Cisco UCS C シリーズ ソフトウェア リリース 4.0(2) リリース ノート

初版：2019 年 1 月 2 日

最終更新：2020 年 5 月 5 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(2) 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 5 月 5 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。

改定	日付	説明
I0	2019 年 12 月 20 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。 • このバージョンを 4.0(2m) 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
H0	2019 年 12 月 9 日	次の点が変更されました。 • 「セキュリティ修正」の項を更新。 • このバージョンを 4.0(2l) 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
G0	2019 年 11 月 4 日	次の点が変更されました。 • 「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。 • このバージョンを 4.0(2k) 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
F0	2019 年 9 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。 • このバージョンを 4.0(2i) 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
E0	2019 年 8 月 1 日	次の点が変更されました。 • 「解決済みの警告」の項を更新。 • 「セキュリティ修正」の項を更新。 • このバージョンを 4.0(2h) 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
D0	2019 年 5 月 15 日	次の点が変更されました。 • 「解決済みの警告」の項を更新。 • 「新しいハードウェア」の項を更新しました。 • HUU バージョンを 4.0(2g) 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
C0	2019 年 3 月 13 日	次の点が変更されました。 • 「解決済みの警告」の項を更新。 • HUU バージョンを 4.0 (2f) 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
B0	2019 年 1 月 17 日	次の点が変更されました。 • 「解決済みの警告」の項を更新。 • HUU バージョンを 4.0(2d) 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 1 月 2 日	4.0(2c) 向けリリース ノートを作成しました。

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

サーバ モデルの概要

サポートされるプラットフォーム

リリース 4.0(2m)

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 S3260 M4
- UCS S3260 M5

リリース 4.0(2l)

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 M4
- UCS C240 M4
- UCS C460 M4
- UCS S3260 M4

リリース 4.0(2k)

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 S3260 M4
- UCS S3260 M5

リリース 4.0(2i)

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 C460 M4
- UCS S3260 M4
- UCS S3260 M5

リリース 4.0 (2d)

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 S3260 M4
- UCS C125 M5
- UCS C220 M5
- UCS C240 M5
- UCS C480 M5
- UCS S3260 M5

リリース 4.0(2c)

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 C480 M5 ML
- UCS C125 M5
- UCS C220 M5
- UCS C240 M5
- UCS C480 M5
- UCS S3260 M5
- UCS S3260 M4
- UCS C220 M4
- UCS C240 M4
- UCS C460 M4

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。

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

C シリーズ ラックマウント サーバ向け Cisco UCS C シリーズ および Cisco UCS Manager 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。

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 (2m)	サポートしない	S3260 M4 および M5
4.0 (2l)	サポートしない	C125 M5 サーバを除くすべての M4 および M5 サーバ。
4.0 (2k)	サポートしない	S3260 M4 および M5
4.0 (2i)	サポートしない	C460 M4、S3260 M4、および S3260 M5
4.0 (下半期)	4.0(2e)	すべての M4、M5 サーバ、C125 M5 および C480 ML M5 サーバ。
4.0 (2f)	4.0(2d)	すべての M4、M5 サーバ、C125 M5 および C480 ML M5 サーバ。
4.0(2d)	4.0(2b)	すべての M4、M5 サーバ、C125 M5 および C480 ML M5 サーバ。
4.0(2c)	4.0(2a)	すべての M4、M5 サーバ、C125 M5 および C480 ML 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 (1e)	サポートなし。	すべての M4、M5 サーバと C125 M5
4.0(1d)	4.0(1d)	すべての M4、M5 サーバと C125 M5
4.0(1c)	4.0(1c)	すべての M4、M5 サーバと C125 M5
4.0(1b)	4.0(1b)	すべての M4、M5 サーバと C125 M5
4.0(1a)	4.0(1a)	すべての M4、M5 サーバと C125 M5
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。	C480 M5、C220 M5、C240 M5、S3260 M5
3.1 (3i)	3.2(3i)	C480 M5、C220 M5、C240 M5、S3260 M5
3.1(3h)	3.2(3h)	C480 M5、C220 M5、C240 M5、S3260 M5
3.1(3g)	3.2(3g)	C480 M5、C220 M5、C240 M5、S3260 M5
3.1(3f)	3.2 (3f)	C480 M5、C220 M5、C240 M5、S3260 M5
3.1(3d)	3.2(3e)	C480 M5, C220 M5, C240 M5, S3260 M5
3.1(3c)	3.2(3d)	C480 M5, C220 M5, C240 M5, S3260 M5
3.1(3b)	3.2(3b)	C480 M5、C220 M5、C240 M5
3.1(3a)	3.2(3a)	C480 M5, C220 M5, C240 M5, S3260 M5
3.1(2d)	3.2(2d)	C480 M5, C220 M5, C240 M5
3.1(2c)	3.2(2c)	C480 M5, C220 M5, C240 M5

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(2b)	3.2(2b)	C480 M5, C220 M5, C240 M5
3.1 (1d)	3.2(1d)	C220 M5、C240 M5
3.0(3a)	3.1(3a)	C220 M4、C240 M4 のみ
3.0(2b)	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。	C220 M4、C240 M4 のみ
3.0(1d)	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。	C420 M3 を除くすべての M3 および M4 サーバ
2.0(13e)	3.1(2b)	すべての M3 および M4 サーバ。ただし、C420 M3 を除く
2.0(10b)	3.1(1g)	C220 M4、C240 M4 のみ
2.0 (9c)	3.1(1e)	その他のすべての M3/M4 サーバ
2.0(9f)	2.2 (7b)	その他のすべての M3/M4
2.0(10b)	2.2 (7b)	C220 M4、C240 M4 のみ
2.0 (9c)	2.2 (8f)	その他のすべての M3/M4
2.0(10b)	2.2(8f)	C220 M4、C240 M4 のみ
2.0 (12b)	2.2(8f)	C460 M4 のみ
2.0 (8d)	2.2(6c)	その他のすべての M3/M4
2.0(6d)	2.2(5a)	その他のすべての M3/M4
2.0 (4c)	2.2 (4b)	その他のすべての M3/M4
2.0 (3d) 1	2.2(3a)	その他のすべての M3/M4

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(2) 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-c480m5-huu-4.0.2 ucs-c125-huu-4.0.2 ucs-c240m5-huu-4.0.2 ucs-c220m5-huu-4.0.2 ucs-s3260-huu-4.0.2 ucs-c240m4-huu-4.0.2 ucs-c220m4-huu-4.0.2 ucs-c460m4-huu-4.0.2 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.4.0.2.iso	ドライバ
Unified Computing System（UCS）ユーティリティ	ucs-cxxx-utils-efi.4.0.2.iso ucs-cxxx-utils-linux.4.0.2.iso ucs-cxxx-utils-vmware.4.0.2.iso ucs-cxxx-utils-windows.4.0.2.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

Supported Features

サポートされる機能

リリース 4.0(2m)

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 (2d)

次の新しいソフトウェア機能がリリース 4.0(2d) でサポートされます。

- CLI および XML API コマンドを使用して、デバイス コネクタのファームウェア バージョンを更新するためのサポートが追加されました。

リリース 4.0(2c)

次の新しいソフトウェア機能がリリース 4.0(2c) でサポートされます。

- 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可能な**証明書マネージャ**を追加しました。

- **単一 IP プロパティ**：Cisco IMC 管理への IPv4 アドレスの割り当てを可能にする単一の IP プロパティを設定するオプションが追加されました。

  （注） この機能は、S3260 サーバでのみ使用できます。

- **PCI スイッチの更新**：存在する PCI スイッチに関する情報を表示するオプションが追加されました。また、特定の PCI スイッチの詳細を表示することもできます。

  （注） 特定のスイッチの詳細を表示するオプションは、C480 M5 ML サーバでのみ使用できます。

- **vNIC 設定更新**：vNICs で**[マルチ キュー (Multi Queues)]**を有効にして設定するためのオプションが追加されました。
- **VMMQ Windows サポート**：14xx シリーズ アダプタで Windows 2016 以降の VMMQ サポートが追加されました。
- **vHBA 設定の更新**：**[vHBA タイプ (vHBA Type)]**を設定するためのオプションが追加されました。設定オプションは以下のとおりです。
  - **fc-initiator**
  - **fc-target**
  - **fc-nvme-initiator**
  - **fc-nvme-target**
- **FC 上の NVMe サポート**：VIC 14xx シリーズ アダプタの FV 上の NVMe サポートを追加しました。
- **管理者以外のユーザーのパスワードの変更**: 読み取り専用のユーザー権限を持つユーザーがパスワードを変更できる機能が追加されました。

  （注） このオプションは、管理者ユーザーには使用できません。

- **BIOS トークンの更新**：**Bios テクニカルログ レベル**と**optionrom 起動最適化**BIOS トークンが追加されました。
- **仮想 KVM コンソール更新**：KVM セッションの統計情報と USB 接続をリセットするオプションを表示するオプションが追加されました。

リリース 4.0(2) の新規ハードウェア

リリース 4.0 (2g)

次の新しいハードウェアがリリース 4.0 (2g) で追加されました。

C125 M5 サーバ上の Intel® XXV710 25G 2 ポート SFP PCIe アダプタ (UCSC pcie ID25GF) をサポートします。

リリース 4.0(2c)

次の新しいハードウェアがリリース 4.0 (2c) で追加されました。

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 インターコネクト）
- 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 台のスモール フォーム ファクタ（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 M5 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

（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。

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。

- 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）

- 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。
- 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 M5 での QLogic FastLinQ QL41132HORJ デュアル ポート 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 M5 での QLogic FastLinQ QL41232HOCU デュアル ポート 25G ネットワーク アダプタ カード (UCSC-PCIE-QD25GF) をサポートしています。
- UCS C480 M5 ML での QLogic FastLinQ QL45611H 100GbE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。
- 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。
- UCS C240 M5 サーバ上の AMD Radeon Pro V340、2X16GB GB、300W GPU カード (UCSC-GPU-V340) をサポートします。

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。

リリース 4.0 (2) のセキュリティ修正

リリース 4.0(2l) のセキュリティ修正

次のセキュリティ修正がリリース 4.0(2l) に追加されました。

リリース	不具合 ID	CVE	症状
4.0 (2l)	CSCvr54416	• CVE-2019-0151 • CVE-2019-11137	

リリース	不具合 ID	CVE	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-2019-0151 (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。 このリリースには、Cisco UCS M4 世代サーバ

リリース	不具合 ID	CVE	症状
			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 (2) のセキュリティ修正

次のセキュリティ修正がリリース 4.0(2h) に追加されました。

リリース	不具合 ID	CVE	症状
4.0 (下半期)	CSCvq66225	• CVE-2019-9836	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、次を参照してください。 https://www.amd.com/en/corporate/product-security

リリース 4.0(2g) のセキュリティ修正

リリース 4.0 (2g) 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 (2g)	CSCvp34790 CSCvp34799	• 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 C シリーズおよび S シリーズ 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。 • 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 M4 世代サー

リリース	不具合 ID	CVE	症状
			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。

リリース	不具合 ID	CVE	症状
4.0 (2g)	CSCvp34786	• 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 C シリーズおよび S シリーズ 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。 • 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 M4 世代サー

リリース	不具合 ID	CVE	症状
			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。

リリース	不具合 ID	CVE	症状
4.0 (2g)	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。

リリース 4.0(2c) のセキュリティ修正

次のセキュリティ修正は、リリース 4.0(2c) で対処されました。

リリース	不具合 ID	CVE	説明
4.0(2c)	CSCvm35067	CVE-2016-1549 CVE-2018-7184 CVE-2018-7170 CVE-2018-7185 CVE-2018-7182 CVE-2018-7183	Cisco 統合管理コントローラには、次の一般的な脆弱性と暴露 (CVE) ID によって識別された脆弱性の影響を受ける ntpd のバージョンが含まれています。 CVE-2016-1549、CVE-2018-7184、CVE-2018-7170、CVE-2018-7185、CVE-2018-7182、CVE-2018-7183。 この脆弱性は、リリース 4.0(2c) で修正されました。

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。

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 *3 : 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)
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)

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
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 *4 :* 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 *5 : 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 *6 :* 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 *7 : 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 *8 : 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 *9 : 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 *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
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 *11 :* 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 *12 : 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)

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
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 *13 : 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 *14 :* 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)

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
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 *15 : 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 *16 :* 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(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 *17 : 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 *18 :* 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)

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 *19 : 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 *20 : 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 (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 *21 : 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 *22 :* 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 *23* : 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 *24 : 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 *25 :* 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