

# Cisco UCS ラック サーバー ソフトウェア、 リリース 4.2(3) のリリース ノート

---

初版 : 2023 年 1 月 6 日

最終更新 : 2023 年 3 月 20 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(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 \(32 ページ\)](#) 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
B0	2023年3月20日	<p>次のサーバーの 4.2(3d) のリリース ノートを作成しました。</p> <p>Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー</p> <p>Cisco UCS C220 M5、C240 M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー</p> <p>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。<a href="#">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</a></p>
A0	2023年1月6日	<p>次のサーバーの 4.2(3b) のリリース ノートを作成しました。</p> <p>Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー</p> <p>Cisco UCS C220 M5、C240 M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー</p> <p>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。<a href="#">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</a></p>

## 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 S3260 M5
- Cisco UCS C480 M5
- Cisco UCS C480 M5 ML
- Cisco UCS C125 M5
- Cisco UCS S3260 M4

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

CiscoUCSC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(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
4.2(3d)	4.2(3d)	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

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(3b)	4.2(3b)	<p>Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー</p> <p>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</p>

表 2: 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)	<p>Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー</p> <p>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</p>
4.2(2f)	4.2(2c)	<p>Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー</p> <p>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</p>
4.2 (2a)	4.2 (2a)	<p>Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー</p> <p>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</p>

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
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 4.2(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 5: 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

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 (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 6: 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(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

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(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 7: 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 8: 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



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(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
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 9: 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 10: 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
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

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(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 11 : 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 12: 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せん。	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 13: 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 14: 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 15: 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

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 (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
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 16: 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 17: 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せん。	C220 M4/C240 M4 のみ

表 18: 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せん。	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



Cisco IMC のリリース	UCS Manager のリリース	ラックマウント サーバ
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(3)に次のブラウザを推奨しています。

推奨されるブラウザ	推奨されるブラウザの最小バージョン	推奨される最小オペレーティング 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	Microsoft Windows 10 x64
	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](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中でテストされます。スイッチの後のストレージ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 19: 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

ポート名	ポート番号
HTTPS ポート	443
SMTP ポート (SMTP Port)	25
KVM ポート	2068
Andromeda Management ポート	8889
Andromeda 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
外部Syslog	514

## アップグレードとダウングレードのガイドライン

Cisco IMC で可能なすべてのアップグレードパスの完全な概要を取得するには、[Cisco UCS ラック サーバアップグレードサポートマトリックス](#)を参照してください。



- (注) リリース4.2(3d)からダウングレードする前に、ターゲット構成ごとの LUN を [1-1024] に変更してください。

## 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 20: リリース 4.2(3x)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(3b)	4.2(3d)	<p>以下のアップグレードパスに従ってください:</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• NIHHU 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(3b) でリリースされた Python スクリプトを使用します。</li> <li>• クライアント側で OpenSSL 1.0.1e-fips を使用します (NIHHU python スクリプトが実行中)</li> <li>• <a href="#">ここ</a> から HUU iso をダウンロードします。</li> <li>• <a href="#">ここ</a> から NIHHU をダウンロードします。</li> </ul>
<ul style="list-style-type: none"> <li>• Cisco UCS C220 M6</li> <li>• Cisco UCS C240 M6</li> <li>• Cisco UCS C245 M6</li> <li>• Cisco UCS C225 M6</li> <li>• Cisco UCS C220 M5</li> <li>• Cisco UCS C240 M5</li> <li>• Cisco UCS C240 SD M5</li> <li>• Cisco UCS C480 M5</li> <li>• Cisco UCS C480 M5 ML</li> <li>• Cisco UCS S3260 M5</li> <li>• Cisco UCS C125 M5</li> <li>• Cisco UCS S3260 M4</li> </ul>	<ul style="list-style-type: none"> <li>• 4.2(3d)</li> <li>• 4.2(3b)</li> </ul>	<p>以下のアップグレードパスに従ってください:</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• NIHHU 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 4.2(2) でリリースされた Python スクリプトを使用します。</li> <li>• クライアント側で OpenSSL 1.0.1e-fips を使用します (NIHHU python スクリプトが実行中)</li> <li>• <a href="#">ここ</a> から HUU iso をダウンロードします。</li> <li>• <a href="#">ここ</a> から NIHHU をダウンロードします。</li> </ul>

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
<p>4.2(1) からのすべての Cisco UCS M6 サーバー。</p> <p>サポートされているプラットフォームについては、<a href="#">表 21: リリース 4.2(1a) へのアップグレードパス (23 ページ)</a> を参照してください。</p>	<ul style="list-style-type: none"> <li>• 4.2(3d)</li> <li>• 4.2(3b)</li> </ul>	<p>以下のアップグレードパスに従ってください:</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• NIHHU 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 4.2(1) でリリースされた Python スクリプトを使用します。</li> <li>• クライアント側で OpenSSL 1.0.1e-fips を使用します (NIHHU python スクリプトが実行中)</li> <li>• <a href="#">ここ</a> から HUU iso をダウンロードします。</li> <li>• <a href="#">ここ</a> から NIHHU をダウンロードします。</li> </ul>
<p>4.1(3) 以降の次の Cisco UCS サーバー:</p> <ul style="list-style-type: none"> <li>• Cisco UCS C220 M5</li> <li>• Cisco UCS C240 M5</li> <li>• Cisco UCS C240 SD M5</li> <li>• Cisco UCS C480 M5</li> <li>• Cisco UCS C480 M5 ML</li> <li>• Cisco UCS S3260 M5</li> <li>• Cisco UCS C125 M5</li> <li>• Cisco UCS S3260 M4</li> </ul>	<ul style="list-style-type: none"> <li>• 4.2(3d)</li> <li>• 4.2(3b)</li> </ul>	<p>以下のアップグレードパスに従ってください:</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• NIHHU 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。</li> <li>• クライアント側で OpenSSL 1.0.1e-fips を使用します (NIHHU python スクリプトが実行中)</li> <li>• <a href="#">ここ</a> から HUU iso をダウンロードします。</li> <li>• <a href="#">ここ</a> から NIHHU をダウンロードします。</li> </ul>

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
<p>4.1(2) 以降の次の Cisco UCS サーバー:</p> <ul style="list-style-type: none"> <li>• Cisco UCS C220 M5</li> <li>• Cisco UCS C240 M5</li> <li>• Cisco UCS C240 SD M5</li> <li>• Cisco UCS C480 M5</li> <li>• Cisco UCS C480 M5 ML</li> <li>• Cisco UCS S3260 M5</li> <li>• Cisco UCS C125 M5</li> <li>• Cisco UCS S3260 M4</li> </ul>	<ul style="list-style-type: none"> <li>• 4.2(3d)</li> <li>• 4.2(3b)</li> </ul>	<p>以下のアップグレードパスに従ってください:</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• NIHHU 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。</li> <li>• クライアント側で OpenSSL 1.0.1e-fips を使用します (NIHHU python スクリプトが実行中)</li> <li>• <a href="#">ここ</a> から HUU iso をダウンロードします。</li> <li>• <a href="#">ここ</a> から NIHHU をダウンロードします。</li> </ul>
<p>4.1(1) 以降の次の Cisco UCS サーバー:</p> <ul style="list-style-type: none"> <li>• Cisco UCS C220 M5</li> <li>• Cisco UCS C240 M5</li> <li>• Cisco UCS C480 M5</li> <li>• Cisco UCS C480 M5 ML</li> <li>• Cisco UCS S3260 M5</li> <li>• Cisco UCS C125 M5</li> <li>• Cisco UCS S3260 M4</li> </ul>	<ul style="list-style-type: none"> <li>• 4.2(3d)</li> <li>• 4.2(3b)</li> </ul>	<p>以下のアップグレードパスに従ってください:</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• NIHHU 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。</li> <li>• クライアント側で OpenSSL 1.0.1e-fips を使用します (NIHHU python スクリプトが実行中)</li> <li>• <a href="#">ここ</a> から HUU iso をダウンロードします。</li> <li>• <a href="#">ここ</a> から NIHHU をダウンロードします。</li> </ul>

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: <ul style="list-style-type: none"> <li>• Cisco UCS C220 M5</li> <li>• Cisco UCS C240 M5</li> <li>• Cisco UCS C480 M5</li> <li>• Cisco UCS C480 M5 ML</li> <li>• Cisco UCS S3260 M4</li> </ul>	<ul style="list-style-type: none"> <li>• 4.2(3d)</li> <li>• 4.2(3b)</li> </ul>	以下のアップグレードパスに従ってください: <ul style="list-style-type: none"> <li>• 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。</li> <li>• NIHHU 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。</li> <li>• クライアント側で OpenSSL 1.0.1e-fips を使用します (NIHHU python スクリプトが実行中)</li> <li>• <a href="#">ここ</a> から HUU iso をダウンロードします。</li> <li>• <a href="#">ここ</a> から NIHHU をダウンロードします。</li> </ul>

表 21: リリース 4.2(1a) 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
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 C225 M6	4.2 (1a)	4.2(1c)、4.2(1e)、4.2(1f)、および 4.2(1g)
Cisco UCS C245 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(3) 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.4.2.3b.iso	ドライバ
Unified Computing System (UCS) ユーティリティ	ucs-cxxx-utils-efi.4.2.3b.iso ucs-cxxx-utils-linux.4.2.3b.iso ucs-cxxx-utils-vmware.4.2.3b.iso ucs-cxxx-utils-windows.4.2.3b.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](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>

## 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。

<https://cisco.github.io/cisco-mibs/>

## 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。

## リリース 4.2 の新しいハードウェア

### リリース 4.2(3d) 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。

- Cisco UCS M6 サーバーでの 1200W Artesyn および Lite-On 電源ユニットのサポート。

### リリース 4.2(3b) 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。

- Cisco UCS M6 サーバーでの UCS VIC 15238 のサポート。
- Solidigm (旧 Intel) P5520 および P5620 QLC 15TB

## リリース 4.2 での新しいソフトウェア機能

### リリース 4.2(3d) 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(3d) でサポートされています。

- データの無害化 - リリース4.2(3d)以降、Cisco IMC はデータの無害化機能をサポートしています。データサニタイズプロセスを使用して、Cisco IMC はすべての機密データを消去し、お客様データの抽出または回復を不可能にします。Cisco IMC が消去プロセスを進めると、ステータス レポートが更新されます。レポートから個々のデバイス消去のデータサニタイズプロセスのステータスと進行状況を確認し、必要に応じて問題を特定して修正することができます。

データサニタイズの消去プロセスは、サーバーコンポーネントで次の順序で実行されます。

- ストレージ
- VIC
- BIOS

- Cisco IMC

すべてのサーバー コンポーネントでデータ サニタイズを実行するか、データ サニタイズのために VIC およびストレージ コンポーネントのみを選択するかを選択できます。

データ サニタイズ プロセスが完了し、レポートを生成すると、Cisco IMC が再起動します。

詳細については、[Cisco UCS ラックマウント サーバー Cisco IMC リリース 4.2 XML API プログラマ ガイド](#)を参照します。



- (注)
- この機能は、Redfish API インターフェイスでのみサポートされています。
  - この機能は、Cisco UCS C シリーズ M5 と M6 サーバーでサポートされています。

- 13xx、14xx、15xxx VIC アダプタの Linux および ESX OS では、ターゲットあたりの最大 LUN が [1-1024] から [1-4096] に増加しました。

この変更は、vHBA タイプの FC イニシエータにのみ適用されます。ESX 7.x および ESX 8.0 は、ホストごとに合計 1024 個の LUN をサポートします。



- (注) リリース4.2(3d)からダウングレードする前に、ターゲット構成ごとの LUN を [1-1024] に変更してください。

## リリース 4.2 のセキュリティ修正

### リリース4.2(3d)でのセキュリティ修正

#### 欠陥識別子 - CSCwc73237

Cisco UCS C シリーズ M6 サーバーは、Intel® Whitley プロセッサ (アイス レイク) 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ト (CVE) ID によって特定された脆弱性の影響を受けます。

- **CVE-2022-21216**—一部の Intel® Atom および Intel Xeon スケーラブル プロセッサの帯域外管理におけるアクセス制御の粒度が不十分で、特権ユーザーが隣接ネットワークアクセスを介して特権のエスカレーションを可能にする可能性があります。
- **CVE-2022-33196** — Intel® Software Guard Extensions を使用している場合、一部の Intel® Xeon® プロセッサの一部のメモリ コントローラ構成で、特権を持つ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可能にする可能性のある不適切なデフォルトのアクセス許可。

- **CVE-2022-38090**— Intel® Software Guard Extensions を使用しているときに、一部の Intel® プロセッサで共有情報技術を不適切に分離すると、特権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-2022-33972**— 一部の第 3 世代 Intel® Xeon® スケーラブル プロセッサのマイクロコード キーイング メカニズムの不適切な計算により、特権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-2022-32231**— 一部の Intel® プロセッサの BIOS ファームウェアの不適切な初期化により、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-2021-0187**— 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-2022-26837**— 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、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-2022-36348**— バージョン SPS\_E5\_04.04.04.300.0 より前の一部のインテル® SPS ファームウェアの現用系デバッグ コードにより、認証されたユーザーがローカルアクセスを介して権限の昇格を可能にする可能性があります。

#### 欠陥識別子 - CSCwd61013

Cisco UCS C シリーズ M5 サーバーは、インテル® Purley 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) 識別子によって特定された脆弱性の影響を受けます。

- **CVE-2022-26343**— 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-2022-32231**— 一部の Intel® プロセッサの BIOS ファームウェアの不適切な初期化により、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

### リリースで解決済みの問題 4.2(3d)

リリース 4.2(3d) では、次の問題が解決されました。

表 22: 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
CSCwd90347	<p>NVMe ドライブをホットリムーブまたは挿入すると、Redfish PCI インベントリが更新されません。同じインベントリが他の Cisco IMC インターフェイス (GUI または CLI) で更新されます。</p> <p>この問題は解決されました。</p>	4.2(3b)	4.2(3d)
CSCwc12006	<p>Cisco UCS S3260 サーバーでは、シャーシ 2 の冗長性が低下し、自動クリアされると、Cisco UCS マネージャによって電源状態にエラーが生成されます。</p> <p>この問題は解決されました。</p>	4.0(4a)	4.2(3d)

表 23: ext-intel-cntrlr

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
CSCwd49108	<p>ファームウェアバージョンを 4.2 (1b) から 4.2 (2a) にアップデートした後、NIC カードがポートを検出しません。</p> <p>Intel は、4.2(2a) リリースの Intel E810-XXVDA2 ファームウェアから「FC-FEC」のサポートを削除しました。スイッチが 25G/s イーサネット接続に推奨される「RS-FEC」をサポートしていない場合、リンクダウンの問題が発生する可能性があります。</p> <p>この問題は解決されました。</p>	4.2(3b)	4.2(3d)

## リリースで解決済みの問題 4.2(3b)

リリース 4.2(3b) では、次の問題が解決されました。

表 24: 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
CSCwc44412	Solidigm (旧 Intel) P5520、P5620、および P5316 QLC ドライブのアクティビティ LED は、接続されていて、サーバーがアイドル状態のときは消灯しています。ドライブが動作しているのに、ドライブの LED が点滅しません。  この問題は解決されました。	4.2 (2a)	4.2(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 4.2(3b)

リリース 4.2(3b) では、既知の制限事項として次の問題があります。

表 25: 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
CSCwc64817	Cisco UCS S3260 M5 サーバーで、Redfish API ユーザーインターフェイスは、 <b>SimpleStorage</b> 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。  <b>SimpleStorage</b> リソースの下のリソースは非推奨です。	4.1(3g)
CSCwd15480	Cisco UCS S3260 M5 サーバーでは、SIOC1 または SIOC2 に VIC カードがない場合、ファームウェアの更新が失敗します。	SIOC1 または SIOC2 に適切な VIC カードを追加します。	4.2(2f)

## 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。