Cisco Intersight サーバー ファームウェアのリリース ノート

初版：2022 年 2 月 15 日

最終更新：2022 年 11 月 7 日

概要

はじめに

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、HyperFlex™ ハイパーコンバージド インフラストラクチャ（HCI）、およびサードパーティ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。

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

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
2022 年 11 月 23 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。
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

5.0(2b) の新しいハードウェア リリース

次のサポートが追加されました。

- Cisco UCSX-210C-M6 サーバー用の UCSX-ML-V5D200G モジュラ LAN オン マザーボード（mLOM）アダプタのサポート。
- 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
- UCSX-210C-M6 サーバーを備えた UCSX-440P 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：

- UCSX-GPU-T4-16
- UCSX-GPU-A40
- UCSX-GPU-A100-80
- UCSX-GPU-A16

5.0(1a) の新しいハードウェア リリース

Cisco UCS X210c M6 コンピューティング ノード（X シリーズ サーバー）

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。

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)**
5.0(2)	はい	はい
5.0(1)	はい	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(2b)	はい	はい
4.2(1)	はい	非対応
4.1(3)	はい	非対応

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 (2a)	はい	はい
4.2(1)	はい	はい
4.1(3)	はい	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 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。1983 年の rcp から派生した scp 実装により、サーバーはクライアントに送信されるファイル/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。1983 年の rcp から派生した scp 実装により、サーバーはクライアントに送信されるファイル/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。

（注） Cisco Bug Search Tool にログインしてこのツールを使用するには、Cisco.com アカウントが必要です。アカウントがない場合は、アカウントを登録できます。

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

（注） Intersight の欠陥は、ファームウェアとは別に追跡されます。Intersight の未解決の欠陥については、「Intersight の未解決の警告」を参照してください。

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	リリースで解決済み
CSCvx55355	C220 および C240 M6 サーバーの AMI ラベルの更新。	5.0(2d)	5.0(2e)
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)	5.0(2e)
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(1a)	5.0(2e)
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(1a)	5.0(2e)
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(1a)	5.0(2e)
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)	5.0(2e)
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(1a)	5.0(2e)

不具合 ID	説明	影響を受ける最初のバンドル	リリースで解決済み
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)	5.0(2e)
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)	5.0(2e)

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	リリースで解決済み
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)	5.0(2d)
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)	5.0(2d)

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	リリースで解決済み
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)	5.0(1f)

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	リリースで解決済み
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(1a)	5.0 (2b)
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)	5.0 (2b)
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(1a)	5.0 (2b)
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(1a)	5.0 (2b)
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(1a)	5.0 (2b)
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)	5.0 (2b)
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(1a)	5.0 (2b)

不具合 ID	説明	影響を受ける最初のバンドル	リリースで解決済み
CSCwa67582	仮想インターフェイス カード（*VIC*）および LAN-on-motherboard（*mLOM*）アダプタの状態をモニタおよび維持するために、ファン制御に温度センサーを追加します。	5.0(1a)	5.0 (2b)
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(1a)	5.0 (2b)
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)	5.0 (2b)
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)	5.0 (2b)
CSCwc03295	Cisco UCS X210c M6 サーバーでは、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)	5.0 (2b)

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	リリースで解決済み
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。	4.2(1a) および 5.0(1a)	5.0(1e)
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。	4.2(1a) および 5.0(1a)	5.0(1e)
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)	5.0(1e)

不具合 ID	説明	影響を受ける最初のバンドル	リリースで解決済み
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)	5.0(1e)
CSCwa98937	5.1 パッケージ 52.20.0-4432 から 5.0(1a) 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(1.a)	5.0(1e)
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(1a)	5.0(1e)
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)	5.0(1e)
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(1.a)	5.0(1e)

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	リリースで解決済み
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(1a)	5.0 (1c)
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(1.202)	5.0 (1c)

不具合 ID	説明	影響を受ける最初のバンドル	リリースで解決済み
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	(4.2.1h)B	5.0 (1c)
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)	5.0 (1c)
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。	4.2(1f)B	5.0 (1c)
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(1.109)	5.0 (1c)
CSCvz91249	Cisco UCSX-210C-M6 サーバーで UCS-SD76TBKNK9（7.6TB 2.5 インチ エンタープライズ バリュー 12G SAS SSD（1DWPD、SED-FIPS））のサポートが追加されました。	4.1(3c)S9	5.0 (1c)
CSCvz91247	Cisco UCSX-210C-M6 サーバーで UCS-SD480G63X-EP（480GB 2.5 インチ エンタープライズ パフォーマンス 6GSATA SSD）のサポートが追加されました。	4.1(3d)HS17	5.0 (1c)

不具合 ID	説明	影響を受ける最初のバンドル	リリースで解決済み
CSCvz91245	Cisco UCSX-210C-M6 サーバーで UCS-SD480G6I1X-EV（480GB 2.5 インチ エンタープライズ バリュー 6G SATA SSD）のサポートが追加されました。	4.1(3d)HS17	5.0 (1c)
CSCvz91242	Cisco UCSX-210C-M6 サーバーでの UCS-SD800GS3X-EP（800GB 2.5 インチ エンタープライズ パフォーマンス 12G SAS SSD）のサポートが追加されました。	4.1(3c)HS21	5.0 (1c)
CSCvz91238	Cisco UCSX-210C-M6 サーバーで UCS-SD19TS1X-EV（1.9TB 2.5 インチ エンタープライズ バリュー 12G SAS SSD）のサポートが追加されました。	4.1(3c)HS21	5.0 (1c)
CSCvz91236	Cisco UCSX-210C-M6 サーバーで UCS-SD960G6S1X-EV（960GB 2.5 インチ エンタープライズ バリュー 6G SATA SSD）のカタログ サポートが追加されました。	4.1(3d)HS14 および 4.2(1c)H	5.0 (1c)

未解決の不具合

（注） Intersight の欠陥は、ファームウェアとは別に追跡されます。Intersight の未解決の欠陥については、「Intersight の未解決の警告」を参照してください。

リリース 5.0(1f)で未解決の問題

リリース 5.0(1f) では、次の警告が未解決です。

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)

リリース 5.0(2b)で未解決の警告

リリース 5.0(2b) では、次の警告が未解決です。

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)

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

『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。