Cisco UCS Manager リリース 6.0 リリース ノート

最終更新：2025 年 12 月 30 日

Cisco UCS Manager

Cisco UCS™ Manager リリース 6.0 では、複数のシャーシ、Cisco UCS サーバ、および数千の仮想マシンで Cisco ユニファイド コンピューティング™システム (Cisco UCS) のすべてのソフトウェアおよびハードウェア コンポーネントを統合して組み込み管理できます。Cisco UCS Manager は、Cisco UCS Manager 機能すべてで包括的なアクセスのために直感的な GUI、コマンド ライン インターフェイス (CLI)、または XML API を使用して、シングル エンティティとして Cisco UCS を管理します。Cisco UCS Manager の詳細については、Cisco.com の Cisco UCS Manager を参照してください。

このマニュアルには、Cisco UCS Manager リリース 6.0 に関する新機能、解決済みの問題、未解決の問題および回避策の詳細情報が記載されていますこのマニュアルには、次の内容も含まれています。

- 技術マニュアルが発行された後で見つかった最新情報
- このリリースに関連付けられているブレードおよびラック サーバやその他の Cisco Unified Computing System（UCS）コンポーネントに関連するファームウェアおよび BIOS

マニュアルの変更履歴

表 *1 :* リリース *6.0(1)*

リリース	日付	説明
6.0(1c)	2025 年 10 月 9 日	Cisco UCS Manager リリース 6.0(1c) リリース ノート
6.0(1b)	2025 年 9 月 2 日	Cisco UCS Manager リリース 6.0(1b) リリース ノート

新機能

新しいハードウェア機能

- リリース 6.0(1c) の新しいハードウェア：なし

新しいソフトウェア機能

新しいハードウェア機能

リリース 6.0(1b) の新しいハードウェア

- Cisco UCS 6664 ファブリック インターコネクト：Cisco UCS 6664 ファブリック インターコネクト は、データセンター内のトップオブラック展開向けに設計された、2 ラック ユニット（RU）の固定ポート システムです。ファブリック インターコネクトには、イーサネットおよびユニファイド ポートの両方があります。ユニファイド ポートにより、Fibre Channel over Ethernet（FCoE）、ファイバチャネル、NVMe over Fabric、およびイーサネットを提供します。これらの異なるプロトコルをサポートすることにより、サーバーで単一のマルチプロトコル仮想インターフェイス カード（VIC）を実現します。

  Cisco UCS 6664 ファブリック インターコネクト は、ギガビットイーサネット（GbE）、ファイバチャネル（FC）、および Fibre Channel over Ethernet（FCoE）ポートの配列をサポートして、ピア データセンター デバイスへの接続を提供します。このデバイスは、最新のデータセンターでの高性能でスケーラブル、かつセキュアなネットワーキングにも最適です。

- Cisco UCS X215c M8 コンピューティング ノードで UCSX-X10C-PTE3 パス コントローラをサポートします。

- Cisco UCS C225 M8 サーバーで 30TB 2.5 インチ pTLC Micron 6550 NVMe ドライブをサポートします

- Cisco UCS Manager は、Cisco UCS C240 M8 サーバー上の Cisco トライモード M1 24G RAID（UCSC- RAID -M1L16）コントローラのデュアル サポートを導入し、同じサーバー環境内の 2 つのコントローラの独立した構成と管理を可能にします。

新しいソフトウェア機能

リリース 6.0(1b) の新規ソフトウェア機能

次のソフトウェア機能のサポート。

- Linux 監査フレームワーク（auditd）を使用したファブリック インターコネクト監査ログのサポート、Cisco UCS 6600、6500 および 6400 シリーズ ファブリック インターコネクト上のユーザーおよびシステム アクティビティの包括的な監視と追跡。この機能により、アクティビティをファブリック インターコネクト監査ログ ファイルに記録することで、セキュリティと規則遵守を強化できます。

- Cisco UCS X シリーズ ダイレクト（ファブリック インターコネクト 9108 100G）が Cisco UCS C シリーズ ラック サーバーをサポートするようになり、1 つのドメインでUCS X シリーズ コンピューティング ノードと C シリーズ サーバーの両方を統合して管理できます。また、セカンダリ シャーシのサポートも追加され、1 つの X ダイレクト ドメインに 2 番目の UCS X9508 シャーシと最大 20 台のサーバーを展開できます。これらの機能拡張により、拡張性が向上し、データセンターのハードウェア管理が簡素化されます。
- Cisco UCS サーバーのインターネット プロトコル バージョン 6（IPv6）を使用した iSCSI ブートのサポートにより、IPv6 対応 IP ネットワークへのシームレスな統合を実現します。これにより、IPv4 の制限に対応し、次世代のインフラストラクチャ展開の拡張性と管理を向上させます。
- イーサネットアップリンクポートの AES マスター キーおよびMACsec（タイプ 6 [AES]、タイプ 0、およびタイプ 7 暗号化）サポートが、Cisco UCS 6664 ファブリック インターコネクトおよび Cisco UCS X シリーズ ダイレクト（Cisco UCS ファブリック インターコネクト9108 100G）で利用できるようになりました。
- Cisco UCS X シリーズ ダイレクト（Cisco UCS ファブリック インターコネクト 9108 100G）での ERSPAN のサポート。
- Cisco UCS 6600 シリーズ Fabric Interconnect 用の移行のサポート、以下が含まれます。
  - UCS-FI-6454 からUCS-FI-6664 へ
  - UCS-FI-64108 からUCS-FI-6664 へ
  - UCS-FI-6536 からUCS-FI-6664 へ
- vNIC でのネイティブ VLAN 構成の変更に関する警告メッセージを追加しました。ネイティブ VLAN が変更された場合のポート フラップと短時間の接続への影響（約 20 ～ 40 秒）を強調します。この機能強化は、管理者がVLANの変更をより適切に計画および管理するのに役立ちます。
- Cisco UCS C シリーズ M8、M7、および M6 サーバーでのインバンドを介した KVM ダイレクト アクセスのサポート。管理者がインバンドネットワークを介してサーバー コンソールに直接アクセスして管理できるようにし、Cisco UCS C シリーズ サーバーの業務効率と柔軟性を向上させます。
- コマンドライン インターフェイス（CLI）を使用した、Cisco UCS 6400、6500、6600 シリーズ、および X シリーズ ダイレクト ファブリック インターコネクトのすべてのデータの安全な削除のサポート。この機能強化により、すべてのデータを完全に削除し、データの取得や回復の可能性を排除することで、顧客のデータのプライバシーが確保されます。
- ユーザー ログイン試行ルールの設定可能なルールにより、管理者がアクセスを監視および監査できるようになった、強化されたログインプロファイルセキュリティ。システムは、指定された回数の失敗した試行の後に設定された時間、以降のログインをブロックして不正アクセスを防ぐことができます。さらに、Cisco UCS Manager は、認証の失敗について、ユーザー ID、ドメイン ID、IP アドレス、アカウント ステータスなどの詳細情報を提供する syslog メッセージを生成するようになりました。

セキュリティ修正

リリース6.0(1c)でのセキュリティ修正

リリース 6.0(1c) に新しいセキュリティ修正はありません。

リリース6.0(1b)でのセキュリティ修正

不具合 ID - CSCwm98102

Cisco UCS B シリーズ ブレード サーバー、UCS C シリーズ ラック サーバー、UCS X シリーズ コンピューティング ノードには、以下の共通脆弱性識別子（CVE）ID で識別される脆弱性の影響を受ける、オプションの Trusted Platform Module（TPM）2.0 が含まれています：

- CVE-2025-2884：TCG TPM2.0 リファレンスの実装の CryptHmacSign ヘルパー関数は、署名キーのアルゴリズムで署名スキームの検証が不足しているため、境界外読み取りに対して脆弱です。TCG 標準規格 TPM2.0 については、エラッタ リビジョン 1.83 およびアドバイザリ TCGVRT0009 を参照してください。

Cisco UCS サーバーには、次のオプション TPM モジュールのいずれかが搭載されています。

- UCSX-TPM2-002
- UCSX-TPM-002C
- UCS-TPM-002D
- UCSX-TPM-002D

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

不具合 ID - CSCwb83414

Cisco UCS Manager には、次の Common Vulnerabilities および Exposures （CVE）によって識別される脆弱性の影響を受けるサードパーティ ソフトウェアが含まれています。

- CVE-2009-5155：GNU C ライブラリ (glibc) の glob 実装は、長いパターンを適切に処理しません。そのため、コンテキスト依存の攻撃者は、パターン組み立てにより、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2010-3192：GNU C ライブラリ（bcgli）が、setuid/setgid バイナリの LD_AUDIT環境変数の使用を適切に制限していません。そのため、ローカルユーザーはこの変数セットを使用して setuid プログラムを実行して特権を取得できます。
- CVE-2013-0242：GNU C ライブラリ（glibc）の iconv プログラムは、特定の無効なマルチバイト入力シーケンスを適切に処理しません。そのため、リモートの攻撃者がサービス拒否を引き起こしたり、任意のコードを実行したりする可能性があります。

- CVE-2014-4043：GNU C ライブラリ（glibc）の wordexp 関数により、コンテキスト依存の攻撃者は、特定のケースで適切に処理されないシェル文字を使用して、意図されている制限をバイパスできます。
- CVE-2014-9402：GNU C ライブラリ（glibc）の __hcreate_r 関数が整数オーバーフローを適切にチェックしないため、攻撃者は、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2014-9761：GNU C ライブラリ（glibc）の gethostbyname 関数が長いホスト名を適切に処理しないため、リモートの攻撃者がサービス拒否を引き起こすことや、特定できないその他の影響を及ぼす可能性があります。
- CVE-2015-5180：GNU C ライブラリ（glibc）のiconv関数で、特定の入力シーケンスが適切に処理されないため、攻撃者は、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2015-8776：GNU C ライブラリ（glibc）の catopen 関数が負の値を適切に処理しないため、ローカルユーザーは、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2015-8777：GNU C ライブラリ（glibc）の regcomp 関数により、コンテキスト依存の攻撃者は、巧妙に細工された正規表現を介して、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2015-8778：GNU C ライブラリ（glibc）の getnetbyname 関数で、長いネットワーク名が適切に処理されないため、攻撃者は、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2015-8779：GNU C ライブラリ（glibc）の getaliasbyname 関数は、長いエイリアス名を適切に処理しません。これにより、攻撃者は、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2015-8982：GNU C ライブラリ（glibc）の Ann、Nanf、および Nanl 関数が、特定の不正な形式の文字列を適切に処理しません。そのため、攻撃者は、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2015-8983：GNU C ライブラリ（glibc）の strftime 関数は、特定のフォーマット文字列を適切に処理しません。これにより、攻撃者は、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2015-8984：GNU C ライブラリ（glibc）の fnmatch 関数で特定のパターンが適切に処理されないため、攻撃者は、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2015-8985：GNU C ライブラリ（glibc）の glob 関数は、特定のパターンを適切に処理しません。これにより、攻撃者は、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。

- CVE-2016-10228：GNU C ライブラリ（glibc）の iconv プログラムは、特定の不正な形式の入力シーケンスを適切に処理しません。これにより、攻撃者は、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2016-10739：GNU C ライブラリ（glibc）の getaddrinfo 関数は、大きな AF_INET6 応答を適切に処理しません。これにより、リモートの攻撃者は、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2016-1234：GNU C ライブラリ（glibc）のリゾルバの send_dg 関数が特定の応答を適切に処理しません。そのため、リモートの攻撃者は、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2016-4429：GNU C ライブラリ（glibc）のリゾルバが、巧妙に細工された DNS 応答を適切に処理しません。これにより、リモートの攻撃者は、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2017-1000366：GNU C ライブラリ（glibc）のダイナミック リンカーで、特定の環境変数が適切に処理されません。これにより、ローカルの攻撃者は、特権を取得することや、セキュリティ制限をバイパスすることが可能になります。
- CVE-2017-12132：GNU C ライブラリ（glibc）の _dl_init_paths 関数が特定の環境変数を適切に処理しません。これにより、ローカルユーザーは、昇格した特権を取得することや、セキュリティ制限をバイパスすることが可能になります。
- CVE-2017-15670：GNU C ライブラリ（glibc）の glob 関数は、特定のパターンを適切に処理しません。これにより、攻撃者は、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2017-15671：GNU C ライブラリ（glibc）の glob 関数は、メモリ割り当ての失敗を適切に処理しません。これにより、攻撃者は、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2017-15804：GNU C ライブラリ（glibc）の glob 関数は、特定のファイル システム状態を適切に処理しません。これにより、攻撃者は、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2018-1000001：GNU C ライブラリ（gli）の realpath 関数で長いパスが適切に処理されないため、攻撃者は、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2018-11236：GNU C ライブラリ（glibc）は、特定の条件下でスタックポインタの使用を適切に制限していません。これにより、ローカルの攻撃者が、任意コードを実行することや、サービス拒否を生じさせることが可能になります。
- CVE-2018-11237：GNU C ライブラリ（glibc）は、特定のメモリ操作の誤った処理をトリガーする巧妙に細工された入力を介して、攻撃者が、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能にしています。

- CVE-2018-19591：GNU C ライブラリ（glibc）の getcwd 関数は、非常に長いディレクトリ名を適切に処理しません。これにより、ローカルの攻撃者が、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2018-20796：GNU C ライブラリ（glibc）の glob 関数は、巧妙に細工されたパターンを適切に処理しません。これにより、攻撃者が、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2018-6485：GNU C ライブラリ（glibc）の _dl_map_object_from_fd 関数で特定の ELF ファイルが適切に処理されません。これにより、ローカルの攻撃者が、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2019-25013：GNU C ライブラリ（glibc）の iconv 関数で、特定の入力シーケンスが適切に処理されません。これにより、攻撃者が、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2019-6488：GNU C ライブラリ（glibc）の glob 関数は、メモリ割り当ての失敗を適切に処理しません。これにより、攻撃者が、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2019-7309：GNU C ライブラリ（glibc）の glob 関数は、特定の条件で巧妙に細工されたパターンを適切に処理しません。これにより、攻撃者が、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2019-9169：GNU C ライブラリ（glibc）の __libc_open 関数は、特定の状況でファイル記述子を適切に処理しません。これにより、攻撃者が、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2020-10029：32 ビットシステムの GNU C ライブラリ（glibc）の memmem 関数が境界外を読み取る可能性があります。これにより、攻撃者が、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2020-1751：GNU C ライブラリ（glibc）の nss_dns モジュールは、巧妙に細工された DNS 応答を適切に処理しません。これにより、攻撃者が、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2020-1752：GNU C ライブラリ（glibc）の getaddrinfo 関数は、特定の巧妙に細工された応答を適切に処理しません。これにより、攻撃者が、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2020-27618：GNU C ライブラリ（glibc）の iconv 関数で、特定の入力シーケンスが適切に処理されません。これにより、攻撃者が、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2020-29573：GNU C ライブラリ（glibc）の qsort 関数は、ポインタのオーバーフローを適切にチェックしないため、攻撃者が、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。

- CVE-2020-6096：GNU C ライブラリ（glibc）の x86-64 memcpy 関数は、重複するメモリ領域を適切に処理しないため、攻撃者が、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2021-3326：GNU C ライブラリ（glibc）の mq_notify 関数は、特定のパラメータを適切に処理しません。これにより、攻撃者が、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2021-35942：GNU C ライブラリ（glibc）の wordexp 関数は、巧妙に細工されたパターンを適切に処理しません。これにより、攻撃者が、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2021-38604：GNU C ライブラリ（glibc）の iconv 関数で、特定の入力シーケンスが適切に処理されません。これにより、攻撃者が、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2022-23218：GNU C ライブラリ（glibc）のiconv関数で、特定の不正な形式の入力シーケンスが適切に処理されません。これにより、攻撃者が、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2022-23219：GNU C ライブラリ（glibc）の iconv 関数で、特定の不正な形式の入力シーケンスが適切に処理されません。これにより、攻撃者が、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

不具合 ID - CSCwb84351

Cisco UCS Manager には、次の Common Vulnerabilities および Exposures （CVE）によって識別される脆弱性の影響を受けるサードパーティ ソフトウェアが含まれています。

- CVE-2015-5602：1.8.14 より前の sudo は sudoers ルールを適切に解析しないため、ローカル ユーザーが意図した制限をバイパスし、除外（感嘆符）演算子が続くネット グループを含むユーザー指定を介して任意のコマンドを実行できる可能性があります。
- CVE-2016-7076：1.8.18 より前の sudo は、TZ 環境変数を適切に管理しないため、ローカルユーザーはセキュリティ制限をバイパスすることや、sudo コマンドの環境で細工された TZ の値を使用して任意のコードを実行することができます。
- CVE-2017-1000367：1.8.20 より前の sudo では、安全でないライブラリ検索パスが原因で、sudo 権限を持つ攻撃者がルートとして任意のコマンドを実行できる可能性があり、特権昇格が発生する可能性があります。
- CVE-2017-1000368 ：1.8.20 より前の sudo では、特定のコマンドライン引数が不適切に処理されるため、ローカルユーザーが競合状態を利用して、意図しないアクセスを取得することや、別のユーザーとして任意のコマンドを実行することができます。

- CVE-2019-14287：1.8.28 より前の sudoの欠陥により、アクセス許可を持つユーザーは、ルートを除く任意のユーザーとしてコマンドを実行でき、ユーザーID -1 または4294967295を指定してルートとしてコマンドを実行できます。
- CVE-2019-18634- 1.8.26 より前の sudoでは、pwflowebackback オプションが適切に処理されません。これにより、ローカルユーザーがスタックベースのバッファオーバーフローを引き起こし、任意のコードを実行することや、権限を昇格させたりする可能性があります。
- CVE-2021-23239 ー 1.9.5p2 より前の sudo が Runas ユーザー仕様の特定の sudoers ルールを不適切に処理するため、ユーザーがセキュリティポリシーをバイパスして、意図されていないユーザーとしてコマンドを実行できる可能性があります。
- CVE-2021-23240 ー 1.9.5p2 より前の sudoで、ローカルユーザーが sudoers ファイルの不正な解析が原因でRunasユーザー制限をバイパスして、ポリシーで意図されているユーザー以外のユーザーとしてコマンドを実行できる可能性があります。
- CVE-2021-3156：「Baron Samedit」と呼ばれる 1.9.5p2 以前の sudo のヒープベースのバッファ オーバーフローの脆弱性により、ローカル ユーザーがコマンドライン引数の不適切な処理をトリガーしてルート権限を取得できる可能性があります。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

不具合 ID - CSCwf97363

Cisco UCS Manager には、次の Common Vulnerabilities および Exposures （CVE）によって識別される脆弱性の影響を受けるサードパーティ ソフトウェアが含まれています。

- CVE-2012-0876：OpenSSL 1.0.0h より前、および 1.0.1-beta3 より前 1.0.1-beta により、リモートの攻撃者は、範囲外の読み取りをトリガーする巧妙に細工されたレコードを使用して、サービス拒否を引き起こすことができます。
- CVE-2012-2135：Python 2.7.3 より前、および 3.2.3 より前の 3.x は、urllib モジュールの Unicode 文字列を適切に処理しません。これにより、リモートの攻撃者が、クロスサイトスクリプティング（XSS）攻撃を実行したり、機密情報を取得したりできる可能性があります。
- CVE-2013-1753：Python 2.7.5 より前、および 3.3.2 より前の 3.x では、リモートの攻撃者がSSLモジュールへの巧妙に細工された入力を介してサービス拒否を引き起こし、過剰なCPU消費を発生させることができます。
- CVE-2013-2099：バッファ モジュールや unicodeobject モジュールなど、 Pythonの複数の整数オーバーフローの脆弱性により、リモートの攻撃者が任意のコードを実行することや、サービス拒否を引き起こしたりすることがあります。
- CVE-2013-4238：OpenSSL 1.0.1e より前では、特定の DTLS 再送信が適切に処理されないため、リモートの攻撃者が、巧妙に細工されたDTLSパケットを介してサービス拒否を引き起こす可能性があります。

- CVE-2013-7040： Python 2.7.7 より前の 2.7、および 3.3.3 より前の 3.x は、特定の SSL 証明書属性を適切に処理しません。これにより、リモート攻撃者が、巧妙に細工された証明書を介して SSL サーバーをスプーフィングできる可能性があります。
- CVE-2013-7338： Python 2.7.7 より前の 2.7、および 3.3.3 より前の 3.x では、リモートの攻撃者は、 SSL モジュールで無限ループをトリガーする巧妙に細工された入力を介して、サービス拒否を引き起こすことができます。
- CVE-2013-7440：Python 2.7.9 より前、および 3.4.3 より前の 3.x の CGIHTTPServer モジュールにより、リモートの攻撃者は、シェル コマンドを挿入する巧妙に細工されたHTTP要求を介して任意のコードを実行できます。
- CVE-2014-0224：OpenSSL の 1.0.1h より前では、クライアントとサーバーの両方に脆弱がある場合、中間攻撃者が、SSL/TLSハンドシェイク プロセスの欠陥を利用してトラフィックを復号し、変更できます。
- CVE-2014-1912： Python 2.7.7 より前の 2.7、および 3.3.3 よりも前の 3.x では、リモートの攻撃者が、ソケット モジュールへの巧妙に細工された入力を介してサービス拒否を引き起こし、メモリの破損をトリガーする可能性があります。
- CVE-2014-2667：urllib3 ライブラリのバージョン 1.8 より前では、X.509 証明書の subjectAltName フィールドが適切に処理されないため、リモートの攻撃者が、巧妙に細工された証明書を使用して SSL サーバーをスプーフィングできる可能性があります。
- CVE-2014-4616：OpenSSL の 1.0.1i より前では、DTLS パケットの処理が適切に制限されないため、リモートの攻撃者は、巧妙に細工されたDTLSハンドシェイク メッセージを介してサービス拒否を引き起こすことができます。
- CVE-2014-4650：Python 2.7.8 より前、および 3.4.2 より前の 3.x の ssl モジュールは、特定の TLS ハンドシェイク メッセージを適切に処理しません。これにより、リモート攻撃者がサービス拒否を引き起こす可能性があります。
- CVE-2014-7185：Python 2.7.9 より前、および 3.4.3 より前の 3.x では、リモートの攻撃者が、安全でないロードをトリガーする巧妙に細工されたピクルデータを介して任意のコードを実行できるようになります。
- CVE-2014-9365：Python 2.7.9 より前、および 3.4.3 より前の 3.x の電子メール モジュールでは、特定のヘッダーが適切に処理されません。これにより、リモートの攻撃者がヘッダー インジェクション攻撃を実行する可能性があります。
- CVE-2015-1283：Python 2.7.9 より前、および 3.4.3 より前の 3.x の zipimport モジュールでの整数オーバーフローにより、攻撃者が任意のコードを実行したり、細工されたZIPアーカイブを介してサービス拒否を引き起こしたりできる可能性があります。
- CVE-2015-20107： Python 3.10.0 ～ 3.10.6 および 3.11.0a1 ～ 3.11.0b3 では、特定のファイルを解析するときに mailcap モジュールを介したコマンド インジェクションが可能で、攻撃者が任意のコマンドを実行できる可能性があります。

- CVE-2015-5652：OpenSSL 1.0.2d および 1.0.1p より前では、特定のASN.1 構造が適切に検証されないため、リモートの攻撃者がサービス拒否を引き起こしたり、任意のコードを実行したりする可能性があります。
- CVE-2016-0718：Python 2.7.11 より前、および 3.4.4 より前の 3.x の _json モジュールで、コンテキスト依存の攻撃者が、誤った例外をトリガーする巧妙に細工された JSON ドキュメントを介してサービス拒否を引き起こす可能性があります。
- CVE-2016-0772：Python 2.7.10 より前、および 3.4.4 より前の 3.x の ssl.match_hostname 関数は、ホスト名の IP アドレスを適切に照合しないため、攻撃者はSSLサーバーをスプーフィングできる可能性があります。
- CVE-2016-1000110：urllib3 およびリクエスト ライブラリ（urllib3 1.23 およびリクエスト 2.20.0 より前）は、特定の HTTP ヘッダーを適切に処理しません。これにより、リモートの攻撃者が巧妙に細工されたヘッダーを介してCRLFインジェクション攻撃を実行する可能性があります。
- CVE-2016-2183：SWEET32 攻撃は、TLSの 64 ビットブロック暗号（3DES や Blowfish など）に影響を与え、リモートの攻撃者が長時間の暗号化セッションに対するグリーティング攻撃を介してプレーン テキスト データを回復できるようにします。
- CVE-2016-3189：Python 2.7.12 より前、および 3.5.2 より前の 3.x では、ssl.match_hostname 関数を使用する場合に証明書が適切に検証されないため、リモートの攻撃者が SSL サーバーをスプーフィングできる可能性があります。
- CVE-2016-4472：Python 2.7.13 より前、および 3.5.2 より前の 3.x は、httplib モジュールの特定の HTTP 応答を適切に処理しません。これにより、リモートの攻撃者が HTTP ヘッダー攻撃を実行する可能性があります。
- CVE-2016-5636：OpenSSL 1.0.2i および 1.0.1u より前では、特定の証明書フィールドが適切に検証されないため、リモートの攻撃者が、なりすまし攻撃を実行したり、サービス拒否を引き起こしたりする可能性があります。
- CVE-2016-5699：Python 2.7.13 より前、および 3.5.2 より前の 3.x は、urllib の特定の HTTP 応答を適切に処理しません。これにより、攻撃者がHTTP応答分割攻撃を実行できる可能性があります。
- CVE-2016-9063：OpenSSL や NSS で使用されている DES 暗号と Triple DES 暗号には、約 40 億ブロックの誕生日攻撃の制約があり、リモートの攻撃者がこの攻撃（SWEET32）によって平文データを回復することを可能にしています。
- CVE-2017-1000158： Python 2.7.13 以前の 2.7 、および 3.6.1 以前の 3.x は、urllib および http ライブラリの特定の Unicode 文字列を適切に処理しないため、リモートの攻撃者が CRLF インジェクション攻撃を実行する可能性があります。
- CVE-2017-9233： Python 2.7.14 以前、および 3.6.2 以前の 3.x の _strxfrm 関数で特定の入力が適切に検証されないため、攻撃者がサービス拒否を引き起こしたり、任意のコードを実行したりする可能性があります。

- CVE-2018-1000030：Python 2.7.14 より前、および 3.6.4 より前の 3.x で、symlinks とともに shutil.rmtree を使用すると、ローカルの攻撃者が競合状態を介して任意のファイルを削除できる場合があります。
- CVE-2018-1000802- Python 2.7、3.4、3.5 および 3.6 では、ローカル ユーザーが、昇格された権限でスクリプトを実行するときにシステム ディレクトリの前に検索されるローカル ディレクトリ内のトロイの木馬モジュールを介してルートとして任意のコードを実行できます。
- CVE-2018-1060： Python 2.7.15 より前の 2.7、および 3.4.6 より前の 3.x、および 3.5.3 より前の 3.5.x で、difflib および poplib モジュールの特定の正規表現が正しく処理されないため、攻撃者が拒否を引き起こす可能性があります。
- CVE-2018-1061： Python 2.7.15 より前の 2.7、および 3.4.6 より前の 3.x、および 3.5.3 より前の 3.5.x では、リモート攻撃者が、細工された電子メールアドレスを使用して email.utils.parseaddr 関数を利用し、サービス拒否を引き起こすことが可能です。
- CVE-2018-14647：PyYAML ライブラリ 4.1 より前のバージョンでは、yaml.load 関数の安全でない使用が原因で、リモートの攻撃者が巧妙に細工された YAML 入力を介して任意のコードを実行できます。
- CVE-2018-20406： Python 2.7.16 より前の 2.7、および 3.4.10 より前の 3.x、 3.5.7 より前の 3.5.x、および 3.6.9 より前の 3.6.x は、difflib モジュールの特定の正規表現を正しく処理しません。攻撃者がサービス拒否を引き起こす可能性があります。
- CVE-2018-20852： Python 3.7.4 より前の 3.7.x、および 3.8.1 より前の 3.8.x では、urllib.parse モジュールの特定の入力が適切に処理されないため、攻撃者が URL 解析の制限をバイパスできる可能性があります。
- CVE-2018-25032：zlib 1.2.11 までには、inflateMark 関数に関連するメモリ破損の問題があります。これにより、攻撃者がサービス拒否を引き起こしたり、任意のコードを実行したりする可能性があります。
- CVE-2019-10160：Python 2.7（2.7.16 より前）および 3.x（3.7.3 より前）では、difflib モジュールの特定の正規表現が正しく処理されないため、攻撃者がサービス拒否を引き起こす可能性があります。
- CVE-2019-12900：zlib 1.2.11 までには、inflate 関数にメモリ破損の問題があります。これにより、リモートの攻撃者がサービス拒否を引き起こしたり、任意のコードを実行したりする可能性があります。
- CVE-2019-15903： Python 2.7（2.7.17 より前）および 3.x（3.7.5 より前）では、tarfile モジュールの入力が適切に検証されないため、リモート攻撃者が細工された TAR アーカイブを介して意図したディレクトリ外のファイルを書き込む可能性があります。
- CVE-2019-16056：Python 2.7（2.7.17 より前）および 3.x（3.7.5 より前）は、http.client モジュールの特定の入力を適切に処理しません。これにより、攻撃者がHTTPヘッダーインジェクション攻撃を実行できる可能性があります。

- CVE-2019-16935：Python 2.7（2.7.18 より前）および 3.x（3.7.6 より前）には、XML 解析モジュール（xmlrpc）に問題があります。これにより、リモート攻撃者が細工された XML データを介してサービス拒否を引き起こす可能性があります。
- CVE-2019-18348：urllib3 の 1.25.3 より前のライブラリでは、別のホストへのリダイレクトが発生したときに承認ヘッダーが適切に削除されないため、リモートの攻撃者がリダイレクトされた要求をインターセプトして機密情報を取得できる可能性があります。
- CVE-2019-20907： Python 3.4.x から 3.8.x では re モジュールの特定の正規表現が誤って処理され、攻撃者が巧妙に細工された正規表現パターンを介してサービス拒否を引き起こす可能性があります。
- CVE-2019-5010：Python 2.7.16 より前、および 3.x（3.7.2 より前）では、xmlrpc.client および xmlrpc.server モジュールへの特定の入力で null バイトが誤って処理され、リモートの攻撃者がサービス拒否を引き起こす可能性があります。
- CVE-2019-9636：Python 3.x（3.7.3 より前）は、urlsplit および urlparse 関数で入力を適切にサニタイズしないため、攻撃者がセキュリティ制限をバイパスしたり、 URL スプーフィングなどの攻撃を実行したりする可能性があります。
- CVE-2019-9674： Python 3.0 ～ 3.7.2 では、zipfile モジュール内の特定の細工された ZIP アーカイブが不適切に処理され、攻撃者がサービス拒否を引き起こしたり、任意のコードを実行したりする可能性があります。
- CVE-2019-9947：Python 2.7（2.7.16 より前）および 3.x（3.7.3 より前）では、urllib モジュールの特定の改行文字が誤って処理され、攻撃者が HTTP ヘッダーインジェクション攻撃を実行する可能性があります。
- CVE-2019-9948： Python 2.7（2.7.16 より前）および 3.x（3.7.3 より前）では、urllib モジュールの特定の入力が誤って処理され、攻撃者がHTTPヘッダーインジェクション攻撃を実行する可能性があります。
- CVE-2020-10735： Python 3.7 から 3.10 では、int から大きな整数への変換が誤って処理されるため、攻撃者が過剰な CPU 使用によってサービス拒否を引き起こす可能性があります。
- CVE-2020-14422： Python 2.7（2.7.18 より前）および 3.x（3.7.7 より前）では、http.client モジュールの特定の入力が誤って処理され、攻撃者が HTTP ヘッダーインジェクション攻撃を実行する可能性があります。
- CVE-2020-15523： Python 2.7（2.7.18 より前）および 3.x（3.8.4 より前）は、difflib および poplib モジュールの特定の正規表現を誤って処理するため、攻撃者がサービス拒否を引き起こす可能性があります。
- CVE-2020-15801：Python 3.8.x（3.8.5 より前）では、tarfile モジュールの特定の入力が誤って処理され、リモート攻撃者が細工された TAR アーカイブを介して意図したディレクトリ外のファイルに書き込める可能性があります。

- CVE-2020-26116：Python 3.x（3.9.0 より前）は、difflib モジュールの特定の正規表現を誤って処理するため、攻撃者が過剰なCPU消費によってサービス拒否を引き起こす可能性があります。
- CVE-2020-27619：Python 3.8.x（3.8.6 より前）は、http.client モジュールの特定の入力を誤って処理するため、攻撃者がHTTPヘッダー攻撃を実行できる可能性があります。
- CVE-2020-8315： Python 2.7（2.7.18 より前）および 3.x（3.8.3 より前）では、urllib モジュールの特定の入力が誤って処理されるため、攻撃者がHTTPヘッダーインジェクション攻撃を実行する可能性があります。
- CVE-2020-8492： Python 2.7（2.7.18 より前）および 3.x（3.8.2 より前）では、urllib.parse モジュールの特定の入力が誤って処理されるため、攻撃者がセキュリティ制限をバイパスしたり、 URLスプーフィングなどの攻撃を実行したりする可能性があります。
- CVE-2021-23336： Python 3.6.x ～ 3.8.x は、urllib.parse モジュールの特定の URL を誤って処理するため、攻撃者がセキュリティ制限をバイパスしたり、 URL スプーフィングなどの攻撃を実行したりする可能性があります。
- CVE-2021-3177：Python 3.x（3.9.2 より前）では、ctypes モジュールの PyCArg_repr 関数にバッファ オーバーフローがあります。これにより、攻撃者が任意のコードを実行したり、サービス拒否を引き起こしたりできる可能性があります。
- CVE-2021-3426：Python 3.7.x（3.7.10 より前）、3.8.x（3.8.8 より前）、および 3.9.x（3.9.2 より前）では、re モジュールで特定の正規表現が誤って処理され、過剰な CPU 使用率により、攻撃者がサービス拒否を引き起こす可能性があります。
- CVE-2021-3733： Python 3.6.x ～ 3.9.x では、urllib.parse モジュールの特定の入力が誤って処理され、攻撃者がセキュリティ制限をバイパスしたり、 URL スプーフィングなどの攻撃を実行したりする可能性があります。
- CVE-2021-3737： Python 3.6.x ～ 3.9.x では、urllib.parse モジュールの特定の入力が誤って処理され、攻撃者がセキュリティ制限をバイパスしたり、 URL スプーフィングなどの攻撃を実行したりする可能性があります。
- CVE-2021-4189： Python 3.6.x ～ 3.9.x は、urllib.request モジュールの特定の入力を誤って処理するため、攻撃者がセキュリティ制限をバイパスしたり、 URL スプーフィングなどの攻撃を実行したりする可能性があります。
- CVE-2022-0391： Python 3.7.x ～ 3.9.x は、urllib.parse モジュールの特定の入力が誤って処理するため、攻撃者がセキュリティ制限をバイパスしたり、 URL スプーフィングなどの攻撃を実行したりする可能性があります。
- CVE-2022-26488： Python 2.7（2.7.18 より前）および 3.x（3.8.10 より前）では、http.client モジュールの特定の入力が誤って処理されるため、攻撃者が HTTP ヘッダーインジェクション攻撃を実行できる可能性があります。
- CVE-2022-37454：Python 3.15 より前の、PyCryptodome で使用されている「random」モジュールは、特定の条件下で予測可能な乱数を生成する可能性があります。これにより、暗号化操作が低下し、攻撃者が秘密値を推測できる可能性があります。

- CVE-2022-45061： Python 3.9.x（3.9.16 より前）、3.10.x（3.10.9 より前）、および 3.11.x（3.11.1 より前）では、urllib モジュールで特定の正規表現が誤って処理され、過剰な CPU 使用率により、攻撃者がサービス拒否を引き起こす可能性があります。
- CVE-2023-24329： Python 3.x（3.10.10 より前）、および 3.11.x（3.11.2 より前）は、空白文字を含む URL を適切に解析しないため、攻撃者はセキュリティチェックをバイパスしたり、スプーフィング攻撃を実行したりできる可能性があります。
- CVE-2023-27043： Python 3.7.x ～ 3.11.x は、urllib.parse モジュールの特定の入力を誤って処理するため、攻撃者は入力検証をバイパスして、 HTTPヘッダーインジェクションやその他の攻撃を実行する可能性があります。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

不具合 ID：**CSCwf97368**

Cisco UCS Manager には、次の Common Vulnerabilities および Exposures （CVE）によって識別される脆弱性の影響を受けるサードパーティ ソフトウェアが含まれています。

- CVE-2011-2939： Perl 5.14.2 および 5.12.4 より前のバージョンでは、コンテキスト依存の攻撃者は、ヒープ ベースのバッファ オーバーフローをトリガーする巧妙に細工された正規表現を使用して、任意のコードを実行したり、サービス拒否を引き起こしたりできます。
- CVE-2012-5195：3.63 より前のPerl CGI モジュールにより、リモートの攻撃者は、特定の CGI パラメータの値に改行文字を使用してHTTPヘッダーを挿入できます。
- CVE-2012-6329：Perl 5.16.1 より前の エンコードモジュールは、特定の UTF-8 入力を適切に処理しません。そのため、コンテキスト依存の攻撃者が、サービス拒否を引き起こしたり、任意のコードを実行したりする可能性があります。
- CVE-2013-1667：Perl 5.14.3 より前、および 5.16.3 より前の 5.16.x の CGI モジュールは、MIMEヘッダー内の特殊文字を適切に処理しません。これにより、リモートの攻撃者が、任意の HTTP ヘッダーを挿入できる可能性があります。
- CVE-2014-4330：Perl 5.20.1 より前では、特定の巧妙に細工された正規表現が誤って処理されます。これにより、コンテキスト依存の攻撃者がサービス拒否を引き起こしたり、任意のコードを実行したりする可能性があります。
- CVE-2015-8853 - 2.26 より前のPerlの File::Temp モジュールが、一時ファイルのアクセス許可を適切にチェックしないため、ローカルユーザーが機密情報を取得したり、シンボリック リンク攻撃を介してデータを変更したりする可能性があります。
- CVE-2016-1238：Perl 5.24.1 より前では、ライブラリパスが正しく検索されないため、ローカルユーザーが安全でないディレクトリのトロイの木馬モジュールを介して任意のコードを実行できる可能性があります。

- CVE-2016-2381：5.24.0 より前の Perl の DB_File モジュールにより、コンテキスト依存の攻撃者、任意のコードを実行したり、メモリ破損をトリガーする巧妙に細工された入力を介してサービス拒否を引き起こしたりできます。
- CVE-2017-12814：Perl 5.24.3 より前、および 5.26.1 より前の 5.26.x の XSLoader モジュールは、特定の入力が適切に処理されません。これにより、攻撃者が任意のコードを実行したり、サービス拒否を引き起こしたりする可能性があります。
- CVE-2017-12837：Perl 5.26.2 より前では、特定の巧妙に細工された正規表現が誤って処理されます。これにより、コンテキスト依存の攻撃者がサービス拒否を引き起こしたり、任意のコードを実行したりする可能性があります。
- CVE-2017-12883：Perl 5.26.2 より前では、特定の巧妙に細工された正規表現が誤って処理されます。これにより、コンテキスト依存の攻撃者がサービス拒否を引き起こしたり、任意のコードを実行したりする可能性があります。
- CVE-2018-12015：Perl 2.24 より前のPerlの Archive::Tar モジュールにより、リモートの攻撃者は TAR アーカイブ内のシンボリックリンク攻撃を介して任意のファイルを上書きできます。
- CVE-2018-18311：Perl 5.28.1 より前では、特定の巧妙に細工された正規表現が誤って処理されます。これにより、コンテキスト依存の攻撃者がサービス拒否を引き起こしたり、任意のコードを実行したりする可能性があります。
- CVE-2018-18312：Perl 5.28.1 より前では、特定の巧妙に細工された正規表現を誤って処理します。これにより、コンテキスト依存の攻撃者がサービス拒否を引き起こしたり、任意のコードを実行したりする可能性があります。
- CVE-2018-18313：Perl 5.28.1 より前では、特定の巧妙に細工された正規表現を誤って処理します。これにより、コンテキスト依存の攻撃者がサービス拒否を引き起こしたり、任意のコードを実行したりする可能性があります。
- CVE-2018-18314：Perl 5.28.1 より前では、特定の巧妙に細工された正規表現を誤って処理します。これにより、コンテキスト依存の攻撃者がサービス拒否を引き起こしたり、任意のコードを実行したりする可能性があります。
- CVE-2018-6913：5.26.2 より前の Perl の Encode モジュールにより、コンテキスト依存の攻撃者が、バッファ オーバーフローをトリガーする巧妙に細工された入力を介してサービス拒否を引き起こす可能性があります。
- CVE-2020-10543 - 5.30.3 より前のPerl は特定の巧妙に細工された正規表現を誤って処理し、コンテキスト依存の攻撃者がサービス拒否を引き起こしたり、任意のコードを実行したりする可能性があります。
- CVE-2020-10878 - 5.30.3 より前のPerl は特定の巧妙に細工された正規表現を誤って処理し、コンテキスト依存の攻撃者がサービス拒否を引き起こしたり、任意のコードを実行したりする可能性があります。

- CVE-2020-12723 - 5.30.3 より前のPerl は特定の巧妙に細工された正規表現を誤って処理し、コンテキスト依存の攻撃者がサービス拒否を引き起こしたり、任意のコードを実行したりする可能性があります。
- CVE-2023-31486：2.40 より前の Perl の「Archive::Tar」モジュールは、TAR アーカイブのファイルパスを適切に検証しません。これにより、攻撃者は、細工されたアーカイブを介して意図されたディレクトリ外のファイルに書き込みを行える可能性があります。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

欠陥 ID - CSCwb84668

Cisco UCS Manager には、次の Common Vulnerabilities および Exposures （CVE）によって識別される脆弱性の影響を受けるサードパーティ ソフトウェアが含まれています。

- CVE-2014-9471：2.26 より前の util-linux の chfn および chsh ユーティリティは、ユーザー入力の改行文字を適切にチェックしません。これにより、ローカル ユーザーがセキュリティ制限をバイパスしたり、構成ファイルに悪意のあるコンテンツを挿入したりできる可能性があります。
- CVE-2015-4042：2.26.2 より前の util-linux の runuser が環境変数を適切にクリアしないため、ローカルユーザーが巧妙に細工された環境を介して特権を取得したり、セキュリティ制限をバイパスしたりする可能性があります。
- CVE-2016-2781：8.25 より前の GNU coreutils の chroot ユーティリティが、コマンドを実行する前に補足グループを適切にドロップしないため、ローカルユーザーが意図されているセキュリティ制限をバイパスする可能性があります。
- CVE-2017-18018：2.30.2 より前の util-linux の runuser が環境変数を適切にクリアしないため、ローカルユーザーが巧妙に細工された環境を介して特権を取得したり、セキュリティ制限をバイパスしたりする可能性があります。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

Resfrom led の警告

リリースで解決済みの問題 6.0(1c)

不具合 ID	症状	影響を受ける最初のバンドル	リリースで解決済み
CSCwq58890	Cisco UCS VIC 15000 シリーズ アダプタのファームウェアが更新され、まれに発生する断続的なメモリの問題が修正され、さまざまなメモリ タイプおよび構成でより堅牢なかつ一貫性のある動作が保証されます。 （注） それでもメモリ エラーが発生する場合は、Cisco TAC にお問い合わせください。	6.0(1b)	6.0(1c)

リリースで解決済みの問題 6.0(1b)

不具合 ID	症状	影響を受ける最初のバンドル	リリースで解決済みバンドル
CSCwo62993	トラストポイントの設定の変更後、一部の Cisco UCS Manager ドメインでセキュア LDAP認証が断続的に失敗します。この問題は、**TLS 開始失敗**エラーや**不明な CA** アラートとして現れ、証明書の検証に問題があることを示します。影響を受けるドメインでは、LDAP サーバーへのネットワーク接続があるにもかかわらず、SSL の検証中に**ローカル発行者証明書のエラーを取得できない**と表示されます。 この問題は解決されました。	4.3 (3a)	6.0(1b)
CSCwp64077	Cisco UCS FI の snmpd プロセスで、カーネルメッセージ **sap recovering failed and so Killed with SIGABRT - kernel** によりトリガーされたクラッシュが繰り返し発生します。 このクラッシュは、BRIDGE- MIB [1.3.6.1.2.1.17 で始まる OID] の OID をクエリすると発生することがあります。 この問題は解決されました。	4.3(5a)A	6.0(1b)A

未解決の不具合

リリースで未解決の問題 6.0(1c)

リリース 6.0(1c) に未解決の問題はありません。

リリースで未解決の問題 6.0(1b)

次の警告は、リリース 6.0(1b)で未解決です。

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCwq17020	UCSX-X10C-RAIDF コントローラ の背後に 3.8TB以上の容量のU3 Micron ドライブを JBOD モードで取り付けた後、EFI ブートイメージのロードに関連する BIOS エラーが原因で Linux OS が起動に失敗します。 この問題は、特に Intel® プロセッサを搭載した Cisco UCS M8 サーバーで発生し、複数のLinuxディストリビューションに影響します。 ドライブが RAID 0 で構成されている場合、問題は発生しません。より小さい容量のドライブを使用している場合、またはRAID 0 を使用している場合、Microsoft Windows® および Linux OS は正常に起動します。	RAIDで構成されたドライブにOSをインストールします。	4.3 (6a)

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCwq34720	**セキュア ブート** を有効にしてWindows 2022 Server を実行している Cisco UCS X210c M7 コンピューティングノードの再関連付けは、次のエラーで失敗します：`SBAT self-check failed: Security Policy Violation`	BIOS トークンから SBAT 変数を削除し、その後 CMOS クリアを実行します。この後、サービスプロファイルの関連付けはセキュアブートが有効な状態で正常に完了し、システムは正常にブートできるようになります。 TAC に問い合わせてサポートを依頼することを推奨します。	4.3(5c)B
CSCwq94580	インフラストラクチャ A バンドルをリリース 6.0(1b) にアップグレードした後、Cisco UCS C シリーズ M5 ラックサーバーでのサーバーメンテナンス操作は、アップグレード中に検出されたサポートされていないハードウェアまたはソフトウェア構成が原因で失敗する可能性があります。 この問題は、Cisco UCS FI モデル 6400 シリーズ、6536、および UCSX-S9108-100G を備えたセットアップで発生します。	最初にセカンダリロール FI を再起動し、それから順番に FI を再起動する必要があります。 （注） FI の再起動は中断を伴う操作であり、一時的なサービスの中断を引き起こします。このタスクは、メンテナンス時間帯に実行を予定することを推奨します。 TAC に問い合わせてサポートを依頼することを推奨します。	6.0(1b)

既知の動作と制限事項

リリース 6.0(1c) の既知の動作および制限事項

リリース 6.0(1c) には、新しい既知の制限はありません。

リリース 6.0(1b) の既知の動作および制限事項

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCwq41000	Cisco UCS X210c サーバー向け Broadcom AERO RAID controller（UCSX-X10C-RAIDF）および Cisco 12G Modular Raid コントローラ、4GB キャッシュ付き（UCSC-RAID-M6T）は、**[自動構成モード（ACM、Auto Configuration Mode）]** がRAID0に設定されていた場合、ストレージプロファイルの再展開およびサーバーの再起動後、ドライブの状態を **[未設定で良好（UG、Unconfigured Good）]** から **[オンライン（Online）]** 状態に遷移しません。結果として、RAID0 LUN は作成されません。 この問題は、4GB キャッシュ搭載の Cisco Tri-Mode 24G SAS RAID コントローラ（UCSC- RAID-HP）でのドライブ状態遷移および RAID0 LUN 作成に影響します。	既知の回避策はありません。	6.0(1b)

互換性

C シリーズ ラックマウント サーバ向け Cisco UCS Manager および Cisco UCS C シリーズ リリース互換性マトリックス

Cisco UCS C シリーズ ラックマウント サーバは、内蔵スタンドアロン ソフトウェア (Cisco Integrated Management Controller (Cisco IMC)) によって管理されます。しかし、C シリーズ ラックマウント サーバを Cisco UCS Manager と統合すると、Cisco IMC ではサーバを管理しません。

各 Cisco UCS Manager リリースには、対応する C シリーズ スタンドアロン リリースが組み込まれています。たとえば、 Cisco UCS Manager リリース 4.3(6) には、すべての M8、M7、M6 および S3260 M5 サーバー向けの 4.3(6) サーバー バンドルが含まれ、他のすべての M5 サーバー向けの 4.3(2) サーバーバンドルが含まれます。これにより、C シリーズ スタンドアロン リリースにリストされているすべての M8、M7、M6、および M5 サーバーのサポートが保証されます。

Cisco Intersight、Cisco IMC、および Cisco UCS Manager の Cisco UCS 同等性マトリックスでは、Cisco Intersight、Cisco Integrated Management Controller（IMC）、および Cisco UCS Manager（UCSM）のリリースタイムラインの概要を説明しています。これには、各パッチが公開された日付、特定のパッチバージョン、各リリースでサポートされているプラットフォームなどの重要な情報が含まれます。このマトリックスを参照することで、サーバーを Cisco Intersight に移行する前にサーバーに必要な適切なファームウェアとソフトウェアのバージョンを特定できます。これにより、サーバーインフラストラクチャが引き続きサポートされ、移行中および移行後も効率的に動作することが保証されます。

次の表には、C シリーズ ラックマウント サーバの Cisco UCS Manager および C シリーズ ソフトウェア スタンドアロン リリースを示します。

表 *2 : C* シリーズ サーバ向け *Cisco UCS Manager* および *C* シリーズ ソフトウェア リリース

Cisco UCS Manager リリース	C シリーズ スタンドアロン リリースが含まれています	C シリーズ スタンドアロン リリースでサポートされる c シリーズ サーバ
6.0(1)	6.0(1)	すべての M8、M7、M6、および S3260 M5
	4.3(2)	すべての M5
4.3(6)	4.3(6)	すべての M8、M7、M6、および S3260 M5
	4.3(2)	すべての M5
4.3(5)	4.3(5)	すべての M8、M7、および M6
	4.3(4)	S3260 M5
	4.3(2)	すべての M5

Cisco UCS Manager リリース	C シリーズ スタンドアロン リリースが含まれています	C シリーズ スタンドアロン リリースでサポートされる c シリーズ サーバ
4.3(4)	4.3(4)	C245 M8 すべての M7、M6、および S3260 M5
	4.3(2)	すべての M5
4.3(3)	4.3(3)	すべての M7、M6、および S3260 M5
	4.3(2)	すべての M5
4.3(2)	4.3(2)	すべての M7、M6、および M5
4.2(3)	4.2(3)	すべての M6、M5、および S3260 M4
	4.1(3)	すべての M5 および S3260 M4
	4.1(2)	C220 M4、C240 M4、および C460 M4
4.2(2)	4.2(2)	すべての M6、M5、および S3260 M4
	4.1(3)	S3260 M4、すべての M5
	4.1(2)	C220 M4、C240 M4、C460 M4
4.2(1)	4.2(1)	すべての M6
	4.1(3)	S3260 M4、すべての M5
	4.1(2)	C220 M4、C240 M4、C460 M4
4.1(3)	4.1(3)	S3260 M4、すべての M5
	4.1(2)	C220 M4、C240 M4、C460 M4
	3.0 (4)	すべての M3
4.1(2)	4.1(2)	C220 M5, C240 M5、C240 SD M5 、C480 M5、S3260 M5、C480 M5 ML、C125 M5、C220 M4、C240 M4、C460 M4、S3260 M4
	3.0 (4)	すべての M3

Cisco UCS Manager リリース	C シリーズ スタンドアロン リリースが含まれています	C シリーズ スタンドアロン リリースでサポートされる c シリーズ サーバ
4.1(1)	4.1(1)	C220 M5、C240 M5、C480 M5、S3260 M5、C125 M5、C480 M5 ML のみ
	4.0(2)	C220 M4、C240 M4、C460 M4、S3260 M4、 C125 M5のみ
	3.0 (4)	すべての M3
4.0(4)	4.0(4)	C220 M5、C240 M5、C480 M5、S3260 M5、 C480 M5 ML のみ
	4.0(2)	C220 M4、C240 M4、C460 M4、S3260 M4、 C125 M5のみ
	3.0 (4)	すべての M3
4.0(2)	4.0(2)	C220 M4、C240 M4、C460 M4、C220 M5、C240 M5、C480 M5、S3260 M4、S3260 M5、C125 M5、C480 M5 ML のみ
	3.0 (4)	すべての M3
4.0(1)	4.0(1)	C220 M4、C240 M4、C460 M4、C220 M5、C240 M5、C480 M5、S3260 M4、S3260 M5、C125 M5 のみ
	3.0 (4)	すべての M3

バージョンをまたがるファームウェアのサポート

Cisco UCS Manager の A バンドル ソフトウェア（Cisco UCS Manager、Cisco NX OS、IOM、および FEX ファームウェア）は、サーバー上で以前のリリースの B または C バンドル リリース（ホスト ファームウェア [FW]、BIOS、Cisco IMC、アダプタ FW およびドライバ）と混在させることができます。有効な組み合わせをすばやく確認するために、このリリースには、次の場所にあるインタラクティブな互換性ツールが含まれています。

Cisco UCS Manager クロスバージョン ファームウェア マトリクス

目的のインフラストラクチャ（A バンドル）およびホスト ファームウェア（B および C バンドル）リリースとともにファブリック インターコネクト モデルを選択することにより、ツールは、各組み合わせがサポートされている構成かどうかを動的に表示します。

（注） Cisco UCS Manager リリース 6.0(1b)以降では、Cisco UCS 6300 シリーズ FI と Cisco UCS 6332 FI はサポートされていません。

表 *3 : Cisco UCS 6664*、*6536*、および *6400* シリーズ ファブリック インターコネクトでサポートされる混在 *Cisco UCS* リリース

	インフラストラクチャのバージョン（**A** バンドル）								
ホストFWのバージョン（BまたはCバンドル）	4.2(1)	4.2(2)	4.2(3)	4.3(2)	4.3(3)	4.3(4)	4.3(5)	4.3(6)	6.0(1)
6.0(1)	—	—	—	—	—	—	—	—	6664、6536、6454、64108
4.3(6)	—	—	—	6332、6332-16UP、6454、64108、6536	6332、6332-16UP、6454、64108、6536	6332、6332-16UP、6454、64108、6536	6332、6332-16UP、6454、64108、6536	6332、6332-16UP、6454、64108、6536	6536、6454、64108
4.3(5)	—	—	—	6332、6332-16UP、6454、64108、6536	6332、6332-16UP、6454、64108、6536	6332、6332-16UP、6454、64108、6536	6332、6332-16UP、6454、64108、6536	6332、6332-16UP、6454、64108、6536	6536、6454、64108
4.3(4)	—	—	—	6332、6332-16UP、6454、64108、6536	6332、6332-16UP、6454、64108、6536	6332、6332-16UP、6454、64108、6536	6332、6332-16UP、6454、64108、6536	6332、6332-16UP、6454、64108、6536	6536、6454、64108
4.3(3)	—	—	—	6332、6332-16UP、6454、64108、6536	6332、6332-16UP、6454、64108、6536	6332、6332-16UP、6454、64108、6536	6332、6332-16UP、6454、64108、6536	6332、6332-16UP、6454、64108、6536	6536、6454、64108

	インフラストラクチャのバージョン（A バンドル）								
4.3(2)	—	—	—	6332、6332-16UP、6454、64108、6536	6332、6332-16UP、6454、64108、6536	6332、6332-16UP、6454、64108、6536	6332、6332-16UP、6454、64108、6536	6332、6332-16UP、6454、64108、6536	6536、6454、64108
4.2(3)	6200、6332、6332-16UP、6454、64108	6200、6332、6332-16UP、6454、64108	6200、6332、6332-16UP、6454、64108、6536	6332、6332-16UP、6454、64108、6536	6332、6332-16UP、6454、64108、6536	6332、6332-16UP、6454、64108、6536	6332、6332-16UP、6454、64108、6536	6332、6332-16UP、6454、64108、6536	6536、6454、64108
4.2(2)	6200、6332、6332-16UP、6454、64108	6200、6332、6332-16UP、6454、64108	6200、6332、6332-16UP、6454、64108	6332、6332-16UP、6454、64108	6332、6332-16UP、6454、64108	6332、6332-16UP、6454、64108	6332、6332-16UP、6454、64108	6332、6332-16UP、6454、64108	—
4.2(1)	6200、6332、6332-16UP、6454、64108	6200、6332、6332-16UP、6454、64108	6200、6332、6332-16UP、6454、64108	6332、6332-16UP、6454、64108	6332、6332-16UP、6454、64108	6332、6332-16UP、6454、64108	6332、6332-16UP、6454、64108	6332、6332-16UP、6454、64108	—

表 *4 : Cisco UCS X* シリーズ ダイレクト でサポートされる混合 *Cisco UCS* リリース

ホスト FW バージョン（B バンドル）	インフラストラクチャのバージョン（A バンドル）			
	4.3(4)	4.3(5)	4.3(6)	6.0(1)
6.0(1)	—	—	—	UCSX-S9108-100G
4.3(6)	UCSX-S9108-100G	UCSX-S9108-100G	UCSX-S9108-100G	UCSX-S9108-100G
4.3(5)	UCSX-S9108-100G	UCSX-S9108-100G	UCSX-S9108-100G	UCSX-S9108-100G
4.3(4)	UCSX-S9108-100G	UCSX-S9108-100G	UCSX-S9108-100G	UCSX-S9108-100G

Cisco UCS ファブリック インターコネクトでサポートされる混合 Cisco UCS リリースの拡張バージョンは、Cisco UCS Manager クロスバージョンファームウェア サポート 6.0で確認することもできます。

参考のため、Cisco Intersight、Cisco IMC、および Cisco UCS Manager の Cisco UCS 同等性マトリックスでは、 Cisco Intersight、Cisco Integrated Management Controller（Cisco IMC）、および

Cisco UCS Manager のリリース タイムラインの概要を説明しています。これには、各パッチが公開された日付、特定のパッチバージョン、各リリースでサポートされているプラットフォームなどの重要な情報が含まれます。このマトリックスを参照することで、サーバーを Cisco Intersight に移行する前にサーバーに必要な適切なファームウェアとソフトウェアのバージョンを特定できます。これにより、サーバーインフラストラクチャが引き続きサポートされ、移行中および移行後も効率的に動作することが保証されます。

アップグレードとダウングレードのガイドライン

Cisco IMC で可能なすべてのアップグレード パスの完全な概要を取得するには、「Cisco UCS Manager アップグレード/ダウングレード サポート マトリクス」を参照してください。

リリース 6.0(1) へのアップグレードおよびダウングレード：

- セットアップに Cisco UCS 6664 ファブリック インターコネクト が備わっている場合、インフラストラクチャ ファームウェア バージョン（A バンドル）を 6.0(1b) より前のリリースにダウングレードすることはできません。
- セットアップに Cisco UCS X シリーズ ダイレクト（ファブリック インターコネクト 9108 100G）および Cisco UCS C シリーズ ラック サーバーまたはセカンダリ シャーシが備わっている場合、6.0(1b) より前のリリースにダウングレードことはできません。
- セットアップに Cisco UCS C240 M8 サーバー上の Cisco トライモード M1 24G RAID （UCSC-RAID -M1L16）コントローラが含まれている場合、 6.0(1b)より前のリリースにダウングレードすることはできません。
- 次の機能のいずれかをいったん有効にすると、6.0(1b)より前のリリースにダウングレードすることはできません。以前のリリースにダウングレードする前に、まずこれらの機能を無効にする必要があります。
  - Cisco UCS 6600、6500、または 6400 シリーズ ファブリック インターコネクトでの Linux 監査フレームワーク（auditd）を使用した**ファブリック インターコネクト監査ログ** のサポート
  - Cisco UCSサーバー向けインターネット プロトコル バージョン 6（IPv6）を使用した iSCSI ブートのサポート
  - Cisco UCS 6664 ファブリック インターコネクトおよび Cisco UCS X シリーズ ダイレクト（Cisco UCS ファブリック インターコネクト 9108 100G）のイーサネット アップリンク ポートの AES マスター キーおよび MACsec （タイプ 6 [AES]、タイプ 0、およびタイプ 7 暗号化）のサポート
  - Cisco UCS X シリーズ ダイレクト（Cisco UCS ファブリック インターコネクト 9108 100G）での ERSPAN のサポート

表 *5 :* リリース *6.0(1)* へのアップグレード パス

リリースからアップグレード	推奨されるアップグレード パス
任意の 4.3(6) リリースからのアップグレード	リリース 6.0(1) への直接アップグレードまたはダウングレード。
任意の 4.3(5) リリースからのアップグレード	リリース 6.0(1) への直接アップグレードまたはダウングレード。
任意の 4.3(4) リリースからのアップグレード	リリース 6.0(1) への直接アップグレード。 ダウングレード： **1.** リリース 6.0(1) からリリース 4.3(5) への最初のダウングレード。 **2.** リリース 4.3(4) へのダウングレード。
4.3(3) リリースからのアップグレード	リリース 6.0(1) への直接アップグレード。 ダウングレード： **1.** リリース 6.0(1) からリリース 4.3(5) への最初のダウングレード。 **2.** リリース 4.3(3) へのダウングレード。
4.3(2) リリースからのアップグレード	リリース 6.0(1) への直接アップグレード。 ダウングレード： **1.** リリース 6.0(1) からリリース 4.3(5) への最初のダウングレード。 **2.** リリース 4.3(2) へのダウングレードします。
任意の 4.2(3) リリースからのアップグレード	リリース 6.0(1) への直接アップグレード。 ダウングレード： **1.** リリース 6.0(1) からリリース 4.3(5) への最初のダウングレード。 **2.** リリース 4.2(3) へのダウングレード。

リリースからアップグレード	推奨されるアップグレード パス
その他の古いリリース	アップグレード： 1. リリース 4.2(3) 以降へのアップグレード。 （注） リリース 4.2(3) への推奨アップグレード パスを特定するには、Cisco UCS Manager リリース 4.2 のリリース ノートを 参照してください。 2. ダウンロードとリリース 6.0(1) へのアップグレード。 ダウングレード： 1. リリース 6.0(1) からリリース 4.3(5) への最初のダウングレード。 2. 任意の他の古いリリースへのダウングレード。 （注） ダウングレード先の特定のバージョンについては、Cisco UCS Manager のリリース ノートを参照してください。

UCS Manager の正常性およびアップグレード前チェック ツール

UCS Manager の正常性およびアップグレード前チェック ツールは、アップグレード前にクラスタが正常であることを確認するために設計された、自動正常性およびアップグレード前チェック機能を提供します。この健全性チェックを実行するだけでなく、正常でないと判明したすべてのクラスタに対して修正措置を講じることが必要です。続行する前に、UCS Manager 正常性チェックによって報告されたすべての問題を修正してください。

内部的な依存関係

ここでは、Cisco UCS ハードウェアと Cisco UCS Manager の各バージョン間の相互依存について説明します。以下の考慮点を含んでいます。

- DIMM などのサーバ FRU アイテムのバージョン依存関係は、サーバ タイプによって異なります。
- ファンや電源などのシャーシのアイテムは、Cisco UCS Manager のすべてのバージョンで動作します。

このリリースでは、選択したリリースに基づいてインフラストラクチャ リリース、ファブリック インターコネクト、サーバー、VIC、および IOM モジュールのサポートされている組み合わせを迅速に判断するために役立つ、対話型の互換性ルックアップツールを使用できます。

Cisco UCS Manager 内部依存関係マトリックス

参考として、次の内部依存関係テーブルの完全バージョンも参照できます。Cisco UCS Manager の内部依存関係、リリース 6.0

サードパーティ ストレージ ベンダーの Cisco UCS NVMeoF サポート マトリクス

表 *6 :* サードパーティ ストレージ ベンダーの *Cisco UCS NVMeoF* サポート マトリクス

ストレージ ベンダー	機能	ストレージ アレイ	Cisco UCS FI	Cisco UCS VIC	オペレーティング システム
NetApp Inc.®	NVMe-FC	ONTAP 9.7 以降	6400 シリーズ 6536	1400 14000 15000	ESXi 7.0U3+ ESXi 8.0+ RHEL 8.6+ RHEL 9.0+ SLES 15SP3+
	NVMe-FC	ONTAP 9.13 以降	UCSX-S9108-100G	15000	ESXi 7.0U3+ ESXi 8.0U2+ RHEL 8.9+ RHEL 9.3+ SLES 15SP4+
	NVMe-FC	ONTAP 9.16 以降	6664	15000 14000	ESXi 8.0 U3+ ESXi 9.0+ RHEL 9.6+ RHEL 10+ SLES 15SP5+
	NVMe-TCP	ONTAP 9.10 以降	6400 シリーズ 6536	1400 14000 15000	ESXi 7.0U3+ ESXi 8.0+ RHEL 9.0+ SLES 15SP3+
	NVMe-TCP	ONTAP 9.13 以降	UCSX-S9108-100G	15000	ESXi 7.0U3+ ESXi 8.0U2+ RHEL 9.3+ SLES 15SP4+
	NVMe-TCP	ONTAP 9.16 以降	6664	15000 14000	ESXi 8.0 U3+ ESXi 9.0+ RHEL 9.6+ RHEL 10+ SLES 15SP5+

ストレージ ベンダー	機能	ストレージ アレイ	Cisco UCS FI	Cisco UCS VIC	オペレーティング システム
（注） Cisco UCS VIC 1300 シリーズは、RHEL 8.6+ 以降でのみサポートされます。 最新のストレージ アレイ サポートの詳細については、 https://hwu.netapp.com/ を参照してください。 互換性情報にアクセスするには、有効な NetApp® アカウントが必要です。 NetApp E シリーズまたは SolidFIre ストレージ モデルではテストされていません。					

ストレージ ベンダー	機能	ストレージ アレイ	Cisco UCS FI	Cisco UCS VIC	オペレーティング システム
Pure Storage, Inc.®	NVMe-FC	Purity//FA 6.1 以降	6300 6400	1300	RHEL 8.6+
	NVMe-FC	Purity//FA 6.1 以降	6300 6400 6536	1400 14000 15000	ESXi 7.0U3+ ESXi 8.0+ RHEL 8.6+ RHEL 9.0+ SLES 15SP1+
	NVMe-FC	Purity//FA 6.6.3 以降	UCSX-S9108-100G	15000	ESXi 7.0U3+ RHEL 8.6+ SLES 15SP3+ ESXi 8.0 RHEL 9.0+
	NVMe-FC	Purity//FA 6.8.7 以降	6664	15000 14000	ESXi 8.0 U3+ ESXi 9.0+ RHEL 9.6+ RHEL 10+ SLES 15SP5+
	NVMe-ROCEv2	Purity//FA 5.2 以降	6300 6400 6536	1400 14000 15000	RHEL 7.2+ RHEL 8.0+ RHEL 9.0+
	NVMe-ROCEv2	Purity//FA 5.2 以降	6400 6536	1400 14000 15000	ESXi 7.0U3 ESXi 8.0
	NVMe-ROCEv2	Purity//FA 6.6.3 以降	UCSX-S9108-100G	15000	ESXi 7.0U3+ ESXi 8.0U2+ RHEL 8.9+ RHEL 9.3+
	NVMe-ROCEv2	Purity//FA 6.8.7 以降	6664	15000 14000	

ストレージ ベンダー	機能	ストレージ アレイ	Cisco UCS FI	Cisco UCS VIC	オペレーティング システム
					ESXi 8.0 U3+ ESXi 9.0+ RHEL 9.6+ RHEL 10+ SLES 15SP5+
	NVMe-TCP	Purity//FA 6.4.2 以降	6300 6400 6536	1400 14000 15000	ESXi 7.0U3+ RHEL 9.0+ SLES 15SP3+
	NVMe-TCP	Purity//FA 6.6.3 以降	UCSX-S9108-100G	15000	ESXi 7.0U3+ ESXi 8.0U2+ RHEL 8.9+ RHEL 9.3+ SLES 15SP4+
	NVMe-TCP	Purity//FA 6.8.7 以降	6664	15000 14000	ESXi 8.0 U3+ ESXi 9.0+ RHEL 9.6+ RHEL 10+ SLES 15SP5+

ストレージ ベンダー	機能	ストレージ アレイ	Cisco UCS FI	Cisco UCS VIC	オペレーティング システム
Dell Inc.®	NVMe-FC	PowerStore PowerMax	6300 6400 6536	1400 14000 15000	ESXi 7.0U3+ RHEL 8.6+ SLES 15SP3+
	NVMe-FC	PowerStore PowerMax	UCSX-S9108-100G	15000	ESXi 7.0U3+ ESXi 8.0U2+ RHEL 8.9+ RHEL 9.3+ SLES 15SP4+
	NVMe-FC	PowerStore PowerMax	6664	15000 14000	ESXi 8.0 U3+ ESXi 9.0+ RHEL 9.6+ RHEL 10+ SLES 15SP5+
	NVMe-TCP	PowerStore PowerMax	6300 6400 6536	1400 14000 15000	ESXi 7.0U3+ RHEL 8.6+ SLES 15SP3+
	NVMe-TCP	PowerStore PowerMax	UCSX-S9108-100G	15000	ESXi 7.0U3+ ESXi 8.0U2+ RHEL 8.9+ RHEL 9.3+ SLES 15SP4+
	NVMe-TCP	PowerStore PowerMax	6664	15000 14000	ESXi 8.0 U3+ ESXi 9.0+ RHEL 9.6+ RHEL 10+ SLES 15SP5+

（注） **[OS サポート（ OS Support ）]** 列の+ は、そのリリース トレインの新しいリリースを指します。

Cisco UCS FI アプライアンス ポート サポート マトリクス

表 *7 : Cisco UCS FI* アプライアンス ポート サポート マトリクス

プロトコル	ベンダー	パートナーサポート	シスコサポート
Nvme-TCP	NetApp Inc.® (ONTAP)	サポート対象	サポート対象
	DELL EMC®	サポート対象	サポート対象
	Pure Storage Inc.®	サポート対象	サポート対象
RoceV2	NetApp Inc.® (ONTAP)	サポート対象外	サポート対象外
	DELL EMC®	サポート対象外	サポート対象外
	Pure Storage Inc.®	サポート対象外	サポート対象外
ISCSI	NetApp Inc.® (ONTAP)	サポート対象	サポート対象
	DELL EMC®	サポート対象	サポート対象
	Pure Storage Inc.®	サポート対象	サポート対象

Cisco UCS ファブリック インターコネクトおよびスイッチの互換性マトリクス

Cisco ファブリック インターコネクトおよび MDS スイッチの互換性およびサポート マトリックス

表 *8 : Cisco UCS* ファブリック インターコネクトおよび *MDS* リリースのサポート マトリックス

ファブリック インターコネクト	MDS の以前のサポート対象リリース	MDS の推奨リリース
Cisco UCS 6664 FI	9.2	9.4
Cisco UCS 6536 FI	9.2	9.4
Cisco UCS 6454 FI	9.2	9.4
Cisco UCS 64108 FI	9.2	9.4
Cisco UCS X シリーズ ダイレクト	-	9.4

（注） サポートされている古いリリースでは、MDS 推奨のマイナー バージョンのみがサポートされます。詳細については、Cisco MDS 9000 シリーズ スイッチの推奨リリースを参照してください。

Cisco ファブリック インターコネクトおよび Nexus スイッチの互換性およびサポート マトリックス

表 *9 : Cisco* ファブリック インターコネクトおよび *Nexus* スイッチ *6.0(1)* の互換性およびサポート マトリックス

ファブリック インターコネクト	NX-OS の以前のサポート対象リリース	NX-OS の推奨リリース
Cisco UCS 6664 FI	—	10.5(x)
Cisco UCS 6536 FI	—	10.5(x)
Cisco UCS 6454 FI	—	10.5(x)
Cisco UCS 64108 FI	—	10.5(x)
Cisco UCS X シリーズ ダイレクト	—	10.5(x)

Cisco ファブリック インターコネクトおよび Brocade スイッチの互換性およびサポート マトリックス

表 *10 : Cisco UCS* ファブリック インターコネクトおよび *Brocade* リリース サポート マトリックス

Cisco UCS ファブリック インターコネクト	Brocade の以前のサポート対象リリース	Brocade の推奨リリース
Cisco UCS 6664 FI	—	9.2
Cisco UCS 6536 FI	—	9.2
Cisco UCS 6454 FI	—	9.2
Cisco UCS 64108 FI	—	9.2
Cisco UCS X シリーズ ダイレクト	—	9.2

サポート対象ハードウェアおよびソフトウェア

サポートされるオペレーティング システム

サポートされているオペレーティング システムの詳細については、インタラクティブな『UCS ハードウェアおよびソフトウェアの互換性』マトリックスを参照してください。

サポートされる Web ブラウザ

Cisco UCS Manager GUI にアクセスするには、Windows、Linux RHEL、および MacOS でサポートされているブラウザのいずれかの最新バージョンを使用することを推奨します。

- Microsoft Edge
- Mozilla Firefox

- Google Chrome
- Apple Safari

（注） HTML 5 UI は、ブラウザあたり 1 つのユーザ セッションをサポートします。

デフォルトのオープン ポート

次の表に、Cisco UCS Manager リリース 6.0 で使用されるデフォルトのオープン ポートを示します。

ポート	インターフェイス	プロトコル	トラフィック タイプ	ファブリック インターコネクト	使用方法
22	CLI	SSH	TCP	UCS 6664 FI UCS 6400 シリーズ FI UCS 6536 FI UCSX-S9108-100G	Cisco UCS Manager CLI アクセス
80	XML	HTTP	TCP	UCS 6664 FI UCS 6400 シリーズ FI UCS 6536 FI UCSX-S9108-100G	Cisco UCS Manager GUI およびサードパーティ管理ステーション。 クライアント ダウンロード
443	XML	HTTP	TCP	UCS 6664 FI UCS 6400 シリーズ FI UCS 6536 FI UCSX-S9108-100G	Cisco UCS Manager ログイン ページ アクセス Cisco UCS Manager XML API アクセス
743	KVM	HTTP	TCP	UCS 6664 FI UCS 6400 シリーズ FI UCS 6536 FI UCSX-S9108-100G	CIMC Web サービス / ダイレクト KVM
7546	CFS	CFSD	[TCP]	UCS 6664 FI UCS 6400 シリーズ FI UCS 6536 FI UCSX-S9108-100G	Cisco ファブリック サービス

ネットワーク要件

『*Cisco UCS Manager* 管理者用管理ガイド、リリース *6.0*』には、Intersight デバイス コネクタの設定に関する詳細情報が掲載されています。

Cisco UCS Central 統合

Cisco UCS Central および Cisco UCS Manager の互換性バージョンの完全なリストについては、『Cisco UCS Central のリリース ノート』の「機能サポート マトリクス」を参照してください。

このリリースでサポートされているプラットフォーム

リリース 6.0(1b)

次のサーバーはこのリリースでサポートされており、同じリリース トレイン内の後続のリリースでも引き続きサポートされます。

- Cisco UCS C240 M8 サーバ
- Cisco UCS C220 M8 サーバ
- Cisco UCS C225 M8 サーバ
- Cisco UCS C245 M8 サーバ
- Cisco UCS X210c M8 コンピューティング ノード
- Cisco UCS X215c M8 コンピューティング ノード
- Cisco UCS C240 M7 サーバ
- Cisco UCS C220 M7 サーバ
- Cisco UCS X410c M7 コンピューティングノード
- Cisco UCS X210c M7 コンピューティング ノード
- Cisco UCS C220 M6 サーバ
- Cisco UCS C240 M6サーバ
- Cisco UCS C245 M6サーバ
- Cisco UCS C225 M6サーバ
- Cisco UCS B200 M6サーバ
- Cisco UCS X210c M6 コンピューティングノード
- Cisco UCS B200 M5 サーバ
- Cisco UCS B480 M5 サーバ
- Cisco UCS S3260 M5 サーバ
- Cisco UCS C220 M5 サーバ

- Cisco UCS C240 M5 サーバ
- Cisco UCS C240 SD M5 サーバ
- Cisco UCS C480 M5 サーバ
- Cisco UCS C480 M5 ML サーバー
- Cisco UCS C125 M5 サーバ

その他のハードウェア

すべてのシャーシ、ファブリック インターコネクト、ファブリック エクステンダ、拡張モジュール、および電源については、最新のソフトウェアバージョンを使用することを推奨します。混合環境の最小ソフトウェアバージョンを確認するには、バージョンをまたがるファームウェアのサポート （25 ページ） を参照してください。次に、サポートされている他のハードウェアのリストを示します。

UCS 6600 シリーズ ファブリック インターコネクトでサポートされるハードウェア

表 *11 : UCS 6600* シリーズ ファブリック インターコネクトでサポートされるハードウェア

タイプ	詳細
シャーシ	Cisco UCSX-9508 シャーシ （Cisco UCS X シリーズ サーバ向け）
ファブリック インターコネクト	UCS 6664
ファブリック エクステンダ	93180YC-FX3（25G サーバー ポート） UCSX-I-9108-25G または UCSX-I-9108-100G（Cisco UCS X シリーズ サーバでサポート）
電源モジュール	UCS-PSU-6600-AC UCSX-PSU-2800AC（Cisco UCSX-9508 シャーシ 向け）

UCS 6500 シリーズ ファブリック インターコネクトでサポートされるハードウェア

表 *12 : UCS 6500* シリーズ ファブリック インターコネクトでサポートされるハードウェア

タイプ	詳細
シャーシ	UCSB-5108-AC2 UCSB-5108-DC2 Cisco UCSX-9508 シャーシ （Cisco UCS X シリーズ サーバ向け）

タイプ	詳細
ファブリック インターコネクト	UCS 6500
ファブリック エクステンダ	93180YC-FX3（25G サーバー ポート） 93180YC-FX3（10G サーバー ポート） 2408 UCSX-I-9108-25G または UCSX-I-9108-100G（Cisco UCS X シリーズ サーバでサポート）
電源モジュール	UCS-PSU-6536-AC UCSX-PSU-2800AC（Cisco UCSX-9508 シャーシ 向け）

UCS 6400 シリーズ ファブリック インターコネクトでサポートされるハードウェア

表 *13 : UCS 6400* シリーズ ファブリック インターコネクトでサポートされるハードウェア

タイプ	詳細
シャーシ	UCSC-C4200-SFF N20 – N20-C6508 UCSB-5108-DC UCSB-5108-AC2 UCSB-5108-DC2 UCSB-5108-HVDC Cisco UCSX-9508 シャーシ （Cisco UCS X シリーズ サーバ向け）
ファブリック インターコネクト	UCS 64108 UCS 6454
ファブリック エクステンダ	93180YC-FX3（25G サーバー ポート） 93180YC-FX3（10G サーバー ポート） 2408 UCSX-I-9108-25G
電源モジュール	UCS-PSU-6332-AC UCS-PSU-6332-DC UCS PSU-64108-AC UCS-PSU-6332-DC

Cisco UCS X シリーズ ダイレクト のサポート対象ハードウェア

表 *14 : Cisco UCS X* シリーズ ダイレクトのサポート対象シャーシ

シャーシ	最小ソフトウェア バージョン	推奨ソフトウェアバージョン
Cisco UCS X9508 シャーシ	4.3(4b)	6.0(1c)

表 *15 : Cisco UCS X* シリーズ ダイレクト のサポート対象ハードウェア

ファブリック インターコネクト	最小ソフトウェア バージョン	推奨ソフトウェアバージョン
Cisco UCS 9108-100G	4.3(4b)	6.0(1c)

GB コネクタ モジュール、トランシーバ モジュールおよびケーブル

次に、Gb コネクタ モジュール、トランシーバ モジュール、サポートされているケーブルのリストを示します。

（注）
- 特定のファブリック インターコネクトでサポートされているトランシーバ モジュールとケーブルは、そのファブリック インターコネクトと互換性のあるすべての VIC アダプタ、IOM、または FEX でサポートされているとは限りません。トランシーバ モジュールの詳細な互換性マトリックスについては、次を参照してください。https://www.cisco.com/c/en/us/support/interfaces-modules/transceiver-modules/products-device-support-tables-list.html
- たとえば、S クラス トランシーバ QSFP 40 G-SR4 S は FCoE をサポートしていません。

表 *16 : Cisco UCS 6600* シリーズ *Fabric Interconnect*

Gb コネクタ モジュール	トランシーバ モジュールおよびケーブル
UCS 6600 シリーズ ファブリック インターコネクトの FC SFP	DS-SFP-FC16G-SW DS-SFP-FC32G-SW DS-SFP-FC64G-SW DS-SFP-FC16G-LW DS-SFP-FC32G-LW DS-SFP-FC64G-LW

Gb コネクタ モジュール	トランシーバ モジュールおよびケーブル
UCS 6600 シリーズ ファブリック インターコネクト向けユニファイド ポートの **10GbE**	SFP-H10GB-CU1M SFP-H10GB-CU2M SFP-H10GB-CU3M SFP-H10GB-CU5M SFP-H10GB-ACU7M SFP-H10GB-ACU10M SFP-10G-AOC1M SFP-10G-AOC10M
UCS 6600 シリーズ ファブリック インターコネクト向け **100G** ポート（および **QSA** ）の **10GbE**	SFP-10G-SR SFP-10G-SR-S SFP-10G-LR SFP-10G-LR-S
UCS 6600 シリーズ ファブリック インターコネクト向けユニファイド ポートの **25GbE**	SFP-25G-SR-S SFP-10/25G-LR-S SFP-10/25G-CSR-S SFP-25G-SL SFP-H25G-SFP-H10GB-CU1M SFP-H25G-CU2M SFP-H25G-SFP-H10GB-CU3M SFP-H25G-CU4M SFP-H25G-CU5M SFP-25G-AOC1M SFP-25G-AOC2M SFP-25G-AOC3M SFP-25G-AOC4M SFP-25G-AOC5M SFP-25G-AOC7M SFP-25G-AOC10M
UCS 6600 シリーズ ファブリック インターコネクト向け **100G** ポート（および **QSA28** ）の **25GbE**	SFP-25G-SR-S SFP-25G-SL

Gb コネクタ モジュール	トランシーバ モジュールおよびケーブル
UCS 6600 シリーズ ファブリック インターコネクト向け **40GbE**	QSFP-40G-SR4 QSFP-40G-SR4-S QSFP-40G-LR4 QSFP-H40G-CU1M QSFP-H40G-CU3M QSFP-H40G-CU5M QSFP-H40G-ACU7M QSFP-H40G-AOC3M QSFP-H40G-AOC5M QSFP-H40G-AOC7M QSFP-H40G-AOC15M QSFP-H40G-AOC20M QSFP-H40G-AOC25M QSFP-H40G-AOC30M CVR-QSFP-SFP10G

Gb コネクタ モジュール	トランシーバ モジュールおよびケーブル
UCS 6600 シリーズ ファブリック インターコネクト向け **100GbE**	QSFP-100G-SR4-S QSFP-100G-PSM4-S QSFP-100G-SM-SR QSFP-100G-SL4 QSFP-40/100-SRBD QSFP-100G-DR-S QSFP-100G-FR-S QSFP-100G-SR1.2 QSFP-100 G-CU1M QSFP-100G-CU2M QSFP-100G-CU3M QSFP-100G-CU5M QSFP-100G-AOC1M QSFP-100G-AOC2M QSFP-100G-AOC3M QSFP-100G-AOC5M QSFP-100G-AOC7M QSFP-100G-AOC10M QSFP-100G-AOC15M QSFP-100G-AOC20M QSFP-100G-AOC25M QSFP-100G-AOC30M

表 *17 : Cisco UCS 6500* シリーズ ファブリック インターコネクト

Gb コネクタ モジュール	トランシーバ モジュールおよびケーブル
UCS 6500 シリーズ ファブリック インターコネクト	DS-SFP-4X32G-SW
UCS 6500 シリーズ ファブリック インターコネクト向け **1GbE**	GLC-TE（QSA）、ポート 9、10 GLC-SX-MMD (QSA)

Gb コネクタ モジュール	トランシーバ モジュールおよびケーブル
UCS 6500 シリーズ ファブリック インターコネクト向け **10GbE**	SFP-10G-SR (QSA) SFP-10G-SR-S(QSA) SFP-10G-LR (QSA) SFP-10G-LR-S (QSA) CVR-QSFP-SFP10G SFP-H10GB-CU1M
UCS 6500 シリーズ ファブリック インターコネクト向け **25GbE**	SFP-10/25G-LR-S SFP-10/25G-CSR-S SFP-25G-SL CVR-QSFP28-SFP25G SFP-H25G-CU1M (P1) SFP-H25G-CU2M (P1) SFP-H25GB-CU3M SFP-25G-AOC2M SFP-25G-AOC3M SFP-25G-SR-S

Gb コネクタ モジュール	トランシーバ モジュールおよびケーブル
UCS 6500 シリーズ ファブリック インターコネクト向け **40GbE**	QSFP-H40G-AOC1M QSFP-H40G-AOC2M QSFP-H40G-AOC3M QSFP-H40G-AOC5M QSFP-H40G-AOC15M QSFP-H40G-AOC25M QSFP-40G-CU1M QSFP-40G-CU2M QSFP-40G-CU3M QSFP-40G-CU5M QSFP-40G-SR4 QSFP-40G-SR4-S QSFP-40G-CSR4 QSFP-40G-LR4 QSFP-40G-LR4-S QSFP-4SFP10G-CU1M QSFP-4SFP10G-CU3M FET-40G （注） FET-40G は、FI と IOM/FEX の間でのみサポートされます。 QSFP-40G-ACU10M QSFP-40G-SR-BD QSFP-100G40G-BIDI （注） QSFP-100G40G-BIDI は、40G モードのボーダーポート/アップリンク ポートでのみサポートされます。

Gb コネクタ モジュール	トランシーバ モジュールおよびケーブル
UCS 6500 シリーズ ファブリック インターコネクト向け **100GbE**	QSFP-100G-SR1.2 QSFP-100G-SR4-S QSFP-100G-LR4-S QSFP-100G-SM-SR QSFP-100G-SL4 QSFP-40/100-SRBD（または） QSFP-100G40G-BIDI （注） QSFP-100G40G-BIDI は、100G モードの FI と I9108-100G IOM/N9K-C93180YC-FX3 FEX/ボーダー ポート間でサポートされます。 QSFP-100 G-CU1M QSFP-100G-CU2M QSFP-100G-CU3M QSFP-100G-CU5M QSFP-4SFP25G-CU1M QSFP-4SFP25G-CU2M QSFP-4SFP25G-CU3M QSFP-4SFP25G-CU5M QSFP-100G-AOC1M QSFP-100G-AOC2M QSFP-100G-AOC3M QSFP-100G-AOC5M QSFP-100G-AOC7M QSFP-100G-AOC10M QSFP-100G-AOC15M QSFP-100G-AOC20M QSFP-100G-AOC25M QSFP-100G-AOC30M QSFP-100G-DR-S QSFP-100G-FR-S

表 *18 : Cisco UCS 6400* シリーズ ファブリック インターコネクト

Gb コネクタ モジュール	トランシーバ モジュールおよびケーブル
UCS 6400 シリーズ ファブリック インターコネクト	DS-SFP-FC8G-SW DS-SFP-FC8G-LW DS-SFP-FC16G-SW DS-SFP-FC16G-LW DS-SFP-FC32G-SW DS-SFP-FC32G-LW
UCS 6400 ファブリック インターコネクトの **100-Gb**	QSFP-100G-SR1.2 QSFP-40/100G-SRBD QSFP-100G-SR4-S QSFP-100G-LR4-S QSFP-100G-SM-SR QSFP-100 G-CU1M QSFP-100G-CU2M QSFP-100G-CU3M QSFP-100G-AOC1M QSFP-100G-AOC2M QSFP-100G-AOC3M QSFP-100G-AOC5M QSFP-100G-AOC7M QSFP-100G-AOC10M QSFP-100G-AOC15M QSFP-100G-AOC20M QSFP-100G-AOC25M QSFP-100G-AOC30M QSFP-4SFP25G-CU1M QSFP-4SFP25G-CU2M QSFP-4SFP25G-CU3M QSFP-4SFP25G-CU5M

Gb コネクタ モジュール	トランシーバ モジュールおよびケーブル
UCS 6400 シリーズ ファブリック インターコネクトの **40-Gb**	QSFP-40G-SR4 QSFP-40G-SR4-S QSFP-40G-SR-BD QSFP-40G-LR4 QSFP-40G-LR4-S QSFP-40G-ER4 WSP-Q40GLR4L QSFP-H40G-CU1M QSFP-H40G-CU3M QSFP-H40G-CU5M QSFP-H40G-ACU7M QSFP-H40G-ACU10M QSFP-H40G-AOC1M QSFP-H40G-AOC2M QSFP-H40G-AOC3M QSFP-H40G-AOC5M QSFP-H40G-AOC10M QSFP-H40G-AOC15M QSFP-4SFP10G-CU1M QSFP-4SFP10G-CU3M QSFP-4SFP10G-CU5M QSFP-4X10G-AC7M QSFP-4X10G-AC10M QSFP-4X10G-AOC1M QSFP-4X10G-AOC3M QSFP-4X10G-AOC5M QSFP-4X10G-AOC7M
UCS 6454 ファブリック インターコネクトの **32-Gb FC**	DS-SFP-FC32G-SW DS-SFP-FC32G-LW
UCS 6454 ファブリック インターコネクトの **25-Gb**	UCSC-O- M5S100GF[1]

Gb コネクタ モジュール	トランシーバ モジュールおよびケーブル
UCS 6400 シリーズ ファブリック インターコネクトの **25-Gb**	SFP-25G-SR-S SFP-H25G-SFP-H10GB-CU1M SFP-H25G-CU2M SFP-H25G-SFP-H10GB-CU3M SFP-H25G-CU5M SFP-H25G-AOC1M SFP-H25G-AOC2M SFP-H25G-AOC3M SFP-H25G-QSFP-4X10G-AOC5M SFP-H25G-QSFP-4X10G-AOC7M SFP-H25G-QSFP-4X10G-AOC10M SFP-10/25G-LR-S SFP-10/25G-CSR-S
UCS 6454 ファブリック インターコネクト向け **16-Gb**	DS-SFP-FC16G-LW DS-SFP-FC16G-SW

Gb コネクタ モジュール	トランシーバ モジュールおよびケーブル
UCS 6400 ファブリック インターコネクトの **10-Gb**	SFP-10G-SR SFP-10G-SR-S SFP-10G-LR SFP-10G-LR-S SFP-10G-ER SFP-10G-ER-S SFP-10G-ZR SFP-10G-ZR-S FET-10G （注） FET-10G はファブリック インターコネクトと IOMs/FEXs 間でのみサポートされています。 SFP-10G-LRM SFP-H10GB-CU1M SFP-H10GB-CU2M SFP-H10GB-CU3M SFP-H10GB-CU5M SFP-H10GB-ACU7M SFP-H10GB-ACU10M SFP-10G-AOC1M SFP-10G-AOC2M SFP-10G-AOC3M SFP-10G-AOC5M SFP-10G-AOC7M SFP-10G-AOC10M
UCS 6400 シリーズ ファブリック インターコネクト向け **8-Gb**	DS-SFP-FC8G-SW DS-SFP-FC8G-LW
UCS 6400 ファブリック インターコネクトの **1-Gb**	GLC-TE GLC-SX-MMD SFP-GE-T

[1] (Cisco UCS Manager リリース 4.1(2) からサポート)

表 *19 : Cisco UCS X* シリーズ ダイレクトのサポート *GB* コネクタ モジュール

Gb コネクタ モジュール	ケーブル
100-GbE	QSFP-100G-SR4-S QSFP-100G-SR4-S（ブレークアウト） QSFP-100G-LR4-S QSFP-100G-SM-SR QSFP-100G-SL4 QSFP-100G-SL4（ブレークアウト） QSFP-100G-SR1.2 QSFP-40/100-SRBD QSFP-100G-DR-S QSFP-100G-FR-S QSFP-100 G-CU1M QSFP-100G-CU2M QSFP-100G-CU3M QSFP-100G-CU5M QSFP-100G-AOC1M QSFP-100G-AOC2M QSFP-100G-AOC3M QSFP-100G-AOC5M QSFP-100G-AOC7M QSFP-100G-AOC10M QSFP-100G-AOC15M QSFP-100G-AOC20M QSFP-100G-AOC25M QSFP-100G-AOC30M
40 GbE	QSFP-40G-SR4 QSFP-40G-SR4（ブレークアウト） QSFP-40G-SR4-S QSFP-40G-SR4-S（ブレークアウト） QSFP-40G-CSR4 QSFP-40G-CSR4（ブレークアウト） QSFP-40G-SR-BD

Gb コネクタ モジュール	ケーブル
4X25GbE	QSFP-4SFP25G-CU1M QSFP-4SFP25G-CU2M QSFP-4SFP25G-CU3M QSFP-4SFP25G-CU5M
10GbE X 4	QSFP-4SFP10G-CU1M QSFP-4SFP10G-CU2M QSFP-4SFP10G-CU3M QSFP-4X10G-AOC3M QSFP-4X10G-AOC5M
QSA28 経由の 25GbE	SFP-25G-SR-S SFP-10/25G-LR-S SFP-10/25G-CSR-S SFP-25G-SL SFP-H25G-SFP-H10GB-CU1M SFP-H25G-CU2M SFP-H25G-SFP-H10GB-CU3M SFP-H25G-CU5M
QSA または QSA28 を介した 10GbE/1GbE	SFP-10G-SR SFP-10G-SR SFP-10G-SR-S SFP-10G-LR（QSA あり） SFP-10G-LR SFP-10G-LR-S SFP-10G-LR-S CVR-QSFP-SFP10G+ GLC-T（ポート 7、8） CVR-QSFP-SFP28+ GLC-T（ポート 7、8）
8G、16G、32G FC	128G QSF を備えた 8G FC ブレークアウト X 4 128G QSFP を使用した 16G FC ブレークアウト X 4 128G QSFP を使用した 32G FC ブレークアウト X 4

サポートされる GPU/GPU PCIe ノード

表 *20 :* サポートされる *GPU/GPU PCIe* ノード

GPU/GPU PCIe ノード	PID	サポート対象のサーバ	最小ソフトウェアバージョン	推奨ソフトウェアバージョン
X440p 上の NVIDIA A16 GPU：PCIE 250W 4X16GB、FHFL	UCSX-GPU-A16	Cisco UCS X210c M8（および PCIe ノード）	4.3 (6a)	6.0(1c)
	UCSC-CGPU-A16	Cisco UCSX215c M8（PCIe ノードで）	4.3(5a)	6.0(1c)
AMD MI210 GPU; 300W 64GB、2 スロット FHFL	UCSX-GPU-MI210	Cisco UCS X215c M8	4.3 (6a)	6.0(1c)
NVIDIA H100-NVL GPU 400W, 94GB, 2 スロット FHFL	UCSX-GPU-H100-NVL	Cisco UCS X210c M8（および PCIe ノード）	4.3 (6a)	6.0(1c)
	UCSC-GPU-H100-NVL	Cisco UCS C240 M8	4.3 (6a)	6.0(1c)
		Cisco UCS X210c M7 Cisco UCSX215c M8（PCIe ノードで）	4.3(5a)	6.0(1c)
		Cisco UCS C245 M8	4.3(5a)	6.0(1c)
		Cisco UCS C240 M7	4.3(5a)	6.0(1c)
NVIDIA L4 メザニン GPU 70W、24GB、1 スロット HHHL GPU	UCSX-GPU-L4-Mezz	Cisco UCS X210c M7 Cisco UCS X215c M8	4.3(5a)	6.0(1c)
UCSX-440P-D GPU PCIe ノード	UCSX-440P-D	Cisco UCS X210c M7、X210c M6、および X410c M7	4.3(4a)	6.0(1c)

GPU/GPU PCIe ノード	PID	サポート対象のサーバ	最小ソフトウェアバージョン	推奨ソフトウェアバージョン
Intel GPU Flex 140、Gen4x8、HHHL、75W PCIe（フロント メザニン）	UCSX-GPU-FLX140MZ	Cisco UCS X210c M7	4.3(2b)	6.0(1c)
Intel GPU Flex 140、Gen4x8、HHHL、75W PCIe	UCSX-GPU-FLEX140	Cisco UCS X410c M7 および X210c M7（PCIe ノード搭載）	4.3(4a)	6.0(1c)
	UCSC-GPU-FLEX140	Cisco UCS C220 M7 および C240 M7	4.3(4a)	6.0(1c)
Intel GPU Flex 170、Gen4x16、HHFL、150W PCIe	UCSX-GPU-FLEX170	Cisco UCS X410c M7 および X210c M7（PCIe ノード搭載）	4.3(4a)	6.0(1c)
	UCSC-GPU-FLEX170	Cisco UCS C240 M7	4.3(4a)	6.0(1c)
NVIDIA TESLA A16 PCIE 250W 4X16GB	UCSX-GPU-A16-D	Cisco UCS X210c M7 および X210c M6（PCIe ノード搭載）	4.3(4a)	6.0(1c)
		Cisco UCS X410c M7（PCIe ノード搭載）	4.3(4a)	6.0(1c)
	UCSC-GPU-A16	Cisco UCS C240 M8	4.3 (6a)	6.0(1c)
		Cisco UCS C240 M6	4.2(1d)	6.0(1c)
		Cisco UCS C245 M6	4.2(1i)	6.0(1c)

GPU/GPU PCIe ノード	PID	サポート対象のサーバ	最小ソフトウェアバージョン	推奨ソフトウェアバージョン
NVIDIA L4 Tensor Core、70W、24GB	UCSX-GPU-L4	Cisco UCS X210c M8（および PCIe ノード）	4.3 (6a)	6.0(1c)
		Cisco UCS X210c M7（PCIe ノード搭載）	4.3(4a)	6.0(1c)
		Cisco UCS X410c M7（PCIe ノード搭載）	4.3(4a)	6.0(1c)
NVIDIA L40 300W、48GB wPWR CBL	UCSX-GPU-L40	Cisco UCS X210c M7（PCIe ノード搭載）	4.3(4a)	6.0(1c)
		Cisco UCS X410c M7（PCIe ノード搭載）	4.3(4a)	6.0(1c)
	UCSC-GPU-L40	Cisco UCS C240 M7	4.3(2b)	6.0(1c)
		Cisco UCSX215c M8（PCIe ノードで）	4.3(5a)	6.0(1c)
NVIDIA L40S：350W、48GB、2 スロット FHFL GPU	UCSX-GPU-L40S	Cisco UCS X210c M8（および PCIe ノード）	4.3 (6a)	6.0(1c)
		Cisco UCS X210c M7（PCIe ノード搭載） Cisco UCS X410c M7（PCIe ノード搭載）	4.3(4a)	
	UCSC-GPU-L40S	Cisco UCS C240 M8	4.3 (6a)	6.0(1c)
		Cisco UCS C240 M7	4.3(4a)	6.0(1c)
		Cisco UCSX215c M8（PCIe ノードで）	4.3(5a)	6.0(1c)

GPU/GPU PCIe ノード	PID	サポート対象のサーバ	最小ソフトウェアバージョン	推奨ソフトウェアバージョン
NVIDIA T4 PCIE 75W 16GB	UCSX-GPU-T4-16	Cisco UCS X210c M6（PCIe ノード搭載）	4.3(4a)	6.0(1c)
	UCSC-GPU-T4-16	Cisco UCS C220 M6	4.3(2b)	6.0(1c)
		Cisco UCS C245 M6	4.2(1f)	6.0(1c)
		Cisco UCS C225 M6	4.2(1l)	6.0(1c)
		Cisco UCS C240 M5、C220 M5、および C480 M5	3.2(3a)	6.0(1c)
		Cisco UCS S3260 M5	3.1(2b)	6.0(1c)
NVIDIA T4 GPU PCIE 75W 16GB、MEZZ フォームファクタ（フロント メザニン）	UCSX-GPU-T4-MEZZ	Cisco UCS X210c M7 および X210c M6	4.3(2b)	6.0(1c)
NVIDIA Hopper L4 70W、24GB、1 スロット HHHL	UCSC-GPU-L4M6	Cisco UCS C220 M6、C240 M6	4.3(4a)	6.0(1c)
NVIDIA H100：350W、80GB、2 スロット FHFL GPU	UCSX-GPU-H100-80	Cisco UCS X210c M7 および X410c M7（PCIe ノード搭載）	4.3(4a)	6.0(1c)
	UCSC-GPU-H100-80	Cisco UCS C240 M7	4.3(4a)	6.0(1c)

GPU/GPU PCIe ノード	PID	サポート対象のサーバ	最小ソフトウェアバージョン	推奨ソフトウェアバージョン
NVIDIA L4:70W、24GB、1 スロット HHHL GPU	UCSC-GPU-L4	Cisco UCS C240 M8 および C220 M8	4.3 (6a)	6.0(1c)
		Cisco UCS C245 M8	4.3(5a)	6.0(1c)
		Cisco UCS C220 M7 および C240 M7	4.3(2b)	6.0(1c)
		Cisco UCSX215c M8（PCIe ノードで）	4.3(5a)	6.0(1c)
NVIDIA P4	UCSC-GPU-P4	Cisco UCS C220 M5	3.2(3a)	6.0(1c)
NVIDIA M10	UCSC-GPU-M10	Cisco UCS C240 M5 および C480 M5	3.2(3a)	6.0(1c)
NVIDIA GRID P6 前面メザニン	UCSB-GPU-P6-F	Cisco UCS B200 M5	3.2(1d)	6.0(1c)
		Cisco UCS B480 M5	3.2(2b)	6.0(1c)
NVIDIA GRID P6 背面メザニン	UCSB-GPU-P6-R	Cisco UCS B200 M5	3.2(1d)	6.0(1c)
		Cisco UCS B480 M5	3.2(2b)	6.0(1c)
TESLA A30、パッシブ冷却、180W、24GB	UCSC-GPU-A30-D	Cisco UCS C240 M7	4.3(2b)	6.0(1c)
	UCSC-GPU-A30	Cisco UCS C240 M6	4.2(1d)	6.0(1c)
		Cisco UCS C245 M6	4.2(1i)	6.0(1c)

GPU/GPU PCIe ノード	PID	サポート対象のサーバ	最小ソフトウェアバージョン	推奨ソフトウェアバージョン
TESLA A40 RTX、パッシブ、300W、48GB	UCSX-GPU-A40-D	Cisco UCS X210c M7 および X210c M6（PCIe ノード搭載）	4.3(4a)	6.0(1c)
		Cisco UCS X410c M7（PCIe ノード搭載）	4.3(4a)	6.0(1c)
	UCSC-GPU-A40-D	Cisco UCS C240 M7	4.3(2b)	6.0(1c)
	UCSC-GPU-A40	Cisco UCS C240 M6	4.2(1d)	6.0(1c)
		Cisco UCS C245 M6	4.2(1i)	6.0(1c)
		Cisco UCS C480 M5	3.2(3a)	6.0(1c)
TESLA A100、パッシブ、300W、80GB12	UCSX-GPU-A100-80-D	Cisco UCS X210c M7 および X210c M6（PCIe ノード搭載）	4.3(4a)	6.0(1c)
		Cisco UCS X410c M7（PCIe ノード搭載）	4.3(4a)	6.0(1c)
	UCSC-GPUA100-80-D	Cisco UCS C240 M7	4.3(2b)	6.0(1c)
	UCSC-GPU-A100-80	Cisco UCS C240 M6	4.2(1d)	6.0(1c)
		Cisco UCS C245 M6	4.2(1i)	6.0(1c)
		すべての Cisco UCS C シリーズ M5	4.2(2c)	6.0(1c)
TESLA A10、パッシブ、150 W、24 GB	UCSC-GPU-A10	Cisco UCS C240 M6	4.2(1d)	6.0(1c)
		Cisco UCS C245 M6	4.2(1i)	6.0(1c)

GPU/GPU PCIe ノード	PID	サポート対象のサーバ	最小ソフトウェアバージョン	推奨ソフトウェアバージョン
NVIDIA H200-NVL GPU	UCSC-GPU-H200-NVL	Cisco UCS C240 M8	4.3(6c)	6.0(1c)

Cisco UCS Manager で廃止されたハードウェアおよびソフトウェア

リリース 6.0(1b)

Cisco UCS Manager リリース 6.0(1b) 以降、以下のハードウェアはサポートされなくなりました。

- Cisco UCS FI モデル：
  - UCS-FI-6300-E6U16
  - UCS-FI-6300-E6-16UP
  - UCS-FI-6332-16UP
  - UCS-FI-6332
  - UCS-FI-M-6324
- IOM モデル：
  - UCS-IOM-2208XP
  - UCS-IOM-2204XP
  - UCS-IOM-2304
  - UCS-IOM-2304V2
- FEX モデル：
  - N2K-C2248TP-1GE
  - N2K-C2248T-1GE
  - N2K-C2148T-1GE
  - N2K-C2232PP-10GE
  - N2K-C2232TM-10GE
  - N2K-C2232TM-E-10GE
  - 10 ギガ-ビット C2348UPQ N2K

機能カタログ

Cisco UCS Manager 機能カタログは調整可能なパラメータ、文字列、およびルールのセットです。Cisco UCS では、カタログを使用して、サーバの新しく承認された DIMM やディスク ドライブなどのコンポーネントの表示と設定可能性を更新します。

機能カタログは Cisco UCS Manager に組み込まれていますが、更新を簡単にするために単一のイメージ ファイルとしてもリリースされる場合があります。

次の表に、このリリースで追加された PID を示し、UCS ソフトウェア リリースを対応する機能カタログ ファイルにマッピングします。

表 *21* : バージョンのマッピング

UCS リリース	カタログ ファイル名	このリリースの追加 PID
6.0(1c)	ucs-catalog 6.0.1 d. .bin	—
6.0(1b)	ucs-catalog 6.0.1 c. .bin	Cisco UCS ファブリック インターコネクトおよびコンポーネント • FI：UCS-FI-6664-U • PSU とファン：UCS-PSU-6600- AC、UCS-FAN-6664 • アクセサリおよびブランク： UCS-ACC-6664 コントローラ: • UCSX-X10C-PTE3

関連資料

詳細については、次のリンクから関連資料を参照できます。

- Cisco UCS ソフトウェアのリリース バンドル コンテンツ
- Cisco UCS C シリーズ ラック サーバ統合ガイド
- Cisco UCS C シリーズ ソフトウェア リリース ノート
- Cisco Intersight インフラストラクチャ ファームウェアのリリース ノート
- 『Release Notes for Cisco UCS Central』
- Cisco UCS Manager アップグレード/ダウングレード サポート マトリックス ツール
- 詳細については、Cisco Intersight、Cisco IMC、および Cisco UCS Manager ツール向け Cisco UCS 同等性マトリクスを参照してください。

- Cisco UCS Manager 内部依存関係マトリックス ツール
- Cisco UCS Manager リリース 6.0 の内部依存関係
- Cisco UCS Manager のクロス バージョン ファームウェア マトリックス ツール
- Cisco UCS Manager クロス バージョン ファームウェア サポート、リリース 6.0

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