Cisco UCS C シリーズ Integrated Management Controller リリース 4.3 GUI コンフィギュレーション ガイド

初版：2023 年 2 月 16 日

最終更新：2023 年 5 月 18 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次

はじめに

この前書きは、次の項で構成されています。

対象読者

このガイドは、次の 1 つ以上に責任を持つ、専門知識を備えたデータセンター管理者を主な対象にしています。

- サーバ管理
- ストレージ管理
- ネットワーク管理
- ネットワーク セキュリティ

表記法

テキストのタイプ	説明
GUI 要素	タブの見出し、領域名、フィールドのラベルのような GUI 要素は、**[GUI 要素]** のように示しています。 ウィンドウ、ダイアログボックス、ウィザードのタイトルのようなメイン タイトルは、[メイン タイトル] のように示しています。
マニュアルのタイトル	マニュアルのタイトルは、イタリック体（*italic*）で示しています。
TUI 要素	テキストベースのユーザ インターフェイスでは、システムによって表示されるテキストは、`courier` フォントで示しています。

テキストのタイプ	説明
システム出力	システムが表示するターミナル セッションおよび情報は、courier フォントで示しています。
CLI コマンド	CLI コマンドのキーワードは、**this font**で示しています。 CLI コマンド内の変数は、このフォント で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

ヒント 「問題解決に役立つ情報」です。ヒントには、トラブルシューティングや操作方法ではなく、ワンポイントアドバイスと同様に知っておくと役立つ情報が記述される場合もあります。

ワンポイント アドバイス 「時間の節約に役立つ操作」です。ここに紹介している方法で作業を行うと、時間を短縮できます。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

警告 安全上の重要事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。

これらの注意事項を保管しておいてください。

Cisco UCS の関連資料

ドキュメント ロードマップ

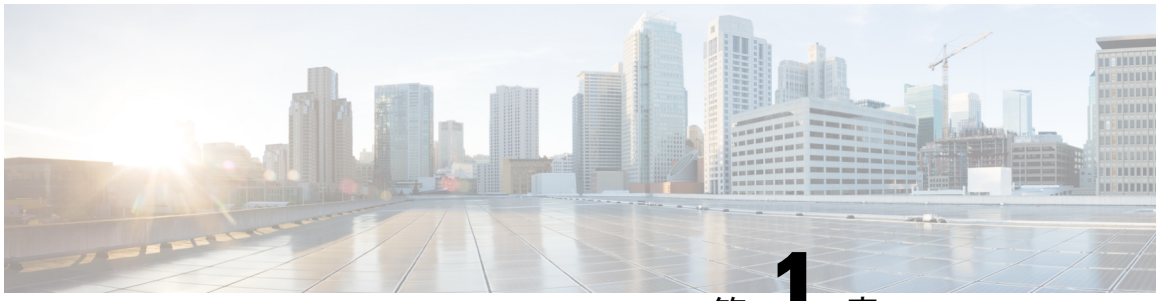
すべての B シリーズ マニュアルの完全なリストについては、次の URL で入手可能な『*Cisco UCS B-Series Servers Documentation Roadmap*』を参照してください。https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_roadmap.html

すべての C-Series マニュアルの完全なリストについては、次の URL で入手可能な『『*Cisco UCS C-Series Servers Documentation Roadmap*』』を参照してください。https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/ucs_rack_roadmap.html

管理用の UCS Manager に統合されたラック サーバでサポートされるファームウェアと UCS Manager のバージョンについては、『Release Bundle Contents for Cisco UCS Software』[英語] を参照してください。

その他のマニュアル リソース

ドキュメントの更新通知を受け取るには、Cisco UCS Docs on Twitter をフォローしてください。



第 1 章

概要

この章は、次の内容で構成されています。

Cisco UCS C シリーズ ラックマウント サーバの概要

Cisco UCS C シリーズ ラックマウント サーバーには、次のモデルがあります。

- Cisco UCS C220 M7 ラックマウス サーバー
- Cisco UCS C240 M7 ラックマウス サーバー
- Cisco UCS C220 M6 ラックマウント サーバー
- Cisco UCS C240 M6 ラックマウント サーバー
- Cisco UCS C225 M6 ラックマウント サーバー
- Cisco UCS C245 M6 ラックマウント サーバー
- Cisco UCS C240 SD M5 ラックマウント サーバ
- Cisco UCS C220 M5 ラックマウント サーバー
- Cisco UCS C240 M5 ラックマウント サーバー
- Cisco UCS C480 M5 ラックマウント サーバー
- Cisco UCS C220 M4 ラックマウント サーバー
- Cisco UCS C240 M4 ラックマウント サーバ

- Cisco UCS C3160 ラックマウント サーバ
- Cisco UCS C460 M4 ラックマウント サーバー
- Cisco UCS C125 ラックマウント サーバー
- Cisco UCS C220 M5 ラックマウント サーバー
- Cisco UCS C240 M5 ラックマウント サーバー
- Cisco UCS C480 M5 ラックマウント サーバー
- Cisco UCS C220 M4 ラックマウント サーバー
- Cisco UCS C240 M4 ラックマウント サーバー
- Cisco UCS C460 M4 ラックマウント サーバー

（注） このファームウェア リリースでサポートされている Cisco UCS C シリーズ ラック マウント サーバーを確認するには、関連するリリース ノートを参照してください。 Cシリーズのリリース ノートは、次の URL にあります。
http://www.cisco.com/en/US/products/ps10739/prod_release_notes_list.html

サーバ ソフトウェアの概要

Cisco UCS C シリーズ ラックマウント サーバには、Cisco IMC ファームウェアが付属しています。

Cisco IMC ファームウェア

Cisco IMC は、マザーボードに組み込まれている独立した管理モジュールです。専用の ARM ベースのプロセッサが、メイン サーバ CPU とは別に、Cisco IMC ファームウェアを実行します。システムには Cisco IMC ファームウェアの実行バージョンが付属しています。Cisco IMC ファームウェアは更新できますが、初期インストールは必要ではありません。

サーバ OS

Cisco UCS C シリーズ ラック サーバは、Windows、Linux、Oracle などのオペレーティング システムをサポートします。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、スタンドアロン *C* シリーズ サーバのハードウェアおよびソフトウェア相互運用性（http://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html）を参照してください。KVM コンソールおよび vMedia を使ってサーバに OS をインストールするために、Cisco IMC を使用できます。

（注） 使用可能な OS のインストール マニュアルには、http://www.cisco.com/go/unifiedcomputing/c-series-doc の『*Cisco UCS C-Series Servers Documentation Roadmap*』からアクセスできます。

サーバ 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 *1*：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
Andromeda Management ポート	8889
Andromeda クラウド ポート	8888
SOL SSH ポート	2400
SNMPポート	161
SNMP トラップ	162
外部Syslog	514

Cisco Integrated Management Controller

Cisco IMC は、C シリーズ サーバー用の管理サービスです。Cisco IMC はサーバー内で動作します。

（注） Cisco IMC 管理サービスは、サーバーがスタンドアロン モードで動作している場合にだけ使用されます。C シリーズ サーバが UCS システムに統合されている場合は、UCS Manager を使用してそのサーバを管理する必要があります。UCS Manager の使用方法については、http://www.cisco.com/go/unifiedcomputing/b-series-doc の『*Cisco UCS B-Series Servers Documentation Roadmap*』にリストされた設定ガイドを参照してください。

管理インターフェイス

Web ベースの GUI または SSH ベースの CLI または XML ベースの API を使用して、サーバにアクセスし、サーバを設定、管理、モニタできます。ほとんどのタスクがいずれかのインターフェイスを使用して実行できます。また、一方のインターフェイスで実行されたタスクの結果を、他方のインターフェイスに表示することができます。ただし、次の操作はできません。

- Cisco IMC CLI を呼び出すために Cisco IMC GUI を使用する
- Cisco IMC CLI で呼び出したコマンドを Cisco IMC GUI に表示する
- Cisco IMC GUI から Cisco IMC CLI 出力を生成する

Cisco IMC で実行可能なタスク

Cisco IMC を使用すると次のシャーシ管理タスクを実行できます。

- サーバーの電源のオン、電源のオフ、電源再投入、リセット、およびシャットダウンを行う
- ロケータ LED を切り替える
- サーバーのブート順を設定する
- サーバのプロパティとセンサーの表示
- リモート プレゼンスの管理
- ローカル ユーザ アカウントの作成と管理、および Active Directory を経由したリモート ユーザ認証の有効化
- NIC プロパティ、IPv4、VLAN、ネットワーク セキュリティなど、ネットワーク関連の設定を行う
- HTTP、SSH、IPMI Over LAN、SNMP などのコミュニケーション サービスを設定する
- 証明書を管理する

- プラットフォーム イベント フィルタを設定する
- Cisco IMC ファームウェアを更新する
- 障害、アラーム、およびサーバのステータスのモニタ
- タイム ゾーンの設定と現地時刻の確認
- Cisco IMC ファームウェアをインストールしてアクティブにする
- BIOS ファームウェアをインストールしてアクティブにする
- CMC ファームウェアをインストールしてアクティブにする

Cisco IMC を使用すると次のサーバー管理タスクを実行できます。

- リモート プレゼンスの管理
- ローカル ユーザ アカウントの作成と管理、および Active Directory を経由したリモート ユーザ認証の有効化
- NIC プロパティ、IPv4、VLAN、ネットワーク セキュリティなど、ネットワーク関連の設定を行う
- HTTP、SSH、IPMI Over LAN、SNMP などのコミュニケーション サービスを設定する
- 証明書を管理する
- プラットフォーム イベント フィルタを設定する
- Cisco IMC ファームウェアを更新する
- 障害、アラーム、およびサーバのステータスのモニタ
- タイム ゾーンの設定と現地時刻の確認

オペレーティング システムやアプリケーションのプロビジョニングや管理はできない

Cisco IMC はサーバーのプロビジョニングを行うため、サーバーのオペレーティング システムの下に存在します。したがって、サーバでのオペレーティング システムやアプリケーションのプロビジョニングおよび管理には、これを使用できません。たとえば、次の操作を実行することはできません。

- Windows や Linux などの OS の展開
- OS やアプリケーションなどのソフトウェアに対するパッチの展開
- アンチウイルス ソフトウェア、モニタリング エージェント、バックアップ クライアントなどのベース ソフトウェア コンポーネントのインストール
- データベース、アプリケーション サーバ ソフトウェア、Web サーバなどのソフトウェア アプリケーションのインストール

- Oracle データベースの再起動、プリンタ キューの再起動、または Cisco IMC 以外のユーザー アカウントの処理を含むオペレータ処理の実行
- SAN や NAS ストレージ上の外部ストレージの設定または管理

Cisco IMC ユーザー インターフェイスの概要

Cisco IMC ユーザー インターフェイスは、Cisco C シリーズ サーバーの Web ベースの管理インターフェイスです。この Web ユーザ インターフェイスは HTML5 および eXtensible Widget Framework（XWT）フレームワークを使用して開発されました。ユーザーインターフェイスを起動して、次の最小要件を満たしている任意のリモート ホストからサーバーを管理できます。

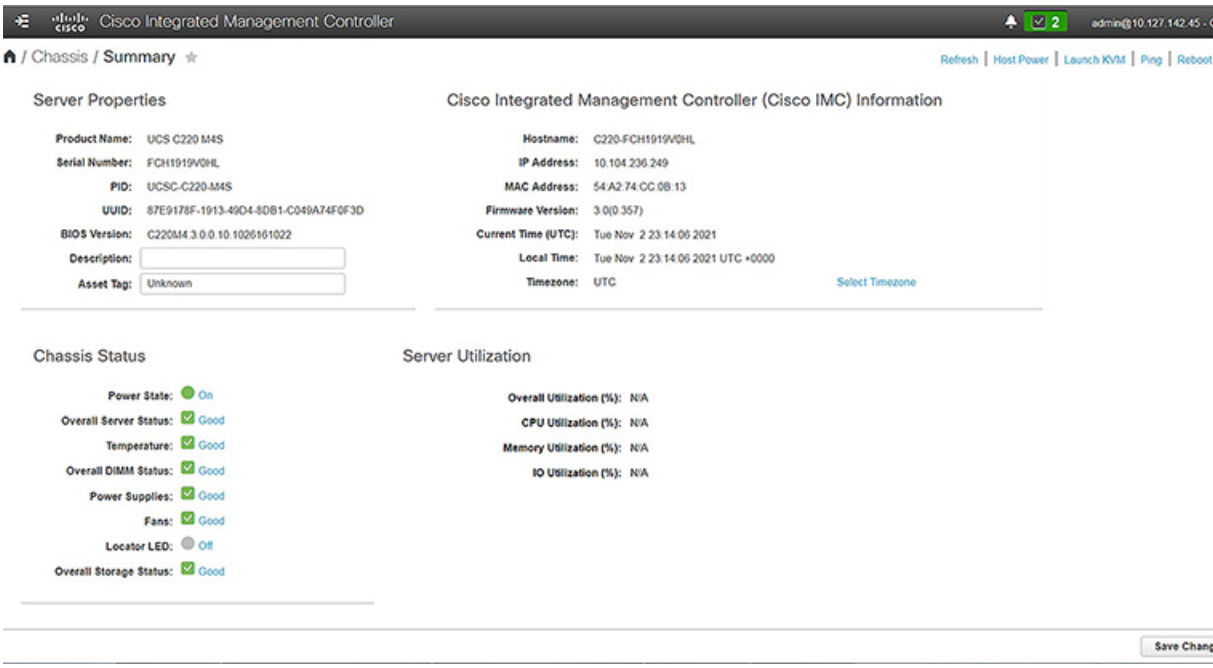
- Microsoft Internet Explorer 6.0 以降、Mozilla Firefox 3.0 以降
- Microsoft Windows 7、Microsoft Windows XP、Microsoft Windows Vista、Apple Mac OS X v10.6、Red Hat Enterprise Linux 5.0 以降のオペレーティング システム
- Transport Layer Security（TLS）バージョン 1.3

（注） Cisco IMC へのログインに使用するパスワードを失効した場合やパスワードを忘れた場合は、使用しているサーバーの Cisco UCS C シリーズ サーバーのインストレーションおよびサービス ガイドでパスワードの回復手順を参照してください。このガイドは http://www.cisco.com/go/unifiedcomputing/c-series-doc の『*Cisco UCS C-Series Servers Documentation Roadmap*』から入手できます。

Cisco IMC のホームページ

Cisco IMC GUI に初めてログインすると、次の図のようなユーザー インターフェイスが表示されます。

（注） リリースごとに機能に影響を与えないユーザー インターフェイスの変更がある場合があります。



[ナビゲーション（Navigation）] ペインと [作業（Work）] ペイン

Cisco Integrated Management Controller GUI は、画面の左側にある [Navigation] ペインと、画面の右側にある [Work] ペインで構成されます。[ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）]、[コンピューティング（Compute）]、[ネットワーク（Networking）]、[ストレージ（Storage）]、または [管理者（Admin）] メニューにあるリンクをクリックすると、右側のペインに関連付けられたタブが表示されます。

[Navigation] ペインのヘッダーにはアクション ボタンが表示され、GUI 全体のナビゲーション マップを表示したり、インデックスを表示したり、お気に入りの作業ペインを選択して直接移動したりできます。[ピン（Pin）] アイコンを使用すると、作業ペインが表示された際、ナビゲーション ペインが隠れません。

[お気に入り（Favorite）] アイコンは星形のボタンで、アプリケーションの特定の作業ペインをお気に入りとして設定することができます。これを行うには、選択する作業ペインに移動し、[お気に入り（Favorite）] アイコンをクリックします。アプリケーションの他の場所からこの作業ペインに直接アクセスするには、[お気に入り] アイコンを再度クリックします。

GUI ヘッダーには、シャーシの全体的なステータスに関する情報およびユーザー ログイン情報が表示されます。

GUI ヘッダーの右側に歯車アイコンがあります。歯車アイコンをクリックすると、ドロップダウンに [パスワードの変更（Change Password）] および [ログアウト（Logout）] オプションがリストされます。[パスワードの変更（Change Password）] オプションを使用してパスワードを変更できます。

（注） パスワードを変更すると、Cisco IMC からログアウトされます。

（注） [パスワードの変更（Change Password）] オプションは、admin としてログインしているときには使用できません。読み取り専用の権限をもつ設定済みのユーザーのパスワードだけが変更できます。

パスワードを変更すると、Cisco IMC からログアウトされます。

[ログアウト（Logouot）] オプションで、Cisco IMC からログアウトできます。

GUI ヘッダーには、障害の総数（緑色または赤色で示されます）も表示され、その横に [Bell] アイコンが付いています。ここで、このアイコンをクリックすると、さまざまなコンポーネントの致命的または重大な障害のサマリのみが表示されます。すべての障害を表示するには、[すべて表示（View All）] ボタンをクリックして、[障害サマリ（Fault Summary）] ペインを表示します。

（注） ユーザ インターフェイスのオプションはサーバによって異なります。

[ナビゲーション（Navigation）] ペインには次のメニューがあります。

- [シャーシ（Chassis）] メニュー
- [コンピューティング（Compute）] メニュー
- [ネットワーキング（Networking）] メニュー
- [ストレージ（Storage）] メニュー
- [管理者（Admin）] メニュー

[Chassis] メニュー

[シャーシ (Chassis)] メニューの各ノードは、**[作業 (Work)]** ペインに表示されるペインに表示される 1 つ以上のタブ **([サマリー (Summary)]** ペインを除く) に続きます。これらのタブからは次の情報へアクセスできます。

[Chassis] メニューのノード名	[作業 (Work)] ペインのタブで提供される情報
要約	サーバプロパティ、シャーシステータス、Cisco Integrated Management Controller (Cisco IMC) 情報、およびサーバ使用率。 （注） サーバー使用率は、一部の Cisco UCS C シリーズ サーバーで使用できます。

[Chassis] メニューのノード名	[作業 (Work)] ペインのタブで提供される情報
Inventory	CPU、メモリ、PCI アダプタ、電源装置、Cisco VIC アダプタ、ネットワーク アダプタ、ストレージ、SAS エクスパンダ、および TPM。
Sensor	電源装置、ファン、温度、電圧、電流、LED、およびストレージ。
電源管理	電力制限の構成と電源モニタリング。 （注） このオプションは、Cisco UCS C125、C245 M6、および C225 M6 サーバーでは使用できません。
Faults and Logs	障害サマリー、障害履歴、システムイベントログ、Cisco IMC ログおよびロギング制御。

[Compute] メニュー

[コンピューティング（Compute）] メニューにはサーバに関する情報が含まれ、作業ペインに次の情報が表示されます。

[コンピューティング（Compute）] メニューのノード名	[作業（Work）] ペインタブは、次のことに関する情報を提供します。
BIOS	インストールされている BIOS ファームウェア バージョンと BIOS プロファイル構成、サーバのブート順序設定、I/O、サーバ管理、セキュリティ、プロセッサ、メモリ、電源、またはパフォーマンス。
Remote Management	LAN 設定上の KVM、仮想メディア、およびシリアル。
トラブルシューティング	ブート ストラップ プロセスの録音アクションには、[録音の再生 (Play Recording)] と [録音のダウンロード (Download Recording)] が含まれ、[クラッシュの録音 (Crash Recording)] アクションには、[録音の再生 (Play Recording)]、[録音のキャプチャ (Capture Recording)]、および [録音のダウンロード (Download Recording)] が含まれます。
Power Policies	電源復元ポリシーの設定。
PID カタログ	CPU、メモリ、PCI アダプタ、および HDD の詳細。
セキュアなキー管理	KMIP サーバの詳細、KMIP ルート CA およびクライアント証明書の詳細、KMIP ログインの詳細、KMIP クライアント秘密キーのステータス

[Networking] メニュー

[ネットワーキング（Networking）] メニューの各ノードは、作業ペインに表示される 1 つ以上のタブにリンクします。これらのタブは次の情報へのアクセスを提供します。

[ネットワーキング（Networking）] メニューのノード名	[作業（Work）] ペイン タブは、次のことに関する情報を提供します。
General	アダプタ カードのプロパティ、ファームウェア、外部イーサネットインターフェイス、設定をエクスポートまたはインポートするアクション、リセット ステータス。
External Ethernet Interfaces	ポート、管理速度、MAC アドレス、リンクステートなどの外部イーサネット インターフェイス情報。
vNIC	名前、CDN、MAC アドレス、MTU、および個々の vNIC プロパティなどのホストイーサネットインターフェイス情報。
vHBA	名前、WWPN、WWNN、ブート、アップリンク、ポート プロファイル、チャネル番号、および個々の vHBA プロパティなどのホスト ファイバ チャネル インターフェイス情報。

[Storage] メニュー

[ストレージ（Storage）] メニューの各ノードは、Cisco UCS C シリーズ ラックマウント サーバにインストールされた LSI MegaRAID コントローラまたはホスト バス アダプタ（HBA）に対応します。各ノードは、[Work] ペインに表示される 1 つ以上のタブに続き、インストールされているコントローラに関する情報を提供します。

[ストレージ（Storage）] メニューのノード名	[作業（Work）] ペイン タブは、次のことに関する情報を提供します。
[コントローラ情報（Controller Info）]	選択した LSI MegaRAID コントローラまたは HBA に関する一般的な情報。
[物理ドライブ情報（Physical Drive Info）]	一般的なドライブ情報、RAID 情報、物理ドライブ情報。
Virtual Drive Info	一般的なドライブ情報、RAID 情報、物理ドライブ情報。
Battery Backup Unit	選択された MegaRAID コントローラのバックアップ バッテリ情報。
Storage Log	ストレージ メッセージ。

[管理者（Admin）] メニュー

[管理者（Admin）] メニューの各ノードは、作業ペインに表示される 1 つ以上のタブにリンクします。これらのタブは次の情報へのアクセスを提供します。

[管理者（Admin）] メニューのノード名	[作業（Work）] ペイン タブは、次のことに関する情報を提供します。
[ユーザー管理（User Management）]	ローカルユーザー管理、LDAP、およびセッション管理。
ネットワーキング	ネットワーク、ネットワーク セキュリティ、および NTP 設定。
コミュニケーション サービス	[通信サービス (Communication Services)] タブには、HTTP、SSH、XML API、Redfish のプロパティ、IPMI over LAN のプロパティ、[SNMP] タブには [SNMPのプロパティ (SNMP Properties)]、[ユーザー設定 (User Settings)]、[トラップ接続先 (Trap Destinations)]が含まれ、[メール アラート (Mail Alert)] タブには SNTP のプロパティと SMTP 受信者が含まれます。
セキュリティ管理	証明書の管理とセキュリティ構成。
[Event Management]	プラットフォーム イベント フィルタのリスト
Firmware Management	Cisco IMC および BIOS ファームウェア情報と管理。
ユーティリティ	リモートおよびローカル ダウンロードへのテクニカル サポート データ収集のエクスポート、システム設定のインポートおよびエクスポート オプション、NMI ホストへの生成、工場出荷時のデフォルト設定の復元、Cisco IMC バナーの追加または更新、インベントリ データの生成、リモートへのハードインベントリ データのエクスポート、PID カタログのアップロード、セキュア アダプタの更新を有効または無効にします。
デバイス コネクタ	Intersight 管理およびネットワーク設定。

ツールバー

ツールバーは [Work] ペインの上に表示されます。

ボタン名	説明
[更新（Refresh）]	現在のページを更新します。
Host Power	電源オプションを選択するためのドロップダウン メニューが表示されます。

ボタン名	説明
Launch KVM	[Launch KVM] ポップアップ ウィンドウを起動します。
ping	[ping の詳細（Ping Details）] ポップアップ ウィンドウが表示されます。
Reboot	Cisco IMC をリブートできます。
[ロケータ LED（Locator LED）]	ロケータ LED をオンまたはオフにできます。

Cisco Integrated Management Controller オンライン ヘルプの概要

Cisco Integrated Management Controller（Cisco IMC）ソフトウェアの GUI は、左側にある [ナビゲーション（Navigation）] ペインと右側にある [ワーク（Work）] ペインの 2 つの主要なセクションに分かれています。

このヘルプ システムは、各 Cisco IMC GUI ページと各ダイアログボックスのフィールドについて説明します。

ページのヘルプにアクセスするには、次のいずれかを実行します。

- Cisco IMC GUI の特定のタブで、[ワーク（Work）] ペインの上のツールバーにある [ヘルプ（Help）] アイコンをクリックします。
- ダイアログボックスで、そのダイアログボックスの [Help] ボタンをクリックします。

（注） C シリーズのすべてのマニュアルの一覧については、次の URL から入手できる『*Cisco UCS C-Series Servers Documentation Roadmap*』を参照してください。 URL: http://www.cisco.com/go/unifiedcomputing/c-series-doc

Cisco IMC へのログイン

手順

ステップ 1 Web ブラウザで、Cisco IMC への Web リンクを入力または選択します。

ステップ 2 セキュリティ ダイアログボックスが表示された場合は、次の操作を実行します。

a) （任意）チェックボックスをオンにして、シスコからのすべてのコンテンツを受け入れます。

b) **[Yes]**をクリックして証明書を受け入れ、続行します。

ステップ 3 ログイン ウィンドウで、ユーザ名とパスワードを入力します。

ヒント　未設定のシステムに対する初回ログイン時には、ユーザー名に**admin**、パスワードに **password** を使用します。

Web UI に初めてログインする際、次のようになります。

- Cisco IMC Web UI または CLI でデフォルトの管理者クレデンシャルを変更するまでは、操作を実行できません。
- パスワードの変更ポップアップ ウィンドウを閉じたりキャンセルしたりすることはできません。UI をタブで開くか、ブラウザ ページを更新すると、ポップアップ ウィンドウが引き続き表示されます。このポップアップ ウィンドウは、初期設定へのリセット後にログインすると表示されます。
- 新しいパスワードとして単語「password」を選択することはできません。スクリプトを実行する際にこのことが問題になる場合は、ユーザ管理オプションにログインし直すことによって、それをパスワードに変更することができますが、これは完全に自己責任において実行するようにしてください。シスコでは推奨していません。

ステップ 4　[Log In] をクリックします。

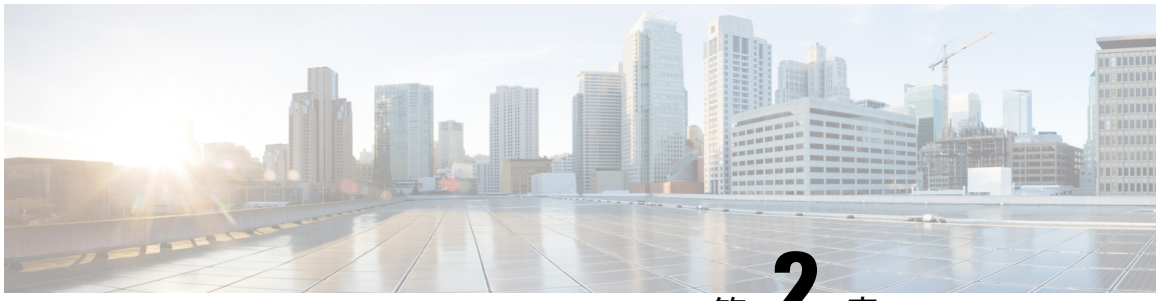
Cisco IMC からのログアウト

手順

ステップ 1　Cisco IMC の右上にある歯車アイコンをクリックし、ドロップダウンリストから **[ログアウト (Log Out)]** をクリックします。

ログアウトすると、Cisco IMC のログイン ページに戻ります。

ステップ 2　（任意） 再度ログインするか、Web ブラウザを閉じます。



第 2 章

サーバー OS のインストール

この章は、次の内容で構成されています。

OS のインストール方法

C シリーズ サーバは、複数のオペレーティング システムをサポートしています。インストールされている OS に関係なく、次のいずれかのツールを使用してサーバにインストールできます。

- KVM コンソール
- PXE インストール サーバ

Cisco UCS サーバ構成ユーティリティに関する詳細情報については、『Cisco UCS サーバ構成ユーティリティ ユーザー ガイド』を参照してください。

仮想 KVM コンソール

vKVM コンソールは Cisco IMC からアクセス可能なインターフェイスであり、サーバへのキーボード、ビデオ、マウス（vKVM）の直接接続をエミュレートします。vKVM コンソールを使用すると、リモートの場所からサーバに接続できます。

Cisco KVM コンソールを使用する主な利点は次のとおりです。

- Cisco KVM コンソールは KVM、SOL、および vMedia への接続を提供しますが、Avocent KVM は KVM および vMedia への接続のみを提供します。
- KVM コンソールでは、vMedia 接続が KVM 起動マネージャで確立され、すべてのユーザーが使用できます。

- KVM コンソールには、ゲストからホストにテキストを貼り付ける際に、サポートされていない文字の高度な文字置換オプションが用意されています。
- KVM コンソールには、CIMC に vMedia マッピングを保存する機能があります。

サーバに物理的に接続された CD/DVD ドライブまたはフロッピー ドライブを使用する代わりに、vKVM コンソールは仮想メディアを使用します。これは、仮想 CD/DVD ドライブまたはフロッピー ドライブにマップされる実際のディスク ドライブまたはディスク イメージ ファイルです。次のいずれでも仮想ドライブにマップできます。

- コンピュータ上の CD/DVD またはフロッピー ドライブ
- コンピュータ上のディスク イメージ ファイル（ISO または IMG ファイル）
- コンピュータ上の USB フラッシュ ドライブ
- ネットワーク上の CD/DVD またはフロッピー ドライブ
- ネットワーク上のディスク イメージ ファイル（ISO または IMG ファイル）
- ネットワーク上の USB フラッシュ ドライブ

vKVM コンソールを使用してサーバに OS をインストールできます。

KVM コンソールを使用した OS のインストール

（注） この手順では、基本的なインストール手順についてのみ説明します。Linux、VMware、および Windows のインストールの詳細なガイドについては、次の URL を参照してください。
http://www.cisco.com/en/US/products/ps10493/products_installation_and_configuration_guides_list.html

始める前に

- OS インストール ディスクまたはディスク イメージ ファイルを見つけます。
- OS をインストールするには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 OS インストール ディスクを CD/DVD ドライブにロードするか、ディスク イメージ ファイルをコンピュータにコピーします。

ステップ 2 Cisco IMC が開いていない場合は、ログインします。

ステップ 3 [ナビゲーション（Navigation）]ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 4 **[コンピューティング（Compute）]**メニューでサーバを選択します。

ステップ 5 作業ウィンドウで **[**リモート管理（**Remote Management**）**]**タブをクリックします。

ステップ 6 [Remote Management] ペインで、[Virtual KVM] タブをクリックします。

ステップ 7 [Actions] 領域で、[Launch KVM Console] をクリックします。

[KVM Console] が別ウィンドウで開きます。

ステップ 8 KVM コンソールから、[VM] タブをクリックします。

ステップ 9 [VM] タブで、次のいずれかの方法を使用して仮想メディアをマップします。

- OS インストール ディスクが含まれている CD/DVD ドライブの [Mapped] チェックボックスをオンにします。
- [Add Image] をクリックし、OS インストール ディスク イメージに移動してこれを選択します。[Open] をクリックしてディスク イメージをマウントし、マウントされたディスク イメージの [Mapped] チェックボックスをオンにします。

（注） OS のインストール プロセスの間は、[VM] タブを開いたままにしておく必要があります。このタブを閉じると、すべての仮想メディアのマップが解除されます。

ステップ 10 サーバをリブートし、ブート デバイスとして仮想 CD/DVD ドライブを選択します。

サーバを再起動すると、仮想 CD/DVD ドライブからインストール プロセスが開始します。残りのインストール プロセスについては、インストールしている OS のインストレーション ガイドを参照してください。

次のタスク

OS のインストールが完了したら、LAN のブート順を元の設定にリセットします。ソフトウェアの相互運用性とドライバの互換性を含め、常に OS ベンダ推奨の設定に従うようにします。ドライバの推奨事項とインストールについて詳しくは、こちらの Cisco UCS ハードウェア互換性リストに従ってください。

https://ucshcltool.cloudapps.cisco.com/public/

PXE インストール サーバ

Preboot Execution Environment（PXE）インストール サーバを使用すると、クライアントはリモートの場所から OS をブートおよびインストールできます。この方法を使用するには、PXE 環境が設定されていて、VLAN（通常は専用のプロビジョニング VLAN）で使用できるようになっている必要があります。さらに、サーバがネットワークからブートするように設定されている必要があります。サーバは、ブートすると、PXE 要求をネットワーク経由で送信します。PXE インストール サーバは、この要求に応答確認し、サーバに OS をインストールするイベントのシーケンスを開始します。

PXE サーバは、インストール ディスク、ディスク イメージ、またはスクリプトを使用して、OS をインストールできます。また、独自のディスクイメージを使用して、OS、追加コンポーネント、またはアプリケーションをインストールすることもできます。

（注） PXE インストールは、多数のサーバに OS をインストールする場合に効率のよい方法です。ただし、この方法を使用するには PXE 環境をセットアップする必要があることを考えると、他のインストール方法を使用する方が簡単な場合があります。

PXE インストール サーバを使用した OS のインストール

始める前に

- VLAN 経由でサーバに到達できることを確認します。
- OS をインストールするには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 **PXE** のブート順を最初に設定します。

ステップ 2 サーバをリブートします。

VLAN で PXE インストール サーバを使用できる場合は、サーバが再起動するとインストール プロセスが開始します。通常、PXE インストールは自動化されており、追加のユーザ入力を必要としません。残りのインストール プロセスについては、インストールしている OS のインストレーション ガイドを参照してください。

次のタスク

OS のインストールが完了したら、LAN のブート順を元の設定にリセットします。ソフトウェアの相互運用性とドライバの互換性を含め、常に OS ベンダ推奨の設定に従うようにします。ドライバの推奨事項とインストールについて詳しくは、こちらの Cisco UCS ハードウェア互換性リストに従ってください。

https://ucshcltool.cloudapps.cisco.com/public/

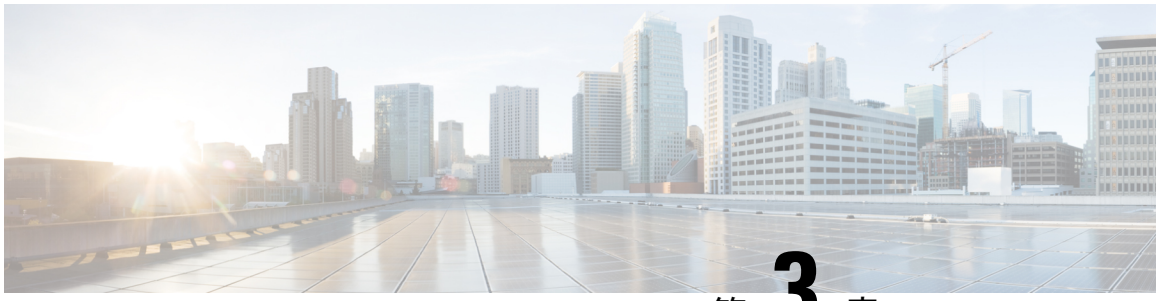
USB ポートからのオペレーティング システムの起動

すべての Cisco UCS C シリーズ サーバでは、サーバ上の任意の USB ポートからオペレーティング システムを起動できます。ただし、USB ポートから OS を起動する前に、いくつかのガイドラインを考慮する必要があります。

- ブート順序の設定を保持するために、内部 USB ポートを使って OS を起動することをお勧めします。
- USB ポートから OS を起動する前に、そのポートを有効にしておく必要があります。

  デフォルトでは、USB ポートは無効になっています。USB ポートを無効化している場合、そこから OS を起動する前に有効にする必要があります。無効化された USB ポートを有効にする方法については、サーバ固有のインストールおよびサービス ガイドにある『内部 *USB* ポートの有効化または無効化』のトピックを参照してください。次のリンクを利用できます。

  http://www.cisco.com/en/US/products/ps10493/prod_installation_guides_list.html.
- USB ポートから OS を起動した後、その USB ソースからサーバが毎回ブートするよう、下位レベルのブート順序を設定する必要があります。



第 3 章

シャーシの管理

この章は、次の内容で構成されています。

シャーシ要約

Intersight Infrastructure Service ライセンス

Intersight インフラストラクチャ サービス ライセンス

リリース以降、Cisco UCS C シリーズ M7 サーバーの場合、デバイス コネクタが Cisco Intersight サービスへの接続を検出しない場合、Cisco IMC は次の警告を表示します。4.3.1.230097

デバイス コネクタは、Cisco Intersight に対しての接続を検出できません。設定を確認し、サーバーが Intersight インフラストラクチャ サービス ライセンスに準拠して Intersight で要求されていることを確認してください。(1/5)

[OK] をクリックして**[デバイス コネクタ（Device Connector）]** に移動し、設定を構成するか、**[キャンセル（Cancel）]** をクリックして続行します。

（注） 警告カウンター（1/5）は、（5/5）に達するまでインクリメントし続けます。プロンプトは、（5/5）に達するか、デバイス コネクタが構成されているかのどちらか早い方で停止します。デバイス コネクタが 1 回構成され、後で無効にされた場合、警告が再度表示され、カウンターは最後のカウントから続行します。カウンターは、工場出荷時のデフォルトの復元が実行された場合にのみリセットされます。

警告とは別に、Cisco IMC は画面の上部に次の静的リボンも表示します：

注：このサーバーには、Intersight インフラストラクチャ サービス ライセンス ライセンスが必要です。詳しくはこちら

詳細をクリックすると、Intersight ヘルプ センターから詳細情報を取得できます。

（注） このメッセージは、デバイス コネクタが構成されている場合は表示されません。デバイス コネクタを一度構成し、後で無効にすると、メッセージが再度表示されます。

シャーシの概要の表示

デフォルトでは、Cisco UCS C シリーズ ラックマウント サーバにログオンすると、シャーシの **[概要（Summary）]**ペインが Web UI に表示されます。次の手順を実行することで、別のタブまたは作業領域を開いている際に、シャーシのサマリーを表示することもできます。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [シャーシ（Chassis）] メニューで [サマリー（Summary）] をクリックします。

ステップ 3 [Chassis Summary] ペインの [Server Properties] 領域で、次の情報を確認します。

名前	説明
[Product Name] フィールド	サーバのモデル名。
[Serial Number] フィールド	サーバのシリアル番号。
[PID] フィールド	製品 ID。
[UUID] フィールド	サーバに割り当てられている UUID。
[BIOS バージョン（BIOS version）] フィールド	サーバーで実行されている BIOS のバージョン。
Slot ID	エンクロージャ内のノードのスロット ID。 （注） このフィールドは、一部の C シリーズ サーバーでのみ使用できます。
[Description] フィールド	サーバーのユーザー定義の説明。 **[説明 (Description)]** フィールドを更新する際には、次のガイドラインを確認する必要があります。 • **説明** は次の特殊文字を含めません： • & • !

名前	説明
[アセット タグ（Asset Tag）] フィールド	ユーザ定義のサーバ タグ。デフォルトでは、新しいサーバーのアセット タグには [Unknown] と表示されます。 次のガイドラインは、**[アセットタグ (Asset Tag)]** フィールドの更新時に確認する必要があります。 • **[アセットタグ (Asset Tag)]** フィールドの最大文字数は32文字です。 • **[アセットタグ (Asset Tag)]** には、次の特殊文字を含めることはできません。 • **&** • **!**
性格分野	リリース以降、ユーザーは XML および Redfish API を使用して、HyperFlex（HX）で使用するために Cisco UCS M6 C シリーズ サーバーのパーソナリティを構成できます。4.2（1a） （注） このフィールドは、HX ですでに構成されている C シリーズ サーバーでのみ使用できます。

ステップ 4 **[シャーシの概要（Chassis Summary）]** ペインの **[Cisco IMC の情報（Cisco IMC Information）]** 領域で、次の情報を確認します。

名前	説明
[Hostname] フィールド	Cisco IMC のユーザー定義のホスト名。デフォルトでは、ホスト名は CXXX-YYYYYY 形式で表示されます（XXX はサーバのモデル番号、YYYYYY はシリアル番号です）。
[IP Address] フィールド	Cisco IMC の IP アドレス
[MAC Address] フィールド	Cisco IMC に対するアクティブなネットワーク インターフェイスに割り当てられている MAC アドレス。
[Firmware Version]フィールド	現在の Cisco IMC ファームウェアのバージョン。

名前	説明
[Current Time] フィールド	Cisco IMC クロックが示している現在の日時。 （注） Cisco IMC NTP が無効になっている場合、サーバー BIOS から現在の日時を取得します。NTP が有効にされている場合、Cisco IMC は NTP サーバから現在の日時を取得します。この情報を変更するには、サーバーをリブートし、BIOS 設定メニューへのアクセスに関するメッセージが表示されたら **F2** キーを押します。メインの BIOS 設定タブでオプションを使用して日付または時刻を変更します。
[ローカル タイム（Local Time）] フィールド	選択したタイムゾーンを基準とした、該当する地域のローカル タイム。
[タイムゾーン] フィールド	[タイムゾーンを選択（Select Timezone）] オプションをクリックすると、タイム ゾーンを選択できます。[Select Timezone] ポップアップ画面で、マップの上にカーソルを移動してロケーションをクリックしてタイム ゾーンを選択するか、または [Timezone] ドロップダウン メニューからタイム ゾーンを選択します。

ステップ 5 **[シャーシの概要（Chassis Summary）]**ペインの **[シャーシ ステータス（Chassis Status）]**領域で、次の情報を確認します。

名前	説明
[Power State] フィールド	現在の電源状態。
POST 完了 ステータス フィールド	BIOS POST 完了 ステータス。
[全体のサーバー ステータス（Overall Server Status）] フィールド	サーバの全体的なステータス。次のいずれかになります。 • [Memory Test In Progress]：サーバは搭載されているメモリのセルフテストを実行しています。 この状態は、通常、ブート プロセスの間に発生します。 • **Good** • **[Moderate Fault]** • **[Severe Fault]**

名前	説明
[Temperature] フィールド	温度ステータス。次のいずれかになります。 • **Good** • **[Fault]** • **[Severe Fault]** このフィールドのリンクをクリックして、詳細な温度情報を表示できます。
[全体の DIMM ステータス（Overall DIMM Status）] フィールド	メモリ モジュールの全体的なステータス。次のいずれかになります。 • **Good** • **[Fault]** • **[Severe Fault]** このフィールドのリンクをクリックして、詳細なステータス情報を表示できます。
[Power Supplies] フィールド	電源装置の全体的なステータス。次のいずれかになります。 • **Good** • **[Fault]** • **[Severe Fault]** このフィールドのリンクをクリックして、詳細なステータス情報を表示できます。
[Fans] フィールド	電源装置の全体的なステータス。次のいずれかになります。 • **Good** • **[Fault]** • **[Severe Fault]** このフィールドのリンクをクリックして、詳細なステータス情報を表示できます。
[Locator LED] フィールド	ロケータ LED がオンかオフか。
[前面のロケータ LED（Front Locator LED）] フィールド	シャーシ上の前面パネルのロケータ LED が点灯しているか、消灯しているかどうか。 （注） このオプションは一部の UCS C シリーズのサーバでのみ利用可能です。

名前	説明
[ストレージ全体のステータス（Overall Storage Status）] フィールド	すべてのコントローラの全体的ステータス。次のいずれかになります。 • **Good** • **[Moderate Fault]** • **[Severe Fault]**

ステップ 6 **[シャーシの概要（Chassis Summary）]**ペインの **[サーバ使用率（Server Utilization）]**領域で、次の情報を確認します。

名前	説明
[全体の使用率（%）（Overall Utilization (%)）] フィールド	システムの CPU、メモリ、および IO（入出力）の全体的な使用率をリアルタイムに表すパーセンテージ。
[CPU 使用率（%）（CPU Utilization (%)）] フィールド	使用可能なすべての CPU 上にあるシステムの CPU またはコンピューティング システムの使用率（パーセンテージ）。
[メモリ使用率（%）（Memory Utilization (%)）] フィールド	使用可能なすべてのメモリ（DIMM）チャネル上のシステム メモリ使用率（%）。
[IO 使用率（%）（IO Utilization (%)）] フィールド	システムの IO リソース使用率のパーセンテージ。

シャーシ インベントリ

電源のプロパティの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [シャーシ（Chassis）] メニューで [インベントリ（Inventory）] をクリックします。

ステップ 3 [Inventory] 作業ウィンドウで、[Power Supplies] タブをクリックし、各電源の次の情報を確認します。

名前	説明
[Device ID] カラム	電源装置ユニットの ID。
[Status] カラム	電源装置のステータス。
[Input] カラム	電源装置への入力（ワット単位）。
[出力（Output）] カラム	電源装置からの最大出力（ワット単位）。
[FW Version] カラム	電源装置のファームウェア バージョン。
[Product ID] カラム	ベンダーによって割り当てられた電源の製品識別子。

Cisco VIC アダプタのプロパティの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [シャーシ（Chassis）] メニューで [インベントリ（Inventory）] をクリックします。

ステップ 3 [Inventory] 作業ウィンドウで、[Cisco VIC Adapters] タブをクリックし、次の概要を確認します。

名前	説明
[Slot Number] カラム	アダプタが装着されている PCI スロット。
[Serial Number] カラム	アダプタのシリアル番号。
[Product ID] カラム	アダプタの製品 ID。
[Cisco IMC Enabled] カラム	アダプタで Cisco IMC を管理できるかどうか。この機能は、設置されているアダプタのタイプと、その設定内容によって異なります。詳細については、使用しているサーバ タイプに対応するハードウェア インストレーション ガイドを参照してください。
[Description] カラム	アダプタの説明。

SAS エクスパンダのプロパティの表示

始める前に

サーバーの電源をオンにする必要があります。そうしないと、プロパティが表示されません。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [シャーシ（Chassis）] メニューで [インベントリ（Inventory）] をクリックします。

ステップ 3 [Inventory] 作業ウィンドウの [SAS Expander] タブをクリックし、次の情報を確認します。

名前	説明
[ID] カラム	エクスパンダの製品 ID。
[Name] カラム	エクスパンダの名前。
[**Firmware Version**] カラム	エクスパンダで使用されているファームウェアのバージョン。
[Secondary Firmware Version] カラム	エクスパンダで使用されているセカンダリ ファームウェアのバージョン。
[Server Up Link Speed] カラム	LSI RAID コントローラを使用した受信アップリンク速度。 （注） 一部の C シリーズ サーバでのみ有効になります。

SAS エクスパンダでの 6G または 12G 混合モードの有効化

このオプション（トグル ボタン）を使用して、カードに対する 6 ギガバイトまたは 12 ギガバイトの混合モード速度のサポートを有効または無効にすることができます。

（注） このオプションを使用できるのは一部の C シリーズ サーバーだけです。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [シャーシ（Chassis）] メニューで [インベントリ（Inventory）] をクリックします。

ステップ 3 [Inventory] 作業領域で、[SAS Expander] タブをクリックします。

ステップ 4 [SAS Expander] 作業領域で、[Enable 6G-12G Mixed Mode] をクリックします。

ステップ 5 （任意） 機能を無効にするには、[Disable 6g-12G Mixed Mode] をクリックします。

ストレージのプロパティの表示

始める前に

サーバーの電源をオンにする必要があります。そうしないと、プロパティが表示されません。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [シャーシ（Chassis）] メニューで [インベントリ（Inventory）] をクリックします。

ステップ 3 [Inventory] 作業ウィンドウの [Storage] タブをクリックし、次の情報を確認します。

名前	説明
[コントローラ（Controller）] フィールド	コントローラ ドライブが存在する PCIe スロット。
[PCIスロット（PCI Slot）] フィールド	コントローラ ドライブが配置されている PCIe スロットの名前。
[製品名（Product Name）] フィールド	コントローラの名前。
[シリアル番号（Serial Number）] フィールド	ストレージ コントローラのシリアル番号。
[ファームウェアパッケージビルド（Firmware Package Build）] フィールド	アクティブなファームウェア パッケージのバージョン番号。
[製品ID（Product ID）] フィールド	コントローラの製品 ID。
[バッテリのステータス（Battery Status）] フィールド	バッテリのステータス。
[キャッシュメモリサイズ（Cache Memory Size）] フィールド	キャッシュ メモリのサイズ（MB 単位）。
[状況（Health）] フィールド	The health of the controller firmware status.

名前	説明
[詳細（Details）] フィールド	コントローラの詳細へのリンク。

ネットワーク アダプタのプロパティの表示

始める前に

サーバーの電源をオンにする必要があります。そうしないと、プロパティが表示されません。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [シャーシ（Chassis）] メニューで [インベントリ（Inventory）] をクリックします。

ステップ 3 [Inventory] 作業ウィンドウの [Network Adapters] タブをクリックし、次の情報を確認します。

名前	説明
[スロット（Slot）] カラム	アダプタが装着されているスロット。
[製品名（Product Name）] カラム	アダプタの製品名。
[インターフェイス数（Number of Interfaces）] カラム	アダプタのインターフェイス数。
External Ethernet Interfaces	[ID]：外部イーサネット インターフェイスの ID。 [MAC Address]：外部イーサネット インターフェイスの MAC アドレス。

GPU インベントリの表示

GPU インベントリ オプションを使用できるのは一部の C シリーズ サーバーだけです。

始める前に

サーバーの電源をオンにする必要があります。そうしないと、プロパティが表示されません。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [シャーシ（Chassis）] メニューで [インベントリ（Inventory）] をクリックします。

ステップ 3 [インベントリ（Inventory）] 作業ウィンドウの [GPUインベントリ（GPU Inventory）] タブをクリックし、次の情報を確認します。

名前	説明
スロット	GPU がインストールされているスロット。
製品名	GPU の名前。
Number of GPUs	スロットに存在する GPU の数。

PCI スイッチ情報の表示

始める前に

サーバーの電源をオンにする必要があります。そうしないと、プロパティが表示されません。

手順

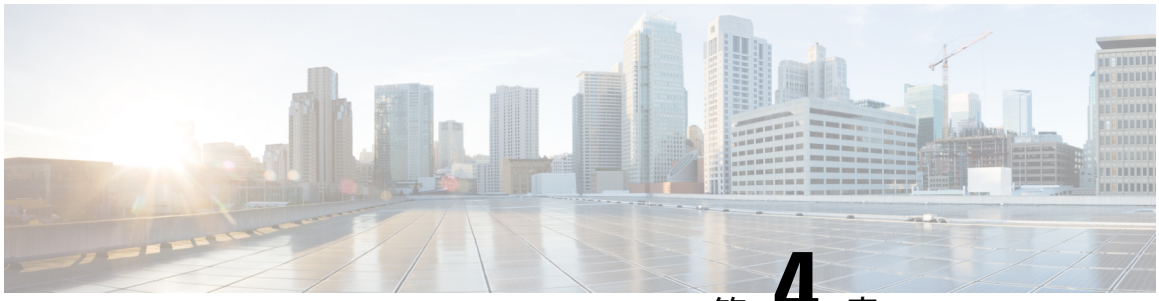
ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [シャーシ（Chassis）] メニューで [インベントリ（Inventory）] をクリックします。

ステップ 3 [インベントリ（Inventory）] 作業ウィンドウの [PCIスイッチ情報（PCI Switch Info）] タブをクリックし、次の情報を確認します。

名前	説明
[コントローラ（Controller）] カラム	コントローラが装着されている PCI スロット。
[Controller Type] 列	スロットに装着されている PCI スイッチのタイプ。
[製品名（Product Name）] 列	PCI スイッチの名前。
[製造元（Manufacturer）] カラム	PCI スイッチのベンダー。
[ベンダー ID（Vendor ID）] カラム	ベンダーによって割り当てられたスイッチ ID。

名前	説明
[サブ ベンダー ID（Sub Vendor ID）] カラム	ベンダーによって割り当てられた 2 番目のスイッチ ID。
[Device ID] カラム	ベンダーによって割り当てられたデバイス ID。
[Sub Device ID] カラム	ベンダーによって割り当てられているセカンダリ デバイス ID。



第 4 章

サーバーの管理

この章は、次の内容で構成されています。

サーバのブート順

Cisco IMC を使用して、使用可能なブートデバイスタイプからサーバがブートを試行する順序を設定できます。レガシーブート順の設定では、Cisco IMC によりデバイスタイプの並び替えが許可されますが、デバイスタイプ内のデバイスの並べ替えはできません。高精度ブート順の設定により、デバイスの線形順序付けができます。Web UI または CLI では、ブート順およびブートモードの変更、各デバイスタイプ下への複数のデバイスの追加、ブート順の並び替え、各デバイス タイプのパラメータの設定ができます。

ブート順の設定を変更すると、Cisco IMC は、サーバが次にリブートされるときに、設定されたブート順を BIOS に送信します。新しいブート順を実装するには、設定の変更後にサーバーをリブートします。新しいブート順は以降のリブートで反映されます。設定されたブート順は、設定が Cisco IMC または BIOS 設定で再度変更されるまで保持されます。

（注） 次のいずれかの条件が発生すると、実際のブート順は設定されたブート順と異なります。

- 設定されたブート順を使用してブートしようとしたときに BIOS で問題が発生した。
- ユーザが BIOS で直接、ブート順を変更した。
- BIOS が、ホストによって認識されているがユーザーから設定されていないデバイスを追加した。

重要 Cisco UCS C220 M5 または C480 M5 サーバをリリース 4.1 (1x) にアップグレードする場合は、次の条件に従います。

- 4.0 よりも前のリリースからアップグレードする場合 (4x)
- **[レガシー ブート モード (Legacy Boot Mode)]** が有効になっていて、**[Cisco IMC のブート順序 (Cisco IMC Boot Order)]** が設定されていない場合
- サーバが Cisco HWRAID アダプタから起動している場合

その後、アップグレードする前に次のいずれかを実行する必要があります。

- ここに記載されている XML API スクリプトと UCSCFG ベースのスクリプトを実行します。

  または

- Cisco IMC GUI または CLI インターフェイスを使用して、目的のブート順序を手動で設定します。

（注） ブート順の設定機能を使用して新しいポリシーを作成する場合、BIOS はこの新しいポリシーをシステムのデバイスにマッピングしようとします。実際にマッピングされたデバイス名とポリシー名が [**Actual Boot Order**] 領域に表示されます。BIOS が Cisco IMC の特定のポリシーにデバイスをマッピングできない場合は、実際のデバイス名が [**Actual Boot Order**] 領域に [**NonPolicyTarget**]として示されます。

（注） Cisco IMC 2.0(x) のアップグレード中に、レガシー ブート順は高精度ブート順に移行されます。前のブート順の設定が削除され、バージョン 2.0 にアップグレードする前に設定されたすべてのデバイス タイプが対応する高精度ブート デバイス タイプに変換され、ダミーのデバイスが同じデバイス タイプ用に作成されます。Web UI の **[構成されたブート順序 (Configured Boot Order)]** 領域でこれらのデバイスを確認できます。CLI でこれらのデバイスを確認するには、**show boot-device** コマンドを入力します。この間に、サーバーの実際のブート順が保持され、Web UI と CLI の実際のブート順オプション下で確認できます。

Cisco IMC を 2.0(x) よりも前のバージョンにダウングレードすると、サーバの最後のブート順が保持され、それを [**Actual Boot Order**] 領域で確認できます。次に例を示します。

- 2.0(x) バージョンでレガシー ブート順でサーバを設定した場合、ダウングレードすると、レガシー ブート順の設定が保持されます。
- 2.0(x) で高精度ブート順でサーバーを設定した場合、ダウングレードすると、最後に設定したレガシー ブート順が保持されます。

重要

- 2.0(x) より前のブート順の設定がレガシー ブート順と見なされます。実行中のバージョンが 2.0(x) の場合、Web UI でレガシー ブート順を設定できませんが、CLI および XML API を介して設定できます。CLI で、**set boot-order HDD,PXE** コマンドを使用してこれを設定できます。CLI または XML API を介してレガシー ブート順を設定できますが、Web UI では設定されたこのブート順は表示されません。
- レガシー ブート順の機能と高精度ブート順の機能は相互に排他的です。レガシー ブート順または高精度ブート順のどちらかを設定できます。レガシーブート順を設定すると、設定されたすべての高精度ブートデバイスがディセーブルになります。高精度ブート順を設定すると、レガシー ブート順の設定が消去されます。

高精度ブート順の設定

始める前に

サーバのブート順を設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 [BIOS] タブで [Configure Boot Order] タブをクリックします。

ステップ 3 **[BIOS プロパティ (BIOS Properties)]** 領域の **[ブート順序の構成 (Configure Boot Order)]** をクリックします。

[ブート順序の構成 (Configure Boot Order)] ダイアログ ボックスが表示されます。

ステップ 4 [Configure Boot Order] ダイアログボックスで、次のプロパティを更新します。

[Basic] タブ

名前	説明
[Device Types] テーブル	サーバのブート オプション。次の 1 つ以上を選択できます。 • **HDD**：ハード ディスク ドライブ • [FDD]：フロッピー ディスク ドライブ • [CDROM]：ブート可能な CD-ROM または DVD • [PXE]：PXE ブート • **EFI**：Extensible Firmware Interface
>>	選択したデバイス タイプを [Boot Order] テーブルに移動します。
<<	選択したデバイス タイプを [Boot Order] テーブルから削除します。
[Boot Order] テーブル	このサーバーがブートできるデバイス タイプが、ブートが試行される順番に表示されます。
Down	選択したデバイス タイプを [ブート順序（Boot Order）] テーブルで高いプライオリティに移動します。
Up	選択したデバイス タイプを [**Boot Order**] テーブルで高いプライオリティに移動します。
変更の保存	このページで加えた変更を保存する場合に、このボタンをクリックします。
[Close] ボタン	変更を保存しないで、または既存の設定を再適用しないで、ダイアログ ボックスを閉じます。

[Advanced] タブ

[ブート デバイスの追加 (Add Boot Device)] ペインに次のリンクのリストが表示されます。

- **ローカル HDD の追加**
- **[Add PXE Boot]**
- **[Add SAN Boot]**
- **[Add iSCSI Boot**

- **[Add USB]**
- **[Add Virtual Media]**
- **[Add PCHStorage]**
- **[Add UEFISHELL]**
- **NVME の追加**
- **ローカル CDD の追加**
- **HTTPブートの追加**

[高度なブート順序構成 (Advanced Boot Order Configuration)] ペインに、追加されたデバイスが表示されます。適切なボタンを選択すると、次のアクションを実行できます。

- **Enable または Disable**
- **修正**
- **[削除（Delete）]**
- **[クローン（Clone）]**
- **再適用**
- **Move Up**
- **Move Down**

ステップ 5 [Save Changes] をクリックします。

サーバに接続しているデバイスによっては、実際のブート順に追加のデバイス タイプが付加される場合があります。

次のタスク

サーバを再起動して、新しいブート順でブートします。

ブート デバイスの管理

始める前に

デバイス タイプをサーバのブート順に追加するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[コンピューティング（Compute）]メニューをクリックします。

ステップ 2 [BIOS] タブで [Configure Boot Order] タブをクリックします。

ステップ 3 [BIOS Properties] 領域の [Configure Boot Order] をクリックします。

ブート順の説明が示されたダイアログボックスが表示されます。

ステップ 4 [Configure Boot Order] ダイアログボックスで、[**Add Boot Device**] テーブルからブート順に追加するデバイスを選択します。

ローカル HDD デバイスを追加するには、[**Add Local HDD**] をクリックし、次のパラメータを更新します。

名前	説明
[名前（Name）] フィールド	デバイスの名前。 （注） 一旦作成すると、デバイスの名前を変更することはできません。
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。次のいずれかになります。 • [有効（Enabled）] : デバイスはブート順の設定で BIOS から認識できます。 • [無効（Disabled）] : デバイスはブート設定で BIOS から認識できません。
[Order]フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。
[Slot] フィールド	デバイスが装着されているスロット。使用可能な範囲のスロット番号を入力します。
[Slot] フィールド	デバイスが装着されているスロット。範囲は C シリーズ サーバーに依存します。 • C220 M4 および C240 M4 サーバーの場合は、「HBA」を入力します。 • C460 M4 サーバの場合、1 ～ 255 の範囲の値または SAS を入力します。 • 他の C シリーズ サーバの場合、1 ～ 255 の範囲の値または M を入力します。
[**Add Device**] ボタン	[**Boot Order**] テーブルにデバイスを追加します。

名前	説明
[Cancel]ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

PXE デバイスを追加するには、[**Add PXE**] をクリックし、次のパラメータを更新します。

名前	説明
[名前（Name）] フィールド	デバイスの名前。 この名前は、デバイスの作成後は変更できません。
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。状態は次のいずれかになります。 • [有効（Enabled）] : デバイスはブート順の設定で BIOS から認識できます。 • [無効（Disabled）] : デバイスはブート順の設定で BIOS から認識できません。
[Order]フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。
[Slot] フィールド	• C220 M4 および C240 M4 サーバでは、1 から 255 の間の数字、L、または MLOM を入力します。 • C3160 サーバでは 1 から 255 の間の値を入力します。 • C460M4 サーバでは 1 から 255 の間の値、L1 または L2 を入力します。 • 他の C シリーズ サーバーの場合は、0 ～ 255 の値または「L」を入力します。
MAC アドレス	ネットワーク イーサネット インターフェイスの MAC アドレス。 （注） このオプションを使用できるのは一部の C シリーズ サーバーだけです。
[Slot] フィールド	デバイスが装着されているスロット。使用可能な範囲のスロット番号を入力します。
[Port] フィールド	デバイスが装着されているスロットのポート。 0 ～ 255 の範囲内の数を入力してください。

SAN ブート デバイスを追加するには、**[SANブートの追加（Add SAN Boot）]** をクリックし、次のパラメータを更新します。

名前	説明
[名前（Name）] フィールド	デバイスの名前。 この名前は、デバイスの作成後は変更できません。
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。状態は次のいずれかになります。 • [有効（Enabled）] : デバイスはブート順の設定で BIOS から認識できます。 • [無効（Disabled）] : デバイスはブート順の設定で BIOS から認識できません。
[Order]フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。
[Slot] フィールド	デバイスが装着されているスロット。範囲は C シリーズ サーバに依存します。 • C220 M4 および C240 M4 サーバでは、1 から 255 の間の数字または MLOM を入力します。 • C460M4 サーバでは 1 から 255 の間の値、L1 または L2 を入力します。 • 他の C シリーズ サーバーの場合は、1 ～ 255 の値を入力します。
[Slot] フィールド	デバイスが装着されているスロット。使用可能な範囲のスロット番号を入力します。
[**LUN**] フィールド	デバイスが装着されているスロットの論理ユニット。 0 ～ 255 の範囲内の数を入力してください。
[変更を保存（Save Changes）] ボタン	[ブート順序（Boot Order）] テーブルにデバイスを追加し、変更を保存します。
[Cancel] ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

iSCSI ブート デバイスを追加するには、**[iSCSIブートの追加（Add iSCSI Boot）]** をクリックし、次のパラメータを更新します。

名前	説明
[名前（Name）] フィールド	デバイスの名前。 この名前は、デバイスの作成後は変更できません。
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。状態は次のいずれかになります。 • [有効（Enabled）] : デバイスはブート順の設定で BIOS から認識できます。 • [無効（Disabled）] : デバイスはブート順の設定で BIOS から認識できません。
[Order]フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。
[Slot] フィールド	デバイスが装着されているスロット。範囲は C シリーズ サーバに依存します。 • C220 M4 および C240 M4 サーバでは、1 から 255 の間の数字、L、または MLOM を入力します。 • C3160 サーバでは 1 から 255 の間の値を入力します。 • C460M4 サーバでは 1 から 255 の間の値、L1 または L2 を入力します。 • 他の C シリーズ サーバーの場合は、1 ～ 255 の値または「L」を入力します。
[Slot] フィールド	デバイスが装着されているスロット。使用可能な範囲のスロット番号を入力します。
[Port] フィールド	デバイスが装着されているスロットのポート。 0 ～ 255 の範囲内の数を入力してください。 （注） VIC カードの場合は、ポート番号ではなく vNIC インスタンスを使用します。
[変更を保存（Save Changes）] ボタン	[ブート順序（Boot Order）] テーブルにデバイスを追加し、変更を保存します。
[Cancel] ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

SD カードを追加するには、[**Add SD Card**] をクリックし、次のパラメータを更新します。

（注） このオプションは一部の UCS C シリーズのサーバでのみ利用可能です。

名前	説明
[名前（Name）] フィールド	デバイスの名前。 この名前は、デバイスの作成後は変更できません。
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。次のいずれかになります。 • [有効（Enabled）] : デバイスはブート順の設定で BIOS から認識できます。 • [無効（Disabled）] : デバイスはブート設定で BIOS から認識できません。
[Order]フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。
[変更を保存（Save Changes）] ボタン	[**Boot Order**] テーブルにデバイスを追加します。
[Cancel]ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

USB デバイスを追加するには、[**Add USB**] をクリックし、次のパラメータを更新します。

名前	説明
[名前（Name）] フィールド	デバイスの名前。 この名前は、デバイスの作成後は変更できません。
[**Sub Type**] ドロップダウン リスト	特定のデバイス タイプの下位のサブデバイス タイプ。次のいずれかになります。 • **[CD]** • **[FDD]** • **[HDD]**
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。次のいずれかになります。 • [有効（Enabled）] : デバイスはブート順の設定で BIOS から認識できます。 • [無効（Disabled）] : デバイスはブート順の設定で BIOS から認識できません。
[Order]フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。

名前	説明
[変更を保存（Save Changes）] ボタン	[**Boot Order**] テーブルにデバイスを追加します。
[Cancel]ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

仮想メディアを追加するには、[**Virtual Media**] をクリックし、次のパラメータを更新します。

名前	説明
[名前（Name）] フィールド	デバイスの名前。 この名前は、デバイスの作成後は変更できません。
[**Sub Type**] ドロップダウン リスト	特定のデバイス タイプの下位のサブデバイス タイプ。これは、次のいずれかになります。 • **[KVM Mapped DVD]** • **Cisco IMC マップされた DVD** • **[KVM Mapped HDD]** • **Cisco IMC マップされた HDD** • **[KVM Mapped FDD]**
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。状態は次のいずれかになります。 • [有効（Enabled）] : デバイスはブート順の設定で BIOS から認識できます。 • [無効（Disabled）] : デバイスはブート順の設定で BIOS から認識できません。
[Order]フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。
[変更を保存（Save Changes）] ボタン	[Boot Order] テーブルにデバイスを追加します。
[取り消し（Cancel）] ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

PCH ストレージ デバイスを追加するには、[**PCH Storage**] をクリックし、次のパラメータを更新します。

名前	説明
[名前（Name）] フィールド	デバイスの名前。 この名前は、デバイスの作成後は変更できません。
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。次のいずれかになります。 • [有効（Enabled）] : デバイスはブート順の設定で BIOS から認識できます。 • [無効（Disabled）] : デバイスはブート順の設定で BIOS から認識できません。
[Order]フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。
[LUN] フィールド	デバイスが装着されているスロットの論理ユニット。 • 0 から 255 までの数字を入力します。 • AHCI モードの SATA：1 から 10 までの値を入力します。 • SWRAID モードの SATA：SATA の場合は 0、SATA の場合は 1 を入力します。 （注） SATA モードを使用できるのは一部の UCS C シリーズ サーバーだけです。
[変更を保存（Save Changes）] ボタン	[**Boot Order**] テーブルにデバイスを追加します。
[Cancel]ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

UEFI シェル デバイスを追加するには、[Add UEFI Shell] をクリックし、次のパラメータを更新します。

名前	説明
[名前（Name）] フィールド	デバイスの名前。 この名前は、デバイスの作成後は変更できません。

名前	説明
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。状態は次のいずれかになります。 • [有効（Enabled）] : デバイスはブート順の設定で BIOS から認識できます。 • [無効（Disabled）] : デバイスはブート順の設定で BIOS から認識できません。
[Order]フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。
[**Add Device**] ボタン	[**Boot Order**] テーブルにデバイスを追加します。
[Cancel]ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

HTTP ブート デバイス デバイスを追加するには、**[HTTPブートの追加（Add HTTP Boot）]** をクリックし、次のパラメータを更新します：

（注） HTTP ブート デバイスでは、次の OS（ISO）がサポートされています：

- SLES 12.x
- RHEL 8.2
- ESX 6.5

次の OS（ISO）は、HTTP ブート デバイスではサポートされていません：

- Windows 2016
- Windows 2019

名前	説明
[名前（Name）] フィールド	デバイスの名前。 この名前は、デバイスの作成後は変更できません。 1 ～ 30 文字の英数字、-（ハイフン）、_（アンダースコア）を入力できます。名前をハイフンまたはアンダースコアで始めることはできません。

名前	説明
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。State には、次のいずれかを指定できます。 • **[有効（Enabled）]**—デフォルトオプション。デバイスはブート順の構成で BIOS から認識できます。 • [**Disabled**]：デバイスはブート順の設定で BIOS から認識できません。
[Order]フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。デフォルトのオプションは、 1 です。
[MAC Address] フィールド	ネットワーク イーサネット インターフェイスの MAC アドレス。
[IP タイプ (IP Type)] ドロップダウン リスト	IP のタイプ。 ドロップダウン リストに表示されている次のいずれかのオプションを選択します： • なし • IPv4 • IPv6 デフォルト値は None です。
[Slot] フィールド	デバイスが装着されているスロット。使用可能な範囲のスロット番号を入力します。 以下のリストから必要な値を入力します。 • OCP • MLOM • L • 1 ～ 255 の範囲内のいずれかの数。
[Port] フィールド	デバイスが装着されているスロットのポート。 0 ～ 255 の範囲内の数を入力してください。

名前	説明
[IP 構成タイプ (IP Config Type)] ドロップダウン リスト	IP 構成の種類。 ドロップダウンリストには、次のオプションが表示されます。 • **[なし（None）]** • **DHCP** • **[静的（Static）]** **DHCP** IP 構成の場合、選択した IP タイプに応じて、次のフィールドが表示されます： • MAC アドレス（MAC Address） • **IPタイプ** • **スロット** • **[ポート（Port）]** **静的** IP 構成の場合、選択した IP タイプに応じて、次のフィールドが表示されます： • **URI** • **IP Address** • **IPv4 ネットマスク**または **IPv6 ネットマスク** • **IPv4 ゲートウェイ**または **IPv6 ゲートウェイ** • **IPv4 優先 DNS サーバー**または **IPv6 優先 DNS サーバー**
URI フィールド	ユニフォーム情報技術識別子 HTTP サーバー パスの場所。 1ー255 文字の入力ができます。
[変更の保存（Save Changes）] ボタン	変更を保存し、デバイスを **ブート順序** 表に追加します。
[Cancel] ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

UEFI セキュア ブートの概要

オペレーティング システムをロードし実行する前に、ロードおよび実行前のすべての EFI ドライバ、EFI アプリケーション、オプション ROM またはオペレーティング システムが確実に署名され信頼性と整合性が確認されるために、Unified Extensible Firmware Interface（UEFI）のセ

キュア ブートを使用できます。Web UI または CLI を使用して、このオプションをイネーブルにできます。UEFI のセキュア ブート モードをイネーブルにすると、ブート モードは UEFI モードに設定され、UEFI のブート モードがディセーブルになるまで、設定されているブート モードを変更できません。

（注） サポートされていない OS で UEFI セキュア ブートをイネーブルにすると、次の再起動時に、その特定の OS から起動することはできません。前の OS から起動しようとすると、Web UI のシステム ソフトウェア イベントの下にエラーが報告され記録されます。前の OS から起動するには、Cisco IMC を使用して UEFI セキュア ブート オプションをディセーブルにする必要があります。

重要 また、サポートされていないアダプタを使用すると、Cisco IMC SEL のエラー ログ イベントが記録されます。エラー メッセージが次のように表示されます。

System Software event: Post sensor, System Firmware error. EFI Load Image Security Violation. [0x5302] was asserted .

UEFI のセキュア ブートは次のコンポーネントでサポートされます。

コンポーネント	種類
サポートされている OS	• Windows Server 2019 • Windows Server 2016 • ESX 6.7 • ESX 6.5 • ESXi 7.0 • Linux
Broadcom PCI アダプタ	• 5709 デュアルおよびクアッド ポート アダプタ • 57712 10GBASE-T アダプタ • 57810 CNA • 57712 SFP ポート
Intel PCI アダプタ	• i350 クアッド ポート アダプタ • X520 アダプタ • X540 アダプタ • LOM

コンポーネント	種類
QLogic PCI アダプタ	• 8362 デュアル ポート アダプタ • 2672 デュアル ポート アダプタ
Fusion-io	
LSI	• LSI MegaRAID SAS 9240-8i • LSI MegaRAID SAS 9220-8i • LSI MegaRAID SAS 9265CV-8i • LSI MegaRAID SAS 9285CV-8e • LSI MegaRAID SAS 9285CV-8e • LSI MegaRAID SAS 9266-8i • LSI SAS2008-8i mezz • LSI Nytro カード

UEFI セキュア ブートのイネーブル化

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[コンピューティング（Compute）]メニューをクリックします。

ステップ 2 作業ウィンドウで **[BIOS]** タブをクリックします。

ステップ 3 **[ブート順序の設定（Configure Boot Order）]** タブの**[BIOS のプロパティ（BIOS Properties）]** 領域で、**[UEFI セキュア ブート（UEFI Secure Boot）]**チェックボックスをオンにします。

（注） オンにすると、ブート モードがUEFIセキュア ブートに設定されます。UEFIセキュア ブート オプションがディセーブルになるまで [**Configure Boot Mode**] は変更できません。

（注） RFD（Reset Factory Default）の場合は、UEFI セキュア ブートを再度有効にする必要があります。

サポートされていない OS で UEFI セキュア ブートをイネーブルにすると、次の再起動時に、その特定の OS から起動することはできません。前の OS から起動しようとすると、Web UI のシステム ソフトウェア イベントの下にエラーが報告され記録されます。前の OS から起動するには、Cisco IMC を使用して UEFI セキュア ブート オプションをディセーブルにする必要があります。

ステップ 4 **[Save Changes]**をクリックします。

次のタスク

サーバを再起動してコンフィギュレーション ブート モード設定を有効にします。

UEFI セキュア ブートのディセーブル化

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[コンピューティング（Compute）]メニューをクリックします。

ステップ 2 **作業ウィンドウで [BIOS]** タブをクリックします。

ステップ 3 [**BIOS Properties**] 領域で、[**UEFI Secure Boot**] チェックボックスをオフにします。

ステップ 4 **[Save Changes]**をクリックします。

次のタスク

サーバを再起動してコンフィギュレーション ブート モード設定を有効にします。

サーバーの実際のブート順の表示

サーバーの実際のブート順とは、サーバーが最後にブートされたときに BIOS によって実際に使用されたブート順です。実際のブート順は、Cisco IMC で設定されたブート順とは異なる場合があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[コンピューティング（Compute）]メニューをクリックします。

ステップ 2 [BIOS] タブで [Configure Boot Order] タブをクリックします。

ステップ 3 [BIOS Properties] 領域の [Configure Boot Order] をクリックします。

この領域には、Cisco IMC を介して設定されたブート順のデバイスと、サーバー BIOS によって使用される実際のブート順が表示されます。

[設定されたブート デバイス（Configured Boot Devices）] セクションに、Cisco IMC で設定されているブート順序（**[基本（Basic）]** または **[詳細設定（Advanced）]**）が表示されます。この設定が変更されると、次回のサーバ ブート時に、Cisco IMC から BIOS にこのブート順序が送信されます。基本設定では、デバイス タイプのみを指定できます。[詳細設定（Advanced）]

設定では、スロット、ポート、および LUN などの特定のパラメータを使用してデバイスを設定できます。

設定済みのブート順序を変更する場合、または以前に設定されていたブート順序を復元する場合は、[ブート順序の設定（Configure Boot Order）] ボタンをクリックします。これらの変更を直ちに適用するには、サーバを再起動する必要があります。[BIOS] タブを更新すると、新しいブート順序を確認できます。

（注） この情報は、次回のサーバーのブート時に BIOS にのみ送信されます。設定が変更されるまでは、Cisco IMC から BIOS に再びブート順序の情報が送信されることはありません。

[Actual Boot Devices] セクションには、サーバーが最後にブートされたときに BIOS によって実際に使用されたブート順が表示されます。次のいずれかの条件が発生すると、実際のブート順は設定されたブート順と異なります。

- 設定されたブート順を使用してブートしようとしたときに BIOS で問題が発生した。
- ユーザーが BIOS で直接、ブート順を変更した。手動による変更をオーバーライドするには、Cisco IMC を使用して設定済みブート順序を変更してから、サーバを再起動します。

（注） 設定されたブート順を使用して新しいポリシーを作成すると、BIOS はこの新しいポリシーをシステムに存在するデバイス（複数の場合あり）にマッピングしようとします。[実際のブート順序（Actual Boot Order）] エリアに、マッピングされた実際のデバイス名とポリシー名が表示されます。BIOS が Cisco IMC で特定のポリシーをマッピングするデバイスを見つけられない場合、[実際のブート順序（Actual Boot Order）] エリアでは実際のデバイス名が [NonPolicyTarget] として表示されます。

1 回限りのブート デバイスを使用してブートするサーバの設定

現在設定されているブート順序を乱さずに、次回のサーバブートに限り特定のデバイスから起動するように、サーバを設定できます。1 回限りのブート デバイスからサーバがブートしたら、その後のリブートはすべて以前に設定されていたブート順序で実行されます。

始める前に

サーバのブート順を設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 [BIOS] タブで [Configure Boot Order] タブをクリックします。

ステップ 3 [BIOS Properties] 領域で、[Configured One Time Boot Device] ドロップダウンからオプションを選択します。

（注） 拡張ブートデバイスを無効にしてホストが設定されている場合でも、ホストは1回限りのブート デバイスにブートします。

サーバ アセット タグの作成

始める前に

このタスクを実行するには、user または admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。
ステップ 2 [シャーシ（Chassis）] メニューで [サマリー（Summary）] をクリックします。
ステップ 3 [Server Properties] 領域で、[Asset Tag] フィールドを更新します。
ステップ 4 **[Save Changes]**をクリックします。

電力ポリシーの設定

電力制限

重要 このセクションは、一部の UCS C シリーズのサーバでのみ利用可能です。

パワー キャッピングによって、サーバの電力消費をアクティブに管理する方法が決定されます。パワーキャッピングオプションを有効にすると、システムにより電力消費がモニタされ、割り当てられている電力制限を超えないように電力が維持されます。サーバが電力制限を維持できない場合、またはプラットフォームの電力を修正時間内に指定の電力制限に戻すことができない場合、**[電力プロファイル（Power Profile）]** 領域の **[アクション（Action）]**フィールドに指定したアクションがパワー キャッピングにより実行されます。

パワーキャッピングが有効になったら、定義された属性を持つ標準電力プロファイルまたは詳細電力プロファイルを使用できるように複数の電力プロファイルを設定できます。標準電力プロファイルを選択する場合は、電力制限、修正時間、修正アクション、中断期間、ハードキャップ、ポリシー状態（有効な場合）を設定できます。詳細電力プロファイルを選択する場合は、

標準電力プロファイルの属性の他に、ドメイン固有の電力制限、安全スロットル レベル、周囲温度に基づくパワー キャッピング属性も設定できます。

（注） 次に示す変更は、Cisco UCS C シリーズ リリース 2.0(13) 以降に適用されます。

- 2.0(13) リリースへのアップグレード後、ホストの電源を初めてオンにするときに、電力特性評価が自動的に実行されます。それ以降は、電力特性評価は**[電力特性評価の実行（Run Power Characterization）]**セクションで指定されているとおりに開始する場合にのみ実行されます。
- また、サーバへの電源再投入が行われ、CPU または DIMM の設定が変更されている場合にも、初回ホスト ブート時に電力特性評価が自動的に実行されます。PCIe アダプタ、GPU、HDD などのハードウェアが変更されている場合は、電力特性評価は実行されません。特性評価された電力範囲は、ホストの電源再投入後に存在するコンポーネントに応じて変更されます。

Web UI の **[パワー キャッピング設定（Power Cap Configuration）]** タブの **[電力特性評価の実行（Run Power Characterization）]**オプションを選択すると、ホストの電源が再投入され、電力特性評価が開始されます。

電源の冗長性ポリシーの設定

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [シャーシ（Chassis）] メニューで [センサー（Sensors）] をクリックします。

ステップ 3 [Sensors] 作業領域で、[Power Supply] タブをクリックします。

ステップ 4 電源装置の次のセンサー プロパティを確認します。

[プロパティ（Properties）] 領域

名前	説明
[Redundancy Status] フィールド	電源装置の冗長性のステータス。

名前	説明
[冗長性ポリシー（Redundancy Policy）] フィールド	電源装置の冗長性のポリシー。次のいずれかになります。 • [非冗長] : N（使用可能なPSU出力性能）は、インストールされているPSUの数に等しくなります。この場合、PSUのエラー、またはグリッドのエラーはサポートされません。 • [N+1] : N（使用可能なPSU出力性能）は、インストールされている PSU の数から 1 を引いた数に等しくなります。この場合、単一の PSU のエラーはサポートされますが、グリッドのエラーはサポートされません。 • [グリッド（Grid）] : N（使用可能なPSU出力性能）は、インストールされている PSU の数の半分に等しくなります。この場合、N 個の PSU のエラー、またはグリッドのエラーがサポートされます。このポリシーは、N個のPSUを 1 つのフィードに接続し、別の N 個の PSU を別のフィードに接続したことを暗黙的に示しています。

電力特性評価の有効化

電力特性評価を有効にできるのは、一部の Cisco UCS C シリーズ サーバーだけです。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 **[シャーシ（Chassis）]**メニューで **[電源管理（Power Management）]** をクリックします。

ステップ 3 [Power Cap Configuration] タブで、[Run Power Characterization] リンクをクリックします。

現在の電力状態に応じてホストの電源がオンになるかまたは再起動することを通知する確認ボックスが表示されます。メッセージを確認してから **[OK]** をクリックしてダイアログボックスを閉じます。

[ステータス（Status）] フィールドで、電力特性評価の進行状況を確認できます。ステータスは、次のいずれかになります。

- **[未実行（Not Run）]**：工場出荷時のデフォルトにリセットされてから、電源特性評価は一度も実行されていません。

- **[実行中（Running）]**：電源特性評価プロセスが進行中です。
- **[完了（Completed Successfully）]**：電源特性評価は正常に実行されました。
- **[デフォルトの使用（Using Defaults）]**：電源特性評価の実行完了後、システムが有効な値を取得できなかった場合は、パワーキャッピングの推奨される最小電力および最大電力としてデフォルト値を使用します。

  電力特性評価の操作の実行後、プラットフォームの電力制限の範囲が最小および最大電力としてワット単位で [Recommended Power Cap] 領域の下に読み込まれます。

  パワー キャッピング制限の 3 つの値が表示されます。[最小値（スロットリングを許可）（Minimum (Allow Throttling)）]、[最小値（効率的）（Minimum (Efficient)）]、および [最大値（Maximum）]。

  - [最小値（スロットリングを許可）]：CPU のスロットリングが有効になっている場合のシャーシの電力の下限です。

    （注） この最小電力の下限値は、[スロットルを許可（Allow Throttle）] チェックボックスがオンになっているときにのみ使用できます。

  - [最小値（効率的）]：CPU のスロットリングが無効になっている場合のシャーシの電力の下限です。
  - [最大値（Maximum）]：シャーシの電力の上限です。

パワー キャッピングの有効化

このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバーだけです。

始める前に

- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。
- 電力特性評価を実行します。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 **[シャーシ（Chassis）]**メニューで **[電源管理（Power Management）]** をクリックします。

ステップ 3 [Power Capping] チェックボックスをオンにします。

（注） これは、パワーキャッピングを有効または無効にするグローバル オプションです。電力プロファイル設定を指定するには、このオプションを有効にする必要があります。

ステップ 4 [Save Changes] をクリックします。

[電源プロファイル（Power Profiles）]

複数のプロファイルを設定し、属性を設定できます。プロファイルは Web UI または CLI のいずれかを使用して設定します。Web UI では、プロファイルは [Power Capping] 領域の下にリストされます。CLI で、**power-cap-config** コマンドを入力するとプロファイルが設定されます。電力制限機能に関する次の電力プロファイルを設定できます。

- [標準（Standard）]：プラットフォーム ドメインの電力制限を設定できます。
- [詳細（Advanced）]：さまざまな属性（電力制限ポリシー、フェールセーフ電力制限ポリシー、周囲温度に基づく電力制限ポリシーなど）を設定できます。

標準電力プロファイルの設定

このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバーだけです。

始める前に

- パワー キャッピングを有効にする必要があります。
- このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 **[シャーシ（Chassis）]**メニューで **[電源管理（Power Management）]** をクリックします。

ステップ 3 [Power Profiles] 領域で、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	電力制限の属性を設定するために選択されたプロファイルの名前。
[プロファイルを有効にする（Enable Profile）] チェックボックス	電源プロファイルの編集を有効にします。
[スロットルの許可（Allow Throttle）] チェックボックス	オンにした場合、プロセッサがより積極的な電源管理メカニズム、たとえば、通常の内部メカニズムに加えて、電力制限を維持するための CPU スロットリング状態（T 状態）やメモリ帯域幅スロットリングなどを使用するようにします。

名前	説明
[訂正時間（Correction Time）] フィールド	[Action] フィールドで指定したアクションが実行される前に、プラットフォームの電力が指定された電力制限に戻る必要のある時間（秒単位）。 範囲は、1 ～ 600 です。 この範囲はサーバの PSU 値によって異なります。 （注） すべての PSU モデルでサポートされている最小訂正時間は 1 秒です。ただし、DPST-1400AB モデルと DPST-1200DB PSU モデルの場合の最小訂正時間は 3 秒です。
[アクション（Action）] ドロップダウン リスト	指定した電力制限が修正用時間内に維持されない場合に実行されるアクション。 • **[アラート（Alert）]**—イベントをシスコ IMC SEL に記録します。 • **[アラートおよびシャットダウン（Alert and Shutdown）]**—イベントをシスコ IMC SEL に記録し、ホストを正規の手順でシャットダウンします。
[電力上限（Power Limit）] チェックボックス	サーバの電力上限。 指定された範囲内での電力を入力します（ワット数）。
[Set Hard Cap] チェックボックス	オンにした場合、設定されている電力制限値を超えてプラットフォーム消費が発生することはないことが保証されます。プラットフォーム電力消費は、構成されている電力制限値より下の安全なオフセット マージンに維持されます。

ステップ 4 [Save Changes] をクリックします。

詳細電力プロファイルの設定

このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバーだけです。

始める前に

- パワー キャッピングを有効にする必要があります。
- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 **[シャーシ（Chassis）]**メニューで **[電源管理（Power Management）]** をクリックします。

ステップ 3 [Power Cap Configuration] タブの [Power Profiles] テーブルから、[Advanced] プロファイルを選択します。
標準プロファイル設定の他に、**[ドメイン固有の電力制限（Domain Specific Power Limit）]**、**[安全スロットル レベル（Safe Throttle Level）]**、および **[周囲温度ベースのパワー キャッピング（Ambient Temperature Based Power Capping）]**領域が表示されます。

ステップ 4 [Domain Specific Power Limit] 領域で、次のフィールドに値を入力します。

名前	説明
[CPU] フィールド	CPU の電力上限。 指定された範囲内での電力を入力します（ワット数）。
[メモリ]フィールド	メモリの電力上限。 指定された範囲内の電力（ワット単位）を入力します。 （注） このフィールドは、Intel® Optane™ DC 永続メモリ モジュールを搭載したサーバでは使用できません。
[Platform] フィールド	プラットフォームの電力上限。 指定された範囲内での電力を入力します（ワット数）。

ステップ 5 [Suspend Period] 領域で、[Configure] をクリックして、中断期間を特定の期間と日付に設定します。

ステップ 6 [Safe Throttle Level] 領域で、次のフィールドに値を入力します。

名前	説明
[フェールセーフタイムアウト（Failsafe Timeout）] フィールド	内部障害（プラットフォームやCPUの電力測定値の欠如など）がパワー キャッピングに影響を及ぼしている場合に適用される、安全なスロットル ポリシー。 値（秒単位）を入力します。
[CPU] フィールド	CPU のスロットリング レベル。 範囲は、0から100までです（パーセント）。
[メモリ]フィールド	メモリのスロットリング レベル。 範囲は、0から100までです（パーセント）。
[プラットフォーム（Platform）] フィールド	プラットフォームのスロットリング レベル。 範囲は、0から100までです（パーセント）。

ステップ 7 **[周囲温度ベースのパワー キャッピング（Ambient Temperature Based Power Capping）]**領域で、次のフィールドに値を入力します。

名前	説明
[プラットフォーム温度トリガー（Platform Temp Trigger）] フィールド	インレット（前面パネル）温度センサー値（摂氏）。 （注） プラットフォームのインレット温度が指定された上限を超えると、システムは温度による電力制限値をパワーキャッピング上限として使用します。
[温度による電力制限（Thermal Power Limit）] フィールド	維持する電力制限（ワット単位）。

ステップ 8 [Save Changes] をクリックします。

電力プロファイルのデフォルトへのリセット

このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバーだけです。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 **[シャーシ（Chassis）]**メニューで **[電源管理（Power Management）]** をクリックします。

ステップ 3 [Power Profiles] 領域で、[Reset Profiles to Default] ボタンをクリックします。

（注） この操作により、すべての電力プロファイル設定が工場出荷時のデフォルト値にリセットされ、パワー キャッピングが無効になります。

ステップ 4 [Save Changes] をクリックします。

電力モニタリング

電力モニタリングは、ホストの電源がオンになる時点またはホストが起動する時点から開始します。この機能は、プラットフォーム、CPU、メモリ ドメインから電力消費に関する統計情報を収集し、収集期間における最小測定値、最大測定値、および平均測定値を提供します。これらの計測値を使用して、ドメインの電力消費トレンドを計算できます。Cisco IMC は、さまざまな期間（時間、日、週など）のグラフをプロットするため、この電力消費統計値を収集して保存します。

（注） 追加で統計情報収集ポリシーを作成することはできません。また、既存のモニタリング ポリシーは削除できません。デフォルト ポリシーを変更することだけが可能です。

電力モニタリングの概要の表示

このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバーだけです。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 **[シャーシ（Chassis）]**メニューで **[電源管理（Power Management）]** をクリックします。

ステップ 3 [作業（Work）] ペインで、[電力モニタリング（Power Monitoring）] タブをクリックします。

ステップ 4 [電力モニタリングの概要（Power Monitoring Summary）] 領域で、次の情報を確認します。

次の表に、最後にリブートされてからシステムとそのコンポーネントによって消費された電力が表示されます。

名前	説明
[Monitoring Period]	システムが最後にリブートされてから現在までのシステムの消費電源モニタリング時間。 モニタリング期間は、日付と HH:MM:SS という形式で表示されます。

（注） **[シャーシ (Chassis)]** の下に **[モニタリング期間 (Monitoring Period)]** が表示されます。

プラットフォーム、**CPU**、および**メモリ**領域は、**サーバ 1** および**サーバ 2** で使用できます。

ステップ 5 [Platform] 領域で、次の情報を確認します。

名前	説明
現在（Current）	現在サーバ、CPU、メモリで使用されている電力（ワット単位）。
[Minimum]	システムが最後にリブートされてから現在までにサーバ、CPU、およびメモリで使用された最小ワット数。
[Maximum]	システムが最後にリブートされてから現在までにサーバ、CPU、およびメモリで使用された最大ワット数。
[Average]	定義された期間におけるサーバ、CPU、およびメモリの平均消費電力量（ワット）。

ステップ 6 [CPU] 領域で、次の情報を確認します。

名前	説明
現在（Current）	現在 CPU で使用されている電力（ワット単位）。
[Minimum]	最後にリブートされてから現在までに CPU で使用された最小ワット数。
[Maximum]	最後にリブートされてから現在までに CPU で使用された最大ワット数。
[Average]	定義された期間におけるサーバ、CPU、およびメモリの平均消費電力量（ワット）。

ステップ 7 [Memory] 領域で、次の情報を確認します。

名前	説明
現在（Current）	現在メモリで使用されている電力（ワット単位）。

名前	説明
[Minimum]	最後にリブートされてから現在までにメモリで使用された最小ワット数。
[Maximum]	最後にリブートされてから現在までにメモリで使用された最大ワット数。
[Average]	定義された期間におけるメモリの平均消費電力量（ワット単位）。

ステップ 8 [Chart Properties] 領域で、グラフ、コンポーネントを確認および更新し、消費電力の詳細を表示します。

名前	説明
[Chart Settings]	チャート プロパティおよびチャートでのデータ表示方法を設定できます。
電力統計情報とサーバー使用率データのダウンロード（Download Power Statistics and Server Utilization Data）	電源統計情報およびホスト サーバの使用状況に関する情報をダウンロードできます。ファイルはローカル ダウンロード フォルダにダウンロードされます。 （注） ダウンロード済みの統計情報ファイルのサイズが256 KB未満の場合、ファイルをダウンロードすると、既存のファイルとは別に、電源統計情報のファイルとホストサーバ使用状況に関する情報のファイルのセットがダウンロードされます。既存のファイルのサイズが 256 KB を超えている場合は、次のファイルセットによって既存のファイルが上書きされます。

名前	説明
[チャート（Chart）] ドロップダウン リスト	選択した期間における各サーバの電力消費傾向を収集できます。次のいずれかになります。 • **過去 1 時間**：5 分おきのグラフを作成します。 • **過去 1 日**：現在の時刻から毎時間のグラフを作成します。 • **過去 1 週間**：毎日のグラフを作成します。

名前	説明
[Component] ドロップダウン リスト	選択した期間の消費電力を表示する対象のコンポーネント。次のいずれかになります。 • **シャーシ** • ***Server 1*** • ***Server 2***
[Domain] ドロップダウン リスト	表示されるデフォルト値は **Platform**です。
[Plot] ボタン	選択したコンポーネントの指定した期間の消費電力が表示されます。
[チャート/テーブル] ビュー（マウスのカーソルを合わせると表示されます）	電源モニタリング サマリを [チャート（Chart）] ビューまたは [テーブル（Table）] ビューのどちらで表示するかを選択します。
[チャート タイプ（Chart Type）]（マウスのカーソルを合わせると表示されます）	表示するチャートのタイプを選択します。次のいずれかを選択できます。 • [折れ線グラフ（Line Chart）]：電力モニタリング データが折れ線グラフで表示されます。 • [縦棒グラフ（Column Chart）]：電力モニタリング データが縦棒グラフで表示されます。 **デフォルトのグラフ**：折れ線グラフです。 （注） [グラフ（Chart）] ドロップダウン リストで [先週（Last Week）] が選択され、複数のコンポーネントが選択された場合、縦棒グラフは表示されず、デフォルトで折れ線グラフが表示されます。このようなシナリオでは、次のメッセージが表示されます。選択した設定では、縦棒グラフをプロットすることはできません。折れ線グラフに戻ります。
[現在（Current）] チェックボックス	このチェックボックスをオンにすると、選択した期間における、選択したコンポーネントの現在の消費電力量がチャートに表示されます。

名前	説明
[平均（Average）] チェックボックス	このチェックボックスをオンにすると、選択した期間における、選択したコンポーネントの平均消費電力量がプロットに表示されます。
[最大（Maximum）] チェックボックス	このチェックボックスをオンにすると、選択した期間における、選択したコンポーネントの最大消費電力量（ワット単位）がプロットに表示されます。
[最小（Minimum）] チェックボックス	このチェックボックスをオンにすると、選択した期間における、選択したコンポーネントの最小消費電力量（ワット単位）がプロットに表示されます。

チャートでの電力統計の表示

このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバーだけです。

始める前に

- パワー キャッピングを有効にする必要があります。
- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 **[シャーシ（Chassis）]**メニューで **[電源管理（Power Management）]** をクリックします。

ステップ 3 [作業（work）] ペインで、[電力モニタリング（Power Monitoring）] タブをクリックします。

ステップ 4 [Power Monitoring] タブで、チャートとコンポーネントを確認して更新し、電力消費の詳細を確認します。

名前	説明
[チャート（Chart）] ドロップダウン リスト	選択した期間における各サーバの電力消費傾向を収集できます。次のいずれかになります。 • [過去 1 時間（Last One Hour）] : 5 分間隔のチャートをプロットします。 • [過去 1 日（Last One Day）] : 現在時刻から 1 時間間隔のチャートをプロットします。 • [過去 1 週間（Last One Week）] : 1 日間隔のチャートをプロットします。
[コンポーネント（Component）] ドロップダウン リスト	選択した期間の消費電力を表示する対象のコンポーネント。次のいずれかになります。 • **Platform** • **CPU** • **メモリ** • **すべて**
[最大（Maximum）] チェックボックス	このチェックボックスをオンにすると、選択した期間における、選択したコンポーネントの最大消費電力量（ワット単位）がプロットに表示されます。
[最小（Minimum）] チェックボックス	オンにすると、選択した期間に選択したコンポーネントが消費した最小ワット数がグラフに表示されます。
[平均（Average）] チェックボックス	オンにすると、選択した期間に選択したコンポーネントが消費した平均電力量がグラフに表示されます。
[現在（Current）] チェックボックス	オンにすると、選択した期間に選択したコンポーネントが消費した現在の電力がグラフに表示されます。
[Plot] ボタン	指定した期間に選択したコンポーネントが消費した電力が表示されます。

電力測定値チャートに、選択されている期間における各種コンポーネントの電力消費値がプロットされます。これらの電力消費値は、ホストの電源がオンになった時点から取り込まれます。電力プロファイルが有効な場合、チャートには電力制限が赤色の線としてプロットされま

す。このプロットから、システムの電力消費トレンドを確認できます。特定のドメインに設定されている電力制限値を確認するには、これらのトレンド線にマウスを移動します。

標準プロファイルを選択する場合、トレンド線は電力制限を示します。詳細プロファイルを選択する場合、電力プロファイル設定に応じてトレンド線はCPU、メモリ、およびプラットフォームの電力制限を示します。

（注） [Power Cap Configuration] タブでプロファイルが無効な場合は、トレンド線は表示されません。

ステップ 5 [Save Changes] をクリックします。

電力統計とサーバ使用率データのダウンロード

このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバーだけです。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 **[シャーシ（Chassis）]**メニューで **[電源管理（Power Management）]** をクリックします。

ステップ 3 [作業（Work）] ペインで、[電力モニタリング（Power Monitoring）] タブをクリックします。

ステップ 4 **[電力モニタリング（Power Monitoring）]** タブで **[電力統計とサーバ使用率データのダウンロード（Download Power Statistics and Server Utilization Data）]** をクリックします。

ファイルはローカル ダウンロード フォルダにダウンロードされます。

（注） ダウンロード済みの統計情報ファイルのサイズが 256 KB 未満の場合、ファイルをダウンロードすると、既存のファイルとは別に、電源統計情報のファイルとホストサーバ使用状況に関する情報のファイルのセットがダウンロードされます。既存のファイルのサイズが 256 KB を超えると、次のファイルのセットが既存のファイルを上書きします。

電力復元ポリシーの設定

電力復元ポリシーによって、シャーシの電力供給が失われた後、サーバーに電力を復元する方法が決定されます。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[コンピューティング（Compute）]メニューをクリックします。

ステップ 2 作業ウィンドウで**[電源ポリシー（Power Policies）]**タブをクリックします。

ステップ 3 [Power Restore Policy] 領域で、次のフィールドを更新します。

名前	説明
[電力復元ポリシー（Power Restore Policy）] ドロップダウン リスト	予期しない電源損失後、シャーシ電源が復元されたときに実行されるアクション。次のいずれかになります。 • [電源オフ（Power Off）]：手動で再起動されるまで、サーバーはオフのままです。 • [電源オン（Power On）]：電源が復元されたときに、サーバーは通常どおりに起動できます。サーバーはただちに再起動できますが、任意で一定の遅延またはランダムな遅延後に再起動することもできます。 • [最後の状態を復元（Restore Last State）]：サーバーが再起動し、システムは電源喪失前に実行されていたプロセスの復元を試みます。

ステップ 4 [Save Changes] をクリックします。

ファン ポリシーの設定

ファン制御ポリシー

ファン制御ポリシーを使ってファンの速度を制御することにより、サーバの消費電力を削減し、ノイズ レベルを下げることができます。これらのファン ポリシーが導入される前は、いずれかのサーバコンポーネントの温度が設定済みしきい値を超過した場合に、ファン速度が自動的に増加しました。ファン速度を低く抑えるために、通常、コンポーネントのしきい値温度を高い値に設定しました。この動作はほとんどのサーバ構成に最適でしたが、次のような状況に対処できませんでした。

- 最大の CPU パフォーマンス

高パフォーマンスを得るには、いくつかの CPU を設定済みしきい値よりもかなり低い温度に冷却する必要があります。これは非常に高速なファン速度を必要とし、結果として電力消費とノイズ レベルが増大しました。

- 低電力消費

  電力消費を最も低く抑えるにはファンを非常に遅くする必要があり、場合によっては、ファン停止をサポートするサーバで完全に停止する必要があります。ただし、ファンの速度を遅くすると、結果としてサーバが過熱します。この状況を回避するには、可能な最低速度よりもやや速くファンを作動させる必要があります。

ファンポリシーを導入すると、サーバ内のコンポーネントに基づき、そのサーバに適したファン速度を決定できます。さらに、最大の CPU パフォーマンスと低消費電力に関連する問題に対処するために、ファン速度を設定することができます。

次のファン ポリシーの中から選択できます。

- [バランス（Balanced）]：この設定はほとんどのサーバー構成を冷却できますが、PCIe カードは容易に過熱するため、これらのカードのあるサーバーには適していない可能性があります。
- [パフォーマンス（Performance）]：この設定は、高パフォーマンスを得るために最高速度でファンを作動させる必要のあるサーバー構成に使用できます。この設定により、ファン速度は、Balanced ファン ポリシーで設定されたファン速度と同じ速度またはより高速で動作します。

（注） このオプションを使用できるのは一部のCシリーズサーバーだけです。

- **[低電力（Low Power）]**：この設定は、PCIe カードが含まれない最小構成のサーバに最適です。
- **[高電力（High Power）]**：このポリシーは、容易に過熱して高温になる PCIe カードを含むサーバーに最適です。
- **[最大電力（Maximum Power）]**：この設定は、非常に高いファン速度を必要とするサーバー構成に使用できます。このポリシーは、容易に過熱して非常に高温になる PCIe カードを含むサーバに最適です。
- **Acoustic**：この設定は、ファンのノイズ レベルを設定するために使用できます。これにより、サーバのノイズ リダクションが可能になります。

  このポリシーを適用すると、システム パフォーマンスに影響するパフォーマンス スロットリングが発生する可能性があります。過剰な温度またはパフォーマンス イベントがイベント ログに記録されている場合は、**低電力**などの標準のファン制御ポリシーを選択します。これは、中断のない変更です。

（注） このオプションは、Cisco UCS C220 M5、C240 SD M5、C240 M5、C220 M6、C240 M6、C245 M6、C225 M6、C220 M7、および C240 M7 サーバーでのみ使用できます。 これらのサーバーでは、**[音響（Acoustic）]** がデフォルトのファン ポリシーです。

他のサーバーの場合、デフォルトのファンポリシーは、サーバー構成とサーバーに存在する PCIe カードの数によって異なります。

（注） Cisco UCS M5 サーバーの場合、Cisco IMC でファン ポリシーを設定することはできますが、実際のファン作動速度はサーバーの構成要件により決定されます。PCIe カードには、温度要件に応じて最小ファン速度のタグが付けられています。サーバーにこれらの PCIe カードが装備されている場合、タグ付けされた要件を下回るファンポリシーを構成することはできません。

[構成ステータス（Configuration Status）] には、Cisco UCS M5 サーバーで構成されたファンポリシーのステータスが表示されます。次のいずれかになります。

- [SUCCESS]：選択されたファンポリシーはサーバで実行されている実際のファン速度に一致します。
- [PENDING]：設定されたファンポリシーはまだ有効になっていません。この原因として、以下が考えられます。
  - サーバの電源がオフになっている
  - BIOS POST が完了していない
- [ファン ポリシーの上書き（FAN POLICY OVERRIDE）]：指定されたファン速度を、サーバーの設定要件によって決定された実際の速度で上書きします。

（注）
- Cisco UCS C220 M7、C240 M7、C220 M6、C240 M6、UCS C220 M5、C240 M5、C240 SD M5、C125 M5、C480 M5、C480-M5ML の場合、**[適用されるファン ポリシー（Applied fan policy）]** は、サーバーに存在する PCIe カードによって異なります。
- Cisco UCS C225 M6 および C245 M6 の場合、**[適用されるファン ポリシー（Applied fan policy）]** は、サーバーに存在する PCIe カードまたは特定の CPU タイプによって異なります。

ファン ポリシーの設定

サーバー設定およびサーバー コンポーネントに基づいて適切なファン ポリシーを決定できます。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 作業ウィンドウで**[電源ポリシー（Power Policies）]**タブをクリックします。

ステップ 3 [Configured Fan Policy] 領域で、ドロップダウン リストからファン ポリシーを選択します。次のいずれかを指定できます。

名前	説明
[ファン ポリシー（Fan Policy）] ドロップダウン リスト	

名前	説明
	次のいずれかになります。 • [バランス（Balanced）]：この設定はほとんどのサーバー構成を冷却できますが、PCIe カードは容易に過熱するため、これらのカードのあるサーバーには適していない可能性があります。 • [パフォーマンス（Performance）]：この設定は、高パフォーマンスを得るために最高速度でファンを作動させる必要のあるサーバー構成に使用できます。 この設定により、ファン速度は、Balanced ファン ポリシーで設定されたファン速度と同じ速度またはより高速で動作します。 （注） このオプションを使用できるのは一部の C シリーズ サーバーだけです。 • **[低電力（Low Power）]**：この設定は、PCIe カードが含まれない最小構成のサーバに最適です。 • **[高電力（High Power）]**：このポリシーは、容易に過熱して高温になる PCIe カードを含むサーバーに最適です。 • **[最大電力（Maximum Power）]**：この設定は、非常に高いファン速度を必要とするサーバー構成に使用できます。このポリシーは、容易に過熱して非常に高温になる PCIe カードを含むサーバに最適です。 • **Acoustic**：この設定は、ファンのノイズ レベルを設定するために使用できます。これにより、サーバのノイズ リダクションが可能になります。 このポリシーを適用すると、システム パフォーマンスに影響するパフォーマンス スロットリングが発生する可能性があります。過剰な温度またはパフォーマンス イベントがイベント ログに記録されている場合は、**低電力**などの標準のファン制御ポリシーを選択します。これは、中断

名前	説明
	のない変更です。 （注） このオプションは、Cisco UCS C220 M5、C240 SD M5、C240 M5、C220 M6、C240 M6、C225 M6、C245 M6、C220 M7、および C240 M7 サーバーでのみ使用できます。 Cisco UCS C シリーズ M6 サーバー、Cisco UCS C シリーズ M7 サーバー、および Cisco UCS C240 SD M5 サーバーの場合、**[アコースティック（Acoustic）]** がデフォルトのファン ポリシーです。 他のすべてのサーバーでは、デフォルトのファンポリシーは **[低電力（Low Power）]** です。

名前	説明
[Applied Fan Policy] フィールド	サーバ上で稼働するファンの実際の速度。 設定済みのファン ポリシーが有効になっていない場合は、[なし（N/A）]が表示されます。設定されたファン ポリシーは、サーバーの電源が入り、POST が完了すると有効になります。 （注） • Cisco UCS C220 M7、C240 M7、C220 M6、C240 M6、UCS C220 M5、C240 M5、C240 SD M5、C125 M5、C480 M5、C480-M5ML の場合、**[適用されるファン ポリシー（Applied Fan Policy）]** は、サーバーに存在する PCIe カードによって異なります。 • Cisco UCS C225 M6 および C245 M6 の場合、**[適用されるファン ポリシー（Applied Fan Policy）]** は、サーバーに存在する PCIe カードまたは特定のタイプの CPU によって異なります。

名前	説明
[Configuration Status] フィールド	ファン ポリシーの設定のステータス。次のいずれかになります。 • [成功（SUCCESS）]：設定したファン速度とサーバで実行している実際のファン速度が一致しています。 • [保留中（PENDING）]：設定されているファン ポリシーが有効になっていません。この原因として、以下が考えられます。 • サーバの電源がオフになっている • BIOS POST が完了していない • [ファン ポリシーの上書き（FAN POLICY OVERRIDE）]：指定されたファン速度を、サーバーの設定要件によって決定された実際の速度で上書きします。 （注） Cisco UCS C220 M7、C240 M7、C220 M6、C240 M6、UCS C220 M5、C240 M5、C240 SD M5、C125 M5、C480 M5、C480 M5 ML の場合、**[適用されるファン ポリシー（Applied Fan Policy）]** は、サーバーに存在する PCIe カードによって異なります。 Cisco UCS C225 M6 および C245 M6 の場合、**[適用されるファン ポリシー（Applied Fan Policy）]** は、サーバーに存在する PCIe カードまたは特定の CPU タイプによって異なります。
[急速冷却の有効化（Enable Aggressive Cooling）] チェックボックス	急速冷却を有効にするには、このオプションをオンにします。 （注） このオプションは、Cisco UCS C220 M7、C240 M7、C220 M6、C240 M6、C245 M6、および C225 M6 サーバーでのみ使用できます。

ステップ 4 **[Save Changes]**をクリックします。

DIMM のブラックリスト化の設定

DIMM のブラックリスト化

Cisco IMC で、デュアル インライン メモリ モジュール（DIMM）の状態は、SEL イベント レコードに基づいています。BIOS が BIOS ポスト中のメモリ テスト実行時に 16000 のエラー件数を伴う修正不可能なメモリ エラーまたは修正可能なメモリ エラーに遭遇した場合、DIMM は不良と判断されます。不良とマークされた DIMM は機能しないデバイスと見なされます。

DIMM のブラックリスト化を有効にすると、Cisco IMC はメモリ テスト実行メッセージをモニタし、あらゆる時点でDIMM SPD データ内でメモリ エラーに遭遇した DIMM をブラックリストに載せます。これにより、ホストはこれらの DIMM をマップから外すことができます。

DIMM がマップから外されるかまたはブラックリストに追加されるのは、修正不可能なエラーが発生した場合だけです。DIMM がブラックリスト化されると、同じチャネル上にある他の DIMM が無視されるかディセーブルとなり、その DIMM は不良として見なされなくなります。

（注） 16000 修正可能エラーの場合、DIMM がマップから外されることや、ブラックリストに追加されることはありません。

DIMM のブラックリストのイネーブル化

始める前に

- 管理者としてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [シャーシ（Chassis）] メニューで [インベントリ（Inventory）] をクリックします。

ステップ 3 [Inventory] ペインの [Memory] タブをクリックします。

ステップ 4 [Memory] ペインの [DIMM Black Listing] 領域で、[Enable DIMM Black List] チェックボックスをオンにします。

BIOS の設定

Configuring BIOS Settings

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[コンピューティング（Compute）]メニューをクリックします。

ステップ 2 [コンピューティング（Compute）] メニューで、[BIOS] タブをクリックします。

ステップ 3 [BIOS] タブで、[BIOSの設定（Configure BIOS）] タブをクリックします。

ステップ 4 サーバー モデル別 BIOS パラメータ （515 ページ）を参照して次のタブを更新します：

- I/O
- サーバ管理
- セキュリティ
- プロセッサ
- メモリ
- 電源/パフォーマンス

（注） 使用可能な BIOS パラメータは、使用しているサーバのモデルによって異なります。

重要 1タブ 個のタブで使用できる BIOS パラメータは、表示しているタブのパラメータだけではなく、すべての利用可能なタブのパラメータに影響を与える可能性があります。

BIOS セットアップの開始

始める前に

- サーバの電源が投入されている。
- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 **作業ウィンドウで [BIOS]** タブをクリックします。

ステップ 3 [Actions] 領域で [Enter BIOS Setup] をクリックします。

ステップ 4 プロンプトで [OK] をクリックします。
BIOS セットアップの開始が有効になります。再起動時に、サーバは BIOS セットアップを開始します。

BIOS CMOS のクリア

始める前に

- サーバの電源が投入されている。
- このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 **作業ウィンドウで [BIOS]** タブをクリックします。

ステップ 3 **[Actions]**領域の **[Clear BIOS CMOS]** をクリックします。

ステップ 4 **[OK]**をクリックして確定します。
BIOS CMOS がクリアされます。

製造元のカスタム BIOS 設定の復元

始める前に

- サーバーの電源が投入されている。
- このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [コンピューティング（Compute）] メニューをクリックします。
ステップ 2 **[コンピューティング（Compute）]** メニューでサーバを選択します。
ステップ 3 **作業ウィンドウで [BIOS]** タブをクリックします。
ステップ 4 [Actions] 領域で、[Restore Manufacturing Custom Settings] をクリックします。
ステップ 5 サーバをすぐに再起動する場合は、**[はい (Yes)]** をクリックします。
ステップ 6 [OK] をクリックして確定します。

BIOS デフォルトの復元

始める前に

- サーバの電源が投入されている。
- このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [コンピューティング（Compute）] メニューをクリックします。
ステップ 2 **[コンピューティング（Compute）]** メニューでサーバを選択します。
ステップ 3 **作業ウィンドウで [BIOS]** タブをクリックします。
ステップ 4 **[アクション (Actions)]** 領域で、**[デフォルトの復元 (Restore Defaults)]** をクリックします。
ステップ 5 サーバをすぐに再起動する場合は、**[はい (Yes)]** をクリックします。
ステップ 6 [OK] をクリックして確定します。

BIOS プロファイル

Cisco UCS サーバでは、デフォルトのトークン ファイルはすべての S3260 サーバ プラットフォームに使用可能で、グラフィック ユーザ インターフェイス（GUI）、CLI インターフェイス、および XML API インターフェイスを使用して、これらのトークンの値を設定できます。サーバー パフォーマンスを最適化するには、これらのトークン値を特定の組み合わせで設定する必要があります。

BIOS プロファイルを設定することで、正しい組み合わせのトークン値が設定された事前設定トークン ファイルを使用することができます。利用可能な事前設定プロファイルには、仮想

化、高性能、低電力などがあります。シスコの Web サイトから事前設定トークン ファイルのさまざまなオプションをダウンロードし、BMC を介してサーバに適用できます。

ダウンロードしたプロファイルを編集し、トークンの値を変更したり、新しいトークンを追加したりできます。これにより、応答時間なしで、要件に合わせてプロファイルをカスタマイズできます。

BIOS プロファイルのアップロード

リモート サーバの場所またはブラウザ クライアントから BIOS プロファイルをアップロードできます。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 **作業ウィンドウで [BIOS]** タブをクリックします。

ステップ 3 **[BIOS プロファイルの設定（Configure BIOS Profile）]**タブをクリックします。

ステップ 4 リモート サーバの場所を使用して BIOS プロファイルをアップロードするには、**[BIOS プロファイル（BIOS Profile）]**領域で **[アップロード（Upload）]**ボタンをクリックします。

ステップ 5 [**BIOS プロファイルのアップロード（Upload BIOS Profile）]** ダイアログボックスで、次のフィールドを更新します。

名前	説明
[Upload BIOS Profile from] ドロップダウン リスト	リモート サーバーのタイプ。次のいずれかになります。 • **TFTP** • **FTP** • **SFTP** • **SCP** • **[HTTP]**
[サーバーIP/ホスト名（Server IP/Hostname）] フィールド	BIOSプロファイル情報を有効にするサーバーの IP アドレスまたはホスト名。[Upload BIOS Profile from] ドロップダウン リストの設定によって、フィールド名は異なる場合があります。

名前	説明
[パスおよびファイル名（Path and Filename）] フィールド	リモート サーバー上の BIOS プロファイルのパスおよびファイル名。
[ユーザ名（Username）] フィールド	リモート サーバのユーザ名。
[パスワード（Password）]フィールド	リモート サーバのパスワード。
[アップロード（Upload）] ボタン	選択したBIOSプロファイルをアップロードします。 （注） このアクションを実行中にリモート サーバのタイプとして SCP または SFTP を選択した場合、ポップアップ ウィンドウが表示され、そこに *[*サーバ（*RSA*）鍵フィンガープリントは *<server_finger_print _ID>* です。続行しますか*?*（*Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*）*]* というメッセージが表示されます。サーバフィンガープリントの信頼度に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーをベースにしており、接続先ホストの特定や確認に利用できます。
[Cancel]ボタン	サーバに保管されているファームウェア バージョンには変更を加えることなく、ウィザードを閉じます。

ステップ 6 ブラウザ クライアントを使用して BIOS プロファイルをアップロードするには、**[BIOS プロファイル（BIOS Profile）]** 領域で **[アップロード（Upload）]** ボタンをクリックします。

ステップ 7 **[BIOS プロファイルのアップロード（Upload BIOS Profile）]** ダイアログボックスで、次のフィールドを更新します。

名前	説明
[File] フィールド	アップロードする BIOS プロファイル。

名前	説明
[Browse] ボタン	ダイアログボックスが表示され、そこで、該当するファイルにナビゲートすることができます。

次のタスク

BIOS プロファイルをアクティブにします。

BIOS プロファイルのアクティブ化

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 **作業ウィンドウで [BIOS]** タブをクリックします。

ステップ 3 **[BIOS プロファイルの設定（Configure BIOS Profile）]** タブをクリックします。

ステップ 4 **[BIOS プロファイル（BIOS Profile）]** 領域から BIOS プロファイルを選択し、**[アクティブ化（Activate）]**をクリックします。

ステップ 5 プロンプトで **[はい（Yes）]**をクリックし、BIOS プロファイルをアクティブにします。

BIOS プロファイルの削除

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 **[コンピューティング（Compute）]**メニューでサーバを選択します。

ステップ 3 **作業ウィンドウで [BIOS]** タブをクリックします。

ステップ 4 [BIOS Profile] 領域から BIOS プロファイルを選択し、[Delete] をクリックします。

ステップ 5 プロンプトで **[OK]**をクリックし、BIOS プロファイルを削除します。

BIOS プロファイルのバックアップ

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 **[コンピューティング（Compute）]**メニューでサーバを選択します。

ステップ 3 **作業ウィンドウで [BIOS]** タブをクリックします。

ステップ 4 [BIOS Profile] 領域から BIOS プロファイルを選択し、[Take Backup] をクリックします。

ステップ 5 プロンプトで**[OK]**をクリックし、BIOS プロファイルのバックアップを作成します。

次のタスク

BIOS プロファイルをアクティブにします。

BIOS プロファイルの詳細の表示

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 **[コンピューティング（Compute）]**メニューでサーバを選択します。

ステップ 3 **作業ウィンドウで [BIOS]** タブをクリックします。

ステップ 4 [BIOS Profile] 領域から BIOS プロファイルを選択し、[Details] をクリックします。

ステップ 5 **[BIOS プロファイルの詳細（BIOS Profile Details）]**ウィンドウで、次の情報を確認します。

名前	説明
[トークン名（Token Name）] カラム	BIOS プロファイルのトークン名が表示されます。
[表示名（Display Name）] カラム	BIOS プロファイルのユーザ名が表示されます。
[プロファイル値（Profile Value）] カラム	アップロードされたファイルに設定された値が表示されます。
[実際の値（Actual Value）] カラム	アクティブな BIOS 設定の値が表示されます。

セキュアブート証明書の管理

4.2 (2a) リリース以降、Cisco IMC では、設定されたセキュア HTTP ブート デバイス用に最大 10 個の証明書をアップロードできます。構成された特定のブート デバイスの新しい証明書を削除してアップロードすることもできます。Cisco IMC では、最大 10 個のルート CA 証明書をアップロードできます。

セキュアブート証明書の詳細の表示

アップロード済みのセキュア ブート証明書の詳細を表示できます。

始める前に

このタスクを実行するには、admin 権限を持つユーザーとして admin としてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 **作業ウィンドウで [BIOS]** タブをクリックします。

ステップ 3 **[セキュアブート証明書の管理（Secure Boot Certificate Management）]**タブをクリックします。

ステップ 4 証明書の表から、表示したい証明書を選択します。

ステップ 5 テーブルの上にある **[セキュア ブート証明書の表示（View Secure Boot Certificate）]** アイコンをクリックします。

ステップ 6 **[セキュア ブート証明書の表示（View Secure Boot Certificate）]** ダイアログ ボックスが表示されます。

以下の情報を確認できます。

表 *2 :* [一般（*General*）] 領域

フィールド	説明
[証明書識別子（Certificate ID）] フィールド	Cisco IMC によって割り当てられた証明書識別子を表示します。
[Serial Number] フィールド	サーバーのシリアル番号。
[Valid From] フィールド	証明書の有効期間の開始日
[Valid To] フィールド	証明書の失効日。

表 *3 :* サブジェクト エリア

フィールド	説明
[Country Code] フィールド	証明書の国コード。
[Locality] フィールド	証明書の地域。
[State Name] フィールド	証明書の状態。
[組織名（Organization Name）] フィールド	証明書の組織。
[Organization Unit] フィールド	証明書の組織単位。
[Common Name] フィールド	証明書名。

表 *4 :* 発行者エリア

フィールド	説明
[Country Code] フィールド	発行者の国コード。
[Locality] フィールド	発行者の地域。
[State Name] フィールド	発行者の状態。
[組織名（Organization Name）] フィールド	発行者の組織。
[Organization Unit] フィールド	発行者の組織単位。
[Common Name] フィールド	発行者名。

セキュア ブート証明書のアップロード

ブート証明書は、リモート サーバーの場所またはローカルの場所からアップロードできます。

始める前に

- このタスクを実行するには、admin 権限を持つユーザーとして admin としてログインする必要があります。
- ローカルアップロードを使用してアップロードする場合は、証明書ファイルがローカルでアクセス可能なファイル システムに存在することを確認してください。
- 生成された証明書のタイプが [Server] であることを確認します。
- 次の証明書形式がサポートされています。
  - .crt
  - .cer
  - .pem

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 作業ウィンドウで **[BIOS]** タブをクリックします。

ステップ 3 **[セキュアブート証明書の管理（Secure Boot Certificate Management）]**タブをクリックします。

ステップ 4 起動証明書をアップロードするには、アップロード ボタン（+）をクリックします。

ステップ 5 次のいずれかの方法を使用して、証明書をアップロードできます：

- 証明書の貼り付けテキスト フィールドに証明書を直接貼り付けます
- ローカル ロケーションからアップロード
- リモートロケーションからアップロード

[セキュア ブート証明書の追加（Add Secure Boot Certificate）] ダイアログ ボックスで、証明書をアップロードする方法に従ってフィールドを更新します：

表 *5:* セキュアブート証明書の追加

フィールド	説明
[セキュア ブート証明書を貼り付け（Paste Secure Boot Certificate）] ラジオ ボタン	署名付き証明書の内容全体をコピーして、証明書の内容を貼り付けテキスト フィールドに貼り付けることができます。 （注） アップロードの前に、証明書に署名が付されていることを確認します。
[ローカルラジオ（Upload from local）] ボタンからアップロード	追加する認証局証明書ファイルの場所を参照してナビゲートできます。

フィールド	説明
[リモート ロケーションからアップロード（Download from remote location）] ラジオ ボタン	リモートロケーションの証明書を選択してアップロードできます。次の詳細を入力します。 • からセキュアブート証明書をアップロード— • TFTP サーバ • FTP サーバ • SFTP サーバ • SCP サーバ • HTTP サーバ • **[サーバー IP/ホスト名（Server IP/Hostname）]**— 証明書ファイルの保管先とするサーバーの IP アドレスまたはホスト名。ドロップダウン リストの証明書アップロードの設定に応じて、フィールドの名前が異なる場合があります。 • **[パスおよびファイル名（Path and Filename）]**：リモート サーバーにファイルをアップロードする際に Cisco IMC が使用する必要があるパスおよびファイル名。 • **[ユーザ名（Username）]**— リモート サーバーにログインするためにシステムが使用するユーザー名。プロトコルが TFTP または HTTP の場合、このフィールドは適用されません。 • **[パスワード（Password）]**—リモート サーバーのユーザー名のパスワード。プロトコルが TFTP または HTTP の場合、このフィールドは適用されません。
セキュアブート証明書ボタンのアップロード	証明書をサーバーにアップロードできるようにします。

セキュアブート証明書の削除

Cisco IMC にすでにアップロードされているブート証明書を削除できます。

始める前に

このタスクを実行するには、admin 権限を持つユーザーとして admin としてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 **作業ウィンドウで [BIOS]** タブをクリックします。

ステップ 3 **[セキュアブート証明書の管理（Secure Boot Certificate Management）]**タブをクリックします。

ステップ 4 証明書の表から、削除したい証明書を選択します。

ステップ 5 テーブルの上にある **[セキュア ブート証明書の削除（Delete Secure Boot Certificate）]** アイコンをクリックします。

ステップ 6 確認のために [はい（Yes）] をクリックします。

前面パネルの動的温度しきい値の設定

前面パネルの動的温度しきい値オプションを使用すると、前面パネルの温度センサーの重要な上限しきい値を設定できます。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [シャーシ（Chassis）] メニューの [センサー（Sensors）] をクリックします。

ステップ 3 [センサー（Sensors）] ペインの [温度（Temperature）] タブをクリックします。

ステップ 4 [前面パネルの動的温度しきい値（Dynamic Front Panel Temperature Threshold）] 領域を展開し、[クリティカル（Critical）] フィールドで前面パネルの温度センサーの重要な上限しきい値を入力します。8 ～ 50 の値を入力できます。

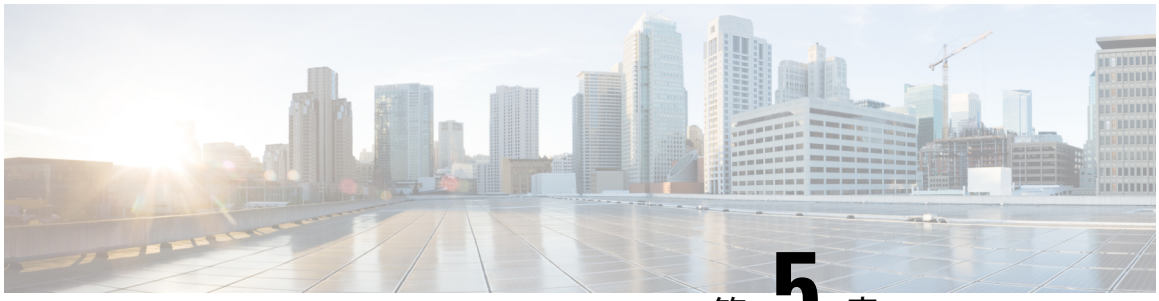
ステップ 5 **[Save Changes]**をクリックします。

永続メモリ モジュール

Cisco UCS C シリーズ リリース 4.0(4) は、Intel® Optane™ Data Center 永続メモリ モジュール (第二世代インテル® Xeon® Scalable プロセッサに基づく UCM M5 サーバ上) のサポートを導入します。永続メモリ モジュールは、第二世代インテル® Xeon® Scalable プロセッサでのみ使用できます。

永続メモリ モジュールは、メモリの低遅延とストレージの永続化を実現する不揮発性メモリ モジュールです。永続メモリ モジュールに保存されているデータは、他のストレージ デバイスに比べてすぐにアクセスでき、電源サイクルで保持されます。

永続メモリ モジュールの設定の詳細については、『Cisco UCS: Intel® Optane™ Data Center 永続メモリモジュールの設定と管理』を参照してください。



第 5 章

サーバーのプロパティの表示

この章は、次の内容で構成されています。

Viewing Server Utilization

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [Chassis] メニューの [Summary] をクリックします。

[概要 (Summary)] ノードは、**[シャーシ プロパティ (Chassis Properties)]**、**[シャーシ ステータス (Chassis status)]**、**[Cisco IMC情報 (Cisco IMC Information)]**、**[電源使用率 (Power Utilization)]**、**[サーバ使用率 (Server Utilization)]** についての情報を提供します。

システムのCPU、メモリ、およびI/O使用率のリアルタイムの監視が、[1秒あたりのコンピュータ使用状況（CUPS）（Computer Usage Per Second (CUPS)）] として提供されます。これは OS からは独立しており、CPU リソースを消費しません。

Cisco のサーバーは以下のセンサーをモニターします。

プラットフォーム CUPS センサー：計算、メモリ、および I/O リソース使用率の値を、プラットフォーム CUPS インデックスの形式で提供します。

コア CUPS センサー： 計算使用率の値を提供します。

メモリ CUPS センサー： メモリ使用率の値を提供します。

IO CUPS センサー：I/O リソース使用率の値を提供します。

（注） CUPS センサーはハードウェア レベルのセンサーであり、値は OS ベースのツールからの値とは一致しません。

これらの使用率の値は、プラットフォームの構成要素（CPU とチップセット）によって提供される専用のサイドバンドテレメトリ カウンタのセットからのデータを照会して取得されます。これらのカウンタは**リソース モニタリング カウンタ（RMC**）と呼ばれます。

RMC は、3 つの主要なプラットフォーム リソースの分野である CPU、メモリ、および I/O に関連するリアルタイムの情報を提供します。これらの分野のそれぞれの使用率情報は、リソース インスタンス レベルの個別のカウンタを集約して取得されます。

ステップ 3 [サーバー使用率（Server Utilization）] 領域で、次の情報を確認します。

名前	説明
全体の使用率（%）	CUPSインデックスとして測定されます。これは、プラットフォーム使用率の高レベル アセスメントを手早く提供するために使用される複合メトリックです。CUPSインデックスは、したがって、サーバーで使用可能な計算能力の余裕の尺度です。そのため、システムが大きな CUPS インデックスを示す場合、システムに追加の負荷をかけるには限られた余裕しかないということになります。リソース消費が減少すると、システムの CUPS インデックスは低下します。低いCUPSインデックスは、計算能力に大きな余裕があることを示しており、そのサーバーが、新たなワークロードを受け取る、あるいは、電力消費を減らすためにワークロードを他へ移してサーバーの電力の状態をより低くする際の主要な対象となることを示しています。こうしたワークロードのモニタリングは、データセンターのワークロードについての高レベルで包括的な視点を提供するために、データセンター全体で適用できます。
CPU Utilization (%)	CPU RMC は CPU 使用率のメトリックを提供します。これらは、集約された個別の CPU コア カウンタであり、パッケージ内のすべてのコアの累積的な使用を可能にします。

名前	説明
メモリ使用率（%）	メモリ RMCはメモリ使用率のメトリックを提供します。これらは、各メモリ チャネルまたはメモリ コントローラのインスタンスで発生するメモリのトラフィックを測定する個別のカウンタです。これらは集計されて、パッケージ内のすべてのメモリ チャネルの累積メモリ トラフィックを測定します。
I/O 使用率（%）	IO RMC は IO 使用率のメトリックを提供します。これらは、PCI Express ルート コンプレックスのルート ポートごとに 1 つある個別のカウンタであり、当該のルート ポートおよびその下のセグメントから生じる、またはそれらに向けられる PCI Express のトラフィックを測定します。これらのカウンタは集計されて、パッケージから生じるすべての PCI Express セグメントの PCI express トラフィックを測定します。PCI Express ルート ポートは 1 つの PCI セグメントを表しており、そのため、そのセグメントによって生じるトラフィック全体を搬送する単一の中心的なコンポーネントということになります。

CPU のプロパティの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [シャーシ（Chassis）] メニューで [インベントリ（Inventory）] をクリックします。

ステップ 3 [Inventory] ペインの [CPUs] タブをクリックします。

ステップ 4 各 CPU で次の情報を確認します。

名前	説明
[Socket Name] フィールド	CPU が装着されているソケット。
[Vendor]フィールド	CPU のベンダー。
[Status] フィールド	CPU のステータス。

名前	説明
[Family] フィールド	この CPU が属するファミリ。
[Version] フィールド	CPU のバージョン情報。
[Speed] フィールド	CPU の速度（メガヘルツ単位）。
[Number of Cores] フィールド	CPU のコアの数。
[Signature] フィールド	CPU の署名情報。
[Number of Threads] フィールド	CPU が同時に処理できる最大スレッド数。

メモリのプロパティの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。
ステップ 2 [シャーシ（Chassis）] メニューで [インベントリ（Inventory）] をクリックします。
ステップ 3 [Inventory] ペインの [Memory] タブをクリックします。
ステップ 4 [Memory Summary] 領域で、メモリに関する次のサマリー情報を確認します。

名前	説明
[Memory Speed] フィールド	メモリ速度（メガヘルツ単位）。
[Total Memory] フィールド	すべての DIMM が完全に機能している場合に、サーバーで使用できるメモリの合計量。

名前	説明
[Effective Memory] フィールド	現在サーバーが使用できる実際のメモリの量。 サーバに Intel® Optane™ DC 永続メモリモジュールが搭載されている場合、有効なメモリは次のように計算されます。 • **メモリ モードまたは混合モード**: すべての DCPMM メモリのおおよその合計です。 （注） メモリ モードと混合モードは、一部のサーバでのみ使用できます。 • **Appdirect モード**: すべての DCPMM メモリと DRAMS メモリのおおよその合計です。 （注） Cisco UCS C シリーズ M7 サーバーは DCPMM メモリをサポートしていません。
[Redundant Memory] フィールド	冗長ストレージに使用されるメモリの量。
[Failed Memory] フィールド	現在障害が発生しているメモリの量（メガバイト単位）。
[Ignored Memory] フィールド	現在使用できないメモリの量（メガバイト単位）。
[Number of Ignored DIMMs] フィールド	サーバーがアクセスできない DIMM の数。
[Number of Failed DIMMs] フィールド	障害が発生し、使用できない DIMM の数。
[使用可能なメモリ RAS（Memory RAS Possible）] フィールド	サーバーでサポートされている RAS メモリ構成の詳細。

名前	説明
[メモリの設定（Memory Configuration）] フィールド	現在のメモリ設定。次のいずれかになります。 • [最大パフォーマンス（Maximum Performance）]：システムは自動的にメモリのパフォーマンスを最適化します。 • [ミラーリング（Mirroring）]：サーバーはメモリ内のデータのコピーを 2 つ保持します。このオプションを使用すると、サーバー上の使用可能なメモリが等分され、その半分はミラー コピー用に自動的に予約されます。 • [ロックステップ（Lockstep）]：サーバー内の DIMM ペアが、同一のタイプ、サイズ、および構成を持ち、SMI チャネルにまたがって装着されている場合、ロックステップ モードを有効にして、メモリ アクセス遅延の最小化およびパフォーマンスの向上を実現できます。
[DIMM location diagram]	現在のサーバーの DIMM またはメモリのレイアウトを示します。

ステップ 5 [**DIMM Black Listing**] 領域で、DIMM の全体的なステータスを確認し、DIMM のブラックリスト化をイネーブルにします。

名前	説明
[DIMM 全体のステータス（Overall DIMM Status）] フィールド	DIMM の全体的なステータス。次のいずれかになります。 • [良好（Good）]：DIMM ステータスは使用可能です。 • [Severe Fault]：修正不可能な ECC エラーがある場合の DIMM ステータス。
[**Enable DIMM Black List**] チェックボックス	DIMM のブラックリスト化を有効にする場合はこのオプションをオンにします。

ステップ 6 [Memory Details] テーブルで、各 DIMM に関する次の詳細情報を確認します。

ヒント カラムの見出しをクリックすると、そのカラムのエントリに従って表の行がソートされます。

名前	説明
[Name] カラム	メモリ モジュールが装着されている DIMM スロットの名前
[Capacity] カラム	DIMM のサイズ。
[Channel Speed] カラム	メモリ チャネルのクロック速度（メガヘルツ単位）。
[Channel Type] カラム	メモリ チャネルのタイプ。

名前	説明
[Memory Type Detail] カラム	デバイスで使用されるメモリのタイプ。
[Bank Locator] カラム	メモリ バンク内の DIMM の場所。
[Manufacturer] カラム	製造業者のベンダー ID。次のいずれかになります。 • [0x2C00]：Micron Technology, Inc. • [0x5105]：Qimonda AG i. In. • [0x802C]：Micron Technology, Inc. • [0x80AD]：Hynix Semiconductor Inc. • [0x80CE]：Samsung Electronics, Inc. • [0x8551]：Qimonda AG i. In. • [0xAD00]：Hynix Semiconductor Inc. • [0xCE00]：Samsung Electronics, Inc.
[Serial Number] カラム	DIMM のシリアル番号。
[Asset Tag] カラム	DIMM に関連付けられた資産タグ（存在する場合）。
[Part Number] カラム	ベンダーによって割り当てられた DIMM の部品番号。
[Visibility] カラム	DIMM がサーバに対して使用可能であるかどうか。
[Operability] カラム	DIMM が現在正常に動作しているかどうか。
[Data Width] カラム	DIMM がサポートするデータの量（ビット単位）。

PCI アダプタのプロパティの表示

始める前に

サーバーの電源をオンにする必要があります。そうしないと、プロパティが表示されません。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。
ステップ 2 [シャーシ（Chassis）] メニューで [インベントリ（Inventory）] をクリックします。

ステップ 3 [Inventory] ペインの [PCI Adapters] タブをクリックします。

ステップ 4 [PCI Adapters] 領域で、装着されている PCI アダプタの次の情報を確認します。

名前	説明
[Slot ID] カラム	アダプタが存在するスロット。
[Product Name] カラム	アダプタの名前。
[オプション ROM のステータス（Option ROM Status）] カラム	オプションの ROM のステータスを示します。次のいずれかになります。 • [ロード済み（Loaded）]：データはカードで使用できます。 • [未ロード（Unloaded）]：データはカードで使用できません。 • [ロード エラー（Load Error）]：カードが存在し、オプションの ROM が有効になっています。しかし、カードのエラーにより、オプションの ROM がロードに失敗しました。
[**Firmware Version**] カラム	アダプタのファームウェア バージョン。 （注） 標準の UEFI インターフェイス経由でバージョンを提供するアダプタのファームウェア バージョンのみ表示されます。たとえば、Intel LOM や Emulex アダプタなどです。
[Vendor ID] カラム	ベンダーによって割り当てられたアダプタ ID。
[Sub Vendor ID] カラム	ベンダーによって割り当てられているセカンダリ アダプタ ID。
[Device ID] カラム	ベンダーによって割り当てられたデバイス ID。
[Sub Device ID] カラム	ベンダーによって割り当てられているセカンダリ デバイス ID。

ストレージのプロパティの表示

始める前に

サーバーの電源をオンにする必要があります。そうしないと、プロパティが表示されません。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[コンピューティング（Compute）]メニューをクリックします。

ステップ 2 **[コンピューティング（Compute）]**メニューでサーバを選択します。

ステップ 3 作業ウィンドウで **[インベントリ（Inventory）]**タブをクリックします。

ステップ 4 **[ストレージ (Storage)]** タブで、次の情報を確認します。

名前	説明
[コントローラ（Controller）] フィールド	コントローラ ドライブが存在する PCIe スロット。
[PCIスロット（PCI Slot）] フィールド	コントローラ ドライブが配置されている PCIe スロットの名前。
[製品名（Product Name）] フィールド	コントローラの名前。
[シリアル番号（Serial Number）] フィールド	ストレージ コントローラのシリアル番号。
[ファームウェアパッケージビルド（Firmware Package Build）] フィールド	アクティブなファームウェア パッケージのバージョン番号。
[製品ID（Product ID）] フィールド	コントローラの製品 ID。
[バッテリのステータス（Battery Status）] フィールド	バッテリのステータス。
[キャッシュメモリサイズ（Cache Memory Size）] フィールド	キャッシュ メモリのサイズ（MB 単位）。
[状況（Health）] フィールド	コントローラのヘルス状態。

TPM のプロパティの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [シャーシ（Chassis）] メニューで [インベントリ（Inventory）] をクリックします。

ステップ 3 [**Inventory**] ペインの [**TPM**] タブをクリックします。

ステップ 4 次の情報を確認します。

名前	説明
[Version] フィールド	TPM のバージョン。TPM のバージョン詳細情報が使用できない場合、このフィールドには **NA** と表示されます。
[Presence] フィールド	ホスト サーバーでの TPM モジュールの有無。 • [**Equipped**]：TPM はホスト サーバにあります。 • [空（Empty）]：TPM はホスト サーバーにありません。
[Model] フィールド	TPM のモデル番号。TPM がホスト サーバーにない場合、このフィールドには [適用しない（NA）] と表示されます。
[有効になっているステータス（Enabled Status）] フィールド	TPM がイネーブルかどうか。 • [有効（Enabled）]：TPM はイネーブルです。 • [無効（Disabled）]：TPM はディセーブルです。 • [不明（Unknown）]：TPM はホスト サーバーにありません。
[Vendor] フィールド	TPM ベンダーの名前。TPM がホスト サーバーにない場合、このフィールドには [適用しない（NA）] と表示されます。
[アクティブ ステータス（Active Status）] フィールド	TPM のアクティベーション ステータス。 • [**Activated**]：TPM はアクティブです。 • [**Deactivated**]：TPM は非アクティブです。 • [不明（Unknown）]：TPM はホスト サーバにありません。 （注） TPM バージョン 2.0 をインストールしている一部の C シリーズ サーバーでは、[アクティブ ステータス（Active Status）] は [適用しない（NA）] として表示されます。

名前	説明
[Serial] フィールド	TPM のシリアル番号。TPM がホスト サーバーにない場合、このフィールドには [適用しない（NA）] と表示されます。
[所有権（Ownership）] フィールド	TPM の所有ステータス。 • [**Owned**]：TPM は所有されています。 • [**Unowned**]：TPM は所有されていません。 • [不明（Unknown）]：TPM はホスト サーバにありません。 （注） TPM バージョン 2.0 をインストールしている一部の C シリーズ サーバーでは、[所有（Ownership）] ステータスは [適用しない（NA）] として表示されます。
[Revision] フィールド	TPM の改訂番号。TPM がホスト サーバーにない場合、このフィールドには [適用しない（NA）] と表示されます。
[Firmware Version] フィールド	ファームウェア バージョンの詳細。

PID カタログの表示

手順

ステップ 1 [Navigation] ペインの [Compute] タブをクリックします。

ステップ 2 [Compute] 作業領域で、[PID Catalog] タブをクリックします。

ステップ 3 PID カタログについて次の概要情報を確認します。

- **アクティベーション ステータス**：PID カタログのアクティベーション ステータス。
- **現在アクティブなバージョン**：アクティブな PID カタログのバージョン。

ステップ 4 **[CPU]** の表で、CPU に関する次の情報を確認します。

名前	説明
[ソケット名 (Socket Name)] カラム	CPU が装着されているソケット
[Product ID] カラム	CPU の製品 ID。
[Model] カラム	CPU のモデル番号。

ステップ 5 [Memory] テーブルで、メモリに関する次の情報を確認します。

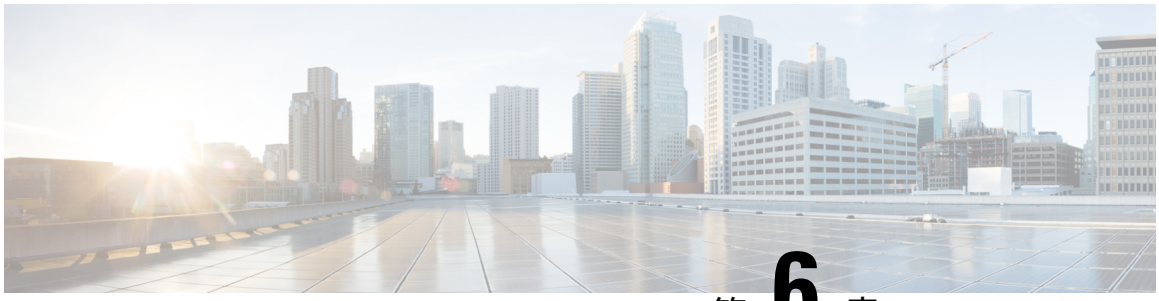
名前	説明
[名前 (Name)] カラム	メモリ スロットの名前。
[Product ID] カラム	ベンダーによって割り当てられたメモリ スロットの製品 ID。
[Vendor ID] カラム	ベンダーによって割り当てられた ID。
[Capacity] カラム	メモリのサイズ。
[速度 (MHz) (Speed (MHz))]カラム	メモリ速度（メガヘルツ単位）。

ステップ 6 [PCI アダプタ（PCI Adapters）] テーブルで、PCI アダプタに関する次の情報を確認します。

名前	説明
[Slot] カラム	アダプタが存在するスロット。
[Product ID] カラム	アダプタの製品 ID。
[Vendor ID] カラム	ベンダーによって割り当てられたアダプタ ID。
[Sub Vendor ID] カラム	ベンダーによって割り当てられているセカンダリ アダプタ ID。
[Device ID] カラム	ベンダーによって割り当てられたデバイス ID。
[Sub Device ID] カラム	ベンダーによって割り当てられているセカンダリ デバイス ID。

ステップ 7 [HDD] テーブルで、HDD に関する次の情報を確認します。

名前	説明
[ディスク (Disks)] カラム	ハード ドライブのディスク。
[Product ID] カラム	ハード ドライブの製品 ID。
[コントローラ (Controller)] カラム	選択した Cisco Flexible Flash コントローラのシステム定義の名前。この名前は変更できません。
[Vendor] カラム	ハード ドライブのベンダー。
[Model] カラム	ハード ドライブのモデル。



第 6 章

センサーの表示

この章は、次の内容で構成されています。

シャーシ センサーの表示

電源センサーの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [シャーシ（Chassis）] メニューで [センサー（Sensors）] をクリックします。

ステップ 3 [Sensors] 作業領域で、[Power Supply] タブをクリックします。

ステップ 4 電源装置の次のセンサー プロパティを確認します。

[プロパティ（Properties）] 領域

名前	説明
[Redundancy Status] フィールド	電源装置の冗長性のステータス。

[Threshold Sensors] 領域

名前	説明
[Sensor Name] カラム	サーバの名前。

名前	説明
[センサー ステータス（Sensor Status）] 列	センサーのステータス。次のいずれかになります。 • 不明 • **[Informational]** • 標準 • 警告 • **[Critical]** • **Non-Recoverable**
[Reading] カラム	現在の電力使用量（ワット単位）。
[Warning Threshold Min] カラム	Warning の最小しきい値。
[Warning Threshold Max] カラム	Warning の最大しきい値。
[Critical Threshold Min] カラム	Critical の最小しきい値。
[Critical最大しきい値（Critical Threshold Max）] カラム	Critical の最大しきい値。

[Discrete Sensors] 領域

名前	説明
[Sensor Name] カラム	センサーの名前。
[センサー ステータス（Sensor Status）] 列	センサーのステータス。次のいずれかになります。 • 不明 • **[Informational]** • 標準 • 警告 • **[Critical]** • **Non-Recoverable**
[Reading] カラム	センサーの基本的な状態。

ファン センサーの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [シャーシ（Chassis）] メニューで [センサー（Sensors）] をクリックします。

ステップ 3 [Sensors] 作業領域で、[Fan] タブをクリックします。

ステップ 4 次のファン センサー プロパティを確認します。

名前	説明
[Sensor Name] カラム	サーバの名前。
[センサー ステータス（Sensor Status）] 列	センサーのステータス。次のいずれかになります。 • **不明** • **[Informational]** • **標準** • **警告** • **[Critical]** • **Non-Recoverable**
[速度（RPM）（Speed (RPMS)）] 列	ファンの速度（RPM 単位）。
[Warning Threshold Min] カラム	Warning の最小しきい値。
[Warning Threshold Max] カラム	Warning の最大しきい値。
[Critical Threshold Min] カラム	Critical の最小しきい値。
[Critical最大しきい値（Critical Threshold Max）] カラム	Critical の最大しきい値。
[回復不可能な最小しきい値（Non-Recoverable Threshold Min）] カラム	回復不可能な最小しきい値。
[回復不可能な最大しきい値（Non-Recoverable Threshold Max）] カラム	回復不可能な最大しきい値。

温度センサーの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [シャーシ（Chassis）] メニューで [センサー（Sensors）] をクリックします。

ステップ 3 [Sensors] 作業領域で、[Temperature] タブをクリックします。

ステップ 4 次の温度センサーのプロパティを確認します。

名前	説明
[Sensor Name] カラム	サーバの名前。
[センサー ステータス（Sensor Status）] 列	センサーのステータス。次のいずれかになります。 • **不明** • **[Informational]** • **標準** • **警告** • **[Critical]** • **Non-Recoverable**
[Temperature] カラム	現在の温度（摂氏単位）。
[Warning Threshold Min] カラム	Warning の最小しきい値。
[Warning Threshold Max] カラム	Warning の最大しきい値。
[Critical Threshold Min] カラム	Critical の最小しきい値。
[Critical最大しきい値（Critical Threshold Max）] カラム	Critical の最大しきい値。
[回復不可能な最小しきい値（Non-Recoverable Threshold Min）] カラム	回復不可能な最小しきい値。
[回復不可能な最大しきい値（Non-Recoverable Threshold Max）] カラム	回復不可能な最大しきい値。

電圧センサーの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [シャーシ（Chassis）] メニューで [センサー（Sensors）] をクリックします。

ステップ 3 [Sensors] 作業領域で、[Voltage] タブをクリックします。

ステップ 4 次の電圧センサーのプロパティを確認します。

名前	説明
[Sensor Name] カラム	サーバの名前。
[センサー ステータス（Sensor Status）] 列	センサーのステータス。次のいずれかになります。 • **不明** • **[Informational]** • **標準** • **警告** • **[Critical]** • **Non-Recoverable**
[電圧（V）（Voltage (V)）] 列	現在の電圧（ボルト単位）。
[Warning Threshold Min] カラム	Warning の最小しきい値。
[Warning Threshold Max] カラム	Warning の最大しきい値。
[Critical Threshold Min] カラム	Critical の最小しきい値。
[Critical最大しきい値（Critical Threshold Max）] カラム	Critical の最大しきい値。
[回復不可能な最小しきい値（Non-Recoverable Threshold Min）] カラム	回復不可能な最小しきい値。
[回復不可能な最大しきい値（Non-Recoverable Threshold Max）] カラム	回復不可能な最大しきい値。

電流センサーの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [シャーシ（Chassis）] メニューで [センサー（Sensors）] をクリックします。

ステップ 3 [Sensors] 作業領域で、[Current] タブをクリックします。

ステップ 4 次の電流センサー プロパティを確認します。

名前	説明
[Sensor Name] カラム	サーバの名前。
[センサー ステータス（Sensor Status）] 列	センサーのステータス。次のいずれかになります。 • **不明** • **[Informational]** • **標準** • **警告** • **[Critical]** • **Non-Recoverable**
[Current (A) (電流 (A))] カラム	アンペア (A) の現在の値。
[Warning Threshold Min] カラム	Warning の最小しきい値。
[Warning Threshold Max] カラム	Warning の最大しきい値。
[Critical Threshold Min] カラム	Critical の最小しきい値。
[Critical最大しきい値（Critical Threshold Max）] カラム	Critical の最大しきい値。
[回復不可能な最小しきい値（Non-Recoverable Threshold Min）] カラム	回復不可能な最小しきい値。
[回復不可能な最大しきい値（Non-Recoverable Threshold Max）] カラム	回復不可能な最大しきい値。

LED センサーの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [シャーシ（Chassis）] メニューで [センサー（Sensors）] をクリックします。

ステップ 3 [Sensors] 作業領域で、[LEDs] タブをクリックします。

ステップ 4 次の LED センサー プロパティを確認します。

名前	説明
[Sensor Name] カラム	サーバの名前。
[LED ステータス（LED Status）] 列	LED が点灯、点滅、または消灯しているかどうか。
[LED Color] カラム	LED の現在のステータス。 色の意味の詳細については、使用しているサーバ タイプに対応するハードウェア インストレーション ガイドを参照してください。

ストレージ センサーの表示

手順

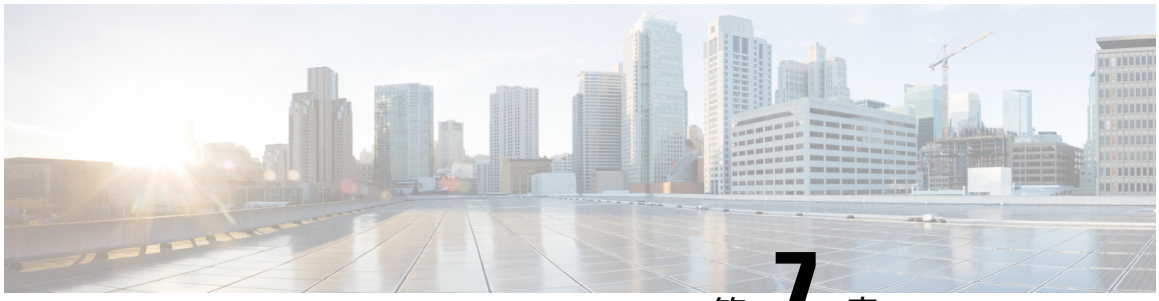
ステップ 1 [ナビゲーション（Navigation）] ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 [Compute] メニューでサーバを選択します。

ステップ 3 作業ペインの **[センサー (Sensors)]** タブをクリックします。

ステップ 4 **[ストレージ (Storage)]** タブの **[ストレージ センサー (Storage Sensors)]** 領域で、サーバの次のストレージに関する統計情報を表示します。

名前	説明
[Name] カラム	ストレージ デバイスの名前。
[Status]カラム	ストレージ デバイスのステータスに関する簡単な説明。



第 7 章

リモート プレゼンスの管理

この章は、次の内容で構成されています。

Serial over LAN の設定

Serial over LAN を使用すると、管理対象システムのシリアル ポートの入出力を IP 経由でリダイレクトできます。ホスト コンソールへ Cisco IMC を使用して到達する場合は、サーバーで Serial over LAN を設定して使用します。

重要　ネイティブ シリアル リダイレクトと serial over LAN 同時に使用することはできません。

始める前に

Serial over LAN を設定するには、管理者権限のあるユーザでログインする必要があります。

手順

ステップ 1　[ナビゲーション（Navigation）]ペインの[コンピューティング（Compute）]メニューをクリックします。

ステップ 2　**[コンピューティング（Compute）]**メニューでサーバを選択します。

ステップ 3　作業ウィンドウで **[リモート管理（Remote Management）]**タブをクリックします。

ステップ 4　[Remote Presence] ペインの [Serial over LAN] タブをクリックします。

ステップ 5　[Serial over LAN Properties] 領域で、次のプロパティを更新します。

名前	説明
[有効（Enabled）] チェックボックス	オンにすると、このサーバで Serial over LAN が有効になります。
[Baud Rate] ドロップダウン リスト	システムが SoL 通信に使用するボー レート。次のいずれかになります。 • **[9600 bps]** • **[19.2 kbps]** • **[38.4 kbps]** • **[57.6 kbps]** • **[115.2 kbps]**
[COM ポート（Com Port）] ドロップダウン リスト	システムが SoL 通信をルーティングするシリアル ポート。 次のいずれかを選択できます。 • **[com0]**：SoL 通信は、外部デバイスへの物理 RJ45 接続またはネットワーク デバイスへの仮想 SoL 接続をサポートする、外部からアクセス可能なシリアル ポートである COM ポート 0 を介してルーティングされます。 このオプションを選択すると、システムは、SoL を有効にして、RJ45 接続を無効にします。これは、サーバが外部シリアル デバイスをサポートできなくなることを意味します。 • **[com1]**：SoL 通信は COM ポート 1 経由でルーティングされます。このポートは、SoL のみを介してアクセスできる内部ポートです。 このオプションを選択した場合、COM ポート 1 上の SoL および COM ポート 0 上の物理 RJ45 接続を使用できます。 （注） COM ポートの設定を変更すると、既存のすべての SoL セッションが切断されます。
[SSH ポート（SSH Port）] フィールド	Serial over LAN に直接アクセスするときに経由するポート。このポートを使用すると、Cisco IMC シェルをバイパスして、SoL への直接アクセスを提供できます。 有効な範囲は 1024 ～ 65535 です。デフォルト値は 2400 です。 （注） SSH ポートの設定を変更すると、既存のすべての SSH セッションが切断されます。

ステップ 6 [Save Changes] をクリックします。

仮想メディアの設定

始める前に

仮想メディアを設定するには、admin権限を持つユーザーとしてログインする必要があります。

手順

ステップ 1 **[ナビゲーション (Navigation)]** ペインの **[コンピューティング (Compute)]** タブをクリックします。

ステップ 2 [Compute] メニューでサーバを選択します。

ステップ 3 **[リモート管理 (Remote Management)]** タブをクリックします。

ステップ 4 [リモート管理（Remote Management）] タブで、[仮想メディア（Virtual Media）] タブをクリックします。

ステップ 5 **[vKVM コンソール ベース vMedia プロパティ領域 (vKVM Console Based vMedia Properties Area)]** で、次のプロパティを更新します。

名前	説明
[有効（Enabled）] チェックボックス	オンにすると、仮想メディアがイネーブルになります。 （注） このチェックボックスをオフにすると、すべての仮想メディアデバイスはホストから自動的に切断されます。
[Active Sessions] フィールド	現在実行されている仮想メディア セッションの数。
[低電力 USB を有効化 (Low Power USB enabled)] チェックボックス	これを選択すると、低電力 USB が有効になります。 低電力 USB が有効化された場合、ISO をマッピングしてホストを再起動した後、ブート選択メニューに仮想ドライブが表示されます。 ただし、UCS VIC P81E カードのあるサーバに ISO をマッピングするとき、NIC が Cisco カード モードである場合には、仮想ドライブがブート選択メニューに表示されるようにするために、このオプションを無効にする必要があります。

ステップ 6 [Save Changes] をクリックします。

Cisco IMC マップされた vMedia ボリュームの作成

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 **[コンピューティング（Compute）]**メニューでサーバを選択します。

ステップ 3 **作業ウィンドウで [リモート管理（Remote Management）]**タブをクリックします。

ステップ 4 [Remote Management] タブで、[Virtual Media] タブをクリックします。

ステップ 5 **[現在マッピング (Current Mappings)]** 領域で、**[新しいマッピングの追加 (Add New Mapping)]** をクリックします。

ステップ 6 [Add New Mapping] ダイアログボックスで、次のフィールドを更新します。

名前	説明
[ボリューム（Volume）] フィールド	マッピング用にマウントしたイメージの ID。
[Mount Type] ドロップダウン リスト	マッピングのタイプです。次のいずれかになります。 （注） 選択するマウントタイプの通信ポートがスイッチ上で有効になっていることを確認してください。たとえば、マウント タイプとして CIFS を使用する場合、ポート 445（CIFS の通信ポート）がスイッチ上で有効になっていることを確認します。同様に、HTTP、HTTPS、または NFS を選択する場合は、ポート 80（HTTP の場合）、ポート 443（HTTPS の場合）、またはポート 2049（NFS の場合）を有効にします。 • [NFS]：ネットワーク ファイル システム。 • [CIFS]：共通インターネット ファイル システム。 • [WWW(HTTP/HTTPS)]：HTTP ベースまたは HTTPS ベースのシステム。 （注） 仮想メディアをマウントする前に、Cisco IMC はサーバーに ping を実行することによって、エンドサーバーへの到達可能性の確認を試みます。

名前	説明
[リモート共有（Remote Share）] フィールド	マップするイメージの URL。形式は選択した [マウント タイプ（Mount Type）] に応じて異なります。 • [NFS]：**serverip:/share** を使用します。 • [CIFS]：**//serverip/share** を使用します。 • [WWW(HTTP/HTTPS)]：**http[s]://serverip/share** を使用します。
[Remote File] フィールド	リモート共有に含まれる .iso または .img ファイルの名前と場所。

名前	説明
[マウント オプション（Mount Options）] フィールド	

名前	説明
	カンマ区切りリストで入力される業界標準のマウント オプション。オプションは選択した [マウント タイプ（Mount Type）] に応じて異なります。 [NFS] を使用している場合、フィールドを空白にしておくか、次のうちの 1 つ以上を入力します。 • **ro** • **rw** （注） 共有されているフォルダは、読み取り/書き込みオプションを使用するための書き込み権限を持っている必要があります。読み取り/書き込みオプションは、.img ファイルに対してのみ使用できます。 • **nolock** • **noexec** • **soft** • **port=VALUE** • **timeo=VALUE** • **retry=VALUE** • **rsize=VALUE** • **wsize=VALUE** • **vers=VALUE** [CIFS] を使用している場合は、このフィールドを空白のままにするか、次の中から 1 つ以上を入力します。 • **ro** • **rw** （注） 共有されているフォルダは、読み取り/書き込みオプションを使用するための書き込み権限を持っている必要があります。読み取り/書き込みオプションは、.img ファイルに対してのみ使用できます。 • **soft** • **nounix** • **noserverino**

名前	説明
	• **guest** • [username=VALUE]：**guest** が入力された場合は無視されます。 • [password=VALUE]：**guest** が入力された場合は無視されます。 • **sec=VALUE** リモート サーバと通信する際の認証に使用するプロトコル。CIFS 共有の設定に応じて、**VALUE** は次のいずれかになります。 • [なし（None）]：認証は使用されません。 • [Ntlm]：NT LAN Manager（NTLM）セキュリティ プロトコル。このオプションは、Windows 2008 R2 および Windows 2012 R2 でのみ使用します。 • [Ntlmi]：NTLMi セキュリティ プロトコル。このオプションは、CIFS Windows サーバで [デジタル署名（Digital Signing）] を有効にした場合にのみ使用します。 • [Ntlmssp]：NT LAN Manager Security Support Provider（NTLMSSP）プロトコル。このオプションは、Windows 2008 R2 および Windows 2012 R2 でのみ使用します。 • [Ntlmsspi]：NTLMSSPi プロトコル。このオプションは、CIFS Windows サーバで [デジタル署名（Digital Signing）] を有効にした場合にのみ使用します。 • [Ntlmv2]：NTLMv2 セキュリティ プロトコル。このオプションは、Samba Linux でのみ使用します。 • [Ntlmv2i]：NTLMv2i セキュリティ プロトコル。このオプションは、Samba Linux でのみ使用します。 • **vers=VALUE** （注） 値の形式は *x.x* である必要があります [WWW(HTTP/HTTPS)] を使用している場合は、このフィールドを空白のままにするか、次のように入力します。

名前	説明
	• **noauto** （注） 仮想メディアをマウントする前に、Cisco IMC はサーバーに ping を実行することによって、エンドサーバーへの到達可能性の確認を試みます。 • **username=VALUE** • **password=VALUE**
[ユーザ名（User Name）] フィールド	指定した [マウント タイプ（Mount Type）] のユーザ名（必要な場合）。
[パスワード（Password）] フィールド	選択されたユーザー名のパスワード（必要な場合）。

ステップ 7 [保存（Save）] をクリックします。

Cisco IMC によりマップされた vMedia ボリュームのプロパティの表示

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 **[コンピューティング（Compute）]**メニューでサーバを選択します。

ステップ 3 **作業ウィンドウで [リモート管理（Remote Management）]**タブをクリックします。

ステップ 4 [Remote Management] タブで、[Virtual Media] タブをクリックします。

ステップ 5 [Current Mappings] テーブルから行を選択します。

ステップ 6 [Properties] をクリックし、次の情報を確認します。

名前	説明
[Add New Mapping] ボタン	新しいイメージを追加できるダイアログボックスが開きます。
[Properties] ボタン	選択したイメージのプロパティを表示または変更できるダイアログボックスが開きます。
[Unmap] ボタン	マウントされた vMedia のマップを解除します。

名前	説明
Last Mapping Status	最後に試行されたマッピングのステータス。
[Volume] 列	イメージの ID。
[Mount Type] ドロップダウンリスト	マッピングのタイプです。
[Remote Share] フィールド	イメージの URL。
[Remote File] フィールド	イメージの厳密なファイル位置。
[Status] フィールド	マップの現在のステータス。次のいずれかになります。 • [OK]：マッピングは正常です。 • [In Progress]：マッピングが進行中です。 • [Stale]：Cisco IMC にマッピングが古いという理由を示すテキスト文字列が表示されます。 • [**Error**]：Cisco IMC にエラーの理由を示すテキスト文字列が表示されます。

Cisco IMC によりマップされた vMedia ボリュームの削除

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 **[コンピューティング（Compute）]**メニューでサーバを選択します。

ステップ 3 **作業ウィンドウで [リモート管理（Remote Management）]**タブをクリックします。

ステップ 4 [Remote Management] タブで、[Virtual Media] タブをクリックします。

ステップ 5 **[現在のマッピング（Current Mappings）]**テーブルから行を選択します。

ステップ 6 **[マップ解除（Unmap）]**をクリックします。

既存の Cisco IMC vMedia イメージの再マッピング

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 **[コンピューティング（Compute）]** メニューでサーバを選択します。

ステップ 3 **作業ウィンドウで [リモート管理（Remote Management）]** タブをクリックします。

ステップ 4 [Remote Management] タブで、[Virtual Media] タブをクリックします。

ステップ 5 **[現在のマッピング（Current Mappings）]** テーブルから行を選択します。

ステップ 6 **[再マッピング（Remap）]** をクリックします。

Cisco IMC vMedia イメージの削除

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 **[コンピューティング（Compute）]** メニューでサーバを選択します。

ステップ 3 **作業ウィンドウで [リモート管理（Remote Management）]** タブをクリックします。

ステップ 4 [Remote Management] タブで、[Virtual Media] タブをクリックします。

ステップ 5 **[現在のマッピング（Current Mappings）]** テーブルから行を選択します。

ステップ 6 [削除（Delete）] をクリックします。

仮想 KVM コンソール

vKVM コンソールは Cisco IMC からアクセス可能なインターフェイスであり、サーバへのキーボード、ビデオ、マウス（vKVM）の直接接続をエミュレートします。vKVM コンソールを使用すると、リモートの場所からサーバに接続できます。

Cisco KVM コンソールを使用する主な利点は次のとおりです。

- Cisco KVM コンソールは KVM、SOL、および vMedia への接続を提供しますが、Avocent KVM は KVM および vMedia への接続のみを提供します。
- KVM コンソールでは、vMedia 接続が KVM 起動マネージャで確立され、すべてのユーザーが使用できます。
- KVM コンソールには、ゲストからホストにテキストを貼り付ける際に、サポートされていない文字の高度な文字置換オプションが用意されています。
- KVM コンソールには、CIMC に vMedia マッピングを保存する機能があります。

サーバに物理的に接続された CD/DVD ドライブまたはフロッピー ドライブを使用する代わりに、vKVM コンソールは仮想メディアを使用します。これは、仮想 CD/DVD ドライブまたはフロッピー ドライブにマップされる実際のディスク ドライブまたはディスク イメージ ファイルです。次のいずれでも仮想ドライブにマップできます。

- コンピュータ上の CD/DVD またはフロッピー ドライブ
- コンピュータ上のディスク イメージ ファイル（ISO または IMG ファイル）
- コンピュータ上の USB フラッシュ ドライブ
- ネットワーク上の CD/DVD またはフロッピー ドライブ
- ネットワーク上のディスク イメージ ファイル（ISO または IMG ファイル）
- ネットワーク上の USB フラッシュ ドライブ

vKVM コンソールを使用してサーバに OS をインストールできます。

KVM コンソールの起動

KVM コンソールは、ホームページまたは [リモート管理（Remote Management）] 領域から起動できます。

手順

ステップ 1 ホームページからコンソールを起動するには、[Navigation] ペインで、[Chassis] メニューをクリックします。

ステップ 2 [シャーシ（Chassis）] メニューで [サマリー（Summary）] をクリックします。

ステップ 3 ツール バーから、**[vKVM の起動 (Launch vKVM)]** をクリックし、 を選択します。

ステップ 4 または、[Navigation] ペインの [Compute] メニューをクリックします。

ステップ 5 **[コンピューティング（Compute）]**メニューでサーバを選択します。

ステップ 6 **作業ウィンドウで [リモート管理（Remote Management）]**タブをクリックします。

ステップ 7 [Remote Management] ペインで、[Virtual KVM] タブをクリックします。

ステップ 8 **[仮想 vKVM (Virtual vKVM)]**タブで、**[vKVM コンソールの起動 (Launch vKVM console)]** をクリックします。

ステップ 9 必須: ポップアップ ウィンドウに表示されている URL リンクをクリックして、クライアントアプリケーションをロードします。vKVM コンソールを起動するたびにリンクをクリックする必要があります。

仮想 KVM コンソール - Cisco UCS C-Series M6 以降のサーバー

vKVM コンソールは Cisco IMC からアクセス可能なインターフェイスであり、サーバへのキーボード、ビデオ、マウス（vKVM）の直接接続をエミュレートします。遠隔地のサーバから接続して制御し、この vKVM セッション中にアクセスできる仮想ドライブに物理ロケーションをマッピングすることができます。

リリース4.2（1a）以降、Cisco IMC は、次のオプションを備えた C シリーズ M6 サーバー用の Cisco ベースの vKVM コンソールを提供します。

コンソール メニュー

メニュー項目	説明
KVM	現用系なコンソールとして KVM（Keyboard Video and Mouse）を選択します。
SOL	現用系なコンソールとして SOL（Serial Over LAN）を選択します。 （注） SOL が非アクティブな場合、SOL は表示されません。代わりに、Activate SOL が表示されます。
SOLを有効化	ユーザー名とパスワードを使用して SOL セッションにログインできます。 （注） SOL をアクティブにするオプションは、何らかの理由で SOL セッションがアクティブでない場合にのみ表示されます。

[File] メニュー

メニュー項目	説明
クリップボードのテキストを貼り付ける	クリップボードテキストの貼り付け（**Paste Clipboard Text**）ダイアログボックスを開いて、コンテンツの貼り付けを許可します。

メニュー項目	説明
クリップボードテキストの貼り付け（**Paste Clipboard Text**）	

メニュー項目	説明
	（注） このオプションは、KVM コンソールでのみサポートされています。サポートされていない文字の処理は、英語の文字のみをサポートするため、KVM コンソールでのみ見つかります。SOL コンソールは、すべての Unicode 文字をサポートします。 [クリップボード テキストの貼り付け] ダイアログ ボックスには、次のオプションがあります。 • **貼り付けたテキストにサポートされていない文字があります** ドロップダウンリスト： • サポートされていないすべての文字を無視する - テキスト内のサポートされていない文字をすべて無視します。 • 貼り付け操作をキャンセル - 送信操作をキャンセルします。 • 文字をマップされた値で置き換える - 文字がマップされていない場合、[サポートされていない文字] ダイアログ ボックスが開きます。詳細については、「表 6 : [サポートされていない文字（Unsupported Character）] ダイアログボックス （127 ページ）」を参照してください。 • 文字の処理方法を尋ねる—サポートされていない文字ダイアログ ボックスを開きます。詳細については、「表 6 : [サポートされていない文字（Unsupported Character）] ダイアログボックス （127 ページ）」を参照してください。 • 文字マッピング ボタン—文字マッピングを編集/削除するためのサブメニューを開きます。文字マッピングは、サポートされていない文字をユーザー定義の文字列

メニュー項目	説明
	(文字長なし) に置き換えます。 • [保存] ボタン - [貼り付けたテキストにサポートされていない文字が見つかった場合:] ドロップダウン リストで選択したオプションを保存します。 （注） このオプションは、設定が更新された場合にのみ表示されます。 • 貼り付けるテキスト（**Text to Paste**）フィールドに入力します。 • 送信ボタン—テキストを送信します。
ファイルにキャプチャ	保存（**Save**） ダイアログボックスを開くと、PNG イメージとして現在の画面を保存できます。

表 *6 : [*サポートされていない文字（***Unsupported Character***）*]* ダイアログボックス

オプション	説明
文字コンテキスト	サポートされていない文字が見つかった 11 文字のグループ。サポートされていない文字の前後 5 文字。ただし、11 文字を作成するのに十分な数の前後の文字が利用できない場合、サポートされていない文字の前後の文字がプルされます。
希望の操作をサポートされていない文字ドロップダウン リストから選択してください。	次の操作の 1 つを選択できます。 • 文字を無視する - サポートされていない文字を無視するかどうかを決定するための追加オプションを提供します。 • 貼り付け操作をキャンセル—操作をキャンセルします。 文字を置き換える - サポートされていない文字を何に置き換えるかを決定するための追加オプションを提供します。

オプション	説明
置換フィールド	（注） このオプションは、[文字を置換] オプションでのみ表示されます。 置換文字を入力します。
この置換のマッピングをサポートされていない文字チェック ボックスに保存します	（注） このオプションは、[文字を置換] オプションでのみ表示されます。 キャラクター マッピングを保存できます。
すべてのサポートされていな文字チェックボックスに対してこのアクションを繰り返します	評価されているサポートされていない文字のすべてのインスタンスに対して、選択したアクションを繰り返します。
すべてのサポートされていない文字チェックボックスに対してこのアクションを繰り返します。	（注） このオプションは、[貼り付け操作をキャンセル] オプションの場合にのみ表示されません。 サポートされていない同じキャラクターに対して同じアクションを保存できます。

[表示（View）] メニュー

メニュー項目	説明
[更新（Refresh）]	コンソールの表示をサーバーの現在のビデオ出力で更新します。 （注） このオプションは、KVM コンソールでのみサポートされています。
ビデオ品質	サブメニューから次のものの 1 つを選択できます。 • 高 • 中 • 低 • 超低 （注） このオプションは、KVM コンソールでのみサポートされています。

メニュー項目	説明
SOLコンソールをクリア	Cisco SOL 端末をクリアします。 （注） このオプションは、SOL コンソールでのみサポートされています。
Full Screen	画面全体になるように vKVM コンソールを拡大します。

全画面

（注） マクロ メニューは KVM コンソールでのみサポートされます。

メニュー項目	説明
静的マクロ	マクロ サブメニューの事前定義されたセットを表示します。
[ユーザ定義マクロ（User Defined Macros）]	マクロ サブメニューのユーザー定義されたセットを表示します。

メニュー項目	説明
管理	[マクロの管理] ダイアログ ボックスを開きます。このダイアログ ボックスでは、マクロを追加、削除、編集できます。定義済みのマクロ セットを復元します。マクロにホットキーを割り当てます。
	新しいマクロを作成するには、[マクロ マネージャ マクロ][新しいマクロの作成]をクリックします。 > > [新しいマクロの作成] ダイアログ ボックスを開きます。 • **新しいユーザー定義マクロのキーストロークを入力します**—希望のキーを入力します。 • [特殊文字] ドロップダウン リスト—目的の特殊文字を選択し、[追加] をクリックします。 • [作成] ボタン—新しいマクロを保存します。
	定義済みのマクロ セットを復元するには、[マクロ マネージャー マクロ][静的マクロの復元]をクリックします。 > >

[Tools] メニュー

メニュー項目	説明
統計（Stats）	

メニュー項目	説明
	[統計] ダイアログ ボックスを開きます。 KVM 統計： • **Total Bytes Rec**—受信した合計バイト数。 • Total Bytes Sent — 送信された合計バイト数。 • **Rx Bandwidth—**秒あたりの KB 数で測定された受信帯域幅。 • **Tx Bandwidth—** 秒あたりの KB 数で測定された送信帯域幅。 • **Frame Rate—** 秒あたりのフレーム数で測定されたフレーム速度。 • **ビデオタイルレート**—秒あたりにレンダリングされるビデオタイル。 vMedia がアクティブ化されると、**vKVM-Mapped vMedia Stats** エリアが次のとおり表示します。 • **Total Bytes Rec**—受信した合計バイト数。 • Total Bytes Sent — 送信された合計バイト数。 • **Device**—ローカルデバイスのタイプ。 • **Mapped File**—ホストサーバーデバイスがマップされるローカルデバイスまたはイメージファイルのタイプ。 • **Duration**—マップするデバイスの経過時間。 • **読み取りバイト数** — vKVMメディアから読み取られたバイト数。 • 書き込みバイト数—vKVM メディアに書き込まれたバイト数。 • 所有者 — メディアをブラウザにマップしたユーザー。 CIMC マップされた vMedia Stats 領域には、次の情報が表示されます。

メニュー項目	説明
	• **Device**—ローカルデバイスのタイプ。 • **Mapped File**—ホストサーバーデバイスがマップされるローカルデバイスまたはイメージファイルのタイプ。

メニュー項目	説明
	• デバイス ステータス - 可能なデバイス ステータス: • デバイスのマウントが進行中です • マウントされたデバイス • デバイスの取り出しが進行中です • ホストからイジェクトされました 以下はエラーステータス • マウントが失敗しました • アンマウントに失敗しました • 接続がタイムアウトしました • ファイルサーバーが接続を拒否しました • ファイルサーバーがクレデンシャルを拒否しました • ファイルサーバーパスが見つかりません • ファイルが見つかりません • ファイルはまだ使用中です • 読み取り専用としてファイルを開くことができませんでした • 読み取り/書き込みに失敗したためファイルを開く • ファイルの入出力に失敗しました • HTTPサーバーがコンテンツ長を返しませんでした • HTTPサーバーは範囲要求をサポートしていません • 無効なパラメータ • 無効なデバイス使用 • 無効なデバイスタイプ

メニュー項目	説明
[セッション ユーザ リスト（Session User List）]	アクティブな vKVM セッションを持つすべてのユーザ ID を表示する **[セッション ユーザ リスト（Session User List）]** ダイアログ ボックスを開きます。 上部の [Session User List] アイコンからも同じようにアクセスできます。
Keyboard	ユーザがデータの入力に使用できる vKVM コンソールの仮想キーボードを表示します。 （注） このオプションは、SOL コンソールでのみサポートされています。
USBのリセット	キーボード、マウス、および仮想メディアをリセットするオプションを提供します。 （注） USB 接続をリセットすると、仮想メディア、キーボード、マウスを含むサーバーへのすべての入力に影響します。

[Power] メニュー

メニュー項目	説明
システムの電源オン	システムの電源を入れます。 このオプションは、システムの電源がオンになっている場合は無効で、システムの電源がオフになっている場合に有効です。
システムの電源オフ	仮想コンソール セッションからシステムの電源をオフにします。 このオプションは、システムの電源がオンの場合に有効で、システムの電源がオフの場合は無効です。
[システムのリセット（Reset System）]	電源をオフにすることなくシステムを再起動します。 このオプションは、システムの電源がオンの場合に有効で、システムの電源がオフの場合は無効です。

メニュー項目	説明
システムの電源再投入	システムの電源をオフにしてから、再度オンにします。 このオプションは、システムの電源がオンの場合に有効で、システムの電源がオフの場合は無効です。

[ブートデバイス（Boot Device）] メニュー

名前	説明
[No Override]	ホストが構成された最初のデバイスから起動できるようにします。
[Boot Device] リスト	現在設定されているブート順序を変更せず、次回のサーバ 再起動時のみサーバがブートに使用するブートデバイスのリスト。ワンタイム ブート デバイスからサーバーを起動すると、事前に設定されているブート順で以降のすべてのリブートが行われます。最大 15 のデバイスが vKVM コンソールに表示されます。

[仮想メディア（Virtual Media）] メニュー

名前	説明
Create Image	ISO イメージを作成できます。[Create Image] ダイアログボックスでファイルまたはフォルダをドラッグアンドドロップします。これらのファイルまたはフォルダは ISO イメージに変換されます。ローカル マシンに ISO イメージを保存するには、**[ISO イメージのダウンロード（Download ISO Image）]** ボタンを使用できます。 （注） **イメージの作成（Create Image）** オプションは Safari ブラウザでは使用できません。

名前	説明
vMedia をアクティブにする	ユーザー名とパスワードを使用して vMedia セッションにログインできます。 （注） [Activate vMedia] オプションは、何らかの理由で vMedia セッションがアクティブでない場合にのみ表示されます。 [vMedia のアクティブ化] オプションが表示されている場合、他の vMedia オプションは表示されません。
vKVM-Mapped vDVD	**[仮想メディアのマップ - CD/DVD]** ダイアログ ボックスを開きます。このダイアログ ボックスでは、ローカル コンピューターから ISO イメージを選択し、ドライブをマップできます。 （注） 読み取り専用ユーザーは仮想メディアを使用できません。
vKVM マッピングされた vHDD	**[仮想メディアのマップ - リムーバブル ディスク]** ダイアログ ボックスを開きます。ローカル コンピューターから ISO イメージを選択して、ドライブをマップできます。 （注） 読み取り専用ユーザーは仮想メディアを使用できません。
vKVM-Mapped vFDD	**[仮想メディアのマップ - フロッピー ディスク]** ダイアログ ボックスを開きます。このダイアログ ボックスでは、ローカル コンピューターから ISO イメージを選択し、ドライブをマップできます。 （注） 読み取り専用ユーザーは仮想メディアを使用できません。

名前	説明
CIMC-Mapped vDVD	[仮想メディアのマップ - CD/DVD] ダイアログ ボックスを開きます。このダイアログ ボックスでは、ローカル コンピューターから ISO イメージを選択し、ドライブをマップできます。また、マッピングを保存、編集、および削除することもできます。 マウントオプションの詳細については、次を参照して表 7 : [Add New Mapping] ダイアログ ボックス （138 ページ）ください。 （注） 読み取り専用ユーザーは仮想メディアを使用できません。
CIMC-Mapped vHDD	[仮想メディアのマップ - CD/DVD] ダイアログ ボックスを開きます。このダイアログ ボックスでは、ローカル コンピューターから ISO イメージを選択し、ドライブをマップできます。また、マッピングを保存、編集、および削除することもできます。 マウントオプションの詳細については、次を参照して表 7 : [Add New Mapping] ダイアログ ボックス （138 ページ）ください。 （注） 読み取り専用ユーザーは仮想メディアを使用できません。

表 *7 : [Add New Mapping]* ダイアログボックス

名前	説明
[名前（Name）] フィールド	仮想メディアのユーザー定義名。
NFS ボタン	ネットワーク ファイル システム ベースのマッピング。
CIFS ボタン	共通インターネット ファイル システム ベースのマッピング
HTTP/S	HTTP ベースまたは HTTPS ベースのマッピング。
[ファイルの場所] フィールド	次の形式の .iso ファイルの場所 : • *<IP* アドレスまたは *DNS* 名>[:ポート]/*.iso* ファイル パス

名前	説明
[Username] フィールド	（注） **CIFS** および **HTTP/S** ベースのマッピングでのみ使用できます。 ユーザ名（該当する場合）。
[パスワード（Password）] フィールド	（注） **CIFS** および **HTTP/S** ベースのマッピングでのみ使用できます。 選択したユーザ名のパスワード（該当する場合）。
[マウント オプション（Mount Options）] フィールド	（注） **CIFS** および **NFS** ベースのマッピングでのみ使用できます。 選択されたマウント オプション。 • NFS — NFS の場合、フィールドを空白のままにするか、次の 1 つ以上を入力してください。 • wsize=VALUE • vers=VALUE • timeo=VALUE • retrans=VALUE • retry=VALUE • rsize=VALUE • CIFSの場合、フィールドを空白のままにするか、次の1つ以上入力してください。 • nounix • noserverino • sec=VALUE • vers=VALUE
[自動再マップ] チェックボックス	ホスト システムがメディアを排出すると、Cisco IMC はデバイスを自動的に再マッピングします。
保存された vMedia ボタン	右側に追加の領域を開き、それぞれのリストから保存されている vMedia を選択します。
[**保存（Save）**] ボタン	vMedia を保存します。

名前	説明
[マップ ドライブ] ボタン	マウントされた vMedia を保存してマッピングします。
CD/DVD パネル	保存されている vMedia のリストを提供します。**CIMC マップされた vDVD** オプションを使用してマッピングしている場合は、このリストから任意の vMedia を編集または削除することもできます。
[リムーバブル ディスク] パネル	保存されている vMedia のリストを提供します。**CIMC-Mapped vHDD** オプションを使用してマッピングしている場合は、このリストから任意の vMedia を編集または削除することもできます。

チャットメニュー

メニュー項目	説明
[Chat]	他のユーザーと通信するための [Chat] ボックスを開きます。

ヘルプ アイコン

名前	説明
サイトツアーを実施	新しいコンソールのクイックインタラクティブツアーを提供します。
Help Topics	このオプションをクリックすると、このウィンドウに戻ります。
弊社について	Cisco vKVM コンソールのバージョン番号を表示します。

言語アイコン

サポートされている言語のドロップダウン リストを表示します。リストから目的の言語を選択できます。

プロフィールメニューアイコン

プロファイル メニュー アイコンは、コンソールの右上隅にあります。

名前	説明
ロール	ユーザ ロール名を表示します。
サーバ	ホスト名と IP アドレスを表示します。
[設定（Settings）]	[設定Settingsダイアログボックスを開きます。 • 縦横比の維持トグル - ビューアウィンドウの縦横比を維持します。 • マウスのモード • 絶対配置 — ビュー内のカーソル位置は、ローカル マシンのカーソル位置を反映します。 • 相対位置 — ビュー内のカーソル位置は、前の位置を基準にして計算されます。 • [ビデオ非アクティブ タイムアウト] ドロップダウン リスト — コンソール ビデオがタイムアウトするまでの、事前設定された時間またはコンソールでの非アクティブを選択できます。 • Number of terminal scrollback lines フィールド：Cisco SOL 端末でスクロールできる行数を設定できます。 • テーマ — ダークテーマとライトテーマを切り替えることができます。 • 保存ボタン—すべてのユーザーの設定を保存します。
サインアウト	サインアウトして、vKVM コンソールを閉じます。

仮想 KVM の設定

始める前に

仮想 KVM を設定するには、admin 権限を持つユーザーとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 **[コンピューティング（Compute）]**メニューでサーバを選択します。

ステップ 3 作業ウィンドウで **[リモート管理（Remote Management）]**タブをクリックします。

ステップ 4 [Remote Management] ペインで、[Virtual KVM] タブをクリックします。

ステップ 5 [Virtual KVM] タブ の **[vKVM プロパティ (vKVM Properties)]** 領域で、次のフィールドに値を入力します。

名前	説明
[Enabled] チェックボックス	オンにすると、仮想 KVM がイネーブルになります。 （注） 仮想メディア ビューアには KVM を使用してアクセスします。KVM コンソールをディセーブルにすると、Cisco IMC はホストに接続されているすべての仮想メディアデバイスへのアクセスもディセーブルにします。
[Max Sessions] ドロップダウンリスト	許可されている KVM の同時セッションの最大数。選択できる数値は 1 ～ 4 です。
[Active Sessions] フィールド	サーバで実行されている KVM セッションの数。
[リモートポート（Remote Port）] フィールド	KVM 通信に使用するポート。
[Enable Video Encryption] チェックボックス	オンにすると、サーバは KVM で送信されるすべてのビデオ情報を暗号化します。
[Enable Local Server Video] チェックボックス	オンにすると、KVMセッションはサーバに接続されているすべてのモニタにも表示されます。

ステップ 6 [Save Changes] をクリックします。

仮想 KVM のイネーブル化

始める前に

仮想 KVM をイネーブルにするには、admin 権限を持つユーザーとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [コンピューティング（Compute）] メニューをクリックします。
ステップ 2 **[コンピューティング（Compute）]** メニューでサーバを選択します。
ステップ 3 **作業ウィンドウで [リモート管理（Remote Management）]** タブをクリックします。
ステップ 4 [Remote Management] ペインで、[Virtual KVM] タブをクリックします。
ステップ 5 [Virtual KVM] タブで、[Enabled] チェックボックスをオンにします。
ステップ 6 [Save Changes] をクリックします。

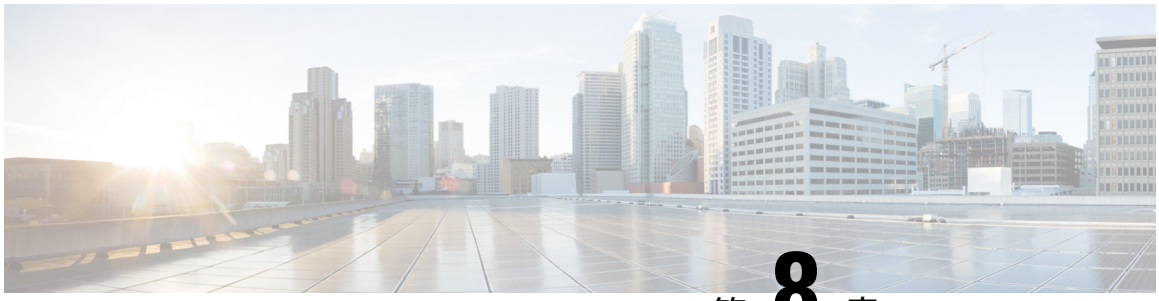
仮想 KVM のディセーブル化

始める前に

仮想 KVM をディセーブルにするには、admin 権限を持つユーザーとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [コンピューティング（Compute）] メニューをクリックします。
ステップ 2 **[コンピューティング（Compute）]** メニューでサーバを選択します。
ステップ 3 **作業ウィンドウで [リモート管理（Remote Management）]** タブをクリックします。
ステップ 4 [Remote Management] ペインで、[Virtual KVM] タブをクリックします。
ステップ 5 [Virtual KVM] タブで、[Enabled] チェックボックスをオフにします。
ステップ 6 [Save Changes] をクリックします。



第 8 章

ユーザー アカウントの管理

この章は、次の内容で構成されています。

Cisco USC C シリーズ M7 および以降のサーバー向けローカル ユーザーの追加

Cisco IMC では、強力なパスワード ポリシーが実装されるようになったため、サーバーに最初にログインした際に、ガイドラインに従って強力なパスワードを設定するよう要求されます。**[ローカル ユーザ（Local User）]**タブに表示される **[強力なパスワードの無効化（Disable Strong Password）]** ボタンを使用すると、強力なパスワード ポリシーを無効にし、ガイドラインを無視して自由にパスワードを設定できます。強力なパスワードを無効にすると、**[強力なパスワードの有効化（Enable Strong Password）]**ボタンが表示されます。デフォルトでは、強力なパスワード ポリシーが有効になっています。

始める前に

ローカルユーザーアカウントを追加するには、admin権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーザ管理（User Management）] をクリックします。

ステップ 3 [ユーザー管理（User Management）] ペインの [ローカルユーザー管理（Local User Management）] タブをクリックします。

ステップ 4

ステップ 5 ローカル ユーザー アカウントを追加するには、**[ユーザーを追加 （Add User）]**をクリックします。

ローカル ユーザー アカウントを変更するには、**[ローカル ユーザー管理（Local User Management）]**ペインで行をクリックし、**[ユーザの変更（Modify User**）をクリックします。

ステップ 6 **[ユーザーの詳細の変更（Modify User Details）]** または、**[ローカル ユーザー詳細（Local User Details）]** ダイアログボックスで、次のプロパティを更新します。

名前	説明
[ID] フィールド	ユーザーの固有識別情報。識別子はユーザーが構成できません。識別子が自動的に割り当てられます。
[ユーザー名（Username）] フィールド	ユーザーのユーザー名。 ユーザー名は、**CIMC** および **SNMP** ユーザー タイプ（任意の組み合わせ）の場合は最大 32 文字、**IPMI** ユーザー タイプ（任意の組み合わせ）の場合は最大 16 文字です。**ユーザー タイプ**の詳細については、**ユーザー タイプ** チェック ボックスの説明を参照してください。

名前	説明
[Role Played] フィールド	ユーザに割り当てられているロール。次のいずれかになります。 • [read-only]：このロールのユーザは情報を表示できますが、変更することはできません。 • [user]：このロールのユーザは、次のタスクを実行できます。 • すべての情報を表示する • 電源のオン、電源再投入、電源のオフなどの電力制御オプションを管理する • vKVM コンソールと仮想メディアを起動する • すべてのログをクリアする • ping • [admin]：このロールのユーザーは、GUI、CLI、IPMI で可能なすべてのアクションを実行できます。 • **snmponly** - SNMP ロールのみを持つユーザー。 （注） 管理ロールを持つユーザーには、**[設定 (Settings)]** ドロップダウン メニューの右上隅にある **[パスワードの変更 (Change Password)]** オプションがありません。 非管理ユーザーとしてパスワードを変更するには、**[読み取り専用 (read-only)]** または **[ユーザー (User)]** ロールを選択します。**[管理者 (admin)]** ロールは選択しません。
ユーザー タイプ チェックボックス	次のタイプのユーザーを作成できます。 • CIMC • SNMP • IPMI 単独のユーザーに複数のタイプを割り当てることができます。
[有効（Enabled）] チェックボックス	オンにすると、ユーザーはCisco IMC で有効にされています。

表 *8 : CIMC* ユーザー タイプ

名前	説明
[Password] フィールド	適切なパスワードを入力します。パスワード要件の詳細については、カーソルを**[提案（Suggest）]**ボタンの横にある**?**アイコンにホバーさせます。
[Confirm Password] フィールド	確認のために繰り返して入力するパスワード。
[提案（Suggest）] ボタン	このオプションは、システムが生成したパスワードに使用できます。

表 *9 : SNMP* ユーザー タイプ

名前	説明
[Security Level] ドロップダウン リスト	このユーザのセキュリティ レベル。次のいずれかになります。 • [no auth, no priv]：このユーザには、許可パスワードもプライバシー パスワードも不要です。 • [auth, no priv]：このユーザーには、許可パスワードが必要ですが、プライバシー パスワードは不要です。このオプションを選択すると、Cisco IMC は後述の Auth フィールドを有効にします。 • [auth, priv]：このユーザには、許可パスワードとプライバシー パスワードの両方が必要です。このオプションを選択すると、Cisco IMC は Auth フィールドおよび Privacy フィールドを有効にします。
[Auth Type] ドロップダウン	許可タイプ。次のいずれかになります。 • **HMAC_SHA96** • **HMAC128_SHA224** • **HMAC192_SHA256** • **HMAC256_SHA384** • **HMAC384_SHA512**

名前	説明
[Auth Password] フィールド	この SNMP ユーザの許可パスワード。 8～64 個の文字またはスペースを入力します。 （注） Cisco IMC は先頭または末尾のスペースを自動的に切り詰めます。
[Confirm Auth Password] フィールド	確認のための許可パスワードの再入力。
[プライバシー タイプ（Privacy Type）] ドロップダウン	プライバシー タイプ。次のいずれかになります。
[Privacy Password] フィールド	この SNMP ユーザのプライバシー パスワード。 8～64 個の文字またはスペースを入力します。 （注） Cisco IMC は先頭または末尾のスペースを自動的に切り詰めます。
[Confirm Privacy Password] フィールド	確認のための許可パスワードの再入力。

表 *10 : IPMI* ユーザー タイプ

名前	説明
[Password] フィールド	適切なパスワードを入力します。パスワード要件の詳細については、カーソルを**[提案（Suggest）]** ボタンの横にある **?** アイコンにホバーさせます。
[Confirm Password] フィールド	確認のために繰り返して入力するパスワード。
[提案（Suggest）] ボタン	このオプションは、システムが生成したパスワードに使用できます。

ステップ 7 [保存（Save）] をクリックします。

Cisco USC C シリーズ M7 および以降のサーバー向けローカル ユーザーの変更

Cisco IMC に強力なパスワード ポリシーが導入されました。このポリシーでは、初めてサーバにログオンするときに、ガイドラインに従って強力なパスワードを設定する必要があります。

[ローカル ユーザ（Local User）]タブに表示される **[強力なパスワードの無効化（Disable Strong Password）]** ボタンを使用すると、強力なパスワードポリシーを無効にし、ガイドラインを無視して自由にパスワードを設定できます。強力なパスワードを無効にすると、**[強力なパスワードの有効化（Enable Strong Password）]**ボタンが表示されます。デフォルトでは、強力なパスワード ポリシーが有効になっています。

始める前に

ローカルユーザーアカウントを設定または変更するには、admin 権限を持つユーザーとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーザ管理（User Management）] をクリックします。

ステップ 3 [ユーザー管理（User Management）] ペインの [ローカルユーザー管理（Local User Management）] タブをクリックします。

ステップ 4 ローカルユーザアカウントを変更するには、**[ローカル ユーザ管理（Local User Management）]** ペインで行をクリックし、**[ユーザの変更（Modify User）]** をクリックします。

ステップ 5 [ユーザーの詳細の変更（Modify User Details）] ダイアログボックスで、次のプロパティを更新します。

名前	説明
[ID] フィールド	ユーザーの固有識別情報。 これは、ユーザーが構成することはできません。
[ユーザー名（Username）] フィールド	ユーザーのユーザー名。 1 ～ 16 文字の範囲で入力します。

名前	説明
[割り当てられるロール（Role Played）] フィールド	ユーザに割り当てられているロール。次のいずれかになります。 • [read-only]：このロールのユーザは情報を表示できますが、変更することはできません。 • [user]：このロールのユーザは、次のタスクを実行できます。 • すべての情報を表示する • 電源のオン、電源再投入、電源のオフなどの電力制御オプションを管理する • vKVM コンソールと仮想メディアを起動する • すべてのログをクリアする • ロケータ LED の点灯・消灯（リモート作業者に場所を示す） • タイムゾーンの設定 • ping • [admin]：このロールのユーザーは、GUI、CLI、IPMI で可能なすべてのアクションを実行できます。
ユーザータイプ	ユーザー タイプを次のように更新できます： • CIMC • SNMP • IPMI 単独のユーザーに複数のタイプを割り当てることができます。
[Enabled] チェックボックス	オンにすると、ユーザはCisco IMC でイネーブルになります。
[Change Password] チェックボックス	オンにすると、変更を保存した場合、このユーザのパスワードが変更されます。パスワードを変更するには、このチェックボックスをオンにする必要があります。 **[パスワードの変更（Change Password）]** チェック ボックスも、チェックされているすべての **[ユーザー タイプ（User Type）]** オプションを開きます。

表 *11 : CIMC* ユーザー タイプ

名前	説明
[Password] フィールド	適切なパスワードを入力します。パスワード要件の詳細については、カーソルを**[提案（Suggest）]**ボタンの横にある**?**アイコンにホバーさせます。
[Confirm Password] フィールド	確認のために繰り返して入力するパスワード。
[提案（Suggest）] ボタン	このオプションは、システムが生成したパスワードに使用できます。

表 *12 : SNMP* ユーザー タイプ

名前	説明
[Security Level] ドロップダウン リスト	このユーザのセキュリティ レベル。次のいずれかになります。 • [no auth, no priv]：このユーザには、許可パスワードもプライバシー パスワードも不要です。 • [auth, no priv]：このユーザーには、許可パスワードが必要ですが、プライバシー パスワードは不要です。このオプションを選択すると、Cisco IMC は後述の Auth フィールドを有効にします。 • [auth, priv]：このユーザには、許可パスワードとプライバシー パスワードの両方が必要です。このオプションを選択すると、Cisco IMC は Auth フィールドおよび Privacy フィールドを有効にします。
[Auth Type] ドロップダウン	許可タイプ。次のいずれかになります。 • **HMAC_SHA96** • **HMAC128_SHA224** • **HMAC192_SHA256** • **HMAC256_SHA384** • **HMAC384_SHA512**

名前	説明
[Auth Password] フィールド	この SNMP ユーザの許可パスワード。 8～64 個の文字またはスペースを入力します。 （注） Cisco IMC は先頭または末尾のスペースを自動的に切り詰めます。
[Confirm Auth Password] フィールド	確認のための許可パスワードの再入力。
[プライバシー タイプ（Privacy Type）] ドロップダウン	プライバシー タイプ。次のいずれかになります。
[Privacy Password] フィールド	この SNMP ユーザのプライバシー パスワード。 8～64 個の文字またはスペースを入力します。 （注） Cisco IMC は先頭または末尾のスペースを自動的に切り詰めます。
[Confirm Privacy Password] フィールド	確認のための許可パスワードの再入力。

表 *13 : IPMI* ユーザー タイプ

名前	説明
[Password] フィールド	適切なパスワードを入力します。パスワード要件の詳細については、カーソルを**[提案（Suggest）]** ボタンの横にある **?** アイコンにホバーさせます。
[Confirm Password] フィールド	確認のために繰り返して入力するパスワード。
[提案（Suggest）] ボタン	このオプションは、システムが生成したパスワードに使用できます。

ステップ 6 パスワード情報を入力します。

ユーザ アカウントでの SSH キーの管理

SSH キーの設定

すべてのユーザの SSH キーを表示するには、admin 権限を持つユーザとしてログインする必要があります。管理者以外のユーザの場合は、自分のアカウントの SSH キーのみを表示できます。

パブリック SSH キーを使用して認証された Cisco IMC セッションは、パスワードの有効期限が切れてもアクティブのままです。また、パスワードの有効期限が切れた後に、公開 SSH キーを使用して新しいセッションを開始することもできます。

アカウント ロックアウト オプションは、公開キー認証を使用するアカウントには適用されません。

始める前に

- すべてのユーザの SSH キーを設定するには、admin 権限を持つユーザとしてログインする必要があります。
- SSH RSA キーのペア (パブリックおよびプライベート) が作成されていることを確認します。
- SSH キーが .pem または .pub 形式であることを確認します。

手順

ステップ 1 **[ナビゲーション (Navigation)]** ペインの **[管理者 (Admin)]** メニューをクリックします。

ステップ 2 **[管理者（Admin）]** メニューの **[ユーザ管理（User Management）]** タブをクリックします。

ステップ 3 **[ユーザ管理 (User Management)]** ペインの **[ローカル ユーザ管理 (Local User Management)]** タブをクリックします。

ステップ 4 アカウントに設定されている SSH キーの数を確認するには、**[SSH キー数 (SSH Key Count)]** フィールドの詳細を参照します。

ステップ 5 アカウントの SSH キーの詳細を表示するには、**[ローカル ユーザ管理 (Local User Management)]** ペインの行をクリックし、**[SSH キー (SSH keys)]** をクリックします。

[SSH キー (SSH keys)] ウィンドウが表示されます。

ステップ 6 **[SSH キー (SSH Keys)]** ウィンドウで、次のプロパティを表示します。

名前	説明
[ID] フィールド	SSH キーの固有識別子です。

名前	説明
備考	ユーザ名とリモート サーバのホスト名。*username@hostname* の形式を使用します。
Key	特定のユーザに対して設定されている公開 SSH キーの詳細。

次のタスク

SSH キーを追加または変更します。

SSH キーの追加

始める前に

- すべてのユーザに SSH キーを追加するには、admin 権限を持つユーザとしてログインする必要があります。
- 管理者以外のユーザの場合は、自分のアカウントに対してのみ SSH キーを追加できます。

手順

ステップ 1 **[ナビゲーション (Navigation)]** ペインの **[管理者 (Admin)]** メニューをクリックします。

ステップ 2 **[管理者（Admin）]** メニューの **[ユーザ管理（User Management）]** タブをクリックします。

ステップ 3 **[ユーザ管理 (User Management)]** ペインの **[ローカル ユーザ管理 (Local User Management)]** タブをクリックします。

ステップ 4 アカウントの SSH キーを追加するには、**[ローカル ユーザ管理 (Local User Management)]** ペインの行をクリックし、**[SSH キー (SSH keys)]** をクリックします。

[SSH キー (SSH keys)] ウィンドウが表示されます。

ステップ 5 **[ID]** 列の近くにあるオプション ボタンのいずれかをクリックします。

ステップ 6 **[キーの追加 (Add Keys)]** アイコン (**SSH キー (SSH Keys)]** ウィンドウ) をクリックして、SSH キーを追加します。

ステップ 7 SSH キーを追加するには、次のオプション ボタンのいずれかを選択します。

a) **[SSH キーをペースト (Paste SSH key)]** を選択します。

ホストから公開 SSH キーをコピーし、テキスト フィールドにキーを貼り付けます。

b) **[ローカルからアップロード (Upload from local)]** を選択します。

[参照 (Browse)] をクリックし、追加する公開キー ファイルの場所に移動します。

c) **[リモートの場所からアップロード (Upload from remote location)]** を選択します。

次の詳細情報を入力して、リモート ロケーションから公開キーファイルをアップロードします。

名前	説明
[SSH キー ファイルのアップロード元 (Upload SSH key from)] ドロップダウン リスト	リモート サーバーのタイプ。次のいずれかになります。 • TFTP • FTP • SCP • SFTP • HTTP （注） FTP、SCP または SFTP を選択した場合は、ユーザ名とパスワードの入力が求められます。
[サーバIP/ホスト名（Server IP/Hostname）] フィールド	SSH キーファイルが使用可能なサーバの IP アドレスまたはホスト名
[パスおよびファイル名（Path and Filename）] フィールド	公開 SSH キー ファイルの、リモート サーバ上でのパスとファイル名。

ステップ 8 **[SSH キーのアップロード (Upload SSH Key)]** をクリックします。

次のタスク

SSH キーを変更または削除します。

SSH キーの変更

始める前に

- すべてのユーザの SSH キーを変更するには、admin 権限を持つユーザとしてログインする必要があります。
- 管理者以外のユーザの場合は、自分のアカウントの SSH キーのみを変更できます。

手順

ステップ 1 **[ナビゲーション (Navigation)]** ペインの **[管理者 (Admin)]** メニューをクリックします。

ステップ 2 **[管理者（Admin）]** メニューの **[ユーザ管理（User Management）]** タブをクリックします。

ステップ 3 **[ユーザ管理 (User Management)]** ペインの **[ローカル ユーザ管理 (Local User Management)]** タブをクリックします。

ステップ 4 SSH キーを表示および変更するには、**[ローカル ユーザ管理（Local User Management）]** ペインの行をクリックし、**[SSH キー (SSH keys)]** をクリックします。

[SSH キー (SSH keys)] ウィンドウが表示されます。

ステップ 5 SSH キーを変更するには、SSH キーのリストを確認し、**[SSH キー (SSH keys)]** ウィンドウで目的の行を選択します。

ステップ 6 **[キーの変更（Modifye Key）]** アイコンをクリックします。

ステップ 7 SSH キーを変更するには、次のオプション ボタンのいずれかを選択します。

a) **[SSH キーをペースト (Paste SSH key)]** を選択します。

アップデートされた公開 SSH キーをホストからコピーし、テキスト フィールドにキーをペーストします。

b) **[ローカルからアップロード (Upload from local)]** を選択します。

[参照 (Browse)] をクリックし、アップロードする、アップデートされた公開キー ファイルの場所に移動します。

c) **[リモートの場所からアップロード (Upload from remote location)]** を選択します。

次の詳細情報を入力して、アップデートされた公開キー ファイルをリモートの場所からアップロードします。

名前	説明
[SSH キー ファイルのアップロード元 (Upload SSH key from)] ドロップダウン リスト	リモート サーバーのタイプ。次のいずれかになります。 • TFTP • FTP • SCP • SFTP • HTTP （注） FTP、SCP または SFTP を選択した場合は、ユーザ名とパスワードの入力が求められます。
[サーバIP/ホスト名（Server IP/Hostname）] フィールド	更新された SSH キーファイルが使用可能なサーバの IP アドレスまたはホスト名
[パスおよびファイル名（Path and Filename）] フィールド	アップデートされた公開 SSH キー ファイルの、リモート サーバ上でのパスとファイル名。

ステップ 8 **[SSH キーのアップロード (Upload SSH Key)]** をクリックします。

次のタスク

SSH キーを削除します。

SSH キーの削除

始める前に

- すべてのユーザの SSH キーを削除するには、admin 権限を持つユーザとしてログインする必要があります。
- 管理者以外のユーザの場合は、自分のアカウントの SSH キーのみを削除できます。

手順

ステップ 1 **[ナビゲーション (Navigation)]** ペインの **[管理者 (Admin)]** メニューをクリックします。

ステップ 2 **[管理者（Admin）]** メニューの **[ユーザ管理（User Management）]** タブをクリックします。

ステップ 3 **[ユーザ管理 (User Management)]** ペインの **[ローカル ユーザ管理 (Local User Management)]** タブをクリックします。

ステップ 4 ユーザアカウントの SSH キーを表示および削除するには、**[ローカル ユーザ管理（Local User Management）]** ペインの行をクリックし、**[SSH キー (SSH keys)]** をクリックします。

[SSH キー (SSH keys)] ウィンドウが表示されます。

ステップ 5 SSH キーを削除するには、SSH キーのリストを確認し、**[SSH キー (SSH keys)]** ウィンドウで目的の行を選択します。

ステップ 6 **[キーの削除（Delete Key）]** アイコンをクリックします。

ポップアップ ウィンドウに *[*選択した *SSH* キーを削除しますか*? (Do you want to delete the selected SSH key?)]* というメッセージが表示されます。?

ステップ 7 **[はい (Yes)]** をクリックして削除を確認します。

非 IPMI ユーザー モード

リリース4.1 では、IPMI と非 IPMI の両方のユーザー モードを切り替えることができる**ユーザー モード**と呼ばれる新しいユーザー設定オプションが導入されています。非 IPMI ユーザー モードの導入では、ユーザー向けに強化されたパスワードセキュリティと、IPMI 2.0 標準による制約により以前のリリースで制限された BMC データベースに対してセキュリティ強化を提供し

ます。非 IPMI ユーザー モードでは、127 文字を使用してユーザー パスワードを設定できますが、IPMI モードのユーザーはパスワードの長さが 20 文字に制限されます。非 IPMI ユーザー モードでは、このモードで設定されたユーザーに対してより強力なパスワードを設定できます。

次の場合に、ユーザー モードの切り替え中に発生する次の設定変更を考慮する必要があります。

- 非 IPMI モードに切り替えると、IPMI 経由の IPMI はサポートされません。
- 非 IPMI から IPMI モードに切り替えて、すべてのローカル ユーザーを削除し、ユーザー クレデンシャルをデフォルトのユーザー名とパスワードに戻します。続いてログインすると、デフォルトのパスワードを変更するように求められます。

  IPMI から非 IPMI モードに切り替えた場合、ユーザー データは影響を受けません。
- ファームウェアを 4.1 よりも低いバージョンにダウングレードします。ユーザー モードが非 IPMI の場合、はすべてのローカル ユーザーを削除し、ユーザー クレデンシャルをデフォルトのユーザー名とパスワードに戻します。続いてログインすると、デフォルトのパスワードを変更するように求められます。

（注） 工場出荷時の初期状態にリセットすると、ユーザー モードは IPMI モードに戻ります。

IPMI と非 IPMI のユーザー モードの切り替え

注意 この手順を実行すると、SSH、KVM、Web サーバ、XML API、および REST API サービスが再起動されます。また、非 IPMI ユーザー モードに切り替えると、IPMI ユーザー サポートも削除されます。

始める前に

このアクションを実行するには、admin権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 **[管理 (Admin)]** タブの **[ユーザー管理 (User Management)]** をクリックします。

ステップ 3 **[IPMI ユーザー モードの無効化 (DISABLE Ipmi User mode)]** または **[IPMI ユーザー モードの有効化 (Enable IPMI User Mode)]** ボタンをクリックし、**[OK]** をクリックして確定します。

非管理者ユーザーとしてパスワードの変更

（注） このタスクを実行するには、まず管理者としてログインし、読み取り専用権限またはユーザー権限を持つユーザーを追加する必要があります。その場合にのみ、非管理者ユーザーとしてログインしてパスワードを変更できます。

手順

ステップ 1 管理者ユーザーとしてログインします。

ステップ 2 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 3 [管理（Admin）] メニューで [ユーザ管理（User Management）] をクリックします。

ステップ 4 [ユーザー管理（User Management）] ペインの [ローカル ユーザー管理（Local User Management）] タブをクリックします。

ステップ 5 ローカル ユーザ アカウントを設定または追加するには、[ローカルユーザ管理（Local User Management）] ペインの行をクリックして、[ユーザの追加（Add User）] をクリックします。

ステップ 6 **[Add User]** ダイアログボックスで、読み取り専用またはユーザ権限をもつユーザを追加することで、次のプロパティを更新します。

名前	説明
[ID] フィールド	ユーザの固有識別情報。
[ユーザ名（Username）] フィールド	ユーザーのユーザー名。 1 ～ 16 文字の範囲で入力します。

名前	説明
[割り当てられるロール（Role Played）] フィールド	ユーザに割り当てられているロール。次のいずれかになります。 • [read-only]：このロールのユーザは情報を表示できますが、変更することはできません。 • [user]：このロールのユーザは、次のタスクを実行できます。 • すべての情報を表示する • 電源のオン、電源再投入、電源のオフなどの電力制御オプションを管理する • KVM コンソールと仮想メディアを起動する • すべてのログをクリアする • ロケータ LED の点灯・消灯（リモート作業者に場所を示す） • タイムゾーンの設定 • ping • [admin]：このロールのユーザーは、GUI、CLI、IPMI で可能なすべてのアクションを実行できます。 （注） パスワードを変更するには、[読み取り専用（）] または[ユーザー（User）] ロールを選択します。[管理者（admin）] ロールは選択しません。
[Enabled] チェックボックス	オンにすると、ユーザは Cisco IMC でイネーブルになります。
[Change Password] チェックボックス	オンにすると、ユーザがパスワードを変更できるようになります。

名前	説明
[新しいパスワード（New Password）]	このユーザー名のパスワードを入力します。 **[Suggest]** ボタンをクリックして、使用するシステム生成パスワードを取得します。 このフィールドの横にあるヘルプ アイコン上にマウスを移動すると、パスワード設定に関する以下のガイドラインが表示されます。 • パスワードは 8 ～ 14 文字とすること。 IPMI 以外のユーザーの場合、パスワードの最大文字数は 127 文字です。 • パスワードにユーザー名を含めないこと。 • パスワードには次の 4 つのカテゴリの中から 3 つに該当する文字を含めること。 • 英大文字（A から Z まで）。 • 英小文字（a から z まで）。 • 10 進数の数字（0 ～ 9）。 • アルファベット以外の文字（!、@、#、$、%、^、&、*、-、_、=、'）。 これらのガイドラインは、セキュリティ上の理由でユーザーのための強力なパスワードを定義することを意図したものです。しかし、これらのガイドラインを無視して自分で選択したパスワードを設定するには、**[ローカル ユーザ管理（Local User Management）]** タブにある **[強力なパスワードを無効にする（Disable Strong Password）]** ボタンをクリックします。強力なパスワードのオプションが無効になっている場合にパスワードを設定する場合、1 文字以上、20 文字以下のものを使用できます。
[パスワードの確認（Confirm Password）] フィールド	確認のために繰り返して入力するパスワード。

ステップ 7 [Save Changes] をクリックします。

（注） パスワードを変更する場合、Cisco IMC からログアウトされます。

ステップ 8 読み取り専用またはユーザー権限をもつ新しいユーザを作成した後、管理者としてログアウトします。

ステップ 9 ここでは、読み取り専用で新しく作成したログインまたはユーザ ロール。**[Change Password (パスワードの作成)]**オプションは、**[Settings (設定)]**ドロップダウン メニューで右上隅で選択できます。

[Settings] アイコンをクリックすると、ドロップダウンには **[Change Password]** オプションがリストされます。このオプションは、非管理者ユーザとしてログインする場合にのみ表示されます。

ドロップダウン リストに [パスワードの変更（Change Password）] オプションが表示されない場合は、読み取り専用権限またはユーザ権限をもつ非管理者ユーザとしてログインします。

[Change Password] オプションを使用してパスワードを変更できます。パスワードを変更するとすぐに、非管理者ユーザーは自動的にログアウトし、新しいパスワードを使用してログインするように求められます。

パスワードの有効期限切れ

パスワードが期限切れになる有効期限を設定できます。管理者はこの期間を日単位で設定できます。この設定はすべてのユーザに対して共通です。パスワードが期限切れになると、ユーザに対してログイン時にこのことが通知され、パスワードをリセットするまではログインできなくなります。

（注） 古いデータベースにダウングレードすると、既存のユーザが削除されます。データベースはデフォルト設定に戻ります。以前に設定されたユーザが消去され、データベースは空になります。つまり、データベースにはデフォルトのユーザ名「admin」とパスワード「password」が設定されます。サーバにはデフォルトのユーザ データベースが残るため、デフォルト クレデンシャル変更機能が有効になります。つまり、「admin」ユーザはダウングレード後にデータベースに初めてログインするときに、デフォルトのクレデンシャルを変更する必要があります。

パスワード設定時刻

既存のすべてのユーザの「パスワード設定時刻」は、移行またはアップグレードの実行時刻に設定されます。新しいユーザ（アップグレード後に作成されるユーザ）の場合、パスワード設定時刻はそのユーザが作成され、パスワードが設定された時刻に設定されます。ユーザ全般（新規および既存）について、パスワードが変更されるたびにパスワード設定時刻が更新されます。

パスワードの有効期間の設定

始める前に

- パスワードの有効期限を有効にする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーザ管理（User Management）] をクリックします。

ステップ 3 [Local User Management] ペイン（デフォルトで開きます）で、[Password Expiration Details] をクリックします。

ステップ 4 [Password Expiration Details] ダイアログボックスで、次のフィールドを更新します。

名前	説明
[パスワード有効期日を有効にする（Enable Password Expiry）] チェックボックス	このボックスをオンにすると、[パスワード有効期間（Password Expiry Duration）] を設定できます。無効にするには、このチェックボックスをオフにします。
[パスワード有効期間（Password Expiry Duration）] フィールド	既存のパスワードに設定できる有効期間（その時間以後、新しいパスワードを設定するか、または既存のパスワードを変更します）。範囲は 1 ～ 3650 日です。 （注） 管理者により一度設定されたパスワード有効期限は、その後に作成されるすべてのユーザに適用されます。
[Password History] フィールド	パスワードが入力された回数。このフィールドを有効にすると、指定された回数を超えてパスワードを繰り返し使用することができなくなります。0 ～ 5 の間の値を入力します。0 を入力すると、このフィールドが無効になります。
[通知期間（Notification Period）] フィールド	パスワードの期限が切れる時間を通知します。0 日から 15 日までの値を入力します。0 を入力すると、このフィールドが無効になります。 （注） 通知期間の時間は、パスワードの有効期間内でなければなりません。

名前	説明
[Grace Period] フィールド	既存のパスワードをまだ使用できる期間。この期間の後、パスワードは期限切れになります。0 日から 5 日までの値を入力します。0 を入力すると、このフィールドが無効になります。 （注） 猶予期間の時間は、パスワードの有効期間内でなければなりません。

（注） 有効な [パスワードの有効期間（Password Expiry Duration）] は、[通知期間（Notification Period）] および [猶予期間（Grace Period）] より長い必要があります。そうでない場合、**[ユーザ パスワードの有効期限ポリシーの設定エラー（User Password Expiry Policy configuration error）]** が表示されます。

ステップ 5 [Save Changes] をクリックします。

ステップ 6 オプションで、**[値のリセット（Reset Values）]**をクリックしてテキスト フィールドをクリアし、入力した値をリセットします。デフォルト設定に戻すには、**[デフォルトに戻す（Restore Defaults）]**をクリックします。

パスワード有効期限の有効化

始める前に

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーザ管理（User Management）] をクリックします。

ステップ 3 [Local User Management] ペイン（デフォルトで開きます）で、[Password Expiration Details] をクリックします。

ステップ 4 **[パスワードの有効期限の詳細（Password Expiration Details）]** ダイアログボックスで、**[パスワード有効期限の有効化（Enable Password Expiry）]** チェックボックスをオンにします。

[パスワードの有効期間（Password Expiry Duration）] テキスト フィールドが編集可能になるので、有効期間を日数単位で設定できます。

次のタスク

パスワードの有効期間を設定します。

アカウントロックアウトの詳細の構成

手順

ステップ 1 **[ナビゲーション（Navigation）]** ペインで **[管理（Admin）]** メニューをクリックします。

ステップ 2 **[管理（Admin）]** メニューで **[ユーザー管理（User Management）]** をクリックします。

ステップ 3 **[ユーザー管理（User Management）]** ペインで **[ローカル ユーザー管理（Local User Management）]** タブをクリックします。

ステップ 4 **[ローカル ユーザー管理（Local User Management）]** ウィンドウで、**[アカウント ロックアウトの詳細（Account Lockout Details）]** をクリックします。

ステップ 5 **[アカウント ロックアウト詳細（Account Lockout Details）]** ダイアログボックスで、次の手順を行います：

名前	説明
許可された試行（0 ～ 20）フィールド	**[ロックアウト期間]** で定義された期間中にロックアウトされるまでの、ユーザーの失敗したログイン試行の数。
ロックアウト期間 (0 ～ 60 分）フィールド	許可された試行の後、ユーザー アカウントがロックアウトされる時間（分単位）。
ロックアウト状態のユーザーを無効化 チェックボックス	ロックアウト状態でユーザー識別子を無効化します。

ユーザー認証の優先順位の構成

手順

ステップ 1 **[ナビゲーション（Navigation）]** ペインで **[管理（Admin）]** メニューをクリックします。

ステップ 2 **[管理（Admin）]** メニューで **[ユーザー管理（User Management）]** をクリックします。

ステップ 3 **[ユーザー管理（User Management）]** ペインで **[ローカル ユーザー管理（Local User Management）]** タブをクリックします。

ステップ 4 **[ローカル ユーザー管理（Local User Management）]** ウィンドウで、**[ユーザー認証の優先順位の構成（Configure User Authentication Precedence）]** をクリックします。

ステップ 5 **[ユーザー認証の優先順位の構成（Configure User Authentication Precedence）]** ダイアログ ボックスで、優先順位を更新するデータベースを選択します。

ステップ 6 上矢印または下矢印を使用して、データベースの優先順位を変更します。

ユーザー クレデンシャルを工場出荷時の値にリセットする

⚠

注意 この手順を実行すると、現在の IP アドレス設定、NIC ポート設定、NIC 冗長性が失われる可能性があります。この手順を実行する前に、現在のサーバ設定をメモしておくことを推奨します。

始める前に

管理イーサネット ケーブルを専用管理ポートに差し込みます。

手順

ステップ 1 管理者ユーザとしてログインします。

ステップ 2 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 3 [Chassis] メニューの [Summary] をクリックします。

ステップ 4 ツールバーで、**[KVM の起動 (Launch KVM)]**をクリックします。

ステップ 5 または、[Navigation] ペインの [Compute] メニューをクリックします。

1. [Compute] メニューでサーバを選択します。
2. 作業ウィンドウの [Remote Management] タブをクリックします。
3. [Remote Management] ペインで、[Virtual KVM] タブをクリックします。
4. **[仮想 KVM (Virtual KVM)]** タブで、**[HTML ベース KVM コンソールの起動 (Launch HTML based KVM console)]** をクリックします。

ステップ 6 **[電源 (Power)]** メニューから **[システムのリセット (Reset System)]** を選択します。

ステップ 7 プロンプトが表示されたら、**F8** を押して、Cisco IMC 設定ユーティリティを起動します。このユーティリティは、KVM コンソール ウィンドウで開きます。

ステップ 8 **[工場出荷時 (Factory Default)]** チェックボックスをオンにすると、サーバは出荷時の初期状態に戻ります。

ステップ 9 F5 を押して、行った設定に更新します。次の手順でサーバをリブートする前は、新しい設定が表示されメッセージ「**ネットワーク設定が構成されました**」が表示されるまでに約 45 秒かかる場合があります。

ステップ 10 F10 を押して設定を保存し、サーバを再起動します。

LDAP サーバー

Cisco IMC では、情報をディレクトリ内で編成してこの情報へのアクセスを管理するディレクトリ サービスがサポートされます。Cisco IMC は、ネットワークでディレクトリ情報を保管および保持する軽量ディレクトリ アクセス プロトコル（LDAP）をサポートします。さらに、Cisco IMC は Microsoft Active Directory（AD）もサポートします。Active Directory はさまざまなネットワーク サービスを提供するテクノロジーであり、LDAP と同様のディレクトリ サービス、Kerberos ベースの認証、DNS ベースの名前付けなどが含まれます。Cisco IMC は LDAP での Kerberos ベースの認証サービスを利用します。

Cisco IMC で LDAP が有効になっている場合、ローカル ユーザー データベース内に見つからないユーザー アカウントに関するユーザー認証とロール許可は、LDAP サーバーによって実行されます。LDAP ユーザー認証の形式は username@domain.com です。

[LDAP 設定（LDAP Settings）] 領域の [暗号化の有効化（Enable Encryption）] チェックボックスをオンにすると、LDAP サーバへの送信データを暗号化するようサーバに要求できます。

LDAP サーバの設定

ユーザ認証および権限付与のために LDAP を使用するよう、Cisco IMC を設定できます。LDAP を使用するには、Cisco IMC に関するユーザ ロール情報とロケール情報を保持する属性を使ってユーザを設定します。Cisco IMC のユーザ ロールとロケールにマップされた既存の LDAP 属性を使用できます。または、LDAP スキーマを変更して、属性 ID 1.3.6.1.4.1.9.287247.1 を持つ CiscoAVPair 属性などの新しいカスタム属性を追加できます。

重要 スキーマの変更の詳細については、http://technet.microsoft.com/en-us/library/bb727064.aspx の記事を参照してください。

（注） この例では CiscoAVPair という名前のカスタム属性を作成しますが、Cisco IMC のユーザ ロールとロケールにマップされた既存の LDAP 属性を使用することもできます。

Cisco IMC の LDAP 設定でグループ認証を使用している場合、手順 1 ~ 4 をスキップし、*Cisco IMC でLDAP* 設定とグループ認証の構成のセクションに記載されている手順を実行します。

LDAP サーバに対して次の手順を実行する必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーザ管理（User Management）] をクリックします。

ステップ 3 [ユーザ管理（User Management）] ペインで [LDAP] をクリックします。

ステップ 4 LDAP スキーマ スナップインがインストールされていることを確認します。

ステップ 5 スキーマ スナップインを使用して、次のプロパティを持つ新しい属性を追加します。

プロパティ	値
Common Name	**CiscoAVPair**
LDAP Display Name	**CiscoAVPair**
Unique X500 Object ID	**1.3.6.1.4.1.9.287247.1**
Description	**CiscoAVPair**
Syntax	**Case Sensitive String**

ステップ 6 スナップインを使用して、ユーザ クラスに CiscoAVPair 属性を追加します。

a) 左ペインで [Classes] ノードを展開し、**u** を入力してユーザ クラスを選択します。

b) [Attributes] タブをクリックして、[Add] をクリックします。

c) **c** を入力して CiscoAVPair 属性を選択します。

d) [OK] をクリックします。

ステップ 7 Cisco IMC にアクセスできるようにするユーザに対し、次のユーザ ロール値を CiscoAVPair 属性に追加します。

ロール	CiscoAVPair 属性値
admin	**shell:roles="admin"**
user	**shell:roles="user"**
read-only	**shell:roles="read-only"**

（注） 属性に値を追加する方法の詳細については、http://technet.microsoft.com/en-us/library/bb727064.aspx の記事を参照してください。

次のタスク

Cisco IMC を使用して LDAP サーバを設定します。

Cisco IMC での LDAP 設定およびグループ認証の設定

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーザ管理（User Management）] をクリックします。

ステップ 3 [ユーザ管理（User Management）] ペインで [LDAP] をクリックします。

ステップ 4 [LDAP Settings] 領域で、次のプロパティを更新します。

名前	説明
[LDAP を有効にする（Enable LDAP）] チェックボックス	このチェックボックスをオンにすると、まず LDAP サーバによってユーザ認証とロール許可が実行された後、ローカル ユーザ データベース内に見つからないユーザ アカウントの認証が行われます。
[ベース DN（Base DN）] フィールド	ベース識別名。このフィールドは、ユーザーおよびグループのロード元を示します。 Active Directory サーバでは、**dc=domain,dc=com** の形式でなければなりません。
[ドメイン（Domain）]フィールド	すべてのユーザーが属する必要のある IPv4 ドメイン。 グローバル カタログ サーバーのアドレスを少なくとも 1 つ指定していない限り、このフィールドは必須です。
[Enable Secure LDAP] チェックボックス	オンにすると、サーバはセキュア LDAP を有効にし、LDAP CA 証明書をダウンロードするように求めます。LDAP CA 証明書のダウンロード方法については、LDAP CA 証明書のダウンロード （179 ページ） を参照してください。 既存のセキュア LDAP 証明書を削除するには、このオプションをオフにします。システム プロンプトに従って、削除を確認します。

名前	説明
[Timeout (0 - 180) seconds]	LDAP 検索操作がタイムアウトするまで Cisco IMC が待機する秒数。 検索操作がタイムアウトになった場合、Cisco IMC はこのタブで次にリストされているサーバー（存在する場合）に接続しようと試行します。 （注） このフィールドに指定する値は、全体的な時間に影響を及ぼす可能性があります。

（注） **[セキュア LDAP を有効化 (Enable Secure LDAP)]**チェックボックスをオンにする場合には、LDAP サーバのの完全修飾ドメイン名 (FQDN)を **[LDAP サーバ(LDAP Server)]** フィールドに入力します。LDAP サーバーの FQDN を解決するには、Cisco IMC ネットワークの優先 DNS を設定して適切な DNS IP アドレスを指定します。

ステップ 5 [LDAP サーバーの設定（Configure LDAP Servers）] 領域で、次のプロパティを更新します。

名前	説明
[事前設定の LDAP サーバ（Pre-Configure LDAP Servers）] オプション ボタン	これを選択すると、Active Directory は事前設定された LDAP サーバを使用します。
[LDAP サーバ（LDAP Servers）] フィールド	
[サーバー（Server）]	6 つの LDAP サーバの IP アドレス。 LDAP に Active Directory を使用している場合、サーバ 1、2、3 はドメイン コントローラ、サーバ 4、5、6 はグローバル カタログです。LDAP に Active Directory を使用していない場合は、最大で 6 つの LDAP サーバを設定できます。 （注） また、ホスト名の IP アドレスも指定できます。
Port	サーバのポート番号。 LDAP に Active Directory を使用している場合、サーバ 1、2、3（ドメイン コントローラ）のデフォルト ポート番号は 389 です。サーバ 4、5、6（グローバル カタログ）のデフォルト ポート番号は 3268 です。 LDAPS 通信は TCP 636 ポートで行われます。グローバル カタログ サーバへの LDAPS 通信は TCP 3269 ポートで行われます。

名前	説明
[DNS を使用して LDAP サーバを設定する（Use DNS to Configure LDAP Servers）] オプション ボタン	これを選択した場合、DNS を使って LDAP サーバへのアクセスを設定できます。
[DNS パラメータ（DNS Parameters）] フィールド	
[Source] ドロップダウン リスト	DNS SRV 要求に使われるドメイン名を取得する方法を指定します。次のいずれかを指定できます。 • **[抽出済み（Extracted）]**：ログイン ID からのドメイン名抽出ドメインを使用することを指定します。 • **[設定済み（Configured）]**：設定された検索ドメインを使用することを指定します。 • **[設定済み - 抽出済み（Configured-Extracted）]**：設定された検索ドメインよりも、ログイン ID から抽出されるドメイン名を優先することを指定します。
[Domain to Search]	DNS クエリーのソースとして機能する設定済みドメイン名。 **[抽出済み（Extracted）]** としてソースが指定されている場合、このフィールドは無効になります。
[Forest to Search]	DNS クエリーのソースとして機能する設定済みフォレスト名。 **[抽出済（Extracted）]** としてソースが指定されている場合、このフィールドは無効になります。

ステップ 6 [バインド パラメータ（Binding Parameters）] エリアで、次のプロパティを更新します。

名前	説明
[Method] ドロップダウンリスト	次のいずれかを指定できます。 • **[匿名（Anonymous）]**：ユーザ名とパスワードを NULL にする必要があります。このオプションが選択され、LDAP サーバで匿名ログインが設定されている場合は、ユーザがアクセスできます。 • **[設定済みクレデンシャル（Configured Credentials）]**：初期バインドプロセスで既知のクレデンシャル セットを指定する必要があります。初期バインド プロセスが成功した場合、ユーザ名の識別名（DN）が照会されて、その DN が再バインディング プロセスで再利用されます。再バインド プロセスが失敗すると、ユーザはアクセスを拒否されます。 • **[ログイン クレデンシャル（Login Credentials）]**：ユーザ クレデンシャルが必要です。バインド プロセスが失敗すると、ユーザーはアクセスを拒否されます。 デフォルトでは [ログイン クレデンシャル（Login Credentials）] オプションが選択されています。
[Binding DN]	ユーザーの識別名（DN）。このフィールドは、バインディング方式として**[設定済みクレデンシャル（Configured Credentials）]** オプションを選択した場合にのみ編集可能になります。
Password	ユーザーのパスワード。このフィールドは、バインディング方式として [Configured Credentials] オプションを選択した場合にのみ編集可能になります。

ステップ 7 [検索パラメータ（Search Parameters）] エリアで、次のプロパティを更新します。

名前	説明
[Filter Attribute]	このフィールドは、LDAP サーバ上のスキーマの設定済み属性に一致している必要があります。 デフォルトでは、このフィールドに **sAMAccountName** と表示されます。
[グループ属性（Group Attribute）]	このフィールドは、LDAP サーバ上のスキーマの設定済み属性に一致している必要があります。 デフォルトでは、このフィールドに **memberOf** と表示されます。
[属性（Attribute）]	ユーザのロールとロケール情報を保持する LDAP 属性。このプロパティは、常に、名前と値のペアで指定されます。システムは、ユーザ レコードで、この属性名と一致する値を検索します。 LDAP 属性では、Cisco IMC ユーザー ロールおよびロケールにマップされる既存の LDAP 属性を使用することも、スキーマを変更して新しい LDAP 属性を作成することもできます。（たとえば CiscoAvPair など）。
Nested Group Search Depth (1-128)	LDAP グループ マップで別の定義済みグループ内にネストされた LDAP グループを検索するパラメータ。このパラメータでは、ネストされたグループ検索の深さを定義します。

ステップ 8 （任意）[グループ認証（Group Authorization）] エリアで、次のプロパティを更新します。

名前	説明
[LDAP Group Authorization] チェックボックス	このチェックボックスをオンにすると、ローカルユーザ データベースにない LDAP ユーザに関しても、グループ レベルでユーザ認証が行われます。 このチェックボックスをオンにすると、Cisco IMC は **[Configure Group]** ボタンをイネーブルにします。
[Group Name] カラム	サーバへのアクセスが許可された LDAP サーバ データベース内のグループの名前。
[Group Domain] カラム	グループを所属させる LDAP サーバ ドメイン。

名前	説明
[Role] カラム	すべてのユーザーに割り当てられているこの LDAP サーバー グループのロール。次のいずれかになります。 • [read-only]：このロールのユーザは情報を表示できますが、変更することはできません。 • [user]：このロールのユーザは、次のタスクを実行できます。 • すべての情報を表示する • 電源のオン、電源再投入、電源のオフなどの電力制御オプションを管理する • KVM コンソールと仮想メディアを起動する • すべてのログをクリアする • ping • [admin]：このロールのユーザーは、GUI、CLI、IPMI で可能なすべてのアクションを実行できます。
[Configure] ボタン	上にリストされている**グループ名**、**グループドメイン**、および**ロール**オプションが同じ Active directory グループの [**LDAP グループの設定 (Configure LDAP Group**)] ウィンドウを開きます。 設定が完了したら、**[変更の保存 (Save Changes)]** をクリックします。
[Delete] ボタン	既存の LDAP グループを削除します。

ステップ 9 [Save Changes] をクリックします。

LDAP 証明書の概要

Cisco C シリーズ サーバでは、LDAP バインディング ステップ時に、LDAP クライアントがインストール済み CA 証明書またはチェーン CA 証明書に対してディレクトリ サーバ証明書を検証できるようになっています。リモートユーザー認証のために信頼されたポイントまたはチェーン証明書を Cisco IMC に入力できないことにより、誰でもユーザー認証用のディレクトリ サーバーを複製してセキュリティ違反が発生する恐れがある場合は、この機能を導入します。

LDAP クライアントには、暗号化 TLS/SSL 通信中にディレクトリ サーバ証明書を検証できる新しい設定オプションが必要です。

LDAP CA 証明書ステータスの表示

手順

ステップ 1 **[ナビゲーション (Navigation)]** ペインの **[管理者 (Admin)]** メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーザ管理（User Management）] をクリックします。

ステップ 3 [ユーザー管理（User Management）] ペインの [LDAP] タブをクリックします。

ステップ 4 [Certificate Status] 領域で、次のフィールドを確認します。

名前	説明
[Download Status]	このフィールドには、LDAP CA 証明書のダウンロード ステータスが表示されます。
[Eport Status]	このフィールドには、LDAP CA 証明書のエクスポート ステータスが表示されます。

LDAP CA 証明書のエクスポート

始める前に

このアクションを実行するには、admin権限を持つユーザとしてログインする必要があります。

署名付き LDAP CA 証明書をエクスポートするには、あらかじめ証明書がダウンロードされている必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーザ管理（User Management）] をクリックします。

ステップ 3 [ユーザー管理（User Management）] ペインの [LDAP] タブをクリックします。

ステップ 4 **[LDAP CA 証明書のエクスポート（Export LDAP CA Certificate）]** リンクをクリックします。

[LDAP CA 証明書のエクスポート（Export LDAP CA Certificate）] ダイアログボックスが表示されます。

名前	説明
[Export to Remote Location]	

名前	説明
	このオプションを選択すると、リモートロケーションの証明書を選択してエクスポートできます。次の詳細を入力します。 • • **[TFTP サーバー（TFTP Server）]** • **FTP サーバー（FTP Server）** • **SFTP サーバー（SFTP Server）** • **SCP サーバー（SCP Server）** • **HTTP サーバー（HTTP Server）** （注） このアクションを実行中にリモートサーバのタイプとして SCP または SFTP を選択した場合、ポップアップ ウィンドウが表示され、そこに *[*サーバ（*RSA*）鍵フィンガープリントは *<server_finger_print _ID>* です。続行しますか*?*（*Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*）*]* というメッセージが表示されます。サーバフィンガープリントの信頼度に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。 • [サーバー IP/ホスト名（Server IP/Hostname）] フィールド：LDAP CA 証明書ファイルをエクスポートするサーバーの IP アドレスまたはホスト名。[Download Certificate from] ドロップダウン リストの設定によって、このフィールドの名前は異なる場合があります。 • [パスおよびファイル名（Path and Filename）] フィールド：リモートサーバから証明書をダウンロードする際に Cisco IMC が使用するパスとファイル名。

名前	説明
	• **[ユーザ名（Username）]** フィールド—リモート サーバにログインするためにシステムが使用するユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。 • [パスワード（Password）] フィールド：リモート サーバーのユーザー名に対応するパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。
[Export to Local Desktop]	このオプションを選択することで、コンピュータのローカル ドライブに保管されている証明書を選択してエクスポートできます。

ステップ 5 **[証明書のエクスポート（Export Certificate）]** をクリックします。

LDAP CA 証明書のダウンロード

（注） Cisco IMC では CA 証明書またはチェーン CA 証明書のみを使用する必要があります。デフォルトでは、CA 証明書の形式は .cer です。チェーン CA 証明書を使用する場合は、Cisco IMC にダウンロードする前に .cer 形式に変換する必要があります。

手順

1. [Navigation] ペインの [Admin] タブをクリックします。
2. [Admin] メニューで、[User Management] をクリックします。
3. [ユーザー管理（User Management）] ペインの [LDAP] タブをクリックします。
4. **[LDAP CA 証明書のダウンロード（Download LDAP CA Certificate）]** リンクをクリックします。

   [Download LDAP CA Certificate] ダイアログボックスが表示されます。
5. **[LDAP CA 証明書のダウンロード (Download LDAP CA Certificate)]** ダイアログ ボックスで必要な情報を入力します。

名前	説明
[リモートの場所からのダウンロード/アップロード (DownloadUpload from remote location)] オプション ボタン	

名前	説明
	このオプションを選択することで、証明書をリモートの場所から選択してダウンロード/アップロードできます。次の詳細を入力します。 • • **[TFTP サーバー（TFTP Server）]** • **FTP サーバー（FTP Server）** • **SFTP サーバー（SFTP Server）** • **SCP サーバー（SCP Server）** • **HTTP サーバー（HTTP Server）** （注） このアクションを実行中にリモート サーバのタイプとして SCP または SFTP を選択した場合、ポップアップ ウィンドウが表示され、そこに *[*サーバ（*RSA*）鍵フィンガープリントは *<server_finger_print _ID>* です。続行しますか*?*（*Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*）*]* というメッセージが表示されます。サーバ フィンガープリントの信頼度に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。 • [サーバー IP/ホスト名（Server IP/Hostname）] フィールド：LDAP CA 証明書ファイルを保管するサーバーの IP アドレスまたはホスト名。[証明書のダウンロード元/アップロード元 (Download/Upload Certificate from)] ドロップダウン リストの設定によっては、このフィールドの名前は異なる場合があります。 • [パスおよびファイル名 (Path and Filename)] フィールド — Cisco IMC がファイルをリモート サーバにダウンロード/アップロードするときに使用するパスおよびファイル名です。 • [Username] フィールド：システムがリモート サーバーにログインする際に使用するユーザー名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。 • [パスワード（Password）]フィールド：リモート サーバーのユーザー名に対応するパスワード。このフィールドは、

名前	説明
	プロトコルが TFTP または HTTP の場合は適用されません。
[ブラウザクライアントを使用してダウンロード/アップロード (Download/Upload through browser client)] オプション ボタン	このオプションを選択することで、Cisco IMC GUI を実行しているコンピュータのローカル ドライブに保管されている証明書に移動できます。 このオプションを選択すると、Cisco IMC GUI に、インポートするファイルに移動するために使用できる [参照（Browse）] ボタンが表示されます。
[証明書の内容を貼り付け（Paste Certificate content）] オプション ボタン	このオプションを選択すると、署名付き証明書の内容全体をコピーして、[証明書の内容の貼り付け（Paste certificate content）]テキストフィールドに貼り付けることができます。 （注） アップロードする前に証明書が署名済みであることを確認します。
[証明書のダウンロード/アップロード (Download/Upload Certificate)] ボタン	証明書をサーバにダウンロード/アップロードできるようにします。

LDAP バインディングのテスト

始める前に

このアクションを実行するには、admin権限を持つユーザとしてログインする必要があります。

（注） **[暗号化の有効化（Enable Encryption）]** チェックボックスと **[CA 証明書のバインドの有効化（Enable Binding CA Certificate）]** チェックボックスをオンにした場合は、[LDAP サーバ（LDAP Server）] フィールドに LDAP サーバの完全修飾ドメイン名（FQDN）を入力します。LDAP サーバーの FQDN を解決するには、Cisco IMC ネットワークの優先 DNS を設定して適切な DNS IP アドレスを指定します。

手順

ステップ 1 **[ナビゲーション (Navigation)]** ペインの **[管理者 (Admin)]** メニューをクリックします。
ステップ 2 [管理（Admin）] メニューで [ユーザ管理（User Management）] をクリックします。
ステップ 3 [ユーザー管理（User Management）] ペインの [LDAP] タブをクリックします。
ステップ 4 **[LDAP バインドのテスト（Test LDAP Binding）]** リンクをクリックします。

[LDAP CA 証明書バインドのテスト（Test LDAP CA Certificate Binding）] ダイアログボックスが表示されます。

名前	説明
[ユーザー名（Username）] フィールド	ユーザ名を入力します。
[パスワード（Password）] フィールド	対応するパスワードを入力します。

ステップ 5 **[テスト（Test）]** をクリックします。

TACACS+ 認証

4.1（3b） リリース以降、Cisco IMC は Terminal Access Controller Access-Control System Plus（TACACS+）ユーザー認証をサポートします。Cisco IMC は、最大 6 つの TACACS+ リモート サーバーをサポートします。ユーザーが正常に認証されると、ユーザー名に **[（TACACS+）]** が追加されます。これは Cisco IMC インターフェースにも表示されます。

TACACS+ 認証のイネーブル化 （184 ページ） を参照して TACACS+ 認証を有効化します。
Cisco IMC はまた、TACACS+ リモート サーバーにアクセスできない場合のユーザー認証の優先順位もサポートします。ユーザー認証の優先順位の構成 （166 ページ） を使用してユーザー認証の優先順位の構成が行えます。

TACACS+サーバ設定

ユーザーの特権レベルは、そのユーザーに設定された **[cisco-av-pair]** 値に基づいて計算されます。TACACS+ サーバに一 **[cisco-av-pair]** を作成する必要があります。ユーザーは既存の TACACS+ 属性は使用できません。

cisco-av-pair 属性のサポートされる 3 つのシンタックスは、次のとおりです。

- **`admin`** 特権の場合：**[cisco-av-pair=shell:roles=”admin”]**
- **`user`** 権限の場合：**[cisco-av-pair=shell:roles=”user”]**
- **`read-only`** 権限の場合：**[cisco-av-pair=shell:roles=”read-only”]**

必要に応じて、**[comma]** を区切り文字として使用して、さらにロールを追加できます。

（注） **[cisco-av-pair]** が TACACS+ サーバーで構成されていない場合、そのサーバーのユーザーには **[read-only]** 権限があります。

TACACS+ 認証のイネーブル化

始める前に

Terminal Access Controller Access-Control System（TACACS+）ベースのユーザー認証を構成する前に、ユーザーの特権レベルが **[cisco-av-pair]** 値に基づいて TACACS+ サーバーで構成されていることを確認してください。

手順

ステップ 1 **[ナビゲーション（Navigation）]** ペインで **[管理（Admin）]** メニューをクリックします。

ステップ 2 **[管理（Admin）]** メニューで **[ユーザー管理（User Management）]** をクリックします。

ステップ 3 **[ユーザー管理（User Management）]** ペインで **[TACACS+]** タブをクリックします。

ステップ 4 **[TACACS+ のプロパティ（TACACS+ Properties）]** エリアで、次の手順を実行します。

名前	説明
[Enabled] チェックボックス	TACACS+ベースのユーザー認証を有効にするには、このボックスをオンにします。
[接続がない場合のみフォールバック（Fallback only on no connectivity）] チェック ボックス	オンにすると、Cisco IMC が構成済みの TACACS+ サーバーに接続できない場合にのみ、認証は次の優先順位データベースにフォールバックします。 ユーザ認証の優先順位の構成を確認します。ユーザー認証の優先順位の構成（166ページ）を参照してください。
タイムアウト（サーバーごと）：（5 ～ 30）秒（Timeout (for each server): (5 - 30) seconds）] フィールド	Cisco IMC が各 TACACS+ サーバーからの応答を待機する時間（秒単位）

TACACS+ リモート サーバー設定の構成

最大 6 つの TACACS+ リモート サーバーを設定できます。

手順

ステップ 1 **[ナビゲーション（Navigation）]** ペインで **[管理（Admin）]** メニューをクリックします。

ステップ 2 **[管理（Admin）]** メニューで **[ユーザー管理（User Management）]** をクリックします。

ステップ 3 **[ユーザー管理（User Management）]** ペインで **[TACACS+]** タブをクリックします。

ステップ 4 **[サーバー リスト（Server List）]** エリアで、構成するサーバー識別子のラジオ ボタンをクリックし、**[編集（Edit）]** ボタンをクリックします。

ステップ 5 次のフィールドを更新します。

名前	説明
ID	これはサーバーの一意の識別子であり、ユーザーは編集できません。
IPアドレスまたはホスト名	TACACS+ サーバーが稼働している IP アドレス。
[ポート（Port）]	TACACS+ サーバーが稼働しているポート。
[サーバー キー（Server key）]	TACACS+サーバーで構成されているのと同じキー。 **[サーバー キーの確認（Confirm Server Key）]** に対して同じキーを繰り返します。

ユーザ セッションの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

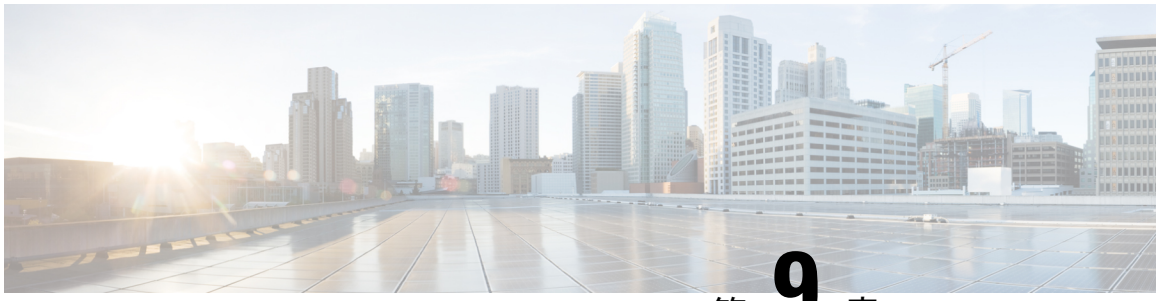
ステップ 2 [管理（Admin）] メニューで [ユーザ管理（User Management）] をクリックします。

ステップ 3 [ユーザ管理（User Management）] ペインで [セッション管理（Session Management）] をクリックします。

ステップ 4 [Sessions] ペインで、現在のユーザー セッションに関する次の情報を表示します。

名前	説明
[Session ID] カラム	セッションの固有識別情報。
BMC セッション ID	BMC セッションの識別子。
[User name (ユーザー名)] カラム	ユーザーのユーザー名。
[IP Address] カラム	ユーザがサーバにアクセスした IP アドレス。シリアル接続の場合は、[N/A] と表示されます。

名前	説明
[Session Type] カラム	ユーザーがサーバーにアクセスするために選択したセッション タイプ。次のいずれかになります。 • [Web GUI（webgui）]：ユーザが Web UI を使用してサーバに接続されていることを示します。 • [CLI]：ユーザが CLI を使用してサーバに接続されていることを示します。 • [serial]：ユーザーがシリアル ポートを使用してサーバーに接続されていることを示します。 • **[XML API]** — ユーザーが XML API を使用してサーバーに接続していることを示します。 • **[Redfish]** — ユーザーが Redfish API を使用してサーバーに接続していることを示します。
[Action] カラム	このカラムには、SoL が有効である場合は [該当なし（N/A）] が表示され、SoL が無効である場合は [終了（Terminate）] が表示されます。Web UI で [終了（Terminate）] をクリックすると、セッションを終了できます。



第 9 章

シャーシ関連の設定

この章は、次の内容で構成されています。

サーバの電源管理

始める前に

このタスクを実行するには、user または admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [シャーシ（Chassis）] メニューで [サマリー（Summary）] をクリックします。

ステップ 3 作業ウィンドウ上部のツールバーで、[Host Power] リンクをクリックします。

ステップ 4 ドロップダウン リストから、次のいずれかのオプションを選択します。

Actions	説明
電源オン	選択されたサーバーの電源を投入します。

Actions	説明
Power Off	タスクがサーバーで実行されていても、選択されたサーバーの電源をオフにします。 重要　ファームウェアまたは BIOS の更新が進行中の場合は、そのタスクが完了するまでサーバーの電源をオフにしたり、サーバーをリセットしたりしないでください。
Power Cycle	選択したサーバの電源をオフにしてからオンにします。
Hard Reset	選択したサーバを再起動します。
Shut Down	オペレーティングシステムがこの機能をサポートしている場合、選択したサーバをシャットダウンします。

Web UI からのホスト名/IP アドレスの ping

始める前に

このタスクを実行するには、user または admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1　作業ウィンドウ上部のツールバーで、[**Ping**] アイコンをクリックします。

ステップ 2　[**Ping Details**] ダイアログボックスで、次のフィールドを更新します。

Actions	説明
*[ホスト名/IPアドレス（Hostname/IP Address）] フィールド	到達するホスト名または IP アドレス。
*[再試行回数（Number of Retries）] フィールド	IP アドレスに ping を送ることが許可された再試行の最大数。デフォルト値は 3 です。有効な範囲は 1 ～ 10 です。
*[タイムアウト（Timeout）] フィールド	ping の最大応答時間。デフォルト値は 10 秒です。有効な範囲は 1 ～ 20 秒です。

Actions	説明
[pingステータス（Ping Status）] フィールド	ping の結果を表示します。
[Details] ボタン	ping アクティビティの詳細が表示されます。
[Ping] ボタン	IP アドレスを ping します。
[Cancel] ボタン	ping せずにダイアログボックスを閉じます。

ステップ 3 **[Ping]**をクリックします。

ロケータ LED の切り替え

始める前に

このタスクを実行するには、user または admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。
ステップ 2 [シャーシ（Chassis）] メニューで [サマリー（Summary）] をクリックします。
ステップ 3 作業ウィンドウ上部のツールバーで、[Locator LED] リンクをクリックします。
ステップ 4 [Turn On Locator LED] または [Turn Off Locator LED] を選択します。

時間帯の選択

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

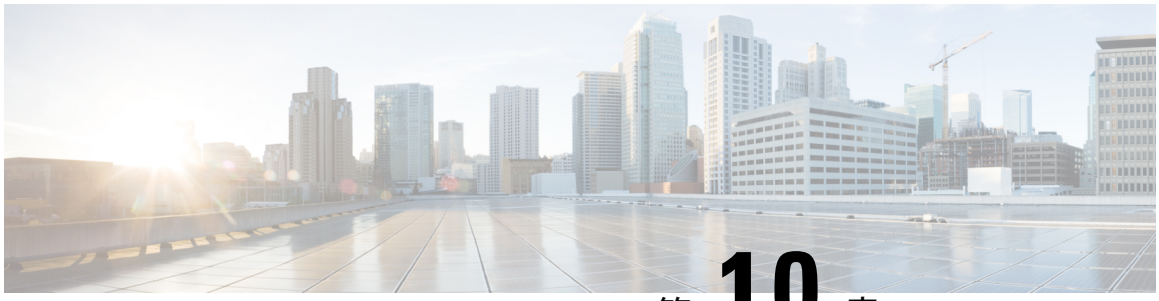
手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。
ステップ 2 [シャーシ（Chassis）] メニューで [サマリー（Summary）] をクリックします。
ステップ 3 [Cisco Integrated Management Controller (Cisco IMC) Information] 領域で、[Select Timezone] をクリックします。

[タイムゾーンの選択（Select Timezone）]画面が表示されます。

ステップ 4 [Select Timezone] ポップアップ画面で、マップの上にカーソルを移動してロケーションをクリックしてタイム ゾーンを選択するか、または [Timezone] ドロップダウン メニューからタイム ゾーンを選択します。

ステップ 5 [OK] をクリックします。



第 10 章

ネットワーク関連の設定

この章は、次の内容で構成されています。

サーバ NIC の設定

サーバー NIC

NIC モード

NIC モード設定により、Cisco IMC に到達できるポートが決定します。プラットフォームに応じて、次のネットワーク モード オプションを使用できます。

- **[専用（Dedicated）]**：Cisco IMC へのアクセスに管理ポートを使用します。
- **[Cisco カード（Cisco Card）]**：アダプタ カード上の任意のポートを Cisco IMC へのアクセスに使用できます。Cisco アダプタ カードは、ネットワーク通信サービス インターフェイス プロトコル サポート（NCSI）のあるスロットに取り付ける必要があります。
- **[共有 LOM（Shared LOM）]**：Cisco IMC にアクセスするために使用できる LOM（LAN On Motherboard）ポート。

- **[共有 LOM 拡張（Shared LOM Extended）]**：Cisco IMC へのアクセスに使用できる LOM ポートまたはアダプタ カードのポート。Cisco アダプタ カードは、NCSI をサポートするスロットに装着する必要があります。

（注） [共有 LOM（Shared LOM）] ポートおよび [共有 LOM 拡張（Shared LOM Extended）] ポートは、一部の C シリーズ サーバでのみ使用できます。

（注） その他の UCS C シリーズ M4、M5、C220 M6、および C240 M6 サーバーでは、NIC のモードは、デフォルトで **[共有 LOM 拡張（Shared LOM Extended）]** に設定されます。

- **共有 OCP**：OCP アダプタ カード LOM ポートは、Cisco IMC にアクセスするために使用されます。次のステップで、[アクティブ-アクティブ（Active-active）] または [アクティブ-スタンバイ（Active-standby）] のいずれかの NIC 冗長化設定を選択する必要があります。
- **共有 OCP 拡張**：この NIC モードでは、DHCP 応答が OCP アダプタ カード LOM ポートと Cisco 仮想インターフェイス カード (VIC) ポートの両方に返されます。サーバがスタンドアロン モードであるために、Cisco VIC 接続でその IP アドレスが Cisco UCS Manager システムから取得されないと判別された場合は、その Cisco VIC からのその後の DHCP 要求は無効になります。

（注） **[共有 OCP（Shared OCP）]** および **[共有 OCP 拡張（Shared OCP Extended）]** ポートは、Cisco UCS C225 M6、C245 M6、C220 M7、および C240 M7 サーバーでのみ使用できます。

デフォルトのNICモード設定：

- UCS C シリーズ C125 M5 サーバーおよび S3260 サーバーの場合、**[NIC モード（NIC Mode）]** はデフォルトで **[Cisco カード（Cisco Card）]** に設定されています。

Cisco UCS C225 M6、C245 M6、C220 M7、および C240 M7 サーバーの場合：

- サーバーに Cisco VIC カードと OCP カードがある場合、デフォルトの NIC モードは**共有 OCP 拡張**になり、**NIC 冗長性**は **active-active** に設定されます。
- サーバーの NCSI 対応スロットに VIC カードが装着されているものの、OCP カードがない場合、デフォルトの NIC モードは **Cisco Card** になります。
- サーバーに VIC カードも OCP カードもない場合、デフォルトの NIC モードは**専用モード**に設定され、**NIC 冗長性**は**なし**に設定されます。

NIC 冗長化

選択した NIC モードとご使用のプラットフォームに応じて、次の NIC 冗長化オプションを使用できます。

- **[アクティブ-アクティブ（active-active）]**：サポートされている場合、設定されている NIC モードに関連付けられたすべてのポートが同時に動作します。これにより、スループットが増加し、Cisco IMC への複数のパスが提供されます。
- **[アクティブ-スタンバイ（active-standby）]**：設定されている NIC モードに関連付けられたポートで障害が発生した場合、トラフィックは、その NIC モードに関連付けられている他のポートの 1 つにフェールオーバーします。

（注） このオプションを選択する場合は、設定されている NIC モードに関連付けられたすべてのポートが同じサブネットに接続され、どのポートが使用されてもトラフィックの安全が保証されるようにする必要があります。

- **[なし（None）]**：専用（*Dedicated*） モードでは、NIC 冗長性は なし（*None*） に設定されます。

使用できる冗長化モードは、選択されているネットワーク モードとプラットフォームによって異なります。使用できるモードについては、次を参照してください、『*Hardware Installation Guide*』（HIG）を参照してください。C シリーズの HIG は、次の URL にあります。
http://www.cisco.com/en/US/products/ps10493/prod_installation_guides_list.html

VIC スロット

Cisco カード モードで管理機能に使用できる VIC スロット。

C240 M6、C245 M6、および C240 M7 の場合、VIC スロット オプションは次のとおりです。

- **[ライザー 1（Riser 1）]**：スロット 1 およびスロット 2
- **[ライザー 2（Riser 2）]**：スロット 4 およびスロット 5
- **mLOM**

（注） C240 M6 および C245 M6 C240 M6、C245 M6、および C240 M7 の場合、工場出荷時のデフォルト設定にリセットした後、スロットの優先順位は次のとおりです。

1. mLOM
2. ライザー 1：スロット 2、およびライザー 2 ～ スロット 5
3. ライザー 1：スロット 1、およびライザー 2 ～ スロット 4

C220 M6 および C225 M6 C220 M6、C225 M6、および C220 M7 の場合、VIC スロット オプションは次のとおりです。

- [ライザー 1（Riser 1）]：スロット 1 が選択されます。
- **[ライザー 3 (Riser 3)]**：スロット 3 が選択されます。
- **mLOM**

（注） C220 M6、C225 M6、および C220 M7 の場合、工場出荷時のデフォルト設定にリセットした後、スロットの優先順位は次のとおりです。

1. mLOM
2. ライザー 1 ：スロット 1
3. ライザー 3 ：スロット 3

C125 M5 の場合、VIC スロット オプションは **[ライザー 2（Riser 2）]** です。

C220 M4、C220 M5 および C240 M5 サーバーでは、VIC スロット オプションは次のとおりです。

- [ライザー 1（Riser 1）]：スロット 1 が選択されます。
- **[ライザー 2（Riser 2）]**：スロット 2 が選択されます。
- **[FLEX LOM]**：スロット 3（MLOM）が選択されます。

C240 M4 サーバーでは、VIC スロット オプションは次のとおりです。

- [Riser 1]：スロット 2 がプライマリ スロットですが、スロット 1 も使用できます。
- **[ライザー 2（Riser 2）]**：スロット 5 がプライマリ スロットですが、スロット 4 も使用できます。
- [FLEX LOM]：スロット 7（MLOM）が選択されます。

C480 M5 ML サーバーの場合、Cisco カード モード スロットはスロット 11 およびスロット 12 です。

次のオプションを使用できるのは一部の UCS C シリーズ サーバーだけです。

- **4**
- **5**
- **9**
- **10**

（注） このオプションを使用できるのは一部の UCS C シリーズ サーバーだけです。

サーバ NIC の設定

NIC モードと NIC 冗長化を設定する場合は、サーバーの NIC を設定します。

始める前に

NIC を設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。
ステップ 2 [管理（Admin）] メニューで [ネットワーク（Networking）] をクリックします。
ステップ 3 [NIC Properties] 領域で、次のプロパティを更新します。

名前	説明
[NIC Mode] ドロップダウン リスト	

名前	説明
	Cisco IMC へのアクセスに使用できるポート。次のいずれかになります。 • **[専用（Dedicated）]**：Cisco IMC へのアクセスに管理ポートを使用します。 • **[Cisco カード（Cisco Card）]**：アダプタ カード上の任意のポートを Cisco IMC へのアクセスに使用できます。Cisco アダプタ カードは、Network Communications Services Interface プロトコル（NCSI）をサポートするスロットに装着する必要があります。 • **[共有 LOM（Shared LOM）]**：Cisco IMC にアクセスするために使用できる LOM（LAN On Motherboard）ポート。 • **[共有 LOM 拡張（Shared LOM Extended）]**：Cisco IMC へのアクセスに使用できる LOM ポートまたはアダプタ カードのポート。Cisco アダプタ カードは、NCSI をサポートするスロットに装着する必要があります。 （注） [共有 LOM（Shared LOM）] ポートおよび [共有 LOM 拡張（Shared LOM Extended）] ポートは、一部の C シリーズ サーバでのみ使用できます。 （注） その他の UCS C シリーズ M4、M5、C220 M6、および C240 M6 サーバーでは、NIC のモードは、デフォルトで **[共有 LOM 拡張（Shared LOM Extended）]** に設定されます。 • **共有 OCP**：OCP アダプタ カード LOM ポートは、Cisco IMC にアクセスするために使用されます。次のステップで、[アクティブ-アクティブ（Active-active）] または [アクティブ-スタンバイ（Active-standby）] のいずれかの NIC 冗長化設定を選択する必要があります。 • **共有 OCP 拡張**：この NIC モードでは、DHCP 応答が OCP アダプタ カード LOM ポートと Cisco 仮想インターフェイス カード (VIC) ポートの両方に返されます。サーバがスタンドアロン モードであるために、Cisco VIC 接続でその IP アドレスが Cisco UCS Manager システムから取得されないと判別された場合は、その Cisco VIC からのその後の DHCP 要求は無効になります。 （注） **[共有 OCP（Shared OCP）]** および **[共有 OCP 拡張（Shared OCP Extended）]** ポートは、Cisco UCS C220 M7、C240 M7、C225 M6 と

名前	説明

	C245 M6 サーバーでのみ使用できます。
	
	デフォルトのNICモード設定：
	• UCS C シリーズ C125 M5 サーバーおよび S3260 サーバーの場合、**[NIC モード（NIC Mode）]** はデフォルトで **[Cisco カード（Cisco Card）]** に設定されています。
	• UCS C シリーズ C220 M7、C240 M7、C225 M6 および C245 M6 サーバーの場合：
	  • サーバーに Cisco VIC カードと OCP カードがある場合、デフォルトの NIC モードは**共有 OCP 拡張**になり、**NIC 冗長性**は **active-active** に設定されます。
	  • サーバーの NCSI 対応スロットに VIC カードが装着されているものの、OCP カードがない場合、デフォルトの NIC モードは **Cisco Card** になります。
	  • サーバーに VIC カードも OCP カードもない場合、デフォルトの NIC モードは**専用モード**に設定され、**NIC 冗長性**は**なし**に設定されます。

名前	説明
[VIC Slot] ドロップダウン リスト	

名前	説明
	Cisco カード モードで管理機能に使用できる VIC スロット。 C240 M7、C240 M6 と C245 M6、VIC スロット オプションは次のとおりです。 • **[ライザー 1（Riser 1）]**：スロット 1 およびスロット 2 • **[ライザー 2（Riser 2）]**：スロット 4 およびスロット 5 • **mLOM** （注） C240 M7、 C240 M6、および C245 M6 の場合、工場出荷時のデフォルト設定にリセットした後、スロットの優先順位は次のとおりです。 **1.** mLOM **2.** ライザー 1：スロット 2、およびライザー 2 ～ スロット 5 **3.** ライザー 1：スロット 1、およびライザー 2 ～ スロット 4 C220 M7、C220 M6 と C225 M6の場合、VIC スロット オプションは次のとおりです： • [ライザー 1（Riser 1）]：スロット 1 が選択されます。 • **[ライザー 3 (Riser 3)]**：スロット 3 が選択されます。 • **mLOM** （注） C220 M7、C220 M6、および C225 M6 の場合、工場出荷時のデフォルト設定にリセットした後、スロットの優先順位は次のとおりです： **1.** mLOM **2.** ライザー 1 ：スロット 1 **3.** ライザー 3 ：スロット 3 C125 M5 の場合、VIC スロット オプションは **[ライザー 2（Riser 2）]** です。 C220 M4、C220 M5 および C240 M5 サーバーでは、VIC スロット オプションは次のとおりです。 • [ライザー 1（Riser 1）]：スロット 1 が選択されます。 • **[ライザー 2（Riser 2）]**：スロット 2 が選択されます。

名前	説明
	• **[FLEX LOM]**：スロット 3（MLOM）が選択されます。 C240 SD M5 サーバでは、VIC スロット オプションは次のとおりです。 • PCIe ライザー 1 と 2B を組み合わせたサーバの場合： • [Riser1] を選択した場合は、スロット 2 に VIC を取り付ける必要があります。 • [Riser2] を選択した場合は、スロット 5 に VIC を取り付ける必要があります。 • PCIe ライザー 1C と 2E を組み合わせたサーバの場合： • [ライザー1（Riser1）] を選択した場合は、スロット 1 に VIC を取り付ける必要があります。 • [ライザー2（Riser2）] を選択した場合は、スロット 2 に VIC を取り付ける必要があります。 • [Flex-LOM] を選択した場合は、mLOM スロットに mLOM タイプの VIC を取り付ける必要があります。 C480 M5 ML サーバーの場合、Cisco カード モード スロットはスロット 11 およびスロット 12 です。 次のオプションを使用できるのは一部の UCS C シリーズ サーバーだけです。 • **4** • **5** • **9** • **10** C240 M4 サーバーでは、VIC スロット オプションは次のとおりです。 • [Riser 1]：スロット 2 がプライマリ スロットですが、スロット 1 も使用できます。 • **[ライザー 2（Riser 2）]**：スロット 5 がプライマリ スロットですが、スロット 4 も使用できます。 • [FLEX LOM]：スロット 7（MLOM）が選択されます。 （注） このオプションを使用できるのは一部の UCS C シリーズ サーバーだけです。

名前	説明
[VIC Slot] ドロップダウン リスト	Cisco カード モードで管理機能に使用できる VIC スロット。次のいずれかになります。 C220 M4 サーバーでは、VIC スロット オプションは次のとおりです。 • [ライザー 1（Riser 1）]：スロット 1 が選択されます。 • **Riser 2**：スロット 2 が選択されます。 • [FLEX LOM]：スロット 3（MLOM）が選択されます。 C240 M4 サーバーでは、VIC スロット オプションは次のとおりです。 • [ライザー 1（Riser 1）]：スロット 2 がプライマリ スロットですが、スロット 1 も使用できます。 • [ライザー 2（Riser 2）]：スロット 5 がプライマリ スロットですが、スロット 4 も使用できます。 • [FLEX LOM]：スロット 7（MLOM）が選択されます。 次のオプションを使用できるのは一部の UCS C シリーズ サーバーだけです。 • **4** • **5** • **9** • **10** （注） このオプションを使用できるのは一部の UCS C シリーズ サーバーだけです。
[SIOC スロット（SIOC Slot）] ドロップダウンリスト	Cisco IMC ネットワーク モードを設定します。システム IO コントローラ（SIOC1）に存在するカードに基づいて、ネットワーク モードを 1 または 2 に変更できます。 （注） このオプションは、一部の UCS S シリーズ サーバーでのみ使用できます。

名前	説明
[NIC Redundancy] ドロップダウン リスト	使用可能な NIC 冗長オプションは、選択した NIC モードおよび使用しているサーバのモデルによって異なります。特定のオプションが表示されない場合、そのオプションは選択されているモードまたはサーバ モデルでは選択できません。 次のいずれかになります。 • [アクティブ-アクティブ（active-active）]：サポートされている場合、設定されている NIC モードに関連付けられたすべてのポートが同時に動作します。この機能により、スループットが増加し、Cisco IMC への複数のパスが提供されます。 • [アクティブ-スタンバイ（active-standby）]：設定されている NIC モードに関連付けられたポートで障害が発生した場合、トラフィックは、その NIC モードに関連付けられている他のポートの 1 つにフェールオーバーします。 （注） • このオプションを選択する場合は、設定されている NIC モードに関連付けられたすべてのポートが同じ VLAN に接続され、どのポートが使用されてもトラフィックの安全が保証されるようにする必要があります。 • [アクティブ-アクティブ（active-active）] を使用する場合は、メンバー インターフェイスの上流に位置するスイッチで port-channel を設定しないでください。port-channel は、[active-standby] を使用する場合に設定できます。 • **[なし（None）]**：専用（*Dedicated*） モードでは、NIC 冗長性は なし（*None*） に設定されます。
[MAC Address] フィールド	[NICモード（NIC Mode）] フィールドで選択されている Cisco IMC ネットワーク インターフェイスの MAC アドレス。

ステップ 4 [Save Changes] をクリックします。

Cisco VIC mLOM および OCP カードの交換に関する考慮事項

Cisco UCS C220 M7、C240 M7、C225 M6 および C245 M6 サーバーで、Cisco VIC mLOM および OCP カードを交換する際には、次の状況で Cisco IMC ネットワークとの接続が失われることがあります。

- MLOM スロットの OCP カードを Cisco VIC カードと交換し、NIC モードを**共有 OCP** または**共有 OCP 拡張** に設定している場合。
- MLOM スロットの Cisco VIC カードを OCP カードと交換し、NIC モードを **Cisco カード MLOM** に設定している場合。

Cisco UCS C220 M7、C240 M7、C225 M6 または C245 M6 サーバーの Cisco VIC mLOM または OCP カードを交換する際は、次の推奨事項に従ってください。

- カードを交換する前に、ネットワークと接続している NIC のモードを、**Cisco カード MLOM**、**共有 OCP**、または **共有 OCP 拡張** 以外のいずれかに設定しておきます。カードの交換後に、適切な NIC モードを設定します。

  NIC モードの設定方法については、ご使用の Cisco IMC リリースの *Server NIC Configuration* の項を参照してください。これは Configuration Guides に記載されています。

- または、カードを交換した後、Cisco IMC Configuration Utility/（F8 キー）を使用して適切な NIC モードを設定します。

  ご使用のサーバーの *Connecting to the Server Locally For Setup* の項を参照してください。これは「」セクションを参照してください。これは Install and Upgrade Guides に記載されています。

- または、カードを交換した後、Cisco IMC Configuration Utility/（F8 キー）を使用して工場出荷時のデフォルト設定に戻してから、次の手順を実行します。

  1. サーバーが再起動を開始したら、F8 キーを押してシステムを Cisco IMC Configuration で起動し、デフォルトのパスワードを変更します。
  2. 適切な NIC モードに設定します。

表 *14* : 工場出荷時設定

mLOM スロットの VIC	mLOM スロットの Intel OCP 3.0 NIC	ライザー スロットの VIC	専用管理ポート。	CIMC アクセスのための NIC モード
はい	いいえ	いいえ	はい	mLOM スロットのカードを使用する **Cisco Card** モード
いいえ	はい	いいえ	はい	**Shared OCP Extended**

mLOM スロットの VIC	mLOM スロットの Intel OCP 3.0 NIC	ライザー スロットの VIC	専用管理ポート。	CIMC アクセスのための NIC モード
いいえ	はい	はい	はい	**Shared OCP Extended**
いいえ	いいえ	はい	はい	優先順位に基づく VIC スロットでの **Cisco カード**： **C220 M7 および C225 M6 の場合**： **1.** ライザー 1：スロット 1 **2.** ライザー 3：スロット 3 **C240 M7 および C245 M6 の場合**： **1.** ライザー 1：スロット 2 **2.** ライザー 2：スロット 5 **3.** ライザー 1：スロット 1 **4.** ライザー 2：スロット 4
いいえ	いいえ	いいえ	はい	**専用**

共通プロパティの設定

共通プロパティの設定の概要

ホスト名

ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）拡張機能は、ホスト名を DHCP パケットに追加することで利用でき、DHCP サーバ側でこれを解釈または表示できま

す。ホスト名は DHCP パケットのオプション フィールドに追加され、（最初に DHCP サーバに送信される）DHCP DISCOVER パケットで送信されます。

サーバのデフォルトのホスト名は ucs-c2XX から CXXX-YYYYYY に変更されます（XXX はサーバのモデル番号で、YYYYYY はシリアル番号です）。この一意のストリングはクライアント ID として機能し、DHCP サーバーから Cisco IMC にリースされる IP アドレスを追跡してマッピングするのに役立ちます。サーバのステッカーまたはラベルとして製造者から提供されるデフォルト シリアル番号は、サーバを識別するのに役立ちます。

ダイナミック DNS

ダイナミック DNS（DDNS）は、Cisco IMC から DNS サーバーのリソース レコードを追加または更新するために使用されます。Web UI または CLI を使用してダイナミック DNS を有効にできます。[DDNS] オプションを有効にすると、DDNS サービスは現在のホスト名、ドメイン名、および管理 IP アドレスを記録し、Cisco IMC から DNS サーバーのリソース レコードを更新します。

（注） DDNS サーバは、次の DNS 設定のいずれかが変更された場合に、DNS サーバの以前のリソース レコード（もしあれば）を削除し、新しいリソース レコードを追加します。

- ホスト名
- LDAP 設定のドメイン名
- DDNS と DHCP が有効な場合に、ネットワークまたはサブネットの変更による新しい IP アドレスまたは DNS IP またはドメイン名を DHCP が取得する場合。
- DHCP がディセーブルの場合に、CLI または Web UI を使用してスタティック IP アドレスを設定する場合。
- **dns-use-dhcp** コマンドを入力する場合。

[**Dynamic DNS Update Domain**]：ドメインを指定できます。ドメインは、メイン ドメインまたはサブ ドメインのどちらでも可です。このドメイン名は、DDNS 更新のため Cisco IMC のホスト名に付加されます。

共通プロパティの設定

サーバーを説明するには、共通プロパティを使用します。

始める前に

共通プロパティを設定するには、admin権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ネットワーク（Networking）] をクリックします。

ステップ 3 [Common Properties] 領域で、次のプロパティを更新します。

名前	説明
[Management Hostname] フィールド	Cisco IMC のさまざまなコンポーネントを管理するシステムのユーザ定義の管理ホスト名。
[Dynamic DNS] チェックボックス	オンにすると、Cisco IMC から DNS に対するリソース レコードが更新されます。
[**Dynamic DNS Update Domain**] フィールド	ダイナミック DNS（DDNS）の更新のためにホスト名に付加されるドメイン名。空白のままだと、ホスト名のみが DDNS 更新要求に送信されます。
[ダイナミックDNSの更新間隔（Dynamic DNS Refresh Interval）]フィールド	ドメイン ネーム システム（DNS）を更新するために設定された時間。 0 ～ 8736 時間の値を設定します。0 に設定すると、無効になります。

ステップ 4 [Save Changes] をクリックします。

IPv4 の設定

始める前に

IPv4 を設定するには、admin 権限を持つユーザーとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ネットワーク（Networking）] をクリックします。

ステップ 3 [IPv4 Properties] 領域で、次のプロパティを更新します。

名前	説明
[Enable IPv4] チェックボックス	オンにすると、IPv4 がイネーブルになります。

名前	説明
[Use DHCP] チェックボックス	オンにすると、Cisco IMC は DHCP を使用します。
[管理 IP アドレス（Management IP Address）] フィールド	管理 IP アドレス。CMC と BMC を管理しやすくする外部仮想 IP アドレス。
[サブネットマスク（Subnet Mask）] フィールド	IP アドレスのサブネット マスク。
[ゲートウェイ（Gateway）] フィールド	IP アドレスのゲートウェイ。
[Obtain DNS Server Addresses from DHCP] チェックボックス	オンにすると、Cisco IMC は DNS サーバ アドレスを DHCP から取得します。
[Preferred DNS Server] フィールド	プライマリ DNS サーバの IP アドレス。
[Alternate DNS Server] フィールド	セカンダリ DNS サーバの IP アドレス。

ステップ 4 [Save Changes] をクリックします。

IPv6 の設定

始める前に

IPv6 を設定するには、admin 権限を持つユーザーとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ネットワーク（Networking）] をクリックします。

ステップ 3 [**IPv6 Properties**] 領域で、次のプロパティを更新します。

名前	説明
[IPv6の有効化（Enable IPv6）] チェックボックス	オンにした場合、IPv6 が有効になります。
[Use DHCP] チェックボックス	オンにすると、Cisco IMC は DHCP を使用します。 （注） ステートフル DHCP のみがサポートされます。

名前	説明
[管理IPアドレス（Management IP Address）] フィールド	管理 IPv6 アドレス。 （注） グローバル ユニキャスト アドレスだけがサポートされます。
[プレフィクス長（Prefix Length）]フィールド	IPv6 アドレスのプレフィクス長。値は 1 ～ 127 の範囲で入力します。デフォルト値は 64 です。
[ゲートウェイ（Gateway）] フィールド	IPv6 アドレスのゲートウェイ。 （注） グローバル ユニキャスト アドレスだけがサポートされます。
[Obtain DNS Server Addresses from DHCP] チェックボックス	オンにすると、Cisco IMC は DNS サーバー アドレスを DHCP から取得します。 （注） [**Use DHCP**] オプションがイネーブルの場合にのみこのオプションを使用できます。
[Preferred DNS Server] フィールド	プライマリ DNS サーバの IPv6 アドレス。
[Alternate DNS Server] フィールド	セカンダリ DNS サーバの IPv6 アドレス。
[リンク ローカル アドレス（Link Local Address）] フィールド	IPv6 アドレスのリンク ローカル アドレス。
[SLAAC アドレス（SLAAC Address）] フィールド	Stateless Address Auto Configuration（SLAAC）は、ネットワークのルータ アドバタイズメント（RA）によって異なります。

ステップ 4 [Save Changes] をクリックします。

VLAN への接続

始める前に

VLAN に接続するには、admin としてログインしている必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ネットワーク（Networking）] をクリックします。

ステップ 3 [VLAN Properties] 領域で、次のプロパティを更新します。

名前	説明
[Enable VLAN] チェックボックス	オンにすると、Cisco IMC は仮想 LAN に接続されます。 （注） VLAN またはポート プロファイルを構成することができますが、その両方を使用することはできません。ポート プロファイルを使用するには、このチェックボックスをオフにしておく必要があります。
[VLAN ID] フィールド	VLAN ID。
[優先順位（Priority）] フィールド	VLAN でのこのシステムのプライオリティ。

ステップ 4 [Save Changes] をクリックします。

ポート プロファイルへの接続

始める前に

ポート プロファイルに接続するには、admin としてログインしている必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ネットワーク（Networking）] をクリックします。

ステップ 3 [Port Properties] 領域で、次のプロパティを更新します。

名前	説明
[Port Profile] フィールド	**[Port Profile]** フィールドの詳細。

名前	説明
[自動ネゴシエーション（Auto Negotiation）] チェックボックス	このオプションを使用すると、スイッチのネットワーク ポートの速度やデュプレックス値を設定したり、システムが自動的にスイッチから値を取得できるようにしたりすることができます。このオプションは、[専用（Dedicated）] モードでのみ使用可能です。 • オンにすると、ネットワーク ポート速度とデュプレックスの設定はシステムによって無視され、Cisco IMC はスイッチに設定された速度を保持します。 • オフにすると、ネットワーク ポートの速度とデュプレックスの値を設定できます。

名前	説明
[管理者モード（Admin Mode）] 領域	[**Network Port Speed**] フィールド ポートのネットワーク速度。次のいずれかになります。 • 10 Mbps • 100 Mbps • 1 Gbps デフォルト値は、100 Mbps です。[専用（Dedicated）] モードで [自動ネゴシエーション（Auto Negotiation）] を無効にすると、ネットワークの速度とデュプレックスの値を設定できます。 （注） • ポートの速度を変更する前に、接続先のスイッチのポートの速度が同じであることを確認します。 [**Duplex**] ドロップダウン リスト Cisco IMC 管理ポートのデュプレックス モード。 次のいずれかになります。 • **半二重** • **全二重** デフォルトでは、デュプレックスモードは[フル（Full）] に設定されます。
[操作モード（Operation Mode）] 領域	オペレーション ネットワークのポートの速度とデュプレックスの値が表示されます。 [自動ネゴシエーション（Auto Negotiation）] チェックボックスをオンにした場合は、スイッチのネットワーク ポートの速度とデュプレックスの詳細が表示されます。オフにすると、[Admin Mode] で設定したネットワーク ポート速度とデュプレックス値が表示されます。

ステップ 4 [Save Changes] をクリックします。

個別設定の指定

この機能は、Cisco UCS S シリーズ サーバーにのみ適用されます。

始める前に

設定を構成するには、管理者としてログインしている必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ネットワーク（Networking）] をクリックします。

ステップ 3 [Individual Settings] 領域で、[CMC 1]、[CMC 2]、[BMC 1]、[BMC 2] のそれぞれの領域で次のフィールドを確認し、更新します。

名前	説明
[Hostname] フィールド	ユーザ定義のホスト名。デフォルトでは、ホスト名は CXXX-YYYYYY 形式で表示されます（XXX はサーバのモデル番号、YYYYYY はシリアル番号です）。
[MAC Address] フィールド	コンポーネントの MAC アドレス。
[IPv4アドレス（IPv4 Address）]フィールド	コンポーネントの IPv4 アドレス。
[IPv6 アドレス（IPv6 Address）] フィールド	コンポーネントの IPv6 アドレス。
[Link Local Address] フィールド	コンポーネントの IPv6 アドレスのリンク ローカル アドレス。

ステップ 4 [Save Changes] をクリックします。

ネットワーク セキュリティの設定

ネットワーク セキュリティ

Cisco IMC は、IP ブロッキングをネットワーク セキュリティとして使用します。IP ブロッキングは、サーバまたは Web サイトと、特定の IP アドレスまたはアドレス範囲との間の接続を防

ぎます。IP ブロッキングは、これらのコンピュータから Web サイト、メール サーバー、またはその他のインターネット サーバーへの不要な接続を効果的に禁止します。

禁止 IP の設定は、一般的に、サービス拒否（DoS）攻撃から保護するために使用されます。Cisco IMC は、IP ブロッキングの失敗回数を設定して、IP アドレスを禁止します。

ネットワーク セキュリティの設定 [英語]

IP ブロッキングの失敗回数を設定する場合は、ネットワーク セキュリティを設定します。

始める前に

ネットワーク セキュリティを設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [ネットワーク（Networking）] ペインで [ネットワークセキュリティ（Network Security）] をクリックします。

ステップ 3 [IP Blocking Properties] 領域で、次のプロパティを更新します。

名前	説明
[Enable IP Blocking] チェックボックス	このチェックボックスをオンにすると、IP ブロッキングがイネーブルになります。
[IP Blocking Fail Count] フィールド	指定された時間ユーザがロックアウトされる前に、ユーザが試行できるログインの失敗回数。 この回数のログイン試行失敗は、[IP Blocking Fail Window] フィールドで指定されている期間内に発生する必要があります。 3 ～ 10 の整数を入力します。
[IP Blocking Fail Window] フィールド	ユーザーをロックアウトするためにログイン試行の失敗が発生する必要のある期間（秒数）。 60 ～ 280 の整数を入力します。
[IP Blocking Penalty Time] フィールド	ユーザが指定されている期間内にログイン試行の最大回数を超えた場合に、ユーザがロックアウトされている秒数。 300 ～ 900 の整数を入力します。

ステップ 4 **[IP フィルタリング (ホワイトリスティング) (IP Filtering (Whitelisting))]** 領域で、次のプロパティを更新します。

名前	説明
[IP フィルタリングを有効にする（Enable IP Filtering）] チェックボックス	このチェックボックスをオンにすると、IP フィルタリングが有効になります。
[IP フィルタ（IP Filter）] フィールド	サーバに対するセキュアなアクセスを確保するために、フィルタを設定して、選択した一連の IP のみがサーバにアクセスできるようにします。このオプションでは、IP アドレスを保存するための 4 つのスロット（IP フィルタ 1、2、3、および 4）が提供されます。IP フィルタの設定時に、単一の IP アドレスまたは IP アドレスの範囲を割り当てることができます。IP フィルタを設定すると、他の IP アドレスを使用してサーバにアクセスすることができなくなります。

ステップ 5 [Save Changes] をクリックします。

Network Time Protocol の設定

Network Time Protocol サービス設定

デフォルトでは、Cisco IMC がリセットされると、ホストと時刻が同期されます。NTP サービスを導入すると、Cisco IMC を設定して NTP サーバーで時刻を同期することができます。デフォルトでは、NTP サーバーは Cisco IMC で動作しません。少なくとも 1 台、最大 4 台の、NTP サーバまたは時刻源サーバとして動作するサーバの IP/DNS アドレスを指定し、NTP サービスを有効にして設定する必要があります。NTP サービスをイネーブルにすると、Cisco IMC は設定された NTP サーバーと時刻を同期します。NTP サービスは Cisco IMC でのみ変更できます。

（注） NTP サービスを有効にするには、DNS アドレスではなく、サーバの IP アドレスを指定することを推奨します。

Network Time Protocol 設定の指定

NTP を設定すると、IPMI の **Set SEL time** コマンドはディセーブルになります。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

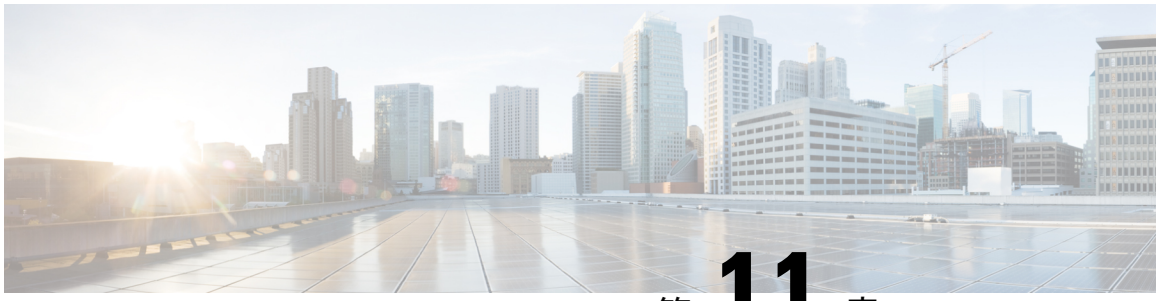
ステップ 2 [管理（Admin）] メニューで [ネットワーク（Networking）] をクリックします。

ステップ 3 [ネットワーク（Networking）] ペインで [NTP設定（NTP Setting）] をクリックします。

ステップ 4 **[NTP プロパティ（NTP Properties）]** エリアで、次のプロパティを更新します。

名前	説明
NTP が有効化された チェックボックス	NTP サービスをイネーブルにするには、このボックスをオンにします。
[サーバ 1 (Server 1)] フィールド	NTP サーバまたはタイム ソース サーバとして機能する 4 台のサーバのうちの 1 台の IP/DNS アドレス。
[サーバ 2 (Server 2)] フィールド	NTP サーバまたはタイム ソース サーバとして機能する 4 台のサーバのうちの 1 台の IP/DNS アドレス。
[サーバ 3 (Server 3)] フィールド	NTP サーバまたはタイム ソース サーバとして機能する 4 台のサーバのうちの 1 台の IP/DNS アドレス。
[サーバ 4 (Server 4)] フィールド	NTP サーバーまたはタイム ソース サーバーとして機能する 4 台のサーバーのうちの 1 台の IP/DNS アドレス。
[ステータス（Status）] メッセージ	サーバーがリモートの NTP サーバーと時刻を同期できるかどうかを示します。これは、ローカル クロックの階層レベルを示す 8 ビットの整数です。次のいずれかになります。 • 0 — 未指定または無効 • 1 — プライマリ サーバー • 2-15 — セカンダリ サーバー（NTP 経由） • 16 — 非同期 • 17-255 — 予約済み

ステップ 5 [Save Changes] をクリックします。



第 11 章

ネットワーク アダプタの管理

この章は、次の内容で構成されています。

Cisco UCS C シリーズ ネットワーク アダプタの概要

（注） この章の手順は、Cisco UCS C シリーズ ネットワーク アダプタがシャーシに設置される場合にのみ使用できます。

Cisco UCS C シリーズ ネットワーク アダプタを設置することで、I/O の統合と仮想化をサポートするためのオプションが提供されます。次のアダプタを使用できます。

- Cisco UCS VIC 15238 仮想インターフェイス カード
- Cisco UCS VIC 15428 仮想インターフェイス カード
- Cisco UCS VIC 1497 仮想インターフェイス カード
- Cisco UCS VIC 1495 仮想インターフェイス カード
- Cisco UCS VIC 1477 仮想インターフェイス カード
- Cisco UCS VIC 1467 仮想インターフェイス カード
- Cisco UCS VIC 1457 仮想インターフェイス カード
- Cisco UCS VIC 1455 仮想インターフェイス カード
- Cisco UCS VIC 1387 仮想インターフェイス カード

- Cisco UCS VIC 1385 仮想インターフェイス カード
- Cisco UCS VIC 1227T 仮想インターフェイス カード
- Cisco UCS VIC 1225 仮想インターフェイス カード
- Cisco UCS P81E Virtual Interface Card

（注） VIC カードをサーバで同じの生成は必須です。たとえば、1 つのサーバで第 3 世代と第 4 世代 VIC カードの組み合わせを持つことはできません。

対話型の *UCS* ハードウェアおよびソフトウェア相互運用性ユーティリティを使用すると、選択したサーバ モデルとソフトウェア リリース用のサポートされているコンポーネントと構成を表示できます。このユーティリティは次の URL で入手できます。
http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html

Cisco UCS VIC 15238 仮想インターフェイス カード

Cisco UCS VIC 15238 は、Cisco UCS C シリーズ ラック サーバーの M6 および M7 世代用に設計された、デュアルポート クワッド Small Form-Factor Pluggable（QSFP/QSFP28/QSFP56）mLOM カードです。このカードは、40/100/200 Gbps イーサネットまたは FCoE をサポートします。PCIe 標準準拠のインターフェイスをホストに提示可能で、NIC または HBA として動的に構成できます。

Cisco UCS VIC 15428 仮想インターフェイス カード

Cisco VIC 15428 は、Cisco UCS C シリーズ ラック サーバーの M6 および M7 世代用に設計された、クワッドポート Small Form-Factor Pluggable（SFP+/SFP28/SFP56）mLOM カードです。このカードは、10/25/50 Gbps イーサネットまたは FCoE をサポートします。PCIe 標準準拠のインターフェイスをホストに提示可能で、NIC または HBA として動的に構成できます。

Cisco UCS VIC 1497 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) 1497 は、Cisco UCS C シリーズ ラックサーバの M5 世代用に設計された、デュアルポート Small Form-Factor (QSFP28) mLOM カードです。このカードは、40/100 Gbps イーサネットおよび FCoE をサポートします。PCIe 標準準拠のインターフェイスをホストに提示可能で、NIC および HBA として動的に構成できます。

Cisco UCS VIC 1495 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) 1495 は、Cisco UCS C シリーズ ラックサーバの M5 世代用に設計された、デュアルポート Small Form-Factor (QSFP28) PCIe カードです。このカードは、40/100 Gbps イーサネットおよび FCoE をサポートします。PCIe 標準準拠のインターフェイスをホストに提示可能で、NIC および HBA として動的に構成できます。

Cisco UCS VIC 1477 仮想インターフェイス カード

Cisco UCS VIC 1477 は、Cisco UCS C シリーズ ラック サーバーの M6 世代用に設計された、デュアルポート クアッド Small Form-Factor（QSFP28）mLOM カードです。このカードは、40/100 Gbps イーサネットまたは FCoE をサポートします。PCIe 標準準拠のインターフェイスをホストに提示可能で、NIC または HBA として動的に構成できます。

Cisco UCS VIC 1467 仮想インターフェイス カード

Cisco UCS VIC 1467 は、Cisco UCS C シリーズ ラック サーバーの M6 世代用に設計された、クワッドポート Small Form-Factor Pluggable（SFP28）mLOM カードです。このカードは、10/25 Gbps イーサネットまたは FCoE をサポートします。PCIe 標準準拠のインターフェイスをホストに提示可能で、NIC または HBA として動的に構成できます。

Cisco UCS VIC 1457 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）1457 は、Cisco UCS C シリーズ ラック サーバの M5 世代用に設計された、クワッドポート Small Form-Factor Pluggable（SFP28）mLOM カードです。このカードは、10/25 Gbps イーサネットまたは FCoE をサポートします。これは Cisco の次世代 CNA テクノロジーを組み込み、包括的にさまざまな機能を提供し、今後のソフトウェアリリースに対応して投資を保護します。PCIe 標準準拠のインターフェイスをホストに提示可能で、NIC および HBA として動的に構成できます。

Cisco UCS VIC 1455 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）1455 は、Cisco UCS C シリーズ ラック サーバの M5 世代用に設計された、クワッドポート Small Form-Factor Pluggable（SFP28）ハーフハイト PCIe カードです。このカードは、10/25 Gbps イーサネットまたは FCoE をサポートします。これは Cisco の次世代 CNA テクノロジーを組み込み、包括的にさまざまな機能を提供し、今後のソフトウェアリリースに対応して投資を保護します。PCIe 標準準拠のインターフェイスをホストに提示可能で、NIC および HBA として動的に構成できます。

Cisco UCS VIC 1387 仮想インターフェイス カード

Cisco UCS VIC 1387 仮想インターフェイス カードは、デュアルポートの拡張型 Quad Small Form-Factor Pluggable（QSFP）40 ギガビット イーサネットおよび Fibre Channel over Ethernet（FCoE）対応のハーフハイト PCI Express（PCIe）カードで、Cisco UCS C シリーズ ラック サーバ専用に設計されています。シスコの次世代統合型ネットワーク アダプタ（CNA）技術は、包括的にさまざまな機能を提供し、今後のソフトウェア リリースに対応して投資を保護します。

Cisco UCS VIC 1385 仮想インターフェイス カード

この Cisco UCS VIC 1385 仮想インターフェイス カードは、デュアルポートの拡張型 Quad Small Form-Factor Pluggable（QSFP）40 ギガビット イーサネットおよび Fibre Channel over Ethernet（FCoE）対応のハーフハイト PCI Express（PCIe）カードで、Cisco UCS C シリーズ ラック サーバ専用に設計されています。シスコの次世代統合型ネットワーク アダプタ（CNA）技術は、

包括的にさまざまな機能を提供し、今後のソフトウェア リリースに対応して投資を保護します。

Cisco UCS VIC 1227T 仮想インターフェイス カード

Cisco UCS VIC 1227T 仮想インターフェイス カードは、Cisco UCS C シリーズ ラック サーバ専用に設計された、デュアルポートの 10GBASE-T（RJ-45）10-Gbps イーサネットおよび Fibre Channel over Ethernet（FCoE）対応の PCI Express（PCIe）モジュラ LAN-on-motherboard（mLOM）アダプタです。Cisco のラック サーバに新たに導入された mLOM スロットを使用すると、PCIe スロットを使用せずに Cisco VIC を装着できます。これにより、I/O 拡張性が向上します。シスコの次世代統合型ネットワーク アダプタ（CNA）技術が取り入れられており、低コストのツイスト ペア ケーブルで、30 メートルまでのビット エラー レート（BER）が 10 ～ 15 のファイバチャネル接続を提供します。また、将来の機能リリースにおける投資保護を実現します。

Cisco UCS VIC 1225 仮想インターフェイス カード

Cisco UCS VIC 1225 仮想インターフェイス カードは、サーバ仮想化によって導入される種々の新しい動作モードを高速化する、高性能の統合型ネットワーク アダプタです。優れた柔軟性、パフォーマンス、帯域幅を新世代の Cisco UCS C シリーズ ラックマウント サーバに提供します。

Cisco UCS P81E Virtual Interface Card

Cisco UCS P81E Virtual Interface Card は、仮想化された環境、物理環境のモビリティ強化を求めている組織、およびNIC、HBA、ケーブル配線、スイッチの減少によるコスト削減と管理オーバーヘッドの軽減を目指しているデータセンターに対して最適化されています。Fibre Channel over Ethernet（FCoE）PCIe カードには、次の利点があります。

- ジャストインタイムのプロビジョニングを使用して、最大で 16 個の仮想ファイバ チャネルと 16 個のイーサネット アダプタを仮想化または非仮想化環境でプロビジョニングできます。それにより、システムの柔軟性が大幅に向上するとともに、複数の物理アダプタを統合することが可能になります。
- 仮想化を全面的にサポートしたドライバ（Cisco VN-Link テクノロジーとパススルー スイチングのハードウェアベースの実装を含む）。
- ネットワーク ポリシーとセキュリティの可視性およびポータビリティが、仮想マシンにまでわたる全域で提供されることにより、システムのセキュリティおよび管理性が向上します。

仮想インターフェイス カードは、親ファブリック インターコネクトに対して Cisco VN-Link 接続を確立します。それにより、仮想マシン内の仮想 NIC を仮想リンクでインターコネクトに接続できるようになります。Cisco Unified Computing System 環境では、仮想リンクを管理し、ネットワーク プロファイルを適用することができます。また、仮想マシンがシステム内のサーバ間を移動する際に、インターフェイスを動的に再プロビジョニングできます。

ネットワーク アダプタのプロパティの設定

始める前に

- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。
- サーバの電源をオンにする必要があります。そうしないと、プロパティが表示されません。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーク（Networking）] メニューをクリックします。

ステップ 2 **[ネットワーキング (Networking)]** メニューでペインで、表示するアダプタ カードを選択し、。

ステップ 3 **[全般 (General)** タブの **[アダプタ カード プロパティ (Adapter Card Properties)]** 領域で、次の情報を確認します

名前	説明
[PCI Slot] フィールド	アダプタが装着されている PCI スロット。
[Vendor]フィールド	アダプタのベンダー。
[Product Name] フィールド	アダプタの製品名。
[製品ID（Product ID）]フィールド	アダプタの製品 ID。
[Serial Number] フィールド	アダプタのシリアル番号。
[Version ID] フィールド	アダプタのバージョン ID。
[PCI Link] フィールド	PCIe リンクが確立されているサーバ。
[Hardware Revision] フィールド	アダプタのハードウェア リビジョン。
[**Cisco IMC Management Enabled**] フィールド	このフィールドに [**yes**] と表示されている場合、そのアダプタは Cisco Card モードで動作しており、サーバーの Cisco IMC に Cisco IMC 管理トラフィックを渡しています。

名前	説明
[Configuration Pending] フィールド	このフィールドに [**yes**] と表示されている場合、そのアダプタの設定は Cisco IMC で変更されていますが、ホストのオペレーティングシステムには変更内容が通知されていません。 変更を有効にするには、管理者がアダプタを再起動する必要があります。
[ISCSI 起動対応（ISCSI Boot Capable）] フィールド	iSCSI 起動がこのアダプタでサポートされているかどうか。
[CDN 対応（CDN Capable）] フィールド	アダプタで CDN がサポートされているかどうか。
[usNIC 対応（usNIC Capable）] フィールド	アダプタおよびアダプタで実行されるファームウェアが usNIC をサポートするかどうか。
[ポートチャネル（Port Channel）] フィールド	ポート チャネルがアダプタでサポートされているかどうかを示します。 （注） このオプションは、一部のアダプタおよびサーバーでのみ使用可能です。
[Description] フィールド	アダプタのユーザ定義の説明。 1 ～ 63 文字の範囲で入力できます。
[Enable FIP Mode] チェックボックス	オンにすると、FCoE 初期化プロトコル（FCoE Initialization Protocol、FIP）モードが有効になります。FIP モードは、アダプタが現在の FCoE 標準との互換性を保つことを保証します。 （注） テクニカルサポートの担当者から明確に指示された場合にだけ、このオプションを使用することを推奨します。

名前	説明
[Enable LLDP] チェックボックス	（注） LLDP の変更を有効にするは、サーバーの再起動が必要です。 S3260 シャーシに 2 つのノードがある場合、プライマリ ノードで LLDP の変更を行った後にセカンダリノードを再起動するようにしてください。 オンにすると、Link Layer Discovery Protocol（LLDP）によってすべての Data Center Bridging Capability Exchange プロトコル（DCBX）機能が有効になります。これには、FCoE、プライオリティ ベースのフロー制御も含まれます。 デフォルトで LLDP オプションは有効になっています。 （注） LLDP オプションを無効にすると、すべての DCBX 機能が無効になるので、このオプションは無効にしないことを推奨します。
[Enable VNTAG Mode] チェックボックス	VNTAG モードが有効の場合： • 特定のチャネルに vNIC と vHBA を割り当てることができます。 • ポート プロファイルに vNIC と vHBA を関連付けることができます。 • 通信に問題が生じた場合、vNIC を他の vNIC にフェールオーバーする。
[Port Channel] チェックボックス	このオプションは、デフォルトで有効です。 ポート チャネルを有効にすると、2 つの vNIC および 2 つの vHBA がアダプタ カードで使用できます。 無効にすると、4 つの vNIC および 4 つの vHBA がアダプタ カードで使用できます。 （注） このオプションは、一部のアダプタおよびサーバでのみ使用可能です。

名前	説明
[物理 NIC モード (Physical NIC Mode)] チェック ボックス	

名前	説明
	このオプションは、デフォルトで無効です。 物理NICモードが有効になっている場合、VICのアップリンク ポートはパススルー モードに設定されます。これにより、ホストは変更を行わずにパケットを送信できます。VIC ASICは、vNIC の VLAN と CoS の設定に基づいてパケットの VLAN タグをリライトしません。 （注） • このオプションは、Cisco UCS VIC 14xx シリーズおよび 15xxx シリーズ アダプタで使用できます。 • VIC 構成の変更を有効にするには、ホストを再起動する必要があります。 • 次のようなアダプタでは、このオプションを有効にすることはできません。 • **[ポート チャネル モード (Port Channel mode)]** が有効になっています • **[VNTAG モード (VNTAG mode)]** が有効になっているもの • **[LLDP]** が有効になっているもの • **[FIP モード (FIP mode)]** が有効になっているもの • **[CISCO IMC 管理が有効 (Cisco IMC Management Enabled)]** 値が **[はい (Yes)]** に設定されています • 複数のユーザーが作成した vNIC 物理NICモードが有効になっている場合、ポップアップ ウィンドウに次のメッセージが表示されま

名前	説明
	す。 **物理 nic-mode が切り替わった後、vNIC構成は失われて新しいデフォルトvNICが作成されます。** [OK] をクリックします。

ステップ 4 [Firmware] 領域で、次の情報を確認します。

名前	説明
[Running Version] フィールド	現在有効なファームウェア バージョン。
[Backup Version] フィールド	アダプタにインストールされている別のファームウェア バージョン（存在する場合）。バックアップ バージョンは現在動作していません。バックアップ バージョンをアクティブにするには、管理者が [Actions] 領域で [Activate Firmware] をクリックします。 （注） アダプタに新しいファームウェアをインストールすると、既存のバックアップバージョンはすべて削除され、新しいファームウェアがバックアップバージョンになります。アダプタで新しいバージョンを実行するには、その新しいバージョンを手動でアクティブにする必要があります。
[Startup Version] フィールド	次回アダプタが再起動されたときにアクティブになるファームウェア バージョン。
[Bootloader Version] フィールド	アダプタ カードに関連付けられたブートローダのバージョン。
[Status] フィールド	このアダプタで前回実行されたファームウェアのアクティブ化のステータス。 （注） このステータスはアダプタがリブートされるたびにリセットされます。

ステップ 5 **[外部イーサネット インターフェイス (External Ethernet Interfaces)]** リンクをクリックして、次の情報を確認します。

（注） **[外部イーサネット インターフェイス (External Ethernet Interfaces)]** が別のタブで開きます。

名前	説明
[Port] カラム	アップリンク ポート ID。
[Admin Speed] カラム	ポートのデータ転送レート。次のいずれかになります。 • **[40 Gbps]** • **[4 X 10 Gbps]** • **自動**
[管理 リンク トレーニング（Admin Link Training）] カラム	ポートで管理 リンク トレーニングが有効化されているかどうかを示します。 管理者リンク トレーニングについて、以下のオプションのいずれかを選択します： • 自動 • オフ • オン 管理者リンク トレーニングは、デフォルトで **自動** に設定されています。 （注） このオプションは、一部のアダプタおよびサーバーでのみ使用可能です。

名前	説明
[管理 FEC モード（Admin FEC Mode）] ドロップダウン リスト	Admin Forward Error Correction（FEC）は、速度 25/100G の Cisco UCS VIC 14xx アダプタおよび速度 25G/50G の Cisco UCS VIC 15xxx アダプタにのみ適用されます。 次の前方誤り訂正（FEC）モード管理のオプションが設定で使用できます。 • cl108（RS-IEEE、108 節） • cl91-cons16（RS-FEC、91 節、コンソーシアム バージョン 1.6） • cl91（RS-FEC、91 条、コンソーシアム バージョン 1.5） • cl74（FC-FEC、74 節）、25G のみ • 消灯 管理 FEC モードは、デフォルトで **[cl91]** に設定されています。 （注） • このオプションは、一部のアダプタおよびサーバーでのみ使用可能です。 • **[管理 FEC モード（Admin FEC Mode）]**の設定を変更すると、**[オペレーティング FEC モード（Operating FEC mode）]**の値が同じであっても、ポートがリセットされます。
[稼働中のFEC モード（Operating FEC Mode）] column	**[稼働中の FEC モード（Operating FEC Mode）]** の値は、次の例外を除いて **[管理 FEC モード（Admin FEC mode）]** と同じです。 • 速度が 10 Gbps または 40 Gbps の場合、値はオフです。これは、FEC がサポートされていないためです。 • 値は、QSFP-100G-LR4-S トランシーバの場合はオフです。 • 値は、QSFP-40/100-SRBD トランシーバの場合はオフです。 （注） このオプションは、一部のアダプタおよびサーバーでのみ使用可能です。

名前	説明
[Operリンク トレーニング（Oper Link Training）] カラム	**[Operリンク トレーニング（Oper Link Training）]** の値は、**[管理リンク トレーニング（Admin Link Training）]** ドロップダウン リストで設定された値から取得されます。 4.2（2a）以降、次の異なる設定は、Cisco UCS VIC 15xxx アダプタと、速度 10G/25G/50G の銅線ケーブルにのみ適用されます。 • 管理リンク トレーニング が Auto に設定されている場合、アダプター ファームウェアは、トランシーバに応じて Oper リンク トレーニング値（AutoNeg）をオンまたはオフに設定します。 • AutoNeg は 25G 銅線で無効 • AutoNeg は 50G 銅線で有効 • 管理リンク トレーニング がオンに設定されている場合、アダプタ ファームウェアは Oper リンク トレーニング値 をオンに設定します。 • AutoNeg は 25G 銅線で有効 • AutoNeg は 50G 銅線で有効 • Admin Link Training が**オフ**の場合、アダプタ ファームウェアは **Oper リンク トレーニング** を **オフ** に設定します。 • AutoNeg は 25G 銅線で無効 • AutoNeg は 50G 銅線で無効 （注） すべての非パッシブ銅線ケーブルでは、**管理リンク トレーニング** モードに関係なく、**Oper リンク トレーニング**（AN）モードがオフに設定されています。 **管理リンク トレーニング**の設定を変更すると、**Oper リンク トレーニング** の値が同じであっても、そのポートのシリーズがリセットされます。
[MAC Address] カラム	アップリンク ポートの MAC アドレス。

名前	説明
[Link State] 列	アップリンク ポートの現在の動作状態。次のいずれかになります。 • **[Fault]** • **[Link Up]** • **[Link Down]** • **[SFP ID Error]** • **[SFP Not Installed]** • **[SFP Security Check Failed]** • **[Unsupported SFP]** （注） • Serdes リセットにより、**リンク状態**フィールドが **リンク アップ** から **リンクダウン** に変わります。 **オペレーション リンク トレーニング**設定が有効な場合、リンク パートナーは、リセット後に **リンク アップ** または **リンク ダウン** を決定します。 • **[リンク状態（Link State）]** フィールドの変更を表示するには、Web UI を数回更新する必要がある場合があります。
[Encap] カラム	アダプタが動作するモード。次のいずれかになります。 • [CE]：クラシカル イーサネット モード。 • [NIV]：ネットワーク インターフェイス仮想化モード。
[Operating Speed] カラム	ポートの動作スピード。次のいずれかになります。 • **10 Gbps** • **25Gbps** • **[40 Gbps]** • **50 Gbps** • **[4 X 10 Gbps]** • **100 Gbps**

名前	説明
[Connector Present] カラム	コネクタが存在するかどうかを示します。次のいずれかになります。 • [Yes]：コネクタは存在します。 • [No]：コネクタは存在しません。 （注） このオプションを使用できるのは一部のアダプタ カードのみです。
[Connector Supported] 列	コネクタがシスコにサポートされているかどうかを示します。次のいずれかになります。 • [Yes]：コネクタはシスコにサポートされています。 • [No]：コネクタはシスコにサポートされていません。 コネクタがサポートされていない場合、リンクはアップしません。 （注） このオプションを使用できるのは一部のアダプタ カードのみです。
[Connector Type] カラム	存在するトランシーバ/ケーブルのシスコ製品識別子（PID）。 （注） このオプションを使用できるのは一部のアダプタ カードのみです。
[Connector Vendor] 列	コネクタのベンダー。 （注） このオプションを使用できるのは一部のアダプタ カードのみです。
[Connector Part Number] カラム	コネクタベンダーの部品番号。 （注） このオプションを使用できるのは一部のアダプタ カードのみです。
[Connector Part Revision] カラム	コネクタベンダーの部品番号の部品修正。 （注） このオプションを使用できるのは一部のアダプタ カードのみです。

vHBA の管理

vHBA 管理のガイドライン

vHBA を管理する場合は、次のガイドラインと制限事項を考慮してください。

- Cisco UCS 仮想インターフェイス カードについている には、デフォルトで 2 個の vHBA と 2 個の vNIC が用意されています。これらのアダプタ カードに最大 14 個の vHBA または vNIC を追加作成できます。

  Cisco UCS1455、1457、および 1467 仮想インターフェイス カードは、非ポートチャネル モードで、デフォルトで 4 個の vHBAs と4 個の Vhbas を提供します。これらのアダプタ カードに最大 10 個の vHBA または vNICs を追加作成できます。

（注） アダプタに対して VNTAG モードが有効になっている場合は、vHBA を作成するときにチャネル番号を割り当てる必要があります。

- FCoE アプリケーションで Cisco UCS 仮想インターフェイス カードを使用する場合は、vHBA を FCoE VLAN に関連付ける必要があります。VLAN を割り当てるには、「**vHBA のプロパティの変更**」で説明されている手順に従います。
- 設定の変更後は、その設定を有効にするためにホストをリブートする必要があります。

vHBA のプロパティの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーク（Networking）] メニューをクリックします。

ステップ 2 **[ネットワーキング (Networking)]** ペインで、表示するアダプタ カード を選択します。

ステップ 3 **[アダプタ カード (Adapter Card)]** エリアで、**[vHBAs]** タブをクリックします。

ステップ 4 [vHBAs] ペインで、[fc0] または [fc1] をクリックします。

ステップ 5 [vHBA Properties] の [General] 領域で、次のフィールドの情報を確認します。

名前	説明
[名前（Name）] フィールド	仮想 HBA の名前。 この名前は、vHBA の作成後は変更できません。

名前	説明
[イニシエータ WWNN（Initiator WWNN）] フィールド	vHBA に関連付けられた WWNN。 WWNN を自動的に生成するには、[AUTO] を選択します。WWNN を指定するには、2 つ目のオプション ボタンをクリックし、対応するフィールドに WWNN を入力します。
[イニシエータ WWPN（Initiator WWPN）] フィールド	vHBA に関連付けられた WWPN。 WWPN を自動的に生成するには、[AUTO] を選択します。WWPN を指定するには、2 つ目のオプション ボタンをクリックし、対応するフィールドに WWPN を入力します。
[FC SAN Boot] チェックボックス	オンにすると、vHBA を使用して SAN ブートを実行できます。
[永続 LUN バインディング (Persistent LUN Binding)] チェック ボックス	オンにすると、LUN ID のアソシエーションは手動でクリアされるまで、メモリに維持されます。
[Uplink Port] ドロップダウン リスト	vHBA に関連付けられたアップリンク ポート。 （注） この値は、システム定義の vHBA である fc0 と fc1 については変更できません。
[MAC アドレス（MAC Address）] フィールド	vHBA に関連付けられた MAC アドレス。 システムが MAC アドレスを生成するようにするには、[AUTO] を選択します。アドレスを指定するには、2 番目のオプション ボタンをクリックし、対応するフィールドに MAC アドレスを入力します。
[Default VLAN] フィールド	この vHBA にデフォルトの VLAN がない場合、[NONE] をクリックします。それ以外の場合は、2 つ目のオプション ボタンをクリックし、フィールドに 1 ～ 4094 の VLAN ID を入力します。
[PCI Order] フィールド	この vHBA が使用される順序。 システムが順序を設定するようにするには、[ANY] を選択します。順序を指定するには、2 つ目のオプション ボタンを選択し、0 ～ 17 の整数を入力します。

名前	説明
[vHBA タイプ (vHBA Type)] ドロップダウン リスト	（注） このオプションは、14xx シリーズ [と VIC 15428（ and VIC 15428 ）] アダプタでのみ使用できます。 このポリシーで使用される vHBA タイプ。サポートされている FC と FC NVMe Vhba は、同じアダプタでここで作成できます。このポリシーで使用される vHBA タイプには、次のいずれかを指定できます。 • fc-initiator：レガシー SCSI FC vHBA イニシエータ • fc-target：SCSI FC ターゲット機能をサポートする vHBA （注） このオプションは、技術プレビューとして使用可能です。 • fc-nvme-initiator：FC NVME イニシエータ、FC NVME ターゲットを検出し、それらに接続する vHBA • fc-nvme-target：FC NVME ターゲットとして機能し、NVME ストレージへ接続する vHBA
[Class of Service] フィールド	vHBA の CoS。 0 ～ 6 の整数を選択します。0 が最も低い優先度で、6 が最も高い優先度になります。 （注） このオプションは VNTAG モードでは使用できません。
[Rate Limit] フィールド	この vHBA 上のトラフィックのデータ レート制限（Mbps 単位）。 この vHBA に無制限のデータ レートを設定するには、[OFF] を選択します。それ以外の場合は、2 つ目のオプション ボタンをクリックし、1 ～ 10,000 の整数を入力します。 （注） このオプションは VNTAG モードでは使用できません。
[EDTOV] フィールド	エラー検出タイムアウト値（EDTOV）。システムが、エラーが発生したと見なすまでに待機するミリ秒数です。 1,000 ～ 100,000 の整数を入力します。デフォルトは 2,000 ミリ秒です。

名前	説明
[RATOV] フィールド	リソース割り当てタイムアウト値（RATOV）。システムが、リソースを適切に割り当てることができないと見なすまでに待機するミリ秒数です。 5,000 ～ 100,000 の整数を入力します。デフォルトは 10,000 ミリ秒です。
[Max Data Field Size] フィールド	vHBA がサポートするファイバ チャネル フレームのペイロード バイトの最大サイズ。 256 ～ 2112 の範囲の整数を入力します。
[Channel Number] フィールド	この vHBA に割り当てるチャネル番号。 1 ～ 1,000 の整数を入力します。 （注） このオプションには VNTAG モードが必要です。
PCI リンク	これは読み取り専用フィールドです。
[Port Profile] ドロップダウン リスト	vHBA に関連付ける必要があるポート プロファイル（ある場合）。 このフィールドには、このサーバが接続しているスイッチに定義されたポート プロファイルが表示されます。 （注） このオプションには VNTAG モードが必要です。

ステップ 6 **[Error Recovery]**領域で、次のフィールドの情報を確認します。

名前	説明
[FCP エラー リカバリの有効化 (Enable FCP Error Recovery)] チェックボックス	オンにすると、システムは FCP Sequence Level Error Recovery プロトコル（FC-TAPE）を使用します。
[Link Down Timeout] フィールド	アップリンク ポートがダウンし、ファブリック接続が失われていることをシステムに通知する前に、アップリンク ポートがオフラインになっていなければならないミリ秒数。 0 ～ 240,000 の整数を入力します。
[ポート ダウン I/O の再試行 (Port Down I/O Retries)]フィールド	ポートが使用不可能であるとシステムが判断する前に、そのポートへの I/O 要求がビジー状態を理由に戻される回数。 0 ～ 255 の整数を入力します。

名前	説明
[I/O タイムアウトの再試行 (I/O Timeout Retry)] フィールド	システムが再試行前にタイムアウトするまで待機する時間。ディスクが定義されたタイムアウト時間内に I/O へ応答しない場合、ドライバは保留中のコマンドを打ち切り、タイマーの期限が切れた後に同じ I/O を再送信します。 1 ～ 59 の整数を入力します。
[Port Down Timeout] フィールド	リモート ファイバ チャネル ポートが使用不可能であることを SCSI 上位層に通知する前に、そのポートがオフラインになっていなければならないミリ秒数。 0 ～ 240,000 の整数を入力します。

ステップ 7 **[Fibre Channel Interrupt]**領域で、次のフィールドの情報を確認します。

名前	説明
[Interrupt Mode] ドロップダウン リスト	優先ドライバ割り込みモード。次のいずれかになります。 • [MSIx]：機能拡張された Message Signaled Interrupts（MSI）。これが推奨オプションです。 • [MSI]：MSI だけ。 • [INTx]：PCI INTx 割り込み。

ステップ 8 **[Fibre Channel Port]**領域で、次のフィールドの情報を確認します。

名前	説明
[I/O Throttle Count] フィールド	vHBA 内に同時に保留可能な I/O 操作の数。 1 ～ 1,024 の整数を入力します。
[LUNs Per Target] フィールド	ドライバでエクスポートされる LUN の最大数。通常は、オペレーティング システム プラットフォームの制限です。 Cisco UCS C シリーズ サーバーの場合は、1 ～ 4096 の整数を入力します。
[LUN Queue Depth] フィールド	HBA が LUN ごとに 1 つのチャンクで送受信できるコマンドの数。このパラメーターは、アダプター上の LUN すべてに対して初期キューの深度を設定します。 デフォルト値は、物理ミニポートの場合は 20、仮想ミニポートの場合は 250 です。

ステップ 9 **[Fibre Channel Port FLOGI]**領域で、次のフィールドの情報を確認します。

名前	説明
[FLOGI Retries] フィールド	システムがファブリックへのログインを最初に失敗してから再試行する回数。 再試行回数を無制限に指定するには、[INFINITE] オプション ボタンを選択します。それ以外の場合は、2 番目のオプション ボタンを選択し、対応するフィールドに整数を入力します。
[FLOGI Timeout] フィールド	システムがログインを再試行する前に待機するミリ秒数。 1,000 ～ 255,000 の整数を入力します。

ステップ 10 [Fibre Channel Port PLOGI] 領域で、次のフィールドの情報を確認します。

名前	説明
[PLOGI Retries] フィールド	システムがポートへのログインを最初に失敗してから再試行する回数。 0 ～ 255 の整数を入力します。
[PLOGI Timeout] フィールド	システムがログインを再試行する前に待機するミリ秒数。 1,000 ～ 255,000 の整数を入力します。

ステップ 11 **[I/O]** 領域で、次のフィールドの情報を確認します。

名前	説明
[CDB Transmit Queue Count] フィールド	システムで割り当てる SCSI I/O キュー リソースの数。 Cisco UCS VIC 14xx シリーズ アダプタの場合、1 ～ 64 の整数を入力します。 その他の VIC アダプタの場合は、1 ～ 245 の整数を入力します。
[CDB Transmit Queue Ring Size] フィールド	各 SCSI I/O キュー内の記述子の数。 64 ～ 512 の整数を入力します。

ステップ 12 [Receive/Transmit Queues] 領域で、次のフィールドの情報を確認します。

名前	説明
[FC Work Queue Ring Size] フィールド	各送信キュー内の記述子の数。 64 ～ 128 の整数を入力します。
[FC Receive Queue Ring Size] フィールド	各受信キュー内の記述子の数。 64 ～ 2048 の整数を入力します。

ステップ 13 （注） ブート テーブルは、Cisco UCS C シリーズ M7 以降のサーバーの個別のタブとして使用できます。**[ブート エントリの追加（Add Boot Entry）]** をクリックして新しいブートエントリを作成するか、既存のエントリを選択して**[ブート エントリの編集（Edit Boot Entry）]** をクリックします。

[ブート テーブル (Boot Table)] 領域で、次のフィールドの情報を確認します。

名前	説明
[Index] カラム	ブート ターゲットの固有識別子。
[Target WWPN] カラム	ブート イメージの場所に対応するワールド ワイド ポート（WWPN）名。
[LUN] カラム	ブート イメージの場所に対応する LUN ID。
[Add Boot Entry] ボタン	新しい WWPN および LUN ID を指定するためのダイアログ ボックスが開きます。
[ブート エントリの編集（Edit Boot Entry）] ボタン	選択したブート ターゲットの WWPN および LUN ID を変更するためのダイアログボックスが開きます。
[ブート エントリの削除（Delete Boot Entry）] ボタン	選択したブート ターゲットを削除します。削除する前に、削除操作を確認するよう求められます。

ステップ 14 （注） **永続的なバインディング**は、Cisco UCS C シリーズ M7 以降のサーバーの個別のタブとして使用できます。**[永続的なバインディングを再構築（Rebuild Persistent Binding）]**をクリックして、バインディングをクリアして新しいバインディングを作成することができます。

[永続バインディング (Persistent Bindings)] 領域で、次のフィールドの情報を確認します。

名前	説明
[Index] カラム	バインディングの固有識別子。
[Target WWPN] カラム	バインディングが関連付けられるターゲットのワールド ワイド ポート名。
[ホスト WWPN（Host WWPN）] カラム	バインドに関連付けるホスト ワールド ワイド ポート名。
[バス ID（Bus ID）] カラム	バインドに関連付けるバス ID。
[ターゲット ID（Target ID）] カラム	バインドに関連付けるホスト システムでのターゲット ID。

名前	説明
[永続バインドの再構築（Rebuild Persistent Bindings）] ボタン	未使用のすべてのバインディングをクリアし、使用されているバインディングをリセットします。

vHBA のプロパティの変更

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーク（Networking）] メニューをクリックします。

ステップ 2 **[ネットワーキング（Networking）]** ペインで、変更するアダプタ カード を選択します。

ステップ 3 **[アダプタ カード (Adapter Card)]** ペインで、**[vHBAs]** タブをクリックします。

ステップ 4 [vHBAs] ペインで、[fc0] または [fc1] をクリックします。

ステップ 5 [General] 領域で、次のフィールドを更新します。

名前	説明
[名前（Name）] フィールド	仮想 HBA の名前。 この名前は、vHBA の作成後は変更できません。
[イニシエータ WWNN（Initiator WWNN）] フィールド	vHBA に関連付けられた WWNN。 WWNN を自動的に生成するには、[AUTO] を選択します。WWNN を指定するには、2 つ目のオプション ボタンをクリックし、対応するフィールドに WWNN を入力します。
[イニシエータ WWPN（Initiator WWPN）] フィールド	vHBA に関連付けられた WWPN。 WWPN を自動的に生成するには、[AUTO] を選択します。WWPN を指定するには、2 つ目のオプション ボタンをクリックし、対応するフィールドに WWPN を入力します。
[FC SAN Boot] チェックボックス	オンにすると、vHBA を使用して SAN ブートを実行できます。
[永続 LUN バインディング (Persistent LUN Binding)] チェック ボックス	オンにすると、LUN ID のアソシエーションは手動でクリアされるまで、メモリに維持されます。

名前	説明
[Uplink Port] ドロップダウン リスト	vHBA に関連付けられたアップリンク ポート。 （注） この値は、システム定義の vHBA である fc0 と fc1 については変更できません。
[MACアドレス（MAC Address）]フィールド	vHBA に関連付けられた MAC アドレス。 システムがMACアドレスを生成するようにするには、[AUTO] を選択します。アドレスを指定するには、2 番目のオプション ボタンをクリックし、対応するフィールドに MAC アドレスを入力します。
[Default VLAN] フィールド	この vHBA にデフォルトの VLAN がない場合、[NONE] をクリックします。それ以外の場合は、2 つ目のオプション ボタンをクリックし、フィールドに 1 ～ 4094 の VLAN ID を入力します。
[PCI Order] フィールド	この vHBA が使用される順序。 システムが順序を設定するようにするには、[ANY] を選択します。順序を指定するには、2 つ目のオプション ボタンを選択し、0 ～ 17 の整数を入力します。
[vHBA タイプ (vHBA Type)] ドロップダウン リスト	（注） このオプションは、14xx シリーズ [と VIC 15428 （ and VIC 15428 ）] アダプタでのみ使用できます。 このポリシーで使用される vHBA タイプ。サポートされている FC と FC NVMe Vhba は、同じアダプタでここで作成できます。このポリシーで使用される vHBA タイプには、次のいずれかを指定できます。 • fc-initiator：レガシー SCSI FC vHBA イニシエータ • fc-target：SCSI FC ターゲット機能をサポートする vHBA （注） このオプションは、技術プレビューとして使用可能です。 • fc-nvme-initiator：FC NVME イニシエータ、FC NVME ターゲットを検出し、それらに接続する vHBA • fc-nvme-target：FC NVME ターゲットとして機能し、NVME ストレージへ接続する vHBA

名前	説明
[Class of Service] フィールド	vHBA の CoS。 0 ～ 6 の整数を選択します。0 が最も低い優先度で、6 が最も高い優先度になります。 （注） このオプションは VNTAG モードでは使用できません。
[Rate Limit] フィールド	この vHBA 上のトラフィックのデータ レート制限（Mbps 単位）。 この vHBA に無制限のデータ レートを設定するには、[OFF] を選択します。それ以外の場合は、2 つ目のオプション ボタンをクリックし、1 ～ 10,000 の整数を入力します。 （注） このオプションは VNTAG モードでは使用できません。
[EDTOV] フィールド	エラー検出タイムアウト値（EDTOV）。システムが、エラーが発生したと見なすまでに待機するミリ秒数です。 1,000 ～ 100,000 の整数を入力します。デフォルトは 2,000 ミリ秒です。
[RATOV] フィールド	リソース割り当てタイムアウト値（RATOV）。システムが、リソースを適切に割り当てることができないと見なすまでに待機するミリ秒数です。 5,000 ～ 100,000 の整数を入力します。デフォルトは 10,000 ミリ秒です。
[Max Data Field Size] フィールド	vHBA がサポートするファイバ チャネル フレームのペイロード バイトの最大サイズ。 256 ～ 2112 の範囲の整数を入力します。
[Channel Number] フィールド	この vHBA に割り当てるチャネル番号。 1 ～ 1,000 の整数を入力します。 （注） このオプションには VNTAG モードが必要です。
PCI リンク	これは読み取り専用フィールドです。

名前	説明
[Port Profile] ドロップダウン リスト	vHBA に関連付ける必要があるポート プロファイル（ある場合）。 このフィールドには、このサーバが接続しているスイッチに定義されたポート プロファイルが表示されます。 （注） このオプションには VNTAG モードが必要です。

ステップ 6 **[Error Recovery]**領域で、次のフィールドを更新します。

名前	説明
[FCP エラー リカバリの有効化 (Enable FCP Error Recovery)] チェックボックス	オンにすると、システムは FCP Sequence Level Error Recovery プロトコル（FC-TAPE）を使用します。
[Link Down Timeout] フィールド	アップリンク ポートがダウンし、ファブリック接続が失われていることをシステムに通知する前に、アップリンク ポートがオフラインになっていなければならないミリ秒数。 0 ～ 240,000 の整数を入力します。
[ポート ダウン I/O の再試行 (Port Down I/O Retries)]フィールド	ポートが使用不可能であるとシステムが判断する前に、そのポートへの I/O 要求がビジー状態を理由に戻される回数。 0 ～ 255 の整数を入力します。
[I/O タイムアウトの再試行 (I/O Timeout Retry)] フィールド	システムが再試行前にタイムアウトするまで待機する時間。ディスクが定義されたタイムアウト時間内に I/O へ応答しない場合、ドライバは保留中のコマンドを打ち切り、タイマーの期限が切れた後に同じ I/O を再送信します。 1 ～ 59 の整数を入力します。
[Port Down Timeout] フィールド	リモート ファイバ チャネル ポートが使用不可能であることを SCSI 上位層に通知する前に、そのポートがオフラインになっていなければならないミリ秒数。 0 ～ 240,000 の整数を入力します。

ステップ 7 **[Fibre Channel Interrupt]**領域で、次のフィールドを更新します。

名前	説明
[Interrupt Mode] ドロップダウン リスト	優先ドライバ割り込みモード。次のいずれかになります。 • [MSIx]：機能拡張された Message Signaled Interrupts（MSI）。これが推奨オプションです。 • [MSI]：MSI だけ。 • [INTx]：PCI INTx 割り込み。

ステップ 8 **[Fibre Channel Port]**領域で、次のフィールドを更新します。

名前	説明
[I/O Throttle Count] フィールド	vHBA 内に同時に保留可能な I/O 操作の数。 1 ～ 1,024 の整数を入力します。
[LUNs Per Target] フィールド	ドライバでエクスポートされる LUN の最大数。通常は、オペレーティング システム プラットフォームの制限です。 Cisco UCS C シリーズ サーバーの場合は、1 ～ 4096 の整数を入力します。
[LUN Queue Depth] フィールド	HBA が LUN ごとに 1 つのチャンクで送受信できるコマンドの数。このパラメーターは、アダプター上の LUN すべてに対して初期キューの深度を設定します。 デフォルト値は、物理ミニポートの場合は 20、仮想ミニポートの場合は 250 です。

ステップ 9 **[Fibre Channel Port FLOGI]**領域で、次のフィールドを更新します。

名前	説明
[FLOGI Retries] フィールド	システムがファブリックへのログインを最初に失敗してから再試行する回数。 再試行回数を無制限に指定するには、[INFINITE] オプション ボタンを選択します。それ以外の場合は、2 番目のオプション ボタンを選択し、対応するフィールドに整数を入力します。
[FLOGI Timeout] フィールド	システムがログインを再試行する前に待機するミリ秒数。 1,000 ～ 255,000 の整数を入力します。

ステップ 10 **[Fibre Channel Port PLOGI]**領域で、次のフィールドを更新します。

名前	説明
[PLOGI Retries] フィールド	システムがポートへのログインを最初に失敗してから再試行する回数。 0 ～ 255 の整数を入力します。
[PLOGI Timeout] フィールド	システムがログインを再試行する前に待機するミリ秒数。 1,000 ～ 255,000 の整数を入力します。

ステップ 11 **[SCSI I/O]**領域で、次のフィールドを更新します。

名前	説明
[CDB Transmit Queue Count] フィールド	システムで割り当てる SCSI I/O キュー リソースの数。 Cisco UCS VIC 14xx シリーズ アダプタの場合、1 ～ 64 の整数を入力します。 その他の VIC アダプタの場合は、1 ～ 245 の整数を入力します。
[CDB Transmit Queue Ring Size] フィールド	各 SCSI I/O キュー内の記述子の数。 64 ～ 512 の整数を入力します。

ステップ 12 [Receive/Transmit Queues] 領域で、次のフィールドを更新します。

名前	説明
[FC Work Queue Ring Size] フィールド	各送信キュー内の記述子の数。 64 ～ 128 の整数を入力します。
[FC Receive Queue Ring Size] フィールド	各受信キュー内の記述子の数。 64 ～ 2048 の整数を入力します。

ステップ 13 [Save Changes] をクリックします。

ステップ 14 （注） ブート テーブルは、Cisco UCS C シリーズ M7 以降のサーバーの個別のタブとして使用できます。**[ブート エントリの追加（Add Boot Entry）]** をクリックして新しいブートエントリを作成するか、既存のエントリを選択して**[ブート エントリの編集（Edit Boot Entry）]** をクリックします。

[ブート テーブル (Boot Table)] 領域で、次のフィールドを更新するか、新しいエントリを追加します。

名前	説明
[Index] カラム	ブート ターゲットの固有識別子。

名前	説明
[Target WWPN] カラム	ブート イメージの場所に対応するワールド ワイド ポート（WWPN）名。
[LUN] カラム	ブート イメージの場所に対応する LUN ID。
[Add Boot Entry] ボタン	新しい WWPN および LUN ID を指定するためのダイアログ ボックスが開きます。
[ブート エントリの編集（Edit Boot Entry）] ボタン	選択したブート ターゲットの WWPN および LUN ID を変更するためのダイアログボックスが開きます。
[ブート エントリの削除（Delete Boot Entry）] ボタン	選択したブート ターゲットを削除します。削除する前に、削除操作を確認するよう求められます。

ステップ 15 （注） **永続的なバインディング**は、Cisco UCS C シリーズ M7 以降のサーバーの個別のタブとして使用できます。**[永続的なバインディングを再構築（Rebuild Persistent Binding）]**をクリックして、バインディングをクリアして新しいバインディングを作成することができます。

[永続バインディング (Persistent Bindings)] 領域で、次のフィールドを更新するか、新しいエントリを追加します。

名前	説明
[Index] カラム	バインディングの固有識別子。
[Target WWPN] カラム	バインディングが関連付けられるターゲットのワールド ワイド ポート名。
[ホスト WWPN（Host WWPN）] カラム	バインドに関連付けるホスト ワールド ワイド ポート名。
[バス ID（Bus ID）] カラム	バインドに関連付けるバス ID。
[ターゲット ID（Target ID）] カラム	バインドに関連付けるホスト システムでのターゲット ID。
[永続バインドの再構築（Rebuild Persistent Bindings）] ボタン	未使用のすべてのバインディングをクリアし、使用されているバインディングをリセットします。

vHBA の作成

Cisco UCS 仮想インターフェイス カードには、デフォルトで 2 個の vHBA と 2 個の vNIC が用意されています。これらのアダプタ カードに最大 14 個の vHBA または vNIC を追加作成できます。

Cisco UCS1455、1457、および 1467 仮想インターフェイス カードは、非ポートチャネル モードで、デフォルトで 4 個の vHBAs と4 個の Vhbas を提供します。これらのアダプタ カードに最大 10 個の vHBA または vNICs を追加作成できます。

始める前に

[全般 (General)] タブの **[アダプタ カードのプロパティ (Adapter Card Properties)]** の **[VNTAG モードの有効化 (Enable VNTAG Mode)]** がオンになっていることを確認します。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーク（Networking）] メニューをクリックします。

ステップ 2 **[ネットワーキング (Networking)]** ペインで、変更するアダプタ カード を選択します。

ステップ 3 **[アダプタ カード (Adapter Card)]** ペインで、**[vHBAs]** タブをクリックします。

ステップ 4 [Host Fibre Channel Interfaces] 領域で、次のアクションのいずれかを選択します。

- デフォルトの設定を使用して vHBA を作成するには、**[vHBA の追加（Add vHBA）]** をクリックします。
- 既存の vHBA と同じ設定を使用して vHBA を作成するには、その vHBA を選択して **[vHBA の複製（Clone vHBA）]** をクリックします。

[Add vHBA] ダイアログボックスが表示されます。

ステップ 5 [Add vHBA] ダイアログボックスで、vHBA の名前を [Name] 入力ボックスに入力します。

ステップ 6 vHBA のプロパティの変更 （239 ページ） の説明に従って、新しい vhba を設定します。

ステップ 7 **[vHBA の追加（Add vHBA）]** をクリックします。

次のタスク

- サーバーをリブートして vHBA を作成します。

vHBA の削除

デフォルトの vHBA は削除できません。VNTAG モードを使用して作成された他の vHBA は削除できます。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーク（Networking）] メニューをクリックします。

ステップ 2 **[ネットワーキング (Networking)]** ペインで、変更するアダプタ カード を選択します。

ステップ 3 **[アダプタ カード (Adapter Card)]** ペインで、**[vHBAs]** タブをクリックします。

ステップ 4 [Host Fibre Channel Interfaces] 領域で、表から vHBA（複数可）を選択します。

（注） 2 つのデフォルトの vHBA である **[fc0]**または **[fc1]** は削除できません。

ステップ 5 [Delete vHBAs] をクリックし、[OK] をクリックして確認します。

次のタスク

サーバをリブートして vHBA を削除します。

vHBA ブート テーブル

vHBA ブート テーブルには、サーバがブート可能な LUN を 4 つまで指定できます。

ブート テーブル エントリの作成

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーク（Networking）] メニューをクリックします。

ステップ 2 **[ネットワーキング (Networking)]** ペインで、変更するアダプタ カード を選択します。

ステップ 3 **[アダプタ カード (Adapter Card)]** ペインで、**[vHBAs]** タブをクリックします。

ステップ 4 **[vHBAs]** タブの **[vHBAs]** で利用可能な vHBA のリストから vHBA を選択します。

関連する **[vHBA プロパティ (vHBA Properties)]** ペインがウィンドウの右側に表示されます。

ステップ 5 手順は次のとおりです。

- Cisco UCS C-Series M7 以降、 **[ブート表（Boot Table）]** タブを選択します。
- Cisco UCS C シリーズ M6 以前のサーバーでは、下にスクロールして**[ブート表（Boot Table）]**を表示します。

ステップ 6 [Add Boot Entry] ボタンをクリックして [Add Boot Entry] ダイアログボックスを開きます。

ステップ 7 **[ブート エントリの追加（Add Boot Entry）]**ダイアログボックスで次の情報を確認し、指定されているアクションを実行します。

名前	説明
[インデックス (Index)] フィールド	このフィールドのデフォルト値は **0** です。
[Target WWPN] フィールド	ブート イメージの場所に対応するワールド ワイド ポート（WWPN）名。 WWPN は **hh:hh:hh:hh:hh:hh:hh:hh** の形式で入力します。
[LUN ID] フィールド	ブート イメージの場所に対応する LUN ID。 ID として 0 ～ 255 の値を入力します。
[Add Boot Entry] ボタン	指定された場所をブート テーブルに追加します。
[Reset Values] ボタン	現在フィールドに入力されている値をクリアします。
[Cancel]ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

ブート テーブル エントリの削除

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーク（Networking）] メニューをクリックします。

ステップ 2 **[ネットワーキング (Networking)]** ペインで、変更するアダプタ カード を選択します。

ステップ 3 **[アダプタ カード (Adapter Card)]** ペインで、**[vHBAs]** タブをクリックします。

ステップ 4 **[vHBAs]** タブの **[vHBAs]** で利用可能な vHBA のリストから vHBA を選択します。

関連する **[vHBA プロパティ (vHBA Properties)]** ペインがウィンドウの右側に表示されます。

ステップ 5 手順は次のとおりです。

- Cisco UCS C-Series M7 以降、 **[ブート表（Boot Table）]** タブを選択します。
- Cisco UCS C シリーズ M6 以前のサーバーでは、下にスクロールして**[ブート表（Boot Table）]**を表示します。

ステップ 6 [Boot Table] 領域で、削除するエントリをクリックします。

ステップ 7 **[ブート エントリの削除（Delete Boot Entry）]** をクリックし、削除することを確認するために **[OK]**をクリックします。

vHBA の永続的なバインディング

永続的なバインディングは、システムによって割り当てられたファイバ チャネル ターゲットのマッピングがリブート後も維持されることを保証します。

永続的なバインディングの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーク（Networking）] メニューをクリックします。

ステップ 2 **[ネットワーキング (Networking)]** ペインで、変更するアダプタ カード を選択します。

ステップ 3 **[アダプタ カード (Adapter Card)]** ペインで、**[vHBAs]** タブをクリックします。

ステップ 4 [vHBAs] ペインで、[fc0] または [fc1] をクリックします。

ステップ 5 手順は次のとおりです。

- Cisco UCS C-Series M7 以降、 **[永続バインド（Persistent Bindings）]** タブを選択します。
- Cisco UCS C シリーズ M6 以前のサーバーでは、下にスクロールして**[永続バインド（Persistent Bindings）]**を表示します。

ステップ 6 **[永続バインディング (Persistent Bindings)]** 領域で、次の情報を確認します。

名前	説明
[Index] カラム	バインディングの固有識別子。
[Target WWPN] カラム	バインディングが関連付けられるターゲットのワールド ワイド ポート名。
[ホスト WWPN（Host WWPN）] カラム	バインドに関連付けるホスト ワールド ワイド ポート名。
[バス ID（Bus ID）] カラム	バインドに関連付けるバス ID。
[ターゲット ID（Target ID）] カラム	バインドに関連付けるホスト システムでのターゲット ID。
[永続バインドの再構築（Rebuild Persistent Bindings）] ボタン	未使用のすべてのバインディングをクリアし、使用されているバインディングをリセットします。

永続的なバインディングの再作成

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーク（Networking）] メニューをクリックします。

ステップ 2 **[ネットワーキング (Networking)]** ペインで、変更するアダプタ カード を選択します。

ステップ 3 **[アダプタ カード (Adapter Card)]** ペインで、**[vHBAs]** タブをクリックします。

ステップ 4 [vHBAs] ペインで、[fc0] または [fc1] をクリックします。

ステップ 5 手順は次のとおりです。

- Cisco UCS C-Series M7 以降、 **[永続バインド（Persistent Bindings）]** タブを選択します。
- Cisco UCS C シリーズ M6 以前のサーバーでは、下にスクロールして**[永続バインド（Persistent Bindings）]** エリアを表示します。

ステップ 6 [Rebuild Persistent Bindings] ボタンをクリックします。

ステップ 7 [OK] をクリックして確定します。

vNIC の管理

vNIC 管理のガイドライン

vNIC を管理する場合は、次のガイドラインと制限事項を考慮してください。

- Cisco UCS 仮想インターフェイス カードには、デフォルトで 2 個の vHBA と 2 個の vNIC が用意されています。これらのアダプタ カードに最大 14 個の vHBA または vNIC を追加作成できます。

  追加の vHBA は、VNTAG モードを使用して作成できます。

  Cisco UCS 1455、1457、および 1467 仮想インターフェイス カードは、非ポートチャネル モードで、デフォルトで 4 個の vHBAs と4 個の Vhbas を提供します。これらのアダプタ カードに最大 10 個の vHBA または vNICs を追加作成できます。

（注） アダプタに対して VNTAG モードが有効になっている場合は、vNIC を作成するときにチャネル番号を割り当てる必要があります。

- 設定の変更後は、その設定を有効にするためにホストをリブートする必要があります。

vNIC のプロパティの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーク（Networking）] メニューをクリックします。

ステップ 2 **[ネットワーキング (Networking)]** ペインで、表示するアダプタ カードを選択します。

ステップ 3 **[アダプタ カード (Adapter Card)]** ペインで、**[vNICs]** タブをクリックします。

ステップ 4 [vNICs] ペインで、[eth0] または [eth1] をクリックします。

ステップ 5 **[vNIC プロパティ (vNIC Properties)]** 領域の **[全般 (General)]** 領域で、次のフィールドの情報を確認します。

[General] 領域

名前	説明
[名前（Name）] フィールド	仮想 NIC の名前。 この名前は、vNIC の作成後は変更できません。
[CDN] フィールド	VIC カードのイーサネット vNIC に割り当てられる一貫性のあるデバイス名（CDN）。特定の CDN をデバイスに割り当てると、ホスト OS 上でそれを識別するのに役立ちます。 （注） この機能は [VIC の CDN サポート（CDN Support for VIC）] トークンが BIOS で有効化されている場合にのみ動作します。
[MTU] フィールド	この vNIC で受け入れられる最大伝送単位、つまりパケット サイズ。 1500 ～ 9000 の整数を入力します。
[Uplink Port] ドロップダウン リスト	この vNIC に関連付けられたアップリンク ポート。この vNIC に対するすべてのトラフィックは、このアップリンク ポートを通過します。
[MACアドレス（MAC Address）] フィールド	vNIC に関連付けられた MAC アドレス。 アダプタが内部プールから使用可能な MAC アドレスを選択するようにするには、[自動（Auto）] を選択します。アドレスを指定するには、2 番目のオプション ボタンをクリックし、対応するフィールドに MAC アドレスを入力します。

名前	説明
[Class of Service] フィールド	この vNIC からのトラフィックに関連付けられるサービス クラス。 0 ～ 6 の整数を選択します。0 が最も低い優先度で、6 が最も高い優先度になります。 （注） このオプションは VNTAG モードでは使用できません。
[Trust Host CoS] チェックボックス	vNIC で、ホスト オペレーティング システムが提供するサービス クラスを使用できるようにするには、このチェックボックスをオンにします。
[PCI Order] フィールド	この vNIC が使用される順序。 順序を指定するには、表示されている範囲内の整数を入力します。
[デフォルト VLAN (Default VLAN)] オプション ボタン	この vNIC にデフォルトの VLAN がない場合には、**[なし (NONE)]** をクリックします。それ以外の場合は、2 番目のオプション ボタンをクリックし、フィールドに 1 ～ 4094 の VLAN ID を入力します。 （注） このオプションは VNTAG モードでは使用できません。
[VLAN Mode] ドロップダウン リスト	VLAN トランキングを使用する場合は、[TRUNK] を選択します。それ以外の場合は [ACCESS] を選択します。 （注） このオプションは VNTAG モードでは使用できません。

名前	説明
PTP チェックボックスを有効にする	このボックスをチェックして、高精度時間プロトコル（PTP）を有効にします。 精密時間プロトコル（Precision Time Protocol、PTP）は、サーバーのクロックを Linux オペレーティング システム上の他のデバイスや周辺機器と正確に同期します。 PTPによって管理されるクロックは、クライアントとワーカーの階層に従い、ワーカーはマスター クライアントに同期されます。階層は、すべてのクロックで実行されるベストマスター クロック（BMC）アルゴリズムによって更新されます。アダプタごとに 1 つの PTP インターフェイスを有効にして、グランド マスター クロックに同期させる必要があります。 （注） • このオプションは Linux オペレーティング システムのみにサポートされます。 • このオプションは、Cisco UCS VIC 15xxx シリーズ アダプタでのみ使用できます。 このオプションは、シスコ UCS C-Series サーバの一部でのみ使用可能です。 • PTPの有効化の効果を出すには、サーバーの再起動が必要です。

名前	説明
[レート制限 (Rate Limit)] オプション ボタン	この vNIC に無制限のデータ レートを設定するには、[OFF] を選択します。それ以外の場合は、2 番目のオプション ボタンをクリックし、関連するフィールドにレート制限を入力します。 1 ～ 10,000 Mbps の整数を入力します。 VIC 13xx コントローラの場合、1 ～ 40,000 Mbps の整数を入力できます。 VIC 1455 、1457 と 1467コントローラの場合： • アダプタがスイッチ上の 25 Gbps リンクに接続されている場合は、**[レート制限 (Rate Limit)]** フィールドに 1 ~ 25000 Mbps の整数を入力できます。 • アダプタがスイッチ上の 10 Gbps リンクに接続されている場合は、**[レート制限 (Rate Limit)]** フィールドに 1 ~ 10000 Mbps の整数を入力できます。 VIC 14951495、1497 と 1477 コントローラの場合： • アダプタがスイッチ上の 40 Gbps リンクに接続されている場合は、**[レート制限 (Rate Limit)]** フィールドに 1 ~ 40000 Mbps の整数を入力できます。 • アダプタがスイッチ上の 100 Gbps リンクに接続されている場合は、[**レート制限 (Rate Limit**)] フィールドに 1 ~ 100000 Mbps の整数を入力できます。 （注） このオプションは VNTAG モードでは使用できません。
[Channel Number] フィールド	この vNIC に割り当てるチャネル番号を選択します。 （注） このオプションには VNTAG モードが必要です。
[PCI リンク（PCI Link）] フィールド	vNIC を接続可能なリンク。これらは、以下の値です。 • **0** - vNIC が設置されている最初のクロス エッジ リンク。 • **1** - vNIC が設置されている 2 番目のクロス エッジ リンク。 （注） • このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバーだけです。

名前	説明
[NVGRE を有効にする（Enable NVGRE）] チェックボックス	Generic Routing Encapsulation を使用するネットワーク仮想化を有効する場合、このボックスをオンにします。 • このオプションは、シスコ UCS C-Series サーバの一部でのみ使用可能です。 • このオプションは、シスコ VIC 1385 カードを取り付けた C-Series サーバでのみ使用可能です。
[VXLAN を有効にする（Enable VXLAN）] チェックボックス	拡張可能仮想 LAN を有効にする場合、このボックスをオンにします。 • このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバーだけです。 • このオプションは、Cisco VIC 1385 カード、VIC 14xx と VIC 15xxxを搭載したCシリーズサーバーでのみ使用できます。

名前	説明
[Geneve オフロード (Geneve Offload)] チェック ボックス	

名前	説明
	リリース 4.1(2a)以降、Cisco IMC では、ESX 7.0（NSX-T 3.0）および ESX 6.7U3（NSX-T 2.5）OS の Cisco VIC 14xx シリーズと VIC 15xxx アダプタを使用した、汎用ネットワーク仮想カプセル化（Geneve）オフロード機能がサポートされています。 Geneve は、ネットワーク トラフィックのトンネル カプセル化機能です。Cisco VIC 14xx シリーズアダプタで Geneve オフロードのカプセル化を有効にする場合は、このチェックボックスをオンにします。 Geneve オフロードを無効にするには、このチェックボックスをオフにします。これにより、接続先ポート番号が Geneve 宛先ポートと一致するカプセル化されていない UDP パケットが、トンネル パケットとして扱われないようにします。 **Geneve Offload** 機能を有効にすると、次の設定が推奨されます。 • 送信キュー数 = 1 • 送信キュー リング サイズ = 4096 • 受信キュー数 = 8 • 受信キュー リング サイズ = 4096 • 完了キュー数 = 9 • 割り込み数 = 11 （注） Cisco VIC 14xx シリーズのセットアップで **Geneve Offload** が有効になっている場合は、次を有効にできません： • 同じ vNIC 上の RDMA • 同じ vNIC 上の usNIC • Cisco VIC 145x アダプタの非ポート チャネル モード • aRFS • 詳細フィルタ • NetQueue （注） Cisco UCS C220 M7 および C240 M7 サーバーは、Cisco VIC 14xx シリーズをサポートしていません。 （注） Cisco VIC 15xxx のセットアップで **Geneve Offload**

名前	説明
	が有効になっている場合は、次を有効にできません： • aRFS • RoCEv2 外部 IPV6 は、GENEVE Offload 機能ではサポートされていません。 ダウングレードの制限：**Geneve Offload** が有効になっている場合、4.1(2a) より前のリリースにダウングレードすることはできません。
[Advanced Filter] チェックボックス	vNIC の高度なフィルタ オプションを有効にするには、このボックスをオンにします。
[Port Profile] ドロップダウンリスト	vNIC に関連付けられているポート プロファイルを選択します。 このフィールドには、このサーバーが接続しているスイッチに定義されたポート プロファイルが表示されます。 （注） このオプションには VNTAG モードが必要です。
[Enable PXE Boot] チェックボックス	vNIC を使用して PXE ブートを実行する場合は、このチェックボックスをオンにします。
[Enable VMQ] チェックボックス	仮想マシン キュー（VMQ）を有効にするには、このチェックボックスをオンにします。

名前	説明
[マルチキューの有効化（Enable Multi Queue）] チェック ボックス	Vnic でマルチキューオプションを有効にするには、このチェック ボックスをオンにします。有効にすると、マルチ キュー vNIC はホストで使用可能になります。デフォルトでは無効になっています。 （注） • マルチ キューは、14xx と VIC 15xxx アダプタを備えた C-Series サーバーでのみサポートされます。 • このオプションを有効にするには、VMQ が有効な状態である必要があります。 • いずれか 1 つの vNIC でこのオプションを有効にすると、他の vNIC での VNQ のみの設定（マルチキューを選択しない）はサポートされません。 • このオプションを有効にすると、usNIC の設定は無効になります。
[サブvNICの数（No. of Sub vNICs）] フィールド	マルチ キュー オプションが有効になっている場合の、ホストで使用可能なサブ vNIC の数。
[Enable aRFS] チェックボックス	Accelerated Receive Flow steering（aRFS）を有効にする場合、このボックスをオンにします。 このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバーだけです。
[Enable Uplink Failover] チェックボックス	通信の問題が発生した場合に、この vNIC 上のトラフィックをセカンダリ インターフェイスにフェールオーバーするには、このチェックボックスをオンにします。 （注） このオプションには VNTAG モードが必要です。
[Failback Timeout] フィールド	セカンダリ インターフェイスを使用して vNIC が始動した後、その vNIC のプライマリ インターフェイスが再びシステムで使用されるには、プライマリ インターフェイスが一定時間使用可能な状態になっている必要があり、その時間の長さをこの設定で制御します。 0 ～ 600 の範囲の秒数を入力します。 （注） このオプションには VNTAG モードが必要です。

ステップ 6 [Ethernet Interrupt] 領域で、次のフィールドの情報を確認します。

名前	説明
[Interrupt Count] フィールド	割り当てる割り込みリソースの数。通常、この値は、完了キュー リソースの数と同じにします。 1 ～ 1024 の整数を入力します。
[Interrupt Mode] ドロップダウン リスト	優先ドライバ割り込みモード。次のいずれかになります。 • [MSI-X]：機能拡張された Message Signaled Interrupts（MSI）。これは推奨オプションです。 • [MSI]：MSI だけ。 • [INTx]：PCI INTx 割り込み。
[Coalescing Time] フィールド	割り込み間の待機時間、または割り込みが送信される前に必要な休止期間。 1 ～ 65535 の整数を入力します。割り込み調停をオフにするには、このフィールドに 0（ゼロ）を入力します。
[Coalescing Type] ドロップダウン リスト	次のいずれかになります。 • [MIN]：システムは、別の割り込みイベントを送信する前に [Coalescing Time] フィールドに指定された時間だけ待機します。 • [IDLE]：アクティビティなしの期間が少なくとも [Coalescing Time] フィールドに指定された時間続くまで、システムから割り込みは送信されません。

ステップ 7 [TCP Offload] 領域で、次のフィールドの情報を確認します。

名前	説明
[Enable Large Receive] チェックボックス	オンにすると、ハードウェアはすべてのセグメント化されたパケットを CPU に送信する前に再構成します。このオプションにより、CPU の使用率が削減され、インバウンドのスループットが増加する可能性があります。 オフにすると、CPU は大きいパケットをすべて処理します。
[Enable TCP Rx Offload Checksum Validation] チェックボックス	オンにすると、CPU はすべてのパケット チェックサムを検証のためにハードウェアに送信します。このオプションにより、CPU のオーバーヘッドが削減される可能性があります。 オフにすると、CPU はすべてのパケット チェックサムを検証します。

名前	説明
[Enable TCP Segmentation Offload] チェックボックス	オンにすると、CPU はセグメント化する必要がある大きな TCP パケットをハードウェアに送信します。このオプションにより、CPU のオーバーヘッドが削減され、スループット率が向上する可能性があります。 オフにすると、CPUは大きいパケットをセグメント化します。 （注） このオプションは、Large Send Offload（LSO）とも呼ばれています。
[Enable TCP Tx Offload Checksum Generation] チェックボックス	オンにすると、CPU はすべてのパケットをハードウェアに送信し、ハードウェアでチェックサムを計算できるようにします。このオプションにより、CPU のオーバーヘッドが削減される可能性があります。 オフにすると、CPUはすべてのパケット チェックサムを計算します。

ステップ 8 [Receive Side Scaling] 領域で、次のフィールドの情報を確認します。

名前	説明
[Enable TCP Receive Side Scaling] チェックボックス	Receive Side Scaling（RSS）は、ネットワーク受信処理をマルチプロセッサ システム内の複数の CPU に分散させます。 オンにすると、可能な場合はネットワーク受信処理がプロセッサ間で共有されます。 オフにすると、ネットワーク受信処理は、追加のプロセッサが使用可能であっても、常に 1 つのプロセッサで処理されます。
[Enable IPv4 RSS] チェックボックス	オンにすると、RSS が IPv4 ネットワークで有効になります。
[Enable TCP-IPv4 RSS] チェックボックス	オンにすると、IPv4 ネットワーク間の TCP 送信に対して RSS が有効になります。
[Enable IPv6 RSS] チェックボックス	オンにすると、RSS が IPv6 ネットワークで有効になります。
[Enable TCP-IPv6 RSS] チェックボックス	オンにすると、IPv6 ネットワーク間の TCP 送信に対して RSS が有効になります。
[Enable IPv6 Extension RSS] チェックボックス	オンにすると、IPv6 拡張に対して RSS が有効になります。
[Enable TCP-IPv6 Extension RSS] チェックボックス	オンにすると、IPv6 ネットワーク間の TCP 送信に対して RSS がイネーブルになります。

ステップ 9 （注） Cisco UCS C-Series M7 以降のサーバーは **[キュー（Queues）]** タブがあります。

以下を確認します

名前	説明
[Enable VMQ] チェックボックス	仮想マシン キュー（VMQ）を有効にするには、このチェックボックスをオンにします。
[マルチキューの有効化（Enable Multi Queue）] チェック ボックス	Vnic でマルチ キュー オプションを有効にするには、このチェック ボックスをオンにします。有効にすると、マルチ キュー vNIC はホストで使用可能になります。デフォルトでは無効になっています。 • マルチ キューは、14xx と VIC 15xxx アダプタを備えた C-Seriesサーバーでのみサポートされます。 • このオプションを有効にするには、VMQ が有効な状態である必要があります。 • いずれか 1 つの vNIC でこのオプションを有効にすると、他の vNIC での VNQ のみの設定（マルチキューを選択しない）はサポートされません。 • このオプションを有効にすると、usNIC の構成は無効になります。
[Trust Host CoS] チェックボックス	vNIC で、ホスト オペレーティング システムが提供するサービス クラスを使用できるようにするには、このチェックボックスをオンにします。
[サブvNICの数（No. of Sub vNICs）] フィールド	マルチ キュー オプションが有効になっている場合の、ホストで使用可能なサブ vNIC の数。

ステップ 10 （注） Cisco UCS C-Series M7 以降のサーバーでは、**イーサネット受信キュー** は、**[キュー（Queues）]** タブの下で利用可能です。

[Ethernet Receive Queue] 領域で、次のフィールドの情報を確認します。

名前	説明
[Count] フィールド	割り当てる受信キュー リソースの数。 1 ～ 256 の整数を入力します。

名前	説明
[Ring Size] フィールド	各受信キュー内の記述子の数。 64 ～ 4096 の整数を入力します。

ステップ 11 （注） Cisco UCS C-Series M7 以降のサーバーでは、**イーサネット送信キュー** は、**[キュー（Queues）]** タブの下で利用可能です。

[Ethernet Transmit Queue] 領域で、次のフィールドの情報を確認します。

名前	説明
[Count] フィールド	割り当てる送信キュー リソースの数。 1 ～ 256 の整数を入力します。
[Ring Size] フィールド	各送信キュー内の記述子の数。 64 ～ 4096 の整数を入力します。

ステップ 12 （注） Cisco UCS C-Series M7 以降のサーバーでは、**完了キュー** は、**[キュー（Queues）]** タブの下で利用可能です。

[Completion Queue] 領域で、次のフィールドの情報を確認します。

名前	説明
[Count] フィールド	割り当てる完了キュー リソースの数。通常、割り当てなければならない完了キュー リソースの数は、送信キュー リソースの数に受信キュー リソースの数を加えたものと等しくなります。 1 ～ 512 の整数を入力します。
Ring Size	各完了キュー内の記述子の数。 この値は変更できません。

ステップ 13 （注） Cisco UCS C-Series M7 以降のサーバーでは、**マルチ キュー** は、**[キュー（Queues）]** タブの下で利用可能です。

[完了キュー (Completion Queue)] 領域で、次のフィールドの情報を確認します。

名前	説明
[Receive Queue Count] フィールド	割り当てる受信キュー リソースの数。 1 ～ 1000 の整数を入力します。
[Transmit Queue Count] フィールド	割り当てる送信キュー リソースの数。 1 ～ 1000 の整数を入力します。

名前	説明
[Completion Queue Count] フィールド	割り当てる完了キュー リソースの数。通常、割り当てなければならない完了キュー リソースの数は、送信キュー リソースの数に受信キュー リソースの数を加えたものと等しくなります。 1 ～ 2000 の整数を入力します。
[RoCE] チェックボックス	RoCE プロパティを変更するには、このチェックボックスをオンにします。 （注） **[マルチ キュー (Multi Queue)]** RoCE が有効になっている場合は、VMQ RoCE も有効になっていることを確認します。
[Queue Pairs] フィールド	アダプタごとのキュー ペアの数。1 ～ 2048 の整数を入力します。この数値は 2 のべき乗の整数にすることをお勧めします。
[Memory Regions] フィールド	アダプタあたりのメモリ領域の数。1 ～ 524288 の整数を入力します。この数値は 2 のべき乗の整数にすることをお勧めします。
[Resource Groups] フィールド	アダプタごとのリソース グループの数。1 ～ 128 の整数を入力します。最適なパフォーマンスを得るには、この数値は、システムの CPU コアの数以上である、2 のべき乗の整数にすることをお勧めします。
[Class of Service] フィールド	このフィールドは読み取り専用で、5 に設定されます。 （注） このオプションは、一部のアダプタでのみ使用可能です。

ステップ 14 （注） Cisco UCS C-Series M7 以降のサーバーでは、**RoCE プロパティ キュー** は、**[キュー（Queues）]** タブの下で利用可能です。

[全般プロパティ (General Properties)] 領域で、次のフィールドの情報を確認します。

名前	説明
[RoCE] チェックボックス	RoCE プロパティを変更するには、このチェックボックスをオンにします。
[キュー ペア (Queue Pairs)] フィールド	アダプタごとのキュー ペアの数。1 ～ 2048 の整数を入力します。 この数値は 2 のべき乗の整数にすることをお勧めします。vNIC ごとのキュー ペアの値としては 2048 が推奨されます。

名前	説明
[Memory Regions] フィールド	アダプタあたりのメモリ領域の数。1 ～ 524288 の整数を入力します。この数は、2 の整数乗にすることをお勧めします。推奨値は 131072 です。 メモリ領域は主に運用チャネルのセマンティクスを送信するために使用されるため、アプリケーション要件を満たすのに十分なメモリ領域の数がサポートされる必要があります。
[Resource Groups] フィールド	アダプタごとのリソース グループの数。1 ～ 128 の整数を入力します。最適なパフォーマンスを得るには、この数値は、システムの CPU コアの数以上である、2 のべき乗の整数にすることをお勧めします。 リソース グループは WQ、RQ、CQ などのハードウェア リソースの合計数と、RDMA 機能をサポートするために必要となる、ホストで使用可能なプロセッサ コアの合計数に基づく割り込み回数を定義します。最大限のパフォーマンスを引き出すとともに、より有効な不均一メモリ アクセスを実現するために、ホストはコアごとに特定のリソース グループを割り当てます。
[Class of Service] ドロップダウン リスト	指定するドロップ QOS COS はありません。この同じ値は、アップリンク スイッチで設定する必要があります。デフォルトの No Drop QOS COS は 5 です。 （注） このオプションは、一部のアダプタでのみ使用可能です。

ステップ 15 （注） Cisco UCS C-Series M7 以降のサーバーでは、**SR-IOV プロパティ キュー** は、**[キュー（Queues）]** タブの下で利用可能です。

[SR-IOVプロパティ（SR-IOV Properties）] エリアで、次のフィールドの情報を確認します。

名前	説明
VFs フィールドの数	1 ～ 64 の整数を入力します。 （注） 他の SR-IOV プロパティは、1 ～ 64 の整数を入力した場合にのみ有効になります。
[VF あたりの受信キュー数（Receive Queue Count Per VF）] フィールド	割り当てる受信キュー リソースの数。 1 ～ 8 の整数を入力します。
[VF あたりの送信キュー数（Transmit Queue Count Per VF）] フィールド	各送信キュー内の記述子の数。 1 ～ 8 の整数を入力します。

名前	説明
[VF あたりの完了キュー数（Completion Queue Count Per VF）] フィールド	割り当てる完了キュー リソースの数。通常、割り当てなければならない完了キュー リソースの数は、送信キュー リソースの数に受信キュー リソースの数を加えたものと等しくなります。 1 ～ 16 の整数を入力します。
[Interrupt Count] フィールド	割り当てる割り込みリソースの数。通常、この値は、完了キュー リソースの数と同じにします。 1 ～ 16 の整数を入力します。

次のタスク

サーバをリブートして vHBA を作成します。

vNIC のプロパティの変更

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーク（Networking）] メニューをクリックします。

ステップ 2 **[ネットワーキング (Networking)]** ペインで、変更するアダプタ カードを選択します。

ステップ 3 **[アダプタ カード (Adapter Card)]** ペインで、**[vNICs]** タブをクリックします。

ステップ 4 [vNICs] ペインで、[eth0] または [eth1] をクリックします。

ステップ 5 **[vNICs]** ペインの **[vNIC プロパティ (vNIC Properties)]** ペインの **[全般 (General)]** 領域で、次のフィールドを更新します。

名前	説明
[名前（Name）] フィールド	仮想 NIC の名前。 この名前は、vNIC の作成後は変更できません。

名前	説明
[CDN] フィールド	VIC カードのイーサネット vNIC に割り当てられる一貫性のあるデバイス名（CDN）。特定の CDN をデバイスに割り当てると、ホスト OS 上でそれを識別するのに役立ちます。 （注） この機能は [VIC の CDN サポート（CDN Support for VIC）] トークンが BIOS で有効化されている場合にのみ動作します。
[MTU] フィールド	この vNIC で受け入れられる最大伝送単位、つまりパケット サイズ。 1500 ～ 9000 の整数を入力します。
[Uplink Port] ドロップダウン リスト	この vNIC に関連付けられたアップリンク ポート。この vNIC に対するすべてのトラフィックは、このアップリンク ポートを通過します。
[MACアドレス（MAC Address）] フィールド	vNIC に関連付けられた MAC アドレス。 アダプタが内部プールから使用可能な MAC アドレスを選択するようにするには、[自動（Auto）] を選択します。アドレスを指定するには、2 番目のオプション ボタンをクリックし、対応するフィールドに MAC アドレスを入力します。
[Class of Service] フィールド	この vNIC からのトラフィックに関連付けられるサービス クラス。 0 ～ 6 の整数を選択します。0 が最も低い優先度で、6 が最も高い優先度になります。 （注） このオプションは VNTAG モードでは使用できません。
[Trust Host CoS] チェックボックス	vNIC で、ホスト オペレーティング システムが提供するサービス クラスを使用できるようにするには、このチェックボックスをオンにします。
[PCI Order] フィールド	この vNIC が使用される順序。 順序を指定するには、表示されている範囲内の整数を入力します。

名前	説明
[デフォルト VLAN (Default VLAN)] オプション ボタン	この vNIC にデフォルトの VLAN がない場合には、**[なし (NONE)]** をクリックします。それ以外の場合は、2 番目のオプション ボタンをクリックし、フィールドに 1 ～ 4094 の VLAN ID を入力します。 （注） このオプションは VNTAG モードでは使用できません。
[VLAN Mode] ドロップダウン リスト	VLAN トランキングを使用する場合は、[TRUNK] を選択します。それ以外の場合は [ACCESS] を選択します。 （注） このオプションは VNTAG モードでは使用できません。
PTP チェックボックスを有効にする	このボックスをチェックして、高精度時間プロトコル（PTP）を有効にします。 精密時間プロトコル（Precision Time Protocol、PTP）は、サーバーのクロックを Linux オペレーティング システム上の他のデバイスや周辺機器と正確に同期します。 PTP によって管理されるクロックは、クライアントとワーカーの階層に従い、ワーカーはマスター クライアントに同期されます。階層は、すべてのクロックで実行されるベストマスター クロック（BMC）アルゴリズムによって更新されます。アダプタごとに 1 つの PTP インターフェイスを有効にして、グランド マスター クロックに同期させる必要があります。 （注） • このオプションは Linux オペレーティング システムのみにサポートされます。 • このオプションは、Cisco UCS VIC 15xxx シリーズ アダプタでのみ使用できます。 このオプションは、シスコ UCS C-Series サーバの一部でのみ使用可能です。 • PTPの有効化の効果を出すには、サーバーの再起動が必要です。

名前	説明
[レート制限 (Rate Limit)] オプション ボタン	この vNIC に無制限のデータ レートを設定するには、[OFF] を選択します。それ以外の場合は、2 番目のオプション ボタンをクリックし、関連するフィールドにレート制限を入力します。 1 ～ 10,000 Mbps の整数を入力します。 VIC 13xx コントローラの場合、1 ～ 40,000 Mbps の整数を入力できます。 VIC 1455 、1457 と 1467コントローラの場合： • アダプタがスイッチ上の 25 Gbps リンクに接続されている場合は、**[レート制限 (Rate Limit)]** フィールドに 1 ~ 25000 Mbps の整数を入力できます。 • アダプタがスイッチ上の 10 Gbps リンクに接続されている場合は、**[レート制限 (Rate Limit)]** フィールドに 1 ~ 10000 Mbps の整数を入力できます。 VIC 14951495、1497 と 1477 コントローラの場合： • アダプタがスイッチ上の 40 Gbps リンクに接続されている場合は、**[レート制限 (Rate Limit)]** フィールドに 1 ~ 40000 Mbps の整数を入力できます。 • アダプタがスイッチ上の 100 Gbps リンクに接続されている場合は、[**レート制限 (Rate Limit**)] フィールドに 1 ~ 100000 Mbps の整数を入力できます。 （注） このオプションは VNTAG モードでは使用できません。
[Channel Number] フィールド	この vNIC に割り当てるチャネル番号を選択します。 （注） このオプションには VNTAG モードが必要です。
[PCI リンク（PCI Link）] フィールド	vNIC を接続可能なリンク。これらは、以下の値です。 • **0** - vNIC が設置されている最初のクロス エッジ リンク。 • **1** - vNIC が設置されている 2 番目のクロスエッジ リンク。 （注） • このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバーだけです。

名前	説明
[NVGRE を有効にする（Enable NVGRE）] チェックボックス	Generic Routing Encapsulation を使用するネットワーク仮想化を有効する場合、このボックスをオンにします。 • このオプションは、シスコ UCS C-Series サーバの一部でのみ使用可能です。 • このオプションは、シスコ VIC 1385 カードを取り付けた C-Series サーバでのみ使用可能です。
[VXLAN を有効にする（Enable VXLAN）] チェックボックス	拡張可能仮想 LAN を有効にする場合、このボックスをオンにします。 • このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバーだけです。 • このオプションは、Cisco VIC 1385 カード、VIC 14xx と VIC 15xxxを搭載したCシリーズサーバーでのみ使用できます。

名前	説明
[Geneve オフロード (Geneve Offload)] チェック ボックス	

名前	説明
	リリース 4.1(2a)以降、Cisco IMC では、ESX 7.0（NSX-T 3.0）および ESX 6.7U3（NSX-T 2.5）OS の Cisco VIC 14xx シリーズと VIC 15xxx アダプタを使用した、汎用ネットワーク仮想カプセル化（Geneve）オフロード機能がサポートされています。 Geneve は、ネットワーク トラフィックのトンネル カプセル化機能です。Cisco VIC 14xx シリーズアダプタで Geneve オフロードのカプセル化を有効にする場合は、このチェックボックスをオンにします。 Geneve オフロードを無効にするには、このチェックボックスをオフにします。これにより、接続先ポート番号が Geneve 宛先ポートと一致するカプセル化されていない UDP パケットが、トンネル パケットとして扱われないようにします。 **Geneve Offload** 機能を有効にすると、次の設定が推奨されます。 • 送信キュー数 = 1 • 送信キュー リング サイズ = 4096 • 受信キュー数 = 8 • 受信キュー リング サイズ = 4096 • 完了キュー数 = 9 • 割り込み数 = 11 （注） Cisco VIC 14xx シリーズのセットアップで **Geneve Offload** が有効になっている場合は、次を有効にできません： • 同じ vNIC 上の RDMA • 同じ vNIC 上の usNIC • Cisco VIC 145x アダプタの非ポート チャネル モード • aRFS • 詳細フィルタ • NetQueue （注） Cisco UCS C220 M7 および C240 M7 サーバーは、Cisco VIC 14xx シリーズをサポートしていません。 （注） Cisco VIC 15xxx のセットアップで **Geneve Offload**

名前	説明
	が有効になっている場合は、次を有効にできません： • aRFS • RoCEv2 外部 IPV6 は、GENEVE Offload 機能ではサポートされていません。 ダウングレードの制限：**Geneve Offload** が有効になっている場合、4.1(2a) より前のリリースにダウングレードすることはできません。
[Advanced Filter] チェックボックス	vNIC の高度なフィルタ オプションを有効にするには、このボックスをオンにします。
[Port Profile] ドロップダウンリスト	vNIC に関連付けられているポート プロファイルを選択します。 このフィールドには、このサーバーが接続しているスイッチに定義されたポート プロファイルが表示されます。 （注） このオプションには VNTAG モードが必要です。
[Enable PXE Boot] チェックボックス	vNIC を使用して PXE ブートを実行する場合は、このチェックボックスをオンにします。
[Enable VMQ] チェックボックス	仮想マシン キュー（VMQ）を有効にするには、このチェックボックスをオンにします。

名前	説明
[マルチキューの有効化（Enable Multi Queue）] チェック ボックス	Vnic でマルチキューオプションを有効にするには、このチェック ボックスをオンにします。有効にすると、マルチ キュー vNIC はホストで使用可能になります。デフォルトでは無効になっています。 （注） • マルチ キューは、14xx と VIC 15xxx アダプタを備えた C-Series サーバーでのみサポートされます。 • このオプションを有効にするには、VMQ が有効な状態である必要があります。 • いずれか 1 つの vNIC でこのオプションを有効にすると、他の vNIC での VNQ のみの設定（マルチキューを選択しない）はサポートされません。 • このオプションを有効にすると、usNIC の設定は無効になります。
[サブvNICの数（No. of Sub vNICs）] フィールド	マルチ キュー オプションが有効になっている場合の、ホストで使用可能なサブ vNIC の数。
[Enable aRFS] チェックボックス	Accelerated Receive Flow steering（aRFS）を有効にする場合、このボックスをオンにします。 このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバーだけです。
[Enable Uplink Failover] チェックボックス	通信の問題が発生した場合に、この vNIC 上のトラフィックをセカンダリ インターフェイスにフェールオーバーするには、このチェックボックスをオンにします。 （注） このオプションには VNTAG モードが必要です。
[Failback Timeout] フィールド	セカンダリ インターフェイスを使用して vNIC が始動した後、その vNIC のプライマリ インターフェイスが再びシステムで使用されるには、プライマリ インターフェイスが一定時間使用可能な状態になっている必要があり、その時間の長さをこの設定で制御します。 0 ～ 600 の範囲の秒数を入力します。 （注） このオプションには VNTAG モードが必要です。

ステップ 6 [Ethernet Interrupt] 領域で、次のフィールドを更新します。

名前	説明
[Interrupt Count] フィールド	割り当てる割り込みリソースの数。通常、この値は、完了キュー リソースの数と同じにします。 1 ～ 1024 の整数を入力します。
[Coalescing Time] フィールド	割り込み間の待機時間、または割り込みが送信される前に必要な休止期間。 1 ～ 65535 の整数を入力します。割り込み調停をオフにするには、このフィールドに 0（ゼロ）を入力します。
[Coalescing Type] ドロップダウン リスト	次のいずれかになります。 • [MIN]：システムは、別の割り込みイベントを送信する前に [Coalescing Time] フィールドに指定された時間だけ待機します。 • [IDLE]：アクティビティなしの期間が少なくとも [Coalescing Time] フィールドに指定された時間続くまで、システムから割り込みは送信されません。
[Interrupt Mode] ドロップダウン リスト	優先ドライバ割り込みモード。次のいずれかになります。 • [MSI-X]：機能拡張された Message Signaled Interrupts（MSI）。これは推奨オプションです。 • [MSI]：MSI だけ。 • [INTx]：PCI INTx 割り込み。

ステップ 7 [TCP Offload] 領域で、次のフィールドを更新します。

名前	説明
[Enable Large Receive] チェックボックス	オンにすると、ハードウェアはすべてのセグメント化されたパケットを CPU に送信する前に再構成します。このオプションにより、CPU の使用率が削減され、インバウンドのスループットが増加する可能性があります。 オフにすると、CPU は大きいパケットをすべて処理します。
[Enable TCP Segmentation Offload] チェックボックス	オンにすると、CPU はセグメント化する必要がある大きな TCP パケットをハードウェアに送信します。このオプションにより、CPU のオーバーヘッドが削減され、スループット率が向上する可能性があります。 オフにすると、CPUは大きいパケットをセグメント化します。 （注） このオプションは、Large Send Offload（LSO）とも呼ばれています。

名前	説明
[Enable TCP Rx Offload Checksum Validation] チェックボックス	オンにすると、CPU はすべてのパケット チェックサムを検証のためにハードウェアに送信します。このオプションにより、CPU のオーバーヘッドが削減される可能性があります。 オフにすると、CPU はすべてのパケット チェックサムを検証します。
[Enable TCP Tx Offload Checksum Generation] チェックボックス	オンにすると、CPU はすべてのパケットをハードウェアに送信し、ハードウェアでチェックサムを計算できるようにします。このオプションにより、CPU のオーバーヘッドが削減される可能性があります。 オフにすると、CPU はすべてのパケット チェックサムを計算します。

ステップ 8 [Receive Side Scaling] 領域で、次のフィールドを更新します。

名前	説明
[Enable TCP Receive Side Scaling] チェックボックス	Receive Side Scaling（RSS）は、ネットワーク受信処理をマルチプロセッサ システム内の複数の CPU に分散させます。 オンにすると、可能な場合はネットワーク受信処理がプロセッサ間で共有されます。 オフにすると、ネットワーク受信処理は、追加のプロセッサが使用可能であっても、常に 1 つのプロセッサで処理されます。
[Enable IPv4 RSS] チェックボックス	オンにすると、RSS が IPv4 ネットワークで有効になります。
[Enable TCP-IPv4 RSS] チェックボックス	オンにすると、IPv4 ネットワーク間の TCP 送信に対して RSS が有効になります。
[Enable IPv6 RSS] チェックボックス	オンにすると、RSS が IPv6 ネットワークで有効になります。
[Enable TCP-IPv6 RSS] チェックボックス	オンにすると、IPv6 ネットワーク間の TCP 送信に対して RSS が有効になります。
[Enable IPv6 Extension RSS] チェックボックス	オンにすると、IPv6 拡張に対して RSS が有効になります。
[Enable TCP-IPv6 Extension RSS] チェックボックス	オンにすると、IPv6 ネットワーク間の TCP 送信に対して RSS が有効になります。

ステップ 9 （注） Cisco UCS C-Series M7 以降のサーバーは **[キュー（Queues）]** タブがあります。

次のことを確認します。

名前	説明
[Enable VMQ] チェックボックス	仮想マシン キュー（VMQ）を有効にするには、このチェックボックスをオンにします。
[マルチキューの有効化（Enable Multi Queue）] チェック ボックス	Vnic でマルチ キュー オプションを有効にするには、このチェックボックスをオンにします。有効にすると、マルチ キュー vNIC はホストで使用可能になります。デフォルトでは無効になっています。 • マルチ キューは、14xx と VIC 15xxx アダプタを備えた C-Seriesサーバーでのみサポートされます。 • このオプションを有効にするには、VMQ が有効な状態である必要があります。 • いずれか 1 つの vNIC でこのオプションを有効にすると、他の vNIC での VNQ のみの設定（マルチキューを選択しない）はサポートされません。 • このオプションを有効にすると、usNIC の構成は無効になります。
[Trust Host CoS] チェックボックス	vNIC で、ホスト オペレーティング システムが提供するサービス クラスを使用できるようにするには、このチェックボックスをオンにします。
[サブvNICの数（No. of Sub vNICs）] フィールド	マルチ キュー オプションが有効になっている場合の、ホストで使用可能なサブ vNIC の数。

ステップ 10 （注） Cisco UCS C-Series M7 以降のサーバーでは、**イーサネット受信キュー** は、**[キュー（Queues）]** タブの下で利用可能です。

[Ethernet Receive Queue]領域で、次のフィールドを更新します。

名前	説明
[Count] フィールド	割り当てる受信キュー リソースの数。 1 ～ 256 の整数を入力します。

名前	説明
[Ring Size] フィールド	各受信キュー内の記述子の数。 64 ～ 16384 の整数を入力します。 VIC 14xx シリーズ アダプタは、最大 4K（4096）のリング サイズをサポートします。 VIC15xxx シリーズのアダプタは、最大 16K のリング サイズをサポートします。

ステップ 11 （注） Cisco UCS C-Series M7 以降のサーバーでは、**イーサネット送信キュー** は、**[キュー（Queues）]** タブの下で利用可能です。

[Ethernet Transmit Queue]領域で、次のフィールドを更新します。

名前	説明
[Count] フィールド	割り当てる送信キュー リソースの数。 1 ～ 256 の整数を入力します。
[Ring Size] フィールド	各送信キュー内の記述子の数。 64 ～ 16384 の整数を入力します。 VIC 14xx シリーズ アダプタは、最大 4K（4096）のリング サイズをサポートします。 VIC15xxx シリーズのアダプタは、最大 16K のリング サイズをサポートします。

ステップ 12 （注） Cisco UCS C-Series M7 以降のサーバーでは、**完了キュー** は、**[キュー（Queues）]** タブの下で利用可能です。

[Completion Queue]領域で、次のフィールドを更新します。

名前	説明
[Count] フィールド	割り当てる完了キュー リソースの数。通常、割り当てなければならない完了キュー リソースの数は、送信キュー リソースの数に受信キュー リソースの数を加えたものと等しくなります。 1 ～ 512 の整数を入力します。
Ring Size	各完了キュー内の記述子の数。 この値は変更できません。

ステップ 13 （注） Cisco UCS C-Series M7 以降のサーバーでは、**マルチ キュー** は、**[キュー（Queues）]** タブの下で利用可能です。

[マルチキュー（Multi Queue）] 領域で、次の詳細情報を更新します。

名前	説明
[Receive Queue Count] フィールド	割り当てる受信キュー リソースの数。 1 ～ 1000 の整数を入力します。
[Transmit Queue Count] フィールド	割り当てる送信キュー リソースの数。 1 ～ 1000 の整数を入力します。
[Completion Queue Count] フィールド	割り当てる完了キュー リソースの数。通常、割り当てなければならない完了キュー リソースの数は、送信キュー リソースの数に受信キュー リソースの数を加えたものと等しくなります。 1 ～ 2000 の整数を入力します。
[RoCE] チェックボックス	RoCE プロパティを変更するには、このチェックボックスをオンにします。 （注） **[マルチ キュー (Multi Queue)]** RoCE が有効になっている場合は、VMQ RoCE も有効になっていることを確認します。
[Queue Pairs] フィールド	アダプタごとのキュー ペアの数。1 ～ 2048 の整数を入力します。この数値は 2 のべき乗の整数にすることをお勧めします。
[Memory Regions] フィールド	アダプタあたりのメモリ領域の数。1 ～ 524288 の整数を入力します。この数値は 2 のべき乗の整数にすることをお勧めします。
[Resource Groups] フィールド	アダプタごとのリソース グループの数。1 ～ 128 の整数を入力します。最適なパフォーマンスを得るには、この数値は、システムの CPU コアの数以上である、2 のべき乗の整数にすることをお勧めします。
[Class of Service] フィールド	このフィールドは読み取り専用で、5 に設定されます。 （注） このオプションは、一部のアダプタでのみ使用可能です。

ステップ 14 （注） Cisco UCS C-Series M7 以降のサーバーでは、**RoCE プロパティ キュー** は、**[キュー（Queues）]** タブの下で利用可能です。

[RoCE プロパティ（RoCE Properties）] 領域で、次のフィールドを更新します。

名前	説明
[RoCE] チェックボックス	RoCEプロパティを変更するには、このチェックボックスをオンにします。 （注） **[マルチ キュー (Multi Queue)]** RoCE が有効になっている場合は、VMQ RoCE も有効になっていることを確認します。
[Queue Pairs] フィールド	アダプタごとのキュー ペアの数。1 ～ 2048 の整数を入力します。この数値は2のべき乗の整数にすることをお勧めします。
[Memory Regions] フィールド	アダプタあたりのメモリ領域の数。1 ～ 524288 の整数を入力します。この数値は 2 のべき乗の整数にすることをお勧めします。
[Resource Groups] フィールド	アダプタごとのリソース グループの数。1 ～ 128 の整数を入力します。最適なパフォーマンスを得るには、この数値は、システムの CPU コアの数以上である、2 のべき乗の整数にすることをお勧めします。
[Class of Service] フィールド	このフィールドは読み取り専用で、5 に設定されます。 （注） このオプションは、一部のアダプタでのみ使用可能です。

ステップ 15 （注） Cisco UCS C-Series M7 以降のサーバーでは、**SR-IOV プロパティ キュー** は、**[キュー（Queues）]** タブの下で利用可能です。

[SR-IOVプロパティ（SR-IOV Properties）] エリアで、次のフィールドの情報を確認します。

名前	説明
VFs フィールドの数	1 ～ 64 の整数を入力します。 （注） 他の SR-IOV プロパティは、1 ～ 64 の整数を入力した場合にのみ有効になります。
[VF あたりの受信キュー数（Receive Queue Count Per VF）] フィールド	割り当てる受信キュー リソースの数。 1 ～ 8 の整数を入力します。
[VF あたりの送信キュー数（Transmit Queue Count Per VF）] フィールド	各送信キュー内の記述子の数。 1 ～ 8 の整数を入力します。

名前	説明
[VF あたりの完了キュー数（Completion Queue Count Per VF）] フィールド	割り当てる完了キュー リソースの数。通常、割り当てなければならない完了キュー リソースの数は、送信キュー リソースの数に受信キュー リソースの数を加えたものと等しくなります。 1 ～ 16 の整数を入力します。
[Interrupt Count] フィールド	割り当てる割り込みリソースの数。通常、この値は、完了キュー リソースの数と同じにします。 1 ～ 16 の整数を入力します。

ステップ 16 [Save Changes] をクリックします。

次のタスク

サーバーを再起動して、vNIC を変更します。

vNIC の作成

Cisco UCS 仮想インターフェイス カードには、デフォルトで 2 個の vHBA と 2 個の vNIC が用意されています。これらのアダプタ カードに最大 14 個の vHBA または vNIC を追加作成できます。

Cisco UCS 1455、1457、および 1467 仮想インターフェイス カードは、非ポートチャネル モードで、デフォルトで 4 個の vHBAs と4 個の Vhbas を提供します。これらのアダプタ カードに最大 10 個の vHBA または vNICs を追加作成できます。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーク（Networking）] メニューをクリックします。

ステップ 2 **[ネットワーキング (Networking)]** ペインで、変更するアダプタ カード を選択します。

ステップ 3 **[アダプタ カード (Adapter Card)]** ペインで、**[vNICs]** タブをクリックします。

ステップ 4 [Host Ethernet Interfaces] 領域で、次のアクションのいずれかを選択します。

- デフォルトの設定を使用して vNIC を作成するには、**[vNIC の追加（Add vNIC）]** をクリックします。
- 既存の vNIC と同じ設定を使用して vNIC を作成するには、既存の vNIC を選択し、**[vNIC の複製（Clone vNIC）]**をクリックします。

[Add vNIC] ダイアログボックスが表示されます。

ステップ 5 **[Add vNIC]** ダイアログボックスで、vNIC の名前を **[Name]** 入力ボックスに入力します。

ステップ 6 [Add vNIC] ダイアログボックスで、vNIC のチャネル番号を [Channel Number] 入力ボックスに入力します。

（注） アダプタで VNTAG が有効になっている場合、vNIC を作成するときに vNIC のチャネル番号を割り当てる必要があります。

ステップ 7 [Add vNIC] をクリックします。

次のタスク

設定の変更が必要な場合は、vNIC のプロパティの変更 （266 ページ）の説明に従って、新しい vNIC を設定します。

vNIC の削除

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーク（Networking）] メニューをクリックします。

ステップ 2 **[ネットワーキング (Networking)]** ペインで、変更するアダプタ カード を選択します。

ステップ 3 **[アダプタ カード (Adapter Card)]** ペインで、**[vNICs]** タブをクリックします。

ステップ 4 [Host Ethernet Interfaces] 領域で、表から vNIC を選択します。

（注） デフォルトの 2 つの vNIC（**[eth0]** と **[eth1]** ）は、どちらも削除することはできません。

ステップ 5 **[vNIC の削除（Delete vNIC）]**をクリックし、削除することを確認するために**[OK]**をクリックします。

iSCSI ブート機能の設定

vNIC の iSCSI ブート機能の設定

vNIC で iSCSI ブート機能を設定する方法は、次のとおりです。

- このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。
- iSCSI ストレージ ターゲットからサーバをリモートでブートするように vNIC を設定するには、vNIC の PXE ブート オプションを有効にする必要があります。

（注） ホストごとに最大 2 つの iSCSI vNIC を設定できます。

vNIC 上の iSCSI ブート機能の設定

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーク（Networking）] メニューをクリックします。

ステップ 2 **[ネットワーキング (Networking)]** ペインで、変更するアダプタ カードを選択します。

ステップ 3 **[アダプタ カード (Adapter Card)]** ペインで、**[vNICs]** タブをクリックします。

ステップ 4 [vNICs] ペインで、[eth0] または [eth1] をクリックします。

ステップ 5 **[iSCSI ブート プロパティ (iSCSI Boot Properties)]** 領域を選択します。

ステップ 6 **[一般（General ）]** エリアで、次のフィールドを更新します：

名前	説明
[名前（Name）] フィールド	vNIC の名前。
[DHCP ネットワーク（DHCP Network）] チェックボックス	vNIC に対して DHCP ネットワークが有効かどうか。 有効にすると、イニシエータのネットワーク構成が DHCP サーバから取得されます。
[DHCP iSCSI] チェックボックス	vNIC に対して DHCP iSCSI が有効かどうか。これを有効にして DHCP ID が設定されている場合、イニシエータ IQN とターゲットの情報が DHCP サーバから取得されます。 （注） DHCP iSCSI が DHCP ID なしで有効化されている場合は、ターゲット情報のみが取得されます。
[DHCP ID] フィールド	イニシエータ IQN とターゲットの情報を DHCP サーバから取得するためにアダプタが使用するベンダー識別文字列。 最大 64 文字の文字列を入力します。
[DHCP Timeout] フィールド	イニシエータが DHCP サーバーが使用できないと判断するまでに待機する秒数。 60 ～ 300 の整数を入力します（デフォルト：60 秒）。
[リンク タイムアウト（Link Timeout）] フィールド	イニシエータがリンクが使用できないと判断するまでに待機する秒数。 0 ～ 255 の整数を入力します（デフォルト：15 秒）。

名前	説明
[LUN 再試行回数値の入力] フィールド	iSCSI LUN 検出中にエラーが発生した場合に接続を再試行する回数。 0 ～ 255 の整数を入力します。デフォルトは 15 です。
[IP バージョン（IP Version）] フィールド	iSCSI のブート中に使用する IP のバージョン。

ステップ 7 **[イニシエータ（Initiator）]** エリアで、次のフィールドを更新します：

名前	説明
[名前（Name）] フィールド	iSCSI イニシエータ名を定義する正規表現。 任意の英数字および次の特殊文字を入力できます。 • .（ピリオド） • :（コロン） • -（ダッシュ） （注） 名前は、IQN 形式です。
[IP Address] フィールド	iSCSI イニシエータの IP アドレス。
[サブネットマスク（Subnet Mask）] フィールド	iSCSI イニシエータのサブネット マスク。
[ゲートウェイ（Gateway）] フィールド	デフォルト ゲートウェイ。
[プライマリ DNS（Primary DNS）] フィールド	プライマリ DNS サーバーのアドレス。
[優先度 (Priority)] ドロップダウン リスト	イニシエータの優先順位ドロップダウン リスト。
[Secondary DNS] フィールド	セカンダリ DNS サーバー アドレス。
[TCP タイムアウト（TCP Timeout）] フィールド	イニシエータによって TCP が使用不可であると判断されるまでに待機する秒数。 0 ～ 255 の整数を入力します（デフォルト：15 秒）。
[CHAP 名（CHAP Name）] フィールド	イニシエータの Challenge Handshake Authentication Protocol（CHAP）の名前。
[CHAP 機密（CHAP Secret）] フィールド	イニシエータの Challenge Handshake Authentication Protocol（CHAP）の共有秘密。

ステップ 8 **[プライマリ ターゲット（Primary Target）]** エリアで、次のフィールドを更新します：

名前	説明
[名前（Name）] フィールド	IQN 形式のプライマリ ターゲットの名前。
[IP Address] フィールド	ターゲットの IP アドレス。
[TCP ポート（TCP Port）] フィールド	ターゲットに関連付けられている TCP ポート。
[ブート LUN（Boot LUN）] フィールド	ターゲットに関連付けられているブート LUN。
[CHAP 名（CHAP Name）] フィールド	イニシエータの Challenge Handshake Authentication Protocol（CHAP）の名前。
[CHAP 機密（CHAP Secret）] フィールド	イニシエータの Challenge Handshake Authentication Protocol（CHAP）の共有秘密。

ステップ 9 **[セカンダリ ターゲット（Secondary Target）]** エリアで、次のフィールドを更新します：

名前	説明
[名前（Name）] フィールド	IQN 形式のセカンダリ ターゲットの名前。
[IP Address] フィールド	ターゲットの IP アドレス。
[TCP ポート（TCP Port）] フィールド	ターゲットに関連付けられている TCP ポート。
[ブート LUN（Boot LUN）] フィールド	ターゲットに関連付けられているブート LUN。
[CHAP 名（CHAP Name）] フィールド	イニシエータの Challenge Handshake Authentication Protocol（CHAP）の名前。
[CHAP 機密（CHAP Secret）] フィールド	イニシエータの Challenge Handshake Authentication Protocol（CHAP）の共有秘密。

名前	説明
[iSCSI を設定（Configure ISCSI）] ボタン	選択された vNIC で iSCSI ブートを設定します。
[iSCSI を設定解除（Unconfigure ISCSI）] ボタン	選択された vNIC の設定を削除します。
[Reset Values]ボタン	vNIC の値を、このダイアログボックスを最初に開いたときに有効だった設定に復元します。

名前	説明
[Cancel] ボタン	変更を行わずにダイアログボックスを閉じます。

ステップ 10 **[Save Changes]**をクリックします。

vNIC からの iSCSI ブート設定の除去

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーク（Networking）] メニューをクリックします。

ステップ 2 **[ネットワーキング (Networking)]** ペインで、変更するアダプタ カード を選択します。

ステップ 3 **[アダプタ カード (Adapter Card)]** ペインで、**[vNICs]** タブをクリックします。

ステップ 4 [vNICs] ペインで、[eth0] または [eth1] をクリックします。

ステップ 5 **[iSCSI ブート プロパティ (iSCSI Boot Properties)]** 領域を選択します。

ステップ 6 **[iSCSI ブート プロパティ (iSCSI Boot Properties)]** 領域下部にある **[ISCSI の構成解除 (Unconfigure ISCSI)]** ボタンをクリックします。

次のタスク

サーバーを再起動して、iSCSI ブート構成を削除します。

Cisco usNIC の管理

Cisco usNIC の概要

The Cisco user-space NIC (Cisco usNIC) 機能は、ネットワーキング パケットを送受信するときにカーネルをバイパスすることで、データセンターの Cisco UCS サーバーで実行されるソフトウェア アプリケーションのパフォーマンスを改善します。アプリケーションは Cisco UCS VIC 1225 などの Cisco UCS VIC 第 2 世代以降のアダプタと直接やり取りし、これによってハイ パフォーマンス コンピューティング クラスタのネットワーキング パフォーマンスが向上します。Cisco usNIC のメリットを享受するには、ソケットやその他の通信 API ではなく、Message Passing Interface（MPI）をアプリケーションで使用する必要があります。

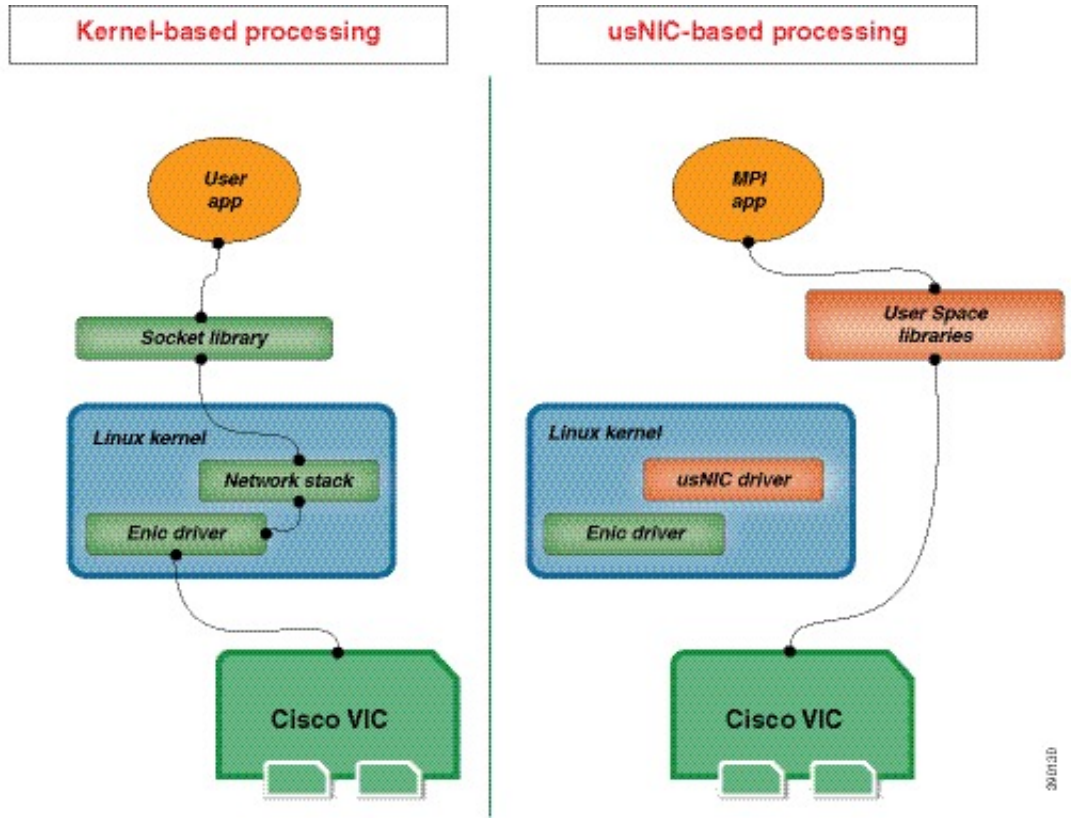
Cisco usNIC を使用すると、MPI アプリケーションで次の利点が得られます。

- 低遅延で、高スループットの通信転送を提供します。

- 標準のアプリケーション非依存イーサネット プロトコルを採用しています。
- 次に示すシスコ データセンター プラットフォームで、低遅延の転送、ユニファイド ファブリック、統合管理のサポートを活用します。
  - Cisco UCS サーバー
  - Cisco UCS 第二世代以降の VIC アダプタ
  - 10 または 40GbE ネットワーク

標準イーサネットアプリケーションは、Linux カーネルのネットワーキング スタックを呼び出すユーザ領域のソケット ライブラリを使用します。次に、ネットワーキング スタックは Cisco eNIC ドライバを使用して、Cisco VIC ハードウェアと通信します。次の図は、通常のソフトウェア アプリケーションと Cisco usNIC を使用する MPI アプリケーションの対比を示します。

Figure 1: カーネル ベースのネットワーク通信と ***Cisco usNIC*** ベースの通信



Cisco IMC GUI を使用した Cisco usNIC の表示および設定

始める前に

このタスクを実行するには、管理権限を持つユーザーとして Cisco IMC GUI にログインする必要があります。このビデオの [再生 (Play)] をクリックして、Cisco IMC で Cisco usNIC を設定する方法を視聴します。

手順

ステップ 1 [Cisco IMC GUI] にログインします。

Cisco IMC へのログイン方法に関する詳細については、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』を参照してください。

ステップ 2 [ナビゲーション（Navigation）] ペインの [ネットワーク（Networking）] メニューをクリックします。

ステップ 3 **[ネットワーキング (Networking)]** ペインで、変更するアダプタ カードを選択します。

ステップ 4 **[アダプタ カード (Adapter Card)]** ペインで、**[vNICs]** タブをクリックします。

ステップ 5 [vNICs] ペインで、[eth0] または [eth1] をクリックします。

ステップ 6 **[usNIC]** 領域で、次のフィールドを確認して更新します。

名前	説明
[名前（Name）]	usNIC の親である vNIC の名前。 （注） このフィールドは読み取り専用です。
[usNIC] フィールド	特定の vNIC に割り当てられる usNIC の数。 0 ～ 225 の整数を入力します。 指定の vNIC に追加の usNIC を割り当てるには、既存の値よりも高い値を入力してください。 指定の vNIC から usNIC を削除するには、既存の値よりも小さい値を入力します。 vNIC に割り当てられたすべての usNIC を削除するには、ゼロを入力します。
[Transmit Queue Count] フィールド	割り当てる送信キュー リソースの数。 1 ～ 256 の整数を入力します。
[Receive Queue Count] フィールド	割り当てる受信キュー リソースの数。 1 ～ 256 の整数を入力します。

名前	説明
[Completion Queue Count] フィールド	割り当てる完了キュー リソースの数。通常、割り当てなければならない完了キュー リソースの数は、送信キュー リソースの数に受信キュー リソースの数を加えたものと等しくなります。 1 ～ 512 の整数を入力します。
[Transmit Queue Ring Size] フィールド	各送信キュー内の記述子の数。 64 ～ 4096 の整数を入力します。
[Receive Queue Ring Size] フィールド	各受信キュー内の記述子の数。 64 ～ 4096 の整数を入力します。
[Interrupt Count] フィールド	割り当てる割り込みリソースの数。通常、この値は、完了キュー リソースの数と同じにします。 1 ～ 514 の整数を入力します。
[Interrupt Coalescing Type] ドロップダウン リスト	次のいずれかになります。 • [MIN]：システムは、別の割り込みイベントを送信する前に [Coalescing Time] フィールドに指定された時間だけ待機します。 • [IDLE]：アクティビティなしの期間が少なくとも [Coalescing Time] フィールドに指定された時間続くまで、システムから割り込みは送信されません。
[Interrupt Coalescing Timer Time] フィールド	割り込み間の待機時間、または割り込みが送信される前に必要な休止期間。 1 ～ 65535 の整数を入力します。割り込み調停をオフにするには、このフィールドに 0（ゼロ）を入力します。
[Class of Service] フィールド	この usNIC からのトラフィックに関連付けられるサービス クラス。 0 ～ 6 の整数を選択します。0 が最も低い優先度で、6 が最も高い優先度になります。 （注） このオプションは VNTAG モードでは使用できません。

名前	説明
[TCP Segment Offload] チェックボックス	オンにすると、CPU はセグメント化する必要がある大きな TCP パケットをハードウェアに送信します。このオプションにより、CPU のオーバーヘッドが削減され、スループット率が向上する可能性があります。 オフにすると、CPU は大きいパケットをセグメント化します。 （注） このオプションは、Large Send Offload（LSO）とも呼ばれています。
[Large Receive] チェックボックス	オンにすると、ハードウェアはすべてのセグメント化されたパケットを CPU に送信する前に再構成します。このオプションにより、CPU の使用率が削減され、インバウンドのスループットが増加する可能性があります。 オフにすると、CPU は大きいパケットをすべて処理します。
[TCP Tx Checksum] チェックボックス	オンにすると、CPUはすべてのパケットをハードウェアに送信し、ハードウェアでチェックサムを計算できるようにします。このオプションにより、CPU のオーバーヘッドが削減される可能性があります。 オフにすると、CPU はすべてのパケット チェックサムを計算します。
[TCP Rx Checksum] チェックボックス	オンにすると、CPU はすべてのパケット チェックサムを検証のためにハードウェアに送信します。このオプションにより、CPU のオーバーヘッドが削減される可能性があります。 オフにすると、CPU はすべてのパケット チェックサムを検証します。

ステップ 7 [Save Changes] をクリックします。

変更内容は次のサーバのリブート時に有効になります。

usNIC プロパティの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーク（Networking）] メニューをクリックします。

ステップ 2 **[ネットワーキング（Networking）]** ペインで、表示するアダプタ カードを選択します。

ステップ 3 **[アダプタ カード (Adapter Card)]** ペインで、**[vNICs]** タブをクリックします。

ステップ 4 [vNICs] ペインで、[eth0] または [eth1] をクリックします。

ステップ 5 [Host Ethernet Interfaces] ペインの [usNIC Properties] 領域で、次のフィールドの情報を確認します。

名前	説明
名前（Name）	usNIC の親である vNIC の名前。 （注） このフィールドは読み取り専用です。
[usNIC] フィールド	特定の vNIC に割り当てられる usNIC の数。 0 ～ 225 の整数を入力します。 指定の vNIC に追加の usNIC を割り当てるには、既存の値より大きい値を入力してください。 指定の vNIC から usNIC を削除するには、既存の値より小さい値を入力してください。 vNIC に割り当てられたすべての usNIC を削除するには、ゼロを入力します。
[Transmit Queue Count]フィールド	割り当てる送信キュー リソースの数。 1 ～ 256 の整数を入力します。
[Receive Queue Count] フィールド	割り当てる受信キュー リソースの数。 1 ～ 256 の整数を入力します。
[Completion Queue Count] フィールド	割り当てる完了キュー リソースの数。通常、割り当てなければならない完了キュー リソースの数は、送信キュー リソースの数に受信キュー リソースの数を加えたものと等しくなります。 1 ～ 512 の整数を入力します。

名前	説明
[Transmit Queue Ring Size] フィールド	各送信キュー内の記述子の数。 64 ～ 4096 の整数を入力します。
[Receive Queue Ring Size] フィールド	各受信キュー内の記述子の数。 64 ～ 4096 の整数を入力します。
[Interrupt Count] フィールド	割り当てる割り込みリソースの数。通常、この値は、完了キュー リソースの数と同じにします。 1 ～ 514 の整数を入力します。
[Interrupt Coalescing Type] ドロップダウン リスト	次のいずれかになります。 • [MIN]：システムは、別の割り込みイベントを送信する前に [Coalescing Time] フィールドに指定された時間だけ待機します。 • [IDLE]：アクティビティなしの期間が少なくとも [Coalescing Time] フィールドに指定された時間続くまで、システムから割り込みは送信されません。
[Interrupt Coalescing Timer Time] フィールド	割り込み間の待機時間、または割り込みが送信される前に必要な休止期間。 1 ～ 65535 の整数を入力します。割り込み調停をオフにするには、このフィールドに 0（ゼロ）を入力します。
[Class of Service] フィールド	この usNIC からのトラフィックに関連付けるサービス クラス。 0 ～ 6 の整数を選択します。0 が最も低い優先度で、6 が最も高い優先度になります。 （注） このオプションは VNTAG モードでは使用できません。

名前	説明
[TCP Segment Offload] チェックボックス	オンにすると、CPU はセグメント化する必要がある大きな TCP パケットをハードウェアに送信します。このオプションにより、CPU のオーバーヘッドが削減され、スループット率が向上する可能性があります。 オフにすると、CPU は大きいパケットをセグメント化します。 （注） このオプションは、Large Send Offload（LSO）とも呼ばれています。
[Large Receive] チェックボックス	オンにすると、ハードウェアはすべてのセグメント化されたパケットを CPU に送信する前に再構成します。このオプションにより、CPU の使用率が削減され、インバウンドのスループットが増加する可能性があります。 オフにすると、CPU は大きいパケットをすべて処理します。
[TCP Tx Checksum] チェックボックス	オンにすると、CPUはすべてのパケットをハードウェアに送信し、ハードウェアでチェックサムを計算できるようにします。このオプションにより、CPU のオーバーヘッドが削減される可能性があります。 オフにすると、CPU はすべてのパケットチェックサムを計算します。
[TCP Rx Checksum] チェックボックス	オンにすると、CPU はすべてのパケットチェックサムを検証のためにハードウェアに送信します。このオプションにより、CPU のオーバーヘッドが削減される可能性があります。 オフにすると、CPU はすべてのパケットチェックサムを検証します。

アダプタ設定のバックアップと復元

アダプタ設定のエクスポート

アダプタ設定は、次のいずれかのリモート サーバに XML ファイルとしてエクスポートできます。

- TFTP
- FTP
- SFTP
- SCP
- HTTP

始める前に

リモート サーバの IP アドレスを取得します。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーク（Networking）] メニューをクリックします。

ステップ 2 **[ネットワーキング (Networking)]** ペインで、変更するアダプタ カードを選択します。

ステップ 3 **[アダプタ カード (Adapter Card)]** ペインで、**[全般 (General)]** タブをクリックします。

ステップ 4 **全般 (General)** タブの **[アクション (Actions)]** 領域で、**[vNIC のエクスポート (Export vNIC)]** をクリックします。

[(vNIC のエクスポート (Export vNIC)] ダイアログボックスが開きます。

ステップ 5 [Export Adapter Configuration] ダイアログボックスで、次のフィールドを更新します。

名前	説明
[Export To] ドロップダウン リスト	リモート サーバーのタイプ。次のいずれかになります。 • **[TFTP サーバー（TFTP Server）]** • **FTP サーバー（FTP Server）** • **SFTP サーバー（SFTP Server）** • **SCP サーバー（SCP Server）** • **HTTP サーバー（HTTP Server）** （注） このアクションを実行中にリモート サーバのタイプとしてSCPまたはSFTPを選択した場合、ポップアップ ウィンドウが表示され、そこに *[*サーバ（*RSA*）鍵フィンガープリントは *<server_finger_print _ID>* です。続行しますか*?*（*Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*）*]* というメッセージが表示されます。サーバフィンガープリントの信頼度に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。
[IP アドレスまたはホスト名 (IP Address or Host Name)] フィールド	アダプタ設定ファイルのエクスポート先となるサーバーの IPv4 アドレスか IPv6 アドレス、またはホスト名。[エクスポート先（Export to）] ドロップダウン リストの設定によって、フィールド名は異なる場合があります。
[パスおよびファイル名（Path and Filename）] フィールド	ファイルをリモート サーバーにエクスポートするときに、Cisco IMC が使用する必要のあるパスおよびファイル名。
ユーザ名	システムがリモート サーバへのログインに使用する必要のあるユーザ名。プロトコルが TFTP または HTTP の場合、このフィールドは適用されません。
パスワード	リモート サーバのユーザ名のパスワード。プロトコルが TFTP または HTTP の場合、このフィールドは適用されません。

ステップ 6 **[vNIC のエクスポート (Export vNIC)]** をクリックします。

アダプタ設定のインポート

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーク（Networking）] メニューをクリックします。

ステップ 2 **[ネットワーキング (Networking)]** ペインで、変更するアダプタ カード を選択します。

ステップ 3 [General] タブを選択します。

ステップ 4 **全般 (General)** タブの **[アクション (Actions)]** 領域で、**[vNIC のインポート (Import vNIC)]** をクリックします。

[vNIC のインポート (Import vNIC)] ダイアログ ボックスが表示されます。

ステップ 5 **[vNIC のインポート (Import vNIC)]** ダイアログ ボックスで、次のフィールドに値を入力します。

名前	説明
[インポート元（Import from）] ドロップダウン リスト	リモート サーバのタイプ。次のいずれかになります。 • **[TFTP サーバー（TFTP Server）]** • **FTP サーバー（FTP Server）** • **SFTP サーバー（SFTP Server）** • **SCP サーバー（SCP Server）** • **HTTP サーバー（HTTP Server）** （注） このアクションを実行中にリモート サーバのタイプとしてSCPまたはSFTPを選択した場合、ポップアップ ウィンドウが表示され、そこに *[サーバ（RSA）鍵フィンガープリントは <server_finger_print _ID> です。続行しますか?（Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?）]* というメッセージが表示されます。サーバフィンガープリントの信頼度に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。
[IP アドレスまたはホスト名 (IP Address or Host Name)] フィールド	アダプタ設定ファイルが存在するサーバーの IPv4 アドレスか IPv6 アドレス、またはホスト名。[インポート元（Import from）] ドロップダウン リストの設定によって、フィールド名は異なる場合があります。

名前	説明
[パスおよびファイル名（Path and Filename）] フィールド	リモート サーバー上の設定ファイルのパスおよびファイル名。
ユーザ名	システムがリモート サーバへのログインに使用する必要のあるユーザ名。プロトコルが TFTP または HTTP の場合、このフィールドは適用されません。
パスワード	リモート サーバのユーザ名のパスワード。プロトコルが TFTP または HTTP の場合、このフィールドは適用されません。

ステップ 6 **[vNIC のインポート (Import vNIC)]** をクリックします。

次のタスク

サーバーをリブートして、インポートした設定を適用します。

アダプタのデフォルトの復元

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーク（Networking）] メニューをクリックします。

ステップ 2 **[ネットワーキング (Networking)]** ペインで、デフォルト設定に復元するアダプタ カードを選択します。

ステップ 3 [General] タブを選択します。

ステップ 4 [General] タブの [Actions] 領域で、[Reset To Defaults] をクリックし、[OK] をクリックして確定します。

アダプタのリセット

手順

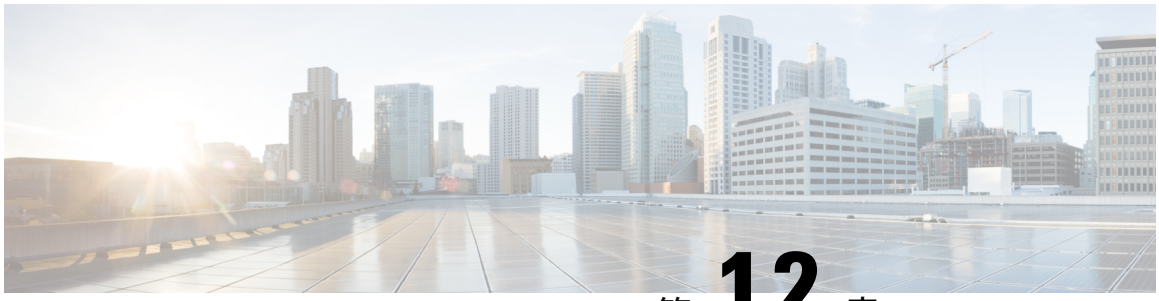
ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーク（Networking）] メニューをクリックします。

ステップ 2 **[ネットワーキング (Networking)]** ペインで、リセットするアダプタ カードを選択します。

ステップ 3 [General] タブを選択します。

ステップ 4 **[全般（General）]** タブの **[アクション（Actions）]** エリアで、**[リセット（Reset）]** をクリックし、**[OK]** をクリックして確定します。

（注） アダプタをリセットすると、ホストもリセットされます。



第 12 章

ストレージ アダプタの管理

この章は、次の内容で構成されています。

ストレージ アダプタの管理

自己暗号化ドライブ（フル ディスク暗号化）

Cisco IMC は、自己暗号化ドライブ（SED）をサポートしています。ドライブ内の特別なハードウェアがリアルタイムで入力データを暗号化し、出力データを復号します。この機能は、フル ディスク暗号化（FDE）とも呼ばれます。

ドライブ上のデータは、ドライブに入力される際に暗号化され、出力される際に復号されます。ただし、ドライブをロックしている場合は、データを取得するためにセキュリティ キーは必要ありません。

ドライブがロックされると、暗号化キーが内部で作成され保存されます。このドライブに保存されているすべてのデータは、そのキーを使用して暗号化され、暗号化された形式で保存されます。データをこのように保存すると、データを非暗号化してドライブから取得するためにセキュリティ キーが必要になります。ドライブのロックを解除すると、その暗号化キーが削除され、保存されたデータは使用できなくなります。これは、Secure Erase と呼ばれます。FDE は、キー ID とセキュリティ キーで構成されます。

FDE 機能は次の操作をサポートしています。

- コントローラでのセキュリティの有効化および無効化
- セキュアな仮想ドライブの作成
- 非セキュアなドライブ グループの保護

- 外部の設定ドライブのロック解除
- 物理ドライブ（JBOD）でのセキュリティの有効化
- セキュアな SED ドライブのクリア
- セキュアな外部設定のクリア

デュアルまたは複数のコントローラの環境でコントローラ セキュリティを設定する場合に考慮すべきシナリオ

（注） デュアルまたは複数のコントローラの接続は一部のサーバーでのみ使用できます。

コントローラのセキュリティは、個別に有効、無効、または変更できます。ただし、ローカル キー管理とリモート キー管理は、サーバー上のすべてのコントローラに適用されます。したがって、キー管理モードの切り替えを伴うセキュリティ アクションは慎重に行う必要があります。両方のコントローラが安全で、コントローラの1つを別のモードに移動する場合は、もう一方のコントローラでも同じ操作を実行する必要があります。

次の 2 つのシナリオを考えてみましょう。

- シナリオ 1：キー管理はリモートに設定されています。両方のコントローラは安全で、リモート キー管理を使用します。ローカル キー管理に切り替える場合は、各コントローラのキー管理を切り替えて、リモート キー管理を無効にします。
- シナリオ2：キー管理はローカルに設定されています。両方のコントローラは安全で、ローカル キー管理を使用します。リモート キー管理に切り替える場合は、リモート キー管理を有効にして、各コントローラのキー管理を切り替えます。

いずれかのコントローラでコントローラ セキュリティ方式を変更しないと、セキュアなキー管理がサポートされていない設定状態になります。

コントローラ セキュリティの有効化

このオプションを使用できるのは一部の C シリーズ サーバーだけです。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。
ステップ 2 [Storage] メニューで、適切な LSI MegaRAID もしくは HBA コントローラをクリックします。
ステップ 3 [Controller Info] 領域で、[Enable Drive Security] をクリックします。
ステップ 4 [Enable Drive Security] ダイアログボックスで、次のフィールドを更新します。

名前	説明
[Controller Security] フィールド	コントローラが無効であることを示します。
[Key Management] フィールド	キーをリモートで管理するかローカルで管理するかを指定します。次のいずれかになります。 • [リモート キー管理（Remote Key Management）] オプション ボタン：リモート KMIP サーバを使用して、コントローラのセキュリティ キーを設定または管理します。 （注） このオプションを選択すると、既存のセキュリティ キーを指定する必要はなくなりますが、キー ID とローカル管理用のセキュリティ キーの入力が必要になります。 • [ローカル キー管理（Local Key Management）] オプション ボタン：コントローラ セキュリティ キーをローカルで設定します。
[セキュリティ キー ID（Security Key Identifier）] フィールド	現在のキー ID。
[セキュリティ キー（Security Key）] フィールド	コントローラのセキュリティを有効にする際に使用するセキュリティ キーです。現在のセキュリティ キーを変更する場合は、このフィールドに新しいキーを入力します。 （注） セキュリティ キーを変更すると、[セキュア キーの検証（Secure Key Verification）] ポップアップ ウィンドウが表示されます。このウィンドウに現在のセキュリティ キーを入力してキーの検証を行う必要があります。
[セキュリティ キーの確認（Confirm Security Key）] フィールド	セキュリティ キーを再度入力します。
[提案（Suggest）] ボタン	割り当てることができるセキュリティ キーまたはキー ID を提案します。

ステップ 5 **[Save]** をクリックします。

これにより、コントローラのセキュリティが有効になります。

コントローラ セキュリティの変更

このオプションを使用できるのは一部の C シリーズ サーバーだけです。

始める前に

- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。
- コントローラ セキュリティを変更するには、最初に有効にしておく必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。

ステップ 2 [Storage] メニューで、適切な LSI MegaRAID もしくは HBA コントローラをクリックします。

ステップ 3 [Controller Info] 領域で、[Modify Drive Security] をクリックします。

ステップ 4 [Modify Drive Security] ダイアログボックスで、次のフィールドを更新します。

名前	説明
[コントローラセキュリティ（Controller Security）] フィールド	コントローラ セキュリティが有効になっているかどうかを示します。次のいずれかになります。 • **有効**— コントローラ セキュリティが有効です。 • **無効**—コントローラ セキュリティが無効です。
[セキュリティ キー ID（Security Key Identifier）] フィールド	現在のキー ID。
[セキュリティ キー（Security Key）] フィールド	コントローラのセキュリティを有効にする際に使用するセキュリティ キーです。現在のセキュリティ キーを変更する場合は、このフィールドに新しいキーを入力します。 （注） セキュリティ キーを変更すると、[セキュア キーの検証（Secure Key Verification）] ポップアップ ウィンドウが表示されます。このウィンドウに現在のセキュリティ キーを入力してキーの検証を行う必要があります。
[セキュリティ キーの確認（Confirm Security Key）] フィールド	セキュリティ キーを再入力します。

名前	説明
[Modify Security Key (セキュリティ キーの変更)] チェックボックス	（注） このオプションは、リモート キー管理の場合にのみ表示されます。 このオプションを選択すると、KMIP サーバのセキュリティ キーが変更されます。
[Suggest] ボタン	割り当てることができるセキュリティ キーまたはキー ID の候補を示します。
[**保存（Save**）] ボタン	データを保存します。
[Cancel] ボタン	アクションを取り消します。

ステップ 5 **[Save]** をクリックします。

これにより、コントローラ セキュリティ設定が変更されます。

コントローラ セキュリティの無効化

このオプションを使用できるのは一部の C シリーズ サーバーだけです。

始める前に

- このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。
- コントローラ セキュリティを無効にするには、最初に有効にしておく必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [Storage] メニューで、適切な LSI MegaRAID もしくは HBA コントローラをクリックします。

ステップ 3 [Controller Info] 領域で、[Disable Drive Security] をクリックします。

ステップ 4 確認ポップアップ ウィンドウで [OK] をクリックします。

これにより、コントローラのセキュリティがディセーブルになります。

ローカルとリモートのキー管理間のコントローラ セキュリティの切り替え

このタスクでは、コントローラのセキュリティをローカル管理からリモート管理、およびリモート管理からローカル管理に切り替えることができます。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。

ステップ 2 [Storage] メニューで、適切な LSI MegaRAID もしくは HBA コントローラをクリックします。

ステップ 3 [Controller Info] 領域で、コントローラのセキュリティをリモート管理からローカル管理に切り替えるには、[Switch to Local Key Management] をクリックします。

（注） リモート キー管理からローカル キー管理に切り替えるときは、まず KMIP セキュア キー管理を無効にしてください。

ステップ 4 （任意）同様に、コントローラのセキュリティをローカル管理からリモート管理に切り替える場合は、[Switch to Remote Key Management] をクリックします。

ステップ 5 [OK] をクリックして確定します。

未使用の物理ドライブからの仮想ドライブの作成

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。

ステップ 2 [Storage] メニューで、適切な LSI MegaRAID もしくは HBA コントローラをクリックします。

ステップ 3 [Actions] 領域で、[Create Virtual Drive from Unused Physical Drives] をクリックします。

[未使用の物理ドライブから仮想ドライブを作成する（Create Virtual Drive from Unused Physical Drives）] ダイアログボックスが表示されます。

ステップ 4 **[未使用の物理ドライブから仮想ドライブを作成する（Create Virtual Drive from Unused Physical Drives）]**ダイアログボックスで、新しい仮想ドライブの RAID レベルを選択します。

次のいずれかになります。

- [Raid 0]：単純なストライピング。
- [Raid 1]：単純なミラーリング。
- [Raid 5]：パリティ付きストライピング。
- [Raid 6]：2 つのパリティ ドライブによるストライピング。

- [Raid 10]：スパンされたミラーリング。
- [Raid 50]：パリティを使用した SPAN ストライピング。
- [Raid 60]：2 つのパリティ ドライブによるスパンされたストライピング。

ステップ 5 **[ドライブ グループの作成（Create Drive Groups）]** 領域で、グループに含める 1 つ以上の物理ドライブを選択します。

[ドライブ グループ（Drive Groups）] テーブルにドライブを追加するには、**[>>]** ボタンを使用します。ドライブ グループから物理ドライブを削除するには、**[<<]** ボタンを使用します。

（注）
- ドライブ グループで最も小さな物理ドライブのサイズによって、すべての物理ドライブに使用される最大サイズが定義されます。すべての物理ドライブの領域が最大限に使用されることを保証するには、ドライブ グループ内のすべてのドライブのサイズをほぼ同じにすることを推奨します。
- Cisco IMC は、RAID コントローラのみを管理し、サーバーに接続された HBA は管理しません。
- 特定の RAID レベルの仮想ドライブを作成するには、使用できる複数のドライブ グループが必要です。これらの RAID レベルのドライブの作成中、必要な数のドライブが選択されている場合にのみ、[ドライブの作成（create drive）] オプションが使用できます。

ステップ 6 [Virtual Drive Properties] 領域で、次のプロパティを更新します。

名前	説明
[仮想ドライブ名（Virtual Drive Name）] フィールド	新しく作成する仮想ドライブの名前。
[読み取りポリシー（Read Policy）] ドロップダウン リスト	先読みキャッシュ モード。
[キャッシュ ポリシー（Cache Policy）] ドロップダウン リスト	読み取りバッファ処理に使用するキャッシュ ポリシー。
[Strip Size] ドロップダウン リスト	各ストリップのサイズ（KB 単位）。

名前	説明
[書き込みポリシー（Write Policy）] ドロップダウン リスト	次のいずれかになります。 • [ライトスルー（Write Through）]：データはキャッシュに取り込まれてから物理ドライブに書き込まれます。以降はキャッシュからデータを読み取ることができるため、パフォーマンスが向上します。 • [ライトバック（Write Back）]：データはキャッシュ内に保管され、キャッシュにスペースが必要になった場合にのみ物理ドライブに書き込まれます。電源障害の発生時にBBUでキャッシュの安全を保障できない場合、このポリシーを要求する仮想ドライブは [ライトスルー（Write Through）] キャッシングにフォールバックします。 • [ライトバック不良BBU（Write Back Bad BBU）]：このポリシーでは、バッテリバックアップユニットに欠陥があるか、バッテリバックアップユニットが放電しているとしても、書き込みキャッシングは [ライトバック（Write Back）] の状態に維持されます。
[ディスク キャッシュ ポリシー（Disk Cache Policy）] ドロップダウン リスト	次のいずれかになります。 • [未変更（Unchanged）]：ディスク キャッシュ ポリシーは変更されていません。 • [有効（Enabled）]：ディスク上のIOキャッシングが許可されます。 • [無効（Disabled）]：ディスク キャッシングは許可されません。
[Access Policy] ドロップダウン リスト	次のいずれかになります。 • [読み取り/書き込み（Read Write）]：ホストにVDに対する読み取り/書き込み操作の実行が許可されます。 • [読み取り専用（Read Only）]：ホストにはVDからの読み取り操作だけが許可されます。 • [ブロック（Blocked）]：ホストにはVDに対する読み取り/書き込み操作がいずれも許可されません。

名前	説明
[サイズ（Size）] フィールド	作成する仮想ドライブのサイズ。値を入力して、次のいずれかの単位を選択します。 • MB • GB • TB

ステップ 7 **[XML API 要求の生成（Generate XML API Request）]** ボタンをクリックして、API 要求を生成します。

ステップ 8 **[閉じる（Close）]** をクリックします。

ステップ 9 **[仮想ドライブの作成（Create Virtual Drive）]**をクリックします。

既存のドライブ グループからの仮想ドライブの作成

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。

ステップ 2 [Storage] メニューで、適切な LSI MegaRAID もしくは HBA コントローラをクリックします。

ステップ 3 [Actions] 領域で、[Create Virtual Drive from an Existing Virtual Drive Group] をクリックします。

[既存の仮想ドライブグループから仮想ドライブを作成する（Create Virtual Drive from an Existing Virtual Drive Group）] ダイアログボックスが表示されます。

ステップ 4 **[既存の仮想ドライブグループから仮想ドライブを作成する（Create Virtual Drive from an Existing Virtual Drive Group）]**ダイアログボックスで、新しい仮想ドライブの作成に使用するドライブ グループの仮想ドライブを選択します。

ステップ 5 **[仮想ドライブのプロパティ（Virtual Drive Properties）]**領域で、次のプロパティを更新します。

名前	説明
[仮想ドライブ名（Virtual Drive Name）] フィールド	新しく作成する仮想ドライブの名前。
[読み取りポリシー（Read Policy）] ドロップダウン リスト	先読みキャッシュ モード。

名前	説明
[キャッシュ ポリシー（Cache Policy）] ドロップダウン リスト	読み取りバッファ処理に使用するキャッシュ ポリシー。
[Strip Size] ドロップダウン リスト	各ストリップのサイズ（KB 単位）。
[書き込みポリシー（Write Policy）] ドロップダウン リスト	次のいずれかになります。 • [ライトスルー（Write Through）]：データはキャッシュに取り込まれてから物理ドライブに書き込まれます。以降はキャッシュからデータを読み取ることができるため、パフォーマンスが向上します。 • [ライトバック（Write Back）]：データはキャッシュ内に保管され、キャッシュにスペースが必要になった場合にのみ物理ドライブに書き込まれます。電源障害の発生時にBBUでキャッシュの安全を保障できない場合、このポリシーを要求する仮想ドライブは [ライトスルー（Write Through）] キャッシングにフォールバックします。 • [ライトバック不良BBU（Write Back Bad BBU）]：このポリシーでは、バッテリバックアップユニットに欠陥があるか、バッテリバックアップユニットが放電しているとしても、書き込みキャッシングは [ライトバック（Write Back）] の状態に維持されます。
[ディスク キャッシュ ポリシー（Disk Cache Policy）] ドロップダウン リスト	次のいずれかになります。 • [未変更（Unchanged）]：ディスク キャッシュ ポリシーは変更されていません。 • [有効（Enabled）]：ディスク上のIOキャッシングが許可されます。 • [無効（Disabled）]：ディスク キャッシングは許可されません。
[Access Policy] ドロップダウン リスト	次のいずれかになります。 • [読み取り/書き込み（Read Write）]：ホストに VD に対する読み取り/書き込み操作の実行が許可されます。 • [読み取り専用（Read Only）]：ホストには VD からの読み取り操作だけが許可されます。 • [ブロック（Blocked）]：ホストには VD に対する読み取り/書き込み操作がいずれも許可されません。

名前	説明
[サイズ（Size）] フィールド	作成する仮想ドライブのサイズ。値を入力して、次のいずれかの単位を選択します。 • MB • GB • TB

ステップ 6 **[XML API 要求の生成（Generate XML API Request）]** ボタンをクリックして、API 要求を生成します。

ステップ 7 **[閉じる（Close）]** をクリックします。

ステップ 8 **[仮想ドライブの作成（Create Virtual Drive）]**をクリックします。

仮想ドライブを転送対応状態に設定

[転送対応に設定（Set Transport Ready）] 機能を使用して、MegaRAID コントローラ間で仮想ドライブを移動できます。これにより、仮想ドライブのすべての保留中IOがそのアクティビティを完了し、仮想ドライブがオペレーティング システムに認識されないようにし、キャッシュをフラッシュし、すべてのバックグラウンド操作を一時停止し、現在の進行状況をディスク データ形式で保存することができるため、ドライブを移動できます。仮想ドライブを移動すると、同じドライブ グループに属する他のすべてのドライブは、移動されたドライブと同じ変更を継承します。

グループで最後に設定された物理ドライブが現行コントローラから取り外されると、ドライブ グループは外部グループになり、すべての外部設定ルールがこのグループに適用されます。ただし、転送対応機能は外部設定の動作を変更しません。

仮想ドライブの転送対応状態をクリアすることもできます。これによって、仮想ドライブがオペレーティング システムに対して使用可能になります。

転送対応仮想ドライブに適用される制約は次のとおりです。

- 現在サポートされている転送対応ドライブ グループの最大数は 16 です。
- この機能はハイ アベイラビリティではサポートされません。
- 次の条件下では仮想ドライブを転送対応として設定できません。
  - ドライブ グループの仮想ドライブが再構築中である場合
  - ドライブ グループの仮想ドライブにピン キャッシュが含まれている場合
  - ドライブ グループの仮想ドライブがキャッシュ可能としてマークされているか、CacheCade 仮想ドライブに関連付けられている場合
  - 仮想ドライブが CacheCade 仮想ドライブの場合

- 仮想ドライブがオフラインの場合
- 仮想ドライブがブート可能な仮想ドライブの場合

仮想ドライブを転送対応として設定

始める前に

- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。
- 転送対応を有効にするには、仮想ドライブが最適な状態である必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。

ステップ 2 **[ストレージ（Storage）]**メニューで、適切なLSI MegaRAIDまたはHBAコントローラをクリックします。

ステップ 3 作業ペインで **[仮想ドライブ情報（Virtual Drive Info）]** タブをクリックします。

ステップ 4 **[仮想ドライブ（Virtual Drives）]** 領域で、転送対応に設定するドライブを選択します。

ステップ 5 **[アクション（Actions）]**領域で、**[転送対応に設定（Set Transport Ready）]** をクリックします。

[転送対応に設定（Set Transport Ready）] ダイアログボックスが表示されます。

ステップ 6 このダイアログボックスで次のプロパティを更新します。

名前	説明
[タイプの初期化（Initialize Type）] ドロップダウン リスト	選択した仮想ドライブを転送準備完了として設定するのに使用する初期化タイプを選択できます。次のいずれかになります。 • [すべて除外する（Exlude All）]：専用ホットスペア ドライブをすべて除外します。 • [すべて含める（Include All）]：排他的に使用できる専用ホットスペア ドライブ、または共有されている専用ホットスペア ドライブをすべて含めます。 • [専用ホットスペア ドライブを含める（Include Dedicated Hot Spare Drive）]：排他的に専用できるホットスペア ドライブを含めます。
[転送準備完了に設定（Set Transport Ready）] ボタン	選択した仮想ドライブを転送準備完了として設定します。
[Cancel] ボタン	操作をキャンセルします。

（注） 仮想ドライブを転送対応に設定すると、その仮想ドライブに関連付けられているすべての物理ドライブが **[削除可能（Ready to Remove）]** として表示されます。

仮想ドライブの転送対応状態のクリア

始める前に

- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。
- 仮想ドライブを転送対応にする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。

ステップ 2 **[ストレージ（Storage）]** メニューで、適切な LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 作業ペインで **[仮想ドライブ情報（Virtual Drive Info）]**タブをクリックします。

ステップ 4 **[仮想ドライブ（Virtual Drives）]**領域で、転送対応に設定するドライブを選択します。

ステップ 5 **[アクション（Actions）]**領域で、**[転送対応をクリア（Clear Transport Ready）]**をクリックします。

選択した転送対応状態の仮想ドライブが、元の最適状態に戻ります。

物理ドライブ ステータス自動構成モードの設定

始める前に

サーバの電源が投入されている。

（注） このダイアログボックスは、一部の C シリーズ サーバでのみ有効になります。

手順

ステップ 1 **[ナビゲーション（Navigation）]** ペインの **[ストレージ（Storage）]** メニューをクリックします。

ステップ 2 ストレージ メニューで、適切な LSI MegaRAID をクリックします。

デフォルトでは、コントローラ エリアには **[コントローラ情報（Controller Info）]** タブが表示されます。

ステップ 3 アクション エリアで、**[物理ドライブステータス自動構成モードの設定（Set Physical Drive Status Auto Config Mode）]** をクリックします。

[物理ドライブステータス自動構成モードの設定（Set Physical Drive Status Auto Config Mode）] ダイアログボックスが表示されます。

名前	説明
[物理ドライブ ステータス自動構成モード（Physical Drive Status Auto Config Mode）] ドロップダウン リスト	コントローラに選択した物理ドライブ ステータスの自動設定モード。次のいずれかになります。 • **[未構成 良好（Unconfigured Good）]** - デフォルトのオプション。サーバーを RAID ボリュームおよび混合 JBOD に使用している場合は、このオプションを選択します。 • **[RAID-0 Write Back]** - ドライブごとの R0 WB にサーバーを使用している場合は、このオプションを選択します。 • **[JBOD]** - サーバーを JBOD のみに使用している場合は、このオプションを選択します。

（注） **[自動構成（Auto Config）]** モードで適切なオプションを選択すると、未使用の物理ドライブのすべてのステータスが変更されます。

ステップ 4 ドロップダウン リストから、必要な自動構成モードを選択します。

ステップ 5 [保存（Save）] をクリックします。

自動構成モードの変更は、新しく挿入されたすべてのドライブに適用されます。

外部設定のインポート

別のコントローラで以前に設定されている 1 つ以上の物理ドライブがサーバにインストールされると、それらは外部設定として識別されます。コントローラにこれらの外部設定をインポートできます。

重要 次の 2 つのシナリオでは外部設定をインポートすることはできません。

1. セキュアな仮想ドライブがリモート キーを使用してサーバー 1（設定のインポート元）で作成され、ローカル キーを使用してサーバー 2（インポート先）で作成された場合。
2. サーバー 2 が、サーバー 1 の KMIP サーバー クラスタの一部でない別の KMIP サーバーで構成されている場合。

これらのシナリオで外部設定をインポートするには、サーバー 2 のコントローラ セキュリティをローカル キー管理からリモート キー管理に変更し、サーバー 1 の KMIP が設定されている同じクラスタから同じ KMIP サーバーを使用します。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [RAID controller] 領域に、[Controller Info] タブがデフォルトで表示されます。

ステップ 3 [**Actions**] 領域で、[**Import Foreign Config**] をクリックします。

（注） KMIP が有効になっていない場合は、[Secure Key Verification] ダイアログボックスが表示され、外部設定のインポート プロセスを開始するためのセキュリティ キーを入力するように指示されます。

KMIP が有効な場合は、[セキュアキー検証（Secure Key Verification）] ダイアログボックスに次のようなメッセージが表示されます。「ドライブのセキュリティがリモート キー管理により有効になっている場合、セキュリティ キーの指定は任意です（*If drive security has been enabled via remote key management, specifying Security key is optional.*）」。*Click on verify to start foreign configuration import.*」

これにより、セキュリティ キーを入力せずに [Verify] をクリックし、インポートを開始することができます。

ステップ 4 [OK] をクリックして確定します。

外部設定のクリア

重要　このタスクでは、コントローラのすべての外部設定がクリアされます。また、外部設定をホスティングしているすべての物理ドライブからすべての設定情報が削除されます。このアクションは元に戻せません。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1　[ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。

ステップ 2　[Storage] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。[RAID Controller] 領域に、[Controller Info] タブがデフォルトで表示されます。

ステップ 3　[Actions] 領域で、[Clear Foreign Config] をクリックします。

ステップ 4　[OK] をクリックして確定します。

ブート ドライブのクリア

重要　このタスクでは、コントローラのブート ドライブ設定がクリアされます。このアクションは元に戻せません。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1　[ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。

ステップ 2　[Storage] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。[RAID Controller] 領域に、[Controller Info] タブがデフォルトで表示されます。

ステップ 3　[**Actions**] 領域で、[**Clear Boot Drive**] をクリックします。

ステップ 4　[OK] をクリックして確定します。

JBOD モードの有効化

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。
ステップ 2 [Storage] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。
ステップ 3 [RAID Controller] 領域で、[Physical Drive Info] タブをクリックします。
ステップ 4 [Physical Drives] 領域で、未設定の適切なドライブを選択します。
ステップ 5 [**Actions**] 領域で [**Enable JBOD**] をクリックします。
ステップ 6 [**Ok**] をクリックして確定します。

JBOD の無効化

（注） このオプションを使用できるのは一部の UCS C シリーズ サーバーだけです。

始める前に

JBOD オプションは、選択したコントローラに対してイネーブルにする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。
ステップ 2 [Storage] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。
ステップ 3 [RAID Controller] 領域で、[Physical Drive Info] タブをクリックします。
ステップ 4 [Physical Drives] 領域で、JBOD ドライブを選択します。
ステップ 5 [**Actions**] 領域で [**Disable JBOD**] をクリックします。
ステップ 6 [**Ok**] をクリックして確定します。

コントローラのストレージ ファームウェア ログの取得

このタスクは、コントローラのストレージ ファームウェア ログを取得し、それを `/var/log` の場所に配置します。これにより、テクニカル サポート データが要求された場合にこのログ データを確実に使用できるようになります。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。
ステップ 2 作業領域に、[Controller Info] タブがデフォルトで表示されます。
ステップ 3 [Actions] 領域で、[Get Storage Firmware Log] をクリックします。
ステップ 4 [OK] をクリックして確定します。

重要 コントローラのストレージ ファームウェア ログを取得するには 2 ～ 4 分かかる場合があります。このプロセスが完了するまで、テクニカル サポート データのエクスポートを開始しないでください。

コントローラの設定のクリア

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。
ステップ 2 [Storage] メニューで、適切な LSI MegaRAID もしくは HBA コントローラをクリックします。
ステップ 3 [Controller Info] 領域で、[Clear All Configuration] をクリックします。
ステップ 4 [OK] をクリックして確定します。

これにより、既存のコントローラ設定がクリアされます。

ストレージ コントローラの工場出荷時の初期状態への復元

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。
ステップ 2 [Storage] メニューで、適切な LSI MegaRAID もしくは HBA コントローラをクリックします。
ステップ 3 [Controller Info] 領域で、[Set Factory Defaults] をクリックします。
ステップ 4 [OK] をクリックして確定します。
これにより、コントローラ設定が出荷時の初期状態に復元します。

ドライブの削除のための準備

（注） [Unconfigured Good] ステータスを表示する物理ドライブのみでこのタスクを実行できます。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。
ステップ 2 [Storage] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。
ステップ 3 [RAID Controller] 領域で、[Physical Drive Info] タブをクリックします。
ステップ 4 [Physical Drives] 領域で、削除するドライブを選択します。
ステップ 5 **[アクション（Actions）]**領域で **[削除の準備（Prepare for Removal）]** をクリックします。
ステップ 6 [OK] をクリックして確定します。

ドライブの削除のための準備の取り消し

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。

ステップ 2 [Storage] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [RAID Controller] 領域で、[Physical Drive Info] タブをクリックします。

ステップ 4 [Physical Drives] 領域で、[Ready to Remove] 状態のドライブを選択します。

ステップ 5 **[アクション（Actions）]** 領域で **[削除準備を元に戻す（Undo Prepare for Removal）]** をクリックします。

ステップ 6 [OK] をクリックして確定します。

専用ホット スペアにする

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの **[Storage]** タブをクリックします。

ステップ 2 [Storage] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [RAID Controller] 領域で、[Physical Drive Info] タブをクリックします。

ステップ 4 [Physical Drives] 領域で、専用ホット スペアを作成する未設定の適切なドライブを選択します。

ステップ 5 **[アクション（Actions）]** 領域で **[専用ホットスペアにする（Make Dedicated Hot Spare）]** をクリックします。

[専用ホットスペアにする（Make Dedicated Hot Spare）] ダイアログボックスが表示されます。

ステップ 6 **[仮想ドライブの詳細（Virtual Drive Details）]**領域で、次のプロパティを更新します。

名前	説明
[仮想ドライブ番号（Virtual Drive Number）] ドロップダウン リスト	物理ドライブをホット スペアとして専用にする仮想ドライブを選択します。
[仮想ドライブ名（Virtual Drive Name）] フィールド	選択された仮想ドライブの名前。
[専用ホット スペアの作成（Make Dedicated Hot Spare）] ボタン	専用のホット スペアを作成します。
[Cancel]ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

ステップ 7 **[専用ホットスペアにする（Make Dedicated Hot Spare）]**をクリックして確定します。

グローバル ホット スペアにする

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの **[Storage]** タブをクリックします。

ステップ 2 [Storage] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [RAID Controller] 領域で、[Physical Drive Info] タブをクリックします。

ステップ 4 [Physical Drives] 領域で、グローバル ホット スペアを作成する未設定の適切なドライブを選択します。

ステップ 5 **[アクション（Actions）]**領域で**[グローバル ホットスペアにする（Make Global Hot Spare）]**をクリックします。

ホット スペア プールからのドライブの削除

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] タブで、適切な LSI MegaRAID コントローラをクリックします。

ステップ 3 作業ペインで [物理ドライブ情報（Physical Drive Info）] タブをクリックします。

ステップ 4 [物理ドライブ（Physical Drives）] 領域で、ホット スペア プールから削除するグローバル ホット スペアまたは専用ホット スペアを選択します。

ステップ 5 [アクション（Actions）] 領域で [ホットスペア プールから削除（Remove From Hot Spare Pools）] をクリックします。

物理ドライブのステータスの切り替え

始める前に

- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。
- コントローラは、JBOD モードをサポートする必要があり、JBOD モードはイネーブルにする必要があります。

手順

ステップ 1 [Navigation] ペインの **[Storage]** タブをクリックします。

ステップ 2 [Storage] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [RAID Controller] 領域で、[Physical Drive Info] タブをクリックします。

ステップ 4 [Physical Drives] 領域で、unconfigured good として設定するドライブを選択します。

ステップ 5 [**Actions**] 領域で、[**Set State as Unconfigured Good**] をクリックします。

ステップ 6 [**OK**] をクリックして、JBOD モードがディセーブルになっていることを確認します。

[**Set State as JBOD**] オプションがイネーブルになります。

ステップ 7 物理ドライブのJBODモードをイネーブルにするには、[**Set State as JBOD**] をクリックします。

ステップ 8 **[OK]**をクリックして確定します。

[**Set State as Unconfigured Good**] オプションがイネーブルになります。

コントローラのブート ドライブとしての物理ドライブの設定

始める前に

- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。
- コントローラは、JBOD モードをサポートする必要があり、JBOD モードはイネーブルにする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。

ステップ 2 [Storage] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [RAID Controller] 領域で、[Physical Drive Info] タブをクリックします。

ステップ 4 [Physical Drives] 領域で、コントローラのブート ドライブとして設定するドライブを選択します。

ステップ 5 **[アクション（Actions）]** 領域で、**[ブート ドライブとして設定（Set as Boot Drive）]** をクリックします。

ステップ 6 [OK] をクリックして確定します。

仮想ドライブの初期化

ドライブを初期化すると、仮想ドライブ上のすべてのデータが失われます。初期化を実行する前に、保存する仮想ドライブのデータをバックアップします。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。

ステップ 2 [Storage] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [RAID Controller] 領域で、[Virtual Drive Info] タブをクリックします。

ステップ 4 [Virtual Drives] 領域で、初期化するドライブを選択します。

ステップ 5 **[アクション（Actions）]**領域で **[初期化（Initialize）]**をクリックします。

[仮想ドライブの初期化（Initialize Virtual Drive）]ダイアログボックスが表示されます。

ステップ 6 仮想ドライブに使用する初期化のタイプを選択します。

次のいずれかになります。

- [Fast Initialize]：このオプションは、仮想ドライブへのデータの書き込みをすぐに開始できます。
- [完全初期化（Full Initialize）]：新しい設定で完全な初期化が実行されます。初期化が完了するまで、新しい仮想ドライブにデータを書き込むことができません。

ステップ 7 **[VD の初期化（Initialize VD）]**をクリックしてドライブを初期化するか、**[キャンセル（Cancel）]** をクリックして、変更を行わずにダイアログボックスを閉じます。

ステップ 8 ドライブで実行しているタスクのステータスを表示するには、**[操作（Operations）]**領域で **[更新（Refresh）]**をクリックします。

次の詳細情報が表示されます。

名前	説明
[Operation]	ドライブで現在実行中の操作の名前。
[Progress in %]	操作の進行状況（完了した割合）。

名前	説明
[Elapsed Time in secs]	操作開始から経過した時間（秒数）。

ブート ドライブとして設定

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。
ステップ 2 [Storage] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。
ステップ 3 [RAID Controller] 領域で、[Virtual Drive Info] タブをクリックします。
ステップ 4 [Virtual Drives] 領域で、コントローラが起動する必要のあるドライブを選択します。
ステップ 5 **[アクション（Actions）]** 領域で、**[ブート ドライブとして設定（Set as Boot Drive）]**をクリックします。
ステップ 6 [OK] をクリックして確定します。

仮想ドライブの編集

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。
ステップ 2 [Storage] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。
ステップ 3 [RAID Controller] 領域で、[Virtual Drive Info] タブをクリックします。
ステップ 4 [Virtual Drives] 領域で、[Edit Virtual Drive] をクリックします。
ステップ 5 この説明を確認してから、[OK] をクリックします。
[仮想ドライブの編集（Edit Virtual Drive）] ダイアログボックスが表示され、その後データのバックアップを作成するよう指示されます。
ステップ 6 [**Select RAID Level to migrate**] ドロップダウン リストから、RAID レベルを選択します。

RAID のマイグレーション基準については次の表を参照してください。

名前	説明
[**Select RAID Level to migrate**] ドロップダウン リスト	移行する RAID レベルを選択します。移行は次の RAID レベルで許可されています。 • **[RAID 0]** から **[RAID 1]** へ • **[RAID 0]** から **[RAID 5]** へ • **[RAID 0]** から **[RAID 6]** へ • **[RAID 1]** から **[RAID 0]** へ • **[RAID 1]** から **[RAID 5]** へ • **[RAID 1]** から **[RAID 6]** へ • **[RAID 5]** から **[RAID 0]** へ • **[RAID 6]** から **[RAID 0]** へ • **[RAID 6]** から **[RAID 5]** へ ある raid レベルから別のレベルに移行する場合、新しいRAIDレベルのデータ アームは、既存のもの以上である必要があります。 RAID 6 の場合、RAID 6 には二重分散パリティがあるため、データ アームはドライブ数から 2 を引いた数になります。たとえば、8 台のドライブで RAID 6 を作成する場合、データ アームの数は 8 – 2 = 6 となります。この場合、RAID 6 から RAID 0 に移行する場合は、RAID 0 には最低 6 台のドライブが必要です。それより少ないドライブ数を選択すると、[**Edit**] または [**Save**] ボタンが無効になります。 追加する場合は、ドライブを削除しないままでRAID 0に移行できます。 （注） RAID レベルの移行は、次の場合にはサポートされません。 • RAID グループに複数の仮想ドライブがある場合。 • SSD/HDD RAID グループの組み合わせがある場合。

ステップ 7 [**Virtual Drive Properties**] 領域の [**Write Policy**] ドロップダウン リストから、次のいずれかを選択します。

- [Write Through]：データがキャッシュによって、物理ドライブに書き込まれます。以降はキャッシュからデータを読み取ることができるため、パフォーマンスが向上します。

- [ライトバック（Write Back）]：データはキャッシュ内に保管され、キャッシュにスペースが必要になった場合にのみ物理ドライブに書き込まれます。電源障害の発生時に BBU でキャッシュの安全を保障できない場合、このポリシーを要求する仮想ドライブは [ライトスルー（Write Through）] キャッシングにフォールバックします。
- [書き込みバック不良 BBU（Write Back Bad BBU）]：このポリシーでは、バッテリ バックアップユニットに欠陥があったり、放電していたりする場合でも、書き込みキャッシングは [書き込みバック（Write Back）] のままです。

ステップ 8 **[Save Changes]**をクリックします。

仮想ドライブの削除

重要 このタスクでは、仮想ドライブ（ブートされたオペレーティング システムを実行するドライブを含む）を削除します。そのため、仮想ドライブを削除する前に、保持するデータをバックアップします。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの [ストレージ（Storage）] メニューをクリックします。
ステップ 2 [Storage] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。
ステップ 3 [RAID Controller] 領域で、[Virtual Drive Info] タブをクリックします。
ステップ 4 [Virtual Drives] 領域で、削除する仮想ドライブを選択します。
ステップ 5 **[アクション（Actions）]**領域で、**[仮想ドライブの削除（Delete Virtual Drive）]**をクリックします。
ステップ 6 [OK] をクリックして確定します。

仮想ドライブの非表示化

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。
ステップ 2 [Storage] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。
ステップ 3 [RAID Controller] 領域で、[Virtual Drive Info] タブをクリックします。
ステップ 4 [Virtual Drives] 領域で、非表示にする仮想ドライブを選択します。
ステップ 5 **[アクション（Actions）]**領域で、**[ドライブの非表示（Hide Drive）]**をクリックします。
ステップ 6 [OK] をクリックして確定します。

バッテリ バックアップ ユニットの学習周期の開始

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。
ステップ 2 [Storage] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。
ステップ 3 [RAID Controller] 領域で、[Battery Backup Unit] タブをクリックします。
ステップ 4 [Actions] ペインで [Start Learn Cycle] をクリックします。
ダイアログでタスクを確認するためのプロンプトが表示されます。
ステップ 5 [OK] をクリックします。

ストレージ コントローラ ログの表示

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。
ステップ 2 [Storage] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。
ステップ 3 [RAID Controller] 領域で、[Storage Log] タブをクリックし、次の情報を確認します。

名前	説明
[Time] カラム	イベントが発生した日時。
[Severity] カラム	イベントのシビラティ（重大度）。次のいずれかになります。 • 緊急（Emergency） • アラート（Alert） • クリティカル（Critical） • エラー（Error） • Warning • 通知（Notice） • 情報（Informational） • デバッグ（Debug）
[Description] カラム	イベントの説明。

MegaRAID コントローラの SSD スマート情報の表示

ソリッド ステート ドライブのスマート情報を表示できます。次の手順を実行します。

手順

ステップ 1 [Navigation] ペインの **[Storage]** タブをクリックします。

ステップ 2 **[ストレージ（Storage）]** メニューで、適切な LSI MegaRAID コントローラをクリックします。

ステップ 3 **作業**ペインで **[物理ドライブ情報（Physical Drive Info）]** タブをクリックします。

ステップ 4 **[スマート情報（Smart Information）]**領域で、次の情報を確認します。

名前	説明
[電源再投入カウント（Power Cycle Count）] フィールド	ドライブが製造されてから現在までに電源の再投入が行われた回数。
[電源オン時間（Power on Hours）] フィールド	ドライブが「電源オン」モードになっている合計時間数。

名前	説明
[残量（パーセンテージ）（Percentage Life Left）] フィールド	半導体ドライブ（SSD）のライフタイムで残っている書き込みサイクルの回数。たとえば、ライフタイムを通して 100 回の書き込みサイクルに対応できる SSD で 15 回の書き込みが行われた場合、ドライブのライフタイムの残りのパーセンテージは 85% となります。パーセンテージの各範囲は異なる色で表されます。たとえば、75% ～ 100% は緑、1% ～ 25% は赤で表されます。
[消耗ステータス（日数）（Wear Status in Days）] フィールド	SSD で書き込みサイクルが行われた日数。 SSD ベンダーが提示する 1 日あたりの SSD 書き込みの有限回数に基づいて、SSD が機能し続ける合計年数を計算できます。
[動作温度（Operating Temperature）] フィールド	選択した SSD が、それを選択した時点で動作していたドライブの温度。
[消費された予約済みの容量の割合（Percentage Reserved Capacity Consumed）] フィールド	（SSD 用に予約されているパーセンテージのうち）SSD が消費する合計容量。
[前回の更新時刻（Time of Last Refresh）] フィールド	ドライブが最後に更新されてからの時間。

NVMe コントローラの詳細の表示

始める前に

- サーバーの電源をオンにする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] メニューをクリックします。
ステップ 2 [ストレージ（Storage）] メニューで、適切な NVMe コントローラをクリックします。
ステップ 3 [Controller] 領域に、[Controller Info] タブがデフォルトで表示されます。
ステップ 4 [Work] ペインの [Health/Status] 領域で次の情報を確認します。

名前	説明
[複合状態（Composite Health）] フィールド	コントローラの状態。次のいずれかになります。 • [良好（Good）] : コントローラ下のすべてのドライブは最適な状態です。 • [重大な障害（Severe Fault）] : コントローラ下の 1 つまたは複数のドライブが不良状態のときに表示されます。 • **該当なし**
[ドライブ数（Drive Count）] フィールド	コントローラ上で設定されているドライブの数。

ステップ 5 [製造者情報（Manufacturer Information）] 領域で、次の情報を確認します。

名前	説明
[Vendor ID] フィールド	NVMe コントローラのベンダ ID。
[Product ID] フィールド	コントローラの製品 ID。
[コンポーネントID（Component ID）] フィールド	NVMe コントローラのコンポーネント ID。
[Product Revision] フィールド	ボードのリビジョン番号（存在する場合）。

ステップ 6 [グループPCI情報（Group PCI Info））] 領域で、次の情報を確認します。

名前	説明
[Vendor ID] フィールド	PCI ベンダー ID（16 進）。
[Device ID] フィールド	PCI デバイス ID（16 進）。

ステップ 7 [グループファームウェア情報（Group Firmware Information）] 領域で、次の情報を確認します。

名前	説明
[実行中のファームウェアイメージ（Running Firmware Images）] フィールド	NVMe ドライブのファームウェア バージョン。

ステップ 8 [グループスイッチ情報（Group Switch Information）] 領域で、次の情報を確認します。

名前	説明
[Temperature] フィールド	スイッチの温度（摂氏）。

名前	説明
[スイッチステータス（Switch Status）] フィールド	スイッチの現在のステータス。次のいずれかになります。 • [Optimal]：コントローラは正常に機能しています。 • [Failed]：コントローラは機能していません。 • [Unresponsive]：コントローラがダウンしています。
[リンクステータス（Link Status）] フィールド	リンクの現在の状態。このフィールドは、スイッチのアップストリームまたはダウンストリームのリンクのいずれかがダウンしているかどうかを示します。個々のドライブにも、どのドライブが原因でスイッチのリンクの状態がリンク低下を示しているかを特定するために使用できるリンクのステータスがあります。次のいずれかになります。 • [Optimal]：コントローラは正常に機能しています。 • [Failed]：コントローラは機能していません。 • [Unresponsive]：コントローラがダウンしています。
[シャットダウン温度（Shutdown Temperature）] フィールド	これは、これを超えるとスイッチの安全な動作が保証できず、システムをシャットダウンすることが推奨される温度です。

NVMe 物理ドライブの詳細の表示

始める前に

- サーバーの電源をオンにする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、適切な NVMe コントローラをクリックします。

ステップ 3 [物理ドライブ（Physical Drive）] タブをクリックし、次の情報を確認します。

名前	説明
[物理ドライブ（Physical Drives）] カラム	使用可能な物理ドライブのリスト。
[PCI Slot] カラム	物理ドライブが存在する PCI スロット番号。
[Managed ID] カラム	デバッグで参照される内部 ID。
[Product Name] カラム	ベンダーによって割り当てられたドライブの名前。
[**Firmware Version**] カラム	ドライブで実行されているファームウェアバージョン。
[Vendor] カラム	ドライブのベンダー名。
[Serial Number] カラム	ドライブのシリアル番号。

ステップ 4 [物理ドライブ（Physical Drives））] 詳細

（注） リストされた物理ドライブのいずれかを展開すると、物理ドライブのこれらの詳細が表示されます。

名前	説明
[PCI Slot] フィールド	物理ドライブが存在する PCI スロット番号。
[Managed ID] カラム	デバッグで参照される内部 ID。
[Throttle State] フィールド	スロットルの状態。
[Serial Number] フィールド	コントローラのシリアル番号。
[チップの温度（Chip Temperature）] フィールド	ドライブの温度（摂氏）。これはドライブの内部センサで読み取られた最高温度です。
[Percentage Drive Life Used] フィールド	ドライブ ライフタイムのうち、使用された時間のパーセンテージ。
[Device ID] フィールド	PCI デバイス ID（16 進）。
[Sub Device ID] フィールド	PCI サブデバイス ID（16 進）。

名前	説明
[Drive Status] フィールド	デバイスの状態。
[パフォーマンス レベル（Performance Level）] フィールド	ドライブのパフォーマンスを示します。
[Shutdown Temperature] フィールド	ドライブがシャット ダウンする温度。
[電源オン総時間の割合（Percentage of Total Power On Hours）] フィールド	ドライブが電源オンであった時間の割合。
[Vendor ID] フィールド	PCI ベンダー ID（16 進）。
[SubVendor ID] フィールド	PCI サブベンダー ID（16 進）。
[LED Fault Status] フィールド	LED 障害のステータス。
[Controller Temperature] フィールド	コントローラの温度（摂氏）。これは、NVMe サブシステム ID の全体的な合成温度です。
[実行中のファームウェアイメージ（Running Firmware Images）] フィールド	NVMe ドライブのファームウェア バージョン。
[Throttle Start Temperature] フィールド	ドライブがスロットルを開始する温度。

PCI スイッチの詳細の表示

始める前に

サーバーの電源をオンにする必要があります。そうしないと、プロパティが表示されません。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] メニューをクリックします。

ステップ 2 **[Storage]** メニューで、適切な **PCI スイッチ** コントローラをクリックします。次の情報を確認します。

[コントローラ（Controller）] 領域

名前	説明
[Composite Health] フィールド	PCI スイッチの全体的なヘルス ステータスを示します。修正可能なまたは修正不可能なエラーがあるかどうかを表示し、またアップストリームおよびダウンストリーム ポートのステータスを反映されます。
[PCI スロット（PCI Slot）] フィールド	コントローラが装着されている PCI スロット。
[コントローラタイプ（Controller Type）] フィールド	スロットに存在する PCI コントローラのタイプ。
[製品名（Product Name）] 列	PCI コントローラの名前。
[製品リビジョン（Revision）] カラム	コントローラ設定のリビジョン情報を表示します。

[スイッチ情報（Switch Information）] 領域

名前	説明
[Temperature] フィールド	スイッチの温度 (摂氏)。

[製造者情報（Manufacturer Information））] 領域

名前	説明
[製造元（Manufacturer）] カラム	PCI スイッチのベンダー。
[ベンダー ID（Vendor ID）] カラム	ベンダーによって割り当てられたスイッチ ID。
[サブ ベンダー ID（Sub Vendor ID）] カラム	ベンダーによって割り当てられた 2 番目のスイッチ ID。
[Device ID] カラム	ベンダーによって割り当てられたデバイス ID。
[Sub Device ID] カラム	ベンダーによって割り当てられているセカンダリ デバイス ID。

[GPUとPCIアダプタ（GPU and PCI Adapters）] 領域

名前	説明
[Slot] カラム	GPU または PCI アダプタが存在するスロットの ID。

名前	説明
[リンクステータス（Status）] カラム	リンクの現在の状態。このフィールドは、スイッチのアップストリームまたはダウン ストリームのリンクのいずれかがダウンしているかどうかを示します。
[リンク速度(GT/s)（Link Speed (GT/s)）] カラム	PCI 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。
[リンク幅（Link Width）] カラム	The number of data lanes of the link.リンクのデータ レーンの数。
[ステータス（Status）] カラム	アダプタのステータス。

コピーバック操作の開始

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [Storage] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [RAID Controller] 領域で、[Physical Drive Info] タブをクリックします。

ステップ 4 [物理ドライブ（Physical Drives）] 領域で、オンライン状態のドライブを選択します。

ステップ 5 [アクション（Actions）] 領域で、[コピーバックの開始（Start Copyback）] をクリックします。

ステップ 6 [コピーバック操作の開始（Start Copyback Operation）] ダイアログボックスが表示されます。

ステップ 7 コピーバック操作を行う [コピー先物理ドライブ（Destination Physical Drive）] を選択します。

ステップ 8 [コピーバックの開始（Start Copyback）] をクリックします。

ステップ 9 次のコピーバック操作を行うこともできます。

- [コピーバックの中断（Pause Copyback）]：ドライブがコピーバック状態の場合に、コピーバック操作を一時停止できます。
- [コピーバックの再開（Resume Copyback）]：一時停止したコピーバック操作を再開することができます。
- [コピーバックの中止（Abort Copyback）]：ドライブがコピーバック状態の場合に、コピーバック操作を中止できます。

Flexible Flash コントローラの管理

Cisco Flexible Flash

M5 サーバでは、Flexible Flash コントローラはミニ ストレージ モジュール ソケットに挿入されます。ミニストレージソケットはマザーボードの M.2 スロットに挿入されます。M.2 スロットは SATA M.2 SSD スロットもサポートしています。

（注） M.2 スロットは、このリリースでは NVMe をサポートしていません。

C シリーズ ラックマウント サーバ の中には、サーバ ソフトウェア ツールおよびユーティリティのストレージとして、内蔵 Secure Digital（SD）メモリ カードをサポートしているものがあります。この SD カードは Cisco Flexible Flash ストレージ アダプタでホストされます。

Cisco IMC では、単一ハイパーバイザ（HV）パーティション構成として SD ストレージが使用可能です。以前のバージョンでは 4 つの仮想 USB ドライブがありました。3 つには Cisco UCS Server Configuration Utility、Cisco ドライバ、および Cisco Host Upgrade Utility が事前ロードされ、4 番目はユーザ インストールによるハイパーバイザでした。また、Cisco IMC の最新バージョンにアップグレードするか、旧バージョンにダウングレードした後、設定をリセットした場合にも、単一 HV パーティション構成が作成されます。

M.2 ドライブのインストールおよび設定の詳細については、次の URL にある C240 M5 サーバ用の『Cisco UCS サーバ インストレーションおよびサービス ガイド』の**「ストレージ コントローラに関する考慮事項（組み込み SATA RAID の要件）」**および**「M.2 用ミニストレージ キャリア内の M.2 SSD の交換」**のセクションを参照してください。

https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-rack-servers/products-installation-guides-list.html

シスコ ソフトウェア ユーティリティおよびパッケージの詳細については、次の URL の『*Cisco UCS C-Series Servers Documentation Roadmap*』 を参照してください。

http://www.cisco.com/go/unifiedcomputing/c-series-doc

Cisco Flexible Flash コントローラのカード管理機能

Cisco Flexible Flash コントローラでは、単一のカードに加えて 2 つの SD カードを RAID-1 ペアとして管理できます。カード管理機能の導入により、次の作業を実行できます。

（注）
- バージョン 1.4(5e) から 1.5(4) 以降のバージョンにアップグレードする場合は、まずバージョン 1.5(2) にアップグレードしてから、Cisco IMC の上位バージョンにアップグレードする必要があります。
- すべての Cisco IMC ファームウェアのアップグレード後に、最新の Flex Flash ファームウェアをロードするには、Cisco Flexible Flash コントローラをリセットします。

アクション	説明
Reset Cisco Flex Flash	コントローラをリセットできます。
Reset Partition Defaults	選択したスロットの設定をデフォルト設定にリセットできます。
Synchronize Card Configuration	ファームウェア バージョン 253 以降をサポートする SD カードの設定を保持できます。
Configure Operational Profile	選択した Cisco Flexible Flash コントローラの SD カードを設定できます。

RAID パーティションの列挙

非 RAID パーティションは常にプライマリ カードから列挙されます。列挙はプライマリ カードのステータスに依存しません。

次に、Cisco Flexible Flash コントローラに 2 枚のカードがあるときの RAID パーティションの列挙の動作を示します。

シナリオ	動作
シングル カード	RAIDパーティションは、カードが正常に動作している場合、およびモードが **Primary** または **Secondary-active** の場合に列挙されます。
デュアル ペア カード	RAIDパーティションは、カードの1つが正常に動作していれば列挙されます。 1枚のカードだけが正常に動作している場合、すべての読み取り/書き込み操作は、この正常に動作しているカードで行われます。2 つのRAIDパーティションを同期するにはUCS SCUを使用する必要があります。

シナリオ	動作
デュアル非ペア カード	サーバを再起動するときにこのシナリオが検出された場合、RAIDパーティションはいずれも列挙されません。 サーバが稼働しているときにこのシナリオが検出された場合、ユーザが新しいSDカードを取り付けても、そのカードは Cisco Flexible Flash コントローラによって管理されません。これはホストの列挙には影響しません。これらを管理するためにカードをペアにする必要があります。カードをペアにするには、**[Reset Partition Defaults]** または **[Synchronize Card Configuration]** オプションを使用できます。

FlexFlash でのシングル カード ミラーリングからデュアル カード ミラーリングへのアップグレード

次のいずれかの方法で、FlexFlash を使用したシングル カード ミラーリングからデュアル カード ミラーリングにアップグレードできます。

- サーバーに空の FlexFlash カードを追加し、最新バージョンにファームウェアをアップグレードします。
- FlexFlash ファームウェアを最新バージョンにアップグレードした後、空のカードをサーバーに追加します。

このいずれかの方法を使用する前に、次のガイドラインに注意してください。

- RAID1 ミラーリングを作成するには、サーバーに追加される空のカードのサイズが、サーバー上の既存のカードと正確に同じである必要があります。RAID1 ミラーリングをセットアップするうえで、同じカード サイズは必須事項です。
- ハイパーバイザ パーティション内の有効なデータを持つカードが、プライマリ正常カードとしてマークされていることを確認してください。Cisco IMC GUI または Cisco IMC CLI でこの状態を判別できます。カードの状態をプライマリ正常としてマークするには、Cisco IMC GUI の [**Reset Configuration**] オプションを使用するか、Cisco IMC CLI で **reset-config** コマンドを実行することができます。特定のカードの設定をリセットすると、セカンダリ カードはセカンダリ アクティブ非正常としてマークされます。
- RAID 正常性「Degraded」状態である場合、すべての読み取りおよび書き込みトランザクションは正常なカードで実行されます。このシナリオでは、データのミラーリングは行われません。データのミラーリングは、正常な RAID 状態の場合にのみ行われます。
- データのミラーリングはRAIDパーティションにのみ適用されます。C シリーズ サーバーでは、RAID モードでハイパーバイザ パーティションだけが動作します。

- 旧バージョンで使用するよう SD カードを設定していない場合、最新バージョンにアップグレードすると最新の 253 ファームウェアがロードされ、4 個のパーティションすべてがホストに列挙されます。

FlexFlash バージョンのアップグレード中に次のエラー メッセージが表示される場合があります。

```
Unable to communicate with Flexible Flash controller: operation ffCardsGet, status
CY_AS_ERROR_INVALID_RESPONSE"
```

さらに、カード ステータスが [missing] と示されることもあります。このエラーが発生する原因は、1.4(x) などの代替リリースまたは旧バージョンに意図せず切替えたためです。このシナリオでは、最新バージョンに戻すか、元の FlexFlash 1.4(x) 設定に切り替えることができます。最新の Cisco IMC バージョンに戻すことを選択した場合、Cisco FlexFlash 設定はそのまま残ります。旧バージョンの設定に切り替えることを選択した場合は、Flexflash 設定をリセットする必要があります。その場合、次の点に注意する必要があります。

- 複数のカードが存在する状態で旧バージョンに戻すと、2 番目のカードを検出したり管理したりすることはできません。
- カード タイプが SD253 である場合、Cisco IMC CLI から **reset-config** コマンドを 2 回実行する必要があります。1 回目は古いファームウェアをコントローラに再ロードして SD253 から SD247 タイプに移行し、2 回目の実行では列挙を開始します。

Flexible Flash コントローラ プロパティの設定

Cisco IMC の最新バージョンにアップグレードするか、以前のバージョンにダウングレードしてから設定をリセットすると、サーバーは HV パーティションだけにアクセスします。

始める前に

- このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされている必要があります。

（注） このタスクを実行すると、ホストですべての仮想ドライブが再スキャンされるため、仮想ドライブに接続できなくなります。仮想ドライブを使用する前に Cisco Flexible Flash コントローラを設定するか、このタスクを開始する前にホストの電源を切ることをお勧めします。

手順

ステップ 1 [Navigation] ペインの **[Storage]** タブをクリックします。

ステップ 2 [ストレージ（Storage）] タブの [Cisco FlexFlash] をクリックします。

ステップ 3 [Controller Info] タブの [Configure Operational Profile] をクリックします。

ステップ 4 [Operational Profile] ダイアログボックスで、次のフィールドを更新します。

表 *15 : C220*、*C240*、*C22*、*C24*、*C460 M4* の操作プロファイル フィールド

名前	説明
[Controller] フィールド	選択された Cisco Flexible Flash コントローラのシステム定義名。 この名前は変更できません。
[Virtual Drives Enabled] フィールド	USB 形式のドライブとして、サーバに対して使用可能にできる仮想ドライブ。 単一の HV パーティションに対するチェックボックスが表示されます。 （注） 旧バージョンでは、各仮想ドライブに対して 4 個のチェックボックスが表示されます。単一パーティションを既に作成し、旧バージョンの Cisco IMC にダウングレードした場合、HV のみが有効であっても他の仮想ドライブが表示されます。
[RAID Primary Member] フィールド	プライマリ RAID メンバが存在するスロット。
[RAID セカンダリ ロール（RAID Secondary Role）] フィールド	値として **secondary-active** を指定する必要があります。
[I/O Read Error Threshold] フィールド	Cisco Flexible Flash カードへのアクセス中に許容される読み取りエラーの数。あるカードでの読み取りエラーの数がこのしきい値を超えた場合、そのカードには正常でないというマークが付けられます。 読み取りエラーしきい値を指定するには、1 以上 255 以下の整数を入力します。検出されたエラー数に関係なく、カードが無効にならないように指定するには、**0**（ゼロ）を入力します。
[I/O 書き込みエラーしきい値（I/O Write Error Threshold）] フィールド	Cisco Flexible Flash カードへのアクセス中に許可される書き込みエラーの数。あるカードでの書き込みエラーの数がこのしきい値を超えた場合、そのカードには正常でないというマークが付けられます。 書き込みエラーしきい値を指定するには、1 以上 255 以下の整数を入力します。検出されたエラー数に関係なく、カードが無効にならないように指定するには、**0**（ゼロ）を入力します。

名前	説明
[エラーをクリア（Clear Errors）] チェックボックス	オンにした場合、[変更を保存（Save Changes）] をクリックすると、読み取り/書き込みエラーがクリアされます。

（注）
- 次の表は、C220 M4 および C240 M4 サーバーでのみ有効です。
- [Mirror] モードでは、[Slot1 Read/Write Error Threshold] が両方の SD カード（2 枚のカードがある場合）に適用されます。
- [Util] モードでは、[Slot1 Read/Write Error Threshold] がスロット 1 のカードに適用され、[Slot2 Read/Write Error Threshold] がスロット 2 のカードに適用されます。

表 *16 : C220 M4*、*C240 M4* の操作プロファイル フィールド

名前	説明
[Controller] フィールド	選択された Cisco Flexible Flash コントローラのシステム定義名。 この名前は変更できません。
[ファームウェア動作モード（irmware Operating Mode）]F フィールド	現在のファームウェア動作モード。次のいずれかになります。 • **[Mirror]** • **[Util]**
[スロット 1 読み取りエラーしきい値（SLOT-1 Read Error Threshold）] フィールド	Cisco Flexible Flash カードのスロット 1 へのアクセス中に許容される読み取りエラーの数。あるカードでの読み取りエラーの数がこのしきい値を超えた場合、そのカードには正常でないというマークが付けられます。 読み取りエラーしきい値を指定するには、1 以上 255 以下の整数を入力します。検出されたエラー数に関係なく、カードが無効にならないように指定するには、**0**（ゼロ）を入力します。
[SLOT-1 Write Error Threshold] フィールド	Cisco Flexible Flash カードのスロット 1 へのアクセス中に許容される書き込みエラーの数。あるカードでの書き込みエラーの数がこのしきい値を超えた場合、そのカードには正常でないというマークが付けられます。 書き込みエラーしきい値を指定するには、1 以上 255 以下の整数を入力します。検出されたエラー数に関係なく、カードが無効にならないように指定するには、**0**（ゼロ）を入力します。

名前	説明
[SLOT-2 Read Error Threshold] フィールド	Cisco Flexible Flash カードのスロット 2 へのアクセス中に許容される読み取りエラーの数。あるカードでの読み取りエラーの数がこのしきい値を超えた場合、そのカードには正常でないというマークが付けられます。 読み取りエラーしきい値を指定するには、1 以上 255 以下の整数を入力します。検出されたエラー数に関係なく、カードが無効にならないように指定するには、**0**（ゼロ）を入力します。
[SLOT-2 Write Error Threshold] フィールド	Cisco Flexible Flash カードのスロット 2 へのアクセス中に許容される書き込みエラーの数。あるカードでの書き込みエラーの数がこのしきい値を超えた場合、そのカードには正常でないというマークが付けられます。 書き込みエラーしきい値を指定するには、1 以上 255 以下の整数を入力します。検出されたエラー数に関係なく、カードがディセーブルにならないように指定するには、**0**（ゼロ）を入力します。

ステップ 5 [運用プロファイル（Operational Profile）] ダイアログボックスで、次のフィールドを更新します。

表 *17 : M5* サーバーの操作プロファイル フィールド

名前	説明
[Controller] フィールド	選択された Cisco Flexible Flash コントローラのシステム定義名。 この名前は変更できません。
[Firmware Operating Mode] フィールド	システムによって表示されるメッセージ。ファームウェアの動作モードがミラーとして表示されます。
[スロット 1 読み取りエラーしきい値（SLOT-1 Read Error Threshold）] フィールド	Cisco Flexible Flash カードのスロット 1 へのアクセス中に許容される読み取りエラーの数。あるカードでの読み取りエラーの数がこのしきい値を超えた場合、そのカードには正常でないというマークが付けられます。 読み取りエラーしきい値を指定するには、1 以上 255 以下の整数を入力します。検出されたエラー数に関係なく、カードが無効にならないように指定するには、**0**（ゼロ）を入力します。

名前	説明
[SLOT-1 Write Error Threshold] フィールド	Cisco Flexible Flash カードのスロット 1 へのアクセス中に許容される書き込みエラーの数。あるカードでの書き込みエラーの数がこのしきい値を超えた場合、そのカードには正常でないというマークが付けられます。 書き込みエラーしきい値を指定するには、1 以上 255 以下の整数を入力します。検出されたエラー数に関係なく、カードが無効にならないように指定するには、**0**（ゼロ）を入力します。

ステップ 6 [保存（Save）] をクリックします。

Flexible Flash コントローラ ファームウェア モードの設定

始める前に

- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされている必要があります。

（注） このタスクを実行すると、ホストですべての仮想ドライブが再スキャンされるため、仮想ドライブに接続できなくなります。仮想ドライブを使用する前に Cisco Flexible Flash コントローラのプロパティを設定するか、このタスクを開始する前にホストの電源を切ることをお勧めします。

手順

ステップ 1 [Navigation] ペインの **[Storage]** タブをクリックします。

ステップ 2 [ストレージ（Storage）] タブの [Cisco FlexFlash] をクリックします。

ステップ 3 [Actions] 領域で、[Configure Firmware Mode] をクリックします。

ステップ 4 確認ボックスで [OK] をクリックします。

コントローラ ファームウェア モードを現在のファームウェア モードから他のモードに切り替えます。

Flexible Flash コントローラ カードの設定

始める前に

- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされている必要があります。

（注） このタスクを実行すると、ホストですべての仮想ドライブが再スキャンされるため、仮想ドライブに接続できなくなります。仮想ドライブを使用する前に Cisco Flexible Flash コントローラのプロパティを設定するか、このタスクを開始する前にホストの電源を切ることをお勧めします。

手順

ステップ 1 [Navigation] ペインの **[Storage]** タブをクリックします。

ステップ 2 [ストレージ（Storage）] タブの [Cisco FlexFlash] をクリックします。

ステップ 3 [Actions] 領域で、[Configure Cards] をクリックします。
[Configure Cards] ダイアログボックスが表示されます。

ステップ 4 [Configure Cards] ダイアログボックスで、次のフィールドを更新します。

名前	説明
[Mirror] オプション ボタン	次を入力します。 • [ミラー パーティション名（Mirror Partition Name）] フィールド：パーティションに割り当てる名前。 • [自動同期（Auto Sync）] チェックボックス：このチェックボックスをオンにすると、選択したプライマリ カードからのデータが自動的にセカンダリ カードと同期されます。 （注） • このオプションを選択するには、2 つのカードが必要です。 • このオプションを選択すると、セカンダリ カード上のデータが消去され、プライマリ カード上のデータで上書きされます。 • このステータスは、[物理ドライブ情報（Physical Driver Info）] タブに表示されます。 • [プライマリ カードの選択（Select Primary Card）] ドロップダウン：プライマリ カードとして設定するスロットを選択します。次のいずれかになります。 • **[Slot1]** • **[Slot2]**

名前	説明
[ユーティリティ（Util）] オプション ボタン	ユーティリティ モードでカードを設定する場合は、このオプションを選択します。ユーティリティ モードでカードを設定すると、次の状況になります。 • 選択したスロット内のカードで 4 つのパーティションが作成されて、SCU、HUU、ドライバの各ユーティリティに 1 つずつパーティションが割り当てられ、残りの 1 つはユーザが使用できるパーティションになり、カードは正常としてマークされます。 • もう一方のスロット内のカード（存在する場合）で単一のパーティションが作成されて、そのカードが正常としてマークされます。 • カードの読み取り/書き込みエラー カウントおよび読み取り/書き込みしきい値が 0 に設定されます。 • ホスト接続が中断される可能性があります。 • 設定済みカードがペアになります。 次を入力します。 • [ユーザ パーティション名（User Partition Name）] フィールド：ユーティリティ カードの 4 番目のパーティションに割り当てる名前。 • [非ユーティリティ カード パーティション名（Non Util Card Partition Name）] フィールド：2 つ目のカード（存在する場合）上の単一のパーティションに割り当てる名前。 • [ユーティリティ カードの選択（Select Util Card）] ドロップダウン：ユーティリティに設定するスロット。次のいずれかになります。 • **[Slot1]** • **[Slot2]** • [None]：サーバーに SD カードが 1 枚ある場合にのみ適用されます。

ステップ 5 [Configure Cards] ダイアログボックスで、次のフィールドを更新します。

名前	説明
[Mode] フィールド	モード タイプをミラーとして表示します。

名前	説明
[ミラー パーティション名（Mirror Partition Name）] フィールド	パーティションに割り当てる名前。
[自動同期（Auto Sync）] チェックボックス	このチェックボックスをオンにすると、選択したプライマリ カードからのデータが自動的にセカンダリ カードと同期されます。 （注） • このオプションを選択するには、カードが 2 枚必要です。 • このオプションを選択すると、セカンダリ カードのデータは消去され、プライマリ カードのデータで上書きされます。 • このステータスは、[仮想ドライブ（Virtual Drive）] タブに表示されます。
[Select Primary Card] ドロップダウン	プライマリ カードとして設定するスロット。次のいずれかになります。 • **[Slot1]** • **[Slot2]**
[仮想ドライブ（Virtual Drive）] ドロップダウン	仮想ドライブのタイプ。次のいずれかになります。 • **削除可能** • **削除不可能**

ステップ 6 [Save] をクリックします。

カードが選択したモードで設定されます。

Flexible Flash カードからのブート

Cisco Flexible Flash カード上に、ブート可能な仮想ドライブを指定できます。これは、サーバーに定義されているデフォルトのブート順に関係なく、サーバーが次に再始動されたときに、デフォルトのブート優先順位を上書きします。指定したブート デバイスは一度だけ使用されます。サーバーがリブートした後、この設定は無効になります。Cisco Flexible Flash カードが使用可能な場合にのみ、ブート可能な仮想ドライブを選択できます。それ以外の場合は、サーバーはデフォルトのブート順を使用します。

（注） サーバーをリブートする前に、選択した仮想ドライブが Cisco Flexible Flash カード上でイネーブルであることを確認します。[**Storage**] タブに移動してカードを選択し、[**Virtual Drive Info**] サブタブに進みます。

始める前に

- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされている必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [BIOS] をクリックします。

ステップ 3 [Actions] 領域で、[Configure Boot Override Priority] をクリックします。

[Boot Override Priority] ダイアログボックスが表示されます。

ステップ 4 [**Boot Override Priority**] ドロップダウン リストから、起動元の仮想ドライブを選択します。

ステップ 5 [適用（Apply）] をクリックします。

Flexible Flash コントローラのリセット

通常の操作では、Cisco Flexible Flash のリセットが必要になることはありません。テクニカル サポートの担当者から明確に指示された場合にだけ、この手順を実行することを推奨します。

（注） この操作は、Cisco Flexible Flash コントローラ上の仮想ドライブへのトラフィックを中断させます。

始める前に

- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされている必要があります。

手順

ステップ 1 [Storage Adapters] ペインの **[Cisco FlexFlash]** をクリックします。

ステップ 2 [Cisco FlexFlash] ペインの [Controller Info] タブをクリックします。
ステップ 3 [Actions] 領域で [Reset FlexFlash Controller] をクリックします。
ステップ 4 [OK] をクリックして確定します。

仮想ドライブの有効化

始める前に

- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされている必要があります。

（注） このタスクを実行すると、ホストですべての仮想ドライブが再スキャンされるため、仮想ドライブに接続できなくなります。仮想ドライブを使用する前に Cisco Flexible Flash コントローラのプロパティを設定することをお勧めします。

手順

ステップ 1 [Navigation] ペインの **[Storage]** タブをクリックします。
ステップ 2 [ストレージ（Storage）] タブの [Cisco FlexFlash] をクリックします。
ステップ 3 [Virtual Drive Info] タブをクリックします。
ステップ 4 [Virtual Drive Info] タブで、[Enable/Disable Virtual Drive(s)] をクリックします。
ステップ 5 [Enable/Disable VD(s)] ダイアログボックスで、有効にする仮想ドライブを選択します。
ステップ 6 [Save] をクリックします。
選択した仮想ドライブがホストで有効になります。

仮想ドライブの消去

始める前に

- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされている必要があります。

（注） このタスクを実行すると、ホストですべての仮想ドライブが再スキャンされるため、仮想ドライブに接続できなくなります。仮想ドライブを使用する前に Cisco Flexible Flash コントローラのプロパティを設定することをお勧めします。

手順

ステップ 1 [Navigation] ペインの **[Storage]** タブをクリックします。
ステップ 2 [ストレージ（Storage）] タブの [Cisco FlexFlash] をクリックします。
ステップ 3 [Virtual Drive Info] タブをクリックします。
ステップ 4 [Virtual Drive Info] タブで、[Erase Virtual Drive(s)] をクリックします。
ステップ 5 [Erase Virtual Drive(s)] ダイアログボックスで、消去する仮想ドライブを選択します。
ステップ 6 [Save] をクリックします。
選択した仮想ドライブのデータが消去されます。

仮想ドライブの同期

始める前に

- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされている必要があります。
- カードはミラー モードにする必要があります。

（注） このタスクを実行すると、ホストですべての仮想ドライブが再スキャンされるため、仮想ドライブに接続できなくなります。仮想ドライブを使用する前に Cisco Flexible Flash コントローラのプロパティを設定することをお勧めします。

手順

ステップ 1 [Navigation] ペインの **[Storage]** タブをクリックします。
ステップ 2 [ストレージ（Storage）] タブの [Cisco FlexFlash] をクリックします。
ステップ 3 [Virtual Drive Info] タブをクリックします。
ステップ 4 [Virtual Drive Info] タブで、[Sync Virtual Drive] をクリックします。
ステップ 5 確認ダイアログボックスで [OK] をクリックします。

仮想ドライブのハイパーバイザをプライマリ カードと同期させます。

ISO イメージ設定の追加

始める前に

- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされている必要があります。
- カードは Util モードで設定する必要があります。

（注） このタスクを実行すると、ホストですべての仮想ドライブが再スキャンされるため、仮想ドライブに接続できなくなります。仮想ドライブを使用する前に Cisco Flexible Flash コントローラのプロパティを設定するか、このタスクを開始する前にホストの電源を切ることをお勧めします。

手順

ステップ 1 [Navigation] ペインの **[Storage]** タブをクリックします。

ステップ 2 [ストレージ（Storage）] タブの [Cisco FlexFlash] をクリックします。

ステップ 3 [Virtual Drive Info] タブをクリックします。

ステップ 4 [Virtual Drive Info] タブで、イメージを追加する仮想ドライブを選択し、[Add Image] をクリックします。

ステップ 5 [Add Image] ダイアログボックスで、次のフィールドを更新します。

名前	説明
[ボリューム（Volume）] フィールド	マッピング用にマウントしたイメージの ID。次のいずれかになります。 • **[SCU]** • **[HUU]** • **[Drivers]**
[Mount Type] ドロップダウン リスト	マッピングのタイプです。次のいずれかになります。 • [NFS]：ネットワーク ファイル システム。 • [CIFS]：共通インターネット ファイル システム。

名前	説明
[リモート共有（Remote Share）] フィールド	マップするイメージの URL。形式は選択した [マウント タイプ（Mount Type）] に応じて異なります。 • [NFS]：**serverip:/share** のパスを使用します。 • [CIFS]：**//serverip/share** のパスを使用します。
[Remote File] フィールド	名前およびリモート共有の .iso ファイルの場所。次に、リモート共有ファイルの例を示します。 • [NFS]：**/softwares/ucs-cxx-scu-3.1.9.iso** • [CIFS]：**/softwares/ucs-cxx-scu-3.1.9.iso**
[マウント オプション（Mount Options）] フィールド	カンマ区切りリストで入力される業界標準のマウント オプション。オプションは選択した [マウント タイプ（Mount Type）] に応じて異なります。 [NFS] を使用している場合、フィールドを空白にしておくか、次のうちの 1 つ以上を入力します。 • **ro** • **rw** • **nolock** • **noexec** • **soft** • **port=VALUE** • **timeo=VALUE** • **retry=VALUE** [CIFS] を使用している場合、フィールドを空白にしておくか、次のうちの 1 つ以上を入力します。 • **soft** • **nounix** • **noserverino**
[ユーザ名（User Name）] フィールド	指定した [マウント タイプ（Mount Type）] のユーザ名（必要な場合）。
[パスワード（Password）] フィールド	選択されたユーザー名のパスワード（必要な場合）。

ステップ 6 [保存（Save）] をクリックします。

ISO イメージの更新

始める前に

- このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされている必要があります。
- このタスクは、カードが [Util] モードで設定されている場合にのみ使用できます。

（注） このタスクを実行すると、ホストですべての仮想ドライブが再スキャンされるため、仮想ドライブに接続できなくなります。仮想ドライブを使用する前に Cisco Flexible Flash コントローラのプロパティを設定するか、このタスクを開始する前にホストの電源を切ることをお勧めします。

手順

ステップ 1 [Navigation] ペインの **[Storage]** タブをクリックします。

ステップ 2 [ストレージ（Storage）] タブの [Cisco FlexFlash] をクリックします。

ステップ 3 [Virtual Drive Info] タブをクリックします。

ステップ 4 [Virtual Drive Info] タブで、イメージを更新する仮想ドライブを選択し、[Update Image] をクリックします。

（注） SCU および HUU の更新には最大 1 時間、ドライバの更新には最大 5 時間かかる場合があります。

ISO イメージのマップ解除

始める前に

- このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされている必要があります。

（注） このタスクを実行すると、ホストですべての仮想ドライブが再スキャンされるため、仮想ドライブに接続できなくなります。仮想ドライブを使用する前に Cisco Flexible Flash コントローラのプロパティを設定するか、このタスクを開始する前にホストの電源を切ることをお勧めします。

手順

ステップ 1 [Navigation] ペインの **[Storage]** タブをクリックします。

ステップ 2 [ストレージ（Storage）] タブの [Cisco FlexFlash] をクリックします。

ステップ 3 [Virtual Drive Info] タブをクリックします。

ステップ 4 [Virtual Drive Info] タブで、イメージのマッピングを解除する仮想ドライブを選択し、[Unmap Image] をクリックします。

Cisco Flexible Flash カード設定のリセット

Cisco Flexible Flash カードのスロットの設定をリセットすると、次の状況が発生します。

- 選択したスロット内のカードは、正常なプライマリとしてマークされます。
- もう一方のスロットのカードは、非正常なセカンダリアクティブとしてマークされます。
- 1 つの RAID パーティションが作成されます。
- カードの読み取り/書き込みエラー カウントおよび読み取り/書き込みしきい値が 0 に設定されます。
- ホスト接続が中断される可能性があります。

最新バージョンにアップグレードして設定リセットのオプションを選択すると、単一のハイパーバイザ（HV）パーティションが作成されて、既存の 4 つのパーティション構成は消去されます。これにより、データを損失する可能性もあります。損失したデータを取得するには、HV パーティションにまだデータを書き込んでいないこと、および前のバージョンにダウングレードすることが条件となります。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Storage Adapters] ペインの **[Cisco FlexFlash]** をクリックします。

ステップ 2 [Cisco FlexFlash] ペインで、[コントローラ情報（Controller Info）] タブをクリックします。

ステップ 3 [アクション（Actions）] エリアで [パーティション デフォルトへのリセット（Reset Partition Defaults）] をクリックします。

ステップ 4 [パーティション デフォルトへのリセット（Reset Partition Defaults）] ダイアログボックスで、次のフィールドを更新します。

名前	説明
[スロット（Slot）] オプション ボタン	カードに [プライマリ - 正常（primary healthy）] のマークを付けるスロットを選択します。 他のスロットにカードがある場合は、[セカンダリアクティブ - 非正常（secondary-active unhealthy）] のマークが付けられます。
[パーティションデフォルトへのリセット（Reset Partition Defaults）] ボタン	選択したスロットの設定をリセットします。
[Cancel] ボタン	変更を行わずにダイアログボックスを閉じます。

ステップ 5 **[はい（Yes）]** をクリックします。

Cisco Flexible Flash カードの設定の保持

次の状況では、ファームウェア バージョン 253 以降のカードをサポートする FlexFlash の設定を保持できます。

- 2 つの非ペアの FlexFlash があります
- 単一 FlexFlash からサーバが稼働していて、非ペアの FlexFlash が他のスロットにあります。
- 1 つの FlexFlash がファームウェア バージョン 253 をサポートし、もう 1 つの FlexFlash はパーティション化されていません。

設定を保持する場合、次の状況が発生します。

- 選択されたスロットの FlexFlash の設定は、もう 1 つのカードにコピーされます。
- 選択したスロット内のカードは、正常なプライマリとしてマークされます。
- セカンダリ スロットのカードは、非正常なセカンダリ アクティブとしてマークされます。

始める前に

- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Storage Adapters] ペインの **[Cisco FlexFlash]** をクリックします。

ステップ 2 [Cisco FlexFlash] ペインで、[コントローラ情報（Controller Info）] タブをクリックします。

ステップ 3 [アクション（Actions）] エリアの [カード設定の同期（Synchronize Card Configuration）] をクリックします。

ステップ 4 [カード設定の同期（Synchronize Card Configuration）] ダイアログボックスで、次のフィールドを更新します。

名前	説明
[スロット（Slot）] オプションボタン	設定を保持するスロットを選択します。選択したスロットから他のスロットのカードに設定がコピーされ、選択したスロットのカードには [プライマリ - 正常（primary healthy）] のマークが付けられます。
[カード設定を同期（Synchronize Card Configuration）] ボタン	選択したカードのタイプが SD253 で単一の HV 設定が存在する場合にのみ、選択したカードから設定をコピーします。
[Cancel] ボタン	変更を行わずにダイアログボックスを閉じます。

ステップ 5 **[はい（Yes）]** をクリックします。

FlexFlash ログの詳細の表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで [Cisco Flexible Flashコントローラ（Cisco Flexible Flash Controller）] をクリックします。

ステップ 3 [FlexFlashログ（FlexFlash Logs）] タブの [FlexFlashログテーブル（FlexFlash LogTable）] 領域で、次のフィールドを確認します。

名前	説明
[Time] カラム	イベントが発生した日時。

名前	説明
[Severity] カラム	イベントのシビラティ（重大度）。次のいずれかになります。 • 緊急（Emergency） • アラート（Alert） • クリティカル（Critical） • エラー（Error） • Warning • 情報 • 注記 • デバッグ
[Description] カラム	イベントの説明。

ステップ 4 [FlexFlashログ（FlexFlash Logs）] タブの [アクション（Actions）] 領域で、次のフィールドを確認します。

名前	説明
[表示（Show）] ドロップダウン リスト	フィルタを使用して Cisco IMC ログ エントリを表示する方法をカスタマイズします。これらの内容は次のとおりです。 • [クイックフィルタ（Quick Filter）]：デフォルト ビュー • **[Advanced Filter]**：1 つ以上の条件に基づきログエントリを表示するフィルタ オプション。マッチング ルールを使用して、[フィルタ（Filter）] フィールドで指定したルールのすべてまたはいくつかのルールの組み合わせと一致するエントリを表示できます。 新しいフィルタ条件を追加するには、[+] をクリックします。 設定したフィルタ条件に一致するエントリを表示するには、[Go] をクリックします。 設定したフィルタ基準は、[Save] アイコンをクリックして保存することができます。これはユーザー定義のフィルタになり、後で使用できます。 （注） ユーザ定義のフィルタは [プリセット フィルタの管理（Manage Preset Filters）] ダイアログボックスに表示されます。 • [すべて（All）]：すべてのエントリが表示されます。 • [プリセット フィルタの管理（Manage Preset Filters）]：ユーザ定義のフィルタが表示されます。このダイアログボックスで、ユーザ定義のフィルタを編集したり削除したりできます。 • [事前定義されたフィルタのリスト（List of pre-defined filters）]：システム定義のフィルタが表示されます。

名前	説明
[フィルタ（Filter）] アイコン	クイック フィルタ フィールドを表示または非表示にします。
[列（Column）] ドロップダウン リスト	表示する列を選択できます。

ステップ 5 [FlexFlashログ（FlexFlash Logs）] タブの [ログナビゲーションツールバー（Log Navigation Toolbar）] 領域で、次のフィールドを確認します。

名前	説明
<<Newest	イベントが1ページに入りきらない場合、このリンクをクリックすると最新のエントリが表示されます。 表示されるエントリの合計数は [Entries per Page] ドロップダウン リストの設定によって異なります。
<Newer	イベントが1ページに入りきらない場合、このリンクをクリックすると次ページが表示され、現在表示されているエントリより新しいエントリを確認できます。
[Log Entries] フィールド	このフィールドは、表に現在表示されているのがどのログ エントリなのかを示します。
Older>	イベントが1ページに入りきらない場合、このリンクをクリックすると次ページが表示され、現在表示されているエントリより古いエントリを確認できます。
Oldest>>	イベントが1ページに入りきらない場合、このリンクをクリックすると最も古いエントリが表示されます。
[ページ番号（Page Number）] ドロップダウン リスト	特定のページに移動できます。ドロップダウン リストからページ番号を選択します。
[行数（Number of Rows）] フィールド	現在のページに表示されている行数が表示されます。

FlexUtil コントローラの管理

C シリーズ M5 ラックマウント サーバーは、サーバー ソフトウェア ツールおよびユーティリティのストレージ用に microSD メモリ カードをサポートします。ライザー 1 にはこの microSD メモリ カード スロットがあります。Cisco FlexUtil は、32 GB の microSD カードのみをサポートします。

次のユーザー認識可能なパーティションが microSD カードに存在します。

- Server Configuration Utility（SCU）–1.25 GB
- 診断-0.25 GB
- Host Update Utility（HUU）–1.5 GB
- ドライバ–8 GB
- ユーザー（User）

（注） MicroSD の各パーティションの数とサイズは固定されています。

いつでも、ホストに2つのパーティションをマップできます。（ユーザーパーティションを除く）これらのパーティションは、CIFS または NFS 共有により更新できます。第 2 レベルの BIOS ブート順序のサポートは、すべての起動可能なパーティションにも使用できます。

（注） ユーザーパーティションはストレージにのみ使用する必要があります。このパーティションは OS のインストールをサポートしていません。

FlexUtil コントローラのプロパティの設定

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。

ステップ 2 [Storage] メニューで [Cisco FlexUtil Controller] をクリックします。

ステップ 3 [一般（General）] タブの [操作（Actions）] 領域で、[運用プロファイルの設定（Configure Operational Profile）] をクリックします。

ステップ 4 [運用プロファイル（Operational Profile）] ダイアログボックスで、次のフィールドを更新します。

名前	説明
[Controller] フィールド	選択された Flex Util コントローラのシステム定義名。 この名前は変更できません。

名前	説明
[読み取りエラーしきい値（Read Error Threshold）] フィールド	Flex Util カードへのアクセス時の読み取りエラーの許容数。あるカードでの読み取りエラーの数がこのしきい値を超えた場合、そのカードには正常でないというマークが付けられます。 読み取りエラーしきい値を指定するには、1 以上 255 以下の整数を入力します。検出されたエラー数に関係なく、カードが無効にならないように指定するには、**0**（ゼロ）を入力します。
[書き込みエラーしきい値（Write Error Threshold）] フィールド	Flex Util カードへのアクセス時の書き込みエラーの許容数。あるカードでの書き込みエラーの数がこのしきい値を超えた場合、そのカードには正常でないというマークが付けられます。 書き込みエラーしきい値を指定するには、1 以上 255 以下の整数を入力します。検出されたエラー数に関係なく、カードが無効にならないように指定するには、**0**（ゼロ）を入力します。

FlexUtil カード設定のリセット

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。

ステップ 2 [Storage] メニューで [Cisco FlexUtil Controller] をクリックします。

ステップ 3 [一般（General）] タブの [操作（Actions）] 領域で、[カード設定のリセット（Reset Card Configuration）] をクリックします。

このアクションは、FlexUtil カードの設定をデフォルトの設定にリセットします。

Cisco FlexUtil コントローラのプロパティの表示

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。

ステップ 2 [Storage] メニューで [Cisco FlexUtil Controller] をクリックします。

ステップ 3 [一般（General）] タブの [一般（General）] 領域で、次のフィールドを確認します。

名前	説明
[Product Name] フィールド	製品の名前。
[コントローラ名（Controller Name）] フィールド	コントローラの名前。
[コントローラ ステータス（Controller Status）] フィールド	FlexUtil カードの現在のステータス。次のいずれかになります。 • カードが存在しません • カードに異常があります • メタデータ読み取りエラー（**Metadata Read Error**） • カード アクセス エラー • 無効なカード サイズ（**Invalid Card size**） • メタデータが障害発生状態です • パーティションがありません。リセットが必要です • 無効なパーティションです。リセットが必要です • カードが書き込み禁止です

名前	説明
[Internal State] フィールド	コントローラの内部ステート。次のいずれかになります。 • [未初期化（Uninitialized）] : FlexUtil モニタリングが初期化されていません。 • [初期化中（Initializing）] : FlexUtil モニタリングが初期化中です。 • [設定中（Configuring）] : コントローラは FlexUtil カードの設定を確認しています。 • [OK] : FlexUtil カードはホストに接続されていません。 • [Connecting] : コントローラはホストに接続しようとしています。 • [Connected] : コントローラはホストに接続されています。 • **[Failed]** : コントローラに障害が発生しました。詳細については、**[Controller Status]** フィールドを参照してください。 • [削除中（Erasing）] : FlexUtil カードを削除しています。 • [更新中（Updating）] : FlexUtil カードを更新しています。 • [リセット中（Resetting）] : カードの設定がリセットされます。

ステップ 4 [一般（General）] タブの [物理ドライブ数（Physical Drive Count）] 領域で、次のフィールドを確認します。

名前	説明
[Physical Drive Count] フィールド	サーバーで検出された FlexUtil カードの数。

ステップ 5 [一般（General）] タブの [仮想ドライブ数（Virtual Drive Count）] 領域で、次のフィールドを確認します。

名前	説明
[Virtual Drive Count] フィールド	サーバーに搭載された FlexUtil カード上で設定されている仮想ドライブの数。

物理ドライブのプロパティの表示

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。

ステップ 2 [Storage] メニューで [Cisco FlexUtil Controller] をクリックします。

ステップ 3 [物理ドライブ（Physical Drive）]タブの[一般（General）]領域で、次のフィールドを確認します。

名前	説明
ドライブ	デバイスの名前。
ドライブ ステータス	ドライブが存在するかどうかを示します。
[Serial Number] フィールド	FlexUtil カードのシリアル番号。
[Manufacturer ID] フィールド	FlexUtil カードの製造業者 ID。
[OEM ID] フィールド	FlexUtil カードの OEM ID（該当する場合）。
[Product Name] フィールド	FlexUtil カードの名前。
[Product Revision] フィールド	FlexUtil カードのリビジョン番号。
[Manufacturing Date] フィールド	FlexUtil カードが製造された日付（mm/yy 形式）。
[Write Enabled] フィールド	このフィールドに [true] と表示されている場合、FlexUtil カードで書き込みが受け入れられます。
[Block Size] フィールド	FlexUtil カード上のブロック サイズ（バイト単位）。
[Capacity] フィールド	FlexUtil カードの容量（メガバイト単位）。

名前	説明
ヘルス（**Health**）	次のいずれかになります。 • **正常** • **異常**

ステップ 4 [物理ドライブ（Physical Drive）] タブの [エラーカウンタ（Error Counters）] 領域で、次のフィールドを確認します。

名前	説明
[読み取りエラーしきい値（Read Error Threshold）] フィールド	FlexUtil カードへのアクセス時の読み取りエラーの許容数。
[Read Error Count] フィールド	FlexUtil カードが最初にインストールされてから現在までに I/O トラフィックの処理中に発生した読み取りエラーの数。
[Write Error Threshold] フィールド	FlexUtil カードへのアクセス時の書き込みエラーの許容数。
[書き込みエラー カウント（Write Error Count）] フィールド	FlexUtil カードが最初にインストールされてから現在までに I/O トラフィックの処理中に発生した書き込みエラーの数。

ステップ 5 [物理ドライブ（Physical Drive）] タブの [パーティション（Partition）] 領域で、次のフィールドを確認します。

名前	説明
[パーティション カウント（Partition Count）] フィールド	FlexUtil カード上のパーティションの数。
[Drives Enabled] フィールド	FlexUtil カード上のアクセスが有効になっている仮想ドライブ。

仮想ドライブのプロパティの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [Storage] メニューで [Cisco FlexUtil Controller] をクリックします。

ステップ 3 [物理ドライブ（Physical Drive）] タブの [仮想ドライブ（Virtual Drives）] 領域で、次のフィールドを確認します。

名前	説明
[Virtual Drive] カラム	仮想ドライブの名前。
[ID] カラム	仮想ドライブ ID。
LUN ID	LUN ID（使用可能な場合）。
[Drive Scope] カラム	仮想ドライブがどのように設定されているか。これは常に [非RAID（NON RAID）] になります。
[サイズ（Size）] カラム	仮想ドライブのサイズ（MB 単位）。
[Drive Status] カラム	デバイスの状態。次のいずれかになります。 • **正常** • **異常**
[Host Accessible] カラム	仮想ドライブがホストにマップされているかどうかを示します。次のいずれかになります。 • **接続中** • **未接続** このフィールドに [接続中（connected）] と表示される場合、仮想ドライブがホストにマップされていることを意味します。
[Drive Type] カラム	ドライブのタイプ。これは常に [削除可能（Removable）] になります。
[Operation in Progress] カラム	進行中の操作。次のいずれかになります。 • **削除中（Erasing）** • **削除保留中（Erase-Pending）** • **更新** • **更新保留中（Update-Pending）** • **該当なし** （注） 何らかの操作の実行中にCisco IMCを再起動すると、その操作は中断され再起動後に操作の状態は NA に設定されます。

名前	説明
[最後の操作ステータス（Last Operation Status）] 列	直前の操作の状態。次のいずれかになります。 • **削除成功（Erase-Success）** • **削除失敗（Erase-Failed）** • **更新成功（Update-Success）** • **UPDATE_FAILED**
[常駐画像（Resident Image）]	仮想ドライブに存在するイメージ ファイルの名前を表示します。

ステップ 4 [物理ドライブ（Physical Drive）] タブの [アクション（Actions）] 領域で、次のフィールドを確認します。

名前	説明
仮想ドライブを有効/無効にします	仮想ドライブを有効/無効にできます。
仮想ドライブの消去（Erase Virtual Drive(s)）	仮想ドライブを FAT 32 形式にフォーマットできます。 （注） 進行中の消去操作または保留中の消去操作を取り消すことはできません。
画像の追加（Add Image）	SCU、HUU、診断、およびドライバの ISO イメージの設定を追加できます。
Update Image	仮想ドライブをISOイメージで更新できます。 （注） • 任意の仮想ドライブで削除または更新が進行中または保留状態の時は、**[Virtual]** タブで使用可能ないずれのアクションも実行できません。 • 進行中の更新処理をキャンセルするには、[更新のキャンセル（Cancel Update）] ボタンを使用します。
更新のキャンセル	進行中の更新処理を取り消します。

名前	説明
イメージのマップ解除（**Unmap Image**）	ISO イメージの設定を削除できます。

仮想ドライブへのイメージのマッピング

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。

ステップ 2 [Storage] メニューで [Cisco FlexUtil Controller] をクリックします。

ステップ 3 [仮想ドライブ（Virtual Drives）] タブをクリックします。

ステップ 4 [仮想ドライブ（Virtual Drives）] 領域で、仮想ドライブを選択して、[イメージの追加（Add Image）] をクリックします。

ステップ 5 [新しいイメージの追加（Add New Image）] ダイアログボックスで、次のフィールドを更新します。

名前	説明
[ボリューム（Volume）] フィールド	マッピング用にマウントしたイメージの ID。次のいずれかになります。 • **[SCU]** • **診断** • **[HUU]** • **[Drivers]**
[Mount Type] ドロップダウンリスト	マッピングのタイプです。次のいずれかになります。 • [NFS]：ネットワーク ファイル システム。 • [CIFS]：共通インターネット ファイル システム。 • [WWW(HTTP/HTTPS)]：HTTP ベースまたは HTTPS ベースのシステム。

名前	説明
[リモート共有（Remote Share）] フィールド	マップするイメージの URL。形式は選択した [マウント タイプ（Mount Type）] に応じて異なります。 • [NFS]：**serverip:/share** のパスを使用します。 • [CIFS]：**//serverip/share path** を使用します。 • [WWW(HTTP/HTTPS)]：http[s]://serverip/share を使用します。
[Remote File] フィールド	名前およびリモート共有の .iso ファイルの場所。次に、リモート共有ファイルの例を示します。 • [NFS]：**/softwares/ucs-cxx-scu-3.1.9.iso** • [CIFS]：**/softwares/ucs-cxx-scu-3.1.9.iso** • [WWW(HTTP/HTTPS)]：**http[s]://softwares/ucs-cxx-scu-3.1.9.iso**

名前	説明
[マウント オプション（Mount Options）] フィールド	カンマ区切りリストで入力される業界標準のマウント オプション。オプションは選択した [マウント タイプ（Mount Type）] に応じて異なります。 [NFS] を使用している場合、フィールドを空白にしておくか、次のうちの 1 つ以上を入力します。 • **ro** • **rw** • **nolock** • **noexec** • **soft** • **port=VALUE** • **timeo=VALUE** • **retry=VALUE** [CIFS] を使用している場合、フィールドを空白にしておくか、次のうちの 1 つ以上を入力します。 • **soft** • **nounix** • **noserverino** [WWW(HTTP/HTTPS)] を使用している場合は、このフィールドを空白のままにするか、次のように入力します。 • **noauto** （注） イメージをマウントする前に、Cisco IMC はサーバーに ping を実行することによって、エンドサーバーへの到達可能性の確認を試みます。 • **username=VALUE** • **password=VALUE**

ステップ 6 省略可能：[イメージの追加（Add Image）] ボタンはトグル ボタンです。イメージをマップした後、ドライブから同じイメージを解除する場合は、仮想ドライブを選択して [イメージのマップ解除（Unmap Image）] をクリックします。

仮想ドライブ上のイメージの更新

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [Storage] メニューで [Cisco FlexUtil Controller] をクリックします。

ステップ 3 [仮想ドライブ（Virtual Drives）] タブをクリックします。

ステップ 4 [仮想ドライブ（Virtual Drives）] 領域で、イメージを更新する仮想ドライブを選択し、[イメージの更新（Update Image）] をクリックします。

ステップ 5 省略可能：実行中の更新操作をキャンセルする場合は、[更新のキャンセル（Cancel Update）] をクリックします。

仮想ドライブからのイメージのマッピング解除

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [Storage] メニューで [Cisco FlexUtil Controller] をクリックします。

ステップ 3 [仮想ドライブ（Virtual Drives）] タブをクリックします。

ステップ 4 [仮想ドライブ（Virtual Drives）] 領域で、イメージを削除する仮想ドライブを選択し、[イメージのマップ解除（Unmap Image）] をクリックします。

仮想ドライブの消去

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。
ステップ 2 [Storage] メニューで [Cisco FlexUtil Controller] をクリックします。
ステップ 3 [仮想ドライブ（Virtual Drives）] タブをクリックします。
ステップ 4 [仮想ドライブ（Virtual Drives）] 領域で、削除する仮想ドライブを選択して、[仮想ドライブの削除（Erase Virtual Drive）] をクリックします。

Cisco ブート最適化 M.2 Raid コントローラ

Cisco ブート最適化 M. 2 Raid コントローラの詳細の表示

始める前に

サーバの電源が投入されている。

手順

ステップ 1 [Navigation] ペインの [Storage] メニューをクリックします。
ステップ 2 **[Storage (ストレージ)]** メニューで、適切な M.2 コントローラをクリックします。
ステップ 3 [Controller] 領域に、[Controller Info] タブがデフォルトで表示されます。
ステップ 4 [Work (作業)] ペインの **[Health/Status (ヘルス/ステータス)]** 領域で、次の情報を確認します。

名前	説明
[Composite Health] フィールド	コントローラ、接続ドライブ、およびバッテリ バックアップ ユニットの全体的な状態。次のいずれかになります。 • **Good** • **[Moderate Fault]** • **[Severe Fault]** • 該当なし

名前	説明
[Controller Status] フィールド	コントローラの現在のステータス。次のいずれかになります。 • [Optimal]：コントローラは正常に機能しています。 • [Failed]：コントローラが機能していません。

ステップ 5 [Firmware Versions] 領域で、次の情報を確認します。

名前	説明
[Product Name] フィールド	Cisco ブート最適化 M.2 Raid コントローラの名前。
[Product PID (製品 PID)] フィールド	Cisco ブート最適化 M.2 Raid コントローラの製品 PID。
[Serial Number] フィールド	Cisco ブート最適化 M.2 Raid コントローラのシリアル番号。
[Firmware Package Build] フィールド	アクティブなファームウェアパッケージのバージョン番号。 ファームウェア コンポーネントのバージョン番号については、[Running Firmware Images] 領域を参照してください。

ステップ 6 [PCI Info] 領域で、次の情報を確認します。

名前	説明
[PCI Slot] フィールド	コントローラが配置されている PCIe スロットの名前。
[Vendor ID] フィールド	PCI ベンダー ID（16 進）。
[Device ID] フィールド	PCI デバイス ID（16 進）。
[SubVendor ID] フィールド	PCI サブベンダー ID（16 進）。
[SubDevice ID] フィールド	PCI サブデバイス ID（16 進）。

ステップ 7 [Manufacturing Data] 領域で、次の情報を確認します。

名前	説明
[Manufactured Date] フィールド	Cisco Boot 最適化 M. 2 Raid コントローラの製造日 (yyyy-mm-dd 形式)。
[Revision No] フィールド	ボードのリビジョン番号（存在する場合）。

ステップ 8 **[Next Patrol Read Schedule (次のパトロール読み込みスケジュール)]** 領域で、次の情報を確認します。

名前	説明
[PR State (PR 状態)] フィールド	M. 2 Raid コントローラのパトロール読み取り状態。次のいずれかを指定できます。 • **ready** • **stopped** • **active** デフォルト状態: **N/A**。
[PR Schedule Mode (PR スケジュールモード)] フィールド	M. 2 Raid コントローラのパトロール読み取りスケジュール モード。 **[PR Schedule Mode (PR スケジュール モード)]** は、デフォルトでは**手動**です。

ステップ 9 [Running Firmware Images] 領域で、次の情報を確認します。

名前	説明
[BIOS Version] フィールド	BIOS オプション PROM のバージョン番号。
[ファームウェアのバージョン（Firmware Version）] フィールド	アクティブなファームウェアのバージョン番号。
[Boot Block Version] フィールド	ブート ブロックのバージョン番号。

ステップ 10 [Virtual Drive Count] 領域で、次の情報を確認します。

名前	説明
[Virtual Drive Count] フィールド	コントローラ上で設定されている仮想ドライブの数。
[Degraded Drive Count] フィールド	コントローラ上の低下状態の仮想ドライブの数。

名前	説明
[Offline Drive Count] フィールド	コントローラ上の障害が発生した仮想ドライブの数。

ステップ 11 [Physical Drive Count] 領域で、次の情報を確認します。

名前	説明
[Disk Present Count] フィールド	コントローラ上に存在する物理ドライブの数。
[Critical Disk Count (クリティカル ディスク数)] フィールド	コントローラ上のクリティカル状態の物理ドライブの数。
[Failed Disk Count] フィールド	コントローラ上の障害が発生した物理ドライブの数。

ステップ 12 [Capabilities] 領域で、次の情報を確認します。

名前	説明
[RAID Levels Supported] フィールド	コントローラでサポートされるRAID レベル。 [Raid 1]：単純なミラーリング。

ステップ 13 [HW Configuration] 領域で、次の情報を確認します。

名前	説明
[Number of Backend Ports] フィールド	コントローラ上の SATA ポートの数。

Viewing Physical Drive Info for Cisco Boot Optimized M.2 Raid Controller

始める前に

サーバの電源が投入されている。

手順

ステップ 1 [Navigation] ペインの [Storage] メニューをクリックします。

ステップ 2 **[Storage (ストレージ)]** メニューで、適切な M.2 コントローラをクリックします。

ステップ 3 **[Physical Drive Info (物理ドライブ情報)]** タブをクリックし、**[Physical Drives (物理ドライブ)]** 領域で次の情報を確認します。

名前	説明
[Controller] カラム	コントローラ ドライブが配置されている PCIe スロットの名前。
[Physical Drive Number] カラム	物理ドライブ番号。
[ステータス（Status）] カラム	物理ドライブのステータス。次のいずれかになります。 • **JBOD**—ドライブが JBOD モードです。 • [**Failed**]：ドライブは使用中ですが、障害が発生しています。 • [**Offline**]：ドライブはオフラインでアクセスできません。 • [**Online**]：ドライブはドライブ グループの一部として使用されています。 • [**Predicted Failure**]：ドライブはコントローラによって失敗すると即座にマークされています。 • [**Rebuild**]：ドライブは現在再構築されています。 • **不明**—ドライブ ステータスが不明です。
[State] カラム	物理ドライブの状態。次のいずれかになります。 • **JBOD**—物理ドライブが JBOD 状態です。 • **オンライン**：ドライブはドライブ グループの一部として使用されています。 • **失敗**: 物理ドライブは障害状態です。 • **再構築**— 物理ドライブが再構築状態です。

名前	説明
[Health] カラム	物理ドライブの状態。次のいずれかになります。 • **Good** • **[Moderate Fault]** • **[Severe Fault]** [状況（Health）] フィールドには、テキストと色分けされたアイコンの両方が含まれます。色分けされたアイコンが表示される場合は、次のようになります。 • 緑色: 通常の動作を示します。 • 黄色: 情報メッセージです。 • 赤色: 警告、重大、および回復不能なエラーを示します。
[ドライブ ファームウェア（Drive Firmware）] カラム	ドライブで実行されているファームウェアバージョン。
[Model] カラム	ドライブのベンダー名。
[Type] カラム	ドライブがハード ドライブ（HDD）であるか、ソリッド ステート ドライブ（SSD）であるか。

ステップ 4 **[Health/Status (ヘルス/ステータス)]** 領域で、次の情報を確認します。

名前	説明
[ヘルス（Health）]	物理ドライブのヘルス状況。次のいずれかになります。 • **Good** • **[Moderate Fault]** • **[Severe Fault]**

名前	説明
状態	物理ドライブの状態。次のいずれかになります。 • **JBOD**—物理ドライブがJBOD状態です。 • **オンライン**：ドライブはドライブ グループの一部として使用されています。 • **失敗**: 物理ドライブは障害状態です。 • **再構築**— 物理ドライブが再構築状態です。
Status（ステータス）	物理ドライブのステータス。次のいずれかになります。 • **JBOD**—ドライブが JBOD モードです。 • [**Failed**]：ドライブは使用中ですが、障害が発生しています。 • [**Offline**]：ドライブはオフラインでアクセスできません。 • [**Online**]：ドライブはドライブ グループの一部として使用されています。 • [**Predicted Failure**]：ドライブはコントローラによって失敗すると即座にマークされています。 • [**Rebuild**]：ドライブは現在再構築されています。 • **不明**—ドライブ ステータスが不明です。
[Fault]	このフィールドに **[true]** が表示される場合、ドライブは **[failed (失敗)]**状態です。
オンライン	このフィールドに **[true]** が表示される場合、ドライブは **[online (オンライン)]** 状態です。

ステップ 5 [Smart Information] 領域で、次の情報を確認します。

名前	説明
電源の再投入回数	製造された時点からドライブの電源が再投入された回数。[Power Cycle Count (電源の再投入回数)] フィールド

名前	説明
電源オン時間	ドライブが「電源オン」モードにある時間の合計数。
残量 (パーセンテージ)	M.2 ドライブに残っている書き込みサイクル数。たとえば、M.2 ドライブがライフタイム中に 100 の書き込みサイクルに対応でき、15 の書き込みを完了している場合、ドライブの残りのライフのパーセンテージは 85% です。パーセンテージの各範囲は異なる色で表されます。たとえば、75% ～ 100% は緑、1% ～ 25% は赤で表されます。
消耗状態 (日数)	M.2 ドライブが書き込みサイクルを実行した日数。
動作温度 (°C)	選択した M.2 ドライブが選択時点で動作しているドライブの現在の温度。
使用された予約済み容量の割合	M.2 ドライブによって消費された総容量（そのために予約されている割合のうちの）。
前回の更新時刻	ドライブが最後に更新されてからの時間。

ステップ 6 **[Operation Status (動作ステータス)]** 領域で、次の情報を確認します。

名前	説明
[Operation]	ドライブで進行中の現在の操作。次のいずれかになります。 • **Rebuild in progress** • **Patrol read in progress**
[Progress in %]	操作の進行状況のパーセンテージ。

ステップ 7 **[Inquiry Data (インクエリ データ)]** 領域で、次の情報を確認します。

名前	説明
製品 ID	ドライブの製品 ID。通常、このフィールドにはドライブのモデル番号が表示されます。
Vendor	ドライブのベンダー。
ドライブ ファームウェア	ドライブ上のアクティブなファームウェアバージョン。

名前	説明
ドライブのシリアル番号	ドライブのシリアル番号。

ステップ 8 **[General (全般)]** 領域で、次の情報を確認します。

名前	説明
スロット番号	物理ドライブが存在するスロット番号。
未加工サイズ	フォーマットに使用された領域を含むドライブの容量（MB 単位）。
ネゴシエートされたリンク速度	ドライブとコントローラ間のリンクの速度。
メディア タイプ	ドライブ タイプは、ソリッド ステート ドライブ (SSD) です。
インターフェイス タイプ	ドライブのインターフェイス タイプ。
エンクロージャ関連	ドライブをコントローラに直接接続するのか否かを示します。ここに表示される値は次のとおりです。 **直接接続**: ドライブはコントローラに直接接続されます。

Cisco ブート最適化 M.2 Raid コントローラの仮想ドライブ情報の表示

手順

ステップ 1 [Navigation] ペインの [Storage] メニューをクリックします。

ステップ 2 **[Storage (ストレージ)]** メニューで、M.2 Raid コントローラをクリックします。

ステップ 3 **[Virtual Drive Info (仮想ドライブ情報)]** タブを選択し、**[Virtual Drives (仮想ドライブ)]** 領域で次の情報を確認します。

名前	説明
[Virtual Drive Number] カラム	仮想ドライブの番号。
[Name] カラム	仮想ドライブの名前。

名前	説明
[ステータス（Status）] カラム	仮想ドライブの状態。次のいずれかになります。 • **部分的に低下**: 仮想ドライブまたは物理ドライブの再構築が進行中です。 • **低下**: ドライブの 1 つ以上のスパンに冗長性がありません。 • **オフライン**: ドライブはホストに表示されません。 • **不明**: 仮想ドライブの状態は不明です。 • **最適**: ドライブには完全な冗長性があります。
[状態（Health）] カラム	仮想ドライブの状態。次のいずれかになります。 • **Good** • **[Moderate Fault]** • **[Severe Fault]** [状況（Health）] フィールドには、テキストと色分けされたアイコンの両方が含まれます。色分けされたアイコンが表示される場合は、次のようになります。 • 緑色: 通常の動作を示します。 • 黄色: 情報メッセージです。 • 赤色: 警告、重大、および回復不能なエラーを示します。
[Size] カラム	ドライブの容量（MB 単位）。
[RAID Level] カラム	仮想ドライブ上の RAID レベル。 [Raid 1] : 単純なミラーリング。

ステップ 4 **[General (全般)]** 領域で、次の情報を確認します。

名前	説明
名前（Name）	仮想ドライブの名前。

名前	説明
ストリップ サイズ	各ストライプのサイズ（KB 単位）。

ステップ 5 **[Physical Drive (物理ドライブ)]** 領域で、次の情報を確認します。

名前	説明
物理ドライブ番号	物理ドライブ番号。
状態	物理ドライブの状態。次のいずれかになります。 • **JBOD**—物理ドライブが JBOD 状態です。 • **オンライン**：ドライブはドライブ グループの一部として使用されています。 • **失敗**: 物理ドライブは障害状態です。 • **再構築**— 物理ドライブが再構築状態です。
Status（ステータス）	物理ドライブのステータス。次のいずれかになります。 • **JBOD**—ドライブが JBOD モードです。 • [**Failed**]：ドライブは使用中ですが、障害が発生しています。 • [**Offline**]：ドライブはオフラインでアクセスできません。 • [**Online**]：ドライブはドライブ グループの一部として使用されています。 • [**Predicted Failure**]：ドライブはコントローラによって失敗すると即座にマークされています。 • [**Rebuild**]：ドライブは現在再構築されています。 • **不明**—ドライブ ステータスが不明です。

ステップ 6 **[Operation Status (動作ステータス)]** 領域で、次の情報を確認します。

名前	説明
[Operation]	ドライブで進行中の現在の操作。ここに表示される値は次のとおりです。 **Rebuild in progress**
[Progress in %]	操作の進行状況のパーセンテージ。

Cisco FlexMMC

Cisco FlexMMC の詳細の表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] メニューをクリックします。

ステップ 2 **[ストレージ（Storage）]** メニューで、**[Cisco FlexMMC]** をクリックします。

ステップ 3 **[IMC イメージのメモリ（Memory for IMC Image）]** エリアで、次を表示します：

フィールド	説明
Total Space	Cisco IMC イメージに使用可能な合計スペース。
使用可能なスペース	Cisco IMC イメージに使用可能な残りのスペース。

ステップ 4 **[ファイル ストレージのメモリ（Memory for File Storage）]** エリアビューで、次を表示します：：

フィールド	説明
Total Space	ファイルの利用可能な総容量。
使用可能なスペース	ファイルに使用できる残りのスペース。
最後のファイル操作のステータス	最後にアップロードされた画像のステータス。

ステップ 5 **[コピーしたファイル（Files Copied）]** エリアで、次を表示します：

フィールド/アクション	説明
アップロード ファイル ボタン	**アップロード ファイル** ダイアログ ボックスを開きます。
[ファイルの削除/アップロードのキャンセル（Delete File/Cancel Upload）] ボタン	**[ファイルの削除（Delete File）]** と **[アップロードのキャンセル（Cancel Upload）]** を切り替えます。 アップロード後に選択した画像を削除します。 ファイルのアップロード中にアップロード プロセスをキャンセルします。
マップ画像 ボタン	選択した画像をマッピングします。
ファイル名 カラム	保存されている画像のファイル名。
ファイル タイプ カラム	イメージの種類
ファイル サイズカラム	イメージのサイズ。
[Partition] カラム	パーティションの数。
アップロード時間列	アップロードされた画像のタイムスタンプ。
[Progress %] カラム	画像ファイルのアップロードの進行状況。
[ステータス（Status）] カラム	画像ファイルの全体的な状態。

新しいイメージ ファイルのアップロード

始める前に

アップロード進行中のファイルがないことを確認してください。一度にアップロードできるイメージファイルは1つだけです。新しいファイルをアップロードするには、まず既存のファイルをマッピング解除して削除する必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。

ステップ 2 **[ストレージ（Storage）]** メニューで、**[Cisco FlexMMC]** をクリックします。

ステップ 3 **[ファイルのコピー（Files Copied）]** エリアで、**[ファイルのアップロード（Upload File）]** をクリックします。

ステップ 4 **[ファイルのアップロード（Upload File）]** ダイアログボックスで、次に値を入力します：

フィールド	説明
[パーティション（Partition）] ドロップダウン リスト	パーティションのタイプ次のように指定します。 • **IMC イメージ**：Cisco .iso ファイル。 • **ユーザ ファイル**：任意の .iso、イメージ、またはその他のファイル形式。 アップロードできるのは 1 つの .iso ファイルのみです。 （注） 他のファイル形式を選択した場合、Cisco IMC はファイルをイメージ ファイルに変換します。 その他のファイル形式の場合、ファイル サイズは 10 MB を超える必要があります。また、変換のために余分なスペースが必要です。
[Mount Type] ドロップダウン リスト	マッピングのタイプです。次のいずれかになります。 （注） 選択するマウント タイプの通信ポートがスイッチ上で有効になっていることを確認してください。たとえば、マウント タイプとして CIFS を使用する場合、ポート 445（CIFS の通信ポート）がスイッチ上で有効になっていることを確認します。同様に、HTTP、HTTPS、または NFS を選択する場合は、ポート 80（HTTP の場合）、ポート 443（HTTPS の場合）、またはポート 2049（NFS の場合）を有効にします。 • [NFS]：ネットワーク ファイル システム。 • [CIFS]：共通インターネット ファイル システム。 • [WWW(HTTP/HTTPS)]：HTTP ベースまたは HTTPS ベースのシステム。

フィールド	説明
[リモート共有（Remote Share）] フィールド	マップするイメージの URL。形式は選択された [Mount Type] によって異なります。 • [NFS]：serverip:/share を使用します。 • [CIFS]：serverip://share を使用します。 • [WWW(HTTP/HTTPS)]：http[s]://serverip/share を使用します。
[Remote File] フィールド	リモート共有に含まれる .iso または .img ファイルの名前と場所。

フィールド	説明
[マウント オプション（Mount Options）] フィールド	

フィールド	説明
	カンマ区切りリストで入力される業界標準のマウント オプション。オプションは選択された [Mount Type] によって異なります。 [NFS] を使用している場合は、このフィールドを空白のままにするか、次の中から 1 つ以上を入力します。 • **ro** • **nolock** • **noexec** • **soft** • **port=VALUE** [CIFS] を使用している場合は、このフィールドを空白のままにするか、次の中から 1 つ以上を入力します。 • **ro** • **nounix** • **noserverino** • **port=VALUE** • [Ntlm]：NT LAN Manager（NTLM）セキュリティ プロトコル。このオプションは、Windows 2008 R2 および Windows 2012 R2 でのみ使用します。 • **vers=VALUE** （注） 値の形式は x.x である必要があります [WWW(HTTP/HTTPS)] を使用している場合は、このフィールドを空白のままにするか、次のように入力します。 • **noauto** （注） 仮想メディアをマウントする前に、Cisco IMC はサーバーに ping を実行することによって、エンドサーバーへの到達可能性の確認を試みます。

フィールド	説明
	• **username=VALUE** • **password=VALUE**
[ユーザ名（User Name）]フィールド	指定した [マウント タイプ（Mount Type）] のユーザ名（必要な場合）。
[パスワード（Password）]フィールド	選択されたユーザー名のパスワード（必要な場合）。

ステップ 5 [保存（Save）] をクリックします。

ファイルのアップロード ステータスは、**[コピーされたファイル（Files Copied）]** エリアで確認できます。

（注） アップロードプロセスが完了する前にキャンセルする場合は、ファイルを選択して **[アップロードのキャンセル（Cancel Upload）]** をクリックします。

イメージ ファイルの削除

始める前に

次の点を確認します。

- アップロード進行中のファイルはありません。アップロード進行中のファイルは削除できません。
- マッピングされているファイルはありません。すでにマッピングされているファイルは削除できません。ファイルを削除する前に、まずファイルのマッピングを解除する必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] メニューをクリックします。

ステップ 2 **[ストレージ（Storage）]** メニューで、**[Cisco FlexMMC]** をクリックします。

ステップ 3 **[コピーされたファイル（Files Copied）]** エリアで画像ファイルを選択し、**[ファイルを削除（Delete File）]** をクリックします。

イメージのマッピングまたはマップ解除

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[ストレージ（Storage）]メニューをクリックします。

ステップ 2 **[ストレージ（Storage）]** メニューで、**[Cisco FlexMMC]** をクリックします。

ステップ 3 **[コピーされたファイル（Files Copied）]** エリアで画像ファイルを選択し、**[マップ画像（Map Image）]** または **[マップ解除画像（UnMap Image）]** をクリックします。

FlexMMC をデフォルト設定へリセット

この手順を実行して、FlexMMC をデフォルトの Cisco IMC 設定にリセットします。

（注） この手順を実行すると、アップロードされたすべてのイメージが削除されます。

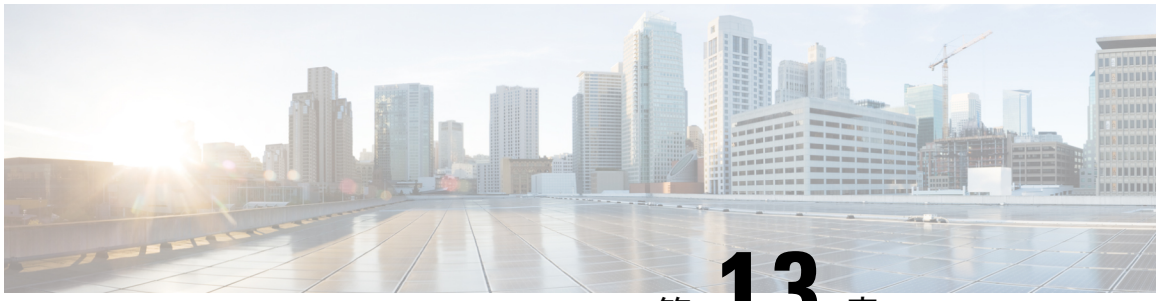
始める前に

次の点を確認します。

- アップロード進行中のファイルはありません。ファイルのアップロードが進行中は、FlexMMC をデフォルト設定にリセットできません。
- マッピングされているファイルはありません。ファイルがすでにマッピングされている場合、FlexMMC をリセットすることはできません。FlexMMC をリセットする前に、まずファイルのマッピングを解除する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	[ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] メニューをクリックします。	
ステップ 2	**[ストレージ（Storage）]** メニューで、**[Cisco FlexMMC]** をクリックします。	
ステップ 3	**[デフォルトに復元（Restore to Defaults）]** をクリックします。	
ステップ 4	確認のために [はい（Yes）] をクリックします。	



第 13 章

コミュニケーション サービスの設定

この章は、次の内容で構成されています。

TLS v1.2 の有効化または無効化

リリース 4.2 (2a) 以降、Cisco IMC は TLS v1.2 の無効化と、v1.2 と v1.3 の両方の暗号値のカスタマイズをサポートしています。

始める前に

[セキュリティの設定（Security Configuration）] の **[CC]**（コモンクライテリア）が有効になっている場合、TLS v1.2 を無効にすることはできません。TLS v1.2 を無効にする前に、**[CC]** が無効になっていることを確認してください。

TLS v1.2 を有効または無効にすると、vKVM、Web サーバー、XML API、および Redfish API セッションが再起動します。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [Admin] メニューの [Communication Services] をクリックします。

ステップ 3 **[TLS 構成（TLS Configuration）]** エリアで、次のプロパティを更新します。

名前	説明
TLS v1.2 を有効にするチェックボックス	Cisco IMC で TLS v1.2 が有効になっているかどうか。 （注） TLS v1.2 を有効または無効にすると、vKVM、Web サーバー、XML API、および Redfish API セッションが再起動します。 （注） **[セキュリティの設定（Security Configuration）]** の **[CC]**（コモンクライテリア）が有効になっている場合、TLS v1.2 を無効にすることはできません。
[TLSバージョンの構成（Configured TLS Version）] フィールド	Cisco IMC でサポートされる TLS バージョン。 このフィールドはユーザーが構成できません。ここに表示される値は、**[TLS v1.2 を有効にする]** チェック ボックスで選択した値によって異なります。
TLS v1.2 暗号モードドロップダウン リスト	TLS v1.2 が有効になっている場合、希望の暗号モードを選択できます。次のいずれかになります。 • **高** • **中** • **低** （注） **セキュリティ構成**で **FIPS** が有効になっている場合、**低**モードを選択することはできません。 • **カスタム** — カスタム暗号値を入力できます。 カスタム暗号フィールドで提供される特定の暗号の OpenSSL の同等の暗号名については、https://www.openssl.org/docs/man1.0.2/man1/ciphers.html を参照してください。 例： **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384** を設定するには、暗号リストの **ECDHE-RSA-AES256-GCM-SHA384** 入力を入力として提供します。

名前	説明
[TLS v1.2暗号リスト] フィールド	**[TLS v1.2 暗号モード]** ドロップダウン リストで選択した値に基づいて、暗号のリストを表示します。**TLS v1.2 暗号モード**を**カスタム**として選択した場合、暗号値を編集できます。 （注） FIPS が有効になっている場合、FIPS でサポートされていない暗号を設定することはできません。 （注） 入力された暗号値が無効またはサポートされていない場合、設定の保存中に、Cisco IMC は自動的に**TLS v1.2 暗号モード**の値を**高**に変更し、設定を保存します。次に例を示します。 **DH-RSA-AES256-GCM-SHA384** が設定されている場合、**TLS v1.2 暗号化モード**は自動的に**高**に設定されます 設定を保存した後、Cisco IMC は **TLS v1.2 暗号リスト** フィールドを無効にし、マウスを **TLS v1.2 カスタム暗号ステータス** アイコンの上に置くと、次のようなエラー メッセージが表示されます。 `TLS v1.2 カスタム暗号ステータス: エラー: 無効またはサポートされていない TLS v1.2 暗号リストを構成しています-' Cipher_Name '。TLS v1.2 暗号モードを高に設定します。`
TLS v1.3暗号スイート フィールド	TLS v1.3 の暗号値を編集できます。 （注） FIPS が有効になっている場合、FIPS でサポートされていない暗号を設定することはできません。

HTTP の設定

リリース 4.1(2b) 以降、Cisco IMC は個別の HTTPS および HTTP 通信サービスをサポートします。この機能を使用して無効にできるのは HTTP サービスのみです。

この機能は、次のサーバーでのみサポートされています。

- Cisco UCS C220 M5
- Cisco UCS C240 M5
- Cisco UCS C480 M5
- Cisco UCS C480 ML M5

- Cisco UCS C240 SD M5
- Cisco UCS C125 M5

（注） 4.1(2b) より以前のリリースで **[HTTP を HTTPS にリダイレクトすることを有効化する（Redirect HTTP to HTTPS Enabled）]** が無効になっている場合、4.1(2b) 以降のリリースにアップグレードすると、システムによって **[HTTP 有効化（HTTP Enabled）]** の値が **[無効（Disabled）]** に設定されます。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [通信サービス（Communication Services）] をクリックします。

ステップ 3 [HTTP Properties] 領域で、次のプロパティを更新します。

名前	説明
[HTTPS 有効（HTTPS Enabled）] チェックボックス	警告 このオプションを無効にすると、終了 Cisco IMC Web GUI セッションが終了します。このオプションを無効にすると、Cisco IMC への HTTP サービスと HTTPS サービスの両方が無効になります。 このオプションは、HTTPS サービスのみが Cisco IMC にアクセスできるようにします。
[HTTP 有効（HTTP Enabled）] チェックボックス	警告 このオプションの変更を正常に保存するには、Cisco IMC Web GUI は自動的に再起動されます。管理コントローラとの通信が一時的に失われ、再起動後に再度ログインする必要があります。 このオプションは、HTTP サービスのみが Cisco IMC にアクセスできるようにします。 （注） HTTPS を無効にすると、Cisco IMC にアクセスするための HTTP サービスも無効になります。

名前	説明
[Redirect HTTP to HTTPS Enabled] チェックボックス	（注） このオプションは、[HTTP 有効（HTTP Enabled）] がオンの場合にのみ適用されます。 イネーブルの場合、HTTP 経由で試行される通信はすべて同等の HTTPS アドレスにリダイレクトされます。 HTTP をイネーブルにしている場合は、このオプションをイネーブルにすることを強く推奨します。
[HTTP Port] フィールド	HTTP 通信に使用するポート。デフォルトは 80 です。
[HTTPS Port] フィールド	HTTPS 通信に使用するポート。デフォルトは 443 です。
[Session Timeout] フィールド	HTTP 要求の間、Cisco IMC がタイムアウトしてセッションを終了するまで待機する秒数。 60 ～ 10,800 の範囲の整数を入力します。デフォルトは 1,800 秒です。
[Max Sessions] フィールド	Cisco IMC で許可されている HTTP および HTTPS の同時セッションの最大数。 この値は変更できません。
[Active Sessions] フィールド	Cisco IMC で現在実行されている HTTP および HTTPS セッションの数。

ステップ 4 [Save Changes] をクリックします。

SSH の設定

始める前に

SSH を設定するには、admin 権限を持つユーザーとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。
ステップ 2 [管理（Admin）] メニューで [通信サービス（Communication Services）] をクリックします。
ステップ 3 [SSH Properties] 領域で、次のプロパティを更新します。

名前	説明
[SSH Enabled] チェックボックス	SSH が Cisco IMC でイネーブルかどうか。
[SSH Port] フィールド	セキュア シェル アクセスに使用するポート。デフォルトは 22 です。
[SSH Timeout] フィールド	SSH 要求がタイム アウトしたものとシステムが判断するまで待機する秒数。 60 ～ 10,800 の範囲の整数を入力します。デフォルトは 1,800 秒です。
[Max Sessions] フィールド	Cisco IMC で許可されている SSH の同時セッションの最大数。 この値は変更できません。
[Active Sessions] フィールド	現在 Cisco IMC で実行されている SSH セッションの数。

ステップ 4 [Save Changes] をクリックします。

XML API の設定

Cisco IMC 用の XML API

Cisco Cisco IMC XML アプリケーション プログラミング インターフェイス（API）は、C シリーズ ラックマウント サーバー用の Cisco IMC に対するプログラマチック インターフェイスです。この API は、HTTP または HTTPS 経由で XML ドキュメントを受け取ります。

XML API の詳細については、『*Cisco UCS Rack-Mount Servers Cisco IMC XML API Programmer's Guide*』を参照してください。

XML API のイネーブル化

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。
ステップ 2 [管理（Admin）] メニューで [通信サービス（Communication Services）] をクリックします。

ステップ 3 [XML API Properties] 領域で、次のプロパティを更新します。

名前	説明
[XML API Enabled] チェックボックス	このサーバで API アクセスが許可されているかどうか。
[Max Sessions] フィールド	Cisco IMC で許可されている API の同時セッションの最大数。 この値は変更できません。
[Active Sessions] フィールド	現在 Cisco IMC で実行されている API セッションの数。

ステップ 4 [Save Changes] をクリックします。

Redfish のイネーブル化

始める前に

このアクションを実行するには、admin としてログオンする必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Communications Services] をクリックします。

ステップ 3 [Redfishプロパティ（SSH Properties）] 領域で、次のプロパティを更新します。

名前	説明
[XML API Enabled] チェックボックス	このサーバで API アクセスが許可されているかどうか。
[Max Sessions] フィールド	Cisco IMC で許可されている API の同時セッションの最大数。 この値は変更できません。
[Active Sessions] フィールド	現在 Cisco IMC で実行されている API セッションの数。

ステップ 4 [Save Changes] をクリックします。

IPMI の設定

IPMI Over LAN

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）では、サーバ プラットフォームに組み込まれているサービス プロセッサとのインターフェイスのためのプロトコルを定義しています。このサービス プロセッサはベースボード管理コントローラ（BMC）と呼ばれ、サーバのマザーボードに存在します。BMC は、メイン プロセッサおよびボード上の他の要素に、簡単なシリアル バスを使用してリンクします。

通常動作の間、IPMI は、サーバのオペレーティング システムがシステム ヘルスについての情報を取得し、システムのハードウェアを制御できるようにします。たとえば、IPMI を使用すると、温度、ファンの速度、および電圧などのセンサーをモニタして、問題を事前に検出できます。サーバの温度が指定されているレベルより高くなった場合、サーバのオペレーティング システムは BMC に対して、ファンの速度を上げたり、プロセッサの速度を下げたりして問題に対処するよう指示できます。

IPMI over LAN の設定

IPMI over LAN は、Cisco IMC を IPMI メッセージで管理する場合に設定します。

（注）
- 暗号キーを発行しないで IPMI コマンドを実行する場合は、Cisco IMC で、[暗号キー（Encryption Key）] フィールドを偶数個のゼロに設定し保存します。これにより、暗号キーを含めることなく IPMI コマンドを発行できます。
- 最大 4 個の同時 IPMI セッションのみ許可されています。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [通信サービス（Communication Services）] をクリックします。

ステップ 3 [IPMI over LAN Properties] 領域で、BMC 1、BMC 2、CMC 1、CMC 2 の次のプロパティを更新します。

名前	説明
[有効（Enabled）] チェック ボックス	このサーバで IPMI アクセスが許可されているかどうか。
[Privilege Level Limit] ドロップダウン リスト	このサーバで IPMI セッションに割り当て可能な最高特権レベル。次のいずれかになります。 • [read-only]：IPMI ユーザは情報を表示できますが、変更することはできません。このオプションを選択した場合、「Administrator」、「Operator」、または「User」ユーザ ロールを持つ IPMI ユーザが作成できるのは、読み取り専用の IPMI セッションだけです。それ以外に所持している IPMI 特権は関係ありません。 • [user]：IPMI ユーザはいくつかの機能を実行できますが、管理タスクは実行できません。このオプションを選択した場合、「Administrator」または「Operator」ユーザ ロールを持つ IPMI ユーザがこのサーバで作成できるのは、ユーザ セッションと読み取り専用セッションだけです。 • [admin]：IPMI ユーザは使用可能なすべてのアクションを実行できます。このオプションを選択した場合、管理者（Administrator）ロールを持つ IPMI ユーザは、管理者、ユーザ、および読み取り専用セッションをこのサーバで作成できます。
[Encryption Key] フィールド	IPMI 通信に使用する IPMI 暗号キー。
[ランダム化（Randomize）] ボタン	IPMI 暗号化キーを乱数値に変更できます。

ステップ 4 [Save Changes] をクリックします。

SNMP の設定

SNMP

Cisco UCS C シリーズ ラックマウント サーバ は、サーバの設定およびステータスを表示したり、SNMP トラップによって障害とアラートを送信したりするために、簡易ネットワーク管理プロトコル（SNMP）をサポートしています。Cisco IMC サポートされている Management Information Base（MIB）ファイルの詳細については、次の URL にある『*MIB Quick Reference for Cisco UCS*』を参照してください。http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/mib/b-series/b_UCS_MIBRef.html

リリース 4.1（3b） 以降、Cisco IMC では SNMP v3 バージョンの拡張認証プロトコルが導入されています。

SNMP プロパティの設定

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [通信サービス（Communication Services）] をクリックします。

ステップ 3 [Communications Services] ペインの [SNMP] タブをクリックします。

ステップ 4 [SNMP Properties] 領域で、次のプロパティを更新します。

名前	説明
[SNMP Enabled] チェックボックス	このサーバが指定のホストに SNMP トラップを送信するかどうか。 （注） このチェックボックスをオンにしたら、SNMP ユーザーまたはトラップを設定する前に、[Save Changes] をクリックする必要があります。
[SNMP v2c が有効化されている（SNMP v2c Enabled）] チェックボックス	SNMP v2c バージョンを有効または無効にすることができます。
[SNMP v3 が有効化されている（SNMP v3 Enabled）] チェックボックス	SNMP v3 バージョンを有効または無効にすることができます。
[SNMP Port] フィールド	Cisco IMC SNMP エージェントを実行するポート。 1 ～ 65535 の範囲内の SNMP ポート番号を入力します。デフォルト ポート番号は、161 です。 （注） システム コールに予約済みのポート番号（たとえば 22、23、80、123、443、623、389、636、3268、3269、2068 など）は、SNMP ポートとして使用できません。
[Access Community String] フィールド	Cisco IMC が任意の SNMP に含めるデフォルトの SNMP v1 または v2c コミュニティ名により、動作が実行されます。 最大 18 文字の文字列を入力します。

名前	説明
[SNMP コミュニティ アクセス（SNMP Community Access）] ドロップダウン リスト	次のいずれかになります。 • [無効（Disabled）]：このオプションは、インベントリ テーブルの情報へのアクセスをブロックします。 • [制限付き（Limited）]：このオプションは、インベントリ テーブルの情報の読み取りアクセスを部分的に提供します。 • [フル（Full）]：このオプションは、インベントリテーブルの情報の読み取りフル アクセスを提供します。 （注） [SNMP コミュニティ アクセス（SNMP Community Access）] は、SNMP v1 および v2c ユーザのみに適用されます。
[Trap Community String] フィールド	他のデバイスに SNMP トラップを送信するために使用される SNMP コミュニティ グループの名前。 最大 18 文字の文字列を入力します。 （注） このフィールドは、SNMP v1 および v2c ユーザーのみに表示されます。SNMP v3 バージョンは SNMP v3 クレデンシャルを使用する必要があります。
[System Contact] フィールド	SNMP の実装を担当するシステムの連絡先。 電子メール アドレスや名前、電話番号など、最大 254 文字の文字列を入力します。
[System Location] フィールド	SNMP エージェント（サーバー）が実行するホストの場所。 最大 254 文字の文字列を入力します。
[SNMP Input Engine ID] フィールド	ユーザが定義した静的エンジンの一意の ID。
[SNMP エンジン ID（SNMP Engine ID）] フィールド	管理目的でデバイスを識別する固有の文字列。これは、[SNMP 入力エンジン ID（SNMP Input Engine ID）] がすでに定義されている場合はこの ID から生成され、それ以外の場合は BMC シリアル番号から生成されます。

ステップ 5 [Save Changes] をクリックします。

次のタスク

SNMP トラップ設定を指定します。

SNMP トラップ設定の指定

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [通信サービス（Communication Services）] をクリックします。

ステップ 3 [Communications Services] ペインの [SNMP] タブをクリックします。

ステップ 4 [Trap Destinations] タブをクリックします。

ステップ 5 [トラップ宛先（Trap Destinations）] 領域で、次のいずれかを実行できます。

- テーブルから既存のユーザを選択し、[トラップの変更（Modify Trap）] をクリックします。
- [トラップの追加（Add Trap）] をクリックして新しいユーザを作成します。

（注） フィールドが強調表示されていない場合は、[有効（Enabled）] を選択します。

ステップ 6 [Trap Details] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[ID] フィールド	トラップの宛先 ID。この値は変更できません。
Enabled check box	オンにすると、このトラップがサーバーでアクティブになります。
[バージョン（Version）] ドロップダウン リスト	トラップに使用される SNMP バージョンおよびモデル。次のいずれかになります。 • **[V2]** • **V3**
[トラップタイプ（Trap Type）] オプション ボタンドロップダウン リスト	送信するトラップのタイプ。次のいずれかになります。 • [トラップ（Trap）]：このオプションを選択すると、トラップが宛先に送信されても、通知を受信することはありません。 • [通知する（Inform）]：このオプションは、V2 ユーザに対してのみ選択できます。これを選択すると、宛先でトラップが受信されたときに通知を受け取ります。

名前	説明
[ユーザ（User）] ドロップダウン リスト	ドロップダウン リストに使用可能なすべてのユーザーが表示されます。そのリストからユーザーを選択します。 （注） SNMP v3 バージョンの構成時に、暗号化方式が **DES** に設定された SNMP ユーザーは、ドロップダウン リストに表示されません。
[トラップの宛先アドレス（Trap Destination Address）] フィールド	SNMP トラップ情報の送信先のアドレス。トラップの宛先として IPv4 または IPv6 アドレスまたはドメイン名を設定できます。
Port	サーバがトラップの宛先との通信に使用するポート。 1 ～ 65535 の範囲内のトラップの宛先のポート番号を入力します。

ステップ 7 [Save Changes] をクリックします。

ステップ 8 トラップの宛先を削除する場合は、行を選択し、[削除（Delete）] をクリックします。

削除の確認プロンプトで、[OK] をクリックします。

テスト SNMP トラップ メッセージの送信

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [通信サービス（Communication Services）] をクリックします。

ステップ 3 [通信サービス（Communication Services）] ペインで [SNMP] をクリックします。

ステップ 4 [Trap Destinations] 領域で、目的の SNMP トラップ宛先の行を選択します。

ステップ 5 **[SNMP テスト トラップの送信（Send SNMP Test Trap）]** をクリックします。

SNMP テスト トラップ メッセージがトラップ宛先に送信されます。

（注） テストメッセージを送信するために、トラップは設定済みで、イネーブルにされている必要があります。

Cisco USC C シリーズ M7 および以降のサーバー向け SNMP ユーザーの管理

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [管理（Admin）] メニューで [通信サービス（Communication Services）] をクリックします。

ステップ 3 [Communications Services] ペインの [SNMP] タブをクリックします。

ステップ 4 **[v3 ユーザー設定（v3 User Settings）]**エリアで、**[ここをクリックしてユーザー構成を変更します（CLICK HERE to change the Users configurations）]**

ユーザー設定の変更のためには、Cisco USC C シリーズ M7 および以降のサーバー向けローカル ユーザーの追加 （145 ページ）を参照してください。

SMTP を使用して電子メール アラートを送信するようにサーバーを設定する

Cisco IMC は、SNMP に依存せずに受信者に対する電子メール ベースのサーバー障害の通知をサポートします。システムは Simple Mail Transfer Protocol（SMTP）を使用して、設定された SMTP サーバーに電子メール アラートとしてサーバー障害を送信します。

最大 4 人の受信者がサポートされます。

電子メール アラートを受信するための SMTP サーバーの設定

サーバー障害に関する電子メール通知を受信するように、[Mail Alert] タブで SMTP プロパティを設定し、電子メール受信者を追加します。

始める前に

このタスクを実行するには、admin 権限を持つユーザーとしてログインする必要があります。

手順

ステップ 1

ステップ 2 [Admin] メニューの [Communication Services] をクリックします。

ステップ 3 [Communications Services] ペインの [Mail Alert] タブをクリックします。

ステップ 4 [SMTP Properties] 領域で、次のプロパティを更新します。

名前	説明
[SMTP を有効にする（SMTP Enabled）] チェック ボックス	オンにすると、SMTP サービスが有効になります。
[SMTP サーバ アドレス（SMTP Server Address）] フィールド	SMTP サーバ アドレスを入力できます。
[SMTP ポート（SMTP Port）] フィールド	SMTP ポート番号を入力できます。デフォルトのポート番号は 25 です。
SMTP送信元アドレス	送信される SMTP メール アラートの送信元アドレスを設定できます。ここで入力するメール アドレスは、受信するすべてのSMTPメール アラートの送信元アドレス（メール送信者のアドレス）として表示されます。 （注） これはオプションのフィールドです。このフィールドに電子メールアドレスを入力しない場合、デフォルトで、サーバーのホスト名 ID が送信元アドレス（メール送信者のアドレス）として表示されます。

ステップ 5 [SMTP Recipients] 領域で、次の手順を実行します。

a) [Add (+)] ボタンをクリックして、通知の送信先としての電子メール受信者を追加します。電子メール ID を入力して、[Save] をクリックします。

電子メール受信者を削除するには、電子メール受信者を選択し、[Delete (X)] ボタンをクリックします。

b) **[最小シビラティ（重大度）レベル（最小シビラティ（重大度）レベル）]**ドロップダウン リスト電子メールアラートを受信するための最小シビラティ（重大度）レベルを選択できます：次のいずれかになります。

- の条件
- 警告
- マイナー
- メジャー
- 重大

最小シビラティ（重大度）レベルを選択した場合、そのレベルと、それよりも高い他のシビラティ（重大度）レベルについてメールアラートが送信されます。たとえば、最小シビラティ（重大度）レベルとして「Minor」を選択すると、マイナー、メジャー、およびクリティカルな障害イベントに関する電子メール アラートが送信されます。

c) [Send Test Mail] をクリックして、追加した電子メール受信者に到達可能であるかどうかを確認します。
電子メール アドレスと SMTP 設定が有効な場合は、電子メールが送信されたことを示すメッセージとともに確認ポップアップ ウィンドウが表示されます。設定が有効でない場合は、電子メールが送信されていないことを示すメッセージとともに確認ポップアップ ウィンドウが表示されます。[Reachability] カラムは、テスト メールが電子メール受信者に正常に送信されたかどうかを示します。[Reachability] カラムの値は次のいずれかになります。

- [Yes]（テスト メールが正常に送信された場合）
- [いいえ（No）]（テスト メールが正常に送信されていない場合）
- [na]（テスト メールが送信されていない場合）

ステップ 6 [Save Changes] をクリックします。

トラブルシューティング

次の表では、（到達可能性ステータスが [なし（No）] の場合に）Cisco IMC ログに表示される可能性のある SMTP メールアラートの設定の問題に対するトラブルシューティング上の推奨事項を説明しています。

問題	推奨されるソリューション
タイムアウトに達しました	設定されている SMTP の IP アドレスに到達できない場合に発生する可能性があります。有効な IP アドレスを入力してください。
ホスト名を解決できませんでした	設定されている SMTP ドメイン名に到達できない場合に発生する可能性があります。有効なドメイン名を入力します。
サーバーに接続できませんでした	SMTP IP またはドメイン名またはポート番号が正しく設定されていない場合、発生する可能性があります。有効な設定の詳細を入力します。
ピアへのデータ送信に失敗しました	無効な受信者の電子メール ID が設定されている場合に発生する可能性があります。有効な電子メール ID を入力します。

SMTP 電子メール受信者の追加

サーバー障害に関する電子メール通知を受信するように、[Mail Alert] タブで電子メール受信者を追加します。

始める前に

- このタスクを実行するには、admin 権限を持つユーザーとしてログインする必要があります。

- [SMTP Properties] 領域で、SMTP サーバー プロパティを設定します。電子メール アラートを受信するための SMTP サーバーの設定 （402 ページ）を参照してください。

手順

ステップ 1 [Navigation] ペインの [Admin] メニューをクリックします。

ステップ 2 [Admin] メニューの [Communication Services] をクリックします。

ステップ 3 [Communications Services] ペインの [Mail Alert] タブをクリックします。

ステップ 4 [SMTP Recipients] 領域で、次の手順を実行します。

a) [Add (+)] ボタンをクリックして、通知の送信先としての電子メール受信者を追加します。電子メール ID を入力して、[Save] をクリックします。

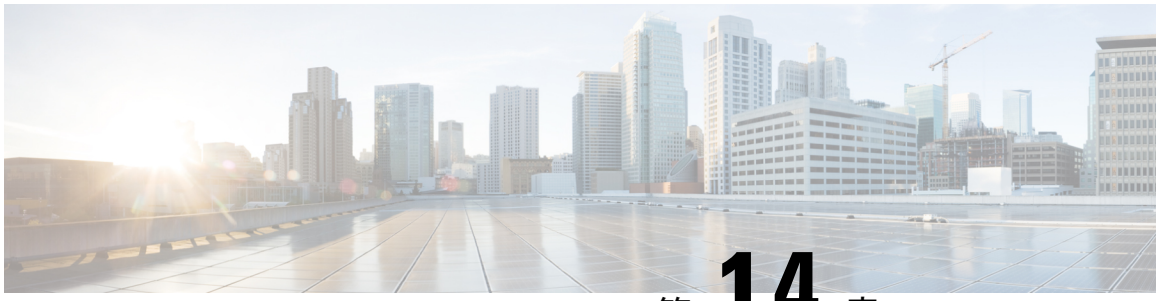
b) **[最小シビラティ（重大度）レベル（最小シビラティ（重大度）レベル）]**ドロップダウン リスト電子メール アラートを受信するための最小シビラティ（重大度）レベルを選択できます：次のいずれかになります。

- の条件
- 警告
- マイナー
- メジャー
- 重大

最小シビラティ（重大度）レベルを選択した場合、そのレベルと、それよりも高い他のシビラティ（重大度）レベルについてメール アラートが送信されます。たとえば、最小シビラティ（重大度）レベルとして「Minor」を選択すると、マイナー、メジャー、およびクリティカルな障害イベントに関する電子メール アラートが送信されます。

c) [Send Test Mail] をクリックして、追加した電子メール受信者に到達可能であるかどうかを確認します。
電子メール アドレスと SMTP 設定が有効な場合は、電子メールが送信されたことを示すメッセージとともに確認ポップアップ ウィンドウが表示されます。設定が有効でない場合は、電子メールが送信されていないことを示すメッセージとともに確認ポップアップ ウィンドウが表示されます。[Reachability] カラムは、テスト メールが電子メール受信者に正常に送信されたかどうかを示します。[Reachability] カラムの値は次のいずれかになります。

- [Yes]（テスト メールが正常に送信された場合）
- [いいえ（No）]（テスト メールが正常に送信されていない場合）
- [該当なし（na）]（テスト メールが送信されていない場合）



第 14 章

証明書とサーバー セキュリティの管理

この章は、次の内容で構成されています。

サーバ証明書の管理

証明書署名要求（CSR）を生成して新しい証明書を取得し、新しい証明書を Cisco IMC にアップロードして現在のサーバー証明書と交換することができます。サーバー証明書は、Verisign のようなパブリック認証局（CA）、または独自に使用している認証局のいずれかによって署名されます。生成された証明書のキーの長さは 2048 ビットです。

（注） この章に記載されている以下のタスクを実行する前に、Cisco IMC の時刻が現在の時刻に設定されていることを確認します。

手順

ステップ 1 Cisco IMC から CSR を生成します。

ステップ 2 証明書の発行と署名を行う認証局に CSR ファイルを送信します。組織で独自の自己署名証明書を生成している場合は、CSR ファイルを使用して自己署名証明書を生成できます。

ステップ 3 新しい証明書を Cisco IMC にアップロードします。

（注） アップロードされた証明書は、Cisco IMC によって生成された CSR から作成される必要があります。この方法で作成されていない証明書はアップロードしないでください。

証明書署名要求の生成

（注） [Common Name] および [Organization Unit] フィールドには特殊文字（たとえばアンパサンド（**&**））を使用しないでください。

始める前に

- 証明書を設定するには、admin 権限を持つユーザとしてログインする必要があります。
- Cisco IMC の時刻が現在の時刻に設定されていることを確認します。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）]メニューで [セキュリティ管理（Security Management）]をクリックします。

ステップ 3 [Actions] 領域で、[Generate New Certificate Signing Request] リンクをクリックします。

[Generate New Certificate Signing Request] ダイアログボックスが表示されます。

ステップ 4 [Generate New Certificate Signing Request] ダイアログボックスで、次のプロパティを更新します。

名前	説明
[コモンネーム（Common Name）] フィールド	Cisco IMC の完全修飾名。 デフォルトでは、サーバの CN は CXXX-YYYYYY 形式で表示されます（XXX はサーバのモデル番号で YYYYYY はシリアル番号です）。 最新バージョンにアップグレードするとき、CNはそのまま保持されます。

名前	説明
サブジェクト代替名（SAN）	これでサブジェクト代替名の追加の入力パラメータを入力できます。これには証明書の subject フィールドを使用して関連付けられるさまざまな値を使用できます。 SAN のさまざまなオプションには次のものがあります。 • Email • DNS name • IP アドレス • Uniform Resource Identifier（URI） （注） このフィールドは任意です。各タイプの SAN インスタンスの数をどのようにも設定できますが、インスタンスの合計の数は 10 を超えることはできません。
[Organization Name] フィールド	証明書を要求している組織。
[組織単位（Organization Unit）] フィールド	組織ユニット
[地域（Locality）] フィールド	証明書を要求している会社の本社が存在する市または町。
[State Name] フィールド	証明書を要求している会社の本社が存在する州または行政区分。
[Country Code] ドロップダウンリスト	会社が存在する国。
[電子メール（Email）] フィールド	会社の電子メールの連絡先。

名前	説明
Signature Algorithm	証明書署名要求を生成するための署名アルゴリズムを選択できます。次のいずれかになります。 • SHA1 • SHA256 • SHA384 • SHA512 • ECDSA • RSA 証明書署名要求を生成するために選択されているデフォルトの署名アルゴリズムは SHA384 です。
[キーの長さ（Key Length）] ドロップダウン リスト	（注） このオプションは、**ECDSA** を除くすべての**[署名アルゴリズム（Signature Algorithm）]**で使用できます。 次のいずれかを選択できます： • 1024 • 2048 • 4096
[キー カーブ（Key Curve）] ドロップダウン リスト	（注） このオプションは、**ECDSA [署名アルゴリズム（Signature Algorithm）]** でのみ使用できます。 次のいずれかを選択できます： • P256 • P384 • P512

名前	説明
[Challenge Password (チャレンジ パスワード)] チェック ボックス	**チャレンジ パスワード**は、証明書署名要求 (CSR) ダイアログ ボックスに組み込まれています。このダイアログ ボックスでは、発行元認証局 (CA) が証明書を認証するために使用します。 **[Challenge Password (チャレンジ パスワード)]** オプションが選択されている場合は、有効なパスワード文字列を入力するためユーザーに**チャレンジ パスワード文字列**が入力されます。 （注） ユーザーには**チャレンジパスワード**を選択しないオプションがあります。この場合、**チャレンジパスワード文字列**は入力されません。ただし、ユーザーはCSRの正常な生成に進むことができます。
[チャレンジパスワード文字列（Challenge Password String）] フィールド	このオプションは、**[チャレンジパスワード文字列（Challenge Password String）]** が選択されている場合にのみ表示されます。文字列を入力してください。
[String Mask (文字列マスク)] ドロップダウン リスト	これにより、証明書署名要求 (CSR) ダイアログ ボックスで許可される文字列タイプのマスクが設定されます。このオプションは、特定のフィールドの特定の文字列タイプを使用する場合にはマスクしません。文字列のタイプは次のとおりです。 • **デフォルト**: Printablestring、T61String、bmpstring を使用します。 • **pkix**: Printablestring、BMPstring を使用します。 • **utf8only**: UTF8Strings のみを使用します。 • **nombstr**: Printablestring、T61String (BMPStrings または UTF8Strings 以外) を使用します。
[**Self Signed Certificate**] チェックボックス	自己署名した証明書を生成します。 警告 証明書の生成が成功した後、Cisco IMC Web GUI が再起動します。管理コントローラとの通信が一時的に切断され、再ログインが必要な場合があります。 （注） イネーブルの場合、CSRが生成され、自動的に署名およびアップロードが行われます。
[CSRの生成（Generate CSR）] ボタン	クリックして、証明書を生成します。
[Reset Values]ボタン	ダイアログ ボックスのすべての値をリセットします。

（注）　自己署名証明書が有効な場合は、ステップ 5 および 6 を無視します。

ステップ 5　[CSR の作成（Generate CSR）] をクリックします。

[Opening csr.txt] ダイアログボックスが表示されます。

ステップ 6　CSR ファイル csr.txt を管理するには、次のいずれかの手順を実行します。

a) [Open With] をクリックして csr.txt を表示します。
b) [Save File] をクリックしてから [OK] をクリックし、ローカル マシンに csr.txt を保存します。

次のタスク

- 証明書の発行と署名を行う認証局に CSR ファイルを送信します。組織で独自の自己署名証明書を生成している場合は、CSR ファイルを使用して自己署名証明書を生成できます。
- 証明書のタイプが**サーバ**証明書であることを確認します。

自己署名証明書の作成

パブリック認証局（CA）を使用してサーバ証明書の生成と署名を行う代わりに、独自の CA を運用して独自の証明書に署名することができます。このセクションでは、Linux で実行されている OpenSSL 証明書サーバーを使用して CA を作成するコマンドおよびサーバー証明書を生成するコマンドについて説明します。OpenSSL の詳細については、http://www.openssl.org を参照してください。

（注）　これらのコマンドは、Cisco IMC ではなく、OpenSSL パッケージを使用している Linux サーバーで入力します。

始める前に

- 組織内のサーバで、証明書サーバのソフトウェア パッケージを取得してインストールします。
- Cisco IMC の時刻が現在の時刻に設定されていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**openssl genrsa -out** *CA_keyfilename keysize* 例： `# openssl genrsa -out ca.key 2048`	このコマンドは、CA で使用される RSA 秘密キーを生成します。 （注） ユーザ入力なしで CA がキーにアクセスできるように、このコマンドに -des3 オプションは使用しないでください。 指定されたファイル名には、指定されたサイズの RSA キーが含まれています。
ステップ 2	**openssl req -new -x509 -days** *numdays* **-key** *CA_keyfilename* **-out** *CA_certfilename* 例： `# openssl req -new -x509 -days 365 -key ca.key -out ca.crt`	このコマンドは、指定されたキーを使用して、CA の自己署名証明書を新規に作成します。証明書は指定された期間有効になります。このコマンドは、ユーザに証明書の追加情報を求めるプロンプトを表示します。 証明書サーバーは、アクティブな CA です。
ステップ 3	**echo "nsCertType = server" > openssl.conf** 例： `# echo "nsCertType = server" > openssl.conf`	このコマンドは、証明書がサーバー限定の証明書であることを指定する行を OpenSSL 設定ファイルに追加します。この指定により、認証されたクライアントがサーバになりすます man-in-the-middle 攻撃を防御できます。 OpenSSL 設定ファイル openssl.conf には、"nsCertType = server" という文が含まれています。
ステップ 4	**openssl x509 -req -days** *numdays* **-in** *CSR_filename* **-CA** *CA_certfilename* **-set_serial 04 -CAkey** *CA_keyfilename* **-out** *server_certfilename* **-extfile openssl.conf** 例： `# openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 04 -CAkey ca.key -out myserver05.crt -extfile openssl.conf`	このコマンドは、CA が CSR ファイルを使用してサーバー証明書を生成するように指示します。 サーバー証明書は、出力ファイルに含まれています。

	コマンドまたはアクション	目的
ステップ 5	**openssl x509 -noout -text -purpose -in <cert file>** 例： `openssl x509 -noout -text -purpose -in <cert file>`	生成された証明書のタイプが [サーバー（Server）] であることを確認します。 （注） フィールド [Server SSL] および [Netscape SSL] サーバーの値が [Yes] でない場合は、タイプが [Server] の証明書を生成するように openssl.conf が設定されていることを確認します。
ステップ 6	（任意） 生成された証明書に正しい使用期限が設定されていない場合は、Cisco IMC の時刻が現在の時刻に設定されていることを確認し、ステップ 1 ～ 5 を繰り返して証明書を再生成します。	正しい有効期限が設定された証明書が作成されます。

例

この例は、CA の作成方法、および新規に作成された CA が署名するサーバ証明書の生成方法を示します。これらのコマンドは、OpenSSL を実行している Linux サーバーで入力します。

```
# /usr/bin/openssl genrsa -out ca.key 2048 Generating RSA private key, 2048
bit long modulus .............++++++ .....++++++ e is 65537 (0x10001) #
/usr/bin/openssl req -new -x509 -days 365 -key ca.key -out ca.crt You are about
 to be asked to enter information that will be incorporated into your certificate
 request. What you are about to enter is what is called a Distinguished Name
or a DN. There are quite a few fields but you can leave some blank For some
fields there will be a default value, If you enter '.', the field will be left
 blank. ----- Country Name (2 letter code) [GB]:US State or Province Name (full
 name) [Berkshire]:California Locality Name (eg, city) [Newbury]:San Jose
Organization Name (eg, company) [My Company Ltd]:Example Incorporated
Organizational Unit Name (eg, section) []:Unit A Common Name (eg, your name or
 your server's hostname) []:example.com Email Address []:admin@example.com #
echo "nsCertType = server" > openssl.conf # /usr/bin/openssl x509 -req -days
365 -in csr.txt -CA ca.crt -set_serial 01 -CAkey ca.key -out server.crt -extfile
 openssl.conf Signature ok subject=/C=US/ST=California/L=San Jose/O=Example
Inc./OU=Unit A/CN=example.com/emailAddress=john@example.com Getting CA Private
 Key #
```

次のタスク

新しい証明書を Cisco IMC にアップロードします。

Windows を使用した自己署名証明書の作成

始める前に

- 証明書を設定するには、admin 権限を持つユーザとしてログインする必要があります。
- Cisco IMC の時刻が現在の時刻に設定されていることを確認します。

手順

ステップ 1 [**IIS Manager**] を開いて管理するレベルに移動します。

ステップ 2 [**Features**] 領域で、[**Server Certificate**] をダブルクリックします。

ステップ 3 [**Action**] ペインで、[**Create Self-Signed Certificate**] をクリックします。

ステップ 4 [**Create Self-Signed Certificate**] ウィンドウで、[**Specify a friendly name for the certificate**] フィールドに証明書の名前を入力します。

ステップ 5 **[OK]**をクリックします。

ステップ 6 （任意） 生成された証明書に正しい使用期限が設定されていない場合は、Cisco IMC の時刻が現在の時刻に設定されていることを確認し、ステップ 1 ～ 5 を繰り返して証明書を再生成します。
正しい有効期限が設定された証明書が作成されます。

サーバ証明書のアップロード

サーバーにアップロードする証明書を参照して選択するか、または署名付き証明書のすべての内容をコピーして [Paste certificate content] テキスト フィールドに貼り付け、それをアップロードできます。

始める前に

- 証明書をアップロードするには、admin 権限を持つユーザとしてログインする必要があります。
- アップロードする証明書ファイルは、ローカルにアクセスできるファイル システムに配置されている必要があります。
- 生成された証明書のタイプが [サーバー（Server）] であることを確認します。
- 次の証明書形式がサポートされています。
  - .crt
  - .cer

- .pem

（注） [Cisco IMC Certificate Management] メニューを使用して最初に CSR を生成してから、その CSR を使用してアップロードする証明書を取得する必要があります。この方法で取得されていない証明書はアップロードしないでください。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [証明書の管理（Certificate Management）] をクリックします。

ステップ 3 [Actions] 領域で、[Upload Server Certificate] をクリックします。

[Upload Certificate] ダイアログボックスが表示されます。

ステップ 4 [Upload Certificate] ダイアログボックスで、次のプロパティを更新します。

名前	説明
ブラウザ クライアント ボタンから証明書をアップロード	証明書をアップロードできます。
ファイル	アップロードする証明書ファイル。
[参照（Browse）] ボタン	適切な証明書ファイルに移動できるダイアログボックスが表示されます。
[Paste Certificate content] オプション ボタン	テキスト ボックスが開き、そこで署名付き証明書の内容全体をコピーして、**[証明書の内容を貼り付け（Paste certificate content）]**テキストフィールドに貼り付けることができます。 （注） アップロードの前に、証明書に署名が付されていることを確認します。
[アップロード（Upload）] ボタン	証明書をアップロードするには、**[アップロード（4.3.1.230097）]** をクリックします。

ステップ 5 **[Upload Certificate]**をクリックします。

外部証明書の管理

4.1.2 リリースより前のリリースでは、証明書署名要求 (CSR) を生成し、新しいサーバ証明書を Cisco IMC にアップロードすることができます。リリース 4.1.2 以降では、サーバ証明書に

加えて、ワイルドカードまたは外部証明書および外部秘密キーをアップロードすることもできます。サーバ証明書とは異なり、**複数**の Cisco IMC サーバに同じ外部証明書とキーペアをアップロードして使用することができます。

1. 外部証明書と外部秘密キーを Cisco IMC にアップロードします。
2. アップロードされた証明書をアクティブにします。

   アクティブ化すると、新しい証明書と秘密キーのペアによって、Cisco IMC の既存の証明書とキーペアが置き換えられます。

外部証明書のアップロード

始める前に

- admin 権限を持つユーザとしてログインする必要があります。
- アップロードする証明書ファイルは、ローカルにアクセスできるファイルシステムに配置されている必要があります。
- 次の証明書形式がサポートされています。
  - .crt
  - .cer
  - .pem

（注）
- Cisco IMC は、Cisco UCS C シリーズ M4 サーバで、2048ビットおよび4096ビットの外部秘密キー サイズをサポートしています。
- Cisco IMC は、Cisco UCS C シリーズ M5 サーバで 2048ビット、4096ビット、および8192ビットの外部秘密キー サイズをサポートしています。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Certificate Management] をクリックします。

ステップ 3 **[アクション（Actions）]** 領域で、**[サーバ証明書のアップロード（Upload Server Certificate）]** をクリックします。

[外部証明書のアップロード（External Upload Certificate）] ダイアログ ボックスが表示されます。

ステップ 4 [外部証明書のアップロード (Upload External Certificate)] ダイアログ ボックスで、適切なオプションを選択し、関連する詳細情報を入力します。

- **[リモートの場所からアップロード (Upload from remote location)]**: リモートの場所から外部証明書をアップロードするには、このオプションボタンを選択します。

名前	説明
[リモートの場所からアップロード (Upload from remote location)] フィールド	次のいずれかのプロトコルを選択します。 • TFTP • FTP • SCP • SFTP • HTTP （注） FTP、SCP または SFTP を選択した場合は、ユーザ名とパスワードの入力が求められます。
[サーバ IP/ホスト名 (Server IP/Hostname)] ボタン	リモート サーバのホスト名または IP アドレスを入力します。
パスおよびファイル名	外部証明書をアップロードするリモートサーバ上のファイルパスとファイル名を入力します。 （注） このオプションを使用するアップロードでサポートされるファイルの最大サイズは次のとおりです。 • Cisco UCS C シリーズ M5 サーバで最大 8 KB • Cisco UCS C シリーズ M4 サーバで最大 4 KB
Username	リモート サーバのユーザ名を入力します。
Password	リモート サーバのパスワードです。

- **[ブラウザ クライアントでアップロード (Upload by Browser client)]**: ブラウザ クライアントを使用して外部証明書をアップロードするには、このオプション ボタンを選択します。

  [参照 (Browse)] をクリックして、外部証明書をアップロードする場所に移動します。

（注） このオプションを使用するアップロードで、以下の機種でサポートされるファイルサイズは、最大 5 KB です。

- Cisco UCS C シリーズ M4 サーバ
- Cisco UCS C シリーズ M5 サーバ

- **[外部証明書の内容をペースト (Paste External Certificate Content)]**: このオプション ボタンを選択すると、外部証明書の詳細がダイアログボックスに直接貼り付けられます。

（注） このオプションを使用するアップロードでサポートされるファイルの最大サイズは次のとおりです。

- Cisco UCS C シリーズ M5 サーバで最大 8 KB
- Cisco UCS C シリーズ M4 サーバで最大 4 KB

ステップ 5 **[アップロード (Upload)]** をクリックし、外部証明書をアップロードします。

次のタスク

外部秘密キーをアップロードしてから、アップロードした外部証明書をアクティブにします。

重要 外部証明書と外部秘密キーをアップロードすると、**[外部証明書の有効化 (Activate External certificate)]** タブが有効になります。アップロードした外部証明書をアクティブにするには、**[外部証明書の有効化 (Activate External certificate)]** を選択します。

アップロードされた証明書をアクティブにすると、既存の証明書とキーのペアが置き換えられ、既存のすべての HTTPS セッションと SSH セッションが切断されます。

外部秘密キーのアップロード

始める前に

- 外部秘密キーをアップロードするには、admin 権限を持つユーザとしてログインする必要があります。
- 外部証明書がアップロード済みであることを確認します。

（注）
- Cisco IMC は、Cisco UCS C シリーズ M4 サーバで、2048ビットおよび4096ビットの外部秘密キー サイズをサポートしています。
- Cisco IMC は、Cisco UCS C シリーズ M5 サーバで 2048ビット、4096ビット、および8192ビットの外部秘密キー サイズをサポートしています。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Certificate Management] をクリックします。

ステップ 3 **[アクション（Actions）]** 領域で、**[外部秘密キーのアップロード（Upload External Private Key）]** をクリックします。

[外部秘密キーのアップロード（Upload External Private Key）]ダイアログ ボックスが表示されます。

ステップ 4 **[外部秘密キーのアップロード（Upload External Private Key）]** ダイアログ ボックスで、適切なオプションを選択し、関連する詳細情報を入力します。

- **[リモートの場所からアップロード (Upload from remote location)]**: リモートの場所から外部証明書をアップロードするには、このオプションボタンを選択します。

名前	説明
[リモートの場所からアップロード (Upload from remote location)] フィールド	次のいずれかのプロトコルを選択します。 • SFTP • SCP
[サーバ IP/ホスト名 (Server IP/Hostname)] ボタン	リモート サーバのホスト名または IP アドレスを入力します。
パスおよびファイル名	外部秘密キーをアップロードするリモート サーバ上のファイルパスとファイル名を入力します。 （注） このオプションを使用するアップロードでサポートされるファイルの最大サイズは次のとおりです。 • Cisco UCS C シリーズ M5 サーバで最大 8 KB • Cisco UCS C シリーズ M4 サーバで最大 4 KB

名前	説明
Username	リモート サーバのユーザ名を入力します。
Password	リモート サーバのパスワードです。

- **[ブラウザ クライアントでアップロード (Upload by Browser client)]**: ブラウザ クライアントを使用して外部秘密キーをアップロードするには、このオプション ボタンを選択します。

  [参照 (Browse)] をクリックして、外部秘密キーをアップロードする場所に移動します。

  （注） このオプションを使用するアップロードで、以下の機種でサポートされるファイルサイズは、最大 5 KB です。

  - Cisco UCS C シリーズ M4 サーバ
  - Cisco UCS C シリーズ M5 サーバ

- **[外部秘密キーの内容をペースト (Paste External Private Key Content)]**]: このオプション ボタンを選択すると、外部証明書の詳細がダイアログボックスに直接貼り付けられます。

  （注） このオプションを使用するアップロードでサポートされるファイルの最大サイズは次のとおりです。

  - Cisco UCS C シリーズ M5 サーバで最大 8 KB
  - Cisco UCS C シリーズ M4 サーバで最大 4 KB

ステップ 5 **[アップロード (Upload)]** をクリックし、外部秘密キーをアップロードします。

次のタスク

外部証明書と外部秘密キーをアップロードした後、アップロードされた外部証明書をアクティブにします。

重要 外部証明書と外部秘密キーをアップロードすると、**[外部証明書の有効化 (Activate External certificate)]** タブが有効になります。アップロードした外部証明書をアクティブにするには、**[外部証明書の有効化 (Activate External certificate)]** を選択します。

アップロードされた証明書をアクティブにすると、既存の証明書とキーのペアが置き換えられ、既存のすべての HTTPS セッションと SSH セッションが切断されます。

外部証明書の有効化

始める前に

- 外部証明書を有効化するには、admin 権限を持つユーザとしてログインする必要があります。
- 外部証明書と外部秘密キーがアップロードされていることを確認します。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 **[管理 (Admin)]** タブの **[証明書管理 (Certificate Management)]** をクリックします。

外部証明書と外部秘密キーをアップロードすると、**[外部証明書の有効化 (Activate External certificate)]** タブ (**[アクション (Actions)]** 領域) が有効になります。

ステップ 3 **[外部証明書の有効化 (Activate External certificate)]** をクリックします。

（注） 外部証明書をアクティブにすると、既存のすべての証明書とキーペアが上書きされ、既存のすべての HTTPS セッションと SSH セッションが切断されます。

SPDM セキュリティ：MCTP SPDM

SPDM セキュリティ

Cisco M6 サーバーには、デバイス自体に対する攻撃のベクトルを提供したり、デバイスを使用してシステム内の別のデバイスを攻撃したりする可能性のある可変コンポーネントが含まれている場合があります。これらの攻撃から防御するために、SPDM（セキュリティ プロトコルおよびデータ モデル）の仕様は、さまざまなトランスポートおよび物理メディアを介してデバイス間でメッセージ交換を実行するためのメッセージ、データ オブジェクト、およびシーケンスを定義します。これは、管理コンポーネント トランスポート プロトコル（MCTP）を介した管理コントローラとエンドポイント デバイス間のメッセージ交換を調整します。

メッセージ交換には、コントローラにアクセスするハードウェア ID の認証が含まれます。SPDM は、デバイス認証および証明書管理の管理レベルを指定することにより、低レベルのセキュリティ機能と操作へのアクセスを可能にします。この機能は、Cisco IMC リリース 4.2（1a）で Cisco UCS C220 および 240 M6 サーバーでサポートされています。

エンドポイント証明書と認証局（ルート CA）証明書は、サーバーのすべてのユーザー インターフェイスにリスト表示されます。1 つ以上の外部デバイス証明書のコンテンツを Cisco IMC にアップロードすることもできます。SPDM ポリシーを使用すると、必要に応じて外部ルート

CA 証明書または設定を変更または削除できます。不要になったルート CA 証明書を削除または置き換えることもできます。

SPDMセキュリティポリシーでは、次にリストするように、3つのセキュリティ レベル設定のいずれかを指定できます。

- フル セキュリティ：

  これは、最高のMCTPセキュリティ設定です。この設定を選択した場合、エンドポイントの認証が失敗すると、障害が生成されます。また、エンドポイントのいずれかでエンドポイント認証がサポートされていない場合も、障害が発生します。

- 部分的なセキュリティ：

  この設定を選択した場合、エンドポイントの認証が失敗すると、障害が生成されます。エンドポイントのいずれかでエンドポイント認証がサポートされていない場合には、障害が生成されません。これはデフォルト設定として選択されています。

- No Security

  この設定を選択した場合（エンドポイント測定が失敗しても）障害は発生しません。

MCTP SPDM 障害アラート設定の構成と表示

（注） 一部の C シリーズ サーバでのみ有効になります。

次の手順を実行して、障害アラート設定を表示および変更できます。

手順

ステップ 1 **[ナビゲーション（Navigation）]** ペインで **[管理（Admin）]** メニューをクリックします。

ステップ 2 [管理（Admin）]メニューで [セキュリティ管理（Security Management）]をクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]** タブ > **[MCTP SPDM]** タブ > **[アクション（Actions）]** エリアで、**[障害アラート設定（Fault Alert Setting）]** ドロップダウンをクリックします。

次のいずれかになります。

- **[完全（Full）]** - このオプションを選択した場合、エンドポイントの認証が失敗すると、障害が生成されます。

  このオプションを選択した場合、エンドポイントがエンドポイント認証をサポートしていないときに障害が生成されます。

- **[一部（Partial）]** - デフォルトのオプション。このオプションを選択した場合、エンドポイントの認証が失敗すると、障害が生成されます。

このオプションを選択した場合、エンドポイントがエンドポイント認証をサポートしていなくても障害は生成されません。

- **[無効（Disabled）]** - このオプションを選択した場合、エンドポイント認証の失敗に対して障害は生成されません。

次のタスク

デバイスの構成証明が失敗した場合に障害が生成された場合、**[ナビゲーション（Navigation）]** ペインの **[シャーシ（Chassis）]** メニューの **[障害とログ（Faults and Logs）]** タブで、それぞれの障害の詳細を表示できます。

SPDM 認証 ステータスの表示

次の手順を実行すると、SPDM 認証ステータスと SPDM 証明書チェーンを表示できます。

始める前に

（注） 一部の C シリーズ サーバでのみ有効になります。

手順

	コマンドまたはアクション	目的
ステップ 1	**[ナビゲーション（Navigation）]** ペインで **[管理（Admin）]** メニューをクリックします。	
ステップ 2	[管理（Admin）]メニューで [セキュリティ管理（Security Management）]をクリックします。	
ステップ 3	**[セキュリティ管理（Security Management）]** タブ > **[MCTP SPDM]** タブ > **[アクション（Actions）]** エリアで、次の詳細を表示できます。	• **[証明書のアップロードの進行状況（Certificate Upload Progress）]** - 証明書のアップロードの進行状況を表示します。 • **[証明書のアップロードのステータス（Certificate Upload Status）]** - 証明書のアップロードのステータスを表示します。

	コマンドまたはアクション	目的
		• **[SPDM ステータス（SPDM Status）]** - SDPM 認証ステータス全体を表示します。

認証局証明書の追加

始める前に

（注） 一部の C シリーズ サーバでのみ有効になります。

手順

ステップ 1 **[ナビゲーション（Navigation）]** ペインで **[管理（Admin）]** メニューをクリックします。

ステップ 2 [管理（Admin）]メニューで [セキュリティ管理（Security Management）]をクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]** タブ > **[証明書（Certificates）]** エリア内で **[認証局（Authorities）]** タブをクリックします。

ステップ 4 権限タブで、**[追加（Add）]** アイコンをクリックします。

[機関証明書の追加（Add Authorities Certificate）] ダイアログ ボックスが表示されます。

ステップ 5 次のいずれかのオプションを選択して、認証局の証明書を追加します。

- **[当局証明書の貼り付け（Paste Authorities Certificate）]** を選択します。

  ホストから当局証明書をコピーし、テキスト フィールドにキーを貼り付けます。

- **[ローカルからアップロード (Upload from local)]** を選択します。

  [参照（Browse）] をクリックして、追加する認証局証明書ファイルの場所に移動します。

- **[リモートの場所からアップロード (Upload from remote location)]** を選択します。

  次の詳細情報を入力して、リモート ロケーションから当局証明書ファイルをアップロードします。

名前	説明
ドロップダウン リストから当局証明書をアップロード	リモート サーバーのタイプ。次のいずれかになります。 • TFTP • FTP • SCP • SFTP • HTTP （注） FTP、SCP または SFTP を選択した場合は、ユーザ名とパスワードの入力が求められます。
[サーバIP/ホスト名（Server IP/Hostname）] フィールド	当局証明書ファイルが使用可能なサーバーの IP アドレスまたはホスト名
[Path and Filename] フィールド	リモート サーバー上の当局証明書 ファイルのパスとファイル名。

ステップ 6 **[認証局証明書のアップロード（Upload Authorities Certificate）]** をクリックします。

MCTP SPDM タブの次のフィールドから、アップロードの進行状況とステータスを表示できます。

- 証明書のアップロードの進行状況
- 証明書のアップロードステータス

アップロードが完了して成功すると、認証局の証明書がアップロードされ、詳細が **[認証局（Authorities）]** タブに表示されます。

証明書および証明書の詳細のリストを表示する

始める前に

（注） 一部の C シリーズ サーバでのみ有効になります。

手順

	コマンドまたはアクション	目的
ステップ 1	**[ナビゲーション（Navigation）]** ペインで **[管理（Admin）]** メニューをクリックします。	
ステップ 2	[管理（Admin）]メニューで [セキュリティ管理（Security Management）]をクリックします。	
ステップ 3	**[セキュリティ管理（Security Management）]** タブ > **MCTP SPDM** タブ > **[証明書（Certificates）]** エリア内で **[エンドポイント（Endpoints）]** タブをクリックします。	エンドポイントのリストには、次の詳細が表示されます： • **[共通名（Common Name）]** - エンドポイントのルート CA 証明書の共通名を表示します。 • **[エンドポイント 識別子（Endpoint ID）]** - PCIe スロット識別子を表示します。 • **[ステータス（Status）]** - エンドポイントの最終的な SPDM ハンドシェイク ステータスを表示します。
ステップ 4	**[セキュリティ管理（Security Management）]** タブ > **MCTP SPDM** タブ > **[証明書（Certificates）]** エリア内で **[認証局（Authorities）]** タブをクリックします。	アップロードされた SPDM ルート CA 証明書のリストが、次の詳細とともに表示されます。 • **[共通名（Common Name）]** - 機関証明書の共通名を表示します。 • **[発行者（Issued By）]** - 認証局証明書の発行者の詳細を表示します。 • **[有効期限（Expires）]** - 認証局の証明書の有効性を表示します。 （注） 工場から出荷される証明書の横にロック アイコンが表示されます。ロック アイコンのある証明書を削除することはできません。
ステップ 5	特定の証明書の詳細を表示するには、次の手順を行います：	1. **[認証局（Authorities）]** タブ内で表の任意の行のチェック ボックスを選択します。

	コマンドまたはアクション	目的
		2. エンドポイント証明書の詳細を表示するには **[表示（View）]** アイコンをクリックします。 **[証明書の表示（View Certificate）]** ダイアログボックスに、認証局証明書の次の詳細が表示されます。

証明書の削除

始める前に

（注） 一部の C シリーズ サーバでのみ有効になります。

手順

	コマンドまたはアクション	目的
ステップ 1	**[ナビゲーション（Navigation）]** ペインで **[管理（Admin）]** メニューをクリックします。	
ステップ 2	[管理（Admin）]メニューで [セキュリティ管理（Security Management）]をクリックします。	
ステップ 3	**[セキュリティ管理（Security Management）]** タブ > **MCTP SPDM** タブ > **[証明書（Certificates）]** エリア内で **[認証局（Authorities）]** タブをクリックします。	
ステップ 4	**[認証局（Authorities）]** タブ内で表の任意の行のチェック ボックスを選択します。	（注） 工場から出荷される証明書の横にロック アイコンが表示されます。ロック アイコンのある証明書を削除することはできません。
ステップ 5	エンドポイント証明書を削除するには、**[削除（Delete）]** アイコンをクリックします。	ポップウィンドウに次のメッセージが表示されます： **証明書が正常に削除されました。CIMC はすべてのデバイスを再認証します。**

	コマンドまたはアクション	目的
ステップ 6	[OK] をクリックします。	

キー管理相互運用性プロトコル

キー管理相互運用性プロトコル（KMIP）は、主要な管理サーバーでキーまたは機密データを処理するためのメッセージ形式を定義する通信プロトコルです。KMIP はオープン スタンダードで、複数のベンダーによってサポートされています。キー管理には、複数の相互運用可能な実装が伴うため、KMIP クライアントは KMIP サーバーと効率的に連動します。

自己暗号化ドライブ（SED）には、リアルタイムで着信データを暗号化し、発信データを復号するハードウェアが含まれています。ドライブまたはメディア暗号化キーは、この機能を制御します。しかし、セキュリティを維持するために、ドライブはロックされている必要があります。セキュリティ キー ID とセキュリティ キー（キー暗号キー）を使用すると、この目的を達成できます。キー ID では、ドライブに一意の ID が提供されます。

異なるキーには異なる使用要件があります。現在、ローカル キーの管理および追跡の責任は主にユーザーにあるため、人的ミスが生じる可能性があります。ユーザーはさまざまなキーとそれらの機能を覚えている必要があり、それが困難な場合があります。KMIP は、この懸念領域に対処し、人的関与なしでキーを効率的に管理します。

セキュアなキー管理設定の表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）]メニューで [セキュリティ管理（Security Management）]をクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]**ペインで **[セキュア キーの管理（Secure Key Management）]**をクリックします。

ステップ 4 [Work] ペインで、次の情報を確認します。

名前	説明
[セキュア キー管理の有効化（Enable Secure Key Management）] チェックボックス	このチェックボックスをオンにすると、セキュア キーの管理機能を有効にできます。

ステップ 5 [Actions] 領域で、次の情報を確認します。

名前	説明
[ルート CA 証明書のダウンロード（Download Root CA Certificate）] リンク	このリンクを使用して、ルート CA 証明書を Cisco IMC にダウンロードできます。

名前	説明
[ルートCA証明書のエクスポート（Export Root CA Certificate）] リンク	このリンクを使用して、ダウンロードしたルートCA証明書をローカルファイルまたはリモート サーバにエクスポートできます。
[ルート CA 証明書の削除（Delete Root CA Certificate）] リンク	このリンクを使用して、ルート CA 証明書を削除できます。
[クライアント証明書のダウンロード（Download Client Certificate）] リンク	このリンクを使用して、クライアント証明書を Cisco IMC にダウンロードできます。
[クライアント証明書のエクスポート（Export Client Certificate）] リンク	このリンクを使用して、ダウンロードしたクライアント証明書をローカル ファイルまたはリモート サーバにエクスポートできます。
[クライアント証明書の削除（Delete Client Certificate）] リンク	このリンクを使用して、クライアント証明書を削除できます。
[クライアント秘密鍵のダウンロード（Download Client Private Key）] リンク	このリンクを使用して、クライアント秘密鍵を Cisco IMC にダウンロードできます。
[クライアント秘密鍵のエクスポート（Export Client Private Key）] リンク	このリンクを使用して、ダウンロードしたルートCA証明書をローカルファイルまたはリモート サーバにエクスポートできます。
[クライアント秘密鍵の削除（Delete Client Private Key）] リンク	このリンクを使用して、ルート CA 証明書を削除できます。
[KMIP ログインの削除（Delete KMIP Login）] リンク	このリンクを使用して、KMIP ログイン詳細を削除できます。

ステップ 6 [KMIP サーバー（KMIP Servers）] 領域で、次のフィールドを確認します。

名前	説明
[ID] フィールド	KMIP サーバ設定の ID。
[IPアドレス（IP Address）] フィールド	KMIP サーバの IP アドレス。
[ポート（Port）] フィールド	KMIP サーバとの通信ポート。
[タイムアウト（Timeout）] フィールド	Cisco IMC が KMIP サーバからの応答を待機する時間。
[削除（Delete）] ボタン	KMIP サーバ設定を削除します。
[テスト接続（Test Connection）] ボタン	KMIP 接続が成功したかどうかをテストします。

ステップ 7 [KMIP Root CA Certificate] 領域で、次のフィールドを確認します。

名前	説明
[サーバ ルート CA 証明書（Server Root CA Certificate）] フィールド	ルート CA 証明書の可用性を示します。
[ダウンロード ステータス（Download Status）] フィールド	このフィールドには、ルート CA 証明書のダウンロード ステータスが表示されます。
[ダウンロード中（Download Progress）] フィールド	このフィールドには、ルート CA 証明書ダウンロードの進行状況が表示されます。
[エクスポート ステータス（Export Status）] フィールド	このフィールドには、ルート CA 証明書のエクスポート ステータスが表示されます。
[エクスポート中（Export Progress）] フィールド	このフィールドには、ルート CA 証明書エクスポートの進行状況が表示されます。

ステップ 8 [KMIP Client Certificate] 領域で、次のフィールドを確認します。

名前	説明
[クライアント証明書（Client Certificate）] フィールド	クライアント証明書の可用性を示します。
[ダウンロード ステータス（Download Status）] フィールド	このフィールドには、クライアント証明書のダウンロード ステータスが表示されます。
[ダウンロード中（Download Progress）] フィールド	このフィールドには、クライアント証明書ダウンロードの進行状況が表示されます。
[エクスポート ステータス（Export Status）] フィールド	このフィールドには、クライアント証明書のエクスポート ステータスが表示されます。
[エクスポート中（Export Progress）] フィールド	このフィールドには、クライアント証明書エクスポートの進行状況が表示されます。

ステップ 9 [KMIP Login Details] 領域で、次のフィールドを確認します。

名前	説明
[KMIP ログインの使用（Use KMIP Login）] チェックボックス	KMIP ログインの詳細を使用するかどうかを選択できます。
[KMIP サーバへのログイン名（Login name to KMIP Server）] フィールド	KMIP サーバのユーザ名。
[KMIP サーバへのパスワード（Password to KMIP Server）] フィールド	KMIP サーバのパスワード。

名前	説明
[パスワードの変更（Change Password）] チェックボックス	KMIP パスワードを変更できます。
[新しいパスワード（New Password）] フィールド	KMIP サーバに割り当てる新しいパスワードを入力できます。 （注） このオプションは、[Change Password] チェックボックスを有効にしている場合にのみ表示されます。
[パスワードの確認（Confirm Password）] フィールド	このフィールドにもう一度新しいパスワードを入力します。 （注） このオプションは、[Change Password] チェックボックスを有効にしている場合にのみ表示されます。

ステップ 10 [KMIP Client Private Key] 領域で、次のフィールドを確認します。

名前	説明
[クライアント秘密鍵（Client Private Key）] フィールド	クライアント秘密鍵の可用性を示します。
[ダウンロード ステータス（Download Status）] フィールド	このフィールドには、クライアント秘密鍵のダウンロード ステータスが表示されます。
[ダウンロード中（Download Progress）] フィールド	このフィールドには、クライアント秘密鍵ダウンロードの進行状況が表示されます。
[エクスポート ステータス（Export Status）] フィールド	このフィールドには、クライアント秘密鍵のエクスポート ステータスが表示されます。
[エクスポート中（Export Progress）] フィールド	このフィールドには、クライアント秘密鍵エクスポートの進行状況が表示されます。

KMIP 設定のクライアント秘密キーおよびクライアント証明書の作成

パブリック認証局（CA）を使用してサーバ証明書の生成と署名を行う代わりに、独自の CA を運用して独自の証明書に署名することができます。このセクションでは、Linux で実行されている OpenSSL 証明書サーバーを使用して CA を作成するコマンドおよびサーバー証明書を

生成するコマンドについて説明します。OpenSSL の詳細については、http://www.openssl.org を参照してください。

（注） これらのコマンドは、Cisco IMC ではなく、OpenSSL パッケージを使用している Linux サーバーで入力します。

始める前に

- 組織内のサーバーで、証明書サーバーのソフトウェア パッケージを取得してインストールします。
- Cisco IMC の時刻が現在の時刻に設定されていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**openssl genrsa -out** *Client_Privatekeyfilename keysize* **例：** `# openssl genrsa -out client_private.pem 2048`	このコマンドは、クライアント証明書の生成に使用されるクライアント秘密キーを生成します。 指定されたファイル名には、指定されたサイズの RSA キーが含まれています。
ステップ 2	**openssl req -new -x509 -days** *numdays* **-key** *Client_Privatekeyfilename* **-out** *Client_certfilename* **例：** `# openssl req -new -x509 -key client_private.pem -out client.pem -days 365`	このコマンドは、前の手順で入手したクライアント秘密キーを使用して、新しい自己署名クライアント証明書を生成します。証明書は指定された期間有効になります。このコマンドは、ユーザーに証明書の追加情報を求めるプロンプトを表示します。 新しい自己署名クライアント証明書が作成されます。
ステップ 3	KMIP サーバーから KMIP ルート CA 証明書を取得します。	ルート CA 証明書の取得については、KMIP のベンダーマニュアルを参照してください。

次のタスク

新しい証明書を Cisco IMC にアップロードします。

クライアント証明書のダウンロード

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）]メニューで [セキュリティ管理（Security Management）]をクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]**ペインで **[セキュア キーの管理（Secure Key Management）]**をクリックします。

ステップ 4 [Secure Key Management] タブの [Actions] 領域で、[Download Client Certificate] をクリックします。

ステップ 5 [Download Client Certificate] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[リモートロケーションからダウンロード（Download From Remote Location）] オプションボタン	このオプションを選択することで、証明書をリモートの場所から選択してダウンロードできます。次の詳細を入力します。 • **[TFTP サーバー（TFTP Server）]** • **FTP サーバー（FTP Server）** • **SFTP サーバー（SFTP Server）** • **SCP サーバー（SCP Server）** • **HTTP サーバー（HTTP Server）** （注） このアクションを実行中にリモートサーバのタイプとして SCP または SFTP を選択した場合、ポップアップ ウィンドウが表示され、そこに *[*サーバ（*RSA*）鍵フィンガープリントは *<server_finger_print _ID>* です。続行しますか*?*（*Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*）*]* というメッセージが表示されます。サーバ フィンガープリントの信頼度に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。 • [サーバー IP/ホスト名（Server IP/Hostname）] フィールド：クライアント証明書ファイルを保管するサーバーの IP アドレスまたはホスト名。[Download Certificate from] ドロップダウン リストの設定によって、このフィールドの名前は異なる場合があります。 • [Path and Filename] フィールド：リモート サーバーにファイルをダウンロードする際に Cisco IMC に使用する必要があるパスおよびファイル名。 • [Username] フィールド：システムがリモート サーバーにログインする際に使用するユーザー名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。 • [パスワード（Password）] フィールド：リモート サーバーのユーザー名に対応するパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。

名前	説明
[ブラウザ クライアントによるダウンロード（Download Through Browser Client）] オプション ボタン	このオプションを選択することで、Cisco IMC GUI を実行しているコンピュータのローカル ドライブに保管されている証明書に移動できます。 このオプションを選択すると、Cisco IMC GUI に [参照（Browse）] ボタンが表示されます。このボタンを使用して、インポートするファイルに移動できます。
[内容を貼り付け（Paste Content）] オプション ボタン	このオプションを選択すると、署名付き証明書の内容全体をコピーして、[証明書の内容の貼り付け（Paste Certificate Content）] テキスト フィールドに貼り付けることができます。 （注） アップロードの前に、証明書に署名が付されていることを確認します。

クライアント証明書のエクスポート

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [セキュリティ管理（Security Management）] をクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]** ペインで **[セキュア キーの管理（Secure Key Management）]** をクリックします。

ステップ 4 [Secure Key Management] タブの [Actions] 領域で、[Export Client Certificate] をクリックします。

ステップ 5 [Export Client Certificate] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Export to Remote Location]	

名前	説明
	このオプションを選択すると、リモートロケーションの証明書を選択してエクスポートできます。次の詳細を入力します。 • • **[TFTP サーバー（TFTP Server）]** • **FTP サーバー（FTP Server）** • **SFTP サーバー（SFTP Server）** • **SCP サーバー（SCP Server）** • **HTTP サーバー（HTTP Server）** （注） このアクションを実行中にリモートサーバのタイプとして SCP または SFTP を選択した場合、ポップアップ ウィンドウが表示され、そこに *[*サーバ（*RSA*）鍵フィンガープリントは *<server_finger_print _ID>* です。続行しますか*?*（*Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*）*]* というメッセージが表示されます。サーバフィンガープリントの信頼度に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。 • [サーバー IP/ホスト名（Server IP/Hostname）] フィールド：証明書ファイルをエクスポートするサーバーの IP アドレスまたはホスト名。[Download Certificate from] ドロップダウン リストの設定によって、このフィールドの名前は異なる場合があります。 • [パスおよびファイル名（Path and Filename）] フィールド：リモートサーバから証明書をダウンロードする際に Cisco IMC が使用するパスとファイル名。

名前	説明
	• **[ユーザ名（Username）]** フィールド—リモート サーバにログインするためにシステムが使用するユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。 • [パスワード（Password）] フィールド：リモート サーバーのユーザー名に対応するパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。
[Export to Local File]	このオプションを選択することで、コンピュータのローカル ドライブに保管されている証明書を選択してエクスポートできます。

クライアント証明書の削除

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。
ステップ 2 [管理（Admin）]メニューで [セキュリティ管理（Security Management）]をクリックします。
ステップ 3 **[セキュリティ管理（Security Management）]**ペインで **[セキュア キーの管理（Secure Key Management）]**をクリックします。
ステップ 4 [Secure Key Management] タブの [Actions] 領域で、[Delete Client Certificate] をクリックします。
ステップ 5 プロンプトで、[OK] をクリックしてクライアント証明書を削除するか、または [Cancel] をクリックして操作をキャンセルします。

ルート CA 証明書のダウンロード

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。
ステップ 2 [管理（Admin）]メニューで [セキュリティ管理（Security Management）]をクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]**ペインで **[セキュア キーの管理（Secure Key Management）]**をクリックします。

ステップ 4 [Secure Key Management] タブの [Actions] 領域で、[Download Root CA Certificate] をクリックします。

ステップ 5 [Download Root CA Certificate] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[リモートロケーションからダウンロード（Download From Remote Location）] オプションボタン	このオプションを選択することで、証明書をリモートの場所から選択してダウンロードできます。次の詳細を入力します。 • **• [TFTP サーバー（TFTP Server）]** **• FTP サーバー（FTP Server）** **• SFTP サーバー（SFTP Server）** **• SCP サーバー（SCP Server）** **• HTTP サーバー（HTTP Server）** （注） このアクションを実行中にリモートサーバのタイプとして SCP または SFTP を選択した場合、ポップアップ ウィンドウが表示され、そこに *[*サーバ（*RSA*）鍵フィンガープリントは *<server_finger_print _ID>* です。続行しますか*?*（*Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*）*]* というメッセージが表示されます。サーバ フィンガープリントの信頼度に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。 • [サーバー IP/ホスト名（Server IP/Hostname）] フィールド：ルート CA 証明書ファイルを保管するサーバーの IP アドレスまたはホスト名。[Download Certificate from] ドロップダウン リストの設定によって、このフィールドの名前は異なる場合があります。 • [Path and Filename] フィールド：リモート サーバーにファイルをダウンロードする際に Cisco IMC に使用する必要があるパスおよびファイル名。 • [Username] フィールド：システムがリモート サーバーにログインする際に使用するユーザー名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。 • [パスワード（Password）] フィールド：リモート サーバーのユーザー名に対応するパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。

名前	説明
[ブラウザ クライアントによるダウンロード（Download Through Browser Client）] オプション ボタン	このオプションを選択することで、Cisco IMC GUI を実行しているコンピュータのローカル ドライブに保管されている証明書に移動できます。 このオプションを選択すると、Cisco IMC GUI に [参照（Browse）] ボタンが表示されます。このボタンを使用して、インポートするファイルに移動できます。
[内容を貼り付け（Paste Content）] オプション ボタン	このオプションを選択すると、署名付き証明書の内容全体をコピーして、[証明書の内容の貼り付け（Paste Certificate Content）] テキスト フィールドに貼り付けることができます。 （注） アップロードの前に、証明書に署名が付されていることを確認します。

ルート CA 証明書のエクスポート

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [セキュリティ管理（Security Management）] をクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]** ペインで **[セキュア キーの管理（Secure Key Management）]** をクリックします。

ステップ 4 [Secure Key Management] タブの [Actions] 領域で、[Export Root CA Certificate] をクリックします。

ステップ 5 [Export Root CA Certificate] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Export to Remote Location]	

名前	説明
	このオプションを選択すると、リモートロケーションの証明書を選択してエクスポートできます。次の詳細を入力します。 • • **[TFTP サーバー（TFTP Server）]** • **FTP サーバー（FTP Server）** • **SFTP サーバー（SFTP Server）** • **SCP サーバー（SCP Server）** • **HTTP サーバー（HTTP Server）** （注） このアクションを実行中にリモートサーバのタイプとして SCP または SFTP を選択した場合、ポップアップ ウィンドウが表示され、そこに *[*サーバ（*RSA*）鍵フィンガープリントは *<server_finger_print _ID>* です。続行しますか*?*（*Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*）*]* というメッセージが表示されます。サーバフィンガープリントの信頼度に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。 • [サーバー IP/ホスト名（Server IP/Hostname）] フィールド：証明書ファイルをエクスポートするサーバーの IP アドレスまたはホスト名。[Download Certificate from] ドロップダウン リストの設定によって、このフィールドの名前は異なる場合があります。 • [パスおよびファイル名（Path and Filename）] フィールド：リモートサーバから証明書をダウンロードする際に Cisco IMC が使用するパスとファイル名。

名前	説明
	• **[ユーザ名（Username）]** フィールド—リモート サーバにログインするためにシステムが使用するユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。 • [パスワード（Password）] フィールド：リモート サーバーのユーザー名に対応するパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。
[Export to Local File]	このオプションを選択することで、コンピュータのローカル ドライブに保管されている証明書を選択してエクスポートできます。

ルート CA 証明書の削除

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）]メニューで [セキュリティ管理（Security Management）]をクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]**ペインで **[セキュア キーの管理（Secure Key Management）]**をクリックします。

ステップ 4 [Secure Key Management] タブの [Actions] 領域で、[Delete Root CA Certificate] をクリックします。

ステップ 5 プロンプトで、[OK] をクリックしてルート CA 証明書を削除するか、または [Cancel] をクリックして操作をキャンセルします。

クライアント秘密キーのダウンロード

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）]メニューで [セキュリティ管理（Security Management）]をクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]**ペインで **[セキュア キーの管理（Secure Key Management）]**をクリックします。

ステップ 4 [Secure Key Management] タブの [Actions] 領域で、[Download Client Private Key] をクリックします。

ステップ 5 [Download Client Private Key] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[リモート ロケーションからダウンロード（Download From Remote Location）] オプション ボタン	このオプションを選択すると、リモート ロケーションにある秘密鍵を選択してダウンロードできます。次の詳細を入力します。 • **• [TFTP サーバー（TFTP Server）]** **• FTP サーバー（FTP Server）** **• SFTP サーバー（SFTP Server）** **• SCP サーバー（SCP Server）** **• HTTP サーバー（HTTP Server）** （注） このアクションを実行中にリモート サーバのタイプとして SCP または SFTP を選択した場合、ポップアップ ウィンドウが表示され、そこに *[*サーバ（*RSA*）鍵フィンガープリントは *<server_finger_print _ID>* です。続行しますか*?*（*Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*）*]* というメッセージが表示されます。サーバ フィンガープリントの信頼度に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。 • [サーバー IP/ホスト名（Server IP/Hostname）] フィールド：クライアント秘密キーを保管するサーバーの IP アドレスまたはホスト名。[Download Certificate From] ドロップダウン リストの設定によって、このフィールドの名前は異なる場合があります。 • [Path and Filename] フィールド：リモート サーバーにファイルをダウンロードする際に Cisco IMC に使用する必要があるパスおよびファイル名。 • [Username] フィールド：システムがリモート サーバーにログインする際に使用するユーザー名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。 • [パスワード（Password）] フィールド：リモート サーバーのユーザー名に対応するパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。

名前	説明
[ブラウザ クライアントによるダウンロード（Download Through Browser Client）] オプション ボタン	このオプションを選択すると、Cisco IMC GUI を実行しているコンピュータのローカル ドライブ上に保管されている秘密鍵に移動できます。 このオプションを選択すると、Cisco IMC GUI に、インポートするファイルに移動するために使用できる [参照（Browse）] ボタンが表示されます。
[内容を貼り付け（Paste Content）] オプション ボタン	このオプションを選択すると、署名付き秘密鍵の内容全体をコピーして、[秘密鍵の内容の貼り付け（Paste Private Key Content）]テキスト フィールドに貼り付けることができます。

次のタスク

クライアント秘密キーのエクスポート

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）]メニューで [セキュリティ管理（Security Management）]をクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]**ペインで **[セキュア キーの管理（Secure Key Management）]**をクリックします。

ステップ 4 [Secure Key Management] タブの [Actions] 領域で、[Export Client Private Key] をクリックします。

ステップ 5 [Export Client Private Key] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Export to Remote Location]	

名前	説明
	このオプションを選択すると、リモートロケーションの証明書を選択してエクスポートできます。次の詳細を入力します。 • **• [TFTP サーバー（TFTP Server）]** **• FTP サーバー（FTP Server）** **• SFTP サーバー（SFTP Server）** **• SCP サーバー（SCP Server）** **• HTTP サーバー（HTTP Server）** （注） このアクションを実行中にリモートサーバのタイプとして SCP または SFTP を選択した場合、ポップアップ ウィンドウが表示され、そこに *[*サーバ（*RSA*）鍵フィンガープリントは *<server_finger_print _ID>* です。続行しますか*?*（*Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*）*]* というメッセージが表示されます。サーバフィンガープリントの信頼度に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。 • [サーバー IP/ホスト名（Server IP/Hostname）] フィールド：証明書ファイルをエクスポートするサーバーの IP アドレスまたはホスト名。[Download Certificate from] ドロップダウン リストの設定によって、このフィールドの名前は異なる場合があります。 • [パスおよびファイル名（Path and Filename）] フィールド：リモートサーバから証明書をダウンロードする際に Cisco IMC が使用するパスとファイル名。

名前	説明
	• **[ユーザ名（Username）]** フィールド—リモート サーバにログインするためにシステムが使用するユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。 • [パスワード（Password）] フィールド：リモート サーバーのユーザー名に対応するパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。
[Export to Local File]	このオプションを選択することで、コンピュータのローカル ドライブに保管されている証明書を選択してエクスポートできます。

クライアント秘密キーの削除

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。
ステップ 2 [管理（Admin）]メニューで [セキュリティ管理（Security Management）]をクリックします。
ステップ 3 **[セキュリティ管理（Security Management）]**ペインで **[セキュア キーの管理（Secure Key Management）]**をクリックします。
ステップ 4 [Secure Key Management] ペインの [Actions] 領域で、[Delete Client Private Key] をクリックします。
ステップ 5 プロンプトで、[OK] をクリックしてクライアント秘密キーを削除するか、または [Cancel] をクリックして操作をキャンセルします。

KMIP サーバー接続のテスト

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。
ステップ 2 [管理（Admin）]メニューで [セキュリティ管理（Security Management）]をクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]**ペインで **[セキュア キーの管理（Secure Key Management）]**をクリックします。

ステップ 4 [Secure Key Management] タブの [KMIP Servers] 領域で、チェックボックスをオンにすることで行を選択し、[Test Connection] をクリックします。

ステップ 5 接続に成功すると、成功メッセージが表示されます。

KMIP サーバーのデフォルト設定への復元

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）]メニューで [セキュリティ管理（Security Management）]をクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]**ペインで **[セキュア キーの管理（Secure Key Management）]**をクリックします。

ステップ 4 [Secure Key Management] タブの [KMIP Servers] 領域で、チェックボックスをオンにすることで行を選択し、[Delete] をクリックします。

ステップ 5 プロンプトで [OK] をクリックします。

これで、KMIP サーバーがデフォルト設定に復元されます。

KMIP ログイン詳細の削除

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）]メニューで [セキュリティ管理（Security Management）]をクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]**ペインで **[セキュア キーの管理（Secure Key Management）]**をクリックします。

ステップ 4 [Secure Key Management] ペインの [Actions] 領域で、[Delete KMIP Login] をクリックします。

ステップ 5 プロンプトで、[OK] をクリックして KMIP ログインの詳細を削除するか、または [Cancel] をクリックして操作をキャンセルします。

Cisco IMC での FIPS 140-2 の準拠

Federal Information Processing Standard（FIPS）パブリケーション 140-2 は、暗号モジュールの認定に使用される米国政府のコンピュータ セキュリティ標準です3.1(3) リリースでは、ラック Cisco IMC は NIST ガイドラインに従った FIPS 対応ではありません。これは FIPS 140-2 で承認された暗号化アルゴリズムとモジュールに従っていません。このリリースで、すべての CIMC サービスは、Cisco FIPS オブジェクト モジュール（FOM）を使用します。これにより、FIPS 140-2 に準拠した暗号化モジュールが提供されます。

Cisco FIPS オブジェクト モジュールは、Cisco の広範なネットワー キング製品およびコラボレーション製品に暗号化サービスを提供するソフトウェア ライブラリです。モジュールは、IPSec（IKE）、SRTP、SSH、TLS、SNMP などのサービスに対して、FIPS 140 の検証済みの暗号化アルゴリズムと KDF 機能を提供します。

セキュリティ設定の有効化

始める前に

このタスクを実行するには、admin 権限を持つユーザーとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）]メニューで [セキュリティ管理（Security Management）]をクリックします。

ステップ 3 [セキュリティ管理（Security Management）] ペインで、[セキュリティ設定（Security Configuration）] をクリックします。

ステップ 4 [連邦情報処理標準設定（FIPS）とコモンクライテリア（CC）設定（Federal Information Processing Standard Configuration (FIPS) and Common Criteria (CC) Configuration）] ペインで、 [FIPS の有効化（Enable FIPS）] チェック ボックスをオンにします。

表 *18 :* 連邦情報処理標準（*FIPS*）およびコモンクライテリア（*CC*）の構成

名前	説明
[FIPSの有効化（Enable FIP Mode）] チェックボックス	

名前	説明
	オンにすると、FIPS 機能を有効にすることができます。デフォルトでは、このオプションは無効になっています。 FIPS を有効にすると、SNMP 設定に次のような影響があります。 • SNMPv2 プロトコル向けのコミュニティ文字列の設定、および [noAuthNoPriv] または [authNoPriv] が指定された SNMPv3 ユーザーのセキュリティ レベル オプションが無効になります。 • [NoAuthNoPriv] のセキュリティ レベル オプションが指定された SNMPv2 または SNMPv3 ユーザー向けに設定されたトラップが無効になります。 • [MD5] および [DES] 認証タイプおよびプライバシー タイプが無効になります。 （注） DES プライバシー タイプは、リリース 4.1（3b） 以降には適用されません。ただし、DES をリリース 4.1（3b） 以降にアップグレードする前に以前のリリースで構成されていた場合は、DES プライバシー タイプが表示される場合がありますが、FIPS が有効になっている場合は無効になります。 （注） **[MD5]** および **[DES]** 認証タイプとプライバシー タイプは、Cisco UCS M6 C シリーズ サーバーではサポートされていません。 • また、SSH、Webサーバー、vKVM 接続で FIPS 準拠の暗号方式のみが使用されるようになります。 • コモンクライテリアを有効にすることができます。 • TACACS+認証を無効にします。

名前	説明
[CCの有効化（Enable CC）] チェックボックス	（注） CCを有効化するには、FIPSを有効化する必要があります。 オンにすると、CC機能を有効にすることができます。デフォルトでは、このオプションは無効になっています。 （注） **[通信サービス（Communication Services）]** の **[TLS v1.2の有効化（Enable TLS v1.2）]** チェックが無効になっている場合、**CC** を有効にすることはできません。

（注） FIPSモードまたはCCモードを切り替えると、SSH、KVM、SNMP、webサーバー、XMLAPI、およびredfishサービスが再起動されます。続行するかどうかの確認を求められます。続行するには [OK] をクリック、そうでない場合は [キャンセル（Cancel）] をクリックします。

セキュリティ設定（FIPS）の有効化

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）]メニューで [セキュリティ管理（Security Management）]をクリックします。

ステップ 3 [セキュリティ管理（Security Management）] ペインで、[セキュリティ設定（Security Configuration）] をクリックします。

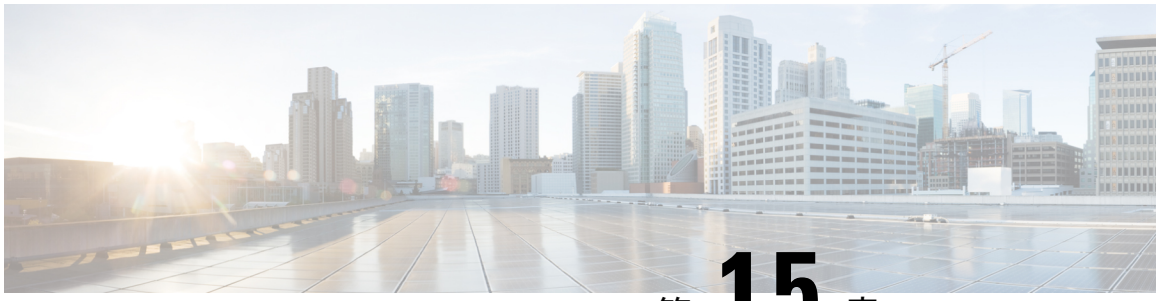
ステップ 4 [ワーク（Work）] ペインで、[FIPSの有効化（Enable FIPS）] チェックボックスをオンにします。

（注） FIPSモードを切り替えると、SSH、KVM、SNMP、webサーバー、XMLAPI、およびredfishサービスが再起動されます。

ステップ 5 続行するかどうかの確認を求められます。続行するには [OK] をクリック、そうでない場合は [キャンセル（Cancel）] をクリックします。

（注） FIPS を有効にすると、SNMP 設定に次のような影響があります。

- SNMPv2 プロトコル向けのコミュニティ文字列の設定、および [noAuthNoPriv] または [authNoPriv] が指定された SNMPv3 ユーザーのセキュリティ レベル オプションが無効になります。
- [NoAuthNoPriv] のセキュリティ レベル オプションが指定された SNMPv2 または SNMPv3 ユーザー向けに設定されたトラップが無効になります。
- [MD5] および [DES] 認証タイプおよびプライバシー タイプが無効になります。
- また、SSH、Webサーバー、KVM 接続で FIPS 準拠の暗号方式のみが使用されるようになります。



第 15 章

ファームウェアの管理

この章は、次の内容で構成されています。

ファームウェア管理の概要

次のファームウェア コンポーネントは Web UI の 1 つのページで管理できます。

- アダプタ ファームウェア：メインのオペレーティング ファームウェア（アクティブイメージとバックアップイメージで構成）は、次のようなさまざまなインターフェイスからインストールできます。
  - Host Upgrade Utility（HUU）
  - Web UI：ローカル プロトコルおよびリモート プロトコル
  - PMCLI：リモート プロトコル
  - XML API：リモート プロトコル

  ファームウェア イメージをローカル ファイル システムまたは TFTP サーバからアップロードできます。
- ブートローダ ファームウェア：ブートローダ ファームウェアは、Cisco IMC からインストールできません。このファームウェアは、Host Upgrade Utility を使用してインストールできます。

次の各コンポーネントのファームウェアを更新できます。

- BMC
- BIOS

- CMC
- SAS エクスパンダ
- アダプタ

ハードディスク ドライブ（HDD）のファームウェアは、上述のアダプタ ファームウェアと同じインターフェイスからインストールすることもできます。

ファームウェア コンポーネントの表示

手順

ステップ 1 [管理（Admin）] メニューで [ファームウェア管理（Firmware Management）] をクリックします。

ステップ 2 [General] タブの [Firmware Management] 領域で、次の情報を確認します。

名前	説明
[Update] ボタン	ローカルマシンまたはリモートサーバで利用可能なファームウェアイメージファイルをインストールするダイアログボックスを開きます。
[Activate] ボタン	サーバでアクティベートする利用可能なファームウェアバージョンを選択するダイアログボックスを開きます。 **重要** ファームウェアまたは BIOS の更新が進行中の場合は、それらのタスクが完了するまで新しいファームウェアをアクティブ化しないでください。
[アクティベーションのキャンセル] ボタン	（注） このボタンは、[アクティベーションの保留] 状態の BIOS ファームウェアを選択した場合にのみ表示されます。 このボタンを使用して、選択した保留状態の BIOS のアクティベーションをキャンセルできます。
[component] 列	ファームウェアを更新できる、使用可能なコンポーネントのリストです。

名前	説明
[Running Version] カラム	現在アクティブなコンポーネントのファームウェア バージョン。
[Backup Version] カラム	サーバにインストールされた代替ファームウェア バージョン（あれば）。バックアップ バージョンは現在動作していません。アクティベートするには、[Activate] をクリックします。 （注） 新しいファームウェアをインストールする際、既存のバックアップ バージョンがあるなら、すべて削除され、新しいファームウェアがバックアップ バージョンになります。新規のバージョンをサーバで実行する場合、手動で新規のファームウェアをアクティベートする必要があります。
[Bootloader Version] カラム	コンポーネントのブートローダ ソフトウェアに関連付けられたブートローダのバージョン。
[Status]カラム	このサーバのファームウェアアクティベーションのステータス。
[Progress in %] カラム	操作の進捗状況のパーセント表示。

ファームウェアの更新

[ファームウェア管理（Firmware Management）]領域で選択するコンポーネントに応じて、ローカル ディスクまたはリモート サーバからファームウェア パッケージをインストールできます。インストールを確認した後、BMC によってコンポーネントのバックアップ メモリ スロット内のファームウェア バージョンが選択したバージョンに置き換えられます。

手順

ステップ 1 [管理（Admin）] メニューで [ファームウェア管理（Firmware Management）] をクリックします。

ステップ 2 [Firmware Management] 領域で、[Component] カラムからコンポーネントを選択し、[Update] をクリックします。

[Update Firmware] ダイアログボックスが表示されます。

ステップ 3 このダイアログボックスで次の情報を確認します。

名前	説明
[Install Firmware through Browser Client] オプション ボタン	ファームウェア パッケージがローカル マシンに存在する場合は、このオプション ボタンをクリックします。
[リモートサーバーによるファームウェアのインストール（Install Firmware through Remote Server）] オプション ボタン	ファームウェア パッケージがリモート サーバーに存在する場合は、このオプション ボタンをクリックします。

ステップ 4 ブラウザのクライアントを介してファームウェアをインストールするには、[Browse] をクリックしてインストールするファームウェア ファイルに移動します。

ステップ 5 ファイルを選択してから、[Install Firmware] をクリックします。

ステップ 6 リモート サーバーを使用してファームウェアを更新するには、[Install Firmware from] ドロップダウンリストからリモート サーバーのタイプを選択します。次のいずれかを選択できます。

- **TFTP**
- **FTP**
- **SFTP**
- **SCP**
- **[HTTP]**

ステップ 7 選択したリモート サーバーのタイプに応じて、サーバーの [IP/Hostname] および [Image Path and Filename] フィールドに詳細を入力します。

ファームウェアをインストールすると、新しいイメージが非アクティブなイメージと置き換わります。インストール後にイメージをアクティブにすることができます。

重要 FTP、SFTP、SCP サーバー タイプの場合は、ユーザー クレデンシャルを提供する必要があります。

ステップ 8 [Install Firmware] をクリックして、ダウンロードとインストールを開始します。

ファームウェアのアクティブ化

手順

ステップ 1 [管理（Admin）] メニューで [ファームウェア管理（Firmware Management）] をクリックします。

ステップ 2 [Firmware Management] 領域で、[Component] カラムからコンポーネントを選択し、[Activate] をクリックします。

[Activate Firmware] ダイアログボックスが表示されます。

ステップ 3 [Activate Firmware] ダイアログボックスで、アクティブにするファームウェア イメージ（オプション ボタン）を選択します。このイメージは実行中のバージョンになります。

ステップ 4 [Activate Firmware] をクリックします。

選択したファームウェア イメージに応じて、アクティブ化のプロセスが開始されます。

重要 アクティブ化の進行中は、次のことを行わないでください。

- サーバのリセット、電源切断、シャットダウン
- BMC のリブートまたはリセット
- 他のファームウェアのアクティベート
- テクニカル サポートまたは設定データのエクスポート

ファームウェアのアクティベーションのキャンセル

始める前に

アクティベーションをキャンセルするためには、BIOSファームウェアは[アクティベーションの保留（Activation Pending）] 状態である必要があります。

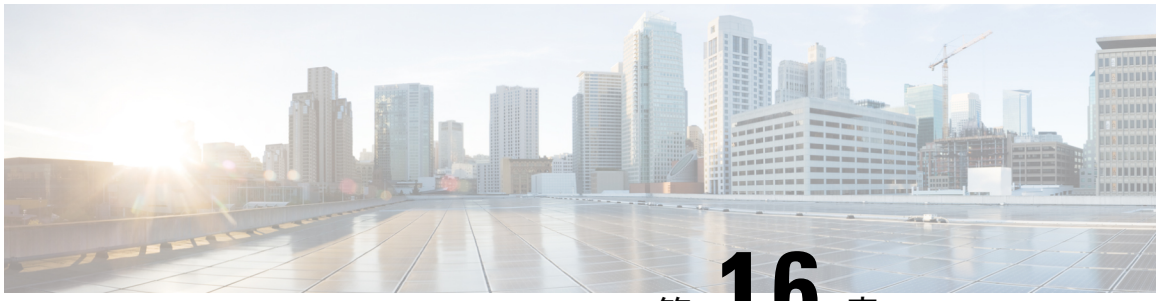
手順

ステップ 1 [管理（Admin）] メニューで [ファームウェア管理（Firmware Management）] をクリックします。

ステップ 2 **[Firmware Management]** 領域で、アクティベーションをキャンセルする BIOS ファームウェアを選択します。

ステップ 3 [アクティベーションのキャンセル（Cancel Activation）] をクリックします。

[アクティベーションの保留（Activation Pending）]状態の BIOSファームウェアを選択した場合にのみ [アクティベーションのキャンセル（Cancel Activation）] ボタンが表示されます。



第 16 章

障害およびログの表示

この章は、次の内容で構成されています。

障害サマリ

障害サマリーの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Faults and Logs] をクリックします。

ステップ 3 [Faults Summary] タブで、次の情報を確認します。

表 *19 : [Actions]* 領域

名前	説明
[Total]	[Fault Entries] テーブルの合計行数を表示します。
[列（Column）] ドロップダウン リスト	表示する列を選択できます。

名前	説明
[表示（Show）] ドロップダウン リスト	フィルタを使用して障害のエントリを表示する方法をカスタマイズします。これらの内容は次のとおりです。 • [簡易フィルタ（Quick Filter）]：デフォルト ビュー。 • [高度なフィルタ（Advanced Filter）]：1つ以上の条件に基づいて障害エントリを表示するためのフィルタ オプション。マッチング ルールを使用して、[フィルタ（Filter）] フィールドで指定したルールのすべてまたはいくつかのルールの組み合わせと一致するエントリを表示できます。 [Go] をクリックすると、設定したフィルタ基準と一致するエントリが表示されます。 設定したフィルタ基準は、[Save] アイコンをクリックして保存することができます。保存されたフィルタ基準は、ユーザ定義のフィルタとして後で使用できます。 （注） ユーザ定義のフィルタは [Manage Preset Filters] ダイアログボックスに表示されます。 • [All]：すべてのエントリが表示されます。 • [Manage Preset Filters]：ユーザ定義のフィルタが表示されます。このダイアログボックスで、ユーザ定義のフィルタを編集したり削除したりできます。 • [List of pre-defined filters）]：システム定義のフィルタが表示されます。 （注） [Filter] アイコンを使用して、フィルタ フィールドを非表示または非表示解除できます。

表 *20 : [*障害エントリ（*Fault Entries*）*]* 領域

名前	説明
[Time]	障害が発生した時刻。
シビラティ（重大度）（**Severity**）	次のいずれかになります。 • [クリア済み（Cleared）] : 障害または状態がクリアされました。 • **[Critical]** • **[Info]** • メジャー • マイナー • 警告
[Code]	障害に割り当てられた固有識別情報。
[DN]	識別名（DN）は、サーバ上でのデバイスエンドポイントおよびそのインスタンスの階層表現です。
[Probable Cause]	障害の原因となったイベントに関連付けられた固有識別情報。
[Description]	障害についての詳細情報。 提案されるソリューションも含まれます。

障害履歴

障害履歴の表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。
ステップ 2 [Chassis] メニューで、[Faults and Logs] をクリックします。
ステップ 3 [Faults History] タブで、次の情報を確認します。

表 *21 : [Actions]* 領域

名前	説明
[Total]	[Fault History] テーブルの合計行数を表示します。
[Column] ドロップダウン リスト	表示する列を選択できます。
[Show] ドロップダウン リスト	フィルタを使用して障害履歴エントリを表示する方法をカスタマイズします。これらの内容は次のとおりです。 • [Quick Filter]：デフォルト ビュー。 • [Advanced Filter]：1 つ以上の条件に基づいてエントリを表示するフィルタ オプション。マッチング ルールを使用して、[Filter] フィールドで指定したルールのすべてまたはいくつかのルールの組み合わせと一致するエントリを表示できます。 [Go] をクリックすると、設定したフィルタ基準と一致するエントリが表示されます。 設定したフィルタ基準は、[Save] アイコンをクリックして保存することができます。保存されたフィルタ基準は、ユーザ定義のフィルタとして後で使用できます。 （注） ユーザ定義のフィルタは [Manage Preset Filters] ダイアログボックスに表示されます。 • [All]：すべてのエントリが表示されます。 • [Manage Preset Filters]：ユーザ定義のフィルタが表示されます。このダイアログボックスで、ユーザ定義のフィルタを編集したり削除したりできます。 • [List of pre-defined filters）]：システム定義のフィルタが表示されます。 （注） [Filter]アイコンを使用して、フィルタ フィールドの表示/非表示を切り替えることできます。

表 *22 : [Fault History]* エリア

名前	説明
[Time]	障害が発生した時刻。
シビラティ（重大度）（**Severity**）	次のいずれかになります。 • **[緊急（Emergency）]** • **[アラート（Alert）]** • **[Critical]** • **[エラー（Error）]** • 警告 • **[Notice]** • **[Informational]** • **デバッグ（Debug）**
[Source]	イベントをログに記録したソフトウェア モジュール。
[Probable Cause]	障害の原因となったイベントに関連付けられた固有識別情報。
[Description]	障害についての詳細情報。 提案されるソリューションも含まれます。

次のタスク

Cisco IMC ログ

Cisco IMC ログの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。
ステップ 2 [Chassis] メニューで、[Faults and Logs] をクリックします。
ステップ 3 [Cisco IMC Log] タブで、次の情報を確認します。

表 *23 : [Actions]* 領域

名前	説明
[Clear Log] ボタン	すべてのログ ファイルをクリアします。 （注） このオプションは、ユーザ ID に **admin** または **user** ユーザ ロールが割り当てられている場合のみ使用できます。
[Total]	[Cisco IMC Log] テーブルの合計行数を表示します。
[Column] ドロップダウン リスト	表示する列を選択できます。

名前	説明
[Show] ドロップダウン リスト	フィルタを使用して Cisco IMC ログ エントリを表示する方法をカスタマイズします。これらの内容は次のとおりです。 • [Quick Filter]：デフォルト ビュー。 • [Advanced Filter]：1 つ以上の条件に基づいてログ エントリを表示するフィルタ オプション。マッチング ルールを使用して、[Filter] フィールドで指定したルールのすべてまたはいくつかのルールの組み合わせと一致するエントリを表示できます。 [Go] をクリックすると、設定したフィルタ基準と一致するエントリが表示されます。 設定したフィルタ基準は、[Save] アイコンをクリックして保存することができます。保存されたフィルタ基準は、ユーザ定義のフィルタとして後で使用できます。 （注） ユーザ定義のフィルタは [Manage Preset Filters] ダイアログボックスに表示されます。 • [All]：すべてのエントリが表示されます。 • [Manage Preset Filters]：ユーザ定義のフィルタが表示されます。このダイアログボックスで、ユーザ定義のフィルタを編集したり削除したりできます。 • [List of pre-defined filters）]：システム定義のフィルタが表示されます。 （注） [Filter] アイコンを使用して、フィルタ フィールドの表示/非表示を切り替えることできます。

表 *24 : [Cisco IMC Log]* テーブル

名前	説明
[Time] カラム	イベントが発生した日時。

名前	説明
[Severity] カラム	イベントのシビラティ（重大度）。次のいずれかになります。 • **[緊急（Emergency）]** • **[アラート（Alert）]** • **[Critical]** • **[エラー（Error）]** • **警告** • **[Notice]** • **[Informational]** • **デバッグ（Debug）**
[Source] カラム	イベントをログに記録したソフトウェア モジュール。
[Description] カラム	イベントの説明。

システム イベント ログ

システム イベント ログの表示

[システムイベントログ（System Event Log）] タブには、シスコ システム イベント ログ（Cisco SEL）の内部に保存される総容量である 131068 エントリに対して、最新の 3008 システム イベントのみが表示されます。Cisco SEL の最大容量（131068 レコード）に達すると、最も古いエントリが最新のエントリで上書きされます。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Faults and Logs] をクリックします。

ステップ 3 [System Event Log] タブで、次の情報を確認します。

表 *25 : [Actions]* 領域

名前	説明
SEL フルネス インジケータ	[システムイベントログ（System Event Log）] タブの使用済み領域にパーセントで表示されます。この割合は3008エントリを基準として計算されます（[システムイベントログ（System Event Log）] タブには、常に最新の 3008 システム イベントのみが表示されます）。たとえば、[システムイベントログ（System Event Log）] タブに 1504 エントリがある場合、50 パーセントとして表示されます。 最初に3008エントリのセットに達した後は、SEL がクリアされるまで、状態は常に 100% として表示されます。
[Clear Log] ボタン	ログ ファイルからすべてのイベントをクリアします。 （注） このオプションは、ユーザ ID に **admin** または **user** ユーザ ロールが割り当てられている場合のみ使用できます。
[Chassis] ドロップダウン リスト	ログを表示する対象のシャーシまたはサーバを選択します。
[Total]	[System Event Log] テーブルの合計行数を表示します。
[Column] ドロップダウン リスト	表示する列を選択できます。

名前	説明
[Show] ドロップダウン リスト	フィルタを使用してイベントを表示する方法をカスタマイズします。これらの内容は次のとおりです。 • [Quick Filter]：デフォルト ビュー。 • [Advanced Filter]：1 つ以上の条件に基づいてイベントを表示するためのフィルタ オプション。マッチング ルールを使用して、[Filter] フィールドで指定したルールのすべてまたはいくつかのルールの組み合わせと一致するエントリを表示できます。 [Go] をクリックすると、設定したフィルタ基準と一致するエントリが表示されます。 設定したフィルタ基準は、[Save] アイコンをクリックして保存することができます。保存されたフィルタ基準は、ユーザ定義のフィルタとして後で使用できます。 （注） ユーザ定義のフィルタは [Manage Preset Filters] ダイアログボックスに表示されます。 • [All]：すべてのエントリが表示されます。 • [Manage Preset Filters]：ユーザ定義のフィルタが表示されます。このダイアログボックスで、ユーザ定義のフィルタを編集したり削除したりできます。 • [List of pre-defined filters）]：システム定義のフィルタが表示されます。 （注） [フィルタ（Filter）]アイコンを使用して、フィルタ フィールドの表示/非表示を切り替えることできます。

表 *26 : [System Event Log]* テーブル

名前	説明
[Time] カラム	イベントが発生した日時。
[Severity] カラム	シビラティ（重大度）フィールドには、テキストと色分けされたアイコンの両方が含まれます。アイコンについては、緑色は通常動作、黄色は情報を示し、警告、クリティカルおよび回復不能なエラーは赤色で表示されます。
[Description] カラム	イベントの説明。

ロギング制御

ロギング制御の表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Faults and Logs] をクリックします。

ステップ 3 [Logging Controls] タブで、次の情報を確認します。

リモート ロギング

名前	説明
[有効（Enabled）] チェックボックス	オンにすると、Cisco IMC は [IP Address] フィールドで指定された Syslog サーバーにログ メッセージを送信します。
セキュアリモートsyslogの有効化	オンにすると、Cisco IMC は、ロギング用の安全な接続をサポートするリモート Syslog サーバへの安全な暗号化されたアウトバウンド接続を確立します。 （注） このチェックボックスをオンにすると、デフォルトで **[プロトコル（Protocol）]** フィールドが無効になります。
[Host Name/IP Address] フィールド	Cisco IMC ログを保存する Syslog サーバのアドレス。リモート システムのアドレスとして IPv4 または IPv6 アドレスまたはドメイン名を設定できます。

名前	説明
[ポート（Port）]フィールド	1 ～ 65535 の範囲内の Syslog サーバの宛先ポート番号を入力します。デフォルト ポート番号は、514 です。
[Protocol] フィールド	syslog メッセージの送信用のトランスポート層プロトコル。次のいずれかを選択できます。 • TCP • UDP
[握手状態（Handshake Status）]	セキュアなリモート Syslog が有効になっている場合、Cisco IMC は SSL ハンドシェイクを実行して、証明書が指定された IP アドレス用であるかどうかを確認します。
[リポートするための最小シビラティ（重大度）（Minimum Severity to Report）] フィールド	リモート ログに含めるメッセージの最初レベルを指定します。次のいずれかを選択できます。 • **[緊急（Emergency）]** • **[アラート（Alert）]** • **[Critical]** • **[エラー（Error）]** • **警告** • **[Notice]** • **[Informational]** • **デバッグ（Debug）**

（注） Cisco IMC では、選択したシビラティ（重大度）よりも低いシビラティ（重大度）のメッセージは、リモートでログに記録されません。たとえば、[Error] を選択した場合、Cisco IMC リモート ログにはシビラティ（重大度）が [Emergency]、[Alert]、[Critical]、または [Error] のすべてのメッセージが含まれます。[Warning]、[Notice]、[Informational]、または [Debug] のメッセージは表示されません。

Local Logging

このエリアには、上記の表に示す [Minimum Severity to Report] ドロップダウン リストだけが表示されます。ローカル ログに含めるメッセージの最低レベルを指定できます。

リモート サーバへの Cisco IMC ログの送信

Cisco IMC ログ エントリを受信するように 1 台または 2 台のリモート syslog サーバーのプロファイルを設定できます。

始める前に

- リモート syslog サーバが、リモート ホストからログを受信するように設定されている必要があります。
- リモート syslog サーバが、認証関連のログを含め、すべてのタイプのログを受信するように設定されている必要があります。
- リモート syslog サーバのファイアウォールが、syslog メッセージが syslog サーバに到達するように設定されている必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Faults and Logs] をクリックします。

ステップ 3 [Remote Syslog Server] 領域のいずれかで、次のフィールドに値を入力します。

名前	説明
[有効（Enabled）] チェックボックス	オンにすると、Cisco IMC は [IP アドレス（IP Address）] フィールドに指定された Syslog サーバにログ メッセージを送信します。
[**Host Name/IP Address**] フィールド	Cisco IMC ログを保存する Syslog サーバのアドレス。リモート システムのアドレスとして IPv4 または IPv6 アドレスまたはドメイン名を設定できます。
[ポート（Port）]フィールド	1 ～ 65535 の範囲内の Syslog サーバの宛先ポート番号を入力します。デフォルト ポート番号は、514 です。

ステップ 4 （任意） **[Minimum Severity to Report]**ドロップダウン リストで、リモート ログに含まれるメッセージの最低レベルを指定します。

次のいずれかを選択できます。シビラティ（重大度）の高いものから順に並んでいます。

- **[緊急（Emergency）]**
- **[アラート（Alert）]**
- **[Critical]**
- **[エラー（Error）]**
- 警告
- **[Notice]**
- **[Informational]**
- デバッグ（**Debug**）

（注） Cisco IMC では、選択したシビラティ（重大度）よりも低いシビラティ（重大度）のメッセージは、リモートでログに記録されません。たとえば、[**Error**] を選択した場合、Cisco IMC リモート ログにはシビラティ（重大度）が Emergency、Alert、Critical、または Error のすべてのメッセージが含まれます。Warning、Notice、Informational、または Debug のメッセージは表示されません。

ステップ 5 **[Save Changes]**をクリックします。

Cisco IMC ログしきい値の設定

始める前に

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Faults and Logs] をクリックします。

ステップ 3 必須: [**Local Logging**] 領域で、[**Minimum Severity to Report**] ドロップダウン リストを使用して、Cisco IMC ログに含まれるメッセージの最低レベルを指定します。

次のいずれかを選択できます。シビラティ（重大度）の高いものから順に並んでいます。

- **[緊急（Emergency）]**
- **[アラート（Alert）]**
- **[Critical]**
- **[エラー（Error）]**
- 警告
- **[Notice]**
- **[Informational]**
- デバッグ（**Debug**）

（注） Cisco IMC では、選択したシビラティ（重大度）よりも低いシビラティ（重大度）のメッセージはログに記録されません。たとえば、[**Error**] を選択した場合、Cisco IMC ログにはシビラティ（重大度）が Emergency、Alert、Critical、または Error のすべてのメッセージが含まれます。Warning、Notice、Informational、または Debug のメッセージは表示されません。

リモート サーバーへのテスト Cisco IMC ログの送信

始める前に

- リモート syslog サーバが、リモート ホストからログを受信するように設定されている必要があります。
- リモート syslog サーバが、認証関連のログを含め、すべてのタイプのログを受信するように設定されている必要があります。
- リモート syslog サーバのファイアウォールが、syslog メッセージが syslog サーバに到達するように設定されている必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Faults and Logs] をクリックします。

ステップ 3 [Faults and Logs] ペインの [Logging Controls] タブをクリックします。

ステップ 4 [**Action**] 領域の [**Send Test Syslog**] をクリックします。

設定されているリモート サーバーにテスト Cisco IMC ログが送信されます。

リモート Syslog 証明書の管理

リリース 4.2 (2a) 以降、リモート Syslog 証明書を Cisco UCS C シリーズ サーバーにアップロードできます。証明書を 1 つまたは 2 つの Cisco UCS C シリーズ サーバーにアップロードできます。

リモート Syslog 証明書のアップロード

リモート サーバーの場所またはローカルの場所からリモート Syslog 証明書をアップロードできます。

始める前に

- admin 権限を持つユーザとしてログインする必要があります。
- アップロードする証明書ファイルは、ローカルにアクセスできるファイル システムに配置されている必要があります。
- 次の証明書形式がサポートされています。
  - .crt
  - .cer

- .pem

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 **[シャーシ（Chassis）]** メニューで、**[障害とログ（Faults and Logs）]** を選択します。

ステップ 3 **[障害とログ（Faults and Logs）]**ペインの **[ロギング制御（Logging Controls）]**を選択します。

ステップ 4 リモート Syslog 証明書をアップロードするには、**[リモート Syslog 証明書のアップロード（Upload Remote Syslog Certificate）]** ボタンをクリックします。

[リモート Syslog 証明書のアップロード（Upload Remote Syslog Certificate）] ダイアログボックスが表示されます。

ステップ 5 **[サーバーの選択:（Select Server:）]** ドロップダウン リストから、リモート Syslog 証明書をアップロードするサーバーを選択します。

ステップ 6 次のいずれかの方法を使用して、証明書をアップロードできます。

- リモートロケーションからアップロード
- ブラウザクライアント経由のアップロード
- **[リモート Syslog 証明書の貼り付け（Paste Remote Syslog Certificate）]** テキスト ボックスに証明書の内容を直接貼り付けます。
- **[リモートの場所からアップロード (Upload from remote location)]**: リモートの場所からリモート syslog 証明書をアップロードするには、このオプションボタンを選択します。

名前	説明
[リモートの場所からアップロード (Upload from remote location)] フィールド	次のいずれかのプロトコルを選択します。 • TFTP • FTP • SCP • SFTP • HTTP （注） FTP、SCP または SFTP を選択した場合は、ユーザ名とパスワードの入力が求められます。
[サーバ IP/ホスト名 (Server IP/Hostname)] ボタン	リモート サーバのホスト名または IP アドレスを入力します。
パスおよびファイル名	リモート syslog 証明書をアップロードするリモート サーバ上のファイルパスとファイル名を入力します。

名前	説明
Username	リモート サーバのユーザ名を入力します。
Password	リモート サーバのパスワードです。

- **[ブラウザ クライアントでアップロード (Upload by Browser client)]**: ブラウザ クライアントを使用してリモート syslog 証明書をアップロードするには、このオプション ボタンを選択します。

  [参照 (Browse)] をクリックして、リモート syslog 証明書をアップロードする場所に移動します。

- **[リモート Syslog 証明書の内容をペースト (Paste リモート Syslog Certificate Content)]**]: このオプション ボタンを選択すると、外部証明書の詳細がテキスト ボックスに直接貼り付けられます。

リモート Syslog 証明書の削除

サーバーからリモート Syslog 証明書を削除できます。

始める前に

admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 **[シャーシ（Chassis）]** メニューで、**[障害とログ（Faults and Logs）]** を選択します。

ステップ 3 **[障害とログ（Faults and Logs）]**ペインの **[ロギング制御（Logging Controls）]**を選択します。

ステップ 4 リモート Syslog 証明書を削除するには、**[リモート Syslog 証明書の削除（Delete Remote Syslog Certificate）]** ボタンをクリックします。

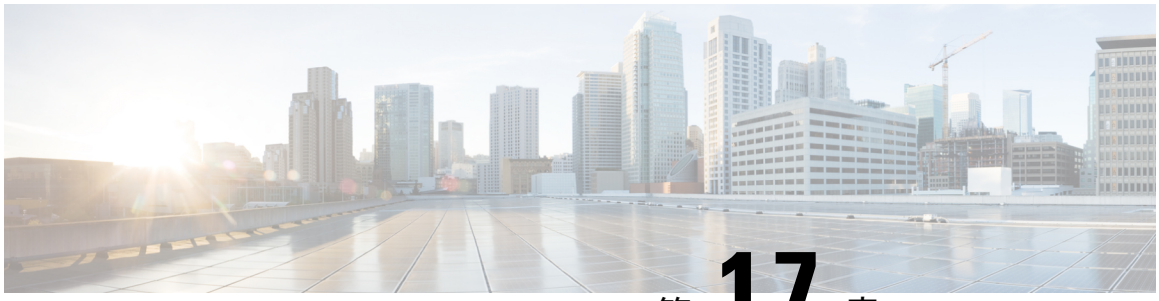
[リモート Syslog 証明書の削除（Delete Remote Syslog Certificate）] ダイアログボックスが表示されます。

ステップ 5 リモート Syslog 証明書を削除するサーバーのそれぞれのチェック ボックスを選択します。

ステップ 6 [削除（Delete）] をクリックします。

ポップアップ ウィンドウに削除の確認メッセージが表示されます。

ステップ 7 [OK] をクリックします。



第 17 章

サーバー ユーティリティ

この章は、次の内容で構成されています。

テクニカル サポート データのエクスポート

テクニカル サポート データのエクスポート

このタスクは、Cisco Technical Assistance Center（TAC）から要求された場合に実行します。このユーティリティは、TACが技術上の問題をトラブルシューティングおよび解決する際に役立つ設定情報、ログ、および診断データが含まれる要約レポートを作成します。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [ユーティリティ（Utilities）] ペインの [アクション（Actions）] 領域で、[テクニカルサポートデータのエクスポート（Export Technical Support Data）] をクリックします。

ステップ 4 **[Export Technical Support Data]**ダイアログボックスで、次のフィールドに入力します。

名前	説明
[テクニカル サポート データのエクスポート先（Export Technical Support Data to）] ドロップダウン リスト	リモート サーバのタイプ。次のいずれかになります。 • **[TFTP サーバー（TFTP Server）]** • **FTP サーバー（FTP Server）** • **SFTP サーバー（SFTP Server）** • **SCP サーバー（SCP Server）** • **HTTP サーバー（HTTP Server）** （注） このアクションを実行中にリモート サーバのタイプとして SCP または SFTP を選択した場合、ポップアップ ウィンドウが表示され、そこに *[サーバ（RSA）鍵フィンガープリントは <server_finger_print _ID> です。続行しますか?（Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?）]* というメッセージが表示されます。サーバ フィンガープリントの信頼度に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。

名前	説明
[テクニカル サポート データのエクスポート元（Export Technical Support Data through）] ドロップダウン リスト	（注） [前面パネル USB（Front Panel USB）] オプションは、[スマート アクセス USB（Smart Access USB）] が有効で、USB ストレージ デバイスがサーバに接続されている場合にのみ表示されます。 テクニカル サポート データは、リモート サーバまたはサーバに接続された USB ストレージ デバイスにエクスポートできます。次のいずれかを選択できます。 • [リモート（Remote）]：次のいずれかのプロトコルを使用して、リモート サーバにテクニカル サポート データをエクスポートできます。 • **TFTP** • **FTP** • **SFTP** • **SCP** • **[HTTP]** （注） このアクションを実行しながら、リモート サーバー タイプとして SCP または SFTP を選択した場合、「*Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼度に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。 • [Front Panel USB]：これにより、テクニカル サポート データをサーバーに接続された USB ストレージ デバイスにエクスポートできます。
[サーバ IP/ホスト名（Server IP/Hostname）] フィールド	サポート データ ファイルの保存先とするサーバの IP アドレスまたはホスト名。[テクニカル サポート データのエクスポート先（Export Technical Support Data to）] ドロップダウン リストの設定に応じて、フィールドの名前は異なります。

名前	説明
[Path and Filename] フィールド	ファイルをリモート サーバーにエクスポートするときに、Cisco IMC が使用する必要のあるパスおよびファイル名。 （注） サーバーにサポート対象ネットワーク アダプタ カードのいずれかがある場合、データ ファイルにはアダプタ カードからのテクニカル サポート データも含まれています。
ユーザ名	システムがリモート サーバへのログインに使用する必要のあるユーザ名。プロトコルが TFTP または HTTP の場合、このフィールドは適用されません。
パスワード	リモート サーバのユーザ名のパスワード。プロトコルが TFTP または HTTP の場合、このフィールドは適用されません。

ステップ 5 [エクスポート（Export）] をクリックします。

次のタスク

生成されたレポート ファイルを Cisco TAC に提供します。

ローカル ファイルへのテクニカル サポート データのダウンロード

このタスクは、Cisco Technical Assistance Center（TAC）から要求された場合に実行します。このユーティリティは、TAC が技術上の問題をトラブルシューティングおよび解決する際に役立つ設定情報、ログ、および診断データが含まれる要約レポートを作成します。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [Utilities] ペインの [Actions] 領域で、[Generate Technical Support Data for Local Download] をクリックします。

ステップ 4 **[Download Technical Support Data to Local File]** ダイアログボックスで、次のフィールドに入力します。

名前	説明
[Generate Technical Support Data] オプション ボタン	Cisco IMCダウンロードするテクニカル サポート データ ファイルがない場合、このオプション ボタンは無効にされます。 [Generate] をクリックして、データ ファイルを作成します。データ収集が完了したら、[Actions] 領域の [Download Technical Support Data to Local File] をクリックして、ファイルをダウンロードします。
[Regenerate Technical Support Data] オプション ボタン	Cisco IMCこのオプション ボタンは、ダウンロードするテクニカル サポート データ ファイルがある場合に表示されます。 既存のサポート データ ファイルを新しいものと置き換えるには、このオプションを選択し、[Regenerate] をクリックします。データ収集が完了したら、[Actions] 領域の [Download Technical Support Data to Local File] をクリックして、ファイルをダウンロードします。
[Download to local file] オプション ボタン	Cisco IMCこのオプション ボタンは、ダウンロードするテクニカル サポート データ ファイルがある場合に有効になります。 既存のファイルをダウンロードするには、このオプションを選択し、[Download] をクリックします。 （注） サポートされているネットワーク アダプタ カードがサーバに組み込まれている場合、そのアダプタ カードからの技術サポート データもデータ ファイルに取り込まれます。
[生成（Generate）] ボタン	テクニカル サポート データ ファイルを生成できます。
[Download] ボタン	生成されたテクニカル サポート データ ファイルをダウンロードできます。

ステップ 5 **[Generate]** をクリックして、データ ファイルを作成します。データ収集が完了したら、**[アクション（Actions）]** 領域の **[テクニカル サポート データのローカル ファイルへのダウンロード（Download Technical Support Data to Local File）]**をクリックして、ファイルをダウンロードします。

次のタスク

生成されたレポート ファイルを Cisco TAC に提供します。

出荷時の初期状態へのリセット

現在実行されているファームウェアで問題が発生した場合やサーバーのトラブルシューティング時など、稀なケースで、サーバーコンポーネントの出荷時デフォルトへのリセットが必要になることがあります。これを行うと、ユーザーが設定可能なすべての設定がリセットされます。

この手順は、通常のサーバー メンテナンスには含まれません。サーバー コンポーネントをリセットした後は、ログオフしてから再びログインする必要があります。また、接続が失われ、ネットワーク設定を再び指定する必要がある場合もあります。この移行中、一部のインベントリ情報が使用できない場合があります。

BMC を工場出荷時の設定にリセットすると、シリアル番号が Cisco IMCXXXXXX 形式で表示されます。XXXXXX はサーバーのシリアル番号です。

重要 **VIC アダプタを他の世代の C シリーズ サーバー（たとえば M4）から M5 世代の C シリーズ サーバーまたは M5 サーバーから他の世代のサーバーに移動する際は、アダプタを出荷時のデフォルトにリセットする必要があります。**

始める前に

サーバー コンポーネントを出荷時デフォルトにリセットするには、admin 権限を持つユーザーとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [Utilities] ペインの [Actions] 領域で、[Reset to Factory Default] をクリックします。

ステップ 4 [工場出荷時のデフォルトへのリセット（Reset to Factory Default）] ダイアログボックスで、次の情報を確認します。

Actions	説明
[次の設定を工場出荷時のデフォルトにリセット（Reset to factory Default Setting of）] ドロップダウン リスト	工場出荷時の設定にリセットするシャーシまたはBMC を選択できます。次のいずれかになります。 • **シャーシ** • **BMC1** • **BMC2**

名前	説明
[すべて（All）] チェックボックス	オンにすると、サーバのすべてのコンポーネントを工場出荷時の設定にリセットします。 展開することで、工場出荷時の設定にリセットする特定のコンポーネントを選択できます。
[BMC] チェックボックス	オンにすると、BMCを工場出荷時の設定にリセットします。 （注） BMC を工場出荷時の設定にリセットすると、シリアル番号がCisco IMCXXXXXX形式で表示されます。XXXXXXはサーバーのシリアル番号です。BMC NIC モードの工場出荷時のデフォルトの後に**共有LOMの拡張**がデフォルトで設定されます。
[Storage] チェックボックス	オンにすると、使用可能なすべてのストレージ アダプタが工場出荷時の設定にリセットされます。ストレージ アダプタをリセットすると、ディスク上のデータは変更されませんが、仮想ドライブのメタ データは消去され、データ損失が発生することがあります。展開して工場出荷時の設定にリセットする特定のストレージ アダプタを選択します。 （注） 工場出荷時のデフォルトにストレージアダプタをリセットするには、ホストの電源をオンにする必要があります。
[VIC] チェックボックス	オンにすると、使用可能なすべての VIC を工場出荷時の設定にリセットします。 展開することで、工場出荷時の設定にリセットする特定のVICを選択できます。 （注） 工場出荷時のデフォルトにVICをリセットするには、ホストの電源をオンにする必要があります。
[Reset] ボタン	選択したコンポーネントを工場出荷時の設定にリセットします。

ステップ 5 [Reset] をクリックして、選択したコンポーネントを工場出荷時の設定にリセットします。

ホストがBIOS POST（電源投入時自己診断テスト）を実行しているとき、またはEFIシェル内にあるときにCisco IMC を再起動すると、ホストの電源が短時間オフになります。準備ができると、Cisco IMC の電源はオンになります。再起動時に、ネットワーク設定モードは **[Cisco カード (Cisco Card)]**モードにデフォルトで設定されます。

Cisco IMC 設定のエクスポートとインポート

Cisco IMC 設定のエクスポートとインポート

Cisco IMC 設定のバックアップを実行するには、システム設定のスナップショットを作成し、生成された Cisco IMC 設定ファイルをネットワーク上の場所にエクスポートします。エクスポート操作で保存されるのは、管理プレーンからの情報だけです。サーバ上のデータはバックアップされません。ユーザアカウントやサーバ証明書など、機密情報の設定はエクスポートされません。

エクスポートされた Cisco IMC 設定ファイルは、同じシステムで復元したり、別の Cisco IMC システムにインポートしたりできます。ただし、インポートするシステムのソフトウェアのバージョンとエクスポートするシステムのソフトウェアのバージョンが同じであるか、両者の設定に互換性があることが前提となります。設定ファイルを設定テンプレートとして他のシステムにインポートする場合は、IP アドレスやホスト名などシステム固有の設定を変更する必要があります。インポート操作によって情報が変更されるのは、管理プレーンだけです。

Cisco IMC 設定ファイルは XML テキスト ファイルで、その構造と要素は Cisco IMC コマンドモードに対応しています。

エクスポートまたはインポート操作を実行する場合は、次のガイドラインを考慮してください。

- エクスポートまたはインポートは、システムがアップ状態で、稼働しているときに実行できます。エクスポート操作によるサーバまたはネットワーク トラフィックへの影響はありませんが、インポート操作によって IP アドレスなどが変更されると、トラフィックが中断されたりサーバがリブートされたりすることがあります。
- エクスポートとインポートを同時に実行することはできません。

次の機能でインポートまたはエクスポート操作を実行できます。

- Cisco IMC バージョン

（注） この情報のみをエクスポートできます。

- ネットワーク設定
- テクニカル サポート
- ローカル ログおよびリモート ログのロギング制御
- 電力ポリシー
- BIOS - BIOS パラメータ

（注） 高精度ブートはサポートされません。

- 通信サービス
- リモート プレゼンス
- ユーザ管理 - LDAP
- イベント管理
- SNMP

Cisco IMC 設定のエクスポート

（注） セキュリティ上の理由から、この操作でユーザーアカウントやサーバー証明書をエクスポートしないでください。

始める前に

バックアップ リモート サーバの IP アドレスを取得します。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [Utilities] ペインの [Actions] 領域で、[Export Configuration] をクリックします。

ステップ 4 **[設定のエクスポート（Export Configuration）]** ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[エクスポートするコンポーネントの選択（Select Component for Export）] ドロップダウンリスト	コンポーネントのタイプ。次のいずれかになります。 • **[BMC]** • **VIC アダプタ** 選択したコンポーネントに応じて、そのコンポーネントの設定がエクスポートされます。

名前	説明
[エクスポート先（Export to）] ドロップダウン リスト	XML 設定ファイルを保存する場所。次のいずれかになります。 • [ローカル（Local）]：Cisco IMC GUI を実行しているコンピュータのローカル ドライブに XML 設定ファイルを保存するには、このオプションを選択して [エクスポート（Export）] をクリックします。 このオプションを選択すると、Cisco IMC GUI に [ファイルのダウンロード（File Download）] ダイアログボックスが表示され、設定ファイルを保存する場所に移動できます。 • [Remote Server]：XML 設定ファイルをリモート サーバーからインポートするには、このオプションを選択します。 このオプションを選択すると、Cisco IMC GUI にリモート サーバーのフィールドが表示されます。 • [Front Panel USB]：サーバーに接続された USB ストレージ デバイスに設定ファイルをエクスポートするには、このオプションを選択します。 （注） • Cisco IMC の設定をエクスポートするための [前面パネル USB（Front Panel USB）] オプションは、スマート アクセス USB が有効で、USB ストレージデバイスがサーバに接続されている場合にのみ使用できます。 • このオプションは、[コンポーネントの選択（Select Component）] ドロップダウン リストで [BMC] を選択した場合にのみ使用できます。

名前	説明
[エクスポート先（Export to）] ドロップダウン リスト	リモート サーバーのタイプ。次のいずれかになります。 • **[TFTP サーバー（TFTP Server）]** • **FTP サーバー（FTP Server）** • **SFTP サーバー（SFTP Server）** • **SCP サーバー（SCP Server）** • **HTTP サーバー（HTTP Server）** （注） このアクションを実行中にリモート サーバのタイプとして SCP または SFTP を選択した場合、ポップアップ ウィンドウが表示され、そこに *[サーバ（RSA）鍵フィンガープリントは <server_finger_print _ID> です。続行しますか?（Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?）]* というメッセージが表示されます。サーバ フィンガープリントの信頼度に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。
[サーバーIP/ホスト名（Server IP/Hostname）] フィールド	設定ファイルのエクスポート先となるサーバーの IPv4 または IPv6 アドレス、またはホスト名。[エクスポート先（Export to）] ドロップダウン リストで選択したリモート サーバのタイプに応じて、フィールドの名前は異なる場合があります。
[Path and Filename] フィールド	ファイルをリモート サーバーにエクスポートするときに、Cisco IMC が使用する必要のあるパスおよびファイル名。
ユーザ名	システムがリモート サーバへのログインに使用する必要のあるユーザ名。プロトコルが TFTP または HTTP の場合、このフィールドは適用されません。
パスワード	リモート サーバのユーザ名のパスワード。プロトコルが TFTP または HTTP の場合、このフィールドは適用されません。
[Passphrase]	エクスポートした設定ファイル内の LDAP および SNMP v3 ユーザ パスワードを、AES256 アルゴリズムを使用して暗号するためのパスフレーズ。6 ～ 127 文字の文字列を入力します。次の文字は入力しないでください：! # $ & < > ? ; ' | ` ~ \ % ^ ( ) "

ステップ 5 [エクスポート（Export）] をクリックします。

Cisco IMC 設定のインポート

始める前に

コンフィギュレーション ファイルのインポート時に SNMP 設定情報を復元する場合は、インポートを行う前にこのサーバで SNMP がディセーブルになっていることを確認します。インポートを実行するときに SNMP がイネーブルになっている場合、Cisco IMC では設定ファイルに保存されている値によって現在の値は上書きされません。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [Utilities] ペインの [Actions] 領域で、[Import Configuration] をクリックします。

ステップ 4 **[設定のインポート（Import Configuration）]** ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[インポートするコンポーネントの選択（Select Component for Import）] ドロップダウン リスト	コンポーネントのタイプ。次のいずれかになります。 • **[BMC]** • **VIC アダプタ** 選択したコンポーネントに応じて、そのコンポーネントの設定がインポートされます。

名前	説明
[インポート元（Import From）] ドロップダウン リスト	XML 設定ファイルの場所。次のいずれかになります。 • [ローカル（Local）]：Cisco IMC GUI を実行しているコンピュータのローカル ドライブに XML 設定ファイルをインポートするには、このオプションを選択します。 このオプションを選択すると、Cisco IMC GUI に [参照（Browse）] ボタンが表示され、インポートするファイルに移動できます。 • [Remote Server]：XML 設定ファイルをリモート サーバーからインポートするには、このオプションを選択します。 このオプションを選択すると、Cisco IMC GUI にリモート サーバーのフィールドが表示されます。 • [Front Panel USB]：サーバーに接続された USB ストレージ デバイスから設定ファイルをインポートするには、このオプションを選択します。 （注） • Cisco IMC の設定をインポートするための [前面パネル USB（Front Panel USB）] オプションは、スマート アクセス USB が有効で、USB ストレージデバイスがサーバに接続されている場合にのみ使用できます。 • このオプションは、[コンポーネントの選択（Select Component）] ドロップダウン リストで [BMC] を選択した場合にのみ使用できます。

名前	説明
[インポート元（Import From）] ドロップダウン リスト	（注） これらのオプションは、[リモート（Remote）] を選択した場合にのみ使用できます。 リモート サーバーのタイプ。次のいずれかになります。 • **[TFTP サーバー（TFTP Server）]** • **FTP サーバー（FTP Server）** • **SFTP サーバー（SFTP Server）** • **SCP サーバー（SCP Server）** • **HTTP サーバー（HTTP Server）** （注） このアクションを実行中にリモートサーバのタイプとして SCP または SFTP を選択した場合、ポップアップ ウィンドウが表示され、そこに *[サーバ（RSA）鍵フィンガープリントは <server_finger_print _ID> です。続行しますか?（Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?）]* というメッセージが表示されます。サーバフィンガープリントの信頼度に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。
[サーバーIP/ホスト名（Server IP/Hostname）] フィールド	設定ファイルを保存するサーバーの IPv4 または IPv6 アドレス、またはホスト名。[インポート元（Import From）] ドロップダウン リストで選択したリモート サーバのタイプに応じて、フィールドの名前は異なる場合があります。
[Path and Filename] フィールド	リモート サーバ上の構成ファイルのパスとファイル名。
ユーザ名	システムがリモート サーバへのログインに使用する必要のあるユーザ名。プロトコルが TFTP または HTTP の場合、このフィールドは適用されません。
パスワード	リモートサーバのユーザ名のパスワード。プロトコルが TFTP または HTTP の場合、このフィールドは適用されません。

名前	説明
[Passphrase]	インポートした設定ファイル内の LDAP および SNMP v3 ユーザ パスワードを AES256 アルゴリズムを使用して暗号化するためのパスフレーズ。6 ～ 127 文字の文字列を入力します。次の文字は入力しないでください：! # $ & < > ? ; ' | ` ~ \ % ^ ( ) " （注） 設定ファイルの暗号化されたセクションを編集しそれをインポートしようとすると、編集内容は無視され、インポート操作画面には部分的な成功メッセージが表示されます。

ステップ 5 [Import] をクリックします。

ホストへのマスク不可能な割り込みの生成

状況によっては、サーバがハングして、従来のデバッグ メカニズムに応答しない場合があります。ホストへのマスク不能割り込み（NMI）を生成することにより、サーバのクラッシュ ダンプ ファイルを作成および送信して、サーバのデバッグに使用することができます。

サーバーに関連付けられたオペレーティング システムの種類によっては、このタスクで OS が再起動される場合があります。

始める前に

- admin 権限を持つユーザとしてログインする必要があります。
- サーバの電源が投入されている。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [Utilities] ペインの [Actions] 領域で、[Generate NMI to Host] をクリックします。

ステップ 4 **[ホストへの NMI の生成（Generate NMI to Host）]** ダイアログボックスで、次の情報を確認します。

Actions	説明
[Generate NMI to] ドロップダウン リスト	マスク不能割り込み（NMI）を生成するサーバーを選択できます。次のいずれかになります。 • **[サーバー 1（Server 1）]** • **[サーバー 2（Server 2）]**

ステップ 5 **[送信]**をクリックします。

このアクションは、OS を再起動する可能性のあるホストに NMI 信号を送信します。

Cisco IMC バナーの追加または更新

著作権やカスタマイズしたメッセージなどの重要な情報を入力して、Cisco IMC バナーを追加または更新できます。次の手順を実行します。

始める前に

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [Utilities] ペインの [Actions] 領域で、[Add/Update Cisco IMC Banner] をクリックします。

ステップ 4 **[Cisco IMC バナーの追加/更新（Add/Update Cisco IMC Banner）]**ダイアログボックスで、次のフィールドに入力します。

名前	説明
[Banner (80 Chars per line. Max 2K Chars.)] フィールド	Web UI またはコマンドライン インターフェイスにログインする前に、ログイン画面に表示する著作権情報またはメッセージを入力します。
[SSH の再起動（Restart SSH）] チェックボックス	オンにすると、[Save Banner] ボタンをクリックした後にアクティブな SSH セッションが終了します。

ステップ 5 **[バナーの保存（Save Banner）]**をクリックします。

次のタスク

Cisco IMC の最後のリセット理由の表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。
ステップ 2 [管理（Admin）] メニューで [ユーティリティ（Utilities）] をクリックします。
ステップ 3 [Utilities] ペインの [Actions] 領域で、[Last Reset Reason] 領域の下にある次の情報を確認します。

名前	説明
[コンポーネント（Component）] フィールド	最後にリセットされたコンポーネント。
[Status] フィールド	コンポーネントが前回リセットされた理由。次のいずれかになります。 • **watchdog-reset** — カーネル パニックまたはハング タスクが原因でウォッチドッグ タイマーが期限切れになりました。 • [ac-cycle]：PSU 電源ケーブルが取り外されています（電源入力なし）。 • [graceful-reboot]：Cisco IMC のリブートが実行されます。 • **OOM-reset** — メモリがフル キャパシティに達すると（ウォッチドッグ タイマーなしで）Cisco IMC がリブートします。

ローカル ファイルへのハードウェア インベントリのダウンロード

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。
ステップ 2 [管理（Admin）] メニューで [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [Utilities] ペインの [Actions] 領域で、[Generate Inventory Data] をクリックします。

ステップ 4 **[インベントリ データの生成（Generate Inventory Data）]**ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Generate Inventory Data] オプション ボタン	Cisco IMCこのオプション ボタンは、ダウンロードするハードウェア インベントリ データ ファイルがない場合に表示されます。
[Download to local file] オプション ボタン	Cisco IMCこのオプション ボタンは、ダウンロードするインベントリ データ ファイルがある場合に有効になります。 既存のファイルをダウンロードするには、このオプションを選択し、[Download] をクリックします。

ステップ 5 [Generate] をクリックして、データ ファイルを作成します。データ収集が完了したら、[Download Inventory Data to Local File] オプション ボタンを選択して [Download] をクリックし、ファイルをローカルにダウンロードします。

リモート サーバへのハードウェア インベントリ データのエクスポート

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [Utilities] ペインの [Actions] 領域で、[Export Hardware Inventory Data to Remote] をクリックします。

ステップ 4 **[ハードウェア インベントリ データのエクスポート（Export Hardware Inventory Data）]**ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[ハードウェア インベントリ データのエクスポート先（Export Hardware Inventory Data to）] ドロップダウン リスト	リモート サーバのタイプ。次のいずれかになります。 • **[TFTP サーバー（TFTP Server）]** • **FTP サーバー（FTP Server）** • **SFTP サーバー（SFTP Server）** • **SCP サーバー（SCP Server）** • **HTTP サーバー（HTTP Server）** （注） このアクションを実行中にリモート サーバのタイプとして SCP または SFTP を選択した場合、ポップアップ ウィンドウが表示され、そこに *[サーバ（RSA）鍵フィンガープリントは <server_finger_print _ID> です。続行しますか?（Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?）]* というメッセージが表示されます。サーバ フィンガープリントの信頼度に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。
[サーバーIP/ホスト名（Server IP/Hostname）] フィールド	データ ファイルを保存する必要のあるサーバーの IP アドレスまたはホスト名。[ハードウェア インベントリ データのエクスポート先（Export Hardware Inventory Data to）] ドロップダウン リストの設定に応じて、フィールドの名前は異なります。
[Path and Filename] フィールド	ファイルをリモート サーバーにエクスポートするときに、Cisco IMC が使用する必要のあるパスおよびファイル名。
ユーザ名	システムがリモート サーバへのログインに使用する必要のあるユーザ名。プロトコルが TFTP または HTTP の場合、このフィールドは適用されません。
パスワード	リモート サーバのユーザ名のパスワード。プロトコルが TFTP または HTTP の場合、このフィールドは適用されません。

ステップ 5 [エクスポート（Export）] をクリックします。

PID カタログのアップロード

始める前に

PID カタログをアップロードするには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 **[Navigation]**ペインの **[Admin]**タブをクリックします。

ステップ 2 **[Admin]**タブの**[Utilities]** をクリックします。

ステップ 3 作業ペインで**[PID カタログのアップロード（Upload PID Catalog）]**リンクをクリックします。

[PID カタログのアップロード（Upload PID Catalog）] ダイアログボックスが表示されます。

カタログ ファイルの場所に応じて、いずれかのオプションを選択します。

ステップ 4 **[カタログのアップロード元：ローカル ファイル（Upload PID Catalog from Local File）]** ダイアログボックスで**[参照（Browse）]**をクリックし、**[アップロードするファイルの選択（Choose File to Upload）]**ダイアログボックスでアップロードするカタログ ファイルを選択します。

名前	説明
[File] フィールド	アップロードする PID カタログ ファイル。
[Browse] ボタン	ダイアログボックスが表示され、そこで、該当するファイルにナビゲートすることができます。

ステップ 5 **[カタログのアップロード元：リモート サーバ（Upload PID Catalog from Remote Server）]**ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[PID カタログのアップロード元：リモート サーバ（Upload PID Catalog from Remote Server）]ドロップダウン リスト	リモート サーバーのタイプ。次のいずれかになります。 • **TFTP** • **FTP** • **SFTP** • **SCP** • **[HTTP]**

名前	説明
[サーバーIP/ホスト名（Server IP/Hostname）] フィールド	PID カタログ情報を有効にするサーバーの IP アドレスまたはホスト名。[Upload PID Catalog from Remote Server] ドロップダウン リストの設定によって、フィールド名は異なる場合があります。
[パスおよびファイル名（Path and Filename）] フィールド	リモート サーバー上のカタログ ファイルのパスおよびファイル名。
[ユーザ名（Username）] フィールド	リモート サーバのユーザ名。
[パスワード（Password）]フィールド	リモート サーバのパスワード。
[アップロード（Upload）] ボタン	選択したPIDカタログをアップロードします。 （注） このアクションを実行中にリモート サーバのタイプとして SCP または SFTP を選択した場合、ポップアップ ウィンドウが表示され、そこに *[サーバ（RSA）鍵フィンガープリントは <server_finger_print _ID> です。続行しますか?（Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?）]* というメッセージが表示されます。サーバフィンガープリントの信頼度に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーをベースにしており、接続先ホストの特定や確認に利用できます。
[Cancel]ボタン	サーバに保管されているファームウェア バージョンには変更を加えることなく、ウィザードを閉じます。

PID カタログの有効化

⚠

注意 PID カタログがアクティブになると、BMC が自動的に再起動します。

PID カタログをアクティブ化した後、サーバを再起動する必要があります。

始める前に

PIDカタログを有効にするには、admin権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 **[Admin]** タブの**[Utilities]** をクリックします。

ステップ 3 **作業**ペインで **[PID カタログの有効化（Activate PID Catalog）]** タブをクリックします。

[PID カタログの有効化（Activate PID Catalog）] ダイアログボックスが表示されます。次のフィールドに入力します。

名前	説明
[アクティブ化（Activate）] ボタン	PID カタログをアクティベートできます。

（注） 初めてシステムにログオンする場合は、**[PID カタログの有効化（Activate PID Catalog）]**リンクが灰色で表示されます。PID カタログをサーバにアップロードすると、このリンクが有効になります。PIDファイルをアップロードした後もリンクは引き続きアクティブであり、PID を複数回アクティブにできます。

PID カタログを削除

⚠

注意 PID カタログが削除されると、BMC が自動的に再起動します。

PID カタログを削除した後、サーバを再起動する必要があります。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 **[管理 (Admin)]** タブの **[ユーティリティ (Utilities)]** をクリックします。

ステップ 3 [ユーティリティ (Utilities)] ペインの **[アクション (Actions)]** 領域で、**[PID カタログの削除 (Delete PID Catalog)]**] をクリックし、**[OK]** をクリックして確定します。

（注） PID カタログは、以前に更新およびアクティブ化されている場合にのみ削除できます。

スマート アクセス USB の有効化

スマート アクセス USB 機能を有効にすると、フロント パネルの USB デバイスはホスト オペレーティング システムから切断され、Cisco IMC に接続します。スマート アクセス USB 機能を有効にした後は、フロント パネルの USB デバイスを使用して、テクニカル サポート データをエクスポート、Cisco IMC 構成をインポートまたはエクスポート、あるいは Cisco IMC、BIOS および VIC のファームウェアを更新できます。

スマート アクセス USB でサポートされるファイル システムは次のとおりです。

- EXT2
- EXT3
- EXT4
- FAT 32
- FAT 16
- DoS

（注） 巨大ファイル サポートは BMC ではサポートされません。EXT4 ファイルシステムの場合、巨大ファイルのサポートをオフにする必要があります。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [アクション（Actions）] 領域で [スマートアクセスUSBの有効化（Enable Smart Access USB）] をクリックします。

これはトグル ボタンです。スマート アクセスを無効にするには、[スマートアクセスUSBの無効化（Disable Smart Access USB）] をクリックします。スマート アクセス USB を有効にした後にのみ、このボタンが表示されます。スマート アクセス USB 機能を無効にすると、フロント パネルの USB デバイスは Cisco IMC から切断してホスト オペレーティング システムに接続します。

Cisco Intersight 管理の有効化/無効化

Intersight 管理を有効にすると、Intersight クラウド アプリケーションと M5 サーバー間の双方向通信が確立されます。

（注） ポート番号 8888-8889 は、Intersight 通信を行うために予約されています。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [デバイスコネクタ（Device Connector）] をクリックします。

ステップ 3 **[Intersight Management]** 領域で **[On]** をクリックして Intersight 管理を有効にします。
[Connection] 領域に Intersight 管理の接続状態が表示されます。デバイス コネクタの Intersight 管理への接続が確立できていない場合は、[詳細と推奨事項（Details & Recommendations）] ドロップダウン リストに表示される推奨事項を確認し、接続の問題を修正します。

ステップ 4 [アクセス モード（Access Mode）] で [読み取り専用（Read-only）] または [制御を許可（Allow Control）] を選択します。
[読み取り専用（Read-only）] アクセス モードを選択すると、Intersight を使用してデバイスを構成できなくなります。したがって、クラウドからデバイス コネクタに送信される構成は、エラー コードを伴って拒否されます。[制御を許可（Allow Control）] モードを選択すると、Intersight を使用してデバイスの構成を完全に制御できます。

ステップ 5 Intersight 管理を無効にするには、[オフ（Off）] をクリックします。
Intersight 管理を無効にすると、[接続（Connection）] 領域に接続状態が [管理上無効（Administratively Disabled）] として表示されます。

デバイス コネクタの HTTPS プロキシ設定の設定

サーバーの HTTPS プロキシ設定を手動で構成できます。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [デバイスコネクタ（Device Connector）] をクリックします。

ステップ 3 [接続（Connections）] エリアで、[HTTPSプロキシ設定（HTTPS Proxy Settings）] をクリックしてプロキシ設定を入力します。

アクション名	説明
[オフ（Off）] ボタン	HTTPS プロキシ設定を無効にします。
[手動（Manual）] ボタン	HTTPS プロキシ設定を手動で構成できます。
[プロキシホスト名/IP（Proxy Hostname/IP）] フィールド	プロキシ サーバーの IP アドレスまたはホスト名。
[プロキシポート（Proxy Port）] フィールド	プロキシ サーバーのポート番号。
[認証（Authentication）] トグル ボタン	このオプションを有効にすると、プロキシサーバーのクレデンシャルを提供できます。
[ユーザー名（Username）] フィールド	プロキシ サーバーのクレデンシャルです。
[パスワード（Password）] フィールド	

ステップ 4 [HTTPSプロキシ設定（HTTPS Proxy Settings）] ダイアログ ボックスで、情報を追加してから [保存（Save）] をクリックします。

Intersight デバイス コネクタのプロパティの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [デバイスコネクタ（Device Connector）] をクリックします。

ステップ 3 [Intersight管理（Intersight Management）] 領域で、次の情報を確認します。

アクション名	説明
[Enabled] オプション ボタン	Intersightの管理を有効または無効にできます。次のいずれかになります。 • [オン（On）]：Intersight の管理を有効にします。このシステムを請求してCisco Intersight の機能を活用できます。 • [オフ（Off）]：Intersight の管理を無効にします。Cisco Intersightへの通信は許可されません。

ステップ 4 [接続（Connection）] 領域で、次の情報を確認します。

名前	説明
[Status] フィールド	Intersight への接続の状態を表示します。次のいずれかになります。 • [管理上無効（Administratively Disabled）]：Intersight の管理が無効にされていることを示します。 • [DNS誤設定（DNS Misconfigured）]：BMC で DNS の詳細が設定されていないことを示します。 • [UCS接続ネットワークエラー（UCS Connect Network Error）]：無効なネットワーク構成を示します。 • **[Certificate Error]**—無効な証明書を示します。 • [要求あり（Claimed）]：Intersight でデバイスが要求されていることを示します。 • [要求なし（Not Claimed）]：デバイスが Intersight に登録されているが要求されてはいないことを示します。
[接続再試行（Retry Connection）] リンク	Intersight への接続を再試行できます。このオプションは、Intersight の接続に問題がある場合にのみ表示されます。
[詳細と推奨事項（Details & Recommendations）] ドロップダウン リスト	状態に基づいて接続の問題を修正するための詳細と推奨事項を表示します。

名前	説明
[HTTPSプロキシ設定（HTTPS Proxy Settings）] ダイアログ ボックス	Intersight 接続に必要な HTTPS プロキシ設定を手動で構成できます。
[シリアル番号（Serial Number）] フィールド	BMC のシリアル番号を表示します。
[セキュリティトークン（Security Token）] フィールド	接続ステータスが [要求なし（Not Claimed）] の場合に表示されます。Intersight にサーバーを安全に搭載するにはセキュリティ トークンを使用します。

ステップ 5 [接続（Connections）] エリアで、[HTTPSプロキシ設定（HTTPS Proxy Settings）] をクリックして次の情報を確認します。

アクション名	説明
[オフ（Off）] ボタン	HTTPS プロキシ設定を無効にします。
[手動（Manual）] ボタン	HTTPS プロキシ設定を手動で構成できます。
[プロキシホスト名/IP（Proxy Hostname/IP）] フィールド	プロキシ サーバーの IP アドレスまたはホスト名。
[プロキシポート（Proxy Port）] フィールド	プロキシ サーバーのポート番号。
[認証（Authentication）] トグル ボタン	このオプションを有効にすると、プロキシサーバーのクレデンシャルを提供できます。
[ユーザー名（Username）] フィールド	プロキシ サーバーのクレデンシャルです。
[パスワード（Password）] フィールド	

Intersight デバイス コネクタのプロパティの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理者（Admin）] タブをクリックします。
ステップ 2 [管理者（Admin）] タブの [デバイスコネクタ（Device Connector）] をクリックします。
ステップ 3 [Intersight管理（Intersight Management）] 領域で、次の情報を確認します。

アクション名	説明
[Enabled] オプション ボタン	Intersightの管理を有効または無効にできます。次のいずれかになります。 • [オン（On）]：Intersight の管理を有効にします。このシステムを請求してCisco Intersight の機能を活用できます。 • [オフ（Off）]：Intersight の管理を無効にします。Cisco Intersightへの通信は許可されません。

ステップ 4 [接続（Connection）] 領域で、次の情報を確認します。

名前	説明
[Status] フィールド	Intersight への接続の状態を表示します。次のいずれかになります。 • [管理上無効（Administratively Disabled）]：Intersight の管理が無効にされていることを示します。 • [DNS誤設定（DNS Misconfigured）]：BMC で DNS の詳細が設定されていないことを示します。 • [UCS接続ネットワークエラー（UCS Connect Network Error）]：無効なネットワーク構成を示します。 • [証明書検証エラー（Certification Validation Error）]：無効な証明書を示します。 • [要求あり（Claimed）]：Intersight でデバイスが要求されていることを示します。 • [要求なし（Not Claimed）]：デバイスが Intersight に登録されているが要求されてはいないことを示します。
アクセス モード	デフォルトでは、このモードは [制御を許可（Allow Control）] に設定されます。
[詳細と推奨事項（Details & Recommendations）] ドロップダウン リスト	状態に基づいて接続の問題を修正するための詳細と推奨事項を表示します。
デバイス ID	これはデバイスの ID を示します。

名前	説明
登録コード	これは Intersight からデバイスを要求するために必要なセキュリティ コードです。 （注） このコードは、[接続（Connection）] ステータスが [要求なし（Not Claimed）] のときにのみ使用できます。

ステップ 5 [Settings] 領域で、次の情報を確認します。

名前	説明
[General] タブ	**アクセス モード** • **[Read-only]**：**[Read-only]** アクセス モードを選択すると、Intersight を使用してデバイスを設定できなくなります。 • **[Allow Control]** — **[Allow Control]** モードを選択すると、Intersight を使用したデバイスの構成を完全に制御できます。 **[Intersightだけからの設定（Configuration from Intersight only）]** このオプションは、[制御を許可（Allow Control）] モードが有効になっている場合にのみ設定できます。[ロックアウトの設定（Configure Lockout）] オプションは次のとおりです。 **[OFF]**— デバイスを、ローカルでも Intersight からでも管理するには、オプション **[Configuration from Intersight only] をオフにします。**. この設定により、すべての既存のセッション（webUi、XML および CLI）が終了します。 **[ON:** — Intersight の Cisco IMC 設定をロックするには、オプション **[Configuration from Intersight only]** をオンにします。この設定により、すべての既存のセッション（webUi、XML および CLI）が終了します。 （注） 設定ロック アウト モードで admin としてログインしている場合、admin ロールはユーザー ロールにマッピングされるため、インターフェイスはユーザー ロールでログインしたユーザーとして動作します。
[Proxy Configuration] タブ	Intersight 接続に必要な HTTPS プロキシ設定を手動で構成できます。

名前	説明
[HTTPS プロキシ (HTTPS Proxy)] フィールド オプション ボタンを選択します	OFF - HTTPS プロキシ設定を無効にします。 ON - HTTPS プロキシ設定を有効にします。
[プロキシホスト名/IP（Proxy Hostname/IP）] フィールド	プロキシ サーバーの IP アドレスまたはホスト名。
[プロキシポート（Proxy Port）] フィールド	プロキシ サーバーのポート番号。
[認証（Authentication）] トグル ボタン	このオプションを有効にすると、プロキシサーバーのクレデンシャルを提供できます。 （注） デバイス コネクタには、ログイン クレデンシャルの形式は必須ではありません。これらは設定済みの HTTP プロキシ サーバーにそのまま渡されます。 ユーザー名をドメイン名で限定する必要があるかどうかは、HTTP プロキシ サーバーの構成によって異なります。
[Username] フィールド [Password] フィールド	プロキシ サーバーのクレデンシャルです。

名前	説明
[証明書マネージャ (Certificate Manager)] タブ	信頼できる証明書のリストを表示し、有効な信頼できる証明書をインポートできます。 • **[インポート (Import)]** - CA 署名付き証明書をインポートすることができます。 （注） インポートされた証明書が *.pem (base64 エンコード) 形式である必要があります。 • 次の情報と証明書のリストを表示することができます。 • **[名前 (Name)]**—CA 証明書の共通名。 • **[In Use]** - 信頼ストアで証明書を正常にリモート サーバの確認に使用されたかどうか。 • **[Issued By]**: 証明書の発行認証局。 • **[Expires]**—証明書の有効期限。 （注） バンドルされている証明書 (ロック アイコンが証明書) を削除することはできません。

PCIe スイッチの回復

始める前に

- admin 権限を持つユーザーとしてログインする必要があります。
- サーバーの電源が投入されている。

手順

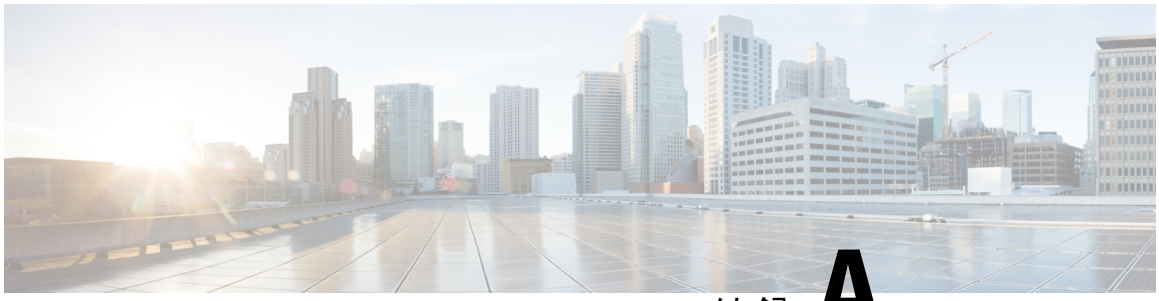
ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーティリティ（Utilities）] をクリックします。

ステップ 3 **[Utilities (ユーティリティ)]** ペインの **[Actions (アクション)]** 領域で、**[Recover PCIe Switch (PCIe スイッチの回復)]** をクリックします。

ステップ 4 **[Recover PCIe Switch (PCIe スイッチの回復)]** ダイアログ ボックスで、次の情報を確認します。

名前	説明
[Controller] ドロップダウン	サーバで使用可能なPCIeスイッチの一覧を示します。このリストから、[recover controller (コントローラの回復)] アクションを実行するスイッチを選択できます。
[Recover Controller (コントローラの回復)] ボタン	[Recover Controller (コントローラの回復)] ボタンをクリックすると、選択したコントローラのリカバリが開始されます。
[Cancel (キャンセル)] ボタン	アクションをキャンセルし、ダイアログ ボックスを閉じます。



付録 A

サーバー モデル別 BIOS パラメータ

C220 M7 および C240 M7 サーバー

I/O Tab

Note BIOS parameters listed in this tab may vary depending on the server.

Table 27: BIOS Parameters in I/O Tab

Name	Description
Reboot Host Immediately check box	If the Reboot Host Immediately check box is checked, the server is rebooted immediately and the new BIOS settings go into effect. Otherwise the changes are saved until the server is manually rebooted.

サーバー モデル別 BIOS パラメータ

Name	Description
MLOM OptionROM drop-down list	This options allows you to control the Option ROM execution of the PCIe adapter connected to the MLOM slot. This can be one of the following: • **Disabled**—Does not execute Option ROM of the PCIe adapter connected to the MLOM slot. • **Enabled**—Executes Option ROM of the PCIe adapter connected to the MLOM slot.
MLOM Link Speed drop-down list	This option allows you to restrict the maximum speed of an adapter card installed in PCIe MLOM slot. This can be one of the following: • **Disabled**—The maximum speed is not restricted. • **Auto**—System selects the maximum speed allowed. • **GEN1**—2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **GEN2**—5GT/s is the maximum speed allowed. • **GEN3**—8GT/s is the maximum speed allowed. • **GEN4**—16GT/s is the maximum speed allowed.
PCIe Slot*n* OptionROM drop-down list	Whether the server can use the Option ROMs present in the PCIe card slot designated by *n*. This can be one of the following: • **Disabled**—Option ROM for slot *n* is not available. • **Enabled**—Option ROM for slot *n* is available.

Name	Description
PCIe Slot*n* Link Speed drop-down list	System IO Controller *n* (SIOCn) add-on slot (designated by *n*) link speed. This can be one of the following: • **Disabled**—Slot is disabled, and the card is not enumerated. • **Auto**— The default link speed. Link speed is automatically assigned. • **GEN1**—Link speed can reach up to first generation. • **GEN2**—Link speed can reach up to second generation. • **GEN3**—Link speed can reach up to third generation.
MRAID OptionROM drop-down list	This options allows you to control the Option ROM execution of the MRAID PCIe adapter connected. This can be one of the following: • **Disabled**—Does not execute Option ROM of the MRAID PCIe adapter. • **Enabled**—Executes Option ROM of the MRAID PCIe adapter.
MRAID Link Speed drop-down list	This option allows you to restrict the maximum speed of an MRAID adapter card installed. This can be one of the following: • **Disabled**—The maximum speed is not restricted. • **Auto**—System selects the maximum speed allowed. • **GEN1**—2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **GEN2**—5GT/s is the maximum speed allowed. • **GEN3**—8GT/s is the maximum speed allowed. • **GEN4**—16GT/s is the maximum speed allowed.

サーバー モデル別 BIOS パラメータ

Name	Description
Front NVME-*n* OptionROM drop-down list	This options allows you to control the Option ROM execution of the PCIe adapter connected to the SSD:NVMe slot *n*. This can be one of the following: • **Disabled**—Does not execute Option ROM of the PCIe adapter connected to the SSD:NVMe1 slot. • **Enabled**—Executes Option ROM of the PCIe adapter connected to the SSD:NVMe1 slot
Front NVME-*n* Link Speed drop-down list	Link speed for NVMe front slot designated by slot *n*. This can be one of the following: • **Disabled**—Slot is disabled, and the card is not enumerated. • **Auto**—The default link speed. Link speed is automatically assigned. • **GEN1**—Link speed can reach up to first generation. • **GEN2**—Link speed can reach up to second generation. • **GEN3**—Link speed can reach up to third generation. • **GEN4**—Link speed can reach up to fourth generation.
PCIe Slot MSTOR RAID OptionROM drop-down list	Whether the server can use the Option ROMs present in the PCIe MSTOR RAID. This can be one of the following: • **Disabled**—Option ROM is not available. • **Enabled**—Option ROM is available.
Intel VTD Coherency Support drop-down list	Whether the processor supports Intel VT-d Coherency. This can be one of the following: • **Disabled**—The processor does not support coherency. • **Enabled**—The processor uses VT-d Coherency as required.

Name	Description
Intel VT for Directed IO drop-down list	Whether the processor uses Intel Virtualization Technology (VT), which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following: • **Disabled**—The processor does not permit virtualization. • **Enabled**—The processor allows multiple operating systems in independent partitions. **Note** If you change this option, you must power cycle the server before the setting takes effect.
VMD Enable drop-down list	Intel Volume Management Device (VMD) is for PCIe NVMe SSDs that provides hardware logic to manage and aggregate NVMe SSDs. This can be one the following: • **Enabled**— Enables benefits like robust surprise hot-plug, status LED management. • **Disabled**— Disables the feature. Default value: **Disabled**. Refer Intel® Virtual RAID on CPU User Guide to configure VMD. **Note** VROC is not supported with Cisco UCS C-Series M7 servers.
PCIe RAS Support drop-down list	Whether PCIe RAS Support is available on the PCIe slot. This can be one of the following: • **Disabled**—PCIe RAS is not available on the slot. • **Enabled**—PCIe RAS is available on port.
USB Port Rear drop-down list	Whether the rear panel USB devices are enabled or disabled. This can be one of the following • **Disabled**— Disables the rear panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled**— Enables the rear panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.

サーバー モデル別 BIOS パラメータ

Name	Description
VGA Priority drop-down list	Allows you to set the priority for VGA graphics devices if multiple VGA devices are found in the system. This can be one of the following: • **OnBoard**—Priority is given to the onboard VGA device. BIOS post screen and OS boot are driven through the onboard VGA port. • **OffBoard**—Priority is given to the PCIE Graphics adapter. BIOS post screen and OS boot are driven through the external graphics adapter port. • **OnBoardDisabled**—Priority is given to the PCIe Graphics adapter, and the onboard VGA device is disabled. The vKVM does not function when the onboard VGA is disabled.
IPV6 PXE Support drop-down list	Enables or disables IPv6 support for PXE. This can be one of the following • **Disabled**—IPv6 PXE support is not available. • **Enabled**—IPv6 PXE support is always available.
PCIe PLL SSC drop-down list	Enable this feature to reduce EMI interference by down spreading clock 0.5%. Disable this feature to centralize the clock without spreading. This can be one of the following: • **Auto**—EMI interference is auto adjusted. **Disabled**—EMI interference is auto adjusted. • **ZeroPointFive**—EMI interference is reduced by down spreading the clock 0.5%.
Network Stack drop-down list	This option allows you to monitor IPv6 and IPv4. This can be one of the following • **Disabled**—Network Stack support is not available. **Note** When disabled, the value set for **IPV4 PXE Support** does not impact the system. • **Enabled**—Network Stack support is always available.

Name	Description
IPV4 PXE Support drop-down list	Enables or disables IPv4 support for PXE. This can be one of the following • **Disabled**—IPv4 PXE support is not available. • **Enabled**—IPv4 PXE support is always available.
External SSC enable drop-down list	This option allows you to reduce the EMI of your motherboard by modulating the signals it generates so that the spikes are reduced to flatter curves. This can be one of the following: • **Disabled**—Clock Spread Spectrum support is not available. • **Enabled**—Clock Spread Spectrum support is always available.
IPV4 HTTP Support drop-down list	Enables or disables IPv4 support for HTTP. This can be one of the following: • **Disabled**—IPv4 HTTP support is not available. • **Enabled**—IPv4 HTTP support is always available.
IIO eDPC Support drop-down list	eDPC allows a downstream link to be disabled after an uncorrectable error, making recovery possible in a controlled and robust manner. This can be one of the following: • Disabled—eDPC support is disabled. • On Fatal Error—eDPC is enabled only for fatal errors. • On Fatal and Non-Fatal Errors—eDPC is enabled for both fatal and non-fatal errors.
IPV6 HTTP Support drop-down list	Enables or disables IPv6 support for HTTP. This can be one of the following: • **Disabled**—IPv6 HTTP support is not available. • **Enabled**—IPv6 HTTP support is always available.

[Server Management] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *28 : [*サーバ管理（*Server Management*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（**Reboot Host Immediately**）**]** チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[OS ブート ウォッチドッグ タイマー ポリシー（OS Boot Watchdog Timer Policy）] ドロップダウン リスト	ウォッチドッグ タイマーが切れた場合にシステムで実行されるアクション。次のいずれかになります。 • [電源オフ（Power Off）]：OS のブート中にウォッチドッグ タイマーの期限が切れた場合、サーバの電源がオフになります。 • [Reset]：OS のブート中にウォッチドッグ タイマーが切れた場合、サーバーはリセットされます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にする場合にのみ適用されます。
[FRB 2 タイマー（FRB 2 Timer）] ドロップダウン リスト	POST 中にシステムがハングした場合に、システムを回復するために Cisco IMC によって FRB2 タイマーが使用されるかどうか。次のいずれかになります。 • [無効（Disabled）]：FRB2 タイマーは使用されません。 • [Enabled]：POST 中に FRB2 タイマーが開始され、必要に応じてシステムの回復に使用されます。

名前	説明
[OS ウォッチドッグ タイマー（OS Watchdog Timer）] ドロップダウン リスト	BIOS が指定されたタイムアウト値でウォッチドッグ タイマーをプログラムするかどうか。次のいずれかになります。 • [Disabled]：サーバーのブートにかかる時間をトラッキングするためにウォッチドッグ タイマーは使用されません。 • [有効（enabled）]：サーバーがブートにかかる時間をウォッチドッグ タイマーで追跡します。サーバーのブートが [OS ブート ウォッチドッグ タイマー タイムアウト（OS Boot Watchdog Timer Timeout）] フィールドで指定された時間内に完了しない場合は、Cisco IMC によってエラーがログに記録され、[OS ブート ウォッチドッグ ポリシー（OS Boot Watchdog Policy）] フィールドで指定されたアクションが実行されます。
[OS ブート ウォッチドッグ タイマー タイムアウト（OS Watchdog Timer Timeout）] ドロップダウン リスト	OS が指定された時間内にブートしない場合、OS ウォッチドッグ タイマーの期限が切れ、システムはタイマーポリシーに基づいてアクションを実行します。次のいずれかになります。 • [5 分（5 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [10 分（10 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [15 分（15 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [20 分（20 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にした場合にのみ適用されます。

サーバー モデル別 BIOS パラメータ

名前	説明
[ボー レート（Baud Rate）] ドロップダウン リスト	シリアル ポートの伝送速度として使用されるボー レート。[コンソール リダイレクション（Console Redirection）] を無効にした場合、このオプションを使用できません。次のいずれかになります。 • [9.6k]：9,600 ボー レートが使用されます。 • [19.2k]：19,200 ボー レートが使用されます。 • [38.4k]：38,400 ボー レートが使用されます。 • [57.6k]：57,600 ボー レートが使用されます。 • [115.2k]：115,200 ボー レートが使用されます。 この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。
[フロー制御（Flow Control）] ドロップダウン リスト	フロー制御にハンドシェイク プロトコルを使用するかどうかを設定します。送信要求/クリア ツー セント（RTS/CTS）を使用すると、隠れた端末の問題が原因で発生する可能性がある、フレーム コリジョンを減らすことができます。次のいずれかになります。 • [なし（None）]：フロー制御は使用されません。 • [RTS/CTS]：RTS/CTS がフロー制御に使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。

名前	説明
[コンソール リダイレクション（Console Redirection）] ドロップダウン リスト	POST および BIOS のブート中に、シリアル ポートをコンソール リダイレクションで使用できるようにします。OS起動後は、コンソールのリダイレクトが関係なくなります。次のいずれかになります。 • **[COM 0]**：POST 中にシリアル ポート A でコンソール リダイレクションを有効にします。 • **[COM 1]**：POST 中にシリアル ポート B でコンソール リダイレクションを有効にします。 • [Disabled]：POST 中にコンソール リダイレクションは発生しません。
[ターミナル タイプ（Terminal Type）] ドロップダウン リスト	コンソール リダイレクションに使用される文字フォーマットのタイプ。次のいずれかになります。 • [PC-ANSI]：PC-ANSI 端末フォントが使用されます。 • [VT100]：サポートされている VT100 ビデオ端末とその文字セットが使用されます。 • [VT100-PLUS]：サポートされている VT100-plus ビデオ端末とその文字セットが使用されます。 • [VT-UTF8]：UTF-8 文字セットのビデオ端末が使用されます。
[PCIe Slots CDN コントロール（PCIe Slots CDN Control）] ドロップダウンリスト	イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [無効（Disabled）]：VIC カードに対する CDN サポートは無効です。 • [有効（Enabled）]：VIC カードの CDN サポートが有効になります。

サーバー モデル別 BIOS パラメータ

名前	説明
[CDN コントロール（CDN Control）] ドロップダウン リスト	イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [無効（Disabled）]：VIC カードに対する CDN サポートは無効です。 • [有効（Enabled）]：VIC カードの CDN サポートが有効になります。
[OptionROM起動最適化（OptionROM Launch Optimization）]	このオプションが [有効（Enabled）] の場合、ブート順序のポリシーに存在するコントローラにのみ OptionROMs が起動されます。 （注） オンボードストレージコントローラ、Emulex FC アダプタおよび GPU コントローラなどのいくつかのコントローラについて、ブート順序のポリシーに含まれていなくても、OptionROM が起動されます。 このオプションが [無効（Disabled）] の場合、すべての OptionROMs が起動されます。 デフォルト値：[有効（Enabled）]

名前	説明
適応型メモリ トレーニング	このオプションを[有効（Enabled）]にすると、次のようになります。 メモリ トレーニングは毎回のブートでは実行されず、BIOSは、保存されたメモリ トレーニングの結果を毎回のリブートで使用します。 毎回のブートでメモリ トレーニングが実行されるいくつかの例外には、次のものがあります。 BIOS の更新、CMOS のリセット、CPU やメモリの設定変更、SPD または実行時の修正不可能なエラー、または、前回のブートから 24 時間以上経過している場合。 このオプションが [無効（Disabled）] の場合、毎回のブートでメモリ トレーニングが行われます。 デフォルト値：[有効（Enabled）]。 （注） [高速ブート（Fast Boot）] オプションを無効にするには、エンドユーザーは次のトークンを下記の説明のとおりに設定する必要があります。 [適応型メモリ トレーニング（Adaptive Memory Training）]を [無効（Disabled）] に [BIOS Techlogレベル（BIOS Techlog level）] を [標準（Normal）] に [OptionROM起動最適化（OptionROM Launch Optimization）] を [無効（Disabled）] に

名前	説明
[BIOS Techlogレベル（BIOS Techlog Level）]	このオプションは、**BIOS tech ログファイル**のメッセージのタイプを示します。 ログファイルには、次のタイプのいずれかを指定できます。 • [最小（Minimum）]：重要なメッセージがログファイルに表示されます。 • [標準（Normal）]：警告およびロードメッセージがログファイルに表示されます。 • [最大（Maximum）]：標準に加え、情報関連のメッセージがログファイルに表示されます。 デフォルト値：[最小（Minimum）] （注） このオプションは、主に、内部のデバッグを目としています。

[セキュリティ（Security）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *29 : [*セキュリティ管理（*Security Management*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。

名前	説明
[トラステッド プラットフォーム モジュール状態（Trusted Platform Module State）] ドロップダウン リスト	信頼されたプラットフォーム モジュール（TPM）は、主に暗号キーを使用する基本的なセキュリティ関連機能を提供するように設計されたマイクロチップです。このオプションを使用すると、システムの TPM セキュリティ デバイス サポートを制御できます。次のいずれかになります。 • [Disabled]：サーバーはTPMを使用しません。 • [有効（Enabled）]：サーバはTPMを使用します。 （注） オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせください。
セキュリティ デバイス サポート（Security Device Support）] ドロップダウン リスト	セキュリティ デバイスのサポートを有効にするには、TPM サポートを有効にする必要があります。次のいずれかになります。 • **[無効（Disabled）]**：機能は無効です。 • **[有効（Enabled）]**：TPM が有効な場合、機能が有効になります。
[SHA-256 PCR バンク（SHA-256 PCR Bank）] ドロップダウン リスト	BIOS が測定を実行しているときに OS で使用可能な PCR バンクです。 • **[無効（Disabled）]**：SHA256 PCR バンクは BIOS で使用できません。 • **[有効（Enabled）]**：SHA256 PCR バンクは BIOS で使用できます。
[SHA-1 PCR バンク（SHA-1 PCR Bank）] ドロップダウン リスト	BIOS が測定を実行しているときに OS で使用可能な PCR バンクです。 • **[無効（Disabled）]**：SHA-1 PCR バンクは BIOS で使用できません。 • **[有効（Enabled）]**：SHA-1 PCR バンクは BIOS で使用できます。

名前	説明
[TPM の最小限の物理的存在（TPM Minimal Physical Presence）] ドロップダウン リスト	このトークンを使用すると、TPM に推奨される Microsoft のデフォルト設定を適用できます。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[TPM 保留中の操作（TPM Pending Operation）] ドロップダウン リスト	トラステッド プラットフォーム モジュール（TPM）Pending Operation オプションを使用すると、保留中の操作のステータスを制御できます。次のいずれかになります。 • [None]：アクションなし。 • TpmClear：保留中の操作をクリアします。
[電源オン パスワード（Power On Password）] ドロップダウン リスト	このトークンでは、F2 BIOS 設定を使用する前にBIOSパスワードを設定する必要があります。有効にすると、BIOS関数（IO設定、BIOSセットアップ、BIOSを使用したオペレーティング システムへのブート）にアクセスする前にパスワードの検証が必要になります。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[Intel Trusted Execution Technology サポート（Intel Trusted Execution Technology Support）] ドロップダウン リスト	信頼されたプラットフォームモジュール(TPM)が 有効 である場合にのみ 有効 に設定できます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

名前	説明
[マルチキー トータル メモリ暗号化（Multikey Total Memory Encryption、MK-TME） ドロップダウン リスト	MK-TME を使用すると、独自のキーを持つ 1 つの暗号化ドメインを複数持つことができます。異なるメモリ ページを異なるキーで暗号化できます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[トータル メモリ暗号化（Total Memory Encryption、TME）] ドロップダウン リスト	システムの物理メモリ全体を暗号化する機能を提供します。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SGX 工場出荷時リセット（SGX Factory Reset）] ドロップダウン リスト	その後の起動時にシステムが SGX の工場出荷時リセットを実行できるようにします。これにより、すべての登録データが削除されます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SWガード拡張（SW Guard Extensions、SGX）] ドロップダウン リスト	ソフトウェア ガード拡張（SGX）機能を有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

名前	説明
[SGX QoS] ドロップダウン リスト	SGX QoS を有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SGX パッケージ情報インバンド アクセス（SGX Pkg info In-Band Access）] ドロップダウン リスト	SGX パッケージ情報インバンドアクセスを有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SGX 書き込み有効（SGX Write Enable）] ドロップダウン リスト	SGX 書き込み機能を有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[所有者 EPOCH入力タイプ選択（Select Owner EPOCH input type）] ドロップダウン リスト	作成され、ロックされたメモリ領域に使用されるセキュリティ キーのシードを変更できます。次のいずれかになります。 • **SGX 所有者 EPOCH 有効化（SGX Owner EPOCH activated）]**：現在の入力タイプを変更しません。 • **[新しいランダム所有者 EPOCH に変更（Change to New Random Owner EPOCHs）]**：EPOCH をシステムが生成したランダムな数値に変更します。 • **[手動ユーザー定義所有者 EPOCH（Manual User Defined Owner EPOCHs）]**：EPOCH シードをユーザーが入力した 16 進値に変更します。

名前	説明
[SProcessor Epoch*n*] フィールド	*n* で指定された EPOCH 番号の SGX EPOCH 所有者値を定義できます。
[SGX 自動 MP レジストレーション エージェント（SGX Auto MP Registration Agent）] ドロップダウン リスト	レジストレーション エージェント サービスがプラットフォーム キーを保存できるようにします。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SGX PUBKEY HASH*n*] フィールド	ソフトウェア ガード拡張（SGX）の値を設定できます。この値の設定範囲は、以下のとおりです。 • SGX PUBKEY HASH0 — 7 ～ 0 の間 • SGX PUBKEY HASH1 — 15 ～ 8 の間 • SGX PUBKEY HASH2 — 23 ～ 16 の間 • SGX PUBKEY HASH3 — 31 ～ 24 の間
[CPU PA を 46 ビットに制限（LIMIT CPU PA to 46 Bits）] ドロップダウン リスト	Intel ® VT-d でこのオプションを有効にして、2019 OS でブートできるようにします。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[DMA 制御オプトイン フラグ（DMA Control Opt-In Flag）] ドロップダウン リスト	DMA 制御オプトイン フラグ：このトークンを有効にすると、オペレーティング システムは入出力メモリ管理ユニット（IOMMU）を有効にして、悪意のあるデバイスからの DMA 攻撃を防ぐことができます。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

メモリ タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *30 : [*メモリ（*Memory*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（**Reboot Host Immediately**）**]** チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。

名前	説明
[メモリ RAS 構成の選択（Select Memory RAS configuration）] ドロップダウン リスト	サーバーに対するメモリの信頼性、可用性、およびサービス性（RAS）の設定方法。次のいずれかになります。 • [最大パフォーマンス（Maximum Performance）]：システムのパフォーマンスが最適化されます。 • **ADDDC のスペアリング**: 適応可能な仮想ロックステップは、ADDDC モードをサポートするためにハードウェアおよびファームウェアで実装されるアルゴリズムです。選択すると、アルゴリズムがアクティブになるまでシステムのパフォーマンスが最適化されます。このアルゴリズムは、DRAM デバイスで障害が発生した場合にアクティブになります。アルゴリズムがアクティブになると、仮想ロックステップ リージョンがアクティブになり、実行時に障害が発生したリージョンが動的にマッピングされ、パフォーマンスへの影響はリージョン レベルで制限されます。 • [ミラー モード 1LM（Mirror Mode 1LM）]：システムのメモリの半分をバックアップとして使用することにより、システムの信頼性が最適化されます。 • **部分的なミラー モード 1LM**: 部分的な DIMM ミラーリングによって完全なミラーコピーを保持するのではなく、メモリ セルの特定の領域のミラーコピーが作成されます。部分的なミラーリングでは、部分的なミラー コピーの属性を使用して、メモリ マップにミラー領域が作成されます。最大 4 個の部分的なミラーを使用して、合計メモリ容量の最大 50% をミラーリングできます。

サーバー モデル別 BIOS パラメータ

名前	説明
[NUMA] ドロップダウン リスト	BIOS で Non-Uniform Memory Access（NUMA）がサポートされているかどうか。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[部分的なキャッシュ行の節約（Partial Cache Line Sparing）] ドロップダウンリスト	パーシャル キャッシュ ライン スペアリング (PCLS) は、メモリ コントローラーのエラー防止メカニズムです。PCLS は、メモリ アクセス中に置換できるように、ビットの欠陥のあるニブルの場所を、対応するデータ コンテンツとともにスペア ディレクトリに静的にエンコードします。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[ディスク タイプの選択 (Select Disk Type)] ドロップダウン リスト	Cisco IMC は、指定された障害のある行から指定されたスペア行へのアクセスを永続的に再マッピングする、**ハード PPR**をサポートしています。 次のいずれかになります。 • **[ハード PPR (Hard PPR)]**: サポートは有効になっています。 （注） ハード PPR は、**[メモリ RAS 設定 (Memory RAS Configuration)]**が **[ADDDC スペア (ADDDC Sparing)]**に設定されている場合にのみ使用できます。他の RA の選択では、この設定を **Disabled** に設定する必要があります。 • **[無効 (Disabled)]**：サポートは無効になっています。

名前	説明
[BME DMA 移行 (BME DMA Mitigation)] ドロップダウン リスト	不正な外部 DMA からの脅威を緩和する PCI BME ビットを無効にできます。次のいずれかになります。 • **[無効 (disabled)]**: PCI BME ビットは BIOS で無効になっています。 • **[有効 (Enabled)**: PCI BME ビットは BIOS で有効になっています。
[4 G 以上の復号化（Above 4G Decoding）] ドロップダウン リスト	4 GB 以上の MMIO を有効または無効にします。次のいずれかになります。 • [Disabled]：サーバーでは 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングしません。 • [有効（Enabled）]：サーバで 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングします。 （注） PCI デバイスが 64 ビット対応でも、レガシーなオプション ROM を使用する場合は、この設定をイネーブルにしても正しく機能しない場合があります。
[Partial Memory Mirror Mode (部分メモリ ミラー モード)]ドロップダウン リスト	部分的なメモリ サイズは、パーセンテージまたは GB 単位のいずれかです。次のいずれかになります。 • **割合**: 部分的なメモリのミラーはパーセンテージで定義されます。 • **値 (GB)**: 部分的なメモリ ミラーは GB で定義されます。 • **無効**: 部分的なメモリ ミラーが無効になります。

名前	説明
[DCPMM Firmware Downgrade (DCPMM ファームウェアのダウングレード)] ドロップダウン リスト	BIOS が DCPMM ファームウェアのダウングレードをサポートしているかどうか。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[部分ミラー *n* サイズ（GB）（Partial Mirror n Size in GB）] フィールド	最初の部分メモリ ミラーのサイズ（GB）。 n = 1、2、または 3 0 ～ 65535 の整数を入力します。 （注） すべての部分的なミラーの合計メモリ サイズは、物理メモリ サイズの 50% を超えないようにする必要があります。
[部分的なミラー パーセンテージ (Partial Mirror percentage)] フィールド	4GB を超えてミラーリングするメモリの割合。 0 ～ 60 の整数を入力します。
[メモリ サイズ制限 (GB) (Memory Size Limit in GB)] フィールド	このオプションを使用して、物理メモリの上限のサイズを GB 単位で減らします。 0 ～ 65535 の整数を入力します。
[NVM パフォーマンス設定 (NVM Performance Setting)] ドロップダウンリスト	ワークロードの動作に応じて、NVM ベースラインのパフォーマンス設定を設定できます。 • **BW 最適化** • **遅延の最適化** • **バランス プロファイル**
[CR QoS] ドロップダウンリスト	CR QoS 調整を選択できます。 次のいずれかになります。 • **[モード 1（Mode 1）]** : • **[モード 2（Mode 2）]** : • **[モード 0（Mode 0）]** : **[CR QoS]** 機能は無効です。

名前	説明
[AD の Snoopy モード (Snoopy mode for AD)] ドロップダウン リスト	新しい AD 固有の機能を有効にして、NUMA に最適化されていないワークロードからDDRT メモリへのディレクトリ更新を回避します。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[CR Fastgo Config] ドロップダウンリスト	CR QoS 設定プロファイルを選択できるようにします。 次のいずれかになります。 • **[最適化の有効化（Enable Optimization）]** • **[最適化の無効化（Disable Optimization）]** • **Auto**
[メモリ リフレッシュ レート（Memory Refresh Rate）] ドロップダウンリスト	メモリのリフレッシュ レートを増減できます。DRAM のリフレッシュ レートを上げると、次のリフレッシュの前に発生する可能性のあるアクティブ化（ハンマー）の最大数が減少します。 次のいずれかになります。 • **[1X リフレッシュ（1X Refresh）]**：リフレッシュ レートは最小です。 • **[2X リフレッシュ（2X Refresh）]**：リフレッシュは 2 倍高速です。
[2LM の Snoopy モード (Snoopy mode for 2LM)] ドロップダウン リスト	NUMA に最適化されていないワークロードから far メモリへのディレクトリ更新を回避できます。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

サーバー モデル別 BIOS パラメータ

名前	説明
[メモリ サーマル スロットリング モード（Memory Thermal Throttling Mode）] ドロップダウンリスト	この関数は、メモリ温度の調整に使用されます。この機能を有効にした後、メモリ温度が極端に高くなると、メモリアクセスレートが低下し、Baseboard Management Controller（BMC）がファンを調整してメモリを冷却し、DIMM の損傷を防ぎます。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • **PECI を使用した CLTT**：プラットフォーム環境制御インターフェイスを使用してクローズドループ サーマル スロットリングを有効にします。
[パニックと高水準点（Panic and High Watermark）] ドロップダウンリスト	低に設定した場合、**[メモリ更新レート（Memory Refresh Rate）]** が **[1X リフレッシュ（1X Refresh）]** に設定されている間、メモリコントローラは更新を延期しません。 次のいずれかになります。 • **[低（Low）]**：リフレッシュ レートは低に設定します。 • **[高（High）]**：リフレッシュ レートは高に設定します。
[UMA] ドロップダウンリスト	UMA 設定を設定できます。次のいずれかになります。 • Disable(All2All) • Hemisphere(2-clusters)

名前	説明
[拡張メモリ テスト（Enhanced Memory Test）] ドロップダウンリスト	（注） この機能は、Samsung、Hynix、および Micron DIMM にのみ適用されます。 この機能を使用して、BIOS POST 中に高度な DIMM テストを有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[eADR サポート（eADR Support）] ドロップダウンリスト	拡張非同期 DRAM リフレッシュ（eADR）のサポートにより、CPU キャッシュに格納されているデータを永続メモリに移動するためのキャッシュ フラッシュ コマンドの待機期間を回避できます。これによりパフォーマンスが向上します。次のいずれかになります。 • **Disabled** • **有効化** • **Auto**
[揮発性メモリ モード（Volatile Memory Mode）] ドロップダウンリスト	揮発性メモリ モードの設定は、BIOS が Intel® Optane™ PMem をサポートしている場合に表示されます。次のいずれかになります。 • **[1LM]**：このオプションは、Intel® Optane™ PMem を App-Direct モードで設定するために使用できます。 • **[2LM]**：このオプションにより、2LM は DDR4 メモリをキャッシュとして動作させることができます。

サーバー モデル別 BIOS パラメータ

名前	説明
[アダプティブ リフレッシュ管理レベル（Adaptive Refresh Management Level）] ドロップダウン リスト	リフレッシュ管理設定は読み取り専用です。現用系 RFM により、コントローラは RFM レベルと呼ばれる追加の RFM しきい値設定を柔軟に選択できます。RFM レベルにより、コントローラが発行した RFM コマンドと、これらのコマンドの DRAM 内管理との調整が可能になります。 次のいずれかになります。 • **デフォルト (Default)** • **[レベル A（Level A）]** • **[レベル B（Level B）]** • **[レベル C（Level C）]**
[メモリ帯域幅ブースト（Memory Bandwidth Boost）] ドロップダウンリスト	Intel® メモリ帯域幅ブーストは、Intel® Optane™ パーシステント メモリの機能であり、サーマル ヘッドルームが利用可能な場合に、ダイナミック レンジの電力と帯域幅を提供します。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[エラー チェック スクラブ（Error Check Scrub）] ドロップダウン リスト	結果収集の有無にかかわらず、メモリ チェックを有効にすることができます。次のいずれかになります。 • **Disabled** • **[結果収集なしで有効化（Enabled without Result Collection）]** • **[結果収集ありで有効化（Enabled with Result Collection）]**

名前	説明
[ランク マージン ツール（Rank Margin Tool）] ドロップダウン リスト	ランク マージン ツールが使用されているかどうか、およびマージン テスト（メモリ シーケンスと電圧信号をテストするもの）が実行されているかどうかを示します。次のいずれかになります。 • **Disabled** • **有効化**

[電源/パフォーマンス（Power/Performance）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *31 : [*電源/パフォーマンス（*Power/Performance*）*] タブの BIOS* パラメータ

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[隣接キャッシュ ライン プリフェッチャ（Adjacent Cache Line Prefetcher）] ドロップダウン リスト	プロセッサで必要な行のみを取得するのではなく、偶数または奇数のペアのキャッシュ行を取得するかどうか。次のいずれかになります。 • [Disabled]：プロセッサで必要な行のみを取得します。 • [Enabled]：プロセッサで必要な行およびペアの行の両方を取得します。

名前	説明
[ハードウェア プリフェッチャ（Hardware Prefetcher）] ドロップダウン リスト	プロセッサで、インテル ハードウェア プリフェッチャが必要に応じてデータおよび命令ストリームをメモリから取得し、統合 2 次キャッシュに入れることを許可するかどうか。次のいずれかになります。 • [Disabled]：ハードウェア プリフェッチャは使用しません。 • [Enabled]：プロセッサで、キャッシュの問題が検出されたときにプリフェッチャを使用します。
[DCU IP プリフェッチャ（DCU IP Prefetcher）] ドロップダウン リスト	プロセッサで DCU IP プリフェッチ メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。次のいずれかになります。 • [Disabled]：プロセッサでキャッシュ データをプリロードしません。 • [Enabled]：DCU IP プリフェッチャで最も関連性が高いと判断されたデータを含む L1 キャッシュをプリロードします。
[DCU ストリーマ プリフェッチ（DCU Streamer Prefetch）] ドロップダウン リスト	プロセッサで DCU IP プリフェッチ メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。次のいずれかになります。 • [Disabled]：プロセッサはキャッシュ読み取り要求を予測しようとせず、明示的に要求された行のみを取得します。 • [Enabled]：DCU Prefetcher でキャッシュ読み取りパターンを分析し、必要と判断した場合にキャッシュ内の次の行を事前に取得します。

名前	説明
[仮想 Numa（Virtual Numa）] ドロップダウン リスト	仮想 NUMA（仮想非均一メモリ アクセス）は、VMware 仮想マシン（VM）のメモリ アクセス最適化方法であり、メモリ帯域幅のボトルネックを防ぐのに役立ちます。 次のいずれかになります。 • **[無効（Disabled）]**：機能は無効です。 • **[有効（Enabled）]**：機能は有効です。
[CPU パフォーマンス（CPU Performance）] ドロップダウン リスト	上記のオプションに対し CPU パフォーマンス プロファイルを設定します。次のいずれかになります。 • [Enterprise]：すべてのオプションがイネーブルです。 • [HPC]：すべてのオプションがイネーブルです。この設定はハイ パフォーマンス コンピューティングとも呼ばれます。 • [高スループット（Hight Throughput）]：DCU IP Prefetcher のみが有効です。残りのオプションは無効になります。 • [Custom]：パフォーマンス プロファイルのすべてのオプションをサーバの BIOS セットアップから設定できます。また、[ハードウェア プリフェッチャ（Hardware Prefetcher）] オプションと [隣接キャッシュ ライン プリフェッチャ（Adjacent Cache Line Prefetcher）] オプションも同様に設定できます。

サーバー モデル別 BIOS パラメータ

名前	説明
[LLC デッドライン（LLC Dead Line）] ドロップダウンリスト	CPU の非包括的キャッシュ スキームでは、MLC から削除された内容が LLC に書き込まれます。行を MLC から削除する際、コアはそれらに **[デッド（dead）]** としてフラグを立てることがあります（再度読み取られる可能性が小さい場合）。LLC には、デッドラインを削除し、LLC に書き込まないオプションがあります。 この機能が無効の場合、デッド ラインは常に削除されます。LLC に書き込まれることはありません。 この機能が有効の場合、使用可能な空きスペースがある場合にデッドラインを LLC に書き込むことを LLC に許可します。 次のいずれかになります。 • **[無効（Disabled）]**：機能は無効です。 • **[有効（Enabled）]**：機能は有効です。 • **[自動（Auto）]**：CPU が LLC のデッドラインの割り当てを決定します。
[XPT リモート プリフェッチ（XPT Remote Prefetch） ドロップダウンリスト	この機能は、LLC 要求を複製し、最近の LLC 履歴に基づいてリモート マシンの適切なメモリ コントローラに送信して、待ち時間を減らします。 次のいずれかになります。 • **[無効（Disabled）]**：機能は無効です。 • **[有効（Enabled）]**：機能は有効です。 • **[自動（Auto）]**：CPU が機能を決定します。
[UPI リンク有効化（UPI Link Enablement）] ドロップダウンリスト	プロセッサが必要とする最小数の UPI リンクを有効にします。 次のいずれかになります。 • **1** • **2** • **Auto**

名前	説明
[強化 CPU パフォーマンス（Enhanced CPU Performance）] ドロップダウンリスト	（注） この機能を有効にすると、**[電源特性の有効化（Enable Power Characterization）]** および **[パワーキャッピング（Power Capping）]** を有効にすることはできません。 サーバー設定を自動的に調整することにより、CPU パフォーマンスを向上させます。 （注） この機能を有効にすると、消費電力が増加する可能性があります。 この機能を使用するには、サーバーが次の要件を満たしている必要があります。 • サーバーが、Barlow Pass DIMM を使用していないこと • Cisco UCS C220 M6 サーバーの DIMM モジュール サイズは 64 GB 未満であり、Cisco UCS C240 M6 サーバーでは 256 GB 未満であること • サーバーに GPU カードが搭載されていないこと。 次のいずれかになります。 • **[無効（Disabled）]**：プロセッサでこの機能を使用しません。 • **[自動（Auto）]**：Cisco IMC がサーバー設定を調整して、パフォーマンスを向上させることができます。
[C1 自動降格（C1 Auto Demotion）] ドロップダウンリスト	有効にすると、CPU は非コア自動降格情報に基づいて C1 状態に自動的に降格します。 • **[無効（Disabled）]**：プロセッサでこの機能を使用しません。 • **[有効（Enabled）]**：機能は有効です。

名前	説明
[UPI 電力管理（UPI Power Manangement）] ドロップダウンリスト	UPI 電力管理は、サーバーの電力を節約するために使用されます。 次のいずれかになります。 • **[無効（Disabled）]**：プロセッサでこの機能を使用しません。 • **[自動（Auto）]**：機能は有効です。
[C1 自動降格解除（C1 Auto UnDemotion）] ドロップダウンリスト	プロセッサが C1 降格状態から自動的に解除できるようにするかどうかを選択します。 • **[無効（Disabled）]**：プロセッサでこの機能を使用しません。 • **[有効（Enabled）]**：機能は有効です。

[プロセッサ（Processor）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *32 : [*プロセッサ（*Processor*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[拡張 APIC（Extended APIC）] ドロップダウンリスト	拡張 APIC サポートをイネーブルまたはディセーブルにできます。次のいずれかになります。 • 有効：APIC サポートを有効にします • [無効（Disabled）]：APIC サポートを無効にします。

名前	説明
[Intel Virtualization Technology] ドロップダウン リスト	プロセッサで Intel Virtualization Technology（VT）を使用するかどうか。このテクノロジーでは、1つのプラットフォームで、複数のオペレーティング システムとアプリケーションをそれぞれ独立したパーティション内で実行できます。次のいずれかになります。 • [Disabled]：プロセッサでの仮想化を禁止します。 • [有効（Enabled）]：プロセッサで、複数のオペレーティング システムをそれぞれ独立したパーティション内で実行できます。
[プロセッサ C6 レポート（Processor C6 Report）] ドロップダウン リスト	BIOS からオペレーティング システムに C6 レポートを送信するかどうか。OS はレポートを受信すると、プロセッサを電力量の少ない C6 状態に移行してエネルギー使用量を減らし、最適なプロセッサ パフォーマンスを維持できます。次のいずれかになります。 • [Disabled]：BIOS から C6 レポートを送信しません。 • [Enabled]：BIOS から C6 レポートを送信し、OS がプロセッサを電力量の少ない C6 状態に移行できるようにします。 （注） [CPUPowerManagement] を [カスタム（Custom）] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。 （注） このオプションを使用できるのは一部の C シリーズ サーバーだけです。

サーバー モデル別 BIOS パラメータ

名前	説明
[プロセッサ C1E（Processor C1E）] ドロップダウン リスト	C1 ステートに入ったときに、CPU が最小周波数に移行するかどうか。次のいずれかになります。 • [無効（Disabled）]：CPU は C1 ステートでも引き続き最大周波数で動作します。 • [有効（Enabled）]：CPU は最小周波数に移行します。このオプションでは C1 ステートで節約される電力量が最大になります。 （注） このオプションを使用できるのは一部の C シリーズ サーバーだけです。
[EIST PSD 関数（EIST PSD Function）] ドロップダウンリスト	EIST は、電圧と周波数のペア（P 状態）の変更に固有の遅延を短縮するため、これらの遷移がより頻繁に発生するようになります。これにより、より詳細なデマンドベースのスイッチングが可能になり、アプリケーションの要求に基づいて電力とパフォーマンスのバランスを最適化できます。次のいずれかになります。 • **[HW ALL]**：プロセッサは、論理プロセッサの依存関係間の P 状態を調整します。OS は、すべての論理プロセッサで P-state 要求を最新の状態に保ちます。 • **[SW ALL]**：OS Power Manager によって、依存関係にある論理プロセッサ間の P-state を調整します。すべての論理プロセッサで遷移を開始します。

名前	説明
[ターボ モード（Turbo Mode）] ドロップダウンリスト	プロセッサでインテル ターボ ブースト テクノロジーを使用するかどうか。このテクノロジーでは、仕様よりも低い電力、温度、または電圧でプロセッサが動作していると、自動的にそのプロセッサの周波数が上がります。次のいずれかになります。 • [Disabled]：プロセッサの周波数は自動的には上がりません。 • [Enabled]：必要に応じてプロセッサで Turbo Boost Technology が利用されます。 （注） [CPUPowerManagement] を [カスタム（Custom）] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[非コア周波数スケーリング (Uncore Frequency Scaling)] ドロップダウンリスト	この機能を使用すると、プロセッサのコア以外の周波数のスケーリングを設定できます。次のいずれかになります。 • **[Enabled]**：プロセッサの非コア部分の周波数を、負荷に応じて上下します。 • **[無効 (Disabled)]**: プロセッサのコア以外の周波数を固定します。 『Intel® Dear Customer Letter (DCL)』には、固定されていない場合の**[非コア周波数スケーリング (Uncore Frequency Scaling)]**の固定の上限値と下限値が記されています。
[ブート パフォーマンス モード（Boot Performance Mode）] ドロップダウン リスト	オペレーティング システムのハンドオフ前に設定される BIOS パフォーマンス状態を選択できます。次のいずれかになります。 • [Max Performance]：プロセッサの P-state 率は最大です • **[最大効率（Max Efficient）]**：プロセッサの P-state の比率が最小です。 • **[Intel NM による設定（Set by Intel NM）]**：値は自動的に設定されます。

サーバー モデル別 BIOS パラメータ

名前	説明
[TDP の設定（Config TDP）]ドロップダウンリスト	**[TDP の設定（Config TDP）]**機能により、プロセッサの温度設計の電力値を調整できます。プロセッサの動作とパフォーマンス レベルを変更することにより、プロセッサの消費電力と TDP を同時に調整できます。したがって、プロセッサは、使用可能な冷却容量と望ましい消費電力に応じて、パフォーマンス レベルが高いまたは低い方で動作します。次のいずれかになります。 • **[標準 (Normal)]** • **[レベル 1 (Level 1)]** • **[レベル 2 (Level 2)]** TDP レベルの値については、『Intell® Dear Customer Letter (DCL)』を参照してください。
[SpeedStep（Pstates）] ドロップダウンリスト	プロセッサで拡張版 Intel SpeedStep テクノロジーを使用するかどうか設定します。このテクノロジーでは、プロセッサの電圧やコア周波数をシステムが動的に調整できます。このテクノロジーにより、平均電力消費量と平均熱発生量が減少する可能性があります。次のいずれかになります。 • [Disabled]：プロセッサの電圧または周波数を動的に調整しません。 • [有効（Enabled）]：プロセッサで Enhanced Intel SpeedStep Technology が使用され、サポートされているすべてのスリープ状態でさらに電力を節約することが可能になります。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。 （注） [CPUPowerManagement] を [カスタム（Custom）] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。

名前	説明
[Processor CMCI] ドロップダウン リスト	CPU が corrected machine check events で割り込みをトリガーできるようにします。corrected machine check interrupt（CMCI）により、従来のポーリング タイマーよりも反応速度を向上できます。次のいずれかになります。 • [無効（Disabled）] : CMCI が無効になります。 • [有効（有効）] : CMCI が有効になります。これはデフォルト値です。
[HyperThreading [All]] ドロップダウン リスト	プロセッサでインテル ハイパースレッディング テクノロジーを使用するかどうか。このテクノロジーでは、マルチスレッド ソフトウェア アプリケーションのスレッドを各プロセッサ内で並列に実行できます。次のいずれかになります。 • [Disabled] : プロセッサでのハイパースレッディングを禁止します。 • [有効（Enabled）] : プロセッサでの複数スレッドの並列実行を許可します。
[Workload Configuration] ドロップダウン リスト	この機能を使用すると、ワークロードを最適化できます。オプションは [Balanced] と [I/O Sensitive] です。 • **[バランス（Balanced）]** • **[I/O 重視（IO Sensitive）]**

サーバー モデル別 BIOS パラメータ

名前	説明
[コアは有効化されました（Cores Enabled）] ドロップダウン リスト	サーバー上の 1 つ以上の物理コアを無効にできます。次のいずれかになります。 • [All]：すべての物理コアをイネーブルにします。 これにより、関連付けられている論理プロセッサ コアで Hyper Threading もイネーブルになります。 • **[1] ～ [48]**：サーバーで実行できる物理プロセッサ コアの数を指定します。各物理コアには、論理コアが関連付けられています。 （注） オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせください。
[UPI リンク周波数選択 (UPI Link Frequency Select)] ドロップダウン リスト	（注） **[UPI リンク周波数選択 (UPI Link Frequency Select)]** トークンは、単一ソケット構成には適用されません。 この機能を使用すると、複数のソケット間の Intel Ultra Path Interconnect (UPI) リンク速度を設定できます。次のいずれかになります。 • **[自動 (auto)]**]: このオプションは、最適なリンク速度を自動的に設定します。 • **[9.6 GT/s]**: このオプションは、最適なリンク速度として 9.6GT/s を使用します。 • **[10.4 GT/s]**—このオプションは、最適なリンク速度として 10.4GT/s を使用します。

名前	説明
[UPI プリフェッチ（UPI Prefetch）] ドロップダウン リスト	UPI プリフェッチは、DDR バス上でメモリ読み込みが早期に開始されるようにするメカニズムです。これは次のいずれかになります。 • [無効（disabled）][無効（Disabled）]：プロセッサでキャッシュデータをプリロードしません。 • [有効（enabled）][有効（Enabled）]：UPI プリフェッチャで最も関連性が高いと判断されたデータを含むL1キャッシュをプリロードします。 • **[自動（Auto）]**：CPU が UPI プリフェッチ モードを決定します。
[Sub NUMA Clustering] ドロップダウンリスト	CPUがサブNUMAクラスタリングをサポートするかどうか。そのクラスタリングでは、タグディレクトリとメモリ チャネルは常に同じ領域にあります。次のいずれかになります。 • [disabled][Disabled]：サブNUMA クラスタリングは発生しません。 • [enabled][Enabled]：サブNUMA クラスタリングが発生します。
[電力パフォーマンスの調整（Power Performance Tuning）] ドロップダウン リスト	BIOS またはOS によってエネルギー パフォーマンスのバイアス調整をオンにできるかどうかを指定します。オプションは [BIOS] と [OS] です。 • **[BIOS]**：エネルギー効率の調整のためにBIOS を選択します。 • **[OS]**：エネルギーパフォーマンスの調整にOSを選択します。 • **[OS]**：エネルギー パフォーマンス チューニング用のプラットフォーム環境制御インターフェースを選択します。

サーバー モデル別 BIOS パラメータ

名前	説明
[XPT Prefetch] ドロップダウン リスト	XPT プリフェッチを使用して、最後のレベルのキャッシュに読み取り要求を送信できるようにして、その要求のコピーをメモリ コントローラのプリフェッチャに発行するかどうか。次のいずれかになります。 • [disabled][Disabled]：CPUは XPT Prefetch オプションを使用しません。 • [enabled][Enabled]：CPUはXPTプリフェッチ オプションを有効にします。

名前	説明
[パッケージのCステート（Package C State）] ドロップダウン リスト	アイドル時にサーバー コンポーネントが使用できる電力量。次のいずれかになります。 • [no-limit][制限なし（No Limit）]：サーバーは、使用可能な任意のC ステートに入ることがあります。 • [自動（auto）][自動（Auto）]：物理的な高度をCPU が決定します。 • [C0 C1 ステート（C0 C1 State）]：サーバーはすべてのサーバー コンポーネントに常にフル パワーを提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • [C2]：CPU のアイドル時に、システムの電力消費をC1 オプションよりもさらに低減します。この場合、必要な電力はC1 またはC0 よりも少なくなりますが、サーバーがハイ パフォーマンス モードに戻るのに要する時間が少し長くなります。 • [C6 保持なし（C6 Non Retention）]：CPU のアイドル時に、C3 オプションよりもさらに電力消費が低減されます。このオプションを使用すると、C0、C1、またはC3 よりも電力量が節約されますが、サーバーがフルパワーに戻るまでにパフォーマンス上の問題が発生する可能性があります。 • [C6 保持（C6 Retention）]：CPU のアイドル時に、C3 オプションよりもさらに電力消費が低減されます。このオプションを使用すると、C0、C1、またはC3 よりも電力量が節約されますが、サーバーがフルパワーに戻るまでにパフォーマンス上の問題が発生する可能性があります。

サーバー モデル別 BIOS パラメータ

名前	説明
[エネルギー パフォーマンスのバイアス構成（Energy/Performance Bias Config）] ドロップダウン リスト	システム パフォーマンスまたはエネルギー効率がこのサーバーで重要かどうかを判断できます。次のいずれかになります。 • **[Performance]**— サーバではすべてのサーバ コンポーネントにフルパワーを常時提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • **[Balanced Performance]** — サーバはすべてのサーバ コンポーネントに、パフォーマンスとパワーのバランスを保つのに十分な電力を提供します。 • [バランス電力（Balanced Power）]：サーバーは、すべてのサーバー コンポーネントに、パフォーマンスと電力のバランスを保つのに十分な電力を提供します。 • [電力（Power）]：サーバーは、すべてのサーバー コンポーネントに、消費電力の低減を維持するのに最大の電力を提供します。
[ハードウェア P ステート（Hardware P-States）] ドロップダウン リスト	プロセッサ ハードウェアの P ステートを有効にします。次のいずれかになります。 • [disabled][Disabled]：HWPMがディセーブルになります。 • [hwpm-native-mode][HWPM Native Mode]：HWPMネイティブ モードがイネーブルになります。 • [hwpm-oob-mode][HWPM OOB Mode]：HWPMアウトオブボックス モードがイネーブルになります。 • [Native Mode with no Legacy]（GUI のみ）

名前	説明
[LLC Prefetch] ドロップダウン リスト	プロセッサがLLCプリフェッチ メカニズムを使用して日付を LLC にフェッチするかどうか。次のいずれかになります。 • [disabled][Disabled]：プロセッサでキャッシュデータをプリロードしません。 • [enabled][Enabled]：LLCPrefetcher で最も関連性が高いと判断されたデータを含む L1 キャッシュをプリロードします。
[自律コア C 状態（Autonomous Core C-state）] ドロップダウン リスト	HALT 命令を MWAIT 命令に変換する CPU Autonomous C-State を有効にします。次のいずれかになります。 • [Disabled]：CPU Autonomous C-state が無効です。 • [有効（Enabled）]：CPU 自律 C-state が有効になります。
[エネルギー効率ターボ（Energy Efficient Turbo）] ドロップダウンリスト	エネルギー効率の高いターボが有効になっている場合、CPUの最適なターボ周波数は、CPU使用率に基づいてダイナミックになります。パワー/パフォーマンスのバイアス設定も、エネルギー効率の高いターボに影響します。次のいずれかになります。 • **[無効（Disabled）]**：エネルギー効率ターボが無効です。 • **[有効（Enabled）]**：エネルギー効率ターボが有効です。

名前	説明
[パトロール スクラブ（Patrol Scrub）] ドロップダウンリスト	システムにサーバーのメモリ（未使用部分も含む）における単一ビット メモリ エラーを検出させて修復させることが可能です。次のいずれかになります。 • [Disabled]：CPU がメモリ アドレスの読み取りまたは書き込みを行うときのみ、システムはメモリの ECC エラーをチェックします。 • [有効（Enabled）]：システムは定期的にメモリを読み書きして ECC エラーを探します。エラーが見つかると、システムは修復を試みます。このオプションにより、単一ビット エラーは複数ビット エラーになる前に修正される場合がありますが、パトロール スクラブの実行時にパフォーマンスが低下する場合もあります。 • **[POST の最後に有効化する（Enable at End of POST）]**：システムは、BIOS POST 後にメモリ ECC エラーをチェックします。
[プロセッサ EPP プロファイル（Processor EPP Profile）] ドロップダウンリスト	システム パフォーマンスまたはエネルギー効率がこのサーバーで重要かどうかを判断できます。次のいずれかになります。 • Performance • Balanced Performance • Balanced Power • 電源

名前	説明
[Intel ダイナミック速度選択（Intel Dynamic Speed Select）] ドロップダウンリスト	**[Intel ダイナミック速度選択（Intel Dynamic Speed Select）]** モードでは、ユーザーは自動モードで異なる速度とコアを使用して CPU を動作させることができます。次のいずれかになります。 • **[無効（Disabled）]** : **[Intel ダイナミック速度選択（Intel Dynamic Speed Select）]** が無効になっています。 • **[有効（Enabled）]** : **[Intel ダイナミック速度選択（Intel Dynamic Speed Select）]** が有効になっています。
[Intel Speed Select (Intel の速度選択)] ドロップダウン リスト	**[Intel の速度選択（Intel Speed Select）]** モードでは、ユーザーは異なる速度とコアを使用して CPU を実行できます。 次のいずれかになります。 • **基本**): ユーザーは最大コアおよび熱設計電力 (TDP) 比率にアクセスすることができます。 • **設定 3** ユーザーは **基本**より小さいコアと TDP 比率にアクセスできます。 • **[構成 4（Config 4）]** : ユーザーは **[構成 3（Config 3）]** より小さいコアと TDP 比率にアクセスできます。 デフォルト値: **基本**。

C220 M6 および C240 M6 サーバー

I/O Tab

Note BIOS parameters listed in this tab may vary depending on the server.

サーバー モデル別 BIOS パラメータ

Table 33: BIOS Parameters in I/O Tab

Name	Description
Reboot Host Immediately check box	If the Reboot Host Immediately check box is checked, the server is rebooted immediately and the new BIOS settings go into effect. Otherwise the changes are saved until the server is manually rebooted.
MLOM OptionROM drop-down list	This options allows you to control the Option ROM execution of the PCIe adapter connected to the MLOM slot. This can be one of the following: • **Disabled**—Does not execute Option ROM of the PCIe adapter connected to the MLOM slot. • **Enabled**—Executes Option ROM of the PCIe adapter connected to the MLOM slot.
MLOM Link Speed drop-down list	This option allows you to restrict the maximum speed of an adapter card installed in PCIe MLOM slot. This can be one of the following: • **Disabled**—The maximum speed is not restricted. • **Auto**—System selects the maximum speed allowed. • **GEN1**—2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **GEN2**—5GT/s is the maximum speed allowed. • **GEN3**—8GT/s is the maximum speed allowed. • **GEN4**—16GT/s is the maximum speed allowed.
PCIe Slot*n* OptionROM drop-down list	Whether the server can use the Option ROMs present in the PCIe card slot designated by *n*. This can be one of the following: • **Disabled**—Option ROM for slot *n* is not available. • **Enabled**—Option ROM for slot *n* is available.

Name	Description
PCIe Slot*n* Link Speed drop-down list	System IO Controller *n* (SIOCn) add-on slot (designated by *n*) link speed. This can be one of the following: • **Disabled**—Slot is disabled, and the card is not enumerated. • **Auto**— The default link speed. Link speed is automatically assigned. • **GEN1**—Link speed can reach up to first generation. • **GEN2**—Link speed can reach up to second generation. • **GEN3**—Link speed can reach up to third generation.
Front NVME-*n* OptionROM drop-down list	This options allows you to control the Option ROM execution of the PCIe adapter connected to the SSD:NVMe slot *n*. This can be one of the following: • **Disabled**—Does not execute Option ROM of the PCIe adapter connected to the SSD:NVMe1 slot. • **Enabled**—Executes Option ROM of the PCIe adapter connected to the SSD:NVMe1 slot
Front NVME-*n* Link Speed drop-down list	Link speed for NVMe front slot designated by slot *n*. This can be one of the following: • **Disabled**—Slot is disabled, and the card is not enumerated. • **Auto**—The default link speed. Link speed is automatically assigned. • **GEN1**—Link speed can reach up to first generation. • **GEN2**—Link speed can reach up to second generation. • **GEN3**—Link speed can reach up to third generation. • **GEN4**—Link speed can reach up to fourth generation.

サーバー モデル別 BIOS パラメータ

Name	Description
Rear NVME-*n* OptionROM drop-down list	This options allows you to control the Option ROM execution of the PCIe adapter connected to the rear SSD:NVMe slot *n*. This can be one of the following: • **Disabled**—Does not execute Option ROM of the PCIe adapter connected to the SSD:NVMe1 slot. • **Enabled**—Executes Option ROM of the PCIe adapter connected to the SSD:NVMe1 slot
Rear NVME-*n* Link Speed drop-down list	Link speed for NVMe rear slot designated by slot *n*. This can be one of the following: • **Disabled**—Slot is disabled, and the card is not enumerated. • **Auto**—The default link speed. Link speed is automatically assigned. • **GEN1**—Link speed can reach up to first generation. • **GEN2**—Link speed can reach up to second generation. • **GEN3**—Link speed can reach up to third generation. • **GEN4**—Link speed can reach up to fourth generation.
Legacy USB Support drop-down list	Whether the system supports legacy USB devices. This can be one of the following: • **Disabled**—USB devices are only available to EFI applications. • **Enabled**—Legacy USB support is always available. • **Auto**—Feature is is automatically assigned.
PCIe Slot MSTOR RAID OptionROM drop-down list	Whether the server can use the Option ROMs present in the PCIe MSTOR RAID. This can be one of the following: • **Disabled**—Option ROM is not available. • **Enabled**—Option ROM is available.

Name	Description
Intel VTD Coherency Support drop-down list	Whether the processor supports Intel VT-d Coherency. This can be one of the following: • **Disabled**—The processor does not support coherency. • **Enabled**—The processor uses VT-d Coherency as required.
Intel VT for Directed IO drop-down list	Whether the processor uses Intel Virtualization Technology (VT), which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following: • **Disabled**—The processor does not permit virtualization. • **Enabled**—The processor allows multiple operating systems in independent partitions. **Note** If you change this option, you must power cycle the server before the setting takes effect.
VMD Enable drop-down list	Intel Volume Management Device (VMD) is for PCIe NVMe SSDs that provides hardware logic to manage and aggregate NVMe SSDs. This can be one the following: • **Enabled**— Enables benefits like robust surprise hot-plug, status LED management. • **Disabled**— Disables benefits like robust surprise hot-plug, status LED management. Default value: **Disabled**. Refer Intel® Virtual RAID on CPU User Guide and Intel® Virtual RAID on CPU (Intel® VROC) to configure VMD.

サーバー モデル別 BIOS パラメータ

Name	Description
	Details of VMD supported and unsupported ports for Cisco UCS C480 M5 servers: Cisco UCS C480 NVMe SKU (32 drive NVME System) • DMI connected ports 7, 8, and 23 do not support VMD. • All other twenty nine ports support VMD. Cisco UCS C480 Non-NVMe SKU • DMI connected ports 1, 2, and 18 do not support VMD. • Ports 7, 8, 9, 10, 15, 16, 17, 23, 24 support VMD.
Intel VTD ATS support drop-down list	Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following: • **Disabled**—The processor does not support ATS. • **Enabled**—The processor uses VT-d ATS as required.
LOM Port *n* OptionROM drop-down list	Whether Option ROM is available on the LOM port slot *n*. This can be one of the following: • **Disabled**—Option ROM is not available on LOM port 1. • **Enabled**—Option ROM is available on LOM port 1.
PCIe RAS Support drop-down list	Whether PCIe RAS Support is available on the PCIe slot. This can be one of the following: • **Disabled**—PCIe RAS is not available on the slot. • **Enabled**—PCIe RAS is available on port.
All Onboard LOM Ports drop-down list	Whether Option ROM is available on all LOM ports. This can be one of the following: • **Disabled**—Option ROM is disabled on all the ports. • **Enabled**—Option ROM is enabled on all the ports.

Name	Description
USB Port Rear drop-down list	Whether the rear panel USB devices are enabled or disabled. This can be one of the following • **Disabled**— Disables the rear panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled**— Enables the rear panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.
VGA Priority drop-down list	Allows you to set the priority for VGA graphics devices if multiple VGA devices are found in the system. This can be one of the following: • **OnBoard**—Priority is given to the onboard VGA device. BIOS post screen and OS boot are driven through the onboard VGA port. • **OffBoard**—Priority is given to the PCIE Graphics adapter. BIOS post screen and OS boot are driven through the external graphics adapter port. • **OnBoardDisabled**—Priority is given to the PCIe Graphics adapter, and the onboard VGA device is disabled. The vKVM does not function when the onboard VGA is disabled.
IPV6 PXE Support drop-down list	Enables or disables IPv6 support for PXE. This can be one of the following • **Disabled**—IPv6 PXE support is not available. • **Enabled**—IPv6 PXE support is always available.
USB Port Internal drop-down list	Whether the internal USB devices are enabled or disabled. This can be one of the following • **Disabled**— Disables the internal USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled**— Enables the internal USB ports. Devices connected to these ports are detected by the BIOS and operating system.

サーバー モデル別 BIOS パラメータ

Name	Description
PCIe PLL SSC drop-down list	Enable this feature to reduce EMI interference by down spreading clock 0.5%. Disable this feature to centralize the clock without spreading. This can be one of the following: • **Auto**—EMI interference is auto adjusted. **Disabled**—EMI interference is auto adjusted. • **ZeroPointFive**—EMI interference is reduced by down spreading the clock 0.5%.
Network Stack drop-down list	This option allows you to monitor IPv6 and IPv4. This can be one of the following • **Disabled**—Network Stack support is not available. **Note** When disabled, the value set for **IPV4 PXE Support** does not impact the system. • **Enabled**—Network Stack support is always available.
IPV4 PXE Support drop-down list	Enables or disables IPv4 support for PXE. This can be one of the following • **Disabled**—IPv4 PXE support is not available. • **Enabled**—IPv4 PXE support is always available.
External SSC enable drop-down list	This option allows you to reduce the EMI of your motherboard by modulating the signals it generates so that the spikes are reduced to flatter curves. This can be one of the following: • **Disabled**—Clock Spread Spectrum support is not available. • **Enabled**—Clock Spread Spectrum support is always available.
IPV4 HTTP Support drop-down list	Enables or disables IPv4 support for HTTP. This can be one of the following: • **Disabled**—IPv4 HTTP support is not available. • **Enabled**—IPv4 HTTP support is always available.

Name	Description
IIO eDPC Support drop-down list	eDPC allows a downstream link to be disabled after an uncorrectable error, making recovery possible in a controlled and robust manner. This can be one of the following: • Disabled—eDPC support is disabled. • On Fatal Error—eDPC is enabled only for fatal errors. • On Fatal and Non-Fatal Errors—eDPC is enabled for both fatal and non-fatal errors.
IPV6 HTTP Support drop-down list	Enables or disables IPv6 support for HTTP. This can be one of the following: • **Disabled**—IPv6 HTTP support is not available. • **Enabled**—IPv6 HTTP support is always available.

[Server Management] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *34 : [*サーバ管理（***Server Management***）*]* タブの ***BIOS*** パラメータ

名前	説明
[ホストを即座リブート（**Reboot Host Immediately**）**]** チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。

サーバー モデル別 BIOS パラメータ

名前	説明
[OS ブート ウォッチドッグ タイマー ポリシー（OS Boot Watchdog Timer Policy）] ドロップダウン リスト	ウォッチドッグ タイマーが切れた場合にシステムで実行されるアクション。次のいずれかになります。 • [電源オフ（Power Off）]：OS のブート中にウォッチドッグ タイマーの期限が切れた場合、サーバの電源がオフになります。 • [Reset]：OS のブート中にウォッチドッグ タイマーが切れた場合、サーバーはリセットされます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にする場合にのみ適用されます。
[FRB 2 タイマー（FRB 2 Timer）] ドロップダウン リスト	POST 中にシステムがハングした場合に、システムを回復するために Cisco IMC によって FRB2 タイマーが使用されるかどうか。次のいずれかになります。 • [無効（Disabled）]：FRB2 タイマーは使用されません。 • [Enabled]：POST 中に FRB2 タイマーが開始され、必要に応じてシステムの回復に使用されます。

名前	説明
[OS ウォッチドッグ タイマー（OS Watchdog Timer）] ドロップダウン リスト	BIOS が指定されたタイムアウト値でウォッチドッグ タイマーをプログラムするかどうか。次のいずれかになります。 • [Disabled]：サーバーのブートにかかる時間をトラッキングするためにウォッチドッグ タイマーは使用されません。 • [有効（enabled）]：サーバーがブートにかかる時間をウォッチドッグ タイマーで追跡します。サーバーのブートが [OS ブート ウォッチドッグ タイマー タイムアウト（OS Boot Watchdog Timer Timeout）] フィールドで指定された時間内に完了しない場合は、Cisco IMC によってエラーがログに記録され、[OS ブート ウォッチドッグ ポリシー（OS Boot Watchdog Policy）] フィールドで指定されたアクションが実行されます。
[OS ブート ウォッチドッグ タイマー タイムアウト（OS Watchdog Timer Timeout）] ドロップダウン リスト	OS が指定された時間内にブートしない場合、OS ウォッチドッグ タイマーの期限が切れ、システムはタイマーポリシーに基づいてアクションを実行します。次のいずれかになります。 • [5 分（5 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [10 分（10 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [15 分（15 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [20 分（20 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にした場合にのみ適用されます。

サーバー モデル別 BIOS パラメータ

名前	説明
[ボー レート（Baud Rate）] ドロップダウン リスト	シリアル ポートの伝送速度として使用されるボー レート。[コンソール リダイレクション（Console Redirection）] を無効にした場合、このオプションを使用できません。次のいずれかになります。 • [9.6k]：9,600 ボー レートが使用されます。 • [19.2k]：19,200 ボー レートが使用されます。 • [38.4k]：38,400 ボー レートが使用されます。 • [57.6k]：57,600 ボー レートが使用されます。 • [115.2k]：115,200 ボー レートが使用されます。 この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。
[フロー制御（Flow Control）] ドロップダウン リスト	フロー制御にハンドシェイク プロトコルを使用するかどうかを設定します。送信要求/クリア ツー セント（RTS/CTS）を使用すると、隠れた端末の問題が原因で発生する可能性がある、フレーム コリジョンを減らすことができます。次のいずれかになります。 • [なし（None）]：フロー制御は使用されません。 • [RTS/CTS]：RTS/CTS がフロー制御に使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。

名前	説明
[コンソール リダイレクション（Console Redirection）] ドロップダウン リスト	POST および BIOS のブート中に、シリアル ポートをコンソール リダイレクションで使用できるようにします。OS 起動後は、コンソールのリダイレクトが関係なくなります。次のいずれかになります。 • **[COM 0]**：POST 中にシリアル ポート A でコンソール リダイレクションを有効にします。 • **[COM 1]**：POST 中にシリアル ポート B でコンソール リダイレクションを有効にします。 • [Disabled]：POST 中にコンソール リダイレクションは発生しません。
[ターミナル タイプ（Terminal Type）] ドロップダウン リスト	コンソール リダイレクションに使用される文字フォーマットのタイプ。次のいずれかになります。 • [PC-ANSI]：PC-ANSI 端末フォントが使用されます。 • [VT100]：サポートされている VT100 ビデオ端末とその文字セットが使用されます。 • [VT100-PLUS]：サポートされている VT100-plus ビデオ端末とその文字セットが使用されます。 • [VT-UTF8]：UTF-8 文字セットのビデオ端末が使用されます。

名前	説明
[PCIe Slots CDN コントロール（PCIe Slots CDN Control）] ドロップダウンリスト	（注） このオプションは、スロット 2 または 5 に Mellanox カードを搭載した Cisco UCS C240 M6 サーバーでのみ使用できます。 イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [無効（Disabled）]：VIC カードに対する CDN サポートは無効です。 • [有効（Enabled）]：VIC カードの CDN サポートが有効になります。
[CDN コントロール（CDN Control）] ドロップダウン リスト	イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [無効（Disabled）]：VIC カードに対する CDN サポートは無効です。 • [有効（Enabled）]：VIC カードの CDN サポートが有効になります。
[OptionROM起動最適化（OptionROM Launch Optimization）]	このオプションが [有効（Enabled）] の場合、ブート順序のポリシーに存在するコントローラにのみ OptionROMs が起動されます。 （注） オンボードストレージコントローラ、Emulex FC アダプタおよび GPU コントローラなどのいくつかのコントローラについて、ブート順序のポリシーに含まれていなくても、OptionROM が起動されます。 このオプションが [無効（Disabled）] の場合、すべての OptionROMs が起動されます。 デフォルト値：[有効（Enabled）]

名前	説明
適応型メモリ トレーニング	このオプションを[有効（Enabled）]にすると、次のようになります。 メモリ トレーニングは毎回のブートでは実行されず、BIOSは、保存されたメモリ トレーニングの結果を毎回のリブートで使用します。 毎回のブートでメモリ トレーニングが実行されるいくつかの例外には、次のものがあります。 BIOS の更新、CMOS のリセット、CPU やメモリの設定変更、SPD または実行時の修正不可能なエラー、または、前回のブートから 24 時間以上経過している場合。 このオプションが [無効（Disabled）] の場合、毎回のブートでメモリ トレーニングが行われます。 デフォルト値：[有効（Enabled）]。 （注） [高速ブート（Fast Boot）] オプションを無効にするには、エンドユーザーは次のトークンを下記の説明のとおりに設定する必要があります。 [適応型メモリ トレーニング（Adaptive Memory Training）]を [無効（Disabled）] に [BIOS Techlogレベル（BIOS Techlog level）] を [標準（Normal）] に [OptionROM起動最適化（OptionROM Launch Optimization）] を [無効（Disabled）] に

名前	説明
[BIOS Techlogレベル（BIOS Techlog Level）]	このオプションは、**BIOS tech ログファイル**のメッセージのタイプを示します。 ログファイルには、次のタイプのいずれかを指定できます。 • [最小（Minimum）]：重要なメッセージがログファイルに表示されます。 • [標準（Normal）]：警告およびロードメッセージがログファイルに表示されます。 • [最大（Maximum）]：標準に加え、情報関連のメッセージがログファイルに表示されます。 デフォルト値：[最小（Minimum）] （注） このオプションは、主に、内部のデバッグを目としています。

[セキュリティ（Security）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *35 : [*セキュリティ管理（*Security Management*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[SHA-1 PCR バンク（SHA-1 PCR Bank）] ドロップダウンリスト	BIOS が測定を実行しているときに OS で使用可能な PCR バンクです。 • **[無効（Disabled）]**：SHA-1 PCR バンクは BIOS で使用できません。 • **[有効（Enabled）]**：SHA-1 PCR バンクは BIOS で使用できます。

名前	説明
[トラステッド プラットフォーム モジュール状態（Trusted Platform Module State）] ドロップダウンリスト	信頼されたプラットフォーム モジュール（TPM）は、主に暗号キーを使用する基本的なセキュリティ関連機能を提供するように設計されたマイクロチップです。このオプションを使用すると、システムの TPM セキュリティ デバイス サポートを制御できます。次のいずれかになります。 • [Disabled]：サーバーはTPMを使用しません。 • [有効（Enabled）]：サーバはTPMを使用します。 （注） オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせください。
[DMA 制御オプトイン フラグ（DMA Control Opt-In Flag）] ドロップダウンリスト	DMA 制御オプトイン フラグ：このトークンを有効にすると、オペレーティング システムは入出力メモリ管理ユニット（IOMMU）を有効にして、悪意のあるデバイスからの DMA 攻撃を防ぐことができます。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[TPM 保留中の操作（TPM Pending Operation）] ドロップダウンリスト	トラステッド プラットフォーム モジュール（TPM）Pending Operation オプションを使用すると、保留中の操作のステータスを制御できます。次のいずれかになります。 • [None]：アクションなし。 • TpmClear：保留中の操作をクリアします。

名前	説明
[SHA-256 PCR バンク（SHA-256 PCR Bank）] ドロップダウンリスト	BIOS が測定を実行しているときに OS で使用可能な PCR バンクです。 • **[無効（Disabled）]**：SHA256 PCR バンクは BIOS で使用できません。 • **[有効（Enabled）]**：SHA256 PCR バンクは BIOS で使用できます。
[電源オン パスワード（Power On Password）] ドロップダウン リスト	このトークンでは、F2 BIOS 設定を使用する前に BIOS パスワードを設定する必要があります。有効にすると、BIOS 関数（IO 設定、BIOS セットアップ、BIOS を使用したオペレーティング システムへのブート）にアクセスする前にパスワードの検証が必要になります。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[TPM の最小限の物理的存在（TPM Minimal Physical Presence）] ドロップダウンリスト	このトークンを使用すると、TPM に推奨される Microsoft のデフォルト設定を適用できます。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[Intel Trusted Execution Technology サポート（Intel Trusted Execution Technology Support）] ドロップダウン リスト	信頼されたプラットフォームモジュール(TPM)が 有効 である場合にのみ 有効 に設定できます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

名前	説明
[マルチキー トータル メモリ暗号化（Multikey Total Memory Encryption、MK-TME） ドロップダウンリスト	MK-TME を使用すると、独自のキーを持つ 1 つの暗号化ドメインを複数持つことができます。異なるメモリ ページを異なるキーで暗号化できます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[トータル メモリ暗号化（Total Memory Encryption、TME）] ドロップダウンリスト	システムの物理メモリ全体を暗号化する機能を提供します。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SGX 工場出荷時リセット（SGX Factory Reset）] ドロップダウンリスト	その後の起動時にシステムが SGX の工場出荷時リセットを実行できるようにします。これにより、すべての登録データが削除されます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SWガード拡張（SW Guard Extensions、SGX）] ドロップダウンリスト	ソフトウェア ガード拡張（SGX）機能を有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

名前	説明
[SGX QoS] ドロップダウンリスト	SGX QoS を有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SGX パッケージ情報インバンド アクセス（SGX Pkg info In-Band Access）] ドロップダウンリスト	SGX パッケージ情報インバンドアクセスを有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SGX 書き込み有効（SGX Write Enable）] ドロップダウンリスト	SGX 書き込み機能を有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[所有者 EPOCH入力タイプ選択（Select Owner EPOCH input type）] ドロップダウンリスト	作成され、ロックされたメモリ領域に使用されるセキュリティ キーのシードを変更できます。次のいずれかになります。 • **SGX 所有者 EPOCH 有効化（SGX Owner EPOCH activated）]**：現在の入力タイプを変更しません。 • **[新しいランダム所有者 EPOCH に変更（Change to New Random Owner EPOCHs）]**：EPOCH をシステムが生成したランダムな数値に変更します。 • **[手動ユーザー定義所有者 EPOCH（Manual User Defined Owner EPOCHs）]**：EPOCH シードをユーザーが入力した 16 進値に変更します。

名前	説明
[SProcessor Epoch*n*] フィールド	*n* で指定された EPOCH 番号の SGX EPOCH 所有者値を定義できます。
[SGX 自動 MP レジストレーション エージェント（SGX Auto MP Registration Agent）] ドロップダウンリスト	レジストレーション エージェント サービスがプラットフォーム キーを保存できるようにします。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SGX PUBKEY HASH*n*] フィールド	ソフトウェア ガード拡張（SGX）の値を設定できます。この値の設定範囲は、以下のとおりです。 • SGX PUBKEY HASH0 — 7 ～ 0 の間 • SGX PUBKEY HASH1 — 15 ～ 8 の間 • SGX PUBKEY HASH2 — 23 ～ 16 の間 • SGX PUBKEY HASH3 — 31 ～ 24 の間
[CPU PA を 46 ビットに制限（LIMIT CPU PA to 46 Bits）] ドロップダウンリスト	Intel ® VT-d でこのオプションを有効にして、2019 OS でブートできるようにします。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

メモリ タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

サーバー モデル別 BIOS パラメータ

表 *36 : [*メモリ（*Memory*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（**Reboot Host Immediately**）**]** チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。

名前	説明
[メモリ RAS 構成の選択（Select Memory RAS configuration）] ドロップダウン リスト	サーバーに対するメモリの信頼性、可用性、およびサービス性（RAS）の設定方法。次のいずれかになります。 • [最大パフォーマンス（Maximum Performance）]：システムのパフォーマンスが最適化されます。 • **ADDDC のスペアリング**: 適応可能な仮想ロックステップは、ADDDC モードをサポートするためにハードウェアおよびファームウェアで実装されるアルゴリズムです。選択すると、アルゴリズムがアクティブになるまでシステムのパフォーマンスが最適化されます。このアルゴリズムは、DRAM デバイスで障害が発生した場合にアクティブになります。アルゴリズムがアクティブになると、仮想ロックステップ リージョンがアクティブになり、実行時に障害が発生したリージョンが動的にマッピングされ、パフォーマンスへの影響はリージョン レベルで制限されます。 • [ミラー モード 1LM（Mirror Mode 1LM）]：システムのメモリの半分をバックアップとして使用することにより、システムの信頼性が最適化されます。 • **部分的なミラー モード 1LM**: 部分的な DIMM ミラーリングによって完全なミラーコピーを保持するのではなく、メモリ セルの特定の領域のミラーコピーが作成されます。部分的なミラーリングでは、部分的なミラー コピーの属性を使用して、メモリ マップにミラー領域が作成されます。最大 4 個の部分的なミラーを使用して、合計メモリ容量の最大 50% をミラーリングできます。

サーバー モデル別 BIOS パラメータ

名前	説明
[NUMA] ドロップダウン リスト	BIOS で Non-Uniform Memory Access（NUMA）がサポートされているかどうか。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[パーシャル キャッシュ ライン スペアリング（Partial Cache Line Sparing）] ドロップダウン リスト	パーシャル キャッシュ ライン スペアリング (PCLS) は、メモリ コントローラーのエラー防止メカニズムです。PCLS は、メモリ アクセス中に置換できるように、ビットの欠陥のあるニブルの場所を、対応するデータ コンテンツとともにスペア ディレクトリに静的にエンコードします。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[ディスク タイプの選択 (Select Disk Type)] ドロップダウン リスト	Cisco IMC は、指定された障害のある行から指定されたスペア行へのアクセスを永続的に再マッピングする、**ハード PPR**をサポートしています。 次のいずれかになります。 • **[ハード PPR (Hard PPR)]**: サポートは有効になっています。 （注） ハード PPR は、**[メモリ RAS 設定 (Memory RAS Configuration)]**が **[ADDDC スペア (ADDDC Sparing)]**に設定されている場合にのみ使用できます。他の RA の選択では、この設定を **Disabled** に設定する必要があります。 • **[無効 (Disabled)]**：サポートは無効になっています。

名前	説明
[BME DMA 移行 (BME DMA Mitigation)] ドロップダウン リスト	不正な外部 DMA からの脅威を緩和する PCI BME ビットを無効にできます。次のいずれかになります。 • **[無効 (disabled)]**: PCI BME ビットは BIOS で無効になっています。 • **[有効 (Enabled)**: PCI BME ビットは BIOS で有効になっています。
[4 G 以上の復号化（Above 4G Decoding）] ドロップダウン リスト	4 GB 以上の MMIO を有効または無効にします。次のいずれかになります。 • [Disabled]：サーバーでは 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングしません。 • [有効（Enabled）]：サーバで 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングします。 （注） PCI デバイスが 64 ビット対応でも、レガシーなオプション ROM を使用する場合は、この設定をイネーブルにしても正しく機能しない場合があります。
[Partial Memory Mirror Mode (部分メモリ ミラー モード)]ドロップダウン リスト	部分的なメモリ サイズは、パーセンテージまたは GB 単位のいずれかです。次のいずれかになります。 • **割合**: 部分的なメモリのミラーはパーセンテージで定義されます。 • **値 (GB)**: 部分的なメモリ ミラーは GB で定義されます。 • **無効**: 部分的なメモリ ミラーが無効になります。

サーバー モデル別 BIOS パラメータ

名前	説明
[DCPMM Firmware Downgrade (DCPMM ファームウェアのダウングレード)] ドロップダウン リスト	BIOS が DCPMM ファームウェアのダウングレードをサポートしているかどうか。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[部分ミラー *n* サイズ（GB）（Partial Mirror n Size in GB）] フィールド	最初の部分 *nth* メモリ ミラーのサイズ（GB）。 n = 1、2、または 3 0 ～ 65535 の整数を入力します。 （注） すべての部分的なミラーの合計メモリ サイズは、物理メモリ サイズの 50% を超えないようにする必要があります。
[部分的なミラー パーセンテージ (Partial Mirror percentage)] フィールド	4GB を超えてミラーリングするメモリの割合。 0 ～ 60 の整数を入力します。
[メモリ サイズ制限 (GB) (Memory Size Limit in GB)] フィールド	このオプションを使用して、物理メモリの上限のサイズを GB 単位で減らします。 0 ～ 65535 の整数を入力します。
[NVM パフォーマンス設定 (NVM Performance Setting)] ドロップダウンリスト	ワークロードの動作に応じて、NVM ベースラインのパフォーマンス設定を設定できます。 • **BW 最適化** • **遅延の最適化** • **バランス プロファイル**
[CR QoS] ドロップダウンリスト	CR QoS 調整を選択できます。 次のいずれかになります。 • **[モード 1（Mode 1）]**： • **[モード 2（Mode 2）]**： • **[モード 0（Mode 0）]**：**[CR QoS]** 機能は無効です。

名前	説明
[AD の Snoopy モード (Snoopy mode for AD)] ドロップダウン リスト	新しい AD 固有の機能を有効にして、NUMA に最適化されていないワークロードからDDRT メモリへのディレクトリ更新を回避します。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[CR Fastgo Config] ドロップダウンリスト	CR QoS 設定プロファイルを選択できるようにします。 次のいずれかになります。 • **[最適化の有効化（Enable Optimization）]** • **[最適化の無効化（Disable Optimization）]** • **Auto**
[メモリ リフレッシュ レート（Memory Refresh Rate）] ドロップダウンリスト	メモリのリフレッシュ レートを増減できます。DRAM のリフレッシュ レートを上げると、次のリフレッシュの前に発生する可能性のあるアクティブ化（ハンマー）の最大数が減少します。 次のいずれかになります。 • **[1X リフレッシュ（1X Refresh）]**：リフレッシュ レートは最小です。 • **[2X リフレッシュ（2X Refresh）]**：リフレッシュは 2 倍高速です。
[2LM の Snoopy モード (Snoopy mode for 2LM)] ドロップダウン リスト	NUMA に最適化されていないワークロードから far メモリへのディレクトリ更新を回避できます。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

サーバー モデル別 BIOS パラメータ

名前	説明
[メモリ サーマル スロットリング モード（Memory Thermal Throttling Mode）] ドロップダウンリスト	この関数は、メモリ温度の調整に使用されます。この機能を有効にした後、メモリ温度が極端に高くなると、メモリアクセスレートが低下し、Baseboard Management Controller（BMC）がファンを調整してメモリを冷却し、DIMM の損傷を防ぎます。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • **PECI を使用した CLTT**：プラットフォーム環境制御インターフェイスを使用してクローズドループ サーマル スロットリングを有効にします。
[パニックと高水準点（Panic and High Watermark）] ドロップダウン リスト	低に設定した場合、**[メモリ更新レート（Memory Refresh Rate）]** が **[1X リフレッシュ（1X Refresh）]** に設定されている間、メモリコントローラは更新を延期しません。 次のいずれかになります。 • **[低（Low）]**：リフレッシュ レートは低に設定します。 • **[高（High）]**：リフレッシュ レートは高に設定します。
[UMA] ドロップダウン リスト	UMA 設定を設定できます。次のいずれかになります。 • Disable(All2All) • Hemisphere(2-clusters)

名前	説明
[高度なメモリ テスト（Advanced Memory Test）] ドロップダウン リスト	（注） この機能は、Samsung、Hynix、および Micron DIMM にのみ適用されます。 この機能を使用して、BIOS POST 中に高度な DIMM テストを有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[eADR サポート（eADR Support）] ドロップダウン リスト	拡張非同期 DRAM リフレッシュ（eADR）のサポートにより、CPU キャッシュに格納されているデータを永続メモリに移動するためのキャッシュ フラッシュ コマンドの待機期間を回避できます。これによりパフォーマンスが向上します。次のいずれかになります。 • **Disabled** • **有効化** • **Auto**
[揮発性メモリ モード（Volatile Memory Mode）] ドロップダウン リスト	揮発性メモリ モードの設定は、BIOS が Intel® Optane™ PMem をサポートしている場合に表示されます。次のいずれかになります。 • **[1LM]**：このオプションは、Intel® Optane™ PMem を App-Direct モードで設定するために使用できます。 • **[2LM]**：このオプションにより、2LM は DDR4 メモリをキャッシュとして動作させることができます。

名前	説明
[メモリ帯域幅ブースト（Memory Bandwidth Boost）] ドロップダウン リスト	Intel® メモリ帯域幅ブーストは、Intel® Optane™ パーシステント メモリの機能であり、サーマル ヘッドルームが利用可能な場合に、ダイナミック レンジの電力と帯域幅を提供します。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

[電源/パフォーマンス（Power/Performance）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *37 : [*電源/パフォーマンス（*Power/Performance*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[隣接キャッシュ ライン プリフェッチャ（Adjacent Cache Line Prefetcher）] ドロップダウン リスト	プロセッサで必要な行のみを取得するのではなく、偶数または奇数のペアのキャッシュ行を取得するかどうか。次のいずれかになります。 • [Disabled]：プロセッサで必要な行のみを取得します。 • [Enabled]：プロセッサで必要な行およびペアの行の両方を取得します。

名前	説明
[ハードウェア プリフェッチャ（Hardware Prefetcher）] ドロップダウン リスト	プロセッサで、インテル ハードウェア プリフェッチャが必要に応じてデータおよび命令ストリームをメモリから取得し、統合 2 次キャッシュに入れることを許可するかどうか。次のいずれかになります。 • [Disabled]：ハードウェア プリフェッチャは使用しません。 • [Enabled]：プロセッサで、キャッシュの問題が検出されたときにプリフェッチャを使用します。
[DCU IP プリフェッチャ（DCU IP Prefetcher）] ドロップダウン リスト	プロセッサで DCU IP プリフェッチ メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。次のいずれかになります。 • [Disabled]：プロセッサでキャッシュ データをプリロードしません。 • [Enabled]：DCU IP プリフェッチャで最も関連性が高いと判断されたデータを含む L1 キャッシュをプリロードします。
[DCU ストリーマ プリフェッチ（DCU Streamer Prefetch）] ドロップダウン リスト	プロセッサで DCU IP プリフェッチ メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。次のいずれかになります。 • [Disabled]：プロセッサはキャッシュ読み取り要求を予測しようとせず、明示的に要求された行のみを取得します。 • [Enabled]：DCU Prefetcher でキャッシュ読み取りパターンを分析し、必要と判断した場合にキャッシュ内の次の行を事前に取得します。

名前	説明
[仮想 Numa（Virtual Numa）] ドロップダウン リスト	仮想 NUMA（仮想非均一メモリ アクセス）は、VMware 仮想マシン（VM）のメモリ アクセス最適化方法であり、メモリ帯域幅のボトルネックを防ぐのに役立ちます。 次のいずれかになります。 • **[無効（Disabled）]** — 機能は無効です。 • **[有効（Enabled）]** — 機能は有効です。
[CPU パフォーマンス（CPU Performance）] ドロップダウン リスト	上記のオプションに対し CPU パフォーマンス プロファイルを設定します。次のいずれかになります。 • [Enterprise]：すべてのオプションがイネーブルです。 • [HPC]：すべてのオプションがイネーブルです。この設定はハイ パフォーマンス コンピューティングとも呼ばれます。 • [高スループット（Hight Throughput）]：DCU IP Prefetcher のみが有効です。残りのオプションは無効になります。 • [Custom]：パフォーマンス プロファイルのすべてのオプションをサーバの BIOS セットアップから設定できます。また、[ハードウェア プリフェッチャ（Hardware Prefetcher）] オプションと [隣接キャッシュ ライン プリフェッチャ（Adjacent Cache Line Prefetcher）] オプションも同様に設定できます。

名前	説明
[LLC デッド ライン（LLC Dead Line）] ドロップダウン リスト	CPU の非包括的キャッシュ スキームでは、MLC から削除された内容が LLC に書き込まれます。行を MLC から削除する際、コアはそれらに **[デッド（dead）]** としてフラグを立てることがあります（再度読み取られる可能性が小さい場合）。LLC には、デッド ラインを削除し、LLC に書き込まないオプションがあります。 この機能が無効の場合、デッド ラインは常に削除されます。LLC に書き込まれることはありません。 この機能が有効の場合、使用可能な空きスペースがある場合にデッドラインを LLC に書き込むことを LLC に許可します。 次のいずれかになります。 • **[無効（Disabled）]** — 機能は無効です。 • **[有効（Enabled）]** — 機能は有効です。 • **[自動（Auto）]** — CPU が LLC のデッド ラインの割り当てを決定します。
[XPT リモート プリフェッチ（XPT Remote Prefetch） ドロップダウン リスト	この機能は、LLC 要求を複製し、最近の LLC 履歴に基づいてリモート マシンの適切なメモリ コントローラに送信して、待ち時間を減らします。 次のいずれかになります。 • **[無効（Disabled）]** — 機能は無効です。 • **[有効（Enabled）]** — 機能は有効です。 • **[自動（Auto）]** — CPU が機能を決定します。
[UPI リンク有効化（UPI Link Enablement）] ドロップダウン リスト	プロセッサが必要とする最小数の UPI リンクを有効にします。 次のいずれかになります。 • **1** • **2** • **Auto**

名前	説明
[強化 CPU パフォーマンス（Enhanced CPU Performance）] ドロップダウン リスト	（注） この機能を有効にすると、**[電源特性の有効化（Enable Power Characterization）]**および**[パワーキャッピング（Power Capping）]**を有効にすることはできません。 サーバー設定を自動的に調整することにより、CPU パフォーマンスを向上させます。 （注） この機能を有効にすると、消費電力が増加する可能性があります。 この機能を使用するには、サーバーが次の要件を満たしている必要があります。 • サーバーが、Barlow Pass DIMM を使用していないこと • Cisco UCS C220 M6 サーバーの DIMM モジュール サイズは 64 GB 未満であり、Cisco UCS C240 M6 サーバーでは 256 GB 未満であること • サーバーにGPUカードが搭載されていないこと。 次のいずれかになります。 • **[無効（Disabled）]** — プロセッサでこの機能を使用しません。 • **[自動（Auto）]** — Cisco IMC がサーバー設定を調整して、パフォーマンスを向上させることができます。
[C1 自動降格（C1 Auto Demotion）] ドロップダウン リスト	有効にすると、CPU は非コア自動降格情報に基づいて C1 状態に自動的に降格します。 • **[無効（Disabled）]**：プロセッサでこの機能を使用しません。 • **[有効（Enabled）]**：機能は有効です。

名前	説明
[UPI 電力管理（UPI Power Manangement）] ドロップダウン リスト	UPI 電力管理は、サーバーの電力を節約するために使用されます。 次のいずれかになります。 • **[無効（Disabled）]** — プロセッサでこの機能を使用しません。 • **[自動（Auto）]** — 機能は有効です。
[C1 自動降格解除（C1 Auto UnDemotion）] ドロップダウン リスト	プロセッサが C1 降格状態から自動的に解除できるようにするかどうかを選択します。 • **[無効（Disabled）]** — プロセッサでこの機能を使用しません。 • **[有効（Enabled）]** — 機能は有効です。

[プロセッサ（Processor）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *38 : [プロセッサ（Processor）] タブの BIOS パラメータ*

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[拡張 APIC（Extended APIC）] ドロップダウンリスト	拡張 APIC サポートをイネーブルまたはディセーブルにできます。次のいずれかになります。 • 有効：APIC サポートを有効にします • [無効（Disabled）]：APIC サポートを無効にします。

サーバー モデル別 BIOS パラメータ

名前	説明
[Intel Virtualization Technology] ドロップダウン リスト	プロセッサで Intel Virtualization Technology（VT）を使用するかどうか。このテクノロジーでは、1つのプラットフォームで、複数のオペレーティング システムとアプリケーションをそれぞれ独立したパーティション内で実行できます。次のいずれかになります。 • [Disabled]：プロセッサでの仮想化を禁止します。 • [有効（Enabled）]：プロセッサで、複数のオペレーティング システムをそれぞれ独立したパーティション内で実行できます。
[プロセッサ C6 レポート（Processor C6 Report）] ドロップダウン リスト	BIOS からオペレーティング システムに C6 レポートを送信するかどうか。OS はレポートを受信すると、プロセッサを電力量の少ない C6 状態に移行してエネルギー使用量を減らし、最適なプロセッサ パフォーマンスを維持できます。次のいずれかになります。 • [Disabled]：BIOS から C6 レポートを送信しません。 • [Enabled]：BIOS から C6 レポートを送信し、OS がプロセッサを電力量の少ない C6 状態に移行できるようにします。 （注） [CPUPowerManagement] を [カスタム（Custom）] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。 （注） このオプションを使用できるのは一部の C シリーズ サーバーだけです。

名前	説明
[プロセッサ C1E（Processor C1E）] ドロップダウン リスト	C1 ステートに入ったときに、CPU が最小周波数に移行するかどうか。次のいずれかになります。 • [無効（Disabled）]：CPU は C1 ステートでも引き続き最大周波数で動作します。 • [有効（Enabled）]：CPU は最小周波数に移行します。このオプションでは C1 ステートで節約される電力量が最大になります。 （注） このオプションを使用できるのは一部の C シリーズ サーバーだけです。
[EIST PSD 関数（EIST PSD Function）] ドロップダウンリスト	EIST は、電圧と周波数のペア（P 状態）の変更に固有の遅延を短縮するため、これらの遷移がより頻繁に発生するようになります。これにより、より詳細なデマンドベースのスイッチングが可能になり、アプリケーションの要求に基づいて電力とパフォーマンスのバランスを最適化できます。次のいずれかになります。 • **[HW ALL]**：プロセッサは、論理プロセッサの依存関係間の P 状態を調整します。OS は、すべての論理プロセッサで P-state 要求を最新の状態に保ちます。 • **[SW ALL]**：OS Power Manager によって、依存関係にある論理プロセッサ間の P-state を調整します。すべての論理プロセッサで遷移を開始します。

名前	説明
[ターボ モード（Turbo Mode）] ドロップダウンリスト	プロセッサでインテル ターボ ブースト テクノロジーを使用するかどうか。このテクノロジーでは、仕様よりも低い電力、温度、または電圧でプロセッサが動作していると、自動的にそのプロセッサの周波数が上がります。次のいずれかになります。 • [Disabled]：プロセッサの周波数は自動的には上がりません。 • [Enabled]：必要に応じてプロセッサで Turbo Boost Technology が利用されます。 （注） [CPUPowerManagement] を [カスタム（Custom）] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[非コア周波数スケーリング (Uncore Frequency Scaling)] ドロップダウンリスト	この機能を使用すると、プロセッサのコア以外の周波数のスケーリングを設定できます。次のいずれかになります。 • **[Enabled]**：プロセッサの非コア部分の周波数を、負荷に応じて上下します。 • **[無効 (Disabled)]**: プロセッサのコア以外の周波数を固定します。 『Intel® Dear Customer Letter (DCL)』には、固定されていない場合の **[非コア周波数スケーリング (Uncore Frequency Scaling)]** の固定の上限値と下限値が記されています。
[ブート パフォーマンス モード（Boot Performance Mode）] ドロップダウン リスト	オペレーティング システムのハンドオフ前に設定される BIOS パフォーマンス状態を選択できます。次のいずれかになります。 • [Max Performance]：プロセッサの P-state 率は最大です • **[最大効率（Max Efficient）]**：プロセッサの P-state の比率が最小です。 • **[Intel NM による設定（Set by Intel NM）]**：値は自動的に設定されます。

名前	説明
[TDP の設定（Config TDP）]ドロップダウンリスト	**[TDP の設定（Config TDP）]**機能により、プロセッサの温度設計の電力値を調整できます。プロセッサの動作とパフォーマンス レベルを変更することにより、プロセッサの消費電力と TDP を同時に調整できます。したがって、プロセッサは、使用可能な冷却容量と望ましい消費電力に応じて、パフォーマンス レベルが高いまたは低い方で動作します。次のいずれかになります。 • **[標準 (Normal)]** • **[レベル 1 (Level 1)]** • **[レベル 2 (Level 2)]** TDP レベルの値については、『Intell® Dear Customer Letter (DCL)』を参照してください。
[SpeedStep（Pstates）] ドロップダウンリスト	プロセッサで拡張版 Intel SpeedStep テクノロジーを使用するかどうか設定します。このテクノロジーでは、プロセッサの電圧やコア周波数をシステムが動的に調整できます。このテクノロジーにより、平均電力消費量と平均熱発生量が減少する可能性があります。次のいずれかになります。 • [Disabled]：プロセッサの電圧または周波数を動的に調整しません。 • [有効（Enabled）]：プロセッサで Enhanced Intel SpeedStep Technology が使用され、サポートされているすべてのスリープ状態でさらに電力を節約することが可能になります。 オペレーティングシステムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。 （注） [CPUPowerManagement] を [カスタム（Custom）] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。

サーバー モデル別 BIOS パラメータ

名前	説明
[Processor CMCI] ドロップダウン リスト	CPU が corrected machine check events で割り込みをトリガーできるようにします。corrected machine check interrupt（CMCI）により、従来のポーリング タイマーよりも反応速度を向上できます。次のいずれかになります。 • [無効（Disabled）]：CMCI が無効になります。 • [有効（有効）]：CMCI が有効になります。これはデフォルト値です。
[HyperThreading [All]] ドロップダウン リスト	プロセッサでインテル ハイパースレッディング テクノロジーを使用するかどうか。このテクノロジーでは、マルチスレッド ソフトウェア アプリケーションのスレッドを各プロセッサ内で並列に実行できます。次のいずれかになります。 • [Disabled]：プロセッサでのハイパースレッディングを禁止します。 • [有効（Enabled）]：プロセッサでの複数スレッドの並列実行を許可します。
[Workload Configuration] ドロップダウン リスト	この機能を使用すると、ワークロードを最適化できます。オプションは [Balanced] と [I/O Sensitive] です。 • **[バランス（Balanced）]** • **[I/O 重視（IO Sensitive）]**

名前	説明
[コアは有効化されました（Cores Enabled）] ドロップダウン リスト	サーバー上の 1 つ以上の物理コアを無効にできます。次のいずれかになります。 • [All]：すべての物理コアをイネーブルにします。 これにより、関連付けられている論理プロセッサ コアで Hyper Threading もイネーブルになります。 • **[1] ～ [48]**：サーバーで実行できる物理プロセッサ コアの数を指定します。各物理コアには、論理コアが関連付けられています。 （注） オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせください。
[UPI リンク周波数選択 (UPI Link Frequency Select)] ドロップダウン リスト	（注） **[UPI リンク周波数選択 (UPI Link Frequency Select)]** トークンは、単一ソケット構成には適用されません。 この機能を使用すると、複数のソケット間の Intel Ultra Path Interconnect (UPI) リンク速度を設定できます。次のいずれかになります。 • **[自動 (auto)]**]: このオプションは、最適なリンク速度を自動的に設定します。 • **[9.6 GT/s]**: このオプションは、最適なリンク速度として 9.6GT/s を使用します。 • **[10.4 GT/s]**—このオプションは、最適なリンク速度として 10.4GT/s を使用します。

サーバー モデル別 BIOS パラメータ

名前	説明
[UPI プリフェッチ（UPI Prefetch）] ドロップダウン リスト	UPI プリフェッチは、DDR バス上でメモリ読み込みが早期に開始されるようにするメカニズムです。これは次のいずれかになります。 • [無効（disabled）][無効（Disabled）]：プロセッサでキャッシュデータをプリロードしません。 • [有効（enabled）][有効（Enabled）]：UPI プリフェッチャで最も関連性が高いと判断されたデータを含むL1キャッシュをプリロードします。 • **[自動（Auto）]**：CPU が UPI プリフェッチ モードを決定します。
[Sub NUMA Clustering] ドロップダウンリスト	CPUがサブNUMAクラスタリングをサポートするかどうか。そのクラスタリングでは、タグディレクトリとメモリ チャネルは常に同じ領域にあります。次のいずれかになります。 • [disabled][Disabled]：サブNUMAクラスタリングは発生しません。 • [enabled][Enabled]：サブNUMA クラスタリングが発生します。
[電力パフォーマンスの調整（Power Performance Tuning）] ドロップダウン リスト	BIOS またはOS によってエネルギー パフォーマンスのバイアス調整をオンにできるかどうかを指定します。オプションは[BIOS] と [OS] です。 • **[BIOS]**：エネルギー効率の調整のためにBIOS を選択します。 • **[OS]**：エネルギーパフォーマンスの調整にOSを選択します。 • **[OS]**：エネルギー パフォーマンス チューニング用のプラットフォーム環境制御インターフェースを選択します。

名前	説明
[XPT Prefetch] ドロップダウン リスト	XPT プリフェッチを使用して、最後のレベルのキャッシュに読み取り要求を送信できるようにして、その要求のコピーをメモリ コントローラのプリフェッチャに発行するかどうか。次のいずれかになります。 • [disabled][Disabled]：CPUは XPT Prefetch オプションを使用しません。 • [enabled][Enabled]：CPUはXPTプリフェッチ オプションを有効にします。

サーバー モデル別 BIOS パラメータ

名前	説明
[パッケージのCステート（Package C State）] ドロップダウン リスト	アイドル時にサーバー コンポーネントが使用できる電力量。次のいずれかになります。 • [no-limit][制限なし（No Limit）]：サーバーは、使用可能な任意のC ステートに入ることがあります。 • [自動（auto）][自動（Auto）]：物理的な高度をCPU が決定します。 • [C0 C1 ステート（C0 C1 State）]：サーバーはすべてのサーバー コンポーネントに常にフル パワーを提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • [C2]：CPU のアイドル時に、システムの電力消費をC1 オプションよりもさらに低減します。この場合、必要な電力はC1 または C0 よりも少なくなりますが、サーバーがハイ パフォーマンス モードに戻るのに要する時間が少し長くなります。 • [C6 保持なし（C6 Non Retention）]：CPU のアイドル時に、C3 オプションよりもさらに電力消費が低減されます。このオプションを使用すると、C0、C1、またはC3 よりも電力量が節約されますが、サーバーがフルパワーに戻るまでにパフォーマンス上の問題が発生する可能性があります。 • [C6 保持（C6 Retention）]：CPU のアイドル時に、C3 オプションよりもさらに電力消費が低減されます。このオプションを使用すると、C0、C1、または C3 よりも電力量が節約されますが、サーバーがフルパワーに戻るまでにパフォーマンス上の問題が発生する可能性があります。

名前	説明
[エネルギー パフォーマンスのバイアス構成（Energy/Performance Bias Config）] ドロップダウン リスト	システム パフォーマンスまたはエネルギー効率がこのサーバーで重要かどうかを判断できます。次のいずれかになります。 • **[Performance]** — サーバではすべてのサーバ コンポーネントにフルパワーを常時提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • **[Balanced Performance]** — サーバはすべてのサーバ コンポーネントに、パフォーマンスとパワーのバランスを保つのに十分な電力を提供します。 • [バランス電力（Balanced Power）]：サーバーは、すべてのサーバー コンポーネントに、パフォーマンスと電力のバランスを保つのに十分な電力を提供します。 • [電力（Power）]：サーバーは、すべてのサーバー コンポーネントに、消費電力の低減を維持するのに最大の電力を提供します。
[ハードウェア P ステート（Hardware P-States）] ドロップダウン リスト	プロセッサ ハードウェアの P ステートを有効にします。次のいずれかになります。 • [disabled][Disabled]：HWPMがディセーブルになります。 • [hwpm-native-mode][HWPM Native Mode]：HWPMネイティブ モードがイネーブルになります。 • [hwpm-oob-mode][HWPM OOB Mode]：HWPMアウトオブボックス モードがイネーブルになります。 • [Native Mode with no Legacy]（GUI のみ）

サーバー モデル別 BIOS パラメータ

名前	説明
[LLC Prefetch] ドロップダウン リスト	プロセッサがLLCプリフェッチメカニズムを使用して日付を LLC にフェッチするかどうか。次のいずれかになります。 • [disabled][Disabled]：プロセッサでキャッシュデータをプリロードしません。 • [enabled][Enabled]：LLCPrefetcher で最も関連性が高いと判断されたデータを含む L1 キャッシュをプリロードします。
[自律コア C 状態（Autonomous Core C-state）] ドロップダウン リスト	HALT 命令を MWAIT 命令に変換する CPU Autonomous C-State を有効にします。次のいずれかになります。 • [Disabled]：CPU Autonomous C-state が無効です。 • [有効（Enabled）]：CPU 自律 C-state が有効になります。
[エネルギー効率ターボ（Energy Efficient Turbo）] ドロップダウンリスト	エネルギー効率の高いターボが有効になっている場合、CPUの最適なターボ周波数は、CPU使用率に基づいてダイナミックになります。パワー/パフォーマンスのバイアス設定も、エネルギー効率の高いターボに影響します。次のいずれかになります。 • **[無効（Disabled）]**：エネルギー効率ターボが無効です。 • **[有効（Enabled）]**：エネルギー効率ターボが有効です。

名前	説明
[パトロール スクラブ（Patrol Scrub）] ドロップダウンリスト	システムにサーバーのメモリ（未使用部分も含む）における単一ビット メモリ エラーを検出させて修復させることが可能です。次のいずれかになります。 • [Disabled]：CPU がメモリ アドレスの読み取りまたは書き込みを行うときのみ、システムはメモリの ECC エラーをチェックします。 • [有効（Enabled）]：システムは定期的にメモリを読み書きして ECC エラーを探します。エラーが見つかると、システムは修復を試みます。このオプションにより、単一ビット エラーは複数ビット エラーになる前に修正される場合がありますが、パトロール スクラブの実行時にパフォーマンスが低下する場合もあります。 • **[POST の最後に有効化する（Enable at End of POST）]**：システムは、BIOS POST 後にメモリ ECC エラーをチェックします。
[プロセッサ EPP プロファイル（Processor EPP Profile）] ドロップダウンリスト	システム パフォーマンスまたはエネルギー効率がこのサーバーで重要かどうかを判断できます。次のいずれかになります。 • Performance • Balanced Performance • Balanced Power • 電源

名前	説明
[Intel ダイナミック速度選択（Intel Dynamic Speed Select）] ドロップダウンリスト	**[Intel ダイナミック速度選択（Intel Dynamic Speed Select）]** モードでは、ユーザーは自動モードで異なる速度とコアを使用して CPU を動作させることができます。次のいずれかになります。 • **[無効（Disabled）]** : **[Intel ダイナミック速度選択（Intel Dynamic Speed Select）]** が無効になっています。 • **[有効（Enabled）]** : **[Intel ダイナミック速度選択（Intel Dynamic Speed Select）]** が有効になっています。
[Intel Speed Select (Intel の速度選択)] ドロップダウン リスト	**[Intel の速度選択（Intel Speed Select）]** モードでは、ユーザーは異なる速度とコアを使用して CPU を実行できます。 次のいずれかになります。 • **基本)**: ユーザーは最大コアおよび熱設計電力 (TDP) 比率にアクセスすることができます。 • **設定 3** ユーザーは **基本**より小さいコアと TDP 比率にアクセスできます。 • **[構成 4（Config 4）]** : ユーザーは **[構成 3（Config 3）]** より小さいコアと TDP 比率にアクセスできます。 デフォルト値: **基本**。

C225 M6 および C245 M6 サーバー

[I/O] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *39 : [I/O]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[MLOM OptionROM] ドロップダウン リスト	このオプションでは、MLOM スロットに接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • [無効（Disabled）] : MLOM スロットに接続されている PCIe アダプタのオプション ROM を実行しません。 • [有効（Enabled）] : MLOM スロットに接続されている PCIe アダプタのオプション ROM を実行します。
[MLOM リンク速度（MLOM Link Speed）] ドロップダウン リスト	このオプションを使用すると、PCIe MLOM スロットに装着されているアダプタ カードの最大速度を制限できます。次のいずれかになります。 • [無効（Disabled）] : 最大スピードは制限されていません。 • [自動（Auto）] : システムは許可される最大速度を選択します。 • [GEN1] : 最大 2.5 GT/s（ギガトランスファー/秒）までの速度が許可されます。 • [GEN2] : 最大 5 GT/s までの速度が許可されます。 • [GEN3] : 最大 8 GT/s までの速度が許可されます。 • **[GEN3]** : 最大 16GT/s までの速度が許可されます。

サーバー モデル別 BIOS パラメータ

名前	説明
[PCIe Slot*n* OptionROM] ドロップダウン リスト	サーバーが *n* で指定した PCIe カード スロットにあるオプション ROM を使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：スロット *n* のオプションの ROM は使用できません。 • [有効（Enabled）]：スロット *n* のオプション ROM は使用可能です。
[PCIe スロット *n* リンク速度（PCIe Slot n Link Speed）] ドロップダウン リスト	システム IO コントローラ *n*（SIOCn）アドオン スロット（*n* によって示される）のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効となり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。 • **[GEN4]**：リンク速度は第 4 世代まで到達可能です。
MRAID OptionROM	サーバーが *n* で指定された PCIe カード スロット内の RAID オプションの ROM を使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：スロット *n* のオプションの ROM は使用できません。 • [有効（Enabled）]：スロット *n* のオプション ROM は使用可能です。

名前	説明
[MRAID リンク速度（MRAID Link Speed）] ドロップダウン リスト	RAID IO コントローラ *n*（SIOCn）アドオン スロット（*n*によって指定）のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効となり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。 • **[GEN4]**：リンク速度は第 4 世代まで到達可能です。
[前面 NVME-*n* OptionROM（Front NVME-n OptionROM）] ドロップダウン リスト	このオプションでは、SSD:NVMe スロット*n*に接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • [無効（Disabled）]：SSD:NVMe1 スロットに接続されている PCIe アダプタのオプションの ROM を実行しません。 • [有効（Enabled）]：SSD:NVMe1 スロットに接続されている PCIe アダプタのオプション ROM を実行します

名前	説明
[前面 NVME *n*リンク速度（Front NVME n Link Speed）] [ドロップダウン リスト（drop-down list）]	スロット *n* で指定された NVMe 前面スロットのリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効となり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。 • **[GEN4]**：リンク速度は第 4 世代まで到達可能です。
[背面 NVME-*n* OptionROM（Rear NVME-n OptionROM）] ドロップダウンリスト	（注） このオプションは、Cisco UCS C245 M6 サーバーにのみ適用されます。 このオプションでは、SSD:NVMe スロット*n*に接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • [無効（Disabled）]：SSD:NVMe1 スロットに接続されている PCIe アダプタのオプションの ROM を実行しません。 • [有効（Enabled）]：SSD:NVMe1 スロットに接続されている PCIe アダプタのオプション ROM を実行します

名前	説明
Rear NVME *n* Link Speed [ドロップダウンリスト（drop-down list）]	（注） このオプションは、Cisco UCS C245 M6 サーバーにのみ適用されます。 スロット *n* で指定された NVMe 前面スロットのリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効となり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。 • **[GEN4]**：リンク速度は第 4 世代まで到達可能です。
[PCIe スロット MSTOR RAID OptionROM (PCIe Slot MSTOR RAID OptionROM)] ドロップダウン リスト	サーバが PCIe MSTOR RAID のオプション ROM を使用するかどうか。次のいずれかになります。 • Disabled：オプション ROM は使用できません。 • [Enabled]—オプション ROM は使用できます。

名前	説明
[PCIe Slot MSTOR リンク速度（PCIe Slot MSTOR Link Speed）] ドロップダウンリスト	スロット *n* で指定された PCIe 前面スロットのリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効となり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。 • **[GEN4]**：リンク速度は第 4 世代まで到達可能です。
[IPV6 PXE サポート（IPV6 PXE Support）] ドロップダウン リスト	PXE の IPv6 サポートを有効または無効にします。次のいずれかになります • **[無効(Disabled)]** : PV6 PXE のサポートは利用できません。 • **[Enabled (有効)]**:IPV6 PXE のサポートを常に利用できます。
[IPV4 PXE サポート (IPV4 PXE Support)] ドロップダウン リスト	PXE の IPv4 サポートを有効または無効にします。次のいずれかになります • **[無効(Disabled)]**: IPV4 PXE のサポートは利用できません。 • **[Enabled (有効)]**: IPV4 PXE のサポートを常に利用できます。

名前	説明
[PCIe ARI サポート (PCIe ARI Support)] ドロップダウン リスト	Windows での PCI 代替ルーティング ID 解釈（ARI）サポートが有効になっているかどうか。次のいずれかになります。 • **[自動（Auto）]**：ARI サポートは、システムによって自動制御されるように設定されます。 • **Disabled**：ARI サポートは使用できません。 • **Enabled**：ARI サポートを常に使用できます。
[SR-IOVサポート（SR-IOV Support）] ドロップダウン リスト	SR-IOV 機能により、PCIe デバイスは複数の個別の物理 PCIe デバイスのように見えます。次のいずれかになります。 • **[無効（Disabled）]**：SR-IOV 機能は無効です。 • **[有効（Enabled）]**：SR-IOV 機能は有効です。
[IPv6 HTTP サポート（IPv6 HTTP Support）] ドロップダウン リスト	HTTP の IPv6 サポートを有効または無効にします。次のいずれかになります。 • **[無効（Disabled）]**：IPv6 HTTP サポートは使用できません。 • **[有効（Enabled）]**：IPv6 HTTP サポートを常に使用できます。
[IPV4 HTTP サポート（IPV4 HTTP Support）] ドロップダウン リスト	HTTP の IPv4 サポートを有効または無効にします。次のいずれかになります。 • **[無効（Disabled）]**：IPv4 HTTP サポートは使用できません。 • **[有効（Enabled）]**：IPv4 HTTP サポートを常に使用できます。

名前	説明
[Network Stack (ネットワーク スタック)] ドロップダウン リスト	このオプションでは、IPv6 と IPv4 をモニタできます。次のいずれかになります • **[無効 (Disabled)]**: ネットワーク スタックのサポートは使用できません。 （注） 無効にすると、**IPV4 PXE サポート**に設定された値はシステムに影響しません。 • **[Enabled (有効)]**: ネットワーク スタックのサポートを常に利用できます。

[Server Management] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *40 : [*サーバ管理（*Server Management*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[OS ブート ウォッチドッグ タイマー ポリシー（OS Boot Watchdog Timer Policy）] ドロップダウン リスト	ウォッチドッグ タイマーが切れた場合にシステムで実行されるアクション。次のいずれかになります。 • [電源オフ（Power Off）]：OS のブート中にウォッチドッグ タイマーの期限が切れた場合、サーバの電源がオフになります。 • [Reset]：OS のブート中にウォッチドッグ タイマーが切れた場合、サーバーはリセットされます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にする場合にのみ適用されます。

名前	説明
[FRB 2 タイマー（FRB 2 Timer）] ドロップダウン リスト	POST 中にシステムがハングした場合に、システムを回復するために Cisco IMC によって FRB2 タイマーが使用されるかどうか。次のいずれかになります。 • [無効（Disabled）]：FRB2 タイマーは使用されません。 • [Enabled]：POST 中に FRB2 タイマーが開始され、必要に応じてシステムの回復に使用されます。
[OS ウォッチドッグ タイマー（OS Watchdog Timer）] ドロップダウン リスト	BIOS が指定されたタイムアウト値でウォッチドッグ タイマーをプログラムするかどうか。次のいずれかになります。 • [Disabled]：サーバーのブートにかかる時間をトラッキングするためにウォッチドッグ タイマーは使用されません。 • [有効（enabled）]：サーバーがブートにかかる時間をウォッチドッグ タイマーで追跡します。サーバーのブートが [OS ブート ウォッチドッグ タイマー タイムアウト（OS Boot Watchdog Timer Timeout）] フィールドで指定された時間内に完了しない場合は、Cisco IMC によってエラーがログに記録され、[OS ブート ウォッチドッグ ポリシー（OS Boot Watchdog Policy）] フィールドで指定されたアクションが実行されます。

名前	説明
[OS ブート ウォッチドッグ タイマー タイムアウト（OS Watchdog Timer Timeout）] ドロップダウン リスト	OS が指定された時間内にブートしない場合、OS ウォッチドッグ タイマーの期限が切れ、システムはタイマーポリシーに基づいてアクションを実行します。次のいずれかになります。 • [5 分（5 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [10 分（10 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [15 分（15 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [20 分（20 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にした場合にのみ適用されます。

名前	説明
[ボー レート（Baud Rate）] ドロップダウン リスト	シリアル ポートの伝送速度として使用されるボー レート。[コンソール リダイレクション（Console Redirection）] を無効にした場合、このオプションを使用できません。次のいずれかになります。 • [9.6k]：9,600 ボー レートが使用されます。 • [19.2k]：19,200 ボー レートが使用されます。 • [38.4k]：38,400 ボー レートが使用されます。 • [57.6k]：57,600 ボー レートが使用されます。 • [115.2k]：115,200 ボー レートが使用されます。 この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。
[フロー制御（Flow Control）] ドロップダウン リスト	フロー制御にハンドシェイク プロトコルを使用するかどうかを設定します。送信要求/クリア ツー セント（RTS/CTS）を使用すると、隠れた端末の問題が原因で発生する可能性がある、フレーム コリジョンを減らすことができます。次のいずれかになります。 • [なし（None）]：フロー制御は使用されません。 • [RTS/CTS]：RTS/CTS がフロー制御に使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。

サーバー モデル別 BIOS パラメータ

名前	説明
[コンソール リダイレクション（Console Redirection）] ドロップダウン リスト	POST および BIOS のブート中に、シリアル ポートをコンソール リダイレクションで使用できるようにします。OS 起動後は、コンソールのリダイレクトが関係なくなります。次のいずれかになります。 • **[COM 0]**：POST 中に COM 1 でコンソール リダイレクションを有効にします。 • **[COM 1]**：POST 中に COM 1 でコンソール リダイレクションを有効にします。 • [Disabled]：POST 中にコンソール リダイレクションは発生しません。
[ターミナル タイプ（Terminal Type）] ドロップダウン リスト	コンソール リダイレクションに使用される文字フォーマットのタイプ。次のいずれかになります。 • [PC-ANSI]：PC-ANSI 端末フォントが使用されます。 • [VT100]：サポートされている VT100 ビデオ端末とその文字セットが使用されます。 • [VT100-PLUS]：サポートされている VT100-plus ビデオ端末とその文字セットが使用されます。 • [VT-UTF8]：UTF-8 文字セットのビデオ端末が使用されます。

名前	説明
[PCIe Slots CDN コントロール（PCIe Slots CDN Control）] ドロップダウンリスト	（注） このオプションは、スロット 2 または 5 に Mellanox カードを搭載した Cisco UCS C245 M6 サーバーでのみ使用できます。 イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [無効（Disabled）]：VIC カードに対する CDN サポートは無効です。 • [有効（Enabled）]：VIC カードの CDN サポートが有効になります。
[CDN コントロール（CDN Control）] ドロップダウン リスト	イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [無効（Disabled）]：VIC カードに対する CDN サポートは無効です。 • [有効（Enabled）]：VIC カードの CDN サポートが有効になります。
[OptionROM起動最適化（OptionROM Launch Optimization）]	このオプションが [有効（Enabled）] の場合、ブート順序のポリシーに存在するコントローラにのみ OptionROMs が起動されます。 （注） オンボードストレージコントローラ、Emulex FC アダプタおよび GPU コントローラなどのいくつかのコントローラについて、ブート順序のポリシーに含まれていなくても、OptionROM が起動されます。 このオプションが [無効（Disabled）] の場合、すべての OptionROMs が起動されます。

名前	説明
[BIOS Techlogレベル（BIOS Techlog Level）]	このオプションは、**BIOS tech ログファイル**のメッセージのタイプを示します。 ログファイルには、次のタイプのいずれかを指定できます。 • [最小（Minimum）]：重要なメッセージがログファイルに表示されます。 • [標準（Normal）]：警告およびロードメッセージがログファイルに表示されます。 • [最大（Maximum）]：標準に加え、情報関連のメッセージがログファイルに表示されます。 デフォルト値：[最小（Minimum）] （注） このオプションは、主に、内部のデバッグを目としています。

[セキュリティ（Security）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *41 : [*セキュリティ管理（*Security Management*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。

名前	説明
[トラステッド プラットフォーム モジュール状態（Trusted Platform Module State）] ドロップダウンリスト	信頼されたプラットフォーム モジュール（TPM）は、主に暗号キーを使用する基本的なセキュリティ関連機能を提供するように設計されたマイクロチップです。このオプションを使用すると、システムの TPM セキュリティ デバイス サポートを制御できます。次のいずれかになります。 • [Disabled]：サーバーはTPMを使用しません。 • [有効（Enabled）]：サーバはTPMを使用します。 （注） オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせください。
[SHA-1 PCR バンク（SHA-1 PCR Bank）] ドロップダウンリスト	SHA-1 PCRバンクを有効または無効にします。次のいずれかになります。 • **[無効（Disabled）]**：サーバーはこの機能を使用しません。 • **[有効（Enabled）]**：サーバーはこの機能を使用します。
[SHA-256 PCR バンク（SHA-256 PCR Bank）] ドロップダウンリスト	SHA256 PCR バンクを有効または無効にします。次のいずれかになります。 • **[無効（Disabled）]**：サーバーはこの機能を使用しません。 • **[有効（Enabled）]**：サーバーはこの機能を使用します。

名前	説明
[電源オン パスワード（Power On Password）] ドロップダウン リスト	このトークンでは、F2 BIOS 設定を使用する前にBIOSパスワードを設定する必要があります。有効にすると、BIOS関数（IO設定、BIOSセットアップ、BIOSを使用したオペレーティング システムへのブート）にアクセスする前にパスワードの検証が必要になります。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

メモリ タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *42 : [*メモリ（*Memory*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（**Reboot Host Immediately**）**]** チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しいBIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。

名前	説明
[ソケットごとのNUMAノード（NUMA Nodes per Socket）] ドロップダウンリスト	ソケットごとにメモリNUMAドメインを構成できます。次のいずれかになります。 • **[自動（Auto）]**：チャネル数を自動に設定します。 • **[NPS0]**：システムごとのNUMAノード数を1にします。 • **[NPS1]**：ソケットごとのNUMAノード数を1にします。 • **[NPS2]**：ソケットごとのNUMAノード数を2にし、SoCの左半分と右半分に1つずつにします。 • **[NPS4]**：ソケットごとのNUMAノード数を4にし、クワドラントごとに1つにします。
[4 G以上の復号化（Above 4G Decoding）] ドロップダウン リスト	4 GB以上のMMIOを有効または無効にします。次のいずれかになります。 • [Disabled]：サーバーでは64ビットPCIデバイスのI/Oを4 GB以上のアドレス空間にマッピングしません。 • [有効（Enabled）]：サーバで64ビットPCIデバイスのI/Oを4 GB以上のアドレス空間にマッピングします。 （注） PCIデバイスが64ビット対応でも、レガシーなオプションROMを使用する場合は、この設定をイネーブルにしても正しく機能しない場合があります。

サーバー モデル別 BIOS パラメータ

名前	説明
[Chipselect Interleaving] ドロップダウンリスト	ノード 0 に選択する DRAM チップ経由でメモリブロックがインターリーブされるかどうか。次のいずれかになります。 • **[無効（Disabled）]**：チップの選択は、メモリ コントローラ内でインターリーブされません。 • **[自動（Auto）]**：CPU でチップ セレクトのインタリーブの方法を自動的に決定します。
[メモリ インターリービング サイズ（Memory Interleaving Size）] ドロップダウンリスト	インターリーブされるメモリ ブロックのサイズを決定します。また、インターリーブの開始アドレス（ビット 8、9、10、11）も指定します。次のいずれかになります。 • **Auto** • **256 バイト** • **512 バイト** • **1 KB** • **2 KB** • **4 KB**
[IOMMU] ドロップダウンリスト	出入力メモリ管理ユニット（IOMMU） により、AMDプロセッサが物理アドレスへ仮想アドレスをマッピングすることが可能です。次のいずれかになります。 • **[自動（Auto）]**：これらのアドレスのマッピング方法を CPU で決定します。 • **[無効（Disabled）]**：IOMMU は使用されません。 • **[有効（Enabled）]**：IOMMU によりアドレスマッピングを行います。

名前	説明
BankGroupSwap	物理アドレスをアプリケーションに割り当てる方法を決定します。次のいずれかになります。 • **[自動（Auto）]**：アプリケーションへの物理アドレスの割り当て方法を CPU で自動的に決定します。 • **[無効（Disabled）]**：バンク グループ スワップは使用されません。 • **[有効（Enabled）]**：バンク グループ スワップによりアプリケーションのパフォーマンスを向上させます。
[TSME] ドロップダウンリスト	透過的セキュア メモリ暗号化（TSME）を有効にすることができます。次のいずれかになります。 • **[自動（Auto）]**：機能の使用は自動に設定されます。 • **[無効（Disabled）]**：プロセッサで TSME 機能を使用しません。 • **[有効（Enabled）]**：プロセッサで TSME 機能を使用します。
[SMEE] ドロップダウンリスト	プロセッサで、メモリの暗号化サポートを実現する Secure Memory Encryption Enable（SMEE）機能を使用するかどうかを指定します。次のいずれかになります。 • **[自動（Auto）]**：これらのアドレスのマッピング方法を CPU で決定します。 • **[無効（Disabled）]**：プロセッサで SMEE 機能を使用しません。 • **[有効（Enabled）]**：プロセッサで SMEE 機能を使用します。

名前	説明
[SNP メモリ カバレッジ（SNP Memory Coverage）] ドロップダウンリスト	SNP メモリ カバレッジを設定できます。次のいずれかになります。 • **[自動（Auto）]**：システムがメモリ カバレッジを決定します。 • **[無効（Disabled）]**：プロセッサはこの機能を使用しません。 • **[有効（Enabled）]**：この機能は有効です。 • **[カスタム（Custom）]**：カスタム サイズは、**[カバーする SNP メモリ サイズ（SNP Memory Size to Cover）]** で定義できます。
[SEV-SNP サポート（SEV-SNP Support）] ドロップダウン リスト	セキュア ネスティッド ページング機能を有効にできます。次のいずれかになります。 • **[無効（Disabled）]**：プロセッサで SEV-SNP 機能を使用しません。 • **[有効（Enabled）]**：プロセッサで SEV-SNP 機能を使用します。
[BME DMA 移行 (BME DMA Mitigation)] ドロップダウン リスト	不正な外部 DMA からの脅威を緩和する PCI BME ビットを無効にできます。次のいずれかになります。 • **[無効 (disabled)]**: PCI BME ビットは BIOS で無効になっています。 • **[有効 (Enabled)**: PCI BME ビットは BIOS で有効になっています。
[カバーされる SNP メモリ サイズ（MB）（SNP Memory Size to Cover in MB）] フィールド	SNP メモリ サイズを設定できます。
バーストおよび遅延された更新（Burst and Postponed Refresh）] フィールド	• **[無効（Disabled）]**：プロセッサはこの機能を使用しません。 • **[有効（Enabled）]**：プロセッサはこの機能を使用します。

名前	説明
[パッケージ修復のポスト（Post Package Repair）] フィールド	Cisco IMC は、指定された障害のある行から指定されたスペア行へのアクセスを永続的に再マッピングする、ハード PPR をサポートしています。次のいずれかになります。 • **[ハード PPR (Hard PPR)]**: サポートは有効になっています。 • [Disabled]：サポートはディセーブルになっています。

[電源/パフォーマンス（Power/Performance）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *43 : [*電源/パフォーマンス（*Power/Performance*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[Core Performance Boost] ドロップダウンリスト	AMD プロセッサがアイドル状態（ほとんど使用されていない状態）のときにコアの周波数を上げるかどうかを指定します。次のいずれかになります。 • **[Auto]**：パフォーマンスをブーストする方法を CPU で自動的に決定します。 • **[Disabled]**：CPU により自動的にブーストパフォーマンスが決定されます。

名前	説明
[Global C-state Control] ドロップダウンリスト	AMD プロセッサが IO ベースの C ステートおよびDF Cステートを制御するかどうかに関係なく、これは次のうちいずれかになります。 • **[Auto]**：CPU で IO ベースの C ステートの生成方法を自動的に決定します。 • **[Disabled]**：グローバル C ステートの制御が無効になります。 • **[Enabled]**：グローバル C ステートの制御が有効になります。
[L1 Stream HW Prefetcher] ドロップダウンリスト	プロセッサで、AMDハードウェアプリフェッチャが必要に応じてデータおよび命令ストリームをメモリから取得し、L1 キャッシュに入れることを許可するかどうか。次のいずれかになります。 • [auto][Auto]：CPUは、I/Oデバイスからプロセッサ キャッシュにデータを配置する方法を決定します。 • [disabled][Disabled]：ハードウェア プリフェッチャは使用しません。 • [enabled][Enabled]：プロセッサで、キャッシュの問題が検出されたときにハードウェアプリフェッチャを使用します。
[L2 Stream HW Prefetcher] ドロップダウンリスト	プロセッサで、AMDハードウェアプリフェッチャが必要に応じてメモリからデータおよび命令ストリームを取得し、L2 キャッシュに入れることを許可するかどうかを指定します。次のいずれかになります。 • [auto][Auto]：CPUは、I/Oデバイスからプロセッサ キャッシュにデータを配置する方法を決定します。 • [disabled][Disabled]：ハードウェア プリフェッチャは使用しません。 • [enabled][Enabled]：プロセッサで、キャッシュの問題が検出されたときにハードウェアプリフェッチャを使用します。

名前	説明
[Determinism Slider] ドロップダウンリスト	AMDプロセッサにより動作方法を決定できます。次のいずれかになります。 • **[Auto[**：CPU はデフォルトの決定論的な電源設定を自動で使用します。 • **[Performance]**：プロセッサは、最適なパフォーマンスかつ一貫した方法で動作します。 • **[Power]**：プロセッサは、ダイごとに許容される最大のパフォーマンスで動作します。
[CPPC] ドロップダウンリスト	コラボレーティブ プロセッサ パフォーマンス制御を設定できます。 次のいずれかになります。 • **自動**：CPU はデフォルトの CPPC 設定を自動で使用します。 • **無効**：機能は無効です。 • **有効**：コラボレーティブ プロセッサ パフォーマンスが有効になっています。
[効率モードの有効（Efficiency Mode Enable）] ドロップダウン リスト	効率に基づいて消費電力を設定できます。 次のいずれかになります。 • **自動**：CPU はデフォルトの設定を自動で使用します。 • **有効**：効率モードは有効です。

[プロセッサ（Processor）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

サーバー モデル別 BIOS パラメータ

表 *44 : [*プロセッサ（*Processor*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（**Reboot Host Immediately**）**]** チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[SVM Mode] ドロップダウンリスト	プロセッサが AMD セキュア仮想マシン テクノロジを使用するかどうか。次のいずれかを選択できます。 • **[Disabled]**：プロセッサで SVM テクノロジーを使用しません。 • **[Enabled]**：プロセッサで SVM テクノロジーを使用します。
[SMT Mode] ドロップダウンリスト	プロセッサで AMD Simultaneous MultiThreading テクノロジーを使用するかどうかを指定します。このテクノロジーでは、マルチスレッド ソフトウェア アプリケーションのスレッドを各プロセッサ内で並列に実行できます。次のいずれかになります。 • **[Auto]**：プロセッサは、マルチスレッドの並列実行を許可します。 • **[**無効（**Disabled**）**]**：プロセッサで SMT モードを使用しません。 • **[**有効（**Enabled**）**]**：プロセッサで SMT モードを使用します。

名前	説明
[ダウンコア制御 7xx2（Downcore control 7xx2）] ドロップダウンリスト	（注） このトークンは、7xx2 モデルのプロセッサを搭載した Tehama サーバーにのみ適用されます。 1 つ以上のコアの動作を停止する機能を提供します。シリコン回路でサポートされています。OS の制限、またはシステムの電力削減要件により、コア数を減らすことが望ましい場合があります。この項目により、実行中のコアの数を制御できます。この設定では、プロセッサで使用可能なコアの数を減らすことしかできません。次のいずれかになります。 • **[Auto]**：有効化する必要のあるコアの数を CPU で判断します。 • TWO（1+1）：片方の CPU コンプレックスで 2 つのコアを有効にします。 • FOUR（2+2）：1 つの CPU コンプレックスで 4 つのコアを有効にします。 • SIX（3+3）：1 つの CPU コンプレックスで 6 つのコアを有効にします。

名前	説明
[CPU ダウンコア制御 7xx3（CPU Downcore control 7xx3） ドロップダウンリスト	（注） このトークンは、7xx3 モデルのプロセッサを搭載した Tehama サーバーにのみ適用されます。 1つ以上のコアの動作を停止する機能を提供します。シリコン回路でサポートされています。OS の制限、またはシステムの電力削減要件により、コア数を減らすことが望ましい場合があります。この項目により、実行中のコアの数を制御できます。この設定では、プロセッサで使用可能なコアの数を減らすことしかできません。次のいずれかになります。 • **[Auto]**：有効化する必要のあるコアの数を CPU で判断します。 • One（1+0）：1 つの CPU コンプレックスで 1 つのコアを有効にします。 • [TWO（2+0）]：片方の CPU コンプレックスのみで 2 つのコアを有効にします。 • [THREE（3+0）]：片方の CPU コンプレックスのみで 3 つのコアを有効にします。 • [FOUR（4+0）]：片方の CPU コンプレックスのみで 4 つのコアを有効にします。 • Five（5+0）：1 つの CPU コンプレックスで 5 つのコアを有効にします。 • SIX（6+0）：1 つの CPU コンプレックスで 6 つのコアを有効にします。 • SEVEN（7+0）：1 つの CPU コンプレックスで 7 つのコアを有効にします。

名前	説明
[固定 SOC P ステート（Fixed SOC P-State）] ドロップダウンリスト	このオプションは、APBDIS が設定されている場合のターゲット PState を定義します。**P*x***：取り付けられているプロセッサの有効な P ステートを指定します。次のいずれかになります。 • P0 • P1 • P2 • P3 • 自動（Auto）
[APBDIS] ドロップダウンリスト	SMU の APB 無効化の値を選択できます。次のいずれかになります。 • **0**：SMU への ApbDis をクリアします。 • **[1]**：SMU への ApbDis を設定します。 • **[自動（Auto）]**：CPU が値を判断します。
[CCD 制御（CCD Control）] ドロップダウンリスト	システムで有効にしたい CCD の数を指定できます。次のいずれかになります。 • **[自動（Auto）]**：プロセッサによって提供される最大数の CCD が有効になります。 • 2 CCD • 3 CCD • 4 CCD • 6 CCD
[Cisco xGMI 最大速度（Cisco xGMI Max Speed）] ドロップダウンリスト	このオプションは、18 Gbps XGMI リンク速度を有効にします。次のいずれかになります。 • **[無効（Disabled）]**：機能は無効です。 • **[有効（Enabled）]** — 機能は有効です。

名前	説明
[NUMAドメインとしての ACPI SRAT L3 キャッシュ（ACPI SRAT L3 Cache As NUMA Domain）] ドロップダウンリスト	各 CCX がそのオン ドメインにあると宣言されている物理ドメインの上に仮想ドメインのレイヤーを作成します。次のいずれかになります。 • **[自動（Auto）]**：自動モードに設定します。 • **[無効（Disabled）]**：ドメイン構成に NPS 設定を使用します。 • **[有効（Enabled）]**：各 CCX を独自のドメインにあると宣言します。
[ストリーミング ストア制御（Streaming Stores Control）] ドロップダウンリスト	ストリーミング ストア機能を有効にします。次のいずれかになります。 • **[自動（Auto）]**：自動モードに設定します。 • **[無効（Disabled）]**：機能は無効です。 • **[有効（Enabled）]** — 機能は有効です。
[DF C ステート（DF C-States）] ドロップダウンリスト	システムで長時間のアイドル状態が予想される場合、この制御により、システムは、システムをさらに低電力状態に設定できる DF C ステートに移行できます。次のいずれかになります。 • **[自動（Auto）]**：自動モードに設定します。 • **[無効（Disabled）]**：長時間のアイドル状態は予想されないため、省電力は実現されません。 • **[有効（Enabled）]**：このオプションはアクティブです。システムがアイドル状態のときに電力を節約します。

C125 サーバの場合

[Server Management] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

表 *45 : [*サーバ管理（*Server Management*）*]* タブの *BIOS* パラメータ

名前	説明
[Reboot Host Immediately] チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[OS ブート ウォッチドッグ タイマー ポリシー（OS Boot Watchdog Timer Policy）] ドロップダウン リスト	ウォッチドッグ タイマーが切れた場合にシステムで実行されるアクション。次のいずれかになります。 • [電源オフ（Power Off）] : OS のブート中にウォッチドッグ タイマーの期限が切れた場合、サーバの電源がオフになります。 • [Reset] : OS のブート中にウォッチドッグ タイマーが切れた場合、サーバーはリセットされます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にする場合にのみ適用されます。

サーバー モデル別 BIOS パラメータ

名前	説明
[OS ウォッチドッグ タイマー（OS Watchdog Timer）] ドロップダウン リスト	BIOS が指定されたタイムアウト値でウォッチドッグ タイマーをプログラムするかどうか。次のいずれかになります。 • [Disabled]：サーバーのブートにかかる時間をトラッキングするためにウォッチドッグ タイマーは使用されません。 • [有効（enabled）]：サーバーがブートにかかる時間をウォッチドッグ タイマーで追跡します。サーバーのブートが [OS ブート ウォッチドッグ タイマー タイムアウト（OS Boot Watchdog Timer Timeout）] フィールドで指定された時間内に完了しない場合は、Cisco IMC によってエラーがログに記録され、[OS ブート ウォッチドッグ ポリシー（OS Boot Watchdog Policy）] フィールドで指定されたアクションが実行されます。
[ボー レート（Baud Rate）] ドロップダウン リスト	シリアル ポートの伝送速度として使用されるボー レート。[コンソール リダイレクション（Console Redirection）] を無効にした場合、このオプションを使用できません。次のいずれかになります。 • [9.6k]：9,600 ボー レートが使用されます。 • [19.2k]：19,200 ボー レートが使用されます。 • [38.4k]：38,400 ボー レートが使用されます。 • [57.6k]：57,600 ボー レートが使用されます。 • [115.2k]：115,200 ボー レートが使用されます。 この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。

名前	説明
[コンソール リダイレクション（Console Redirection）] ドロップダウン リスト	POST および BIOS のブート中に、シリアル ポートをコンソール リダイレクションで使用できるようにします。OS 起動後は、コンソールのリダイレクトが関係なくなります。次のいずれかになります。 • [シリアル ポート A（Serial Port A）]：POST 中にシリアル ポート A でコンソール リダイレクションを有効にします。 • [シリアル ポート B（Serial Port B）]：POST 中にシリアル ポート B でコンソール リダイレクションを有効にします。 • [無効（Disabled）]：POST 中にコンソール リダイレクションは発生しません。

サーバー モデル別 BIOS パラメータ

名前	説明
[BIOS Techlogレベル（BIOS Techlog Level）]	このオプションは、**BIOS tech ログファイル**のメッセージのタイプを示します。 ログファイルには、次のタイプのいずれかを指定できます。 • [最小（Minimum）]：重要なメッセージがログファイルに表示されます。 • [標準（Normal）]：警告およびロードメッセージがログファイルに表示されます。 • [最大（Maximum）]：標準に加え、情報関連のメッセージがログファイルに表示されます。 デフォルト値：[最小（Minimum）] （注） このオプションは、主に、内部のデバッグを目としています。 （注） [高速ブート（Fast Boot）] オプションを無効にするには、エンドユーザは次のトークンを下記の説明のとおりに設定する必要があります。 [BIOS Techlogレベル（BIOS Techlog level）] を [標準（Normal）] に [OptionROM起動最適化（OptionROM Launch Optimization）] を [無効（Disabled）] に

名前	説明
[OptionROM起動最適化（OptionROM Launch Optimization）]	このオプションが [有効（Enabled）] の場合、ブート順序のポリシーに存在するコントローラにのみ OptionROMs が起動されます。 （注） ブート順序のポリシーにはリストされていないオンボードストレージコントローラでは、OptionROM が起動されます。 このオプションが [無効（Disabled）] の場合、すべての OptionROMs が起動されます。 デフォルト値：[有効（Enabled）]
[FRB 2 タイマー（FRB 2 Timer）] ドロップダウン リスト	POST 中にシステムがハングした場合に、システムを回復するために Cisco IMC によって FRB2 タイマーが使用されるかどうか。次のいずれかになります。 • [無効（Disabled）]：FRB2 タイマーは使用されません。 • [Enabled]：POST 中に FRB2 タイマーが開始され、必要に応じてシステムの回復に使用されます。

名前	説明
[OS ブート ウォッチドッグ タイマー タイムアウト（OS Watchdog Timer Timeout）] ドロップダウン リスト	OS が指定された時間内にブートしない場合、OS ウォッチドッグ タイマーの期限が切れ、システムはタイマーポリシーに基づいてアクションを実行します。次のいずれかになります。 • [5 分（5 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [10 分（10 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [15 分（15 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [20 分（20 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 （注） このオプションは [OS ブート ウォッチドッグ タイマー（OS Boot Watchdog Timer）] を有効にした場合にのみ適用されます。
[フロー制御（Flow Control）] ドロップダウン リスト	フロー制御にハンドシェイク プロトコルを使用するかどうかを設定します。送信要求/クリア ツー セント（RTS/CTS）を使用すると、隠れた端末の問題が原因で発生する可能性がある、フレーム コリジョンを減らすことができます。次のいずれかになります。 • [なし（None）]：フロー制御は使用されません。 • [RTS/CTS]：RTS/CTS がフロー制御に使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。

名前	説明
[ターミナル タイプ（Terminal Type）] ドロップダウン リスト	コンソール リダイレクションに使用される文字フォーマットのタイプ。次のいずれかになります。 • [PC-ANSI]：PC-ANSI 端末フォントが使用されます。 • [VT100]：サポートされている VT100 ビデオ端末とその文字セットが使用されます。 • [VT100-PLUS]：サポートされている VT100-plus ビデオ端末とその文字セットが使用されます。 • [VT-UTF8]：UTF-8 文字セットのビデオ端末が使用されます。
[CDN コントロール（CDN Control）] ドロップダウン リスト	イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [無効（Disabled）]：VICカードに対するCDNサポートは無効です。 • [有効（Enabled）]：CDNサポートはVICカードに対して有効です。

[セキュリティ（Security）] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

サーバー モデル別 BIOS パラメータ

表 *46 : [*セキュリティ（*Security*）*]* タブの *BIOS* パラメータ

名前	説明
[Reboot Host Immediately] チェックボックス	**[ホストを即座にリブート（Reboot Host Immediately）]** チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい **BIOS** 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[信頼されたプラットフォームモジュールのサポート（Trusted Platform Module Support）] ドロップダウン リスト	信頼されたプラットフォーム モジュール（TPM）は、主に暗号キーを使用する基本的なセキュリティ関連機能を提供するように設計されたマイクロチップです。このオプションを使用すると、システムの TPM セキュリティ デバイス サポートを制御できます。次のいずれかを指定できます。 • [Disabled]：サーバーは TPM を使用しません。 • [有効（Enabled）]：サーバは TPM を使用します。 （注） オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせください。
[電源オン パスワード（Power On Password）] ドロップダウン リスト	このトークンでは、F2 BIOS 設定を使用する前に BIOS パスワードを設定する必要があります。有効にすると、BIOS 関数（IO 設定、BIOS セットアップ、BIOS を使用したオペレーティング システムへのブート）にアクセスする前にパスワードの検証が必要になります。次のいずれかを指定できます。 • **[無効（Disabled）]**：サポートは無効になります。 • [Enabled]：サポートはイネーブルになっています。

[Memory] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

表 *47 : [*メモリ（***Memory***）*]* タブの ***BIOS*** パラメータ

名前	説明
[今すぐホストを再起動（Reboot Host Immediately）] チェックボックス	このチェックボックスをオンにすると、直ちにホスト サーバが再起動します。このチェックボックスは、変更を保存してからオンにする必要があります。
[4 G 以上の復号化（Above 4G Decoding）] ドロップダウン リスト	4 GB 以上の MMIO を有効または無効にします。次のいずれかになります。 • [Disabled]：サーバーでは 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングしません。 • [有効（Enabled）]：サーバで 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングします。 （注） PCI デバイスが 64 ビット対応でも、レガシーなオプション ROM を使用する場合は、この設定をイネーブルにしても正しく機能しない場合があります。

名前	説明
[Memory Interleaving]ドロップダウン リスト	物理メモリの更新中に別のメモリにアクセスできるよう、AMD CPU がメモリをインターリーブするかどうかを指定します。このオプションは、ファブリック レベルでメモリのインターリーブを制御します。チャネル、ダイ、ソケットの要件はメモリによって異なるため、選択したオプションがメモリでサポートされない場合これらは無視されます。次のいずれかを選択できます。 • **[Auto]**：CPU がメモリのインターリーブの方法を決定します。 • **[Channel]**：各チャネルに単一の連続したアドレス空間を配置するのではなく、複数のチャネル全体に物理アドレス空間をインターリーブします。 • **[Die]**：各ダイに単一の連続したアドレス空間を配置するのではなく、複数のダイ全体に物理アドレス空間をインターリーブします。 • **[None]**：同一の物理メモリから連続したメモリ ブロックにアクセスします。 • **[Socket]**：各ソケットに単一の連続したアドレス空間を配置するのではなく、複数のソケット全体に物理アドレス空間をインターリーブします。 • [Platform Default][platform-default]：BIOSは、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Memory Interleaving] ドロップダウン リスト	インターリーブされるメモリ ブロックのサイズを決定します。また、インターリーブの開始アドレス（ビット 8、9、10、11）も指定します。次のいずれかになります。 • 1 KB • 2 KB • 256 バイト • 512 バイト • **自動**: CPU、メモリ ブロックのサイズを決定します。 • [Platform Default][platform-default]：BIOSは、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[Chipselect Interleaving] ドロップダウンリスト	ノード 0 に選択する DRAM チップ経由でメモリ ブロックがインターリーブされるかどうか。次のいずれかになります。 • **[Auto]**：CPU でチップ セレクトのインタリーブの方法を自動的に決定します。 • **[Disabled]**：チップの選択は、メモリ コントローラ内でインターリーブされません。 • [Platform Default][platform-default]：BIOSは、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Bank Group Swap] ドロップダウンリスト	物理アドレスをアプリケーションに割り当てる方法を決定します。次のいずれかになります。 • **[Auto]**：アプリケーションへの物理アドレスの割り当て方法を CPU で自動的に決定します。 • **[Disabled]**：バンク グループ スワップは使用されません。 • **[Enabled]**：バンク グループ スワップによりアプリケーションのパフォーマンスを向上させます。 • [Platform Default][platform-default]：BIOSは、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[IOMMU] ドロップダウンリスト	出入力メモリ管理ユニット（IOMMU） により、AMDプロセッサが物理アドレスへ仮想アドレスをマッピングすることが可能です。次のいずれかになります。 • **[Auto]**：これらのアドレスのマッピング方法を CPU で決定します。 • **[Disabled]**：IOMMU は使用されません。 • **[Enabled]**：IOMMU によりアドレス マッピングを行います。 • [Platform Default][platform-default]：BIOSは、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[SMEE] ドロップダウンリスト	プロセッサで、メモリの暗号化サポートを実現する Secure Memory Encryption Enable（SMEE）機能を使用するかどうかを指定します。次のいずれかになります。 • **[Disabled]**：プロセッサで SMEE 機能を使用しません。 • **[Enabled]**：プロセッサで SMEE 機能を使用します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[TSME] ドロップダウンリスト	プロセッサで、メモリの暗号化サポートを実現する透過的セキュアメモリ暗号化（TSME）機能を使用するかどうかを指定します。次のいずれかになります。 • **[無効（Disabled）]**：プロセッサは TSME 機能を使用しません。 • **[有効（Enabled）]**：プロセッサは TSME 機能を使用します。 • **[自動（Auto）]**：BIOS は、サーバー タイプとベンダーに関する BIOS のデフォルト設定に含まれるこの属性の値を使用します。
[SEV] ドロップダウンリスト	VM のコードとデータが分離された、暗号化仮想マシン（VM）の実行を有効にします。次のいずれかになります。 • **[253 ASIDs]**：値は 253 の最小アドレス空間識別子（ASID）に設定されます。 • **[509 ASIDs]**：値は 509 の最小アドレス空間識別子（ASID）に設定されます。 • **[自動（Auto）]**：BIOS は、サーバー タイプとベンダーに関する BIOS のデフォルト設定に含まれるこの属性の値を使用します。

名前	説明
[DRAM SW サーマル スロットリング（DRAM SW Thermal Throttling）] ドロップダウンリスト	ソフトウェアが温度制限内で機能することを保証する保護メカニズムを提供します。温度が最大しきい値を超えると、パフォーマンスを低下させ、最小しきい値まで冷却します。次のいずれかになります。 • **[無効（Disabled）]**：プロセッサはこの機能を使用しません。 • **[有効（Enabled）]**：プロセッサはこの機能を使用します。 • **[自動（Auto）]**：BIOS は、サーバー タイプとベンダーに関する BIOS のデフォルト設定に含まれるこの属性の値を使用します。
[バーストおよび遅延リフレッシュ（Burst and Postponed Refresh）] ドロップダウンリスト	• **[無効（Disabled）]**：プロセッサはこの機能を使用しません。 • **[有効（Enabled）]**：プロセッサはこの機能を使用します。 • **[自動（Auto）]**：BIOS は、サーバー タイプとベンダーに関する BIOS のデフォルト設定に含まれるこの属性の値を使用します。

[I/O] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

表 *48 : [I/O]* タブの *BIOS* パラメータ

名前	説明
[今すぐホストを再起動（Reboot Host Immediately）] チェックボックス	このチェックボックスをオンにすると、直ちにホスト サーバが再起動します。このチェックボックスは、変更を保存してからオンにする必要があります。

名前	説明
[PCIe スロット *n* Oprom（Pcie Slot n Oprom）] ドロップダウン リスト	サーバーが *n* で指定した PCIe カード スロットにあるオプション ROM を使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：スロット *n* のオプションの ROM は使用できません。 • [有効（Enabled）]：スロット *n* のオプション ROM は使用可能です。
[PCIe スロット *n* リンク速度（PCIe Slot n Link Speed）] ドロップダウン リスト	システム IO コントローラ *n*（SIOCn）アドオン スロット（*n* によって示される）のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効となり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。
[IPV6 PXE サポート（IPV6 PXE Support）] ドロップダウン リスト	PXE の IPv6 サポートを有効または無効にします。次のいずれかになります • [無効（disabled）][無効（Disabled）]：IPV6PXE のサポートは利用できません。 • [enabled][Enabled]：IPV6PXE のサポートを常に利用できます。
[IPV4 PXE サポート (IPV4 PXE Support)] ドロップダウン リスト	PXE の IPv4 サポートを有効または無効にします。次のいずれかになります。 • [無効（disabled）][無効（Disabled）]：IPV4PXE のサポートは利用できません。 • [enabled][Enabled]：IPV4PXE のサポートを常に利用できます。
[SR-IOV サポート（SR-IOV Support）] ドロップダウン リスト	サーバー上で SR-IOV（Single Root I/O Virtualization）を有効にするか無効にするか。次のいずれかになります。 • [Disabled]：SR-IOV は無効になります。 • [有効（Enabled）]：SR-IOV はイネーブルになります。

名前	説明
[前面 NVME *n* OptionROM（Front NVME n OptionROM）] ドロップダウンリスト	このオプションでは、SSD:NVMe *n* スロットに接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • **[無効（Disabled）]**：SSD:NVMe *n* スロットに接続されている PCIe アダプタのオプションの ROM を実行しません。 • **[有効（Enabled）]**：SSD:NVMe *n* スロットに接続されている PCIe アダプタのオプションの ROM を実行します。
[前面 NVME *n* リンク速度（Front NVME n Link Speed）] ドロップダウンリスト	NVMe 前面スロット *n* のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効となり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。
[PCIe スロット MSTOR RAID OptionROM (PCIe Slot MSTOR RAID OptionROM)] ドロップダウン リスト	サーバが PCIe MSTOR RAID のオプション ROM を使用するかどうか。次のいずれかになります。 • Disabled：オプション ROM は使用できません。 • [Enabled]—オプション ROM は使用できます。
[PCIe ARI サポート (PCIe ARI Support)] ドロップダウン リスト	リリース 4.1(2a) 以降、Cisco IMC は PCIe 代替ルーティング ID (ARI) 解釈機能をサポートしています。PCIe 仕様では、8 個以上の機能を有効にする PCIeヘッダーのデバイス番号フィールドを再解釈する ARI の実装を通じて、より多くの仮想機能をサポートしています。次のいずれかになります。 • **無効**：PCIe ARI サポートは使用できません。 • **有効**：PCIe ARIサポートを使用できます。 • **自動**：PCIe ARI サポートは自動モードです。

名前	説明
[IPv6 HTTP サポート（IPv6 HTTP Support）] ドロップダウンリスト	HTTP の IPv6 サポートを有効または無効にします。次のいずれかになります。 • **[無効（Disabled）]**：IPv6 HTTP サポートは使用できません。 • **[有効（Enabled）]**：IPv6 HTTP サポートを常に使用できます。
[IPV4 HTTP サポート（IPV4 HTTP Support）] ドロップダウンリスト	HTTP の IPv4 サポートを有効または無効にします。次のいずれかになります。 • **[無効（Disabled）]**：IPv4 HTTP サポートは使用できません。 • **[有効（Enabled）]**：IPv4 HTTP サポートを常に使用できます。

[電源/パフォーマンス（Power/Performance）] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

表 *49 : [*電源/パフォーマンス（*Power/Performance*）*] タブの BIOS* パラメータ

名前	説明
[今すぐホストを再起動（Reboot Host Immediately）] チェックボックス	このチェックボックスをオンにすると、直ちにホスト サーバが再起動します。このチェックボックスは、変更を保存してからオンにする必要があります。
[Core Performance Boost] ドロップダウンリスト	AMDプロセッサがアイドル状態（ほとんど使用されていない状態）のときにコアの周波数を上げるかどうかを指定します。次のいずれかになります。 • **[Auto]**：パフォーマンスをブーストする方法を CPU で自動的に決定します。 • **[Disabled]**：CPU により自動的にブースト パフォーマンスが決定されます。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Global C-state Control] ドロップダウンリスト	AMD プロセッサが IO ベースの C ステートおよび DF C ステートを制御するかどうかに関係なく、これは次のうちいずれかになります。 • **[Auto]**：CPU で IO ベースの C ステートの生成方法を自動的に決定します。 • **[Disabled]**：グローバル C ステートの制御が無効になります。 • **[Enabled]**：グローバル C ステートの制御が有効になります。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[L1 Stream HW Prefetcher] ドロップダウンリスト	プロセッサで、AMD ハードウェア プリフェッチャが必要に応じてデータおよび命令ストリームをメモリから取得し、L1 キャッシュに入れることを許可するかどうか。次のいずれかになります。 • [auto][Auto]：CPUは、I/O デバイスからプロセッサ キャッシュにデータを配置する方法を決定します。 • [disabled][Disabled]：ハードウェア プリフェッチャは使用しません。 • [enabled][Enabled]：プロセッサで、キャッシュの問題が検出されたときにハードウェアプリフェッチャを使用します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[L2 Stream HW Prefetcher] ドロップダウンリスト	プロセッサで、AMD ハードウェア プリフェッチャが必要に応じてメモリからデータおよび命令ストリームを取得し、L2 キャッシュに入れることを許可するかどうかを指定します。次のいずれかになります。 • [auto][Auto]：CPUは、I/Oデバイスからプロセッサ キャッシュにデータを配置する方法を決定します。 • [disabled][Disabled]：ハードウェア プリフェッチャは使用しません。 • [enabled][Enabled]：プロセッサで、キャッシュの問題が検出されたときにハードウェアプリフェッチャを使用します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[Determinism Slider] ドロップダウンリスト	AMDプロセッサにより動作方法を決定できます。次のいずれかになります。 • **[Auto[**：CPU はデフォルトの決定論的な電源設定を自動で使用します。 • **[Performance]**：プロセッサは、最適なパフォーマンスかつ一貫した方法で動作します。 • **[Power]**：プロセッサは、ダイごとに許容される最大のパフォーマンスで動作します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

[Processor] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

サーバー モデル別 BIOS パラメータ

表 *50 : [*プロセッサ（*Processor*）*]* タブの *BIOS* パラメータ

名前	説明
[Reboot Host Immediately] チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[SMT Mode] ドロップダウンリスト	プロセッサで AMD Simultaneous MultiThreading テクノロジーを使用するかどうかを指定します。このテクノロジーでは、マルチスレッド ソフトウェア アプリケーションのスレッドを各プロセッサ内で並列に実行できます。次のいずれかになります。 • **[Auto]**：プロセッサは、マルチスレッドの並列実行を許可します。 • **[Off]**：プロセッサでマルチスレッディングを禁止します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[SVM Mode] ドロップダウンリスト	プロセッサが AMD セキュア仮想マシン テクノロジを使用するかどうか。次のいずれかを選択できます。 • **[Disabled]**：プロセッサで SVM テクノロジーを使用しません。 • **[Enabled]**：プロセッサで SVM テクノロジーを使用します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Downcore control] ドロップダウンリスト	AMDプロセッサ コアを無効にしているため、有効にするコアの数を選択できます。次のいずれかになります。 • [FOUR（2+2）]：各 CPU コンプレックスで 2 つのコアを有効にします。 • [FOUR（4+0）]：片方の CPU コンプレックスのみで 4 つのコアを有効にします。 • [SIX（3+3）]：各 CPU コンプレックスで 3 つのコアを有効にします。 • [THREE（3+0）]：片方の CPU コンプレックスのみで 3 つのコアを有効にします。 • [TWO（1+1）]：各 CPU コンプレックスで 1 つのコアを有効にします。 • [TWO（2+0）]：片方の CPU コンプレックスのみで 2 つのコアを有効にします。 • **[Auto]**：有効化する必要のあるコアの数を CPU で判断します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

C220 M5、C240 M5、C240 SD M5、および C480 M5 サーバ

I/O タブ

（注） このタブに記載されている BIOS のパラメータは、サーバによって異なります。

表 *51 : [I/O]* タブの *BIOS* のパラメータ

名前	説明
[Reboot Host Immediately] チェックボックス	オンにすると、ホスト サーバが直ちに再起動されます。このチェックボックスは、変更を保存してからオンにする必要があります。
[レガシー USB サポート（Legacy USB Support）] ドロップダウン リスト	システムでレガシー USB デバイスをサポートするかどうか。次のいずれかになります。 • [Disabled]：USB デバイスは、EFI アプリケーションでのみ使用できます。 • [Enabled]：レガシー USB のサポートは常に使用できます。
[ダイレクト IO への Intel VT（Intel VT for directed IO）] ドロップダウン リスト	プロセッサで Intel Virtualization Technology（VT）を使用するかどうか。このテクノロジーでは、1 つのプラットフォームで、複数のオペレーティング システムとアプリケーションをそれぞれ独立したパーティション内で実行できます。次のいずれかになります。 • [Disabled]：プロセッサでの仮想化を禁止します。 • [Enabled]：プロセッサで、複数のオペレーティング システムをそれぞれ独立したパーティション内で実行できます。 （注） このオプションを変更した場合は、設定を有効にするためにサーバの電源を再投入する必要があります。
[Intel VTD coherency サポート（Intel VTD coherency support）] ドロップダウン リスト	プロセッサで Intel VT-d Coherency をサポートするかどうか。次のいずれかになります。 • [Disabled]：プロセッサでコヒーレンシをサポートしません。 • [Enabled]：プロセッサで VT-d Coherency を必要に応じて使用します。
[Intel VTD ATS サポート（Intel VTD ATS support）] ドロップダウン リスト	プロセッサで Intel VT-d Address Translation Services（ATS）をサポートするかどうか。次のいずれかになります。 • [Disabled]：プロセッサで ATS をサポートしません。 • [Enabled]：プロセッサで VT-d ATS を必要に応じて使用します。

名前	説明
[VMD Enable (VMD の有効化)] ドロップダウン リスト	Intel Volume Management Device (VMD) は、NVMe SSD を管理および集約するためのハードウェア ロジックを提供する PCIe NVMe SSD 向けです。 これは次のいずれかになります。 • **有効**: 堅牢で安定したホットプラグ、ステータス LED 管理などの利点を有効にします。 • **無効**: 堅牢で安定したホットプラグ、ステータス LED 管理などの利点を無効にします。 デフォルト値：**無効**。 VMD を設定するには、『CPU ユーザー ガイドの Intel® 仮想 RAID』と『CPU の Intel® 仮想 RAID』を参照してください。
	Cisco UCS C480 M5 サーバでサポートされている VMD およびサポートされていないポートの詳細は次のとおりです。 Cisco UCS C480 NVMe SKU (32 ドライブ NVME システム) • DMI 接続ポート7、8、および 23 は、VMD をサポートしていません。 • その他の 29 個のポートはすべて、VMD をサポートしています。 Cisco UCS C480 非 NVMe SKU • DMI 接続ポート 1、2、および 18 は、VMD をサポートしていません。 • ポート7、8、9、10、15、16、17、23、24 は、VMD をサポートします。
[すべてのオンボード LOM Oprom（All Onboard LOM Oprom）] ドロップダウン リスト	オプション ROM がすべての LOM ポートで使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：すべてのポートでオプション ROM を無効にします。 • [有効（Enabled）]：すべてのポートでオプション ROM を有効にします。

サーバー モデル別 BIOS パラメータ

名前	説明
[オンボードLOMポート0 Oprom（Onboard LOM Port0 Oprom）] ドロップダウン リスト	オプション ROM が LOM ポート 0 で使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：LOM ポート 0 でオプション ROM を 使用できません。 • [有効（Enabled）]：LOM ポート 0 でオプション ROM を使用できます。
[オンボードLOMポート1 Oprom（Onboard LOM Port1 Oprom）] ドロップダウン リスト	オプション ROM が LOM ポート 1 で使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：LOM ポート 1 でオプション ROM を 使用できません。 • [有効（Enabled）]：LOM ポート 1 でオプション ROM を使用できます。
[PCIe スロット *n* Oprom（Pcie Slot n Oprom）] ドロップダウン リスト	サーバが *n* で指定した PCIe カード スロットにあるオプション ROM を使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：スロット *n* のオプション ROM は使用できません。 • [有効（Enabled）]：スロット *n* のオプション ROM は使用可能です。
[MLOM Oprom] ドロップダウン リスト	このオプションでは、MLOM スロットに接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • [無効（Disabled）]：MLOM スロットに接続されている PCIe アダプタのオプション ROM を実行しません。 • [有効（Enabled）]：MLOM スロットに接続されている PCIe アダプタのオプション ROM を実行します。
[HBA Oprom] ドロップダウン リスト	このオプションでは、HBA スロットに接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • [無効（Disabled）]：HBA スロットに接続されている PCIe アダプタのオプション ROM を実行しません。 • [有効（Enabled）]：HBA スロットに接続されている PCIe アダプタのオプション ROM を実行します。

名前	説明
[フロント NVME1 Oprom（Front NVME1 Oprom）] ドロップダウン リスト	このオプションでは、SSD:NVMe1 スロットに接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • [無効（Disabled）]：SSD:NVMe1 スロットに接続されている PCIe アダプタのオプション ROM を実行しません。 • [有効（Enabled）]：SSD:NVMe1 スロットに接続されている PCIe アダプタのオプション ROM を実行します
[フロント NVME2 Oprom（Front NVME2 Oprom）] ドロップダウン リスト	このオプションでは、SSD:NVMe2 スロットに接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • [無効（Disabled）]：SSD:NVMe2 スロットに接続されている PCIe アダプタのオプション ROM を実行しません。 • [有効（Enabled）]：SSD:NVMe2 スロットに接続されている PCIe アダプタのオプション ROM を実行します
[HBA リンク速度（HBA Link Speed）] ドロップダウン リスト	このオプションを使用すると、PCIe HBA スロットに装着されているアダプタ カードの最大速度を制限できます。次のいずれかになります。 • [無効（Disabled）]：最大速度は制限されません。 • [自動（Auto）]：システムは許容最大速度を選択します。 • [GEN1]：最大 2.5GT/s（ギガトランスファー/秒）までの速度が許可されます。 • [GEN2]：最大 5 GT/s までの速度が許可されます。 • [GEN3]：最大 8 GT/s までの速度が許可されます。
[MLOM リンク速度（MLOM Link Speed）] ドロップダウン リスト	このオプションを使用すると、PCIe MLOM スロットに装着されているアダプタ カードの最大速度を制限できます。次のいずれかになります。 • [無効（Disabled）]：最大速度は制限されません。 • [自動（Auto）]：システムは許容最大速度を選択します。 • [GEN1]：最大 2.5GT/s（ギガトランスファー/秒）までの速度が許可されます。 • [GEN2]：最大 5 GT/s までの速度が許可されます。 • [GEN3]：最大 8 GT/s までの速度が許可されます。

名前	説明
[PCIe スロット *n* リンク速度（PCIe Slot n Link Speed）] ドロップダウン リスト	システム IO コントローラ *n*（SIOCn）アドオン スロット（*n* によって示される）のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効であり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。
[フロント NVME1 リンク速度（Front NVME1 Link Speed）] ドロップダウン リスト	NVMe フロント スロット 1 のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効であり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。
[フロント NVME2 リンク速度（Front NVME2 Link Speed）] ドロップダウン リスト	NVMe フロント スロット 2 のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効であり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。

名前	説明
[リア NVME1 リンク速度（Rear NVME1 Link Speed）] ドロップダウン リスト	NVMe 背面のスロット 1 のリンク速度。次のいずれかになります。 • [無効（Disabled）] : スロットは無効であり、カードは列挙されません。 • [自動（Auto）] : デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1] : リンク速度は第 1 世代まで到達可能です。 • [GEN2] : リンク速度は第 2 世代まで到達可能です。 • [GEN3] : リンク速度は第 3 世代まで到達可能です。
[リア NVME2 リンク速度（Rear NVME2 Link Speed）] ドロップダウン リスト	NVMe 背面のスロット 2 のリンク速度。次のいずれかになります。 • [無効（Disabled）] : スロットは無効であり、カードは列挙されません。 • [自動（Auto）] : デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1] : リンク速度は第 1 世代まで到達可能です。 • [GEN2] : リンク速度は第 2 世代まで到達可能です。 • [GEN3] : リンク速度は第 3 世代まで到達可能です。
[VGA 優先順位（VGA Priority）] ドロップダウン リスト	システムに複数の VGA デバイスがある場合は、VGA グラフィックス デバイスの優先順位を設定できます。次のいずれかになります。 • [オンボード（OnBoard）] : オンボード VGA デバイスが優先されます。BIOS ポスト画面および OS ブートはオンボード VGA ポート経由で駆動されます。 • [オフボード（OffBoard）] : PCIE グラフィックス アダプタが優先されます。BIOS ポスト画面および OS ブートは外部グラフィックス アダプタ ポート経由で駆動されます。 • [オンボードを無効（OnBoardDisabled）] : PCIE グラフィックス アダプタが優先され、オンボード VGA デバイスは無効になります。オンボード VGA が無効の場合、vKVM は機能しません。

サーバー モデル別 BIOS パラメータ

名前	説明
[P-SATA OptionROM] ドロップダウン リスト	PCH SATA オプション ROM モードを選択できます。次のいずれかになります。 • [LSI SW Raid]：SATA コントローラと sSATA コントローラを LSI SW Raid の raid モードに設定します。 • [無効（Disabled）]：SATA コントローラと sSATA コントローラを無効にします。
[M2.SATA OptionROM] ドロップダウン リスト	Serial Advanced Technology Attachment（SATA）ソリッド ステート ドライブ（SSD）の動作モード。次のいずれかになります。 • [AHCI]： SATA コントローラと sSATA コントローラの両方を AHCI モードに設定します。 • [LSI SW Raid]：SATA コントローラと sSATA コントローラを LSI SW Raid の raid モードに設定します。 • [無効（Disabled）]：SATA コントローラと sSATA コントローラを無効にします。
[リア USB ポート（USB Port Rear）] ドロップダウン リスト	背面パネルの USB デバイスが有効か無効か。次のいずれかになります。 • [無効（Disabled）]：背面パネルの USB ポートを無効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [有効（Enabled）]：背面パネルの USB ポートを有効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。
[フロント USB ポート（USB Port Front）] ドロップダウン リスト	前面パネルの USB デバイスが有効か無効か。次のいずれかになります。 • [無効（Disabled）]：前面パネルの USB ポートを無効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [有効（Enabled）]：前面パネルの USB ポートを有効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。

名前	説明
[内部 USB ポート（USB Port Internal）] ドロップダウン リスト	内部 USB デバイスが有効か無効か。次のいずれかになります。 • [無効（Disabled）]：内部の USB ポートを無効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [有効（Enabled）]：内部の USB ポートを有効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。
[KVM USB ポート（USB Port KVM）] ドロップダウン リスト	vKVM ポートが有効になっているか、無効になっているか。次のいずれかになります • **[無効（Disabled）]**—vKVM キーボードとマウス デバイスを無効にします。キーボードとマウスは KVM ウィンドウで機能しなくなります。 • **[有効 (Enabled)]**—vKVM キーボードとマウス デバイスを有効にします。
[SD カード USB ポート（USB Port SD Card）] ドロップダウン リスト	SD カードが有効か無効か。次のいずれかになります。 • [無効（Disabled）]：SD カードのポートを無効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [有効（Enabled）]：SD カードのポートを有効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。
[IPV6 PXE サポート（IPV6 PXE Support）] ドロップダウン リスト	PXE の IPv6 サポートを有効または無効にします。次のいずれかになります • **[無効(Disabled)]** : PV6 PXE のサポートは利用できません。 • **[Enabled (有効)]**:IPV6 PXE のサポートを常に利用できます。
PCIe PLL SSC ドロップダウン リスト	この機能を有効にすると、クロックを 0.5% 下方に拡散することにより、EMI 干渉が軽減されます。この機能を無効にすると、拡散せずにクロックを集中管理できます。 これは次のいずれかになります。 • **[自動 (Auto)]**—EMI 干渉は自動調整されます。 **[無効 (Disabled)]**—EMI 干渉は自動調整されます。 • **[ZeroPointFive]**—クロックを 0.5% 下方に拡散することにより、EMI 干渉を軽減します。

名前	説明
[IPV4 PXE サポート (IPV4 PXE Support)] ドロップダウン リスト	PXE の IPv4 サポートを有効または無効にします。次のいずれかになります • **[無効(Disabled)]**: IPV4 PXE のサポートは利用できません。 • **[Enabled (有効)]**: IPV4 PXE のサポートを常に利用できます。
[Network Stack (ネットワーク スタック)] ドロップダウン リスト	このオプションでは、IPv6 と IPv4 をモニタできます。次のいずれかになります • **[無効 (Disabled)]**: ネットワーク スタックのサポートは使用できません。 （注） 無効にすると、 **IPV4 PXE サポート**に設定された値はシステムに影響しません。 • **[Enabled (有効)]**: ネットワーク スタックのサポートを常に利用できます。
[外部データベース（External Database）] ドロップダウン リスト	このオプションを使用すると、マザーボードからの EMI を、マザーボードが発生する信号に変調をかけ、スパイクがより平坦な曲線になるようにして、軽減します。 次のいずれかになります。 • **[無効 (Disabled)]**—クロック拡散スペクトルのサポートは使用できません。 • **[Enabled (有効)]**—クロック拡散スペクトルのサポートは常に使用できます。
[PCIe スロット MSTOR RAID OptionROM (PCIe Slot MSTOR RAID OptionROM)] ドロップダウン リスト	サーバが PCIe MSTOR RAID のオプション ROM を使用するかどうか。次のいずれかになります。 • Disabled：オプション ROM は使用できません。 • [Enabled]—オプション ROM は使用できます。

[Server Management] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

表 *52 : [*サーバ管理（*Server Management*）*]* タブの *BIOS* パラメータ

名前	説明
[Reboot Host Immediately] チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[OS ブート ウォッチドッグ タイマー ポリシー（OS Boot Watchdog Timer Policy）] ドロップダウン リスト	ウォッチドッグ タイマーが切れた場合にシステムで実行されるアクション。次のいずれかになります。 • [電源オフ（Power Off）]：OS のブート中にウォッチドッグ タイマーの期限が切れた場合、サーバの電源がオフになります。 • [Reset]：OS のブート中にウォッチドッグ タイマーが切れた場合、サーバーはリセットされます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にする場合にのみ適用されます。
[OS ウォッチドッグ タイマー（OS Watchdog Timer）] ドロップダウン リスト	BIOS が指定されたタイムアウト値でウォッチドッグ タイマーをプログラムするかどうか。次のいずれかになります。 • [Disabled]：サーバーのブートにかかる時間をトラッキングするためにウォッチドッグ タイマーは使用されません。 • [有効（enabled）]：サーバーがブートにかかる時間をウォッチドッグ タイマーで追跡します。サーバーのブートが [OS ブート ウォッチドッグ タイマー タイムアウト（OS Boot Watchdog Timer Timeout）] フィールドで指定された時間内に完了しない場合は、Cisco IMC によってエラーがログに記録され、[OS ブート ウォッチドッグ ポリシー（OS Boot Watchdog Policy）] フィールドで指定されたアクションが実行されます。

サーバー モデル別 BIOS パラメータ

名前	説明
[OS ブート ウォッチドッグ タイマー タイムアウト（OS Watchdog Timer Timeout）] ドロップダウン リスト	OS が指定された時間内にブートしない場合、OS ウォッチドッグ タイマーの期限が切れ、システムはタイマーポリシーに基づいてアクションを実行します。次のいずれかになります。 • [5 分（5 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [10 分（10 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [15 分（15 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [20 分（20 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にした場合にのみ適用されます。
[ボー レート（Baud Rate）] ドロップダウン リスト	シリアル ポートの伝送速度として使用されるボー レート。[コンソール リダイレクション（Console Redirection）] を無効にした場合、このオプションを使用できません。次のいずれかになります。 • [9.6k]：9,600 ボー レートが使用されます。 • [19.2k]：19,200 ボー レートが使用されます。 • [38.4k]：38,400 ボー レートが使用されます。 • [57.6k]：57,600 ボー レートが使用されます。 • [115.2k]：115,200 ボー レートが使用されます。 この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。

名前	説明
[コンソール リダイレクション（Console Redirection）] ドロップダウン リスト	POST および BIOS のブート中に、シリアル ポートをコンソール リダイレクションで使用できるようにします。OS 起動後は、コンソールのリダイレクトが関係なくなります。次のいずれかになります。 • [シリアル ポート A（Serial Port A）]：POST 中にシリアル ポート A でコンソール リダイレクションを有効にします。 • [シリアル ポート B（Serial Port B）]：POST 中にシリアル ポート B でコンソール リダイレクションを有効にします。 • [無効（Disabled）]：POST 中にコンソール リダイレクションは発生しません。

サーバー モデル別 BIOS パラメータ

名前	説明
適応型メモリ トレーニング	このオプションを[有効（Enabled）]にすると、次のようになります。 メモリ トレーニングは毎回のブートでは実行されず、BIOSは、保存されたメモリ トレーニングの結果を毎回のリブートで使用します。 毎回のブートでメモリ トレーニングが実行されるいくつかの例外には、次のものがあります。 BIOS の更新、CMOS のリセット、CPU やメモリの設定変更、SPD または実行時の修正不可能なエラー、または、前回のブートから 24 時間以上経過している場合。 このオプションが [無効（Disabled）] の場合、毎回のブートでメモリ トレーニングが行われます。 デフォルト値：[有効（Enabled）]。 （注） [高速ブート（Fast Boot）] オプションを無効にするには、エンドユーザーは次のトークンを下記の説明のとおりに設定する必要があります。 [適応型メモリ トレーニング（Adaptive Memory Training）]を [無効（Disabled）] に [BIOS Techlogレベル（BIOS Techlog level）] を [標準（Normal）] に [OptionROM起動最適化（OptionROM Launch Optimization）] を [無効（Disabled）] に

名前	説明
[BIOS Techlogレベル（BIOS Techlog Level）]	このオプションは、 **BIOS tech ログファイル** のメッセージのタイプを示します。 ログファイルには、次のタイプのいずれかを指定できます。 • [最小（Minimum）]：重要なメッセージがログファイルに表示されます。 • [標準（Normal）]：警告およびロードメッセージがログファイルに表示されます。 • [最大（Maximum）]：標準に加え、情報関連のメッセージがログファイルに表示されます。 デフォルト値：[最小（Minimum）] （注） このオプションは、主に、内部のデバッグを目としています。
[OptionROM起動最適化（OptionROM Launch Optimization）]	このオプションが [有効（Enabled）] の場合、ブート順序のポリシーに存在するコントローラにのみ OptionROMs が起動されます。 （注） オンボードストレージコントローラ、Emulex FC アダプタおよび GPU コントローラなどのいくつかのコントローラについて、ブート順序のポリシーに含まれていなくても、OptionROM が起動されます。 このオプションが [無効（Disabled）] の場合、すべての OptionROMs が起動されます。 デフォルト値：[有効（Enabled）]
[CDN コントロール（CDN Control）] ドロップダウン リスト	イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [無効（Disabled）]：VIC カードに対する CDN サポートは無効です。 • [有効（Enabled）]：CDNサポートはVIC カードに対して有効です。

サーバー モデル別 BIOS パラメータ

名前	説明
[FRB 2 タイマー（FRB 2 Timer）] ドロップダウン リスト	POST 中にシステムがハングした場合に、システムを回復するために Cisco IMC によって FRB2 タイマーが使用されるかどうか。次のいずれかになります。 • [無効（Disabled）]：FRB2 タイマーは使用されません。 • [Enabled]：POST 中に FRB2 タイマーが開始され、必要に応じてシステムの回復に使用されます。
[フロー制御（Flow Control）] ドロップダウン リスト	フロー制御にハンドシェイク プロトコルを使用するかどうかを設定します。送信要求/クリア ツー センド（RTS/CTS）を使用すると、隠れた端末の問題が原因で発生する可能性がある、フレーム コリジョンを減らすことができます。次のいずれかになります。 • [なし（None）]：フロー制御は使用されません。 • [RTS/CTS]：RTS/CTS がフロー制御に使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。
[ターミナル タイプ（Terminal Type）] ドロップダウン リスト	コンソール リダイレクションに使用される文字フォーマットのタイプ。次のいずれかになります。 • [PC-ANSI]：PC-ANSI 端末フォントが使用されます。 • [VT100]：サポートされている VT100 ビデオ端末とその文字セットが使用されます。 • [VT100-PLUS]：サポートされている VT100-plus ビデオ端末とその文字セットが使用されます。 • [VT-UTF8]：UTF-8 文字セットのビデオ端末が使用されます。

名前	説明
[PCIe Slots CDN コントロール（PCIe Slots CDN Control）] ドロップダウンリスト	（注） このオプションは、スロット 2 または 5 に Qlogic カードを搭載した Cisco UCS C240 M5 サーバーでのみ使用できます。 イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [無効（Disabled）]：VIC カードに対する CDN サポートは無効です。 • [Enabled]：VIC カードの CDN サポートが有効になります。

[セキュリティ（Security）] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

表 *53 : [*セキュリティ（*Security*）*]* タブの *BIOS* パラメータ

名前	説明
[Reboot Host Immediately] チェックボックス	**[**ホストを即座にリブート（**Reboot Host Immediately**）**]** チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい **BIOS** 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[トラステッド プラットフォーム モジュール状態（**Trusted Platform Module State**）**]** ドロップダウンリスト	信頼されたプラットフォーム モジュール（TPM）は、主に暗号キーを使用する基本的なセキュリティ関連機能を提供するように設計されたマイクロチップです。このオプションを使用すると、システムの TPM セキュリティ デバイス サポートを制御できます。次のいずれかを指定できます。 • [Disabled]：サーバーは TPM を使用しません。 • [有効（Enabled）]：サーバは TPM を使用します。 （注） オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせください。
SHA-1 PCRバンク	SHA-1 PCR バンクを有効または無効にします。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
SHA256 PCRバンク	SHA256 PCR バンクを有効または無効にします。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

名前	説明
[Reboot Host Immediately] チェックボックス	**[ホストを即座にリブート（Reboot Host Immediately）]** チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい **BIOS** 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[Intel Trusted Execution Technology のサポート（Intel Trusted Execution Technology Support）]	信頼されたプラットフォームモジュール(TPM)が 有効 である場合にのみ 有効 に設定できます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[電源オン パスワード（Power On Password）] ドロップダウンリスト	このトークンでは、F2 BIOS 設定を使用する前に BIOS パスワードを設定する必要があります。有効にすると、BIOS 関数（IO 設定、BIOS セットアップ、BIOS を使用したオペレーティング システムへのブート）にアクセスする前にパスワードの検証が必要になります。次のいずれかを指定できます。 • **[無効（Disabled）]**：サポートは無効になります。 • [Enabled]：サポートはイネーブルになっています。

[Processor] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

サーバー モデル別 BIOS パラメータ

表 *54 : [*プロセッサ（*Processor*）*]* タブの *BIOS* パラメータ

名前	説明
[Intel Virtualization Technology] ドロップダウン リスト	プロセッサで Intel Virtualization Technology（VT）を使用するかどうか。このテクノロジーでは、1 つのプラットフォームで、複数のオペレーティング システムとアプリケーションをそれぞれ独立したパーティション内で実行できます。次のいずれかになります。 • [Disabled]：プロセッサでの仮想化を禁止します。 • [有効（Enabled）]：プロセッサで、複数のオペレーティング システムをそれぞれ独立したパーティション内で実行できます。
[拡張 APIC（Extended APIC）] ドロップダウン リスト	拡張 APIC サポートをイネーブルまたはディセーブルにできます。次のいずれかになります。 • [有効（Enabled）]：APIC サポートを有効にします • [無効（Disabled）]：APIC サポートを無効にします。
[プロセッサ C1E（Processor C1E）] ドロップダウン リスト	C1 ステートに入ったときに、CPU が最小周波数に移行するかどうか。次のいずれかになります。 • [無効（Disabled）]：CPU は C1 ステートでも引き続き最大周波数で動作します。 • [有効（Enabled）]：CPU は最小周波数に移行します。このオプションでは C1 ステートで節約される電力量が最大になります。 （注） このオプションを使用できるのは一部の C シリーズ サーバーだけです。

名前	説明
[プロセッサ C6 レポート（Processor C6 Report）] ドロップダウン リスト	BIOS からオペレーティング システムに C6 レポートを送信するかどうか。OS はレポートを受信すると、プロセッサを電力量の少ない C6 状態に移行してエネルギー使用量を減らし、最適なプロセッサ パフォーマンスを維持できます。次のいずれかになります。 • [Disabled]：BIOS から C6 レポートを送信しません。 • [Enabled]：BIOS から C6 レポートを送信し、OS がプロセッサを電力量の少ない C6 状態に移行できるようにします。 （注） [CPUPowerManagement] を [カスタム（Custom）] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。 （注） このオプションを使用できるのは一部の C シリーズ サーバーだけです。
[XD ビット（Execute Disable Bit）] ドロップダウンリスト	アプリケーション コードを実行できる場所を指定するために、サーバーのメモリ領域を分類します。この分類の結果、悪意のあるワームがバッファにコードを挿入しようとした場合、プロセッサでコードの実行を無効化します。この設定は、損害、ワームの増殖、および特定クラスの悪意のあるバッファ オーバーフロー攻撃を防止するのに役立ちます。次のいずれかになります。 • [Disabled]：プロセッサでメモリ領域を分類しません。 • [有効（Enabled）]：プロセッサでメモリ領域を分類します。 （注） オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせください。

サーバー モデル別 BIOS パラメータ

名前	説明
[ターボ モード（Turbo Mode）] ドロップダウンリスト	プロセッサでインテル ターボ ブースト テクノロジーを使用するかどうか。このテクノロジーでは、仕様よりも低い電力、温度、または電圧でプロセッサが動作していると、自動的にそのプロセッサの周波数が上がります。次のいずれかになります。 • [Disabled]：プロセッサの周波数は自動的には上がりません。 • [Enabled]：必要に応じてプロセッサで Turbo Boost Technology が利用されます。 （注） [CPUPowerManagement] を [カスタム（Custom）] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[EIST PSD 関数（EIST PSD Function）] ドロップダウンリスト	EIST は、電圧と周波数のペア（P 状態）の変更に固有の遅延を短縮するため、これらの遷移がより頻繁に発生するようになります。これにより、より詳細なデマンドベースのスイッチングが可能になり、アプリケーションの要求に基づいて電力とパフォーマンスのバランスを最適化できます。次のいずれかになります。 • HW ALL：プロセッサは、論理プロセッサの依存関係間の P 状態を調整します。OS は、すべての論理プロセッサで P-state 要求を最新の状態に保ちます。 • SW ALL：OS Power Manager によって、依存関係にある論理プロセッサ間の P-state を調整します。すべての論理プロセッサで遷移を開始します。

名前	説明
[SpeedStep（Pstates）] ドロップダウンリスト	プロセッサで拡張版 Intel SpeedStep テクノロジーを使用するかどうか設定します。このテクノロジーでは、プロセッサの電圧やコア周波数をシステムが動的に調整できます。このテクノロジーにより、平均電力消費量と平均熱発生量が減少する可能性があります。次のいずれかになります。 • [Disabled]：プロセッサの電圧または周波数を動的に調整しません。 • [有効（Enabled）]：プロセッサで Enhanced Intel SpeedStep Technology が使用され、サポートされているすべてのスリープ状態でさらに電力を節約することが可能になります。 オペレーティングシステムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。 （注） [CPUPowerManagement] を [カスタム（Custom）] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[HyperThreading [All]] ドロップダウンリスト	プロセッサでインテル ハイパースレッディング テクノロジーを使用するかどうか。このテクノロジーでは、マルチスレッド ソフトウェア アプリケーションのスレッドを各プロセッサ内で並列に実行できます。次のいずれかになります。 • [Disabled]：プロセッサでのハイパースレッディングを禁止します。 • [有効（Enabled）]：プロセッサでの複数スレッドの並列実行を許可します。

サーバー モデル別 BIOS パラメータ

名前	説明
[コアは有効化されました（Cores Enabled）] ドロップダウンリスト	サーバー上の 1 つ以上の物理コアを無効にできます。次のいずれかになります。 • [All]：すべての物理コアをイネーブルにします。 これにより、関連付けられている論理プロセッサ コアで Hyper Threading もイネーブルになります。 • **[1] ～ [27]**：サーバーで実行できる物理プロセッサ コアの数を指定します。各物理コアには、論理コアが関連付けられています。 （注） オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせください。
[Processor CMCI] ドロップダウン リスト	CPU が corrected machine check events で割り込みをトリガーできるようにします。corrected machine check interrupt（CMCI）により、従来のポーリング タイマーよりも反応速度を向上できます。次のいずれかになります。 • [無効（Disabled）]：CMCI が無効になります。 • [有効（有効）]：CMCI が有効になります。これはデフォルト値です。

名前	説明
[Enhanced Intel SpeedStep Tech] ドロップダウン リスト	プロセッサで拡張版 Intel SpeedStep テクノロジーを使用するかどうか設定します。このテクノロジーでは、プロセッサの電圧やコア周波数をシステムが動的に調整できます。このテクノロジーにより、平均電力消費量と平均熱発生量が減少する可能性があります。次のいずれかになります。 • [Disabled]：プロセッサの電圧または周波数を動的に調整しません。 • [有効（Enabled）]：プロセッサで Enhanced Intel SpeedStep Technology が使用され、サポートされているすべてのスリープ状態でさらに電力を節約することが可能になります。 オペレーティングシステムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。 （注） [CPUPowerManagement] は、[カスタム（Custom）] に設定する必要があります。設定しな場合、サーバはこのパラメータの設定を無視します。
[Workload Configuration] ドロップダウン リスト	この機能を使用すると、ワークロードを最適化できます。オプションは [Balanced] と [I/O Sensitive] です。 • **NUMA** • **UMA**

名前	説明
[Sub NUMA Clustering] ドロップダウンリスト	CPUがサブNUMAクラスタリングをサポートするかどうか。そのクラスタリングでは、タグディレクトリとメモリチャネルは常に同じ領域にあります。次のいずれかになります。 • [disabled][Disabled]：サブNUMAクラスタリングは発生しません。 • [enabled][Enabled]：サブNUMAクラスタリングが発生します。 • [自動（Auto）][自動（auto）]：BIOSかサブNUMAのクラスタリングされるかが決まります。
エネルギー/パフォーマンスのバイアス構成	エネルギーまたはパフォーマンスのバイアス構成を表示します。 次のいずれかになります。 • Balanced Performance • Performance • Balanced Power • 電源
[IMC インターリーブ（IMC Interleaving）] ドロップダウンリスト	このBIOSオプションは、Integrated Memory Controller（IMC）間のインターリーブを制御します。 • [1-way Interleave]：インターリーブはありません。 • [2-way Interleave]：2つのIMC間でアドレスがインターリーブされます。 • [Auto]：CPUがIMCのインターリーブモードを決定します。

名前	説明
[XPT Prefetch] ドロップダウン リスト	XPT プリフェッチを使用して、最後のレベルのキャッシュに読み取り要求を送信できるようにして、その要求のコピーをメモリ コントローラのプリフェッチャに発行するかどうか。次のいずれかになります。 • [disabled][Disabled]：CPUは XPT Prefetch オプションを使用しません。 • [enabled][Enabled]：CPUはXPTプリフェッチ オプションを有効にします。
[UPI プリフェッチ（UPI Prefetch）] ドロップダウン リスト	UPI プリフェッチは、DDR バス上でメモリ読み込みが早期に開始されるようにするメカニズムです。これは次のいずれかになります。 • [無効（disabled）][無効（Disabled）]：プロセッサでキャッシュデータをプリロードしません。 • [有効（enabled）][有効（Enabled）]：UPIプリフェッチャで最も関連性が高いと判断されたデータを含むL1キャッシュをプリロードします。

名前	説明
[エネルギー パフォーマンスのバイアス構成（Energy/Performance Bias Config）] ドロップダウンリスト	システム パフォーマンスまたはエネルギー効率がこのサーバーで重要かどうかを判断できます。次のいずれかになります。 • [パフォーマンス（Performance）]：サーバーでは、すべてのサーバー コンポーネントに全電力を常時提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • [バランス パフォーマンス（Balanced Performance）]：サーバーは、すべてのサーバー コンポーネントに、パフォーマンスと電力のバランスを保つのに十分な電力を提供します。 • [バランス電力（Balanced Power）]：サーバーは、すべてのサーバー コンポーネントに、パフォーマンスと電力のバランスを保つのに十分な電力を提供します。 • [電力（Power）]：サーバーは、すべてのサーバー コンポーネントに、消費電力の低減を維持するのに最大の電力を提供します。
[電力パフォーマンスの調整（Power Performance Tuning）] ドロップダウン リスト	BIOS または OS によってエネルギー パフォーマンスのバイアス調整をオンにできるかどうかを指定します。オプションは [BIOS] と [OS] です。 • [bios][BIOS]： エネルギー効率を調整する場合は [BIOS] を選択します。 • [os][OS]： エネルギー効率を調整する場合は [OS] を選択します。

名前	説明
[LLC Prefetch] ドロップダウン リスト	プロセッサが LLC プリフェッチ メカニズムを使用して日付を LLC にフェッチするかどうか。次のいずれかになります。 • [disabled][Disabled]：プロセッサでキャッシュデータをプリロードしません。 • [enabled][Enabled]：LLCPrefetcher で最も関連性が高いと判断されたデータを含む L1 キャッシュをプリロードします。

名前	説明
[パッケージのCステート（Package C State）] ドロップダウン リスト	アイドル時にサーバー コンポーネントが使用できる電力量。次のいずれかになります。 • [no-limit][制限なし（No Limit）]：サーバーは、使用可能な任意のC ステートに入ることがあります。 • [自動（auto）][自動（Auto）]：物理的な高度をCPU が決定します。 • [C0 C1 ステート（C0 C1 State）]：サーバーはすべてのサーバー コンポーネントに常にフル パワーを提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • [C2]：CPU のアイドル時に、システムの電力消費をC1 オプションよりもさらに低減します。この場合、必要な電力はC1 または C0 よりも少なくなりますが、サーバーがハイ パフォーマンス モードに戻るのに要する時間が少し長くなります。 • [C6 保持なし（C6 Non Retention）]：CPU のアイドル時に、C3 オプションよりもさらに電力消費が低減されます。このオプションを使用すると、C0、C1、またはC3 よりも電力量が節約されますが、サーバーがフルパワーに戻るまでにパフォーマンス上の問題が発生する可能性があります。 • [C6 保持（C6 Retention）]：CPU のアイドル時に、C3 オプションよりもさらに電力消費が低減されます。このオプションを使用すると、C0、C1、または C3 よりも電力量が節約されますが、サーバーがフルパワーに戻るまでにパフォーマンス上の問題が発生する可能性があります。

名前	説明
[ハードウェア P ステート（Hardware P-States）] ドロップダウン リスト	プロセッサ ハードウェアの P ステートを有効にします。次のいずれかになります。 • [disabled][Disabled]：HWPMがディセーブルになります。 • [hwpm-native-mode][HWPM Native Mode]：HWPMネイティブ モードがイネーブルになります。 • [hwpm-oob-mode][HWPM OOB Mode]：HWPMアウトオブボックス モードがイネーブルになります。 • [Native Mode with no Legacy]（GUI のみ）
[Intel Speed Select (Intel の速度選択)] ドロップダウン リスト	**[Intel Speed Select (Intel の速度選択)]** モードでは、ユーザーは異なる速度とコアを使用して CPU を実行できます。 次のいずれかになります。 • **基本**): ユーザーは最大コアおよび熱設計電力 (TDP) 比率にアクセスすることができます。 • **設定 1** ユーザーは **基本**より小さいコアと TDP 比率にアクセスできます。 • **設定 2** ユーザーは **設定 1** より小さいコアと TDP 比率にアクセスできます。 デフォルト値: **基本**。
[非コア周波数スケーリング (Uncore Frequency Scaling)] ドロップダウンリスト	この機能を使用すると、プロセッサのコア以外の周波数のスケーリングを設定できます。次のいずれかになります。 • **[Enabled]**：プロセッサの非コア部分の周波数を、負荷に応じて上下します。 • **[無効 (Disabled)]**: プロセッサのコア以外の周波数を固定します。 『Intel® Dear Customer Letter (DCL)』には、固定されていない場合の **[非コア周波数スケーリング (Uncore Frequency Scaling)]** の固定の上限値と下限値が記されています。

名前	説明
[TDP の設定（Config TDP）]ドロップダウンリスト	**[TDP の設定（Config TDP）]**機能により、プロセッサの温度設計の電力値を調整できます。プロセッサの動作とパフォーマンス レベルを変更することにより、プロセッサの消費電力と TDP を同時に調整できます。したがって、プロセッサは、使用可能な冷却容量と望ましい消費電力に応じて、パフォーマンス レベルが高いまたは低い方で動作します。次のいずれかになります。 • **[標準 (Normal)]** • **[レベル 1 (Level 1)]** • **[レベル 2 (Level 2)]** TDP レベルの値については、『Intell® Dear Customer Letter (DCL)』を参照してください。
[UPI リンク速度（UPIH Link Speed）] ドロップダウンリスト	（注） **[UPI リンク周波数選択 (UPI Link Frequency Select)]** トークンは、単一ソケット構成には適用されません。 この機能を使用すると、複数のソケット間の Intel Ultra Path Interconnect (UPI) リンク速度を設定できます。次のいずれかになります。 • **[自動 (auto)]**]: このオプションは、最適なリンク速度を自動的に設定します。 • **[9.6 GT/s]**: このオプションは、最適なリンク速度として 9.6GT/s を使用します。 • **[10.4 GT/s]**—このオプションは、最適なリンク速度として 10.4GT/s を使用します。

名前	説明
[エネルギー効率ターボ（Energy Efficient Turbo）] ドロップダウンリスト	エネルギー効率の高いターボが有効になっている場合、CPUの最適なターボ周波数は、CPU使用率に基づいてダイナミックになります。パワー/パフォーマンスのバイアス設定も、エネルギー効率の高いターボに影響します。次のいずれかになります。 • **[無効（Disabled）]**：エネルギー効率ターボが無効です。 • **[有効（Enabled）]**：エネルギー効率ターボが有効です。
プロセッサEPPの有効化	プロセッサ EPP の有効化で選択した値を表示します。 • **[無効（Dissabled）]**：プロセッサ EPP の有効化が無効です。 • **[有効（Enabled）]**：プロセッサ EPP の有効化が有効です。
[自律コア C 状態（Autonomous Core C-state）] ドロップダウンリスト	HALT 命令を MWAIT 命令に変換する CPU Autonomous C-State を有効にします。次のいずれかになります。 • [Disabled]：CPU Autonomous C-state が無効です。 • [有効（Enabled）]：CPU 自律 C-state が有効になります。

名前	説明
[パトロール スクラブ（Patrol Scrub）] ドロップダウンリスト	システムにサーバーのメモリ（未使用部分も含む）における単一ビット メモリ エラーを検出させて修復させることが可能です。次のいずれかになります。 • [Disabled]：CPU がメモリ アドレスの読み取りまたは書き込みを行うときのみ、システムはメモリの ECC エラーをチェックします。 • [有効（Enabled）]：システムは定期的にメモリを読み書きして ECC エラーを探します。エラーが見つかると、システムは修復を試みます。このオプションにより、単一ビット エラーは複数ビット エラーになる前に修正される場合がありますが、パトロール スクラブの実行時にパフォーマンスが低下する場合もあります。 • **[POST の最後に有効化する（Enable at End of POST）]**：システムは、BIOS POST 後にメモリ ECC エラーをチェックします。
[プロセッサ EPP プロファイル（Processor EPP Profile）] ドロップダウンリスト	システム パフォーマンスまたはエネルギー効率がこのサーバーで重要かどうかを判断できます。次のいずれかになります。 • Performance • Balanced Performance • Balanced Power • 電源

メモリ タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *55 : [*メモリ（*Memory*）*]* タブの *BIOS* パラメータ

名前	説明
[今すぐホストを再起動（Reboot Host Immediately）] チェックボックス	このチェックボックスをオンにすると、直ちにホスト サーバが再起動します。このチェックボックスは、変更を保存してからオンにする必要があります。
[メモリ RAS 構成の選択（Select Memory RAS configuration）] ドロップダウン リスト	サーバーに対するメモリの信頼性、可用性、およびサービス性（RAS）の設定方法。次のいずれかになります。 • [最大パフォーマンス（Maximum Performance）] : システムのパフォーマンスが最適化されます。 • **ADDDC のスペアリング**: 適応可能な仮想ロックステップは、ADDDC モードをサポートするためにハードウェアおよびファームウェアで実装されるアルゴリズムです。選択すると、アルゴリズムがアクティブになるまでシステムのパフォーマンスが最適化されます。このアルゴリズムは、DRAM デバイスで障害が発生した場合にアクティブになります。アルゴリズムがアクティブになると、仮想ロックステップ リージョンがアクティブになり、実行時に障害が発生したリージョンが動的にマッピングされ、パフォーマンスへの影響はリージョン レベルで制限されます。 • [ミラー モード 1LM（Mirror Mode 1LM）] : システムのメモリの半分をバックアップとして使用することにより、システムの信頼性が最適化されます。 • **部分的なミラー モード 1LM**: 部分的な DIMM ミラーリングによって完全なミラーコピーを保持するのではなく、メモリ セルの特定の領域のミラーコピーが作成されます。部分的なミラーリングでは、部分的なミラー コピーの属性を使用して、メモリ マップにミラー領域が作成されます。最大 4 個の部分的なミラーを使用して、合計メモリ容量の最大 50% をミラーリングできます。

サーバー モデル別 BIOS パラメータ

名前	説明
[4 G 以上の復号化（Above 4G Decoding）] ドロップダウン リスト	4 GB 以上の MMIO を有効または無効にします。次のいずれかになります。 • [Disabled]：サーバーでは 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングしません。 • [有効（Enabled）]：サーバで 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングします。 （注） PCI デバイスが 64 ビット対応でも、レガシーなオプション ROM を使用する場合は、この設定をイネーブルにしても正しく機能しない場合があります。
[DCPMM Firmware Downgrade (DCPMM ファームウェアのダウングレード)]ドロップダウン リスト	BIOS が DCPMM ファームウェアのダウングレードをサポートしているかどうか。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[Partial Memory Mirror Mode (部分メモリ ミラー モード)]ドロップダウン リスト	部分的なメモリ サイズは、パーセンテージまたは GB 単位のいずれかです。次のいずれかになります。 • **割合**:部分的なメモリのミラーはパーセンテージで定義されます。 • **値 (GB)**: 部分的なメモリ ミラーは GB で定義されます。 • **無効**:部分的なメモリ ミラーが無効になります。
[部分的なミラー パーセンテージ (Partial Mirror percentage)] フィールド	4GBを超えてミラーリングするメモリの割合。 0 ～ 60 の整数を入力します。

名前	説明
[部分ミラー 1 サイズ (GB) (Partial Mirror1 Size in GB)] フィールド	最初の部分メモリ ミラーのサイズ (GB)。 0 ～ 65535 の整数を入力します。 （注） すべての部分的なミラーの合計メモリ サイズは、物理メモリ サイズの 50% を超えないようにする必要があります。
[部分ミラー 2 サイズ (GB) (Partial Mirror2 Size in GB)] フィールド	2 番目の部分メモリ ミラーのサイズ (GB 単位)。 0 ～ 65535 の整数を入力します。 （注） すべての部分的なミラーの合計メモリ サイズは、物理メモリ サイズの 50% を超えないようにする必要があります。
[部分ミラー 3 サイズ (GB) (Partial Mirror3 Size in GB)] フィールド	3 番目の部分メモリ ミラーのサイズ (GB 単位)。 0 ～ 65535 の整数を入力します。 （注） すべての部分的なミラーの合計メモリ サイズは、物理メモリ サイズの 50% を超えないようにする必要があります。
[部分ミラー 4 サイズ (GB) (Partial Mirror4 Size in GB)] フィールド	4 番目の部分メモリ ミラーのサイズ (GB 単位)。 0 ～ 65535 の整数を入力します。 （注） すべての部分的なミラーの合計メモリ サイズは、物理メモリ サイズの 50% を超えないようにする必要があります。
[メモリ サイズ制限 (GB) (Memory Size Limit in GB)] フィールド	このオプションを使用して、物理メモリの上限のサイズを GB 単位で減らします。 0 ～ 65535 の整数を入力します。

名前	説明
[NUMA] ドロップダウン リスト	BIOS で Non-Uniform Memory Access（NUMA）がサポートされているかどうか。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[BME DMA 移行 (BME DMA Mitigation)] ドロップダウン リスト	不正な外部 DMA からの脅威を緩和する PCI BME ビットを無効にできます。次のいずれかになります。 • **[無効 (disabled)]**: PCI BME ビットは BIOS で無効になっています。 • **[有効 (Enabled)**: PCI BME ビットは BIOS で有効になっています。
[ディスク タイプの選択 (Select Disk Type)] ドロップダウン リスト	Cisco IMC は、指定された障害のある行から指定されたスペア行へのアクセスを永続的に再マッピングする、**ハード PPR**をサポートしています。 次のいずれかになります。 • **[ハード PPR (Hard PPR)]**: サポートは有効になっています。 （注） ハード PPR は、**[メモリ RAS 設定 (Memory RAS Configuration)]**が **[ADDDC スペア (ADDDC Sparing)]**に設定されている場合にのみ使用できます。他の RA の選択では、この設定を**Disabled**に設定する必要があります。 • **[無効 (Disabled)]**：サポートは無効になっています。

名前	説明
[CR QoS] ドロップダウンリスト	CR QoS 調整を選択できます。 次のいずれかになります。 • **[レシピ 1 (Recipe 1)]**: QoS ノブ向けで、アクティブなディレクトリでの2-2-2メモリ設定に推奨されます。 • **[レシピ 2 (Recipe 2)]**: QoS ノブ向けで、アクティブなディレクトリでの他のメモリ設定に推奨されます。 • **[レシピ 3 (Recipe 3)]**: QoS ノブ向けで、チャネルごとに1つの DIMM を設定することを推奨します。 • **[無効 (Disabled)]**:**CR QoS**機能は無効になります。
[AD の Snoopy モード (Snoopy mode for AD)] ドロップダウン リスト	新しい AD 固有の機能を有効にして、NUMA に最適化されていないワークロードからDDRTメモリへのディレクトリ更新を回避します。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[CR Fastgo Config] ドロップダウンリスト	CR QoS 設定プロファイルを選択できるようにします。 次のいずれかになります。 • **デフォルト (Default)** • **オプション 1 (Option 1)** • **オプション 2 (Option 2)** • **オプション 3 (Option 3)** • **オプション 4 (Option 4)** • **オプション 5 (Option 5)** • **自動 (Auto)**

サーバー モデル別 BIOS パラメータ

名前	説明
[NVM パフォーマンス設定 (NVM Performance Setting)] ドロップダウンリスト	ワークロードの動作に応じて、NVMベースラインのパフォーマンス設定を設定できます。 • **BW 最適化** • **遅延の最適化** • **バランス プロファイル**
[2LM の Snoopy モード (Snoopy mode for 2LM)] ドロップダウン リスト	NUMA に最適化されていないワークロードからfarメモリへのディレクトリ更新を回避できます。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[メモリ サーマル スロットリング モード（Memory Thermal Throttling Mode）] ドロップダウンリスト	この関数は、メモリ温度の調整に使用されます。この機能を有効にした後、メモリ温度が極端に高くなると、メモリアクセスレートが低下し、Baseboard Management Controller（BMC）がファンを調整してメモリを冷却し、DIMM の損傷を防ぎます。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • **PECI を使用した CLTT**：プラットフォーム環境制御インターフェイスを使用してクローズドループ サーマル スロットリングを有効にします。

名前	説明
[メモリ リフレッシュ レート（Memory Refresh Rate）] ドロップダウンリスト	メモリのリフレッシュ レートを増減できます。DRAM のリフレッシュ レートを上げると、次のリフレッシュの前に発生する可能性のあるアクティブ化（ハンマー）の最大数が減少します。 次のいずれかになります。 • **[1X リフレッシュ（1X Refresh）]**：リフレッシュ レートは最小です。 • **[2X リフレッシュ（2X Refresh）]**：リフレッシュは 2 倍高速です。
[パニックと高水準点（Panic and High Watermark）] ドロップダウンリスト	低に設定した場合、**[メモリ更新レート（Memory Refresh Rate）]** が **[1X リフレッシュ（1X Refresh）]** に設定されている間、メモリコントローラは更新を延期しません。 次のいずれかになります。 • **[低（Low）]**：リフレッシュ レートは低に設定します。 • **[高（High）]**：リフレッシュ レートは高に設定します。
[高度なメモリ テスト（Advanced Memory Test）] ドロップダウンリスト	（注） この機能は、Samsung、Hynix、および Micron DIMM にのみ適用されます。 この機能を使用して、BIOS POST 中に高度な DIMM テストを有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

名前	説明
[拡張メモリ テスト（Enhanced Memory Test）] ドロップダウンリスト	次のいずれかになります。 • **[自動（Auto）]**：サポートは自動に設定されています。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

[電源/パフォーマンス（Power/Performance）] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

表 *56 : [*電源/パフォーマンス（*Power/Performance*）*]* タブの *BIOS* パラメータ

名前	説明
[今すぐホストを再起動（Reboot Host Immediately）] チェックボックス	このチェックボックスをオンにすると、直ちにホスト サーバが再起動します。このチェックボックスは、変更を保存してからオンにする必要があります。
[ハードウェア プリフェッチャ（Hardware Prefetcher）] ドロップダウン リスト	プロセッサで、インテル ハードウェア プリフェッチャが必要に応じてデータおよび命令ストリームをメモリから取得し、統合 2 次キャッシュに入れることを許可するかどうか。次のいずれかになります。 • [Disabled]：ハードウェア プリフェッチャは使用しません。 • [Enabled]：プロセッサで、キャッシュの問題が検出されたときにプリフェッチャを使用します。
[隣接キャッシュ ライン プリフェッチャ（Adjacent Cache Line Prefetcher）] ドロップダウン リスト	プロセッサで必要な行のみを取得するのではなく、偶数または奇数のペアのキャッシュ行を取得するかどうか。次のいずれかになります。 • [Disabled]：プロセッサで必要な行のみを取得します。 • [Enabled]：プロセッサで必要な行およびペアの行の両方を取得します。

名前	説明
[DCU ストリーマ プリフェッチ（DCU Streamer Prefetch）] ドロップダウン リスト	プロセッサで DCU IP プリフェッチ メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。次のいずれかになります。 • [Disabled]：プロセッサはキャッシュ読み取り要求を予測しようとせず、明示的に要求された行のみを取得します。 • [Enabled]：DCU Prefetcher でキャッシュ読み取りパターンを分析し、必要と判断した場合にキャッシュ内の次の行を事前に取得します。
[DCU IP プリフェッチャ（DCU IP Prefetcher）] ドロップダウン リスト	プロセッサで DCU IP プリフェッチ メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。次のいずれかになります。 • [Disabled]：プロセッサでキャッシュ データをプリロードしません。 • [Enabled]：DCU IP プリフェッチャで最も関連性が高いと判断されたデータを含む L1 キャッシュをプリロードします。
[CPU パフォーマンス（CPU Performance）] ドロップダウン リスト	上記のオプションに対し CPU パフォーマンス プロファイルを設定します。次のいずれかになります。 • [Enterprise]：すべてのオプションがイネーブルです。 • [HPC]：すべてのオプションがイネーブルです。この設定はハイ パフォーマンス コンピューティングとも呼ばれます。 • [高スループット（Hight Throughput）]：DCU IP Prefetcher のみが有効です。残りのオプションは無効になります。 • [Custom]：パフォーマンス プロファイルのすべてのオプションをサーバの BIOS セットアップから設定できます。さらに、[ハードウェア プリフェッチャ（Hardware Prefetcher）] オプションと [隣接キャッシュ：ライン プリフェッチ（Adjacent Cache-Line Prefetch）] オプションも設定できます。

C460 M4 サーバ

C460 M4 サーバの [メイン（Main）] タブ

主要な BIOS パラメータ

名前	説明
[今すぐホストを再起動（Reboot Host Immediately）] チェックボックス	このチェックボックスをオンにすると、直ちにホスト サーバが再起動します。このチェックボックスは、変更を保存してからオンにする必要があります。
[TPM Support]	TPM（トラステッドプラットフォームモジュール）は、主に暗号キーを使用する基本的なセキュリティ関連機能を提供するように設計されたマイクロチップです。このオプションを使用すると、システムの TPM セキュリティ デバイス サポートを制御できます。次のいずれかを指定できます。 • [Disabled]：サーバーは TPM を使用しません。 • [有効（Enabled）]：サーバは TPM を使用します。 （注） オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。
[Power ON Password Support] ドロップダウン	このトークンでは、F2 BIOS 設定を使用する前に BIOS パスワードを設定する必要があります。有効にすると、BIOS 関数（IO 設定、BIOS セットアップ、BIOS を使用したオペレーティング システムへのブート）にアクセスする前にパスワードの検証が必要になります。次のいずれかを指定できます。 • **[無効（Disabled）]**：サポートは無効になります。 • **[有効（Enabled）]**：サポートは有効になります。

[Actions] 領域

名前	説明
[**Save**] ボタン	BIOS パラメータの設定を保存して、ダイアログボックスを閉じます。 **[Reboot Host Immediately]** チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[Reset] ボタン	3 つすべてのタブ上の BIOS パラメータの値が、このダイアログボックスを最初に開いた際に有効だった設定にリセットされます。
[Restore Defaults] ボタン	3 つのタブすべての BIOS パラメータをそのデフォルト値に設定します。

C460 M4 サーバの [詳細設定（Advanced）] タブ

サーバ リブート オプション

[Save Changes] をクリックした後で変更内容を自動的に適用するには、[Reboot Host Immediately] チェックボックスをオンにします。Cisco IMC によってサーバがただちにリブートされて、変更が適用されます。

変更内容を後で適用するには、[Reboot Host Immediately] チェックボックスをオフにします。Cisco IMC によって変更が保存され、次回サーバがリブートするときに適用されます。

（注） 保留中の BIOS パラメータの変更がすでにある場合、Cisco IMC は、[Save Changes] をクリックしたときに、保存されている値を現在の設定で自動的に上書きします。

サーバー モデル別 BIOS パラメータ

[Processor Configuration] のパラメータ

名前	説明
[Intel Hyper-Threading Technology] ドロップダウン リスト	プロセッサでインテル ハイパースレッディング テクノロジーを使用するかどうか。このテクノロジーでは、マルチスレッド ソフトウェア アプリケーションのスレッドを各プロセッサ内で並列に実行できます。次のいずれかになります。 • [Disabled]：プロセッサでのハイパースレッディングを禁止します。 • [有効（Enabled）]：プロセッサでの複数スレッドの並列実行を許可します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。
[有効化されたコア数（Number of Enabled Cores）] ドロップダウン リスト	サーバー上の 1 つ以上の物理コアを無効にできます。次のいずれかになります。 • [All]：すべての物理コアをイネーブルにします。これにより、関連付けられている論理プロセッサ コアで Hyper Threading もイネーブルになります。 • [1] ～ [***n***]：サーバで実行できる物理プロセッサ コアの数を指定します。各物理コアには、論理コアが関連付けられています。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせてください。

名前	説明
[Execute Disable] ドロップダウン リスト	アプリケーション コードを実行できる場所を指定するために、サーバーのメモリ領域を分類します。この分類の結果、悪意のあるワームがバッファにコードを挿入しようとした場合、プロセッサでコードの実行を無効化します。この設定は、損害、ワームの増殖、および特定クラスの悪意のあるバッファ オーバーフロー攻撃を防止するのに役立ちます。次のいずれかになります。 • [Disabled]：プロセッサでメモリ領域を分類しません。 • [有効（Enabled）]：プロセッサでメモリ領域を分類します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。
[Intel VT]	プロセッサで Intel Virtualization Technology（VT）を使用するかどうか。このテクノロジーでは、1つのプラットフォームで、複数のオペレーティング システムとアプリケーションをそれぞれ独立したパーティション内で実行できます。次のいずれかになります。 • [Disabled]：プロセッサでの仮想化を禁止します。 • [有効（Enabled）]：プロセッサで、複数のオペレーティングシステムをそれぞれ独立したパーティション内で実行できます。 （注） このオプションを変更した場合は、設定を有効にするためにサーバーの電源を再投入する必要があります。
[Intel VT-d]	Intel Virtualization Technology for Directed I/O（VT-d）をプロセッサで使用するかどうか。次のいずれかになります。 • [Disabled]：プロセッサで仮想化テクノロジーを使用しません。 • [Enabled]：プロセッサで仮想化テクノロジーを使用します。

名前	説明
[Intel(R) 割り込み再マッピング（Intel(R) Interrupt Remapping）] ドロップダウン リスト	プロセッサで Intel VT-d Interrupt Remapping をサポートするかどうか。次のいずれかになります。 • [Disabled]：プロセッサでリマッピングをサポートしません。 • [Enabled]：プロセッサで VT-d Interrupt Remapping を必要に応じて使用します。
[Intel(R) パススルー DMA（Intel(R) Passthrough DMA）] ドロップダウン リスト	プロセッサで Intel VT-d Pass-through DMA をサポートするかどうか。次のいずれかになります。 • [Disabled]：プロセッサでパススルー DMA をサポートしません。 • [Enabled]：プロセッサで VT-d Pass-through DMA を必要に応じて使用します。
[Intel VT-d Coherency Support]	プロセッサで Intel VT-d Coherency をサポートするかどうか。次のいずれかになります。 • [Disabled]：プロセッサでコヒーレンシをサポートしません。 • [Enabled]：プロセッサで VT-d Coherency を必要に応じて使用します。
[Intel VT-d ATS Support]	プロセッサで Intel VT-d Address Translation Services（ATS）をサポートするかどうか。次のいずれかになります。 • [Disabled]：プロセッサで ATS をサポートしません。 • [Enabled]：プロセッサで VT-d ATS を必要に応じて使用します。

名前	説明
[CPU Performance]	サーバーのCPUパフォーマンス プロファイルを設定します。パフォーマンス プロファイルは次のオプションで構成されます。 • DCU Streamer Prefetcher • DCU IP Prefetcher • ハードウェア プリフェッチャ • Adjacent Cache-Line Prefetch 次のいずれかになります。 • [Enterprise]：すべてのオプションがイネーブルです。 • [High Throughput]：DCU IP Prefetcher のみがイネーブルです。残りのオプションはディセーブルになります。 • [HPC]：すべてのオプションがイネーブルです。この設定はハイ パフォーマンス コンピューティングとも呼ばれます。 • [Custom]：パフォーマンス プロファイルのすべてのオプションをサーバの BIOS セットアップから設定できます。また、Hardware Prefetcher オプションと Adjacent Cache-Line Prefetch オプションは、下記のフィールドで設定できます。
[ハードウェア プリフェッチャ（Hardware Prefetcher）] ドロップダウン リスト	プロセッサで、インテル ハードウェア プリフェッチャが必要に応じてデータおよび命令ストリームをメモリから取得し、統合 2 次キャッシュに入れることを許可するかどうか。次のいずれかになります。 • [Disabled]：ハードウェア プリフェッチャは使用しません。 • [Enabled]：プロセッサで、キャッシュの問題が検出されたときにプリフェッチャを使用します。

名前	説明
[隣接キャッシュラインプリフェッチャ（Adjacent Cache Line Prefetcher）] ドロップダウン リスト	プロセッサで必要な行のみを取得するのではなく、偶数または奇数のペアのキャッシュ行を取得するかどうか。次のいずれかになります。 • [Disabled]：プロセッサで必要な行のみを取得します。 • [有効（Enabled）]：プロセッサで必要な行およびペアの行の両方を取得します。
[DCUストリーマープリフェッチ（DCU Streamer Prefetch）] ロップダウン リスト	プロセッサで DCU IP プリフェッチ メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。次のいずれかになります。 • [Disabled]：プロセッサはキャッシュ読み取り要求を予測しようとせず、明示的に要求された行のみを取得します。 • [Enabled]：DCU Prefetcher でキャッシュ読み取りパターンを分析し、必要と判断した場合にキャッシュ内の次の行を事前に取得します。
[DCU IPプリフェッチャ（DCU IP Prefetcher）] ドロップダウン リスト	プロセッサで DCU IP プリフェッチ メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。次のいずれかになります。 • [Disabled]：プロセッサでキャッシュ データをプリロードしません。 • [Enabled]：DCU IP プリフェッチャで最も関連性が高いと判断されたデータを含むL1 キャッシュをプリロードします。
[ダイレクトキャッシュアクセスサポート（Direct Cache Access Support）] ドロップダウン リスト	プロセッサで、データをI/Oデバイスから直接プロセッサ キャッシュに入れることにより、I/O パフォーマンスを向上させることができます。この設定はキャッシュ ミスを減らすのに役立ちます。次のいずれかになります。 • [Disabled]：データはI/Oデバイスから直接プロセッサ キャッシュには入れられません。 • [Enabled]：データはI/Oデバイスから直接プロセッサ キャッシュに入れられます。

名前	説明
[Power Technology]	次のオプションの CPU 電源管理設定を指定できます。 • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 [Power Technology] は次のいずれかになります。 • [Custom]：前述の BIOS パラメータの個々の設定が使用されます。これらの BIOS パラメータのいずれかを変更する場合は、このオプションを選択する必要があります。 • [Disabled]：サーバーで CPU 電源管理は実行されず、前述の BIOS パラメータの設定が無視されます。 • [Energy Efficient][Energy_Efficient]：前述の BIOS パラメータに最適な設定が決定され、これらのパラメータの個々の設定は無視されます。
[Enhanced Intel Speedstep Technology] ドロップダウン リスト	プロセッサで拡張版 Intel SpeedStep テクノロジーを使用するかどうか設定します。このテクノロジーでは、プロセッサの電圧やコア周波数をシステムが動的に調整できます。このテクノロジーにより、平均電力消費量と平均熱発生量が減少する可能性があります。次のいずれかになります。 • [Disabled]：プロセッサの電圧または周波数を動的に調整しません。 • [有効（Enabled）]：プロセッサで Enhanced Intel SpeedStep Technology が使用され、サポートされているすべてのスリープ状態でさらに電力を節約することが可能になります。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。 （注） [Power Technology][CPUPowerManagement] を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。

名前	説明
[Intel Turbo Boost Technology]	プロセッサでインテル ターボ ブースト テクノロジーを使用するかどうか。このテクノロジーでは、仕様よりも低い電力、温度、または電圧でプロセッサが動作していると、自動的にそのプロセッサの周波数が上がります。次のいずれかになります。 • [Disabled]：プロセッサの周波数は自動的には上がりません。 • [Enabled]：必要に応じてプロセッサで Turbo Boost Technology が利用されます。 （注） [Power Technology][CPUPowerManagement] を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[Processor C3 Report]	BIOS からオペレーティング システムに C3 レポートを送信するかどうか。OS はレポートを受信すると、プロセッサを電力量の少ない C3 状態に移行してエネルギー使用量を減らし、最適なプロセッサ パフォーマンスを維持できます。次のいずれかになります。 • [Disabled]：BIOS は C3 レポートの送信を行いません。 • [Enabled]：BIOS から C3 レポートを送信し、OS がプロセッサを電力量の少ない C3 状態に移行できるようにします。 （注） [Power Technology][CPUPowerManagement] を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。

名前	説明
[Processor C6 Report]	BIOS からオペレーティング システムに C6 レポートを送信するかどうか。OS はレポートを受信すると、プロセッサを電力量の少ない C6 状態に移行してエネルギー使用量を減らし、最適なプロセッサ パフォーマンスを維持できます。次のいずれかになります。 • [Disabled]：BIOS から C6 レポートを送信しません。 • [Enabled]：BIOS から C6 レポートを送信し、OS がプロセッサを電力量の少ない C6 状態に移行できるようにします。 （注） [Power Technology][CPUPowerManagement] を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[プロセッサの電源状態C1拡張（Processor Power State C1 Enhanced）] ドロップダウン リスト	C1 ステートに入ったときに、CPU が最小周波数に移行するかどうか。次のいずれかになります。 • [無効（Disabled）]：CPU は C1 ステートでも引き続き最大周波数で動作します。 • [有効（Enabled）]：CPU は最小周波数に移行します。このオプションでは C1 ステートで節約される電力量が最大になります。

サーバー モデル別 BIOS パラメータ

名前	説明
[P-STATE調整（P-STATE Coordination）] ドロップダウン リスト	BIOS がオペレーティング システムに P-state サポート モデルを伝達する方法を定義できます。Advanced Configuration and Power Interface（ACPI）仕様では、次の 3 つのモデルが定義されています。 • [HW_ALL]：プロセッサ ハードウェアによって、依存関係にある論理プロセッサ（パッケージ内のすべての論理プロセッサ）間の P-state を調整します。 • [SW_ALL]：OS Power Manager（OSPM）によって、依存関係にある論理プロセッサ（物理パッケージ内のすべての論理プロセッサ）間の P-state を調整します。すべての論理プロセッサで遷移を開始する必要があります。 • [SW_ANY]：OS Power Manager（OSPM）によって、依存関係にある論理プロセッサ（パッケージ内のすべての論理プロセッサ）間の P-state を調整します。ドメイン内の任意の論理プロセッサで遷移を開始できます。 （注） [Power Technology][CPUPowerManagement] を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[SINGLE_PCTL] ドロップダウン リスト	プロセッサの電源管理を向上させるために単一 PCTL サポートを促進します。次のいずれかになります。 • **[いいえ（No）]** • ○
[TDPの設定（Config TDP）] ドロップダウン リスト	システムの熱設計電力（TDP）を設定できます。TDP は、過熱イベントを引き起こすことなくアプリケーションを実行できる最大電力量です。次のいずれかになります。 • [無効（Disabled）]：TDP の設定を無効にします。これはデフォルト値です。 • [有効（Enabled）]：TDP の設定を有効にします。

名前	説明
[エネルギーパフォーマンスの調整（Energy Performance Tuning）] ドロップダウン リスト	エネルギー効率のバイアス調整のために BIOS またはオペレーティング システムを選択できます。次のいずれかになります。 • [OS]：エネルギーパフォーマンスの調整にOSを選択します。 • [BIOS]：エネルギー効率の調整のために BIOS を選択します。
[エネルギーパフォーマンス（Energy Performance）] ドロップダウン リスト	システム パフォーマンスまたはエネルギー効率がこのサーバーで重要かどうかを判断できます。次のいずれかになります。 • **Balanced Energy** • **Balanced Performance** • **Energy Efficient** • **Performance**

名前	説明
[パッケージのCステートの制限（Package C State Limit）] ドロップダウン リスト	アイドル時にサーバー コンポーネントが使用できる電力量。次のいずれかになります。 • [C0 state][C0_state]：サーバーはすべてのサーバー コンポーネントに常にフルパワーを提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • **[C1 state]**：CPU のアイドル時に、システムは電力消費を少し減らします。このオプションでは、必要な電力が C0 よりも少なく、サーバーはすばやくハイ パフォーマンス モードに戻ることができます。 • **[C3 state]**：CPU のアイドル時に、システムは C1 オプションの場合よりもさらに電力消費を減らします。この場合、必要な電力は C1 または C0 よりも少なくなりますが、サーバーがハイ パフォーマンス モードに戻るのに要する時間が少し長くなります。 • **[C6 state]**：CPU のアイドル時に、システムは C3 オプションの場合よりもさらに電力消費を減らします。このオプションを使用すると、C0、C1、または C3 よりも電力量が節約されますが、サーバーがフルパワーに戻るまでにパフォーマンス上の問題が発生する可能性があります。 • **[C7 state]**：CPU のアイドル時に、サーバはコンポーネントが使用できる電力量を最小にします。このオプションでは、節約される電力量が最大になりますが、サーバーがハイ パフォーマンス モードに戻るのに要する時間も最も長くなります。 • **[No Limit]**：サーバは、使用可能な任意の C ステートに入ることがあります。
[Extended APIC]	拡張 APIC サポートをイネーブルまたはディセーブルにできます。次のいずれかになります。 • [XAPIC]：APIC サポートを有効にします。 • [X2APIC]：APIC を有効にして、Intel VT-d と Interrupt Remapping も有効にします。

名前	説明
[Workload Configuration]	ワークロードの特性を最適化するようにパラメータを設定できます。次のいずれかになります。 • [Balanced]：最適化のためにバランスのとれたオプションを選択します。 • [I/O Sensitive]：最適化のために I/O を考慮したオプションを選択します。 （注） ワークロード構成は [Balanced] に設定することをお勧めします。
[IIO エラーの有効化（IIO Error Enable）] ドロップダウン リスト	IIO 関連のエラーを生成できます。次のいずれかになります。 • 〇 • **[いいえ（No）]**

[Memory Configuration] のパラメータ

名前	説明
[Select Memory RAS]	サーバーに対するメモリの信頼性、可用性および機密性（RAS）の設定方法。次のいずれかになります。 • **[Maximum Performance]**：システムのパフォーマンスが最適化されます。 • [Mirroring]：システムのメモリの半分をバックアップとして使用することにより、システムの信頼性が最適化されます。 • [Lockstep]：サーバ内の DIMM ペアが、同一のタイプ、サイズ、および構成を持ち、SMI チャネルにまたがって装着されている場合、ロックステップ モードをイネーブルにすることで、メモリ アクセス遅延の最小化およびパフォーマンスの向上を図ることができます。このオプションを使用した場合、[Mirroring] よりもシステム パフォーマンスが向上し、[Maximum Performance] よりも信頼性が向上しますが、[Mirroring] よりも信頼性が低く、[Maximum Performance] よりもシステム パフォーマンスは低下します。

サーバー モデル別 BIOS パラメータ

名前	説明
[DRAMクロックスロットリング（DRAM Clock Throttling）] ドロップダウン リスト	メモリ帯域幅と消費電力に関してシステム設定を調整できます。次のいずれかになります。 • [Balanced]：DRAM クロック スロットリングを低下させ、パフォーマンスと電力のバランスをとります。 • [Performance]：DRAM クロック スロットリングを無効化し、追加の電力を使用してメモリ帯域幅を増やします。 • [Energy Efficient]：DRAM のクロックスロットリングを上げてエネルギー効率を向上させます。
[低電圧DDRモード（Low Voltage DDR Mode）] ドロップダウン リスト	低電圧と高周波数のどちらのメモリ動作をシステムで優先するか。次のいずれかになります。 • [Power Saving Mode][Power_Saving_Mode]：低電圧のメモリ動作が高周波数のメモリ動作よりも優先されます。 このモードでは、電圧を低く維持するために、メモリの周波数が低下する可能性があります。 • [Performance Mode][Performance_Mode]：高周波数の動作が低電圧の動作よりも優先されます。
[クローズドループ サーマル スロッティング（Closed Loop Therm Throt）] ドロップダウン リスト	閉ループ サーマル スロットリングのサポートを可能にします。これにより信頼性が向上し、CPU がアイドル状態の間は自動電圧制御により CPU の電力消費が低減します。次のいずれかになります。 • [無効（Disabled）]：閉ループ サーマル スロットリングを無効にします。 • [有効（Enabled）]：閉ループ サーマル スロットリングを有効にします。これがデフォルト値です。

名前	説明
[チャネルインターリーブ（Channel Interleaving）] ドロップダウン リスト	CPU がメモリ ブロックを分割して、インターリーブされたチャネル間にデータの連続部分を分散し、同時読み取り動作を有効にするかどうか。次のいずれかになります。 • [Auto]：実行するインターリーブを、CPU が決定します。 • [1 Way][1_Way]：一部のチャネルインターリーブが使用されます。 • [2 Way][2_Way] • [3 Way][3_Way] • [4 Way][4_Way]：最大のチャネルインターリーブが使用されます。
[Rank Interleaving]	1 つのランクを更新中に別のランクにアクセスできるよう、CPU がメモリの物理ランクをインターリーブするかどうか。次のいずれかになります。 • [Auto]：実行するインターリーブを、CPU が決定します。 • [1 Way][1_Way]：一部のランクインターリーブが使用されます。 • [2 Way][2_Way] • [4 Way][4_Way] • [8 Way][8_Way]：最大量のランクインターリーブが使用されます。

サーバー モデル別 BIOS パラメータ

名前	説明
[Patrol Scrub]	システムがサーバー上のメモリの未使用部分でも単一ビット メモリ エラーをアクティブに探して訂正するかどうか。次のいずれかになります。 • [Disabled]：CPUがメモリ アドレスの読み取りまたは書き込みを行うときのみ、システムはメモリのECC エラーをチェックします。 • [有効（Enabled）]：システムは定期的にメモリを読み書きしてECCエラーを探します。エラーが見つかると、システムは修復を試みます。このオプションにより、単一ビット エラーは複数ビット エラーになる前に修正される場合がありますが、パトロール スクラブの実行時にパフォーマンスが低下する場合もあります。
[デマンドスクラブ（Demand Scrub）] ドロップダウン リスト	CPU または I/O から読み取り要求があった時に発生したシングル ビット メモリ エラーを、システムで修正するかどうか。次のいずれかになります。 • [無効（Disabled）]：シングル ビット メモリ エラーは修正されません。 • [Enabled]：シングル ビット メモリ エラーがメモリ内部で修正され、修正されたデータが読み取り要求に応じて設定されます。
[高度（Altitude）] ドロップダウン リスト	物理サーバーがインストールされている地点のおよその海抜（m 単位）。次のいずれかになります。 • [Auto]：物理的な高度をCPUによって判別します。 • [300 M][300_M]：サーバーは海抜約300 m の位置にあります。 • [900 M][900_M]：サーバーは海抜約900 m の位置にあります。 • [1500 M][1500_M]：サーバーは海抜約1500 m の位置にあります。 • **[3000 M]**：サーバーは、海抜約 3000 m です。

名前	説明
[パニックと高水準点（Panic and High Watermark）] ドロップダウンリスト	低に設定した場合、**[メモリ更新レート（Memory Refresh Rate）]** が **[1X リフレッシュ（1X Refresh）]** に設定されている間、メモリ コントローラは更新を延期しません。 次のいずれかになります。 • **[低（Low）]**：リフレッシュ レートは低に設定します。 • **[高（High）]**：リフレッシュ レートは高に設定します。

[QPI Configuration] のパラメータ

名前	説明
[QPI Link Frequency Select]	Intel QuickPath Interconnect（QPI）リンク周波数（ギガトランスファー/秒（GT/s）単位）。次のいずれかになります。 • [Auto]：QPI リンク周波数はCPUによって決定されます。 • **6.4 GT/s** • **7.2 GT/s**7.2_GT/s] • **8.0 GT/s**
[QPI Snoop Mode]	Intel QuickPath Interconnect（QPI）スヌープ モード。次のいずれかになります。 • [無効（Disabled）]：QPI スヌープ モードを無効にします。 • [クラスタ オン ダイ（Cluster on Die）]：クラスタ オン ダイが有効になります。有効化した LLC はそれぞれに独立したキャッシング エージェントで 2 つのパートに分割されます。これにより、一部のワークロードのパフォーマンスが向上します。このモードは、10 個以上のコアを搭載したプロセッサでのみ使用できます。高度にNUMA最適化されたワークロードに最適なモードです。 • [自動（Auto）]：CPU は自動的に早期スヌープ モードとして認識します。これはデフォルト値です。

サーバー モデル別 BIOS パラメータ

[USB Configuration] のパラメータ

名前	説明
[レガシーUSBサポート（Legacy USB Support）] ドロップダウン リスト	システムでレガシーUSBデバイスをサポートするかどうか。次のいずれかになります。 • [無効（Disabled）]：USBデバイスは、EFIアプリケーションでのみ使用できます。 • [有効（Enabled）]：レガシーUSBのサポートは常に使用できます。 • [Auto]：USBデバイスが接続されていない場合、レガシーUSBのサポートがディセーブルになります。
[Port 60/64 Emulation]	完全なUSBキーボードレガシーサポートのために60h/64hエミュレーションをシステムでサポートするかどうか。次のいずれかになります。 • [無効（Disabled）]：60h/64エミュレーションはサポートされません。 • [有効（Enabled）]：60h/64エミュレーションはサポートされます。 サーバーでUSB非対応オペレーティングシステムを使用する場合は、このオプションを選択する必要があります。
[すべてのUSBデバイス（All USB Devices）] ドロップダウン リスト	すべての物理および仮想USBデバイスを有効にするか無効にするか。次のいずれかになります。 • [Disabled]：すべてのUSBデバイスが無効です。 • [Enabled]：すべてのUSBデバイスが有効になります。
[USB Port: Rear]	背面パネルのUSBデバイスを有効にするか無効にするか。次のいずれかになります。 • [無効（Disabled）]：背面パネルのUSBポートをディセーブルにします。これらのポートに接続されるデバイスは、BIOSおよびオペレーティング システムによって検出されません。 • [有効（Enabled）]：背面パネルのUSBポートをイネーブルにします。これらのポートに接続されるデバイスは、BIOSおよびオペレーティング システムによって検出されます。

名前	説明
[USB Port: Internal]	内部USBデバイスを有効にするか無効にするか。次のいずれかになります。 • [無効（Disabled）]：内部USBポートをディセーブルにします。これらのポートに接続されるデバイスは、BIOSおよびオペレーティングシステムによって検出されません。 • [有効（Enabled）]：内部USBポートをイネーブルにします。これらのポートに接続されるデバイスは、BIOSおよびオペレーティング システムによって検出されます。
[USB Port: KVM]	vKVM ポートが有効か無効か。次のいずれかになります。 • **無効**：vKVM キーボードおよびマウス デバイスを無効にします。キーボードとマウスは vKVM ウィンドウで機能しなくなります。 • **有効**：vKVM キーボードとマウス デバイスを有効にします。
[USB Port: vMedia]	仮想メディア デバイスを有効にするか無効にするか。次のいずれかになります。 • [無効（Disabled）]：vMediaデバイスをディセーブルにします。 • [Enabled]：vMedia デバイスを有効にします。
[xHCI Mode]	xHCIコントローラのレガシーサポートを有効または無効にします。次のいずれかになります。 • [Disabled]：xHCI コントローラのレガシー サポートを無効にします。 • [Enabled]：xHCIコントローラのレガシーサポートを有効にします。

[PCI Configuration] のパラメータ

名前	説明
[Memory Mapped I/O Above 4GB]	4GB を超える MMIO をイネーブルまたはディセーブルにするかどうか。次のいずれかになります。 • [Disabled]：サーバーでは 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングしません。 • [有効（Enabled）]：サーバで 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングします。 （注） PCI デバイスが 64 ビット対応でも、レガシーなオプション ROM を使用する場合は、この設定をイネーブルにしても正しく機能しない場合があります。
[SR-IOV サポート（SR-IOV Support）] ドロップダウン リスト	サーバー上で SR-IOV（Single Root I/O Virtualization）を有効にするか無効にするか。次のいずれかになります。 • [Disabled]：SR-IOV は無効になります。 • [有効（Enabled）]：SR-IOV はイネーブルになります。

[Serial Configuration] のパラメータ

名前	説明
[Out-of-Band Mgmt Port]	Windows 緊急管理サービスで使用可能な COM ポート 0 を設定することができます。このセットアップ オプションに基づいて ACPI SPCR テーブルが報告されます。次のいずれかになります。 • [Disabled]：Windows オペレーティング システムで使われる汎用ポートとして COM ポート 0 を設定します。 • [有効（Enabled）]：Windows 緊急管理サービス用のリモート管理ポートとして COM ポート 0 を設定します。

名前	説明
[コンソールリダイレクション（Console redirection）] ドロップダウン リスト	POSTおよびBIOSのブート中に、シリアル ポートをコンソール リダイレクションで使用できるようにします。BIOSのブートが完了し、オペレーティング システムがサーバを担当すると、コンソール リダイレクションの関連性はなくなり、無効になります。次のいずれかになります。 • [Disabled]：POST 中にコンソール リダイレクションは発生しません。 • [COM 0]：POST 中にCOM ポート 0 でコンソール リダイレクションを有効にします。 • [COM 1]：POST 中にCOM ポート 1 でコンソール リダイレクションを有効にします。
[Terminal type]	コンソール リダイレクションに使用される文字フォーマットのタイプ。次のいずれかになります。 • [PC-ANSI]：PC-ANSI 端末フォントが使用されます。 • [VT100]：サポートされている vt100 ビデオ端末とその文字セットが使用されます。 • [VT100+]：サポートされている vt100-plus ビデオ端末とその文字セットが使用されます。 • [VT-UTF8]：UTF-8 文字セットのビデオ端末が使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。
[Bits per second]	シリアル ポートの伝送速度として使用されるボー レート。[Console Redirection] を無効にする場合は、このオプションを使用できません。次のいずれかになります。 • [9600]：9,600 ボー レートが使用されます。 • [19200]：19,200 ボー レートが使用されます。 • [38400]：38,400 ボー レートが使用されます。 • [57600]：57,600 ボー レートが使用されます。 • [115200]：115,200 ボー レートが使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。

名前	説明
[フロー制御（Flow Control）] ドロップダウン リスト	フロー制御にハンドシェイク プロトコルを使用するかどうかを設定します。送信要求/クリア ツーセンド（RTS/CTS）を使用すると、隠れた端末の問題が原因で発生する可能性がある、フレーム コリジョンを減らすことができます。次のいずれかになります。 • [None]：フロー制御は使用されません。 • **[Hardware RTS/CTS]**：フロー制御に RTS/CTS が使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。
[Putty KeyPad]	PuTTY ファンクション キーおよびテンキーの最上段のキーのアクションを変更できます。次のいずれかになります。 • [VT100]：ファンクション キーによって **ESC OP** ～ **ESC O[** を生成します。 • [LINUX]：Linux 仮想コンソールを模倣します。ファンクション キー F6 ～ F12 はデフォルト モードと同様に動作しますが、F1 ～ F5 は **ESC [[A** ～ **ESC [[E** を生成します。 • [XTERMR6]：ファンクション キー F5 ～ F12 がデフォルト モードと同様に動作します。ファンクション キー F1 ～ F4 によって ESC OP ～ ESC OS を生成します。これはデジタル端末のキーパッドの上段によって生成されるシーケンスです。 • [SCO]：ファンクション キー F1 ～ F12 によって **ESC [M** ～ **ESC [X** を生成します。ファンクション キーと Shift キーによって **ESC [Y** ～ **ESC [j** を生成します。Ctrl キーとファンクション キーによって **ESC [k** ～ **ESC [v** を生成します。Shift、Ctrl およびファンクション キーによって **ESC [w** ～ **ESC [{** を生成します。 • [ESCN]：デフォルト モードです。ファンクション キーはデジタル端末の一般的な動作と一致します。ファンクション キーによって **ESC [11~** や **ESC [12~** などのシーケンスを生成します。 • [VT400]：ファンクション キーはデフォルト モードと同様に動作します。テンキーの最上段のキーによって **ESC OP** ～ **ESC OS** を生成します。

名前	説明
[Redirection After BIOS POST]	BIOS POST が完了し、OS ブートローダに制御が渡された後に、BIOS コンソール リダイレクションがアクティブであるかどうか。次のいずれかになります。 • **[Always Enable]**：OS のブートおよび実行時に BIOS レガシー コンソール リダイレクションがアクティブになります。 • [Bootloader]：OS ブートローダに制御が渡される前に BIOS レガシー コンソール リダイレクションがディセーブルになります。

[LOM and PCIe Slots Configuration] のパラメータ

名前	説明
[VICに対するCDNサポート（CDN Support for VIC）] ドロップダウン リスト	イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [無効（Disabled）]：VICカードに対するCDNサポートは無効です。 • [有効（Enabled）]：CDNサポートはVICカードに対して有効です。 （注） VIC カードの CDN サポートは、Windows 2012 または最新の OS でのみ機能します。
[PCI ROM CLP]	PCI ROM Command Line Protocol（CLP）は、カード上の iSCSI や PxE などのさまざまなオプション ROM の実行を制御します。デフォルト設定は、ディセーブルです。 • [Enabled]：ポートごとに個別に、iSCSI や PxE などのさまざまなオプション ROM の実行を設定できるようにします。 • [Disabled]：デフォルト オプションです。異なるオプション ROM は選択できません。デフォルト オプション ROM は PCI 列挙中に実行されます。

サーバー モデル別 BIOS パラメータ

名前	説明
[PCH SATA Mode]	このオプションでは、PCH SATA モードを選択できます。次のいずれかになります。 • [AHCI]：SATA コントローラと sSATA コントローラの両方を AHCI モードに設定します。 • [Disabled]：SATA コントローラと sSATA コントローラを無効にします。 • [LSI SW Raid]：SATA コントローラと sSATA コントローラを LSI SW Raid の raid モードに設定します。
[All Onboard LOM Ports]	すべての LOM ポートを有効にするか無効にするか。次のいずれかになります。 • [Disabled]：すべての LOM ポートが無効です。 • [Enabled]：すべての LOM ポートが有効になります。
[LOM Port *n* OptionROM]	***n*** で指定された LOM ポートでオプション ROM を使用できるかどうか。次のいずれかになります。 • [Disabled]：スロット ***n*** のオプション ROM は使用できません。 • [Enabled]：スロット ***n*** のオプション ROM は使用可能です。 • **[UEFI Only]**：スロット ***n*** のオプション ROM は UEFI にのみ使用できます。 • **[Legacy Only]**：スロット ***n*** のオプション ROM はレガシーにのみ使用できます。
[All PCIe Slots OptionROM]	PCIe カードのオプション ROM をサーバーが使用できるかどうか。次のいずれかになります。 • [Disabled]：スロット ***n*** のオプション ROM は使用できません。 • [Enabled]：スロット ***n*** のオプション ROM は使用可能です。 • **[UEFI Only]**：スロット ***n*** のオプション ROM は UEFI にのみ使用できます。 • **[Legacy Only]**：スロット ***n*** のオプション ROM はレガシーにのみ使用できます。

名前	説明
[PCIe Slot:*n* OptionROM	PCIe カードのオプション ROM をサーバーが使用できるかどうか。次のいずれかになります。 • [Disabled]：スロット ***n*** のオプション ROM は使用できません。 • [Enabled]：スロット ***n*** のオプション ROM は使用可能です。 • **[UEFI Only]**：スロット ***n*** のオプション ROM は UEFI にのみ使用できます。 • **[Legacy Only]**：スロット ***n*** のオプション ROM はレガシーにのみ使用できます。
[PCIe Slot:MLOM OptionROM]	このオプションでは、MLOM スロットに接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • [Enabled]：レガシーおよび UEFI オプション ROM の両方を実行します。 • **[無効（Disabled）]**：レガシーおよび UEFI の両方のオプション ROM は実行されません。 • **[UEFI のみ（UEFI Only）]**：UEFI オプション ROM のみを実行します。 • [Legacy Only]：レガシー オプション ROM のみを実行します。
[PCIe Slot:HBA OptionROM]	このオプションでは、HBA スロットに接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • [Enabled]：レガシーおよび UEFI オプション ROM の両方を実行します。 • **[無効（Disabled）]**：レガシーおよび UEFI の両方のオプション ROM は実行されません。 • **[UEFI のみ（UEFI Only）]**：UEFI オプション ROM のみを実行します。 • [Legacy Only]：レガシー オプション ROM のみを実行します。

名前	説明
[PCIe Slot:N1 OptionROM]	このオプションでは、SSD:NVMe1 スロットに接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • [Enabled]：レガシーおよび UEFI オプション ROM の両方を実行します。 • **[無効（Disabled）]**：レガシーおよび UEFI の両方のオプション ROM は実行されません。 • **[UEFI のみ（UEFI Only）]**：UEFI オプション ROM のみを実行します。 • [Legacy Only]：レガシー オプション ROM のみを実行します。
[PCIe Slot:N2 OptionROM]	このオプションでは、SSD:NVMe2 スロットに接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • [Enabled]：レガシーおよび UEFI オプション ROM の両方を実行します。 • **[無効（Disabled）]**：レガシーおよび UEFI の両方のオプション ROM は実行されません。 • **[UEFI のみ（UEFI Only）]**：UEFI オプション ROM のみを実行します。 • [Legacy Only]：レガシー オプション ROM のみを実行します。
[PCIe Slot:N2 OptionROM]	このオプションでは、SSD:NVMe2 スロットに接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • [Enabled]：レガシーおよび UEFI オプション ROM の両方を実行します。 • **[無効（Disabled）]**：レガシーおよび UEFI の両方のオプション ROM は実行されません。 • **[UEFI のみ（UEFI Only）]**：UEFI オプション ROM のみを実行します。 • [Legacy Only]：レガシー オプション ROM のみを実行します。

名前	説明
[PCIe Slot:HBA Link Speed] **PCIe SlotHBALinkSpeed**	このオプションを使用すると、PCIe HBA スロットに装着されているアダプタ カードの最大速度を制限できます。次のいずれかになります。 • [自動（Auto）]：システムは許可される最大速度を選択します。 • [GEN1]：最大 2.5 GT/s（ギガトランスファー/秒）までの速度が許可されます。 • [GEN2]：最大 5 GT/s までの速度が許可されます。 • [GEN3]：最大 8 GT/s までの速度が許可されます。 • [Disabled]：最大速度は制限されません。

[BIOS Configuration] ダイアログボックスのボタン バー

重要 このダイアログボックスのボタンは、表示しているタブのパラメータのみでなく、使用可能なすべてのタブのすべての BIOS パラメータに影響します。

名前	説明
[Save Changes] ボタン	3 つのタブすべての BIOS パラメータの設定を保存し、ダイアログボックスを閉じます。 [Reboot Host Immediately] チェックボックスがオフの場合、サーバはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバが手動でリブートされるまで保存されます。
[Reset Values] ボタン	3 つのタブすべての BIOS パラメータの値を、このダイアログボックスを最初に開いたときに有効だった設定に復元します。
[Restore Defaults] ボタン	3 つのタブすべての BIOS パラメータをそのデフォルト値に設定します。
[Cancel] ボタン	変更を行わずにダイアログボックスを閉じます。

C460 M4 サーバの [サーバ管理（Server Management）] タブ

サーバ リブート オプション

[Save Changes] をクリックした後で変更内容を自動的に適用するには、[Reboot Host Immediately] チェックボックスをオンにします。Cisco IMC によってサーバがただちにリブートされて、変更が適用されます。

変更内容を後で適用するには、[Reboot Host Immediately] チェックボックスをオフにします。Cisco IMC によって変更が保存され、次回サーバがリブートするときに適用されます。

（注） 保留中の BIOS パラメータの変更がすでにある場合、Cisco IMC は、[Save Changes] をクリックしたときに、保存されている値を現在の設定で自動的に上書きします。

サーバ管理 BIOS パラメータ

名前	説明
[FRB-2 Timer]	POST 中にシステムがハングアップした場合に、システムを回復するために Cisco IMC で FRB2 タイマーを使用するかどうか。次のいずれかになります。 • [無効（Disabled）]：FRB2 タイマーは使用されません。 • [Enabled]：POST 中に FRB2 タイマーが開始され、必要に応じてシステムの回復に使用されます。
[OS ウォッチドッグ タイマー（OS Watchdog Timer）] ドロップダウン リスト	BIOS が指定されたタイムアウト値でウォッチドッグ タイマーをプログラムするかどうか。次のいずれかになります。 • [Disabled]：サーバーのブートにかかる時間をトラッキングするためにウォッチドッグ タイマーは使用されません。 • [Enabled]：サーバーのブートにかかる時間をウォッチドッグ タイマーでトラッキングします。サーバーが [OSブートウォッチドッグタイマータイムアウト（OS Boot Watchdog Timer Timeout）] フィールドに指定された時間内にブートしない場合、Cisco IMC はエラーをログに記録し、[OSブートウォッチドッグポリシー（OS Boot Watchdog Policy）] フィールドに指定されたアクションを実行します。

名前	説明
[OSウォッチドッグタイマータイムアウト（OS Watchdog Timer Timeout）] ドロップダウン リスト	OSが指定された時間内にブートしない場合、OS ウォッチドッグ タイマーの期限が切れ、システムはタイマー ポリシーに基づいてアクションを実行します。次のいずれかになります。 • **[5 Minutes]**：OS ウォッチドッグ タイマーは、ブートが開始されてから 5 分後に期限が切れます。 • **[10 Minutes]**：OS ウォッチドッグ タイマーは、ブートが開始されてから 10 分後に期限が切れます。 • **[15 Minutes]**：OS ウォッチドッグ タイマーは、ブートが開始されてから 15 分後に期限が切れます。 • **[20 Minutes]**：OS ウォッチドッグ タイマーは、ブートが開始されてから 20 分後に期限が切れます。 （注） このオプションは [OS Boot Watchdog Timer] をイネーブルにした場合にのみ適用されます。
[OSウォッチドッグタイマーポリシー（OS Watchdog Timer Policy）] ドロップダウン リスト	ウォッチドッグ タイマーが切れた場合にシステムで実行されるアクション。次のいずれかになります。 • **[Do Nothing]**：OS のブート中にウォッチドッグ タイマーの期限が切れた場合、アクションは実行されません。 • **[電源オフ（Power Down）]**：OS のブート中にウォッチドッグタイマーの期限が切れた場合、サーバーの電源がオフになります。 • [Reset]：OS のブート中にウォッチドッグ タイマーが切れた場合、サーバーはリセットされます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にする場合にのみ適用されます。

[BIOS Configuration] ダイアログボックスのボタン バー

重要 このダイアログボックスのボタンは、表示しているタブのパラメータのみでなく、使用可能なすべてのタブのすべての BIOS パラメータに影響します。

名前	説明
[Save Changes] ボタン	3 つのタブすべての BIOS パラメータの設定を保存し、ダイアログボックスを閉じます。 [Reboot Host Immediately] チェックボックスがオフの場合、サーバはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバが手動でリブートされるまで保存されます。
[Reset Values] ボタン	3 つのタブすべての BIOS パラメータの値を、このダイアログボックスを最初に開いたときに有効だった設定に復元します。
[Restore Defaults] ボタン	3 つのタブすべての BIOS パラメータをそのデフォルト値に設定します。
[Cancel] ボタン	変更を行わずにダイアログボックスを閉じます。

C220 M4 および C240 M4 サーバ

C220M4 および C240M4 サーバのメイン タブ

主要な BIOS パラメータ

名前	説明
[今すぐホストを再起動（Reboot Host Immediately）] チェックボックス	このチェックボックスをオンにすると、直ちにホスト サーバが再起動します。このチェックボックスは、変更を保存してからオンにする必要があります。
[TPM Support]	TPM（トラステッドプラットフォーム モジュール）は、主に暗号キーを使用する基本的なセキュリティ関連機能を提供するように設計されたマイクロチップです。このオプションを使用すると、システムの TPM セキュリティ デバイス サポートを制御できます。次のいずれかを指定できます。 • [Disabled]：サーバーは TPM を使用しません。 • [有効（Enabled）]：サーバは TPM を使用します。 （注） オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。

名前	説明
[Power ON Password Support] ドロップダウン	このトークンでは、F2 BIOS 設定を使用する前に BIOS パスワードを設定する必要があります。有効にすると、BIOS 関数（IO 設定、BIOS セットアップ、BIOS を使用したオペレーティング システムへのブート）にアクセスする前にパスワードの検証が必要になります。次のいずれかを指定できます。 • **[無効（Disabled）]**：サポートは無効になります。 • **[有効（Enabled）]**：サポートは有効になります。

[Actions] 領域

名前	説明
[**Save**] ボタン	BIOS パラメータの設定を保存して、ダイアログボックスを閉じます。 **[Reboot Host Immediately]** チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[Reset] ボタン	3 つすべてのタブ上の BIOS パラメータの値が、このダイアログボックスを最初に開いた際に有効だった設定にリセットされます。
[Restore Defaults] ボタン	3 つのタブすべての BIOS パラメータをそのデフォルト値に設定します。

C220M4 および C240M4 サーバの [詳細（Advanced）] タブ

サーバ リブート オプション

[Save Changes] をクリックした後で変更内容を自動的に適用するには、[Reboot Host Immediately] チェックボックスをオンにします。Cisco IMC によってサーバがただちにリブートされて、変更が適用されます。

変更内容を後で適用するには、[Reboot Host Immediately] チェックボックスをオフにします。Cisco IMC によって変更が保存され、次回サーバがリブートするときに適用されます。

（注） 保留中の BIOS パラメータの変更がすでにある場合、Cisco IMC は、[Save Changes] をクリックしたときに、保存されている値を現在の設定で自動的に上書きします。

サーバー モデル別 BIOS パラメータ

[Processor Configuration] のパラメータ

名前	説明
[Intel Hyper-Threading Technology] ドロップダウン リスト	プロセッサでインテル ハイパースレッディング テクノロジーを使用するかどうか。このテクノロジーでは、マルチスレッド ソフトウェア アプリケーションのスレッドを各プロセッサ内で並列に実行できます。次のいずれかになります。 • [Disabled]：プロセッサでのハイパースレッディングを禁止します。 • [有効（Enabled）]：プロセッサでの複数スレッドの並列実行を許可します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。
[有効化されたコア数（Number of Enabled Cores）] ドロップダウン リスト	サーバー上の 1 つ以上の物理コアを無効にできます。次のいずれかになります。 • [All]：すべての物理コアをイネーブルにします。これにより、関連付けられている論理プロセッサ コアで Hyper Threading もイネーブルになります。 • [1] ～ [***n***]：サーバで実行できる物理プロセッサ コアの数を指定します。各物理コアには、論理コアが関連付けられています。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせてください。

名前	説明
[Execute Disable] ドロップダウン リスト	アプリケーション コードを実行できる場所を指定するために、サーバーのメモリ領域を分類します。この分類の結果、悪意のあるワームがバッファにコードを挿入しようとした場合、プロセッサでコードの実行を無効化します。この設定は、損害、ワームの増殖、および特定クラスの悪意のあるバッファ オーバーフロー攻撃を防止するのに役立ちます。次のいずれかになります。 • [Disabled]：プロセッサでメモリ領域を分類しません。 • [有効（Enabled）]：プロセッサでメモリ領域を分類します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。
[Intel VT]	プロセッサで Intel Virtualization Technology（VT）を使用するかどうか。このテクノロジーでは、1つのプラットフォームで、複数のオペレーティング システムとアプリケーションをそれぞれ独立したパーティション内で実行できます。次のいずれかになります。 • [Disabled]：プロセッサでの仮想化を禁止します。 • [有効（Enabled）]：プロセッサで、複数のオペレーティングシステムをそれぞれ独立したパーティション内で実行できます。 （注） このオプションを変更した場合は、設定を有効にするためにサーバーの電源を再投入する必要があります。
[Intel VT-d]	Intel Virtualization Technology for Directed I/O（VT-d）をプロセッサで使用するかどうか。次のいずれかになります。 • [Disabled]：プロセッサで仮想化テクノロジーを使用しません。 • [Enabled]：プロセッサで仮想化テクノロジーを使用します。

名前	説明
[Intel VTD割り込み再マッピング（Intel VTD interrupt Remapping）] ドロップダウンリスト	プロセッサで Intel VT-d Interrupt Remapping をサポートするかどうか。次のいずれかになります。 • [Disabled]：プロセッサでリマッピングをサポートしません。 • [Enabled]：プロセッサで VT-d Interrupt Remapping を必要に応じて使用します。
[Intel VT-d PassThrough DMA] ドロップダウン リスト	プロセッサで Intel VT-d Pass-through DMA をサポートするかどうか。次のいずれかになります。 • [Disabled]：プロセッサでパススルー DMA をサポートしません。 • [Enabled]：プロセッサで VT-d Pass-through DMA を必要に応じて使用します。
[Intel VT-d Coherency Support]	プロセッサで Intel VT-d Coherency をサポートするかどうか。次のいずれかになります。 • [Disabled]：プロセッサでコヒーレンシをサポートしません。 • [Enabled]：プロセッサで VT-d Coherency を必要に応じて使用します。
[Intel VT-d ATS Support]	プロセッサで Intel VT-d Address Translation Services（ATS）をサポートするかどうか。次のいずれかになります。 • [Disabled]：プロセッサで ATS をサポートしません。 • [Enabled]：プロセッサで VT-d ATS を必要に応じて使用します。

名前	説明
[CPU Performance]	サーバーの CPU パフォーマンス プロファイルを設定します。パフォーマンス プロファイルは次のオプションで構成されます。 • DCU Streamer Prefetcher • DCU IP Prefetcher • ハードウェア プリフェッチャ • Adjacent Cache-Line Prefetch 次のいずれかになります。 • [Enterprise]：すべてのオプションがイネーブルです。 • [High Throughput]：DCU IP Prefetcher のみがイネーブルです。残りのオプションはディセーブルになります。 • [HPC]：すべてのオプションがイネーブルです。この設定はハイ パフォーマンス コンピューティングとも呼ばれます。 • [Custom]：パフォーマンス プロファイルのすべてのオプションをサーバの BIOS セットアップから設定できます。また、Hardware Prefetcher オプションと Adjacent Cache-Line Prefetch オプションは、下記のフィールドで設定できます。
[ハードウェア プリフェッチャ（Hardware Prefetcher）] ドロップダウン リスト	プロセッサで、インテル ハードウェア プリフェッチャが必要に応じてデータおよび命令ストリームをメモリから取得し、統合 2 次キャッシュに入れることを許可するかどうか。次のいずれかになります。 • [Disabled]：ハードウェア プリフェッチャは使用しません。 • [Enabled]：プロセッサで、キャッシュの問題が検出されたときにプリフェッチャを使用します。

名前	説明
[隣接キャッシュラインプリフェッチャ（Adjacent Cache Line Prefetcher）] ドロップダウン リスト	プロセッサで必要な行のみを取得するのではなく、偶数または奇数のペアのキャッシュ行を取得するかどうか。次のいずれかになります。 • [Disabled]：プロセッサで必要な行のみを取得します。 • [有効（Enabled）]：プロセッサで必要な行およびペアの行の両方を取得します。
[DCUストリーマープリフェッチ（DCU Streamer Prefetch）] ロップダウン リスト	プロセッサで DCU IP プリフェッチ メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。次のいずれかになります。 • [Disabled]：プロセッサはキャッシュ読み取り要求を予測しようとせず、明示的に要求された行のみを取得します。 • [Enabled]：DCU Prefetcher でキャッシュ読み取りパターンを分析し、必要と判断した場合にキャッシュ内の次の行を事前に取得します。
[DCU IPプリフェッチャ（DCU IP Prefetcher）] ドロップダウン リスト	プロセッサで DCU IP プリフェッチ メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。次のいずれかになります。 • [Disabled]：プロセッサでキャッシュ データをプリロードしません。 • [Enabled]：DCU IP プリフェッチャで最も関連性が高いと判断されたデータを含むL1 キャッシュをプリロードします。
[ダイレクトキャッシュアクセスサポート（Direct Cache Access Support）] ドロップダウン リスト	プロセッサで、データをI/Oデバイスから直接プロセッサ キャッシュに入れることにより、I/O パフォーマンスを向上させることができます。この設定はキャッシュ ミスを減らすのに役立ちます。次のいずれかになります。 • [Disabled]：データはI/Oデバイスから直接プロセッサ キャッシュには入れられません。 • [Enabled]：データはI/Oデバイスから直接プロセッサ キャッシュに入れられます。

名前	説明
[Power Technology]	次のオプションの CPU 電源管理設定を指定できます。 • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 [Power Technology] は次のいずれかになります。 • [Custom]：前述の BIOS パラメータの個々の設定が使用されます。これらの BIOS パラメータのいずれかを変更する場合は、このオプションを選択する必要があります。 • [Disabled]：サーバーで CPU 電源管理は実行されず、前述の BIOS パラメータの設定が無視されます。 • [Energy Efficient][Energy_Efficient]：前述の BIOS パラメータに最適な設定が決定され、これらのパラメータの個々の設定は無視されます。
[Enhanced Intel Speedstep Technology] ドロップダウン リスト	プロセッサで拡張版 Intel SpeedStep テクノロジーを使用するかどうか設定します。このテクノロジーでは、プロセッサの電圧やコア周波数をシステムが動的に調整できます。このテクノロジーにより、平均電力消費量と平均熱発生量が減少する可能性があります。次のいずれかになります。 • [Disabled]：プロセッサの電圧または周波数を動的に調整しません。 • [有効（Enabled）]：プロセッサで Enhanced Intel SpeedStep Technology が使用され、サポートされているすべてのスリープ状態でさらに電力を節約することが可能になります。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。 （注） [Power Technology][CPUPowerManagement] を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。

名前	説明
[Intel Turbo Boost Technology]	プロセッサでインテル ターボ ブースト テクノロジーを使用するかどうか。このテクノロジーでは、仕様よりも低い電力、温度、または電圧でプロセッサが動作していると、自動的にそのプロセッサの周波数が上がります。次のいずれかになります。 • [Disabled]：プロセッサの周波数は自動的には上がりません。 • [Enabled]：必要に応じてプロセッサで Turbo Boost Technology が利用されます。 （注） [Power Technology][CPUPowerManagement] を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[Processor C3 Report]	BIOS からオペレーティング システムに C3 レポートを送信するかどうか。OS はレポートを受信すると、プロセッサを電力量の少ない C3 状態に移行してエネルギー使用量を減らし、最適なプロセッサ パフォーマンスを維持できます。次のいずれかになります。 • [Disabled]：BIOS は C3 レポートの送信を行いません。 • [Enabled]：BIOS から C3 レポートを送信し、OS がプロセッサを電力量の少ない C3 状態に移行できるようにします。 （注） [Power Technology][CPUPowerManagement] を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。

名前	説明
[Processor C6 Report]	BIOS からオペレーティング システムに C6 レポートを送信するかどうか。OS はレポートを受信すると、プロセッサを電力量の少ない C6 状態に移行してエネルギー使用量を減らし、最適なプロセッサ パフォーマンスを維持できます。次のいずれかになります。 • [Disabled]：BIOS から C6 レポートを送信しません。 • [Enabled]：BIOS から C6 レポートを送信し、OS がプロセッサを電力量の少ない C6 状態に移行できるようにします。 （注） [Power Technology][CPUPowerManagement] を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[プロセッサの電源状態C1拡張（Processor Power State C1 Enhanced）] ドロップダウン リスト	C1 ステートに入ったときに、CPU が最小周波数に移行するかどうか。次のいずれかになります。 • [無効（Disabled）]：CPU は C1 ステートでも引き続き最大周波数で動作します。 • [有効（Enabled）]：CPU は最小周波数に移行します。このオプションでは C1 ステートで節約される電力量が最大になります。

名前	説明
[P-STATE調整（P-STATE Coordination）] ドロップダウン リスト	BIOS がオペレーティング システムに P-state サポート モデルを伝達する方法を定義できます。Advanced Configuration and Power Interface（ACPI）仕様では、次の 3 つのモデルが定義されています。 • [HW_ALL]：プロセッサ ハードウェアによって、依存関係にある論理プロセッサ（パッケージ内のすべての論理プロセッサ）間の P-state を調整します。 • [SW_ALL]：OS Power Manager（OSPM）によって、依存関係にある論理プロセッサ（物理パッケージ内のすべての論理プロセッサ）間の P-state を調整します。すべての論理プロセッサで遷移を開始する必要があります。 • [SW_ANY]：OS Power Manager（OSPM）によって、依存関係にある論理プロセッサ（パッケージ内のすべての論理プロセッサ）間の P-state を調整します。ドメイン内の任意の論理プロセッサで遷移を開始できます。 （注） [Power Technology][CPUPowerManagement] を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[Boot Performance Mode] ドロップダウン リスト	オペレーティング システムのハンドオフ前に設定される BIOS パフォーマンス状態を選択できます。次のいずれかになります。 • [最大パフォーマンス（Max Performance）]：プロセッサの P-state の比率が最大です。 • [Max Efficient]：プロセッサの P-state 率は最小です
[エネルギーパフォーマンスの調整（Energy Performance Tuning）] ドロップダウン リスト	エネルギー効率のバイアス調整のために BIOS またはオペレーティング システムを選択できます。次のいずれかになります。 • [OS]：エネルギーパフォーマンスの調整にOSを選択します。 • [BIOS]：エネルギー効率の調整のために BIOS を選択します。

名前	説明
[エネルギーパフォーマンス（Energy Performance）] ドロップダウン リスト	システム パフォーマンスまたはエネルギー効率がこのサーバーで重要かどうかを判断できます。次のいずれかになります。 • **Balanced Energy** • **Balanced Performance** • **Energy Efficient** • **Performance**
[パッケージのCステートの制限（Package C State Limit）] ドロップダウン リスト	アイドル時にサーバー コンポーネントが使用できる電力量。次のいずれかになります。 • [C0 state][C0_state]：サーバーはすべてのサーバー コンポーネントに常にフルパワーを提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • **[C1 state]**：CPU のアイドル時に、システムは電力消費を少し減らします。このオプションでは、必要な電力が C0 よりも少なく、サーバーはすばやくハイ パフォーマンス モードに戻ることができます。 • **[C3 state]**：CPU のアイドル時に、システムは C1 オプションの場合よりもさらに電力消費を減らします。この場合、必要な電力は C1 または C0 よりも少なくなりますが、サーバーがハイ パフォーマンス モードに戻るのに要する時間が少し長くなります。 • **[C6 state]**：CPU のアイドル時に、システムは C3 オプションの場合よりもさらに電力消費を減らします。このオプションを使用すると、C0、C1、または C3 よりも電力量が節約されますが、サーバーがフルパワーに戻るまでにパフォーマンス上の問題が発生する可能性があります。 • **[C7 state]**：CPU のアイドル時に、サーバはコンポーネントが使用できる電力量を最小にします。このオプションでは、節約される電力量が最大になりますが、サーバーがハイ パフォーマンス モードに戻るのに要する時間も最も長くなります。 • **[No Limit]**：サーバは、使用可能な任意の C ステートに入ることがあります。

サーバー モデル別 BIOS パラメータ

名前	説明
[Extended APIC]	拡張 APIC サポートをイネーブルまたはディセーブルにできます。次のいずれかになります。 • [XAPIC]：APIC サポートを有効にします。 • [X2APIC]：APIC を有効にして、Intel VT-d と Interrupt Remapping も有効にします。
[Workload Configuration]	ワークロードの特性を最適化するようにパラメータを設定できます。次のいずれかになります。 • [Balanced]：最適化のためにバランスのとれたオプションを選択します。 • [I/O Sensitive]：最適化のために I/O を考慮したオプションを選択します。 （注） ワークロード構成は [Balanced] に設定することをお勧めします。
[CPU HWPM] ドロップダウンリスト	CPU のパフォーマンスやエネルギー効率を引き上げるためのハードウェア電源管理（HWPM）インターフェイスを有効にします。次のいずれかになります。 • [無効（Disabled）]：P-state は前世代のプロセッサと同じ方法で制御されます。 • [ネイティブモード（Native Mode）]：HWPM はソフトウェアインターフェイスを介してオペレーティング システムと連動します。 • [OOBモード（OOB Mode）]：CPU は、オペレーティング システムのエネルギー効率に基づいて周波数を自律的に制御します。
[CPU自律C-state] ドロップダウン リスト	HALT 命令を MWAIT 命令に変換する CPU 自律 C-state を有効にします。次のいずれかになります。 • [無効（Disabled）]：CPU 自律 C-state が無効になります。これはデフォルト値です。 • [有効（Enabled）]：CPU 自律 C-state が有効になります。

名前	説明
[プロセッサCMCI（Processor CMCI）] ドロップダウン リスト	CPU が corrected machine check events で割り込みをトリガーできるようにします。corrected machine check interrupt（CMCI）により、従来のポーリング タイマーよりも反応速度を向上できます。次のいずれかになります。 • [無効（Disabled）]：CMCI が無効になります。 • [有効（有効）]：CMCI が有効になります。これはデフォルト値です。

[Memory Configuration] のパラメータ

名前	説明
[Select Memory RAS]	サーバーに対するメモリの信頼性、可用性および機密性（RAS）の設定方法。次のいずれかになります。 • **[Maximum Performance]**：システムのパフォーマンスが最適化されます。 • [Mirroring]：システムのメモリの半分をバックアップとして使用することにより、システムの信頼性が最適化されます。 • [Lockstep]：サーバ内の DIMM ペアが、同一のタイプ、サイズ、および構成を持ち、SMI チャネルにまたがって装着されている場合、ロックステップ モードをイネーブルにすることで、メモリ アクセス遅延の最小化およびパフォーマンスの向上を図ることができます。このオプションを使用した場合、[Mirroring] よりもシステム パフォーマンスが向上し、[Maximum Performance] よりも信頼性が向上しますが、[Mirroring] よりも信頼性が低く、[Maximum Performance] よりもシステム パフォーマンスは低下します。

名前	説明
[NUMA] ドロップダウン リスト	BIOS で Non-Uniform Memory Access（NUMA）がサポートされているかどうか。次のいずれかになります。 • [Disabled]：BIOS で NUMA をサポートしません。 • [有効（Enabled）]：NUMA に対応したオペレーティング システムに必要な ACPI テーブルを BIOS に含めます。このオプションを有効にする場合は、一部のプラットフォームでシステムのソケット間メモリ インターリーブを無効にする必要があります。
[チャネルインターリーブ（Channel Interleaving）] ドロップダウン リスト	CPU がメモリ ブロックを分割して、インターリーブされたチャネル間にデータの連続部分を分散し、同時読み取り動作を有効にするかどうか。次のいずれかになります。 • [Auto]：実行するインターリーブを、CPU が決定します。 • [1 Way][1_Way]：一部のチャネルインターリーブが使用されます。 • [2 Way][2_Way] • [3 Way][3_Way] • [4 Way][4_Way]：最大のチャネルインターリーブが使用されます。
[Rank Interleaving]	1 つのランクを更新中に別のランクにアクセスできるよう、CPU がメモリの物理ランクをインターリーブするかどうか。次のいずれかになります。 • [Auto]：実行するインターリーブを、CPU が決定します。 • [1 Way][1_Way]：一部のランクインターリーブが使用されます。 • [2 Way][2_Way] • [4 Way][4_Way] • [8 Way][8_Way]：最大量のランクインターリーブが使用されます。

名前	説明
[Patrol Scrub]	システムがサーバー上のメモリの未使用部分でも単一ビット メモリ エラーをアクティブに探して訂正するかどうか。次のいずれかになります。 • [Disabled]：CPU がメモリ アドレスの読み取りまたは書き込みを行うときのみ、システムはメモリの ECC エラーをチェックします。 • [有効（Enabled）]：システムは定期的にメモリを読み書きして ECC エラーを探します。エラーが見つかると、システムは修復を試みます。このオプションにより、単一ビット エラーは複数ビット エラーになる前に修正される場合がありますが、パトロール スクラブの実行時にパフォーマンスが低下する場合もあります。
[デマンドスクラブ（Demand Scrub）] ドロップダウン リスト	CPU または I/O から読み取り要求があった時に発生したシングル ビット メモリ エラーを、システムで修正するかどうか。次のいずれかになります。 • [無効（Disabled）]：シングル ビット メモリ エラーは修正されません。 • [Enabled]：シングル ビット メモリ エラーがメモリ内部で修正され、修正されたデータが読み取り要求に応じて設定されます。
[高度（Altitude）] ドロップダウン リスト	物理サーバーがインストールされている地点のおよその海抜（m 単位）。次のいずれかになります。 • [Auto]：物理的な高度を CPU によって判別します。 • [300 M][300_M]：サーバーは海抜約300 m の位置にあります。 • [900 M][900_M]：サーバーは海抜約900 m の位置にあります。 • [1500 M][1500_M]：サーバーは海抜約1500 m の位置にあります。 • **[3000 M]**：サーバーは、海抜約 3000 m です。

名前	説明
[パニックと高水準点（Panic and High Watermark）] ドロップダウンリスト	低に設定した場合、**[メモリ更新レート（Memory Refresh Rate）]** が **[1X リフレッシュ（1X Refresh）]** に設定されている間、メモリ コントローラは更新を延期しません。 次のいずれかになります。 • **[低（Low）]**：リフレッシュ レートは低に設定します。 • **[高（High）]**：リフレッシュ レートは高に設定します。

[QPI Configuration] のパラメータ

名前	説明
[QPI Link Frequency Select]	Intel QuickPath Interconnect（QPI）リンク周波数（ギガトランスファー/秒（GT/s）単位）。次のいずれかになります。 • [Auto]：QPI リンク周波数はCPUによって決定されます。 • **6.4 GT/s** • **7.2 GT/s**7.2_GT/s] • **8.0 GT/s**

名前	説明
[QPI Snoop Mode]	Intel QuickPath Interconnect（QPI）スヌープ モード。次のいずれかになります。 • [Auto]：CPU は自動的に早期スヌープ モードとして認識します。 • [早期スヌープ（Early Snoop）]：分散キャッシュ リング停止で、別のキャッシング エージェントにスヌープ プローブまたは要求を直接送信できます。このモードは、遅延が少なく、スレッド全体でデータ セットを共有しているためにキャッシュ間転送からメリットが得られるワークロードやNUMA最適化されていないワークロードに最適です。 • [ホーム スヌープ（Home Snoop）]：スヌープは、常に、メモリ コントローラのホーム エージェント（集中型リング停止）によって起動されます。このモードは早期スヌープよりもローカル遅延が高くなりますが、多数の未処理トランザクションに追加のリソースを提供します。 • [Home Directory Snoop]：ホーム ディレクトリはオプションで使用できる機能で、プロセッサ内の HA ロジックと iMC ロジックの両方に実装されています。ディレクトリの目的は、スケーラブルなプラットフォーム、および 2S と 4S の設定内のリモートソケット、およびノード コントローラへスヌープをフィルタリングすることです。 • [Home Directory Snoop with OSB]：Opportunistic Snoop Broadcast（OSB）ディレクトリ モードでは、HA は、ディレクトリ情報が収集されてチェックされる前であっても、非常に負荷の軽い状況下で推測的ホーム スヌープ ブロードキャストを選択できます。 • [クラスタ オン ダイ（Cluster on Die）]：クラスタ オン ダイが有効になります。有効化した LLC はそれぞれに独立したキャッシング エージェントで 2 つのパートに分割されます。これにより、一部のワークロードのパフォーマンスが向上します。このモードは、10 個以上のコアを搭載したプロセッサでのみ使用できます。高度にNUMA最適化されたワークロードに最適なモードです。

[USB Configuration] のパラメータ

名前	説明
[レガシーUSBサポート（Legacy USB Support）] ドロップダウン リスト	システムでレガシーUSBデバイスをサポートするかどうか。次のいずれかになります。 • [無効（Disabled）]：USBデバイスは、EFIアプリケーションでのみ使用できます。 • [有効（Enabled）]：レガシーUSBのサポートは常に使用できます。 • [Auto]：USBデバイスが接続されていない場合、レガシーUSBのサポートがディセーブルになります。
[Port 60/64 Emulation]	完全なUSBキーボードレガシーサポートのために60h/64hエミュレーションをシステムでサポートするかどうか。次のいずれかになります。 • [無効（Disabled）]：60h/64エミュレーションはサポートされません。 • [有効（Enabled）]：60h/64エミュレーションはサポートされます。 サーバーでUSB非対応オペレーティングシステムを使用する場合は、このオプションを選択する必要があります。
[xHCI Mode]	xHCIコントローラのレガシーサポートを有効または無効にします。次のいずれかになります。 • [Disabled]：xHCIコントローラのレガシーサポートを無効にします。 • [Enabled]：xHCIコントローラのレガシーサポートを有効にします。
[xHCI Legacy Support] ドロップダウン リスト	システム上でのレガシーxHCIコントローラのサポートを有効/無効にします。次のいずれかになります。 • [無効（Disabled）]：xHCIレガシーサポートを無効にします。 • [有効（Enabled）]：xHCIレガシーサポートを有効にします。これはデフォルト値です。

名前	説明
[すべてのUSBデバイス（All USB Devices）] ドロップダウン リスト	すべての物理および仮想USBデバイスを有効にするか無効にするか。次のいずれかになります。 • [Disabled]：すべての USB デバイスが無効です。 • [Enabled]：すべての USB デバイスが有効になります。
[USB Port: Rear]	背面パネルのUSBデバイスを有効にするか無効にするか。次のいずれかになります。 • [無効（Disabled）]：背面パネルのUSBポートをディセーブルにします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [有効（Enabled）]：背面パネルのUSBポートをイネーブルにします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。
[USB ポート：前面（USB Port:Front）]	前面パネルのUSBデバイスを有効にするか無効にするか。次のいずれかになります。 • [無効（Disabled）]：前面パネルのUSBポートをディセーブルにします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [有効（Enabled）]：前面パネルのUSBポートをイネーブルにします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。
[USB Port: Internal]	内部USBデバイスを有効にするか無効にするか。次のいずれかになります。 • [無効（Disabled）]：内部USBポートをディセーブルにします。これらのポートに接続されるデバイスは、BIOSおよびオペレーティングシステムによって検出されません。 • [有効（Enabled）]：内部USBポートをイネーブルにします。これらのポートに接続されるデバイスは、BIOSおよびオペレーティング システムによって検出されます。

名前	説明
[USB Port: KVM]	vKVM ポートが有効か無効か。次のいずれかになります。 • **無効**：vKVM キーボードおよびマウス デバイスを無効にします。キーボードとマウスは vKVM ウィンドウで機能しなくなります。 • **有効**：vKVM キーボードとマウス デバイスを有効にします。
[USB Port: vMedia]	仮想メディア デバイスを有効にするか無効にするか。次のいずれかになります。 • [無効（Disabled）]：vMedia デバイスをディセーブルにします。 • [Enabled]：vMedia デバイスを有効にします。

[PCI Configuration] のパラメータ

名前	説明
[Memory Mapped I/O Above 4GB]	4GB を超える MMIO をイネーブルまたはディセーブルにするかどうか。次のいずれかになります。 • [Disabled]：サーバーでは 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングしません。 • [有効（Enabled）]：サーバで 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングします。 （注） PCI デバイスが 64 ビット対応でも、レガシーなオプション ROM を使用する場合は、この設定をイネーブルにしても正しく機能しない場合があります。
[Sriov]	サーバー上で SR-IOV（Single Root I/O Virtualization）を有効にするか無効にするか。次のいずれかになります。 • [Disabled]：SR-IOV は無効になります。 • [有効（Enabled）]：SR-IOV はイネーブルになります。

名前	説明
[ASPM サポート（ASPM Support）] ドロップダウン リスト	BIOS での ASPM（アクティブ電源状態管理）サポートのレベルを設定できます。次のいずれかになります。 • [Disabled]：BIOS での ASPM サポートが無効です。 • [Force L0]：すべてのリンクを強制的に L0 スタンバイ（L0s）状態にします。 • [自動（Auto）]：電力状態を CPU によって判別します。
[NVMe SSD ホットプラグのサポート（NVMe SSD Hot-Plug Support）] ドロップダウン リスト	サーバの電源を切ることなく、NVMe SSD を交換できます。次のいずれかになります。 • [無効（Disabled）]：NVMe SSD ホットプラグ サポートが無効です。これはデフォルト値です。 • [有効（Enabled）]：NVMe SSD ホットプラグ サポートが有効です。
[VGA 優先順位（VGA Priority）] ドロップダウン リスト	システムに複数の VGA デバイスがある場合は、VGA グラフィックス デバイスの優先順位を設定できます。次のいずれかになります。 • [Onboard]：オンボード VGA デバイスが優先されます。BIOS ポスト画面および OS ブートはオンボード VGA ポート経由で駆動されます。 • [Offboard]：PCIE グラフィックス アダプタが優先されます。BIOS ポスト画面および OS ブートは外部グラフィックス アダプタ ポート経由で駆動されます。 • [オンボード VGA 無効（Onboard VGA Disabled）]：PCIE グラフィックス アダプタが優先され、オンボード VGA デバイスは無効になります。

サーバー モデル別 BIOS パラメータ

[Serial Configuration] のパラメータ

名前	説明
[Out-of-Band Mgmt Port]	Windows 緊急管理サービスで使用可能な COM ポート 0 を設定することができます。このセットアップ オプションに基づいて ACPI SPCR テーブルが報告されます。次のいずれかになります。 • [Disabled]：Windows オペレーティング システムで使われる汎用ポートとして COM ポート 0 を設定します。 • [有効（Enabled）]：Windows 緊急管理サービス用のリモート管理ポートとして COM ポート 0 を設定します。
[コンソールリダイレクション（Console redirection）] ドロップダウン リスト	POST および BIOS のブート中に、シリアル ポートをコンソール リダイレクションで使用できるようにします。BIOS のブートが完了し、オペレーティング システムがサーバを担当すると、コンソール リダイレクションの関連性はなくなり、無効になります。次のいずれかになります。 • [Disabled]：POST 中にコンソール リダイレクションは発生しません。 • [COM 0]：POST 中にCOM ポート 0 でコンソール リダイレクションを有効にします。 • [COM 1]：POST 中にCOM ポート 1 でコンソール リダイレクションを有効にします。
[Terminal type]	コンソール リダイレクションに使用される文字フォーマットのタイプ。次のいずれかになります。 • [PC-ANSI]：PC-ANSI 端末フォントが使用されます。 • [VT100]：サポートされている vt100 ビデオ端末とその文字セットが使用されます。 • [VT100+]：サポートされている vt100-plus ビデオ端末とその文字セットが使用されます。 • [VT-UTF8]：UTF-8 文字セットのビデオ端末が使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。

名前	説明
[Bits per second]	シリアル ポートの伝送速度として使用されるボー レート。[Console Redirection] を無効にする場合は、このオプションを使用できません。次のいずれかになります。 • [9600]：9,600 ボー レートが使用されます。 • [19200]：19,200 ボー レートが使用されます。 • [38400]：38,400 ボー レートが使用されます。 • [57600]：57,600 ボー レートが使用されます。 • [115200]：115,200 ボー レートが使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。
[フロー制御（Flow Control）] ドロップダウン リスト	フロー制御にハンドシェイク プロトコルを使用するかどうかを設定します。送信要求/クリア ツー センド（RTS/CTS）を使用すると、隠れた端末の問題が原因で発生する可能性がある、フレーム コリジョンを減らすことができます。次のいずれかになります。 • [None]：フロー制御は使用されません。 • **[Hardware RTS/CTS]**：フロー制御に RTS/CTS が使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。

名前	説明
[Putty KeyPad]	PuTTY ファンクション キーおよびテンキーの最上段のキーのアクションを変更できます。次のいずれかになります。 • [VT100]：ファンクション キーによって **ESC OP** ～ **ESC O[** を生成します。 • [LINUX]：Linux 仮想コンソールを模倣します。ファンクション キー F6 ～ F12 はデフォルト モードと同様に動作しますが、F1 ～ F5 は **ESC [[A** ～ **ESC [[E** を生成します。 • [XTERMR6]：ファンクション キー F5 ～ F12 がデフォルト モードと同様に動作します。ファンクション キー F1 ～ F4 によって ESC OP ～ ESC OS を生成します。これはデジタル端末のキーパッドの上段によって生成されるシーケンスです。 • [SCO]：ファンクション キー F1 ～ F12 によって **ESC [M** ～ **ESC [X** を生成します。ファンクション キーと Shift キーによって **ESC [Y** ～ **ESC [j** を生成します。Ctrl キーとファンクション キーによって **ESC [k** ～ **ESC [v** を生成します。Shift、Ctrl およびファンクション キーによって **ESC [w** ～ **ESC [{** を生成します。 • [ESCN]：デフォルト モードです。ファンクション キーはデジタル端末の一般的な動作と一致します。ファンクション キーによって **ESC [11~** や **ESC [12~** などのシーケンスを生成します。 • [VT400]：ファンクション キーはデフォルト モードと同様に動作します。テンキーの最上段のキーによって **ESC OP** ～ **ESC OS** を生成します。
[Redirection After BIOS POST]	BIOS POST が完了し、OS ブートローダに制御が渡された後に、BIOS コンソール リダイレクションがアクティブであるかどうか。次のいずれかになります。 • **[Always Enable]**：OS のブートおよび実行時に BIOS レガシー コンソール リダイレクションがアクティブになります。 • [Bootloader]：OS ブートローダに制御が渡される前に BIOS レガシー コンソール リダイレクションがディセーブルになります。

[LOM and PCIe Slots Configuration] のパラメータ

名前	説明
[VICに対するCDNサポート（CDN Support for VIC）] ドロップダウン リスト	イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [無効（Disabled）]：VICカードに対するCDNサポートは無効です。 • [有効（Enabled）]：CDNサポートはVICカードに対して有効です。 （注） VIC カードの CDN サポートは、Windows 2012 または最新の OS でのみ機能します。
[PCI ROM CLP]	PCI ROM Command Line Protocol（CLP）は、カード上の iSCSI や PxE などのさまざまなオプション ROM の実行を制御します。デフォルト設定は、ディセーブルです。 • [Enabled]：ポートごとに個別に、iSCSI や PxE などのさまざまなオプション ROM の実行を設定できるようにします。 • [Disabled]：デフォルト オプションです。異なるオプション ROM は選択できません。デフォルト オプション ROM は PCI 列挙中に実行されます。
[PCH SATA Mode]	このオプションでは、PCH SATA モードを選択できます。次のいずれかになります。 • [AHCI]：SATA コントローラと sSATA コントローラの両方を AHCI モードに設定します。 • [Disabled]：SATA コントローラと sSATA コントローラを無効にします。 • [LSI SW Raid]：SATA コントローラと sSATA コントローラを LSI SW Raid の raid モードに設定します。
[All Onboard LOM Ports]	すべての LOM ポートを有効にするか無効にするか。次のいずれかになります。 • [Disabled]：すべての LOM ポートが無効です。 • [Enabled]：すべての LOM ポートが有効になります。

名前	説明
[LOM Port *n* OptionROM]	***n*** で指定された LOM ポートでオプション ROM を使用できるかどうか。次のいずれかになります。 • [Disabled]：スロット ***n*** のオプション ROM は使用できません。 • [Enabled]：スロット ***n*** のオプション ROM は使用可能です。 • **[UEFI Only]**：スロット ***n*** のオプション ROM は UEFI にのみ使用できます。 • **[Legacy Only]**：スロット ***n*** のオプション ROM はレガシーにのみ使用できます。
[All PCIe Slots OptionROM]	PCIe カードのオプション ROM をサーバーが使用できるかどうか。次のいずれかになります。 • [Disabled]：スロット ***n*** のオプション ROM は使用できません。 • [Enabled]：スロット ***n*** のオプション ROM は使用可能です。 • **[UEFI Only]**：スロット ***n*** のオプション ROM は UEFI にのみ使用できます。 • **[Legacy Only]**：スロット ***n*** のオプション ROM はレガシーにのみ使用できます。
[PCIe Slot:*n* OptionROM	PCIe カードのオプション ROM をサーバーが使用できるかどうか。次のいずれかになります。 • [Disabled]：スロット ***n*** のオプション ROM は使用できません。 • [Enabled]：スロット ***n*** のオプション ROM は使用可能です。 • **[UEFI Only]**：スロット ***n*** のオプション ROM は UEFI にのみ使用できます。 • **[Legacy Only]**：スロット ***n*** のオプション ROM はレガシーにのみ使用できます。

名前	説明
[PCIe Slot:MLOM OptionROM]	このオプションでは、MLOM スロットに接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • [Enabled]：レガシーおよび UEFI オプション ROM の両方を実行します。 • **[無効（Disabled）]**：レガシーおよび UEFI の両方のオプション ROM は実行されません。 • **[UEFI のみ（UEFI Only）]**：UEFI オプション ROM のみを実行します。 • [Legacy Only]：レガシー オプション ROM のみを実行します。
[PCIe Slot:HBA OptionROM]	このオプションでは、HBA スロットに接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • [Enabled]：レガシーおよび UEFI オプション ROM の両方を実行します。 • **[無効（Disabled）]**：レガシーおよび UEFI の両方のオプション ROM は実行されません。 • **[UEFI のみ（UEFI Only）]**：UEFI オプション ROM のみを実行します。 • [Legacy Only]：レガシー オプション ROM のみを実行します。
[PCIe Slot:N1 OptionROM]	このオプションでは、SSD:NVMe1 スロットに接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • [Enabled]：レガシーおよび UEFI オプション ROM の両方を実行します。 • **[無効（Disabled）]**：レガシーおよび UEFI の両方のオプション ROM は実行されません。 • **[UEFI のみ（UEFI Only）]**：UEFI オプション ROM のみを実行します。 • [Legacy Only]：レガシー オプション ROM のみを実行します。

名前	説明
[PCIe Slot:N2 OptionROM]	このオプションでは、SSD:NVMe2 スロットに接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • [Enabled]：レガシーおよび UEFI オプション ROM の両方を実行します。 • **[無効（Disabled）]**：レガシーおよび UEFI の両方のオプション ROM は実行されません。 • **[UEFI のみ（UEFI Only）]**：UEFI オプション ROM のみを実行します。 • [Legacy Only]：レガシー オプション ROM のみを実行します。
[PCIe Slot:HBA Link Speed] **PCIe SlotHBALinkSpeed**	このオプションを使用すると、PCIe HBA スロットに装着されているアダプタ カードの最大速度を制限できます。次のいずれかになります。 • [自動（Auto）]：システムは許可される最大速度を選択します。 • [GEN1]：最大 2.5 GT/s（ギガトランスファー/秒）までの速度が許可されます。 • [GEN2]：最大 5 GT/s までの速度が許可されます。 • [GEN3]：最大 8 GT/s までの速度が許可されます。 • [Disabled]：最大速度は制限されません。

[BIOS Configuration] ダイアログボックスのボタン バー

重要 このダイアログボックスのボタンは、表示しているタブのパラメータのみでなく、使用可能なすべてのタブのすべての BIOS パラメータに影響します。

名前	説明
[Save Changes] ボタン	3 つのタブすべての BIOS パラメータの設定を保存し、ダイアログボックスを閉じます。 [Reboot Host Immediately] チェックボックスがオフの場合、サーバはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバが手動でリブートされるまで保存されます。

名前	説明
[Reset Values] ボタン	3 つのタブすべての BIOS パラメータの値を、このダイアログボックスを最初に開いたときに有効だった設定に復元します。
[Restore Defaults] ボタン	3 つのタブすべての BIOS パラメータをそのデフォルト値に設定します。
[Cancel] ボタン	変更を行わずにダイアログボックスを閉じます。

C220M4 および C240M4 サーバの [サーバ管理（Server Management）] タブ

サーバ リブート オプション

[Save Changes] をクリックした後で変更内容を自動的に適用するには、[Reboot Host Immediately] チェックボックスをオンにします。Cisco IMC によってサーバがただちにリブートされて、変更が適用されます。

変更内容を後で適用するには、[Reboot Host Immediately] チェックボックスをオフにします。Cisco IMC によって変更が保存され、次回サーバがリブートするときに適用されます。

（注） 保留中の BIOS パラメータの変更がすでにある場合、Cisco IMC は、[Save Changes] をクリックしたときに、保存されている値を現在の設定で自動的に上書きします。

サーバ管理 BIOS パラメータ

名前	説明
[FRB-2 Timer]	POST 中にシステムがハングアップした場合に、システムを回復するために Cisco IMC で FRB2 タイマーを使用するかどうか。次のいずれかになります。 • [無効（Disabled）]：FRB2 タイマーは使用されません。 • [Enabled]：POST 中に FRB2 タイマーが開始され、必要に応じてシステムの回復に使用されます。

サーバー モデル別 BIOS パラメータ

名前	説明
[OS ウォッチドッグ タイマー（OS Watchdog Timer）] ドロップダウン リスト	BIOS が指定されたタイムアウト値でウォッチドッグ タイマーをプログラムするかどうか。次のいずれかになります。 • [Disabled]：サーバーのブートにかかる時間をトラッキングするためにウォッチドッグ タイマーは使用されません。 • [Enabled]：サーバーのブートにかかる時間をウォッチドッグタイマーでトラッキングします。サーバーが [OSブートウォッチドッグタイマータイムアウト（OS Boot Watchdog Timer Timeout）] フィールドに指定された時間内にブートしない場合、Cisco IMC はエラーをログに記録し、[OSブートウォッチドッグポリシー（OS Boot Watchdog Policy）] フィールドに指定されたアクションを実行します。
[OSウォッチドッグタイマータイムアウト（OS Watchdog Timer Timeout）] ドロップダウン リスト	OS が指定された時間内にブートしない場合、OS ウォッチドッグ タイマーの期限が切れ、システムはタイマー ポリシーに基づいてアクションを実行します。次のいずれかになります。 • **[5 Minutes]**：OS ウォッチドッグ タイマーは、ブートが開始されてから 5 分後に期限が切れます。 • **[10 Minutes]**：OS ウォッチドッグ タイマーは、ブートが開始されてから 10 分後に期限が切れます。 • **[15 Minutes]**：OS ウォッチドッグ タイマーは、ブートが開始されてから 15 分後に期限が切れます。 • **[20 Minutes]**：OS ウォッチドッグ タイマーは、ブートが開始されてから 20 分後に期限が切れます。 （注） このオプションは [OS Boot Watchdog Timer] をイネーブルにした場合にのみ適用されます。

名前	説明
[OSウォッチドッグタイマーポリシー（OS Watchdog Timer Policy）] ドロップダウン リスト	ウォッチドッグ タイマーが切れた場合にシステムで実行されるアクション。次のいずれかになります。 • **[Do Nothing]**：OS のブート中にウォッチドッグ タイマーの期限が切れた場合、アクションは実行されません。 • **[電源オフ（Power Down）]**：OS のブート中にウォッチドッグタイマーの期限が切れた場合、サーバーの電源がオフになります。 • [Reset]：OS のブート中にウォッチドッグ タイマーが切れた場合、サーバーはリセットされます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にする場合にのみ適用されます。

[BIOS Configuration] ダイアログボックスのボタン バー

重要 このダイアログボックスのボタンは、表示しているタブのパラメータのみでなく、使用可能なすべてのタブのすべての BIOS パラメータに影響します。

名前	説明
[Save Changes] ボタン	3 つのタブすべての BIOS パラメータの設定を保存し、ダイアログボックスを閉じます。 [Reboot Host Immediately] チェックボックスがオフの場合、サーバはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバが手動でリブートされるまで保存されます。
[Reset Values] ボタン	3 つのタブすべての BIOS パラメータの値を、このダイアログボックスを最初に開いたときに有効だった設定に復元します。
[Restore Defaults] ボタン	3 つのタブすべての BIOS パラメータをそのデフォルト値に設定します。
[Cancel] ボタン	変更を行わずにダイアログボックスを閉じます。

サーバー モデル別 BIOS パラメータ

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。