Cisco UCS C シリーズ ソフトウェア リリース 4.0(1) リリース ノート

初版：2018 年 8 月 14 日

最終更新：2019 年 6 月 25 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(1) 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

リビジョン	日付	説明
G0	2019 年 6 月 25 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 (1g) 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 2 月 18 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 (1e) 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

リビジョン	日付	説明
E0	2018 年 12 月 10 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 (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
D0	2018 年 11 月 5 日	次のソフトウェアリリース (バージョン 4.0 (1.240)) は、延期通知とともに再度投稿され、ダウンロードできなくなりました。詳細については、ソフトウェアに掲載されている延期通知を参照してください。 • https://software.cisco.com/download/home/286318809/type/283850974/release/4.0%25281.240%2529 • https://software.cisco.com/download/home/286318800/type/283850974/release/4.0%25281.240%2529

リビジョン	日付	説明
C0	2018 年 10 月 11 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」の項が追加されました。 • このバージョンを 4.0 (1c) 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	2018 年 9 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。
		• バージョンが 4.0 (1b) に変更されました。次のハードウェアのファームウェアが更新されました。
		  • Intel® SSD DC S4500 および DC S4600 シリーズ SATA
		  • Micron 5100 SATA SSD (M.2 および U.2)
		  • Intel® SSD DC P4500 および P4600 シリーズ NVMe
		
		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

リビジョン	日付	説明
A0	2018 年 8 月 14 日	4.0(1a) のリリース ノートを作成

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 30 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 7、Microsoft Windows XP、Microsoft Windows Vista、Microsoft Windows 10、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

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 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、アダプタ ユーティリティ、およびストレージ アレイの相互運用性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

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(1e)	サポートしない	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

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(1a)	4.0(1a)	すべての M4、M5 サーバと C125 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
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

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
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 HUU (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 HUU (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。 • 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 HUU (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 HUU (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

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
		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。

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(1) 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-c125-huu-4.0.1 ucs-c240m5-huu-4.0.1 ucs-c220m5-huu-4.0.1.iso ucs-c480m5-huu-4.0.1.iso ucs-s3260-huu-4.0.1.iso ucs-c240m4-huu-4.0.1.iso ucs-c220m4-huu-4.0.1.iso ucs-c460m4-huu-4.0.1.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 4.0.1	ドライバ
Unified Computing System（UCS）ユーティリティ	ucs-cxxx-utils-efi.4.0.1.iso ucs-cxxx-utils-linux.4.0.1.iso ucs-cxxx-utils-vmware.4.0.1.iso ucs-cxxx-utils-windows.4.0.1.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
- 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

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。

http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-rack-servers/products-user-guide-list.html

Supported Features

サポートされる機能

次の新しいソフトウェア機能がリリース 4.0(1a) でサポートされます。

- **デバイスコネクタの更新**: 次の更新が追加されました。
  - Cisco Intersight のみを使用して、C シリーズサーバを設定するためのサポートが追加されました。このオプションを使用すると、Cisco IMC と Cisco Intersight の両方を使用するか、Cisco Intersight のみを使用して、サーバ設定を管理できます。
  - **[接続 (Connections)]** 領域に**デバイス ID**と**クレーム コード**フィールドが追加されました。
- **ネットワーク アダプタの更新**: 次の変更が追加されました。
  - **一般的なアダプタ プロパティの変更**:

    ポート チャネル: ポート チャネルを有効にするオプションが追加されました。このオプションを有効にすると、2 つの vNIC と 2 つの vHBA がアダプタ カードに使用できます。無効にすると、4 つの vNIC と 4 つの vHBAs が使用できます。
  - **ポート チャネル対応**: アダプタ上のポートチャネルサポートを示すフィールドが追加されました。
  - **外部イーサネット インターフェイスの変更:**

    ADMIN FEC モード: 管理前方誤り訂正 (FEC) モードを設定するためのオプションが追加されました。

（注） FEC モードは、25G リンク速度に対してのみ適用されます。14xx アダプタでは、アダプタに設定された FEC モードはスイッチの FEC モードと一致している必要があります。そうしないと、リンクは機能しません。

  - **動作中の FEC モード**)] 動作前方誤り訂正 (FEC) モードを表示するオプションが追加されました。

- **BIOS アクティベーションの更新**: ホストが**オン**のときに BIOS をアクティブ化するためのサポートが追加されました。保留中の BIOS アクティベーションをキャンセルするための BIOS アクティベーション機能のキャンセルも追加されました。
- **セキュリティ設定の更新**:**共通基準 (CC)**を有効にするオプションが追加されました。
- **Flexutil 仮想ドライブの更新**: 仮想ドライブに存在するイメージ ファイルの名前を表示する **[常駐イメージ (present image)]** フィールドが追加されました。
- **XML API の更新**: Cisco Intersight デバイス コネクタ、ポート チャネル、ポート チャネル対応、管理 FEC モード、およびオペレーティング FEC モードに対する XML API サポートが追加されました。
- **監査ログの更新**: 監査ログは、Cisco IMC を使用して UCS C シリーズサーバで行った設定変更の詳細(実行された変更、ユーザの詳細、および使用されているインターフェイス)を使用して生成されます。
- **PXE IPv6 サポート**—Cisco UCS C シリーズおよび S シリーズ M4 サーバは、PXE ブートデバイスで IPv6 オプションをサポートします。

（注） このオプションは、リリース 3.1 (2) および S シリーズ (S3260 M5) からリリース 3.1 (3) 以降の C シリーズ M5 サーバでサポートされています。

リリース 4.0 (1) の新しいハードウェア

Cisco UCS C125 M5 サーバ

Cisco UCS C125 M5 サーバ のサポート。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 シリーズ ラック サーバ シャーシは、2 ー 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
- 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

- 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 サーバの新しい Generation System I/O CONTROL (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。

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。

- 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

このリリースでは、VIC 1455 または VIC 1457 を搭載した Nexus スイッチと C シリーズサーバ間の 10/25G イーサネット接続がサポートされています。

14xx VIC カードを搭載したネットワークアダプタを設定する際には、次の点を考慮する必要があります。

- ポート チャネル上での FCoE はサポートされていません。FCoE は、非ポート チャネル モードではサポートされています。
- VMQ はサポートされていません。
- VXLAN がサポートされています。

これらの VIC カードの詳細については、「CISCO UCS 仮想インターフェイスカードのデータシート」を参照してください。

周辺機器（Peripherals）

- Intel Xpoint ブランド NVMe Med。C220、C240、C480、および S3260を含む M5 サーバのパフォーマンス ドライブ。
- UCS C220、C240、C480 M5 プラットフォーム上の LSI 9400 8e 外部 SAS HBA 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。

セキュリティ修正

リリース 4.0 (1g) でのセキュリティ修正

リリース 4.0 (1g) 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(1g)	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 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 Cisco IMC 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 Uncacheable 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 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。 • 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

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(1g)	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(1g)	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 4.0 (1c) 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 (1c) で対処されました。

リリース	不具合 ID	CVE	説明
4.0(1c)	CSCvm35067	CVE-2018-3655	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。この脆弱性は、リリース 4.0 (1c) で修正されました。

解決済みの不具合 (p.11)

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(1) の解決済みの問題

リリース 4.0 (1g)

次の警告はリリース 4.0(1g) で解決されました。

表 *3 : 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
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 (1g)

リリース 4.0(1e)

次の警告はリリース 4.0(1e) で解決されました。

表 *4 : 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 (1e)
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 (1e)

リリース 4.0 (1d)

次の警告はリリース 4.0(1d) で解決されました。

表 *5 : 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
CSCvn02204	Cisco IMC をバージョン 4.0 (1a) にアップグレードすると、SNMP が動作を停止します。	4.0(1a)	4.0(1d)
CSCvm89001	特殊文字を含む期限切れのパスワードを変更することはできません。	3.0 (4a)	4.0(1d)

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
CSCvn26128	QL45212H および QL41212H アダプタのファームウェアアップデートステータスには更新が表示されますが、ファームウェアは変更されません。	3.0(4j)	4.0(1d)

リリース 4.0 (1c)

次の警告はリリース 4.0(1c) で解決されました。

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
CSCvm34402	BMC を 4.0 (1a) にアップグレードすると、シャーシのファン速度が最大速度 (RPM) に変更され、ノイズが発生します。	4.0(1a)	4.0(1c)

リリース 4.0(1b)

次の警告はリリース 4.0(1b) 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
CSCvk52168	S3260 サーバでは、SLAAC を使用して KVM または Cisco IMC web UI を起動すると、BMC SLAAC IP が ping に応答しません。	3.0 (4i)	4.0(1b)

リリース 4.0 (1a)

リリース 4.0(1a) では、次の問題が解決されます。

表 *9 : 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
CSCve46673	高精度のブート順序では、レガシーモードのサードパーティ製ネットワークアダプタはリストされません。	3.1 (1d)	4.0(1a)

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
CSCvi52975	Cisco IMC のログと障害履歴には、設定されたタイムゾーンは表示されません。これは、デフォルトのタイムゾーンを変更し、選択したタイムゾーンを設定した場合に発生します。	3.1(3a)	4.0(1a)
CSCvi53766	S3260 M5 および S3260 M4 サーバでは、Cisco IMC web UI の [**タイムゾーン**の設定] ページに空白の画面が表示されます。	3.1(3a)	4.0(1a)
CSCvg34851	ユーザパスワードに「$」記号を使用すると、ftp を使用した vNIC 設定 (vNIC) のエクスポートが失敗します。	3.0(3a)	4.0(1a)

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
CSCvj66524	S3260 サーバで、BIOS POST タイムアウトエラーが Cisco IMC に表示される場合があります。これは、サーバが正常にブートし、問題なく実行されている場合でも発生します。 次のエラーメッセージが表示されます。「BIOSPOST_TIMEOUT: BIOS POST TIMEOUT が発生しました: CISCO TAC に問い合わせてください」	3.0(1c)	4.0(1a)
CSCvj74285	ファームウェアバージョン 3.1 (3a) を搭載した M5 サーバのメモリ不足 (OOM) により、Cisco IMC がリブートします。Cisco IMC はネットワーク経由でアクセスできません。	3.1(3a)	4.0(1a)

表 *11* : 外部ストレージ :

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
CSCvh31592	Windows 2016 OS がクラッシュすると、BSOD が発生し、ホストがリブートします。これは、RAID 1 ボリュームでの IO トランザクションを伴う高負荷 IO が長時間にわたって実行される場合に発生します。	3.1(3a)	4.0(1a)

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
CSCvb96598	サーバをリリース 3.0 (1x) にアップグレードした後、SAS HBA コントローラで「CTRL+C」ユーティリティを使用してブートデバイスを再挿入しようとすると、デフォルトの add キー「+」は期待どおりに機能しません。[Boot Order] フィールドは、複数のコントローラが存在することを示す値または 0または1を受け入れます。ただし、現在、フィールドの値を変更したり、入力したりすることはできません。 これは、リリース 2.0 (10) または 2.0 (13) などの以前のリリースからアップグレードする場合に発生します。	3.0(1c)	4.0(1a)
CSCvd07355	S3260 サーバでは、接続管理を有効または無効にすると、予測不可能な I/O パフォーマンスが得られます。これは、ホストがオンラインになったときに発生します。	3.0(3a)	4.0(1a)
CSCvd25263	まれに、Cisco 12G SAS モジュール型 RAID コントローラは、高負荷の IO ロードが発生している間にマルチビット ECC エラーを発生させる可能性があります。	3.0(3a)	4.0(1a)

表 *12 : Web* 管理

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
CSCvj37231	Cisco IMC が 3.0 (4a) バージョンにアップグレードされた後、SMTP はメールアラートの送信を停止します。	3.0 (4a)	4.0(1a)

表 *13 : 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
CSCus94537	HDD を使用する HDD ファームウェアの更新は、HDD ファームウェアが順番に更新されるため、時間がかかります。これにより、多くの HDD を搭載したサーバのアップグレードにかかる時間が長くなります。	2.0(3d)	4.0(1a)

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(1) で未解決の問題

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 *14 : 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)

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(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 *15 : 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 *16 :* 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 リリースノート
- 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