Cisco UCS ラック サーバー ソフトウェア、リリース 4.2(2) のリリース ノート

初版：2022 年 7 月 8 日

最終更新：2023 年 1 月 10 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 (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 シリーズのソフトウェア リリース 4.2(2) 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 （47 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
C1	2023 年 1 月 10 日	**4.2（2g）内の解決済みの問題** のセクションを更新します。

改定	日付	説明
C0	2022 年 11 月 23 日	次のサーバーの 4.2（2g） のリリース ノートを作成しました。 Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー Cisco UCS C220 M5、C240 M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー 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 4.2
B2	2022 年 10 月 31 日	**「4.2（2f）リリース内の新しいハードウェア」**のセクションを更新しました。
A5	2022 年 10 月 31 日	**「4.2（2a）リリース内の新しいハードウェア」**のセクションを更新しました。
A4	2022 年 10 月 18 日	**「4.2（2a）リリース内の新しいソフトウェア機能」**のセクションを更新しました。
A3	2022 年 10 月 10 日	**「4.2（2a）リリース内の新しいハードウェア」**のセクションを更新しました。

改定	日付	説明
B0	2022 年 9 月 20 日	次のサーバーの 4.2(2f) のリリース ノートを作成しました。 Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー Cisco UCS C220 M5、C240 M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー 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 4.2
A2	2022 年 8 月 10 日	**既知の動作と制限事項**で CSCwc64817 を追加しました。
A1	2022 年 7 月 28 日	**リリース 4.2 へのアップグレード パス**を更新しました。
A0	2022 年 7 月 8 日	次のサーバーの 4.2 (2a) のリリース ノートを作成しました。 Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー Cisco UCS C220 M5、C240 M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー 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 4.2

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

このリリースでは、次のサーバがサポートされています。

- Cisco UCS C220 M6
- Cisco UCS C240 M6
- Cisco UCS C245 M6
- Cisco UCS C225 M6
- Cisco UCS C220 M5
- Cisco UCS C240 M5
- Cisco UCS C240 SD M5
- Cisco UCS C480 M5
- Cisco UCS S3260 M5
- Cisco UCS C480 M5
- Cisco UCS C480 M5 ML
- Cisco UCS C125 M5
- Cisco 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 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、ラックマウント サーバーを Cisco UCS Manager と統合すると、UCSM エンドユーザー インターフェイスを使用して、サーバーを管理します。

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 4.2(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
4.2（2g）	4.2(2d)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー Cisco UCS C220 M5、C240 M5、C240 SD M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー
4.2(2f)	4.2(2c)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー Cisco UCS C220 M5、C240 M5、C240 SD M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー
4.2 (2a)	4.2 (2a)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー Cisco UCS C220 M5、C240 M5、C240 SD M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー

表 *2 : Cisco IMC 4.2(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
4.2(1j)	4.2(1n)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー
4.2(1i)	4.2(1m)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー
4.2(1g)	サポートなし	Cisco UCS C225 M6、および C245 M6 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
4.2(1f)	4.2(1k)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー
4.2(1e)	4.2(1i)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー
4.2(1c)	サポートなし	Cisco UCS C225 M6、および C245 M6 サーバー
4.2(1b)	4.2(1f)	Cisco UCS C220 M6、および C240 M6 サーバー
4.2（1a）	4.2(1d)	Cisco UCS C220 M6、C240 M6、および C245 M6 サーバー

表 *3 : Cisco IMC 4.2(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
4.2(1j)	4.2(1n)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー
4.2(1i)	4.2(1m)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー
4.2(1g)	サポートなし	Cisco UCS C225 M6、および C245 M6 サーバー
4.2(1f)	4.2(1k)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー
4.2(1e)	4.2(1i)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー
4.2(1c)	サポートなし	Cisco UCS C225 M6、および C245 M6 サーバー
4.2(1b)	4.2(1f)	Cisco UCS C220 M6、および C240 M6 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
4.2（1a）	4.2(1d)	Cisco UCS C220 M6、C240 M6、および C245 M6 サーバー

表 *4 : 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
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 *5 : 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
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 *6 : 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
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 *7 : 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

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(4k)	4.0(4h)	Cisco UCS C220 M5、C240 M5、および S3260 M5 サーバ
4.0(4j)	サポートなし	Cisco UCS S3260 M5 サーバ
4.0(4i)	4.0(4g)	Cisco UCS C220 M5、C240 M5、C480 M5 および S3260 M5 サーバ
4.0(4h)	4.0(4e)	Cisco UCS C220 M5、C240 M5、C480 M5 および S3260 M5 サーバ
4.0(4f)	4.0(4d)	Cisco UCS C220 M5、C240 M5、C480 M5、S3260 M5 および C480 ML M5 サーバ
4.0(4e)	4.0(4c)	Cisco UCS C220 M5、C240 M5、C480 M5、S3260 M5 および C480 ML M5 サーバ
4.0(4d)	サポートなし	Cisco UCS C220 M5、C240 M5、C480 M5 および S3260 M5 サーバ
4.0(4b)	4.0(4a)	Cisco UCS C220 M5、C240 M5、C480 M5、S3260 M5 および C480 ML M5 サーバ

表 *8 : 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 *9 : 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

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(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
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

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(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 *10 : 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
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 *11 : 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

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(3j)	サポートなし （注） Cisco UCS Manager で検出とアップグレードまたはダウングレード機能をサポートしています。	Cisco UCS C480 M5、C220 M5、C240 M5、および S3260 M5 サーバ
3.1(3i)	3.2(3i)	Cisco UCS C480 M5、C220 M5、C240 M5、および S3260 M5 サーバ
3.1(3h)	3.2(3h)	Cisco UCS C480 M5、C220 M5、C240 M5、および S3260 M5 サーバ
3.1(3g)	3.2(3g)	Cisco UCS C480 M5、C220 M5、C240 M5、および S3260 M5 サーバ
3.1(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 *12 : 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

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(2b)	3.2(2b)	Cisco UCS C480 M5、C220 M5、および C240 M5

表 *13 : 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 *14 : 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
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

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 (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
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 *15 : 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

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(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 *16 : 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 *17 : 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

Cisco IMC のリリース	UCS Manager のリリース	ラックマウント サーバ
2.0(13e)	3.1(2b)	C420 M3 を除くすべての M3/M4
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
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
1.5(9d)	2.2 (7b)	C420-M3、C260-M2、C460-M2 のみ
1.5(9d)	2.2 (8f)	C420-M3、C260-M2、C460-M2 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
1.5(8a)	2.2(6g)	C420 M3、C260 M2、C460 M2 のみ
2.0 (8d)	2.2(6c)	その他のすべての M3/M4
1.5(7f)	2.2(5b)	C420 M3、C260 M2、C460 M2 のみ
2.0(6d)	2.2(5a)	その他のすべての M3/M4
1.5(7a)2	2.2 (4b)	C420 M3、C260 M2、C460 M2 のみ
2.0 (4c)	2.2 (4b)	その他のすべての M3/M4
1.5(7c)1	2.2 (3b)	C420 M3、C260 M2、C460 M2 のみ
2.0 (3d) 1	2.2(3a)	その他のすべての 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 4.2(2) に次のブラウザを推奨しています。

推奨されるブラウザ	Browser Version	推奨されるオペレーティング システム
Microsoft Edge	95.0.1020.53（公式ビルド）（64 ビット）	Microsoft Windows 10 x64
	98.0.1108.50（公式ビルド）（64 ビット）	Microsoft Windows 10 x64
Google Chrome	96.0.4664.45	
	96.0.4664.45（公式ビルド）（64 ビット）	
	94.0.4606.71（公式ビルド）（64 ビット）	
Mozilla Firefox	94.0.2 ビルド ID：20211119140621	MAC Monterey v.12.0.1
	97.0.1	Microsoft Windows 10 x64
	78.9.0 ESR（64 ビット）	RHEL 8.4
Safari	14.1.2（16611.3.10.1.6）	MAC Monterey v.12.0.1
	15.1（17612.2.9.1.20）	

（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、「Cisco Optics-to-Device 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

デフォルトポート

次に示すのは、サーバ ポートとそのデフォルトのポート番号のリストです。

表 *18* : サーバ ポート

ポート名	ポート番号
LDAP Port 1	389
LDAP Port 2	389
LDAP Port 3	389
LDAP Port 4	3268
LDAP Port 5	3268
LDAP Port 6	3268
SSHポート	22
[HTTP ポート（HTTP Port）]	80
HTTPS ポート	443
SMTP ポート（SMTP Port）	25
KVM ポート	2068
Intersight 管理ポート	8889
Intersight クラウド ポート	8888
SOL SSH ポート	2400
SNMPポート	161
SNMP トラップ	162

ポート名	ポート番号
外部Syslog	514

リリース 4.2 へのパスのアップグレード

このセクションではリリース 4.2(x) へのアップグレード パスについて説明します。

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 *19 :* リリース *4.2(2x)* へのアップグレード パス

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
4.2 (2a)	• 4.2（2g） • 4.2(2f)	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 4.2 (2a) 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
4.2（1a） からのすべての Cisco UCS M6 サーバー	• 4.2（2g） • 4.2(2f) • 4.2 (2a)	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 4.2（1a） 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。
4.1(3) 以降の次の Cisco UCS サーバー: • Cisco UCS C220 M5 • Cisco UCS C240 M5 • Cisco UCS C240 SD M5 • Cisco UCS C480 M5 • Cisco UCS C480 M5 ML • Cisco UCS S3260 M5 • Cisco UCS C125 M5 • Cisco UCS S3260 M4	• 4.2(2f) • 4.2 (2a)	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。 • NIHUU ツールを使用してファームウェアを更新する際には、バージョン 4.1(3) 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
4.1(2) 以降の次の Cisco UCS サーバー: • Cisco UCS C220 M5 • Cisco UCS C240 M5 • Cisco UCS C240 SD M5 • Cisco UCS C480 M5 • Cisco UCS C480 M5 ML • Cisco UCS S3260 M5 • Cisco UCS C125 M5 • Cisco UCS S3260 M4	• 4.2(2f) • 4.2 (2a)	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更新する際には、バージョン 4.1(2) 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。
4.1(1) 以降の次の Cisco UCS サーバー: • Cisco UCS C220 M5 • Cisco UCS C240 M5 • Cisco UCS C480 M5 • Cisco UCS C480 M5 ML • Cisco UCS S3260 M5 • Cisco UCS C125 M5 • Cisco UCS S3260 M4	• 4.2(2f) • 4.2 (2a)	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更新する際には、バージョン 4.1(1) 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
4.0(4) 以降の次の Cisco UCS サーバー: • Cisco UCS C220 M5 • Cisco UCS C240 M5 • Cisco UCS C480 M5 • Cisco UCS C480 M5 ML • Cisco UCS S3260 M4	• 4.2(2f) • 4.2 (2a)	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 4.0(4) 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。

Cisco IMC 4.2（1a） リリースからのアップグレード オプションについては、表を参照してください。

表 *20 :* リリース *4.2(1a)* へのアップグレード パス

サーバー	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
Cisco UCS C220 M6	4.2（1a）	4.2(1b)、4.2(1e)、および 4.2(1f)
Cisco UCS C240 M6	4.2（1a）	4.2(1b)、4.2(1e)、および 4.2(1f)
Cisco UCS C245 M6	4.2（1a）	4.2(1g)、4.2(1c)、4.2(1e)、4.2(1f)、および 4.2(1g)
Cisco UCS C225 M6	4.2(1c)	4.2(1e)、4.2(1f)、および 4.2(1g)

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 4.2(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	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 4.2 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.4.2.2a.iso	ドライバ
Unified Computing System（UCS）ユーティリティ	ucs-cxxx-utils-efi.4.2.2a.iso ucs-cxxx-utils-linux.4.2.2a.iso ucs-cxxx-utils-vmware.4.2.2a.iso ucs-cxxx-utils-windows.4.2.2a.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、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 4.2 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
- ストレージ コントローラのファームウェア

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 **[更新とアクティブ化（Update & Activate）]**オプションを使用することをお勧めします。コンポーネントを強制的に更新するには、**アドバンス モード**を切り替えて必要なファームウェア コンポーネントを選択し、**[更新とアクティブ化（Update & Activate）]** をクリックします。ファームウェアを展開したら、**[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

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 4.2 での新しいソフトウェア機能

新しいソフトウェア機能: 4.2 (2a)

Release 4.2 (2a) での新しいソフトウェア機能

次の新しいソフトウェア機能がリリース 4.2 (2a) でサポートされています。

- Cisco UCS S3260 M5 サーバーの UCSC-9400-8E - Cisco 9400-8e 12G SAS HBA のサポート
- リリース 4.2 (2a) 以降、Cisco IMC は、Cisco UCS VIC 14xx または UCS VIC 15xxx シリーズ カードを搭載した Cisco UCS M5、S3260 M5、および M6 サーバで優先タグ付けまたは物理 NIC モードをサポートします。

  このオプションは、デフォルトで無効です。物理 NIC モードが有効になっている場合、VIC のアップリンク ポートはパススルー モードに設定されます。これにより、ホストは変更を行わずにパケットを送信できます。VIC ASIC は、vNIC の VLAN と CoS の設定に基づいてパケットの VLAN タグをリライトしません。

（注）

- 次のようなアダプタでは、このオプションを有効にすることはできません。
  - **[ポート チャネル モード (Port Channel mode)]** が有効になっています
  - **[VNTAG モード (VNTAG mode)]** が有効になっているもの
  - **[LLDP]** が有効になっているもの
  - **[FIP モード (FIP mode)]** が有効になっているもの
  - **[CISCO IMC 管理が有効 (Cisco IMC Management Enabled)]** 値が **[はい (Yes)]** に設定されています

  物理 NIC モードを有効にする前に、上記のオプションが無効になっていることを確認します。
- デフォルトの 2 つまたは 4 つの vNIC のみを使用する必要があります (アダプタのタイプによって異なります)。
- iSCSI またはその他のストレージ ネットワーク テクノロジはサポートされていません。
- 以下は、**物理 NIC モード**ではサポートされていません。
  - usNIC
  - Geneve オフロード
  - Cisco カード モード
- Cisco IMC から**物理 NIC モード**を無効にする場合は、他のすべての必要な機能を手動で有効にする必要があります。アダプタの vNIC 構成をデフォルト設定にリセットするために、**[デフォルトにリセット（Reset to Defaults）]** を選択します。

『Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide, Release 4.2』または『Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 4.2』を参照してください。

- リリース 4.2 (2a) 以降、Cisco IMC は TLS v1.2 の無効化と、v1.2 と v1.3 の両方の暗号値のカスタマイズをサポートしています。
- 4.2 (2a) リリース以降、Cisco IMC では、設定されたセキュア HTTP ブート デバイス用に最大 10 個の証明書をアップロードできます。構成された特定のブート デバイスの新しい証明書を削除してアップロードすることもできます。Cisco IMC では、最大 10 個のルート CA 証明書をアップロードできます。

- スタンドアロン サーバーおよびFI接続サーバーでのセキュアなSyslog—リリース4.2 (2a)以降、Cisco IMCでは、ユーザーがリモートSyslogサーバー（サーバーとして機能）へのセキュアな暗号化されたアウトバウンド接続を確立し、ロギングのセキュアな接続をサポートすることができます。

  『Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide, Release 4.2』または『Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 4.2』を参照してください。

- SAS/SATA ドライブ タイプのドライブ診断機能 — リリース 4.2 (2a) 以降、SATA ドライブでもドライブ診断セルフテストを実行できます。詳細については、『Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 4.2』を参照してください。

（注） この機能は、NVME JBOD ドライブをサポートしていません。サードパーティのツールを使用して、NVME JBOD ディスク エラーを診断できます。

- 4.2(2a) リリース以降、Cisco IMC は新しい HUU ユーザー インターフェイスをサポートします。詳細については、『Cisco Host Upgrade Utility User Guide, Release 4.2』を参照してください。
- **PCIe スロット CDN 制御**オプションを有効にするサポート。
- eMMC 機能の Redfish API サポートのサポート。
- Cisco UCS S3260 M4 および M5 サーバーの Redfish API のサポート。
- パーソナリティ構成のクリア—リリース 4.2 (2a) 以降、コマンドライン インターフェイスを使用してパーソナリティ構成をクリアできます。

  詳細については、『Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 4.2』を参照してください。
- **[ビデオ暗号化を有効にする（Enable Video Encryption）]** チェック ボックス オプションは廃止されました。
- ファームウェア バージョンを含む PCIe 接続デバイス データの読み取りのサポート。

リリース 4.2 の新しいハードウェア機能

リリース 4.2(2f) の新しいハードウェア

次のサポートが追加されました。

- Cisco UCS M5 と M6 サーバー用の Nvidia GPU-A100-80 GPU（UCSC-GPU-A100-80）。
- Cisco UCS C245 M6 および C240 M6 サーバー用の Nvidia GPU-A30 GPU（UCSC-GPU-A30）。

リリース 4.2 (2a) の新しいハードウェア

周辺機器（Peripherals）

次のサポートが追加されました。

- UCS-M2-HWRAID - Cisco UCS M6 サーバー上の Cisco M.2 ブート最適化 RAID コントローラは、シングル ドライブ構成とデュアル ドライブ構成の両方をサポートするようになりました。
- Cisco UCS M6 サーバーでの UCS VIC 15428 のサポート。

  SFP-10G-TX トランシーバーは、スタンバイ電源の場合、ポート 2 および 4 の VIC 15428 でサポートされます。サーバーの電源が完全にオンになると、SFP-10G-TX トランシーバーは 4 つのポートすべてで有効になります。15428 VIC カードと SFP-10G-TX でケーブル タイプを混在させる場合、ポート 1 および 3 はパッシブ銅ケーブル（10/25G）のみをサポートします。
- Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバーを搭載した Intel X710T4LG 4x10 GbE RJ45 PCIe NIC（カールスビル ASIC）。
- Qlogic QLE 2772 ファイバー チャネル アダプターと Cisco UCS C125 M5 サーバー。
- Qlogic QLE 2772 または QLE 2742 ファイバー チャネル アダプターと Cisco UCS S3260 サーバー。
- QLogic QLE2772 2x32GFC Gen 6 拡張 PCIe HBA)、Cisco UCS C225 M6 および C245 M6 サーバーを使用
- MLNX MCX623106AS-CDAT、2x100 GbE QSFP56 PCIe (非暗号化/TLS)、Cisco UCS C225 M6 および C245 M6 サーバー。
- UCSC-P-B7D32GF（Cisco-Emulex LPe35002-M2-2x32GFC Gen 7 PCIe HBA）

セキュリティ修正

リリース4.2(2f)でのセキュリティ修正

リリース 4.2(2f) では、次のセキュリティ修正が追加されました。

欠陥 ID - CSCwb67205

4Cisco UCS C-Series M6 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インテル CPU を搭載しています。

- **CVE-2022-0005** — SGX を搭載した一部のインテル® プロセッサーの JTAG インターフェイスを物理的にプローブすることによってアクセス可能な機密情報により、特権のないユーザーが物理アクセスを介して情報開示を可能にする可能性があります。
- **CVE-2022-21136** — 一部のインテル® Xeon® プロセッサー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。

- **CVE-2022-21151** — 一部のインテル® プロセッサーのプロセッサー最適化の削除またはセキュリティ クリティカルなコードの変更により、認証されたユーザーがローカル アクセスを介して情報開示を可能にする可能性があります。
- **CVE-2021-33060** — ユーザーは、インストールの修復が行われるディレクトリにアクセスできます。MS インストーラーでは通常のユーザーが修復を実行できるため、攻撃者はインストールの修復を開始し、特別に細工された EXE をチェック ポイント リモート アクセス クライアント権限で実行される修復フォルダーに置くことができます。
- **CVE-2022-21233** — レガシー xAPIC MMIO リージョンへの不正な読み取りの結果として、古いデータが返される可能性があります。この問題は、従来の xAPIC モードでのみ発生し、x2APIC モードには影響しません。これは、SGX エンクレーブ内の機密情報を公開するために使用できます。

リリース4.2 (2a)でのセキュリティ修正

リリース 4.2 (2a) 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 - CSCvw39931

Cisco UCS 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-2020-8690**— バージョン 7.3 より前のインテル(R) イーサネット 700 シリーズ コントローラーの保護メカニズムの障害により、特権ユーザーがローカルアクセスを介して特権の昇格またはサービス拒否を可能にする可能性があります。
- **CVE-2020-8691**— インテル(R) イーサネット 700 シリーズ コントローラーのファームウェアのロジックの問題により、特権ユーザーがローカルアクセスを介して特権の昇格またはサービス拒否を可能にする可能性があります。

- **CVE-2020-8691**—バージョン 7.3 より前のインテル(R) イーサネット 700 シリーズ コントローラーのファームウェアのアクセス制御が不十分なため、特権ユーザーがローカルアクセスを介して特権の昇格またはサービス拒否を可能にする可能性があります。
- 6**CVE-2020-8691**—インテル(R) イーサネット 700 シリーズ コントローラーのファームウェアの不適切なバッファ制限により、特権ユーザーがローカルアクセスを介して特権の昇格またはサービス拒否を可能にする可能性があります。

欠陥 ID - CSCvy53109

Cisco UCS C220 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-2019-20006**— ezXML 0.8.3 から 0.8.6 で問題が発見されました。関数 ezxml_char_content は、より大きなブロックの内部アドレスへのポインタを xml->txt として配置します。これは後で (free を使用して) 割り当てが解除され、セグメンテーション違反が発生します。
- **CVE-2021-26220** — ezxml 0.8.6 以前の ezxml_toxml 関数は、メモリ プールを使い果たした後に XML ファイルを開くときの OOB 書き込みに対して脆弱です。
- **CVE-2021-26221** — ezXML 0.8.6 以前の ezxml_new 関数は、メモリ プールを使い果たした後に XML ファイルを開くときの OOB 書き込みに対して脆弱です。
- **CVE-2021-26222** — ezXML 0.8.6 以前の ezxml_new 関数は、メモリ プールを使い果たした後に XML ファイルを開くときの OOB 書き込みに対して脆弱です。
- **CVE-2021-31598** —ezXML 0.8.6 の libezxml.a に問題が発見されました。関数 ezxml_decode() は、巧妙に細工された XML ファイルの解析中に不適切なメモリ処理を実行し、ヒープベースのバッファ オーバーフローを引き起こします。

欠陥 ID - CSCvz49944

電源の再投入後、ハイパーバイザに到達できないため、Cisco UCS C125 M5 サーバは SD カードから起動できません。

欠陥 ID - CSCvz49660

Cisco UCS 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** — SM2 暗号化データを暗号解読するために、アプリケーションは API 関数 `EVP_PKEY_decrypt()` を呼び出す必要があります。アプリケーションは、この関数を 2 回呼び出します。最初の開始時には、「out」パラメーターを NULL にすることができ、終了時には、暗号解読された平文を保持するために必要なバッファ サイズが「outlen」パラメーターに設定されます。その後、アプリケーションは十分なサイズのバッファを割り当て、`EVP_PKEY_decrypt()` を再度呼び出すことができます。ただし、今回は、「out」パラメータに NULL 以外の値を渡します。

  SM2 暗号解読コードの実装のバグは、`EVP_PKEY_decrypt()` への最初の呼び出しによって返されるプレーンテキストを保持するために必要なバッファ サイズの計算が、2 番目の呼び

出しによって必要とされる実際のサイズよりも小さくなる可能性があることを意味します。これにより、アプリケーションによって `EVP_PKEY_decrypt()` が小さすぎるバッファを使用して2回目に呼び出されたときに、バッファ オーバーフローが発生する可能性があります。

暗号解読のために SM2 コンテンツをアプリケーションに提示できる攻撃者は、攻撃者が選択したデータを最大 62 バイトまでバッファをオーバーフローさせ、バッファの後に保持されている他のデータの内容を変更する可能性があります。これにより、アプリケーションの動作が変化したり、アプリケーションがクラッシュする可能性もあります。バッファの場所はアプリケーションに依存しますが、ヒープに割り当てられます。OpenSSL 1.1.1l（影響を受ける 1.1.1-1.1.1k）で修正されました。

欠陥 ID - CSCvz83417

Cisco UCS 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-2019-20005 — ezXML 0.8.3 から 0.8.6 で問題が発見されました。巧妙に細工された XML ファイルの解析中に、関数 ezxml_decode が不適切なメモリ処理を実行し、`strchr()` の実行中に、「*\0*」文字（文字列の処理が終了した場所）の後のポインターから始まる、ヒープ ベースのバッファのオーバーリードにつながります。
- **CVE-2019-20006** — ezXML 0.8.3 から 0.8.6 で問題が発見されました。関数 `ezxml_char_content` は、大きなブロックの内部アドレスへのポインタを xml として txt に置きます。これは後で（free を使用して）割り当て解除され、セグメンテーション違反が発生します。
- **CVE-2019-20007** — ezXML 0.8.2 から 0.8.6 で問題が発見されました。巧妙に細工された XML ファイルの解析中に、関数 `ezxml_str2utf8` が `ezxml.c` で長さゼロの再割り当てを実行し、NULL ポインタを返します（一部のコンパイラ）。この後、関数 `ezxml_parse_str` は、`ezxml.c` 内の `s` 変数が NULL ではないかどうかをチェックしないため、NULL ポインターの逆参照とクラッシュ（セグメンテーション違反）が発生します。
- **CVE-2019-20198** — ezXML 0.8.3 から 0.8.6 で問題が発見されました。関数 `ezxml_ent_ok()` は再帰を誤って処理し、巧妙に細工されたXMLファイルのスタック消費につながります。
- **CVE-2019-20199** — ezXML 0.8.3 から 0.8.6 で問題が発見されました。巧妙に細工された XML ファイルの解析中に、関数 `ezxml_decode` が不正なメモリ処理を実行し、NULL ポインターで `strlen()` を実行しているときに NULL ポインターの逆参照を引き起こします。
- **CVE-2019-20200** —ezXML 0.8.3 から 0.8.6 で問題が発見されました。巧妙に細工された XML ファイルの解析中に、関数 `ezxml_decode` が誤ったメモリ処理を実行し、**行末の正規化**機能でヒープベースのバッファオーバーリードに導かれます。
- **CVE-2019-20201** — ezXML 0.8.3 から 0.8.6 で問題が発見されました。`ezxml_parse_*` 関数は XML エンティティを誤って処理し、メモリ割り当てが発生する無限ループにつながります。

- **CVE-2019-20202** — ezXML 0.8.3 から 0.8.6 で問題が発見されました。関数 `ezxml_char_content()` は、割り当てられていないブロックで realloc を使用し、無効な解放およびセグメンテーション違反を引き起こします。
- **CVE-2021-26220** — ezxml 0.8.6 以前の `ezxml_toxml` 関数は、メモリ プールを使い果たした後、XML ファイルを開く際の OOB 書き込みに対して脆弱です。
- **CVE-2021-26221** — ezXML 0.8.6 以前の `ezxml_new` 関数は、メモリ プールを使い果たした後、XML ファイルを開く際の OOB 書き込みに対して脆弱です。
- **CVE-2021-26222** — ezXML 0.8.6 以前の `ezxml_new` 関数は、メモリ プールを使い果たした後、XML ファイルを開く際の OOB 書き込みに対して脆弱です。
- **CVE-2021-30485** —ezXML 0.8.6 の libezxml.a に問題が発見されました。巧妙に細工された XML ファイルの解析中に、関数 `ezxml_internal_dtd()` が不正なメモリ処理を実行し、NULL ポインタで `strcmp()` を実行しているときに NULL ポインタの逆参照を引き起こします。
- **CVE-2021-31229** — ezXML 0.8.6 の libezxml.a に問題が発見されました。巧妙に細工された XML ファイルの解析中に、関数 `ezxml_internal_dtd()` が不適切なメモリ処理を実行し、1 バイト定数の境界外書き込みにつながります。
- **CVE-2021-31347** — ezXML 0.8.6 の libezxml.a に問題が発見されました。関数 `ezxml_parse_str()` は、巧妙に細工された XML ファイル（mmap によって作成されたメモリ領域の外部への書き込み）の解析中に、不正なメモリ処理を実行します。
- **CVE-2021-31348** —ezXML 0.8.6 の `libezxml.a` に問題が発見されました。巧妙に細工された XML ファイルを解析しているときに、関数 `ezxml_parse_str()` が不正なメモリ処理を実行します（特定の strcspn 障害後の境界外読み取り）。
- **CVE-2021-31598** —ezXML 0.8.6 の `libezxml.a` に問題が発見されました。巧妙に細工された XML ファイルの解析中に、関数 `ezxml_decode()` が不適切なメモリ処理を実行し、ヒープベースのバッファ オーバーフローを引き起こします。

欠陥 ID - CSCwb67158

Cisco UCS M4 サーバー（Cisco UCS C460 M4 を除く）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-2021-0153** — 一部のインテル(R) プロセッサの BIOS ファームウェアで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-2021-0154** — 一部のインテル(R) プロセッサの BIOS ファームウェアで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(R) 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-2021-0190** — 一部のインテル (R) プロセッサの BIOS ファームウェアのキャッチされない例外により、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場合があります。
- **CVE-2021-33123** — 一部のインテル (R) 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 (R) プロセッサの BIOS 認証コード モジュールで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昇格を有効にできる可能性があります。

欠陥 ID - CSCwb67157

Cisco UCS C460 M4 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-2021-0154** — 一部のインテル(R) プロセッサの BIOS ファームウェアで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(R) 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 (R) プロセッサの BIOS ファームウェアのキャッチされない例外により、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場合があります。
- **CVE-2021-33123** — 一部のインテル (R) 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 (R) プロセッサの BIOS 認証コード モジュールで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昇格を有効にできる可能性があります。

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。

解決済みの不具合 (p.11)

の解決済みの問題 4.2（2g）

リリース 4.2（2g） では、次の問題が解決されました。

表 *21 : 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
CSCwd18446	HX-PCIE-OFFLOAD-1 および UCS 4.2（1n） を搭載した Cisco UCS HX240-M6 サーバーは、インストーラの展開段階でさまざまな GUI エラーが機能不全になります。 この問題は解決されました。	4.2(1j)	4.2（2g）

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
CSCwd03250	Cisco UCS 4.2（2a）ファームウェアを搭載し、グローバルホットスペア/未構成良好として構成され、ドライブの自己テスト機能が有効になっているドライブを搭載した Cisco UCS サーバーでは、次の障害が表示される場合があります。 ローカル ディスク X が劣化しています。 この問題は解決されました。	4.2 (2a)	4.2（2g）

の解決済みの問題 4.2(2f)

リリース 4.2(2f) では、次の問題が解決されました。

表 *23 : 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
CSCvz47731	タイムゾーンが Cisco IMC サーバーで直接変更され、Intersight でサポートされていない場合、デフォルトのタイムゾーンは、Intersight のサーバープロファイルの詳細ビューの **[構成のばらつき]** に表示されます。 この問題は解決されました。	4.2(2f)	4.2(2f)

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
CSCwb46682	1 番目の SIOC の UCS VIC 1455 および 2 番目の SIOC の QLE2692 を備えた PCI SIOC を装備した Cisco UCS S3260 M5 サーバー（シングル IP モードで構成されたデュアル SIOC を備えた単一のサーバー）では、アクティブな CMC が再起動されると、Cisco IMC がスタンバイ SIOC にフェイルオーバーしません。 この問題は解決されました。	4.2(2f)	4.2(2f)

表 *24 : 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
CSCwc46398	VIC 14xx が搭載され、マルチキュー構成が有効になっている Cisco UCS サーバーでは、Cisco IMC UI に受信/送信/完了キュー カウントパラメータの誤った値が表示されます。 この問題は解決されました。	4.1(3f)	4.2(2f)

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
CSCwc06871	デフォルト設定および Cisco IMC で構成された Cisco UCS M5 サーバーは、SSH接続を許可します。これは、悪意のあるユーザーによって利用される可能性があります。 この問題は解決されました。	4.1(3f)	4.2(2f)
CSCwc47846	**RoCE プロパティ** セクションの**サービス クラス** フィールドの値は、Cisco IMC UI で更新されません。これは、Intersight サーバー プロファイルとポリシーを使用して、RDMA とマルチキューで構成された VIC カードを備えた Cisco UCS M5 サーバーで発生します。 この問題は解決されました。	4.1(3f)	4.2(2f)

表 *25 : 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
CSCvz61901	DIMM が Cisco IMC で失敗したと報告されると、オブジェクト識別子はステータスを**不明**と報告します。 この問題は解決されました。	4.1(1c)	4.2(2f)

表 *26* : 外部 *LSI SAS* 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
CSCwc18223	Cisco UCS C240 M6 サーバーでは、サーバーのリブート後に、1 つ以上の SED ドライブが**未構成の正常**としてマークされます。 この問題は解決されました。	4.2(1f)	4.2(2f)

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。

の未解決の問題4.2(2f)

次の障害はリリース 4.2(2f) で未解決です。

表 *27* : *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
CSCwc70846	Solidigm ADP RR ドライブを搭載した Cisco UCS サーバーは、IMM UI で間違ったドライブサイズ、プロトコル、およびドライブタイプを表示します。	既知の回避策はありません。 **モデル**フィールドまたは UCS PID から NVMe SSD サイズを見つけることができます。 ドライブのプロトコルとタイプは暗黙的です。	4.2(2f)

の未解決の問題4.2 (2a)

リリース 4.2 (2a) では、次の問題が未解決です。

表 *28 :* ハードウェア

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCwb92046	特定の高いクラスタ使用率の条件下で、ドライブはCisco UCS C240 M6 サーバーの I/O エラーを表示します。ドライブ障害の詳細は、ドライブ診断レポートには記録されません。	ホストをリブートし、ドライブ診断を実行します。	4.2 (2a)

表 *29 : BIOS*

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvz28553	スロット 4 に Cisco UCS VIC 1495 を搭載し、RHEL OS を実行している Cisco UCS C245 M6 サーバーでは、Cisco IMC からの**一貫したデバイス命名**（CDN）名が正しく報告されず、OS で異なって表示されます。	Cisco UCS VIC 1455 カードのライザー 1、スロット 1 を使用できます。	4.2(1c)
CSCwa26477	VLAN を有効にして Cisco IMC 構成ユーティリティを開くと、スタンドアロンから Cisco カード モードへの切り替え時に、最初の試行で警告メッセージが表示されます。 この問題は、VLAN 設定の選択の不一致が原因で発生します。	次の操作を行ってください。 1. 起動中に **F8**（Cisco IMC 設定ユーティリティ）を入力します。 2. **F10** を押して、設定を保存します。 警告メッセージは表示されません。	4.2 (2a)

表 *30 : BMC*

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCwb41346	Cisco UCS M5 サーバーと Cisco VIC 1385 カードを備えたセットアップでは、FcIfs 作成 XML クエリは、PCI オーダー 2 では無効な PCI オーダー エラー（0,1）、PCI オーダー 3 では（0,2）を表示します。この問題は、Cisco VIC 1385 に存在する 2 番目のデフォルト vNIC に対して PCI リンクを **0** として設定した場合にのみ発生します。	要求で 2 番目のアダプターの PCI リンクを送信しないでください。 変更のリクエストで指定された他のすべてのパラメータは、正常に変更されます。	4.1(2f)
CSCwb45042	MLOM スロットに Cisco UCS M6 サーバーと Cisco VIC 15xxx カードを搭載したセットアップでは、Cisco IMC SEL のエラー ログイベントが次のメッセージとともに記録されます。 `MLOM_FAN_SPEED`：ファンセンサー、回復不能イベント、低レベルの回復不能（`0 <= 0 RPM`）がアサートされました。	この Cisco IMC SEL エラー ログ イベントは無視できます。この障害は機能に影響を与えません。	4.2 (2a)

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 4.2 (2a)

リリース 4.2 (2a) では、既知の制限事項として次の問題があります。

表 *31 : 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 4.2 (2a) 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)

表 *32 : BMC*

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvy89810	Cisco UCS C245 M6 サーバでは、**NIC モード**が**共有 OCP 拡張**として設定されている場合、リリース 4.2（1a）にダウングレードした後に BMC にアクセスできなくなります。		4.2(1c)

不具合 ID	症状	回避策	最初に影響を受けるリリース
		Cisco IMC ネットワークを回復するには、次の手順を実行します。 **1.** ローカル モニターを VGA ポートに接続します。 **2.** 電源ボタンを使用してホストを再起動します。 **3.** 起動中に **F8**（Cisco IMC 設定ユーティリティ）を入力し、**Factory Defaults** オプションを選択します。 **4.** **F10** キーを押して保存します。 Cisco IMC が工場出荷時のデフォルト設定にリブートします。 サポートされているライザー スロットに VIC が装着されている場合、**NIC モード**は **Cisco カード** モードに切り替わります。VIC がない場合、**NIC モード**は**専用**モードに切り替わります。 ホストを再起動し、**F8** ユーティリティを入力してネットワーク設定を構成します。	

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvz75479	SMB 1.0 プロトコルを使用したファイルのマウントとアップロードは、すべての Cisco IMC インターフェイスで失敗します。	SMB 1.0 プロトコルを使用してファイルをアップロードまたはマウントするときに、手動で `vers=1.0` マウント オプションを追加します。	4.2 (2a)
CSCwb01860	Cisco UCS M6 サーバーでは、ストレージ ファームウェアのダウングレードが次のメッセージで失敗します。 失敗：フラッシュ イメージはサポートされていません この問題は、次の機能を備えた Cisco UCS M6 サーバーで発生します。 • PCIe ベンダー ID 1000h およびデバイス ID 10E2h のアダプター • ファームウェア：システム内の MR 7.20 以上、7.19 以下にダウングレード	ストレージ ファームウェア バージョン 7.20 を含む最新のパッチにアップグレードします。	4.2 (2a)

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCwb71501	Cisco UCS M6 サーバーの BIOS 設定では、**メモリ リフレッシュ レート**のデフォルト値は 2x リフレッシュ レートです。 ただし、BIOS は、128 および 256 DIMM の場合、**メモリ リフレッシュ レート**の値を 1x リフレッシュ レートに変更します。	既知の回避策はありません。	4.2 (2a)

制限事項

問題（Issue）

Cisco UCS C225 M6 または C245 M6 サーバーと Cisco VIC 15xxx カードを MLOM スロットに搭載し、25G ケーブルで接続したセットアップでは、次のオプションがデフォルト値で設定されていると、Cisco IMC にアクセスできなくなります。

- **Admin FEC モード**は **c191** に設定されています。

回避策

次の手順を実行して、**Admin FEC モード**を適切な値に設定し、Cisco IMC にアクセスします。

1. 電源ボタンを使用してホストを再起動します。
2. 起動中に **F8**（Cisco IMC 設定ユーティリティ）を入力します。

   NIC モードを**専用**モードに設定する
3. ホストを再起動し、Cisco IMC にログインします。
4. [ナビゲーション（Navigation）] ペインの [ネットワーク（Networking）] メニューをクリックします。
5. **[ネットワーキング (Networking)]** ペインで、表示するアダプタカードを選択します。
6. **[外部イーサネット インターフェイス]** リンクをクリックします。

   [外部イーサネット インターフェイス (External Ethernet Interfaces)] が別のタブで開きます。
7. **Admin FEC モード**を **c174** に設定します。

（注） この問題は、Cisco UCS C225 M6 または C245 M6 サーバの MLOM スロットに Cisco VIC 15xxx カードが含まれており、10G ケーブルで接続されている場合は発生しません。

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。

- 『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。