Cisco Intersight Managed Mode Infrastructure Firmware、Release 4.2 のリリース ノート

最終更新：2025 年 4 月 23 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。

Intersight Managed Mode（IMM）は、Redfish ベースの標準モデルを通じて UCS ファブリック インターコネクト システムを管理する新しい IIS アーキテクチャです。IMM は、UCS システムの機能と Intersight のクラウドベースの柔軟性を統合し、スタンドアロンおよびファブリック インターコネクト接続システムの管理エクスペリエンスを統合します。

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情報が記載されています

- FI カーネルおよびシステム
- シャーシ IOM および IFM I/O モジュール

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

（注） このドキュメントには、Cisco Intersight 管理モード（IMM）に適用されるコンポーネントに固有の情報が含まれています。UCSM 管理モード（UMM）またはスタンドアロンモードの Cisco UCS サーバーに関連する既知の問題と制限については、次を参照してください。

- Cisco UCS Manager リリースノート
- Cisco IMC のリリース ノート

Cisco Intersight、Cisco IMC、および Cisco UCS Manager 間のファームウェア バージョンの同等性

詳細については、「Cisco Intersight、Cisco IMC、および Cisco UCS Manager 向け Cisco UCS 同等性マトリクス」を参照してください。

更新履歴

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
2025 年 2 月 21 日	インフラストラクチャ ファームウェア リリース 4.2(3m) のリリース ノートを更新しました。このリリースには、以下への更新が含まれます。 • リリースで解決済みの問題 4.2(3m) （7 ページ） • リリースで未解決の問題 4.2(3m) （19 ページ） 新しいハードウェアのサポート、セキュリティ修正は含まれていません。
2024 年 12 月 19 日	Cisco UCS X シリーズ 5.0(4h)、B シリーズ4.2(3k)、C シリーズ 4.2(3n) サーバ ファームウェア バージョンがリリースされました。対応するインフラストラクチャ ファームウェア リリースはありません。
2024 年 10 月 1 日	インフラストラクチャ ファームウェア リリース 4.2(3l) のリリース ノートを更新しました。このリリースには、リリース 4.2(3l) のセキュリティ修正 と リリース 4.2(3l) の解決済みの問題の更新が含まれています。新しいハードウェアのサポートや未解決の問題は含まれていません。
2024 年 8 月 20 日	リリース 4.2(3k) で解決済みの問題を更新しました。

改訂日	説明
2024 年 6 月 17 日	Intersight インフラストラクチャ ファームウェア リリース 4.2(3k) のリリース ノートを更新しました。
2024 年 4 月 17 日	**クロス バージョン ファームウェア サポート**の表を更新しました。
2024 年 2 月 22 日	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(3j) がリリースされました。このリリースでは、リリース 4.2(3j) の解決済みの不具合セクションに更新が含まれています。新しいハードウェアのサポート、セキュリティ修正、未解決の問題は含まれていません。
2023 年 9 月 29 日	Intersight インフラストラクチャ ファームウェア リリース 4.2(3h) のリリース ノートを更新しました。
2023 年 7 月 24 日	Intersight インフラストラクチャ ファームウェア リリース 4.2(3g) のリリース ノートを更新しました。
2023 年 5 月 17 日	Intersight インフラストラクチャ ファームウェア リリース 4.2(3e) のリリース ノートを更新しました。
2023 年 3 月 27 日	Intersight インフラストラクチャ ファームウェア リリース 4.2(3d) のリリース ノートを更新しました。
2023 年 3 月 16 日	Intersightインフラストラクチャ ファームウェア リリースごとにサポートされるハードウェア情報を含むようにリリース ノートを更新しました。
2023 年 1 月 20 日	Intersight インフラストラクチャ ファームウェア リリース 4.2(2a) のリリース ノートを更新しました。
2023 年 1 月 12 日	Intersight インフラストラクチャ ファームウェア リリース 4.2(3c) のリリース ノートを更新しました。
2023 年 1 月 10 日	Intersight インフラストラクチャ ファームウェア リリース 4.2(3b) のリリース ノートを更新しました。
2022 年 8 月 4 日	Intersight インフラストラクチャ ファームウェア リリース 4.2(2b) のリリース ノートを更新しました。
2022 年 2 月 15 日	Intersightインフラストラクチャ ファームウェア リリース4.2(1l) のリリース ノートを作成しました。

新しいソフトウェア サポート

Intersight ソフトウェア機能では、Intersight ファームウェア リリース スケジュールに一致しない場合があります。最新のソフトウェア機能についての詳細は、Intersight ヘルプ センターの「新機能」セクションを参照してください。

このリリースの新機能

インフラ ファームウェア リリースの新しいハードウェア機能

4.2(3m) での新しいハードウェア サポート：なし

4.2(3c) の新しいハードウェア サポート

Intersight 管理モードでの次の IOM のサポート：

- UCS-IOM-2304
- UCS-IOM-2304V2

（注） 上記の 2 つの IOM は、Cisco UCS 6500 シリーズ ファブリック インターコネクトでのみサポートされ、CMC ファームウェア バージョン 4.2(2.30) 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。

4.2(3b) の新しいハードウェア サポート

（注）

- Cisco UCS X210c M7 コンピューティング ノードには、サーバ ファームウェア バージョン 5.1（0.230096）および 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。
- Cisco UCS C220 M7 および C240 M7 サーバには、サーバ ファームウェア バージョン 4.3（1.230097）および Cisco Intersight Infrastructure Firmware version 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。

4.2(2b) 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-FI-6536 ファブリック インターコネクトのサポート
- Cisco UCSX-I-9108-100G インテリジェント ファブリック モジュール（IFM）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。

4.2(1e) の新しいハードウェア サポート

Cisco UCS X9508 シャーシ

Cisco UCS X シリーズ モジュラシステムは、適応力の高い Cisco UCS X9508 シャーシを備えており、将来の変化にも対応できます。ミッドプレーンのない設計となっているため、X9508 シャーシの I/O 接続には、シャーシ背面の水平方向の I/O 接続モジュールと交差する、垂直方向のフロントローディング コンピューティング ノードが使用されます。ユニファイド イーサネット ファブリックは、Cisco UCS 9108 インテリジェント ファブリック モジュールに付属しています。

- 7 ラック ユニット（7RU）シャーシには、前面に 8 個のフレキシブルスロットがあります。これらは、コンピューティング ノードの組み合わせと、GPU アクセラレータ、ディスク ストレージ、不揮発性メモリなどの将来の I/O リソースのプールを収容できます。
- シャーシをアップストリームの Cisco UCS 6400 シリーズ ファブリック インターコネクトに接続するシャーシ上部の 2 つの Cisco UCS 9108 インテリジェント ファブリック モジュール（IFM）。各 IFM 機能：
  - コンピューティング ノードあたり最大 100 Gbps のユニファイド ファブリック接続
  - 8 個の 25 Gbps SFP28 アップリンク ポート。
- 6 台の2800 W電源装置（PSU）が、N、N + 1、および N + N 冗長性を備えたシャーシに 54V の電力を供給します。
- 効率的な 4x100mm 二重反転ファンにより、業界トップクラスのエアーフローと電力効率を実現します。

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、IMMドメイン内でサポートされるサーバおよびインフラストラクチャ ファームウェアの組み合わせを示しています。追加のインフラストラクチャ ファームウェア制限は、特定の「新しいハードウェア サポート」セクションでメモとしてハイライトされます。

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	非対応	はい
5.1(0)	いいえ	非対応	はい
5.0（4）	はい	はい	はい
5.0(2)	はい	はい	はい

5.0(1)	はい	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(3)**
4.3(1)	はい	はい	はい
4.2(3)	はい	はい	はい
4.2(2)	はい	はい	はい
4.2(1)	はい	はい	はい
4.1(3)	はい	はい	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)	はい	はい	はい
4.2(3)	はい	はい	はい
4.2(2)	はい	はい	はい
4.2(1)	はい	はい	はい
4.1(3)	はい	はい	はい

セキュリティ修正

リリースでのセキュリティ修正4.2(3m)：なし

リリース 4.2(3l) 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。

不具合識別子 ：CSCwk62264

Cisco Intersight 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-2024-6387**：シグナル ハンドラに関連する sshd サービスで競合状態が特定されました。LoginGraceTime 期間（デフォルトは 120 秒、以前の OpenSSH バージョンでは 600 秒）内にクライアントが認証に失敗した場合、sshd SIGALRMハンドラが非同期的にトリガされます。ただし、このハンドラは、syslog() など、シグナル ハンドラ内から呼び出すのが安全ではないいくつかの関数を呼び出します。

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。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。

障害 ID：**CSCwi59915**

Cisco Intersight 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 でバイパスが発生します（CBC が使用されている場合は、-etm @openssh.com MAC アルゴリズム）。

  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。

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

リリースで解決済みの問題 4.2(3m)

次の問題はリリース 4.2(3m) で解決済みです。

不具合 ID	説明	影響を受ける最初のバージョン	リリースで解決済み
CSCwb61769	ファームウェア 4.2.2c にアップグレードした後、UCS 64108 FI でランダムな SNMP OID 問題が発生します。OID「.1.3.6.1.2.1.2.2.1.10.xxxxx」は「noSuchInstance」を返し、OID「.1.3.6.1.2.1.2.1.0」は誤った値「1」を報告します。現在、回避策はありません。	4.2(2c)	4.2(3m)
CSCwb63137	ファームウェア 4.2(2c) の UCS-FI-6454 では、NGINX プロセスがシグナル 6 で断続的にクラッシュし、一時的なアクセス損失を引き起こす可能性があります。ユーザーの操作なしでプロセスが自動再起動します。ログはクラッシュの詳細をキャプチャし、インベントリアラートは自動的にクリアされます。	4.2(2c)	4.2(3m)
CSCwem80801	パッチ KB5040434 を NPS に適用すると、メッセージ認証の問題により、Cisco UCS デバイスで RADIUS ログインが失敗します。パッチをロールバックすると問題は解決し、他の Cisco のデバイスは影響を受けません。	4.2（3h）	4.2(3m)

不具合 ID	説明	影響を受ける最初のバージョン	リリースで解決済み
CSCwem83085	ファームウェア 4.3 の UCS-FI 6454 では、VSAN の FCoE VLAN の変更により、ストレージパスの中断が発生しますが、FC インターフェイスはアクティブなままです。接続は、FC インターフェイスをフラッピングすることにより復元されます。	4.3(4.240074)	4.2(3m)
CSCwn32035	UCS-IOM-2408 ボードで I2C ロックが発生し、SDA ライン ホールドの延長により、システムファンに障害があるとマークされます。ドライバの更新により、I2C チャネルの保留が 5 ミリ秒に延長され、ロック解除プロセスが支援され、永続的なロックが減少します。ファンを一時的に再度装着すると回復する場合がありますが、永続的な問題は IOM の交換が必要になる場合があります。	4.3.5.240021	4.2(3m) 4.3（5.250030）

リリース 4.2(3l) の解決済みの問題

リリース 4.2(3l)では、次の不具合が解決されています。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwk28221	FI が FC スイッチ モードのときに FCoE VLAN を 3121 から 3120 に変更すると、イニシエータは FLOGI して FCID を取得できますが、ターゲット ポートへの PLOGI に失敗し、タイムアウトが無期限になります。FC リンクまたはポートチャネルの管理ダウン/アップにより、問題が解決します。この変更により ESXi でパス損失が発生し、ホスト ログには FLOGI と FCIDの割り当ては成功しましたが、PLOGI タイムアウトが表示されます。	4.3(2b)A
CSCwj28488	無効な証明書を持つ BIOS/bt/biosSecureVars/dbx_os ファイルにより PNUOS の動作が妨げられるため、Cisco UCS サーバは PNUOS を起動できません。 dbx_os ファイルは、オペレーティング システムによって追加された証明書を保持し、ロードを禁止する証明書を指定します。失敗の原因はセキュア ブート違反であり、次のエラー メッセージが表示されます。 `Invalid signature detected. Check secure boot policy in setup.`	4.3(3a)A
CSCwb47042	Cisco UCS 6300 FI シリーズから Cisco UCS 6500 FI シリーズへの移行中に、FC ストレージポートを設定するとエラーが発生し、FC ブレークアウトがサポートされていないことが示されます。	4.2(3i)A

リリース 4.2(3k) で解決済みの問題

次の警告は、リリース 4.2(3k) で解決されました。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwf83491	Cisco UCSX-I-9108-25G では、1 つの I/O ファブリック モジュール（IFM）が温度センサーデータの読み取りに失敗し、ファン速度が最大になり、GUI 要求に応答しなくなる。両方の IFM がスロットを正しく識別してオンラインに戻るようにするには、IFM 2 を再挿入し、オンラインに戻るのを待ってから、IFM 1 を再挿入します。	4.2(3b)A

不具合 ID	説明	影響を受ける最初のバンドル
CSCwb47181	ファームウェア バージョン4.2(1f) および Cisco カスタム VMWare ESXi OS を搭載した UCS Manager サーバーには、ホストインベントリ注釈がありません。一部のキーと値のペアは、ESXi 内の UCS ツールインベントリでは正しいものの、UCSM 管理対象オブジェクトで一致していないか、欠落しています。この問題を解決するには、Intersight からインベントリ収集を手動で開始します。	4.2(1f)
CSCwe35644	64GB DIMM（UCS-MR-X64G2RW）を搭載し、ADDDC が有効になっている Cisco UCS C シリーズおよび B シリーズM5 および M6 サーバーでは、Cisco UCS Manager からの障害のない単一の DIMMで複数の ECC が確認されます。	4.1(3e)B および C
CSCwf03588	Cisco UCS 6454 FI を搭載したセットアップでは、すべての IOM に次の障害が表示れます。 クリティカル `F1707` タイムスタンプ `6270802` `CMCLowMem`：詳細については、[正常性（`Health`）] タブを確認してください	4.2(2d)A
CSCwh65058	リリース4.2(1l) で動作する Cisco UCS 6454 FI では、リリース10.2(6)M 上の 93180YC-FX スイッチでFC （ファイバ チャネル）ポート チャネルを確立する際に問題が発生する可能性があります。 リンクがアクティブになるとすぐに、ポート チャネルが error-disabled ステートになる可能性があります。	4.2(1l)A
CSCwe38504	4.2(1)リリースで動作している Cisco UCS 6454 FI により、bladeAG の CPU 使用率のサージが 100% に急増し、プロセスが使用可能なメモリを使い果たします。 その結果、スタートアップにピア ファブリック インターコネクトがプログラムされなくなります。	4.2(1i)A
CSCwi76042	アップリンクと vNIC の両方で利用されている VLAN グループから VLAN を削除すると、vNIC の接続が瞬間的に失われ、ENM ピン接続障害エラーが表示されます。 vNIC は自動的に接続を復元し、再び動作可能になります。Cisco UCS Manager は、vNIC ステータスを **ダウン** として示し、ENM ピン接続送信元の障害に属性を特定します。	4.2(3e)A

不具合 ID	説明	影響を受ける最初のバンドル
CSCwj10758	Cisco UCS Managerリリース4.3(3)、4.3(2)、および4.2(3) では、LDAP、RADIUS、または TACACS を介して認証されたユーザーの SSH ログインが Cisco UCS 6500 および 6400 シリーズ FI で失敗するが、 Cisco UCS 6300 FI にはありません。 同じユーザーに対して現用系 HTTP/ HTTPS Web セッションまたは既存の SSHセッションがある場合、SSH ログインは成功します。この問題は、リモートで認証されたユーザーの GUI または Telnet ログインには影響しません。また、ローカルの Cisco UCS Manager ログイン情報を使用した SSH ログインにも影響しません。	4.2(3i)
CSCwj28369	Cisco UCS 6454 ファブリック インターコネクトで、高可用性（HA）ポリシーのリセット、特に Link Layer Discovery Protocol（LLDP）関連の問題が原因で障害が発生します。show system reset-reason で取得したシステム ログは、HA ポリシーにビア デバイスのリセットが自動的に実行されていることを確認します。	4.2(3j)
CSCwd35712	Cisco UCS Manager でインスタンス ID が見つからないというエラーにより、**データ管理エンジン（DME）**がクラッシュするという重大な不具合が確認されました。 その他の症状には、Cisco UCS Manager GUI にアクセス不能、クラスタ管理サービスが機能不全、SSH 経由の **show pmon state** コマンドでコア ダンプが表示されることが含まれます。 この問題はファームウェア固有ではなく、Cisco UCS Manager ドメインに影響を与える可能性があります。ドメインのデータ プレーンとサーバの操作に影響はありませんが、この問題に対する回避策はなく、影響を受ける環境にはバックアップから復元することを必要とする可能性があります。	4.2(1d)

リリース 4.2(3j) の解決済みの不具合

次の表は、リリース 4.2(3j) で解決された不具合を一覧表示します。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwf93621	Cisco UCS C240 M5SX サーバーでの ComputeRackUnitDiscover:OobStorageConfig プロセス中に、検出または関連付けがエラー メッセージ *Remote-Invocation-Error: Waiting for storage Subsystem to initialize* で失敗することがよくあります。この問題は、サーバー ファームウェアを 4.2(3d) にアップグレードした後に発生しました。 3.8TB または 7.6TB ドライブを使用するサーバーに影響を与えるようです。	4.2(3d)C
CSCwe96606	Cisco UCS 6454 ファブリック インターコネクト で *svc_sam_samcproxy* プロセス障害メッセージが表示されます。	4.2(3d)A
CSCwh86319	4.3(2.230117) バージョンで動作する Cisco UCS 6400 シリーズおよび 6500 シリーズ ファブリック インターコネクトでは、ストレージ領域の枯渇とファームウェア アップグレードの失敗という永続的な問題が確認されました。	4.3(2.230117)
CSCwd15750	Cisco UCS 6454 ファブリック インターコネクトを搭載したセットアップでは、自動インストール中にユーザーの承認なしに再起動します。この問題は、インフラストラクチャ ファームウェアのバージョン 4.1(3e)A からバージョン 4.2(1i)A へのアップグレード プロセス中に確認されました。	4.1(3e)A
CSCwe95417	Cisco UCS 6332-16UP ファブリック インターコネクトをインフラストラクチャ ファームウェア 4.2(2c)A にアップグレードした後、シャーシの電源チャートに異常な測定値が表示されます。	4.2(2c)A
CSCwe88483	マシン チェック例外（MCE）エラーにより、Cisco UCS 6454 ファブリック インターコネクトがクラッシュします。	4.2(2c)A
CSCwi54393	Linux OS を使用したセットアップでは、多数の SAN LUN とともに PXE ブートでブート時間を開始すると、一部の LUN がマウントされません。	4.1(3b)

リリース 4.2(3h) の解決済みの不具合

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	説明	影響を受ける最初のバンドル
CSCwf61835	Cisco UCS 15000 シリーズ VIC アダプタと ESXi OS を搭載したセットアップでは、アダプタが到達不能になり、ハング状態になることがあります。内部 PO がダウンし、バックプレーン接続リンクもリンク ダウンとして表示されます。すべての vNIC/vHBA もダウン状態です。	4.2 (2a)
CSCwf52054	Cisco UCS 2200/2300/2400 IOM は、リリース 4.2(3d) へのアップグレード後にオフラインになることがあります。	4.2(3d)
CSCwe98053	CRC エラーは、Cisco UCS B シリーズ サーバーの HIF ポートに接続された Cisco UCS 2408 IOM を搭載したセットアップで発生します。	4.2 (2a)
CSCwh15315	リリース 4.2(2a) 以降にアップグレードすると、サードパーティ製 SFP がサポート対象外の状態になります。	4.2 (2a)
CSCwf92065	SNMPD の再起動後に NXOS で SNMP 構成が復元されない。	4.2(2c)
CSCwf73403	Cisco UCS 6454 ファブリック インターコネクトでは、初期起動時または設定の消去後に、ファブリック インターコネクトが初期設定プロンプトで起動しませんでした。起動が完了すると、ファブリック インターコネクトにデフォルトのホスト名である switch のログインプロンプトが表示されます。	4.2(3b)

リリース 4.2(3g) の解決済みの不具合

次の表は、リリース 4.2(3g) で解決された不具合をリストします。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwe45912	Cisco UCS 6400 シリーズ FI または 6536 FI を使用したクラスタ設定では、サーバーのリブート後に、影響を受ける FI を介して MAC アドレスが学習されると、ARP はどの OS でも解決できません。この問題は、リブートされないサーバーには影響しません。	4.2(1i)

不具合 ID	説明	影響を受ける最初のバンドル
CSCwf05062	次のエラーにより、Cisco UCS 6454 FI がクラッシュして回復します。 `%SYSMGR-2-SERVICE_CRASHED: Service "mfdm" (PID 15518) hasn't caught signal 6 (core will be saved).%$ VDC-1 %$ %SYSMGR-2-HAP_FAILURE_SUP_RESET: Service "mfdm" in vdc 1 has had a hap failure`	4.2(1d)
CSCwf44680	Cisco UCS 6454 FI を搭載したセットアップでは、リンク層ブロードキャスト宛ての IP ユニキャスト/サブネット ブロードキャスト パケットが FI の Mgmt ポートを介して受信されると、パケットは Mgmt0 インターフェイスを介してルーティングされます。これにより、FI は Mgmt0 送信元 MAC アドレスを持つ受信パケットを送り返し、ネットワーク上のアップストリーム デバイスが異なる送信元 MAC アドレスを持つ同じ宛先 IP アドレスを検出します。	4.2(3e)

リリース 4.2(3e) で解決済みの問題

次の表は、リリース 4.2(3e) で解決された不具合を一覧表示します。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwe07549	CHAP 認証が有効になっている Intersight 管理モードのサーバでは、iSCSI LUN 検出が失敗します。 X210c M6 コンピューティング ノードは、チャレンジ ハンドシェイク認証プロトコル（CHAP）認証が有効になっている iSCSI プロファイルで構成されました。サーバを再起動すると、BIOS で iSCSI ブート LUN が見つかりません。iSCSI 構成の BIOS からの Intersight の iSCSI ブート プロファイルで CHAP が有効になっているにもかかわらず、認証モードが none として表示されることが検出されます。	4.2(1l)

リリース 4.2(3d) の解決済みの不具合

次の表は、リリース 4.2(3d) で解決された不具合を一覧表示します。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwd41247	Cisco UCS 6400 FI を搭載したセットアップでは、ハングした **Samcproxy** の複数のインスタンスが観察されます。また、**Samcproxy** の状態が悪いことに関連するその他の障害がドメインにある可能性もあります。	4.2(3c)
CSCwe24011	Cisco UCS 6536 FI および Cisco UCS 6400 FI シリーズ FI では、通常の操作中に予期しない再起動が発生します。	4.2(3c)
CSCwd90187	Cisco UCS 6536 FI を搭載したセットアップでは、次の条件下で QSFP-100G-DR/FR-S を QSFP-100G-CUxM に置き換えると、ポートが**リンク未接続**ステータスになります。 • 1 つの 100G インターフェイス。 • インターフェイスは **FEC Auto** で設定されています • インターフェイスは QSFP-100G-FR、QSFP-100G-DR トランシーバを使用していました。インターフェイスは QSFP-100G-CUxM を使用するようになりました。CUxM は CU1M、CU2M などを指します。	4.2(3c)
CSCwe28336	MTS バッファが vsh.bin プロセスでスタックします。 制限に達するとプロセスがクラッシュし、他の機能に影響を与えます。	4.2(3c)
CSCwe28336	Cisco UCS 6400 FI を備えたセットアップでは、マルチキャスト ストリームはサーバによって受け入れられません。	4.2(3c)

リリース 4.2（3c）内の解決済みの不具合

次の表は、リリース 4.2(3c) で解決された不具合をリストします。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwd86029	インフラストラクチャ ファームウェアを 4.2(1d) から 4.2(2a)、4.2(3b)、または 4.2(3c) リリースにアップグレードしているときに、2 つの IFM アップグレードの間にタイム ラグがある場合、このタイム インターバルにいずれかの IFM で Redfish クエリが失敗します。IMM での接続障害として表示される場合があります。	4.2(2c)

リリース 4.2（3b）の解決済みの問題

次の表は、リリース 4.2(3b) で解決された不具合をリストします。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwd37309	UCS X シリーズ シャーシで、ファン UCSX-9508-FAN を使用すると、「[シャーシ ファン モジュール] に重大な速度しきい値状態があります」というアラートが表示されます。この動作は、複数のシャーシで発生する場合があり、異なるファン モジュールで発生する場合があります。障害が発生し、独自にクリアされます。この問題は、ファン速度が LOW の状態で検出されます。障害が解決せず、自然に解決しない場合は、ファンを物理的に取り付け直します。再装着後も障害が続く場合は、別の問題が発生している可能性があるため、Cisco TAC に連絡してください。	4.2(1l)

リリース 4.2(2d) で解決済みの問題

次の表は、リリース 4.2(2d) で解決された不具合をリストします。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwd37309	UCS X シリーズ シャーシで、ファン UCSX-9508-FAN を使用すると、「[シャーシ ファン モジュール] に重大な速度しきい値状態があります」というアラートが表示されます。この動作は、複数のシャーシで発生する場合があり、異なるファン モジュールで発生する場合があります。障害が発生し、独自にクリアされます。この問題は、ファン速度が LOW の状態で検出されます。障害が解決せず、自然に解決しない場合は、ファンを物理的に取り付け直します。再装着後も障害が続く場合は、別の問題が発生している可能性があるため、Cisco TAC に連絡してください。	4.2(1l)

リリース 4.2(1n) で解決済みの問題

次の表は、リリース 4.2(1n) で解決済みの問題のリストです。

不具合 ID	説明	影響を受ける最初のバンドル
CSCwb90201	Cisco UCS 6500 シリーズ FI では、アップリンク ポートの追加メンバー ポートがブロードキャスト トラフィックの転送に失敗します。これは、Fibre Channel over Ethernet（FCoE）メンバー ポートがアップリンク ポートに正しく含まれていないために発生します。	4.2(1l)

不具合 ID	説明	影響を受ける最初のバンドル
CSCwb00770	Cisco UCS 6500 シリーズ FI では、ファブリック ポートが UDP ポート範囲 100～150 のユニキャスト トラフィックを転送できません。	4.2(1l)
CSCwb43580	QSFP-40G-LR4 ステータスの FI スイッチ リンクは、リモート エンド ポートをシャットダウンするかケーブルを抜いた後でも、1 分以上アップとして表示されます。FI スイッチは、Cisco 1400 シリーズ アダプタを使用して C シリーズ サーバーに接続されています。	4.2(1l)
CSCwb07198	Cisco UCS 6500 シリーズ FI の場合、アプライアンス サーバーから FI に 1 つの igmp join のみを送信する場合でも、Syslog に IGMP 16k 制限通知が表示されます。	4.2(1l)
CSCwb73274	ファブリック フェールオーバー中の IP マルチキャスト トラフィックでは、100 秒を超えるコンバージェンス時間が観察されます。これは、FI 上の 3K VLAN およびスヌープが有効になっている N9K がすべての VLAN で構成されている場合に観察されます。異なる VLAN の N9K に 5 つを超えるクエリア構成されています。3 つのグループは、異なるホスト/サーバーからの異なる VLAN に参加しています。	4.2(1l)
CSCwb78536	FI の再起動後、ファイバー チャネル ストレージ ポートが Init でスタックします。ポートは 32G Netapp に接続されており、ファブリック インターコネクト B のリブート前に FCoE トラフィックがポートに送信されます。	4.2(1l)
CSCwb64509	FC アップリンク ポートとブレークアウト インターフェイスを有効にした後に FI を再起動すると、snmpd_log コアが影響を受けます。	4.2(1l)

リリース 4.2(1n) で解決済みの問題

次の表は、リリース 4.2(1l) 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
CSCvz92352	インテリジェント ファブリック管理（IFM）で、シャーシの電源ユニットの障害が原因で再起動ループが発生します。障害のある PSU は、PSU LED が緑色に点灯していないことで示されます。	4.2 (2a)

未解決の不具合

リリースで未解決の問題 4.2(3m)

次の問題がリリース 4.2(3m) 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ージョン
CSCwn65484	ファブリック インターコネクト（FI）によっては、FCOE_NPV_PKG ライセンスが見つからないという警告が記録されますが、FCoE 機能は名義ベースのライセンスの下で正常に動作し続けます。	回避策はありません。	4.3 (3a)

リリース 4.2(3l) で未解決の不具合：なし

リリース 4.2(3k) の未解決の問題：なし

リリース 4.2(3c) の未解決の不具合

リリース 4.2(3c) では、次の問題が未解決です。

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCwd52370	UCS-IOM-2408 を使用して UCSB-5108-AC2 シャーシのファブリック インターコネクトのファームウェアをアップグレードすると、Intersight への接続が失われます。 ポート フラップにより、CMC はシャーシ情報を設定解除し、有用な情報が /var/isconfig から削除されます。シャーシ情報が再度設定されると、CMC DC はデータが再度読み込まれた後に /var/isconfig ファイルを再読み取りしない場合があり、CMC が Intersight から切断されます。	CMC DC を再起動します（/etc/init.d/dc 再起動）	4.2(2c)

リリース 4.2(2a) で未解決の問題

リリース 4.2(2a) では、次の問題が未解決です。

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCwd82136	Cisco VIC 1457/1455/1467 を使用して Cisco UCS C シリーズ サーバーに接続された Cisco UCS 6400 シリーズ FI を備えたセットアップでは、リンクフラップの後、FI のポートが **errDisabledExcessportIn** 理由でエラー ディセーブル状態になることがあります。	Cisco UCS C シリーズ サーバーに接続されている FI ポートをフラップします。	4.2 (2a)

不具合 ID	症状	回避策	影響を受ける最初のバンドル
CSCwd90187	Cisco UCS 6536 FI を搭載したセットアップでは、次の条件下で QSFP-100G-DR/FR-S を QSFP-100G-CUxM に置き換えると、ポートが**リンク未接続**ステータスになります。 • 1 つの 100G インターフェイス。 • インターフェイスは **FEC Auto** で設定されています • インターフェイスは QSFP-100G-FR、QSFP-100G-DR トランシーバを使用していました インターフェイスは QSFP-100G-CUxM を使用するようになりました。CUxM は CU1M、CU2M などを指します。	この問題には 2 つの回避策があります。 • 次の操作を行ってください。 1. FEC 機能のない光または AOC トランシーバを挿入します。たとえば、インターフェイス上の QSFP-100G-SR または QSFP-100G-AOC3M。 2. ステップ 1 のトランシーバを取り外します。 3. パッシブ銅ケーブルを挿入し直します。 • FI を再起動します。	4.2 (2a)

関連資料

リリース ノート

- Cisco Intersight のリリース ノートとリリース バンドル

- 『Release Notes for Cisco UCS Manager』
- Cisco Integrated Management Controller のリリース ノート

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。