFGH:~# ovftool --skipManifestCheck -ds=datastore http://<path to ova/CiscoHXDataPlatformInstaller-3.5.2-31725-esx.ova vi://root@<IP of management ESX host>/`
		2. OVA を展開し、以前指定した ESXi ホストの vCenter に存在している必要があります。
		3. VM とコンソールの電源をオンにします
		4. root / Cisco123 のユーザー名/パスワードのデフォルトの組み合わせで VM にログインします
		5. **vi /etc/network/eth0.interface** を発行して VM の IP を静的に設定します
		6. 「iface eth0 inet dhcp」を「iface eth0 inet static」に変更します。次のいずれかが独自のラインと指定したタブで必要になります
		`address <desired ip address of installer>`
		`netmask X.X.X.X`
		`gateway X.X.X.X`
		`<esc> :wq`
		7. ファイルを確認および保存後、VM が再起動します。VM は現在希望している IP	

不具合 ID	症状	回避策	リリースで検出された障害
		アドレスでブートされる必要があります **8.** WebGUI 経由での最初のログイン（引き続きデフォルトのユーザー名/パスワードの組み合わせ）は、ユーザーがパスワードを変更します。 **9.** パスワードの変更後、ユーザーは希望のインストール/拡大/ノードの交換アクティビティを開始できます。	
CSCvo69067	クラスタにドライブを追加すると、クラスタ容量が増加することはありません。	解決のために TAC に連絡してください。	3.0(1e) 3.5(1a)
CSCvn07634	最初に HXDP 3.5 (1a) より前に最初に展開されたクラスタで、3.5 (1a) ノード展開を試行すると、vCON ポリシーの参照エラーがトリガされます。さらに、展開前に作成された既存のサービスプロファイルは、保留中の確認応答状態になる可能性があります。	既存のサービス プロファイルの変更を手動で確認しないでください。代わりに、ここで使用可能な手順を実行します。	3.5(1a)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvh04307	ストレージコントローラ VM へのソフトウェア パッケージのインストールは、次のエラーで失敗します。 システムにロックされたドライブがあります。ロック解除して再度展開してください。 さらに、リリース 2.6 (1e) から 3.0 (1c) にアップグレードすると、次の条件が表示されます。 • アップグレードは、「クラスタの準備状況を確認する」ときに長時間スタックします。 • Stcli クラスタ情報は SED ディスクが使用不可であることを示しているため、クラスタは正常な状態に回復できません。	この問題から回復するには、Cisco TAC に問い合わせて、リリース 3.0 (1c) の情報を参照してください。	3.0(1a)
CSCvh09129	クラスタ拡張: ノードをクラスタに追加する前に、検証 (十分な DR IP アドレス) が必要です。	クラスタの新しいノードに割り当てるため、十分な複製 IP アドレスがあることを確認します。必要な場合、複製ネットワーク設定を変更して、追加 IP 範囲を含みます。	2.6(1a)
CSCve73004	2.1 (1b) から2.5 へのファームウェアアップグレードが HX Data Platformによって開始された場合、UCS Manager はディスク ファームウェアのステータスを更新しません。	ソフト リセットを実行します。 # `CIMC-soft-rest`	2.5(1a)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvc62266	オフライン アップグレード後、VMware EAM の問題により、一部のコントローラ VM が再起動しないことがあります。`stcli start cluster` コマンドが「ノードは使用できません」というエラーを返します。	コントローラ VM の電源を手動でオンにして、クラスタを開始します。 **1.** コントローラ VM の電源を手動でオンにします。 • vSphere Web クライアントにログインします。 • 電源がオンになっていないコントローラ VM を見つけ出します。vCenter ナビゲータで **[Inventory Lists (インベントリ リスト)]** > **[Virtual Machines (仮想マシン)]** > **[vm]** を選択します。ストレージ コントローラ VM の名前には、`stCtlVM` というプレフィックスが付きます。 • [Actions (アクション)] メニューから、**[Power (電源)]** > **[Power On (電源オン)]** を選択します。 **2.** ストレージ クラスタを再起動します。 • 任意のコントローラ VM のコマンド ラインにログインします。 • コマンドを実行します。 `# stcli cluster start`	2.0(1a)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvb94112	HX インストーラは、クラスタ拡張プロセス中に、クラスタ拡張検証画面でスタックする可能性があります。	1. ログを確認して、拡張ワークフローがハングしていることを確認します。 2. ブラウザに *http://ip_of_installer/api/reset* と入力して、ワークフローを再起動します。	1.8(1c)
Hyper-V			
CSCvm59573	場合によっては、インストール プロセスでハイパーバイザの設定中に Hyper-v OS のインストールが失敗することがあります。	これは断続的な問題です。ほとんどの場合、ハイパーバイザの設定手順を再試行すると、この問題が解決します。	3.5(1a)
CSCvm05523	まれに、VM のライブ移行がエラー コード 0x138D で失敗する場合があります。	Microsoft から次の回避策を参照し、操作を再試行してください。 • サーバ 2016 S2D クラスタはドレイン ロールを実行できません • ライブ移行は、クラスタ認識更新からのドレイン中に失敗します • Windows Server 2012 で計画されたメンテナンスのためのノードのドレイン	3.0(1e)
CSCvk37044	ユーザーアカウント内のユーザー名にピリオド (".") が含まれている場合、展開は失敗します。	この問題を回避するには、ユーザー名にピリオド(「.」)は使用しないでください。	3.0(1e)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvi56910	データストアの作成後すぐに、ディレクトリのリストはエラー「別の目的のために使用されているため、プロセスがファイル `\\xyz.cloud.local\\ds1` にアクセスできません」で失敗する可能性があります。"	データストアの作成後数分待機して、コマンドを再試行してください。	3.0(1a)
CSCvi16323	HX がグレーアウト表示されているため、Hyper-V Manager (Remote) の特定の HX に移動できない場合があり、**[Inspect Disk (ディスクの検査)]** オプションは使用できません。	これは既知の問題です。	3.0(1a)
CSCvi59119	大文字小文字の場合にのみ異なる既存のデータストア名を複製すると、不明な動作が発生する可能性があります。	これは既知の制限です。大文字小文字での区別は現在サポートされておらず、今後のリリースで対処されます。	3.0(1a)
CSCvh80044, CSCvi59119	HX Connect UI を使用すると、異なる場合に限り、可能性のある既存のデータストア名を複製することで、データストアを作成できます。たとえば、Ds3、ds3、dS3 は有効なデータストアとして許可されます。	これは既知の制限です。大文字小文字での区別は現在サポートされておらず、今後のリリースで対処されます。	3.0(1a)
CSCvh25238	HX Data Platform 展開中に、DNS に 1 個以上の IP アドレスを追加する場合、コントローラ VM は 1 個の DNS アドレスのみ割り当て可能です。	通常、プライマリ DNS は、HX コントローラ VM が動作するのに十分です。追加の DNS が必要な場合、コントローラ VM の eth0 インターフェイス ファイルを編集し、追加の DNS を追加します。	3.0(1a)
管理			

不具合 ID	症状	回避策	リリースで検出された障害
CSCvk46179, CSCvm47257	大規模なクラスタでは、「サーバ コーるに失敗しました」というエラーが HX Connect に表示されることがあります。	この問題が発生した場合は、ページを更新するか、ページの特定のセクションを更新してください。	3.5(1a)
CSCvj31645	まれに、Windows を実行している重複またはダミーのストレージ コントローラ VM (Stctlvm) が ESXi クラスタに表示されることがあります。	この問題が発生した場合は、次のように 3.0 (1b) を実行します。 **1.** vCenter のダミー stCtlVMsfrom を削除します。 **2.** 古い拡張機能をクリーンアップします。 **3.** 元の vCenter に再登録します。	3.0(1e)
CSCvg47332	HX スナップショットで VM の休止オプションを使用すると、VM の機能が発生する可能性があります。	休止オプションを使用する予定の場合は、HX スナップショットを有する VM には使用しないでください。 休止オプションを使用する必要がある場合は、すべての HX スナップショットを削除し、VMware スナップショットを使用します。	2.1(1b)
CSCvf90091	間違ったゲートウェイが提供されると、クラスタやクラスタ作成後にエラーが表示されます。	コントローラ VM にログインして、ゲートウェイを修正します。	2.5(1c)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvf25130	30 分後に HX Connect がタイムアウトします	アイドル状態のまま 30 分が経過すると、HX Connect 仮想マシンでページ タイムアウトが発生します。ページに戻って任意の場所をクリックすると、更新されたデータが不完全になるか、「*VI SDK invoke exception: nested exception is:* `com.vmware.vim25.NotAuthenticated`」というエラーを受信する可能性があります。認証されていません。 ブラウザまたは HX Connect ボタンを使用して、HX Connect の更新を再試行します。代わりに、HX Connect からログアウトして、もう一度ログインします。 これは、VMware の既知の問題です。「VMware KB、vCenter サーバ ログによるエラーの報告: SOAP セッションのカウントが上限に達しました (2004663)」も参照してください。	2.5(1a)
Replication			
CSCvf29202	仮想マシンが保護されているため、復元にはデータストア上の同じフォルダにないディスクを含まない可能性があります。	仮想マシン ディスクが同じフォルダ以外にあり、保護された仮想マシンのデータストアが存在する場合: 1. ディスクをデータストアの同じフォルダに移動します。 2. 仮想マシンにディスクを追加 (再度追加) します。 これにより、保護と復元作業が正常に行われていることを確認します。	2.5(1a)
暗号化			

不具合 ID	症状	回避策	リリースで検出された障害
CSCvf17183	`Modify security` コマンドの実行中に CIMC がリブートし、サーバがローカル キー管理で保護されている場合、サーバが使用する正しいキーを認識していないため、後続の `disable-security` コマンドが失敗することがあります。	`modify-security` コマンドが進行中だった場合、CIMC がリブートしました。 コントローラ VM にログインし、sed-client を使用して、物理ドライブ キーを更新してサーバのキーに一致させます。	2.5(1a)
CSCvf06510	UCS Manager は、部分的に無効になっている暗号化セキュリティを示している可能性があります。	対処不要です。これはレポートインターフェイス間の同期問題です。 HX Connect から確認するには、**[System Information (システム情報)]** > **[Disks (ディスク)]** > **[Security (セキュリティ)]** を選択します。すべてのディスクおよびコントローラ VM は、セキュリティの無効化を示す必要があります。	2.5(1a)

関連する問題

不具合 ID	症状	リリースで検出された障害	リリースで解決済み
CSCvq41985	組み込みのキックスタート ファイルを使用して CIMC にマウントされた ISO から ESXi 6.5 または 6.7 をインストールしようとすると、組み込み KS.CFG ファイルを読み取るときにインストールが失敗することがあります。ESXi インストーラでは、ポップアップ エラーが次の状態になります。 <path>/KS.CFG □□□□□□□□□□□□□□□□□□□□□	Cisco IMC 4.0 (1a)	オープン（Open）

関連資料

マニュアル	説明
設置前チェックリスト	設置作業を開始する前に**必要な**構成情報を収集するための、編集可能なファイルです。チェックリストに記入し、シスコアカウント チームにご提出ください。
VMware ESXi インストレーション ガイド	HyperFlex Systems の初期構成、および関連するポスト クラスタ設定タスクに関する詳細情報です。複数の HX クラスタの設定方法、HX クラスタの展開方法、混在した HX クラスタのセットアップ方法や、外部ストレージの接続方法についても説明しています。
ストレッチ クラスタ ガイド	HyperFlex ストレッチ クラスタのインストールと設定手順を提供し、ミッションクリティカルなワークロードにアクティブ-アクティブなディザスタ回避ソリューションを展開できるようになります。
Microsoft Hyper-V インストレーション ガイド	Microsoft Hyper-V に Cisco HyperFlex システムをインストールし、設定する方法について、インストールおよび設定手順を説明します。
エッジ導入ガイド	リモート、ブランチ オフィス（ROBO）、およびエッジ環境にハイパー コンバージェンスをもたらすように設計された、HyperFlex Edge の導入手順を説明します。
アドミニストレーション ガイド	クラスタ、暗号化、データの保護（複製とリカバリ）、ReadyClone、ネイティブ スナップショット、およびユーザ管理を管理および監視する方法について説明します。インターフェイスには、HX Connect、HX Data Platform プラグイン、および`stcli`コマンドが含まれます。
HyperFlex Intersight インストレーションガイド	クラウドから安全なインフラストラクチャ管理を提供するように設計された HyperFlex Intersight のインストール、設定、および導入手順を提供します。
アップグレード ガイド	Cisco HX Data Platform の既存のインストールのアップグレード方法、アップグレード ガイドライン、およびさまざまなアップグレード タスクに関する情報を提供します。
ネットワーク/外部ストレージ管理ガイド	HyperFlex Systems 固有のネットワークおよび外部ストレージ管理タスクに関する情報を提供します。
コマンド ライン インターフェイス（CLI）ガイド	HX Data Platform の `stcli` コマンドについての CLI リファレンス情報を提供します。

マニュアル	説明
障害復旧の Cisco HyperFlex PowerShell Cmdlets	データ保護のために Cisco PowerShell Cisco HXPowerCLI cmdlets を使用する方法に関する情報を提供します。
REST API 入門ガイド REST API リファレンス	外部アプリケーションが Cisco HyperFlex の管理プレーンと直接対話できるようにする、REST API に関連する情報を提供します。
トラブルシューティング ガイド	設置、構成、 から への構成、および から への構成に関するトラブルシューティング ガイドです。さらにこのガイドでは、システム イベント、エラー、Smart Call Home、およびシスコ サポートに関する情報を提供します。
技術メモ	独立したナレッジ ベースからの記事を記載しています。