Cisco UCS ラック サーバー ソフトウェア、リリース 4.1(3) のリリース ノート

初版：2021 年 1 月 4 日

最終更新：2023 年 1 月 17 日

Cisco UCS C シリーズと S シリーズ サーバー

Cisco UCS C シリーズおよび S 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（Cisco IMC）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 シリーズおよび S シリーズのソフトウェア リリース 4.1(3) の新機能、システム要件、未解決の問題、および既知の動作について説明します。このドキュメントは、関連資料 （56 ページ） セクションの一覧にあるドキュメントと併せて使用します。

（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、マニュアルの更新については、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
F0	2023 年 1 月 17 日	4.1(3l) のリリース ノートを作成 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 から入手可能です。

改定	日付	説明
E1	2022 年 8 月 10 日	4.1(3g) の「**既知の動作と制限**」の項を更新しました。
G0	2022 年 8 月 1 日	4.1(3i) のリリース ノートを作成 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 4.1 から入手可能です。
F0	2022 年 6 月 27 日	4.1(3h) のリリース ノートを作成 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 4.1 から入手可能です。
E0	2022 年 4 月 11 日	4.1(3g) のリリース ノートを作成 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 4.1 から入手可能です。
D1	2022 年 3 月 21 日	CSCvz77885 を更新 - **4.1(3f) で解決された警告**の不具合 ID。

改定	日付	説明
D0	2022 年 01 月 31 日	4.1(3f) のリリース ノートを作成 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 4.1 から入手可能です。
A3	2021 年 8 月 18 日	リリース 4.1（3b） の新しいハードウェア サポートを更新。
B1	2021 年 8 月 3 日	4.1（3c） の解決済みの不具合が更新されました。
C0	2021 年 7 月 30 日	4.1（3d） のリリース ノートを作成 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 4.1 から入手可能です。
B0	2021 年 5 月 31 日	4.1（3c） のリリース ノートを作成 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 4.1 から入手可能です。
A2	2021 年 3 月 30 日	4.1（3b） の解決済みの不具合が更新されました。
A1	2021 年 2 月 1 日	Cisco UCS C125 M5 サーバーのダウングレード制限を追加。

改定	日付	説明
A0	2021 年 1 月 13 日	4.1（3b）のリリース ノートを作成 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 4.1 から入手可能です。

サポートされるプラットフォームとリリースの互換性マトリクス

このリリースでサポートされているプラットフォーム

次の Cisco UCS サーバーがこのリリースでサポートされています。

- UCS C125 M5
- UCS C220 M5
- UCS C240 SD M5
- UCS C240 M5
- UCS C480 M5
- UCS C480 ML M5
- UCS S3260 M5
- UCS S3260 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。

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

Cisco UCS C シリーズと S 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 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、ラックマウント サーバのサポートされたプラットフォーム、Cisco IMC リリース、および Cisco UCS Manager リリースを示します。

表 *1 : Cisco IMC 4.1(3)* リリースのラック マウント サーバー用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.1(3l)	4.1(3k)	Cisco UCS C480 M5、C220 M5、および C240 M5 サーバー

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.1(3i)	4.1(3j)	Cisco UCS C220 M5、C240 M5、C480 M5、S3260 M4、S3260 M5、C125 M5 サーバー
4.1(3h)	4.1(3i)	Cisco UCS C220 M5、C240 M5、C480 M5、S3260 M4、S3260 M5、C125 M5 サーバー
4.1(3g)	サポートなし	Cisco UCS S3260 M4 および S3260 M5 サーバ
4.1(3f)	4.1(3h)	Cisco UCS C220 M5、C240 M5、C480 M5、S3260 M4、S3260 M4、S3260 M5、および C125 M5 サーバー
4.1（3d）	4.1(3e)	Cisco UCS C220 M5、C240 SD M5 、C240 M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー
4.1（3c）	4.1（3d）	Cisco UCS C220 M5、C240 SD M5 、C240 M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー
4.1（3b）	4.1(3a)	Cisco UCS C220 M5、C240 SD M5 、C240 M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー

表 *2 : Cisco IMC 4.1(2)* リリースのラック マウント サーバー用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.1(2l)	サポートなし	Cisco UCS C220 M4、C240 M4 サーバー。
4.1(2k)	サポートなし	Cisco UCS C220 M4、C240 M4、および C460 M4 サーバー
4.1(2j)	サポートなし	Cisco UCS C220 M4、C240 M4、および C460 M4 サーバー

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.1(2h)	サポートなし	Cisco UCS C220 M4、C240 M4、および C460 M4 サーバー
4.1(2g)	サポートなし	Cisco UCS C220 M4、C240 M4、および C460 M4 サーバー
4.1(2f)	4.1（2c）	Cisco UCS C220 M5、C240 SD M5、C240 M5、C480 M5、C480 ML M5、S3260 M5、C220 M4、C240 M4、C460 M4、および S3260 M4 サーバー
4.1(2e)	サポートなし	Cisco UCS C125 M5 サーバー
4.1(2d)	サポートなし	Cisco UCS C240 M5 および C240 SD M5 サーバー
4.1(2b)	4.1(2b)	Cisco UCS C220 M5、C240 SD M5、C240 M5、C480 M5、C480 ML M5、S3260 M5、C125 M5、C220 M4、C240 M4、C460 M4、および S3260 M4 サーバー
4.1(2a)	4.1(2a)	Cisco UCS C220 M5、C240 SD M5、C240 M5、C480 M5、C480 ML M5、S3260 M5、C125 M5、C220 M4、C240 M4、C460 M4、および S3260 M4 サーバー

表 *3 : Cisco IMC 4.1(1)* リリースのラック マウント サーバ用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.1(1h)	4.1(1e)	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
4.1(1g)	4.1(1d)	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

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.1(1f)	4.1(1c)	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
4.1(1d)	4.1(1b)	Cisco UCS C220 M5、C240 M5、C480 M5、および C480 ML M5 サーバ
4.1(1c)	4.1(1a)	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

表 *4 : Cisco IMC 4.0(4)* リリースのラックマウント サーバ用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.0(4n)	4.0(4l)	Cisco UCS C220 M5、C240 M5、C480 M5、および S3260 M5 サーバ
4.0(4m)	4.0(4j)	Cisco UCS C220 M5、C240 M5、C480 M5、および S3260 M5 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

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント 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

表 *5 : Cisco IMC 4.0(3)* リリースのラックマウント サーバ用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.0(3b)	4.0(3a)	Cisco UCS C220 M5 および C240 M5 サーバ

表 *6 : Cisco IMC 4.0(2)* リリースのラックマウント サーバ用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.0(2r)	サポートなし	Cisco UCS C220 M4、C240 M4、および C460 M4 サーバー。
4.0(2q)	4.0(4l)	Cisco UCS C220 M4、C240 M4、C460 M4、および S3260 M4 サーバ
4.0(2p)	サポートしない	Cisco UCS C125 M5 サーバー
4.0(2o)	4.0(4j)	Cisco UCS C220 M4、C240 M4、C460 M4、および S3260 M4 サーバ
4.0(2n)	サポートしない	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

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.0(2m)	サポートなし	Cisco UCS S3260 M4 および M5 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 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)	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、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(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

表 *7 : Cisco IMC 4.0(1)* リリースのラックマウント サーバ用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.0 (1h)	サポートしない	Cisco UCS C220 M4、C240 M4、C460 M4、C220 M5、C240 M5、C480 M5 サーバーおよび C125 M5

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.0 (1g)	サポートしない	Cisco UCS C220 M4、C240 M4、C460 M4、C220 M5、C480 M5 サーバーおよび C125 M5
4.0 (1e)	サポートしない	Cisco UCS M4、M5 サーバおよび C125 M5
4.0(1d)	4.0(1d)	Cisco UCS M4、M5 サーバおよび C125 M5
4.0(1c)	4.0(1c)	Cisco UCS M4、M5 サーバおよび C125 M5
4.0(1b)	4.0(1b)	Cisco UCS M4、M5 サーバおよび C125 M5
4.0(1a)	4.0(1a)	Cisco UCS M4、M5 サーバおよび C125 M5

表 *8 : Cisco IMC 3.1(3)* リリースのラック マウント サーバ用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
3.1(3k)	3.2(3p)	Cisco UCS C480 M5、C220 M5、C240 M5、および S3260 M5 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

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント 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(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

表 *9 : Cisco IMC 3.1(2)* リリースのラック マウント サーバ用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
3.1(2d)	3.2(2d)	Cisco UCS C480 M5、C220 M5、および C240 M5
3.1(2c)	3.2(2c)	Cisco UCS C480 M5、C220 M5、および C240 M5
3.1(2b)	3.2(2b)	Cisco UCS C480 M5、C220 M5、および C240 M5

表 *10 : Cisco IMC 3.1(1)* リリースのラックマウント サーバ用 *Cisco IMC* および *UCS Manager* 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
3.1 (1d)	3.2(1d)	Cisco UCS C220 M5/C2540 M5

表 *11 : Cisco IMC 3.0(4)* リリースのラック マウント サーバ用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
3.0(4s)	サポートなし	Cisco UCS C220 M3、C240 M3、C3160 M3、S3260 M4

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
3.0(4r)	サポートなし	Cisco UCS C220 M4、C240 M4、C460 M4、S3260 M4、C22 M3、C24 M3、C220 M3、C240 M3、C3160 M3、S3260 M3
3.0(4q)	サポートなし	Cisco UCS C220 M4、C240 M4、C460 M4、S3260 M4、C22 M3、C24 M3、C220 M3、C240 M3、C3160 M3、S3260 M3
3.0(4p)	3.2(3o)	Cisco UCS C220 M4、C240 M4、C460 M4、S3260 M4、C22 M3、C24 M3、C220 M3、C240 M3、C3160 M3、S3260 M3
3.0(4o)	サポートなし	Cisco UCS C220 M4、C240 M4、C460 M4、S3260 M4、C22 M3、C24 M3、C220 M3、C240 M3、C3160 M3、S3260 M3
3.0 (同一)	サポートしない	Cisco UCS C220 M4、C240 M4、C460 M4、S3260 M4、C22 M3、C24 M3、C220 M3、C240 M3、C3160 M3、S3260 M3
3.0 (4m)	サポートしない	Cisco UCS C220 M4、C240 M4、C460 M4、S3260 M4、C22 M3、C24 M3、C220 M3、C240 M3、C3160 M3、S3260 M3
3.0 (4l)	サポートしない	Cisco UCS C220 M4、C240 M4、C460 M4、S3260 M4、C22 M3、C24 M3、C220 M3、C240 M3、C3160 M3、S3260 M3
3.0 (4k)	サポートしない	Cisco UCS C220 M4、C240 M4、C460 M4、S3260 M4、C22 M3、C24 M3、C220 M3、C240 M3、C3160 M3、S3260 M3
3.0(4j)	3.1(3k)	Cisco UCS C220 M4、C240 M4、C460 M4、S3260 M4、C22 M3、C24 M3、C220 M3、C240 M3、C3160 M3、S3260 M3

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
3.0 (4i)	3.1(3j)	Cisco UCS C220 M4、C240 M4、C460 M4、S3260 M4、C22 M3、C24 M3、C220 M3、C240 M3、C3160 M3、S3260 M3
3.0 (4e)	サポートなし	Cisco UCS C220 M4、C240 M4、C460 M4、S3260 M4、C22 M3、C24 M3、C220 M3、C240 M3、C3160 M3、S3260 M3
3.0 (4d)	3.1(3h)	Cisco UCS C220 M4、C240 M4、C460 M4、S3260 M4、C22 M3、C24 M3、C220 M3、C240 M3、C3160 M3、S3260 M3
3.0 (4a)	3.1(3f)	Cisco UCS C220 M4、C240 M4、C460 M4、S3260 M4、C22 M3、C24 M3、C220 M3、C240 M3、C3160 M3、S3260 M3

表 *12 : Cisco IMC 3.0(3)* リリースのラック マウント サーバ用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
3.0(3f)	-	Cisco UCS C240 M4、および C220 M4
3.0(3e)	3.0(3e)	Cisco UCS C22 M3、C24 M3、C220 M3、C240 M3、C220 M4、C240 M4、C460 M4、C3160 M3、S3260 M4、および S3260 M3 サーバ
3.0 (3c)	3.0 (3c)	Cisco UCS C240 M4、および C220 M4
3.0 (3b)	3.0 (3b)	Cisco UCS S3260 M3、C3160 M3、C460 M4、C240 M4、および C220 M4
3.0(3a)	3.1(3a)	Cisco UCS C22 M3、C24 M3、C220 M3、C240 M3、C220 M4、C240 M4、C460 M4、C3160 M3、S3260 M4、および S3260 M3 サーバ

表 *13 : Cisco IMC 3.0(2)* リリースのラックマウント サーバ用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
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

表 *14 : Cisco IMC 3.0(1)* リリースのラックマウント サーバ用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
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/M4
3.0(1c)	サポートなし	C420 M3 を除くすべての M3/M4

オペレーティング システムとブラウザの要件

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

シスコでは、Cisco UCS ラック サーバー ソフトウェア、リリース 4.1(3) に次のブラウザを推奨しています。

- Microsoft Edge 87.0.664.47 以降（64 ビット）
- Google Chrome バージョン 87.0.4280.66 以降（64 ビット）
- Microsoft Internet Explorer 11.0.9600 以降
- Mozilla Firefox 66.0.2 以降（64 ビット）
- Safari 14.0.1 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。

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 4.1 へのアップグレード パス

このセクションではリリース 4.1(x) へのアップグレード パスについて説明します。

重要 Cisco UCS C220 M5、C240 M5 または C480 M5 サーバをリリース 4.1 にアップグレードする場合は、次の条件に従います。

- 4.0(4) よりも前のリリースからアップグレードする場合
- **[レガシー ブート モード (Legacy Boot Mode)]** が有効になっていて、**[Cisco IMC のブート順序 (Cisco IMC Boot Order)]** が設定されていない場合
- サーバが Cisco HWRAID アダプタから起動している場合

その後、アップグレードする前に次のいずれかを実行する必要があります。

- XML API を使用した UCS ブート順序の設定で提供される XML-API スクリプトおよび UCSCFG ベースのスクリプトを実行します。

  または

- Cisco IMC GUI または CLI インターフェイスを使用して、目的のブート順序を手動で設定します。

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 *15* : リリース *4.1* 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
リリース 4.0 からのすべての M5 サーバー	4.1	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。 • NIHUU ツールを使用してファームウェアをアップデートする際には、 バージョン 4.1（3b） でリリースされた 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
3.1 からのすべての M5 サーバ	4.1	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。 • NIHUU ツールを使用してファームウェアをアップデートする際には、 バージョン 4.1（3b） でリリースされた 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
3.0(3a) よりも大きなリリースのすべての M4 サーバーの場合	4.1	3.0(3a) 以降のリリースから 4.1（3b） 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。 • 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。 • NIHUU ツールを使用してファームウェアをアップデートする際には、 バージョン 4.1（3b） でリリースされた 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 をセキュアにする場合、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
3.0(3a) より小さいリリースのすべての M4 サーバーの場合	4.1	

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
		3.0(3a) 以前のリリースから 4.1（3b） 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。 **3.0(3a) 以前のバージョンから 3.0(3a) 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 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 1.0.1e-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。 **3.0(3a) から 4.1 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。 • NIHUU ツールを使用してファームウェアをアップデートする際には、 バージョン 4.1（3b） でリリー

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
		スされた 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 をセキュアにする場合、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。

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

リリース 4.1(3) の Unified Computing System（UCS）サーバー ファームウェア、ドライバ、およびユーティリティの詳細については、「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 4.1」を参照してください。

（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、http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html を参照してください。

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 4.1 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
- DCPMM メモリ

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ー 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、ホスト更新ユーティリティからすべての選択して、**[更新]** または **[更新とすべての更新して有効化（Update & Activate 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

ダウングレードに関する制限事項

Cisco UCS C125 M5 サーバーのダウングレード制限

リリース 4.1（3b） では、ハードウェアに根ざしたブート整合性を実装する Cisco UCS C125 M5 サーバーに AMD プラットフォーム セキュア ブート（PSB）が導入されています。リリース 4.1（3b） 以降にアップグレードすると、次のことができなくなります。

- 第 2 世代 AMD EPYC 7002 シリーズ プロセッサ（Rome）に基づく Cisco UCS C125 M5 ラック サーバー ノードを、4.1(2e) より前のリリースにダウングレードします。
- AMD EPYC 7001（Naples）に基づく Cisco UCS C125 M5 ラック サーバー ノードを 4.0(2p) より前のリリースにダウングレードします。

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 4.1 の新しいソフトウェア機能

リリース 4.1（3d） での新しいソフトウェア機能

Cisco UCS C125 M5 サーバーの新しい BIOS トークンのサポート:

- **バーストおよび延期された更新**（デフォルト値 - **無効**）

リリース 4.1（3b） での新しいソフトウェア機能

新機能の詳細については、『Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide, Release 4.1 』または『Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 4.1』を参照してください。

次の新しいソフトウェア機能がリリース 4.1（3b） でサポートされています。

- SNMP v3 ユーザーは、DES セキュリティ プロトコルでは追加できません。
- リリース 4.1（3b） では、ハードウェアに根ざしたブート整合性を実装する Cisco UCS C125 M5 サーバーに AMD プラットフォーム セキュア ブート（PSB）が導入されています。PSB は、ハードウェアに統合された信頼のルートを使用して、ROM イメージの整合性と信頼性を保証します。
- Cisco IMC から HTTP サービスのみを無効にできるようになりました。
- TLS 1.3 通信のサポート
- Cisco IMC は、ハード ディスク ドライブ（HDD）診断セルフテストをサポートしています。セルフテストで取得した診断データを使用して、ドライブの状態とパフォーマンスを監視できます。
- Cisco IMC は Terminal Access Controller Access-Control System Plus（TACACS+）認証をサポートしています。最大 6 つの TACACS+ リモート サーバーを設定できます。
- SMTP 受信者ごとに**報告する最小セキュリティ**を構成できます。
- **COB 送信キュー カウント**は、14xx シリーズ アダプタでは最大 64 個の SCSI I/O キューをサポートし、他のアダプタでは最大 245 個のキューをサポートするようになりました。
- このリリースでは、次の BIOS トークンが導入されています。
  - メモリのサーマル スロットリング モード
  - パニックと高水準点
  - メモリのリフレッシュレート
- Cisco UCS M5 サーバーは、OS をインストールするための TFTP ベースの PXE 方式よりも優れたパフォーマンスを提供する HTTP ブート機能をサポートするようになりました。HTTP ブート機能を使用して、診断または構成のためにリモート HTTP サーバーから EFI 実行可能ファイルを実行することもできます。

Intersight 管理モード

Intersight 管理モード（IMM）は、Cisco Intersight で導入された新しい機能セットで、C シリーズ FI の管理対象サーバーのサーバー プロファイルを構成、展開、管理することができます。IMM は、Cisco IMC で最初に導入されたコンセプトを新しく実装しており、ポリシー モデルのオーナシップを Cisco Intersight に移行しています。

Cisco UCS インフラストラクチャおよびサーバー FW バージョン 4.1(3) では、IMM を有効にします (FI および接続されたサーバー用のポリシー駆動型設定プラットフォーム)。IMM を有効にすると、UCS ドメイン全体が工場出荷時のデフォルトにリセットされ、ドメイン内のサーバで実行されているワークロードが中断されます。

リリース 4.1 の新しいハードウェア機能

リリースでの新しいハードウェア サポート 4.1（3d）

リリース 4.1（3d） では、次の新しいハードウェアがサポートされています。

- Cisco UCS C480 M5 サーバーの NVIDIA A-40 GPU のサポート。

リリース 4.1（3b） での新しいハードウェア サポート

リリース 4.1（3b） では、次の新しいハードウェアがサポートされています。

- Cisco UCS C240 M5 および C480 M5 サーバーでの NVIDIA A-100 GPU のサポート。
- 25G の VIC 1455/57 から FI 6454 および N9300 への 4 メートルの AOC ケーブル接続のサポート
- Cisco UCS C240 M5 および C220 M5 サーバーでの Cisco Nexus K3P-S FPGA SmartNIC のサポート。

セキュリティ修正

リリース4.1(3i)でのセキュリティ修正

次のセキュリティ修正がリリース 4.1(3i) に追加されました。

欠陥 ID - CSCwb67159

4Cisco UCS C-Series M5 ラック サーバーは、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るIntel® プロセッサ を搭載しています。

- **CVE-2021-0189** — 一部の Intel® プロセッサの BIOS ファームウェアで範囲外のポインターオフセットを使用すると、特権ユーザーがローカル アクセスを介して特権のエスカレーションを有効にできる可能性があります。
- **CVE-2021-0159** — 一部の Intel® プロセッサの BIOS 認証コード モジュールの不適切な入力検証により、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる可能性があります。
- **CVE-2021-33123** — 一部の Intel® プロセッサの BIOS 認証コード モジュールの不適切なアクセス制御により、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる可能性があります。

- **CVE-2021-33124** — 一部の Intel® プロセッサの BIOS 認証コード モジュールの境界外書き込みにより、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる場合があります。
- **CVE-2022-21131** — 一部の Intel® Xeon® プロセッサの不適切なアクセス制御は認証されたユーザーに対しローカル アクセスを通じて情報開示を許可する可能性があります。
- **CVE-2022-21136** — 一部の Intel® Xeon® プロセッサの不適切な入力検証により、特権ユーザーがローカル アクセスを介してサービス拒否を可能にする可能性があります。

リリース4.1(3h)でのセキュリティ修正

次のセキュリティ修正がリリース 4.1(3h) に追加されました。

欠陥 ID - CSCwb67159

Cisco UCS M5 サーバーは、インテル® プロセッサに基づく Cisco UCS M5 サーバは、次の一般的な脆弱性およびエクスポージャ (CVE) ID によって特定された脆弱性の影響を受けます。

- **CVE-2021-0154** — 一部のインテル® プロセッサの BIOS ファームウェアの不適切な入力検証により、特権ユーザーがローカルアクセスを介して特権の昇格を有効にできる可能性があります。
- **CVE-2021-0155** — 一部のインテル® プロセッサの BIOS ファームウェアの戻り値がチェックされていないため、特権ユーザーがローカルアクセスを介して情報開示を有効にできる可能性があります。
- **CVE-2021-0189** — 一部のインテル® プロセッサの BIOS ファームウェアで範囲外のポインター オフセットを使用すると、特権ユーザーがローカル アクセスを介して特権のエスカレーションを有効にできる可能性があります。
- **CVE-2021-33123** — 一部のインテル® プロセッサの BIOS 認証コード モジュールの不適切なアクセス制御により、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる可能性があります。
- **CVE-2021-33124** — 一部のインテル® プロセッサの BIOS 認証コード モジュールの境界外書き込みにより、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる場合があります。

リリース4.1(3f)でのセキュリティ修正

リリース 4.1(3f) では、次のセキュリティ修正が追加されました。

欠陥 ID - CSCvy91321

Cisco Integrated Management Controller (IMC) ソフトウェアは、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-2021-34736**— Cisco Integrated Management Controller (IMC) ソフトウェアの Web ベースの管理インターフェイスの脆弱性により、認証されていないリモートの攻撃者が Web ベースの管理インターフェイスを予期せず再起動する可能性があります。

  この脆弱性は、Webベースの管理インターフェイスでの入力に対する不十分な検証に起因します。攻撃者は、該当デバイスに巧妙に細工されたHTTP要求を送信することにより、この脆弱性を不正利用する可能性があります。不正利用が成功すると、攻撃者はインターフェイスの再開を引き起こし、その結果サービス妨害（DoS）状態が発生する可能性があります。

  この脆弱性に対処するソフトウェア アップデートは、すでにCiscoからリリースされています。脆弱性に対処する回避策はありません。

欠陥 ID - CSCvz48566

Cisco UCS C220 M4 およびM5 サーバーは、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-2021-3712** —ASN.1 文字列は、OpenSSL 内で ASN1_STRING 構造として内部的に表されます。これには、文字列データを保持するバッファと、バッファ長を保持するフィールドが含まれます。これは、NUL (0) バイトで終了する文字列データのバッファとして表される通常の C 文字列とは対照的です。厳密な要件ではありませんが、OpenSSL 独自の **d2i** 関数 (および他の同様の解析関数) を使用して解析される ASN.1 文字列、および ASN1_STRING_set() 関数で値が設定されている文字列は、 追加のNUL で ASN1_STRING 構造のバイト アレイを終了します。

  ただし、アプリケーションは、ASN1_STRINGアレイの「データ」および「長さ」フィールドを直接設定することにより、バイトアレイをNULで終了しない有効なASN1_STRING構造を直接構築することができます。これは、ASN1_STRING_set0() 関数を使用して行うこともできます。ASN.1データを出力する多数のOpenSSL関数は、ASN1_STRINGバイトアレイが NUL で終了することを想定していますが、これは直接構築された文字列に対しては保証されていません。アプリケーションが ASN.1 構造の印刷を要求し、その ASN.1 構造に、**データ フィールド**を NUL で終了させることなくアプリケーションによって直接構築された ASN1_STRING が含まれている場合、読み取りバッファ オーバーランが発生する可能性があります。

  同じことが、証明書の名前制約処理中にも発生する可能性があります (たとえば、証明書が OpenSSL 解析関数を介してロードする代わりにアプリケーションによって直接構築され、証明書に NUL で終了しない ASN1_STRING 構造が含まれている場合)。X509_get1_email()、X509_REQ_get1_email()、およびX509_get1_ocsp() 関数でも発生する可能性があります。

  攻撃者は、アプリケーションに ASN1_STRING を直接構築させ、影響を受ける OpenSSL 関数の 1 つを介してそれを処理させることができ、この問題が発生する可能性があります。これにより、クラッシュが発生する可能性があります（サービス拒否攻撃を引き起こします）。また、プライベート メモリの内容（プライベート キー、機密性の高い平文など）が漏洩する可能性もあります。

このリリースには、Cisco UCS M4 および M5 ラック サーバーの SSL 改定が含まれています。これらの改訂には、これらの脆弱性の緩和に必要なラック サーバー向けの 更新が含まれています。

欠陥 ID - CSCvz48570

Cisco UCS C220 M4 および M5 サーバーは、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-2021-3711** — API 関数を呼び出して SM2 暗号化データを復号化するときにバッファオーバーフローを引き起こす可能性のある SM2 暗号解読コードの実装。特別に細工された SM2 コンテンツを提示する攻撃者は、この脆弱性を悪用してアプリケーションの動作を変更したり、アプリケーションをクラッシュさせたりする可能性があります。この脆弱性を悪用する攻撃者は、プライベート メモリの内容を開示したり、サービス拒否（DoS）攻撃を実行したりできる可能性があります。

このリリースには、Cisco UCS M4 および M5 ラック サーバーの SSL 改定が含まれています。これらの改訂には、これらの脆弱性の緩和に必要なラック サーバー向けの 更新が含まれています。

リリース4.1（3d）でのセキュリティ修正

リリース 4.1（3d） では、次のセキュリティ修正が追加されました。

欠陥 ID - CSCvy16762

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 サーバーは、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-2020-12358**—一部の Intel® プロセッサのファームウェアの境界外書き込みにより、特権をもつユーザーがローカルアクセスを介してサービスの拒否ができるようになる場合があります。
- **CVE-2020-12360**—一部の Intel® プロセッサのファームウェアの境界外読み取りにより、認証済みユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる場合があります。
- **CVE-2020-24486** — 一部の Intel®プロセッサのファームウェアの不適切な入力検証により、認証済みのユーザーがローカルアクセスを介してサービスの拒否を有効にできる可能性があります。
- **CVE-2020-24511**—一部の Intel® プロセッサでの共有リソースの分離が不適切なため、認証されたユーザーがローカル アクセスを通じて情報開示できるようになる可能性があります。

このリリースには、Cisco UCS M5 ラック サーバーの 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、Cisco UCS M5 サーバー向けの マイクロコードの更新が含まれています。

リリース4.1（3c）でのセキュリティ修正

リリース 4.1（3c） では、次のセキュリティ修正が追加されました。

欠陥 ID - CSCvx82648

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 サーバーは、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-2021-3449** — リモートの認証されていないユーザーが TLS サーバーをクラッシュさせ、サービス拒否 (DoS) 状態を引き起こす可能性があります。
- **CVE-2021-3450** — リモートの認証されていないユーザーが、巧妙に細工された証明書を提供することにより、MiTM攻撃を実行したり、別のユーザーまたはデバイスになりすますことができる可能性があります。

リリース4.1（3b）でのセキュリティ修正

リリース 4.1（3b） では、次のセキュリティ修正が追加されました。

欠陥 ID - CSCvv34145

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 サーバーは、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-2020-0587**— 一部の Intel®プロセッサの BIOS ファームウェアの不適切なアクセス制御により、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる可能性があります。
- **CVE-2020-0588**— 一部の Intel®プロセッサの BIOS ファームウェアの不適切なアクセス制御により、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる可能性があります。
- **CVE-2020-0590** — 一部の Intel®プロセッサの BIOS ファームウェアの不適切な入力検証により、認証済みのユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる可能性があります。
- **CVE-2020-0588**— 一部の Intel®プロセッサの BIOS ファームウェアの不適切なアクセス制御により、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる可能性があります。
- **CVE-2020-0592**—一部の Intel® プロセッサの BIOS ファームウェアの境界外書き込みにより、認証済みユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる場合があります。
- **CVE-2020-0593**— 一部の Intel®プロセッサの BIOS ファームウェアの不適切なアクセス制御により、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる可能性があります。

- **CVE-2020-8696** — 一部の Intel® プロセッサでの保管または転送前の機微な情報の不適切な削除は、認証済みユーザーに対しローカルアクセスを通じて情報開示を許可する可能性があります。
- **CVE-2020-8698**—一部のIntel® プロセッサでの共有リソースの分離が不適切なため、認証されたユーザーがローカル アクセスを通じて情報開示を可能にする可能性があります。
- **CVE-2020-8705** — 11.8.80、11.12.80、11.22.80、12.0.70、13.0.40、13.30.10、5、14.0 より前のバージョンの Intel® CSME での Intel® Boot Guard のリソースの安全でないデフォルトの初期化、3.1.80 および 4.0.30 より前の Intel® TXE バージョン、E5_04.01.04.400、E3_04.01.04.200、SoC-X_04.00.04.200、および SoC-A_04.00.04.300 より前の Intel(R) SPS バージョンでは、認証されていないユーザーが物理的なアクセスを通じて権限の昇格を可能にする可能性があります。
- **CVE-2020-8755** — 12.0.70 および 14.0.45 より前の Intel® CSME バージョン、E5_04.01.04.400 および E3_05.01.04.200 より前の Intel® SPS バージョンのサブシステムの競合状態により、物理的なアクセスを介して、認証されていないユーザーが特権の潜在的にエスカレーションを有効にできる可能性があります。
- **CVE-2020-8738**— 一部の Intel®プロセッサの Intel® BIOS プラットフォーム サンプル コードのファームウェアの不適切なアクセス制御により、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる可能性があります。
- **CVE-2020-8739** — 一部のインテル® プロセッサ向けのインテル BIOS プラットフォームのサンプルコードで潜在的に危険な関数を使用すると、認証されたユーザーがローカルアクセスを介して権限の昇格を可能にする可能性があります。
- **CVE-2020-8740**— 一部の Intel®プロセッサの Intel BIOS プラットフォーム サンプル コードでの境界外書き込みは、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる可能性があります。
- **CVE-2022-8764**— 一部の Intel® プロセッサの BIOS ファームウェアの不適切なアクセス制御により、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる可能性があります。

解決済みの不具合 (p.11)

の解決済みの問題 4.1(3l)

リリース 4.1(3l) では、次の問題が解決されました。

表 *16 : 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
CSCwd20131	Cisco UCS C480 M5 サーバーでは、次のアダプタ PID の BIOS トークンが表示されません。 • DN2-HW-APL-XL-U ただし、次のアダプタ PID の BIOS トークンが表示されます。 • DN2-HW-APL-XL この問題は解決されました。	4.1（3d）	4.1(3l)

表 *17 : BIOS-EX*

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
CSCwd04797	NVMe ドライブを搭載した Cisco UCS M5 サーバーは、UCS ファームウェアのアップグレード後にレガシー ブート モードで POST でスタックします。 この問題は解決されました。	4.1(3h)	4.1(3l)

の解決済みの問題 4.1(3h)

次の問題はリリース 4.1(3h) で解決済みです。

表 *18 : 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
CSCwa85667	BMC のリセットは、カーネルのクラッシュとウォッチドッグのリセットが原因で、Cisco UCS C シリーズ M5/M6 サーバーで観察されます。 この問題は解決されました。	4.0(4m)	4.2（1a）
CSCwb33753	IMM の展開中に、サーバー上のデバイスコネクタの自動更新が失敗し、次のエラーメッセージが表示されることがあります。 標準エラー（Stderr）：マウント：ループ デバイスをセットアップできません：そのようなファイルまたはディレクトリはありません この問題は解決されました。	4.1(3f)	4.2(1i)

表 *19 : Firmware* アップグレード

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
CSCwb21128	特定の条件下では、ハードドライブの遅延時間が長くなり、遅延の影響を受けやすいアプリケーションの操作中に望ましくない結果が生じる可能性があります。 この問題は、ブロックサイズが小さく、順次書き込みが行われる場合に発生する可能性があります。 この問題は解決されました。	4.1（3c）	4.1(3g)

の解決済みの問題 4.1(3g)

次の問題はリリース 4.1(3g) で解決済みです。

表 *20 : Firmware* アップグレード

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
CSCwa98283	サーバーの Intersight アップグレード中に、サーバーは正しいターゲットデバイスではなくホストアップグレードユーティリティで再起動します。 この問題は解決されました。	4.1（3c）	4.1(3g)

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
CSCwb21128	特定の条件下では、ハードドライブの遅延時間が長くなり、遅延の影響を受けやすいアプリケーションでの作業中に望ましくない結果が生じることがあります。 この問題は、小さなブロックサイズと順次書き込みで発生する可能性があります。 この問題は解決されました。	4.1（3c）	4.1(3g)

の解決済みの問題 4.1(3f)

次の問題はリリース 4.1(3f) で解決済みです。

表 *21 : 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
CSCvz29291	HTTP または HTTPS 経由で Cisco API を使用して Cisco UCS C シリーズサーバーに ISO をマウントしようとすると、失敗し、次のエラーメッセージが表示されます。 「ローカル デバイスのマウントに失敗しました（Local Device Mount Failed）」が表示されました。 この問題は解決されました。	4.1（3b）	4.1(3f)

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
CSCvz76449	Cisco UCS C シリーズ M5 サーバでは、Intersight を使用してサービスプロファイルを作成しているときに、2 つの RoCE vNics と 2 つの VMQ/VMMQ vNics を持つプロファイルを適用できない場合があります。次のエラーメッセージが表示されます。 アダプターに 2 つ以上の rdma プロファイルを構成することはできません この問題は解決されました。	4.1（3c）	4.1(3f)
CSCvz73890	Cisco UCS C シリーズ M5 サーバーは、Intersight のリストに表示されません。次のメッセージが表示されます。 現在の操作に失敗しました。CIMC が重大な操作を実行しているか、エラー状態になっている可能性があります。しばらくしてから再試行するか、必要に応じて CIMC を再起動します この問題は解決されました。	4.1(2b)	4.1(3f)

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
CSCvy78034	Redfish API は、誤った CPU スレッド数を表示します。 この問題は解決されました。	4.1（3b）	4.1(3f)
CSCvz77885	Cisco UCS C シリーズ M5 サーバーでは、ウォッチドッグサービスのリセットにより、Cisco IMC が予期せず再起動します。 この問題は解決されました。	4.1（3d）	4.1(3f)

表 *22 : BMC* ストレージ

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
CSCvy11359	Cisco UCS Manager と統合された Cisco UCS HX-M5 ラック サーバーには、SASS Expander のテクニカルサポート情報が含まれていません。 この問題は解決されました。	4.1（3d）	4.1(3f)

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
CSCvy74166	Cisco UCS C シリーズ M4 ラック サーバでは、HX Connect を介して暗号化を有効にした後、HX Connect はステータスを**部分的に暗号化**されていると表示しますが、Cisco UCS Manager と HX CLI は暗号化が期待どおりに有効化されます。 この問題は解決されました。	4.1(2b)	4.1(3f)

表 *23 : 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
CSCvz36957	Cisco UCS C シリーズ サーバーのサーバープロファイルに設定されているサーバー UUID は、サーバーインベントリ ページに表示されません。 この問題は解決されました。	4.1（3d）	4.1(3f)

表 *24 : Firmware* アップグレード

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
CSCvy75787	Emulex LPe32002 デュアル ポート 32G FC HBA を搭載した Cisco UCS C240 M5 サーバーでは、いずれかのリンクのリンク ステータスが**バイパス**状態になります。 この問題は解決されました。	4.1(2d)	4.1(3f)

表 *25 : FlexFlash*

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
CSCvz49944	Cisco UCS C125 M5 サーバーの電源を入れ直した後、SD カードを検出できず、起動デバイスに到達できないため起動できません。 この問題は解決されました。	4.1（3c）	4.1(3f)

表 *26 :* ホスト ファームウェア アップグレード

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
CSCvz95318	ポート 1 と 2 の構成が Qlogic カードで同一の場合、サーバーが再起動するたびにポート 1 が切断されます。 この問題は解決されました。	4.1（3c）	4.1(3f)

の解決済みの問題 4.1（3d）

次の問題はリリース 4.1（3d） で解決済みです。

表 *27 : 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
CSCvy50012	Cisco C220 M5 サーバーでは、IPv6アドレスを使用しているときに NTP サーバーを設定しているときに、Redfish API にエラーが表示されます。 この問題は解決されました。	4.1（3b）	4.1（3d）
CSCvy87338	Redfish Python ライブラリから **logout()** メソッドを使用して Redfish セッションを削除または終了すると、HTTP 応答コード 404 エラーで失敗します。 この問題は解決されました。	4.1（3c）	4.1（3d）

表 *28 : SNMP*

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
CSCvy51599	Cisco IMC バージョン 4.1(3b) 以降を実行している Cisco UCS C シリーズ M5 サーバーでは、より高い **Cr** 値を持つ **snmpbulkget** が Cisco IMC に対してトリガーされると、SNMP サービスが頻繁に再起動します。 この問題は解決されました。	4.1（3c）	4.1（3d）

の解決済みの問題 4.1（3c）

次の問題はリリース 4.1（3c） で解決済みです。

表 *29 : 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
CSCvw51939	Cisco IMC は、通常の操作中に Cisco UCS C シリーズ M5 サーバーで突然リセットされることがあります。 この問題は解決されました。	4.1(2b)	4.1（3c）
CSCvy26376	Cisco IMC メール アラートは Cisco UCS C シリーズ C220 M5 サーバーで失敗し、障害が生成されても電子メールは送信されません。 この問題は解決されました。	4.1（3b）	4.1（3c）

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
CSCvx65636	LDAP 認証をデバッグするための Cisco IMC CLI コマンドは、結果を表示しません。 この問題は解決されました。	4.1（3b）	4.1（3c）
CSCvw57963	Intersight ハードウェア互換性リストには、最新のサーバーのドライバー バージョン コンプライアンスの問題が誤って表示されます。 この問題は解決されました。	4.1(2b)	4.1（3c）

表 *30 : CMC*

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
CSCvw38535	Cisco UCS S3260 M5 サーバーでは、CMC でハートビートが失われたため、両方の SASEXP がリセットされます。 この問題は解決されました。	4.0(4f)	4.1（3c）

表 *31* : 外部 *PSU*

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
CSCvx04641	Cisco UCS M5 サーバーでは、サーバーが補助電源モード (サーバーの電源がオフ) で実行されているときに、PSUが予期しない高入力電力を BMC に報告します。BMC はこれをSELログで報告します。 この問題は解決されました。	4.0(1a)	4.1（3c）

表 *32* : ホスト ファームウェア アップグレード

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
CSCvu63139	Qlogic カードが FC LUNに接続されている場合、Cisco UCS C240 M5 スタンドアロンサーバーでは、起動中に HUU が応答しません。 この問題は解決されました。	4.0(1c)	4.1（3c）

表 *33 : SNMP*

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
CSCvx03201	Cisco UCS C240 M5 サーバーでは、1 つの PSU が取り外されると、SNMP がすべてのサーバーステータスに対して正しく表示されません。 この問題は解決されました。	4.0(4b)	4.1（3c）

表 *34 : XML API*

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
CSCvx42679	Cisco UCS C220 M5 サーバの XML API を使用して NTP LDAP でホスト名設定を設定しているときに、次のエラーが表示されます。 は、ユニオン タイプ emptyStringOrHostNameOrIPv4AddressOrIPv6Address の有効な値ではありません この問題は解決されました。	4.0(4m)	4.1（3c）

の解決済みの問題 4.1（3b）

次の問題はリリース 4.1（3b） で解決済みです。

表 *35 : 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
CSCvw43093	Cisco IMC の更新が長時間進行し、続行されない場合、NIHUU の更新は Cisco UCS C125 サーバーノードでタイムアウトします。 この問題は解決されました。	4.1（3b）	4.1（3b）
CSCvw49192	リリース 4.1(2b) にアップグレードした後、一部のシステム構成で電力特性評価を実行できず、POST エラーが発生する場合があります。**[PTU ドライバのロード（Loading PTU driv）]** 画面でシステムがフリーズします。CATERR も SEL に記録されます。 この問題は解決されました。	4.1(2b)	4.1(2f) および 4.1（3b）

表 *36 : 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
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) および 4.1（3b）
CSCvv97789	Cisco UCS M4 サーバーは、次の条件下で F8 ブート ユーティリティでデフォルトの管理者パスワードを受け入れることができません。 • サーバーがリリース 4.1(1c) または 4.1(2a) を実行している • サーバーは何らかの理由で工場出荷時のデフォルト設定にリセットされている このため、F8 構成ユーティリティは使用できません。 この問題は解決されました。	4.1(2a)	4.1（3b）

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
CSCvv08053	UCS Manager 接続モードの Cisco UCS C シリーズ M4 以前のモデル サーバー：同じ VLAN ID からインバンド モードで 2 つの IP アドレスが構成されている場合、ファブリック フェイルオーバー後に 1 つの IP アドレスのみが割り当てられます。 この問題は解決されました。	4.1(2a)	4.1（3b）
CSCvi46928	Cisco IMC は、Cisco UCS C480 サーバーで理由もなく再起動します。Cisco IMC ログには、エラーやメモリ不足の問題は表示されません。 この問題は解決されました。	3.1(2b)	4.1（3b）

表 *37 :* 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	Cisco UCS C240 M5 サーバーで自動インストールを使用して、リリース 4.0(2x) 以前のリリースからリリース 4.0(4b) またはそれ以降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。	4.0 (4d)	4.0(4l)、4.1(1g) および 4.1（3b）

未解決の不具合

リリースで未解決の問題 4.1（3c）

リリース 4.1（3c） では、次の問題が未解決です。

表 *38 :*

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvy51599	Cisco IMC バージョン 4.1（3b） 以降を実行している Cisco UCS C シリーズ M5 サーバでは、より高い **Cr** 値を持つ **snmpbulkget** が Cisco IMC に対してトリガーされると、SNMP サービスが頻繁に再起動します。	Cisco IMC を再起動します。	4.1（3b）

リリースで未解決の問題 4.1（3b）

リリース 4.1（3b） では、次の問題が未解決です。

表 *39 : BMC*

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvv10194	次の場合、Cisco IMC Web GUI にアクセスできません。 • Web ブラウザで TLS 1.3 通信が有効になっており、TLS 1.2 通信が無効になっています。 • Cisco IMC で**コモン クライテリア モード**が有効になっています。	Web ブラウザで TLS 1.2 通信を有効にします。	4.1（3b）

表 *40 :* 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
CSCvr49058	次の条件下では、Cisco UCS M5 サーバの POST 中に Intel x520 iSCSI LUN が検出されません。 • iSCSI ブートが Intel x520 アダプタで構成されている • Intel x520 アダプタがファームウェア バージョン 0x800008A4-1.817.3 以降を実行している ブートモードは UEFI に設定されています。	Intel x520 アダプターのファームウェアバージョンを 0x800008A4-1.812.1 にダウングレードします。	4.1（3b）

表 *41* : ホスト ファームウェア アップグレード

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvw68180	Cisco UCS S シリーズ サーバーでは、ISO マッピングエラーが原因で がリリース 4.1（3b） へのアップグレードに失敗します。これは、次のような状況で発生します。 • ISO マッピング共有が CIFS として構成されている • **mountOption** パラメータは、NIHUU 構成ファイルで指定されます。	次の回避策の 1 つを実行してください。 **1.** ISO マッピングには、NFS 共有を使用します。 **2.** ISO マッピングには、HTTP/HTTPS 共有を使用します。 **3.** ISO マッピングに **mountOption** パラメータを必要としない CIFS 共有を使用します。 **4.** XML API を使用して Cisco IMC ファームウェアを更新してアクティブ化します。 **5.** Cisco IMC Web GUI を使用して、Cisco IMC ファームウェアを更新してアクティブ化します。	4.1（3b）

既知の動作と制限事項

リリース での既知の動作と制限事項 4.1(3g)

次の警告は、リリース 4.1(3g) の既知の制限事項です。

表 *42 : BMC* ストレージ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCwc64817	Cisco IMC リリース 4.1(3g) を実行している Cisco UCS S3260 M5 サーバーの場合： Redfish API ユーザーインターフェイスは、**SimpleStorage** リソースの下のドライブリストに入力しません。	**ストレージ**リソースの下のリソースを使用します。 **SimpleStorage** リソースの下のリソースは非推奨です。	4.1(3g)

リリース での既知の動作と制限事項 4.1（3d）

リリース 4.1（3d） では、既知の制限事項として次の問題があります。

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
CSCvy34100	Cisco IMC リリース 4.1(3x) を実行し、VMedia マッピングを保存した Cisco UCS S3260 M4 サーバでは、次の問題が観察されます。 保存された VMedia マッピングは、Cisco IMC がリリース 4.1(2a) 以前にダウングレードされると表示されません。ユーザーは、Cisco IMC GUI を使用して新しい VMedia をマップできません。	Cisco IMC CLI を使用して、保存された VMEDIA マッピングをクリアするには、次の手順を実行します。 1. UCS# scope server *n* 2. UCS /server # scope vmedia 3. UCS /server/vmedia # delete-saved-mappings 4. 確認するには、**[yes]** と入力します。 クリアすると、VMedia マッピングはすべてのインターフェイス（GUI、CLI、および XML API）から期待どおりに機能します。	4.1（3c）

リリース での既知の動作と制限事項 4.1（3b）

リリース 4.1（3b） では、既知の制限事項として次の問題があります。

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
CSCvu62006	SLES 15.2 および Ubuntu 20.04 OS は、UEFI ブート エントリを使用して Cisco UCS C シリーズおよび S シリーズ M4 サーバに正常にインストールされます。ただし、再起動後に UEFI のデフォルト ブート エントリでブートすると非アクティブになります。	次の操作を行ってください。 **1.** BIOS セットアップに入り、管理者パスワードを作成します。 **2.** **[Advanced]** > **[Trusted Computing]** に移動し、TPM 1.2 または 2.0 UEFI バージョンの [TCG_2] を選択します。 **3.** F10 を押して、設定を保存し、終了します。	4.0(2m)

表 *45 : BMC*

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvu99928	FIPS が有効になっている場合、古い SSH クライアントは Cisco IMC への接続に失敗します。	SSH クライアント バージョンをアップグレードするか、Cisco IMC で FIPS を無効にします。	4.1（3b）

表 *46 :* 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
CSCvw22319	HGST NVME ドライブを使用した VMD は、Cisco UCS C480 M5 サーバーではサポートされていません	Cisco UCS C480 M5 サーバーで HGST ドライブが使用されている場合は、VMD を無効にします。	4.1（3b）

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvo39645	複数の同時リブート時に 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)
CSCvs30287	HGST NVMe ドライブを搭載した AMD EPYC 7352（ROME）プロセッサに基づく Cisco UCS C125 サーバーで、複数の重大な SEL イベントが観察されます。	サーバをリブートします。	4.1(2a)

表 47：オペレーティングシステム

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvu80469	Intel 710 シリーズアダプタとパススルー HBA コントローラを搭載した Cisco UCS サーバの SLES 12.5 OS に i40e ドライバをインストールした後、mpt3sas ドライバのインストールが失敗します。 次の警告メッセージが表示されます。 更新中/インストール中... 1:lsi-mpt3sas-kmp-default-30.00.01.# [100%]depmod: WARNING: //lib/modules/4.12.14-119-default/kernel/drivers/infiniband/hw/i40iw/i40iw.koシンボル i40e_unregister_client depmod のバージョンに同意しません 4.12.14-119-default is inconsistent 警告：弱い更新のシンボリックリンクが作成されない可能性があります	次のいずれかを実行します。 1. i40eドライバのアンインストール 2. インストールの順序の変更最初に mpt3sas ドライバをインストールし、次に i40e ドライバをインストールします。	4.1(2a)

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

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