

# Cisco UCS ラック サーバソフトウェア、リリース 4.3(4) のリリース ノート

最終更新 : 2024 年 8 月 30 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 4.3(4) 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 \(31 ページ\)](#) 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	2024 年 6 月 25 日	次のサーバーの 4.3.4.241014 のリリース ノートを作成しました。 <ul style="list-style-type: none"><li>• Cisco UCS C245 M8 サーバ</li></ul>

改定	日付	説明
A0	2024年6月5日	<p>次のサーバーの4.3.4.240152のリリースノートを作成しました。</p> <ul style="list-style-type: none"> <li>• Cisco UCS C220 M7 および C240 M7 サーバー</li> <li>• Cisco UCS C220 M6、C240 M6、C225 M6 および C245 M6 サーバおよび S3260 M5 サーバ</li> </ul> <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4.3</a></p>

## Cisco IMC リリース番号と .ISO イメージ名

リリース 4.3 以降、シスコでは、.ISO イメージに合わせてリリース番号の命名規則を更新しています。

例：4.3.1.YYXXXX

- **4.3** — メイン リリースを表します。
- **.1** — 最初のリリースを表します。

現在の 4.3 メイン リリースの場合、**.1** は最初のリリース番号を表します。

後続のメンテナンス リリースでは、この番号は関連するメンテナンス リリース番号を表します。

- **YY** — リリース年を表します。

現在の 4.3 メイン リリースでは、**23** は 2023 年に由来します。

- **XXXX** — 最後の 4 桁は、毎年増加するビルド番号のシーケンスを表します。

最初の 4.3 メイン リリースの場合、番号は **0097** 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

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 C245 M8
- Cisco UCS C220 M7
- Cisco UCS C240 M7
- Cisco UCS C220 M6
- Cisco UCS C240 M6
- Cisco UCS C245 M6
- Cisco UCS C225 M6
- Cisco UCS S3260 M5

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 4.3(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
4.3.4.241014	4.3(4b)	Cisco UCS C245 M8 サーバ
4.3.4.240152	4.3(4a)	<ul style="list-style-type: none"> <li>• Cisco UCS C220 M7 および C240 M7 サーバー</li> <li>• Cisco UCS C220 M6、C240 M6、C225 M6 および C245 M6 サーバーおよび S3260 M5 サーバー</li> </ul>

表 2: Cisco IMC 4.3(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
4.3.3.240043	NA	<ul style="list-style-type: none"> <li>• Cisco UCS C220 M7 および C240 M7 サーバー</li> <li>• Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバー</li> </ul>
4.3.3.240041	NA	<ul style="list-style-type: none"> <li>• Cisco UCS S3260 M5 サーバ</li> </ul>
4.3.3.240022	4.3 (3a)	<ul style="list-style-type: none"> <li>• Cisco UCS C220 M7 および C240 M7 サーバー</li> <li>• Cisco UCS C220 M6、C240 M6、C225 M6 および C245 M6 サーバーおよび S3260 M5 サーバー</li> </ul>

表 3: Cisco IMC 4.3(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
4.3.2.xxxxx	NA	Cisco UCS C220 M5、C240 M5、C480 M5、C125 M5 および S3260 M5 サーバー
4.3.2.240053	NA	Cisco UCS C220 M5、C240 M5、C480 M5、C125 M5 および S3260 M5 サーバー
4.3.2.240037	NA	<ul style="list-style-type: none"> <li>• Cisco UCS C225 M6、および C245 M6 サーバー</li> </ul>
4.3.2.240009	NA	<ul style="list-style-type: none"> <li>• Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバー</li> <li>• Cisco UCS C220 M5、C240 M5、C480 M5、C125 M5 および S3260 M5 サーバー</li> </ul>

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウントサーバ
4.3.2.240002	4.3(2)	<ul style="list-style-type: none"> <li>• Cisco UCS C220 M7 および C240 M7 サーバー</li> <li>• Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバー</li> <li>• Cisco UCS C220 M5、C240 M5、C480 M5、C125 M5 および S3260 M5 サーバー</li> </ul>
4.3.2.230270	4.3(2)	<ul style="list-style-type: none"> <li>• Cisco UCS C220 M7 および C240 M7 サーバー</li> <li>• Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバー</li> <li>• Cisco UCS C220 M5、C240 M5、C480 M5、C125 M5 および S3260 M5 サーバー</li> </ul>
4.3.2.230207	4.3(2)	<ul style="list-style-type: none"> <li>• Cisco UCS C220 M7 および C240 M7 サーバー</li> <li>• Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバー</li> <li>• Cisco UCS C220 M5、C240 M5、C480 M5、C125 M5 および S3260 M5 サーバー</li> </ul>

表 4: Cisco IMC 4.3(1) 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
4.3.1.230138	サポートなし	Cisco UCS C220 M7 および C240 M7 サーバー
4.3.1.230124	サポートなし	Cisco UCS C220 M7 および C240 M7 サーバー
4.3.1.230097	サポートなし	Cisco UCS C220 M7 および C240 M7 サーバー

表 5: Cisco IMC 4.2(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
4.2(3l)	4.2(3k)	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(3k)	NA	Cisco UCS S3260 M5 サーバ
4.2(3j)	4.2(3j)	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(3i)	4.2(3i)	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(3g)	4.2(3g)	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(3e)	4.2(3e)	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(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
4.2(3b)	4.2(3b)	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 6 : 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

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(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 7: 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

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(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  (注) Cisco UCS Manager は、Cisco UCS C245 M6 サーバーをサポートしません。

表 8: 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(3n)	NA	Cisco UCS C220 M5、C240 M5、C480 M5 および S3260 M5 および S3260 M4 サーバー
4.1(3m)	4.1(3m)	Cisco UCS C220 M5、C240 M5、C480 M5 および S3260 M5 および S3260 M4 サーバー
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

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 (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 9: 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(2m)	サポートなし	Cisco UCS C220 M4、C240 M4、および C460 M4 サーバー。
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

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(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 10: 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

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(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

## 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。

Cisco では、Cisco UCS ラック サーバ ソフトウェア、リリース 4.3(4) 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
Google Chrome	バージョン 122.0.6261.129 (公式ビルド) (x86_64)	Mac OS 14.2.1 (23C71)
	バージョン 122.0.6261.131 (公式ビルド) (64 ビット)	Microsoft Windows 11 Enterprise
	バージョン 123.0.6312.59 (公式ビルド) (64 ビット)	Microsoft Windows 11 Enterprise
	バージョン 123.0.6312.58 (公式ビルド) (64 ビット)	Microsoft Windows 11 Enterprise
Safari	バージョン 17.2.1 (19617.1.17.11.12)	Mac OS 14.2.1 (23C71)
Mozilla Firefox	123.0.1	Microsoft Windows 11 Enterprise
	124.0.1 (64 ビット)	
	24.0.1	



(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

## 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 11: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
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。

リリース 4.3.4.240152 のダウングレードに関する制限事項：

サーバのアップグレードパスを確認するには、『[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。

リリース 4.3.3.240022 のダウングレードに関する制限事項：

リリース 4.3.3.240022では、第 5 世代 Intel® Xeon® プロセッサを搭載した Cisco UCS M7 サーバーをダウングレードすることはできません。

Cisco IMC をダウングレードしようとする、CLI、GUI、Redfish API、および XML API のユーザー インターフェイスに次のエラーメッセージが表示されます。

**CLI/WEBUI/Redfish/XML = などの異なるインターフェイスを使用した BMC ダウングレード中のエラーメッセージ**

「アップデートは中止されました。INCOMPATIBLE\_IMAGE」

BIOS をダウングレードしようとする、CLI、GUI、Redfish API、および XML API のユーザー インターフェイスに次のエラーメッセージが表示されます。

アップロードされたイメージとプラットフォームの間で CPU ID が一致しません。



(注) 第 4 世代 Intel® Xeon® スケーラブルプロセッサを搭載した Cisco UCS M7 サーバをダウングレードできます。

リリース 4.3(2) へのインフラストラクチャのアップグレードおよびダウングレード:

- Cisco UCS M4 サーバーは、4.3.2.230207 以降のリリースではサポートされていません。
- システムに新しいハードウェア コンポーネントを追加した後に、ファームウェアの更新を実行する必要があります。
- サーバーに Cisco UCS VIC 15237 または 15427 をインストールする場合は、4.3.2.230270 以降のバージョンにサーバーをアップグレードしてから、アダプタをサーバーに挿入します。  
4.3.2.230270 よりも前のバージョンを実行しているサーバーに Cisco UCS VIC 15237 または 15427 を挿入する場合は、サーバーを 4.3.2.230270 以降のバージョンにアップグレードし、サーバーの電源を再投入してアダプタを認識させます。
- サーバーに Cisco UCS VIC 15235 または 15425 をインストールする場合は、サーバーを 4.3.2.230207 以降のバージョンにアップグレードしてから、アダプタをサーバーに挿入します。  
4.3.2.230207 よりも前のバージョンを実行しているサーバーに Cisco UCS VIC 15235 または 15425 を挿入する場合は、サーバーを 4.3.2.230207 以降のバージョンにアップグレードし、サーバーの電源を再投入してアダプタを認識させます。

#### Cisco UCS C245 M8 サーバのサポート

Cisco UCS C245 M8 サーバは、リリース 4.3.4.241014 以降サポートされています。

#### Cisco UCS M7 サーバーのサポート

Cisco UCS M7 サーバーは、リリース 4.3.1.230097 以降サポートされています。

次のリリースは、Cisco UCS M7 サーバー専用です。

- 4.3.1.230138
- 4.3.1.230124
- 4.3.1.230097

## リリース 4.3.4 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 4.3.4(x) へのアップグレードパスについて説明します。

Cisco IMC 4.3.4.241014 リリースは、Cisco UCS C245 M8 サーバのみをサポートします。

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 12: リリース 4.3(4x) 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 4.3.1.230097 以降の次の Cisco UCS サーバー <ul style="list-style-type: none"> <li>• Cisco UCS C220 M7</li> <li>• Cisco UCS C240 M7</li> </ul>	<ul style="list-style-type: none"> <li>• 4.3.4.240152</li> <li>• 4.3.3.240043</li> <li>• 4.3.3.240022</li> <li>• 4.3.2.240002</li> <li>• 4.3.2.230270</li> <li>• 4.3.2.230207</li> <li>• 4.3.1.230138</li> <li>• 4.3.1.230124</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 (NIHUU) スクリプトを使用できます。</li> <li>• 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 4.3.4.240152 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 (NIHUU 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 NIHUU 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
リリース 4.2(3b) 以降の Cisco UCS サーバー <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> </ul>	<ul style="list-style-type: none"> <li>• 4.3.4.240152</li> <li>• 4.3.3.240043</li> <li>• 4.3.3.240022</li> <li>• 4.3.2.230270</li> <li>• 4.3.2.230207</li> <li>• 4.2(3g)</li> <li>• 4.2(3e)</li> <li>• 4.2(3d)</li> </ul> (注) Cisco UCS M5 サーバの場合、次のリリースは Cisco UCS S3260 M5 サーバのみをサポートします。 4.3.3.240022	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 4.3.2.230207 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 4.2(2) 以降の 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 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> </ul>	<ul style="list-style-type: none"> <li>• 4.3.2.240002</li> <li>• 4.3.2.230270</li> <li>• 4.3.2.230207</li> <li>• 4.2(3g)</li> <li>• 4.2(3e)</li> <li>• 4.2(3d)</li> <li>• 4.2(3b)</li> </ul> (注) Cisco UCS M5 サーバの場合、次のリリースは Cisco UCS S3260 M5 サーバのみをサポートします。 4.3.4.240152 4.3.3.240022	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、表 13: リリース 4.2(1a) へのアップグレードパス (20 ページ) を参照してください。</p>	<ul style="list-style-type: none"> <li>• 4.3.4.240152</li> <li>• 4.3.3.240043</li> <li>• 4.3.3.240022</li> <li>• 4.3.2.240002</li> <li>• 4.3.2.230270</li> <li>• 4.3.2.230207</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> </ul>	<ul style="list-style-type: none"> <li>• 4.3.2.240002</li> <li>• 4.3.2.230270</li> <li>• 4.3.2.230207</li> <li>• 4.2(3g)</li> <li>• 4.2(3e)</li> <li>• 4.2(3d)</li> <li>• 4.2(3b)</li> </ul> <p>(注) Cisco UCS M5 サーバの場合、次のリリースは Cisco UCS S3260 M5 サーバのみをサポートします。</p> <p>4.3.4.240152 4.3.3.240022</p>	<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>• 4.3.2.240002</li> <li>• 4.3.2.230270</li> <li>• 4.3.2.230207</li> <li>• 4.2(3g)</li> <li>• 4.2(3e)</li> <li>• 4.2(3d)</li> <li>• 4.2(3b)</li> </ul> <p>(注) Cisco UCS M5 サーバの場合、次のリリースは Cisco UCS S3260 M5 サーバのみをサポートします。</p> <p>4.3.4.240152 4.3.3.240022</p>	<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> </ul>	<ul style="list-style-type: none"> <li>• 4.3.2.240002</li> <li>• 4.3.2.230270</li> <li>• 4.3.2.230207</li> <li>• 4.2(3g)</li> <li>• 4.2(3e)</li> <li>• 4.2(3d)</li> <li>• 4.2(3b)</li> </ul> <p>(注) Cisco UCS M5 サーバの場合、次のリリースは Cisco UCS S3260 M5 サーバのみをサポートします。</p> <p>4.3.4.240152 4.3.3.240022</p>	<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> </ul>	<ul style="list-style-type: none"> <li>• 4.3.2.240002</li> <li>• 4.3.2.230270</li> <li>• 4.3.2.230207</li> <li>• 4.2(3g)</li> <li>• 4.2(3e)</li> <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 (NIHUU) スクリプトを使用できます。</li> <li>• 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。</li> <li>• 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)</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 NIHUU をダウンロードします。</li> </ul>

表 13: 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	<ul style="list-style-type: none"> <li>• 4.3.3.240043</li> <li>• 4.3.3.240022</li> <li>• 4.3.2.240002</li> <li>• 4.3.2.230270</li> <li>• 4.3.2.230207</li> <li>• 4.2(3g)</li> <li>• 4.2(3e)</li> <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 (NIHUU) スクリプトを使用できます。</li> <li>• 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 4.2(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 (NIHUU 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 NIHUU をダウンロードします。</li> </ul>
Cisco UCS C240 M6		
Cisco UCS C225 M6		
Cisco UCS C245 M6		

## ファームウェア ファイル

### 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、 <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</a> 、 <a href="#">リリース 4.3</a> 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-drivers4.3.4.240152.iso	ドライバ

Unified Computing System (UCS) ユーティリティ	ucs-cxxx-utils-efi4.3.4.240152.iso	ユーティリティ
	ucs-cxxx-utils-linux4.3.4.240152.iso	
	ucs-cxxx-utils-vmware4.3.4.240152.iso	
	ucs-cxxx-utils-windows4.3.4.240152.iso	



- (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 4.3](#) 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
- Broadcom 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
- PCI Gen5 リタイマー

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>

## 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)
- 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 4.3.4 の新しいハードウェア

### リリース 4.3.4.241014 の新しいハードウェア

#### Cisco UCS C245 M8 サーバ

Cisco UCS C245 M8 サーバは、ビッグ データ分析、データベース、コラボレーション、仮想化、統合、AI/ML、および 2RU フォームファクタで最大 2 つの AMD<sup>®</sup> CPU をサポートするハイパフォーマンスコンピューティングなど、幅広いストレージおよび I/O 集約型のアプリケーションに最適です。

Cisco UCS C245 M8 サーバは、Cisco UCS サーバポートフォリオの機能を拡張します。AMD Infinity Guard などの高度な機能により、コンピューティング集約型アプリケーションのパフォーマンスが大幅に向上し、電力効率やコスト効率などのメリットが得られます。

Cisco UCS C245 M8 サーバは、UCS AMD<sup>®</sup> サーバラインに多くの新しい革新をもたらします。高速 I/O、DDR5 メモリバス、および拡張ストレージ機能用の PCIe Gen 5.0 拡張スロットの導入により、サーバはパフォーマンスと効率を大幅に向上させ、アプリケーションのパフォーマンスを大幅に向上させます。次の機能が含まれています。

- 最大 256 CPU コア（ソケットあたり 128 コア）を駆動するように設計されたサーバで、最大 2 つの第 4 世代 AMD EPYC<sup>™</sup> CPU をサポート
- 最大 24 枚の DDR5 DIMM スロット、256 GB DIMM を使用して最大 6 TB の容量（ソケットあたり 12 枚の DIMM を使用）
- 最大 4800 MT/秒の DDR5 メモリ
- 最大 8 個の PCIe Gen 4.0 スロットまたは最大 4 個の PCIe Gen 5.0 スロット、およびマザーボード上のハイブリッドモジュラー LAN（mLOM）/OCP 3.0 スロット
- Cisco UCS VIC 15000 シリーズ アダプタとサードパーティのホストの NIC オプションのサポート
- 最大 28 台のホットスワップ可能な小型フォームファクタ（SFF）SAS/SATA または NVMe ドライブ（最大 8 台の直接接続 NVMe ドライブ）および新規 tri-mode RAID コントローラは SAS4 プラス NVMe ハードウェア RAID をサポートします。
- M.2 起動用ドライブ（オプション）
  - ハードウェア RAID を備えた最大 2 台の 960GB SATA M.2 ドライブのサポート
  - NVMe ハードウェア RAID を備えた最大 2 台の 960GB NVMe M.2 ドライブ
- 最大 8 個の GPU をサポート
- モジュラ LOM / OCP 3.0
  - 背面パネルの追加接続用に、mLOM または OCP 3.0 カードを追加するために使用できる専用の PCIe 4 世代 x16 のスロット 1 個

- 10/25/50 Gbps のクワッドポートまたは 40/100/200 Gbps のデュアルネットワーク接続をサポートし、PCIe スロットを使用せずに、Cisco UCS 仮想インターフェイスカード (VIC) をスロットで搭載可能
- OCP 3.0 スロットは、一部のアダプターに対して、完全なアウトオブバンド管理を可能にします

## リリース 4.3.4.240152 の新しいハードウェア

リリース 4.3.4.240152 では、次の新しいハードウェアがサポートされています。

- 以下の RAID コントローラのサポート :
  - Cisco UCS C220 M7 および C240 M7 サーバを持つ Cisco ブート最適化 M.2 NVMe RAID コントローラ (UCS-M2-NVRAID)
 

このコントローラは、RAID0、RAID1、または JBOD (default - JBOD) モードのみ、および UEFI ブートモードのみサポートします。
  - Cisco UCS C220 M6、C240 M6、C220 M7、および C240 M7 サーバを持つ UCS-TPM-002D TPM モジュールをサポートします。
- 以下の GPU のサポート :
  - Intel<sup>®</sup> Data Center GPU Flex 140、HHHL、75W PCIe (Cisco UCS C220 M7 および C240 M7 サーバ搭載) のサポート
  - Intel<sup>®</sup> Data Center GPU Flex 170、FH-3/4L、150W PCIe (Cisco UCS C240 M7 サーバ搭載) のサポート
  - Cisco UCS C220 および C240 M6 サーバを搭載した NVIDIA<sup>®</sup> Hopper L4 70W、24GB、1-slot HHHH (UCSC-GPU-L4M6)
  - Cisco UCS C240 M7/M6 サーバの NVIDIA<sup>®</sup> 350W、40GB、2 スロット FHFL L40S GPU (UCSX-GPU-L40S)
  - Cisco UCS C240 M7/M6 サーバの NVIDIA<sup>®</sup> H100

## リリース 4.3.4 の新しいソフトウェア

### リリース 4.3.4.240152 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 4.3.4.240152 でサポートされています。

- 4.3.4.240152 リリース以降、Cisco は更新された UI とセキュリティ強化を備えた IMC の新しいバージョンをリリースしました。

新しい UI (ベータ版) には、より直感的なインターフェイス、合理化されたワークフロー、他の管理ツールとの統合の改善などの機能が含まれています。

- Cisco UCS C シリーズ サーバ上の Cisco UCS VIC 15000 シリーズ カードでの送信拡張モードをサポートしました。

送信拡張モードが有効になっている場合、Cisco IMC により、ファームウェアは 1000 ~ 1560 パケットサイズの IPv4 ネットワーク間で TCP 送信のトラフィック転送を最適化できます。

- リリース 4.3.4.240152 は、Thales® の新しい CipherTrust KMIP サーバを認定します。これは、段階的に廃止されている古い SafeNet および Vormetric サーバから引き継ぐように設定されています。新しい CipherTrust KMIP サーバは、使いやすさと拡張された機能セットを提供しますが、ユーザー エクスペリエンスは同じままです。Cisco IMC の新しい CipherTrust のサポートは、バージョン 4.3.4.240152 で開始されます。CipherTrust KMIP マネージャの構成プロセスの詳細については、Thales® が提供する CipherTrust Manager ユーザー ガイドを参照してください。
- 4.3.4.240152 リリース以降、Cisco IMC UI には、サードパーティ製アダプタに関する次の追加の詳細が表示されます。

表 14: サードパーティ製アダプタの情報

名前	説明
名前 (Name)	PCIe アダプタの名前。
ベンダー	PCIe アダプタのベンダー。
シリアル番号	PCIe アダプタのシリアル番号。
製品番号	PCIe アダプタの部品番号。
製造元	PCIe アダプタの製造元。
Firmware Version	PCIe アダプタの現在のファームウェア バージョン

表 15: ポートの詳細

名前	説明
[Port] カラム	アダプタへの外部接続に使用されるポート。
[Status] カラム	PCIe アダプタのステータス。これは、アップまたはダウンのいずれかです。
[リンク速度 (Link Speed)] カラム	PCIe スロットに装着されているアダプタカードの速度を表示します。
[WWPN] カラム	アダプタのワールドワイドポート名。
[ファクトリ WWPN (Factory WWPN)] 列	工場提供されるアダプタのワールドワイドポート名。

名前	説明
[WWNN] カラム	アダプタの世界ワイドノード名。
[ファクトリ WWNN (Factory WWNN) ]列	工場出荷時の設定からのアダプタの世界ワイドノード。

詳細については、『Cisco UCS C シリーズ統合管理コントローラ GUI 構成ガイド、リリース 4.3』または『Cisco UCS C シリーズサーバ統合管理コントローラ CLI 構成ガイド、リリース 4.3』を参照してください。

## 解決済みの不具合 (p.11)

### の解決済みの問題 4.3.4.240152

リリース 4.3.4.240152 では、次の問題が解決されました。

表 16: 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
CSCwj49647	<p>Cisco UCS サーバの Cisco IMC Web UI で障害のあるドライブの通知が表示される。</p> <p>いずれかのドライブでデータのサニタイズが失敗した場合は、ドライブの状態を確認します。</p> <p>ストレージドライブが障害状態の場合、障害は予期されています。</p> <p>場合によっては、ストレージドライブに中程度の障害が発生している可能性があります。これらのドライブでは、ドライブがホストに表示されている場合、データのサニタイズが成功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(3d)	4.3.4.240152

## 未解決の不具合

### リリースで未解決の問題 4.3.4.241014

リリース 4.3.4.241014 では、次の問題が未解決です。

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCwk12507	まれに、Cisco UCS C245 M8 サーバに接続されている Qlogic アダプタが、サーバのリブート後に期待どおりに列挙されないことがあります。	サーバの電源を再投入します。	4.3.4.241014

### リリースで未解決の問題 4.3.4.240152

リリース 4.3.4.240152 では、次の問題が未解決です。

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCwi60571	Cisco UCS M6 サーバでは、ポートのネットワーク速度は一部の Mellanox サードパーティ製アダプタでは使用できません。  Cisco IMC ユーザーインターフェイスでは、[ネットワークポート速度 (Network Port Speed)] フィールドに表示される値は <b>NA</b> です。	ホストオペレーティングシステムを使用して、ポートのネットワーク速度を確認できます。	4.3.4.240152

## 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 4.3.4.240152

#### 新しい Cisco IMC UI の制限事項

リリース 4.3.4.240152 以降、Cisco は、UI が更新され、セキュリティが強化された Cisco IMC の新しいバージョンをリリースしました。

次に、新しい Cisco IMC UI (ベータ版) の制限事項を示します。

- デバイス コネクタの構成ページは、新しい Cisco IMC UI では使用できません。
- ブラウザベースのローカルアップロードまたはダウンロードをサポートする機能は、新しい Cisco IMC UI では使用できません。

- 古い Cisco IMC UI と新しい Cisco IMC UI で最大 4 つのセッションが可能です。
- 他の Cisco IMC インターフェイスから新しい Cisco IMC UI のアクティブなセッションを終了することはできません。
- ログアウトされたセッションおよび非アクティブなタイムアウトセッションには影響しません。

#### 既知の動作と制限事項

リリース 4.3.4.240152 では、既知の制限事項として次の問題があります。

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCwi67637	<p>Cisco UCS M6 および M7 サーバでは、Cisco PID は表示されません。</p> <p>サードパーティ製アダプタの FRU 名が Cisco 製品名 (PID カタログ 製品名) と一致しません。</p>	<p>サードパーティ製アダプタを注文するには、『製品 ID カタログ』で入手可能な「Cisco PID/製品名の情報」を参照してください。</p> <p>Cisco IMC で PID カタログを表示して、サードパーティ製のアダプタまたはハードウェアコンポーネントの Cisco PID と製品名を確認できます。</p>	4.3.4.240152

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCwi73879	<p>次のフィールドは、サードパーティ製アダプタの Cisco IMC インターフェイスには表示されません。</p> <ul style="list-style-type: none"> <li>• アダプタの温度</li> <li>• ポートステータス</li> <li>• [FRU情報]</li> </ul>	<p>ホストアップグレードユーティリティ (HUU) を使用して、すべてのファームウェア コンポーネント (サードパーティ製アダプタファームウェアを含む) を最新のファームウェアに更新してアクティブ化し、MCTP を有効にします。</p> <p>HUU 更新後にサードパーティの管理機能が動作しない場合は、[更新の適用 (Force Update)] を実行し、サードパーティアダプタファームウェアのリストから特定のサードパーティアダプタコンポーネントを更新します。</p>	4.3.4.240152

## リリース 4.3.4 でのセキュリティ修正

### リリース 4.3.4.240152 でのセキュリティ修正

#### 障害 ID : CSCwi59840

Cisco IMC には、次の Common Vulnerabilities および Exposures (CVE) によって識別される脆弱性の影響を受けるサードパーティ ソフトウェアが含まれています。

- CVE-2023-48795 : 9.6 より前の OpenSSH およびその他の製品で見つかった特定の OpenSSH 拡張機能を備えた SSH トランスポートプロトコルにより、リモートの攻撃者は、一部のパケットが (拡張ネゴシエーションメッセージから) 省略されるなどの整合性チェックをバイパスできます。その結果、クライアントおよびサーバでは、一部のセキュリティ機能がダウングレードまたは無効化された接続 (Terrapin 攻撃とも呼ばれる) が発生する可能性があります。

これは、これらの拡張機能によって実装された SSH バイナリパケットプロトコル (BPP) が、ハンドシェイク フェーズとシーケンス番号の使用を誤って処理するために発生しま

す。たとえば、SSH による ChaCha20-Poly1305（および Encrypt-then-MAC を使用した CBC）の使用に対する効果的な攻撃がある場合、`chacha20-poli1305@openssh.com` でパスワードが発生します（CBC が使用されている場合は、`-etm@openssh.com` MAC アルゴリズム）。

## 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。