Cisco UCS C シリーズ ソフトウェア リリース 4.0(4) リリース ノート

初版：2019 年 4 月 26 日

最終更新：2020 年 6 月 1 日

Cisco UCS C シリーズ サーバ

Cisco UCS C シリーズサーバは、業界標準のラック筐体でユニファイド コンピューティングの機能を提供できるため、総所有コストの軽減と俊敏性の向上に役立ちます。このシリーズの各モデルは、処理、メモリ、I/O、内蔵ストレージ リソースのバランスを取ることで、処理負荷にまつわるさまざまな課題に対応しています。

リリース ノートについて

このマニュアルでは、Cisco Integrated Management Controller ソフトウェアおよび関連する BIOS、ファームウェア、ドライバを含む C シリーズのソフトウェア リリース 4.0(4) の新機能、システム要件、未解決の警告、および既知の動作ついて説明します。このドキュメントは、関連資料の項に示されているマニュアルと併せてご利用ください。

（注） 元のドキュメントの発行後に、ドキュメントを更新することがあります。したがって、マニュアルのアップデートについては、Cisco.com で確認してください。

マニュアルの変更履歴

改定	日付	説明
J0	2020 年 6 月 1 日	• 「解決済みの問題」の項を更新しました。 • 「未解決の問題」の項を更新しました。 • HUU のバージョンを 4.0(4l) に更新しました。 個々のリリースに対する Cisco ホストアップグレードユーティリティのファームウェアファイルは、次から入手可能です。Cisco UCS C シリーズ統合管理コントローラファームウェアファイル、リリース 4.0
A3	2020 年 5 月 21 日	4.0(4b) の「未解決の問題」の項を更新しました。
D2	2020 年 4 月 9 日	4.0(4e) の「未解決の問題」の項を更新しました。
I1	2020 年 4 月 2 日	4.0(4k) の「解決済みの問題」の項を更新しました。
I0	2020 年 3 月 23 日	• 「解決済みの問題」の項を更新しました。 • 「未解決の問題」の項を更新しました。 • 「セキュリティ修正」の項を更新しました。 • HUU のバージョンを 4.0(4k) に更新しました。 個々のリリースに対する Cisco ホストアップグレードユーティリティのファームウェアファイルは、次から入手可能です。Cisco UCS C シリーズ統合管理コントローラファームウェアファイル、リリース 4.0

改定	日付	説明
A1	2020 年 3 月 11 日	リリース 4.0(4b) の「未解決の問題」の項を更新しました。
H0	2019年12月20日	• 「サポートされている機能」の項を更新しました。 • HUU のバージョンを 4.0(4j) に更新しました。 個々のリリースに対する Cisco ホストアップグレードユーティリティのファームウェアファイルは、次から入手可能です。Cisco UCS C シリーズ統合管理コントローラファームウェアファイル、リリース 4.0
G0	2019 年 12 月 9 日	• 「サポートされている機能」の項を更新しました。 • 「解決済みの問題」の項を更新しました。 • 「未解決の問題」の項を更新しました。 • 「既知の動作と制限」の項を更新しました。 • HUU のバージョンを 4.0(4i) に更新しました。 個々のリリースに対する Cisco ホストアップグレードユーティリティのファームウェアファイルは、次から入手可能です。Cisco UCS C シリーズ統合管理コントローラファームウェアファイル、リリース 4.0

改定	日付	説明
F0	2019 年 9 月 27 日	次の点が変更されました。 • 「サポートされている機能」の項を更新しました。 • 「解決済みの問題」の項を更新しました。 • HUU のバージョンを 4.0(4h) に更新しました。 個々のリリースに対する Cisco ホストアップグレードユーティリティのファームウェアファイルは、次から入手可能です。Cisco UCS C シリーズ統合管理コントローラファームウェアファイル、リリース 4.0
E0	2019 年 8 月 26 日	次の点が変更されました。 • 「解決済みの警告」の項を更新。 • 「未解決の問題」の項を更新。 • HUU のバージョンを 4.0(4f) に更新しました。 個々のリリースに対する Cisco ホストアップグレードユーティリティのファームウェアファイルは、次から入手可能です。Cisco UCS C シリーズ統合管理コントローラファームウェアファイル、リリース 4.0

改定	日付	説明
D0	2019 年 8 月 1 日	次の点が変更されました。 • 「サポートされている機能」の項を更新しました。 • 「未解決の問題」の項を更新しました。 • 「解決済みの問題告」の項を更新しました。 • 「既知の動作」セクションが更新されました。 • HUU のバージョンを 4.0(4e) に更新しました。 個々のリリースに対する Cisco ホストアップグレードユーティリティのファームウェアファイルは、次から入手可能です。Cisco UCS C シリーズ統合管理コントローラファームウェアファイル、リリース 4.0
C0	2019 年 7 月 15 日	次の点が変更されました。 • このリリースでは、サーバ製造チームを有効にするために M5 サーバのソフトウェアイメージが更新されています。 • HUU バージョンを 4.0 (4d) に更新しました。 個々のリリースに対する Cisco ホストアップグレードユーティリティのファームウェアファイルは、次から入手可能です。Cisco UCS C シリーズ統合管理コントローラファームウェアファイル、リリース 4.0

改定	日付	説明
B0	2019 年 5 月 17 日	次の点が変更されました。 • 「サポートされている機能」の項を更新しました。 • 「未解決の問題」の項を更新しました。 • 「セキュリティフィックス」の項を追加しました。 • このバージョンを 4.0 (4c) に更新しました。 個々のリリースに対する Cisco ホストアップグレードユーティリティのファームウェアファイルは、次から入手可能です。Cisco UCS C シリーズ統合管理コントローラファームウェアファイル、リリース 4.0
A0	2019 年 4 月 26 日	4.0(4b) のリリースノートを作成しました。

サポートされているプラットフォームとリリース互換性マトリクス

このリリースでサポートされているプラットフォーム

このリリースでは、次のサーバがサポートされています。

- UCS C220 M5
- UCS C240 M5
- UCS C480 M5
- UCS C480 ML M5
- UCS S3260 M5

これらのサーバの情報については、「サーバの概要」を参照してください。

Cisco IMC および Cisco UCS Manager リリース互換性マトリクス

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。

次の表には、C シリーズ ラックマウント サーバ向けの C シリーズ ソフトウェア スタンドアロンおよび Cisco UCS Manager リリースをリストします。

表 *1 : CC* シリーズ サーバ向けの *Cisco C* シリーズと *UCS Manager S* s ソフトウェア リリース

C シリーズ スタンドアロン リリース	Cisco UCS Manager リリース	C シリーズ サーバ
4.0(4l)	4.0(4i)	Cisco UCS C220 M5、C240 M5、C480 M5、および S3260 M5 サーバ
4.0(4k)	4.0(4h)	Cisco UCS C220 M5、C240 M5、および S3260 M5 サーバ
4.0(4j)	サポートなし	Cisco UCS S3260 M5 サーバ
4.0(4i)	4.0(4g)	Cisco UCS C220 M5、C240 M5、C480 M5 および S3260 M5 サーバ
4.0(4h)	4.0(4e)	Cisco UCS C220 M5、C240 M5、C480 M5 および S3260 M5 サーバ
4.0(4f)	4.0(4d)	Cisco UCS C220 M5、C240 M5、C480 M5、S3260 M5 および C480 ML M5 サーバ
4.0(4e)	4.0(4c)	Cisco UCS C220 M5、C240 M5、C480 M5、S3260 M5 および C480 ML M5 サーバ
4.0(4d)	サポートなし	Cisco UCS C220 M5、C240 M5、C480 M5 および S3260 M5 サーバ
4.0(4b)	4.0(4a)	Cisco UCS C220 M5、C240 M5、C480 M5、S3260 M5 および C480 ML M5 サーバ
4.0(2m)	サポートなし	Cisco UCS S3260 M4 および S3260 M5 サーバ

C シリーズ スタンドアロン リリース	Cisco UCS Manager リリース	C シリーズ サーバ
4.0(2l)	サポートなし	Cisco UCS C220 M5、C240 M5、C480 M5、C480 ML M5、S3260 M5、C220 M4、C240 M4、C460 M4、および S3260 M4 サーバ
4.0(2k)	サポートなし	Cisco UCS S3260 M4 および S3260 M5 サーバ
4.0(2i)	サポートなし	Cisco UCS C460 M4、S3260 M4、および S3260 M5 サーバ
4.0(2h)	サポートなし	Cisco UCS C220 M5、C240 M5、C480 M5、C480 ML M5、S3260 M5、C125 M5、C220 M4、C240 M4、C460 M4、および S3260 M4 サーバ
4.0(2g)	4.0(2e)	Cisco UCS C220 M5、C240 M5、C480 M5、C480 ML M5、S3260 M5、C125 M5、C220 M4、C240 M4、C460 M4、および S3260 M4 サーバ
4.0(2f)	4.0(2d)	Cisco UCS C220 M5、C240 M5、C480 M5、C480 ML M5、S3260 M5、C125 M5、C220 M4、C240 M4、C460 M4、および S3260 M4 サーバ
4.0(2d)	4.0(2b)	Cisco UCS C220 M5、C240 M5、C125 M5、S3260 M4、S3260 M5、および C480 ML M5 サーバ
4.0(2c)	4.0(2a)	Cisco UCS C220 M5、C240 M5、C480 M5、C480 ML M5、S3260 M5、C125 M5、C220 M4、C240 M4、C460 M4、および S3260 M4 サーバ
4.0 (1e)	サポートなし	Cisco UCS C220 M5、C240 M5、C480 M5、S3260 M5、C125 M5、C220 M4、C240 M4、C460 M4、および S3260 M4 サーバ

C シリーズ スタンドアロン リリース	Cisco UCS Manager リリース	C シリーズ サーバ
4.0(1d)	4.0(1d)	Cisco UCS C220 M5、C240 M5、C480 M5、S3260 M5、C125 M5、C220 M4、C240 M4、C460 M4、および S3260 M4 サーバ
4.0(1c)	4.0(1c)	Cisco UCS C220 M5、C240 M5、C480 M5、S3260 M5、C125 M5、C220 M4、C240 M4、C460 M4、および S3260 M4 サーバ
4.0(1b)	4.0(1b)	Cisco UCS C220 M5、C240 M5、C480 M5、S3260 M5、C125 M5、C220 M4、C240 M4、C460 M4、および S3260 M4 サーバ
4.0(1a)	4.0(1a)	Cisco UCS C220 M5、C240 M5、C480 M5、S3260 M5、C125 M5、C220 M4、C240 M4、C460 M4、および S3260 M4 サーバ
3.1(3j)	サポートなし （注） Cisco UCS Manager で検出とアップグレードまたはダウングレード機能をサポートしています。	Cisco UCS C480 M5、C220 M5、C240 M5、および S3260 M5 サーバ
3.1(3i)	3.2(3i)	Cisco UCS C480 M5、C220 M5、C240 M5、および S3260 M5 サーバ
3.1(3h)	3.2(3h)	Cisco UCS C480 M5、C220 M5、C240 M5、および S3260 M5 サーバ
3.1(3g)	3.2(3g)	Cisco UCS C480 M5、C220 M5、C240 M5、および S3260 M5 サーバ
3.1(3f)	3.2(3f)	Cisco UCS C480 M5、C220 M5、C240 M5、および S3260 M5 サーバ

C シリーズ スタンドアロン リリース	Cisco UCS Manager リリース	C シリーズ サーバ
3.1(3d)	3.2(3e)	Cisco UCS C480 M5、C220 M5、C240 M5、および S3260 M5 サーバ
3.1(3c)	3.2(3d)	Cisco UCS C480 M5、C220 M5、C240 M5、および S3260 M5 サーバ
3.1(3b)	3.2(3b)	Cisco UCS C480 M5、C220 M5、および C240 M5 サーバ
3.1(3a)	3.2(3a)	Cisco UCS C480 M5、C220 M5、C240 M5、および S3260 M5 サーバ
3.1(2d)	3.2(2d)	Cisco UCS C480 M5、C220 M5、および C240 M5 サーバ
3.1(2c)	3.2(2c)	Cisco UCS C480 M5、C220 M5、および C240 M5 サーバ
3.1(2b)	3.2(2b)	Cisco UCS C480 M5、C220 M5、および C240 M5 サーバ
3.1(1d)	3.2(1d)	Cisco UCS C220 M5 および C240 M5 サーバ

システム要件

管理クライアントは、次の最小システム要件を満たしているか、これを超えている必要があります。

- Sun JRE 1.8.0_92 以降
- HTML ベースのインターフェイスは次でサポートされています。
  - Microsoft Internet Explorer 10.0 または 11
  - Mozilla Firefox 47.0 以降
  - Google Chrome 38 以降
  - Safari 7 以降

（注） 管理クライアントがサポートされていないブラウザを使用して開始されている場合、サポートされているブラウザバージョンのログイン ウィンドウで入手可能な「サポートされたブラウザの最も良い結果のために」のオプションからのヘルプ情報を確認してください。

- Microsoft Windows 10、Microsoft Windows 7、Microsoft Windows XP、Microsoft Windows Vista、Apple Mac OS X v10.6、Red Hat Enterprise Linux 5.0 またはそれ以上のオペレーティング システム
- Transport Layer Security（TLS）バージョン 1.2

ハードウェアおよびソフトウェアの相互運用性

ストレージ スイッチ、オペレーティング システム、アダプタに関する詳細については、以下のURLにあるお使いのリリースの『ハードウェアおよびソフトウェア相互運用性マトリクス』を参照してください。

http://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html

（注） 接続は、サーバと最初に接続されたデバイスの間でテストされます。スイッチの後のストレージ アレイなどのその他の接続は、Cisco UCS ハードウェア互換性リストには表示されませんが、これらのデバイスのベンダー サポート マトリクスでは強調表示される場合があります。

VIC カードでサポートされているトランシーバーとケーブルの詳細は、「トランシーバー モジュールの互換性マトリックス」を参照してください。

その他の互換性に関する情報については、VIC データ シートも参照できます。Cisco UCS 仮想インターフェイス カード データ シート

リリース 4.0 へのパスのアップグレード

この項はリリース 4.0(x) へのアップグレード パスの情報を示します。さまざまな Cisco UCS C シリーズ IMC バージョンのアップグレード パスの表を参照してください。

表 *2 :* リリース *4.0(x)* へのパスのアップグレード

リリースからアップグレード	リリースにアップグレード	推奨されるアップグレード パス
3.1(x) からのすべての MS サーバ	4.0(x)	以下のアップグレード パスに従ってください: • サーバをアップグレードするには、インタラクティブ HUU または非インタラクティブ HUU (NIHHU) スクリプトを使用できます。 • 非インタラクティブ NIHUU ツールを使用して、ファームウェアを更新する間、バージョン 4.0(1a) でリリースされる Python スクリプトを使用します。 • クライアント側で OpenSSL 1.0.1e-fips を使用します (NIHUU python スクリプトが実行中) • ここ から HUU iso をダウンロードします。 • ここ から NIHUU をダウンロードします。

リリースからアップグレード	リリースにアップグレード	推奨されるアップグレード パス
2.0(4c) よりも大きなリリースのすべての M4 サーバの場合 3.0(x) からのすべての M4 サーバの場合	4.0(x)	以下のアップグレード パスに従ってください: • サーバをアップグレードするには、インタラクティブ HUU または NIHHU スクリプトを使用できます。 • 非インタラクティブ NIHUU ツールを使用して、ファームウェアを更新する間、バージョン 4.0(1a) でリリースされる Python スクリプトを使用します。 • クライアント側で OpenSSL 1.0.1e-fips を使用します (NIHUU python スクリプトが実行中) • Cimc Boot をセキュアする場合、フラグ **use_cimc_secure** を python **multiserver_config** ファイルで **yes** にセットします。file present with python script. • ここ から HUU iso をダウンロードします。 • ここ から NIHUU をダウンロードします。

リリースからアップグレード	リリースにアップグレード	推奨されるアップグレード パス
2.0(4c) より小さいリリースのすべての M4 サーバの場合	4.0(x)	

リリースからアップグレード	リリースにアップグレード	推奨されるアップグレード パス
		2.0(4c) より小さいものから 4.0(x) にアップグレードするには、これらのステップに従ってください。: **2.0(4c) より小さいものから 2.0(4c) バージョンへのアップグレード** • サーバをアップグレードするには、インタラクティブ HUU または NIHHU スクリプトを使用できます。 • 非インタラクティブ NIHUU ツールを使用して、ファームウェアを更新する間、バージョン 3.0(3a) でリリースされる Python スクリプトを使用します。 • クライアント側で OpenSSL 1.0.0e-fips を使用します (NIHUU python スクリプトが実行中) • ここ から HUU iso をダウンロードします。 • ここ から NIHUU をダウンロードします。 **2.0(4c) から 4.0(x) へのアップグレード** • サーバをアップグレードするには、インタラクティブ HUU または NIHHU スクリプトを使用できます。 • 非インタラクティブ NIHUU ツールを使用して、ファームウェアを更新する間、バージョン 4.0(1a) でリリースされる Python スクリプトを使用します。 • クライアント側で OpenSSL 1.0.1e-fips を使用します (NIHUU python スクリプトが実行中) • Cimc Boot をセキュアする場合、フラグ **use_cimc_secure** を python **multiserver_config** ファイルで **yes** にセットします。file present with python script. • ここ から HUU iso をダウンロードします。

リリースからアップグレード	リリースにアップグレード	推奨されるアップグレード パス
		• ここ から NIHUU をダウンロードします。

ファームウェア アップグレードの詳細

ファームウェア ファイル

C シリーズのソフトウェア リリース 4.0(4) には、次のソフトウェア ファイルが含まれます。

CCO ソフトウェア タイプ	ファイル名	備考
Unified Computing System（UCS）サーバ ファームウェア	ucs-c240m5-huu-4.0.4.iso ucs-c220m5-huu-4.0.4.iso ucs-c480m5-huu-4.0.4.iso ucs-s3260-huu-4.0.4.iso リリース特有の ISO バージョンについては、Cisco UCS C シリーズ統合管理コントローラ ファームウェア ファイル、リリース 4.0 を参照してください。	ホスト アップグレード ユーティリティ
Unified Computing System（UCS）ドライバ	ucs-cxxx-drivers.4.0.4.iso	ドライバ
Unified Computing System（UCS）ユーティリティ	ucs-cxxx-utils-efi.4.0.4.iso ucs-cxxx-utils-linux.4.0.4.iso ucs-cxxx-utils-vmware.4.0.4.iso ucs-cxxx-utils-windows.4.0.4.iso	ユーティリティ

（注） 必ず BIOS、Cisco IMC および CMC を HUU ISO からアップグレードしてください。予期しない動作の原因となる場合があるため、コンポーネント（BIOS のみ、または Cisco IMC のみ）を個別にアップグレードしないでください。BIOS をアップグレードし、HUU ISO からではなく、Cisco IMC を個別にアップグレードすることを選択した場合は、Cisco IMC と BIOS の両方を同じコンテナリリースにアップグレードしてください。BIOS と Cisco IMC のバージョンが異なるコンテナリリースからのものである場合、予期しない動作が発生する可能性があります。Cisco IMC、BIOS、およびその他すべてのサーバコンポーネント (VIC、RAID コントローラ、PCI デバイス、および LOM) のファームウェアバージョンを更新するには、Host Upgrade Utility から [すべて更新 (Update All)] オプションを使用することを推奨します。

ホスト アップグレード ユーティリティ

Cisco Host Upgrade Utility (HUU) は、Cisco UCS C シリーズファームウェアをアップグレードするツールです。

ファームウェアのイメージファイルは、ISOに埋め込まれています。ユーティリティにメニューが表示され、これを使用してアップグレードするファームウェア コンポーネントを選択することができます。このユーティリティに関する詳細については、以下を参照してください。

http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html

個々のリリースに対する Cisco ホストアップグレードユーティリティのファームウェアファイルは、Cisco UCS C シリーズ統合管理コントローラファームウェアファイル、リリース 4.0 を参照してください。

ファームウェアの更新

Host Upgrade Utility を使用して、C シリーズのファームウェアを更新します。Host Upgrade Utility は、次のソフトウェア コンポーネントをアップグレードできます。

- BIOS
- Cisco IMC
- CMC
- Cisco VIC アダプタ
- DCPMM メモリ
- LSI アダプタ
- オンボード LAN
- PCIe アダプタ ファームウェア
- HDD ファームウェア
- SAS エクスパンダ ファームウェア

各リリースのサーバで使用可能なコンポーネントに関する詳細情報については、「Cisco UCS C-Series Integrated Management Controller Firmware Files」を参照してください。

すべてのファームウェアは、サーバが正常に動作するようにまとめてアップグレードする必要があります。

（注） Cisco IMC、BIOS、およびその他のすべてのサーバコンポーネント (VIC、RAID コントローラ、PCI デバイス、および LOM) のファームウェアバージョンを更新するには、Host Upgrade Utility から **[すべて更新 (Update All)]** オプションを使用することをお勧めします。ファームウェアを導入したら、**[終了 (Exit)]** をクリックします。

ユーティリティを使用してファームウェアをアップグレードする方法の詳細については、次を参照してください。

Cisco Host Upgrade Utility ユーザガイド

リリース 4.0(4x) の新しいソフトウェア機能

リリース 4.0(4j) の新しいソフトウェア機能

リリース 4.0(2m) では、次の HDD モデルのファームウェアが更新されています。

- HUH721008AL4200：ファームウェアがバージョン A3Z4 に更新されました
- HUH721010AL42C0：ファームウェアがバージョン A3Z4 に更新されました
- HUH721010AL5200：ファームウェアがバージョン A3Z4 に更新されました
- HUH721010AL52C0：ファームウェアがバージョン A3Z4 に更新されました
- HUH721010AL4200：ファームウェアがバージョン A3Z4 に更新されました

リリース4.0(4h) の新しいソフトウェア機能

障害 ID

障害 IDは Cisco IMC ログに含まれています。

物理 NIC モード

Cisco UCS VIC 14xx シリーズカードを搭載した S3260 サーバでは、ネットワーク アダプタの設定に、実験ベースで**物理 NIC モード**が追加されました。このオプションが有効になっている場合、VIC のアップリンク ポートはパススルー モードに設定されます。これにより、ホストは変更を行わずにパケットを送信できます。VIC ASIC は、vNIC の VLAN と CoS の設定に基づいてパケットの VLAN タグをリライトしません。このオプションはデフォルトでは無効になっています。

（注） 次のようなアダプタでは、このオプションを有効にすることはできません。

- **[ポート チャネル モード (Port Channel mode)]** (14xx シリーズカードの場合のみ) が有効になっているもの
- **[VNTAG モード (VNTAG mode)]** が有効になっているもの
- **[LLDP]** が有効になっているもの
- **[FIP モード (FIP mode)]** が有効になっているもの
- **[Cisco IMC 管理が有効 (Cisco IMC Management Enabled)]** の値が [はい (Yes)] に設定さっれているもの
- 複数のユーザーが作成した vNIC

物理NIC モードを有効にする前に、上記のオプションが無効になっていることを確認します。

リリース 4.0(4e) の新しいソフトウェア機能

S3260 サーバ上のデバイス コネクタ

Cisco Intersight へのアクセスを可能にする、S3260 サーバ上のデバイスコネクタの有効化サポートが追加されました。

ADDDC のスペアリング

C125 M5 を除くすべての M5 サーバに対して、**ADDDC スペアリング** オプションが、**メモリ選択 RAS 構成** BIOS トークンに追加されました。これは、このトークンの新しいデフォルト値になります。

ADDDC RAS の変更 - 適応型ダブル デバイス データ 補正 (ADDDC) は、補正できないエラーが発生して停止する前に、修正されたエラーをモニタして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。

NVMe に対する Intel ® VMD の機能強化

NVMe でのボリューム管理デバイス (VMD) のサポート。オプションの VMD ドライバは、Cisco のダウンロード サイトから入手できます。VMD がサポートされるのは、次のオペレーティング システムです。

- 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。

ロックアウト時のユーザ無効化

ロックアウト時のユーザ無効化機能が追加されました。このオプションを選択すると、ロックアウト時にユーザアカウントが無効になります。

リリース 4.0(4d) の新しいソフトウェア機能

Intel® Optane™ データセンター永続メモリモジュール

Cisco UCS C シリーズ リリース 4.0(4) では、USC M5 サーバでの 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ました。このサーバは、第 2 世代 Intel® Xeon® スケーラブル プロセッサに基づいています。Intel® Optane™ DC 永続メモリ モジュールは、第 2 世代 Intel® Xeon® スケーラブル プロセッサでのみ使用できます。

このリリースでは、Cisco IMC およびホストのオペレーティングシステムツールを使用して 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。

リリース 4.0(4c) の新しいソフトウェア機能

ロックアウトする（Account Lockout）

ローカル ユーザのログイン試行失敗 (パスワードの誤りのため) の最大回数を設定するためのサポートが追加されました。また、ユーザがロックアウトされる期間を設定することもできます。

リリース 4.0(4b) の新しいソフトウェア機能

Cisco ブート最適化 M.2 RAID コントローラのサポート

Cisco C シリーズ リリース 4.0(4b) は、Cisco Boot 最適化 M. 2 RAID コントローラ (UCS-M2-HWRAID) のサポートを導入します。Cisco IMC インターフェイスを使用すると、コントローラと物理ドライブの詳細を表示したり、関連する設定タスクを実行したりすることができます。

PCIe スイッチの更新

PCIe スイッチを回復するためのオプションが追加されました。この機能を使用して、PCIe スイッチのファームウェアを再フラッシュできます。

BIOS トークンの更新

NVMe コントローラを搭載したサーバでは、**Intel® Speed Select** BIOS トークンが追加されました。

Redfish

Redfish スキーマが更新されました。

統合ドライバのサポート

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が追加されました。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。

署名付きドライバのサポート

—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のサポートが追加されました。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。

（注） **レガシーブートモード**でブートすると、Cisco の署名付きドライバ モジュールをロードするときに、Linux カーネルは次のような警告を表示します。

不明なモジュールキー「Cisco UCS ドライバ署名の REL 証明書の要求:...」 (Request for unknown module key 'Cisco UCS Driver Signing REL Cert:...)

この警告は、ドライバ署名を検証するためのキーが存在しないことを意味します。ただし、Linux カーネルは Cisco のドライバのロードを続行できます。この警告は、**レガシー ブート モード**で表示されます。ドライバ署名の検証に使用される Cisco 暗号キーは、UCS シャーシが**セキュア ブート モード**でブートした場合にのみ利用可能になるからです。

リリース 4.0(4x) の新しいハードウェア機能

リリース 4.0(4e) で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

次の NVMe ドライブのファームウェア サポートは、リリース 4.0(4e) で導入されました。

NMVe ドライブ	PID
Intel ® P4510 1TB (SSDPE2KX010T8K)	UCSC-NVME2H-I1000
Intel ® P4510 2TB (SSDPE2KX020T8K)	UCSC-NVME2H-I2TBV
Intel ® P4510 4TB (SSDPE2KX040T8K)	UCSC-NVME2H-I4000
Intel ® P4510 8TB (SSDPE2KX080T8K)	UCSC-NVMEHW-I8000
Intel ® P4610 1.6TB (SSDPE2KE016T8K)	UCSC-NVME2H-I1600
Intel ® P4610 3.2TB (SSDPE2KE032T8K)	UCSC-NVME2H-I3200

リリース4.0(4d) の新しいハードウェア

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 2 世代 Intel® Xeon® スケーラブル プロセッサでのみ使用できます。

Cisco UCS C シリーズ リリース 4.0(4b)では、第 2 世代 Intel® Xeon® スケーラブル プロセッサに基づく次のサーバで、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 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 IMC 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。

リリース 4.0(4b) の新しいハードウェア

第 2 世代 Intel® Xeon® スケーラブル プロセッサ。

Cisco UCS C シリーズ リリース 4.0(4b)では、次のサーバでの Intel® Xeon® スケーラブル プロセッサの導入がサポートされています。

- 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

Cisco ブート最適化 M.2 RAID コントローラ

Cisco UCS C シリーズリリース 4.0(4b) は、次のサーバ上の Cisco Boot 最適化 M. 2 RAID コントローラ (UCS-M2-HWRAID) のサポートを導入します。

- Cisco UCS C220 M5 サーバ
- Cisco UCS C240 M5 サーバ
- Cisco UCS C480 M5 サーバ

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 C240 M5
- UCS C220 M5
- UCS C480 M5

このリリースでサポートされているすべての 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。

Mellanox MCX4121A-ACAT デュアル ポート 10/25G SFP28 NIC (UCSC-P-M4D25GF) のサポート

新機能

ソフトウェア ユーティリティ

次の標準ユーティリティを使用できます。

- Host Update Utility（HUU）
- BIOS および Cisco IMC ファームウェアのアップデート ユーティリティ
- サーバ設定ユーティリティ (SCU)
- サーバ診断ユーティリティ (SDU)

ユーティリティ機能は次のとおりです。

- USB 上の HUU、SCU のブート可能なイメージとしての可用性。USB にはドライバ ISO も含まれており、ホストのオペレーティングシステムからアクセスできます。

SNMP

このリリース以降のリリースでサポートされている MIB 定義については、次のリンクを参照してください。

ftp://ftp.cisco.com/pub/mibs/supportlists/ucs/ucs-C-supportlist.html

（注） 上記のリンクは、IE 9.0 と互換性がありません。

セキュリティ修正

リリース 4.0(4k) のセキュリティ修正

リリース 4.0(4k) では、次のセキュリティ修正が追加されました。

リリース	不具合 ID	CVE ID	症状
4.0(4k)	CSCvs31877	• CVE-2019-0139 • CVE-2019-0140 • CVE-2019-0142 • CVE-2019-0143 • CVE-2019-0144 • CVE-2019-0145 • CVE-2019-0146 • CVE-2019-0147 • CVE-2019-0148 • CVE-2019-0149 • CVE-2019-0150	

リリース	不具合 ID	CVE ID	症状
			Intel® Ethernet 700 シリーズコントローラを搭載した Cisco UCS C シリーズおよび S シリーズ M5 サーバでは、次の共通脆弱性(CVE) ID で識別される脆弱性の影響を受けます。 • CVE-2019-0139 は、7.0 より前のファームウェアバージョンを実行しているコントローラに影響します。ファームウェアのアクセス コントロールが不十分なため、この脆弱性により権限を持つユーザーが、ローカル アクセス経由で権限の昇格、サービス拒否、または情報漏えいが可能になる可能性があります。 • CVE-2019-0140 は、7.0 より前のファームウェアバージョンを実行しているコントローラに影響します。ファームウェアのバッファ オーバーフローが原因で、この脆弱性により、認証されていないユーザーが隣接アクセスを通じて権限の昇格が可能になる

リリース	不具合 ID	CVE ID	症状
			可能性があります。 • CVE-2019-0142 は、1.33.0.0 より前のファームウェア バージョンを実行しているコントローラに影響します。`ilp60x64.sys` ドライバのアクセス コントロールが不十分なため、この脆弱性により権限を持つユーザーが、ローカル アクセス経由で権限の昇格が可能になる可能性があります。 • CVE-2019-0143 は、7.0 より前のファームウェア バージョンを実行しているコントローラに影響します。カーネル モード ドライバで未処理の例外が発生したため、この脆弱性により、認証されたユーザーがローカル アクセスを通じてサービス拒否を有効にする可能性があります。

リリース	不具合 ID	CVE ID	症状
			• CVE-2019-0148 は、7.0 より前のファームウェアバージョンを実行しているコントローラに影響します。カーネルモード ドライバで未処理の例外が発生するため、この脆弱性により、認証されたユーザーがローカルアクセスを通じてサービス拒否を有効にする可能性があります。 • CVE-2019-0145 は、2.8.43 より前のファームウェアバージョンを実行しているコントローラに影響します。i40e ドライバのバッファオーバーフローが原因で、この脆弱性により、認証されていないユーザーが隣接アクセスを通じて権限の昇格が可能になる可能性があります。

リリース	不具合 ID	CVE ID	症状
			• CVE-2019-0146 は、2.8.43 より前のファームウェアバージョンを実行しているコントローラに影響します。i40e ドライバでリソースの漏えいが発生したため、この脆弱性により、認証されたユーザーがローカル アクセスを通じてサービス拒否を有効にする可能性があります。 • CVE-2019-0147 は、7.0 より前のファームウェアバージョンを実行しているコントローラに影響します。i40e ドライバで不十分な入力検証が発生したため、この脆弱性により、認証されたユーザーがローカル アクセスを通じてサービス拒否を有効にする可能性があります。

リリース	不具合 ID	CVE ID	症状
			• CVE-2019-0148 は、7.0 より前のファームウェアバージョンを実行しているコントローラに影響します。i40e ドライバでリソースの漏えいが発生したため、この脆弱性により、認証されたユーザーがローカル アクセスを通じてサービス拒否を有効にする可能性があります。 • CVE-2019-0149 は、2.8.43 より前のファームウェアバージョンを実行しているコントローラに影響します。i40e ドライバで不十分な入力検証が発生したため、この脆弱性により、認証されたユーザーがローカル アクセスを通じてサービス拒否を有効にする可能性があります。

リリース	不具合 ID	CVE ID	症状
			• CVE-2019-0150 は、7.0 より前のファームウェア バージョンを実行しているコントローラに影響します。ファームウェア アクセス制御が不十分なため、この脆弱性により、権限のあるユーザーがローカル アクセスを通じてサービス拒否を有効にする可能性があります。

リリース	不具合 ID	CVE ID	症状
4.0(4k)	CSCvs81690	• CVE-2020-0548 • CVE-2020-0549	Intel® プロセッサに基づく Cisco UCS C シリーズおよびS シリーズ 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。 • CVE-2020-0548 は、一部の Intel® プロセッサのクリーンアップ エラーが、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る場合、影響を及ぼします。 • CVE-2020-0549 は、一部の Intel® プロセッサにおけるデータ キャッシュ消去でのクリーンアップ エラーが、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る場合、影響を及ぼします。

リリース 4.0(4i) のセキュリティ修正

リリース 4.0(4i) では、次のセキュリティ修正が追加されました。

リリース	不具合 ID	CVE ID	症状
4.0(4i)	CSCvr54415	• 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 ID	症状
			Intel® プロセッサに基づく Cisco UCS C シリーズおよび S シリーズ 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。 • CVE-2019-11135 (TSX Asynchronous Abort Advisory) 条件は、投機的実行を利用する第 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及ぼし、認証されたユーザに対し、ローカル アクセスのサイドチャネルを通じた情報開示を可能にすることがあります。 • 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®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。 • 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・プロセッサー、インテル® Xeon ® プロセッサー D-2100、D-3100、インテル® Xeon ® プロセッサー W-2100、W-3100 に影響を与え、

リリース	不具合 ID	CVE ID	症状
			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。 • 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。

リリース	不具合 ID	CVE ID	症状
			• 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。 このリリースには、Cisco UCS C シリーズ 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 マイクロコードおよび Secure Initialization (SINIT) Authenticated Code Modules (ACM) が含まれています。

リリース 4.0 (4c) のセキュリティ修正

リリース 4.0 (4c) では、次のセキュリティ修正が追加されました。

リリース	不具合 ID	CVE	症状
4.0 (4c)	CSCvp34806	• CVE-2018-12126 • CVE-2018-12127 • CVE-2018-12130 • CVE-2019-11091	

リリース	不具合 ID	CVE	症状
			Cisco UCS M5 サーバは、Intel ® Xeon ® 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スプロイトのバリアントに対して脆弱です。 • 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 Cisco IMC 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 Cisco IMC 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 Cisco IMC 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。 • 17 CVE-2019-11091 (Microarchitectural Uncacheable Data Sampling) は、CPU の到達不能なメモリに影響を及ぼし、UCS Cisco IMC 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。 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

リリース	不具合 ID	CVE	症状
			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。

解決済みの不具合

次の項では、解決済みの警告をリストします。

リリース 4.0(4) の解決済みの問題

リリース 4.0(4l)

次の問題はリリース Release 4.0(4l) で解決済みです。

表 *3 : BIOS*

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvt64871	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。サーバはメモリテスト手順でスタックします。これにより、メモリ システムでのブート ループ トリガー #IERR および M2M タイムアウトになります。 詳細については、以下を参照してください。 • Intelのエラッタ - SKX108 • Intelのエラッタ - CLX37 この問題は解決されました。	4.0(4e)	4.0(4l)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済みリリース
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、Cisco UCS C220 M5、C240 M5、および S3260 M5 サーバの起動が、メモリテストの手順で停止します。 • C220M5.4.0.4p.0.0224200755 • C240M5.4.0.4r.0.0305200743 • S3X60M5.4.0.4o.0.0224200755 この問題は解決されました。	4.0(4h)	4.0(4l)

表 *4 : BMC*

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み

CSCvs92008	Cisco IMC と BMC 間のソケット接続が最大制限に達すると、次のエラーメッセージが表示され、さらに接続がブロックされます。
	`Error: Maxed out all client socket connections to remote manager in BMC. Please retry after a while`
	または
	`Communication to peer CMC remote manager. Internal Error. Please retry`
	この問題は解決されました。
		4.0(4b)	4.0(4l) および 4.1(1f)

CSCvp35008	Cisco UCS C シリーズ M5 サーバに Intel Xx710 アダプタが搭載されており、これらのアダプタの 1 つ以上でオプション ROM が有効になっている場合、UEFI モードでの SLES/RHEL OS のインストールは失敗します。 この問題は解決されました。	4.0(4b)	4.0(4l)

表 *5 :* 外部コントローラ

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvq53066		4.0(4d)	4.0(4l)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
	Cisco UCS C240 M5 サーバで自動インストールを使用して、リリース 4.0(2x) 以前の任意のリリースからリリース 4.0(4b) にホスト ファームウェアをアップグレードすると、SAS コントローラ ファームウェアのアクティベーションが失敗します。次の問題が表示されます。 • F78413 - ストレージコントローラで更新に失敗しました (F78413 - Update Failed on Storage Controller) • F0181: ドライブの状態: 未構成の不良 (F0181 - Drive state: unconfigured bad) • F0856 - アクティベーションが失敗し、アクティベート ステータスが失敗に設定されました (F0856 - Activation failed and Activate Status set to failed) この問題は解決されました。		

リリース 4.0(4k)

次の問題はリリース Release 4.0(4k) で解決済みです。

表 *6 : BIOS*

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvs51200	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。 • 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 • IQN がプロファイルレベルで定義されている • 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 この問題は解決されました。	4.0(4f)	4.0(4k)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvr79388	Cisco 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。 詳細については、以下を参照してください。 • Intelのエラッタ - SKX108 • Intelのエラッタ - CLX37 （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、「未解決の問題」セクションの「CSCvt64871」を参照してください。	4.0(4e)	4.0(4k)

表 *7 : BMC*

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvq84999	Cisco IMC は、cisco UCS 1387 アダプタを搭載した Cisco UCS C シリーズ M5 サーバにファン制御ポリシーを適用できません。次のエラーメッセージが表示されます。 `The selected Fan Control Profile could not be applied due to unmanageable PCI card presence! Configured Policy: 10, Derived Policy: 20! Applied Policy: Balanced, Configuration Status: FAN POLICY OVERRIDE - Card(s) "unknown card PCI-Ids: 0x1137-0x0043-0x1137-0x015D" present` この問題は解決されました。	4.0(1c)	4.0(4k)
CSCvr70687	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。 `CimcVMedia Error: Error retrieving vmedia attributes list-MC Error(-6)` 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。 この問題は解決されました。	4.0(4d)	4.0(4k)

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvs86186	共有サーバパスワードの特殊文字を認識できず、「権限が拒否されました」というエラー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(2h)	4.0(4k)
CSCvt07824	共有サーバパスワードの特殊文字を認識できず、「権限が拒否されました」というエラー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(4g)	4.0(4k)

表 *8:* 外部コントローラ

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvr95365	Cisco 12G モジュラ SAS HBA コントローラが搭載された Cisco UCS C240 M5 サーバの検出は、次のいずれかのエラーで失敗します。 • mc_attrib_set_suboem_id は SubOEM ID を設定できませんでした • Cisco IMC はドライブを検出できません。 この問題は解決されました。	4.0(4i)	4.0(4k)

表 *9 :* ホスト ファームウェア アップグレード

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvs48461	Cisco UCS S3260 M5 および M4 サーバで Cisco IMC を 4.0 (2m) または 4.0 (4i) にアップグレードする場合、実際の更新が成功した後でも、HUU および NIHUU は HDD ファームウェアの更新が失敗したと報告します。 この問題は解決されました。	4.0 (2m)	4.0(4k)

リリース 4.0(4j)

4.0(4j) に解決済みの問題はありません。

リリース 4.0(4i)

次の問題はリリース 4.0(4i) で解決済みです。

表 *10 : BMC*

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvo76406	Cisco IMC GUI では、Cisco UCS C シリーズ M5 サーバの適用済み名前空間の編集はサポートされていません。ただし、名前空間は Cisco IMC CLI または XMP API を使用して編集できますが、データと設定が失われる原因になります。 Cisco IMC CLI または XML API を使用する適用済み名前空間の編集はサポートされなくなりました。	4.0(4a)	4.0(4i)

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvr72565	管理者以外のユーザでも、Cisco IMC CLI インターフェイスを使用して Cisco UCS C240 M5 サーバのタイムゾーンを変更できました。 この問題は解決されました。管理者以外のユーザは、Cisco IMC CLI インターフェイスを使用してタイムゾーンを変更することができなくなりました。	3.0(4n)	4.0(4i)
CSCvr43466	Cisco UCS Manager と統合された Cisco UCS C シリーズ ラックサーバは、ハードウェアインベントリの不一致を示します。 この問題は解決されました。	4.0(4b)	4.0(4i)
CSCvo62515	Cisco IMC がクラッシュするか、応答不能になり、次のエラー ログが記録されます:ドライバ/bmc/cisco_proc_lib でのカーネル バグ (kernel BUG at drivers/bmc/cisco_proc_lib) /cisco_proc_lib c ログ この問題は解決されました。	3.1(3h)	4.0(4i)
CSCvp90030	Cisco IMC がクラッシュし、次のカーネル エラー ログが記録されます。 oops のスタック トレースで log_i2c_tx (log_i2c_tx in the stack trace of oops) この問題は解決されました。	4.0(4c)	4.0(4i)

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvr78701	Cisco UCS manager の統合 C シリーズサーバは、Cisco UCS Manager をリリース 4.0 (2b) からリリース 4.0 (4c) にアップグレードした後、Cisco IMC カーネルパニックを体験するために使用します。 この問題は解決されました。	4.0(4c)	4.0(4i)
CSCvr96140	Cisco UCS M5 サーバでは、**IPMI ウォッチドッグ タイマー**が有効になっている場合、オペレーティングシステムは突然再起動し,次のオンボード障害ロギング (obfl) ログエラーメッセージが記録されます。 "oem_common.c:309: エラー 'メッセージング' スレッドが停止しています" ("oem_common.c:309:Error: the 'messaging' thread is stalled") 回避策として、意図しないリブートを避けるために、オペレーティングシステムで**ウォッチドッグ タイマー**を無効にすることができます。 この問題は解決されました。	4.0(2d)	4.0(4i)

表 *11 : Cisco VIC*

不具合 ID	症状	最初に影響を受けるリリース	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。 この問題は解決されました。	4.0(4g)	4.0(4i)

表 *12 :* 外部コントローラ

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
4.0(4l)		4.0(4e)	4.0(4i)

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
	Cisco UCS C シリーズ M5 サーバでは、Cisco IMC は Intel® Youngsville ドライブの検出に失敗しました。ファームウェアをバージョン CS05 からバージョン CS07 にアップグレードした後、Intel® Youngsville ドライブと他の SATA ドライブの一部が Cisco IMC のストレージセクションで**未構成の不良**として表示されます。 この問題は、Cisco 12G モジュール型 SAS HBA コントローラが Intel ドライブおよび SAS ドライブに接続されている場合にのみ発生しました。これは、ストレージコントローラの HII/ホストインターフェイスでドライブが正常として表示される、Cisco IMC アウトオブバンドインターフェイスでのみ観察されました。 （注） 場合によっては、Cisco IMC からのコントローラとドライブの適切なステータスを反映するために約15分かかるこ		

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
	とがあります。 この問題は解決されました。		

リリース 4.0(4h)

次の問題はリリース 4.0(4h) で解決済みです。

表 *13 : Cisco VIC*

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvr04369	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。 • 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: • 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: • 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。	4.0(4e)	4.0(4h)

リリース 4.0(4f)

次の問題はリリース 4.0(4i) で解決済みです。

表 *14 :* サーバ

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvq95077	S3260 M5 サーバはリブート状態のままになり、電源をオンにできず、BIOS POST を完了しません。	4.0(4e)	4.0(4f)

表 *15 : BMC*

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvq26149	M5 サーバファンは、PECI の温度読み取り障害が発生した後、最大速度で動作します。サーバの電源を再投入するまで、ファン速度は引き続き最大速度のままになります。	4.0(4c)	4.0(4f)
CSCvq93258	新しい Intel® Optane™ データセンターの永続メモリモジュール部分の製品 ID (PID) は、バージョン 4.0(4d) では不明 (UNKNOWN) として表示されます。 PID カタログを 4.0(4e) にアップグレードすると、正しい PID 番号が表示されます。	4.0(4d)	4.0(4f)
CSCvq86332	システムに存在する SED ドライブの PID が、非 SED ドライブとして表示されます。	4.0(4e)	4.0(4f)

表 *16 :* ホスト ファームウェア アップグレード

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvq58364	非インタラクティブな HUU (NIHUU) デバイスの更新は、タイムアウトエラーで失敗します。これは、1つまたは複数のドライブのHDDファームウェアを NIHUU でアップグレードするときに発生します。	4.0(4d)	4.0(4f)

表 *17* : 外部コントローラ

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvq81930	4.0(2c) から 4.0(4b) または 4.0(4e) へのアップグレード中に、次の Intel ドライブのファームウェアアップデートが失敗します。 • SSDSC2KB038T7K : 3.8TB 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	4.0(4b)	4.0(4f)

リリース 4.0(4e)

次の問題はリリース 4.0(4e) で解決済みです。

表 *18 : BIOS*

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvp39108	UEFI モードの Intel X710-t4 アダプタを搭載している Cisco UCS M5 サーバで、iSCSI が Intel X710-t4 X710-DA4 Quad Port 10Gb SFP + 統合 NIC を使用して設定されている場合、UEFI ブートプロセスを完了できません(OS ブートおよび PXE ブートを実行できません)。	4.0(4b)	4.0(4e)

表 *19 : BMC*

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvo55902	ネットワーク リンク アクティビティ LED に、正しい LOM ポートと LED ステータスが表示されません。	4.0(4b)	4.0(4e)

表 *20 :* 外部コントローラ

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvp43280	2つ以上の Intel PCI アダプタが UCS C シリーズおよび S シリーズ M5 サーバに装着されているときに、HUU を使用して PCI カードのファームウェアをアップグレードすると、失敗する可能性があります。	4.0(2c)	4.0(4e)
CSCvo93353	StorCLI コマンド **storcli /cX show all** では、ドライブのワールド ワイド番号 (WWN) は表示されません。これは、StorCLI バージョン7.0813 以前を使用している場合に発生します。	4.0(2f)	4.0(4e)

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvp08512	MegaRAID コントローラのファームウェアでは、ホットスペアの物理ドライブサイズはチェックされず、小さなサイズの専用ホットスペアを作成して割り当てることができます。	4.0(4b)	4.0(4e)

表 *21 : Intel® Optane™* データ センター永続メモリ モジュール*: Intel* の解決済み問題

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
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。 Intel IPS のケースのフィールド。	4.0(4b)	4.0(4e)
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。 Intel IPS のケースのフィールド。	4.0(4b)	4.0(4e)

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvp38555	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。 Intel IPS のケースのフィールド。	4.0(4b)	4.0(4e)

リリース 4.0(4d)

次の問題はリリース 4.0(4d) で解決済みです。

表 *22 : HUU*

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvp74003	リリース 4.0(4d) から以前のリリースにダウングレードすると、HUU と NI-HUU は DCPMM の検出に失敗します。 この問題は解決されました。	4.0(4b)	4.0(4d)

リリース 4.0(4b)

リリース 4.0(4b) では、次の問題が解決されます。

表 *23 : BMC*

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvo97900	OS ブートが FlexFlash を介して設定され、ストレージプロビジョニングが SAN を介して行われている場合、HDD または NVMe ケージを搭載していない C480 M5 サーバでは、次のエラーが表示されます。「SAS_EEPROM_PRSNT: アドインカード9がありません: 再装着またはアドインカード9を交換してください」。	4.0(2c)	4.0(4b)
CSCvo18799	Cisco IMC を使用してファームウェアを更新する際に、電力シーケンサー (PWR_SEQ) の更新が失敗し、次のメッセージが表示されます。「AC サイクルシステムのファームウェアの更新に失敗しました。やり直してください」。PWRSEQ	3.0(3e)	4.0(4b)
CSCvo15978	M393A4K40BB2 CTD Dimm を搭載したサーバでは、IPMI が動作を停止する可能性があります。管理コンソールの温度、CPU、および/または DIMM の不一致に関連するエラー、ファン速度 100%、およびシャーシの通知が報告されます。	4.0(1a)	4.0(4b)
CSCvo02861	重大度を報告する Syslog の最小重大度が機能していません。	3.1(3a)	4.0(4b)
CSCvo85413	ファームウェアバージョン 4.0 (2c) で実行されている S3260 サーバで Cisco IMC を使用して KVM コンソールを起動できません。	4.0(2c)	4.0(4b)

表 *24 : BMC* ストレージ

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvn29592	次のドライブ: • KPM51RUG480G • KPM51RUG960G • KPM51RUG1T92 • KPM51RUG3T84 • KPM51VUG400G • KPM51VUG800G • KPM51VUG1T60 • KPM51VUG3T20 • MZ6ER400HAGL/003 Cisco IMC では、**磨耗の状態が日単位で**表示され、**寿命のパーセント**がゼロのまま表示されます。	4.0(2c)	4.0(4b)

表 *25 : BIOS*

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvn77825	Windows Hyper-v 2019 が保護されたホスト機能と TPM を使用しているサーバでは、この環境でシールドされた仮想マシンを実行すると、ホストガーディアンのシールド付き VM の認証エラーが発生し、不正な UEFI 変数データ構造が返されます。	4.0(1c)	4.0(4b)

表 *26 : CMC*

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvo25387	4.0 (1b) バージョンで稼働している S3260 サーバでは、シャーシが SAFE 状態になり、MEZZ温度センサーの測定値が欠落しているためにファンが 100% の RPM で回転している可能性があります。	4.0(1b)	4.0(4b)

表 *27 : CMC* ストレージ

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvo03830	SAS エクスパンダのリンク アドレスは、エクスパンダの接続が解除された後、HGST ドライブで0に設定されます。	4.0(1a)	4.0(4b)

表 *28 :* 外部コントローラ

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvn34219	ブート中に回復不能な障害が発生したため、UCSC UCSC-RAID-M5HD コントローラのブートに失敗します。Cisco IMC Web UI で次のエラーが報告されます: ストレージコントローラが動作不能です。UCSC UCSC-RAID-M5HD コントローラによってホストされているすべてのブートおよびデータボリュームは使用できません。これは、オンラインの RAID レベルの移行が進行中で、システムで電源の再投入またはシャットダウンが発生した場合に発生します。	4.0(2c)	4.0(4b)

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvm94424	S3260 サーバを 4.0 (1a) にアップグレードした後、F1256 機器が欠落している情報障害が空のドライブスロットに対して記録されています。	4.0(1a)	4.0(4b)

Resolved Caveats in Release 4.0(2)

リリース 4.0(2m)

リリース 4.0 (2m) では、次の障害が解決されました。

表 29 : Firmware Upgrade

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvr91935	Cisco UCS S3260 M4 および M5 サーバでは、Cisco UCS VIC 1455 および 1495 カードのファームウェアのアクティベーションが NI-HUU/HUU の更新後に失敗します。 この問題は解決されました。	4.0 (2k)	4.0 (2m)
CSCvo18736	HUU バージョン 4.0(2d) 以降とセットになっている Intel X710-t4 NIC ファームウェアのアップグレードに失敗すると、ネットワーク接続の中断が発生します。 この問題は解決されました。	4.0(2d) 以降	4.0 (2m)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvr88803	NI HUU スクリプトは `vmedia mapping has gone bad` エラーで失敗します。設定ファイルでオプション「`update_verify = yes`」が設定されている場合、このスクリプトは検証ブートで失敗する可能性があります。 この問題は解決されました。	4.0 (2k)	4.0 (2m)
CSCvr71907	S3260 M4 サーバでは、タイムアウト エラーが発生しても、NI HUU ファームウェアのアップグレードまたはダウングレードが失敗することがあります。 この場合、一部のコンポーネントのみが更新され、一部のコンポーネントのファームウェアを再度更新する必要があります。 この問題は解決されました。	4.0 (2k)	4.0 (2m)

リリース 4.0(2l)

リリース 4.0(2l) で解決済みの問題はありません。

リリース 4.0(2k)

リリース 4.0(2k) では、次の障害が解決されました。

表 *30 :* ユーティリティ

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvr61928	NI HUU を使用して M4 および M5 サーバのファームウェアを更新する際に、CMC のアクティベーションが失敗します。これは、BIOS ファームウェア バージョンに変更がなく、BMC および CMC ファームウェア バージョンが変更された場合に発生します。	4.0(1a)	4.0 (2k)

リリース 4.0(2i)

リリース 4.0(2i) では、次の障害が解決されました。

表 *31 : BIOS*

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvo77732	Intel Xeon v2 CPU を搭載した UCS C460 M4 を 4.0 ファームウェア バージョンにアップグレードすると、サーバがクラッシュ (PSOD) し、応答しなくなったり、CATERR が発生したりします。	4.0(1c)	4.0 (2i)

表 *32 :* ユーティリティ

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvr07491	非インタラクティブな HUU を使用して複数の S3260 サーバのファームウェアをアップグレードした後、BMC、BIOS、CMC、SAS エクスパンダなどのいくつかのサーバコンポーネントのファームウェアのアクティブ化が失敗します。	4.0(1a)	4.0 (2i)

リリース 4.0(2h)

リリース 4.0(2h) では、次の障害が解決されました。

表 *33 : BIOS*

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvo48006	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。	4.0(2c)	4.0 (下半期)

リリース 4.0 (2g)

次の障害は、リリース 4.0 (2g) で解決されました。

表 *34 : BMC*

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvo15978	M393A4K40BB2 CTD Dimm を搭載したサーバでは、IPMI が動作を停止する可能性があります。管理コンソールの温度、CPU、および/または DIMM の不一致に関連するエラー、ファン速度 100%、およびシャーシの通知が報告されます。	4.0(1a)	4.0 (2g)
CSCvp41543	SSH クライアントが Cisco IMC への接続を確立できません。このことは、SSH クライアントが `diffie-hellman-group14-sha1` をデフォルトの KEX アルゴリズムとして使用するときに発生します。この KEX アルゴリズムが Cisco IMC から削除されているためです。 SSH セッションを確立するために、より厳格な KEX アルゴリズムを使用する最新バージョンに SSH クライアントを更新します。	3.0(4j)	4.0 (2g)

表 *35 : Firmware Upgrade*

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvp34583	VIC カードまたは UCSC C3260 SIOC カードのファームウェアアクティベーションが、4.0 (2c) よりも前のリリースでは失敗します。これは、Cisco カードモードのすべての M4 および M5 サーバで発生します。	4.0 (2c) より前のリリース	4.0 (2g)

リリース 4.0 (2f)

リリース 4.0 (2f) では、次の障害が解決されました。

表 *36 : BMC*

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvn81570	Flex Flash SD カード VD の LUN ID の変更が、次のエラーで失敗します: デバイスの設定エラー	4.0(1c)	4.0 (2f)
CSCvn80088	NI HUU で指定されたリモート共有パスワードが次の特殊文字 ; | ? を含むときに、非対話形式の HUU の更新を開始できません$! @ # % ^ * - _ +	4.0(1a)	4.0 (2f)

リリース 4.0 (2d)

次の障害は、リリース 4.0 (2d) で解決されました。

表 *37* : ユーティリティ

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvn92435	Host Update Utility が次のプラットフォームで起動していません: BE7M-M5-K9。HUU は「`Host Update Utility は CISCO IMC` ファームウェアを検出できません」というエラーメッセージで失敗します。	4.0(2c)	4.0(2d)

リリース 4.0(2c)

リリース 4.0 (2c) では、次の障害が解決されました。

表 *38 : BMC*

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvm12144	物理的な電力損失が発生していないにもかかわらず、PSU 入力電圧損失アサートの問題が発生しました。	3.1(3b)	4.0(2c)
CSCvm27310	NVIDIA P40 カードが取り付けられている C シリーズサーバでは、常に 100% でファンが動作しています。BMC は、NVIDIA GPU P40 カードが取り付けられているサーバでは、サーバを**高電力**ポリシーではなく、**最大電力** ポリシーに設定します。	3.1 (1d)	4.0(2c)
CSCvn04038	RAID を2つの SD カード間にセットアップすることはぜきず、その結果、次のエラーが発生します。 コントローラの状態：ホストからパーティションが切断されています	3.1 (1d)	4.0(2c)

表 *39 : CMC* ストレージ

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvj95793	[Show fault entries] リストには、管理 IP を使用してログインしたときに下位 CMC から報告された障害は表示されません。プライマリ CMC の障害のみが報告されます。	4.0(1a)	4.0(2c)

表 *40 :* 外部コントローラ

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvj74706	M4 サーバでは、UCSC SAS12GHBA によって管理される物理ドライブは、物理ドライブの状態を **JBOD** ではなく **Unconfigured Good** として表示します。	3. (3a)	4.0(2c)
CSCvm83587	3.1 (3a) ファームウェアバージョンを搭載した C220 および 240 M5 サーバでは、VMware ホストのファイル転送により、ドライババージョン8.21 で実行されている Qlogic 25G カード (QL41212H) の Rx パケット ドロップおよび CRC エラーが発生します。	3.1(3a)	4.0(2c)

表 *41 : Firmware Upgrade*

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvk76542	Cisco UCS VIC カードまたは UCSC C3260 SIOC カードのアクティベーションが、リリース 4.0(2c) 以降へのアップグレード後に失敗します。これは、すべての C シリーズサーバ、およびこれらのカードを搭載した S3260 M5 サーバで発生します。	4.0(2c)	4.0(2c)

表 *42 :* ユーティリティ

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvi65660	Cisco VIC アダプタ ファームウェアは、ユーザが使用しているサーバコンポーネントのファームウェアをアップグレードすると、自動的にアクティブ化されない場合があります。これは、シングル サーバ デュアル SIOC が有効になっている場合に発生します。	4.0(1a)	4.0(2c)

未解決の不具合

次の項では、未解決の警告をリストしています。

リリース 4.0(4) で未解決の問題

リリース 4.0(4l)

リリース 4.0(4l) には、次の未解決の問題があります。

表 *43 : BMC*

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvt23154	Cisco UCS M5 サーバでは、両方の CPU で障害が発生した場合でも、CPU2 だけが無効 POR の障害サマリー メッセージにリストされます。	既知の回避策はありません。	4.0(4b)

表 *44 : BIOS*

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvu37394	AMD Firepro 7150X2 16 GB GPU が搭載され、レガシー ブート モードに設定されている Cisco UCS C480 M5 サーバでは、起動中に次のエラーが表示されます。 システムソフトウェア イベント: Post センサー、システム ファームウェア エラー (Post エラー)、回復不能なビデオコントローラの障害 [0xFF09] がアサートされました この問題による機能への影響はありません。	UEFI ブートモードに変更します。	4.0(4k)

表 *45 :* 外部コントローラ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvt86961	Cisco UCS C240 M5 サーバでは、アップグレード後に SAS エクスパンダファームウェアのアクティベーションが失敗すること、またはサーバのリブート後に SAS エクスパンダがリセットされることがあります。	Cisco UCS Manager を使用して、次のいずれかを実行します。 1. サーバを再認識します。 2. サービスプロファイルのプロパティを変更し、関連付けをトリガーします。	4.0(4h)

リリース 4.0(4i)

リリース 4.0(4i) には、次の未解決の問題があります。

表 *46 : BIOS*

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvs13053	Cisco UCS S3260 M5 サーバは、リリース 4.0(4i) へのアップグレード後に起動しなくなります。ブートプロセスは、次の段階で応答不能になります。 `Ptu` ドライバのロード中 この問題は、Intel Speed Step、NUMA、および Memory RAS モード BIOS トークンによって引き起こされる NVRAM オフセットが原因で発生します。	BIOS トークン値を次のようなデフォルト値に変更します。 • Intel Speed Step • NUMA • Memory RAS	4.0(4i)

表 *47 :* エクスパンダ

不具合 ID	症状	回避策	最初に影響を受けるリリース
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)

リリース 4.0(4f)

リリース 4.0(4f) には、次の未解決の問題があります。

表 *48 :* 外部コントローラ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvq50290	アップグレード後、Cisco IMC は SATA ディスク UCS SD960G63X を認識できなくなります。これは、4.0(2c) またはそれ以下のバージョンから 4.0(4) バージョンにアップグレードすると発生します。	この問題が発生した場合は、次の手順を実行します。 **1.** 4.0.(2d) HUU にブートします。 **2.** ストレージ コントローラのバージョンを00.00.00.58にダウングレードします。 **3.** 再起動してドライブを検出し、バージョンSCV1CS07にアップグレードします。 **4.** 4.0(4) リリースから起動します。 **5.** 4.0(4) リリースで使用可能な最新バージョンにストレージ コントローラをアップグレードします。	4.0(4b)

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvr03037	ファームウェアをバージョンCS05からバージョン CS07 にアップグレードした後、Cisco IMC ストレージ セクションでは、Intel ドライブと他の SATA ドライブの一部が**未設定の不良 (Unconfigured bad)** として表示されます。 この問題は、Cisco 12G モジュール型 SAS HBA コントローラが Intel ドライブおよび SAS ドライブに接続されている場合にのみ発生します。これは、ドライブがストレージコントローラの HII/ホスト インターフェイスでは正常として表示される、Cisco IMC アウトオブバンド インターフェイスでのみ観察されます。 （注） Cisco IMC からのコントローラとドライブの適切なステータスを反映されるまでには、約15分かかることがあります。	Cisco IMC の再起動を実行します。	4.0(4e)
CSCvr03044	Cisco IMC を 4.0 (2c) から 4.0 (4f) にアップグレードする際、ドライブが Cisco 12G のモジュラー SAS HBA コントローラに接続されていると、SAS ドライブ ファームウェアのアップデートが失敗することがあります。	障害が発生したドライブまたはすべてのドライブを再度更新して、正常に更新されたことを確認します。	4.0(4e)
CSCvr03041	更新が正常に完了した後でも、ホストアップデートユーティリティで、接続されたドライブのスロット番号が**NA**として表示されます。 この問題は、ソフトウェア RAID の設定でのみ見られます。	ドライブは正常に更新されているため、機能上の影響はありません。	4.0(4c)

リリース 4.0(4e)

リリース 4.0(4e) では、次の問題が未解決です。

表 *49* : サーバ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvq95077	S3260 M5 サーバはリブート状態のままになり、電源をオンにできず、BIOS POST を完了しません。	サーバの電源を再投入して、セットアップを回復します。	4.0(4e)

表 *50 :* 外部コントローラ

不具合 ID	症状	回避策	最初に影響を受けるリリース
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。	この問題が発生した場合は、次の手順を実行します。 • UEFI ブート モードに切り替えます。 または 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、問題なく起動します。	4.0(4e)

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvq26156	UCS C 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することがあります。 • SSDSC2KB480G7K - 480GB 2.5 インチ Enterprise Value 6G SATA SSD • SDSC2KB960G7K - 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 この問題は、アップグレード前のドライブ 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。	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。 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。 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。 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。	4.0(4e)

リリース 4.0(4b)

次の障害は、リリース 4.0 (4b) で未解決です。

表 *51 : 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	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。 これは、Intel® Optane™ Data Center persistent memory MODULE HII および UEFI ipmctl tool の問題です。 Intel IPS のケースのフィールド。	既知の回避策はありません。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。	4.0(4b)
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。 Intel IPS のケースのフィールド。	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。	4.0(4b)

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCvp08356, CSCvo72182	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能なエラーが DIMM A1 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。 Intel IPS のケースのフィールド。	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。	4.0(4b)
CSCvp38564	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。 Intel IPS のケースのフィールド。	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(4b)
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わずかにあります。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(4b)

表 *52 : 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	最初に影響を受けるリリース
CSCvo17390	Intel® Optane™ DIMMを搭載したS3260 M5サーバでは、障害エンジンによって、SPDからのRDIMMサイズが0であることを示す警告メッセージが表示されます。	なし。	4.0(4b)
CSCvp03376	障害エンジンは、メモリDIMMのファームウェアバージョンが同じであるにもかかわらず、永続メモリ DIMMに対して「**不一致の FW リビジョン**」警告が表示されます。	なし。	4.0(4b)
CSCvn93216	Intel® Optane™ データセンター永続モジュールを搭載したシステムでは、永続メモリモジュールの障害エンジンの警告サマリーが完了していない可能性があります。CPU1とCPU2の両方で障害が発生した場合、障害サマリーにはCPU2の障害のみが表示されます。	なし。	4.0(4b)
CSCvp11872	重複する障害は、Intel® Optane™データセンター永続メモリモジュールについて報告されます。既存の永続メモリモジュールの障害は、すべてのホストの再起動後に再度報告されます (重複)。	なし。	4.0(4b)
CSCvp13906	Intel® Optane™データセンター永続メモリモジュールが、NUMAを無効状態にした揮発性メモリとして設定されている場合、メモリにアクセスできません。	なし。	4.0(4b)

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvo99814	セキュリティが、Intel® Optane™ データセンター永続メモリモジュールで無効になっている場合、Cisco IMC ではセキュリティの状態が**Disabled、ロック解除、凍結、カウントの期限が切れていない**として表示されます。ただし、ホストツールはセキュリティ状態を**無効、凍結**に表示します。	なし。	4.0(4b)
CSCvp15031	Intel® Optane™ データセンターの永続メモリモジュールのヘルス状態は、ファームウェアを 2019_WW10 から 2019_WW12BKC にアップグレードした後で機能しなくなるように変更されます。	なし。	4.0(4b)
CSCvo20670	Intel® Optane™ データセンター永続メモリモジュールでは、目標設定変更の実行後に**致命的な障害**メッセージが表示されます。	なし	4.0(4b)
CSCvo80193	設定変更の実行中に、メディアエラーが Intel® Optane™ データセンター永続メモリモジュールについて報告されました。これらのエラーは、EFI と OS の両方で表示されます。	なし。	4.0(4b)
CSCvo85065	Intel® Optane™ データセンターの永続メモリモジュールの障害状態の場合、障害を示すために SEL イベントはログに記録されません。	BMC 障害ログ、Windows、または Linux SEL では、ACPI を使用してエラーを確認できます。	4.0(4b)

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvt31090	Cisco UCS S3260 M5 サーバの場合、DCPMM 初期設定へのリセット後、Cisco IMC GUI はローカルの DIMM 番号のリストを表示せずに、名前空間を作成します。その結果、名前空間の作成は失敗します。	Cisco IMC CLI または XML API を使用して名前空間を作成します。 または 次の操作を行ってください。 1. 名前、ソケット ID、容量、およびモードのフィールドを使用して、新しい名前空間を作成します。 2. 設定を保存しますが、設定を適用するためにホストを再起動しないでください。 3. **[メモリ使用量の作成 (Create Memory Usage)]** から、ステップ2でDIMM番号なしで作成された保留中の名前空間エントリを削除します。 4. ここで、ローカルの DIMM 番号とその他のフィールドを使用して、新しい名前空間を作成できます。 5. 設定を保存し、ホストを再起動して設定を適用します。	4.0(4b)

表 *53 : BIOS*

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvo46953	LOM ポート1から iPXE ブートを開始できません。	LOM ポート2を使用します。	4.0(4b)

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvp21118	Cisco UCS C480 M5 サーバの高精度ブート順序(L2ブート順序)機能によって、ブート順序の外部物理 USB ドライブがリストされない場合があります。	BIOS F6 を使用して、必要なデバイスからブートすることができます。	4.0(4b)
CSCvp43349	BIOS ファームウェアを 4.0 (4b) にアップグレードすると、Cisco UCS M5 サーバが以前に設定した (アップグレード前に) iSCSI の試行を失う可能性があります。	サードパーティ製アダプタの BIOS セットアップから iSCSI の試行を追加し、VIC カード用の Cisco IMC GUI を使用することができます。	4.0(4b)
CSCvp36893	一部の CPU Sku を使用している Cisco UCS M5 サーバで PTU TDP テストを実行すると、CPU ドメインの最大電力制限が実際の CPU TDP の半分だけに到達します。	なし。	4.0(4b)

表 *54 :* 外部コントローラ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvp11474	1つのデバイスを使用して複数のドライブのファームウェアを更新する際に、ファームウェアが更新された場合でも、特定のドライブのドライブ更新が「失敗」であることを示すエラーが表示されます。	デバイスがすでに更新されているため、このエラーを無視するか、またはエラーを無視してリブート手順を続行します。	4.0(4b)
CSCvo3964, 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。	ウォームリブートを実行します。	4.0(4b)

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvm15304	PCI Switch1 および PCI Switch Rear に 2 個の Intel ColdStream ドライブが搭載された 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。	なし。	4.0(4b)
CSCvp30283	QL45412H カードを搭載したサーバでは、アダプタファームウェアを更新した後に iSCSI 設定がデフォルト設定に復元されます。これは、BIOS メニューから Qlogic HII 設定ユーティリティを使用して iSCSI を設定すると発生します。	1. F2 BIOS セットアップ メニューを入力し、iSCSI 設定の [詳細設定 (Advanced)] タブにアクセスします。 2. iSCSI**イニシエータ名**と**ターゲット名**を入力します。 3. 保存して終了します。	4.0(4b)
CSCvq81930	4.0(2c) から 4.0(4b) または 4.0(4e) へのアップグレード中に、次の Intel ドライブのファームウェア更新が失敗します。 • SSDSC2KB038T7K : 3.8TB 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	ドライブを更新するには、[u 4.0 (2f)] を使用します。	4.0(4b)

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvo39645	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(4b)

リリース 4.0(2) で未解決の問題

リリース 4.0(2c)

リリース 4.0 (2c) では、次の障害が未解決です。

表 *55 : BIOS*

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvn09309	POST 中に**F12**キーを押して PXE をブートしようとしても、F12 ネットワークブートは Cisco FASTLINQ QL45611HLCU 100gbe アダプタでは機能しません。	**F6** または **F2** キーを押して、PXE ブートのために Cisco fastlinq QL45611HLCU 100GBE アダプタを選択します。	4.0(2c)

表 *56 :* 外部コントローラ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvm78123	Intel® XXV710 DA2 および X710-t4-T4 カードの iSCSI ブートプロトコルは、ファームウェアバージョン 4.0 (1a) を搭載したサーバのブートユーティリティ (bootutil) には表示されません。	なし	4.0(2c)

不具合 ID	症状	回避策	最初に影響を受けるリリース

CSCvm78419	ファームウェアがバージョン 4.0 (1a) に更新された後、ISCSI lun は、Cisco イーサネット統合 NIC X710-t4 DA2 と Intel X710-t4-X710-DA4、および Intel XL710QDA2 PCIe カードとの TCP/IP 接続を確立できない場合があります。	スイッチで次のコマンドを使用します。
		`conf t`
		`no lldp tlv-select dcbxp`
			4.0(2c)

Open Caveats in Release 4.0(1)

リリース 4.0(1a)

リリース 4.0 (1a) では、次の障害が未解決です。

表 *57 : BIOS*

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvk58997	M4 サーバでは、Windows WDS アプリケーションを使用して IPv6 ベースの UEFI PXE を起動すると、サーバのタイムアウトエラーが発生して失敗します。これは、UEFI モードのすべての M4 サーバで発生します。	IPv4 UEFI PXE を使用します。	4.0(1a)
CSCvo77732	Intel® Xeon®プロセッサ v2 から 4.0 (1a) バージョンに C460 M4 サーバをアップグレードした後、サーバが CATERR 障害を検出し、サーバが応答しなくなります。	3.0 (x) バージョンにダウングレードします。	4.0(1a)

表 *58 : VIC*

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvq64055	遠端スイッチの設定が「no shut」に変更された後、Cisco VIC1455 および VIC 1457 インターフェイスではリンクアップ状態に回復するのに 4 分以上かかります。これは、25G 5M 銅線パッシブケーブル (H25G SFP-H10GB-CU5M) ケーブルが VIC1455 または VIC 1457 および N9K-C93180YC-EX スイッチを接続している場合に発生します。	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-SFP-H10GB-CU3M)。 または 光ケーブルを使用します。	4.0(1a)

以前のリリースで未解決の問題

前のリリースの未解決の問題については、次のリリースノートを参照してください。

Cisco UCS C シリーズソフトウェアのリリースノート

既知の動作

次の項では、既知の動作を示します。

リリース 4.0(4) の既知の動作

リリース 4.0(4i)

リリース 4.0(4i) では、既知の制限事項として次の問題があります。

表 *59 : BMC*

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvo27998	Cisco UCS S3260 サーバでは、TFTP プロトコルを使用して、IPv6 IP アドレスを持つサーバにテクニカルサポート データをエクスポートすることができません。	• 設定を 1 つずつエクスポートします。たとえば、CMC、BMC、VIC などです。 • ファームウェアは他の共有を使用して更新します。	4.0(4i)

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvr96199	DCPMM設定のインポートは、100%のメモリモードが有効になっており、セキュリティが無効になっているサーバでのみサポートされています。Cisco UCS S3260 サーバは100% のメモリ モードをサポートしていないため、DCPMM設定のインポートもサポートされていません。	既知の回避策はありません。	4.0(4i)

リリース 4.0(4e)

リリース 4.0(4e) では、既知の制限事項として次の問題があります。

表 *60 : BMC*

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvp65147	複数の誤ったログイン試行が原因でユーザアカウントがロックされている場合でも、ユーザは、アカウントのロックアウト期間中にIPMI によるユーザ認証が成功した後に IPMI コマンドを実行できます。	CLI または XML API または WebUI インターフェイスを使用して、**[ロックアウト時のユーザの無効化 (Disable user on Lockout)]** 機能を有効にします。これにより、ロックされたユーザは無効になり、ユーザはIPMIコマンドを実行できなくなります。	4.0(4c)

表 *61* : 外部コントローラ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvq20893	サポートされているすべての SN200 シリーズ ドライブは、デバイス マネージャ ページまたは ESXi の [ハードウェア情報 (Hardware info)] ページに SN200 として表示されます。ドライブの詳細なバージョンは表示されません。	なし。	4.0(4e)
CSCvq20302	リアエンドに接続されている HGST SN200 NVMe ドライブ (直接接続) は、Windows OS で通知ドライブの削除が行われても、オフラインになりません。ドライブの LED が数秒間点滅した後、緑色の点灯ステータスが表示されます。	なし。	4.0(4e)

リリース 4.0(4b)

リリース 4.0 (2b) では、既知の制限事項として次の問題があります。

表 *62 : Intel® Optane™* データ センター永続メモリ モジュール

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvo21859	ホストツール (F2) を使用して名前空間が空の名前で設定されている場合は、CLI に範囲を設定できません。	ホストツールから空の名前の名前空間を作成しないでください。	4.0(4b)
CSCvo59901	名前に特殊文字が含まれている名前空間 (ホストツール (F2) を使用) を作成するときに、CLI を使用して CLI に範囲を指定したり、名前空間を削除したりすることはできません。	次のサポートされているもの以外の名前空間名には特殊文字を使用しないでください。 #、-、および _	4.0(4b)

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvo21881	混合モードで目標が作成されている場合、揮発性メモリと永続メモリに割り当てられた実際の容量は、設定されているメモリモードの%を使用して実行された計算と一致しません。	なし。	4.0(4b)

表 *63 : BMC*

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvo13512	電力消費は、設定されている最小制限値には減少しません。これは、Intel® 8260c、6254 CPU SKU を搭載したサーバで発生します。	なし。	4.0(4b)

表 *64 :* 外部コントローラ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvn72355	システムでキャッシュされた i/o ポリシーが有効になっている仮想ドライブ (VD) を作成できません。VD の作成時に、キャッシュされた i/o ポリシーは Cisco IMC および LSI Storage Authority (LSA) で無効になっています。	なし。	4.0(4b)

以前のリリースの既知の動作

以前のリリースの既知の動作については、次のリリースノートを参照してください。

Cisco UCS C シリーズソフトウェアのリリースノート

リリース 4.0 (2) の既知の動作

リリース 4.0(2c)

リリース 4.0 (2c) では、次の警告が既知の制限事項です。

表 *65 : BMC*

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvm08504	サーバファームウェアのダウングレード中に、1050W Psu) のファームウェアバージョンを 4.0 (1) から以前のリリースにダウングレードすると、LLF () の更新は失敗します。	なし。	4.0(2c)

表 *66 :* 外部 *GPU* エクスパンダ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvm92237	**Nvidia-smi** ツール GPU スロットマッピングが、**Lspci** 出力および C480 M5ML シルクスクリーンスロット番号と一致しません。	**Lspci** gpu スロット **Nr/busid** を **nvidia-Smi** GPU スロット **nr/busid** にマッピングするには、次のコマンドを実行します (次の例を参照)。	4.0(2c)

Lspci gpu スロット **Nr/busid** を **nvidia-Smi** gpu スロット **nr/busid** にマッピングします。

```
[root@localhost ~]# lspci -tv

Search for Nvidia Devices with BusID 1b and 1c, for example;
the tree will display GPU PCI bridge BusID mapped to nvidia-smi GPU BusID:

lspci GPU PCI bridge BusID: 19:08.0 mapped with nvidia-smi GPU BusID: [1b]
(1B:00.0)
lspci GPU PCI bridge BusID: 19:0c.0 mapped with nvidia-smi GPU BusID: [1c]
(1C:00.0)

-[0000:17]-+-00.0-[18-1c]----00.0-[19-1c]--+-04.0-[1a]--
 |           |                               +-08.0-[1b]----00.0
                                  NVIDIA Corporation Device 1db5
 |           |                               \-0c.0-[1c]----00.0
                                 NVIDIA Corporation Device 1db5

To find a GPU slot nr, run the following command:

[root@localhost ~]# lspci -vvv -s 19:08.0 | grep -i slot
```

```
 Capabilities: [68] Express (v2) Downstream Port (Slot+), MSI 00
  LnkSta: Speed 8GT/s, Width x16, TrErr- Train-
              SlotClk- DLActive+ BWMgmt- ABWMgmt-
   Slot #3, PowerLimit 0.000W; Interlock- NoCompl-
  VC0: Caps: PATOffset=03 MaxTimeSlots=1 RejSnoopTrans-

[root@localhost ~]# lspci -vvv -s 19:0c.0 | grep -i slot
 Capabilities: [68] Express (v2) Downstream Port (Slot+), MSI 00
  LnkSta: Speed 8GT/s, Width x16, TrErr- Train- SlotClk-
             DLActive+ BWMgmt- ABWMgmt-
   Slot #4, PowerLimit 0.000W; Interlock- NoCompl-
  VC0: Caps: PATOffset=03 MaxTimeSlots=1 RejSnoopTrans-

lspci GPU Slot #3 (19:08.0) corresponds to nvidia-smi GPU Slot # 0 (1B:00.0)
lspci GPU Slot #4 (19:0c.0) corresponds to nvidia-smi GPU Slot # 1 (1C:00.0)

Repeat same steps for the other GPUs
```

表 *67* : 外部 *OS*

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvj48637	HDD アクティビティと特定の LED が AHCI コントローラで動作していません。これは、Red Hat Enterprise Linux OS がインストールされている場合に発生します。	なし。	4.0(2c)
CSCvk15263	インストール時に、iSCSI LUN は、XEN 7.2、7.3、または 7.4 OS バージョンを搭載した Cavium OCP 41232 アダプタには表示されません。	なし。	4.0(2c)

リリース 4.0(1) の既知の動作

リリース 4.0(1a)

次の警告は、リリース 4.0 (1a) の既知の制限事項です。

表 *68 : CMC*

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvi46521	3260 サーバでは、デュアル VIC シングルサーバ設定を使用している場合、2 番目の VIC にはアクセスできません。	2 番目の VIC を使用するには、シングルサーバデュアル VIC 機能を有効にする必要があります。	4.0(1a)

表 *69 :* 外部コントローラ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvk11921	QL41232H 25G OCP カードを搭載した C125 サーバでは、リンクは機能しません。これは、OCP カードが 5M SFP ケーブルを使用してスイッチに接続されている場合に発生します。ネットワーク LED が点灯しておらず、ネットワークが機能していません。	1. BIOS 設定を入力します。 2. **[Advanced > QLOGIC QL41232 Option > Port Level Configuration]**に移動します。 3. リンク速度を 25Gbps に変更します。 4. **F10** を押します。 5. 保存して終了します。	4.0(1a)

以前のリリースの既知の動作

以前のリリースの既知の動作については、次のリリースノートを参照してください。

Cisco UCS C シリーズソフトウェアのリリースノート

関連資料

関連資料

このリリースの設定については、次を参照してください。

- 『Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide』

- 『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』
- Cisco UCS ラックマウント サーバ Cisco IMC API プログラマ ガイド

C シリーズサーバのインストールの詳細については、次を参照してください。

- Cisco UCS C シリーズラックサーバのインストールおよびアップグレードガイド

次の関連資料は、Cisco Unified Computing System（UCS）で入手できます。

- 『Cisco UCS C-Series Servers Documentation Roadmap』
- 『Cisco UCS Site Preparation Guide』
- 『Regulatory Compliance and Safety Information for Cisco UCS』
- 管理用の UCS Manager と統合されたラック サーバでサポートされるファームウェア バージョンとサポートされる UCS Manager バージョンについては、「Release Bundle Contents for Cisco UCS Software」を参照してください。

次の場所にある『Cisco UCS Manager ソフトウェアのリリースノート』および『*Cisco UCS C* シリーズの *Cisco UCS Manager* との統合に関するガイド』を参照してください。

- 『Cisco UCS Manager Release Notes』
- Cisco UCS C シリーズ サーバと Cisco UCS Manager との統合に関するガイド