

Cisco UCS Manager リリース 4.0 リリース ノート

初版：2018年8月14日

最終更新：2020年7月24日

Cisco UCS Manager

Cisco UCS™ Manager リリース4.0 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](https://www.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 4.0 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

Cisco UCS Manager 4.0(x) への直接アップグレードは、リリース 2.2(8)、3.1(3)、それ以降のリリースからサポートされます。UCS ミニに関して、Cisco UCS Manager リリース 4.0(x) への直接アップグレードは、リリース 3.1(3) およびそれ以降のリリースからサポートされます。詳細については、『*Cisco UCS Manager* ファームウェア管理ガイドリリース 4.0』を参照してください。

マニュアルの変更履歴

リリース	日付	説明
4.0 (4i)	2020 年 7 月 6 日	Cisco UCS Manager リリース 4.0 (4i) 向けリリース ノートを作成
	2020 年 7 月 23 日	リリース 4.0 (4i) の解決済みの警告のリストに CSCvt64871 および CSCvu11155 を追加。
	2020 年 7 月 24 日	CSCvq53066を「未解決の問題」から「解決済みの問題」に移動しました。
4.0 (4h)	2020 年 3 月 23 日	Cisco UCS Manager リリース 4.0 (4h) 向けリリース ノートを作成
	2020 年 4 月 3 日	リリース 4.0 (4h) 解決済み警告の CSCvr79388 の説明を更新しました。 リリース 4.0 (4h) の未解決の問題のリストに CSCvt64871 が追加されました。
	2020 年 4 月 8 日	動作の変更が追加されました。 txmit クレジット損失が発生しているファイバチャネルポートは無効になりました。
	2020 年 6 月 12 日	リリース 4.0 (4h) の未解決の問題のリストに CSCvu11155 が追加されました。

リリース	日付	説明
4.0 (4g)	2019年12月9日	Cisco UCS Manager リリース 4.0(4g) 向けリリース ノートを作成
	2020年1月16日	M3 ブレード サーバのサポートを明確にするために、内部依存関係テーブルが更新されました。
	2020年2月27日	未解決の問題点、 CSCvr76930 での ケーブル SFP-H25G-SFP-H10GB-CU3M を、 SFP-H25G-SFP-H10GB-CU5M に修正しました。
4.0 (4f)	2019年11月5日	Cisco UCS Manager リリース 4.0(4f) 向けリリース ノートを作成
	2019年12月2日	リリース 4.0(4f) 解決済み警告の CSCvr40744 の説明を更新しました。
4.0 (4e)	2019年9月27日	Cisco UCS Manager リリース 4.0(4e) 向けリリース ノートを作成
4.0 (4d)	2019年8月19日	Cisco UCS Manager リリース 4.0(4d) 向けリリース ノートを作成
4.0 (4c)	2019年8月1日	Cisco UCS Manager リリース 4.0(4c) 向けリリース ノートを作成
	2019年10月1日	解決済みの警告リストから CSCvn49417 を削除しました。

リリース	日付	説明
4.0(4b)	2019年5月17日	Cisco UCS Manager リリース 4.0(4b) 向けリリース ノートを作成
	2019年5月20日	4.0(4b) のカタログファイル名が更新されました。
	2019年6月3日	既知の制限が追加されました。UCS 6300 シリーズファブリック インターコネクタの ASIC 制限がパッシブケーブルで追加されました。
4.0(4a)	2019年4月26日	Cisco UCS Manager リリース 4.0(4a) 向けリリース ノートを作成
	2019年5月15日	未解決の問題リストに CSCvp68182 が追加されました。 CSCvp68182 のソフトウェア延期通知が追加されました。
	2019年11月14日	追加された動作変更 - キャッシュされた IO ポリシーが有効になっている仮想ドライブを作成できません
4.0(2e)	2019年5月15日	Cisco UCS Manager リリース 4.0(2e) 向けリリース ノートを作成
4.0(2d)	2019年3月13日	Cisco UCS Manager リリース 4.0(2d) 向けリリース ノートを作成
4.0(2b)	2019年1月19日	Cisco UCS Manager リリース 4.0(2b) 向けリリース ノートを作成
	2019年1月22日	「リリース4.0(2b)」の新しいハードウェアで UCS ミニモデル番号を修正しました。

リリース	日付	説明
4.0(2a)	2019年1月2日	Cisco UCS Manager リリース 4.0(2a) 向けリリース ノートを作成
	2019年1月8日	リリース 4.0(2a) の未解決の問題が更新され、CSCvk63036 が含まれるようになりました。
	2019年3月3日	新しいハードウェアのリストに UCSC V100-32 が追加されました。
4.0(1d)	2018年12月20日	Cisco UCS Manager リリース 4.0(1d) 向けリリース ノートを作成
	2019年9月4日	CSCvq28261 の説明が更新されました。 未解決の問題リストに CSCvr08327 が追加されました。
4.0(1c)	2018年10月11日	Cisco UCS Manager リリース 4.0(1c) 向けリリース ノートを作成
4.0(1b)	2018年9月13日	Cisco UCS Manager リリース 4.0(1b) 向けリリース ノートを作成

リリース	日付	説明
4.0(1a)	2018年8月14日	Cisco UCS Manager リリース 4.0(1a) 向けリリース ノートを作成
	2018年8月27日	L1 ターミナル障害に関する問題 (CSCvm03356、CSCvm03351、および CSCvm03339) がセキュリティ修正のリストに追加されました。
	2019年6月7日	動作変更が追加されました。WWN プールの WWPN および WWNN 範囲を許可しました
	2020年2月4日	未解決の問題リストに CSCvr98210 が追加されました。

Cisco UCS Manager リリース 4.0 に移行する主な理由

Cisco UCS Manager リリース 4.0 に移行する主な理由は次のとおりです。

- UCS 6454 ファブリック インターコネクタのサポート
- C4200 シャーシおよび Cisco UCS C125 M5 サーバのサポート
- UCS M5 サーバでの VIC 1400 シリーズ アダプタ カードのサポート
- Cisco UCS C480 M5 ML サーバのサポート
- UCS Intel ベースの M5 サーバ上の 第二世代インテル® Xeon® Scalable プロセッサ更新および Intel® Optane™ データセンター永続メモリ モジュールのサポート
- M5 サーバでのメモリ RAS 機能の向上
- S3260 ストレージ サーバを使用した新しい SIOC のサポート
- Hyperflex 3.5 以降のリリースのサポート
- 新しい周辺機器のサポート

リリース 4.0 の新機能

Cisco UCS Manager リリース 4.0 は、サポートされているすべての UCS ハードウェア プラットフォーム向けの統合ソフトウェア リリースです。

新しいハードウェア機能

- リリース 4.0 (4i) の新しいハードウェア - なし
- リリース 4.0 (4h) の新しいハードウェア - なし
- リリース 4.0 (4g) の新しいハードウェア - なし
- リリース 4.0 (4f) の新しいハードウェア - なし
- [リリース 4.0 \(4e\) の新しいハードウェア \(8 ページ\)](#)
- リリース 4.0 (4d) の新しいハードウェア - なし
- [リリース 4.0 \(4c\) の新しいハードウェア \(8 ページ\)](#)
- リリース 4.0(4b) の新しいハードウェア - なし
- [リリース 4.0\(4a\) の新しいハードウェア \(9 ページ\)](#)
- リリース 4.0(2e) の新しいハードウェア - なし
- リリース 4.0(2d) の新しいハードウェア - なし
- リリース 4.0(2b) の新しいハードウェア - なし
- [リリース 4.0\(2a\) の新しいハードウェア \(10 ページ\)](#)
- リリース 4.0(1d) の新しいハードウェア - なし
- リリース 4.0(1c) の新しいハードウェア - なし
- リリース 4.0(1b) の新しいハードウェア - なし
- [リリース 4.0\(1a\) の新しいハードウェア \(16 ページ\)](#)

新しいソフトウェア機能

- リリース 4.0 (4i) の新しいソフトウェア - なし
- リリース 4.0 (4h) の新しいソフトウェア - なし
- リリース 4.0 (4g) の新しいソフトウェア - なし
- リリース 4.0 (4f) の新しいソフトウェア - なし
- [リリース 4.0 \(4e\) での新しいソフトウェア機能 \(20 ページ\)](#)
- リリース 4.0 (4d) の新しいソフトウェア - なし
- [リリース 4.0 \(4c\) での新しいソフトウェア機能 \(21 ページ\)](#)
- リリース 4.0(4b) の新しいソフトウェア - なし
- [リリース 4.0\(4a\) での新しいソフトウェア機能 \(21 ページ\)](#)
- リリース 4.0(2e) の新しいソフトウェア - なし

- リリース 4.0(2d) の新しいソフトウェア - なし
- リリース 4.0(2b) の新しいソフトウェア - なし
- [リリース 4.0\(2a\) での新しいソフトウェア機能 \(24 ページ\)](#)
- リリース 4.0(1d) の新しいソフトウェア - なし
- リリース 4.0(1c) の新しいソフトウェア - なし
- リリース 4.0(1b) の新しいソフトウェア - なし
- [リリース 4.0\(1a\) での新しいソフトウェア機能 \(26 ページ\)](#)

リリース 4.0 (4e) の新しいハードウェア

周辺機器 (Peripherals)

Cisco UCS 2408 ファブリック エクステンダのサポート (UCS-IOM-2408)

リリース 4.0 (4c) の新しいハードウェア

Intel NVMe P4510/4511 および P4610 ドライブのサポート

Cisco UCS Manager リリース 4.0 (4c) では、ブレードおよびラック サーバ上の次の NVMe ドライブのファームウェア サポートが導入されています。

NVMe ドライブ	ブレード サーバの PID	ラック サーバの PID
Intel P4510 1TB (SSDPE2KX010T8K)	UCSB-NVME2H-I1000	UCSC-NVME2H-I1000
Intel P4510 2TB (SSDPE2KX020T8K)	UCSB-NVME2H-I2TBV	UCSC-NVME2H-I2TBV
Intel P4510 4TB (SSDPE2KX040T8K)	UCSB-NVME2H-I4000	UCSC-NVME2H-I4000
Intel P4510 8TB (SSDPE2KX080T8K)	UCSB-NVMEHW-I8000	UCSC-NVMEHW-I8000
Intel P4610 1.6TB (SSDPE2KE016T8K)	UCSB-NVME2H-I1600	UCSC-NVME2H-I1600
Intel P4610 3.2TB (SSDPE2KE032T8K)	UCSB-NVME2H-I3200	UCSC-NVME2H-I3200

リリース 4.0(4a) の新しいハードウェア

第二世代インテル® Xeon® Scalable プロセッサ

Cisco UCS Manager リリース 4.0(4a) では、次のサーバでの 第二世代インテル® Xeon® Scalable プロセッサのサポートが導入されています。

- Cisco UCS B200 M5 サーバ
- Cisco UCS B480 M5 サーバ
- Cisco UCS C220 M5 サーバ
- Cisco UCS C240 M5 サーバ
- Cisco UCS C480 M5 サーバ
- Cisco UCS S3260 M5 サーバ

Intel® Optane™ データ センター永続メモリ モジュール

Intel® Optane™ データ センター永続メモリ モジュールは、第二世代インテル® Xeon® Scalable プロセッサでのみ使用できます。

Cisco UCS Manager リリース 4.0(4a)では、第二世代インテル® Xeon® Scalableプロセッサに基づく次のサーバ上の Intel® Optane™ DC 永続メモリ モジュールのサポートが導入されています。

- Cisco UCS B200 M5 サーバ
- Cisco UCS B480 M5 サーバ
- Cisco UCS C220 M5 サーバ
- Cisco UCS C240 M5 サーバ
- Cisco UCS C480 M5 サーバ
- Cisco UCS S3260 M5 サーバ

Intel® Optane™ DC 永続メモリ モジュールは、128 GB、256GB および 512 GB の永続メモリをサポートします。これは、Cisco UCS Manager またはホスト オペレーティング システム ツールを使用して設定できます。

周辺機器 (Peripherals)

- 次のサーバ上の NVIDIA T4 16 GB GPU カード (UCSC GPU-T4-16) のサポート。
 - UCS C220 M5
 - UCS C240 M5
 - UCS C480 M5
- AMD Radeon Pro V340、2X16GB GB、300W GPU カードのサポート (UCSC-GPU-V340)

- Cisco UCS 2304V2 ファブリック エクステンダのサポート (UCS-IOM-2304V2)
- Mellanox MCX4121A-ACAT デュアル ポート 10/25G SFP28 NIC (UCSC-P-M4D25GF) のサポート
- Cisco UCS C125 M5 サーバを除くすべての UCS M5 サーバ上での QLogic QL45611HLCU シングル ポート 100GbE PCIe NIC (UCSC pcie QS100GF) のサポート。
- UCS 6454 ファブリック インターコネクタ上の Cisco QSFP 40/100 Gb (QSFP-40/100G SRBD) デュアルレート双方向 (BiDi) トランシーバのサポート。
- 次のサーバ上の Cisco Boot 最適化 M. 2 RAID コントローラ (HWRAID) のハードウェア RAID サポート。
 - Cisco UCS C220 M5 サーバ
 - Cisco UCS C240 M5 サーバ
 - Cisco UCS C480 M5 サーバ
 - Cisco UCS B200 M5 サーバ
 - Cisco UCS B480 M5 サーバ

リリース 4.0(2a) の新しいハードウェア

Cisco UCS C480 M5 ML サーバ

Cisco UCS C480 M5 ML ラック サーバは、ディープラーニング専用のサーバです。これは、トレーニングモデル向けにストレージと I/O が最適化されています。Cisco UCS C480 M5 ML サーバは、スタンドアロンまたは Cisco UCS 管理環境に対応し、4 RU フォームファクタで卓越したストレージ拡張性とパフォーマンスを提供します。以下の機能を装備しています。

- 8 つの NVIDIA SXM2 V100 32G モジュール (NVLink インターコネクタ)
- 最新のインテル® Xeon® スケーラブルプロセッサ (2 プロセッサ構成をサポート、ソケットあたり最大 28 コアを搭載)
- 2666 MHz DDR4 メモリに対応した 24 の DIMM スロット (合計で最大 3 テラバイト (TB) のメモリ容量)
- 最大 4 個の 10/25 または 40/100G Cisco VICs (VIC 1455 および VIC 1495) 用の 4 個の PCI Express (PCIe) 3.0 スロット
- 最大 24 台の Small Form Factor (SFF) 2.5 インチ SAS/SATA ソリッドステートディスク (SSD) およびハードディスクドライブ (HDD) をサポートする柔軟なストレージオプション
- 最大 6 台の PCIe NVMe ディスク搭載可能なドライブオプション
- Cisco 12 Gbps SAS モジュラ RAID コントローラを専用スロットでサポート
- M.2 起動用ドライブ (オプション)

- 組み込みのデュアル 10 ギガビット イーサネット LAN-on-motherboard (LOM) ポート

UCS VIC 1400 シリーズ アダプタ

UCS M5 サーバおよび UCS C125 サーバで次の新規 UCS VIC 1400 シリーズ アダプタ カードをサポートします。

- C シリーズ (UCSC-PCIE-C100-04) 向け VIC 1495 40/100G PCIe
- C シリーズ (UCSC-MLOM-C100-04) 向け VIC 1497 40/100G mLOM

このリリースでは、VIC 1495 または VIC 1497 を使用しているときに、直接接続モードの UCS 6300 シリーズ ファブリック インターコネクタと C シリーズサーバ間の 40G イーサネット接続のサポートが導入されています。

このリリースでは、B シリーズ用の UCS VIC 1400 シリーズ アダプタが UCS ミニ ファブリック インターコネクタでサポートされています。UCS 6454、UCS 6300 シリーズ、および 6200 シリーズ ファブリック インターコネクタでは、すべての UCS VIC 1400 シリーズ アダプタがサポートされています。



- (注) Cisco C シリーズ サーバは、Cisco UCS 6324 ファブリック インターコネクタと Cisco UCS VIC 14xx の組み合わせを使用して Cisco UCS Manager と統合することはできません。



- (注) 同じサーバ上で、異なるシリーズの VIC アダプタをインストールすることはできません。たとえば、同じサーバ上で、UCS VIC 1300 シリーズ アダプタおよび UCS VIC 1400 シリーズ アダプタをインストールできません。

次の表に、Cisco UCS Manager リリース 4.0 (2) でサポートされている VIC 1400 シリーズ アダプタ/サーバの組み合わせを示します。

表 1: M5 B シリーズ サーバの VIC 1400 シリーズ アダプタ サポート

FI	IOM	1400 シリーズ VIC アダプタ			
		VIC 1440	VIC 1440 + ポート エクスパン ダ	VIC 1480	VIC 1440 + VIC 1480
		UCSB-MLOM-40G-04	UCSB-MLOM-40G-04 + UCSB-MLOM-PT-01	UCSB-VIC-M84-4P	UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P
6200 シリーズ	2204/2208	B480 M5、 B200 M5	NA	B480 M5	B480 M5、 B200 M5

FI	IOM	1400 シリーズ VIC アダプタ			
		VIC 1440	VIC 1440 + ポート エクスパン ダ	VIC 1480	VIC 1440 + VIC 1480
		UCSB-MLOM-40G-04	UCSB-MLOM-40G-04 + UCSB-MLOM-PF-01	UCSB-VIC-M84-4P	UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P
6300 シリー ズ :	2304	B480 M5、 B200 M5	B480 M5、 B200 M5	B480 M5	B480 M5、 B200 M5
	2204/2208	B480 M5、 B200 M5	NA	B480 M5	B480 M5、 B200 M5
6454	2204/2208 2408 注: 2408 (B シ リーズ M4 お よび M5 サー バ) のサポート は、リリース 4.0 (4e) で追加 されました。	B480 M5、 B200 M5	NA	B480 M5	B480 M5、 B200 M5
6324 (UCS ミ ニ	NA	B480 M5、 B200 M5	NA	B480 M5	B480 M5、 B200 M5
	2204/2208	NA	NA	NA	NA

表 2: M5 C シリーズおよび S シリーズ サーバの VIC 1400 シリーズ アダプタ サポート

FI	FEX	UCS VIC 1400 シリーズ アダプタ			
		VIC 1455	VIC 1455 および 1457	VIC 1495	VIC 1497
		UCSC-PCIE-C250-04	UCSC-MLOM-C250-04	UCSC PCIE C100 04	UCSC-MLOM-C100-04
6200 シリーズ	直接接続	C220 M5、 C240 M5、 C480 M5、 C480 M5 ML、 S3260 M5 (UCS-S3260 -PCISIOC 付 き)	C220 M5、 C240 M5	NA	NA
	2232 PP	C220 M5、 C240 M5、 C480 M5、 S3260 M5 (UCS-S3260 -PCISIOC 付 き)	C220 M5、 C240 M5	NA	NA
	2232-T	NA	NA	NA	NA

FI	FEX	UCS VIC 1400 シリーズ アダプタ			
		VIC 1455	VIC 1455 および 1457	VIC 1495	VIC 1497
		UCSC-PCIE-C250-04	UCSC-MLOM-C250-04	UCSC-PCIE-C100 04	UCSC-MLOM-C100-04
6300 シリーズ :	直接接続	C220 M5、 C240 M5、 C480 M5、 C125 M5、 C480 M5 ML、 S3260 M5 (UCS-S3260 -PCISIOC 付 き)	C220 M5、 C240 M5	C220 M5、 C240 M5、 C480 M5、 C125 M5、 C480 M5 ML、 S3260 M5 (UCS-S3260 -PCISIOC 付 き)	C220 M5、 C240 M5
	直接接続 (ブ レークアウト)	C220 M5、 C240 M5、 C480 M5、 C125 M5、 S3260 M5 (UCS-S3260 -PCISIOC 付 き)	C220 M5、 C240 M5	C220 M5、 C240 M5、 C480 M5、 C125 M5、 C480 M5 ML、 S3260 M5 (UCS-S3260 -PCISIOC 付 き)	C220 M5、 C240 M5
	2232 PP	C220 M5、 C240 M5、 C480 M5、 C125 M5、 S3260 M5 (UCS-S3260 -PCISIOC 付 き)	C220 M5、 C240 M5	NA	NA
	2232-T	NA	NA	NA	NA
	2348	C220 M5、 C240 M5、 C480 M5、 C125 M5、 S3260 M5 (UCS-S3260 -PCISIOC 付 き)	C220 M5、 C240 M5	NA	NA

FI	FEX	UCS VIC 1400 シリーズ アダプタ			
		VIC 1455	VIC 1455 および 1457	VIC 1495	VIC 1497
		UCSC-PCIE-C250-04	UCSC-MLOM-C250-04	UCSC-PCIE-C100-04	UCSC-MLOM-C100-04
6454	直接接続 (10G/25G)	C220 M5、 C240 M5、 C480 M5、 C125 M5、 C480 M5 ML、 S3260 M5 (UCS-S3260 -PCISIOC 付 き)	C220 M5、 C240 M5	NA	NA
	2232 PP	C220 M5、 C240 M5、 C480 M5、 C125 M5、 S3260 M5 (UCS-S3260 -PCISIOC 付 き)	C220 M5、 C240 M5	NA	NA
	2232-T	NA	NA	NA	NA
	2348	NA	NA	NA	NA
6324 (UCS ミニ)	直接接続 (10G)	NA	NA	NA	NA
	直接接続 (ブ レークアウト)	NA	NA	NA	NA

サーバおよびアダプタの組み合わせの詳細については、「サーバ仕様シート」を参照してください。

- [B シリーズ サーバ仕様シート](#)
- [C シリーズ サーバ仕様シート](#)
- [S シリーズ サーバ仕様シート](#)

UCS VIC 1400 シリーズ アダプタを搭載した UCS ミニ

Cisco UCS Manager リリース 4.0 (2) 以降では、UCS ミニ (6324) ファブリック インターコネク
トは、プライマリ シャーシの B シリーズ サーバに対して、次の VIC 1400 シリーズ アダプタ
をサポートするようになりました。

- UCSB-MLOM-40G-04 (UCS VIC 1440)
- UCSB-VIC-M84-4P (UCS VIC 1480)

周辺機器 (Peripherals)

- UCS C240 M5 サーバ用の NVIDIA V100 PCIe PG500-200 250W 32GB GPU カード (UCSC GPU-C240-32) をサポートします。
- すべての UCS サーバに対して TPM2 (UCSX-TPM2-002-C) をサポートします。
- HyperFlex でのホットプラグ NVMe ドライブ サポートをサポートしています。
- UCS 6454 ファブリック インターコネクタの高電圧 DC 1200 ワット電源 (N9K-PUV-1200W) のサポート
- Intel[®] Optane[™] NVMe エクストリーム パフォーマンス ドライブのサポート (UCSC-NVMEXP-I750)
- UCS C125 での QLogic 10G ネットワーク アダプタ カード (UCSC PCIE QD10GC) をサポートしています。
- UCS C125 での QLogic 25G ネットワーク アダプタ カード (UCSC-PCIE-QD25GF) をサポートします。
- UCS C480 M5 ML での QLogic 100G ネットワーク アダプタ カード (UCSC-PCIE-QS100GF) をサポートしています。

リリース 4.0(1a) の新しいハードウェア

第 4 世代ファブリック インターコネクタ

Cisco UCS 6454 Fabric Interconnect は、Cisco Unified Computing System の中核を成す製品であり、システムのネットワーク接続と管理機能の両方を提供します。また、Cisco UCS 6454 はラインレート、低遅延、ロスレスの 10/25/40/100 ギガビットイーサネット、Fibre Channel over Ethernet (FCoE) およびファイバチャネル接続機能を提供します。

Cisco UCS 6454 54 ポート ファブリック インターコネクタは、1 ラック ユニット (1RU) の 10/25/40/100 ギガビットイーサネット、FCoE、およびファイバチャネルスイッチで、最大 3.82 Tbps のスループットと最大 54 個のポートを提供します。このスイッチは、40 個の 10/25 Gbps 固定イーサネット、8 個の 1/10/25 Gbps イーサネット、8/16/32G ファイバチャネルポート、および 6 個の 40/100 Gbps イーサネットアップリンクポートを備えています。すべてのイーサネットポートは、FCoE をサポートする能力があります。

Cisco UCS C125 M5 サーバ

Cisco UCS Manager 4.0(1) は、UCS 6300 シリーズおよび UCS 6454 ファブリック インターコネクタの Cisco UCS C125 M5 サーバをサポートするようになりました。C125 M5 サーバは、AMD EPYC[™] プロセッサに基づく Cisco の最初のサーバです。Cisco UCS C125 M5 サーバは、Cisco UCS C4200 シリーズラックサーバシャーシに収容されています。各 Cisco UCS C4200 シリー

ブラック サーバシャーシは、2～4個の Cisco UCS C125 M5 サーバノードをサポートします。Cisco UCS C125 M5 サーバでは、次の周辺機器がサポートされています。

- デュアルポート 10Gbase-T および 10G/25G SFP28 OCP カード
- Cisco 12 G 9460-8i PCIe 12 G SAS RAID コントローラ
- 32 GB、64 GB、および 128 GB SD カード
- 32GB マイクロ SD カード



(注) これは、Cisco UCS Manager では管理されません。

- 240 GB および 960 GB M.2 SATA SSD ドライブ
- 16 GB フラッシュ USB ドライブ



(注) これは、Cisco UCS Manager では管理されません。

- SD および M.2 SATA 用ミニストレージキャリア
- オンボード AHCI コントローラ

Cisco UCS S3260 ストレージサーバの新世代 SIOC

Cisco UCS S3260 ストレージサーバシステムは、S3260 M5 サーバを持つ新規サーバ SIOC、UCS-S3260-PCISIOC をサポートしています。この SIOC では、ネットワーク アダプタを交換するための PCIe スロットがあります。これらのスロットでは、Cisco VIC とサードパーティ製のアダプタの両方をサポートしています。さらに、新しい SIOC には2つの NVME スロットがあります。サポートされているカードとアダプタの完全なリストについては、『Cisco UCS Manager リリース 4.0 と Cisco UCS S3260 サーバ統合』を参照してください。

UCS VIC 1400 シリーズ アダプタ

UCS M5 サーバで次の UCS VIC 1400 シリーズ アダプタ カードをサポートします。

- B シリーズ向け VIC 1440 10/40G mLOM (UCSB-MLOM-40G-04)
- B シリーズ (UCSB-VIC-M84-4P) の VIC 1480 10/40G PCIe
- C シリーズおよび S シリーズ (UCSC-PCIE-C25Q-04) 向け VIC 1455 10/25G PCIe
- C シリーズ (UCSC-MLOM-C25Q-04) の VIC 1497 40/100G mLOM

Cisco UCS Manager リリース 4.0 (1) では、UCS 6454、UCS 6300 シリーズ、および 6200 シリーズ ファブリック インターコネクで UCS VIC 1400 シリーズ アダプタがサポートされています。UCS ミニではサポートされていません。このリリースでは、VIC 1455 または VIC 1457 を

搭載した UCS 6454 ファブリック インターコネクトと C シリーズサーバ間の 10G/25G イーサネット接続がサポートされています。



- (注) 同じサーバ上で、異なるシリーズの VIC アダプタをインストールすることはできません。たとえば、同じサーバ上で、UCS VIC 1300 シリーズ アダプタおよび UCS VIC 1400 シリーズ アダプタをインストールできません。

次の表に、Cisco UCS Manager リリース 4.0 (1) でサポートされている VIC 1400 シリーズアダプタ/サーバの組み合わせを示します。

表 3: M5 B シリーズ サーバの VIC 1400 シリーズ アダプタ サポート

FI	IOM	1400 シリーズ VIC アダプタ			
		VIC 1440	VIC 1440 + ポート エクспан ダ	VIC 1480	VIC 1440 + VIC 1480
		UCSB-MLOM-40G-04	UCSB-MLOM-40G-04 + UCSB-MLOM-PT-01	UCSB-VIC-M84-4P	UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P
6200 シリーズ	2204/2208	B480 M5、 B200 M5	NA	B480 M5	B480 M5、 B200 M5
6300 シリー ズ :	2304	B480 M5、 B200 M5	B480 M5、 B200 M5	B480 M5	B480 M5、 B200 M5
	2204/2208	B480 M5、 B200 M5	NA	B480 M5	B480 M5、 B200 M5
6454	2204/2208	B480 M5、 B200 M5	NA	B480 M5	B480 M5、 B200 M5

表 4: M5 C シリーズおよび S シリーズ サーバの VIC 1400 シリーズ アダプタ サポート

FI	FEX	UCS VIC 1400 シリーズ アダプタ	
		VIC 1455	VIC 1455 および 1457
		UCSC-PCIE-C25Q-04	UCSC-MLOM-C25Q-04
6200 シリーズ	直接接続	C220 M5、C240 M5、C480 M5、S3260 M5 (UCS-S3260-PCISIOC を使用)	C220 M5、C240 M5
	2232 PP	C220 M5、C240 M5、C480 M5、S3260 M5 (UCS-S3260-PCISIOC を使用)	C220 M5、C240 M5
	2232-T	NA	NA
6300 シリーズ :	直接接続	C220 M5、C240 M5、C480 M5、C125 M5、S3260 M5 (UCS-S3260-PCISIOC を使用)	C220 M5、C240 M5
	直接接続 (ブレークアウト)	C220 M5、C240 M5、C480 M5、C125 M5、S3260 M5 (UCS-S3260-PCISIOC を使用)	C220 M5、C240 M5
	2232 PP	C220 M5、C240 M5、C480 M5、C125 M5、S3260 M5 (UCS-S3260-PCISIOC を使用)	C220 M5、C240 M5
	2232-T	NA	NA
	2348	C220 M5、C240 M5、C480 M5、C125 M5、S3260 M5 (UCS-S3260-PCISIOC を使用)	C220 M5、C240 M5

FI	FEX	UCS VIC 1400 シリーズ アダプタ	
		VIC 1455	VIC 1455 および 1457
		UCSC-PCIE-C25Q-04	UCSC-MLOM-C25Q-04
6454	直接接続 (10G/25G)	C220 M5、C240 M5、 C480 M5、C125 M5、 S3260 M5 (UCS-S3260-PCISIOC を使用)	C220 M5、C240 M5
	2232 PP	C220 M5、C240 M5、 C480 M5、C125 M5、 S3260 M5 (UCS-S3260-PCISIOC を使用)	C220 M5、C240 M5
	2232-T	NA	NA



(注) サーバおよびアダプタの組み合わせの詳細については、「サーバ仕様シート」を参照してください。

- [B シリーズ サーバ仕様シート](#)
- [C シリーズ サーバ仕様シート](#)
- [S シリーズ サーバ仕様シート](#)

周辺機器 (Peripherals)

- C240Hx M5 サーバを搭載した HX-PCIE-OFFLOAD-1 コプロセッサ カードのサポート
- UCS 6332-16UP ファブリック インターコネクタの高電圧 DC 1200 ワット電源 N9K-PUV-1200W のサポート
- Intel Optane NVMe Med. C220、C240、C480、B200、B480、S3260、および Hyperflex との同等物を含む M5 サーバのパフォーマンス ドライブ。
- UCS C220、C240、C480 M5 サーバ上の LSI 9400 8e 外部 SAS HBA をサポートします。

リリース 4.0 (4e) での新しいソフトウェア機能

UCS ファブリック エクステンダ 2408 のサポート

UCS ファブリック エクステンダ 2408 (UCS-IOM-2408) は、UCS 6454 ファブリック インターコネクタ上でのみ、B シリーズ M4 および M5 サーバへの 10/25 GbE 接続をサポートすることにより、展開の柔軟性を実現します。

リリース 4.0 (4c) での新しいソフトウェア機能

ADDDC RAS の変更

- Adaptive Double Device Data 補正 (ADDDC) は、修正されたエラーをモニタし、修正されていないエラーが発生して停止する前に対処することによって、障害が発生した DRAM の動的なマッピングを可能にするメモリ RAS 機能です。デフォルトでは有効になっています。

ADDDC のスペアリングがメモリ領域を再マップすると、システムは影響を受ける領域をターゲットとするメモリ帯域幅の大幅なワークロードにより、大量のメモリ遅延と帯域幅のペナルティを発生させる可能性があります。ADDDC RAS 障害が報告された後に、障害が発生した DIMM を交換するように予防的メンテナンスをスケジューリングすることを推奨します。

BIOS の更新

- **Select MEMORY RAS 設定** トークンのデフォルトは、すべての M5 サーバの最大パフォーマンスから ADDDC スペアに変更されました。

Intel® VMD Enhancements to NVME

4.0(4c) 以降のリリースでは、ローカルストレージに対するインテル ボリューム管理デバイス (VMD) をサポートします。オプションの VMD ドライバ .iso パッケージは、次のオペレーティング システムの Cisco ダウンロード サイトから入手できます。

- RHEL 7.3、7.4、7.5、7.6
- CENTOS 7.3、7.4、7.5、7.6
- SLES-15、SLES-15 v4
- Windows 2016、Windows 2019
- ESXi 6.5 U2、6.7 U1、6.7 U2
- Ubuntu 18.04.1

VMD によって提供される拡張機能は、PCIe ソリッドステート ドライブ (SSD) のホットプラグのサポートを提供します。また、コマンドラインインターフェイスを使用して、ドライブ ステータスを示す点滅パターンを設定することもできます。

リリース 4.0(4a) での新しいソフトウェア機能

新しいハードウェアのソフトウェア有効化(「新しいハードウェア」の項に記載されています)

Intel® Optane™ データ センター永続メモリ モジュール

Cisco UCS Manager Release 4.0 (4) では、第二世代インテル® Xeon® Scalable プロセッサに基づく UCS M5 サーバ上の Intel® Optane™ データ センター永続メモリ モジュールのサポートが導入さ

れています。Intel® Optane™ DC 永続メモリ モジュールは、第二世代インテル® Xeon® Scalable プロセッサでのみ使用できます。

このリリースでは、Cisco UCS Manager を使用して Intel® Optane™ DC 永続メモリ モジュールを設定し管理する機能が提供されています。永続メモリ モジュールは、メモリの低遅延とストレージの永続化を実現する不揮発性メモリ モジュールです。永続メモリ モジュールに保存されているデータは、他のストレージデバイスに比べてすぐにアクセスでき、電源サイクルで保持されます。

Cisco UCS 6454 ファブリック インターコネクットの機能強化

- マルチキャスト MAC フィルタリング: この機能拡張により、ホストは受信するトラフィックのタイプに登録できるようになり、この基準に基づいて vNICs へのトラフィック転送が容易になります。
- ユニファイド ポートの数が 8 から 16 に増加しました。Cisco UCS Manager リリース 4.0 (4) 以降では、Cisco UCS 6454 ファブリック インターコネクットのポート番号付けは次のとおりです。

表 5: UCS 6454 ファブリック インターコネクットのポート番号付け

ポート	説明	ポート	説明
1-16	ユニファイド ポートは、10/25 Gbps のイーサネットまたは 8/16/32 Gbps ファイバチャネルとして動作できます。FC ポートは、最初の4つのポート (ポート 1 ~ 4) または最初の 8 ポート (ポート 1 ~ 8) で、4つのポートのグループに変換されます。	17-44	各ポートは、10 Gbps または 25 Gbps SFP28 ポートとして動作できます。
45-48	各ポートは、1 Gbps、10 Gbps、または 25 Gbps のイーサネットポートまたは FCoE ポートとして動作できます。	49-54	各アップリンク ポートは、40 Gbps または 100 Gbps のイーサネットポートまたは FCoE ポートとして動作できます。ブレイクアウトケーブルを使用すると、これらのポートの各は 4 x 10 Gbps または 4 x 25 Gbps のイーサネットまたは FCoE ポートとして動作します。 ポート 49 ~ 54 は、UCS サーバポートではなく、イーサネットまたは FCoE アップリンクポートに接続するときに使用できます。

- Cisco UCS 6454 Fabric Interconnect のファイバチャネル スイッチ モードでの FCoE アップリンク ポートをサポートします。
 - FC スイッチモードと FC エンドホストモードの両方で、Cisco UCS 6454 Fabric Interconnect ごとに最大 8 つの FCoE SAN アップリンク ポートチャンネルがサポートされます。最大 4 つの FC SAN ポート チャンネルが Cisco UCS 6454 Fabric Interconnect ごとにサポートされません。
- Cisco UCS 6454 Fabric Interconnect に FC SAN ポートチャンネルと FCoE SAN ポートチャンネルが混在している場合、合計で 8 個以上ののポートチャンネルにすることはできません。

UCS ファブリック エクステンダ 2304V2 のサポート

UCS ファブリック エクステンダ 2304V2 (UCS-IOM-2304V2) は、UCS ファブリック エクステンダ 2304、8 個の 40 ギガビット バックプレーン ポートおよび 4 個の 40 ギガビット アップリンク ポートを備えた I/O モジュールに基づいています。

機能強化

- SUSE Linux Enterprise Server (SLES) の Consistent Device Naming (CDN) サポート: SLES 12 SP3、SLES 12 SP4、および SLES 15 を含むように CDN サポートが拡張されました。
- [Intel Speed Select]: [Intel Speed Select] を使用すると、論理プロセッサ コア、頻度、および TDP スレッド設定の数に基づき、3 つの動作プロファイルのいずれかを選択して、CPU のパフォーマンスを最適化できます。BIOS ポリシー内では、Intel の速度選択を設定できません。ブート時に、BIOS はサポートされている CPU を検出し、ユーザーが指定した 3 つのプロファイルのいずれかに設定します。
- MSwitch ディザスタ リカバリ: この拡張機能を使用すると、破損した MSwitch を回復し、以前動作したファームウェアにロールバックすることができます。
- 代替 KVM ポート: KVM ポートとして 1024~49151 のポート番号を設定できます。
- UCS S3260 M4 および M5 サーバのディスク スクラブ: このリリースでは、UCS S3260 M4 および M5 サーバのディスク スクラブ機能が拡張されています。サービス プロファイルに関連付けられているサーバの場合、サービス プロファイルに使用されているスクラブポリシーに基づいて、割り当て解除時にディスク スクラブが行われます。
- SLES 12 SP4、SLES 15、および RHEL 7.6 上のファイバチャネルおよび NVMe 上での統合ドライバのサポート。これは、SLES 12 SP3 で以前サポートされていたものに追加されています。このサポートは、UCS 6300 シリーズ ファブリック インターコネクトおよび UCS 6454 ファブリック インターコネクトで使用できます。ファイバチャネル上の NVMe は、最大 16 個のインターフェイスをサポートするようになりました。
- サポートされているすべての Linux プラットフォームで署名付きドライバをサポートしています。すべての Cisco Linux ドライバが暗号化されて署名されるようになりました。これは、サポートされているすべての Linux プラットフォームで、UEFI セキュアブートとともに使用できることを意味します。UEFI セキュアブートにより、信頼できるファーム

ウェアとドライバのみがシステムブート時に実行できるようになり、ブート時にマルウェアに対する脆弱性が低下します。

- 次のサーバ上の Cisco Boot 最適化 M. 2 RAID コントローラ (HWRAID) のハードウェア RAID サポート。
 - Cisco UCS C220 M5 サーバ
 - Cisco UCS C240 M5 サーバ
 - Cisco UCS C480 M5 サーバ
 - Cisco UCS B200 M5 サーバ
 - Cisco UCS B480 M5 サーバ

リリース 4.0(2a) での新しいソフトウェア機能

新しいハードウェアのソフトウェア有効化(「新しいハードウェア」の項に記載されています)

Cisco UCS 6454 ファブリック インターコネクットの機能強化

このリリースでは、Cisco UCS 6454 ファブリック インターコネクットで次の機能のサポートが導入されています。

- イーサネットおよびファブリック インターコネクット モードをサポートします。

イーサネット スイッチング モード:

- **VLAN ポート カウント最適化の有効化はサポートされていません。VLAN ポート カウント最適化の有効化を行わず、Cisco UCS 6454 ファブリック インターコネクットは 16000 PV カウントをサポートします。**

ファイバチャネル スイッチング モード:

- FCoE アップリンクはサポートされていません
- サポートされたブレイクアウト ケーブルを使用して、1つの QSFP ポートを 4つの 10/25G ポートに分割をサポートします。これらのポートは、イーサネット アップリンクまたは FCoE アップリンク ポートの 10/25 G スイッチに接続するとしてのみ使用できます。これらは、サーバポート、FCoE ストレージポート、アプライアンス ポートまたはモニタリング ポートとして設定できません。
- UCS 6454 ファブリック インターコネクット MAC セキュリティのサポート

Cisco UCS C480 M5 ML サーバ

このリリースでは、Cisco UCS C480 M5 ML サーバのサポートが導入されています。

次の機能は、Cisco UCS C480 M5 ML サーバではサポートされていません。

- 背面 NVME ケージおよび PCIe NVME スイッチ カード

- 背面補助ドライブ ケージ
- Cisco 12G 9460-8i RAID コントローラ (UCSC-SAS9460-8i)

UCS VIC 1400 シリーズ アダプタの機能拡張

このリリースでは、UCS M5 サーバで新たに導入された UCS VIC 1495 および1497アダプタのサポートが追加されました。

UCS VIC 1400 シリーズ アダプタは、次の機能をサポートするようになりました。

- プライマリ シャーシ上の UCS VIC 1440 および UCS VIC 1480 アダプタでの UCS ミニをサポートしています。
 - ファイバチャネルでの NVMe をサポートし、ファイバチャネル NVMe インターフェイスに適用するためのマッピング プロトコルを定義します。このリリースでは、UCS 6300 シリーズ ファブリック インターコネクトおよび UCS 6454 ファブリック インターコネクトで、**FC NVME イニシエータ**アダプタ ポリシーのサポートが追加されています。
- FC NVME ターゲット** および **FC ターゲット** は、Tech Preview オプションとして使用できます。
- FC マルチ キュー: FC マルチ キューの強化された I/O キュー範囲のサポート。新しい範囲は、1~64 のキューです。
 - Windows 2016 VMQ および SET をサポートしています。
 - eNIC ドライバの Tx キューと Rx キューの増加: B シリーズおよび C シリーズ サーバ上のすべての VIC 1400、1300、および 1200 シリーズ アダプタ カードでサポートされています。この速度を効率的に使用するために、Tx キューと Rx キューの数がそれぞれ 8 から 256 に増加しています。eNIC ドライバは、256 Tx キューと 256 Rx キューをサポートするようになりました。ただし、サポートされている Rx キューと Tx キューの最大数は、システム内の CPU コア数を超えることはできません。

Cisco UCS S3260 ストレージサーバの新世代 SIOC でのアウトオブバンド NVME サポート

S3260 M5 サーバ用 S3260 UCS-S3260-PCISIOC 新世代 SIOC でのアウトオブバンド NVME をサポートするための機能強化。

機能強化

- UCS ミニ ファブリック インターコネクト: Cisco UCS Manager リリース 4.0 (2) の機能強化により、Cisco UCS ミニの次の機能強化が導入されました。
 - Cisco UCS ミニ ファブリック インターコネクトは、プライマリ シャーシの B シリーズサーバに対して、次の VIC 1400 シリーズ アダプタ カードをサポートするようになりました。
 - UCSB-MLOM-40G-04 (UCS VIC 1440)
 - UCSB-VIC-M84-4P (UCS VIC 1480)

- VIC 1300 シリーズ アダプタ カードを搭載した Cisco UCS ミニファブリック インターコネクトは、次の機能をサポートするようになりました。
 - usNIC
 - VXLAN
 - NetFlow
 - スロー ドレイン: Cisco UCS Manager リリース 4.0(2) には、Cisco UCS 6454 ファブリック インターコネクトで QoS 低速ドレインの検出と緩和機能が導入されています。この機能は、ネットワークで輻輳を引き起こしている低速ドレインデバイスを検出することを可能にするさまざまな機能拡張を行い、さらに輻輳回避も提供します。
 - 合理化した RAID0 設定: Cisco UCS Manager は、LUN 設定オプションを使用した個々の RAID0 LUN にディスク スロットの範囲を設定する機能を提供します。
 - B シリーズ M5 サーバでの SED セキュリティ ポリシーのサポート: Cisco UCS Manager リリース 4.0 (2) は、SED セキュリティ ポリシーを UCS B シリーズ M5 サーバに拡張します。
 - ファブリック インターコネクトに接続されている UCS C シリーズ サーバでの Redfish バージョン 1.01 をサポートします。
 - NVMe ドライブの残量: NVMe 統計情報は、そのワークロードに基づいて NVMe ドライブで残量を表示するように強化されています。
 - パラレルディスク アップデート: 複数のディスクでのパラレルファームウェアアップデートをサポートします。
 - UCS M5 サーバのブート時間を短縮するための最適化されたメモリ初期化とテストプロセスのサポート: Cisco UCS Manager リリース 4.0 (2) では、UCS M5 サーバのブート時間を改善するために次の BIOS トークンが導入されています。
 - 適応型メモリ トレーニング コントロール
 - OptionROM 起動最適化コントロール
 - BIOS Tech メッセージ レベル コントロール
- 3 つのトークンすべてのデフォルト値が有効になっています。
- デバイス コネクタの証明書マネージャ: 証明書マネージャでは、信頼できる証明書のリストを表示し、有効な信頼できる証明書をインポートできます。

リリース 4.0(1a) での新しいソフトウェア機能

新しいハードウェアのソフトウェア有効化(「新しいハードウェア」の項に記載されています)

Cisco UCS 6454 Fabric Interconnect

このリリースでは、40/100ギガビットアップリンクポートを使用してファブリック内の10/25ギガビットポートをサポートするCisco UCS 6454 Fabric Interconnectが導入されました。『Cisco UCS Manager リリース 4.0 スタートアップガイド』には、専用ポートに関する詳細情報が掲載されています。

サポートされている新機能

Cisco UCS 6454 ファブリック インターコネクには、次の新機能が導入されています。

- 40/100ギガビットアップリンクポートを使用してファブリック内の10/25ギガビットポートをサポートします。
- VIC 1400 シリーズ アダプタ カードのサポート
- 内部使用のために予約された 128 個の追加の VLAN
- ポートのエラー修正 (FEC) 設定の転送

サポートされていないレガシー機能

次の機能は、Cisco UCS 6454 ファブリック インターコネクにはサポートされていません。

- 非ポート チャネル モードでのシャーシ検出ポリシー
- 非ポート チャネル モードでシャーシの接続ポリシー
- イーサネットまたは FC スイッチング モード
- ダイナミック vNICs を使用したサービス プロファイル
- マルチキャストの最適化
- Netflow
- MAC セキュリティ
- 分散仮想スイッチへのポート プロファイルの割り当て
- VMFEX

異なる構成の機能

次の機能は、Cisco UCS 6454 ファブリック インターコネクには別に設定されています。

- ユニファイドポート: Cisco UCS 6454 ファブリック インターコネクには最大 8 個のユニファイドポートをサポートします。これらは FC として設定できます。
- VLAN 最適化: Cisco UCS 6454 ファブリック インターコネクには、PV カウントは次のようになります。
 - VLAN ポート数の最適化が無効になっている場合: 16000
 - VLAN ポート数の最適化が有効になっている場合: 64000

Cisco UCS C125 M5 サーバ

このリリースでは、Cisco UCS C125 M5 サーバのサポートが導入されています。

次に、C125 M5 サーバと他のラックサーバの2つの主な違いを示します。

- パワー キャッピングは Cisco UCS C125 M5 サーバ ではサポートされません。
- Cisco UCS C125 M5 サーバでは、接続しているすべてのサーバに対して同じ**[Fan Speed Policy]**が選択されていることを確認します。Cisco UCS Managerは最後に関連付けるサーバの**[Fan Speed Policy]**を適用します。すべてのサーバに対して同じ **[Fan Speed Policy]** を選択することで、最後に関連付けるサーバに関係なく希望の **[Fan Speed Policy]** が選択されます。

UCS VIC 1400 シリーズ アダプタ

UCS M5 サーバでの UCS VIC 1400 シリーズ アダプタ カードをサポートします。

これらのアダプタでは、次の新機能のサポートが追加されました。

- Windows 用の VxLAN および NVGRE カプセル化によるステートレス オフロード
- Windows 向け VMMQ
- ESXi および Linux の UDP RSS
- IPv6 ヘッダのサポート
- NetFlow
- QoS のサポート
- UCS VIC 1455 および 1457 アダプタを使用したポート チャネルのサポート



(注) Cisco UCS Manager リリース 4.0(1) では、UCS 6300 シリーズ ファブリック インターコネクタに直接接続しているラックサーバ上で、VIC 1455 または 1457 アダプタ間の FC/FCoE 単一リンク ポート チャネルのみサポートしています。



(注) ポートチャネルでは、両方のポートの速度が同じである必要があります。

次の機能は、UCS VIC 1400 シリーズ アダプタではサポートされていません。

- Hyper-V 用 VM-FEX
- VMware 用 VM-FEX
- ダイナミック vNIC

- UCS VIC 1455 および 1457 アダプタ上の 4 つのメンバポートを持つポートチャンネル
- Cisco UCS C125 M5 サーバの usNIC

Cisco UCS S3260 ストレージサーバの新世代 SIOC

新しいサーバ SIOC UCS-S3260 UCS-S3260-PCISIOC および VIC 1400 シリーズアダプタカードを搭載した S3260 M5 サーバをサポートします。

機能強化

- Hyperflex 3.5 リリース機能の事前有効化サポート
- キー管理サーバとの統合をサポートする C480 M5 での KMIP クライアントのサポート
- Cisco UCS Manager で管理されている C シリーズおよび S シリーズ M4 サーバ上の PXE ブートデバイスでの IPv6 オプションをサポートします。
- **ログイン プロファイル**機能をサポートします。ログインの試行が失敗した後、特定の期間、Cisco UCS Manager へのログイン要求をブロックする機能を提供します。この機能は現在、UCS 6454 ファブリック インターコネクトおよび Cisco UCS Manager リリース 4.0 (1) 以降のリリースでのみサポートされています。

Cisco UCS Manager リリース 4.0 で廃止されたハードウェアおよびソフトウェア

Cisco UCS Manager リリース 4.0 では、UCS B シリーズ M2 世代のブレードサーバはサポートされていません。Cisco UCS Manager リリース 4.0 は、Cisco UCS Manager の以前のリリースで廃止されたハードウェアまたはソフトウェアをサポートしていません。

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 リリースと以前の C シリーズ スタンドアロン リリースの一部が組み込まれています。たとえば、Cisco UCS Manager リリース 4.0 (1) は、M5 サーバ用の C シリーズ スタンドアロン リリース 4.0 (1) と、すべての M3 および M4 サーバのリリース 3.0 (4) と統合されています。そのため、C シリーズ スタンドアロン リリースでサポートされているすべての M5、M4、および M3 サーバをサポートします。

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 6: 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
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
3.2(3)	3.1(3)	C220 M5、C240 M5、C480 M5、S3260 M5 のみ
	3.0 (4)	すべての M3/M4
3.2(2)	3.1(2)	C220 M5、C240 M5、C480 M5 のみ
	3.0(3)	すべての M3/M4
3.2(1)	3.1(1)	C220 M5、C240 M5 のみ
	3.0(3)	すべての M3/M4
3.1(3)	3.0(3)	すべての M3/M4
3.1(2)	2.0(13)	すべての M3/M4
3.1(1)	2.0(10)	C220 M4、C240 M4 のみ
	2.0(9)	その他のすべての M3/M4

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
2.2(8)	2.0(12)	C460 M4 のみ
	2.0(10)	C220 M4、C240 M4 のみ
	1.5 (9)	C420-M3、C260-M2、C460-M2 のみ
	2.0(9)	その他のすべての M3/M4

システム要件

Cisco UCS Central 統合

Cisco UCS Manager リリース4.0 は、Cisco UCS Central リリース 2.0 (1f) 以降にのみ登録できます。

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	Web ブラウザ
HTML5	Microsoft Internet Explorer 11 以降 Mozilla Firefox 45 以降 Google Chrome 45 以降 Apple Safari バージョン 9 以降 Opera バージョン 35 以降

ネットワーク要件

デバイス コネクタ機能を使用するには、HTTPS プロキシを設定する必要があります。『*Cisco UCS Manager* 管理者用管理ガイド』には、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。

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、FEX ファームウェア) は、サーバ上で以前のリリースの B バンドルまたは C バンドル (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) と同時に使用できます。

次の表に、Cisco UCS 6200、6300 および 6454 ファブリック インターコネクでサポートされる A、B、および C バンドルの混在バージョンを示します。

表 7: Cisco UCS 6200、6300、6454 ファブリック インターコネク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)	2.2(8)	3.1(3)	3.2(1)	3.2(2)	3.2(3)	4.0(1)	4.0(2)	4.0(4)
2.2(8)	6200	6200	6200	6200	6200	6200	6200	6200
3.1(3)	—	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP
3.2(1)	—	—	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP
3.2(2)	—	—	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP
3.2(3)	—	—	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP
4.0(1)	—	—	—	—	—	6200,6332、 6332 16UP、 6454	6200,6332、 6332 16UP、 6454	6200,6332、 6332 16UP、 6454
4.0(2)	—	—	—	—	—	6200,6332、 6332 16UP、 6454	6200,6332、 6332 16UP、 6454	6200,6332、 6332 16UP、 6454
4.0(4)	—	—	—	—	—	6200,6332、 6332 16UP、 6454	6200,6332、 6332 16UP、 6454	6200,6332、 6332 16UP、 6454

次の表に、Cisco UCS Mini ファブリック インターコネクでサポートされる A、B、および C の混在バンドルバージョンを示します。

表 8: Cisco UCS Mini ファブリック インターコネク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)	3.1(3)	3.2(1)	3.2(2)	3.2(3)	4.0(1)	4.0(2)	4.0(4)
3.1(3)	6324	6324	6324	6324	6324	6324	6324
3.2(1)	—	6324	6324	6324	6324	6324	6324
3.2(2)	—	6324	6324	6324	6324	6324	6324
3.2(3)	—	6324	6324	6324	6324	6324	6324
4.0(1)	—	—	—	—	6324	6324	6324
4.0(2)	—	—	—	—	6324	6324	6324
4.0(4)	—	—	—	—	6324	6324	6324

次の表に、4.0(4)A バンドルを備えたすべてのプラットフォームでサポートされる、B および C バンドルの混在バージョンを示します。

表 9: 4.0(4)A バンドルを備えたすべてのプラットフォームでサポートされる、B、C バンドルの混在バージョン

	インフラストラクチャのバージョン (A バンドル)			
Host FW Versions (B, C Bundles)	4.0(4)			
	6200	6300	6324	6454
	ucs-k9-bundle-infra. 4.0.x.xxx.A.bin	ucs-6300-k9-bundle-infra. 4.0.x.xxx.A.bin	ucs-mini-k9-bundle-infra. 4.0.x.xxx.A.bin	ucs-6400-k9 -bundle-infra. 4.0.x.xxx.A.bin
2.2(8) (B、C バンド ル)	対応	—	—	—
3.1(3) (B、C バンド ル)	対応	対応	対応	—

	インフラストラクチャのバージョン (A バンドル)			
3.2(1)、3.2(2)、 3.2(3) (B、C バンドル)	対応	対応	対応	—
4.0 (1)、4.0 (2)、4.0 (4) (B、C バンドル)	対応	対応	対応	対応

次の表に、4.0(2)A バンドルを備えたすべてのプラットフォームでサポートされる、B および C バンドルの混在バージョンを示します。

表 10: 4.0(2)A バンドルを備えたすべてのプラットフォームでサポートされる、B、C バンドルの混在バージョン

	インフラストラクチャのバージョン (A バンドル)			
Host FW Versions (B, C Bundles)	4.0(2)			
	6200	6300	6324	6454
	ucs-k9-bundle-infra. 4.0.x.xxx.A.bin	ucs-6300-k9-bundle-infra. 4.0.x.xxx.A.bin	ucs-mini-k9-bundle-infra. 4.0.x.xxx.A.bin	ucs-6400-k9- bundle-infra。 4.0.x.xxx.A.bin
2.2(8) (B、C バンドル)	対応	—	—	—
3.1(3) (B、C バンドル)	対応	対応	対応	—
3.2(1)、3.2(2)、 3.2(3) (B、C バンドル)	対応	対応	対応	—
4.0 (1)、4.0 (2)、4.0 (4) (B、C バンドル)	対応	対応	対応	対応

次の表に、4.0(1)A バンドルを備えたすべてのプラットフォームでサポートされる、B および C バンドルの混在バージョンを示します。

表 11: 4.0(1)A バンドルを備えたすべてのプラットフォームでサポートされる、B、C バンドルの混在バージョン

Host FW Versions (B, C Bundles)	インフラストラクチャのバージョン (A バンドル)			
	4.0(1)			
	6200	6300	6324	6454
	ucs-k9-bundle-infra.4.0.x.xxx.A.bin	ucs-6300-k9-bundle-infra.4.0.x.xxx.A.bin	ucs-mini-k9-bundle-infra.4.0.x.xxx.A.bin	ucs-6400-k9-bundle-infra.4.0.x.xxx.A.bin
2.2(8) (B、C バンドル)	対応	—	—	—
3.1(3) (B、C バンドル)	対応	対応	対応	—
3.2(1)、3.2(2)、3.2(3) (B、C バンドル)	対応	対応	対応	—
4.0 (1)、4.0 (2)、4.0 (4) (B、C バンドル)	対応	対応	対応	対応



重要 バージョンをまたがるファームウェアを設定する場合は、サーバのエンドポイントのファームウェアのバージョンが Cisco UCS ドメイン の設定に対応する必要がある必要があります。

内部的な依存関係

ここでは、Cisco UCS ハードウェアと Cisco UCS Manager のバージョン間の相互依存について説明します。

- 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。

6200シリーズ、6332シリーズ、および6454 ファブリック インターコネクとコンポーネント

ブレード サーバ



-
- (注) ファームウェア設定が混在すると、最小サーババンドルが最小ソフトウェアバージョンに対応していることを推奨します。インフラストラクチャは、最小ソフトウェアバージョン以上である必要があります。
-

表 12: ブレード サーバの最小ホスト ファームウェア バージョン

サーバ	最小ソフトウェアバージョン UCS 6200 シリーズ FI	最小ソフトウェアバージョン UCS 6332、6332-16UP FI	最小ソフトウェアバージョン UCS 6332、6332-16UP FI		最小ソフトウェアバージョン UCS 6454 FI	推奨されるソフトウェアバージョン UCS 6200 シリーズ FI UCS 6332、6332-16UP FI UCS 6454 FI
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304	UCS-IOM-2304/2	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408 *	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408 *
					* UCS-IOM-2408 は、UCS 6454 FI および VIC 1300/1400 を持つ M4 および M5 でサポートされています。	
B22 M3 E5-2400	2.2 (8a)	3.1(3a)	3.1(3a)	4.0 (4i)	4.0(1a)	4.0 (4i)
B22 M3 E5-2400 v2	2.2 (8a)	3.1(3a)				
注: M3 サーバは、6454 FI と 2408 IOM の組み合わせをサポートしていません。ただし、6454 FI と 2208 IOM、および 6454 FI と 2204 IOM の組み合わせをサポートしています。						

サーバ	最小ソフトウェアバージョン UCS 6200 シリーズ FI	最小ソフトウェアバージョン UCS 6332、6332-16UP FI	最小ソフトウェアバージョン UCS 6332、6332-16UP FI		最小ソフトウェアバージョン UCS 6454 FI	推奨されるソフトウェアバージョン UCS 6200 シリーズ FI UCS 6332、6332-16UP FI UCS 6454 FI
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304	UCS-IOM-2304/2	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408 *	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408 *
					* UCS-IOM-2408 は、UCS 6454 FI および VIC 1300/1400 を持つ M4 および M5 でサポートされています。	
B200 M3 E5-2600	2.2 (8a)	3.1(3a)	3.1(3a)	4.0 (4i)	4.0(1a)	4.0 (4i)
B200 M3 E5-2600 v2	2.2 (8a)	3.1(3a)				
注: M3 サーバは、6454 FI と 2408 IOM の組み合わせをサポートしていません。ただし、6454 FI と 2208 IOM、および 6454 FI と 2204 IOM の組み合わせをサポートしています。						
UCS C220 M3	2.2 (8a)	3.1(3a)	3.1(3a)	4.0 (4i)	4.0(1a)	4.0 (4i)
B200 M5	3.2(1d)	3.2(1d)	3.2(1d)	4.0 (4i)	4.0(1a)	4.0 (4i)

サーバ	最小ソフトウェアバージョン UCS 6200 シリーズ FI	最小ソフトウェアバージョン UCS 6332、6332-16UP FI	最小ソフトウェアバージョン UCS 6332、6332-16UP FI		最小ソフトウェアバージョン UCS 6454 FI	推奨されるソフトウェアバージョン UCS 6200 シリーズ FI UCS 6332、6332-16UP FI UCS 6454 FI
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304	UCS-IOM-2304A2	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408 *	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408 *
					* UCS-IOM-2408 は、UCS 6454 FI および VIC 1300/1400 を持つ M4 および M5 でサポートされています。	
B260 M4 E7-2800 v2	2.2 (8a)	3.1(3a)	3.1(3a)	4.0 (4i)	4.0(1a)	4.0 (4i)
B260 M4 E7-4800 v2	2.2 (8a)	3.1(3a)				
B260 M4 E7-8800 v2	2.2 (8a)	3.1(3a)				
B260 M4 E7-4800 v3	2.2 (8a)	3.1(3a)				
B260 M4 E7-8800 v3	2.2 (8a)	3.1(3a)				
B260 M4 E7-4800 v4	2.2 (8b)	3.1(3a)	3.1(3a)	4.0 (4i)	4.0(1a)	4.0 (4i)
B260 M4 E7-8800 v4	2.2 (8b)	3.1(3a)	3.1(3a)			
B420 M3 E5-4600	2.2 (8a)	3.1(3a)	3.1(3a)	4.0 (4i)	4.0(1a)	4.0 (4i)
B420 M3 E5-4600 v2	2.2 (8a)	3.1(3a)				
B420 M4 E5-4600 v3	2.2 (8a)	3.1(3a)	3.1(3a)	4.0 (4i)	4.0(1a)	4.0 (4i)
B420 M4 E5-4600 v4	2.2 (8b)	3.1(3a)	3.1(3a)			

サーバ	最小ソフトウェアバージョン UCS 6200 シリーズ FI	最小ソフトウェアバージョン UCS 6332、6332-16UP FI	最小ソフトウェアバージョン UCS 6332、6332-16UP FI		最小ソフトウェアバージョン UCS 6454 FI	推奨されるソフトウェアバージョン UCS 6200 シリーズ FI UCS 6332、6332-16UP FI UCS 6454 FI
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304	UCS-IOM-2304/2	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408 *	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408 *
					* UCS-IOM-2408 は、UCS 6454 FI および VIC 1300/1400 を持つ M4 および M5 でサポートされています。	
B460 M4 E7-4800 v2	2.2 (8a)	3.1(3a)	3.1(3a)	4.0 (4i)	4.0(1a)	4.0 (4i)
B460 M4 E7-8800 v2	2.2 (8a)	3.1(3a)				
B460 M4 E7-4800 v3	2.2 (8a)	3.1(3a)				
B460 M4 E7-8800 v3	2.2 (8a)	3.1(3a)				
B460 M4 E7-4800 v4	2.2 (8b)	3.1(3a)	3.1(3a)	4.0 (4i)	4.0(1a)	4.0 (4i)
B460 M4 E7-8800 v4	2.2 (8b)	3.1(3a)				
B480 M5	3.2(2b)	3.2(2b)	3.2(2b)	4.0 (4i)	4.0(1a)	4.0 (4i)

[Rack Servers]

表 13: ブレード サーバの最小ホスト ファームウェア バージョン

サーバ	最小ソフトウェアバージョン UCS 6200 シリーズ FI	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6454	推奨されるソフトウェアバージョン UCS 6200 シリーズ FI UCS 6332、6332-16UP FI UCS 6454
C22 M3 および M3L	2.2 (8a)	3.1(3a)	4.0(1a)	4.0 (4i)
C24 M3、M3L、および M3S2	2.2 (8a)	3.1(3a)	4.0(1a)	4.0 (4i)
C220 M3	2.2 (8a)	3.1(3a)	4.0(1a)	4.0 (4i)
C220 M4	2.2 (8a)	3.1(3a)	4.0(1a)	4.0 (4i)
C220 M5	3.2(1d)	3.2(1d)	4.0(1a)	4.0 (4i)
C240 M3	2.2 (8a)	3.1(3a)	4.0(1a)	4.0 (4i)
C240 M4	2.2 (8a)	3.1(3a)	4.0(1a)	4.0 (4i)
C240 M5	3.2(1d)	3.2(1d)	4.0(1a)	4.0 (4i)
C460 M4 E7-2800 v2	2.2 (8a)	3.1(3a)	4.0(1a)	4.0 (4i)
C460 M4 E7-4800 v2	2.2 (8a)	3.1(3a)		
C460 M4 E7-8800 v2	2.2 (8a)	3.1(3a)		
C460 M4 E7-4800 v3	2.2 (8a)	3.1(3a)		
C460 M4 E7-8800 v3	2.2 (8a)	3.1(3a)		
C460 M4 E7-8800 v4	2.2 (8b)	3.1(3a)	4.0(1a)	4.0 (4i)
C480 M5	3.2(2b)	3.2(2b)	4.0(1a)	4.0 (4i)
S3260 M4	3.1(2b)	3.1(3a)	4.0(1a)	4.0 (4i)
S3260 M5	3.2(3a)	3.2(3a)	4.0(1a)	4.0 (4i)

サーバ	最小ソフトウェアバージョン UCS 6200 シリーズ FI	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6454	推奨されるソフトウェアバージョン UCS 6200 シリーズ FI UCS 6332、6332-16UP FI UCS 6454
C125 M5	NA	4.0(1a)	4.0(1a)	4.0 (4i) (UCS 6332、UCS 6332-16UP FI、および UCS 6454 のみ)
C480 M5 ML	4.0(2a)	4.0(2a)	4.0(2a)	4.0 (4i)

アダプタ

表 14: アダプタの最小ソフトウェアバージョン

アダプタ	最小ソフトウェアバージョン UCS 6200 シリーズ FI	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6454	推奨されるソフトウェアバージョン UCS 6200 シリーズ FI UCS 6332、6332-16UP FI UCS 6454
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304 UCS-IOM-2304V2	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*
				* UCS-IOM-2408 は、UCS 6454 FI を持つ M4 および M5 でサポートされています。	
191 UCSC-P-M4D25GF (Mellanox MCX4121A-ACAT デュアルポート 10/25G SFP28 NIC)	4.0 (4i)	4.0 (4i)	4.0 (4i)	4.0 (4i)	4.0 (4i)
UCSC QS100GF (QLogic QL45611HLCU 100GbE)	4.0 (4i)	4.0 (4i)	4.0 (4i)	4.0 (4i)	4.0 (4i)
UCSC C100-04 (UCS VIC 1495)	NA	4.0(2a)	4.0(2a)	NA	4.0 (4i)(UCS 6332、6332-16UP FI の場合のみ)
UCSCMLOMCI004 (UCS VIC 1497)	NA	4.0(2a)	4.0(2a)	NA	4.0 (4i)(UCS 6332、6332-16UP FI の場合のみ)
UCSBMLOM40G04 (UCS VIC 1440)	4.0(1a)	4.0(1a)	4.0(1a)	4.0(1a)	4.0 (4i)

アダプタ	最小ソフトウェアバージョン UCS 6200 シリーズ FI	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6454	推奨されるソフトウェアバージョン UCS 6200 シリーズ FI UCS 6332、6332-16UP FI UCS 6454
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304 UCS-IOM-2304V2	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*
					* UCS-IOM-2408 は、UCS 6454 FI を持つ M4 および M5 でサポートされています。
UCSB-VIC-M844P (UCS VIC 1480)	4.0(1a)	4.0(1a)	4.0(1a)	4.0(1a)	4.0 (4i)
UCSC-PCIE-C25Q04 (UCS VIC 1455)	4.0(1a)	4.0(1a)	4.0(1a)	4.0(1a)	4.0 (4i)
204 UCSGMLOMC25Q04 (UCS VIC 1457)	4.0(1a)	4.0(1a)	4.0(1a)	4.0(1a)	4.0 (4i)
UCSC-PCIE-BD16GF (Emulex LPe31002 デュ アルポート 16G FC HBA)	3.2(3a)	3.2(3a)	3.2(3a)	4.0(1a)	4.0 (4i)
UCSC-PCIE-ID40GF (Intel XL710 ア ダプタ)	3.2(3a)	3.2(3a)	3.2(3a)	4.0(1a)	4.0 (4i)
UCSC-PCIE-IQ10GF (Intel X710-DA4 アダプタ)	3.2(3a)	3.2(3a)	3.2(3a)	4.0(1a)	4.0 (4i)
UCSC-PCIE-ID10GF (Intel X710-DA2 アダプタ)	3.2(3a)	3.2(3a)	3.2(3a)	4.0(1a)	4.0 (4i)

アダプタ	最小ソフトウェアバージョン UCS 6200 シリーズ FI	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6454	推奨されるソフトウェアバージョン UCS 6200 シリーズ FI UCS 6332、6332-16UP FI UCS 6454
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304 UCS-IOM-2304V2	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*
					* UCS-IOM-2408 は、UCS 6454 FI を持つ M4 および M5 でサポートされています。
XXV710-DA2 (Intel XXV710-DA2 アダプタ)	3.2(3a)	3.2(3a)	3.2(3a)	4.0(1a)	4.0 (4i)
UCSC-PCIE-ID10GC (Intel X550-T2 アダプタ)	3.2(3a)	3.2(3a)	3.2(3a)	4.0(1a)	4.0 (4i)
N2XX-AIPCI01 (Intel X520 デュアルポートアダプタ)	3.2(3a)	3.2(3a)	3.2(3a)	4.0(1a)	4.0 (4i)
UCSC-PCIE-ID25GF (Intel X710 25Gb デュアルポート BaseT)	3.2(3a)	3.2(3a)	3.2(3a)	4.0(1a)	4.0 (4i)
UCSC-PCIE-QD25GF (QLogic QL41212H 25GbE)	3.2(2b)	3.2(2b)	3.2(2b)	4.0(1a)	4.0 (4i)
UCSC-PCIE-QD40GF (QLogic QL45212H 40GbE)	3.2(2b)	3.2(2b)	3.2(2b)	4.0(1a)	4.0 (4i)

アダプタ	最小ソフトウェアバージョン UCS 6200 シリーズ FI	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6454	推奨されるソフトウェアバージョン UCS 6200 シリーズ FI UCS 6332、6332-16UP FI UCS 6454
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304 UCS-IOM-2304V2	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*
					*UCS-IOM-2408 は、 UCS 6454 FI を持つ M4 および M5 でサポートされています。
UCSC-PCIE-IQ10GC (Intel X710-T4)	3.2(2b)	3.2(2b)	3.2(2b)	4.0(1a)	4.0 (4i)
UCSC QD16GF (QLogic QLE2692-CSC)	3.2(1d)	3.2(1d)	3.2(1d)	4.0(1a)	4.0 (4i)
UCSC-PCIE-C40Q03 (UCS VIC 1385) UCS-MLOM-C40Q03 (UCS VIC 1387)	2.2 (8a)	3.1(3a)	3.1(3a)	4.0(1a)	4.0 (4i)
UCS-VIC-M82-8P (UCS VIC 1280) UCSB-MLOM-40G-01 (UCS VIC 1240) UCSB-MLOM-PT-01 (Cisco ポート エクスパンダ カード)	2.2 (8a)	3.1(3a)	3.1(3a)	4.0(1a)	4.0 (4i)
UCSB-MLOM-40G-03 (UCS VIC 1340) UCSB-VIC-M83-8P (UCS VIC 1380) UCS-MLOM-CSC-02 (UCS VIC 1227)	2.2 (8a)	3.1(3a)	3.1(3a)	4.0(1a)	4.0 (4i)

アダプタ	最小ソフトウェアバージョン UCS 6200 シリーズ FI	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6454	推奨されるソフトウェアバージョン UCS 6200 シリーズ FI UCS 6332、6332-16UP FI UCS 6454
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304 UCS-IOM-2304V2	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*
				* UCS-IOM-2408 は、UCS 6454 FI を持つ M4 および M5 でサポートされています。	
UCSC-PCIE-CSC-02 (UCS VIC 1225)	2.2 (8a)	3.1(3a)	3.1(3a)	4.0(1a)	4.0 (4i)
UCSCF-FIO-1000MP (Cisco UCS Fusion ioMemory – PX600、1.0 TB) UCSCF-FIO-1300MP (Cisco UCS Fusion ioMemory – PX600、1.3TB) UCSCF-FIO-2600MP (Cisco UCS Fusion ioMemory – PX600、2.6TB) UCSCF-FIO-5200MP (Cisco UCS Fusion ioMemory – PX600、5.2TB)	2.2 (8a)	3.1(3a)	3.1(3a)	4.0(1a)	4.0 (4i)

アダプタ	最小ソフトウェアバージョン UCS 6200 シリーズ FI	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6454	推奨されるソフトウェアバージョン UCS 6200 シリーズ FI UCS 6332、6332-16UP FI UCS 6454
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304 UCS-IOM-2304V2	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*
				*UCS-IOM-2408 は、UCS 6454 FI を持つ M4 および M5 でサポートされています。	
UCSB-FIO-1600MS (Cisco UCS Fusion ioMemory Mezzanine SX300、1.6TB) UCSB-FIO-1300MS (Cisco UCS Fusion ioMemory Mezzanine PX600、1.3TB)	2.2 (8a)	3.1(3a)	3.1(3a)	4.0(1a)	4.0 (4i)
UCSC-INVADER-3108 UCSC-NYIRO-200GB (Cisco Nytro MegaRAID 200GB コントローラ)	2.2 (8a)	3.1(3a)	3.1(3a)	4.0(1a)	4.0 (4i)

アダプタ	最小ソフトウェアバージョン UCS 6200 シリーズ FI	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6454	推奨されるソフトウェアバージョン UCS 6200 シリーズ FI UCS 6332、6332-16UP FI UCS 6454
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304 UCS-IOM-2304V2	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*
				* UCS-IOM-2408 は、 UCS 6454 FI を持つ M4 および M5 でサポートされています。	
	2.2 (8a)	3.1(3a)	3.1(3a)	4.0(1a)	4.0 (4i)

アダプタ	最小ソフトウェアバージョン UCS 6200 シリーズ FI	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6454	推奨されるソフトウェアバージョン UCS 6200 シリーズ FI UCS 6332、6332-16UP FI UCS 6454
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304 UCS-IOM-2304V2	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408 *
					* UCS-IOM-2408 は、UCS 6454 FI を持つ M4 および M5 でサポートされています。
UCSCML0MCI0T02 (UCS VIC 1227T)					
UCSC-PCIE-CI0T-02 (UCS VIC 1225T)					
UCSC-F-FIO-785M (C シリーズ サーバ用 Cisco UCS 785 GB MLC Fusion ioDrive2)					
UCSC-F-FIO-365M (C シリーズ サーバ用 Cisco UCS 365 GB MLC Fusion ioDrive2)					
UCSC-F-FIO-1205M (C シリーズ サーバ用 Cisco UCS 1205GB MLC Fusion ioDrive2)					
UCSC-F-FIO-3000M (C シリーズ					

アダプタ	最小ソフトウェアバージョン UCS 6200 シリーズ FI	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6454	推奨されるソフトウェアバージョン UCS 6200 シリーズ FI UCS 6332、6332-16UP FI UCS 6454
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304 UCS-IOM-2304V2	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*
					* UCS-IOM-2408 は、UCS 6454 FI を持つ M4 および M5 でサポートされています。
サーバ用 Cisco UCS 3.0TB MLC Fusion ioDrive2) UCSCF-FIO-1000PS (ラック M4 用 UCS 1000 GB Fusion ioMemory3 PX Performance ライン) UCSCF-FIO-1300PS (UCSCF-FIO-1300PS) UCSCF-FIO-2600PS (ラック M4 用 UCS 2600 GB Fusion ioMemory3 PX Performance ライン) UCSCF-FIO-5200PS (ラック M4 用 UCS 5200GB Fusion ioMemory3 PX Performance ライン)					

アダプタ	最小ソフトウェアバージョン UCS 6200 シリーズ FI	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6454	推奨されるソフトウェアバージョン UCS 6200 シリーズ FI UCS 6332、6332-16UP FI UCS 6454
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304 UCS-IOM-2304V2	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*
					* UCS-IOM-2408 は、UCS 6454 FI を持つ M4 および M5 でサポートされています。
5 UCSC-F-FIO-6400SS (C シリーズ用 UCS 6400GB Fusion ioMemory3 SX Scale ライン) UCSC-F-FIO-3200SS (C シリーズ用 UCS 3200GB Fusion ioMemory3 SX Scale ライン)					
UCSC PCIE E14102B (Emulex Oce14102b-f-F)	2.2 (8a)	3.1(3a)	3.1(3a)	4.0(1a)	4.0 (4i)

アダプタ	最小ソフトウェアバージョン UCS 6200 シリーズ FI	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6454	推奨されるソフトウェアバージョン UCS 6200 シリーズ FI UCS 6332、6332-16UP FI UCS 6454
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304 UCS-IOM-2304V2	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*
				* UCS-IOM-2408 は、 UCS 6454 FI を持つ M4 および M5 でサポートされています。	
UCSC-PCIE-IQ10GF (Intel X710-DA4 アダプタ) UCSC-PCIE-ID10GF (Intel X710-DA2 アダプタ) UCSC-PCIE-ID40GF (Intel XL710 アダプタ)	—	—	3.1(3a)	4.0(1a)	4.0 (4i)

アダプタ	最小ソフトウェアバージョン UCS 6200 シリーズ FI	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6454	推奨されるソフトウェアバージョン UCS 6200 シリーズ FI UCS 6332、6332-16UP FI UCS 6454
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304 UCS-IOM-2304V2	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*
					* UCS-IOM-2408 は、UCS 6454 FI を持つ M4 および M5 でサポートされています。
	—	3.1(3a)	3.1(3a)	4.0(1a)	4.0 (4i)

アダプタ	最小ソフトウェアバージョン UCS 6200 シリーズ FI	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6454	推奨されるソフトウェアバージョン UCS 6200 シリーズ FI UCS 6332、6332-16UP FI UCS 6454
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304 UCS-IOM-2304V2	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*
					* UCS-IOM-2408 は、UCS 6454 FI を持つ M4 および M5 でサポートされています。
UCSC-F-I80010 (Intel P3700 HHHL 800GB NVMe PCIe SSD)					
UCSC-F-I12003 (Intel P3600 HHHL 1200GB NVMe PCIe SSD)					
UCSC-F-I160010 (Intel P3700 HHHL 1600GB NVMe PCIe SSD)					
UCSC-F-I20003 (Intel P3600 HHHL 2000GB NVMe PCIe SSD)					
UCS-PCI25-40010 (Intel P3700 400GB NVMe PCIe SSD)					
UCS-PCI25-8003 (Intel P3600 800GB NVMe					

アダプタ	最小ソフトウェアバージョン UCS 6200 シリーズ FI	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6454	推奨されるソフトウェアバージョン UCS 6200 シリーズ FI UCS 6332、6332-16UP FI UCS 6454
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304 UCS-IOM-2304V2	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*
					* UCS-IOM-2408 は、UCS 6454 FI を持つ M4 および M5 でサポートされています。
PCIe SSD) UCS-PCI25-80010 (Intel P3700 800GB NVMe PCIe SSD) UCS-PCI25-16003 (Intel P3600 1600GB NVMe PCIe SSD) UCSC-F-H19001 (UCS Rack PCIe/NVMe Storage 1900GB HGST SN150) UCSC-F-H38001 (UCS Rack PCIe/NVMe Storage 3800GB HGST SN150) UCS-PCI25-38001 (UCS PCIe/NVMe2.5"SFF Storage 3800GB HGST SN100)					

アダプタ	最小ソフトウェアバージョン UCS 6200 シリーズ FI	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6454	推奨されるソフトウェアバージョン UCS 6200 シリーズ FI UCS 6332、6332-16UP FI UCS 6454
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304 UCS-IOM-2304V2	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*
				* UCS-IOM-2408 は、UCS 6454 FI を持つ M4 および M5 でサポートされています。	
UCSC QD32GF (Qlogic QLE2742) NXXACRDLAQCI5 (Qlogic QLE2562) UCSC Q2672 (Qlogic QLE2672-CSC) UCSC BD32GF (Emulex LPe32002) UCSC BS32GF (Emulex LPe32001) NXXACRDLAFCI5 (Emulex LPe12002)	—	3.1(3a)	3.1(3a)	4.0(1a)	4.0 (4i)
UCSC-PCIE-E16002 (Emulex LPe16002-M6 16G FC rack HBA)	—	3.2(1d)	3.2(1d)	4.0(1a)	4.0 (4i)

アダプタ	最小ソフトウェアバージョン UCS 6200 シリーズ FI	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6332、6332-16UP	最小ソフトウェアバージョン UCS 6454	推奨されるソフトウェアバージョン UCS 6200 シリーズ FI UCS 6332、6332-16UP FI UCS 6454
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304 UCS-IOM-2304V2	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*
					* UCS-IOM-2408 は、UCS 6454 FI を持つ M4 および M5 でサポートされています。
UCSC-PCIE-IDI0GC (Intel X550 デュアルポート 10GBase-T NIC)	3.1(2b)	3.1(3a)	3.1(3a)	4.0(1a)	4.0 (4i)

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、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 \(31 ページ\)](#) 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。

表 15: UCS 6454 ファブリック インターコネク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
ファブリック インターコネク	UCS 6454

タイプ	詳細
ファブリック エクステンダ	Cisco UCS 2204XP Cisco UCS 2208XP Cisco Nexus 2232PP Cisco Nexus 2232TM-E Cisco UCS 2408
電源モジュール	N9K-PUV-1200W UCSB-PSU-2500HVDC UCSB-PSU-2500DC48 UCSC-PSU-930WDC UCSC-UCSC-PSU2V2-930DC-930WDC UCSC-UCSC-PSUV2-1050DC-1050DC UCSC-PSU1-770W UCSC-PSU1-1050W UCSC-PSU2-1400 UCSC-PSU2V2-1400W UCSC-UCSC-PSU2V2-930DC-650 W UCSC-UCSC-PSU2V2-930DC-1200W UCSB-PSU-2500ACPL UCSB-PSU-2500ACDV N20-N20-PAC5-2500W-2500W

表 16: UCS 6332、UCS 6332-16UP ファブリック インターコネクでサポートされるハードウェア

タイプ	詳細
シャーシ	N20 – N20-C6508 UCSB-5108-DC UCSB-5108-AC2 UCSB-5108-DC2 UCSB-5108-HVDC
ファブリック インターコネク	UCS 6332UP UCS 6332-16UP

タイプ	詳細
ファブリック エクステンダ	Cisco UCS 2208XP Cisco UCS 2204XP Cisco Nexus 2232PP Cisco Nexus 2232TM-E Cisco UCS 2304 Cisco UCS 2304V2 Cisco Nexus 2348UPQ
電源モジュール	UCSB-PSU-2500HVDC UCSB-PSU-2500DC48 UCSC-PSU-930WDC UCSC-UCSC-PSU2V2-930DC-930WDC UCSC-UCSC-PSUV2-1050DC-1050DC UCSC-PSU1-770W UCSC-PSU1-1050W UCSC-PSU2-1400 UCSC-PSU2V2-1400W UCSC-UCSC-PSU2V2-930DC-650 W UCSC-UCSC-PSU2V2-930DC-1200W UCSB-PSU-2500ACPL UCSB-PSU-2500ACDV N20-N20-PAC5-2500W-2500W N9K-PUV-1200W



(注) 40G バックプレーン設定は、22xx IOM には適用されません。

表 17: UCS 6200 ファブリック インターコネクでサポートされるハードウェア

タイプ	詳細
シャーシ	N20 – N20-C6508 UCSB-5108-DC UCSB-5108-AC2 UCSB-5108-DC2 UCSB-5108-HVDC

タイプ	詳細
ファブリック インターコネク	UCS 6248UP UCS 6296UP
ファブリック エクステンダ	UCS 2208XP UCS 2204XP Cisco Nexus 2232PP Cisco Nexus 2232TM-E
拡張モジュール	UCS-FI-E16UP
電源モジュール	UCSB-PSU-2500HVDC UCSB-PSU-25004DC48 UCSC-PSU-930WDC UCSC-UCSC-PSU2V2-930DC-930WDC UCSC-UCSC-PSUV2-1050DC-1050DC UCSC-PSU1-770W UCSC-PSU1-1050W UCSC-PSU2-1400 UCSC-PSU2V2-1400W UCSC-UCSC-PSU2V2-930DC-650 W UCSC-UCSC-PSU2V2-930DC-1200W UCSB-PSU-2500ACPL UCSB-PSU-2500ACDV N20-N20-PAC5-2500W-2500W

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 18: サポートされているトランシーバ モジュールおよび Gb コネクタ モジュール用ケーブル

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 6454 ファブリック インターコネクの FC	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 6454 ファブリック インターコネクの 100-Gb	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

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 6454 ファブリック インターコネクの 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

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 6300 シリーズ ファブリック インターコネクの 40-Gb	SFP-10G-SRに接続された外部 x10G スプリッタを使用した 4x10G モードの QSFP-40G-SR4 QSFP-40G-CSR4 QSFP-40G-LR4 QSFP-40G-LR4-S QSFP-40G-SR-BD QSFP-40G-SR4 QSFP-40G-SR4-S FET-40G QSFP-4SFP10G-CU1M QSFP-4SFP10G-CU3M QSFP-4SFP10G-CU5M QSFP-4X10G-AC7M QSFP-4X10G-AC10M QSFP-4X10G-AOC1M QSFP-4X10G-AOC2M QSFP-4X10G-AOC3M QSFP-4X10G-AOC5M QSFP-4X10G-AOC7M QSFP-4X10G-AOC10M QSFP-H40G-ACU7M QSFP-H40G-ACU10M QSFP-H40G-AOC1M QSFP-H40G-AOC2M QSFP-H40G-AOC3M QSFP-H40G-AOC5M QSFP-H40G-AOC7M QSFP-H40G-AOC10M QSFP-H40G-AOC15M QSFP-H40G-CU1M QSFP-H40G-CU3M QSFP-H40G-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 6454 ファブリック インターコネクの 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
UCS 6454 および UCS 6332UP ファブリック インターコネクの場合は 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 6454 ファブリック インターコネクの 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

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 6300 および 6200 シリーズ ファブリック インターコネクの 10-Gb	SFP-10G-SR SFP-10G-SR-S SFP-10G-LR SFP-10G-LR-S SFP-H10GB-CU1M SFP-H10GB-CU2M SFP-H10GB-CU3M SFP-H10GB-CU5M SFP-H10GB-ACU7M SFP-H10GB-ACU10M FET-10G ¹ SFP-10G-AOC1M SFP-10G-AOC2M SFP-10G-AOC3M SFP-10G-AOC5M SFP-10G-AOC7M SFP-10G-AOC10M
UCS 6454 および UCS 6332UP ファブリック インターコネク用の 8-Gb FC	DS-SFP-FC8G-SW DS-SFP-FC8G-LW
UCS 6300 および 6200 シリーズ ファブリック インターコネクの 4-Gb FC	DS-SFP-FC4G-SW DS-SFP-FC4G-LW
UCS 6454 ファブリック インターコネクの 1-Gb	GLC-TE GLC-SX-MMD SFP-GE-T
UCS 6300 および 6200 シリーズ ファブリック インターコネクの 1-Gb	GLC-TE GLC-SX-MM GLC-LH-SM

¹ SFP-10G-AOC ケーブルは、Cisco 1455 および 1457 VIC カードでのみサポートされています。



- (注) 光ファイバの最大敷設長は、300メートルに制限されています。これは、802.3X/802.1Qbb Priority PAUSE が使用されているためです。SFP-10G-LR はファブリック インターコネクトと FEX の間でサポートされますが、それでも 300 m の制限が適用されます。

Cisco UCS ミニおよびコンポーネント

UCS ミニでサポートされるシャーシ

表 19: UCS ミニシャーシの最小ソフトウェアバージョン

シャーシ	最小ソフトウェアバージョン	推奨されるソフトウェアバージョン
UCSB-5108-AC2	3.0(1e)	4.0 (4i)
UCSB-5108-DC2	3.0 (2c)	4.0 (4i)

UCS ミニでサポートされるブレード およびラック サーバ

表 20: UCS ミニ上のブレードおよびラック サーバの最小ホスト ファームウェアバージョン

サーバ	最小ソフトウェアバージョン	推奨されるソフトウェアバージョン
B200 M5	3.2(1d)	4.0 (4i)
B200 M3	3.1(3a)	4.0 (4i)
UCS C220 M3	3.1(3a)	4.0 (4i)
B260 M4	3.1(3a)	4.0 (4i)
B420 M3	3.1(3a)	4.0 (4i)
B420 M4	3.1(3a)	4.0 (4i)
B460 M4	3.1(3a)	4.0 (4i)
B480 M5	3.1(3a)	4.0 (4i)
B22 M3	3.1(3a)	4.0 (4i)
C220 M3	3.1(3a)	4.0 (4i)
C240 M3	3.1(3a)	4.0 (4i)
C220 M4	3.1(3a)	4.0 (4i)
C240 M4	3.1(3a)	4.0 (4i)

サーバ	最小ソフトウェアバージョン	推奨されるソフトウェアバージョン
C460 M4	3.1(3a)	4.0 (4i)
C220 M5	3.2(1d)	4.0 (4i)
C240 M5	3.2(1d)	4.0 (4i)
C480 M5	3.2(2b)	4.0 (4i)

UCS ミニ対応アダプタ

アダプタ	最小ソフトウェアバージョン	推奨されるソフトウェアバージョン
UCSB-MLOM-40G-04 (UCS VIC 1440) UCSB-VIC-M84-4P (UCS VIC 1480)	4.0(2a)	4.0 (4i)
UCSC-PCIE-IQ10GC (Intel X710-T4) UCSC-PCIE-QD25GF (QLogic QL41212H 25GbE) UCSC-PCIE-QD40GF (QLogic QL45212H 40GbE)	3.2(2b)	4.0 (4i)
UCSC-PCIE-C40Q-03 (UCS VIC 1385) UCSC-MLOM-C40Q-03 (UCS VIC 1387)	3.1(3a)	4.0 (4i)
UCS-VIC-M82-8P (UCS VIC 1280) UCSB-MLOM-40G-01 (UCS VIC 1240) UCSB-MLOM-PT-01 (Cisco ポート エクスパンダ カード)	3.1(3a)	4.0 (4i)
UCSB-MLOM-40G-03 (UCS VIC 1340) UCSB-VIC-M83-8P (UCS VIC 1380) UCSC-MLOM-CSC-02 (UCS VIC 1227)	3.1(3a)	4.0 (4i)

アダプタ	最小ソフトウェアバージョン	推奨されるソフトウェアバージョン
UCSC-PCIE-CSC-02 (UCS VIC 1225)	3.1(3a)	4.0 (4i)

UCS ミニでサポートされるファブリック インターコネク

ファブリック インターコネク	最小ソフトウェアバージョン	推奨されるソフトウェアバージョン
Cisco UCS 6324	3.1(3a)	4.0 (4i)

セカンダリ シャーシでサポートされる UCS ミニ ファブリック エクステンダ

ファブリック エクステンダ	最小ソフトウェアバージョン	推奨されるソフトウェアバージョン
UCS 2204 XP	3.1(3a)	4.0 (4i)
UCS 2208 XP	3.1(3a)	4.0 (4i)

UCS ミニでサポートされる電源装置

電源モジュール	最小ソフトウェアバージョン	推奨されるソフトウェアバージョン
UCSB-PSU-2500ACDV UCSB-PSU-2500DC48 UCSC-PSU-930WDC UCSC-UCSC-PSU2V2-930DC-930WDC UCSC-UCSC-PSUV2-1050DC-1050DC UCSC-PSU1-770W UCSC-PSU2-1400 UCSC-PSU2V2-1400W UCSC-UCSC-PSU2V2-930DC-650W UCSC-UCSC-PSU2V2-930DC-1200W	3.1(3a)	4.0 (4i)

UCS ミニでサポートされる Gb コネクタ モジュール

Gb ポート速度接続には、現在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。次に、Gb コネクタ モジュールと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 インターコネクタ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 インターコネクタ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>

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
40GB	SFP-10G-SR に接続された外部 x10G スプリッタを使用した 4x10G モードの QSFP-40G-SR4 QSFP-4SFP10G-CU1M QSFP-4SFP10G-CU3M QSFP-4SFP10G-CU5M QSFP-4X10G-AC7M QSFP-4X10G-AC10M QSFP-4X10G-AOC1M QSFP-4X10G-AOC2M QSFP-4X10G-AOC3M QSFP-4X10G-AOC5M QSFP-4X10G-AOC7M QSFP-4X10G-AOC10M

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
10 Gb	SFP-10G-LR SFP-10G-LR-S SFP-10G-LR-X SFP-10G-SR SFP-10G-SR-S SFP-10G-SR-X 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
8 Gb	DS-SFP-FC8G-SW DS-SFP-FC8G-LW
4 Gb	DS-SFP-FC4G-SW DS-SFP-FC4G-LW
1 Gb	GLC-TE GLC-LH-SM GLC-SX-MM

アップグレードとダウングレードのガイドライン

- Cisco UCS 6454 ファブリック インターコネクトを搭載したシステムでは、Cisco UCS Manager リリース 4.0 からダウングレードできません。

詳細なアップグレードパスについては、『Cisco UCS Managerファームウェア管理ガイド、リリース4.0』の「[Cisco UCS Manager リリース4.0 へのファームウェア アップグレード](#)」を参照してください。

- ITE-ON 1050W PSU が搭載されているシステムをリリース 4.0(2) Cisco UCS Manager よりも前のリリースにダウングレードしないでください。Cisco UCS Manager リリース 4.0(2) からダウングレードされたときに、LITE-ON 1050W PSU を搭載した UCS C240 M5 サーバのボードコントローラのアクティブ化は、検出プロセス中に失敗する可能性があります。
- Cisco UCS 6454 ファブリック インターコネクタを搭載したシステムでは、このモードが 4.0(2) よりも前のバージョンではサポートされていないため、ファブリック インターコネクタでイーサネットまたは FC スイッチモードが有効になっている場合、Cisco UCS Manager リリース 4.0(2) からダウングレードできません。
また、ネットワーク制御ポリシーでポートセキュリティが有効になっている場合、4.0(2) よりも前のバージョンではサポートされていないため、Cisco UCS Manager リリース 4.0(2) からのダウングレード中は無効になります。
- NVMe の Intel Volume Management Device (VMD) を使用してシステムをアップグレードまたはダウングレードする場合、OS のインストール後に、BIOS で VMD が有効または無効になっていると、システムは起動に失敗します。OS のインストール後に BIOS 設定を変更しないでください。
- ファブリック インターコネクタまたはサーバ (B シリーズおよび C シリーズ) を Cisco UCS Manager リリース 4.0 (4c) から 4.0 (4d) にアップグレードする場合、FSM は検証をスキップし、ファームウェアのアップグレードはリポートせずに完了します。

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
4.0 (4i)	ucs-catalog.4.0.4h.T.bin	<p>UCS B200 M5、C220 M5、および C240 M5 サーバの CPU :</p> <ul style="list-style-type: none"> • UCS-CPU-I6238R • UCS-CPU-I6240R • UCS-CPU-I6242R • UCS-CPU-I6246R • UCS-CPU-I6248R • UCS-CPU-I6226R • UCS-CPU-I6258R • UCS-CPU-I5220R <p>UCS B200 M5、C220 M5、C240 M5、UCS S3260 M5 サーバの CPU :</p> <ul style="list-style-type: none"> • UCS-CPU-I6230R • UCS-CPU-I5218R • UCS-CPU-I4214R • UCS-CPU-I4215R <p>UCS B200 M5、UCS B480 M5、C220 M5、C240 M5、C480 M5 サーバの CPU:</p> <ul style="list-style-type: none"> • UCS-CPU-I8253

UCS リリース	カタログ ファイル名	このリリースの追加 PID
4.0 (4h)	ucs-catalog.4.0.4h.T.bin	<p>UCS B200 M5、C220 M5、および C240 M5 サーバの CPU :</p> <ul style="list-style-type: none"> • UCS-CPU-I6238R • UCS-CPU-I6240R • UCS-CPU-I6242R • UCS-CPU-I6246R • UCS-CPU-I6248R • UCS-CPU-I6226R • UCS-CPU-I6258R • UCS-CPU-I5220R <p>UCS B200 M5、C220 M5、C240 M5、UCS S3260 M5 サーバの CPU :</p> <ul style="list-style-type: none"> • UCS-CPU-I6230R • UCS-CPU-I5218R • UCS-CPU-I4214R • UCS-CPU-I4215R <p>UCS B200 M5、UCS B480 M5、C220 M5、C240 M5、C480 M5 サーバの CPU:</p> <ul style="list-style-type: none"> • UCS-CPU-I8253
4.0 (4g)	ucs-catalog (4.0.4)	<p>UCS B200 M5、C220 M5、および C240 M5 サーバの CPU :</p> <ul style="list-style-type: none"> • UCS-CPU-I4214R • UCS-CPU-I4210R • UCS-CPU-I3206R
4.0 (4f)	ucs-catalog 4.0.4. .bin	—

UCS リリース	カタログ ファイル名	このリリースの追加 PID
4.0 (4e)	ucs-catalog 4.0.4 の e.164	<p>UCS B200 M5、B480 M5、C220 M5、C240 M5、および C480 M5 サーバの CPU:</p> <ul style="list-style-type: none"> • UCS-CPU-I6238 • UCS-CPU-I6238M • UCS-CPU-I6238L • UCS-CPU-I5220S • UCS-CPU-I6226 • UCS-CPU-I6234 • UCS-CPU-I6240L • UCS-CPU-I6240M • UCS-CPU-I6246 • UCS-CPU-I5218B <p>UCS C220 M5、C240 M5、B200 M5、B480 M5、C480 M5、および S3260 M5 サーバの CPU:</p> <ul style="list-style-type: none"> • UCS-CPU-I6222V • UCS-CPU-I6262V <p>UCS C220 M5、C240 M5、および B200 M5 サーバの CPU:</p> <ul style="list-style-type: none"> • UCS-CPU-I5218N <p>UCS C220 M5、C240 M5、B480 M5、および B200 M5 サーバの CPU:</p> <ul style="list-style-type: none"> • UCS-CPU-I6230N <p>UCS C220 M5、C240 M5、C480 M5、および B200 M5 サーバの CPU:</p> <ul style="list-style-type: none"> • UCS-CPU-I6252N <p>ドライブ:</p> <ul style="list-style-type: none"> • UCS-SD76TSB61X-EV • UCS-SD76T61X-EV <p>ファブリック エクステンダ:</p> <ul style="list-style-type: none"> • UCS-IOM-2408

UCS リリース	カタログ ファイル名	このリリースの追加 PID
4.0 (4d)	ucs-catalog 4.0.4 d. .bin	ドライブ: <ul style="list-style-type: none"> • UCS-SD480G2HMK9 • UCS-SD480G2HBNK9 • UCS-SD960G2HTNK9 • UCS-SD960G2HBNK9 • UCS-SD38T2HTNK9 • UCS-SD38T2HBNK9 • S3260-2SD38K9
4.0 (4c)	ucs-catalog 4.0.4 の e.164	<ul style="list-style-type: none"> • UCSC-NVME2H-I1000 • UCSB-NVME2H-I1000 • UCSC-NVME2H-I2TBV • UCSB-NVME2H-I2TBV • UCSC-NVME2H-I4000 • UCSB-NVME2H-I4000 • UCSC-NVMEHW-I8000 • UCSB-NVMEHW-I8000 • UCSC-NVME2H-I1600 • UCSB-NVME2H-I1600
4.0(4b)	ucs-catalog 4.0.4 b. .bin	—

UCS リリース	カタログ ファイル名	このリリースの追加 PID
4.0(4a)	ucs-catalog (4.0.4)	

UCS リリース	カタログ ファイル名	このリリースの追加 PID
		UCS B200 M5、C220 M5、C240 M5 サーバの CPU: <ul style="list-style-type: none"> • UCS-CPU-I3204 • UCS-CPU-I4208 • UCS-CPU-I4210 • UCS-CPU-I4214 • UCS-CPU-I4215 • UCS-CPU-I4216 • UCS-CPU-I5215 • UCS-CPU-I5217 • UCS-CPU-I5218 • UCS-CPU-I5220 • UCS-CPU-I5222 • UCS-CPU-I6230 • UCS-CPU-I6240 • UCS-CPU-I6242 • UCS-CPU-I6244 • UCS-CPU-I6248 • UCS-CPU-I6254 • UCS-CPU-I6252 • UCS-CPU-I8260 • UCS-CPU-I8268 • UCS-CPU-I8270 • UCS-CPU-I8276 • UCS-CPU-I8280 • UCS-CPU-I5215M • UCS-CPU-I8260M • UCS-CPU-I8276M • UCS-CPU-I8280M • UCS-CPU-I5215L • UCS-CPU-I8260L

UCS リリース	カタログ ファイル名	このリリースの追加 PID
		<ul style="list-style-type: none">• UCS-CPU-I8276L• UCS-CPU-I8280L• UCS-CPU-I4214Y• UCS-CPU-I6240Y• UCS-CPU-I8260Y UCS B480 M5 および C480 M5 の CPU:

UCS リリース	カタログ ファイル名	このリリースの追加 PID
		<ul style="list-style-type: none"> • UCS-CPU-I5215 • UCS-CPU-I5217 • UCS-CPU-I5218 • UCS-CPU-I5220 • UCS-CPU-I5222 • UCS-CPU-I6230 • UCS-CPU-I6240 • UCS-CPU-I6242 • UCS-CPU-I6244 • UCS-CPU-I6248 • UCS-CPU-I6254 • UCS-CPU-I6252 • UCS-CPU-I8260 • UCS-CPU-I8268 • UCS-CPU-I8270 • UCS-CPU-I8276 • UCS-CPU-I8280 • UCS-CPU-I5215M • UCS-CPU-I8260M • UCS-CPU-I8276M • UCS-CPU-I8280M • UCS-CPU-I5215L • UCS-CPU-I8260L • UCS-CPU-I8276L • UCS-CPU-I8280L • UCS-CPU-I6240Y • UCS-CPU-I8260Y <p>UCS S3260 M5 の CPU:</p>

UCS リリース	カタログ ファイル名	このリリースの追加 PID
		<ul style="list-style-type: none"> • UCS-CPU-I4214 • UCS-CPU-I5218 • UCS-CPU-I5220 • UCS-CPU-I6240 <p>メモリ :</p> <ul style="list-style-type: none"> • UCS-MR-X16G1RT-H • UCS-MR-X32G2RT-H • UCS-MR-X64G2RT-H • UCS-ML-X64G4RT-H • UCS-ML-128G4RT-H <p>Intel® Optane™ DC 永続メモリ</p> <ul style="list-style-type: none"> • UCS-MP-128GS-A0 • UCS-MP-256 G-A0 • UCS-MP-512 G-A0 <p>ファブリック エクステンダ:</p> <ul style="list-style-type: none"> • UCS-IOM-2304V2 <p>GPU:</p> <ul style="list-style-type: none"> • UCS C240 M5、C220 M5、C480 M5 での UCSC-GPU-16 • UCSC-GPU-V340 <p>ネットワーク インターフェイス カード:</p> <ul style="list-style-type: none"> • UCSC-P-M4D25GF • UCSC-PCIE-QS100GF <p>ハードウェア RAID コントローラ:</p> <ul style="list-style-type: none"> • UCS-M2-HWRAID
4.0(2e)	ucs-catalog 4.0.2 の e.164	—
4.0(2d)	ucs-catalog 4.0.2 d. .bin	—
4.0(2b)	ucs-catalog (4.0.2)	—

UCS リリース	カタログ ファイル名	このリリースの追加 PID
4.0(2a)	ucs-catalog (4.0.2)	

UCS リリース	カタログ ファイル名	このリリースの追加 PID
		<p>Cisco UCS ラックマウント サーバ</p> <ul style="list-style-type: none">• UCSC-C480-M5ML <p>UCSC-C480-M5ML の CPU:</p> <ul style="list-style-type: none">• UCS-CPU-8180• UCS-CPU-8176• UCS-CPU-8170• UCS-CPU-8164• UCS-CPU-8160• UCS-CPU-8153• UCS-CPU-6152• UCS-CPU-6148• UCS-CPU-6138• UCS-CPU-6140• UCS-CPU-6130• UCS-CPU-8168• UCS-CPU-8158• UCS-CPU-8156• UCS-CPU-6154• UCS-CPU-6150• UCS-CPU-6142• UCS-CPU-6132• UCS-CPU-6144• UCS-CPU-6136• UCS-CPU-6126• UCS-CPU-6146• UCS-CPU-6134• UCS-CPU-6128• UCS-CPU-5122• UCS-CPU-4116• UCS-CPU-6142M

UCS リリース	カタログ ファイル名	このリリースの追加 PID
		<ul style="list-style-type: none"> • UCS-CPU-8180M <p>UCSC-C480-M5ML の メモリ:</p> <ul style="list-style-type: none"> • UCS-MR-128G8RS-H • UCS-MR-X64G4RS-H • UCS-ML-X64G4RS-H • UCS-MR-X32G2RS-H • UCS-ML-X32G2RS-H • UCS-MR-X16G1RS-H • UCS-MR-X16G2RS-H <p>UCSC-C480-M5ML の PSU:</p> <ul style="list-style-type: none"> • UCSC-PSU1-フル W <p>UCSC-C480-M5ML のファン モジュール:</p> <ul style="list-style-type: none"> • UCSC-FAN-C480M5 <p>UCSC-C480-M5ML の Cisco VIC:</p> <ul style="list-style-type: none"> • C シリーズおよび S シリーズ (UCSC-PCIE-C25Q-04) 向け VIC 1455 10/25G PCIe • C シリーズ (UCSC-PCIE-C100-04) 向け VIC 1495 40/100G PCIe <p>UCSC-C480-M5ML の NIC:</p> <ul style="list-style-type: none"> • Qlogic QLE45611HLCU シングル ポート 100G NIC (UCSC-PCIE-QS100GF) <p>UCSC-C480-M5ML の HDD:</p> <ul style="list-style-type: none"> • UCS-HD900G15K12N • UCS-HD12TB10K12N • UCS-HD18TB10K4KN • UCS-HD2T7K12N <p>UCSC-C480-M5ML の SSD:</p>

UCS リリース	カタログ ファイル名	このリリースの追加 PID
		<ul style="list-style-type: none"> • UCS-SD16T123X-EP • UCS-SD32T123X-EP • UCS-SD120GM1X-EV • UCS-SD240GM1X-EV • UCS-SD480GM1X-EV • UCS-SD960GM1X-EV • UCS-SD16TM1X-EV • UCS-SD19TM1X-EV • UCS-SD38TM1X-EV • UCS-SD76TM1X-EV <p>UCSC-C480-M5ML のフラッシュ ドライブ:</p> <ul style="list-style-type: none"> • UCS-USBFLSHB-16GB <p>UCSC-C480-M5ML の GPU:</p> <ul style="list-style-type: none"> • NVIDIA SXM2 V100 32GB Nvlink モジュール (UCSC-GPUV100SXM32) <p>UCSC-C480-M5ML の NVMe ドライブ:</p> <ul style="list-style-type: none"> • UCSC-NVMEHW-H3200 <p>C480-M5ML のミニストレージ キャリア:</p> <ul style="list-style-type: none"> • UCS-MSTOR-SD • UCS-MSTOR-M2 <p>C480-M5ML の SD カード:</p> <ul style="list-style-type: none"> • UCS-SD-64G-S • UCS-SD-128G <p>UCSC-C480-M5ML のマイクロ SD カード:</p> <ul style="list-style-type: none"> • UCS-MSD-32G <p>UCSC-C480-M5ML の M.2 SATA SSD:</p> <ul style="list-style-type: none"> • UCS-M2-240GB • UCS-M2-960GB

UCS リリース	カタログ ファイル名	このリリースの追加 PID
		<p>UCSC-C480-M5ML の RAID コントローラ:</p> <ul style="list-style-type: none"> • UCSC-RAID-M5HD <p>Cisco VIC アダプタ:</p> <ul style="list-style-type: none"> • C シリーズ (UCSC-PCIE-C100-04) 向け VIC 1495 40/100G PCIe • C シリーズ (UCSC-MLOM-C100-04) 向け VIC 1497 40/100G mLOM <p>すべての UCS サーバの TPM2:</p> <ul style="list-style-type: none"> • UCSX-TPM2-002-C <p>UCS 6454 ファブリック インターコネクタの高電圧 DC 1200 ワット電源装置:</p> <ul style="list-style-type: none"> • N9K-PUV-1200W <p>M5 サーバ用 Intel Optane NVMe エクストリーム パフォーマンス ドライブ:</p> <ul style="list-style-type: none"> • UCSC-NVMEXP-I750 <p>C240 M5 サーバの GPU:</p> <ul style="list-style-type: none"> • V100-32G: NVIDIA V100 PCIe PG500-200 250W 32GB GPU <p>UCSC C125 用の QLogic ネットワーク アダプタ カード:</p> <ul style="list-style-type: none"> • UCSC-PCIE-QD10GC: 10G ネットワーク アダプタ カード • UCSC-PCIE-QD25GF: 25G ネットワーク アダプタ カード
4.0(1d)	ucs-catalog 4.0.1 c. .bin	<p>ドライブ:</p> <ul style="list-style-type: none"> • UCS-SD480GBHBNK9 • UCS-SD960GBHBNK9 • UCS-SD38TBHBNK9 • UCS-SD480GBHTNK9 • UCS-SD960GBHTNK9 • UCS-SD38TBHTNK9

UCS リリース	カタログ ファイル名	このリリースの追加 PID
4.0(1c)	ucs-catalog (4.0.1)	—
4.0(1b)	ucs-catalog (4.0.1)	—

UCS リリース	カタログ ファイル名	このリリースの追加 PID
4.0(1a)	ucs-catalog (4.0.1)	

UCS リリース	カタログ ファイル名	このリリースの追加 PID
		<p>Cisco UCS 6454 ファブリック インターコネクト:</p> <ul style="list-style-type: none"> • UCS FI-6454 <p>Cisco UCS ラックマウント サーバ</p> <ul style="list-style-type: none"> • UCSC-C125 <p>C125 M5 のシャーシ:</p> <ul style="list-style-type: none"> • UCSC-C4200-SFF <p>UCSC C125 の CPU:</p> <ul style="list-style-type: none"> • UCS-CPU-7601 • UCS-CPU-7551 • UCS-CPU-7501 • UCS-CPU-7451 • UCS-CPU-7401 • UCS-CPU-7351 • UCS-CPU-7301 • UCS-CPU-7281 • UCS-CPU-7261 • UCS-CPU-7251 • UCS-CPU-7551P • UCS-CPU-7401P • UCS-CPU-7351P <p>UCSC C125 のメモリ:</p> <ul style="list-style-type: none"> • UCS-MR-128G8RS-H • UCS-MR-X64G4RS-H • UCS-ML-X64G4RS-H • UCS-MR-X32G2RS-H • UCS-MR-X16G1RS-H • UCS-MR-X16G2RS-H • UCS-MR-X8G1RS-H <p>UCSC-C125 の OCP NIC:</p>

UCS リリース	カタログ ファイル名	このリリースの追加 PID
		<ul style="list-style-type: none"> • UCSC-OCF-QD10GC • UCSC-OCF-QD25GF <p>UCSC C125 のストレージ コントローラ:</p> <ul style="list-style-type: none"> • UCSC-SAS9460-8i <p>UCSC C125 の SD カード:</p> <ul style="list-style-type: none"> • UCS-SD-32G-S • UCS-SD-64G-S • UCS-SD-128G <p>UCSC-C125 のマイクロ SD カード:</p> <ul style="list-style-type: none"> • UCS-MSD-32G <p>UCSC-C125 の M.2 SATA SSD:</p> <ul style="list-style-type: none"> • UCS-M2-240GB • UCS-M2-960GB <p>UCSC-C125 のフラッシュ USB ドライブ:</p> <ul style="list-style-type: none"> • UCS-USBFLSHB-16GB <p>UCSC-C125 のミニストレージ キャリア:</p> <ul style="list-style-type: none"> • UCS-MSTOR-SD • UCS-MSTOR-M2 <p>Cisco VIC アダプタ:</p> <ul style="list-style-type: none"> • B シリーズ向け VIC 1440 10/40G mLOM (UCSB-MLOM-40G-04) • B シリーズ (UCSB-VIC-M84-4P) の VIC 1480 10/40G PCIe • C シリーズおよび S シリーズ (UCSC-PCIE-C25Q-04) 向け VIC 1455 10/25G PCIe • C シリーズ (UCSC-MLOM-C25Q-04) の VIC 1497 40/100G mLOM <p>HX NVMe サーバ:</p> <ul style="list-style-type: none"> • HXAF220C-M5SN

UCS リリース	カタログ ファイル名	このリリースの追加 PID
		<p>C240HX M5 サーバを搭載した PCIe 圧縮および暗号化 CPU オフロード カード</p> <ul style="list-style-type: none"> • HX-PCIE-OFFLOAD-1 <p>Intel Optane NVMe Med. M5 サーバのパフォーマンス ドライブ:</p> <ul style="list-style-type: none"> • UCSC-NVMEXP-I375 • UCSB-NVMEXP-I375 • UCSC-NVMEXP-I750 • UCSB-NVMEXP-I750

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
4.0(4j)4.1(2a)	CSCvu53094	CVE-2020-11022	<p>1.2 から 3.5.0 のバージョンの jQuery ソフトウェアパッケージを使用している Cisco UCS Manager および UCS 6400 シリーズ ファブリック インターコネクには、次の一般的な脆弱性および露出 (CVE) ID によって影響を受ける可能性があります。</p> <ul style="list-style-type: none"> • CVE-2020-11022 : jQuery バージョン 1.2 以上かつ 3.5.0 以前では、HTML をサニタイズした後でも、信頼できないソースから jQuery の DOM 操作方法のいずれか (ie.html(), .append(), その他) に HTML を渡して、信頼できないコードを実行する可能性があります。この問題は、jQuery 3.5.0 で修正されています。

リリース	不具合 ID	CVE	説明
4.0 (4i)	CSCvt86093	<ul style="list-style-type: none"> • CVE-2020-0548 • CVE-2020-0549 	<p>Intel[®] プロセッサに基づく Cisco UCS M5 サーバは、次の一般的な脆弱性およびエクスポージャ (CVE) ID によって特定された脆弱性の影響を受けます。</p> <ul style="list-style-type: none"> • CVE-2020-0548 : 一部の Intel[®] プロセッサでのクリーンアップエラーにより、認証されたユーザがローカルアクセスによる情報開示を有効にできる場合があります。 • CVE-2020-0549 : 一部の Intel[®] プロセッサの一部のデータ キャッシュエビクションでのクリーンアップエラーにより、認証されたユーザがローカルアクセスによる情報開示を有効にできる場合があります。 <p>このリリースには、Cisco UCS M5 サーバの BIOS 改定が含まれています。これらの BIOS 改定には、これらの脆弱性の緩和に必要な更新された Cisco UCS M5 サーバの SINIT ACM が含まれています。</p>
4.0 (4i)	CSCvq33385	CVE-2016-2183	<p>最新の CiscoSSL 1.0.2 6.2.341 には、リストされている一般的な脆弱性およびエクスポージャ (CVE) ID によって識別される、Cisco UCS Manager の OpenSSL 脆弱性の緩和が含まれるようになりました。</p>

リリース	不具合 ID	CVE	説明
4.0 (4h)	CSCvs81686	<ul style="list-style-type: none"> • CVE-2020-0548 • CVE-2020-0549 	<p>Intel[®] プロセッサに基づく Cisco UCS M5 サーバは、次の一般的な脆弱性およびエクスポージャ (CVE) ID によって特定された脆弱性の影響を受けます。</p> <ul style="list-style-type: none"> • CVE-2020-0548、一部の Intel[®] プロセッサのクリーンアップエラーは、認証されたユーザに対しローカルアクセスを通じて情報開示を可能にすることがあります。 • CVE-2020-0549、一部の Intel[®] プロセッサにおけるデータキャッシュ除去でのクリーンアップエラーは、認証されたユーザに対しローカルアクセスを通じて情報開示を可能にすることがあります。 <p>このリリースには、Cisco UCS M5 サーバの BIOS 改定が含まれています。これらの BIOS 改定には、これらの脆弱性の緩和に必要な更新された Cisco UCS M5 サーバの SINIT ACM が含まれています。</p>

リリース	不具合 ID	CVE	説明
4.0 (4g)	CSCvr54409 CSCvr54415	<ul style="list-style-type: none">• CVE-2019-11135• CVE-2019-0151• CVE-2019-0152• CVE-2019-11136• CVE-2019-11137• CVE-2019-11139• CVE-2019-11109	

リリース	不具合 ID	CVE	説明
			<p>Intel® プロセッサに基づく Cisco UCS M5 サーバは、次の一般的な脆弱性およびエクスポージャ (CVE) ID によって特定された脆弱性の影響を受けます。</p> <ul style="list-style-type: none"> • CVE-2019-11135 (TSX Asynchronous Abort Advisory) 条件は、特定の第2世代 Intel® Xeon® スケーラブルプロセッサ、第8世代 Intel® Core™ プロセッサファミリー、第9世代 Intel® Core™ プロセッサファミリー、および第10世代 Intel® Core™ プロセッサファミリーに影響を与え、ローカルアクセスを持つサイドチャンネルを介して認証されたユーザーが情報開示可能になる可能性があります。 • CVE-2019-0151 (CPU Local Privilege Escalation Advisory) は、特定の Intel® 第4世代 Intel® Core™ プロセッサ、第5世代 Intel® Core™ プロセッサ、第6世代 Intel® Core™ プロセッサ、第7世代 Intel® Core™ プロセッサ、第8世代 Intel® Core™ プロセッサ、Intel® Xeon® プロセッサ E3 v2/v3/v4/v5/v6 ファミリー、Intel® Xeon® プロセッサ E5 v3/v4 ファミリー、Intel® Xeon® プロセッサ E7 v3/v4 ファミリー、Intel® Xeon® スケーラブルプロセッサ第2世代、Intel® Xeon® スケーラブルプロセッサ、Intel® Xeon® プロセッサ D-1500/D-2100)、Intel® Xeon® プロセッサ E-2100/E3100、および Intel® Xeon® プロセッサ W-2100/W-310 に影響を与えます (Intel® TXT の十分なメモリ保護によって、権限を持

リリース	不具合 ID	CVE	説明
			<p>つユーザーがローカルアクセスによる権限の昇格を有効にした場合)。これにより、Intel[®] TXT 保護をバイパスする可能性があります。</p> <ul style="list-style-type: none"> • CVE-2019-0152 (CPU ローカル特権エスカレーション・アドバイザリ) は、特定のインテル[®] Xeon[®] スケーラブル・プロセッサ、インテル[®] Xeon[®] プロセッサ D-2100、D-3100、インテル[®] Xeon[®] プロセッサ W-2100、W-3100 に影響を与え、メモリ保護が不十分な場合、特権ユーザーがローカルアクセスを通じて特権特権のエスカレーションを可能にする可能性があります。これにより、システム管理モード (SMM) と Intel[®] TXT 保護がバイパスされる可能性があります。 • システムファームウェアの不十分なアクセスコントロールによって、権限のあるユーザーが潜在的に権限の上昇、サービスの拒否、ローカルアクセスを介した情報開示が可能になる可能性がある場合、CVE-2019-11136 (BIOS 2019.2 IPU Advisory) は、第2世代 Intel[®] Xeon[®] スケーラブルプロセッサ、Intel[®] Xeon[®] スケーラブルプロセッサ、Intel[®] Xeon[®] プロセッサ D ファミリーに影響を与えます。

リリース	不具合 ID	CVE	説明
			<ul style="list-style-type: none"> • システムファームウェアでの入力検証が不十分なことによって、権限のあるユーザーが潜在的に権限の上昇、サービスの拒否、ローカルアクセスを介した情報開示が可能になる可能性がある場合、 CVE-2019-11137 (BIOS 2019.2 IPU Advisory) は、第 2 世代 Intel® Xeon® スケーラブルプロセッサ、Intel® Xeon® スケーラブルプロセッサ、Intel® Xeon® プロセッサ D ファミリー、Intel® Xeon® プロセッサ E5 v4 ファミリー、Intel® Xeon® プロセッサ E7 v4 ファミリー、Intel® Atom® プロセッサ C シリーズに影響を与えます。 • CVE-2019-11139 (Voltage Modulation Technical Advisory) 特定の Intel® Xeon® スケーラブルプロセッサの電圧変調に関する脆弱性により、権限のあるユーザーがローカルアクセスを介してサービス拒否が可能になる可能性があります。 • CVE-2019-11109: バージョン SPS_E5_04.01.04.297.0, SPS_SoC-X_04.00.04.101.0, および SPS_SoC-A_04.00.04.193.0 より前の Intel® サーバー プラットフォームサービスのサブシステムでのロジックの問題により、権限のあるユーザーがローカル経由でサービス拒否を有効にできる場合があります。

リリース	不具合 ID	CVE	説明
			このリリースには、Cisco UCS M5 サーバの BIOS 改定が含まれています。これらの BIOS 改定には、これらの脆弱性の緩和に必要な更新されたマイクロコードおよび Secure Initialization (SINIT) Authenticated Code Modules (ACM) が含まれています。

リリース	不具合 ID	CVE	説明
4.0 (4g)	CSCvr54413 CSCvr54414 CSCvr54416	<ul style="list-style-type: none"> • CVE-2019-0151 • CVE-2019-11137 	

リリース	不具合 ID	CVE	説明
			<p>Intel[®] プロセッサに基づく Cisco UCS M4 サーバは、次の一般的な脆弱性およびエクスポージャ (CVE) ID によって特定された脆弱性の影響を受けます。</p> <ul style="list-style-type: none"> • CVE-2019-0151 (CPU Local Privilege Escalation Advisory) は、特定の Intel[®] 第 4 世代 Intel[®] Core[™] プロセッサ、第 5 世代 Intel[®] Core[™] プロセッサ、第 6 世代 Intel[®] Core[™] プロセッサ、第 7 世代 Intel[®] Core[™] プロセッサ、第 8 世代 Intel[®] コア[™] プロセッサ、Intel[®] Xeon[®] プロセッサ E3 v2/v3/v4/v5/v6 ファミリ、Intel[®] Xeon[®] プロセッサ E5 v3/v4 ファミリ、Intel[®] Xeon[®] プロセッサ E7 v3/v4 ファミリ、Intel[®] Xeon[®] スケーラブル プロセッサ 第 2 世代、Intel[®] Xeon[®] スケーラブル プロセッサ、Intel[®] Xeon[®] プロセッサ D-1500/D-2100)、Intel[®] Xeon[®] プロセッサ E-2100/E3100、および Intel[®] Xeon[®] プロセッサ W-2100/W-310 に影響を与えます (Intel[®] TXT の十分なメモリ保護によって、権限を持つユーザーがローカルアクセスによる権限の昇格を有効にした場合)。これにより、Intel[®] TXT 保護をバイパスする可能性があります。 • システムファームウェアでの入力検証が不十分なことによって、権限の昇格、サービス拒否、またはローカルアクセスによる情報漏えいが可能になる可能性がある場合、CVE-2019-11137 (BIOS 2019.2 IPU Advisory) は、第 2 世代 Intel[®] Xeon[®] スケーラブルプロ

リリース	不具合 ID	CVE	説明
			<p>セッサ、Intel[®] Xeon[®] スケーラブルプロセッサ、Intel[®] Xeon[®] プロセッサ D ファミリー、Intel[®] Xeon[®] プロセッサ E5 v4 ファミリー、Intel[®] Xeon[®] プロセッサ E7 v4 ファミリー、Intel[®] Atom[®] プロセッサ C シリーズに影響を与えます。システムファームウェアでの入力検証が不十分な場合、特権ユーザーが潜在的に有効にできる可能性があります。特権のエスカレーション、サービス拒否、またはローカルアクセスによる情報漏えい。</p> <p>このリリースには、Cisco UCS M4 世代サーバの BIOS 改定が含まれています。これらの BIOS 改定には、これらの脆弱性の緩和に必要な更新された Cisco UCS M4 サーバのマイクロコードおよび SINIT ACM が含まれています。</p>

リリース	不具合 ID	CVE	説明
4.0 (4g)	CSCvr54411	CVE-2019-0151	<p>Intel® プロセッサに基づく Cisco UCS B シリーズおよび C シリーズ M3 サーバは、次の一般的な脆弱性およびエクスポージャ (CVE) ID によって特定された脆弱性の影響を受けます。</p> <ul style="list-style-type: none"> • CVE-2019-0151 (CPU Local Privilege Escalation Advisory) は、特定の Intel® 第 4 世代 Intel® Core™ プロセッサ、第 5 世代 Intel® Core™ プロセッサ、第 6 世代 Intel® Core プロセッサ、第 7 世代 Intel® Core™ プロセッサ、第 8 世代 Intel® コア™ プロセッサ、Intel® Xeon® プロセッサ E3 v2/v3/v4/v5/v6 ファミリ、Intel® Xeon® プロセッサ E5 v3/v4 ファミリ、Intel® Xeon® プロセッサ E7 v3/v4 ファミリ、Intel® Xeon® スケーラブル プロセッサ 第 2 世代、Intel® Xeon® スケーラブル プロセッサ、Intel® Xeon® プロセッサ D-1500/D-2100)、Intel® Xeon® プロセッサ E-2100/E3100、および Intel® Xeon® プロセッサ W-2100/W-310 に影響を与えます (Intel® TXT の十分なメモリ保護によって、権限を持つユーザーがローカルアクセスによる権限の昇格を有効にした場合)。これにより、Intel® TXT 保護をバイパスする可能性があります。 <p>このリリースには、Cisco UCS B シリーズおよび C シリーズ M3 サーバの BIOS 改定が含まれます。これらの BIOS 改定には、これらの脆弱性の緩和に必要な更新された Cisco UCS M3 サーバの SINIT ACM が含まれています。</p>

リリース	不具合 ID	CVE	説明
4.0 (4f)	CSCvq19565	CVE-2019-11479 CVE-2019-11478	<p>このバグは、次の CVE ID によって識別される Linux カーネルに影響する脆弱性について製品を評価するために提出されました。</p> <ul style="list-style-type: none"> • CVE-2019-11479: 低 MSS 値による超過したリソース消費 • CVE-2019-11478: SACK Slowness または Excess リソース使用状況 <p>TCP ネットワーキング脆弱性では、Linux カーネルへの影響を特定しています。最小セグメントサイズおよび TCP Selective Acknowledgement (SACK) 機能に関連する脆弱性。もっとも深刻なダブである「SACK Panic」によって、最新の Linux カーネルでリモートでトリガされるカーネルパニックとなる可能性があります。</p> <p>6200 シリーズ ファブリック インターコネクタを搭載した Cisco UCS サーバは、Linux カーネルの脆弱性のあるバージョンが含まれていることが確認されています。ただし、製品は、次の脆弱性の影響を受けません。</p> <p>CVE-2019-11477: SACK カーネルパニック</p> <p>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はありません。</p> <p>上で一覧になっている脆弱性に関する詳細は、http://cve.mitre.org/cve/cve.html で確認できます</p>

リリース	不具合 ID	CVE	説明
4.0 (4f)	CSCVq21317	CVE-2019-11477 CVE-2019-11478 CVE-2019-11479	<p>このバグは、次の CVE ID によって識別される Linux カーネルに影響する脆弱性について製品を評価するために提出されました。</p> <ul style="list-style-type: none"> • CVE-2019-11477: SACK パニック • CVE-2019-11478: SACK Slowness または Excess リソース使用状況 • CVE-2019-11479: 低 MSS 値による超過したリソース消費 <p>TCP ネットワーキング脆弱性では、Linux カーネルへの影響を特定しています。最小セグメントサイズおよび TCP Selective Acknowledgement (SACK) 機能に特に関連する脆弱性。もっとも深刻なダブである「SACK Panic」によって、最新の Linux カーネルでリモートでトリガされるカーネルパニックとなる可能性があります。</p> <p>6400 シリーズ ファブリック インターコネクトを搭載した Cisco UCS サーバは、Linux カーネルの脆弱性のあるバージョンが含まれていることが確認されています。</p> <p>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はありません。</p> <p>上で一覧になっている脆弱性に関する詳細は、http://cve.mitre.org/cve/cve.html で確認できます</p>

リリース	不具合 ID	CVE	説明
4.0 (4f)	CSCvm80093	CVE-2019-1966	<p>Cisco UCS ファブリック インターコネクトへの特定コマンドの CLI 実装での脆弱性により、認証されたローカルの攻撃者が CLI をエスケープし、デバイスの基盤となるオペレーティングシステムに不正にアクセスできるようになっている可能性があります。</p> <p>攻撃者はこの脆弱性を悪用して CLI をエスケープし、ルートユーザの権限を使用し、基盤となるオペレーティングシステムで任意のコマンドを実行する可能性があります。攻撃者は有効なデバイス クレデンシャルを必要と不再ります。</p> <p>Cisco のセキュリティ脆弱性ポリシーに関する追加情報については、次の URL を参照してください。 セキュリティ脆弱性ポリシー。</p>
4.0 (4f)	CSCvp56979	CVE-2019-9213	<p>6400 シリーズ ファブリック インターコネクトを搭載した Cisco UCS サーバには、次の共通の脆弱性およびエクスポージャ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。</p> <p>CVE-2019-9213: Linux カーネル expand_downwards 関数ヌルポインタの逆参照の脆弱性</p> <p>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。</p> <p>上記の脆弱性の詳細については、http://cve.mitre.org/cve/cve.html を参照してください。</p>

リリース	不具合 ID	CVE	説明
4.0 (4e)	CSCvp62709 CSCvp69717	CVE-2019-11358	<p>Cisco UCS Manager および UCS 6200 シリーズ ファブリック インターコネクには、次の一般的な脆弱性および露出 (CVE) ID によって特定されたクロスサイトスクリプトの脆弱性の影響を受ける可能性がある、jQuery ソフトウェアのバージョンが含まれています。</p> <p>CVE-2019-11358</p> <p>Cisco のセキュリティ脆弱性ポリシーに関する追加情報については、次を参照してください。</p> <p>セキュリティ脆弱性ポリシー</p>

リリース	不具合 ID	CVE	説明
4.0 (4e)	CSCvn23535 CSCvn23538	CVE-2019-1963	<p>Cisco FXOS ソフトウェアおよび Cisco NX-OS ソフトウェアにおける、Simple Network Management Protocol (SNMP) の入力パケットプロセッサの脆弱性により、認証されていないリモートの攻撃者が、該当デバイスの SNMP アプリケーションを予期せず再起動する可能性があります。</p> <p>この脆弱性は、SNMP パケットで抽象構文記法 1 (asn.1) エンコードされた変数の検証が不適切であることに起因します。攻撃者は、該当デバイスの SNMP デーモンに巧妙に細工された SNMP パケットを送信することにより、この脆弱性を不正利用する可能性があります。エクスプロイトが成功すると、攻撃者は SNMP アプリケーションを複数回再起動し、システムレベルの再起動が行われ、サービス妨害 (DoS) 状態になる可能性があります。</p> <p>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はありません。</p> <p>このアドバイザリは、次のリンク先で確認できます。</p> <p>Cisco FXOS および NX OS ソフトウェアにより認証された Simple Network Management Protocol におけるサービス妨害 (Dos) の脆弱性</p>

リリース	不具合 ID	CVE	説明
4.0 (4c)	CSCvp27917	CVE-2018-12126 CVE-2018-12127 CVE-2018-12130 CVE-2019-11091	

リリース	不具合 ID	CVE	説明
			<p>Cisco UCS B シリーズ M3 ブレードサーバは、Intel® Xeon® Sandy Bridge E5-2600 および Ivy Bridge E5 2600 v2 製品ファミリプロセッサに基づいており、Microarchitectural Data Sampling (MDS) を使用して、他のアプリケーションによって CPU で処理されるデータへのアクセスを取得するエクスプロイトの亜種に対して脆弱です。</p> <ul style="list-style-type: none"> • CVE-2018-12126 (Microarchitectural Store Buffer Data Sampling) は、CPU のストアバッファに影響を及ぼし、UCS Manager リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティングシステムおよびハイパーバイザパッチを適用することによって対処されます。 • CVE-2018-12127 (Microarchitectural Load Port Data Sampling) は、CPU のロードバッファに影響を及ぼし、UCS Manager リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティングシステムおよびハイパーバイザパッチを適用することによって対処されます。 • CVE-2018-12130 (Microarchitectural Fill Buffer Data Sampling) は、CPU のラインフィルバッファに影響を及ぼし、UCS Manager リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティングシステムおよびハイパーバイザパッチを適用する

リリース	不具合 ID	CVE	説明
			<p>ことによって対処されます。</p> <ul style="list-style-type: none"> • 17 CVE-2019-11091 (Microarchitectural Data Sampling Uncacheable Memory) は、CPUの到達不能なメモリに影響を及ぼし、UCS Manager リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティングシステムおよびハイパーバイザパッチを適用することによって対処されます。 <p>このリリースには、Cisco UCS M3 世代サーバの BIOS 改定が含まれています。これらの BIOS 改定には、これらの脆弱性の緩和に必要な更新されたマイクロコードが含まれています。</p> <p>上で一覧になっている脆弱性に関する詳細は、http://cve.mitre.org/cve/cve.html で確認できます</p>
4.0 (4c)	CSCvq66225	CVE-2019-9836	<p>Linux オペレーティングシステムを実行している仮想マシンでユーザーが選択可能な AMD セキュア暗号化機能を使用した、AMD EPYC™ プロセッサに基づく Cisco UCS C シリーズサーバでは、暗号化テクノロジーの動作を操作することによって暗号キーが侵害される可能性があります。このリリースには、このリスクを軽減するための BIOS リビジョンが含まれています。この脆弱性の詳細については、https://www.amd.com/en/corporate/product-security を参照してください。</p>

リリース	不具合 ID	CVE	説明
4.0 (4c)	CSCvp12424	CVE-2019-1559	<p>Cisco UCS Manager には、次の一般的な脆弱性および露出 (CVE) ID によって特定された脆弱性の影響を受ける可能性がある、OpenSSH プロトコルのバージョンが含まれています。</p> <ul style="list-style-type: none"> • CVE-2019-1559 <p>アプリケーションで致命的なプロトコルエラーが発生し、<code>SSL_shutdown()</code> を 2 回呼び出すと、データの復号化に使用される可能性があるパディング oracle のように動作する可能性があります。</p> <p>この問題は、OpenSSL ソフトウェアアップデートによって解決されます。詳細については、https://tools.cisco.com/security/center/viewAlert.x?alertId=59697 を参照してください。</p>

リリース	不具合 ID	CVE	説明
4.0(4b)	CSCvo21412	CVE-2018-12126	
4.0(2e)	CSCvp30013	CVE-2018-12127	
		CVE-2018-12130	
		CVE-2019-11091	

リリース	不具合 ID	CVE	説明
			<p>Cisco UCS M4 サーバおよび Hyperflex M4 サーバは、Intel® Xeon® プロセッサ E7 v2、V3、および v4 製品ファミリ プロセッサに基づいており、Microarchitectural Data Sampling (MDS) を使用して、他のアプリケーションによって CPU で処理されるデータへのアクセスを取得するエクスプロイトの亜種に対して脆弱です。</p> <ul style="list-style-type: none"> • CVE-2018-12126 (Microarchitectural Store Buffer Data Sampling) は、CPU のストア バッファに影響を及ぼし、UCS Manager リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティングシステムおよびハイパーバイザパッチを適用することによって対処されます。 • CVE-2018-12127 (Microarchitectural Load Port Data Sampling) は、CPU のロードバッファに影響を及ぼし、UCS Manager リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティングシステムおよびハイパーバイザパッチを適用することによって対処されます。 • CVE-2018-12130 (Microarchitectural Fill Buffer Data Sampling) は、CPU のラインフィルバッファに影響を及ぼし、UCS Manager リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティングシステムおよびハイパーバイザパッチを適用する

リリース	不具合 ID	CVE	説明
			<p>ことによって対処されます。</p> <ul style="list-style-type: none">• 17 CVE-2019-11091 (Microarchitectural Data Sampling Uncacheable Memory) は、CPUの到達不能なメモリに影響を及ぼし、UCS Manager リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティングシステムおよびハイパーバイザパッチを適用することによって対処されます。 <p>このリリースには、Cisco UCS M4 世代サーバの BIOS 改定が含まれています。これらの BIOS 改定には、これらの脆弱性の緩和に必要な更新されたマイクロコードが含まれています。</p>

リリース	不具合 ID	CVE	説明
4.0(4b)	CSCvp28016	CVE-2018-12126	
4.0(2e)		CVE-2018-12127	
		CVE-2018-12130	
		CVE-2019-11091	

リリース	不具合 ID	CVE	説明
			<p>Cisco UCS M4 サーバおよび Hyperflex M4 サーバは、Intel® Xeon® プロセッサ E5、V3、および v4 製品ファミリプロセッサに基づいており、Microarchitectural Data Sampling (MDS) を使用して、他のアプリケーションによって CPU で処理されるデータへのアクセスを取得するエクスプロイトの亜種に対して脆弱です。</p> <ul style="list-style-type: none"> • CVE-2018-12126 (Microarchitectural Store Buffer Data Sampling) は、CPU のストアバッファに影響を及ぼし、UCS Manager リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティングシステムおよびハイパーバイザパッチを適用することによって対処されます。 • CVE-2018-12127 (Microarchitectural Load Port Data Sampling) は、CPU のロードバッファに影響を及ぼし、UCS Manager リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティングシステムおよびハイパーバイザパッチを適用することによって対処されます。 • CVE-2018-12130 (Microarchitectural Fill Buffer Data Sampling) は、CPU のラインフィルバッファに影響を及ぼし、UCS Manager リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティングシステムおよびハイパーバイザパッチを適用する

リリース	不具合 ID	CVE	説明
			<p>ことによって対処されます。</p> <ul style="list-style-type: none"> • 17 CVE-2019-11091 (Microarchitectural Data Sampling Uncacheable Memory) は、CPUの到達不能なメモリに影響を及ぼし、UCS Manager リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティングシステムおよびハイパーバイザパッチを適用することによって対処されます。 <p>このリリースには、Cisco UCS M4 世代サーバの BIOS 改定が含まれています。これらの BIOS 改定には、これらの脆弱性の緩和に必要な更新されたマイクロコードが含まれています。</p>

リリース	不具合 ID	CVE	説明
4.0(4b) 4.0(2e)	CSCvp31847	CVE-2018-12126 CVE-2018-12127 CVE-2018-12130 CVE-2019-11091	

リリース	不具合 ID	CVE	説明
			<p>Cisco UCS M5 サーバおよび Hyperflex M5 サーバは、Intel® Xeon® プロセッサ スケーラブル プロセッサに基づいており、Microarchitectural Data Sampling (MDS) を使用して、他のアプリケーションによって CPU で処理されるデータへのアクセスを取得するエクспロイトの亜種に対して脆弱です。</p> <ul style="list-style-type: none"> • CVE-2018-12126 (Microarchitectural Store Buffer Data Sampling) は、CPU のストアバッファに影響を及ぼし、UCS Manager リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティングシステムおよびハイパーバイザパッチを適用することによって対処されます。 • CVE-2018-12127 (Microarchitectural Load Port Data Sampling) は、CPU のロードバッファに影響を及ぼし、UCS Manager リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティングシステムおよびハイパーバイザパッチを適用することによって対処されます。 • CVE-2018-12130 (Microarchitectural Fill Buffer Data Sampling) は、CPU のラインフィルバッファに影響を及ぼし、UCS Manager リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティングシステムおよびハイパーバイザパッチを適用することによって対処されます。

リリース	不具合 ID	CVE	説明
			<ul style="list-style-type: none">• 17 CVE-2019-11091 (Microarchitectural Data Sampling Uncacheable Memory) は、CPUの到達不能なメモリに影響を及ぼし、UCS Manager リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティングシステムおよびハイパーバイザパッチを適用することによって対処されます。 <p>このリリースには、Cisco UCS M5 世代サーバの BIOS 改定が含まれています。これらの BIOS 改定には、これらの脆弱性の緩和に必要な更新されたマイクロコードが含まれています。</p>

リリース	不具合 ID	CVE	説明
4.0(2a)	CSCvm35067	CVE-2018-3655	<p>Cisco UCS C シリーズ サーバには、次の一般的な脆弱性および露出 (CVE) ID によって特定された脆弱性の影響を受ける可能性がある、Intel[®] コンバージドセキュリティ管理エンジン (CSME) のバージョンが含まれています。</p> <ul style="list-style-type: none"> • CVE-2018-3655 <p>物理的なアクセス権を持つ攻撃者は、これらの脆弱性を使用して次のことを行うことができます。</p> <ul style="list-style-type: none"> • Intel[®] CSME アンチリプレイ保護をバイパスすることにより、Intel CSME 内に保存された秘密に対するブルートフォース攻撃の可能性を許容します。 • Intel[®] MEBX パスワードへの不正アクセスを取得する • Intel[®] csme ファイル システム ディレクトリ、またはサーバ プラットフォーム サービスと信頼できる実行環境 (Intel[®] txe) データ ファイルの整合性を改ざんします。 <p>このリリースには、Cisco UCS M5 世代 C シリーズ サーバの BIOS 改定が含まれています。</p>

リリース	不具合 ID	CVE	説明
4.0(1d)	CSCvm19864	CVE-2016-3115	<p>Cisco UCS Manager および UCS 6200 シリーズ ファブリック インターコネクタには、次の一般的な脆弱性および露出 (CVE) ID によって特定された脆弱性の影響を受ける可能性がある、OpenSSH プロトコルのバージョンが含まれています。</p> <ul style="list-style-type: none">• CVE-2016-3115 <p>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。</p>

リリース	不具合 ID	CVE	説明
4.0(1c)	CSCvk20775	CVE-2018-3655	<p>Cisco UCS B シリーズ サーバには、次の一般的な脆弱性および露出 (CVE) ID によって特定された脆弱性の影響を受ける可能性がある、Intel® コンバージドセキュリティ管理エンジン (CSME) のバージョンが含まれています。</p> <ul style="list-style-type: none"> • CVE-2018-3655 <p>物理的なアクセス権を持つ攻撃者は、これらの脆弱性を使用して次のことを行うことができます。</p> <ul style="list-style-type: none"> • Intel® CSME アンチリプレイ保護をバイパスすることにより、Intel CSME 内に保存された秘密に対するブルートフォース攻撃の可能性を許容します。 • Intel® MEBX パスワードへの不正アクセスを取得する • Intel® csme ファイル システム ディレクトリ、またはサーバ プラットフォーム サービスと信頼できる実行環境 (Intel® txe) データ ファイルの整合性を改ざんします。 <p>このリリースには、Cisco UCS M5 世代 B シリーズ サーバの BIOS 改定が含まれています。</p>

リリース	不具合 ID	CVE	説明
4.0(1a)	CSCvm03356	CVE-2018-3615 CVE-2018-3620 CVE-2018-3646	

リリース	不具合 ID	CVE	説明
			<p>Cisco UCS B シリーズ M3 サーバおよび C シリーズ M3 サーバは、CPU の投機処理とデータ キャッシュのタイミングを使用して権限情報を識別するエクスプロイトに対して脆弱な、Intel® プロセッサに基づいています。これらのエクスプロイトは、総称して L1 Terminal Fault (L1TF) と呼ばれています。</p> <ul style="list-style-type: none"> • CVE-2018-3615 (SGX に影響) は Foreshadow と呼ばれ、既存の Cisco UCS サーバに影響を与えます。これは、Cisco UCS M5 および旧世代サーバと、HyperFlex M5 および旧世代サーバは Intel® SGX テクノロジーを使用しないためです。 • CVE-2018-3620 (OS/システム管理モードに影響) および CVE-2018-3646 (仮想マシンモニタに影響) は、Intel® による L1 Terminal Fault 攻撃とも呼ばれます。これらの脆弱性は、サーバファームウェアバンドルに含まれている Intel® から更新されたプロセッサマイクロコードを適用することによって軽減されます。また、該当するベンダーからのオペレーティングシステムとハイパーバイザのパッチも適用されます。 <p>このリリースには、Cisco UCS M3 世代サーバの BIOS 改定が含まれています。これらの BIOS 改定には、CVE-2018-3620 (OS/SMM) および CVE-2018-3646 (VMM) の緩和に必要な、更新されたプロセッサマイクロコードが含まれています。これらの脆弱性を軽減するた</p>

リリース	不具合 ID	CVE	説明
			<p>めに、適切なベンダーからのオペレーティングシステムおよびハイパーバイザパッチも必要になる場合があります。</p> <p>詳細については、次の Cisco セキュリティアドバイザリを参照してください。</p> <p>CPU サイドチャネル情報漏えいの脆弱性: 2018 年 8 月</p>

リリース	不具合 ID	CVE	説明
4.0(1a)	CSCvm03351	CVE-2018-3615 CVE-2018-3620 CVE-2018-3646	

リリース	不具合 ID	CVE	説明
			<p>Cisco UCS B シリーズ M4 サーバ、C シリーズ M4 サーバ、S3260 M4 ストレージサーバ、HyperFlex M4 サーバは、CPU の投機処理とデータキャッシュのタイミングを使用して権限情報を識別するエクスプロイトに対して脆弱です。これらのエクスプロイトは、総称して L1 Terminal Fault (L1TF) と呼ばれています。</p> <ul style="list-style-type: none"> • CVE-2018-3615 (SGX に影響) は Foreshadow と呼ばれ、既存の Cisco UCS サーバに影響を与えます。これは、Cisco UCS M5 および旧世代サーバと、HyperFlex M5 および旧世代サーバは Intel® SGX テクノロジーを使用しないためです。 • CVE-2018-3620 (OS/システム管理モードに影響) および CVE-2018-3646 (仮想マシンモニタに影響) は、Intel® による L1 Terminal Fault 攻撃とも呼ばれます。これらの脆弱性は、サーバファームウェアバンドルに含まれている Intel® から更新されたプロセッサマイクロコードを適用することによって軽減されます。また、該当するベンダーからのオペレーティングシステムとハイパーバイザのパッチも適用されます。 <p>このリリースには、Cisco UCS M4 世代サーバの BIOS 改定が含まれています。これらの BIOS 改定には、CVE-2018-3620 (OS/SMM) および CVE-2018-3646 (VMM) の緩和に必要な、更新されたプロセッサマイクロコードが含まれていま</p>

リリース	不具合 ID	CVE	説明
			<p>す。これらの脆弱性を軽減するために、適切なベンダーからのオペレーティングシステムおよびハイパーバイザパッチも必要になる場合があります。</p> <p>詳細については、次の Cisco セキュリティアドバイザリを参照してください。</p> <p>CPU サイドチャネル情報漏えいの脆弱性: 2018 年 8 月</p>

リリース	不具合 ID	CVE	説明
4.0(1a)	CSCvm03339	CVE-2018-3615 CVE-2018-3620 CVE-2018-3646	

リリース	不具合 ID	CVE	説明
			<p>Cisco UCS B シリーズ M5 サーバ、C シリーズ M5 サーバ、および HyperFlex M5 サーバは、CPU の投機処理とデータ キャッシュのタイミングを使用して権限情報を識別するエクスプロイトに対して脆弱な、Intel[®] プロセッサに基づいています。これらのエクスプロイトは、総称して L1 Terminal Fault (L1TF) と呼ばれています。</p> <ul style="list-style-type: none"> • CVE-2018-3615 (SGX に影響) は Foreshadow とも呼ばれ、既存の Cisco UCS サーバに影響を与えます。これは、Cisco UCS M5 および旧世代サーバと、HyperFlex M5 および旧世代サーバは Intel[®] SGX テクノロジーを使用しないためです。 • CVE-2018-3620 (OS/システム管理モードに影響) および CVE-2018-3646 (仮想マシンモニタに影響) は、Intel[®] による L1 Terminal Fault 攻撃とも呼ばれます。これらの脆弱性は、サーバファームウェアバンドルに含まれている Intel[®] から更新されたプロセッサマイクロコードを適用することによって軽減されます。また、該当するベンダーからのオペレーティングシステムとハイパーバイザのパッチも適用されます。 <p>このリリースには、Cisco UCS M5 世代サーバの BIOS 改定が含まれています。これらの BIOS 改定には、CVE-2018-3620 (OS/SMM) および CVE-2018-3646 (VMM) の緩和に必要な、更新されたプロセッサマイクロコードが含まれていま</p>

リリース	不具合 ID	CVE	説明
			<p>す。これらの脆弱性を軽減するために、適切なベンダーからのオペレーティングシステムおよびハイパーバイザパッチも必要になる場合があります。</p> <p>詳細については、次の Cisco セキュリティアドバイザリを参照してください。</p> <p>CPU サイドチャネル情報漏えいの脆弱性: 2018 年 8 月</p>
4.0(1a)	CSCvg58650	<ul style="list-style-type: none"> • CVE-2017-5718 	<p>Cisco UCS 6200 および 6300 シリーズファブリックインターコネクには、次の一般的な脆弱性および露出 (CVE) ID によって特定された脆弱性の影響を受ける可能性がある、Intel Core プロセッサの Intel システム ファームウェアのバージョンが含まれています。</p> <ul style="list-style-type: none"> • CVE-2017-5718 は、サーバファームウェアバンドルに含まれている Intel から更新されたプロセッサマイクロコードを適用することによって対応されます。また、該当するベンダーからのオペレーティングシステムとハイパーバイザのパッチも適用されます。 <p>このリリースには、脆弱性に対処するための BIOS リビジョンが含まれています。</p>

リリース	不具合 ID	CVE	説明
4.0(1a)	CSCvh25150	CVE-2017-3883	<p>Cisco Firepower Extensible Operating System (FXOS) および NX OS システムソフトウェアの認証、許可、アカウントिंग (AAA) の実装における脆弱性により、認証されていないリモート攻撃者が該当デバイスのリロードを引き起こす可能性があります。</p> <p>この脆弱性は、影響を受けるデバイスがブルートフォースログイン攻撃などの高レートのログイン試行を受信したときに、NXOS システムマネージャがキープアライブメッセージを受信しないようにするために発生します。システムメモリは、同じ条件下で FXOS デバイスの動作が低下する場合があります。これにより、AAA プロセスが予期せず再起動したり、デバイスのリロードが発生したりする可能性があります。</p> <p>攻撃者は、AAA セキュリティサービスを使用して設定されたデバイスに対してブルートフォースログイン攻撃を実行することで、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功した場合、攻撃者は脆弱性の影響を受けるデバイスをリロードさせることができます。</p> <p>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。</p> <p>詳細については、次の Cisco セキュリティアドバイザリを参照してください。</p> <p>Cisco FXOS および NX OS システムソフトウェアの認証、許可、およびアカウントिंगにおけるサービス妨害 (Dos) の脆弱性</p>

リリース	不具合 ID	CVE	説明
4.0(1a)	CSCva61699	<p>Common Weakness Enumeration (CWE) IDs:</p> <ul style="list-style-type: none"> • 525 • 933 • 16 • 311 • 200 	<p>HTTP 応答および影響を受ける Cisco UCS Manager について、次のセキュリティ脆弱性が特定されました。</p> <ul style="list-style-type: none"> • キャッシュ制御およびプラグマ HTTP ヘッダーセットが不完全または設定されていません • Web ブラウザ XSS 保護が有効になっていません • X: Content-type オプションのヘッダーがありません • セキュアなページに混合コンテンツが含まれています • プライベート IP が公開されています <p>これらのセキュリティの脆弱性のうち、Cisco はこのリリースで次の点に対処しています。</p> <ul style="list-style-type: none"> • Web ブラウザ XSS 保護が有効になっていません • X: Content-type オプションのヘッダーがありません <p>またはキャッシュ制御およびプラグマの HTTP ヘッダーセットが不完全または設定されていない場合の脆弱性は、次の理由により修正されません。</p> <ul style="list-style-type: none"> • キャッシングの無効化の結果、GUI のパフォーマンスが低下します • キャッシングを無効にすると、KVM の起動が影響を受けます

リリース	不具合 ID	CVE	説明
4.0(1a)	CSCvi95784	<ul style="list-style-type: none"> • CVE-2017-15715 • CVE-2018-1303 • CVE-2018-1301 • CVE-2018-1302 • CVE-2018-1283 • CVE-2018-1312 • CVE-2017-15710 	以前の Cisco UCS Manager リリースで使用されていた Apache バージョンは、リストされている共通の脆弱性および露出 (CVE) ID の影響を受けていました。これらの CVE ID のほとんどは低リスクであり、Cisco UCS Manager には適用されません。

デフォルトのオープンポート

次の表に、Cisco UCS Manager リリース 4.0 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	使用法
22	CLI	SSH	TCP	UCS 6200 シリーズ UCS 6300 シリーズ UCS 6400 シリーズ	Cisco UCS Manager CLI アクセス
80	XML	HTTP	TCP	UCS 6200 シリーズ UCS 6300 シリーズ UCS 6400 シリーズ	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 6200 シリーズ UCS 6300 シリーズ UCS 6400 シリーズ	Cisco UCS Manager ログインページアクセス Cisco UCS Manager XML API アクセス

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	使用法
743	KVM	HTTP	TCP	UCS 6200 シリーズ UCS 6300 シリーズ UCS 6400 シリーズ	CIMC Web サービス / ダイレクト KVM
843	xmlPolicy	Adobe Flash	[TCP]	UCS 6200 シリーズ UCS 6300 シリーズ	KVM ランチャで使用される Adobe Flash ポート
5661		HTTPD	[TCP]	UCS 6400 シリーズ	内部通信 Cisco UCS Manager リリース 4.0(4f) で無効
7162		HTTPD	[TCP]	UCS 6400 シリーズ	内部通信 Cisco UCS Manager リリース 4.0(4g) で無効
7546	CFS	CFSD	[TCP]	UCS 6400 シリーズ	Cisco ファブリック サービス

Cisco UCS Manager ネットワーク管理ガイドリリース 4.0には、オープン TCP ポートと UDP ポートの完全なリストが用意されています。

Libfabric およびオープン MPI

Libfabric およびオープン MPI オープン ソース パッケージの Cisco usNIC サポートは、コミュニティ web サイト (<http://libfabric.org/> および <http://www.open-mpi.org/> それぞれ) から簡単に利用できます。

Cisco UCS Manager リリース 3.1 (3) 以降のリリースには、オープン MPI バイナリ パッケージは含まれていません。通常の Cisco ソフトウェア チャンネルを介して配布される今後の UCS ソフトウェア ドライババンドルには、libfabric パッケージ用のバイナリが含まれていない可能性があります。Cisco エンジニアは、Libfabric およびオープン MPI コミュニティの両方において引き続きアクティブであり、通常のコミュニティまたは商用の ISV サポート メカニズム (IBM スペクトラム MPI など) を通じて積極的に開発を行い、ユーザーをサポートします。

解決済みの不具合 (p.11)

リリースで解決済みのバグには、[Cisco バグ検索ツール](#)を使用してアクセスできます。この Web ベース ツールから、この製品やその他のシスコハードウェアおよびソフトウェア製品でのバグと脆弱性に関する最新情報を保守する [Cisco バグ追跡システム](#)にアクセスできます。



(注) Cisco Bug Search Tool にログインしてこのツールを使用するには、Cisco.com アカウントが必要です。アカウントがない場合は、[アカウントを登録](#)できます。

Cisco Bug Search Tool の詳細については、[Bug Search Tool \(BST\) ヘルプおよび FAQ](#) を参照してください。

リリースで解決済みの問題 4.0 (4i)

次の問題はリリース 4.0 (4i) で解決済みです。

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
CSCvt55829	<p>下に示す PID の SanDisk Lightning II ソリッドステートドライブ (SSD) LT0400MO および LT1600MO は、40,000 時間正常に動作した後、利用可能な残りストレージスペースが 0 GB であると報告するようになります。電源サイクルイベントの後に、SSD はオフラインになって使用できなくなり、データ損失が発生します。また、サービス作業で同時に複数のドライブを取り付けていた場合には、すべてのドライブでそうなる可能性があります。</p> <p>この問題の影響を受ける SSD の PID は、次の通りです。</p> <ul style="list-style-type: none"> • (400GB) UCS-SD400G1KHY-EP、UCS-SD400G12S4-EP、UCS-C3X60-12G240 • (1.6TB) UCS-SD16TG1KHY-EP、UCS-SD16TB12S4-EP、UCS-C3X60-12G2160 <p>この問題は解決されました。</p>	3.2(1d)C	4.0 (4i)C

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
CSCvt37895	ファブリックエクステンダを介してファブリックインターコネクに接続されている Cisco C シリーズ統合サーバは、クラスタのフェールオーバーまたはシャロー ディスカバリ中に、ファブリックポートのリンクフラップを検出します。 この問題は解決されました。	4.0 (4e)A	4.0 (4i)A
CSCvq80554	Cisco モデル M4 サーバでは、BMC が HCL ファイル変更の通知を送信できませんでした。 この問題は解決されました。	4.0 (1c) A	4.0 (4i)A
CSCvs61735	UCS Manager は、Cisco 6400 シリーズファブリック インターコネクの IOM の全体的なステータスを正確には提供しませんでした。 この問題は解決されました。	4.0(1a)A	4.0 (4i)A
CSCvm59040	VIC 1225 アダプタが搭載された Cisco スタンドアロン C シリーズサーバ上のホストでは、180日以上稼働時間の経過後に、メモリ不足が発生して、ネットワーク接続が失われることがあります。 この問題は解決されました。	4.0(1a)B および C	4.0 (4i)B および C
CSCvt27869	6200 シリーズファブリック インターコネクで OOB メモリアクセスが検出され、ファブリックインターコネクが再起動します。 この問題は解決されました。	4.0(1a)A	4.0 (4i)A
CSCvt08435	6300 シリーズファブリック インターコネクでは、IOM 2304 で SNMP をモニタしている間、HIF ポート数が断続的にゼロに低下し、サードパーティのモニタリングアプリケーションはトラフィックが高いと報告されます。	4.0(4b)A	4.0 (4i)A

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
CSCvu07675	UCS 管理型の統合 C シリーズラックサーバへのファームウェアの自動インストールは、SAS コントローラのアクティブ化に失敗しました。	4.0(4b)C	4.0 (4i)C
CSCvt65210	1400 シリーズ ファブリック インターコネクトでは、アップリンク ポートのフラップ中に vif_vifid_reserve が失敗しました。	4.0 (4h)A	4.0 (4i)A
CSCvs46320	6400 ファブリックインターコネクトに接続されている UCS サーバは、UCS Manager で設定された時間やタイムゾーンとの同期を失うことがあります。	4.0(1a)A	4.0 (4i)A
CSCvu14656	BIOS を次のいずれかのバージョンにアップグレードすると、M5 サーバの起動が、メモリ テストの手順で停止します。 <ul style="list-style-type: none"> • C220M5.4.1.1c.0.0404202345 • C240M5.4.1.1c.0.0405200025 • B200M5.4.1.1c.0.0404202345 	4.0 (4h)C	4.0 (4i)C
CSCvu16418	Cisco UCS Manager 4.0 (4g) ファームウェアを実行している Cisco UCS 6400 シリーズファブリックインターコネクトでは、アップストリーム MDS でカーネルパニックが発生しても、UCS ファイバチャネル (FC) ポートはオンラインのままになります。構成によっては、この状況により、MDS が動作不能であっても UCS FC アップリンクがオンラインのままになることがあります。これにより、ピン接続された vHBA が起動したままになり、OS が FC インターフェイスが正しく機能していないことを認識できなくなります。 この問題は解決されました。	4.0 (4g)A	4.0 (4i)A

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
CSCvt29474	<p>ファイバチャネル (FC) ストレージユニットに直接接続されたスイッチドモードの Cisco UCS 6332-16UP ファブリックインターコネクト (FI) では、FC インターフェイスの多数のリンクリセット (LR) またはリンクリセット応答 (LRR) により、任意の FI リンクが使用できなくなります。</p> <p>この問題は解決されました。</p>	4.0(2a)A	4.0 (4i)A
CSCvt44506	<p>Cisco UCS Manager は、グラフィック処理ユニット (GPU) カードの複数のデルタイベントを受信します。</p> <p>この問題は解決されました。</p>	4.0 (4h)C	4.0 (4i)C
CSCvs35747	<p>まれに、6300 シリーズ ファブリック インターコネクトの FC アップリンク接続とクレジットが失われると、FC ポートでのトラブルシューティングに必要なポート/リンク/速度 FSM 情報などの重要な情報が失われることがあります。</p> <p>FC ポートの問題のロギングが拡張され、fc-mac 出力にポート/リンク/速度 FSM 情報が表示されるようになりました。</p>	4.0(1b) A	4.0 (4i)A
CSCvt38091	<p>Cisco UCS Manager リリース 4.0 (4e) にアップグレードした後、B200-M5 ブレードサーバに次のようなメッセージが表示されました。</p> <p>モデル名 UCS-FI-6332-16UP のホスト名が、診断テストの失敗を報告しました。</p> <p>「回復済み：サーバ 1/6 (サービス プロファイル：(プロファイル名) アクセス不能)」</p> <p>この問題は解決されました。</p>	4.0 (4e)B	4.0 (4i)B

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
CSCvs97236	<p>C460 M4C シリーズラックサーバがパトリールスクラブ中に修正不能な ECC エラーを検出すると、切り捨てられたシステムアドレス (4 KB ページ境界) をマシンチェックバンクに記録します。iMC Demand Scrubber が修正不能な ECC エラーを検出すると、完全な「キャッシュライン」(切り捨てられていない) アドレスをマシンチェックバンクに記録します。</p> <p>この切り捨てられたメモリアドレスは、アドレスを物理 DIMM に転送変換するために使用されます。システムの装着状況と構成によっては、修正不能な ECC エラーを記録する SEL メッセージが正しい DIMM を指していない可能性があります。</p> <p>この問題は解決されました。</p> <p>デマンドスクラブ中に検出された修正不能な ECC エラーは、物理 DIMM に正しく変換されます。</p>	4.0 (4h)C	4.0 (4i)C
CSCvs73313	<p>Cisco UCS M5 サーバを長期にわたって使用した場合、bladeAG プロセスがクラッシュし、サーバでシャローディスクバリがトリガされることがあります。この条件は、内部メモリーリークのために発生します。</p> <p>この問題は解決されました。</p>	4.0(4a)A	4.0 (4i)A

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
CSCvt64871	<p>Cisco UCS C480 M5 サーバおよび Cisco UCS 480 M5 ML サーバでは、ADDDC 仮想ロックステップをアクティブ化した後、まれに応答が停止して、再起動する場合があります。これにより、メモリシステムの #IERR と M2M タイムアウトが発生します。</p> <p>詳細については、以下を参照してください。</p> <ul style="list-style-type: none"> • Intel® Xeon® Processor Scalable Family Specification Update (エラッタ > SKX108) • Second Generation Intel® Xeon® Scalable Processors Specification Update (Errata -CLX37) (エラッタ > CLX37) 	4.0 (4c)B	4.0 (4i)B
CSCvu11155	<p>BIOS を次のいずれかのバージョンにアップグレードすると、第2世代 Intel® Xeon® スケーラブルプロセッサを搭載した Cisco UCS B シリーズ、C シリーズ、および S シリーズ M5 サーバでパフォーマンスが低下する可能性があります。</p> <ul style="list-style-type: none"> • C240M5.4.0.4r.0.0305200743 • C220M5.4.0.4p.0.0224200755 • B200M5.4.0.4l.0.0305202307 • B480M5.4.0.4m.0.0305202307 • S3X60M5.4.0.4o.0.0224200755 	4.0 (4h)B および C	4.0 (4i)B および C
CSCvq53066	<p>Cisco UCS Manager 4.0(2d) から Cisco UCS Manager 4.0(4b) へのファームウェアの自動アップグレード中に、統合ラックサーバの SAS コントローラ ファームウェアがアクティブになりません。</p>	4.0(4b)	4.0 (4i)

リリースで解決済みの問題 4.0 (4h)

次の問題はリリース 4.0 (4h) で解決済みです。

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
CSCvr83759	UCS Manager 3.2(3c) から 4.0(4c) にアップグレードした後、openSSH または SecureCRT を「パスワード」認証で使用すると、UCS Manager ファブリック インターコネクタへのブレードサーバアクセスが失敗します。 この問題は解決されました。	4.0(1a)A	4.0 (4h)A
CSCvr98210	アプライアンス ポートまたは FCoE ストレージポートを搭載したシステムで Cisco UCS Manager リリース 3.2 からリリース 4.0 以降にアップグレードする場合、LLDP はデフォルトで無効になります。FCoE または LLDP を必要とする接続は、動作を停止する可能性があります。 この問題は解決されました。	4.0(4b)A	4.0 (4h)A
CSCvr91399	次の BIOS トークンは、Cisco UCS Central から UCS Manager にプッシュされるときに、プラットフォームのデフォルトにリセットされます。 SelectMemoryRASConfiguration LocalX2Apic BMEDMAMitigation この問題は解決されました。	4.0(1a)A	4.0 (4h)A
CSCvq76790	Cisco IMC またはファブリック インターコネクタのファームウェアアップグレード後、物理レイヤ1の問題またはファイバチャネルポートのポートモードの設定ミスが原因で、Cisco IMC とファブリック インターコネクタ間の接続が失われます。 この問題は解決されました。	4.0(2b)A	4.0 (4h)A

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
CSCvr74792	<p>Cisco UCS Manager リリース 4.0(2d) で動作している Cisco UCS 6454 ファブリック インターコネクトは、カーネルのパニックとウォッチドッグタイマーのタイムアウトによりリブートされます。これは、PSU ファン データのアクセスにより、カーネルのスピンロックが生じて発生します。</p> <p>この問題は解決されました。</p>	4.0(1a)A	4.0 (4h)A
CSCvr95365	<p>Cisco UCS Manager リリース 4.0(1a) からリリース 4.0(4b) へのファームウェアアップグレード後、Cisco 12G モジュラ SAS HBA コントローラを搭載した Cisco UCS C240 M5 サーバの検出は、次のエラーで失敗します。</p> <p>mc_attrib_set_suboem_id は SubOEM ID を設定できませんでした</p> <p>この問題は解決されました。</p>	4.0(4a)C	4.0 (4h)A
CSCvp71363	<p>VIC 1457 アダプタを搭載した UCS C240 M5 サーバが、UCS ファブリック インターコネクトとの直接接続連携を介して Cisco UCS Manager によって管理されているシステムでは、次の障害が未使用ポートまたは未接続ポートに表示されます。</p> <p>アダプタ アップリンク インターフェイス x/y/z リンク ステート: 使用できません。Please verify connectivity to Fabric Interconnect. シャーシの確認が必要な場合があります。</p> <p>この問題は解決されました。</p>	4.0(2d)A	4.0 (4h)A

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
CSCvr15733	<p>負荷の下では、MLOM-UCSC-MLOM-C25Q-04-04 バージョン 4.0(4b) を動作させている Cisco vNIC 1400 シリーズは、レート制限のシャットオフに関する既知の問題が原因で永続的に停止します。</p> <p>この問題は解決されました。</p>	4.0(1a)B	4.0 (4h)A
CSCvs35789	<p>UCS 6454 ファブリック インターコネクタにフェールオーバーが発生すると、HIF ポートがダウンして、トラフィックがしばらくの間中断します。したがって、ファブリック インターコネクタを再起動すると、接続を回復させるためにさらに時間がかかります。</p> <p>平均遅延が減少します。</p>	4.0 (4c)A	4.0 (4h)A
CSCvs63073	<p>QoS スクリプトの実行中、Cisco UCS 6400 シリーズのファブリック インターコネクタは、スピンロックの状態が発生したシステムウォッチドッグのタイムアウトによりクラッシュします。</p> <p>システム ウォッチドッグのタイムアウトの原因になったスピンドアウン状態は、解決されました。</p>	4.0(1a)A	4.0 (4h)A
CSCvr46327	<p>UCS 2208 IOM を UCS 2408 IOM で置き換えると、仮想イーサネット インターフェイスは使用できなくなります。仮想イーサネット インターフェイスは、<code>show interface virtual</code> ステータス コマンドの出力では利用できませんが、NXOS の <code>show interface brief</code> コマンドの出力では使用できます。</p> <p>この問題は解決されました。</p>	4.0 (4d)A	4.0 (4h)A

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
CSCvs51200	<p>Cisco UCS C シリーズ M5 サーバでは、次の条件下で UEFI ブート LUN が機能しなくなります。</p> <ul style="list-style-type: none"> • OS が ESXi リリース 6.0 アップデート 3 または 6.5 アップデート 1 の場合 • IQN がプロファイルレベルで定義されている場合 • 少なくとも 1 つの iSCSI vNIC が複数のターゲットでブートするように設定されている場合 <p>この問題は解決されました。</p>	4.0 (4f)A	4.0 (4h)A
CSCvr79388	<p>Cisco UCS Intel® プロセッサ ベース M5 サーバでは、ADDDC 仮想ロックステップをアクティブ化した後、まれに応答が停止して、再起動する場合があります。これにより、メモリ システムの #IERR と M2M タイムアウトが発生します。</p> <p>詳細については、以下を参照してください。</p> <ul style="list-style-type: none"> • Intel® Xeon® Processor Scalable Family Specification Update (エラッタ > SKX108) • Second Generation Intel® Xeon® Scalable Processors Specification Update (エラッタ > CLX37) <p>(注) この問題は、Cisco UCS C480 M5 および Cisco UCS 480 M5 ML サーバでも引き続き発生します。詳細については、「リリースで未解決の問題 4.0 (4h)」セクションの「CSCvt64871」を参照してください。</p>	4.0 (4c)B	4.0 (4h)B

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
CSCvr79396	<p>Cisco UCS M5 サーバでは、仮想ロックステップ (VLS) のスペアリングコピーが早期に終了して、ロックステップ領域で誤った値が導き出されます。</p> <p>この問題は解決されました。</p>	4.0 (4e)B	4.0 (4h)B
CSCvs25524	<p>Cisco UCS 6300 シリーズファブリックインターコネクタでは、VDC デバッグログによって一時ディレクトリがいっぱいになるため、次のメッセージがコンソールログに表示されます。</p> <pre>FI6332-DC3-A %SYSMGR-2-TMP_DIR_FULL: システムの一時ディレクトリの使用率が予期せずに 80% を超えました (System temporary directory usage is unexpectedly high at 80%)</pre> <p>この問題は解決されました。</p>	4.0(4b)A	4.0 (4h)A
CSCvs88880	<p>Cisco VIC 1455/1457/1495/1497 アダプタの電源が入ったままの状態、スタンドアロン Cisco IMC または Cisco UCS Manager の管理課にある C シリーズサーバをリブートした場合、次のようになります。</p> <ul style="list-style-type: none"> • Cisco IMC では、VIC アダプタを管理したり、アダプタ設定を表示/変更したりすることができなくなる可能性があります。 • Cisco VIC 1455/1457/1495/1497 アダプタを使用して cisco IMC と Cisco UCSM の間を接続すると、Cisco UCS Manager が Cisco IMC との接続を失う可能性があります。 	4.0(1a)	4.0 (4h)A

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
CSCvr70687	<p>新しい Cisco UCS C240 M5 サーバは検出に失敗するか、次のエラーメッセージを表示して応答しなくなります。</p> <pre>CimcVMedia Error: Error retrieving vmedia attributes list-MC Error(-6)</pre> <p>この同じ問題は、FIの再起動またはアップグレード後、すべての Cisco UCS C240 M5 サーバで発生することがあります。</p> <p>この問題は解決されました。</p>	4.0 (4d)A	4.0 (4h)A

リリースで解決済みの問題 4.0 (4g)

次の問題はリリース 4.0 (4g) で解決済みです。

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
CSCvr43466	<p>Cisco UCS B シリーズおよび C シリーズ M5 サーバに連携されている Cisco UCS Manager は、ハードウェアが変更されていない場合でも次のハードウェアインベントリの不一致の障害を報告しました。</p> <p>ハードウェア インベントリの不一致</p> <p>この問題は解決されました。</p>	4.0(4b)B	4.0 (4g)B
CSCvr67027	<p>Cisco UCS Manager の Red Hat Linux を、UCS-C3K-M4RAID RAID RAID コントローラを搭載した S3260 M4 ラックサーバを統合してアップグレードすると、ブートドライブが動作しなくなります。</p> <p>この問題は解決されました。</p>	3.2(3k)C	4.0 (4g)C

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
CSCvo49554	ブレードサーバが UCS 6332 ファブリック インターコネクットのポート 27 ~ 32、または UCS 6332-16UP ファブリック インターコネクットのポート 35 ~ 40 に接続されている場合、ファブリック インターコネクットのレポート中に多数の ping が失われます。 この問題は解決されました。	4.0(1a)A	4.0 (4g)A
CSCvj70519	ポート 7162 は、UCS Central に登録されている場合にのみ使用でき、6400 シリーズファブリック インターコネクットでオープンしていました。このポートは現在閉じています。	4.0(1a)A	4.0 (4g)A
CSCvs25058	UCS 6454 ファブリック インターコネクットは、サーバの各 vNIC が同一の vntag を使用していた場合に、31 番目にローカル接続された UCS ラックサーバ後に検出されたサーバのペア間でトラフィックを切り替えることができませんでした。その結果、通信していた vNIC が同じ vntag を持つ場合、後でサーバが相互に通信できなくなることが判明しました。ファブリック インターコネクットにピン留めされた vNIC 間など、ファブリック内でスイッチングされたトラフィックのみが影響を受けます。 この問題は解決されました。	4.0(4f)A	4.0 (4g)A
CSCvr06387	UCS 6324 ファブリック インターコネクットの SNMP プロセスが繰り返しクラッシュしました。 この問題は解決されました。	4.0(1a)A	4.0 (4g)A

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
CSCvq37888	UCSM4 ブレードサーバでは、Cisco IMC のメモリが不足したときに、Cisco UCS マネージャと Cisco IMC 間の接続が失われました。ブレードサーバの取り付けが回復するまで、接続を復元できませんでした。 この問題は解決されました。	4.0(1a)B および C	4.0 (4g)B および C
CSCvr78701	Cisco UCS Manager 統合 C220 M5 ラックサーバでは、Cisco UCS Manager のアクティベーション中に Cisco IMC カーネルパニックが発生しました。 この問題は解決されました。	4.0 (4c) C	4.0 (4g)C

リリースで解決済みの問題 4.0 (4f)

次の問題はリリース 4.0 (4f) で解決済みです。

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
CSCvr01259	UCS 2408 に接続されている UCS 6400 シリーズファブリックインターコネクタでは、仮想イーサネットのカウンタに正しいパケット数が示されていても、HIF ポート インターフェイスカウンタはファブリックインターコネクタで更新されませんでした。 この問題は解決されました。	4.0 (4e)A	4.0 (4f)A
CSCvq92352	非常にまれなケースで、接続された FEX からの長さフィールドが破損したメッセージをファブリックインターコネクタの <code>fwm</code> プロセスで受信した場合、ファブリックインターコネクタの再起動がトリガされました。 この問題は解決されました。	2.2 (8f) A	4.0 (4f)A

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
CSCvq57262	RDMA が有効になっている UCS 6454 ファブリック インターコネクットの A バンドルアップグレード中に、ラックサーバの 1 つが保留中のリポート確認応答を示しました。 この問題は解決されました。	4.0(4b)A	4.0 (4f)A
CSCvp52336	UCS 6454 ファブリック インターコネクトは、初期設定時に DHCP IP アドレスを受信できませんでした。 この問題は解決されました。	4.0 (2d) A	4.0 (4f)A
CSCvq51008	単一のアダプタ上の UCS B460 M4 ブレードサーバが、vCon を配置するためのアダプタを見つけられませんでした。これにより関連付けが妨げられ、エラーメッセージ「十分なリソースがと接続配置がないため設定に失敗しました。」が表示されます。 この問題は解決されました。	4.0(4b)A と B	4.0 (4f)A と B
CSCvr35735	vNICs がファブリック インターコネクトにピン接続されている場合、UCS 6454 ファブリック インターコネクトは、UCS ラックサーバのペア間のトラフィックを切り替えることができませんでた。 この問題は解決されました。	4.0(4b)A	4.0 (4f)A
CSCvq98090	6454 ファブリック インターコネクトの SAN パスは、ファブリック インターコネクトの電源が再投入されるとオフラインになります。 この問題は解決されました。	4.0(4b)A	4.0 (4f)A
CSCvr47266	UCS 6248 ファブリック インターコネクトから UCS 6454 ファブリック インターコネクトへの移行中に、UCM 2208 IOM がサイレントに失敗しました。 この問題は解決されました。	4.0(4b)A	4.0 (4f)A

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
CSCvr34407	UCSM4 および M5 ラックサーバ上の UCS 6300 シリーズファブリックインターコネクトは、Cisco UCS Manager からの有効/無効操作後に VLAN 設定を失いました。 この問題は解決されました。	4.0(4b)A	4.0 (4f)A
CSCvq90219	Cisco UCS Manager 3.2 (3k) から UCS Manager 4.0(4d) への手動アップグレード中に、Cisco UCS 6200 シリーズファブリックインターコネクトを搭載したブレードサーバで Cisco UCS Manager のアクティブ化が失敗しました。 この問題は解決されました。	4.0 (4d) A	4.0 (4f)A
CSCvr40744	UCS 6454 ファブリック インターコネクトのポート 5661 および 7546 が開きました。 ポート 5661 と 7546 が無効になりました。	4.0 (4d)A	4.0 (4f)A
CSCvr67352	UCS 6454 ファブリック インターコネクトを使用するブレードサーバおよびラックサーバ上の管理インスタンスは、IO モジュールまたは FEX がリブートされた場合や、ファブリックインターコネクトの 1 つが到達不能になった場合など、特定の条件下で OOB KVM 接続にアクセスできなくなりました。 この問題は解決されました。	4.0 (4e)A	4.0 (4f)A
CSCvn49417	UCS 6454 ファブリック インターコネクトの電源をオンにして初期設定ダイアログ画面を起動すると、ネットワークアップリンクがすぐにオンラインになり、まれにブロードキャストストームが発生する可能性があります。 この問題は解決されました。	4.0 (1a) A	4.0 (4f)A

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
CSCvr68316	スタンドアロンCシリーズサーバでは、VICとスイッチ側の両方でポートチャネルが有効になっているスイッチに UCS VIC 1455/1457 アダプタが接続されている場合、イーサネットおよびファイバチャネルのデータパスは機能しませんでした。	4.0 (4e)C	4.0 (4f)C

リリースで解決済みの問題 4.0 (4e)

次の問題はリリース 4.0 (4e) で解決済みです。

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
CSCvh87378	コミュニティ VLAN 内のサーバは、プライマリ VLAN のサーバが UCS ドメインに存在するとき、Cisco UCS Manager リリース3.2.(2b) またはそれ以降のリリースにアップグレード後にプライマリ VLAN と通信できませんでした。 この問題は解決されました。	3.2(2b)A	4.0 (4e)A
CSCvr08327	UCS 2204 または UCS 2208 ファブリック エクステンダを使用していたブレードシャーシ上の PSU は、ファブリック エクステンダファームウェアのアップグレード中に温度障害によってシャットダウンされました。PSU は再装着されるまで、その後に電源をオンにできませんでした。 この問題は解決されました。	4.0(1d)B	4.0 (4e)B
CSCvq43680	FCPC ハイアベイラビリティ ポリシー (HAP) のリセットにより、ファブリック インターコネクタがランダムにリポートされます。 この問題は解決されました。	4.0(2b)A	4.0 (4e)A

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
CSCvq71404	6400 シリーズ ファブリック インターコネクトを搭載したブレードサーバおよびラックサーバの直接 KVM IP へのアクセスは、Cisco UCS Manager ドメインにリダイレクトされています。 この問題は解決されました。	4.0(2d)A	4.0 (4e)A
CSCvp45607	選択した Cisco UCS Manager ユーザーが現在のユーザーのアクティビティを表示し、すべてを確認すると、あらゆる影響を把握することなく、すべてのユーザーからのレポートを保留した状態で中のすべてのサーバがレポートされます。 [今すぐ確認する (Acknowledge All)] を選択すると、現在のユーザーのアクティビティが自動的に非アクティブになり、レポートの影響を完全に可視化できます。	3.2(3e)A	4.0 (4e)A
CSCvr11045	Cisco IMC Web サービスが無効になっている場合、TCP ポート 81 および 743 は UCS 6454 ファブリック インターコネクトでアクセス可能でした。 この問題は解決されました。	4.0(4b)A	4.0 (4e)A
CSCvr07248	Cisco UCS Manager GUI では、[機器 (Equipment)] > [ポリシー (Policies)] > [電源グループ (Power Groups)] に移動すると、[全般 (General)] タブにのみ情報が示されます。シャーシ、ラックユニット、fex、FI、障害、およびイベントのタブには情報が表示されませんでした。 この問題は解決されました。	4.0(4a)A	4.0 (4e)A

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
CSCvq82024	BIOS メニューのセットアップ項目「AEP エラー インジェクション」が有効になっている場合、エラーが永続メモリデバイスにインジェクトされ、purple screen of death (PSOD) 生成が発生します。オペレーティング システムに通知されなかったため、マシンチェック例外 (MCE) が正しく処理されませんでした。 この問題は解決されました。	4.0(4b)B	4.0 (4e)B

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
CSCvr04369	<p>まれに特定の条件下で、Cisco UCS 14xx アダプタカードのイーサネットポートと接続されたスイッチポートのリンクステータスが、複数回起動できませんでした。これは、イーサネットリンク トレーニング プロトコルを使用しない設定で、VIC アダプタのイーサネット SERDES コンポーネントによって受信されたアナログ電気信号の品質が低いためです。この問題は、次の条件が存在する場合に発生します。</p> <ul style="list-style-type: none"> • Cisco VIC 14xx アダプタ カード インスタンスおよびポート インスタンス: <ul style="list-style-type: none"> • Cisco UCS VIC 1455 • Cisco UCS VIC 1457 • Cisco UCS VIC 1495 • Cisco UCS VIC 1497 • イーサネット自動ネゴシエーション プロトコルを使用しないトランシーバ モジュール インスタンス: <ul style="list-style-type: none"> • 10G CU • 10G Optical • 25G CU • 25G Optical • 40G Optical • 100G Optical • その他可能性のある環境条件。 <p>この問題は解決されました。</p>	4.0(4a)C	4.0 (4e)C

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
CSCvn77341	ボックス内の ndctl ツールを使用して Red Hat Enterprise Linux 7.6 で作成された名前スペースは、BIOS セットアップまたは UEFI IPMCTL ツールで検査されたときに名前スペースが健全であっても「Critical」ヘルス状態と表示されます。 この問題は解決されました。	4.0(4a)B および C	4.0 (4e)B および C
CSCvn81521	Intel® Optane™ データセンターの永続メモリモジュールが 2LM (メモリモード) であるシステムでは、同じチャネル上の DDR4 DIMM (近メモリとして設定されている) でエラーが発生した場合、修正不可能なエラーが永続メモリモジュールに記録されます。 この問題は解決されました。	4.0(4a)B および C	4.0 (4e)B および C

リリースで解決済みの問題 4.0 (4d)

次の問題はリリース 4.0 (4d) で解決済みです。

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
CSCvq26156	UCS C-Series サーバから 4.0(4c) C-Bundle へアップグレードすると、Cisco 12G Modular SAS HBA により一部の Intel S4500 ディスクドライブの検出/通信が停止されます。これにより、これらのドライブのソフトウェアアップグレードが失敗します。 この問題は解決されました。 (注) Cisco HyperFlex は UCS Manager 4.0(4a)、4.0(4b) または 4.0(4c) をサポートしません。	4.0(4a)C	4.0 (4d)A
CSCvq38756	まれに、UCS クラスタで NIC チーミングが設定されている場合、ファブリックインターコネクタがリロードされると、一時的なトラフィック損失が発生します。 この問題は解決されました。	4.0(4b) A	4.0 (4d)A

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
CSCvq84120	ファブリック インターコネク트가リブートすると、時折 vNICs の障害が発生し、intermittant トラフィックが失われることがあります。 この問題は解決されました。	4.0(4b) A	4.0 (4d)A

リリースで解決済みの問題 4.0 (4c)

次の問題はリリース 4.0 (4c) で解決済みです。

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
CSCvp31766	ブレードサーバをアップグレードする場合、VMFEX インターフェイスを使用していた VM は接続を失います。 この問題は解決されました。	4.0(4a)B	4.0 (4c)B
CSCvo99427	Cisco UCS Central をリリース 2.0 (1h) にアップグレードすると、一部の UCS ドメインの可視性が失われました。Cisco UCS Central から可視性が失われた Cisco UCS Manager ドメインへの接続テストを実行すると、接続は成功しても、警告メッセージが表示されます。 この問題は解決されました。	4.0(4a) C	4.0 (4c)A
CSCvp89594	接続中に UCS 6454 ファブリック インターコネク트의一方の側が応答なくなり、ssh セッション中に NX OS に接続できませんでした。 この問題は解決されました。	3.2(1d)A	4.0 (4c)A
CSCvo06391	UCS C125 M5 および C480 M5 サーバの検出が「Discover BMC Preconfig Pnu OS Peer」で失敗しました。 UCS VIC アダプタのイーサネット インターフェイスには、物理リンク ステータスがダウン状態か、イーサネット PC プロトコルエラーとして示されています。 この問題は解決されました。	4.0(4a)A	4.0 (4c)A

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
CSCvo18110	リンクフラップが発生したネームスペースへのファイバチャネル NVMe インターフェイスのパスが失われました。 この問題は解決されました。	4.0(4a)A	4.0 (4c)A
CSCvq28261	UCS 6324 ファブリック インターコネクトを搭載した UCS 2304 ファブリック エクステンダを使用していたブレードシャーシ上の PSU は、ファブリック エクステンダファームウェアのアップグレード中に温度障害によってシャットダウンされました。PSU は再装着されるまで、その後に電源をオンにできませんでした。 この問題は解決されました。	4.0(1d)B	4.0 (4c)B
CSCvo48003	M4 サーバでは、Patrol スクラブ中に修正不可能な ECC エラーが検出されます。CPU IMC (統合メモリ コントローラ) の Patrol Scrubber が修正不可能な ECC エラーを検出すると、切り捨てられた DIMM アドレス (4 KB ページ境界) をマシンチェック バンクに記録します。 この問題は解決されました。	4.0(4a) B	4.0 (4c) B
CSCvp31749	BMC CPU 温度しきい値 (IPMI) は、Intel Speed Select 設定が変更されたときに調整されるようになります。	4.0(4a)B	4.0 (4c)B
CSCvo32597	Cisco UCS Manager は、UCS 5108 シャーシのプラチナ II AC 電源モジュールの IOM から正しいセンサーの読み取り値を受信していませんでした。 この問題は解決されました。	4.0(4b)B	4.0 (4c)B
CSCvq17624	Cisco UCS Manager では、UCS IOM 2408 を搭載した UCS 5108 シャーシから PSU が取り外された場合、古い電源装置 (PSU) データはクリアされません。 この問題は解決されました。	4.0(4b)A	4.0 (4c)A

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
CSCvq29766	6400シリーズファブリックインターコネクトを搭載した UCS Manager マネージドシステムでは、Cisco UCS Central が KVM コンソールを起動できるようになりました。	4.0(4b)A	4.0 (4c)A
CSCvq49222	2 個の 25GE インターフェイスによって 6454 ファブリック インターコネクトに直接接続された VIC 1455 または 1457 インターフェイスカードを搭載した UCS C220 M5 サーバ上ガリブートされると、オペレーティング システムはステータスをダウンとして検出します。 この問題は解決されました。	4.0(4b)A	4.0 (4c)A
CSCvo78920	Intel® Optane™ データセンターの永続メモリ モジュールが搭載されたシステムが起動した場合、場合によっては、永続メモリ モジュールが「機能していない」のヘルス状態になることがあります。 リリースで更新された Intel ファームウェアで解決 4.0 (4c)	4.0(4a)B、C	4.0 (4c)B、C
CSCvp38545	Intel® Optane™ データセンター永続メモリ モジュールは、HiBit DIMM を使用しているチャンバーでテストされたときに「機能しない」ヘルス状態になります。AC 電源の再投入により、障害が発生した永続メモリ モジュールが「致命的な障害」状態になります。 リリースで更新された Intel ファームウェアで解決 4.0 (4c)	4.0(4a)B、C	4.0 (4c)B、C
CSCvp38555	最初の電源投入時に、Intel® Optane™ データセンターの永続メモリ モジュールは、「機能していない」ヘルス状態に移行します。 リリースで更新された Intel ファームウェアで解決 4.0 (4c)	4.0(4a)B、C	4.0 (4c)B、C

リリースで解決済みの問題 4.0(4b)

次の問題はリリース 4.0(4b) で解決済みです。

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
CSCvp40415	<p>Cisco UCS Manager 4.0(4a)にアップグレードすると、サービスプロファイルの関連付け中に、M5 サーバで「永続メモリ設定が一致しません」という警告が表示されます。</p> <p>この問題による機能への影響はありません。関連付けは問題なく完了し、インストールされている場合は、サーバはホスト OS で正常に起動します。</p> <p>この問題は解決されました。警告は表示されません。</p>	4.0(4a)A	4.0(4b)A
CSCvp68182	<p>リリース 3.2 (3j) より前の Cisco UCS Manager リリースから Cisco UCS Manager リリース 4.0 (4a) にアップグレードするか、Cisco UCS Manager リリース 4.0 (1a)、4.0 (1b)、または 4.0 (1c) から Cisco UCS Manager リリース 4.0 (4a) にアップグレードすると、Cisco UCS B200 M5、B480 M5、および S3260 M5 サーバの小規模なサブセットが発生し、BMC への IOM 接続をアクティブ化したり、損失したりしません。</p> <p>この問題は解決されました。</p>	4.0(4a) B および C	4.0(4b) B および C
CSCvn64815	<p>Cisco UCS Manager と統合され、4 個以上の PCI アダプタ (mLOM を含む) が搭載された Cisco UCS C シリーズ サーバを搭載したセットアップでは、Cisco UCS Manager には、インベントリに 4 個のアダプタのみが表示されていました。この問題は解決され、Cisco UCS Manager はインベントリ内のすべてのアダプタを表示するようになりました。</p>	3.2(1d)A	4.0(4b)A
CSCvp23760	<p>Cisco UCS C シリーズ サーバを搭載したセットアップで Cisco UCS Manager リリース 4.0 (4a) にアップグレードすると、Qlogic アダプタの 1 個のポートが接続解除済みとして示されます。この問題は解決され、両方のポートが接続されます。</p>	4.0(4a)C	4.0(4b)C

リリースで解決済みの問題 4.0(4a)

次の問題はリリース 4.0(4a) で解決済みです。

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
CSCvm66006	<p>サービス プロファイルの再設定と再関連付けが完了すると、hifpc メンバのいずれかにハッシュされたトラフィックがドロップされます。これは、DCBX がブレードサーバの影響を受けるインターフェイスで正しく収束しなかった場合に発生します。</p> <p>この問題は解決されました。現在、ファブリック インターコネク トは正しい DCBX ピア ACK をチェックするようになりました。</p>	4.0 (1a) A	4.0(4a)A
CSCvn66725	<p>UCS 6454 ファブリック インターコネク トに接続されている UCS M4 サーバ上で、リモートキー管理相互運用性プロトコル(KMIP)サーバを使用して、自己暗号化ドライブ (SEDs) のドライブセキュリティを有効にしようとしたときに、サービス プロファイルの関連付けが「セッションの作成に失敗しました-要求された操作のタイムアウト」というエラーメッセージで失敗しました。</p> <p>この問題は解決されました。</p>	4.0 (1c) B	4.0(4a)B
CSCvn57345	<p>Cisco Intersight で設定、登録、要求、および接続された UCS デバイスの Cisco UCS Manager フルステート バックアップ ファイルを復元した後、デバイスは Cisco Intersight で接続解除済みとして表示されます。</p> <p>この問題は解決されました。Cisco UCS Manager のフルステート バックアップには、デバイス コネクタ情報はありません。デバイスは、消去設定を実行した後に回収され、完全な状態のバックアップから復元する必要があります。</p>	4.0 (2a) A	4.0(4a)A

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
CSCvo58393	<p>Cisco UCS Manager リリース4.0 にアップグレードした後、FCoEポートチャネルが起動せず、メンバリンクが管理者としてダウンしていることを示しています。次のエラーが表示されました。</p> <pre>Severity: Critical Code: F999676 Last Transition Time: 2019-02-26T03:19:45.668 ID: 23387272 Status: None Description: [FSM:FAILED]: Uplink fc port configuration on B (FSM:sam:dme:SwFcSanBorderDeploy) . Remote-Invocation-Error: [FSM:STAGE:REMOTE-ERROR]: Result: service-unavailable Code: unspecified Message: (sam:dme:SwFcSanBorderDeploy:UpdateConnectivity) Affected Object: sys/switch-B/border-fc Name: Fsm Sam Dme Sw Fc San Border Deploy Fsm Fail Cause: Fsm Failed</pre> <p>この問題は解決されました。</p>	4.0(2a)A	4.0(4a)A
CSCvo64592	<p>UCS 6454 ファブリック インターコネクで UCS C シリーズ サーバと Cisco UCS Manager リリース 4.0 を連携しようとする、サーバの検出に失敗します。この問題は解決されており、ラックサーバは正常に検出されます。</p>	4.0 (1a) A	4.0(4a)A
CSCvo66721	<p>電源投入/電源切断、ポートグループの変更、または VMotion の結果として、VM のピン接続が変更された後、その VM の MAC アドレスがピン接続されていない FI の MAC アドレス テーブルからただちに削除されるようになりました。</p>	4.0 (2a) A	4.0(4a)A
CSCvn82697	<p>サブ組織で定義されているロケールの場合でも、リモートで認証されたユーザーはすべての組織を表示できます。この問題は解決されました。</p>	3.2 (3g) A	4.0(4a)A

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
CSCvo91744	<p>Cisco UCS Manager リリース 4.0(2) にアップグレードした後、MAC セキュリティが拒否に設定されたネットワーク制御ポリシーが設定されている場合、一部のサーバでは、アップグレードされたファブリック インターコネクで VIF がダウンしているように表示されます。</p> <p>この問題は解決されました。</p>	4.0(2a)A	4.0(4a)A

リリースで解決済みの問題 4.0(2e)

次の問題はリリース 4.0(2e) で解決済みです。

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
CSCvn82697	サブ組織で定義されているロケールの場合でも、リモートで認証されたユーザーはすべての組織を表示できます。この問題は解決されました。	3.2 (3g) A	4.0(2e)A 4.0(4a)A
CSCvo19661	UCS 6454 ファブリックインターコネクは、ファブリックインターコネクの管理 IP アドレスをブロードキャストする代わりに、LLDP アップストリーム ACI リーフとダウンストリームを介して、CDP を介して ESXi ホストに KVM アウトオブバンド IP アドレスをブロードキャストしています。この問題は修正されており、ファブリック インターコネクが正しい IP アドレスをブロードキャストするようになりました。	4.0 (1c) A	4.0(2e)A
CSCvo64592	UCS 6454 ファブリック インターコネクで UCS C シリーズ サーバと Cisco UCS Manager リリース 4.0 を連携しようとする、サーバの検出に失敗します。この問題は解決されており、ラック サーバは正常に検出されます。	4.0(1a)A	4.0(2e)A 4.0(4a)A

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
CSCvn77413	6332 または 6332-16 ファブリック インターコネクト上のイーサネットポートでは、入力破棄回数が上昇しましたが、パフォーマンスへの大きな影響はありません。 この問題は解決されました。	3.2 (3h) A	4.0(2e)A

リリースで解決済みの問題 4.0(2d)

次の問題はリリース 4.0(2d) で解決済みです。

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
CSCvn22595	OS として Cisco UCS Manager 3.2(3d) ファームウェアおよび Red Hat Linux を実行しているシステムで、VIC 1340 および VIC 1380 アダプタを搭載した Cisco UCS B200 M5 サーバを使用している場合、同じバス ID を共有しているものの、異なる機能番号を持つ vNICs は同じ入力出力メモリ管理ユニット (IOMMU) に割り当てられなくなります。	3.2(3d)B	4.0(2d)B
CSCvn60002	Cisco VNICs および VHBA では、電源投入またはリンクフラップ後の物理リンクへのアクセスにおける応答時間が低下しなくなりました。Sanboot用に設定されたサーバが正しく起動するようになりました。	4.0(2b)A	4.0(2d)A
CSCvo13678	複数の NVIDIA GPU を搭載した Cisco UCS M5 ラックサーバは検出に失敗し、ラックサーバの Cisco UCS Manager リリース 4.0 (2a) のファームウェアをインストールする際に、コア ファイルを生成します。	4.0(2a)A	4.0(2d)A
CSCvn81327	Cisco UCS-IOM-2304 IO モジュールはクラッシュしなくなり、特定の状況で pick_next_task_rt をポイントするカーネルコアダンプを生成します。トラフィックの転送は影響を受けません。	3.2(2d)A	4.0(2d)A

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
CSCvm66499	インバンド KVM VLAN が設定されていて、サーバ管理が FEX を介して接続されている場合、KVM の起動機能が機能するようになりました。	4.0(1a)C	4.0(2d)C
CSCvh18287	Cisco UCS C240 M5 サーバでは、エラー コード F0776 と、存在しないディスクが動作不能であることを示す障害メッセージが表示されなくなりました。	3.2(1d)C	4.0(2d)C
CSCvm66118	シリアル番号 LIT xxxxxx の PSU が、Cisco UCS Manager 管理対象 6300 シリーズ ファブリック インターコネクタに接続されたシャーシに挿入または再装着されると、ファブリック インターコネクタは PSU ファン障害を報告しなくなります。	3.2(2f)B	4.0(2d)B 3.2(3j)B
CSCvm89871	Cisco UCS Manager 管理対象 C240 M4 ラックサーバは、次の設定シーケンス後、UCS 6332 および 6332-16UP ファブリック インターコネクタでの検出に失敗しなくなりました。 <ol style="list-style-type: none"> 1. アップリンク イーサネット ポートチャネルの一部であるポートを無効にします。 2. ポート チャネルからインターフェイスを削除します。 3. ポート タイプをサーバとして再設定します。 4. サーバを再設定されたポートに接続します。 	3.1(2c)C	4.0(2d)C
CSCvo22832	Cisco UCS Manager VIC 14xx シリーズ アダプタを使用して UCS 6454 ファブリック インターコネクタに直接接続されている C シリーズサーバは、CDP/LLDP パケットを正しくキャプチャするようになりました。	4.0(2a)A	4.0(2d)A

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
CSCvo04128	E モードで設定され、UCS 6454 ファブリック インターコネクでサポートされているファイバチャネルポートは、ブートまたはリンクフラップ後にオンラインになる際に遅延が発生しなくなりました。	4.0(2a)A	4.0(2d)A

リリースで解決済みの問題 4.0(2b)

次の問題はリリース 4.0(2b) で解決済みです。

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
CSCvk63036	Cisco UCS ファブリック インターコネクトペアと Cisco ファイバチャネル スイッチ間に SAN ポートチャネルを形成できません。この場合、スイッチの組織固有 ID (OUI) は次のいずれかになります。 <ul style="list-style-type: none"> • 003a9c • 000831 • d0a5a6 この問題は解決されました。	4.0(2a)A	4.0(2b)A
CSCvn91826	Cisco VIC 14xx アダプタを使用した設定では、サーバ ID 範囲の制限によりサーバ検出が失敗します。サーバ ID の範囲は、現在 1 ~ 254 です。	4.0(2a)A	4.0(2b)A
CSCvk26441	UCS 6454 ファブリック インターコネクで Cisco UCS Manager リリース 4.0(2a) を実行している場合、グループマップルールに aaa および read-only 以外のロールがあると、LDAP ユーザー ログインは失敗しません。	4.0(2a)A	4.0(2b)A
CSCvk53356	UCS 6454 ファブリック インターコネクで Cisco UCS Manager リリース 4.0(2a) を実行している場合、パスワード復元の手順を使用して管理者パスワードを復元できません。この問題は解決されました。	4.0(2a)A	4.0(2b)A

リリースで解決済みの問題 4.0(2a)

次の問題はリリース 4.0(2a) で解決済みです。

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
CSCvk62258 CSCvm04161	UCS S3260 サーバの 1 つのノードで LLDP 設定の変更を行うと、2 番目のサーバノードがクラッシュします。この問題は、Windows オペレーティングシステムで主に観察されました。 この問題は解決されました。	3.1 (3a) C	4.0(2a)C
CSCvn10940	VLAN 4093 は予約済み VLAN のリストから削除されており、設定に使用できます。	4.0 (1a) A	4.0(2a)A
CSCvh97755	Cisco UCS 6200 シリーズ ファブリック インターコネクトは、vEthernet インターフェイスからスイッチのアップストリームアップリンクポートに EAPOL 開始フレームをパスしません。 この問題は解決されました。	3.1 (2c) A	4.0(2a)A
CSCvm08604	Cisco S3260 シャーシのシャーシファームウェアのアップグレード中に、コントローラとドライブの間で自己暗号化ドライブ (SEDs) のセキュリティキーが一致しませんでした。 この問題は解決されました。	3.2 (3b) A	3.2 (3i) A 4.0(2a)A
CSCvk38240	3.2 (3d) ブレードサーバファームウェアバンドルに含まれているアダプタファームウェアバージョン 4.2 (3b) で、UCS VIC 1340 を使用すると、SAN からの UEFI ブートが失敗します。 現在この問題は発生しません。	3.2 (3d) B	4.0(2a)B
CSCvj78742	アクティブ IOM は、リブートされたピア IOM からのフェールオーバー中の satsyslog hap リセットにより、予期せず再起動しなくなります。	3.2 (3d) A	3.2 (3h) A 4.0(2a)A

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
CSCvi66859	VLAN グループが設定され、FI アップリンク インターフェイスにマッピングされているシステムでは、vNIC テンプレートまたは VLAN グループから VLAN が削除されると、予期しない停止が発生しました。 この問題は解決されました。	3.2 (2b) A	4.0(2a)A
CSCvm23975	Cisco UCS Manager によって管理されている C シリーズ ラック サーバおよびすべての V シリーズ GPU アダプタを搭載したシステムでは、C シリーズ ラック サーバに次の GPU アダプタが 1 個以上ある場合でも、GPU モードを Cisco UCS Manager のグラフィック ポリシーを使用して変更できます。 <ul style="list-style-type: none"> • UCSC-GPU-V100-16G • UCSC-GPU-V100-32G 	4.0(1a)A	4.0(2a)A

リリースで解決済みの問題 4.0(1d)

次の問題はリリース 4.0(1d) で解決済みです。

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
CSCvm57553	非常に少ない数の UCS IOM-2304 では、JFFS2 Clearmarker ファイルシステムエラーが原因でブートおよび実行時間が低下する可能性があります。これは、ベンダー固有のカーネル ファイルシステムパッチの制限によって引き起こされ、16-3743-01 またはフラッシュ チップを使用して構築された IOM に影響します。 この問題は解決され、どの UCS IOM にも影響しなくなります。	4.0(1a)A	4.0(1d)A および 3.2(3i)A
CSCvm08604	Cisco S3260 シャーシのシャーシファームウェアのアップグレード中に、コントローラとドライブの間で自己暗号化ドライブ (SEDs) のセキュリティ キーが一致するようになります。	3.2(3b)A	4.0(1d)A および 3.2(3i)A

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
CSCvj98360	BMC が DIMM を検出できず、次のメッセージが表示されてブレードサーバ検索が停止しました。 DIMM 設定の不一致 この問題は解決されました。	4.0(1a)B	4.0(1d)B
CSCvm09239	UCS 2304 IOM が 40G QSFP ケーブルを使用して単一のリンクを介して UCS 6300 シリーズ FI に接続されている設定では、UCS Central からシャーシログファイルを収集している間、IOM は接続解除と再接続を行いません。	3.2(3d)A	4.0(1d)A および 3.2(3i)A
CSCvk36317	Cisco UCS Manager をリリース 3.1 (1l) から 3.2 (3b) にアップグレードした後は、既存の PVLAN 設定が失敗します。プライマリ VLAN 内のアップストリームサーバが、UCS ドメイン内の隔離 VLAN の VM/ホストに到達できるようになりました。	3.2(3a)A	4.0(1d)A および 3.2(3h)A
CSCvm50159	UCS FI-6248UP では、ファンはスイッチによって検出されません。その結果、スイッチは一連のエラーメッセージでシャットダウンします。 System minor alarm on fans: One fan missing or failed Fan module 1 xxxx-FAN removed System shutdown in 60 seconds due to fan removal System major alarm on fans: Multiple fans missing or failed System shutdown in 55 seconds due to fan removal System shutdown in 50 seconds due to fan removal この問題は解決されました。	2.2 (8l) A	4.0(1d)A および 3.2(3i)A
CSCvk63025	UCS 6332-16UP ポート 33/34 は、CUIM パッシブケーブルを使用している C93180YCFX ポート 49/50 との接続の問題がなくなりました。	3.2(3b)A	4.0(1d)A および 3.2(3i)A

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
CSCvm44391	<p>vNIC テンプレートは、LAN クラウドおよびアプライアンスのオプションから重複する vLAN エントリをリストします。</p> <p>この問題は解決されました。vNIC テンプレートは、vLAN エントリをフィルタリングし、固有の vLAN 名のみをリストするようになりました。</p>	3.2(3g)A	4.0(1d)A および 3.2(3i)A
CSCvm91294	<p>次の条件で S3260 シャーシに接続されている UCS FI セットアップでは、シャーシファームウェアのアップグレード後に DME プロセスがクラッシュします。</p> <ul style="list-style-type: none"> UCS UCSC-C3K-M4SRB M4 RAID ストレージコントローラと背面ブート SSD を搭載したサーバ ディスクは両方のコントローラにゾーン分けされ、VD は上位ローディング ディスクと背面ブート SSD で作成されます。 <p>この問題は解決されました。</p>	3.2(3g)A	4.0(1d)A および 3.2(3i)A
CSCvm68038	<p>テクニカルサポートログをダウンロードした後、samdme ユーザーセッションが下位 FI から消去されません。これにより、複数の応答がないセッションが発生し、下位 FI のセッション数が 64 (最大許容) に達すると、FI へのリモートアクセスが失われます。</p> <p>この問題は解決されました。Samdme ユーザーセッションは、techsupport ログのダウンロード後に下位 FI から自動的に消去されます。</p>	3.2(2d)A	4.0(1d)A および 3.2(3i)A
CSCvm21299	<p>ログが pa_setup ファイルに継続的に書き込まれている場合、プライマリ FI のアップグレードは応答しなくなります。</p>	3.2(3a)A	4.0(1d)A および 3.2(3i)A

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
CSCvm54628	<p>UCS 6200 シリーズでは、FI 管理 IP アドレスの変更は IOM または FEX で更新されません。従って、ホスト インターフェイスに接続されているデバイスは、CDP プロセスで古い管理 IP アドレスを受信します。</p> <p>この問題は解決されました。ホスト インターフェイスに接続されているデバイスは、CDP プロセスで更新された IP アドレスを受信します。</p>	3.2(3b)A	4.0(1d)A および 3.2(3i)A
CSCvm95801 CSCvn01215	<p>UCS 6300 シリーズおよび UCS 6324 では、FI 管理 IP アドレスの変更は IOM または FEX で更新されません。従って、ホスト インターフェイスに接続されているデバイスは、CDP プロセスで古い管理 IP アドレスを受信します。</p> <p>この問題は解決されました。ホスト インターフェイスに接続されているデバイスは、CDP プロセスで更新された IP アドレスを受信します。</p>	3.2(3b)A	4.0(1d)A および 3.2(3j)A
CSCvn10940	VLAN 4093 は予約済み VLAN のリストから削除されており、設定に使用できます。	4.0(1a)A	4.0(1d)A および 4.0(2a)A
CSCvn09080	<p>UCS 6454 では、FI 管理 IP アドレスの変更は IOM または FEX で更新されません。従って、ホスト インターフェイスに接続されているデバイスは、CDP プロセスで古い管理 IP アドレスを受信します。</p> <p>この問題は解決されました。ホスト インターフェイスに接続されているデバイスは、CDP プロセスで更新された IP アドレスを受信します。</p>	4.0(1a)A	4.0(1d)A
CSCvn25087	<p>非常に具体的な書き込み/読み取りパターンがあるシナリオでは、3.8 TB および 7.6 TB ミクロン 5100 SSD SATA ドライブのデータ損失が発生する可能性があります。UECC 読み取りエラーと再割り当てされたセクター数は、スマート ログに表示されます。</p> <p>この問題は解決されました。</p>	4.0(1c)B および 4.0(1c)C	4.0(1d)B および 4.0(1d)C

リリースで解決済みの問題 4.0(1c)

次の問題はリリース 4.0(1c) で解決済みです。

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
CSCvh04307	<p>SED ドライブを搭載した Cisco HyperFlex ノードで、ストレージコントローラ VM 上で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。</p> <p>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。</p> <p>再起動されたホストでドライブがロックされる可能性があります。この問題の修正は、リリース 4.0 (1a) に統合されました。</p> <p>さらに、長期間にわたってコールド電源がオフになっているホストでドライブがロックされ、その後リブートされるというシナリオがありました。このシナリオの修正は、リリース 4.0 (1c) で統合されました。</p>	3.1(3c)C	4.0(1c)C
CSCvm14726	<p>新しい SPI フラッシュ デバイスを搭載した Cisco UCS 6324 ファブリック インターコネクタは、以前のソフトウェア リリースでは起動できません。これは、UCS 6324 ファブリック インターコネクタで使用されていた元の SPI フラッシュ デバイスが生成されなくなったためです。したがって、ピン互換の交換部品が今後使用されます。ただし、ベンダーとパーツ ID の変更により、新しいパーツが搭載された UCS 6324 ファブリック インターコネクタは、新しいパーツをサポートしている OS バージョンでのみ動作します。</p> <p>この問題は解決されました。</p>	4.0(1a)A	4.0(1c)A

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
CSCvk30528	<p>UEFI ブート モードでは、Cisco UCS マネージド C シリーズ サーバが、EMC ストレージ デバイスに設定されている iSCSI LUN にインストールされている RHEL または ESXi OS で起動できませんでした。代わりに、再起動するたびに、サーバが UEFI シェル プロンプトを開始します。</p> <p>この問題は解決されました。サーバが OS で正しくブートするようになりました。</p>	4.0(1a)C	4.0(1c)C

リリースで解決済みの問題 4.0(1b)

次の問題はリリース 4.0(1b) で解決済みです。

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
CSCvm17259	<p>Cisco UCS Manager で管理されている C シリーズ ラック サーバを搭載したシステムでは、サーバのサービス プロファイルを設定した後に、ファームウェア ポリシーのホスト ファームウェア パック (HFP) に、UCSC gpu V100-32G GPU のファームウェアが表示されませんでした。この問題は解決され、ファームウェアは HFP に表示されるようになりました。</p>	4.0(1a)A	4.0(1b)A
CSCvm10391	<p>Cisco UCS 6454 ファブリック インターコネク トは、設定された SMTP サーバに Call Home メッセージを送信していませんでした。</p> <p>この問題は解決されました。Call Home メッセージが Cisco UCS 6454 ファブリック インターコネク トによって送信され、設定した SMTP サーバで電子メールとして受信します。</p>	4.0(1a)A	4.0(1b)A

リリースで解決済みの問題 4.0(1a)

次の問題はリリース 4.0(1a) で解決済みです。

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
CSCvh04307	<p>SED ドライブを搭載した Cisco HyperFlex ノードで、ストレージコントローラ VM 上で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。</p> <p>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。</p> <p>さらに、再起動されたホストでドライブがロックされる可能性があります。</p> <p>この問題は解決されました。</p>	3.1(3c)C	4.0(1a)C
CSCva17452	<p>2つの非ドロップクラス(1つのイーサネットと1つの FCoE)がシステムに設定されている場合、Cisco UCS 6332-16IUP ファブリック インターコネクトシリーズのアップポートでは、パケットがドロップされなくなります。</p>	3.1(1e) A	4.0(1a)A
CSCve53858	<p>ブレイクアウトポートを有効または無効にした後、ポートチャネルを作成/削除すると、FI QoS キューは停止しなくなります。</p>	3.2(2b) A	4.0(1a)A
CSCvh79589	<p>タイマーグループライブラリでは、通常の動作状態の間に、bcm_usd プロセスのクラッシュと UCS 6332 シリーズ ファブリック インターコネクトのリポートが行われなくなりました。</p>	3.2(2b) A	4.0(1a)A
CSCvi16121	<p>サーバプールが割り当てられているサービスプロファイルテンプレートの更新にバインドされたサービスプロファイルの設定が変更されると、サーバが予期せず再起動し、サービスプロファイルが再度関連付けされます。これは、サービスプロファイルに割り当てられたサーバがサーバプールに含まれていない場合に発生します。</p> <p>この問題は解決されました。予期せずサーバがリポートしたり、サービスプロファイルの再関連付けが設定変更後に行われたりすることはなくなりました。</p>	3.2(1d) A	4.0(1a)A

未解決の不具合

リリースで未解決のバグには、[Cisco バグ検索ツール](#)を使用してアクセスできます。この Web ベース ツールから、この製品やその他のシスコ ハードウェアおよびソフトウェア製品でのバグと脆弱性に関する最新情報を保守する Cisco バグ追跡システムにアクセスできます。



(注) Cisco Bug Search Tool にログインしてこのツールを使用するには、Cisco.com アカウントが必要です。アカウントがない場合は、[アカウントを登録](#)できます。

Cisco Bug Search Tool の詳細については、[Bug Search Tool \(BST\) ヘルプ](#)および[FAQ](#)を参照してください。

リリースで未解決の問題 4.0 (4i)

次の問題がリリース 4.0 (4i) 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
CSCvt60312	UCSC シリーズサーバのアップグレード中に、サービスプロファイルの関連付けの「サーバインベントリの実行 - PNUOS インベントリ」を実行するために 1~2 時間かかりました。	Cisco UCS Manager で、[インストールされたファームウェア (Installed Firmware)] タブに移動し、すべてのドライブの[アクティベート ステータス (Activate Status)] が [準備完了 (Ready)] になっているかどうかを確認します。すべてのドライブのアクティベートステータスが準備完了の場合は、KVM または Cisco UCS Manager を使用してサーバをリセットして、アップグレードを続行します。	4.0 (4g)B

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvs93286	アダプタでホストファームウェアパック (自動インストールサーバ) を使用してサーバファームウェアのアップグレードを実行した後、アダプタのアクティベーションが pending-next-boot 状態でスタックします。この状態は、BIOS の更新の直後にアダプタのアクティベーションがトリガーされ、その後ホストの電源がオンになった場合、およびサーバ BIOS とアダプタの両方が更新された場合に発生します。	Cisco UCS Manager にログインして、アダプタをリセットします。	4.0 (4g)A、4.0 (4h)A および C
CSCvs06864	SAN LUN へ Windows 2016 または Windows 2019 をインストール中に、ブルースクリーン (BSoD) が発生します。この状態は、2 つ以上の vHBA で構成されたサービスプロファイルが、UCS バージョン 4.0 (4a) 以降にバンドルされている Cisco UCS VIC 14xx シリーズアダプタに関連付けられている場合に発生します。	SAN LUN で Windows 2016 または Windows 2019 をインストールしている間は、Cisco UCS VIC 14xx シリーズの各アダプタで使用する vHBA をアダプタごとに 1 つだけに制限してください。その他の vHBA は、インストール後に追加します。	4.0(4a)

リリースで未解決の問題 4.0 (4h)

次の問題がリリース 4.0 (4h) 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
CSCvt64871	<p>Cisco UCS C480 M5 サーバおよび Cisco UCS 480 M5 ML サーバでは、ADDDC 仮想ロックステップをアクティブ化した後、まれに応答が停止して、再起動する場合があります。これにより、メモリシステムの #IERR と M2M タイムアウトが発生します。</p> <p>詳細については、以下を参照してください。</p> <ul style="list-style-type: none"> • Intel® Xeon® Processor Scalable Family Specification Update (エラッタ > SKX108) • Second Generation Intel® Xeon® Scalable Processors Specification Update(エラッタ > CLX37) 	<p>ADDDC 仮想ロックステップをアクティブ化した後、サーバが何度もクラッシュした場合は、ADDDC を無効にします。</p> <p>詳細については、『Cisco Software Advisory』、https://www.cisco.com/c/en/us/support/docs/field-notices/704/fn70432.html を参照してください。</p>	4.0 (4c)B

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvt55829	<p>下に示す PID の SanDisk Lightning II ソリッドステートドライブ (SSD) LT0400MO および LT1600MO は、40,000 時間正常に動作した後、利用可能な残りストレージスペースが 0 GB であると報告するようになります。電源サイクルイベントの後に、SSD はオフラインになって使用できなくなり、データ損失が発生します。また、サービス作業で同時に複数のドライブを取り付けていた場合には、すべてのドライブでそうなる可能性があります。</p> <p>この問題の影響を受ける SSD の PID は、次の通りです。</p> <ul style="list-style-type: none"> • (400GB) UCSSD400GIKHY4P、 UCS-SD400G12S4EP、 UCS-C3X60-12G240 • (1.6TB) UCSSD161GIKHY4P、 UCS-SD161G12S4EP、 UCS-C3X60-12G2160 <p>この問題は解決されました。</p>	この問題を解決するには、ファームウェアバージョン C405 をインストールします。	4.0 (4h)C 4.0 (4i)C で解決済み
CSCvt46877 CSCvt46838	6400 シリーズ ファブリックインターコネクタでは、ピアの数が多いうちに予期しないリセットが発生します。	ファブリックサービスを無効にします。	4.0 (4h)A 4.0 (4i)A で解決済み

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvn74327	<p>シリーズ 1400 アダプタでファームウェアをアップグレードした後、仮想ポートは使用できなくなり、システムログに次のメッセージが記録されます。</p> <pre> 191024-05:13:13.410919 laser.i2c ERROR: i2c1: stuck bus - failed to clear 191024-05:13:18.529477 laser.i2c ERROR: i2c1: stuck bus - failed to clear 191024-05:13:18.530797 kernel: paloi2c c8004400.i2c1: target 0x20: timeout error 191024-05:13:23.579591 kernel: paloi2c c8004400.i2c1: target 0x20: timeout error 191024-05:13:23.579895 laser.i2c ERROR: i2c1: stuck bus - failed to clear 191024-05:13:28.695617 kernel: paloi2c c8004400.i2c1: target 0x20: timeout error 191024-05:13:28.695951 laser.i2c ERROR: i2c1: stuck bus - failed to clear 191024-05:13:33.747636 kernel: paloi2c c8004400.i2c1: target 0x20: timeout error 191024-05:13:33.747969 laser.i2c ERROR: i2c1: stuck bus - failed to clear </pre>	システムの電源を再投入してください。	4.0 (4h)A 4.0 (4i)A で解決済み

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvu14656	<p>BIOS を次のいずれかのバージョンにアップグレードすると、M5 サーバの起動が、メモリテストの手順で停止します。</p> <ul style="list-style-type: none"> • C240M5404i00805200743 • C220M5404p0024200755 • B200M5404i00805202307 • B480M5404m00805202307 • S3X60M5404i0024200755 	<p>サーバを起動するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. BIOS を以前の動作バージョンに戻し、システムで OS を起動します。 2. ログを確認して、修正可能または修正不可能な ECC エラーが発生している DIMM を特定し、故障した DIMM を交換するか、取り外します。 3. 4.0 (4h) バンドルに含まれている BIOS バージョンにアップグレードし、システムが正常に起動することを確認します。 	<p>4.0 (4h)C 4.0 (4i)C で解決済み</p>

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvu11155	<p>BIOS を次のいずれかのバージョンにアップグレードすると、第2世代 Intel® Xeon® スケーラブルプロセッサを搭載した Cisco UCS B シリーズ、C シリーズ、および S シリーズ M5 サーバでパフォーマンスが低下する可能性があります。</p> <ul style="list-style-type: none"> • C240M540400805200743 • C220M54040024200755 • B200M540400305202307 • B480M5404m00305202307 • S3X60M54040024200755 	既知の回避策はありません。	4.0 (4h)B および C

リリースで未解決の問題 4.0 (4e)

次の問題がリリース 4.0 (4e) 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
CSCvr01259	<p>UCS 6400 シリーズ ファブリック インターコネクタが UCS 2408 IOM に接続されている場合、HIF ポート インターフェイス カウンタはファブリック インターコネクタで更新されません。ただし、仮想イーサネットには正しいパケット数が表示されます。</p>	仮想イーサネットカウンタを使用します。	4.0 (4e)A

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvr42736	<p>6300 シリーズ ファブリックインターコネク トと IOM 間で接続さ れているファブリック リンクが 40GBASE CR4 QSFP タイプ銅 ケーブルの場合、自動 インフラストラクチャ アップグレードがエ ラー『「次のブートを 保留中」で IOM アク ティベーション ス タック』により失敗し ます。</p> <p>この問題は、他のケー ブルタイプでは観測さ れていません。</p>		4.0 (4e)A

不具合 ID	症状	回避策	影響を受ける最初のバンドル
		<p>次の手順を使用します。</p> <ol style="list-style-type: none"> 1. UCS Manager GUI にログインします。 2. A (プライマリ) または B (従属) ファブリックインターコネクタイーサネットポートのいずれかを次のように選択します。 <ul style="list-style-type: none"> • [機器 (Equipment)] <ul style="list-style-type: none"> > [ファブリックインターコネクタ (Fabric Interconnects)] > [ファブリックインターコネクタ A (プライマリ) (Fabric Interconnect A (primary))] > [物理ポート (Physical ports)] > [イーサネットポート ()] • [機器 (Equipment)] <ul style="list-style-type: none"> > [ファブリックインターコネクタ (Fabric Interconnects)] > [ファブリックインターコネクタ B (下 	

不具合 ID	症状	回避策	影響を受ける最初のバンドル
		<p>位) (Fabric Interconnect B (subordinate)]>[物理ポート (Physical ports)]> [イーサネットポート (Ethernet ports)]</p> <p>3. IOMに接続されているファブリックポートを選択し、それらを設定解除します。</p> <p>4. ファブリックポートをサーバポートとして再設定します。</p>	

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvr67352	<p>6454 ファブリック インターコネクに接続したブレードサーバでは、次の条件下で、管理インスタンスが OOB KVM 接続にアクセスできなくなります。</p> <ul style="list-style-type: none"> • IOM がリブートされます • ファブリック インターコネクの 1 つが動作不能になります。 <p>6454 ファブリック インターコネクに接続したラック サーバでは、次の条件下で、管理インスタンスが KVM 接続にアクセスできなくなります。</p> <ul style="list-style-type: none"> • FEX がリブートされます。 • FEX は 1 つのファブリック インターコネクで動作不能です。 • ファブリック インターコネクの 1 つが到達不能です。 <p>この問題は、サービス プロファイルの管理 IP アドレスにのみ適用されます。</p>	Mgmt0 インターフェイスで古い OOB KVM IP アドレスが設定されているファブリック インターコネクをリブートします。	4.0 (4e)A 4.0 (4f)A で解決済み

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvr68316	<p>スタンドアロン C シリーズ サーバでは、VIC とスイッチ側の両方でポートチャネルが有効になっているスイッチに UCS VIC 1455/1457 アダプタが接続されている場合、イーサネットおよびファイバチャネルのデータパスは機能しませんでした。</p> <p>この問題は、スタンドアロン C シリーズ サーバに固有のものであり、UCS Manager で管理されている C シリーズサーバには適用されません。ただし、C シリーズサーバと UCS Manager システムとの統合中に問題が発生する可能性があります。Cisco IMC または VIC アダプタの「工場出荷時のデフォルトにリセット」は、サーバ統合ワークフローの前提条件のステップです。</p>	Cisco IMC から VIC 1455/1457 「ポートチャネル」設定を無効にし、再度有効にします。	<p>4.0 (4e)C</p> <p>4.0 (4f)C で解決済み</p>
CSCvr79388	M5 B シリーズ サーバでは、特定のまれな条件下で、ADDDC 仮想ロックアップのアクティベーション後にサーバがリブートし、その結果、CATERR とメモリシステムの M2M タイムアウトが発生します。	TAC に連絡します。	<p>4.0 (4e)</p> <p>4.0 (4h)C で解決済み</p>

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvr79396	M5 B シリーズサーバでは、仮想ロックステップ (VLS) のスペアリングコピーが早期に終了し、ロックステップ領域で誤った値が導き出されます。	TAC に連絡します。	4.0 (4e)C 4.0 (4h)C で解決済み
CSCvt38091	UCS Manager リリース 4.0 (4e) にアップグレードした後、B200-M5 ブレードサーバに次のようなメッセージが表示されました。01-09-2020 00:44 モデル名 UCS-FI-6332-16UP のホスト名が、診断テストの失敗を報告しました。 「回復済み：サーバ 1/6 (サービス プロファイル：(プロファイル名) アクセス不能)」	メッセージは最終的にはクリアされます。	4.0 (4e)B

リリースで未解決の問題 4.0 (4d)

次の問題がリリース 4.0 (4d) 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
CSCvr23703	<p>サーバのブート時間が長くなる可能性があります。</p> <p>App Direct Modem で Intel[®] Optane[™] Data Center 永続メモリ モジュールを使用する場合など特定の状況下では、多数のネームスペースを使用している場合、ブート時間は最大で 9% 長くなる可能性があります。</p>	なし	4.0 (4d)B
CSCvr47266	<p>モデル 6248 ファブリックインターコネクタからモデル 6454 ファブリックインターコネクタへの移行中に、UCS 2208 IOMs がサイレントに失敗しました。PortAG を必要とするアクションはすべて失敗します。Cisco UCS Manager のすべてのバージョンでバーストサイズ 0 を適用できますが、その結果として 6454 ファブリックインターコネクタのみが失敗します (移行後)。</p>	<p>障害状態であっても、バーストサイズを 512-268435456 の範囲で設定します。</p>	<p>4.0 (4d)A</p> <p>4.0 (4f)A で解決済み</p>

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvr23703	App Direct Mode で Intel® Optane™ Data Center 永続メモリ モジュールを使用し多数のネームスペースを使用するなど、B480 M5 サーバの特定の条件下では、サーバのブート時間が明らかに長くなります。	なし	4.0 (4d)B
CSCvr40744	6400 シリーズ ファブリックインターコネクットのポート 5661 は、httpd および tcpwrapped 用を開いています。	既知の回避策はありません。	4.0 (4d)A と B 4.0 (4f)A で解決済み
CSCvr46327	UCS 2208 IOM を UCS 2408 IOM に置き換えると、仮想イーサネットインターフェイスは使用できなくなります。仮想イーサネットインターフェイスは、 show interface virtual status コマンドの出力では使用できませんが、NXOS での show interface brief コマンドの出力で使用できます。	いずれかが移行を完了した後、ファブリックインターコネクートをリロードしてから、Cisco UCS Manager でファブリックインターコネクートをリロードを実行して、仮想イーサネットインターフェイスを起動します。	4.0 (4d)A

リリースで未解決の問題 4.0 (4c)

次の問題がリリース 4.0 (4c) 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
CSCvq74492	Intel X520 PCIe アダプタがシステムに存在し、iSCSI モードが Intel X550 LOMs に対して有効になっている場合、BIOS post 中にシステムが応答しなくなります。これは、ブートモードがレガシーに設定されている場合にのみ発生します。		4.0 (4c)C

不具合 ID	症状	回避策	影響を受ける最初のバンドル
		<p>この問題が発生した場合は、次の手順を実行します。</p> <ul style="list-style-type: none"> • UEFI ブートモードに切り替えます。 <p>または</p> <ol style="list-style-type: none"> 1. システムがハングしている場合は、CIMC 機能を使用して BIOS トークンを設定するように LOM オプションを設定します。 2. サーバを UEFI シェルに再起動します。 3. Intel bootutil を使用し、X520 アダプタの iSCSI を有効にし、サーバを再起動します (Intel bootutil とそのユーザーガイドはドライバ iso の一部です)。 4. 次回の起動時に、BIOS post を使用して Intel OPROM ユーティリティ (Ctrl + D) を入力し、X550 LOM の iSCSI モードを有効にします。保存して再起動します。 5. LOM iSCSI LUN は、問題なく起動 	

不具合 ID	症状	回避策	影響を受ける最初のバンドル
		しません。	

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvq26156			4.0(1a)C 4.0(2a)C 4.0 (4c)C 4.0 (4d)C で解決済み

不具合 ID	症状	回避策	影響を受ける最初のバンドル
	<p>UCSC シリーズサーバファームウェアを 4.0 (4a) またはそれ以降のリリースにアップグレードすると、Cisco 12G モジュール型 SAS HBA が次の Intel S4500 ドライブモデルの検出を停止し、ディスクファームウェアのアップグレードが失敗する可能性があります。</p> <ul style="list-style-type: none"> • SSDSC2KB480G7K - 480GB 2.5 インチ Enterprise Value 6G SATA SSD • SSDSC2KB960G7K - 960GB 2.5 インチ Enterprise Value 6G SATA SSD • SSDSC2KG019T7K - 1.9TB 2.5 インチ Enterprise performance 6G SATA SSD • SSDSC2KG480G7K - 480GB 2.5 インチ Enterprise performance 6GSATA SSD • SSDSC2KG960G7K - 960GB 2.5 インチ Enterprise performance 6G SATA SSD • SSDSC2KB038T7K - 3.8TB 2.5 インチ Enterprise Value 6G SATA SSD <p>この問題は、アップグレード前のドライブ</p>	<ol style="list-style-type: none"> 1. 4.0 (4a) リリースにアップグレードする前に、ドライブのファームウェアのみをリリース 4.0 (4a) 以降のリリースパッケージの一部である SCV1CS07 にアップグレードします。 2. 次に、4.0 (4a) またはそれ以降のリリースパッケージの完全なアップグレードを続行します。 <p>この問題によってすでに影響がある場合は、次の手順を実行して回復します。</p> <ol style="list-style-type: none"> 1. Cisco 12G モジュール型 SAS HBA を以前の動作バージョン (4.0 (1) および 4.0 (2) リリースパッケージで使用可能な 00.00.00.50 または 00.00.00.58) にダウングレードします。 2. ドライブのファームウェアのみをリリース 4.0 (4a) 以降のリリースパッケージの一部である SCV1CS07 にアップグレードします。 	

不具合 ID	症状	回避策	影響を受ける最初のバンドル
	<p>ファームウェアバージョンがSCV1CS05の場合にのみ発生します。その他のドライブファームウェアバージョンは影響を受けません。</p> <p>(注) Cisco HyperFlex は UCS Manager 4.0(4a)、4.0(4b) または 4.0(4c) をサポートしません。</p>	<p>3. ドライブファームウェアが更新されたら、Cisco 12G モジュール型 SAS HBA ファームウェアを 09.00.00.06 にアップグレードします。これは、リリース 4.0 (4a) 以降のリリースパッケージの一部です。</p>	

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvq64055	<p>25G 銅線パッシブ 5M ケーブルを使用してピアに接続された VIC 1455/1457 インターフェイスを持つ UCS C シリーズサーバの物理リンク (H25G SFP-H10GB-CU5M はリンクアップしていないか、UCSによって検出されていません)。</p> <p>この問題は、VIC 1455/1457 インターフェイスが Cisco Nexus スイッチに接続されているか、または SAN ブートが設定されたサーバに接続されている Cisco UCS Manager の管理対象環境またはスタンドアロン環境で発生します。また、ネットワークブートがブートしない場合、または OS をロードしない場合にも発生する可能性があります。</p> <p>この問題は主に、VIC 1455/1457 インターフェイスで 5M ロング 25G 銅線パッシブ ケーブル (H25G SFP-H10GB-CU5M) との物理リンクを検出する際の遅延が原因で発生します。</p> <p>この問題は、すべての M5 モデルに影響します。</p>	<ol style="list-style-type: none"> 1. より短い銅線パッシブ ケーブル (SFP-25G-CU1M) を使用します。SFP-25G-CU2M、SFP-25G-SFP10GB-CU1M 2. 光ケーブルを使用します。 	4.0(1a)C 4.0(2a)C 4.0(4a)C

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvq38756	Intermittant トラフィック損失は、ファブリックインターコネクットのリロード時に NIC チューニングを使用する UCS クラスターで発生することがあります。	Cisco UCS Manager イーサネットアダプタポリシーで、より大きなフェールバックタイムアウト値を設定します。vNIC がセカンダリインターフェイスにアクセスした後、その vNIC のプライマリインターフェイスが再びシステムで使用されるには、プライマリインターフェイスが一定時間使用可能な状態になっている必要があります。その時間の長さをこの設定で制御します。 0 ~ 600 の範囲の秒数を入力します。	4.0(4b)A 4.0 (4d)A で解決済み
CSCvp49398	各ファブリックで 10/25GE パッシブケーブルを使用して 6454 ファブリックインターコネク트에、VIC 1455/1457 インターフェイスが直接接続された (単一またはデュアルリンク接続のいずれか) C/HX シリーズ M5 サーバの展開では、ファブリックインターコネクットのリブート後に、トラフィックが 75 秒間ドロップされます。	なし	4.0(2d)C

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvq09345	<p>永続メモリ ポリシーを持つサービスプロファイルに関連付けられている Cisco UCS M5 ブレードサーバには、次の設定エラーメッセージが表示されることがあります。</p> <p>サーバに設定されている永続メモリに 永続メモリ DIMM が搭載されていません。</p> <p>これは、サーバリブートや検出と関連付けの複数のサイクル中など、まれなシナリオで発生します。</p>	いったんサーバを停止し、再始動します。	4.0(4b)B
CSCvp90219	Cisco UCS Manager 3.2 (3k) から UCS Manager 4.0.4 への手動アップグレード中に、6200 シリーズ ファブリック インターコネクトを搭載したブレードサーバで UCS Manager のアクティブ化が失敗しました。	なし	4.0 (4c)A 4.0 (4f)A で解決済み

リリースで未解決の問題 4.0(4b)

次の問題がリリース 4.0(4b) 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
CSCvp31766	ブレードサーバをアップグレードする場合、VM-FEX インターフェイスを使用する VM は接続が失われます。	Cisco UCS Manager リリース 4.0 (4c) 以降のリリースにアップグレードします。	4.0(4b)B 4.0 (4c)B で解決済み

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvq17624	Cisco UCS Manager では、UCS IOM 2408 を搭載した UCS 5108 シャーシから PSU が取り外された場合、古い電源装置 (PSU) データはクリアされません。	なし	4.0(4b)A 4.0 (4c)A で解決済み
CSCvq29766	UCS 管理対象ブレードサーバを UCS Manager バージョン 4.0 (4b) にアップグレードした後、UCS Central は KVM コンソールを起動できませんでした。	UCS Manager ドメインから KVM を起動します。	4.0(4b)A 4.0 (4c)A で解決済み
CSCvq49222	2~25GE インターフェイスによって 6454 ファブリックインターコネクタに直接接続された VIC 1455 または 1457 インターフェイスカードを搭載した UCS C220 M5 サーバがリブートされると、オペレーティングシステムは数秒~2分間隔でステータスをダウンとして検出します。	アクティブな光トランシーバーの展開 (例: SFP-10G-ACC1M/2M/3M/5M/7M/10M	4.0(4b)B

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvq26156	<p>UCS C-Series サーバから 4.0(4c) C-Bundle へアップグレードすると、Cisco 12G Modular SAS HBA により一部の Intel S4500 ディスクドライブの検出/通信が停止されます。これにより、これらのドライブのソフトウェアアップグレードが失敗します。</p> <p>この問題が発生するのは、コントローラファームウェアバージョンが09.00.00.06の occurs のみです。</p>	<p>アップグレード前 - ホストファームウェアパッケージで、Raid コントローラアップグレードを排除します。</p> <p>アップグレード後 - Raid コントローラファームウェアをバージョン 00.00.00.58 にロールバックします。</p>	<p>4.0(4a)C</p> <p>4.0 (4d)A で解決済み</p>
CSCvq84120	<p>ファブリックインターコネクトの再起動後、vNICs はポリシーの関連付けのタイミングによって早期にフェールオーバーし、intermittant トラフィック損失が発生することがあります。システムによって次のメッセージが表示されます。「インターフェイスに既存以外のポリシーを適用することはできません。」</p>	なし。	<p>4.0(4b)A</p> <p>4.0 (4d)A で解決済み</p>
CSCvr11045	<p>ポート 81 および 743 は、CIMC web サービスが無効になっていても、UCS 6454 ファブリックインターコネクトでアクセスできます。</p>	なし。	<p>4.0(4b)A</p> <p>4.0 (4d)A で解決済み</p>

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvq09345	<p>永続メモリポリシーを持つサービスプロファイルに関連付けられている Cisco UCS M5 ブレードサーバには、次の設定エラーメッセージが表示されることがあります。</p> <p>「サーバに設定されている永続メモリに永続メモリ DIMM が搭載されていません。」</p> <p>これは、サーバリブートや検出と関連付けの複数のサイクルなど、まれなシナリオで発生します。</p>	いったんサーバを停止し、再始動します。	4.0(4b)A
CSCvq82024	<p>BIOS メニューのセットアップ項目「AEP エラー インジェクション」が有効になっている場合、エラーが Intel[®] Optane[™] Data Center 永続メモリ モジュールにインジェクトされ、PSOD の生成が誤って発生します。オペレーティングシステムに通知されないため、MCE が適切に処理されています。</p>	なし	4.0(4b)B 4.0 (4e)B で解決済み
CSCvq57262	<p>RDMA で UCS 6400 ファブリックインターコネクタのインフラストラクチャバンドルアップグレード中に、ラックサーバの1つが保留中のリブート確認応答を示しました。</p>	なし	4.0(4b)A 4.0 (4f)A で解決済み

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvp52336	UCS 6454 ファブリック インターコネクトは、初期設定時に DHCP IP アドレスを受信できませんでした。	初期設定にスタティック IP を使用する	4.0(4b)A 4.0 (4f)A で解決済み
CSCvp51008	単一のアダプタ上の UCS B460 M4 ブレードサーバは、vCon の配置時に関連付けるアダプタを見つけることができません。エラーメッセージ「十分なリソースがと接続配置がないため設定に失敗しました。」が表示されます。	マスタとスレーブのブレードを交換します。これにより、サーバアダプタ番号3が作成されます。この設定では、サーバはエラーなしで関連付けられます。	4.0(4b)A と B 4.0 (4f)A および B で解決済み
CSCvr35735	vNICs がファブリック インターコネクトにピン接続されている場合、UCS 6454 ファブリック インターコネクトは、UCS ラックサーバのペア間のトラフィックを切り替えることができません。	ファブリック インターコネクトがクラスタ内にある場合、異なるファブリック インターコネクトの影響を受けるペアの vNICs をピン接続します。 ファブリック インターコネクトがスタンドアロンで動作している場合は、別のポートでサーバを検出します。	4.0(4b)A 4.0 (4f)A で解決済み
CSCvq98090	UCS 6454 ファブリック インターコネクトの SAN パスは、ファブリック インターコネクトの電源が再投入されるとオフラインになります。	メンバーリンクを再起動します。	4.0(4b)A 4.0 (4f)A で解決済み

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvr76930	SFP-H25G-CU5M ケーブルを介して 2408 ファブリックエクステンダが接続された UCS 管理対象サーバで、ポートがリンクに失敗する可能性があります。	SFP-H25G-CU5M ケーブルモデルは使用しないでください。 SFP-H25G-CU3M や SFP-H25G-AOC5M などの別のケーブルモデルを使用します。	4.0(4b)B および C
CSCvr34407	UCS 6300 シリーズ ファブリックインターコネクタに接続されている UCS M4 および M5 ラックサーバでは、Cisco UCS Manager からの動作が有効または無効にした後 VLAN 構成が失われます。	サーバを再認識します。	4.0(4b)A 4.0 (4f)A で解決済み
CSCvr47266	6200 シリーズ ファブリックインターコネクタから UCS 6454 ファブリックインターコネクタへの移行中に、Quality of Service ポリシーで誤ったバーストサイズが設定されている場合、PortAG は継続的にブートストラップします。失敗がサイレント: アラートまたはコアファイルが作成されていません。	512~268435456 の範囲でバーストサイズを設定します。Cisco UCS Manager は、障害状態の場合でもこの回避策を適用します。	4.0(4b)A 4.0 (4f)A で解決済み

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvr43466	Cisco UCS B シリーズおよび C シリーズ M5 サーバに連携されている Cisco UCS Manager は、ハードウェアが変更されていない場合でも次のハードウェアインベントリの不一致の障害を報告しました。 ハードウェア インベントリの不一致	サーバを解放して再認識させます。	4.0(4b)B 4.0 (4g)B で解決済み
CSCvr95365	Cisco UCS Manager リリース 4.0(1a) からリリース 4.0(4b) へのファームウェアアップグレード後、Cisco 12G モジュラ SAS HBA コントローラを搭載した Cisco UCS C240 M5 サーバの検出は、次のエラーで失敗します。 <code>mc_attrrib_set_suboem_id</code> は SubOEM ID を設定できませんでした	影響を受ける HBA コントローラを交換してください。	4.0(4b)C
CSCvr98210	アプライアンスポートまたは FCoE ストレージポートを搭載したシステムで UCS Manager 3.2.x を UCS Manager 4.0.x にアップグレードすると、LLDP がデフォルトで無効になり、LLDP を必要とするサービスは動作を停止します。	接続を回復するには、Cisco UCS Manager リリース 4.0 へのアップグレード後に、ネットワーク制御ポリシーで LLDP を無効にしてから再度有効にします。	4.0(4b)A 4.0 (4h)A で解決済み

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvs25524	<p>6300 シリーズ ファブリックインターコネクタでは、次のようなメッセージがコンソールログに表示されます。</p> <pre>FI6332-DC3-A %SYSMGR-2-TMP_DIR_FULL: システムの一時ディレクトリの使用率が予想せずに 80% を超えました (System temporary directory usage is unexpectedly high at 80%)</pre>	<p>TAC ケースをオープンします。TAC は /tmp ディレクトリに移動して、不要なログを空にすることができます。また、一時ディレクトリは RAM に保持されているので、ファブリックインターコネクタを再起動すると、この問題を解決できます。</p>	<p>4.0(4b)A 4.0 (4h)A で解決済み</p>
CSCvt08435	<p>6300 シリーズ ファブリックインターコネクタでは、IOM 2304 で SNMP をモニタしている間、HIF ポート数が断続的にゼロに低下し、サードパーティのモニタリングアプリケーションはトラフィックが高いと報告されます。</p>	なし	<p>4.0(4b)A 4.0 (4i)A で解決済み</p>
CSCvu07675	<p>UCS 管理型の統合 C シリーズ ラック サーバへのファームウェアの自動インストールは、SAS コントローラのアクティブ化に失敗します。</p>	<p>該当するラックサーバを解除してから再認識させます。</p>	<p>4.0(4b)C 4.0 (4i)C で解決済み</p>

リリースで未解決の問題 4.0(4a)

次の問題がリリース 4.0(4a) で未解決です。

表 22: Intel® Optane™ データ センター永続メモリ モジュール: Intel の未解決の問題

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvn77341	<p>ボックス内の ndctl ツールを使用して Red Hat Enterprise Linux 7.6 で作成された名前スペースは、BIOS セットアップまたは UEFI IPMCTL ツールで検査されたときに「Critical」ヘルス状態である可能性があります。ただし、名前スペースは正常であり、その機能は影響を受けません。</p> <p>これは、Intel® Optane™ Data Center persistent memory MODULE HII および UEFI ipmctl tool の問題です。</p> <p>Intel IPS のケースのフィールド。</p>	<p>RHEL 7.6 バージョン 4.20.13-200.fc29 以降のカーネルを使用します。名前スペースは正常であり、その機能は影響を受けません。</p>	<p>4.0(4a) B および C</p> <p>4.0 (4e)B および C で解決済み</p>
CSCvn81521	<p>Intel® Optane™ データセンターの永続メモリモジュールが 2LM (メモリモード) であるシステムでは、同じチャネル上の DDR4 DIMM (近メモリとして設定されている) でエラーが発生した場合、修正不可能なエラーが永続メモリモジュールに記録されます。</p> <p>Intel IPS のケースのフィールド。</p>	<p>MCAOut ファイルを調べて、実際に障害が発生した DIMM の場所を特定します。</p>	<p>4.0(4a) B および C</p> <p>4.0 (4e)B および C で解決済み</p>
CSCvp08356	<p>Intel® Optane™ データセンターの永続メモリモジュールがシステムに装着されており、システムが動作している場合、場合により誤って修正不可能なエラーが DIMMA1 で報告される場合があります。機能への影響はありません。</p> <p>Intel IPS のケースのフィールド。</p>	<p>Cisco UCS Manager で [Reset All Memory errors (すべてのメモリエラーをリセットする)] を使用してエラーをクリアします。</p>	<p>4.0(4a) B および C</p>

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvo78920	<p>Intel® Optane™ データセンターの永続メモリ モジュールが搭載されたシステムが起動した場合、場合によっては、永続メモリ モジュールのヘルス状態が「機能していない」状態になることがあります。場合によっては、AC 電源の再投入後に永続メモリ モジュールが回復（「正常」ヘルス状態）します。永続メモリ モジュールが「機能していない」状態になり回復しない場合は、交換する必要があります。</p> <p>Intel IPS のケースのフィールド。</p>	既知の回避策はありません。	<p>4.0(4a) B および C</p> <p>リリースで更新された Intel ファームウェアで解決 4.0 (4c)</p>
CSCvp38545	<p>Intel® Optane™ データセンター永続メモリ モジュールは、HiBit DIMM を使用しているチャンバーでテストされたときに「機能しない」ヘルス状態になります。AC 電源の再投入により、障害が発生した永続メモリ モジュールが「致命的な障害」状態になります。</p> <p>Intel IPS のケースのフィールド。</p>	既知の回避策はありません。	<p>4.0(4a) B および C</p> <p>リリースで更新された Intel ファームウェアで解決 4.0 (4c)</p>
CSCvp38555	<p>Intel® Optane™ データセンターの永続メモリ モジュールは、最初の電源投入時に「機能していない」ヘルス状態に移行します。</p> <p>Intel IPS のケースのフィールド。</p>	既知の回避策はありません。	<p>4.0(4a) B および C</p> <p>リリースで更新された Intel ファームウェアで解決 4.0 (4c)</p>

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvp38564	<p>Intel[®] Intelligent Power Technology Node Manager (NM) PTU は、App Direct モードの Intel[®] Optane[™] DC 永続メモリモジュールでは動作しません。したがって、電力特性評価の精度が低下します。</p> <p>Intel IPS のケースのフィールド。</p>	永続メモリモジュールがシステムで検出された場合、BIOS は応答または無限ループを防止するために NMPTU をロードしません。	4.0(4a) B および C
CSCvp37389	一部の特定の状況では、インフライトの書き込みトラフィックで DDRT クロック停止が突然発生する可能性があります。これにより、Intel [®] Optane [™] Data Center 永続メモリモジュールが「致命的な障害」状態になり、永続状態になる可能性があり、メモリモジュールのメディアが無効になります。	既知の回避策はありません。	4.0(4a) B および C

表 23: Intel® Optane™ データセンター永続メモリ モジュール: Cisco の未解決の問題

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvp30026	Intel® Optane™ データセンターの永続メモリ モジュールは、セキュアなパスフレーズが有効になっている Cisco UCS Manager によって管理されています。その後、永続メモリ ポリシーが削除され、サーバがホスト管理モードに移行しました。これが発生すると、領域と名前スペースは実際には「正常」状態であっても、Cisco UCS Manager では「管理不能」として報告されます。これはレポートの問題です。機能への影響はありません。	ホストベースのツールを使用し、永続メモリ モジュールのセキュリティを無効にします。サーバを再認識します。	4.0(4a)B
CSCvo52036	App Direct モードの Intel® Optane™ Data Center 永続メモリ モジュールが搭載された Red Hat Enterprise Linux 7.6 にマウントされている既存の名前スペースとともに、名前スペースを追加することで、Red Hat ブート障害が発生する可能性があります。	必要な名前スペースが作成され、マウントポイントとして一度だけ適用されていることを確認します。その後、さらに名前スペースを追加することはできません。	4.0(4a)B
CSCvn64709	ホスト管理モードの Intel® Optane™ データセンター永続メモリ モジュールの場合、BIOS セットアップでパスフレーズを設定することによってセキュリティを有効にすることはできません。セキュリティを有効にするには、Intel UEFI または OS ツールを使用します。	パスフレーズを設定するには、ホストベースのツール IPMCTL ツールを使用します。	4.0(4a)B

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvp36938	<p>[Reset To Factory Default (工場出荷時のデフォルトにリセットする)] 操作が実行されると、[Inventory (インベントリ)]の下で、永続メモリ モジュール設定ステータスが「ホスト管理状態」として表示されます。これは、永続メモリポリシーがサービスプロファイル(UCS管理メモリモジュール)に接続されている場合に発生します。これはレポートの問題です。後続の永続メモリポリシーの変更により、設定がUCS管理モードに復元されます。</p>	領域にスペースがある場合は、最小サイズの名前スペースを追加すると、この状態がクリアされ、永続メモリモジュールの設定ステータスが「 設定済み 」と表示されます。	4.0(4a)B
CSCvp31928	UCS管理モードのIntel [®] Optane [™] データセンター永続メモリモジュールでは、ローカルセキュリティがサーバに設定された後で、そのサーバを削除できます。これにより、セキュリティが無効になります。	ホストベースのツールを使用し、永続メモリモジュールのセキュリティを設定します。	4.0(4a)BおよびC
CSCvp40415	<p>Cisco UCS Manager 4.0(4a)にアップグレードすると、サービスプロファイルの関連付け中に、CシリーズおよびBシリーズM5サーバで「永続メモリ設定が一致しません」という警告が表示されます。</p> <p>機能への影響はありません。関連付けは問題なく完了し、インストールされている場合は、サーバはホストOSで正常に起動します。</p>	既知の回避策はありません。	4.0(4a)A

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvo84482	Intel® Optane™ データセンターの永続メモリ モジュールの場合、Cisco UCS Manager の [health (ヘルス)] タブには、メッセージの重大度に関係なく、最新のヘルス メッセージのみが表示されます。したがって、重大度の低いメッセージが、より重大度の高いメッセージを上書きする可能性があります。	ヘルス メッセージの完全なリストについては、CIMC ログを参照してください。	4.0(4a)B

表 24: ファブリック インターコネクト

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvp23834	UCS 6454 FI のローカル管理プロンプトからの FTP は機能しません。端末はループでスタックします。	SCP を使用して、FI からファイルまたはログをコピーします。	4.0(4a)A

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvo06391		銅のトランシーバ/ケーブルアセンブリを光トランシーバと光ファイバケーブルと交換します。	4.0(4a)A 4.0(4c)で修正されました。

不具合 ID	症状	回避策	影響を受ける最初のバンドル
	<p>UCS C125 M5 および C480 M5 サーバの検出が「Discover Bmc Preconfig Pnu OS Peer」で失敗しました。</p> <p>UCS VIC アダプタのイーサネット インターフェイスでは、次のいずれかの症状が見られます。</p> <ul style="list-style-type: none"> • イーサネット物理リンクステータスが「ダウン」と表示されます • イーサネット PC プロトコル エラー <p>FEX サーバ インターフェイスでは、イーサネット物理リンクのステータスは「アップ」と表示されます。</p> <p>これは、UCS VIC アダプタカードの特定のモデルが特定のトランシーバ/ケーブルアセンブリ モデルを使用して、Nexus FEXes の特定のモデルに接続されている場合に発生します。これらのモデルは次のとおりです。</p> <p>トランシーバメディアタイプ: 10G-CU</p> <p>UCS VIC アダプタ モデル:</p> <ul style="list-style-type: none"> • VIC 1455 および 1457 • VIC 1455 <p>Nexus FEX モデル:</p> <ul style="list-style-type: none"> • 10 ギガ-ビット C2348UPQ N2K <p>FEX NX OS バージョン: 4.0 (1d)、4.0 (2c)、4.0 (3a)</p>		

不具合 ID	症状	回避策	影響を受ける最初のバンドル
	<p>Cisco UCS Manager インフラバンドル バージョン: 4.0 (1d)、4.0 (2d)、4.0 (3a)</p> <p>次のトリガー イベントのいずれか:</p> <ul style="list-style-type: none"> • FEX サーバインターフェイス (HIF) の物理リンクフラップ • サーバの再起動 		
CSCvp31766	ブレードサーバを Cisco UCS Manager リリース 4.0 (4a) にアップグレードした後、VM の VM-FEX インターフェイスを使用すると、接続が失われます。	ファームウェアを 4.0 (4c) にアップグレードするか、以前の作業リリースにファームウェアがダウングレードされます。	4.0(4a)C 4.0 (4c)C で解決済み
CSCvp89594	Cisco UCS Manager 4.0 (4a) にアップグレードすると、接続中に 6454 ファブリック インターコネクットの片側で NX OS がハングし、コマンドプロンプトが表示されなくなり、サーバが ssh セッション中に NX OS に接続できなくなります。	ファブリック インターコネクートをリブートします。	4.0(4a) A 4.0 (4c)A で解決済み
CSCvo18110	リンク フラップが発生しているネームスペースへのファイバチャネルから NVMe へのパスは失われます。	ホストをリブートします。	4.0(4a) A 4.0 (4c)A で解決済み

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvp49398	<p>6454ファブリックインターコネクに直接接続されたneNICドライババージョン 1457</p> <p>1.0.27.0 を使用する UCS C220 M5サーバで、各ファブリックで2~25GE インターフェイスを使用して、ファブリックインターコネクがリブートされると、トラフィックは75秒間ドロップします。この問題は、ファブリック フェールオーバーが発生している単一ファブリック上で、vNICを使用した RHEL でも発生しました。</p>	なし	<p>4.0(2b)A</p> <p>4.0(4a) A</p>
CSCvq26156	<p>UCS C-Series サーバから 4.0(4c) C-Bundle へアップグレードすると、Cisco 12G Modular SAS HBA により一部の Intel S4500 ディスク ドライブの検出/通信が停止されます。これにより、これらのドライブのソフトウェアアップグレードが失敗します。</p> <p>この問題が発生するのは、コントローラファームウェアバージョンが09.00.00.06 の occures のみです。</p>	<p>アップグレード前 - ホストファームウェア パッケージで、Raid コントローラアップグレードを排除します。</p> <p>アップグレード後 - Raid コントローラ ファームウェアをバージョン 00.00.00.58 にロールバックします。</p>	<p>4.0(4a)C</p> <p>4.0 (4d)A で解決済み</p>

表 25: BIOS

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvn73435	システムがリポートストレスまたはその他のストレス下にある場合、Cisco IMC システム イベントログ (SEL) は、システムに存在する各 第二世代インテル® Xeon® Scalable プロセッサに対して「アップ修正可能なエラー」を報告します。	プロセッサ C の状態を BIOS のデフォルトのままにします。	4.0(4a)B

表 26: BMC

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvp68182	リリース 3.2 (3j) より前の Cisco UCS Manager リリースから Cisco UCS Manager リリース 4.0 (4a) にアップグレードするか、Cisco UCS Manager リリース 4.0 (1a)、4.0 (1b)、または 4.0 (1c) から Cisco UCS Manager リリース 4.0 (4a) にアップグレードすると、Cisco UCS B200 M5、B480 M5、および S3260 M5 サーバの小規模なサブセットが発生し、BMC への IOM 接続をアクティブ化したり、損失したりしません。	サーバがすでに問題なく Cisco UCS Manager リリース 4.0 (4a) にアップグレードされている場合は、引き続きリリース 4.0 (4a) を使用してください。 3.2 (3j)、4.0 (1a)、4.0 (1b)、または 4.0 (1c) よりも前の Cisco UCS Manager リリースを実行しているサーバの場合は、Cisco UCS Manager リリース 4.0 (2)、4.0 (4b) 以降にアップグレードします。 詳細については、『Cisco ソフトウェア遅延通知』を参照してください。 https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/SA/SW_Deferral_Notice_CSCvp68182.html	4.0(4a)B、 4.0(4a)C

表 27:外部コントローラ

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvm15304	PCI Switch1 および PCISwitch 背面に 2 個の Intel ColdStream ドライブが搭載された UCS C480 M5 サーバでは、何回かのリブート後に Intel ColdStream Next 750GB ドライブリンクが縮退状態になります。	既知の回避策はありません。	4.0(4a)C
CSCvo39645 CSCvo89921	複数のリブート時に CATERR/IERR が発生し、POST 中にシステムが応答しなくなります。この問題は、mSwitch に接続されている設定上で、NVMe ドライブを搭載しているサーバで発生します。	この問題が発生した場合は、ウォームリブートを実行します。	4.0(4a)C
CSCvo31178	S シリーズ サーバ上の HGST HUS726020ALS210 の特定のドライブ モデルで、ローカル ディスク ファームウェアのアクティベーションに失敗します。	既知の回避策はありません。ドライブ ファームウェアを更新する必要がある場合は、TAC にお問い合わせください。	4.0(4a)C
CSCvp23760	Cisco UCS C シリーズ サーバを搭載したセットアップで Cisco UCS Manager リリース 4.0 (4a) にアップグレードすると、Qlogic アダプタの 1 個のポートが接続解除済みとして示されます。	以前に動作していたリリースにファームウェアをダウングレードします。	4.0(4a)C 4.0(4b)C で解決済み

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvo99427	一部の UCS ドメインに対する UCS Central の可視性が失われます。UCSM DME ログは、Central の証明書の期限が切れていることを示します。	自己署名キーリングを使用している場合は、UCS Central でデフォルトのキーリングを再生成します。 <pre>UCSC # connect policy-mgr UCSC(policy-mgr)# scope org UCSC(policy-mgr) /org# scope device-profile UCSC(policy-mgr) /org/device-profile # scope security UCSC(policy-mgr) /org/device-profile/security # scope keyring default UCSC(policy-mgr) /org/device-profile/security/keyring* # set regenerate yes UCSC(policy-mgr) /org/device-profile/security/keyring* #commit-buffer</pre> <p>サードパーティの証明書を使用している場合は、デフォルトのキーリングを再生成し、デフォルトのキーリングに切り替えてから、サードパーティの証明書キーリングに戻します。</p>	4.0(4a)C 4.0 (4c)C で解決済み
CSCvo48003	UCS M4 サーバでは、Patrol スクラブ中に修正不可能な ECC エラーが検出されます。CPU IMC (統合メモリ コントローラ) の Patrol Scrubber が修正不可能な ECC エラーを検出すると、切り捨てられた DIMM アドレス (4KB ページ境界) をマシンチェックバンクに記録します。	交換する前に、システム ログを確認して、修正不可能な ECC エラーが正しい DIMM に記録されているかどうかを確認します。	4.0(4a) B 4.0 (4c)B で解決済み

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvr07248	UCS 管理 GUI の機器カテゴリの下で、電源グループの[ポリシー (Policy)] ページには[一般 (General)] タブの情報のみが表示されます。シャーシ、ラックユニット、FEX、FI、障害、およびイベントのタブには情報が表示されません。	CLI を使用して、電力グループ情報を取得します。	4.0(4a)A 4.0 (4e)B で解決済み

リリースで未解決の問題 4.0(2a)

次の問題がリリース 4.0(2a) 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
CSCvo13678	NVIDIA GPU が搭載された UCS M5 ラック サーバは、Cisco UCS Manager リリース 4.0 (2) ラック サーバファームウェアのインストール中に検出に失敗します。これは、svc_sam_bladeAG プロセスがクラッシュし、コア ファイルが生成されることに起因します。	この問題が発生した場合は、Cisco UCS Manager リリース 4.0 (2) よりも前のリリースにダウングレードします。	4.0(2a)A 4.0(2d)A で解決済み
CSCvh18287	Cisco C240 M5 サーバでは、エラー コード F0776 と、存在しないディスクが動作不能であることを示す障害メッセージが表示されなくなりました。	障害メッセージは存在しないディスクに対してのみ表示されるため、問題ではありません。	4.0(1a)C 4.0(2a)C

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvk63036	<p>Cisco UCS ファブリック インターコネクトペアと Cisco ファイバチャネルスイッチ間に SAN ポートチャネルまたは トランキングを形成できません。この場合、スイッチの組織固有 ID (OUI) は次のいずれかになります。</p> <ul style="list-style-type: none"> • 003a9c • 000831 • d0a5a6 	<p>ポートチャネルを使用せずに単一の F ポートリンクを使用します。UCS FI および MDS では、トランクモードをオフにする必要があります。</p>	<p>4.0(2a)A 4.0(2b)A で解決済み</p>
CSCvn38097	<p>ケーブルが引っ張られて再び接続されるか、リンク ダウン およびリンク アップが発生する他の同様の動作が実行されると、次のスタックトレースを使用で FC NVMe ストレージを備えた SLES 12 SP3 ホストがクラッシュする可能性があります。</p> <pre>[809.738358] Call Trace: [809.739728] [<ffffffff81302b58>] blk_mq_run_hw_queues+0x48/0x90 [809.741102] [<ffffffff8130441c>] blk_mq_requeue_work+0x10c/0x120 [809.742454] [<ffffffff810989e4>] process_one_work+0x154/0x410 [809.743803] [<ffffffff810995c6>] worker_thread+0x116/0x4a0 [809.745145] [<ffffffff8109ead9>] kthread+0xc9/0xe0 [809.746463] [<ffffffff81616505>] ret_from_fork+0x55/0x80 [809.752620] DWARF2 unwinder stuck at ret_from_fork+0x55/0x80 [809.753954]</pre>	<p>既知の回避策はありません。この問題を解決するには、NVMe コアを修正する必要があります。</p>	<p>4.0(2a)B および C</p>

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvn50292	UCS 6454 ファブリック インターコネクタは、トリガーなしで、スラブ割り当ての IGMP hap がリセットされて再起動します。この問題は Cisco UCS Manager コンテナの再起動時に観測されましたが、同じトリガーまたは異なるトリガーで再度観察されたことはありませんでした。	既知の回避策はありません。ファブリック インターコネクタは、これらの条件で再起動します。	4.0(2a)A
CSCvn66725	UCS 6454 ファブリック インターコネクタに接続されている UCS M4 サーバ上で、リモート キー管理相互運用性プロトコル (KMIP) サーバを使用して、自己暗号化ドライブ (SEDs) のドライブセキュリティを有効にしようとしたときに、サービス プロファイルの関連付けが「セッションの作成に失敗しました-要求された操作のタイムアウト」というエラー メッセージで失敗しました。	既知の回避策はありません。	4.0 (1c) B 4.0(4a)B で解決済み
CSCvn57345	Cisco Intersight で設定、登録、要求、および接続された UCS デバイスの Cisco UCS Manager フルステートバックアップ ファイルを復元した後、デバイスは Cisco Intersight で接続解除済みとして表示されます。	この問題が発生した場合は、次の手順を実行します。 <ol style="list-style-type: none">1. デバイス コネクタを再設定し、クラウドに登録します。2. デバイスをクラウド イベントリから削除します。3. デバイス ID と新しい要求コードを使用して、デバイスを再度要求します (デバイス MO ID は新規になります)。	4.0(2a)A 4.0(4a)A で解決済み

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvo58393	<p>Cisco UCS Manager リリース4.0 にアップグレードした後、FCoE ポートチャネルが起動せず、メンバリンクが管理者としてダウンしていることを示しています。次のエラーが表示されます。</p> <pre>Severity: Critical Code: F999676 Last Transition Time: 2019-02-26T03:19:45.668 ID: 23387272 Status: None Description: [FSM:FAILED]: Uplink fc port configuration on B (FSM:sam:dme:SwFcSanBorderDeploy) - Remote-Invocation-Error: [FSM:STAGE:REMOTE-ERROR]: Result: service-unavailable Code: unspecified Message: (sam:dme:SwFcSanBorderDeploy:UpdateConnectivity) Affected Object: sys/switch-B/border-fc Name: Fsm Sam Dme Sw Fc San Border Deploy Fsm Fail Cause: Fsm Failed</pre>	<p>この問題が発生した場合は、次の手順を実行します。</p> <ul style="list-style-type: none"> イーサネット/FCoE ポートでシャットダウン/非シャットダウンを実行します。 FCoE ポート ロールの設定を解除し、再設定します。 FCoE アップリンク ポートのロール速度を任意の速度に変更します (Cisco UCS Manager CLI を使用)。 	4.0(2a)A 4.0(4a)A で解決済み
CSCvo66721	<p>電源投入/電源切斷、ポートグループの変更、またはVMotionの結果として、VMのピン接続が変更された後、そのVMのMACアドレスがピン接続されていないFIのMACアドレステーブルからただちに削除されません。</p>	<p>この問題が発生した場合は、<code>info_ifacl_label</code> コマンドを使用して <code>info_ifacl_label = 0x00000021</code> を変更します。</p> <p>この問題の回避策として、<code>info_ifacl_label</code> の既存の値の5番目のビットを設定します。</p> <p>ポートのシャットダウン/非シャットダウンが発生するたびに、回避策を適用します。</p>	4.0(2a)A 4.0(4a)A で解決済み

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvn91826	<p>Cisco VIC 14xx アダプタを使用した設定では、ラック サーバ ID がラック サーバ ID の範囲 (1~99) を超えた場合、サーバ検出が失敗することがあります。</p> <p>次のエラー メッセージが表示されることがあります。</p> <pre>ID: 101 Server: sys/rack-unit-101 FSM 1: Remote Result: Service Unavailable Remote Error Code: 1002 Remote Error Description: command chassis associate 101 chassis-serial xxxxx module-serial xxxxx port-profile ucsm_internal_rackserver_portprofile module-side left may need to break down at 8 Status: Discover Sw Configure Port Channel Local Previous Status: Discover Sw Configure Port Channel Local Timestamp: 2019-01-12T23:00:39.348 Try: 2 Flags: 0 Progress (%): 3 Current Task: Configuring port channel for server 101 (FSM-STAGE:sam:dme:</pre>	<p>影響を受けるサーバをデコミッションし、99 よりも小さいサーバ ID を持つ同じサーバを再稼働します。</p>	<p>4.0(2a)A 4.0(2b)A で解決済み</p>
CSCvk26441	<p>UCS 6454 ファブリック インターコネクで Cisco UCS Manager リリース 4.0(2a) を実行している場合、グループ マップ ルールに aaa および read-only 以外のロールがあると、LDAP ユーザー ログインに失敗します。</p>	<p>既知の回避策はありません。</p> <p>この問題が発生した場合は、Cisco UCS Manager をリリース 4.0(2b) またはそれ以降のリリースにアップグレードしてください。</p>	<p>4.0(2a)A 4.0(2b)A で解決済み</p>

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvk53356	UCS 6454 ファブリック インターコネクで Cisco UCS Manager リリース 4.0(2a) を実行している場合、パスワード復元の手順を使用して管理者パスワードを復元できません。	既知の回避策はありません。 この問題が発生した場合は、Cisco UCS Manager をリリース 4.0(2b) またはそれ以降のリリースにアップグレードしてください。	4.0(2a)A 4.0(2b)A で解決済み
CSCvn60002	VNICs および VHBA では、電源投入またはリンクフラップ後の物理リンクの起動における応答時間が悪化します。 Sanboot 用に設定されたサーバが起動に失敗する場合があります。これは、最初のサーバの brup、物理リンクフラップ、または IOM リブートで発生する可能性があります。	Sanboot が失敗した場合は、サーバを再起動します。	4.0(2a)A 4.0(2d)A で解決済み
CSCvo04128	E モードで設定され、UCS 6454 ファブリック インターコネクでサポートされているファイバチャネルポートは、ブートまたはリンクフラップ後にオンラインになる際に時間がかかる可能性があります。	回避策はありません。	4.0(2a)A 4.0(2d)A で解決済み
CSCvo22832	Cisco UCS Manager VIC 14xx シリーズアダプタを使用して UCS 6454 ファブリック インターコネクに直接接続されている連携 C シリーズサーバは、CDP/LLDP パケットをキャプチャできません。これは、ファブリック インターコネクがプラットフォーム ヘッダーを誤って作成して、パケットを送信するための物理インターフェイスが設定されていないことに起因します。	回避策はありません。	4.0(2a)A 4.0(2d)A で解決済み

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvo91744	<p>Cisco UCS Manager リリース 4.0(2) にアップグレードした後、MAC セキュリティが拒否に設定されたネットワーク制御ポリシーが設定されている場合、一部のサーバでは、アップグレードされたファブリック インターコネクで VIF がダウンしているように表示されます。Cisco UCS Manager は影響を受けるサーバで、次の障害を表示します。</p> <pre>Severity: Warning Code: F78413 Status: None Description: [FSM:STAGE:REMOTE-ERROR]: Result: service-unavailable Code: unspecified Message: ERROR: Failed to update maximum value for object Physical Associate Svcs for object Affected Object: sys/chassis-1/blade-4 Name: Fsm Sam Dme Compute Physical Associate Remote Inv Cause: Sw Config Hostoslocal Failed Type: Fsm Acknowledged: No Occurrences: 5 Creation Time: Original Severity: Warning Previous Severity: Warning Highest Severity: Warning</pre> <p>svc_sam_portAG ログでは、次のことが確認されます。</p> <pre>[MAJOR] [] [] [app_sam_portAG:config] Error enabling the port security for the ethernet VIF, details: ERROR: Failed to update maximum value</pre>	アップグレード前にネットワーク制御ポリシーを削除します。	4.0(2a)A 4.0(4a)A で解決済み

リリースで未解決の問題 4.0(1d)

次の問題がリリース 4.0(1d) 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
CSCvq28261	UCS 6324 ファブリック インターコネクトを搭載した UCS 2304 ファブリック エクステンダを使用していたブレードシャーシ上の電源装置は、ファブリック エクステンダファームウェアのアップグレード中に温度障害によってシャットダウンされました。PSU は再装着されるまで、その後に電源をオンにできませんでした。電源装置を取り付け直すには、完全なシャーシの停止が必要になる場合があります。	温度障害がある場合は、ファブリック エクステンダファームウェアをアップグレードしないでください。アップグレードする前に、温度障害をクリアします。	4.0(1d)B 4.0 (4c)B で解決済み
CSCvr08327	UCS 2204 または UCS 2208 ファブリック エクステンダを使用していたブレードシャーシ上の電源装置は、ファブリック エクステンダファームウェアのアップグレード中に温度障害によってシャットダウンされました。PSU は再装着されるまで、その後に電源をオンにできませんでした。電源装置を取り付け直すには、完全なシャーシの停止が必要になる場合があります。	温度障害がある場合は、ファブリック エクステンダファームウェアをアップグレードしないでください。アップグレードする前に、温度障害をクリアします。	4.0(1d)B 4.0 (4e)B で解決済み

リリースで未解決の問題 4.0(1c)

次の問題がリリース 4.0(1c) 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
CSCvo19661	UCS 6454 ファブリックインターコネクタは、ファブリックインターコネクタの管理 IP アドレスをブロードキャストする代わりに、LLDP アップストリーム ACI リーフとダウンストリームを介して、CDP を介して ESXi ホストに KVM アウトオブバンド IP アドレスをブロードキャストしています。	この問題は、送信される正しい CDP または LLDP 情報に依存し、ACI VMM の EPG に影響を与える可能性があります。 ACI VMM を使用する場合、ポリシーを事前プロビジョニングに変更すると、予想しない問題を回避できます。	4.0(1c)A 4.0(2e)A で解決済み

リリースで未解決の問題 4.0(1a)

次の問題がリリース 4.0(1a) 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
CSCvm66006	サービス プロファイルの再設定と再関連付けが完了すると、hifpc メンバのいずれかにハッシュされたトラフィックがドロップされます。これは、DCBX がブレードサーバの影響を受けるインターフェイスに適切にコンバインドしていない場合に発生します。	この問題を回復するようにサーバを再認識させます。 この問題を回避するには、ブレードサーバの連続または同時アソシエーションと再アソシエーションを実行しないでください。	4.0(1a)A 4.0(4a)A で解決済み
CSCvr98210	アプライアンス ポートまたは FCoE ストレージポートを搭載したシステムで Cisco UCS Manager リリース 3.2 からリリース 4.0 以降にアップグレードする場合、LLDP はデフォルトで無効になります。FCoE または LLDP を必要とする接続は、動作を停止する可能性があります。	接続を回復するには、Cisco UCS Manager リリース 4.0 へのアップグレード後に、ネットワーク制御ポリシーで LLDP を無効にしてから再度有効にします。	4.0(1a)A

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvo64592	Ucs C シリーズサーバと UCS 6454 ファブリックインターコネクットの Cisco UCS Manager リリース4.0を統合しようとする と、サーバディスクが失敗します。	この問題が発生した場合は、Cisco UCS Manager コンテナまたは FI を再起動します。	4.0(1a)A A 4.0(4a)および 4.0(2e)A で解決済み
CSCvm23975	Cisco UCS Manager によって管理されている C シリーズラックサーバおよびすべての V シリーズ GPU アダプタを搭載したシステムでは、GPU モードを Cisco UCS Manager のグラフィック ポリシーを使用して変更できません。 これは、C シリーズラックサーバに次の GPU アダプタが 1 個以上ある場合に発生します。 <ul style="list-style-type: none"> • UCSC-GPU-V100-16G • UCSC-GPU-V100-32G 	この問題が発生した場合は、サポートされているすべての OS でネイティブ NVIDIA 「nvidia-smi」ユーティリティツールを使用して、グラフィック モードを設定します。	4.0(1a)A 4.0(2a)A で解決済み

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvm14726	<p>新しい SPI フラッシュ デバイスを搭載した Cisco UCS 6324 ファブリック インターコネク トは、以前のソフトウェア リリースでは起動できません。これは、6324 ファブリック インターコネク トで使用されている元の SPI フラッシュ デバイスが生成されなくなったためです。したがって、ピン互換性のある交換パーツが転送先として使用されています。ただし、ベンダーとパーツ ID の変更により、新しいパーツが搭載された 6324 ファブリック インターコネク トは、新しいパーツをサポートしている OS バージョンでのみ動作します。</p>	<p>新しい SPI フラッシュ デバイスで Cisco UCS 6324 ファブリック インターコネク トを使用する場合は、6324 ファブリック インターコネク トのハードウェア変更後に実行されたリリースのみを使用します。</p>	<p>4.0(1a)A 4.0(1c)A で解決済み</p>
CSCvk30528	<p>UEFI ブートモードでは、Cisco UCS マネージド C シリーズ サーバが、EMC ストレージ デバイスに設定されている iSCSI LUN にインストールされている RHEL または ESXi OS で起動できませんでした。代わりに、再起動するたびに、サーバが UEFI シェル プロンプトを開始します。</p> <p>LUN が EMC 以外のストレージ デバイス由来である場合、サーバは予想どおりに OS にブートします。</p>	<p>サーバが UEFI シェル プロンプトを開始した後、シェル プロンプトを終了すると、サーバが OS に対してブートします。</p>	<p>4.0(1a)C 4.0(1c)C で解決済み</p>

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvm17259	Cisco UCS Manager 統合 C シリーズラックサーバを搭載したシステムでは、サーバのサービスプロファイルを設定した後に、ファームウェアポリシーのホストファームウェアパック (HFP) に、UCSC gpu V100-32G GPU のファームウェアが表示されませんでした。	この問題が発生した場合は、次の手順を実行します。 <ul style="list-style-type: none"> • Cisco UCS Manager 管理モードからサーバをスタンドアロンモードに移行します。 • Host Update Utility (u) iso を使用してサーバを更新します。 • 更新が完了したら、Cisco UCS Manager 管理モードでサーバをバックアップします。 	4.0(1a)A 4.0(1b)A で解決済み
CSCvm10391	Cisco UCS 6454 ファブリックインターコネクタが、設定された SMTP サーバに Call Home メッセージを送信しません。	既知の回避策はありません。	4.0(1a)A 4.0(1b)A で解決済み

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvm03356	<p>Cisco UCS B シリーズ M3 サーバおよび C シリーズ M3 サーバは、CPU の投機処理とデータ キャッシュのタイミングを使用して権限情報を識別するエクスプロイトに対して脆弱な、Intel[®] プロセッサに基づいています。これらのエクスプロイトは、総称して L1 Terminal Fault (L1TF) と呼ばれています。</p> <ul style="list-style-type: none"> • CVE-2018-3615 (SGX に影響) は Foreshadow と呼ばれ、既存の Cisco UCS サーバに影響を与えます。これは、Cisco UCS M5 および旧世代サーバと、HyperFlex M5 および旧世代サーバは Intel[®] SGX テクノロジーを使用しないためです。 • CVE-2018-3620 (OS/システム管理モードに影響) および CVE-2018-3646 (仮想マシンモニタに影響) は、Intel[®] による L1 Terminal Fault 攻撃とも呼ばれます。これらの脆弱性は、サーバファームウェアバンドルに含まれている Intel から更新されたプロセッサマイクロコードを適用することによって軽減されます。また、該当するベンダーからのオペレーティングシステムとハイパーバイザのパッチも適用されます。 	<p>CVE-2018-3620 (OS/SMM) および CVE-2018-3646 (VMM) の修正には、Intel[®] から更新されたプロセッサマイクロコードを適用する必要があります。また、適切なベンダーからの関連オペレーティングシステムおよびハイパーバイザパッチも適用する必要があります。</p> <p>詳細については、次の Cisco セキュリティアドバイザリを参照してください。</p> <p>CPU サイドチャネル情報漏えいの脆弱性: 2018 年 8 月</p>	<p>4.0(1a)B、 4.0(1a)C</p> <p>3.2 (1d)B、3.2 (1d)C</p> <p>3.1 (1e)B、3.1 (1e)C</p> <p>2.2 (1b)B、2.2 (1b)C</p> <p>CSCvm03356 は 4.0(1a)B、4.0(1a)C で解決されます。</p>

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvm03351	<p>Cisco UCS B シリーズ M4 サーバ、C シリーズ M4 サーバ、S3260 M4 ストレージサーバ、HyperFlex M4 サーバは、CPU の投機処理とデータ キャッシュのタイミングを使用して権限情報を識別するエクスプロイトに対して脆弱です。これらのエクスプロイトは、総称して L1 Terminal Fault (L1TF) と呼ばれています。</p> <ul style="list-style-type: none"> • CVE-2018-3615 (SGX に影響) は Foreshadow と呼ばれ、既存の Cisco UCS サーバに影響を与えます。これは、Cisco UCS M5 および旧世代サーバと、HyperFlex M5 および旧世代サーバは Intel® SGX テクノロジーを使用しないためです。 • CVE-2018-3620 (OS/システム管理モードに影響) および CVE-2018-3646 (仮想マシン モニタに影響) は、Intel® による L1 Terminal Fault 攻撃とも呼ばれます。これらの脆弱性は、サーバファームウェアバンドルに含まれている Intel から更新されたプロセッサマイクロコードを適用することによって軽減されます。また、該当するベンダーからのオペレーティング システムとハイパーバイザのパッチも適用されます。 	<p>CVE-2018-3620 (OS/SMM) および CVE-2018-3646 (VMM) の修正には、Intel® から更新されたプロセッサマイクロコードを適用する必要があります。また、適切なベンダーからの関連オペレーティング システムおよびハイパーバイザパッチも適用する必要があります。</p> <p>詳細については、次の Cisco セキュリティアドバイザリを参照してください。</p> <p>CPU サイドチャネル情報漏えいの脆弱性: 2018 年 8 月</p>	<p>4.0(1a)B、4.0(1a)C</p> <p>3.2 (1d)B、3.2 (1d)C</p> <p>3.1 (1e)B、3.1 (1e)C</p> <p>2.2 (1b)B、2.2 (1b)C</p> <p>CSCvm03351 は 4.0(1a)B、4.0(1a)C で解決されます。</p>

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvm03339	<p>Cisco UCS B シリーズ M5 サーバ、C シリーズ M5 サーバ、および HyperFlex M5 サーバは、CPU の投機処理とデータ キャッシュのタイミングを使用して権限情報を識別するエクスプロイトに対して脆弱な、Intel® プロセッサに基づいています。これらのエクスプロイトは、総称して L1 Terminal Fault (L1TF) と呼ばれています。</p> <ul style="list-style-type: none"> • CVE-2018-3615 (SGX に影響) は Foreshadow と呼ばれ、既存の Cisco UCS サーバに影響を与えません。これは、Cisco UCS M5 および旧世代サーバと、HyperFlex M5 および旧世代サーバは Intel® SGX テクノロジーを使用しないためです。 • CVE-2018-3620 (OS/システム管理モードに影響) および CVE-2018-3646 (仮想マシン モニタに影響) は、Intel® による L1 Terminal Fault 攻撃とも呼ばれます。これらの脆弱性は、サーバファームウェア バンドルに含まれている Intel から更新されたプロセッサマイクロコードを適用することによって軽減されます。また、該当するベンダーからのオペレーティング システムとハイパーバイザのパッチも適用されます。 	<p>CVE-2018-3620 (OS/SMM) および CVE-2018-3646 (VMM) の修正には、Intel® から更新されたプロセッサマイクロコードを適用する必要があります。また、適切なベンダーからの関連オペレーティング システムおよびハイパーバイザ パッチも適用する必要があります。</p> <p>詳細については、次の Cisco セキュリティ アドバイザリを参照してください。</p> <p>CPU サイドチャネル情報漏えいの脆弱性: 2018 年 8 月</p>	<p>4.0(1a)B、 4.0(1a)C</p> <p>3.2 (1d)B、3.2 (1d)C</p> <p>3.1 (1e)B、3.1 (1e)C</p> <p>2.2 (1b)B、2.2 (1b)C</p> <p>CSCvm03339 は 4.0(1a)B、4.0(1a)C で解決されます。</p>

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvh06851	ドロップおよび非ドロップの両方の QoS クラストラフィックを送信しているアダプタが混雑を検出すると、IOM はアダプタにユーザー設定 PFC プライオリティ マップの不完全な値をアダプタに送信します。このため、すべての QoS クラスはドロップなしとして扱われ、アダプタは IOM へのドロップトラフィックと非ドロップトラフィックの両方を低速にします。	既知の回避策はありません。	3.2 (2b) A
CSCvi66859	VLAN グループが設定され、FI アップリンク インターフェイスにマッピングされているシステムでは、vNIC テンプレートまたは VLAN グループから VLAN が削除されると、予期しない停止が発生しました。	VLAN グループがアップリンクと vNICs の両方で使用されている場合は、VLAN が VLAN グループから削除される前に次の手順を実行します。 <ol style="list-style-type: none"> 1. VLAN をアップリンクに明示的に追加します。 2. VLAN グループから VLAN を削除します。 3. VLAN がすべての vNICs から削除されるまで待機してから、その VLAN をアップリンクから削除します。 	3.2 (2b) A 4.0(2a)A で解決済み
CSCvj17303	リリース 3.2 (3a) と 4.0(1a) 間の Cisco UCS Manager のアップグレードおよびダウングレード中に、httpd コアが検出されます。	既知の回避策はありません。 httpd が自動的に再起動します。	4.0(1a)A

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCux48594	Cisco UCS Manager をリリース 2.5 (2a) からリリース 3.1 以降のリリースにアップグレードすると、DME コアが発生します。	DME コアが発生してもアクションを実行しないでください。アップグレードプロセスは続行され、正常に完了します。	3.1 (1e) A
CSCvh69831	8 個の vNICs を搭載した Cisco UCS B260 または B460 M4 サーバを使用したセットアップでは、ESXi 6.0/6.5 をインストールした後、ホストポート 2 の vNICs のもう半分が ESXi で最初に順序付けられます。そのため、最初のインストール中の vNIC の順序は正しくありません。	NIC 配置ポリシーを手動で設定し、vNICs のもう半分が最初に順序付けされるようにします。 または vNICs のもう半分をホストポート 1 に手動で割り当てます。	3.1 (3b) B
CSCvj98360	BMC が DIMM を検出できず、次のメッセージが表示されてブレードサーバ検索が停止します。 DIMM 設定の不一致	ホストの電源をオフにし、BMC を再起動してこの状態から回復します。	4.0(1a)B 4.0(1d)B で解決済み
CSCvn49417	新しい UCS 6454 ファブリックインターコネクトを設定するときに、初期設定をブートすると、ファブリックインターコネクトが設定される前にネットワークアップリンクがオンラインになります。ネットワークリンクが早くオンラインになり、ブロードキャストストームがまれに発生する可能性があります。 さらに、CDP ネイバー情報が表示され、以前の展開からの UCS 6454 ファブリックインターコネクトの MAC アドレスがこの段階で学習されます。	このシナリオを回避するには、ファブリックインターコネクトの初期設定が完了するまでネットワークアップリンクがダウンしていることを確認します。 この問題が発生した場合は、アップストリームスイッチの接続をシャットダウンします。	4.0(1a)A

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvn22595	OS として Cisco UCS Manager 3.2(3d) ファームウェアおよび Red Hat Linux を実行しているシステムで、VIC 1340 および VIC 1380 アダプタを搭載した UCS B200 M5 サーバを使用している場合、同じバス ID を共有している vNICs は同じ入力出力メモリ管理ユニット (IOMMU) に割り当てられなくなります。	回避策はありません。	3.2(3d)B 4.0(2d)B で解決済み
CSCvn81327	Cisco 2304 IOM モジュールはクラッシュし、pick_next_task_rt をポイントするカーネルコア ダンプを生成します。この状態が発生した場合、ウォッチドッグタイマーによって再起動がトリガーされるまで、トラフィックの転送が停止します。しかし、再起動する前に影響を受けるモジュールへのトラフィックが失われても、ポートは引き続きアップ状態として表示されます。	回避策はありません。	3.2(2d)C 4.0(2d)C で解決済み
CSCvm66499	インバンド KVM VLAN が設定されていて、サーバ管理が FEX を介して接続されている場合、ファブリック インターコネクト クラスタ フェールオーバーの後に KVM の起動機能が機能しません。	サーバの再認識を実行します。	4.0(1a)C 4.0(2d)C で解決済み
CSCvh18287	Cisco UCS C240 M5 サーバでは、エラー コード F0776 と、存在しないディスクが動作不能であることを示す障害メッセージが表示されます。	該当なし。メッセージは、存在しないドライブを対象としています。	4.0(1a)A 3.2(1d)A 4.0(2d)A で解決済み

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvm66118	シリアル番号 LIT xxxxxx の PSU が、UCS 6300 シリーズ ファブリック インターコネク トに接続されたシャーシに挿入または再装着されると、ファブリック インターコネク トは PSU ファン障害を報告しま す。しかし、PSU LED は緑色 のままで、PSU とファンは引 き続き動作します。	PSU が必要ない場合は、PSU を取り付けないでください。この PSU の取り付けまたは移 動が必要な場合は、PSU の挿入後にファブリックインター コネク トを再起動します。	3.2(2f)B 4.0(2d)A で解 済み
CSCvm89871	Cisco UCS Manager UCS 6332 または 6332-16UP ファブリック インターコネク ト上の統合 C シリーズ ラックサーバは、 次の一連のアクションが発生 した場合に検出に失敗します。 1. アップリンク イーサネッ ト ポートチャネルの一部 であるポートを無効にしま す。 2. ポート チャネルからイ ンターフェイスを削除しま す。 3. ポート タイプをサーバと して再設定します。 4. サーバを再設定されたポー トに接続します。	1. ファブリック インターコネク トとラックサーバの 電源をオンにした状態 で、ケーブルを接続しま す。 2. FI ポートタイプをアッ プリンクとして設定しま す。 3. ポート タイプをサーバと して設定します。	3.1(2c)A 4.0(2d)A で解 済み
CSCvn82697	サブ組織でロケールが定義さ れている場合でも、リモート 認証されたユーザーはすべて の組織を認識できます。	なし	3.2(3g)A 4.0(2e)A で解 済み
CSCvn77413	6332 または 6332-16 ファブ リック インターコネク ト上の イーサネット ポートでは、入 力破棄回数が上昇しましたが、 パフォーマンスへの大きな影 響はありません。	ファブリック インターコネク トで作成された VLAN に対し て、アップストリーム VLAN を照合します。	3.2(3h) A 4.0(2e)A で解 済み

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvr04369		イーサネット自動ネゴシエーションプロトコルを使用するトランシーバタイプを使用します。これらのトランシーバは次のとおりです。 <ul style="list-style-type: none">• 40G CR• 100G CR	4.0 (4d)B 4.0 (4e)B で解決済み

不具合 ID	症状	回避策	影響を受ける最初のバンドル
	<p>Cisco UCS 14xx アダプタカードのイーサネットポートと接続されたスイッチポートのリンクステータスが、複数回起動できませんでした。一般的なケースでは、次の症状によってこの問題がさらに特徴的になります。</p> <ul style="list-style-type: none"> イーサネット物理リンクステータスはフラッピング (CSCvr09649) を維持します。 次のカウンタに正の値と増分があります。 <pre> dbgcli:2> bod-serdes_error uif lane nif ----- 0 0 0 ... linkup_failure = 1275 ... LINKUP_FAILED = 1275 </pre> <ul style="list-style-type: none"> 次のカウンタに正の値と増分があります。 <pre> dbgcli:2> bod-pcs_err 0 0 0-0: linkdown with pcs error happened 311 times </pre> <p>これらのカウンタは、次のリリース以降で使用可能になりました。Cisco UCS Manager (C バンドル) 4.0(4c)、CIMC/VIC (4e)、ファームウェア 5.0(3c)。</p> <p>この問題は、Cisco UCS VIC 1457 アダプタカードモデル (物理イーサネットポート 1) の限られた数のインスタンスで、25G 光トランシーバモジュールの制限付きセットを</p>		

不具合 ID	症状	回避策	影響を受ける最初のバンドル
	<p>搭載している場合に、実際に発生しています。</p> <p>問題の Manifestations は非常にまれであり、展開環境における次の要因に大きく依存します。</p> <ul style="list-style-type: none"> • Cisco VIC 14xx アダプタカードインスタンスおよびポートインスタンス: <ul style="list-style-type: none"> • Cisco UCS VIC 1455 • Cisco UCS VIC 1457 • Cisco UCS VIC 1495 • Cisco UCS VIC 1497 • イーサネット自動ネゴシエーションプロトコルを使用しないトランシーバモジュールインスタンス: <ul style="list-style-type: none"> • 10G CU • 10G Optical • 25G CU • 25G Optical • 40G Optical • 100G Optical • その他可能性のある環境条件。 		
CSCvr95393	TACACS ユーザーは、NOLOGIN ポリシーが設定されている場合でもファブリックインターコネクにログインできます。		4.0(1a) A

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvr83759	UCS Manager 3.2(3c) から 4.0(4c) にアップグレードした後、openSSH または SecureCRT を「パスワード」認証で使用すると、UCS Manager ファブリック インターコネクต์へのブレードサーバアクセスが失敗します。	なし	3.2(3e)A 4.0 (4h)A で解決済み
CSCvj70519	UCS 通信に使用されるポート 7162 は、6400 シリーズ ファブリック インターコネクต์で開かれています。	なし	4.0(1a)A 4.0 (4g)A で解決済み
CSCvr06387	UCS 6324 ファブリック インターコネクットの SNMP プロセスが繰り返しクラッシュします。次のメッセージと同様のメッセージが表示されます。 TIMESTAMP HOSTNAME %CALLHOME-2-EVENT: SAM_ALERT_DIAGNOSTIC_MINOR TIMESTAMP HOSTNAME と最後のメッセージが 2 回繰り返される TIMESTAMP HOSTNAME と最後のメッセージが 1 回繰り返される TIMESTAMP HOSTNAME %SYSMGR-2-SERVICE_CRASHED: サービス「snmpd」(PID XX) はシグナル 6 をキャッチしていません (コアは保存されます)。 TIMESTAMP HOSTNAME %CALLHOME-2-EVENT: スロット 1 の SW_CRASH snmpd が次のクラッシュ タイプでクラッシュしました: ステータスフル クラッシュ	該当なし	4.0(1a)A 4.0 (4g)A で解決済み

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvq37888	UCS M4 サーバでは、Cisco IMC のメモリが不足しているため、UCS マネージャと Cisco IMC 間の接続が失われます。ブレードを取り付け直すまで、接続を復元できませんでした。	UCS マネージャからブレードをリセットします。 ブレードを取り付け直します。 Cisco IMC IP アドレスの KVM ポートでポートスキャナの実行を停止します。デフォルトの KVM ポート番号は 2068 です。	4.0(1a)A 4.0 (4g)A で解決済み
CSCvq77449	UCS S3260 M5 サーバで CMC2 を再起動すると、両方のデュアル RAID コントローラで設定されているすべての仮想ドライブがオフラインになります。ブートドライブを除く他のすべての物理ドライブには、 外部構成 ステータスが表示されます。	サーバーを再起動して、 外部構成 ステータスを表示するドライブ構成を自動インポートします。 再起動中に自動インポートが失敗した場合は、TAC に連絡して設定をインポートしてください。	4.0(1a)C
CSCvr15733	負荷の下では、レート制限のシャットオフの問題により、vNIC becomex が永続的に機能しなくなります。	なし	4.0(1a)A 4.0 (4h)A で解決済み
CSCvs61735	UCS Manager は、Cisco 6400 シリーズファブリックインターコネク트의 IOM の全体的なステータスを正確には提供しません。	なし	4.0(1a)A 4.0 (4i)C で解決済み
CSCvt27869	6200 シリーズファブリックインターコネク트가 OOB メモリアクセスを検出すると、ファブリック インターコネク트가再起動します。	なし	4.0(1a)A 4.0 (4i)C で解決済み

動作の変更と既知の制限事項

txmit クレジット損失が発生しているファイバチャネルポートは無効になりました。

CSCvq76790: 4.0(4h) リリース以降、UCS ファブリック インターコネクットのファイバチャネルリンクは、txmitクレジット損失が発生しているポートを無効にします。デフォルトでは、UCS ファブリック インターコネクットは、ポート モニタ機能が FC ポートで2分間にわたって30しきい値を超えるクレジット損を検出すると、FCポートをエラーとして無効にします。メッセージ、if_index: < if_index_value > の fc ポートをエラーにより無効化 (error disable fc port, if_index: < if_index_value >)が、fcpc トレースログに記録されます。

この変更は、すべてのファイバチャネルタイプのポート、アップリンク、およびストレージアプライアンスのポートに影響します。

キャッシュされた IO ポリシーが有効になっている仮想ドライブを作成できません

CSCvn72355: Cisco UCS Manager リリース 4.0 (4) 以降では、**IO ポリシー**がキャッシュに設定されているシステムに仮想ドライブ (VD) を作成することはできません。VD を作成する間、キャッシュされた IO ポリシーは Cisco UCS Manager GUI および CLI、Cisco IMC および LSI Storage Authority (LSA) で無効です。デフォルトでは、**ダイレクト IO ポリシー**を使用して新しい VD が作成されるようになりました。キャッシュ IO ポリシーが設定されている既存の VD は、**直接 IO ポリシー**に変更されます。

Cisco UCS Manager リリース 4.0 (4) 以降のリリースのシステムでは、VD の作成時に**IO ポリシー**がキャッシュに設定されていません。リリース4.0(4)にアップグレードした後、ストレージプロファイルに対して **IO ポリシー**を**直接**に変更していることを確認します。

UCS 6454 ファブリック インターコネクットの場合、FSM ディスカバリの完了には時間がかかります

特定の条件下では、ファブリック インターコネクットのフェールオーバー後の FSM ディスカバリは、UCS 6200 シリーズおよび 6300 シリーズ ファブリック インターコネクットで実行する場合よりも、UCS 6454 ファブリック インターコネクットで完了する方が時間が長くなります。これは、UCS 6454 ファブリック インターコネクットに使用されているディスカバリ アルゴリズムが原因です。

Cisco UCS Manager のバージョンが UI のログイン画面に表示されなくなった

Cisco UCS Manager リリース 4.0 (4a) 以降では、Cisco UCS Manager のリリースバージョンは UI ログイン画面に表示されなくなりました。

WWN プールに許可される WWPN および WWNN の範囲

Cisco UCS Manager リリース 4.0(1a) 以降では、Cisco UCS 6454 FI の WWN プールに許可されている WWPN と WWNN の範囲は次のように変更されます。

20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF

to

20:00:00:00:00:00:00:00 to 20:FF:00:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:00:FF:FF:FF:FF:FF

WWPN の 3 番目のオクテットは **00** のままにする必要があります。

ファイバチャネルトラフィックが Cisco UCS インフラストラクチャを介して送信されると、送信元 WWPN は MAC アドレスに変換されます。WWPN プール範囲の変更は、送信元マルチキャスト MAC アドレスに変換できる値を回避するために実装されます。

MSwitch を使用した C480 M5 サーバ上のインフラストラクチャおよびホスト ファームウェアバージョンの互換性

CSCvp13552: C480 M5 サーバの場合、Cisco UCS Manager リリース 4.0 (4a) 以降では、MSwitch ファームウェア アップグレードの A バンドルと C バンドルの間の互換性が次のように変更されています。

	4.0 (4a) よりも前のホスト ファームウェア バージョン (C バンドル)	4.0 (4a) よりも後のホスト ファームウェア バージョン (C 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)	compatible	互換性なし
インフラストラクチャバージョン (A バンドル) 以降	互換性なし	compatible

MSwitch を搭載した C480 M5 サーバで、4.0 (4) よりも前のリリースからリリース 4.0 (4) に MSwitch ファームウェアをアップグレードするには、次の順序で実行します。

1. リリース 4.0(4) にインフラストラクチャ A バンドルをアップグレードします。
2. フロント MSwitches の invTag およびモデル名を更新するには、C480 M5 サーバのデコミッション/再稼働または再確認を実行します。
3. リリース 4.0(4) にインフラストラクチャ A バンドルをアップグレードします。

NVIDIA V100 シリーズ GPU のインフラストラクチャとホスト ファームウェアバージョンの互換性

CSCvp05259: Cisco UCS Manager リリース 4.0 (4a) 以降では、NVIDIA SXM2 V100 32GB および NVIDIA V100 PCIe 32GB GPU のファームウェアをアップグレードすると、A と C のバンドル間の互換性が次のように変更されました。

	4.0 (4a) よりも前のホスト ファームウェア バージョン (C バンドル)	4.0 (4a) よりも後のホスト ファームウェア バージョン (C 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)	compatible	互換性なし

	4.0 (4a) よりも前のホスト ファームウェア バージョン (C バンドル)	4.0 (4a) よりも後のホスト ファームウェア バージョン (C バンドル)
インフラストラクチャバージョン (A バンドル) 以降	compatible	compatible

UCS 6300 シリーズ ファブリック インターコネクットの ASIC 制限がパッシブ ケーブルで追加されました。

UCS 6300 シリーズ Fi は、アップリンク ポートを除き、パッシブ ケーブルをサポートします。FI の ASIC は自動ネゴシエーション (CSCvc98464) をサポートしていません。これは、アップリンク ポートで使用するためにアクティブなケーブルだけが推奨されているためです。

この制限は、自動ネゴシエーションをサポートしていないアップストリーム スイッチ ポートに非アップリンク ポートを接続する場合にも適用されます。パッシブ ケーブルを使用する場合 6300 シリーズ FI では自動ネゴシエーションが使用され、ピア スイッチ ポートはサポートしていないため、リンクが機能しない可能性があります。6300 シリーズ FI で自動ネゴシエーションを無効にすることはできません。そのため、このようなシナリオでは、アクティブなケーブルを使用することを推奨します。

ブートが RHEL 7.5 または 7.6 で応答しなくなり、usNIC 機能が影響を受けます

Cisco UCS Manager または Cisco IMC を使用して VIC で両方の usNIC デバイスがプロビジョニングされ、Intel または AMD Input Output Memory Management Unit (IOMMU) が有効になっている場合、Red Hat Enterprise Linux バージョン 7.5 または 7.6 が起動しなくなります。

これは、RHEL v 7.5 および v3.0 の Linux API シグニチャが `inbox usnic_verbs fnic.ko` ドライバで競合状態になり、ブートがハングしているためです。

この場合は、次の手順を実行します。

1. Intel または AMD IOMMU を無効にしてデバイスを起動します。
2. Cisco.com から `enic_verbs` または `usnic_verbs` ドライバをダウンロードし、インストールします。Inbox `usnic_verbs` ドライバとは異なり、これらのドライバはブート時にハングしません。
3. Intel または AMD IOMMU を再度有効にします。

ブートは正常に続行され、usNIC 機能が復元されます。

SSH を介してサーバにログインするための OpenSSH でのアルゴリズムのサポート

Cisco UCS Manager リリース 4.0 以降では、特定の安全でない暗号方式が UCS ファブリック インターコネクットによってブロックされます。SSH プロトコルを使用してサーバにログインするには、次のカテゴリで少なくとも 1 つのアルゴリズムをサポートする OpenSSH のバージョンを使用する必要があります。

- Cisco UCS Manager リリース 4.0(2a) からサポートされるキー交換アルゴリズム

- Cisco ファブリック インターコネクト 6454 の場合 :
 - ecdh-sha2-nistp256
 - ecdh-sha2-nistp384
 - ecdh-sha2-nistp521
 - diffie-hellman-group-exchange-sha256
 - diffie-hellman-group16-sha512
 - diffie-hellman-group18-sha512
 - diffie-hellman-group-exchange-sha1
 - diffie-hellman-group14-sha1

- Cisco Fabric Interconnect 6248、6324、および63xx の場合:
 - diffie-hellman-group-exchange-sha256
 - diffie-hellman-group16-sha512
 - diffie-hellman-group18-sha512

- Cisco UCS Manager リリース 4.0(4a) からサポートされるキー交換アルゴリズム
 - Cisco ファブリック インターコネクト 6454 の場合 :
 - ecdh-sha2-nistp256
 - ecdh-sha2-nistp384
 - ecdh-sha2-nistp521
 - diffie-hellman-group16-sha512
 - diffie-hellman-group14-sha1

 - Cisco Fabric Interconnect 6248、6324、および63xx の場合:
 - diffie-hellman-group-exchange-sha256
 - diffie-hellman-group16-sha512

- 暗号化アルゴリズム
 - aes128-ctr
 - aes192-ctr
 - aes256-ctr

- MAC アルゴリズム
 - hmac-sha2-256
 - hmac-sha2-512

UCS 6454 ファブリック インターコネクタでのプライオリティフロー制御とリンクレベルフロー制御の設定

UCS 6454 ファブリック インターコネクタのインターフェイスではプライオリティフロー制御 (PFC) 管理を**自動**として設定され、リンク レベル フロー制御 (LLFC) 管理が**オン**のとき、一制御 (PFC) admin には、PFC オペレーション モードは**オフ**および LLFC オペレーション モードは**オン**になります。

UCS 6300 シリーズおよび以前のファブリック インターコネクタで、同じ設定で PFC オペレーション モードが**オン**になっていて、LLFC オペレーション モードが**オフ**になる結果になります。

高速ブート用の UCS M5 BIOS トークン

Cisco UCS Manager リリース 4.0 (2) では、UCS M5 サーバのブート時間を改善するために次の BIOS トークンが導入されています。

- 適応型メモリ トレーニング コントロール
- OptionROM 起動最適化コントロール
- BIOS Tech メッセージ レベル コントロール

3 つのトークンすべてのデフォルト値が**有効**になっています。

サーババンドルが Cisco UCS Manager リリース 4.0 (2) にアップグレードされているが、インフラストラクチャバンドルがリリース 4.0 (2) にアップグレードされていない場合、サーバはこれらのトークンをデフォルト値で使います(**有効状態**)。このシナリオでは、これらのトークンを Cisco UCS Manager を使用して管理することはできません。

これらのトークンのポリシー レベル制御を取得するには、古いインフラストラクチャバンドルを続行し、Cisco UCS Manager カタログをリリース 4.0 (2) にアップグレードします。

LITE-ON 1050W PSU を搭載した UCS C240 M5 サーバのボードコントローラのアクティブ化は、Cisco UCS Manager リリース 4.0 (2) からのダウングレード中に失敗する可能性があります。

76 CSCvm08504: Cisco UCS Manager リリース 4.0(2) からダウングレードされたときに、LITE-ON 1050W PSU を搭載した UCS C240 M5 サーバのボードコントローラのアクティブ化は、検出プロセス中に失敗する可能性があります。次のエラー メッセージが表示されます。

エラー: PSU2 の更新に失敗しました

このエラーが発生した場合は、ダウングレードを再試行してください。

このエラーを回避するには、LITE-ON 1050W PSU を備えたシステムをダウングレードしないでください。

Cisco UCS Manager リリース 3.2 (3) 以降のリリースで導入されたサーバの物理ディスプレイが Java KVM コンソールに正しく表示されません

CSCvk24995: Java KVM コンソールでは、Cisco UCS Manager リリース 3.2 (3) 以降のリリースで導入された Cisco UCS Manager 管理 UCS サーバの物理ディスプレイが正しく表示されません。たとえば、C125 M5 サーバは C240-M4L として正しく表示されません。

HTML KVM コンソールでは、すべての Cisco UCS Manager 管理対象 UCS サーバに対して物理ディスプレイが正しく表示されます。

サポートされていない機能を使用したシステムの復元

CSCvk21286: Cisco UCS Manager リリース 4.0(1) では、UCS 6200 シリーズ ファブリック インターコネクタ上で次に示すサポート対象外の機能を使用して Full State バックアップが収集された場合、Full State 復元を使用してこのファイルを UCS 6454 ファブリック インターコネクタ上で復元することはできません。

- シャーシディスクバリエーションポリシーおよびシャーシ接続ポリシーは非ポートチャンネルモードで適用されます。
- スイッチングモードはイーサネットまたは FC のいずれかです。
- 仮想マシン (VMware、Linux KVM または Microsoft ハイパーバイザ) の管理は有効にされます。

25G ケーブルと UCS 6454 ファブリック インターコネクタを使用するポート自動検出ポリシー

CSCvk00796: UCS VIC 1455 を搭載したラックサーバが、25G ケーブルを介して UCS 6454 ファブリック インターコネクタに接続されている場合、ポートの自動検出ポリシーは機能しません。このようなシナリオでは、サーバポートを手動で設定します。

VIC 1455 または VIC 1457 アダプタと UCS 6300 ファブリック インターコネクタ間の FC/FCoE 向け単一リンクポートチャンネル

Cisco UCS Manager リリース 4.0(1) では、UCS 6300 シリーズ ファブリック インターコネクタに直接接続しているラックサーバ上で、VIC 1455 または 1457 アダプタ間の FC/FCoE 単一リンクポートチャンネルのみサポートしています。



(注) 直接接続ラックサーバの VIC 1455 または 1457 アダプタおよび UCS 6300 シリーズ ファブリック インターコネクタ間で、2 個目のポートチャンネルリンクを追加しないでください。

CQ の最大値を超えると、設定が失敗します

VMQ 接続ポリシーを通した VMMQ アダプタポリシーの変更により、完了キュー (CQ) の最大値を超えます。各 VIC 1400 シリーズ アダプタは、最大 1984 ユーザー設定可能ハードウェア CQ リソースをサポートしています。この数字を超過する場合、Cisco UCS Manager GUI に Out

of CQ Resources エラーが表示され、サービス プロファイルの関連付けにて設定障害により vNIC の作成が失敗します。

8 Gbps の FC アップリンク ポートでは、Fill パターンとして IDLE を使用する必要があります。

CSCvj31676: Cisco UCS 6454 ファブリック インターコネクトの場合、FC アップリンク速度が 8 Gbps の場合は、アップリンク スイッチでフィル パターンを IDLE として設定します。フィル パターンが IDLE に設定されていない場合、8 Gbps で動作している FC アップリンクは errDisabled 状態になる、断続的に SYNC を失う、またはエラーや不良パケットに気付く可能性があります。

FI ポートがポート速度の変更を自動検出しない

CSCvi45111: UCS 14xx VIC ASIC を搭載した UCS ラックマウント サーバでは、25G ケーブルを 10G ケーブルに交換すると、対応する FI ポートがダウンし、一時停止状態のままになります。ポート速度が 25G から 10G に変更されたことを、ポートは自動検出しません。この状態から回復するには、ラックマウント サーバを停止してから再稼働します。

C125 M5 サーバ Boot Mode

CSCvj41626: C125 M5 サーバは UEFI ブート モードのみをサポートします。

Cisco VIC 1455 および 1457 の接続性

ポート チャネルの FI アップリンクを FEX に設定する必要があります。

vNIC MTU の設定

VIC 14xx アダプタの場合:

- vNIC の MTU サイズは、ホスト インターフェイスの設定から変更できます。関連付けられた QoS システム クラスで指定された MTU と同等以下でなければなりません。この MTU 値が QoS システム クラスの MTU 値を超えている場合、データ転送中にパケットがドロップされる可能性があります。
- オーバーレイ ネットワークが設定されている場合、全体の MTU サイズは、QoS システム クラスの MTU 値を超えないようにする必要があります。

VIC14xx アダプタに対する Microsoft スタンドアロン NIC チーミングと仮想マシンキューサポート

Microsoft スタンドアロン NIC チーミングは、仮想マシン キュー (VMQ) でのみ動作します。VIC 14xx アダプタの場合、VMQ はシングル キューの VMMQ です。これをサポートするには、1 TQ、1 RQ、2 CQ の組み合わせを使用して新しい VMMQ アダプタ ポリシーを作成し、それを VMQ 接続ポリシーに割り当てる必要があります。

シャーシ検出ポリシーおよびシャーシ接続ポリシー

シャーシ検出ポリシーとシャーシ接続ポリシーは、M5 サーバの新世代 SIOC ではサポートされていません。シャーシ検出ポリシーまたはシャーシ接続ポリシーを設定する場合、Cisco UCS Manager にエラーが表示されます。