Cisco Intersight Server Firmware 4.2, 4.3(1)、5.0、および 5.1 のリリース ノート

初版：2023 年 9 月 29 日

最終更新：2024 年 2 月 22 日

Change in Firmware Version Schema New

- Post Infra Firmware release 4.2(3c):
  - The Server Firmware bundle in IIS will bear the version number in a n instead of the letter format.
  - B-Series Server Firmware version number will be in 5.x series
- With Infra Firmware release 4.3(2), the Infra Firmware bundle in IIS will be number in a new format instead of the letter format.

For example : 4.3(2.230117) , where 23 represents year, 0117 shows the incre number.

（注） 5.2(0.230040) リリースより前の IMM サーバー ファームウェア バンドルでは、X シリーズ BIOS イメージのメジャー バージョンは 5.0 および 5.1 でした

IMM サーバー ファームウェア 5.2(0.230040) 以降、IMM および UCSM BIOS イメージは共通で、4.3(2) から番号が付けられます。

結果として得られる IMM BIOS イメージのメジャー バージョン シーケンスは、5.0 -> 5.1 -> 4.3 -> のようになります。

概要

Cisco Intersight インフラストラクチャ サービス（IIS）には、物理および仮想インフラストラクチャの合理的な展開、モニタリング、管理、サポートのための機能が含まれます。IIS は Cisco

Unified Computing System™ (UCS) サーバーとサードパーティ製デバイスをサポートします。加えて、IIS は、インフラストラクチャの健全性とステータスをグローバルに可視化するとともに、以下の高度な管理およびサポート機能を提供します。

- 問題発生時に手動操作なしでテレメトリ データを分析できます。
- サービス リクエスト（SR）と返品許可（RMA）の処理を自動的に開始します。

IIS は、次の Cisco UCS サーバーを管理します。

- C シリーズ スタンドアロン サーバー
- UCSM 管理対象モード（UMM）B シリーズ、C シリーズ サーバー、および X シリーズ サーバー（FI 接続）
- Intersight 管理対象モード（IMM）B シリーズ、C シリーズ、および X シリーズ サーバー（FI 接続）

リリース ノートについて

このドキュメントには、以下のコンピューティング ノード コンポーネントに関する新機能、解決済みの問題、未解決の問題および回避策の詳細情報が記載されています

- アダプタ
- BIOS
- CIMC
- RAID コントローラ
- ディスク ファームウェア

このマニュアルには、次の内容も含まれています。

- マニュアルが初版発行された後に更新された情報。
- このリリースに関連付けられているブレード、ラック、モジュラ サーバやその他の Cisco Unified Computing System（UCS）コンポーネントに関連するファームウェアおよび BIOS

マニュアルの変更履歴

次の表は、このマニュアルのオンライン改訂履歴を示したものです。

改訂日	説明
2024 年 2 月 22 日	Cisco UCS C シリーズ サーバー ファームウェア、リリース 4.2(3j) のリリース ノートを作成しました。
2023 年 11 月 7 日	Cisco UCS C シリーズ サーバー ファームウェア、リリース 4.2(3i) のリリース ノートを作成しました。

改訂日	説明
2023 年 9 月 29 日	Cisco UCS C シリーズ サーバー ファームウェア、リリース 4.2(3h) のリリース ノートを作成しました。
2023 年 8 月 8 日	Cisco UCS C シリーズ サーバー ファームウェア、リリース 4.2(3g) のリリース ノートを作成しました。
2023 年 6 月 8 日	Cisco UCS X シリーズ サーバー ファームウェア、リリース 5.1(1.230052) のリリース ノートを作成しました。
2023 年 6 月 6 日	Cisco UCS C シリーズ M7 サーバー ファームウェア、リリース 4.3(1.230138) のリリース ノートを作成しました。
2023 年 4 月 12 日	Cisco UCS C シリーズ M7 サーバ ファームウェア、リリース 4.3（1.230124）のリリース ノートを作成しました。
2023 年 3 月 31 日	Cisco UCS X シリーズ M7 サーバ ファームウェア、リリース 5.1（0.230122）、Cisco UCS X シリーズ M6 サーバ ファームウェア、リリース 5.1（0.230075）、Cisco UCS B シリーズ M6 サーバ ファームウェア、リリース 5.1（0.230069）、Cisco UCS B シリーズ M5 サーバ ファームウェア、リリース 5.1（0.230073）のリリース ノートを作成しました。
2023 年 3 月 16 日	Cisco UCS X シリーズ M7 サーバ ファームウェア、リリース 5.1（0.230096）、Cisco UCS X シリーズ M6 サーバ ファームウェア、リリース 5.1（0.230054）、Cisco UCS C シリーズ サーバ ファームウェア、リリース 4.3（1.230097）、Cisco UCS B シリーズ M5 サーバ ファームウェア、リリース 5.1（0.230054）、および Cisco UCS B シリーズ M6 サーバ ファームウェア、リリース 5.1（0.230052）のリリース ノートを作成しました。
2023 年 1 月 10 日	Cisco UCS X シリーズ サーバ ファームウェア、リリース 5.0(4a) のリリース ノートを作成しました。
2022 年 11 月 29 日	Cisco UCS X シリーズ サーバー ファームウェア、リリース 5.0(2e) のリリース ノートを作成しました。
2022 年 9 月 20 日	Cisco UCS X シリーズ サーバー ファームウェア、リリース 5.0(2d) のリリース ノートを作成しました。
September 01, 2022	Cisco UCS X シリーズ サーバー ファームウェア、リリース 5.0(1f) のリリース ノートを作成しました。
2022 年 7 月 21 日	Cisco UCS X シリーズ サーバー ファームウェア、リリース 5.0(2b) のリリース ノートを作成しました。

改訂日	説明
2022 年 6 月 16 日	Cisco UCS X シリーズ サーバー ファームウェア、リリース 5.0(1e) のリリース ノートを作成しました。
2022 年 2 月 15 日	Cisco UCS X シリーズ サーバー ファームウェア、リリース 5.0(1c) のリリース ノートを作成しました。

このリリースの新機能

サーバー ファームウェア リリースの新しいハードウェア フィーチャ

リリース 4.2(3j) での新しいハードウェア サポート：なし

X シリーズ M7 ファームウェア 5.1 での新しいハードウェア サポート（0.230052）

Cisco UCS X410c M7 コンピューティングノード

Cisco UCS X410c M7 コンピューティング ノードは、初めての 4 ソケット第 4 世代Intel® Xeon® スケーラブル プロセッサ コンピューティング デバイスで、Cisco UCS X シリーズ モジュラ システムに統合されます。最大4つのコンピューティング ノード、または2つのコンピューティング ノードと 2 つの GPU ノードを 7 ラック ユニット（7RU）の Cisco UCS X9508 サーバー シャーシに配置でき、幅広いミッションクリティカルなエンタープライズアプリケーション、メモリ集中的なアプリケーションとベアメタルおよび仮想化されたワークロードに対する高い性能と有効性利得を提供します。

Cisco UCS X210c M7 の主な機能は次のとおりです。

- CPU：4 個の第 4 世代 Intel Xeon Scalable Processor（プロセッサあたり最大 60 個のコア）
- メモリ：64 個の 256 GB DDR5-4800 メモリ DIMM を備えた最大 16TB のメイン メモリ
- ストレージ：最大 6 個のホットプラグ対応ソリッド ステート ドライブ（SSD）、または非揮発性メモリ エクスプレス（NVMe）2.5 インチ ドライブ（エンタープライズ クラスの冗長アレイ（RAID）または最大 2 台の M.2 SATA ドライブ パススルー コントローラを選択可能）。
- mLOM 仮想インターフェイス カード：
  - Cisco UCS VIC 15420 は、サーバーのモジュール型 LAN on Motherboard（mLOM）スロットを占有でき、サーバーあたり 100 Gbps 接続に対して各シャーシのインテリジェント ファブリック モジュール（IFM）に最大 50 Gbps で接続できます。
  - Cisco UCS VIC 15231 は、サーバーのモジュール型 LAN on Motherboard（mLOM）スロットを占有でき、サーバーあたり 100 Gbps 接続に対して各シャーシのインテリジェント ファブリック モジュール（IFM）に最大 100 Gbps で接続できます。
- オプションのメザニン仮想インターフェイス カード：

- Cisco UCS 第 5 世代 VIC 15422 は、シャーシの下部にあるサーバーのメザニン スロットに装着できます。このカードの I/O コネクタは、Cisco UCS X ファブリック テクノロジーにリンクします。付属のブリッジ カードは、IFM コネクタを介してこの VIC の 2 倍の 50 Gbps のネットワーク接続を拡張し、合計帯域幅をファブリックあたり 100 Gbps（サーバあたり合計 200 Gbps）にします。
- Cisco UCS X-Fabric の Cisco UCS PCI Mezz カードは、シャーシの下部にあるサーバーのメザニン スロットに装着できます。このカードの I/O コネクタは Cisco UCS X-Fabric モジュールにリンクし、Cisco UCS X440p PCIe ノードへの接続を可能にします。
- すべての VIC メザニン カードは、X410c M7 計算ノードから X440p PCIe ノードへの I/O 接続も提供します。

- セキュリティ：サーバーは、オプションのトラステッド プラットフォーム モジュール（TPM）をサポートします。追加機能には、セキュア ブート FPGA および ACT2 偽造防止条項が含まれます。

（注） Cisco UCS X410c M7 コンピューティング ノードには、インフラストラクチャ ファームウェア バージョン 4.2(3e) 以降が必要です。

詳細については、Intersight 管理モードのサポート対象ハードウェアを参照してください。

X シリーズ ファームウェア 5.1 での新しいハードウェア サポート (0.230096)

次のサポートが追加されました。

- **Cisco UCS X210c M7 コンピューティング ノード**

  Cisco UCS X210c M7 コンピューティング ノードは、Cisco UCS X シリーズ モジュラ システムに統合された第 2 世代コンピューティング ノードです。7 ラック ユニット（7RU）Cisco UCS X9508 サーバ シャーシには、最大 8 個のコンピューティング ノードを配置でき、ラック ユニットあたりのコンピューティング、IO、およびストレージの密度は業界で最も高い 1 つです。

  Cisco UCS X210c M7 の主な機能は次のとおりです。

  - CPU：最大 2 基の第 4 世代 Intel® Xeon® スケーラブル プロセッサ（プロセッサあたり最大 60 コア、コアあたり 2.625 MB レベル 3 キャッシュおよび CPU あたり最大112.5 MB）
  - メモリ：32 個の 256 GB DDR5-4800 DIMM（最大 8 TB のメイン メモリ）。
  - ストレージ：最大 6 個のホットプラグ対応ソリッド ステート ドライブ（SSD）、または非揮発性メモリ エクスプレス（NVMe）2.5 インチ ドライブ（エンタープライズ クラスの独立したディスクの冗長アレイ（RAID）またはパススルー コントローラ（最大 2 台の M.2 SATA ドライブオプションのハードウェア RAID を装備）を選択可能。

- オプションの前面メザニン GPU モジュール：Cisco UCS 前面メザニン GPU モジュールは、最大 2 つの U.2 NVMe ドライブと 2 つの HHHL GPU をサポートするパッシブ PCIe Gen 4.0 前面メザニン オプションです。
- mLOM 仮想インターフェイスカード：Cisco UCS 仮想インターフェイスカード（VIC）15420 は、サーバのモジュラ LAN オンマザーボード（mLOM）スロットを占有でき、サーバあたり 100 Gbps 接続に対して各シャーシのインテリジェント ファブリック モジュール（IFM）に最大 50 Gbps で接続できます。

  Cisco UCS 仮想インターフェイスカード（VIC）15231 は、サーバーのモジュール型 LAN on Motherboard（mLOM）スロットを占有でき、サーバーあたり 100 Gbps 接続に対して各シャーシのインテリジェント ファブリック モジュール（IFM）に最大 100 Gbps で接続できます。
- オプションのメザニン カード：Cisco UCS 第 5 世代仮想インターフェイス カード（VIC）15422 は、シャーシの下部にあるサーバーのメザニン スロットに装着できます。このカードの I/O コネクタは、Cisco UCS X ファブリック テクノロジーにリンクします。付属のブリッジ カードは、IFM コネクタを介してこの VIC の 2 倍の 50 Gbps のネットワーク接続を拡張し、合計帯域幅をファブリックあたり 100 Gbps（サーバあたり合計 200 Gbps）にします。

  X-Fabric の Cisco UCS PCI Mezz カードは、シャーシの下部にあるサーバーのメザニン スロットに装着できます。このカードの I/O コネクタは Cisco UCS X-Fabric モジュールにリンクし、Cisco UCS X440p PCIe ノードへの接続を可能にします。

  すべての VIC メザニン カードは、X210c M7 計算ノードから X440p PCIe ノードへの I/O 接続も提供します。

- 次の Cisco UCS 15000 シリーズ VIC アダプタのサポート：
  - UCSX-ML-V5Q50G：Cisco UCS X210c-M7 コンピューティング ノード用の Cisco UCS VIC 15420 4x25G mLOM アダプタ
  - UCSX-ME-V5Q50G：Cisco UCS X210c-M7 コンピューティング ノード用の Cisco UCS VIC 15422 4x25G メザニン

（注） UCSX-210C-M7 コンピューティング ノードには、Cisco Intersight インフラストラクチャ ファームウェア バージョン 4.2(3b) 以降が必要です。

詳細については、Intersight 管理モードのサポート対象ハードウェアを参照してください。

X シリーズ ファームウェア 5.1 での新しいハードウェア サポート（0.230054）

次の Cisco UCS 15000 シリーズ VIC アダプタのサポート：

- UCSX-ML-V5Q50G：Cisco UCS X210c-M6 コンピューティング ノード用の Cisco UCS VIC 15420 4x25G mLOM アダプタ

- UCSX-ME-V5Q50G：Cisco UCS X210c-M6 コンピューティング ノード用の Cisco UCS VIC 15422 4x25G メザニン

詳細については、Intersight 管理モードのサポート対象ハードウェアを参照してください。

X シリーズ ファームウェア 5.0(4b) での新しいハードウェア サポート

Cisco UCS X210c M6 コンピューティング ノードでの次のカタログ サポート：

- KIOXIA PM7 1.9TB/3.8TB/7.6TB/15TB (1DWPD) SED
- Micron 5400 1DWPD SATA SSD 960GB/1.9TB/480GB
- Micron 5400 1DWPD 3.8TB and 7.6TB SSD SED
- Micron 5400 240GB, 480GB, 960GB M.2 SSD
- Micron 128GB,32GB DIMM

X シリーズ ファームウェア 5.0(2e) での新しいハードウェア サポート

Cisco UCS X210c M6 コンピューティング ノードを備えた UCSX-440P で次のグラフィック処理をサポートします。

- UCSX-GPU-A100-80

詳細については、Intersight 管理モードのサポート対象ハードウェアを参照してください。

X シリーズ ファームウェア 5.0(2d) での新しいハードウェア サポート

Cisco UCS X210c M6 コンピューティング ノードを備えた UCSX-440P で次のグラフィック処理をサポートします。

- UCSX-GPU-T4-16
- UCSX-GPU-A40
- UCSX-GPU-A16

詳細については、Intersight 管理モードのサポート対象ハードウェアを参照してください。

X シリーズ ファームウェア 5.0(2b) での新しいハードウェア サポート

次のサポートが追加されました。

- Cisco UCS X210c M6 コンピューティング ノード上の UCSX-ML-V5D200G モジュラ LAN on motherboard (mLOM) をサポートします。

（注） Cisco UCS VIC 15231（UCSX-ML-V5D200G）には、VIC ファームウェア 5.2(2) を含むインフラストラクチャ ファームウェア バージョン 4.2(2) 以降が必要です。

- Cisco UCSX-210C-M6 サーバーの Front Mezz（UCSX-X10C-GPUFM）のサポート。
- Cisco UCSX-210C-M6 サーバーの NVIDIA T4 GPU（UCSX-GPU-T4-MEZZ）のサポート。
- Cisco UCSX-440P PCIe ノードのサポート

詳細については、Intersight 管理モードのサポート対象ハードウェアを参照してください。

X シリーズ ファームウェア 5.0(1c) での新しいハードウェア サポート

Cisco UCS X210c M6 コンピューティング ノードでの次のカタログ サポート：

- UCS-SD76TBKNK9 （7.6TB 2.5 インチ Enterprise value 12G SAS SSD（1DWPD、SED- FIPS）
- UCS-SD480G63X-EP（480GB 2.5 インチ Enterprise Performance 6GSATA SSD）
- UCS-SD480G6I1X-EV（480GB 2.5 インチ Enterprise Value 6G SATA SSD）
- UCS-SD800GS3X-EP（800GB 2.5 インチ Enterprise Performance 12G SAS SSD）
- UCS-SD19TS1X-EV（1.9TB 2.5 インチ Enterprise Value 12G SAS SSD
- UCS-SD960G6S1X-EV（960GB 2.5 インチ Enterprise Value 6G SATA SSD）

X シリーズ ファームウェア 5.0(1b) での新しいハードウェア サポート

Cisco UCS X210c M6 コンピューティング ノード

Cisco UCS X210c M6 コンピューティング ノードは、Cisco UCS X シリーズ モジュラ システムに統合された最初のコンピューティング デバイスです。7 ラックユニット（7RU）Cisco UCS X9508 シャーシには、業界1といえる、最大8個のコンピューティングノードの配置、ラックユニットあたりのコンピューティング,I/O,およびストレージの密度。

Cisco UCS X210c M6 の主な機能は次のとおりです。

- CPU：最大 2 基の第 3 世代 Intel® Xeon®スケーラブルプロセッサ（プロセッサあたり最大 40 コア、コアあたり 1.5 MB レベル 3 キャッシュ）
- メモリ：最大 32 TB の 256 GB DDR4-3200 DIMM（最大 8 TB のメイン メモリ）。最大 16 個の 512 GB Intel Optane™ 永続メモリ DIMM を設定すると、最大 12 TB のメモリが得られます。
- ストレージ：最大 6 台のホットプラグ可能なソリッド ステート ドライブ（SSD）、または不揮発性メモリ エクスプレス（NVMe）2.5 インチ ドライブで、エンタープライズクラスの Redundant Array of Independent Disk（RAID）、または各レーンの PCIe Gen 4 接続と最大 2 台の M.2 SATA ドライブを搭載した 4 台のパススルー コントローラを選択可能。
- mLOM 仮想インターフェイスカード：Cisco UCS 仮想インターフェイスカード（VIC）14425 は、サーバのモジュラ LAN オンマザーボード（mLOM）スロットを占有でき、サーバあたり 100 Gbps 接続に対して各シャーシのインテリジェント ファブリック モジュール（IFM）に最大 50 Gbps で接続できます。

- オプションのメザニン仮想インターフェイス カード：Cisco UCS 仮想インターフェイス カード（VIC）14825 は、シャーシの下部にあるサーバのメザニン スロットを占有できます。このカードの I/Oコネクタは、将来の I/O 拡張のために計画されている Cisco UCS X-Fabric テクノロジーにリンクします。付属のブリッジカードは、IFM コネクタを介してこの VIC の 2 倍の 50 Gbps のネットワーク接続を拡張し、合計帯域幅をファブリックあたり 100 Gbps（サーバあたり合計 200 Gbps）にします。

（注） Cisco UCS 仮想インターフェイス カード（VIC）14425/14825 には、インフラストラクチャ ファームウェア バージョン 4.2(1) 以降が必要です

詳細については、Intersight 管理モードのサポート対象ハードウェアを参照してください。

C シリーズ ファームウェア 4.3（1.230097）での新しいハードウェア サポート

- Cisco UCS C220 M7 および C240 M7 サーバをサポートします。
- C シリーズ M7 サーバでの次のグラフィックス プロセッシング ユニットのサポート：
  - UCSC-GPU-A16
  - UCSC-GPU-A100-80

詳細については、Intersight 管理モードのサポート対象ハードウェアを参照してください。

C シリーズ ファームウェア 4.2(3b) の新規ハードウェア サポート

- Intersight 管理モードでの次のグラフィック処理ユニットのサポート：
  - Cisco UCS C シリーズ M6 サーバ上の UCSC-GPU-A16
  - Cisco UCS C シリーズ M5 および M6 サーバ上の UCSC-GPU-A100-80

詳細については、Intersight 管理モードのサポート対象ハードウェアを参照してください。

C シリーズ ファームウェア 4.2(2g) での新しいハードウェア サポート

- C シリーズ M5 サーバで次の Cisco UCS VIC 1300 シリーズ アダプタをサポートします。
  - UCSC-PCIE-C40Q-03
  - UCSC-MLOM-C40Q-03

（注） Cisco UCS VIC 1300 シリーズ アダプタには、VIC ファームウェア バージョン 4.5(2d) 以降が必要です。

- 次のカタログ サポート：

- Intel/Solidigm S4520、S4620、および S4520 M.2 SATA FW 7CV1CS02 C220、C240、C480 M5 サーバおよび C220、C240 M6 サーバ用。
- Samsung 256GB Octal ランク 3200 LRDIMM（IMM の C シリーズ M5 サーバ用）。

詳細については、Intersight 管理モードのサポート対象ハードウェアを参照してください。

C シリーズ ファームウェア 4.2(1j) の新規ハードウェア サポート

次のカタログ サポート：

- Micron 64GB RDIMM DRx4 3200 (16Gb) 1anm Z42B（Intersight 管理モードの C シリーズ M5 および M6 サーバ）。
- C220 および C240 M6 サーバ上の Seagate Evans BP 12TB および 18TB SAS 4k。
- C シリーズ M5 および M6 サーバ用の Hynix 128GB LRDIMM QRx4 3200（16Gb、DDP）1znm（C ダイ）。
- C220 および C240 M6 サーバ上の Micron 5300 1.9TB M.2 SSD
- C220 および C240 M6 サーバ上の WD Paris-D 20TB ドライブ
- Samsung PM893 EnterpriseValue SATA SFF 960GB、1.9T、3.8T、7.6T(1DWPD)(00AK1)、C220 および C240 M6 サーバ。

C シリーズ ファームウェア 4.2(1g) での新しいハードウェア サポート

次のカタログ サポート：

- C225 および C245 M6 サーバの A16 PID
- C220 および C240 M6 サーバ上の WD Leo-B He 14TB 4k SAS LFF（MID M6）
- C220 および C240 M6 サーバ上の WD Vela-AX 10TB 12G SAS 7.2K RPM LFF HDD（4K）（MID M6）
- C220 および C240 M6 サーバ上の東芝 MG07 14TB 12G SAS 4k ISE（MID M6）。
- Seagate Skybolt V6 NAND-1.8TB (4k) & 2.4TB (4k) SED-FIPS（C シリーズ M6 サーバ）
- Samsung PM893 EnterpriseValue SATA SFF 960GB、1.9T、3.8T、7.6T(1DWPD)(00AK1)、C220 および C240 M6 サーバ。

C シリーズ ファームウェア 4.2(1f) での新しいハードウェア サポート

次のカタログ サポート：

- Samsung 256GB Octal ランク 3200 LRDIMM（C245 M6 サーバ）
- C シリーズ M6 サーバ上の Micron 5200 1X 3.8TB
- C シリーズ M6 サーバ上の Micron 32GB RDIMM DRx4 3200 (8Gb) 1anm Z41C

- C シリーズ M6 サーバ上の Samsung 32GB RDIMM DRx4 3200 (8Gb) D1z および 16GB RDIMM SRx4 3200 (8Gb) D1y
- C シリーズ M6 サーバ上の Hynix 64GB RDIMM DRx4 3200 (16Gb) 1znm および 16GB RDIMM SRx4 3200 1ynm (8Gb)。

B シリーズ ファームウェア 4.2(2e) での新しいハードウェア サポート

- B シリーズ M5 サーバでの次の Cisco UCS VIC 1300 シリーズ アダプタのサポート。
  - UCSB-MLOM-40G-03
  - UCSB-VIC-M83-8P
  - UCSB-MLOM-PT-01

（注） Cisco UCS VIC 1300 シリーズ アダプタには、VIC ファームウェア バージョン 4.5(2d) 以降が必要です。

- 次のカタログ サポート：
  - Intersight 管理モードの B シリーズ M5 サーバ上の Coldstream 375G 新しいメディア タイプ用の FW E201CP07。
  - Solidigm S4520 YVRR SATA 240GB/960GB/3.8TB 用の FW 7CV1CS02 B シリーズ M5 および M6 サーバ。
  - Seagate Cooper - B シリーズ M5 および M6 サーバ上の 7.6TB（1DWPD）。

詳細については、Intersight 管理モードのサポート対象ハードウェアを参照してください。

UCSM と IMM 間のファームウェア バージョンの同等性

UCSM のファームウェア バージョン	IMM の Cisco UCS X シリーズ サーバーの同等のファームウェア バージョン
4.2(1)	5.0(1)
4.2(2)	5.0(2)
4.2(3)	5.0（4）
4.3(2)	5.2(0)
4.3(3)	5.2(1)

クロス バージョン ファームウェア サポート

ドメイン内の IMM サーバーファームウェアは、特定の IMM インフラストラクチャ ファームウェア バージョンでサポートされます。

次の表に、サポートされているサーバーファームウェアとインフラストラクチャ ファームウェアのバージョンを示します。

X シリーズ サーバー ファーム ウェア バージョン	インフラストラクチャ ファームウェア バージョン		
	4.2(1)	**4.2(2)**	**4.2(3)**
5.1(1)	いいえ	いいえ	はい
5.1(0)	いいえ	いいえ	はい
5.0（4）	はい	○	○
5.0(2)	はい	○	○
5.0(1)	はい	○	○

C シリーズ サーバー ファームウェア バージョン	インフラストラクチャ ファームウェア バージョン		
	4.2(1)	**4.2(2)**	**4.2(3)**
4.3(1)	いいえ	いいえ	はい
4.2(3)	はい	○	○
4.2(2)	はい	○	○
4.2(1)	はい	○	○
4.1(3)	はい	○	○

B シリーズ サーバー ファームウェア バージョン	インフラストラクチャ ファームウェア バージョン		
	4.2(1)	**4.2(2)**	**4.2(3)**
5.1(0)	いいえ	いいえ	はい
4.2(3)	はい	○	○
4.2(2)	はい	○	○
4.2(1)	はい	○	○
4.1(3)	はい	○	○

ファームウェアの更新

Cisco UCS ファームウェアを更新するには、Intersight 管理モードでのファームウェアの管理を参照してください。

セキュリティ修正

リリース 4.2(3j) のセキュリティ修正

次のセキュリティ上の問題が解決されます。

不具合 ID：**CSCwh58728**

Cisco UCS Manager 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-2023-38408：9.3p2 より前の OpenSSH の ssh-agent の PKCS#11 機能には、信頼できる検索パスが不十分であり、エージェントが攻撃者が制御するシステムに転送された場合にリモートでコードが実行される。（/usr/lib のコードは、ssh-agent にロードするのに必ずしも安全ではありません）。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

X シリーズ リリース 5.1（0.230054）のセキュリティ修正

次のセキュリティ上の問題が解決されます。

欠陥 ID：**CSCwd07517**

Cisco UCS M6 コンピューティング ノードには、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-2021-23017：DNS サーバからの UDP パケットを偽造できる攻撃者が 1 バイトのメモリを上書きして、ワーカープロセスのクラッシュやその他の潜在的な影響を引き起こす可能性のある nginx リゾルバーのセキュリティの問題。
- CVE-2021-3618 - TCP/IP レイヤーで犠牲者のトラフィックにアクセスできる MiTM 攻撃者は、トラフィックを 1 つのサブドメインから別のサブドメインにリダイレクトし、有効な TLS セッションを作成できます。

欠陥 ID：**CSCwd10018**

Cisco UCS M6 コンピューティング ノードには、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-2021-39537：v6.2-1 までの ncurses に問題が発見されました。captoinfo.c の _nc_captoinfo には、ヒープベースのバッファ オーバーフローがあります。
- CVE-2022-29458 - パッチ 20220416 より前の ncurses 6.3 には、terminfo ライブラリの tinfo/read_entry.c の convert_strings に境界外読み取りとセグメンテーション違反があります。

リリース 5.0(1f) でのセキュリティ修正

次のセキュリティ上の問題が解決されます。

欠陥 ID：**CSCwb67158**

Cisco UCS B シリーズ M4 ブレード サーバー（B260、B460を除く）および Cisco UCS C シリーズ M6 ラック サーバー（C460 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る Intel® プロセッサを搭載しています。

- CVE-2021-0153 — 一部の Intel® 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可能性があります。
- CVE-2021-0154 — 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-2021-0155 — 一部の Intel® 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Intel® 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エスカレーションを有効にできる可能性があります。
- CVE-2021-33123 — 一部の Intel® プロセッサの BIOS 認証コード モジュールの不適切なアクセス制御により、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる可能性があります。
- CVE-2021-33124 — 一部の Intel® プロセッサの BIOS 認証コード モジュールの境界外書き込みにより、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる場合があります。

欠陥 ID：**CSCwb67159**

Cisco UCS B シリーズ M5 ブレード サーバーおよび Cisco UCS C シリーズ M5 ラック サーバーは、次の一般的な脆弱性およびエクスポージャ（CVE）ID によって特定された脆弱性の影響を受ける Intel® プロセッサを搭載しています。

- CVE-2021-0189 — 一部の Intel®プロセッサの BIOS ファームウェアで範囲外のポインター オフセットを使用すると、特権ユーザーがローカル アクセスを介して特権のエスカレーションを有効にできる可能性があります。

- CVE-2021-0159 — 一部の Intel® プロセッサの BIOS 認証コード モジュールの不適切な入力検証により、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる可能性があります。
- CVE-2021-33123 — 一部の Intel® プロセッサの BIOS 認証コード モジュールの不適切なアクセス制御により、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる可能性があります。
- CVE-2021-33124 — 一部の Intel® プロセッサの BIOS 認証コード モジュールの境界外書き込みにより、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる場合があります。
- CVE-2022-21131 — 一部の Intel® Xeon® プロセッサの不適切なアクセス制御は認証されたユーザーに対しローカル アクセスを通じて情報開示を許可する可能性があります。
- CVE-2022-21136 — 一部の Intel® Xeon® プロセッサの不適切な入力検証により、特権ユーザーがローカル アクセスを介してサービス拒否を可能にする可能性があります。

欠陥 ID：CSCwb67157

Cisco UCS B260 M4 ブレード サーバー、Cisco UCS B460 M4 ブレード サーバー、および Cisco UCS C460 M4 ラック サーバーには、次の Common Vulnerability and Exposures（CVE）ID によって識別される脆弱性の影響を受ける Intel CPU が含まれています。

- CVE-2021-0154 — 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-2021-0155 — 一部の Intel® 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 Intel®プロセッサの BIOS ファームウェアで範囲外のポインターオフセットを使用すると、特権ユーザーがローカル アクセスを介して特権のエスカレーションを有効にできる可能性があります。
- CVE-2021-33123 — 一部の Intel® プロセッサの BIOS 認証コード モジュールの不適切なアクセス制御により、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる可能性があります。
- CVE-2021-33124 — 一部の Intel® プロセッサの BIOS 認証コード モジュールの境界外書き込みにより、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる場合があります。

欠陥 ID—CSCvy67497

Cisco UCS 6400 シリーズ FI 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-2018-14567 — lzma が libxml2 2.9.8 で使用されている場合、CVE-2015-8035 および CVE-2018-9251 とは異なる脆弱性である xmllint で実証されているように、リモートの攻撃者は、LZMA_MEMLIMIT_ERROR をトリガーする巧妙に細工された XML ファイルを介してサービス拒否 (無限ループ) を引き起こすことができます。
- CVE-2018-9251 — lzma が libxml2 2.9.8 の **xzlib.c** の **xz_decomp** 機能で使用されている場合、CVE-2015-8035 とは異なる脆弱性である xmllint で実証されているように、リモートの攻撃者は、LZMA_MEMLIMIT_ERROR をトリガーする巧妙に細工された XML ファイルを介してサービス拒否 (無限ループ) を引き起こすことができます。
- CVE-2021-3541 — libxml2 に欠陥が見つかりました。指数関数的なエンティティ拡張は、既存の保護メカニズムをすべてバイパスし、サービス拒否につながる可能性を攻撃します。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。

CSCwb59981

Cisco UCS M5 サーバーには、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-2021-22600 - net/packet/af_packet.c の packet_set_ring() の double free バグは、特権を昇格またはサービスを拒否するために巧妙に細工された syscall を介してローカル ユーザーによって悪用される可能性があります。影響を受けたバージョンより前のカーネルをアップグレードするか、過去の ec6af094ea28f0f2dda1a6a33b14cd57e36a9755 を再構築することをお勧めします。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。

CSCvm84140

Cisco UCS Manager は、セキュリティ ポスチャと復元力を強化するための新しいセキュア コードのベスト プラクティスで更新されています。

CSCvt82214

Cisco UCS 6400 シリーズ FI 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-2017-15906 - 7.6 より前の OpenSSH の sftp-server.c の process_open 関数は、読み取り専用モードでの書き込み操作を適切に防止しないため、攻撃者は長さゼロのファイルを作成できます。
- CVE-2018-15919 - 7.8 までの OpenSSH の auth-gss2.c のリモートで観察可能な動作は、リモートの攻撃者によって使用され、GSS2 が使用されているときにターゲット システム上のユーザーの存在を検出する可能性があります。

- CVE-2019-6111 - OpenSSH 7.9 で問題が発見されました。scp の実装は 1983 年の rcp から派生しているため、サーバーはクライアントに送信するファイル/ディレクトリを選択します。ただし、scp クライアントは、返されたオブジェクト名の大まかな検証のみを実行します（ディレクトリ トラバーサル攻撃のみが防止されます）。悪意のある scp サーバー（または中間者攻撃者）は、scp クライアントのターゲット ディレクトリ内の任意のファイルを上書きできます。再帰操作（-r）が実行されると、サーバーはサブディレクトリも操作できます（たとえば、.ssh/authorized_keys ファイルを上書きするなど）。

シスコはこれらの脆弱性に対処するソフトウェア アップデートを提供しています。

CSCvu63738

Cisco UCS 6400 シリーズ FI 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-2018-15473 - 7.7 までの OpenSSH は、auth2-hostbased の auth2-gss.c 、auth2-hostbased.c および auth2-pubkey.c に関連して、リクエストを含むパケットが完全に解析されるまで、無効な認証ユーザーの救済を遅らせないため、ユーザー列挙の脆弱性が発生する傾向があります。

- CVE-2018-15919 - 7.8 までの OpenSSH の auth-gss2.c のリモートで観察可能な動作は、リモートの攻撃者によって使用され、GSS2 が使用されているときにターゲット システム上のユーザーの存在を検出する可能性があります。

- CVE-2019-6111 - OpenSSH 7.9 で問題が発見されました。scp の実装は 1983 年の rcp から派生しているため、サーバーはクライアントに送信するファイル/ディレクトリを選択します。ただし、scp クライアントは、返されたオブジェクト名の大まかな検証のみを実行します（ディレクトリ トラバーサル攻撃のみが防止されます）。悪意のある scp サーバー（または中間者攻撃者）は、scp クライアントのターゲット ディレクトリ内の任意のファイルを上書きできます。再帰操作（-r）が実行されると、サーバーはサブディレクトリも操作できます（たとえば、.ssh/authorized_keys ファイルを上書きするなど）。

CSCwa65691

Cisco UCS 6400 シリーズ FI 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-2017-15906 - 7.6 より前の OpenSSH の sftp-server.c の process_open 関数は、読み取り専用モードでの書き込み操作を適切に防止しないため、攻撃者は長さゼロのファイルを作成できます。

- CVE-2018-15919 - 7.8 までの OpenSSH の auth-gss2.c のリモートで観察可能な動作は、リモートの攻撃者によって使用され、GSS2 が使用されているときにターゲット システム上のユーザーの存在を検出する可能性があります。

- CVE-2019-6111 - OpenSSH 7.9 で問題が発見されました。scp の実装は 1983 年の rcp から派生しているため、サーバーはクライアントに送信するファイル/ディレクトリを選択します。ただし、scp クライアントは、返されたオブジェクト名の大まかな検証のみを実行します（ディレクトリ トラバーサル攻撃のみが防止されます）。悪意のある scp サーバー

（または中間者攻撃者）は、scp クライアントのターゲット ディレクトリ内の任意のファイルを上書きできます。再帰操作（-r）が実行されると、サーバーはサブディレクトリも操作できます（たとえば、.ssh/authorized_keys ファイルを上書きするなど）。

不具合

このリリースで未解決のバグおよび解決済みのバグには、Cisco バグ検索ツール を使用してアクセスできます。この Web ベース ツールから、この製品やその他のシスコ ハードウェアおよびソフトウェア製品でのバグと脆弱性に関する最新情報を保守する Cisco バグ追跡システムにアクセスできます。

Cisco Bug Search Tool の詳細については、Bug Search Tool（BST）ヘルプおよび FAQ を参照してください。

解決済みの不具合

X シリーズ サーバー ファームウェアで解決された不具合

X シリーズ M7 および M6 ファームウェア リリース 4.2(3j) で解決された不具合

リリース 4.2(3j)では、次の警告が解決されています。

不具合 ID	症状	影響を受ける最初のバンドル
CSCwh04150	バージョン 4.2(2d) で実行されている UCSX-I-9108-25G を搭載した Cisco UCSX-210C コンピューティング ノードでは、「136.204」で終わる IP アドレス宛てのパケットがファブリック インターコネクト（FI）に到達できず、組み込みロジック アナライザ（ ELAM）。	4.2(2d)A
CSCwh67130	Cisco UCS 9108 25G IFM に接続された Cisco UCS X シリーズサーバーを搭載したセットアップで発生するアップストリーム ネットワーク通信の問題。	4.2(1i)A

X シリーズ M7 ファームウェア リリース 5.1 (0.230122) で解決された警告

次のテーブルでは、X シリーズ M7 ファームウェア リリース 5.1（0.230122）の解決された問題を一覧表示します。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwe52335	libcipmi SDR 情報へのアクセスに失敗しました。fcgi-workers0_core.2823 は、サーバのデコミッション/再コミッション時に生成されます。	5.1(0.230096)

不具合 ID	説明	影響を受ける最初のバンドル
CSCwe54136	HSU を実行すると、powercap 設定が断続的に失敗し、ホストの電源を入れ直し、上限を再同期する必要があります。	5.1(0.230096)
CSCwe54208	Inband2 を別の VLAN で再作成し、Inband1 を追加する前に削除する必要があります。	5.1(0.230096)
CSCwe50974	シャーシに十分なプロファイル バジェットが割り当てられていても、X210c M7 サーバはプロファイルを実行できませんでした。	5.1(0.230096)
CSCwe47118	Redfish monitor core が組み合わせストレス（Redfish stressを含む）中に発生しました。	5.1(0.230096)
CSCwe46276	M7 で OS を起動し、SOL が正常に機能していることを確認します。その後 BMC を再起動し、BMC が起動するまで待ちます。SOL が機能しない場合は、ホスト OS を再起動して回復する必要があります。	5.1(0.230096)
CSCwe65074	デバイス コネクタを 1.0.11.2759 に更新します。	5.1(0.230096)
CSCwe69788	BMC の再起動時にサーマル トリップが発生します。プロセッサ P1_THERMTRIP #0x53 |限界突破」	5.1(0.230096)
CSCwe36415	UpdateService/SoftwareInventory/HSU URL の下にタスク ID を表示しないでくださ い。/redfish/v1/UpdateService/SoftwareInventory/HSU URL は、「RelatedItem」パラメータに関連タスク ID を示します。場合によっては、工場出荷時の状態にリセットした後、またはタスクの数が最大値に達したときに、関連するタスク ID が削除される場合があります。このような場合に表示されるタスクIDを確認すると、そのタスクIDが存在しないため、「クリティカル」エラーが表示されます。スキーマ検証も失敗します。	5.1(0.230096)
CSCwe47304	デフォルト ゲートウェイは、Inband2 > Inband1 > OutbandB > OutbandA に続く優先順位に従って設定されません。	5.1(0.230096)

X シリーズ *M6* ファームウェア リリース *5.1*（*0.230075*）で解決された問題

次のテーブルでは、X シリーズ M6 ファームウェア リリース 5.1（0.230075）で解決された問題を一覧表示しています。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwe65074	デバイス コネクタを 1.0.11.2759 に更新します。	5.1(0.230054)

不具合 ID	説明	影響を受ける最初のバンドル
CSCwe54208	Inband2 を別の VLAN で再作成し、Inband1 を追加する前に削除する必要があります。	5.1(0.230054)
CSCwe47304	デフォルト ゲートウェイは、Inband2 > Inband1 > OutbandB > OutbandA に続く優先順位に従って設定されません。	5.1(0.230054)
CSCwe84278	UCSX-V4-Q25GME-RETIMER の適切なタイムアウト値を追加	5.1(0.230054)

X シリーズ ファームウェア リリース *5.1 (0.230054)* で解決された警告

次のテーブルでは、X シリーズ ファームウェア リリース 5.1（0.230054）の解決された問題を一覧表示します。

不具合 ID	説明	影響を受ける最初のバンドル
CSCvz93600	IPMI ツールとセンサー履歴ログに PCH および Q71 センサーを追加します。	5.0(4b)
CSCwc07335	jolt_util API または Redfish を介して USB 低電力が設定されている場合、値は KVM に伝達されません。	5.0(2e)
CSCwd04607	X シリーズ製品のインバンド サポート用に Redfish を有効にします。	5.0(4b)
CSCwd07888	アクセス ポリシーの展開中に、X210c コンピューティング ノードの 1 つでプロファイルの展開が失敗します。表示されたメッセージ：「更新中、リクエストが拒否されました」。	5.0 (2b)
CSCwd63892	X210c コンピューティング ノード ブレードは、リセットのたびに BIOS POST 中に 3 回ループします。	5.0(1b)
CSCwd68222	IPMI 暗号化キーに対して Redfish サポートを有効にできるように、API サポートを提供します。	5.0(4b)
CSCwe10891	デバイス コネクタを 1.0.11.2611 に更新します。	5.0(4b)

不具合 ID	説明	影響を受ける最初のバンドル
CSCwe25043	CIMC 5.1（0.230031）を実行している X210c M6 コンピューティング ノードで、有効な IMC アクセス ポリシーを使用してサーバ プロファイルを展開します。CIMC は、設定ファイル jolt_network.json および inband_intf の設定を保持します。古い CIMC 5.0(4a) をアクティブ化すると、Intersight はインバンド IP が構成されていることを示しますが、インバンド IP にアクセスできません。	5.0（4a）
CSCwd91329	ライザーを無効にした後、SMBus ダイレクト スパムを介して UCSX-440P PCIe ノードの GPU 温度を読み取ることができません。 GPU は、最初は UCSX-440P（X210c M6 コンピューティング ノードとペア）で完全に検出され、ホストの電源オフ/サイクルは、BIOS POST の完了後に直接（～5 秒以内に）実行されます。PciNodeUnknownPCieCardPresentOnRiser 障害が発生し（UnknownPCIeCardPresentOnRiser[1|2]）、最終的に Riser[1|2]PowerDisabled（次のホストの電源オフが検出された後）が発生し、最終的に BMC ENG syslog で IMM GraphicsCardTemperatureCritical 障害と I2C 温度スパムが発生します。	5.0(4b)

リリース *5.0(4b)* で解決された問題

次の表は、リリース 5.0(4b) で解決済みの不具合のリストです。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwd87584	すべての M6 サーバに Oracle Linux OS のサポートが追加されました。	5.0 (1c)
CSCwd88272	IPv の命名は、すべてのネットワーク ブートで共通である必要があります。	5.0 (1c)
CSCwe16597	Intel XL710-QDA2 デュアル ポート 40Gb アダプター ファームウェアを統合します。	5.0 (1c)
CSCwc48870	UCSX-V4-Q25GML および UCSX-ML-V5D200G アダプタの安全な消去機能を有効にします。	5.0 (1c)
CSCwd66132	ファームウェアが RDMA データなどの分類情報を収集できるようにすることで、UCSX-ML-V5D200G アダプタのテクニカル サポートの収集を改善します。	5.0 (1c)

リリース *5.0(4a)* で解決された問題

次の表は、リリース 5.0(4a) で解決済みの不具合のリストです。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwd73568	次のいずれかの条件の後、一時的な PciNodePower 障害が IMM の UCSX-440P PCIe ノードで発生する可能性があります。 • 5秒未満の短いシャーシの電源サイクル（この場合、ペアのコンピューティング ノードの BMC は、UCX-440P の HSC 障害を報告する可能性があります）。 • UCSX-210C-M6 コンピューティング ノードは、AC 電源の再投入（スロットのリセット）または物理的な取り外し/再挿入を行いますが、UCSX-440P PCIe ノードはペアのスロットにまだ取り付けられています。（この場合、ペアリングされたコンピューティング ノードの BMC は UCSX-440P の DCBrick 障害を報告する可能性があります）	5.0 (2b)
CSCwa04467	UCSX-210C-M6 コンピューティング ノードのボードコントローラは、UCD ファームウェアの更新と構成をサポートする必要があります。	5.0(2e)
CSCwc27394	最新のデバイス コネクタ（DC）1.0.9-2159 を 5.0(4a) ビルドに追加します。	5.0(2a)
CSCwc45638	UCSX-210C-M6 ボードコントローラを 18.0 に更新します。次の場合は更新が必要です。 • UCSX-210C-M6 コンピューティング ノードで確認された M.2 の問題を修正するための 3.3v から 3.4v への UCD アップデート。 • UCD が変更され、fail_pwr_seq のトリガとして P54V UV 障害が追加されました。現在 P54V UV の障害が発生すると、HSC は FAULT GPIO をトリガします。 • VR HOT の問題に対処するための INF VR 画像の更新。 • ボード アップデート 17.0 で i2c トランザクションが失敗する	5.0(2a)

リリース *5.0(2e)* で解決された問題

次の表は、リリース 5.0(2e) で解決済みの不具合のリストです。

不具合 ID	説明	影響を受ける最初のバンドル
CSCvx55355	C220 および C240 M6 サーバーの AMI ラベルの更新。	5.0(2d)
CSCwc80156	ユーザーは、BIOS セットアップ メニューで Intel SGX Enable オプションを選択し、Windows を起動して Intel SGX BIOS Info Tool を実行します。M6 サーバーで SGX が有効になっている MCHECK エラー コード = 0x00004811 に対して uCode が無効であるように見えるため、Intel SGX が有効になっていないことが確認されました。	5.0(2d)
CSCwc91429	M5 および M6 サーバーのデバイス コネクタを 1.0.11-2209 に更新します。	5.0(1b)
CSCwb09233	X210c サーバーの CPWM ファン速度制御に HSC 温度（Q71）および PCH 温度センサーを追加します。	5.0(1b)
CSCvx54489	Intersight は、VideoEncryption プロパティをサポートしなくなりました。すべてのプラットフォームでビデオ暗号化の KVM 構成を削除します。	5.0(1b)
CSCwb37591	「InvalidFanPolicies」プロパティを CPWM ファン制御に追加して、256 GB の DIMM がブレードに存在する場合にファン ポリシーのバランスをとります。	5.0 (1c)
CSCwb79633	HSC、PCH、MLOM、および MLOM DIE 温度センサーから IPMI しきい値を削除します。これらのセンサーを X210c サーバーの CPWM ファン速度制御に追加します。	5.0(1b)
CSCwc08368	XFM2 が削除されると、CIMC で予期されるアラームが発生しません。UCS X440P 上の UCSX-GPU-T4-16、UCSX-GPU-A40、UCSX-GPU-A100-80、UCSX-GPU-A16 グラフィックス プロセッシング ユニットの GUI で、欠落している正常性アラームが表示されます。	5.0 (2b)
CSCwb90464	x210c サーバーを要求して検出した後、ストレージがインベントリに表示されません。	5.0(2d)

リリース *5.0(2d)* で解決された問題

次の表は、リリース 5.0(2d) で解決済みの不具合のリストです。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwb96614	自己暗号化ドライブ (SED) のステータスは、再起動後に未構成と表示されます。5.0(2d) と統合されたストレージ ファームウェア パッケージ（52.20.0-4523）は、この問題を修正します。	5.0 (2b)
CSCwc62657	BIOS バージョン 5.0.1h.0、5.0.1i.0、または 5.0.2c.0 を実行している Cisco UCS X210c M6 サーバーは、次回の再起動時に PPR が完了したときに、複数のメモリ ECC エラーと ADDDC/PCL イベントの後に複数の修正不能エラーを表示します。	5.0(1e)

リリース *5.0(2b)* で解決された問題

次の表は、リリース 5.0(2b) で解決済みの警告のリストです。

不具合 ID	説明	影響を受ける最初のバンドル
CSCvw35916	Cisco UCS X210c M6 サーバーでは、BMC の再起動はクリーンではありません。再起動中に、Network Time Protocol デーモン（ntpd）が 2 回起動し、2 回目は失敗します。	5.0(1b)
CSCvy52485	センサー履歴ログを変更して、1 日の最高気温のみが記録されるようにします。	5.0(1a)
CSCvz14883	Syslog には次のように表示されます。 *Secure-Action-monitor*：*1108*：*97:uem_connect_to_server*：サーバーへの接続エラー *Secure-Action-monitor*：*1108*：*src/monitor.c:1528:Security-Check*：イベントを投稿できませんでした セキュアアクションモニターは、UEMd に接続してイベントを発行できません。 セキュアアクションはブートプロセスの早い段階で開始され、残りのインフラストラクチャが稼働する前に障害を通知しようとします。	5.0(1b)
CSCvz16428	電源復元ポリシーが LastState に設定されている場合、LastPowerState はボードの電源状態に設定されていません。	5.0(1b)

不具合 ID	説明	影響を受ける最初のバンドル
CSCvz55930	UCSX-210C-M6 サーバーの廃止または再稼働後、プロファイル値はデフォルト（350/1300）にリセットされます。すべてのブレードサーバーには有効なプロファイル値（最小値/最大値）があり、ハードウェア構成の一部として変更されないようにする必要があります。	5.0(1b)
CSCvz88277	ブレードサーバーでは、エラー修正コード（ECC）が原因で起動時間が 10 分を超えると、電源プロファイルがタイムアウトになり、電源状態がオフと表示されます。	5.0（1b）
CSCvz96056	X シリーズ サーバーの場合、Cisco IMC では、Intersight 管理モード（IMM）が新しい製品 ID カタログをプッシュし、カタログの更新後にサービスを再開できるようにするインターフェイスが必要です。これは、完全なイメージ検証を必要としないため、特にドライブ、メモリ、または CPU に使用できます。	5.0(1b)
CSCwa67582	仮想インターフェイス カード（*VIC*）および LAN-on-motherboard（*mLOM*）アダプタの状態を監視および維持するために、ファンコントロールに温度センサーを追加します。	5.0(1b)
CSCwa88344	*update-utility.sh* の構文エラー（行 136 および行 140）が原因で、デバイス コネクタ（DC）のアップグレードが失敗します。更新中に DC イメージの正しいバージョン行を見つけるために更新します。	5.0(1b)
CSCwb23534	UCSBX-9508 の場合、最初に REAR-MEZZ として報告された UCSX-V4-PCIME および UCSX-V4-Q25GME のスロットを PCI-MEZZ-XFABRIC（PCI-MEZZ1-XFABRIC および PCI-MEZZ2-XFABRIC）に変更します。	5.0 (1c)
CSCwb85297	デバイス コネクタ (DC) が複数回再起動し、致命的なエラー: 同時マップ書き込み（*fatal error: concurrent map writes*）が表示されます。最新のデバイス コネクタ (DC) 1.0.9-2021 を 5.0(2b) ビルドに追加します。	5.0(1e)
CSCwc03295	Cisco UCS X210c M6 サーバでは、クラッシュダンプの収集中に Cisco Integrated Management Controller（CIMC）libpeci が 0x94 CC を処理していません。この問題を解決するには、BIOS で UMA タイムアウトを無効にし、PECI CC 0x94 を正常に完了したと見なします。	5.0 (1c)

リリース *5.0(1f)* で解決された問題

次の表は、リリース 5.0(1f) で解決済みの不具合のリストです。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwb96971	UCSX-210C-M6 サーバーでは、M.2 ドライブでランダムに障害が発生し、仮想ディスクが劣化します。	5.0(1e)

リリース *5.0(1e)* で解決された問題

次の表は、リリース 5.0(1e) で解決済みの不具合のリストです。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwb09802	BIOS トークンは、ホスト オペレーティング システム (OS) から取得できるように、サーバー プロファイル、テンプレート、およびシステム情報を保持する必要があります。	5.0(1b)
CSCvx95585	システム管理 BIOS タイプ 11 には、$SPI、$SPT、$SYS のパラメータがありません。	5.0(1b)
CSCwb21466	Kioxia PM6-ISE SSD ファームウェア 0103 を Intersight 管理モードで B200 M6 サーバーに追加します。	5.0 (1c)
CSCwb21467	Kioxia PM6-FIPS SSD ファームウェア 0103 を Intersight 管理モードで B200 M6 サーバーに追加します。	5.0 (1c)
CSCwa98937	5.1 パッケージ 52.20.0-4432 から 5.0(1b) パッケージ 52.15.0-3988 へのストレージ ファームウェア ダウングレードの説明メッセージを変更する必要があります。	5.0(1b)
CSCwa22730	ストレージ コントローラ UCSX-X10C-RAIDF SPDM 障害の問題の説明メッセージを修正します。	5.0(1b)
CSCwb88505、CSCwb81096	5.0(1c) のホスト サービス ユーティリティ（HSU）インベントリ中の検出コアの修正。	5.0 (1c)
CSCwb28440	一部の Cisco UCS X210c ブレード サーバーは、デバイス コネクタ（DC）の起動に失敗します。その結果、サーバーで DC マウントが失敗し、すべてのサーバー検出が失敗します。	5.0(1b)

リリース *5.0(1c)* で解決された問題

次の表は、リリース 5.0(1c) で解決済みの不具合のリストです。

不具合 ID	説明	影響を受ける最初のバンドル
CSCvz19856	Intel® Intelligent Power Technology Node Manager (NM) PTU では、起動時に Cisco UCSX-210C-M6 サーバーで失敗が断続的に発生し、電源プロファイルの実行は中断されます。	5.0(1b)
CSCvz25126	Cisco UCSX-210C-M6 サーバーの入力電力測定値とメインのホットスワップ コントローラの出力電力測定値に創痍が発生します。	5.0(1b)
CSCvz69262	BIOS ポリシーで STEP を有効にすると、以下の DIMM では BiosTech.log のチェックとメモリの検出テストが機能しませんでしたが、この問題は解決されました。 • UCS-ML-128G4RW • UCS-MR-X64G2RW • UCS-MR-X32G1RW • UCS-MR-X16G1RW • UCS-ML-128G4RW • UCS-MR-X64G2RW • UCS-MR-X32G1RW • UCS-MR-X16G1RW	5.0(1b)
CSCwa10354	Cisco UCSX-210C-M6 サーバーでは、ノード マネージャが電力上限設定ファイルにアクセスできず、断続的な電力プロファイリングの失敗またはプロファイル データの損失が発生します。	5.0(1b)
CSCwa15349	M6 システムのデフォルトの動作は、DIMM 装着（POR）を強制することです。DIMM 障害が発生すると、この強制によりかなりの量のメモリが無効になり、追加の DIMM に無効な装着としてフラグが付けられます。	5.0(1b)
CSCwa16535	電圧レギュレーター（VR）設定を調整するための CPU パフォーマンス トークン UCSX-210C-M6 の強化のサポートが追加され、プロセッサーのパフォーマンスが向上しました。	5.0(1b)

C シリーズ サーバー ファームウェアで解決された問題

C シリーズ *M7* ファームウェア リリース *4.3*（*1.230138*）で解決された不具合

次の表には、C シリーズ M7 ファームウェア リリース 4.3（1.230138）で解決済みの問題を一覧表示しています。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwe87764	128GB DIMM を搭載した Cisco UCS M7 サーバーでは、システム パフォーマンスを向上させるために電圧レギュレータの値を変更すると、CPU のパフォーマンスが低下する可能性があります。	4.3(1.230124)

C シリーズ *M7* ファームウェア リリース *4.3*（*1.230124*）で解決された問題

次の表には、C シリーズ M7 ファームウェア リリース 4.3（1.230124）で解決済みの問題を一覧表示しています。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwe47118	Redfish monitor core が組み合わせストレス（Redfish stressを含む）中に発生しました。	4.3(1.230097)

C シリーズ *M6* と *M7* ファームウェア リリース *4.2(3j)*）で解決された不具合 - なし

リリース *4.2(3i)* の解決済みの不具合

リリース 4.2(3i)では、次の不具合が解決されています。

不具合 ID	症状	影響を受ける最初のバンドル
CSCwb82433	Cisco UCS VIC 1400 シリーズアダプタを搭載し、*Geneve* が有効になっている Cisco UCS C220 M5 サーバーは、Cisco UCS VIC アダプタが応答しなくなった後にオフラインになります。	4.2 (2a)
CSCwf88211	Cisco UCS C240 M6 サーバーでは、動作中に次のエラーが表示されます。 `AdapterHostEthInterfaceDown` サーバーの機能への影響はありません。	4.2（3h）

C シリーズ ファームウェア リリース *4.2(3h)* で解決された不具合

リリース 4.2(3h)では、次の不具合が解決されています。

不具合 ID	症状	影響を受ける最初のバンドル
CSCwe92151	Cisco UCS C シリーズ M6 または M7 サーバでの操作中に特定のモデルの HDD が挿入されるか、ドライブが初期化されると、サーバの電源が自動的にオフ状態からオンになります。これにより、低レベルのファームウェアの更新が失敗します。	4.3.2.230207

C シリーズ ファームウェア リリース *4.2(3g)* で解決された不具合

次の表には、C シリーズ ファームウェア リリース 4.2(1g) で解決済みの不具合を一覧表示しています。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwe61589	Cisco UCS C220 M5 サーバーでは、アプリケーション ストール メッセージの後にインテリジェント プラットフォーム管理インターフェイス（IPMI）が継続的な再起動ループに入り、IPMI 管理が失敗します。	4.1（3c）
CSCwd46043	Cisco UCS C240 M5 サーバーの通常の動作中に、Cisco IMC が管理プレーンの接続を失う可能性があります。 Cisco IMC（管理プレーン）は影響を受けるコンポーネントであり、接続は自動的に復元されるため、データプレーンには影響がない場合があります。	4.2 (2a)

リリース *4.2*（*3b*）の解決済みの問題

次の表には、C シリーズ ファームウェア リリース 4.2(3b) で解決済みの問題を一覧表示しています。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwd79791	ucs-c245m6-hx-Catalog.json の json ファイルにハイフンがありません。	4.2（2g）
CSCwd68472	サーバファームウェアのアップグレードは、「ファームウェア アップグレードが完了するのを待っています。操作がタイムアウトしました」で失敗しました。	4.2（2g）

リリース *4.2(2g)* で解決された問題

次の表には、C シリーズ ファームウェア リリース 4.2(2g) で解決済みの問題を一覧表示しています。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwd56630	C480 M5 サーバの NIHUU 更新が進行中の場合、予期しないホストの電源サイクルが発生します。	4.2（2f）
CSCwc76592	SAS コントローラがなくなるため、M6 拡張は失敗します。2 つの M6 コンバージ ノードで 2N 5.0.2a M5 エッジ クラスタを拡張しようとすると、「ハイパーバイザ管理ネットワークの構成」で拡張が失敗します。SAS コントローラが CIMC に表示されなくなりました。拡張障害は両方の M6 サーバで見られます。	4.2(2b)
CSCwd03250	DST 機能により、グローバル ホット スペアが誤って不良としてマークされます。4.2(2a) ファームウェアでは、「ローカル ディスク X が劣化しています」という障害が発生する場合があります。これは 7 日ごとに発生する可能性があります。	4.2 (2a)
CSCwb01975	Intel ADP-RR NVMe ドライブに FRU VPD データがありません。FRU VPD から欠落しているフィールドがほとんどありません - 容量（nvme_vpd_mra）、メーカー名、製品名、製品部品番号/モデル、製品バージョン、製品シリアル番号。	4.2（1a）
CSCwd29230	M6 プラットフォームのUCS-NVMEHY-W3200 および UCS-NVMEHY-W1600 LFF PID を削除します。	4.2（2f）
CSCwc10747	SAN ブート中に予期しない順序のイベントが発生すると、VIC FLS プロセスがクラッシュすることがあります。SAN ブートのイベント シーケンスが期待どおりに発生しない非常にまれな状況では、FLS プロセスが VIC アダプタでクラッシュし、ASSERT エラーの後に VIC OBFL に次のように表示されることがあります。 (/bin/fls) シグナル 11 を受信したため終了しました - セグメンテーション エラー（コア ダンプ）	4.2（2f）
CSCwd33432	UCSC-MLOM-C100-04 および UCSC-PCIE-C100-04 アダプタの unconfigAllNic で、C220-M5L サーバでサーバ プロファイルの関連付けが失敗しました。	4.2（2f）

リリース *4.2(2b)* の解決済みの問題

次の表には、C シリーズ ファームウェア リリース 4.2(2b) で解決済みの問題を一覧表示しています。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwc34359	ログ ディレクトリに SAN ドライブの詳細を追加します。SAN ドライブの詳細を /sys/firmware/ibft、/sys/class/fc_host、および /sys/class/fc_transport ディレクトリからログ ディレクトリにコピーすると、この情報がテクニカル サポート ファイルに反映されます。	4.2 (2a)
CSCwc38237	megaraid_sas ドライバ（RHEL8.2、RHEL7.9）で scu ソースコードを更新します。	4.2 (2a)
CSCwc27924	256 MB のサイズ制限があるため、フレックス ユーティリティ パーティションに収まるように SDU iso のサイズを縮小します。	4.2 (2a)
CSCwc26997	HDD モデル MTFDDAK120TDT で、サーバを 4.2(1b) から 4.2(1f) にアップグレードできませんでした。	4.2(1b)

リリース *4.2(1j)* で解決済みの問題

次の表には、C シリーズ ファームウェア リリース 4.2(1j) で解決済みの問題を一覧表示しています。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwb69579	Intel i350 Quad Port 1Gb Adapter の個々のコンポーネント ファームウェアの更新が失敗します。Intel i350 Quad Port 1Gb Adapter の更新がトリガされました。タスク ID の応答が確認されました。「HSU OS を起動できません」エラーで更新が失敗します。	4.2(1i)
CSCwc23748	4.2 から 4.1 への HSU ダウングレード中に、HSU 更新タスクが長時間スタックし、「例外: HSU OS を起動できません」が表示されました。	4.2(1i)
CSCvx55355	C220 および C240 M6 サーバの AMI ラベルをマージします。	4.2(1i)
CSCwa56128	ファームウェアのダウングレード中にすべての Intel カードが失敗します。ファームウェアを ucs-c240m6-huu-4.2.1.144.iso から ucs-c240m6-huu-4.2.1e.211202.iso にダウングレードします。すべてのコンポーネントを選択し、更新をトリガーします。X550 カードのファームウェアの更新に失敗しました。	4.2(1i)
CSCwc37184	CIMC から BIOS を更新した後、RHEL OS が緊急モードになります。これは、最新の BIOS C220M6.4.2.1i.6.0703222157 で確認されています。	4.2(1i)

不具合 ID	説明	影響を受ける最初のバンドル
CSCwc18223	セキュア UEFI が有効になっている場合、一部の SED ドライブは再起動時に未構成で正常に設定されているため、RAID の再構築が強制されます。	4.2(1f)
CSCwb83355	VIC は、RESERVATION_CONFLICT ステータスを受信する IO に対してターゲットが RESID ビットを設定しない場合、ファームウェア/scsi ステータスを DATA_CNT_MISMATCH/RESERVATION_CONFLICT として報告します。 ESX SCSI レイヤーは、DATA_CNT_MISMATCH を障害と見なし、RESERVATION_CONFLICT SCSI ステータスを無視します。 受信した予約の競合が多すぎると、仮想マシンのパフォーマンスが低下する可能性があります。	4.2(1i)

リリース *4.2(1g)* で解決された問題

次の表には、C シリーズ ファームウェア リリース 4.2(1g) で解決済みの問題を一覧表示しています。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwa98283	エンドポイントでのアップグレードが NIHUU アップグレードでスタックし、ホストが継続的に再起動して新しいイメージをマウントしようとし、EULA を要求します。これは、HUU のローカルにマウントされた vmedia を使用して C220 M5 サーバをアップグレードするときに観察されます。	4.1（3c）
CSCwb04635	C225 および C245 M6 サーバのファームウェア コンポーネントを 4.2(1f) から 4.2(1g) に更新しているときに、BIOS の更新/アクティブ化で障害が発生します。	4.2(1f)
CSCwb07978	センサーの読み取りと GPU インベントリは、Nvidia A16 GPU の検出に失敗します。C245 M6 サーバは最新の BIOS および CIMC ファームウェアでアップグレードされ、A16 GPU が接続され、最新の HUU が接続されています。CIMC にログインした後、A16 の詳細がリストされていないことが [GPU インベントリ（GPU Inventory）] ページに表示されます。	4.2(1f)

リリース *4.2(1f)* で解決された問題

次の表には、C シリーズ ファームウェア リリース 4.2(1f) で解決済みの問題を一覧表示しています。

不具合 ID	説明	影響を受ける最初のバンドル
CSCvz89363	C225 および C245 M6 サーバで IT コントローラ ファームウェアを 20.65.05.00 から 16.65.28.00 にダウングレードした後、アウトオブバンド モードが I2c から PCIe に変更され、コントローラが CIMC で検出されません。	4.2(1e)
CSCvz77885	Cisco UCS C240 M5 サーバの通常の動作中に、CIMC の不明な再起動が報告されました。これは、CIMC バージョン 4.1(3d) について報告されています。	4.2(1e)
CSCwa22529	Bios ファームウェアの更新ステータスは、Bios Activation に対して自動的に更新されません。これは、CIMC ビルド 4.2(1d) および Bios Ver C245M6.4.2.1c.0.080621134 を使用する C 225 および C245 M6 サーバで検出されます。	4.2(1e)

B シリーズ サーバー ファームウェアで解決された不具合

B シリーズ *M6* ファームウェア リリース *5.1 (0.230069)* で解決された問題

次のテーブルでは、B シリーズ M6 ファームウェア リリース 5.1（0.230069）で解決された問題を一覧表示しています。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwe47304	デフォルト ゲートウェイは、Inband2 > Inband1 > OutbandB > OutbandA に続く優先順位に従って設定されません。	5.1(0.230052)
CSCwe65074	デバイス コネクタを 1.0.11.2759 に更新します。	5.1(0.230052)
CSCwe54208	Inband2 を別の VLAN で再作成し、Inband1 を追加する前に削除する必要があります。	5.1(0.230052)

B シリーズ *M5* ファームウェア リリース *5.1*（*0.230073*）で解決された問題

次のテーブルでは、B シリーズ M5 ファームウェア リリース 5.1（0.230073）の解決された問題を一覧表示します。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwe65074	デバイス コネクタを 1.0.11.2759 に更新します。	5.1(0.230054)
CSCwe54208	Inband2 を別の VLAN で再作成し、Inband1 を追加する前に削除する必要があります。	5.1(0.230054)

不具合 ID	説明	影響を受ける最初のバンドル
CSCwe47304	デフォルト ゲートウェイは、Inband2 > Inband1 > OutbandB > OutbandA に続く優先順位に従って設定されません。	5.1(0.230054)

B シリーズ ファームウェア リリース *5.1*（*0.230052*）で解決された問題

次のテーブルでは、B シリーズ ファームウェア リリース 5.1（0.230052）の解決された問題を一覧表示します。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwa47736	KVM クライアントの右上のメニューは、ブラウザ ウィンドウのサイズ変更では機能しません。これは、Firefox ブラウザで観察されます。	4.2(3b)
CSCwb87775	カーネル パニックが発生し、B シリーズ M6 サーバのディスカバリ ストレスを実行すると CIMC が再起動します。	4.2(2e)
CSCwd17871	B シリーズ M6 サーバのインバンド IPv4 IP を使用する IPMI コマンドは、OOB IP で機能している間は機能しません。	4.2(3b)
CSCwd04607	B シリーズ製品のインバンド サポート向け Redfish を有効にします。	4.2(3b)
CSCwe10891	デバイス コネクタを 1.0.11.2611 に更新します。	4.2(3b)

B シリーズ ファームウェア リリース *5.1*（*0.230054*）で解決された警告

次のテーブルでは、B シリーズ M5 ファームウェア リリース 5.1（0.230054）の解決された問題を一覧表示します。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwb87775	カーネル パニックが発生し、B シリーズ M5 サーバのディスカバリ ストレスを実行すると CIMC が再起動します。	4.2(2e)
CSCwd17871	B シリーズ M5 サーバのインバンド IPv4 IP を使用する IPMI コマンドは、OOB IP で機能している間は機能しません。	4.2(3b)
CSCwd04607	B シリーズ製品のインバンド サポート向け Redfish を有効にします。	4.2(3b)
CSCwe10891	デバイス コネクタを 1.0.11.2611 に更新します。	4.2(3b)

不具合 ID	説明	影響を受ける最初のバンドル
CSCvs49681	1 つの OOB インターフェイスが削除されると、明示的に削除されていなくても、もう一方の OOB インターフェイスのゲートウェイがクリアされます。もう一方のゲートウェイには、引き続きアドレス、ネットマスク、ホスト名、VLANがあります。	4.2(3b)

B シリーズ ファームウェア リリース *4.2(3j)* で解決された不具合 - なし

B シリーズ ファームウェア リリース *4.2(2e)* で解決された問題

次のテーブルには、B シリーズ ファームウェア リリース 4.2(2e) で解決された問題を一覧表示します。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwd29415	RHEL 8.7 および RHEL9.1 OS サポートを SCU DB に追加します。	4.2(2d)
CSCwd29230	B シリーズ M6 サーバの UCS-NVMEHY-W3200 および UCS-NVMEHY-W1600 LFF PID を削除します。	4.2(2d)
CSCwa79931	UCSB-ML-V5Q10G mLOM の UCSX-I-9108-100G シャーシへの MLOM 温度の温度監視とファン制御を含めます。	4.2(2d)

B シリーズ ファームウェア リリース *4.2*（*2e*）で解決された問題

次のテーブルには、B シリーズ ファームウェア リリース 4.2(2b) で解決された問題を一覧表示します。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwc38237	megaraid_sas ドライバ（RHEL8.2、RHEL7.9）で scu ソース コードを更新します。	4.2 (2a)

B シリーズ ファームウェア リリース *4.2(1h)* で解決された警告

次のテーブルには、B シリーズ ファームウェア リリース 4.2(1h) で解決された問題を一覧表示します。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwc27394	B200 M6 ファームウェア イメージを DC 1.0.9-2159 に更新します。	4.2(1f)
CSCwc03295	クラッシュダンプの収集中に libpeci が 0x94 CC を処理しない。これは、すべてのプラットフォームでのクラッシュダンプ コレクションに影響を与え、CATERR のイベントでシステム デバッグを支援するのに役立たない無効な（ガベージ）データを含むクラッシュダンプ出力 json ファイルを生成します。	4.2(1f)

B シリーズ ファームウェア リリース *4.2(1f)* で解決された警告

次のテーブルには、B シリーズ ファームウェア リリース 4.2(1f) で解決された問題を一覧表示します。

不具合 ID	説明	影響を受ける最初のバンドル
CSCvx95585	Smbios タイプ 11 には、B200 M6 サーバーの $SPI、$SPT、および $SYS がありません。	4.2(1e)
CSCwa33158	UCS-B200-M6 サーバの消費電力の読み取り値は、サーバが消費する実際の電力よりも 9% 少ないことがわかりました。	4.2(1e)
CSCwa85667	カーネルのクラッシュとウォッチドッグのリセットが原因で、M5 および M6 サーバで BMC のリセットが検出されました。これは通常、簡単な検出をトリガします。	4.1(3b)
CSCvx37634	ブレードの検出が失敗し、UCSM で次のエラーが発生します。「Vmedia のセットアップに失敗しました (sam:dme:ComputeBladeDiscover:SetupVm	4.1(3b)

B シリーズ ファームウェア リリース *4.2(1c)* で解決された警告

次のテーブルには、B シリーズ ファームウェア リリース 4.2(1c) で解決された問題を一覧表示します。

不具合 ID	説明	影響を受ける最初のバンドル
CSCvz29291	HTTP または HTTPS でマウントされた vMedia は、特定のホスティング ツールでは機能しない場合があります。HTTP または HTTPS を介して Cisco API を使用して ISO をサーバにマウントしようとすると、サーバはボリュームとリモート共有の詳細を正しく表示します。これで動作し、ステータス列に「ローカルデバイスのマウントに失敗しました」というエラーで最終的に失敗します。	4.1(3b)
CSCvz46580	OTP 資格情報を使用した KVM ログインで、「ログインが拒否されました」と表示されます。	4.1(3b)
CSCvy88260	UCSB-MRAID12G-HE 4x SATA 物理ドライブを備えた B480M5 サーバの場合、「モデル」情報がありません。	4.1(3b)

未解決の不具合

C シリーズ、B シリーズ、および X シリーズ ファームウェア リリース 4.2(3j) の未解決の不具合：なし

X シリーズ ファームウェア リリース 5.0(2b) の未解決の警告

次の問題は、X シリーズ ファームウェア リリース 5.0(2b) で未解決です。

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCwb96316	Cisco UCS X210c M6 サーバーでは、ファームウェアを 5.0(1c) または 5.0(1e) から 5.0(2b) にアップグレードした後、インベントリで MRAID コントローラとディスクが検出されません。	Intersight 管理モードからファームウェアアップグレードを再実行します。	5.0 (1c)

X シリーズ ファームウェア リリース 5.0(1f) の未解決の問題

次の問題は、X シリーズ ファームウェア リリース 5.0(1f) で未解決です。

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCwb96316	Cisco UCS x210c M6 サーバーでは、ファームウェアを 5.0(1c) および 5.0 (1e) から 5.0(1f) にアップグレードすると、MRAID コントローラがインベントリから消えます。	Intersight 管理モードからファームウェアアップグレードを再実行します。	5.0 (1c)

既知の制限事項と動作

VR 設定はCPU パフォーマンスの強化を有効にするために調整されます

CSCwa15491 - UCSX-210C-M6 サーバの BIOS で CPU パフォーマンス拡張設定を有効にするには、VR 設定を調整する必要があります。

関連資料

リリース ノート

- Cisco Intersight インフラストラクチャ ファームウェアのリリース ノート
- Intersight マネージド モード ファームウェアのリリース バンドルのコンテンツ
- 『Release Notes for Cisco UCS Manager』

『Hardware Installation Guides』

- Cisco UCS X210c M6 コンピューティングノードのインストールおよびサービスノート
- Cisco UCS X9508 サーバ シャーシ インストレーション ガイド

Cisco Intersight のリソース

- Advisories
- Cisco TAC およびプロアクティブ RMA との統合 https://intersight.com/help/saas/features/cisco_intersight/settings#integration_with_cisco_tachttps://intersight.com/help/saas/features/cisco_intersight/settings#proactive_support_enabled_through_intersight
- 契約ステータス
- ハードウェア互換性リスト（HCL）との準拠

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。