Cisco UCS C シリーズ Integrated Management Controller GUI 構成ガイド - Cisco UCS M7 以降のラック サーバー、リリース 6.0

最終更新：2026 年 1 月 5 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/

© 2025 Cisco Systems, Inc. All rights reserved.

目 次

はじめに：

はじめに xvii

対象読者 xvii

表記法 xvii

Cisco UCS の関連ドキュメント xix

第 1 章

概要 1

Cisco UCS C シリーズ ラックマウント サーバの概要 1

サーバ ソフトウェアの概要 2

サーバ ポート 3

Cisco Integrated Management Controller 3

Cisco IMC ユーザー インターフェイスの概要 6

ナビゲーションとアプリ 7

メニューバー 10

Cisco Integrated Management Controller オンライン ヘルプの概要 10

Cisco IMC へのログイン 11

Cisco IMC からのログアウト 12

第 2 章

サーバ OS のインストール 13

第 3 章

シャーシの管理 15

Intersight Infrastructure Service ライセンス 15

シャーシの概要の表示 16

シャーシ インベントリ 21

電源のプロパティの表示 21

Cisco VIC アダプタのプロパティの表示 22
ストレージのプロパティの表示 22
GPU インベントリの表示 23

第 4 章 サーバーの管理 27
サーバのブート順 27
高精度ブート順の設定 29
ブート デバイスの管理 33
UEFI セキュア ブートの概要 43
UEFI セキュア ブートのイネーブル化 44
UEFI セキュア ブートのディセーブル化 45
サーバーの実際のブート順の表示 45
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 46
サーバ アセット タグの作成 47
BIOS トークン 47
Cisco UCS C220 M8 および C240 M8 47
[I/O] タブ 47
[Server Management] タブ 57
メモリ タブ 61
[電源/パフォーマンス（Power/Performance）] タブ 68
[プロセッサ（Processor）] タブ 74
[セキュリティ（Security）] タブ 87
Cisco UCS C225 M8 93
[I/O] タブ 93
[Server Management] タブ 109
メモリ タブ 114
[電源/パフォーマンス（Power/Performance）] タブ 121
[セキュリティ（Security）] タブ 124
[プロセッサ（Processor）] タブ 126
Cisco UCS C245 M8 134
[I/O] タブ 134

メモリ タブ 140
[電源/パフォーマンス（Power/Performance）] タブ 147
[プロセッサ（Processor）] タブ 149
[セキュリティ（Security）] タブ 156
[Server Management] タブ 158
Cisco UCS C220 および C240 M7 164
[I/O] タブ 164
メモリ タブ 172
[電源/パフォーマンス（Power/Performance）] タブ 179
[プロセッサ（Processor）] タブ 185
[セキュリティ（Security）] タブ 201
[Server Management] タブ 207
電力ポリシーの設定 212
電力制限 212
電源の冗長性ポリシーの設定 213
電力特性評価の有効化 214
パワー キャッピングの有効化 215
[電源プロファイル（Power Profiles）] 216
標準電力プロファイルの設定 216
詳細電力プロファイルの設定 219
電力プロファイルのデフォルトへのリセット 222
電力モニタリング 222
電力モニタリングの概要の表示 223
チャートでの電力統計の表示 225
電力復元ポリシーの設定 227
ファン ポリシーの設定 229
ファン制御ポリシー 229
ファン ポリシーの設定 231
DIMMブロックリストの構成 235
DIMMブロックリスト 235
DIMM のブロック リストの有効化 236

BIOS の設定 237
Configuring BIOS Settings 237
BIOS セットアップの開始 237
BIOS CMOS のクリア 238
製造元のカスタム BIOS 設定の復元 238
BIOS デフォルトの復元 239
BIOS プロファイル 239
BIOS プロファイルのアップロード 239
BIOS プロファイルのアクティブ化 241
BIOS プロファイルの削除 242
BIOS プロファイルのバックアップ 242
BIOS プロファイルの詳細の表示 242
セキュアブート証明書の管理 243
セキュアブート証明書の詳細の表示 243
セキュア ブート証明書のアップロード 245
セキュアブート証明書の削除 247
前面パネルの動的温度しきい値の設定 248
永続メモリ モジュール 248

第 5 章 サーバのプロパティの表示 251
Viewing Server Utilization 251
サーバー コンポーネントの表示 - 熱パフォーマンス 252
CPU のプロパティの表示 254
メモリのプロパティの表示 256
PCI アダプタのプロパティの表示 260
ストレージのプロパティの表示 261
TPM のプロパティの表示 263
PID カタログの表示 264

第 6 章 センサーの表示 267
温度センサーの表示 267

LED センサーの表示 268
ストレージ センサーの表示 268
電源センサーの表示 269
ファン センサーの表示 270

第 7 章 リモート プレゼンスの管理 273
Serial over LAN の設定 273
仮想メディアの設定 275
Cisco IMC マップされた vMedia ボリュームの作成 276
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 281
Cisco IMC によりマップされた vMedia ボリュームの削除 282
既存の Cisco IMC vMedia イメージの再マッピング 283
Cisco IMC vMedia イメージの削除 283
仮想 KVM コンソール 283
KVM コンソールの起動 284
仮想 KVM コンソール - Cisco UCS C-Series M6 以降のサーバー 285
仮想 KVM の設定 302
仮想 KVM のイネーブル化 304
仮想 KVM のディセーブル化 304

第 8 章 ユーザー アカウントの管理 305
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 305
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 309
ユーザ アカウントでの SSH キーの管理 313
SSH キーの設定 313
SSH キーの追加 315
SSH キーの変更 317
SSH キーの削除 318
パスワードの有効期限切れ 319
パスワードの有効期間の有効化と設定 320
非管理者ユーザーとしてパスワードの変更 321

アカウントロックアウトの詳細の構成 322
ユーザー認証の優先順位の構成 323
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 324
LDAP サーバ 325
LDAP サーバの設定 326
Cisco IMC 上の LDAP サーバーの設定 327
LDAP 設定およびグループ承認の設定 329
LDAP 証明書の概要 333
LDAP CA 証明書ステータスの表示 334
LDAP CA 証明書のエクスポート 334
LDAP CA 証明書のアップロード 335
LDAP バインディングのテスト 337
TACACS+ 認証 337
TACACS+サーバ設定 338
TACACS+ 認証のイネーブル化 338
TACACS+ リモート サーバー設定の構成 339
ユーザー セッションの表示と終了 340

第 9 章 シャーシ関連の設定の指定 343
サーバの電源管理 343
Web UI からのホスト名/IP アドレスの ping 344
ロケータ LED の切り替え 345
時間帯の選択 345

第 10 章 ネットワーク関連の設定 347
ネットワーク関連の設定 347
サーバー NIC 347
サーバ NIC の設定 351
Cisco VIC mLOM および OCP カードの交換に関する考慮事項 357
単一 IP の設定 359
単一 IP プロパティの設定 359

共通プロパティの設定 360
共通プロパティの設定の概要 360
共通プロパティの設定 361
IPv4 の設定 362
IPv6 の設定 363
VLAN への接続 365
ネットワーク セキュリティの設定 365
ネットワーク セキュリティ 365
ネットワーク セキュリティの設定 [英語] 366
Network Time Protocol の設定 367
Network Time Protocol サービス設定 367
Network Time Protocol 設定の指定 367

第 11 章 ネットワーク アダプタの管理 369
Cisco UCS C シリーズ ネットワーク アダプタの概要 369
Cisco UCS ネットワーク アダプタのプロパティの表示 372
vHBA の管理 382
vHBA 管理のガイドライン 382
vHBA のプロパティの表示と変更 383
vHBA の作成 390
vHBA の複製 396
vHBA の削除 398
vHBA ブート テーブル 398
ブート テーブル エントリの作成 398
ブート テーブル エントリの削除 399
vHBA の永続的なバインディング 399
永続バインディングの表示と有効化 399
永続的なバインディングの再作成 400
vNIC の管理 401
vNIC 管理のガイドライン 401
vNIC プロパティの表示と変更 401

vNIC の作成 420
vNIC の複製 435
vNIC の削除 436
iSCSI ブート機能の設定 436
vNIC の iSCSI ブート機能の設定 436
vNIC 上の iSCSI ブート機能の設定 437
vNIC からの iSCSI ブート設定の除去 440
Cisco usNIC の管理 441
vNIC での Cisco usNIC の表示と設定 441
アダプタ設定のバックアップと復元 444
アダプタ設定のエクスポート 444
アダプタ設定のインポート 445
アダプタのデフォルトの復元 447
アダプタのリセット 447

第 12 章 ストレージ アダプタの管理 449
自己暗号化ドライブ（フル ディスク暗号化） 450
コントローラ セキュリティの有効化 451
コントローラ セキュリティの変更 452
コントローラ セキュリティの無効化 453
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 454
未使用の物理ドライブからの仮想ドライブの作成 454
既存のドライブ グループからの仮想ドライブの作成 458
仮想ドライブを転送対応として設定 461
外部設定のインポート 462
外部設定のクリア 463
ブート ドライブのクリア 464
JBOD の有効化 465
JBOD の無効化 465
コントローラの TTY ログの取得 466
コントローラの設定のクリア 466

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 467
ドライブの削除のための準備 467
専用ホット スペアにする 468
グローバル ホット スペアにする 469
ホット スペア プールからのドライブの削除 470
物理ドライブのステータスの切り替え 471
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 471
仮想ドライブの初期化 472
ブート ドライブとして設定 473
仮想ドライブの編集 474
仮想ドライブの削除 476
仮想ドライブの非表示化 477
バッテリ バックアップ ユニットの学習周期の開始 477
ストレージ コントローラ ログの表示 478
MegaRAID コントローラの SSD スマート情報の表示 479
NVMe コントローラの詳細の表示 481
NVMe 物理ドライブの詳細の表示 483
PCI スイッチの詳細の表示 486
コピーバック操作の開始 491
Flexible Flash コントローラの管理 491
Cisco Flexible Flash 491
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 494
Flexible Flash コントローラ プロパティの設定 495
Flexible Flash コントローラ ファームウェア モードの設定 496
Flexible Flash コントローラ カードの設定 497
Flexible Flash カードからのブート 498
Flexible Flash コントローラのリセット 499
仮想ドライブの編集 500
仮想ドライブの消去 502
仮想ドライブの同期 503

ISO イメージ設定の追加 503
ISO イメージの更新 505
ISO イメージのマップ解除 506
Cisco Flexible Flash カード設定のリセット 507
Cisco Flexible Flash カードの設定の保持 508
FlexFlash ログの詳細の表示 509
FlexUtil コントローラの管理 512
FlexUtil コントローラのプロパティの設定 513
FlexUtil カード設定のリセット 514
Cisco FlexUtil コントローラのプロパティの表示 514
物理ドライブのプロパティの表示 517
仮想ドライブのプロパティの表示 523
仮想ドライブへのイメージのマッピング 525
仮想ドライブ上のイメージの更新 528
仮想ドライブからのイメージのマッピング解除 528
仮想ドライブの消去 528
Cisco ブート最適化 M.2 Raid コントローラ 529
Cisco ブート最適化 M. 2 Raid コントローラの詳細の表示 529
Viewing Physical Drive Info for Cisco Boot Optimized M.2 Raid Controller 534
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 542
Cisco FlexMMC 547
Cisco FlexMMC の詳細の表示 547
新しいイメージ ファイルのアップロード 548
イメージ ファイルの削除 553
イメージのマッピングまたはマップ解除 554
FlexMMC をデフォルト設定へリセット 555

第 13 章 コミュニケーション サービスの設定 557
TLS v1.2 の有効化または無効化 557
HTTP の設定 559
SSH の設定 561

XML API の設定 562
Cisco IMC 用の XML API 562
XML API のイネーブル化 562
Redfish のイネーブル化 563
IPMI の設定 564
IPMI Over LAN 564
IPMI over LAN の設定 564
SNMP の設定 565
SNMP 565
SNMP プロパティの設定 566
SNMP トラップ設定の指定 568
テスト SNMP トラップ メッセージの送信 570
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 570
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 571
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 571
SMTP 電子メール受信者の追加 572

第 14 章 証明書とサーバー セキュリティの管理 575
サーバ証明書の管理 575
サーバ証明書の管理 575
証明書署名要求を生成する 576
証明書自己署名要求 580
Linux を使用した自己署名証明書の作成 584
Windows を使用した自己署名証明書の作成 586
サーバ証明書のアップロード 586
外部証明書の管理 588
外部証明書のアップロード 588
外部秘密キーのアップロード 590
外部証明書の有効化 592
SPDM セキュリティ：MCTP SPDM 593
SPDM セキュリティ 593

MCTP SPDM 障害アラート設定の構成と表示 594
SPDM 認証 ステータスの表示 595
認証局証明書の追加 597
証明書および証明書の詳細のリストを表示する 598
証明書の削除 602
キー管理相互運用性プロトコル 603
セキュアなキー管理設定の表示 603
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 605
ルート CA 証明書 606
ルート CA 証明書のダウンロード 606
ルート CA 証明書のエクスポート 608
ルート CA 証明書の削除 609
クライアント証明書のダウンロード 610
Client Certificate 611
クライアント証明書のエクスポート 611
クライアント証明書の削除 613
クライアント秘密キーのダウンロード 613
クライアント秘密キー 615
クライアント秘密キーのダウンロード 615
クライアント秘密キーの削除 617
KMIP サーバー接続のテスト 617
KMIP サーバーのデフォルト設定への復元 618
KMIP ログイン詳細の削除 618
Cisco IMC での FIPS 140-2 の準拠 618
セキュリティ設定の有効化 619
セキュリティ設定（FIPS）の有効化 619

第 15 章 ファームウェアの管理 621
ファームウェア管理の概要 621
ファームウェア コンポーネントの表示 621
ファームウェアの更新 623

ファームウェアのアクティブ化 625
ファームウェアのアクティベーションのキャンセル 626

第 16 章 障害およびログの表示 629
障害サマリーの表示 629
障害履歴の表示 630
システム イベント ログの表示 631
Cisco IMC ログの表示 632
ロギング制御 633
ロギング制御の表示 633
リモート サーバへの Cisco IMC ログの送信 636
Cisco IMC ログしきい値の設定 639
リモート サーバーへのテスト Cisco IMC ログの送信 640
リモート Syslog 証明書の管理 641
リモート Syslog 証明書のアップロード 641
リモート Syslog 証明書の削除 644

第 17 章 サーバ ユーティリティ 645
テクニカル サポート データのエクスポート 645
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 650
出荷時の初期状態へのリセット 652
Cisco IMC 設定のエクスポートとインポート 656
Cisco IMC 設定のエクスポート 656
Cisco IMC 設定のインポート 658
ホストへのマスク不可能な割り込みの生成 660
Cisco IMC バナーの追加または更新 661
Cisco IMC の最後のリセット理由の表示 662
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 662
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 663
PIDカタログ 664
PID カタログのアップロード 664

PID カタログの有効化 666
PID カタログを削除 667
スマート アクセス USB の有効化 668
デバイス コネクタの設定 669
Cisco Intersight 管理の有効化/無効化 669
Intersight デバイス コネクタのプロパティの表示 669
デバイス コネクタの HTTPS プロキシ設定の設定 676

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 （xvii ページ）
- 表記法 （xvii ページ）
- Cisco UCS の関連ドキュメント （xix ページ）

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。

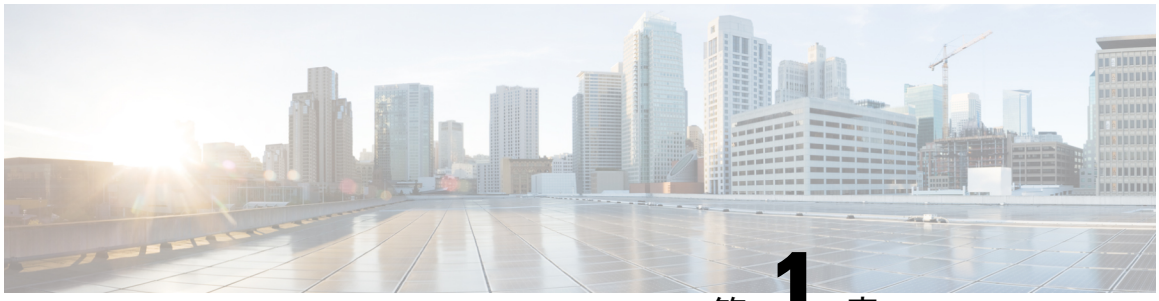
Cisco UCS の関連ドキュメント

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、URL（https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/ucs_rack_roadmap.html）で入手可能な『*Cisco UCS C-Series Servers Documentation Roadmapdoc Roadmap*』を参照してください。

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。



第 1 章

概要

この章は、次の項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 （1 ページ）
- サーバ ソフトウェアの概要 （2 ページ）
- サーバ ポート （3 ページ）
- Cisco Integrated Management Controller （3 ページ）
- Cisco IMC ユーザー インターフェイスの概要 （6 ページ）

Cisco UCS C シリーズ ラックマウント サーバの概要

Cisco Integrated Management Controller の新しい Web GUI は、次のサーバーモデルと互換性があります。

- Cisco UCS C220 M8 ラックマウント サーバー
- Cisco UCS C240 M8 ラックマウント サーバー
- Cisco UCS C225 M8 ラックマウント サーバー
- Cisco UCS C245 M8 ラックマウント サーバー
- Cisco UCS C220 M7 ラックマウント サーバー
- Cisco UCS C240 M7 ラックマウント サーバー

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 M8 ラックマウント サーバー
- Cisco UCS C240 M8 ラックマウント サーバー
- Cisco UCS C225 M8 ラックマウント サーバー
- Cisco UCS C245 M8 ラックマウント サーバー
- Cisco UCS C220 M7 ラックマウント サーバー
- Cisco UCS C240 M7 ラックマウント 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

（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 から入手できます。

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 サーバーには、Cisco Integrated Management Controller（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 サーバー CPU から独立して）Cisco IMC ファームウェアを実行します。システムには、現行バージョンの Cisco IMC ファームウェアが付属しています。Cisco IMC ファームウェアは更新可能ですが、初期インストールは必要ありません。

サーバー OS

Cisco UCS C シリーズ ラック サーバーは、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、『UCS ハードウェアとソフトウェアの互換性』を参照してください。KVM コンソールおよび vMedia を使ってサーバーに 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にある『*Cisco UCS C* シリーズ サーバー ドキュメンテーション ロードマップ』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
Intersight 管理ポート	8889
Intersight クラウド ポート	8888
SOL SSH ポート	2400
SNMPポート	161
SNMP トラップ	162
外部Syslog	514

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 はサーバー内で実行されます。

（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 GUI を使用して Cisco IMC CLI を呼び出すこと。
- Cisco IMC CLI で呼び出したコマンドを Cisco IMC GUI に表示すること。
- Cisco IMC GUI から Cisco IMC CLI 出力を生成すること。

Cisco IMC で実行できるタスク

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 ファームウェアの更新
- 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 ファームウェアのインストールとアクティブ化
- 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

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 ファームウェアの更新
- 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に、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。

OS のバージョン	Browser	Browser Version
MAC OS 14.2.1（23C71）	Google Chrome	バージョン 122.0.6261.129（公式ビルド）（x86_64）
MAC OS 14.2.1（23C71）	Mozilla Firefox	123.0.1
MAC OS 14.2.1（23C71）	Safari	バージョン 17.2.1（19617.1.17.11.12）
Windows 11	Google Chrome	バージョン 122.0.6261.131（公式ビルド）（64 ビット）
Windows 11	Microsoft Edge	バージョン 122.0.2365.92（公式ビルド）（64 ビット）
Windows 11	Google Chrome	バージョン 123.0.6312.59（公式ビルド）（64 ビット）
Windows 11	Firefox	124.0.1（64 ビット）
Windows 11	Firefox	24.0.1
Windows 11	Chrome	123.0.6312.58（公式ビルド）（64 ビット）
Ubuntu 20.04.3 LTS	Mozilla Firefox	125.0.2（64 ビット）

ブラウザの最新の仕様セットについては、『Cisco UCS ラック サーバー ソフトウェア リリース ノート』を参照してください。

（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* シリーズ サーバー ドキュメンテーション ロードマップ』から入手できます。

ナビゲーションとアプリ

Cisco Integrated Management Controller の GUI メニューバーは、次の [アプリ（Apps）] ドロップダウンリストで構成されます。

ダッシュボード アプリ

[ダッシュボード（Dashboard）] アプリには次の情報が表示されます。

- **[サーバーの詳細（Server Details）]**：製品名、シリアル番号などのサーバーの詳細を表示します。また、BIOS の概要、ブート順序、およびアクションを表示できます。
- **[CIMC 情報（CIMC Information）]**：IP アドレス、MAC アドレスなどの Cisco IMC 情報が表示されます。また、タイムゾーンを表示および更新できます。
- **[シャーシステータス（Chassis Status）]**：サーバーコンポーネント全体のステータスを表示します。また、障害の概要ページを表示することもできます。
- **[プロセッサとメモリの概要（Processor and Memory summary）]**：サーバーの CPU とメモリの概要が表示され、CPU とメモリの詳細を表示できます。
- **[ストレージの概要（Storage summary）]**：コントローラ、物理ドライブ、および仮想ドライブの概要を表示します。
- **[ネットワークの概要（Networking summary）]**：アダプタ、ホストインターフェイス、外部インターフェイスの概要を表示します。
- **[インタラクティブ KVM コンソール（Interactive KVM Console）]**：KVM サーバーに対してアクションを実行できます。
- **クイック アクション（Quick Actions）**：リンクにすばやくアクセスして、RAID ボリュームの作成、仮想 NIC インターフェイスの作成、新しいユーザーの作成、仮想 HBA インターフェイスの作成、ファームウェアのアップロード、技術ログの生成、Cisco IMC コンフィギュレーションのインポート/エクスポート、モニタリングなどのアクションを実行でき、パフォーマンスを向上させます。
- **[サーバーアクション（Server Actions）]**：サーバー電源 およびシステム アクションを実行できます。

システム アプリ

[システム（System）] アプリには、次のタブが含まれています。

- **[全般（General）] タブ**：サーバー 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。
- **[インベントリ（Inventory）] タブ**：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。
- **[センサー（Sensors）] タブ**：電源装置、ファン、温度、電圧、電流、LED、およびストレージ。

- **[バックプレーン管理（Backplane Management）] タブ**：ネットワークデバイス内のさまざまなスロットの動作ステータスとモードを監視および設定します。
- **[電源管理（Power Management）タブ]**：電力制限の構成と電源モニタリング。
- **[障害とログ（Faults and Logs）] タブ**：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。

コンピューティング アプリ

[コンピューティング アプリ（Compute App）] には、サーバーに関する次の情報が含まれています。

- **[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。
  - トークン
  - ブート順序
  - プロファイル
  - セキュアブート証明書の管理
- **[リモート管理（Remote Management）]**：LAN 設定上の KVM、仮想メディア、およびシリアル。

ネットワーキング アプリ

[ネットワーキング アプリ（Networking App）] には、[Cisco VIC アダプタ（Cisco VIC Adapters）] の下に次の情報が表示されます。

- **[全般（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。
- **[DCE インターフェイス（DCE Interface）]**：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。
- **[vNIX インターフェイス（vNIC Interface）]**：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 インターフェイス（vHBA Interface）]**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。

ストレージ アプリ

[ストレージ アプリ（Storage App）] には、次の メニューが含まれています。

- コントローラ
  - **[コントローラ情報（Controller Info）]**：RAID コントローラに関する一般的な情報と設定情報。
  - **[物理ドライブ情報（Physical Drive Info）]**：一般的な物理ドライブと対応する RAID 情報。
  - **[仮想ドライブ情報（Virtual Drive Info）]**：一般的な仮想ドライブと対応する RAID 情報。
- [Cisco FlexMMC]：IMC イメージとユーザファイルのストレージに関する一般的な情報。IMCイメージパーティションとユーザーファイルパーティションにファイルをアップロードできます。

管理アプリ

[管理 アプリ（Administration App ）] には、次の メニューが含まれています。

- **[ユーザー管理（User Management）]**：ローカルユーザー管理、LDAP、セッション管理、および TACACS+。
- **[ネットワーキング（Networking）]**：ネットワーク プロパティおよびネットワーク設定。
- **[通信サービス (Communication Services)]**：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)]、[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。
  - **[通信サービス (Communication Services)]**：HTTP プロパティ、SSH プロパティ、XML API プロパティ、Redfish プロパティ、Serial over LAN、TLS 構成、および IPMI over LAN プロパティ
  - **[SNMP]**：SNMP のプロパティ、ユーザ設定、およびトラップ宛先
  - **[メール アラート（Mail Alert）]**：SMTP プロパティと SMTP 受信者
- **[セキュリティ管理（Security Management）]**：証明書管理、セキュリティキー管理、セキュリティ構成、 、MCTP SPDM。
- **[イベント管理（Event Management）]**：プラットフォーム イベント フィルタの有効化/無効化 およびイベント フィルタのリセット
- **[ファームウェア管理（Firmware Management）]**Cisco IMC および BIOS ファームウェア情報と管理。
- **[ユーティリティー（Utilities）]**：最後のテクニカルサポートデータのエクスポート、Cisco IMC の最後のリセット、 Cisco IMC 構成のインポート/エクスポート、インベントリデータ、 VIC アダプタのインポート/エクスポート、 工場出荷時のデフォルト状態、 前面パネル USB。

- **[デバイス コネクタ（Device Connector）]**：Cisco Intersight 管理およびネットワーク設定。

メニューバー

表 *2:* ツールバー

名前	説明
[アプリ（App）] ドロップダウンリスト	リストから目的のアプリを選択できます。
[情報（Information）] アイコン	Cisco IMC バージョン情報を表示できます。
[ヘルプ（Help）] アイコン	オンライン ヘルプを起動できます。
[障害サマリ（Faults Summary）] アイコン	一定期間に発生したさまざまな障害に関する詳細が表示されます。詳細については、を参照してください。
[障害サマリ（Tasks Notification）] アイコン	さまざまなタスク ステータスを表示できます。
[Cisco IMC] 情報	次の情報を表示します。 • ログイン ユーザー ロール • Cisco IMC ホスト名 • [ログアウト（Logout）] ボタン • **[ダーク/ライト（Dark/Light）]** テーマトグルボタン：UIのライトテーマとダークテーマを切り替えられます。

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

リリース 4.3(5) 以降、Cisco Integrated Management Controller (Cisco IMC) ソフトウェア GUI のメニュー バーには次のアプリがあります。

- ダッシュボード アプリ
- システム アプリ
- コンピューティング アプリ
- ネットワーキング アプリ
- ストレージ アプリ
- 管理アプリ

このヘルプ システムは、アプリごとの Cisco IMC GUI ページのフィールドとダイアログ ボックス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、メニュー バーの **[ヘルプ（Help）]** アイコンをクリックします。

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 の Web UI 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 'password' の語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。

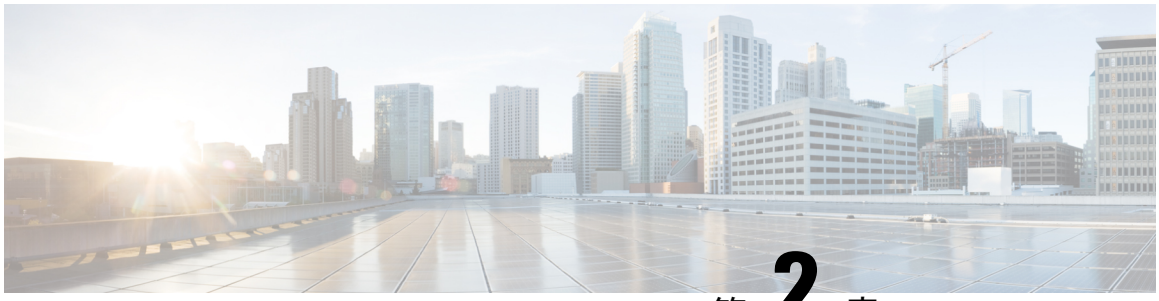
Cisco IMC からのログアウト

手順

ステップ 1 Cisco IMC の右上にあるサーバー情報の領域をクリックし、ドロップダウン ダイアログボックスから **[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。

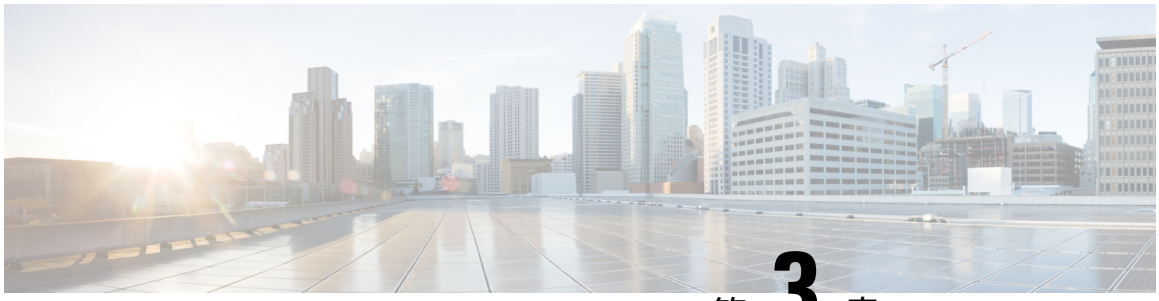
ステップ 2 （任意） 再度ログインするか、Web ブラウザを閉じます。



第 2 章

サーバ OS のインストール

この章は、次の項で構成されています。



第 3 章

シャーシの管理

- Intersight Infrastructure Service ライセンス （15 ページ）
- シャーシの概要の表示 （16 ページ）
- シャーシ インベントリ （21 ページ）

Intersight Infrastructure Service ライセンス

Intersight Infrastructure Service ライセンス

4.3(2.230207) リリース以降、Cisco UCS C シリーズ 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。

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。

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 **[アプリ（Apps）]** ドロップダウン リストから、**[ダッシュボード（Dashboard）]** を選択します。

ステップ 2 **[ダッシュボード（Dashboard）]** ページの **[サーバーの詳細（Server Detail）]** 領域で、次の情報を確認します。

表 *3 : [*サーバーの詳細（*Server Details***）*]* 領域**

名前	説明
製品名	サーバのモデル名。
UUID	サーバーに割り当てられている UUID。
PID	製品 ID。
シリアル番号（Serial Number）	サーバのシリアル番号。
BIOS バージョン	サーバで実行されている BIOS のバージョン。

ステップ 3 **[ダッシュボード（Dashboard）]** ページの **[CIMC 情報（CIMC Information）]** 領域で、次の情報を確認します。

表 *4 : [CIMC* 情報（*CIMC Information***）*]* 領域**

名前	説明
IP アドレス（IP Address）	Cisco IMC の IP アドレス。 クリックして、管理ネットワークの詳細を表示します。

名前	説明
MAC アドレス（MAC Address）	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。
ファームウェアバージョン（Firmware Version）	現在の Cisco IMC ファームウェアのバージョン。
ホスト名（Host Name）	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）。
現在の時刻(UTC)	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	タイムゾーンを選択できます。[タイムゾーンの選択（Select Timezone）] ポップアップ画面で、地図上で対応する場所にマウスのカーソルを合わせてクリックすることでタイムゾーンを選択するか、[タイムゾーン（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 4 **[ダッシュボード（Dashboard）]** ページの **[シャーシのステータス（Chasis Status）]** 領域で、次の情報を確認します。

***表 5 : [Chassis Status]* 領域**

名前	説明
サーバ全体のステータス	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。 • 良好 • Moderate Fault • Severe Fault
DIMM全体のステータス	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。 • 良好 • Fault • Severe Fault

名前	説明
電源モジュール	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。 • 良好 • Fault • Severe Fault
ストレージ全体のステータス	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。 • 良好 • Fault • Severe Fault
電源状態オン（**Power State On**）	現在の電源状態。
温度	温度ステータス。次のいずれかになります。 • 良好 • Fault • Severe Fault
Fans	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。 • 良好 • Fault • Severe Fault
[完了後ステータス（POST Completion Status）]	BIOS POST 完了 ステータス。
[ロケータ LED（Locator LED）]	ロケータ LED がオンかオフか。
冷却	現在の冷却モードを表示します。

ステップ 5 **[ダッシュボード（Dashboard）]** ページの **[プロセッサとメモリ（Processors & Memory）]** 領域で、次の情報を確認します。

表 *6 : [*プロセッサおよびメモリ（***Processors & Memory***）*]* エリア

名前	説明
CPU	サーバーの CPU 数。

名前	説明
コア	CPU のコア数。
Threads	CPU が同時に処理できる最大スレッド数。
有効なコア	コア合計のうち、有効になっているコア数。
CPU速度(MHz)	CPU の基本動作周波数（メガヘルツ単位）。
メモリ容量(MB)	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。
クロック速度(MHz)	メモリ（RAM）の動作周波数（メガヘルツ（MHz）単位で測定）。メモリとストレージの間の読み書き速度を示します。
有効なメモリ(MB)	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。
メモリレイアウト	メモリ DIMMの位置のグラフィカル表示。クリックすると、サーバー内のDIMMの位置がグラフィック表示されます。

ステップ 6 **[ダッシュボード（Dashboard）]** ページの **[ストレージ（Storage）]** 領域で、次の情報を確認します。

表 *7*: *[*ストレージ（*Storage*）*]* 領域

名前	説明
[Controllers]	使用可能な RAID 番号。
OSに使用可能なキャパシティ	インストールされている OS が使用可能なストレージ容量（ギガバイト単位）。
Physical Drives	サーバーで使用可能な ドライブの合計数。

名前	説明
仮想ドライブ	利用可能な仮想ドライブの合計数。

ステップ 7 **[ダッシュボード（Dashboard）]** ページの **[ネットワーキング（Networking）]** 領域で、次の情報を確認します。

表 *8* : *[*ネットワーク（***Networking***）*]* 領域

名前	説明
アダプタ	使用可能な Cisco UCS VIC アダプタの数。
DCEインターフェイス	利用可能な DCE インターフェイスの数。
vNICインターフェイス	使用可能な vNIC インターフェイスの数。
vHBAインターフェイス	使用可能な vHBA インターフェイスの数。

ステップ 8 **[ダッシュボード（Dashboard）]** ページの **[KVMコンソール（KVM Console）]** 領域を使用して、次の情報を表示できます。

表 *9* : *[KVM* コンソール（***KVM Console***）*]* 領域

名前	説明
[KVM の起動（Launch KVM）] アイコン	KVM セッション ウィンドウが、ブラウザの設定に応じて新しいタブまたはウィンドウとして開きます。
[リモート管理（Remote Management）] アイコン	[リモート管理（Remote Management）] ページを開きます。
[KVM Console（KVM コンソール）]インタラクティブ ウィンドウ	このインタラクティブ ウィンドウでは、新しいKVMセッションで実行できるすべてのアクションを実行できます。

ステップ 9 **[ダッシュボード（Dashboard）]** ページの **[クイック アクション（Quick Actions）]** 領域では、次のアクションを実行できます。

表 *10* : *[*クイックアクション（***Quick Actions***）*]* エリア

名前	説明
[RAID ボリュームの作成（Create a RAID Volume）] リンク	**[仮想ドライブの作成（Create Virtual Drive）**] ウィンドウを開きます。
[新規ユーザーの作成（Create a New User）] リンク	**[ローカル ユーザーの詳細（Local User Details）]** ウィンドウを開きます。

名前	説明
[ファームウェアのアップロード（Upload Firmware）] リンク	リモートまたはローカルから BMC または BIOS ファームウェアをアップロードできます。
[Cisco IMC 設定のインポート/エクスポート（Cisco IMC Configuration Import/Export）] エリア	**[Cisco IMC 設定のインポート/エクスポート（Cisco IMC Configuration Import/Export）]** ウィンドウを開きます。
[仮想 NIC インターフェイスの作成（Create a new Virtual NIC Interface）] リンク	vNIC を追加できます。
[仮想 HBA インターフェイスの作成（Create a new Virtual HBA Interface）] リンク	vHBA を追加できます。
[テクニカル サポート ログの生成（Generate Tech Support Logs）] リンク	**[テクニカルサポート データのエクスポート（Export Tech Support Data）]** ウィンドウを開きます。
[パフォーマンスモニター（Performance Monitor）] リンク	サーバー全体および電力の使用率を表示できます。

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 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。

ステップ 2

ステップ 3 **[インベントリ（Inventory）]** タブを選択します。

ステップ 4 [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。

表 *11* : 電源モジュール

名前	説明
[Device ID] フィールド	電源装置ユニットの ID。
[Status] フィールド	電源装置のステータス。
[Firmware Version]フィールド	電源装置のファームウェア バージョン。

名前	説明
[入力（Input）]フィールド	電源装置への入力（ワット単位）。
[出力（Output）] フィールド	電源装置からの最大出力（ワット単位）。
[入力電圧（Input Voltage）] フィールド	電源装置への入力電圧。
[出力ワット数（Output Wattage）]	電源装置の出力ワット数。
[Product ID] フィールド	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 **[アプリ（Apps）]** ドロップダウン リストから、**[ダッシュボード（Dashboard）]** を選択します。
ステップ 2 **[ネットワーキング（Networking）]** で **[アダプタ（Adapters）]** をクリックします。
ステップ 3 **[Cisco VICアダプタ（Cisco VIC Adapters）]** ウィンドウで、次の情報を確認します。

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。
[製品名（Product Name）] カラム	アダプタの製品名。
[**Firmware Version**] カラム	アダプタの現在のファームウェア バージョン。

ステップ 4 **[詳細を表示...（Show More...）]** をクリックすると、詳細を確認できます。

ストレージのプロパティの表示

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ダッシュボード（Dashboard）]** を選択します。

ステップ 2 **[ストレージ（Storage）]**で、**[コントローラ（Controllers）]**をクリックします。

ステップ 3 **[ストレージアダプタ（Storage Adapters）]** ウィンドウで、次の情報を確認します。

表 *12*：ストレージアダプタ

名前	説明
[PCI Slot] カラム	コントローラ ドライブが存在する PCI スロット。
[Name] カラム	コントローラの名前。
[**Firmware Version**] カラム	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。
[Serial Number] カラム	ストレージ コントローラのシリアル番号。

ステップ 4 **[詳細を表示...（Show More...）]** をクリックすると、詳細を確認できます。

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。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。

ステップ 2 **[インベントリ（Inventory）]** タブを選択します。

ステップ 3 ナビゲーション ペインから **[PCIe デバイス（PCIe Devices）]**を選択します。

ステップ 4 ドロップダウン リストから **[GPU]** を選択します。

ステップ 5 次のプロパティを表示することができます：

名前	説明
[ID] カラム	PCIe デバイス ID。
[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（Not Loaded）]：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。

名前	説明
[**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。
MAC アドレス（MAC Address）	Intel(R) ネットワーク コントローラの MAC アドレス （注） このフィールドは、Intel(R) ネットワーク コントローラでのみ表示されます。

（注）
Cisco IMC は、サーバーにインストールされているアダプタに応じて、サードパーティ製アダプタの情報を表示します。

以下に示すすべてのフィールドが表示されない場合があります。一部のアダプタでは、Cisco IMC に表示されているフィールドの値が表示されない場合があります。

表 *13* : サードパーティ製アダプタの情報

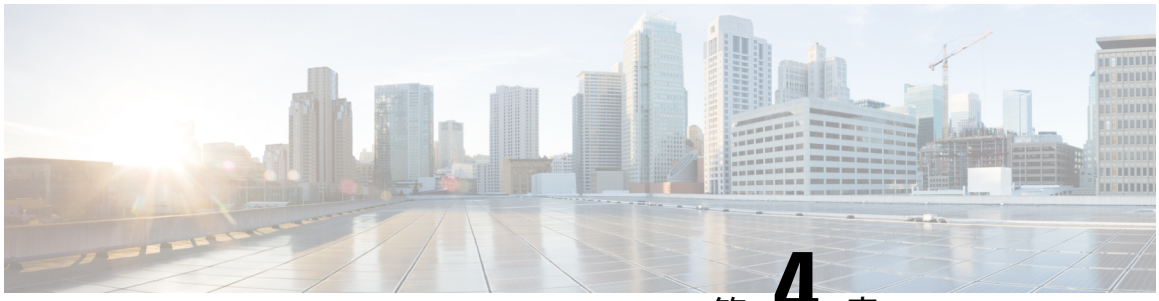
名前	説明
名前（Name）	PCIe アダプタの名前。
ベンダー	PCIe アダプタのベンダー。
シリアル番号	PCIe アダプタのシリアル番号。
製品番号	PCIe アダプタの部品番号。
製造元	PCIe アダプタの製造元。
Firmware Version	PCIe アダプタの現在のファームウェア バージョン

表 *14* : ポートの詳細

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

表 *15* : 温度の詳細

名前	説明
[ID] カラム	PCIe アダプタの ID。
温度(°C / °F)	PCIe アダプタの温度。



第 4 章

サーバーの管理

- サーバのブート順 （27 ページ）
- BIOS トークン （47 ページ）
- 電力ポリシーの設定 （212 ページ）
- ファン ポリシーの設定 （229 ページ）
- DIMMブロックリストの構成 （235 ページ）
- BIOS の設定 （237 ページ）
- BIOS プロファイル （239 ページ）
- セキュアブート証明書の管理 （243 ページ）
- 前面パネルの動的温度しきい値の設定 （248 ページ）
- 永続メモリ モジュール （248 ページ）

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。

[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。

設定されたブート順序を変更したり、以前に設定されたブート順序を復元したりするには、**[ブート順序の設定（Configure Boot Order）]** エリアの**[ブート デバイスの追加（Add Boot Device）]** > **[基本（Basic）]** オプショ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。

[実際のブート順序（Actual Boot Order）] セクションには、サーバ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序が表示されます。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。

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 **[アプリ（Apps）]** ドロップダウン リストから、**[コンピューティング（Compute）]** を選択します。

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

ステップ 3 **[BIOS]** タブで **[ブート順序の設定（Configure Boot Order）]** タブをクリックします。

ステップ 4 **[ブート順序（Boot Drive）]** 領域で、次の情報を確認します。

表 *16 :* プロパティ領域

名前	説明
[Running Version] フィールド	サーバで実行中の BIOS のバージョン。
[UEFI セキュア ブート（UEFI Secure Boot）] トグル ボタン	UEFI セキュア ブートを有効または無効にすることができます。 （注） 有効にした場合、設定済みブートはデフォルトで UEFI モードに設定されます。UEFI セキュア ブートが無効にされるまで、このオプションを編集できなくなります。 （注） RFD（Reset Factory Default）の場合は、UEFI セキュア ブートを再度有効にしてください。
Actual Boot Mode	BIOS を起動するブート モード。 このフィールドは BIOS によって設定される読み取り専用パラメータであり、ホストを再起動した場合にのみ更新されます。

名前	説明
Configured Boot Mode	BIOS でデバイスのブートを試行する際のブート モードを設定します。次のいずれかになります。 • **レガシー** • **UEFI** （注） UEFI セキュア ブートが有効にされている場合、ブート モードはデフォルトで UEFI に設定されます。UEFI セキュア ブート オプションが無効にされるまで、設定済みブート モードは変更できません。
Last Configured Boot Order Source	BIOS でブート順序を設定するために最後に使用された送信元。次のいずれかになります。 • **BIOS** • **CIMC** • **CIMCOneTimeBoot** • **不明**
[ワンタイム ブート デバイスの構成（Configure one time boot device）] ドロップダウン リスト	ドロップダウン リストから、1 回限り設定するブート デバイスを選択します。次回のサーバ ブートに限り、既存の拡張デバイスからブートするようにサーバを設定できます。サーバがそのデバイスからブートした後、以降のサーバ ブートでは既存の設定済みブート順序が使用されます。 （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。

[実際のブート順序（Actual Boot Order）] 領域

表 *17 : [*実際のブート順序（***Actual Boot Order***）*]* 領域

名前	説明
[Name] カラム	ブート デバイスの名前。
[Order] カラム	デバイスのブート順序。
[Type] カラム	ブート デバイスのタイプ。

[ブート順序の設定（Boot Order Configuration）] 領域

[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。

Basic

- **Basic**

Advanced

- **ローカル HDD**
- **[PXE ブート（PXE Boot）]**
- **[SAN ブート（SAN Boot）]**
- **[iSCSI ブート（iSCSI Boot）]**
- **USB**
- 仮想メディア
- **PCHStorage**
- **UEFISHELL**
- **NVMe**
- **[ローカル CDD（Local CDD）]**
- **HTTP ブート**

表 *18* : *[*ブート順序の設定（*Boot Order Configuration*）*]* 領域

名前	説明
[ブート デバイスの追加（**Add Boot Device**）**]** ボタン	次のオプションから選択できます。 • 基本ブート順序の設定 • ローカル HDD ブート デバイスの追加 • PXE ブート デバイスの追加 • SAN ブートデバイスの追加 • iSCSI ブート デバイスの追加 • USB 起動デバイスの追加 • 仮想メディア ブート デバイスの追加 • PCH ストレージ ブート デバイスの追加 • UEFI シェル ブート デバイスの追加 • NVMe ブート デバイスの追加 • ローカル CDD ブート デバイスの追加 • HTTP ブート デバイスの追加 • 組み込みストレージ ブート デバイスの追加
[**Enable/Disable**] ボタン	ブートデバイスをイネーブルまたはディセーブルにできます。 ブート デバイスがある行を選択し、**[**有効化/無効化（ **Enable/Disable** ）**]** をクリックします。
[削除（**Delete**）**]** ボタン	ブート デバイスを削除できます。 ブートデバイスがある行を選択し、**[**削除（**Delete**）**]** をクリックします。
[Name] カラム	ブート デバイスの名前。
[レベル（**Level**）**]** カラム	次のいずれかになります。 • 基本 • 高機能
[Type] カラム	ブート デバイスのタイプ。
[Order] カラム	このブート デバイスの順序。

名前	説明
[State] カラム	デバイスがイネーブルかまたはディセーブルかを表示します。

ステップ 5 **[再適用（Re-apply）]** 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 **[アプリ（Apps）]** ドロップダウン リストから、**[コンピューティング（Compute）]** を選択します。

ステップ 2 左側ペインの **[BIOS]** メニューをクリックします。

ステップ 3 **[BIOS]** メニューで **[ブート順序（Boot Order）]** を選択します。

ステップ 4 **[ブート順序（Boot Order）]** ペインで、**[ブート順序の設定（Boot Order Configuration）]** タブの **[ブート デバイスの追加（Add Boot Device）]** をクリックします。

ステップ 5 **[ブート デバイスの追加（Add Boot Device）]** ドロップダウンリストから、ブート順序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、**[ローカル HDD（Local HDD）]** をクリックし、次のパラメータを更新します。

表 *19 :* ローカル *HDD* ブート デバイスの追加

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。

名前	説明
[有効（Enabled）] トグルボタン	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。
UEFI ブート ローダー パラメータ (オプション)	
[ブートローダ名（Bootloader Name）] フィールド	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。
[ブートローダ パス（Bootloader Path）] フィールド	システムの起動に使用するブートローダのファイル パスを指定します。
[ブートローダの説明（Bootloader Description）] フィールド	ブートローダの簡単な説明。

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

表 *20 : PXE* ブート デバイスの追加

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。
[有効（Enabled）] トグルボタン	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）。

名前	説明
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。
[IP タイプ（IP Type）] ボタン	次のいずれかになります。 • なし • IPv4 • IPv6
[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（SAN Boot）]** をクリックし、次のパラメータを更新します。

表 *21 : SAN* ブートデバイスの追加

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。
[有効（Enabled）] トグルボタン	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。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。

名前	説明
UEFI ブート ローダー パラメータ (オプション)	
[ブートローダ名（Bootloader Name）] フィールド	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。
[ブートローダ パス（Bootloader Path）] フィールド	システムの起動に使用するブートローダのファイル パスを指定します。
[ブートローダの説明（Bootloader Description）] フィールド	ブートローダの簡単な説明。

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

表 *22 : iSCSI* ブート デバイスの追加

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。
[有効（Enabled）] トグルボタン	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。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。

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

表 *23 : USB* 起動デバイスの追加

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。
[有効（Enabled）] トグルボタン	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）。
[**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]**

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

表 *24 :* 仮想メディア ブート デバイスの追加

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。
[状態（State）] トグル ボタン	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）。

名前	説明
[**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]** • **[KVM Mapped HDD]** • **[KVM Mapped FDD]** • **[CIMC マップされた DVD（CIMC Mapped DVD）]** • **[CIMC マップされた HDD(CIMC Mapped HDD）]**

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

表 *25 : PCH* ストレージ ブート デバイスの追加

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。
[有効（Enabled）] トグルボタン	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。

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

表 *26 : UEFI* シェル ブート デバイスの追加

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。
[有効（Enabled）] トグルボタン	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）。

NVME ブート デバイスを追加するには、**[NVME]**を選択し、次のパラメータを更新します。

表 *27 : NVMe* ブート デバイスの追加

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。
[有効（Enabled）] トグルボタン	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）。

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

表 *28* : ローカル *CDD* ブート デバイスの追加

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。
[有効（Enabled）] トグルボタン	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）。

HTTP ブート デバイスを追加するには、**[HTTP ブート（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

表 *29* : *HTTP* ブート デバイスの追加

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
[有効（Enabled）] トグルボタン	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。 • [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。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。
[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。
[IP 構成タイプ（IP Config Type] ボタン	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）]**
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。

名前	説明
[IP タイプ（IP Type）] ボタン	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。

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

表 *30* : 組み込みストレージ ブート デバイスの追加

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。
[有効（Enabled）] トグルボタン	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）。
[**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。 • FlexMMCマッピングされたDVD • FlexMMCマッピングされたHDD

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 2025 • Windows Server 2022 • ESX 6.7 • ESX 6.5 • ESXi 7.0 • ESXi 8.0 • Linux 9.4 • Linux 9.5 • Ubuntu 24.04
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

コンポーネント	種類
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 **[ブート順序（Boot Order）]** タブの **[プロパティ（Properties）]** 領域で、 **[UEFI セキュア ブート（UEFI Secure Boot〜]** トグル ボタンを選択します。

（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 オプションが無効になるまで **[ブート モードの構成（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 2 [保存（Save）] 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 **[プロパティ（Properties）]** 領域で、**[UEFI セキュア ブート（UEFI Secure Boot）]** トグル ボタンをオフにします。

ステップ 2 [保存（Save）] 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 **[アプリ（Apps）]** ドロップダウン リストから、**[コンピューティング（Compute）]** を選択します。

ステップ 2 左側ペインの **[BIOS]** メニューをクリックします。

ステップ 3 **[BIOS]** タブで **[ブート順序（Boot Order）]** タブをクリックします。

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。

[ブート デバイスの設定（Boot Devices Configuration）] 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（Advanced）]**）が表示されます。この設定が変更されると、次回のサーバー 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（Basic）] 設定では、デバイス タイプのみを指定することができます。**[詳細（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。

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。

[実際のブート順序（Actual Boot Order）]セクションには、サーバ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序が表示されます。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 **[アプリ（Apps）]** ドロップダウン リストから、**[コンピューティング（Compute）]** を選択します。

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

ステップ 3 **[BIOS]** タブで **[ブート順序（Boot Order）]** タブをクリックします。

ステップ 4 **[プロパティ（Properties）]**領域の **[設定済みのワンタイム ブート デバイス（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、ユーザまたは管理者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 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。
ステップ 2 **[システム（System）]** メニューの **[全般（General）]** タブをクリックします。
ステップ 3 **[サーバーの詳細（Server Details）]** 領域で、**[アセット タグ（Asset Tag）]** フィールドを更新します。
ステップ 4 [保存（Save）] をクリックします。

BIOSトークン

Cisco UCS C220 M8 および C240 M8

[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、サーバーの構成によって異なります。

表 *31 : I/O*

名前	説明
[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。 • **[GEN4]**：リンク速度は第 4 世代まで到達可能です。 • **[GEN5]**：リンク速度は第 5 世代まで到達可能です。
[MLOM OptionROM] トグル ボタン	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。

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。 • **[GEN5]**：リンク速度は第 5 世代まで到達可能です。
[PCIe スロット オプション ROM（PCIe Slot Option ROM）]	
[PCIe Slot*n* OptionROM] トグル ボタン	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を決める機能を有効または無効にできます。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
[PCIe スロット（PCIe Slot）MSTOR RAID OptionROM] トグル ボタン	サーバーが PCIe MSTOR RAID にあるオプション ROM を使用できるかどうかを決める機能を有効または無効にできます。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。
[MRAID リンク速度（MRAID Link Speed）]	
[MRAID*n* リンク速度（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、装着されている MRAID 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。 • **[GEN4]**：最大 16GT/s までの速度が許可されます。 • **[GEN5]**：リンク速度は第 5 世代まで到達可能です。
MRAID OptionROM	
[MRAID OptionROM] トグル ボタン	このオプションでは、接続された MRAID 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）]**：MRAID PCIe アダプタのオプション ROM を実行しません。 • **[有効（Enabled）]**：MRAID PCIe アダプタのオプション ROM を実行します。

名前	説明
NVMEリンク速度	
[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。 • **[GEN5]**：リンク速度は第 5 世代まで到達可能です。

名前	説明
Rear 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 背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。 • **[GEN5]**：リンク速度は第 5 世代まで到達可能です。
NVME OptionROM	
[前面 NVME（Front NVME）]*n* OptionROM トグル ボタン	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
[背面 NVME（Rear NVME）]*n* [OptionROM] トグル ボタン	このオプションでは、背面 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
[VMD の有効化（VMD Enable）] トグル ボタン	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（Disabled）]**：この機能が無効になります。 デフォルト値：**無効**。 VMD を構成するには、『CPU の Intel® 仮想 RAID』を参照してください。 （注） VROC は、Cisco UCS C シリーズ M7 サーバーではサポートされていません。
[PCIe RAS サポート（PCIe RAS Support）] トグル ボタン	PCIe スロットで PCIe RAS サポートが使用可能な場合に、機能を有効または無効にすることができます。次のいずれかになります。 • **[無効（Disabled）]**：PCIe RAS はスロットで使用不可です。 • **[有効（Enabled）]**：PCIe RAS はスロットで使用可能です。

名前	説明
[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（Off Board）]**：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。オンボード VGA がディセーブルの場合、vKVM は機能しません。
[USB Port Rear] トグル ボタン	背面パネルの USB デバイスを有効または無効にできます。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。
[IPv6 PXE サポート（IPv6 PXE Support）] トグル ボタン	PXE の IPv6 サポートを有効または無効にできます。次のいずれかになります • **無効**：IPv6 PXE サポートは使用できません。 • **[有効（Enabled）]**：IPv6 PXE のサポートを常に利用できます。

名前	説明
[ネットワーク スタック（Network Stack）] トグル ボタン	IPv6 と IPv4 をモニターできます。次のいずれかになります • **無効**：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。 • **[有効（Enabled）]**：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	このオプションは、暗号化操作の外部セキュアソケットコントローラ（SSC）の使用を制御します。通常はトラステッド プラットフォーム モジュール（TPM）機能に関連します。 次のいずれかになります。 • **オフ（Off）** • **OP*n_Percent*** • **ハードウェア**
[IPV4 PXE サポート（IPV4 PXE Support）] トグル ボタン	PXE の IPv4 サポートを有効または無効にできます。次のいずれかになります • **無効**：IPv4 PXE サポートは使用できません。 • **[有効（Enabled）]**：IPv4 PXE のサポートを常に利用できます。

名前	説明
[IIO eDPC サポート（IIO eDPC Support）] ドロップダウン リスト	eDPC を使用すると、修正不可能なエラーの後にダウンストリーム リンクを無効にすることができるため、制御された堅牢な方法で回復することが可能になります。 次のいずれかになります。 • **[無効（Disabled）]**：eDPC サポートは無効です。 • **[致命的なエラーの場合（On Fatal Error）]**：eDPC は致命的なエラーにのみ有効です。 • **[致命的および非致命的なエラーの場合（On Fatal and Non-Fatal Errors）]**：eDPC は、致命的および非致命的なエラーの両方に対して有効です。
[IPv4 HTTP サポート（IPv4 HTTP Support）] トグル ボタン	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**：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。
[IPv6 HTTP サポート（IPv6 HTTP Support）] トグル ボタン	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**：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。
[Re-Size BAR Support] トグル ボタン	この機能を使用すると、システムは BAR のサイズを動的に変更できるため、メモリ リソースをより柔軟で効率的に使用できます。 • **[無効（Disabled）]**：BAR サイズ変更サポートを無効にします。 • **[有効（Enabled）]**：サイズ変更 BAR のサポートが有効になります。

名前	説明
[プリブート DMA 保護（PreBoot DMA Protection）] トグル ボタン	これを使用して、サーバーはプリブートフェーズ中の DMA 操作を制限または制御し、信頼できるデバイスのみがシステム メモリにアクセスできるようにすることができます。 • **[無効（Disabled）]**：BAR サイズ変更サポートを無効にします。 • **[有効（Enabled）]**：サイズ変更 BAR のサポートが有効になります。

[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、サーバーの構成によって異なります。

表 *32 : [*サーバ管理（***Server Management***）*]* タブの ***BIOS*** パラメータ

名前	説明
[FRB 2 タイマー（FRB 2 Timer）] トグル ボタン	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 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）] トグル ボタン	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。
[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
[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。
[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。

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。
[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。
[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。

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、サーバーの構成によって異なります。

表 *33 : [*メモリ（*Memory*）*]* タブの *BIOS* パラメータ

名前	説明
[NUMA] トグル ボタン	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。
[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。 • [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。

名前	説明
[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。
[BME DMA 緩和（BME DMA Mitigation）] トグル ボタン	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。

名前	説明
[パーシャル メモリ ミラー モード（Partial Memory Mirror Mode）] トグル ボタン	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。 • **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。
[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。
[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。
[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。 • **自動（Auto）**：システムの状態と要件に基づいて拡張メモリ テストを実行するかどうかを自動的に決定します。
[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）]**
[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）] トグル ボタン	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**
[MMIO ハイベース（MMIO High Base）] ドロップダウン リスト	MMIO ハイ ベースは、ハイ メモリ マップト I/O（MMIO）リージョンのベース アドレスを設定します。このリージョンは、4 GB のアドレス空間を超えるデバイス メモリと I/O リソースをマップするために使用され、システム メモリの割り当てとパフォーマンスを最適化します。 次のいずれかになります。 • **512G**：MMIO 高ベースを 512 ギガバイトに設定します。 • **1T**：MMIO 高ベースを 1 テラバイトに設定します。 • **[2T]**：MMIO 高ベースを 2 テラバイトに設定します。 • **[4T]**：MMIO 高ベースを 4 テラバイトに設定します。 • **[16T]**：MMIO 高ベースを 16 テラバイトに設定します。 • **[24T]**：MMIO 高ベースを 24 テラバイトに設定します。 • **[32T]**：MMIO 高ベースを 32 テラバイトに設定します。 • **40T**：MMIO 高ベースを 40 テラバイトに設定します。 • **56T**：MMIO 高ベースを 56 テラバイトに設定します。 • **Auto**：サーバーは動的に高いベース値を設定します。

名前	説明
[MMIO 高粒度サイズ（MMIO High Granularity Size）] ドロップダウン リスト	MMIO 高粒度サイズは、高メモリマップド I/O（MMIO）リージョンの粒度を設定し、4GB アドレス範囲を超える MMIO スペースを割り当てるためのサイズの増分を決定します。これは、メモリ割り当てとシステムパフォーマンスの最適化に役立ちます。 次のいずれかになります。 • **1G**：MMIO 高粒度サイズを 1 ギガバイトに設定します。 • **[4G]**：MMIO 高粒度サイズを 4 ギガバイトに設定します。 • **[16G]**：MMIO 高粒度サイズを 16 ギガバイトに設定します。 • **[32G]**：MMIO 高粒度サイズを 32 ギガバイトに設定します。 • **64G**：MMIO 高粒度サイズを 64 ギガバイトに設定します。 • **[256G]**：MMIO 高粒度サイズを 256 ギガバイトに設定します。 • **[1024G]**：MMIO 高粒度サイズを 1024 ギガバイトに設定します。 • **Auto**：サーバーは高粒度サイズを動的に設定します。
UEFIメモリマップの特殊な目的のメモリフラグ	この設定により、特定のオペレーティング システムで CXL カードに影響を与える UEFI メモリ マップの特別なノブの動作を決定します。 次のいずれかになります。 • **Disabled** • **有効化**

名前	説明
ACPI SRATの特殊な目的のメモリフラグ	この設定により、UEFIメモリ マップの特殊目的フラグが有効になっている場合に、ACPI SRAT 特殊目的メモリ フラグの設定を許可または禁止します。 次のいずれかになります。 • **Disabled** • **有効化**
ランタイム ポスト パッケージ修復	OSランタイム中に修正されたメモリ エラーのソフト ポスト パッケージ修復を有効にします。 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、サーバーの構成によって異なります。

表 *34 : [*電源/パフォーマンス（*Power/Performance*）*]* タブの *BIOS* パラメータ

名前	説明
[隣接キャッシュ行のプリフェッチ（Adjacent Cache Line Prefetcher）] トグル ボタン	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）] トグル ボタン	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）] トグル ボタン	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
[Virtual Numa] トグル ボタン	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。 • [カスタム（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ーの 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。

名前	説明
[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** • **4** • **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。 （注） このオプションは、Cisco UCS C220 M8 サーバーでは使用できません。 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。
[UPI Power Management] トグルボタン	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。

名前	説明
LatencyOptimizedMode_M5 トグルボタン	このオプションは、遅延の削減を優先するサーバーの BIOS 設定内のモードを示します。 • **[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、サーバーの構成によって異なります。

表 *35 : [*プロセッサ（*Processor*）*]* タブの *BIOS* パラメータ

名前	説明
[Intel Virtualization Technology] トグル ボタン	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。

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。 • **Auto** • [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。
[Processor C1E] トグルボタン	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
[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。
[Turbo Mode] トグルボタン	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。

名前	説明
[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。 • [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。 • **[最大効率（Max Efficient）]**：プロセッサのP-stateの比率が最小です。
[SpeedStep (Pstates)] トグルボタン	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] トグルボタン	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]] トグルボタン	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 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。

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。 • [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。 • [disabled][Disabled]：サブNUMAクラスタリングは発生しません。 • **[有効（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。 • **[PECI]**：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。
[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**：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（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）

名前	説明
[LLC プリフェッチ（LLC Prefetch）] トグル ボタン	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。
[エネルギー効率ターボ（Energy Efficient Turbo）] トグル ボタン	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。
[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。 • **[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。

名前	説明
[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
[Intel ダイナミック速度選択（Intel Dynamic Speed Select）] トグル ボタン	**[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。
[IOAT の構成（IOAT Configuration）] トグル ボタン	[IOAT の構成（IOAT Configuration）] は、メモリコピー操作をオフロードすることでデータ転送効率を向上させ、CPU オーバーヘッドを削減する、Intel I/O Acceleration Technology（IOAT）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）]**：この機能を無効にします。 • **[有効（Enabled）]**：この機能を有効にします。

名前	説明
[PRMRR サイズ（PRMRR Size）] ドロップダウン リスト	

名前	説明
	[PRMRRサイズ（PRMRR Size）] では、保護範囲メモリ領域レジスタ（PRMRR）のサイズを設定します。これは、システムでのセキュリティと分離を強化するために、保護されたメモリ領域を定義するために使用されます。次のいずれかになります。 • **[128MB]**：128 MB の保護メモリ領域を定義します。 • **[256MB]**：256 MB の保護されたメモリ領域を定義します。 • **512MB**：512 MB の保護メモリ領域を定義します。 • **1GB**：1 ギガバイトの保護メモリ領域を定義します。 • **2GB**：2 ギガバイトの保護メモリ領域を定義します。 • **4GB**：4 ギガバイトの保護メモリ領域を定義します。 • **8GB**：8 ギガバイトの保護メモリ領域を定義します。 • **16GB**：16 ギガバイトの保護メモリ領域を定義します。 • **32GB**：32 ギガバイトの保護メモリ領域を定義します。 • **64GB**：64 GB の保護されたメモリ領域を定義します。 • **128GB**：128 ギガバイトの保護メモリ領域を定義します。 • **256GB**：256 GB の保護されたメモリ領域を定義します。 • **512GB**：512 GB の保護メモリ領域を定義します。 • **[無効な設定（Invalid Config.）]**：保護されたメモリ領域の無効な設定を示します。 • **[自動（Auto）]**：システム要件に基づい

名前	説明
	て、保護メモリ領域のサイズを自動的に設定します。

[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、サーバーの構成によって異なります。

表 *36 : [*セキュリティ管理（*Security Management*）*]* タブの *BIOS* パラメータ

名前	説明
[信頼されたプラットフォーム モジュールの状態（**Trusted Platform Module State**）**]** トグル ボタン	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**）**]** トグル ボタン	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。

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。
[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。
[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。
[SHA384 PCR バンク（SHA384 PCR Bank）] ドロップダウン リスト	プラットフォーム構成レジスタ（PCR）は、TPM 内のメモリ位置です。複数の PCR をまとめて PCR バンクと呼びます。セキュア ハッシュ アルゴリズム 384 ビットまたは SHA-384PCR バンクでは、TPM セキュリティを有効または無効にすることができます。 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
[Intel Trusted Execution Technology のサポート（Intel Trusted Execution Technology Support）] トグル ボタン	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。
[TPM 最小物理プレゼンス（TPM Minimal Physical Presence）] トグル ボタン	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。
[全メモリ暗号化（Total Memory Encryption、TME）] トグル ボタン	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。
[パワー オン時パスワード] トグル ボタン	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
[ソフトウェア ガード拡張（SW Guard Extensions、SGX）] トグル ボタン	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。
[マルチキー全メモリ暗号化（Multikey Total Memory Encryption、MK-TME）] トグル ボタン	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。
[SGX パッケージ情報インバンドアクセス（SGX Pkg info In-Band Access）] トグル ボタン	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 初期設定へのリセット（SGX Factory Reset）] トグル ボタン	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。

名前	説明
[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。 • **[SGX 所有者 EPOCH 無効化（SGX Owner EPOCH deactivated）]**：現在の入力タイプを変更します。 • **[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。
[SGX QoS] トグル ボタン	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 自動 MP 登録エージェント（SGX Auto MP Registration Agent）] トグル ボタン	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。

名前	説明
[SGX Write Enable] トグル ボタン	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。
[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 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
[DMA 制御オプトイン フラグ（DMA Control Opt-In Flag）] トグル ボタン	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。
[CPU PA を 46 ビットに制限（LIMIT CPU PA to 46 Bits）] トグル ボタン	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。

名前	説明
[TDX Secure Arbitration Mode（SEAM）ローダ：（TDX Secure Arbitration Mode (SEAM) Loader:）] トグル ボタン	セキュアな仮想環境での Intel® Trusted Domain Extensions（TDX）を使用できるようにするには、これを有効にします。 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。
[信頼ドメイン エクステンション（Trust Domain Extension（TDX））] トグル ボタン	信頼ドメインと呼ばれる分離された実行環境を作成することで、仮想環境のセキュリティを強化できます。この環境では、ハイパーバイザなどの他のソフトウェアから機密データやコードを保護します。 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。

Cisco UCS C225 M8

[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、サーバーの構成によって異なります。

表 *37 : [I/O]* タブの *BIOS* パラメータ

名前	説明
[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。 • **[GEN4]** : リンク速度は第 4 世代まで到達可能です。 • **[GEN5]** : リンク速度は第 5 世代まで到達可能です。
[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。

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。 • **[GEN5]**：リンク速度は第 5 世代まで到達可能です。

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。 • **[GEN5]**：リンク速度は第 5 世代まで到達可能です。
[PCI スロット（PCI Slot）] *n* [オプション ROM（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。

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。 • **[GEN5]**：リンク速度は第 5 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
[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。 • **[GEN5]**：リンク速度は第 5 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
[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 VGA が無効（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。オンボード VGA が無効の場合、vKVM は機能しません。
[IPv4 PXE サポート（IPv4 PXE Support）] トグル ボタン	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。
[IPv6 PXE サポート（IPv6 PXE Support）] トグル ボタン	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。

名前	説明
[SR-IOV サポート（SR-IOV Support）] トグル ボタン	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。
[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。
[Re-Size BAR Support] トグル ボタン	この機能を使用すると、システムは BAR のサイズを動的に変更できるため、メモリ リソースをより柔軟で効率的に使用できます。 • **[無効（Disabled）]**：BAR サイズ変更サポートを無効にします。 • **[有効（Enabled）]**：サイズ変更 BAR のサポートが有効になります。
[IPv4 HTTP サポート （IPv4 HTTP Support）] トグル ボタン	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。 • **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
[IPv6 HTTP サポート（IPv6 HTTP Support）] トグル ボタン	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。
[IIO eDPC サポート（IIO eDPC Support）] ドロップダウン リスト	eDPC を使用すると、修正不可能なエラーの後にダウンストリーム リンクを無効にすることができるため、制御された堅牢な方法で回復することが可能になります。 次のいずれかになります。 • 無効：eDPC サポートは無効です。 • 致命的および非致命的なエラー：eDPC は、致命的および非致命的なエラーの両方に対して有効です。
[PCIe 10 ビット タグ サポート（PCIe Ten Bit Tag Support）] フィールド	サポートされているデバイスの PCIe 10 ビット タグを有効にします。次のいずれかになります。 • **[無効（Disabled）]**：PCIe 10 ビット タグ サポートは BIOS では無効です。 • **[有効（Enabled）]**：PCIe 10 ビット タグ サポートは BIOS では有効です。
[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。

表 *38 : [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。

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
[MRAID1 リンク速度（MRAID1 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。
MRAID2 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
[MRAID2 リンク速度（MRAID2 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。
[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。

名前	説明
[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。
[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。

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。 • **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。
[IIO eDPC サポート（IIO eDPC Support）] ドロップダウン リスト	eDPC を使用すると、修正不可能なエラーの後にダウンストリーム リンクを無効にすることができるため、制御された堅牢な方法で回復することが可能になります。 次のいずれかになります。 • 無効：eDPC サポートは無効です。 • 致命的および非致命的なエラー：eDPC は、致命的および非致命的なエラーの両方に対して有効です。
[PCIe 10 ビット タグ サポート（PCIe Ten Bit Tag Support）] フィールド	サポートされているデバイスの PCIe 10 ビット タグを有効にします。次のいずれかになります。 • **[無効（Disabled）]**：PCIe 10 ビット タグ サポートは BIOS では無効です。 • **[有効（Enabled）]**：PCIe 10 ビット タグ サポートは BIOS では有効です。

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、サーバーの構成によって異なります。

表 *39* : サーバー管理での *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。
[FRB 2 タイマー（FRB 2 Timer）] トグル ボタン	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 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。 • [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 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
[OSウォッチドッグタイマー（OS Watchdog Timer）] トグル ボタン	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。
[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。

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。
[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
[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。 • [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。
[CDN 制御（CDN Control）] トグル ボタン	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。
[PCIe スロット CDN 制御（PCIe Slots CDN Control）] トグルボタン	（注） このオプションは、Cisco UCS C225 および C245 M8 サーバーで使用できます。 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。

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。

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、サーバーの構成によって異なります。

表 *40*：*[*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
[4G 復号以上（Above 4G Decoding）] トグル ボタン	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。
[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。

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。
[バンク グループ スワップ（Bank Group Swap）]	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。
[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
[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。
[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。
[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。

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。
[カバーされる SNP メモリ サイズ（0 ～ 1048576 MB）（SNP Memory Size to Cover in MB（0 ～ 1048576 MB））] フィールド	SNP メモリ サイズを設定できます。 値を範囲（0 ～ 1048576 MB）で入力します。
[BME DMA 緩和（BME DMA Mitigation）] トグル ボタン	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。
[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。

名前	説明
[ランタイム ポスト パッケージ修復（Runtime Post Package Repair）] トグル ボタン	これは、実行時にプロセッサのパッケージを修復するシステムの機能に関連する特定の構成の設定です。 • **[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。
[バースト リフレッシュおよび遅延リフレッシュ（Burst and Postponed Refresh）] トグル ボタン	このオプションは、メモリ更新操作に関連し、DRAM（Dynamic Random Access Memory）のデータ整合性を維持するために必要なメモリ更新サイクルをシステムが処理する方法に影響します。 • **[無効（Disabled）]**：プロセッサはこの機能を使用しません。 • **[有効（Enabled）]**：プロセッサはこの機能を使用します。
[DRAM スクラブ時間（DRAM Scrub Time）] フィールド	値を選択して、メモリ全体をスクラブする時間を示します。次のいずれかになります。 • **[自動（Auto）]**：機能を自動モードに設定します。 • **[無効 (Disabled)]**：サポートは無効になっています。 • **1時間** • **4時間** • **8時間** • **16 時間** • **24 時間** • **48時間**

名前	説明
[SEV-ES ASID スペース制限（SEV-ES ASID Space Limit）]	SEV-ES ASID Space Limit BIOS 設定は、AMD® SEV-ES の ASID の数を決定し、VM メモリの暗号化と分離に影響します。調整することで、セキュリティのニーズとシステムリソースのバランスが取れます。 1 ～ 1007 の整数を入力します。
[メモリ インターリーブ（Memory interleaving）] フィールド	メモリ インターリーブを無効にできます。ソケットあたりのNUMA ノードは、この設定に関係なく適用されることに注意してください。次のいずれかになります。 • **[自動（Auto）]**：機能を自動モードに設定します。 • [Disabled]：サポートはディセーブルになっています。
[メモリのリフレッシュ レート（Memory Refresh Rate）] フィールド	メモリ コントローラのリフレッシュ レートを制御し、メモリ構成とワークロードに応じて、メモリのパフォーマンスと電力に影響を及ぼせるようにします。次のいずれかになります。 • **1x更新** • **2x更新**
[拡張メモリ テスト（Enhanced Memory Test）] ドロップダウンリスト	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。 • **[自動（Auto）]**：機能を自動モードに設定します。 • [Disabled]：サポートはディセーブルになっています。 • **[Enabled]**：サポートは無効になっています。

[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、サーバーの構成によって異なります。

表 *41 : [*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。
[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。

名前	説明
[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。
[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。

名前	説明
[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。
[電力プロファイル選択 F19h（Power Profile Selection F19h）] ドロップダウン リスト	電力プロファイル選択 F19h BIOS 設定では、AMD® ファミリ 19h プロセッサの特定のパフォーマンスまたはエネルギー効率の目標に合わせて調整された、事前定義された電源管理プロファイルを選択できます。この設定は、選択したプロファイルに基づいて CPU の電力消費とパフォーマンス特性を最適化します。 次のいずれかになります。 • **[高パフォーマンス モード（High Performance Mode）]**：高パフォーマンス モードが有効になります。 • **[効率モード（Efficiency Mode）]**：効率モードが有効になります。 • **[最大 IO パフォーマンス モード（Maximum IO Performance Mode）]**：最大 IO パフォーマンス モードが有効になります。 • **[バランス メモリ パフォーマンス モード（Balanced Memory Performance Mode）]**：バランス メモリ パフォーマンス モードが有効になります。

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 • サーバーに存在する DIMM モジュールサイズは、64GB 未満である必要がある • 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。

[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、サーバーの構成によって異なります。

表 *42 : [*セキュリティ（*Security*）*]* 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。
[セキュリティ デバイスのサポート（**Security Device Support**）**]** トグル ボタン	このオプションを使用すると、システムのセキュリティ 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。 • **[**無効（**Disabled**）**]**：このオプションは無効です。 • **[**有効（**Enabled**）**]**：サーバが無効です。
[信頼されたプラットフォーム モジュールの状態（**Trusted Platform Module State**）**]** トグル ボタン	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**）**]** トグル ボタン	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。

名前	説明
[SHA256 PCR バンク] トグル ボタン	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。
[SHA384 PCR バンク（SHA-384 PCR Finance）] トグルボタン	SHA384 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。
[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。

[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、サーバーの構成によって異なります。

表 *43* : *[*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 モード（**SVM Mode**）**]** トグル ボタン	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
[CPU ダウンコア制御 F19 M10h-1Fh（CPU Downcore control F19 M10h-1Fh）] ドロップダウン リスト	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
[ダウンコア制御（Downcore control）] ドロップダウン リスト	AMDプロセッサがコアを無効にすることを許可します。つまり、有効にするコア数を選択できます。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。 • [EIGHT（4+4）（EIGHT (4+4)）]：1 つの CPU コンプレックスで 8 つのコアが有効になります。 • [TEN（5+5）]：片方の CPU コンプレックスのみで 10 個のコアを有効にします。 • [TWELVE（6+6）]：片方の CPU コンプレックスのみで 12 個のコアを有効にします。 • [FOURTEEN (7+7)]：1 つの CPU コンプレックスで 14 個のコアを有効にします。
[固定 SOC P ステート SP5 F19h（0 -2 P ステート）（Fixed SOC P-State SP5 F19h（0 -2 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）

名前	説明
[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
[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。
[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。

名前	説明
[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。
[ローカル APIC モード（Local APIC Mode）] ドロップダウンリスト	これにより、使用するAPICモードを選択します。 • **[自動（Auto）]**：自動モードに設定します。 • **[互換性（Compatibility）]**：互換性モードに設定します。 • **[XAPIC]**：XAPIC モードに設定します。 • **[X2APIC]**：X2APICモードに設定します。

名前	説明
4 リンク xGMI 最大速度	この設定では、xGMI（チップ間グローバル メモリ インターコネクト）リンクに使用されるレーンの数を手動で指定できます。これは、CPU 間のデータ転送の帯域幅とパフォーマンスに影響を与える可能性があります。この設定の調整は、 の障害対応、パフォーマンスの調整、または特定のワークロードやシステム構成との互換性を確保するために使用できます。 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。 • **20Gbps**：20Gbps に設定します。 • **25Gbps**：25Gbps に設定します。 • **32Gbps**：32Gbps に設定します。
[DF Pstate 周波数オプティマイザ（DF PState Frequency Optimizer）]	DF Pstate 周波数オプティマイザを有効または無効にします。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。
AVX512	AVX-512 BIOS 設定は、AVX-512 命令セット拡張の使用を有効または無効にします。これは、特定の Intel® プロセッサで使用される高度なベクトル拡張であり、重い計算タスクのパフォーマンスを向上させます。この設定を調整すると、一部のソフトウェアとの互換性と安定性に影響を与える可能性があります。CPU の消費電力と発熱量に影響します。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。

名前	説明
パワー ダウンの有効化	この設定は、システムがアイドル状態のとき、または使用率が低いときにメモリ（RAM）を低電力状態にするかどうかを制御します。通常、この設定を有効にすると、RAMの電力消費が少なくなり、エネルギーが節約され、発熱量が減少する可能性がありますが、無効にすると、RAMの電力が完全に維持され、ウェイクアップ時間が短縮される可能性がありますが、電力消費は高くなります。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。
xGMI 強制リンク幅	この設定では、xGMI（チップ間グローバルメモリ インターコネクト）リンクに使用されるレーンの数を手動で指定できます。これは、CPU 間のデータ転送の帯域幅とパフォーマンスに影響を与える可能性があります。この設定の調整は、 の障害対応、パフォーマンスの調整、または特定のワークロードやシステム構成との互換性を確保するために使用できます。 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。 • **[0]**：0 に設定します。 • **[1]**：1 に設定します。 • **[2]**：2 に設定します。

Cisco UCS C245 M8

[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、サーバーの構成によって異なります。

表 *44 : [I/O]* タブの *BIOS* パラメータ

名前	説明
[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。

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
[MRAID1 リンク速度（MRAID1 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。
MRAID2 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
[MRAID2 リンク速度（MRAID2 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。
[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。

名前	説明
[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。
[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。

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。 • **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。
[PCIe 10 ビット タグ サポート（PCIe Ten Bit Tag Support）] フィールド	サポートされているデバイスの PCIe 10 ビット タグを有効にします。次のいずれかになります。 • **[無効（Disabled）]**：PCIe 10 ビット タグ サポートは BIOS では無効です。 • **[有効（Enabled）]**：PCIe 10 ビット タグ サポートは BIOS では有効です。
[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。

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、サーバーの構成によって異なります。

表 *45 : [*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。
[4G 復号以上（**Above 4G Decoding**）] トグル ボタン	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。
[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。

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。
[バンク グループ スワップ（Bank Group Swap）]	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。
[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
[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。
[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。
[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。

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。
[カバーされる SNP メモリ サイズ（0 ～ 1048576 MB）（SNP Memory Size to Cover in MB（0 ～ 1048576 MB））] フィールド	SNP メモリ サイズを設定できます。 値を範囲（0 ～ 1048576 MB）で入力します。
[BME DMA 緩和（BME DMA Mitigation）] トグル ボタン	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。
[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。

名前	説明
[ランタイム ポスト パッケージ修復（Runtime Post Package Repair）] トグル ボタン	これは、実行時にプロセッサのパッケージを修復するシステムの機能に関連する特定の構成の設定です。 • **[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。
[バースト リフレッシュおよび遅延リフレッシュ（Burst and Postponed Refresh）] トグル ボタン	このオプションは、メモリ更新操作に関連し、DRAM（Dynamic Random Access Memory）のデータ整合性を維持するために必要なメモリ更新サイクルをシステムが処理する方法に影響します。 • **[無効（Disabled）]**：プロセッサはこの機能を使用しません。 • **[有効（Enabled）]**：プロセッサはこの機能を使用します。
[DRAM スクラブ時間（DRAM Scrub Time）] フィールド	値を選択して、メモリ全体をスクラブする時間を示します。次のいずれかになります。 • **[自動（Auto）]**：機能を自動モードに設定します。 • **[無効 (Disabled)]**：サポートは無効になっています。 • **1時間** • **4時間** • **8時間** • **16 時間** • **24 時間** • **48時間**

名前	説明
[SEV-ES ASID スペース制限（SEV-ES ASID Space Limit）]	SEV-ES ASID Space Limit BIOS 設定は、AMD® SEV-ES の ASID の数を決定し、VM メモリの暗号化と分離に影響します。調整することで、セキュリティのニーズとシステムリソースのバランスが取れます。 1 ～ 1007 の整数を入力します。
[メモリ インターリーブ（Memory interleaving）] フィールド	メモリ インターリーブを無効にできます。ソケットあたりのNUMA ノードは、この設定に関係なく適用されることに注意してください。次のいずれかになります。 • **[自動（Auto）]**：機能を自動モードに設定します。 • [Disabled]：サポートはディセーブルになっています。
[メモリのリフレッシュ レート（Memory Refresh Rate）] フィールド	メモリ コントローラのリフレッシュ レートを制御し、メモリ構成とワークロードに応じて、メモリのパフォーマンスと電力に影響を及ぼせるようにします。次のいずれかになります。 • **1x更新** • **2x更新**
[拡張メモリ テスト（Enhanced Memory Test）] ドロップダウンリスト	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。 • **[自動（Auto）]**：機能を自動モードに設定します。 • [Disabled]：サポートはディセーブルになっています。 • **[Enabled]**：サポートは無効になっています。

[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、サーバーの構成によって異なります。

表 *46 : [*電源/パフォーマンス（*Power/Performance*）*]* タブの *BIOS* パラメータ

名前	説明
[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。
[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。

名前	説明
[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。
[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。

名前	説明
[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。
[電力プロファイル選択 F19h（Power Profile Selection F19h）] ドロップダウン リスト	電力プロファイル選択 F19h BIOS 設定では、AMD® ファミリ 19h プロセッサの特定のパフォーマンスまたはエネルギー効率の目標に合わせて調整された、事前定義された電源管理プロファイルを選択できます。 この設定は、選択したプロファイルに基づいて CPU の電力消費とパフォーマンス特性を最適化します。 次のいずれかになります。 • **[高パフォーマンス モード（High Performance Mode）]**：高パフォーマンス モードが有効になります。 • **[効率モード（Efficiency Mode）]**：効率モードが有効になります。 • **[最大 IO パフォーマンス モード（Maximum IO Performance Mode）]**：最大 IO パフォーマンス モードが有効になります。 • **[バランス メモリ パフォーマンス モード（Balanced Memory Performance Mode）]**：バランス メモリ パフォーマンス モードが有効になります。

[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、サーバーの構成によって異なります。

表 *47 : [*プロセッサ（*Processor*）*]* タブの *BIOS* パラメータ

名前	説明
[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（Downcore control）] ドロップダウン リスト	AMDプロセッサがコアを無効にすることを許可します。つまり、有効にするコア数を選択できます。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。 • [EIGHT（4+4）（EIGHT (4+4)）]：1 つの CPU コンプレックスで 8 つのコアが有効になります。 • [TEN（5+5）]：片方の CPU コンプレックスのみで 10 個のコアを有効にします。 • [TWELVE（6+6）]：片方の CPU コンプレックスのみで 12 個のコアを有効にします。 • [FOURTEEN (7+7)]：1 つの CPU コンプレックスで 14 個のコアを有効にします。

名前	説明
[CPU ダウンコア制御 F19 M10h-1Fh（CPU Downcore control F19 M10h-1Fh）] ドロップダウン リスト	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。
[固定 SOC P ステート SP5 F19h（Fixed SOC P-State SP5 F19h）] 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）

名前	説明
[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
[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。

名前	説明
[ローカル APIC モード（Local APIC Mode）] ドロップダウンリスト	これにより、使用する APIC モードを選択します。 • **[自動（Auto）]**：自動モードに設定します。 • **[互換性（Compatibility）]**：互換性モードに設定します。 • **[XAPIC]**：XAPIC モードに設定します。 • **[X2APIC]**：X2APIC モードに設定します。
[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。
4 リンク xGMI 最大速度	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。 • **[自動（Auto）]**：自動モードに設定します。 • **20Gbps**：20Gbps に設定します。 • **25Gbps**：25Gbps に設定します。 • **32Gbps**：32Gbps に設定します。

名前	説明
AVX512	AVX512 BIOS 設定は、AVX512 命令セット拡張の使用を有効または無効にします。これは、特定の Intel® プロセッサで使用される高度なベクトル拡張であり、重い計算タスクのパフォーマンスを向上させます。 この設定を調整すると、一部のソフトウェアとの互換性と安定性に影響を与え、CPU の電力消費と発熱量に影響を与える可能性があります。 AVX512 を有効または無効化にします。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 Pstate 周波数オプティマイザ（DF PState Frequency Optimizer）]	DF Pstate 周波数オプティマイザを有効または無効にします。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。

名前	説明
xGMI 強制リンク幅	この設定では、xGMI（チップ間グローバル メモリ インターコネクト）リンクに使用されるレーンの数を手動で指定できます。これは、CPU 間のデータ転送の帯域幅とパフォーマンスに影響を与える可能性があります。この設定の調整は、 の障害対応、パフォーマンスの調整、または特定のワークロードやシステム構成との互換性を確保するために使用できます。 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。 • **[0]**：0 に設定します。 • **[1]**：1 に設定します。 • **[2]**：2 に設定します。
パワー ダウンの有効化	この設定は、システムがアイドル状態のとき、または使用率が低いときにメモリ（RAM）を低電力状態にするかどうかを制御します。 通常、この設定を有効にすると、RAM の電力消費が少なくなり、エネルギーが節約され、発熱量が減少する可能性がありますが、無効にすると、RAM の電力が完全に維持され、ウェイクアップ時間が短縮される可能性がありますが、電力消費は高くなります。次のいずれかになります。 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。

[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、サーバーの構成によって異なります。

表 *48 : [*セキュリティ（*Security*）*]* タブの *BIOS* パラメータ

名前	説明
セキュリティデバイスのサポート	このオプションを使用すると、システムのセキュリティ 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。 • **[無効（Disabled）]**：このオプションは無効です。 • **[有効（Enabled）]**：サーバが無効です。
[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。

名前	説明
[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。
[SHA384 PCR バンク（SHA384 PCR Bank）] ドロップダウン リスト	プラットフォーム構成レジスタ（PCR）は、TPM 内のメモリ位置です。複数の PCR をまとめて PCR バンクと呼びます。セキュア ハッシュ アルゴリズム 384 ビットまたは SHA-384PCR バンクでは、TPM セキュリティを有効または無効にすることができます。 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。
[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。

[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、サーバーの構成によって異なります。

表 *49 : [*サーバ管理（***Server Management***）*]* タブの ***BIOS*** パラメータ

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。 • [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。

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 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。
[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。

Cisco UCS C220 および C240 M7

[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、サーバーの構成によって異なります。

表 *50 : [I/O]* タブの *BIOS* パラメータ

名前	説明
[MLOM OptionROM] トグル ボタン	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。

名前	説明
[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。 • **[GEN4]**：最大 16GT/s までの速度が許可されます。 • **[GEN 5]**：最大 32 GT/s までの速度が許可されます。
[PCIe スロット（PCIe Slot）*n* OptionROM] トグル ボタン	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。

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。 • **[GEN5]**：リンク速度は第 5 世代まで到達可能です。
MRAID OptionROM ドロップダウン リスト	このオプションでは、接続された MRAID 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）]**：MRAID PCIe アダプタのオプション ROM を実行しません。 • **[有効（Enabled）]**：MRAID PCIe アダプタのオプション ROM を実行します。

名前	説明
[MRAID リンク速度（MRAID 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、装着されている MRAID 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。 • **[GEN4]**：最大 16GT/s までの速度が許可されます。 • **[GEN 5]**：最大 32 GT/s までの速度が許可されます。
[前面 NVME-（Front NVME-）]*n* OptionROM トグル ボタン	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。 • **[GEN5]**：リンク速度は第 5 世代まで到達可能です。
[Intel VTD コヒーレンシのサポート（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。

名前	説明
[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。 • [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。
[PCIe RAS サポート（PCIe RAS Support）] ドロップダウン リスト	PCIe RAS サポートが PCIe スロットで使用可能かどうか。次のいずれかになります。 • **[無効（Disabled）]**：PCIe RAS はスロットで使用不可です。 • **[有効（Enabled）]**：PCIe RAS はスロットで使用可能です。
[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。

名前	説明
[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。 • [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。
[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。
[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。

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。
[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。 • **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。
[IIO eDPC サポート（IIO eDPC Support）] ドロップダウン リスト	eDPC を使用すると、修正不可能なエラーの後にダウンストリーム リンクを無効にすることができるため、制御された堅牢な方法で回復することが可能になります。 次のいずれかになります。 • 無効：eDPC サポートは無効です。 • 致命的なエラーの場合：eDPC は致命的なエラーにのみ有効です。 • 致命的および非致命的なエラー：eDPC は、致命的および非致命的なエラーの両方に対して有効です。
[サイズ変更 BAR サポート（Re-size BAR Support）] ドロップダウン リスト	サイズ変更 BAR サポートにより、システムは PCIe デバイスのベースアドレスレジスタ（BAR）のサイズを動的に調整して、メモリの割り当てとパフォーマンスを最適化できます。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。

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。

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、サーバーの構成によって異なります。

表 *51* : *[*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。 • [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。
[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。

名前	説明
[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。
[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。

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。
[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。

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。
[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) • クアドラント（4 クラスタ）
[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。 • **自動（Auto）**：システムの状態と要件に基づいて拡張メモリ テストを実行するかどうかを自動的に決定します。

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**
[MMIO ハイベース（MMIO High Base）] ドロップダウン リスト	MMIO ハイ ベースは、ハイ メモリ マップト I/O（MMIO）リージョンのベースアドレスを設定します。このリージョンは、4 GB のアドレス空間を超えるデバイス メモリと I/O リソースをマップするために使用され、システム メモリの割り当てとパフォーマンスを最適化します。 次のいずれかになります。 • **512G**：MMIO 高ベースを 512 ギガバイトに設定します。 • **1T**：MMIO 高ベースを 1 テラバイトに設定します。 • **[2T]**：MMIO 高ベースを 2 テラバイトに設定します。 • **[4T]**：MMIO 高ベースを 4 テラバイトに設定します。 • **[16T]**：MMIO 高ベースを 16 テラバイトに設定します。 • **[24T]**：MMIO 高ベースを 24 テラバイトに設定します。 • **[32T]**：MMIO 高ベースを 32 テラバイトに設定します。 • **40T**：MMIO 高ベースを 40 テラバイトに設定します。 • **56T**：MMIO 高ベースを 56 テラバイトに設定します。

名前	説明
[MMIO 高粒度サイズ（MMIO High Granularity Size）] ドロップダウン リスト	MMIO 高粒度サイズは、高メモリマップドI/O（MMIO）リージョンの粒度を設定し、4GB アドレス範囲を超える MMIO スペースを割り当てるためのサイズの増分を決定します。これは、メモリ割り当てとシステムパフォーマンスの最適化に役立ちます。 次のいずれかになります。 • **1G**：MMIO 高粒度サイズを 1 ギガバイトに設定します。 • **[4G]**：MMIO 高粒度サイズを 4 ギガバイトに設定します。 • **[16G]**：MMIO 高粒度サイズを 16 ギガバイトに設定します。 • **64G**：MMIO 高粒度サイズを 64 ギガバイトに設定します。 • **[256G]**：MMIO 高粒度サイズを 256 ギガバイトに設定します。 • **[1024G]**：MMIO 高粒度サイズを 1024 ギガバイトに設定します。

[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、サーバーの構成によって異なります。

表 *52 : [*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。

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。 • [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。
[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。

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。
[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。

名前	説明
[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。 • [カスタム（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ーの 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。 • **[自動（Auto）]** : 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
[UPI Power Management] トグルボタン	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。
[最適化された電力モード（Optimized Power Mode）] ドロップダウン リスト	最適化された電力モードは、30ー40% の CPU 使用率で実行される特定のワークロードのパフォーマンスへの影響を最小限に抑えながら、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。 • **[自動（Auto）]** : 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。

[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、サーバーの構成によって異なります。

表 *53* : *[*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）] トグルボタン	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。
[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。

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。
[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
[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。
[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。

名前	説明
[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。 • [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。 • **[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。
[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
[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。
[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 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。

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。 • **[SNC2]**：プロセッサは2つのNUMAノードに分割され、それぞれに独自のメモリアクセス パスがあります。これにより、メモリ遅延の短縮とメモリ帯域幅の増加のメリットがあるワークロードのメモリアクセス時間を改善できます。 • **[SNC4]**：プロセッサは4つのNUMAノードに分割されます。これにより、ワークロードのメモリアクセスパフォーマンスを向上させることができ、メモリの遅延が非常に短く、メモリの帯域幅が高いという点からメリットが得られるようになります。 • [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。
[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。 • **[PECI]**：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**：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。 • **[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。

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）

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。 • [無効（Disabled）]：CPU 自律 C-state が無効になります。 • [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。 • **[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
[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。

名前	説明
[X2APIC オプトアウト フラグ（X2APIC Opt Out Flag）] ドロップダウン リスト	拡張x2APICモードを無効にして、割り込み管理のためにレガシーAPICモードに戻すことができます。次のいずれかになります。 • **[無効（Disabled）]**：この機能を無効にします。 • **[有効（Enabled）]**：この機能を有効にします。
[IOAT の構成（IOAT Configuration）] ドロップダウン リスト	[IOAT の構成（IOAT Configuration）] は、メモリコピー操作をオフロードすることでデータ転送効率を向上させ、CPU オーバーヘッドを削減する、Intel I/O Acceleration Technology（IOAT）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）]**：この機能を無効にします。 • **[有効（Enabled）]**：この機能を有効にします。

名前	説明
[PRMRR サイズ（PRMRR Size）] ドロップダウン リスト	

名前	説明
	[PRMRRサイズ（PRMRR Size）] では、保護範囲メモリ領域レジスタ（PRMRR）のサイズを設定します。これは、システムでのセキュリティと分離を強化するために、保護されたメモリ領域を定義するために使用されます。次のいずれかになります。 • **[128MB]**：128 MB の保護メモリ領域を定義します。 • **[256MB]**：256 MB の保護されたメモリ領域を定義します。 • **512MB**：512 MB の保護メモリ領域を定義します。 • **1GB**：1 ギガバイトの保護メモリ領域を定義します。 • **2GB**：2 ギガバイトの保護メモリ領域を定義します。 • **4GB**：4 ギガバイトの保護メモリ領域を定義します。 • **8GB**：8 ギガバイトの保護メモリ領域を定義します。 • **16GB**：16 ギガバイトの保護メモリ領域を定義します。 • **32GB**：32 ギガバイトの保護メモリ領域を定義します。 • **64GB**：64 GB の保護されたメモリ領域を定義します。 • **128GB**：128 ギガバイトの保護メモリ領域を定義します。 • **256GB**：256 GB の保護されたメモリ領域を定義します。 • **512GB**：512 GB の保護メモリ領域を定義します。 • **[無効な設定（Invalid Config.）]**：保護されたメモリ領域の無効な設定を示します。 • **[自動（Auto）]**：システム要件に基づい

名前	説明
	て、保護メモリ領域のサイズを自動的に設定します。

[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、サーバーの構成によって異なります。

表 *54 : [*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。
[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。

名前	説明
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。
[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
[SHA384 PCR バンク（SHA384 PCR Bank）] ドロップダウン リスト	プラットフォーム構成レジスタ（PCR）は、TPM 内のメモリ位置です。複数の PCR をまとめて PCR バンクと呼びます。セキュア ハッシュ アルゴリズム 384 ビットまたは SHA-384PCR バンクでは、TPM セキュリティを有効または無効にすることができます。 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。
[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。
[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。
[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。

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。
[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。
[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。
[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。

名前	説明
[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。
[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。
[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 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。

名前	説明
[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。
[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 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
[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。
[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。

名前	説明
[TDX セキュア アービトレーション モード（SEAM）ローダー（TDX Secure Arbitration Mode（SEAM）Loader）] ドロップダウン リスト	セキュアな仮想環境での Intel® Trusted Domain Extensions（TDX）を使用できるようにするには、これを有効にします。 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。
[トラスト ドメイン拡張（TDX）（Trust Domain Extension（TDX））] ドロップダウン リスト	信頼ドメインと呼ばれる分離された実行環境を作成することで、仮想環境のセキュリティを強化できます。この環境では、ハイパーバイザなどの他のソフトウェアから機密データやコードを保護します。 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。

[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、サーバーの構成によって異なります。

表 *55 : [*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。

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。 • **[電源オフ（Power Off）]**：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。

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。

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。

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。
[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。

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。

電力制限によって、サーバー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。

[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。次のパスでオプションを有効にすることができます。

[ダッシュボード（Dashboard）] > **[システム（System）]** > **[電源管理（Power Management）]** > **[アクション（Actions）]** ドロップダウン リスト > **[電力特性評価の実行（Run Power Characterization）]**。

（注） **[電源特性評価ステータス（Power Characterization Status）]** オプションは、Cisco UCS C220 M8 および C240 M8 サーバーでは使用できません。

電源の冗長性ポリシーの設定

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。

ステップ 2 **[システム（System）]** メニューから **[電源管理（Power Management）]** タブを選択します。

ステップ 3 **[電源管理（Power Management）]** ページで、**[パワー ポリシー（Power Policies）]** 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
[電源の冗長性ポリシー（Power Supply Redundancy Policy）] ドロップダウン リスト	電源装置の冗長性のポリシー。次のいずれかになります。 • [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。 • [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。 • [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。
[電源の冗長性ステータス（Power Supply Redundancy Status）] フィールド	電源装置の冗長性のステータス。

ステップ 5 [保存（Save）] をクリックします。

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 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。

ステップ 2 **[システム（System）]** ページで **[電源管理（Power Management）]** タブをクリックします。

ステップ 3 **[電源管理（Power Management）]** タブで、**[アクション（Actions）]** ドロップダウン リストをクリックします。

ステップ 4 **[アクション（Actions）]** ドロップダウン リストで、**[電源特性評価（Power Characterization）]** を選択します。

（注）
[電源特性評価ステータス（Power Characterization Status）] オプションは、Cisco UCS C220 M8 および C240 M8 サーバーでは使用できません。

ステップ 5 **[電源特性評価（Power Characterization）]** で **[電源特性評価の実行（Run Power Characterization）]** を選択します。

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。

[電力特性評価のステータス（Power Characterization 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 権限で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 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。

ステップ 2 **[システム（System）]** メニューから **[電源管理（Power Management）]** タブを選択します。

ステップ 3 **[電源管理（Power Management）]** ページで、**[パワー キャッピングの構成（Power Cap Configuration）]** タブをクリックします。

ステップ 4 **[パワー キャッピング（Power Capping）]** トグル ボタンを選択します。

（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。

[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。

（注） **標準**プロファイルは、Cisco UCS C220 M8 および C240 M8 サーバーでは使用できません。

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 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。

ステップ 2 **[システム（System）]** メニューから **[電源管理（Power Management）]** タブを選択します。

ステップ 3 **[電源管理（Power Management）]** ページで、**[パワー キャッピングの構成（Power Cap Configuration）]** タブをクリックします。

ステップ 4 **[パワー キャッピングの構成（Power Cap Configuration）]** ページ > **[パワー キャッピング（Power Cap）]** 領域で、次のフィールドで適切なオプションを選択します。

名前	説明
[パワー キャッピング（Power Capping）] トグル ボタン	有効になっている場合、システムのパワーキャッピング機能が有効になり、個々のパワー キャッピング プロファイルのパラメータを選択して設定できます。 （注） 無効にすると、**[電力プロファイル（Power Profiles）]**エリアでは個々のパワー キャッピング プロファイルを設定または変更できません。 （注） **強化された CPU パフォーマンス** の BIOS トークンが有効になっている場合、パワー キャッピングを有効にすることはできません。
[Recommended Power Cap] 領域	サーバに設定することが推奨される電力上限の値。この範囲は、電力特性評価の実行後に取得されたサーバーにデフォルトで設定されます。これにより、電力制限を設定できます。 • [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。

名前	説明
プラットフォーム	推奨値は次のとおりです。 • 526 W 最小値(スロットリングを許可) • 732 W 最小値(効率的) • 最大 1139 W

表 *56 : [*標準（*Standard*）*]* タブ

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。
[プロファイルの有効化（Enable Profile）] トグル ボタン	電源プロファイルの編集を有効にします。
[スロットルを許可（Allow Throttle）] トグルボタン	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。
[ハード キャップの設定（Set Hard Cap）] トグルボタン	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。
[Action] ドロップダウン リスト	指定された電力制限が訂正時間内に維持されなかった場合に実行するアクション。 • [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。
[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）。

名前	説明
[電力上限（Power Limit）] フィールド	サーバの電力上限を設定できます。

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 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。

ステップ 2 **[システム（System）]** メニューから **[電源管理（Power Management）]** タブを選択します。

ステップ 3 **[電源管理（Power Management）]** ページで、**[パワー キャッピングの構成（Power Cap Configuration）]** タブをクリックします。

ステップ 4 **[パワー キャッピングの構成（Power Cap Configuration）]** ページ > **[パワー キャッピング（Power Cap）]** 領域で、次のフィールドで適切なオプションを選択します。

名前	説明
[パワー キャッピング（Power Capping）] トグル ボタン	有効になっている場合、システムのパワーキャッピング機能が有効になり、個々のパワーキャッピング プロファイルのパラメータを選択して設定できます。 （注） 無効にすると、**[電力プロファイル（Power Profiles）]**エリアでは個々のパワーキャッピング プロファイルを設定または変更できません。 （注） **強化された CPU パフォーマンス** の BIOS トークンが有効になっている場合、パワー キャッピングを有効にすることはできません。

名前	説明
[Recommended Power Cap] 領域	サーバに設定することが推奨される電力上限の値。この範囲は、電力特性評価の実行後に取得されたサーバーにデフォルトで設定されます。これにより、電力制限を設定できます。 • [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。
プラットフォーム	推奨値は次のとおりです。 • 526 W 最小値(スロットリングを許可) • 732 W 最小値(効率的) • 最大 1139 W

表 *57 : [*詳細（*Advanced*）*]* タブ

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。
[プロファイルの有効化（Enable Profile）] トグルボタン	電源プロファイルの編集を有効にします。
[スロットルを許可（Allow Throttle）] トグルボタン	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。 （注） これは、Cisco UCS C220 および C240 M8 サーバーでは使用できません。

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）。 （注） これは、Cisco UCS C220 および C240 M8 サーバーでは使用できません。
[ハード キャップの設定（Set Hard Cap）] トグルボタン	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。 （注） これは、Cisco UCS C220 および C240 M8 サーバーでは使用できません。
[Action] ドロップダウン リスト	指定された電力制限が訂正時間内に維持されなかった場合に実行するアクション。 • [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。

ステップ 5 [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	推奨値：（418 ~ 539）W
メモリ	推奨値: (14～46) W
プラットフォーム	推奨値：（732 ～ 1139）W （注） これは、Cisco UCS C220 および C240 M8 サーバーでは使用できません。

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 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。

ステップ 2 **[システム（System）]** メニューから **[電源管理（Power Management）]** タブを選択します。

ステップ 3 **[電源管理（Power Management）]** ページで、**[パワー キャッピングの構成（Power Cap Configuration）]** タブをクリックします。

ステップ 4 **[パワー キャッピング設定（Power Cap Configuration）]** ページ > **[パワー キャッピング（Power Capping）]** 領域で、**[電力復元ポリシー（Power Restore Policy）]** ドロップダウン リストをクリックします。

名前	説明
電力復元ポリシー(Power Restore Policy)	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。

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 **[アプリ（Apps）]** ドロップダウン リストから、**[ダッシュボード（Dashboard）]** を選択します。

ステップ 2 **[ダッシュボード（Dashboard）]** メニューの **[クイックアクション（Quick Actions）]** で、**[パフォーマンス モニタリング（Performance Monitoring）]**を選択します。

ステップ 3 **[電力 (Power)]** タブで、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。

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。

表 *58 : [*電力モニタリングの概要（***Power Monitoring Summary***）*]* 領域

名前	説明
[Monitoring Period]	一日内のモニタリング期間が HH:MM:SS 形式で表示されます。
プラットフォーム	現在、最小、最大、および平均のサーバー電力使用率を表示します。
CPU	現在、最小、最大、および平均の CPU 電力使用率を表示します。
メモリ	現在、最小、最大、および平均の DIMM 電力使用率を表示します。

ステップ 5 [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。

[チャートのプロパティ（Chart Properties）] 領域で、**[チャート（Chart）]** タブを選択します。

表 *59 : [*チャート プロパティ（***Chart Properties***）*]* 領域

名前	説明
[テーブル/チャート（Table/Chart）] トグル ボタン	テーブル ビューとチャート ビューを切り替えることができます。

名前	説明
[チャート（Chart）] の選択	**過去 1 時間**、 **過去 1 日**、または **先週**のデータから選択できます。
[Download] アイコン	データを `.tar.gz` ファイル形式でダウンロードできます。
[コンポーネント（Component）] ドロップダウン リスト	次のコンポーネントの 1 つ以上を選択できます。 • CPU • メモリー • プラットフォーム
[プロット（Plot）] ドロップダウン リスト	次の電力データから 1 つ以上を選択できます。 • 現在 • 平均 • 最小 • 最大

[チャートのプロパティ（Chart Properties）] 領域で、**[テーブル（Table）]** タブを選択します。

表 *60* : チャート プロパティ テーブル形式

名前	説明
[Time] カラム	データがキャプチャされた時刻を示します。
[プラットフォーム-最小（Platform-Minimum）] カラム	特定のタイムスタンプで行われた**チャート**の選択に応じて、過去 1 時間/日/週にサーバーが消費した最小電力を表示します。
[プラットフォーム-最大（Platform-Maximum）] カラム	特定のタイムスタンプで行われた**チャート**の選択に応じて、過去 1 時間/日/週にサーバーが消費した最大電力が表示されます。
[プラットフォーム-平均（Platform-Average）] カラム	特定のタイムスタンプで行われた**チャート**の選択に応じて、過去 1 時間/日/週にサーバーが消費した平均電力を表示します。
[プラットフォーム-現在（Platform-Current）] カラム	特定のタイムスタンプで行われた **チャート** の選択に応じて、過去 1 時間/日/週にサーバーが消費した現時点の電力を表示します。

名前	説明
[CPU 最小（CPU-Minimum）] カラム	特定のタイムスタンプで行われた**チャート**の選択に応じて、過去 1 時間/日/週に CPU が消費した最小電力を表示します。
[CPU-最大（CPU-Maximum）] カラム	特定のタイムスタンプで行われた**チャート**の選択に応じて、過去 1 時間/日/週に CPU が消費した最大電力を表示します。
[CPU-平均（CPU-Average）] カラム	特定のタイムスタンプで行われた**チャート**の選択に応じて、過去 1 時間/日/週に CPU が消費した平均電力を表示します。
[CPU-現在（CPU-Current）] カラム	特定のタイムスタンプで行われた**チャート**の選択に応じて、過去 1 時間/日/週に CPU が消費した現時点の電力を表示します。
[メモリ-最小（Memory-Minimum）] カラム	特定のタイムスタンプで行われた**チャート**の選択に応じて、過去 1 時間/日/週に DIMM が消費した最小電力を表示します。
[メモリ-最大（Memory-Maximum）] カラム	特定のタイムスタンプで行われた**チャート**の選択に応じて、過去 1 時間、日、週に DIMM が消費した最大電力を表示します。
[メモリ-平均（Memory-Average）] カラム	特定のタイムスタンプで行われた**チャート**の選択に応じて、過去 1 時間、日、週に DIMM が消費した平均電力を表示します。
[メモリ-現在（Memory-Current）] カラム	特定のタイムスタンプで行われた**チャート**の選択に応じて、過去 1 時間/日/週に DIMM が消費した現時点の電力を表示します。

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しておく必要があります。
- 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 **[アプリ（Apps）]** ドロップダウン リストから、**[ダッシュボード（Dashboard）]** を選択します。

ステップ 2 **[ダッシュボード（Dashboard）]** メニューから、**[クイック アクション（Quick Actions）]** > **[パフォーマンス モニタリング（Performance Monitoring）]**を選択します。

ステップ 3 **[電力（Power）]** 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。

[チャート（Chart）]オプションでは、次の表と同じデータがチャート形式で表示されます。チャートデータにマウスカーソルを合わせると、凡例、タイムスタンプ、およびデータ値が表示されます。

表 *61* : チャート プロパティ テーブル形式

名前	説明
[Time] カラム	データがキャプチャされた時刻を示します。
[プラットフォーム-最小（Platform-Minimum）] カラム	特定のタイムスタンプで行われた**チャート**の選択に応じて、過去 1 時間/日/週にサーバーが消費した最小電力を表示します。
[プラットフォーム-最大（Platform-Maximum）] カラム	特定のタイムスタンプで行われた**チャート**の選択に応じて、過去 1 時間/日/週にサーバーが消費した最大電力が表示されます。
[プラットフォーム-平均（Platform-Average）] カラム	特定のタイムスタンプで行われた**チャート**の選択に応じて、過去 1 時間/日/週にサーバーが消費した平均電力を表示します。
[プラットフォーム-現在（Platform-Current）] カラム	特定のタイムスタンプで行われた **チャート** の選択に応じて、過去 1 時間/日/週にサーバーが消費した現時点の電力を表示します。
[CPU 最小（CPU-Minimum）] カラム	特定のタイムスタンプで行われた**チャート**の選択に応じて、過去 1 時間/日/週に CPU が消費した最小電力を表示します。
[CPU-最大（CPU-Maximum）] カラム	特定のタイムスタンプで行われた**チャート**の選択に応じて、過去 1 時間/日/週に CPU が消費した最大電力を表示します。
[CPU-平均（CPU-Average）] カラム	特定のタイムスタンプで行われた**チャート**の選択に応じて、過去 1 時間/日/週に CPU が消費した平均電力を表示します。

名前	説明
[CPU-現在（CPU-Current）] カラム	特定のタイムスタンプで行われた**チャート**の選択に応じて、過去 1 時間/日/週に CPU が消費した現時点の電力を表示します。
[メモリ-最小（Memory-Minimum）] カラム	特定のタイムスタンプで行われた**チャート**の選択に応じて、過去 1 時間/日/週に DIMM が消費した最小電力を表示します。
[メモリ-最大（Memory-Maximum）] カラム	特定のタイムスタンプで行われた**チャート**の選択に応じて、過去 1 時間、日、週に DIMM が消費した最大電力を表示します。
[メモリ-平均（Memory-Average）] カラム	特定のタイムスタンプで行われた**チャート**の選択に応じて、過去 1 時間、日、週に DIMM が消費した平均電力を表示します。
[メモリ-現在（Memory-Current）] カラム	特定のタイムスタンプで行われた**チャート**の選択に応じて、過去 1 時間/日/週に DIMM が消費した現時点の電力を表示します。

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。

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 権限でログインする必要があります。

手順の概要

1. **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。
2. **[システム（System）]** メニューから、**[電源管理（Power Management）]** > **[電源ポリシー（Power Policies）]**を選択します。
3. 右側のペインの **[電源ポリシー（Power Policies）]** 領域で、**[電源復元ポリシー（Power Restore Policy）]** ドロップダウンリストから適切な値をクリックして選択します。
4. [保存（Save）] をクリックします。

手順の詳細

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。

ステップ 2 **[システム（System）]** メニューから、**[電源管理（Power Management）]** > **[電源ポリシー（Power Policies）]** を選択します。

ステップ 3 右側のペインの **[電源ポリシー（Power Policies）]** 領域で、**[電源復元ポリシー（Power Restore Policy）]** ドロップダウンリストから適切な値をクリックして選択します。

名前	説明
電力復元ポリシー(Power Restore Policy)	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 [保存（Save）] 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。
- **[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 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。

ステップ 2 **[システム（System）]** メニューから、**[電源管理（Power Management）]**>**[電源ポリシー（Power Policies）]** を選択します。

ステップ 3 右側のペインの **[電源ポリシー（Power Policies）]** > **[ファン ポリシー（Fan Policies）]** 領域で、**[ファン ポリシー（Fan Policy）]** ドロップダウン リストから適切な値をクリックして選択します。

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。 • **[最大冷却（Maximum Cooling）]**：この設定では、サーバーのファンが最高速度で動作するように設定され、可能な最大の冷却が提供されます。 • [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

名前	説明
	断のない変更です。 （注） このオプションは、Cisco UCS 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 M7 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。
[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 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。

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。 • [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 サーバーの場合、**[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。
[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 M7 および M8 サーバーでのみ使用できます。

ステップ 4 [保存（Save）] をクリックします。

DIMMブロックリストの構成

DIMMブロックリスト

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 のブロ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 をブロ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ロ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 がブロックリスト化されると、同じチャネル上にある他の DIMM が無視されるか無効となり、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、ブロックリストに追加されることはありません。

DIMM のブロック リストの有効化

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 **[アプリ（Apps）]**から、**[システム（System）]**を選択します。

ステップ 2 **[システム（System）]** ページから、**[インベントリ（Inventory）]**を選択します。

ステップ 3 **[インベントリ（Inventory）]** タブで、**[メモリ（Memory）]** をクリックします。

ステップ 4 **[DIMM ブロックリストの有効化/無効化（Enable/Disable DIMM Block List）]** トグルボタンを選択して、**DIMM ブロックリスト**を有効にします。

ステップ 5 [保存（Save）] をクリックします。

工場出荷時のデフォルトに戻す操作を実行した後、デフォルトで、DIMM ブロックリストを有効にする必要があります。

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 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[コンピューティング（Compute）]** を選択します。

ステップ 2 **[コンピューティング（Compute）]** ページで、 **[BIOS]** > **[BIOS トークン（BIOS Tokens）]**を選択します。

ステップ 3 BIOS 設定を更新するには、サーバーの管理 （27 ページ） を参照してください。

（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。各 BIOS 設定のオプションに関する説明および情報については、本ガイドの「サーバ モデル別 *BIOS* パラメータ」の章を参照してください。

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。

ステップ 4 [保存（Save）] をクリックします。

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 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[コンピューティング（Compute）]** を選択します。

ステップ 2 **[コンピューティング（Compute）]** ページで、 **[BIOS]** > **[BIOS トークン（BIOS Tokens）]**を選択します。

ステップ 3 右側のペインの **[アクション（Actions）]** ドロップダウン リストで、 **[BIOS]** > **[BIOS セットアップに入る（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

- このタスクを実行するには、admin 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[コンピューティング（Compute）]** を選択します。

ステップ 2 **[コンピューティング（Compute）]** ページで、 **[BIOS]** > **[BIOS トークン（BIOS Tokens）]**を選択します。

ステップ 3 **[アクション（Actions）]** 領域の**[BIOS]** > **[BIOS CMOS をクリア（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 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[コンピューティング（Compute）]** を選択します。

ステップ 2 **[コンピューティング（Compute）]** ページで、 **[BIOS]** > **[BIOS トークン（BIOS Tokens）]**を選択します。

ステップ 3 **[アクション（Actions）]** ドロップダウンリストで**[BIOS]** > **[製造元のカスタム設定の復元（Restore Manufacturing Custom Settings）]**をクリックします。

ステップ 4 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 5 [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 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[コンピューティング（Compute）]** を選択します。
ステップ 2 **[コンピューティング（Compute）]** ページで、 **[BIOS]** > **[BIOS トークン（BIOS Tokens）]**を選択します。
ステップ 3 右ペインの**[アクション（Actions）]** ドロップダウンリストで、**[デフォルトの復元（Restore Defaults）]** をクリックします。
ステップ 4 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 5 [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 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[コンピューティング（Compute）]** を選択します。

ステップ 2 **[コンピューティング（Compute）]** ページで、 **[BIOS]** > **[BIOS プロファイル（BIOS Profiles）]**を選択します。

ステップ 3 リモート サーバーの場所を使用して BIOS プロファイルをアップロードするには、右側ペインの **[プロファイル（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 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、**[プロファイル（Profiles）]** 領域で次の手順を実行します。

a) [アップロード（Upload）] ボタンをクリックします。

b) **[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。

表 *62:* リモート

名前	説明
リモート ボタン	このオプションは、BIOS プロファイルをリモート ロケーションからアップロードする場合に選択します。
サーバIP/ホスト名	BIOS プロファイルをアップロードするサーバーの詳細。
[Upload Protocol] ボタン	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。
[Path and Filename] フィールド	BIOS プロファイルのサーバーでのファイル パスとファイル名。
[Username] フィールド	リモートサーバのユーザー名。

名前	説明
[パスワード（Password）] フィールド	リモート サーバのパスワードです。
[アップロード（Upload）] ボタン	BIOS プロファイルをアップロードできます。

ステップ 5 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、**[プロファイル（Profiles）]** 領域で次の手順を実行します。

a) [アップロード（Upload）] ボタンをクリックします。

b) **[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。

表 *63 :* ローカル

名前	説明
[ローカル] ボタン	このオプションは、BIOS プロファイルをローカル マシンからアップロードする場合に選択します。 **[参照 (Browse)]** をクリックして、アップロードする BIOS プロファイルに移動します。
[アップロード（Upload）] ボタン	BIOS プロファイルをアップロードできます。

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 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[コンピューティング（Compute）]** を選択します。

ステップ 2 **[コンピューティング（Compute）]** ページで、 **[BIOS]** > **[BIOS プロファイル（BIOS Profiles）]**を選択します。

ステップ 3 **[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 4 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

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[コンピューティング（Compute）]** を選択します。
ステップ 2 **[コンピューティング（Compute）]** ページで、 **[BIOS]** > **[BIOS プロファイル（BIOS Profiles）]**を選択します。
ステップ 3 **[プロファイル（Profile）]** 領域から BIOS プロファイルを選択し、**[削除（Delete）]** 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、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 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[コンピューティング（Compute）]** を選択します。
ステップ 2 **[コンピューティング（Compute）]** ページで、 **[BIOS]** > **[BIOS プロファイル（BIOS Profiles）]**を選択します。
ステップ 3 **[プロファイル（Profile）]** 領域から BIOS プロファイルを選択し、**[バックアップを作成（Take Backup）]** 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、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 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[コンピューティング（Compute）]** を選択します。

ステップ 2 **[コンピューティング（Compute）]** ページで、 **[BIOS]** > **[BIOS プロファイル（BIOS Profiles）]**を選択します。

ステップ 3 **[プロファイル（Profile）]** 領域から BIOS プロファイルを選択し、**[詳細（Details）]** をクリックします。

ステップ 4 **[プロファイルの詳細（Profile Details）]**ウィンドウで、次の情報を確認します。

表 *64 : BIOS*プロファイルの詳細

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 *65 : [*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 *66 :* 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 *67 :* 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。

フィールド	説明
[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 [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

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 *68* : 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

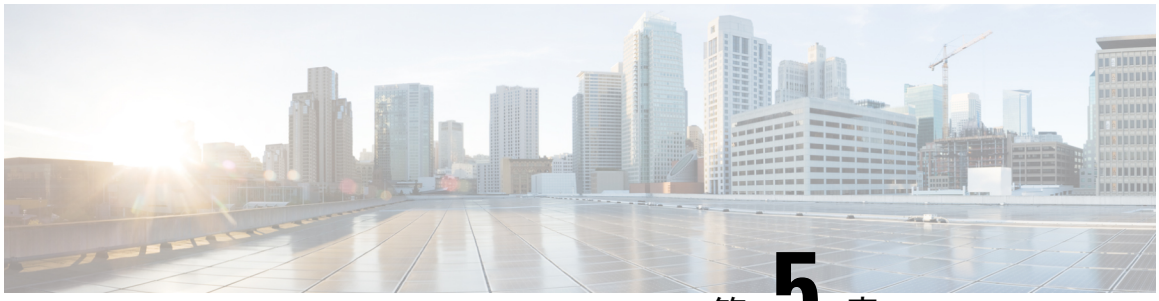
ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。
ステップ 2 **[システム（System）]** ページで、**[センサー（Sensors）]** タブをクリックします。
ステップ 3 [センサー（Sensors）] ペインの [温度（Temperature）] タブをクリックします。
ステップ 4 **[前面パネルの動的温度しきい値（Dynamic Front Panel Temperature Threshold）]** 領域の **[クリティカル（Critical）]** フィールドで前面パネルの温度センサーの上限クリティカル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 [保存（Save）] 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

サーバのプロパティの表示

•
• Viewing Server Utilization （251 ページ）
• サーバー コンポーネントの表示 - 熱パフォーマンス （252 ページ）
• CPU のプロパティの表示 （254 ページ）
• メモリのプロパティの表示 （256 ページ）
• PCI アダプタのプロパティの表示 （260 ページ）
• ストレージのプロパティの表示 （261 ページ）
• TPM のプロパティの表示 （263 ページ）
• PID カタログの表示 （264 ページ）

Viewing Server Utilization

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ダッシュボード（Dashboard）]** を選択します。

ステップ 2 **[ダッシュボード アプリ（Dashboard Apps）]** ページの **[クイック アクション（Quick Actions）]** エリアで、**[パフォーマンス モニター（Performance Monitor）]** を選択します。

[パフォーマンス モニター（Performance Monitor）] ページの **[使用状況（Usage）]** 領域には、**[全体的な使用状況（Overall Utilization）]**、**[CPU の使用状況（CPU Utilization）]**、**[メモリの使用状況（Memory Utilization）]**、および **[I/O の使用状況（IO Utilization）]** に関する情報が表示されます。

システムの CPU、メモリ、および I/O 使用状況のリアルタイムのモニタリング内容が、**[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 **[使用状況（Usage）]** 領域で、次のフィールドを確認して更新します。

表 *69* : サーバー使用率

名前	説明
[全体の使用率（Overall Utilization）] グラフ表示	全体的なサーバー リソースの使用率を表示します。
CPU Utilization (%)	全体の CPU 使用率をパーセンテージで表示します。
[メモリ使用率（%）（Memory Utilization（%））] グラフ表示	全体的な DIMM 使用率をパーセンテージで表示します。
[IO 使用率（%）（IO Utilization（%））] グラフ表示	全体の入出力デバイス使用率をパーセンテージで表示します。

サーバー コンポーネントの表示 - 熱パフォーマンス

リリース 4.3(6) 以降、Cisco IMC では、サーバ内のさまざまなコンポーネントの温度測定値などの熱パフォーマンスを表示およびモニタできます。

デフォルトでは、次の温度しきい値パラメータがコンポーネントに設定されます。

これらのしきい値は、パフォーマンスと安全性のバランスを維持する上で重要であり、過熱による損傷のリスクなくサーバが効率的に動作します。

- **[回復不能上限（Upper Non Recoverable）]**：これは温度制限の設定です。これを超えると、サーバーが重大な状態にあると見なされます。

  コンポーネントの温度がこのしきい値を超えると、コンポーネントの信頼性に大きく影響する可能性があります。

- **[重大上限（Upper Critical）]**：このしきい値は、通常の動作条件よりも高いものの、**[回復不能上限（Upper Non Recoverable）]**しきい値の設定値を下回っている温度レベルを表します。

  このしきい値は、コンポーネントが安全でない動作温度に近づいていることを示す警告として機能します。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ダッシュボード（Dashboard）]** を選択します。

ステップ 2 **[ダッシュボード（Dashboard）]** メニューの **[クイックアクション（Quick Actions）]** で、**[パフォーマンス モニタリング（Performance Monitoring）]**を選択します。

ステップ 3 **[温度 (Thermal)]** タブで、次の情報を確認します。

次の表に、さまざまなサーバーコンポーネントと、温度データが収集およびモニターされるさまざまな期間を示します。

表 *70*：熱管理：チャート エリア

名前	説明
[コンポーネント（Component）] ドロップダウン リスト	次のコンポーネントの 1 つを選択できます。 • プロセッサ • ボード • メモリ • アドイン カード
[期間（Duration）] ドロップダウン リスト	次のいずれかの期間データを選択できます。 • 過去10分間 • 過去 1 時間 • 過去 1 日 • 先週 • 日次最大値

上記のフィールドの **[コンポーネント（Component）]** および **[期間（Duration）]** フィールドで選択した値に基づいて、熱パフォーマンスのデータが右側のペインにチャートとして表示されます。

ステップ 4 上記のフィールドの **[コンポーネント（Component）]** および **[期間（Duration）]** フィールドで選択した値に基づいて、熱パフォーマンスのデータが右側のペインにチャートとして表示されます。

ステップ 5 ページの左ペインに、選択したサーバー コンポーネントにおける次のパラメータのピーク値を表示します。

表 *71 : [*ピーク値（***Peak Values***）*]* エリア

名前	説明
ピーク時間	熱モニタリングの期間が日の HH:MM:SS 形式で表示されます。
温度	選択したコンポーネントの下にあるさまざまなサブコンポーネントの温度を表示します。

次のタスク

CPU のプロパティの表示

手順

ステップ 1 **[**アプリ（**Apps**）**]** ドロップダウン リストから、**[**ダッシュボード（**Dashboard**）**]** を選択します。

ステップ 2 **[**ダッシュボード アプリ（**Dashboard Apps**）**]** ページの **[**プロセッサとメモリ（**Processors & Memory**）**]** 領域で、**[CPU**（**CPUs**）**]** フィールドの下の値をクリックします。

ステップ 3 CPU ごとに次のプロパティを確認します。

（注）
[システム アプリ（**System Apps**）**]** > **[**インベントリ（**Inventory**） > **] [CPU**（**CPUs**）**]**から同じプロパティを表示できます。

表 *72 :* プロセッサ

名前	説明
[Name] カラム	サーバーのプロセッサ数。
[アーキテクチャ（**Architecture** ）**]** カラム	プロセッサで使用されている CPU アーキテクチャ。ここに表示される値は次のとおりです。 • x86 • ARM • SPARC

名前	説明
[Model] カラム	CPU のモデル。
[PID] カラム	Cisco 製品 ID。
[ソケットの名称（Socket Designation）] カラム	CPU が装着されているソケット
[Vendor] カラム	CPU のベンダー。

表 *73* : プロセッサ */ CPU1 / CPU2*

名前	説明
状態	CPU の全般ステータス。ここに表示される値は次のとおりです。 • 良好 • Fault • Severe Fault
CPUステッピング	
[速度（MHz）（Speed（Mhz））]	CPU の速度（メガヘルツ単位）。
モデル（**Model**）	CPU のモデル。
スレッド数	CPU が同時に処理できる最大スレッド数。
コア数	CPU のコア数。
有効なコア数	コア合計のうち、有効になっているコア数。
アーキテクチャ	プロセッサで使用されている CPU アーキテクチャ。ここに表示される値は次のとおりです。 • x86 • ARM • SPARC
ソケット指定	CPU が装着されているソケット
ベンダー	CPU のベンダー。
製品番号	CPU のベンダー製品番号。
PID	CPU のシスコ製品番号。

名前	説明
説明（**Description**）	追加のベンダーと CPU 情報。

メモリのプロパティの表示

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ダッシュボード（Dashboard）]** を選択します。

ステップ 2 **[ダッシュボード アプリ（Dashboard Apps）]** ページの **[プロセッサとメモリ（Processors & Memory）]** 領域で、**[メモリ容量（MB）（Memoriy Capacity（MB））]** フィールドの下の値をクリックします。

ステップ 3 **[メモリのサマリー（Memory Summary）]** 領域で、ドロップダウン矢印をクリックして、メモリのインストール ステータスを表示します。

ステップ 4 プロパティを表示するインストール オプションを選択します。

ステップ 5 **[メモリのサマリー（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。

（注）
[システム アプリ（System Apps）] > **[インベントリ（Inventory）]** > **[メモリ（Memory）]**から同じプロパティを表示できます。

表 74 : Memory Summary

名前	説明
DIMM全体のステータス	DIMM の全体的なステータス。次のいずれかになります。 • [**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。
メモリ速度	メモリ速度（メガヘルツ単位）。
総メモリ	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
有効なメモリ(MB)	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。
冗長メモリ	冗長ストレージに使用されるメモリの量。
[障害が発生したメモリ（Failed Memory）]	現在障害が発生しているメモリの量（メガバイト単位）。
[無視されたメモリ（Ignored Memory）]	現在使用できないメモリの量（メガバイト単位）。
[無視された DIMM 数（Number of Ignored DIMMs）]	サーバーがアクセスできない DIMM の数。
[障害が発生した DIMM の数（Number of Failed DIMMs）]	障害が発生し、使用できない DIMM の数。
[可能なメモリ RAS（Memory RAS Possible）]	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
[Memory Configuration]	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。 • [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。
[DIMM ブロックリストの有効化/無効化（Enable/Disable DIMM Block List）] トグル ボタン	DIMM のブロック 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。 （注） **工場出荷時のデフォルトに復元**した後、DIMM ブロックリストはデフォルトで有効になります。
[ロケーション（Location）] カラム	サーバー内の DIMM の位置。
[Type] カラム	デバイスで使用されるメモリのタイプ。
[PID] カラム	Cisco DIMM の製品番号。
[Serial] カラム	DIMM のシリアル番号。
[容量（MB）（Capacity（MB））] カラム	DIMM のサイズ。
[クロック速度（MHZ）（Clock Speed（MHZ））] カラム	DIMM の動作速度。

ステップ 6 各 DIMM の詳細を表示するには、リストから目的の DIMM をクリックします。

[メモリ/DIMM_location（Memory / DIMM_location）] ページが表示されます。

ステップ 7 **[メモリ/DIMM_location（Memory / DIMM_location）]** ページで、次のプロパティを確認します。

表 *75 :* メモリ / *DIMM* の場所（*Memory / DIMM_location*）

名前	説明
状態	DIMM が有効か無効かを示します。 デフォルトでは、取り付けられているすべてのDIMMが有効になっています。
容量(MB)	DIMM のサイズ。
メモリタイプ	デバイスで使用されるメモリのタイプ。
Channel Type	メモリ チャネルのタイプ。
クロック速度(MHz)	DIMM の動作速度。通常は、取り付けた DIMM でサポートされていて、システムと互換性がある最大速度に設定されます。
データ幅(ビット)	DIMM がサポートするデータの量（ビット単位）。
製造元	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.
シリアル番号（Serial Number）	DIMM のシリアル番号。
製品番号	ベンダーによって割り当てられた DIMM の部品番号。
PID	Cisco DIMM の製品番号。
バンクロケータ	メモリ バンク内の DIMM の場所。
[メモリ タイプの詳細（Memory Type Detail）] カラム	デバイスで使用されるメモリのタイプ。
可視性	DIMM がサーバに対して使用可能であるかどうか。

名前	説明
運用性	DIMM が現在正常に動作しているかどうか。
説明（**Description**）	DIMM に関する追加の説明。

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 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。

ステップ 2 **[インベントリ（Inventory）]** タブを選択します。

ステップ 3 [ナビゲーション（Navigation）] ペインから **[PCIe デバイス（PCIe Devices）]**を選択します。

ステップ 4 ドロップダウン リストから、表示するアダプタのタイプを選択します。

次のオプションから選択できます。

- すべて
- ストレージ
- Cisco VIC アダプタ
- ネットワーク アダプタ

  リリース 4.3(5.240021)以降、**[ネットワーク アダプタ（Network Adapters）]** にリストされている DPU のプロパティを表示できます。
- GPU

ステップ 5 次のプロパティを表示することができます：

名前	説明
[ID] カラム	PCIe デバイス ID。
[Name] カラム	アダプタの名前。

名前	説明
[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（Not Loaded）]：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。
MAC アドレス（MAC Address）	Intel(R) ネットワーク コントローラの MAC アドレス （注） このフィールドは、Intel(R) ネットワーク コントローラでのみ表示されます。

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 **[アプリ（Apps）]** ドロップダウン リストから、**[ダッシュボード（Dashboard）]** を選択します。
ステップ 2 **[ストレージ (Storage)]** エリアで、次の情報を確認します。

表 *76 : [*ストレージ（***Storage***）*]* 領域

名前	説明
[Controllers]	使用可能な RAID 番号。
OSに使用可能なキャパシティ	インストールされている OS が使用可能なストレージ容量（ギガバイト単位）。
Physical Drives	サーバーで使用可能な ドライブの合計数。
仮想ドライブ	利用可能な仮想ドライブの合計数。

ステップ 3 **[コントローラ（Controllers）]**で、番号をクリックして次の [ストレージアダプタ（Storage Adapter）] プロパティを表示します。

表 *77 :* ストレージアダプタ

名前	説明
[PCI Slot] カラム	コントローラ ドライブが存在する PCI スロット。
[Name] カラム	コントローラの名前。
[**Firmware Version**] カラム	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。
[Serial Number] カラム	ストレージ コントローラのシリアル番号。

ステップ 4 **[物理ドライブ（Physical Drives）]** で、番号をクリックして、次の [物理ドライブ（Physical Drives）] プロパティを表示します。

表 *78 : Physical Drives*

名前	説明
[コントローラ（Controller）] カラム	RAID コントローラの名前
[物理ドライブ（Physical Drives）] カラム	使用可能な物理ドライブの合計数。
[合計容量 (GB)（Total Capacity（GB））] カラム	サーバーに存在する物理ディスクの合計容量。

ステップ 5 **[仮想ドライブ（Virtual Drives）]**で、番号をクリックして、次の [仮想ドライブ（Virtual Drives）] プロパティを表示します。

表 *79 :* 仮想ドライブ

名前	説明
[コントローラ（Controller）] カラム	RAID コントローラの名前

名前	説明
[仮想ドライブ（Virtual Drive）] カラム	利用可能な仮想ドライブの合計数。
[合計容量 (GB)（Total Capacity (GB)）] カラム	仮想ドライブの合計キャパシティが表示されます。

TPM のプロパティの表示

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。

ステップ 2 **[インベントリ（Inventory）]** タブを選択します。

ステップ 3 [ナビゲーション（Navigation）] ペインから、**[TPM]** を選択します。

ステップ 4 次のプロパティを表示することができます：

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。

名前	説明
[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。
[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 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。
ステップ 2 **[インベントリ（Inventory）]** タブを選択します。
ステップ 3 [ナビゲーション（Navigation）] ペインから **[PID カタログ（PID Catalog）]** を選択します。
ステップ 4 次のプロパティを表示することができます：

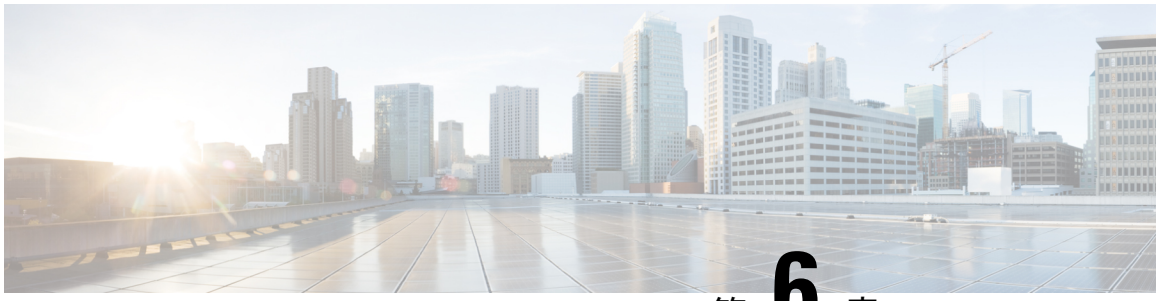
表 *80 : PID*カタログのステータス

名前	説明
アップロードステータス	PID カタログのアップロード ステータス。 値は次のいずれかになります。 • アップロード中（Upload in Progress） • アップロードの成功 • アップロード エラー - TFTP ファイルが見つかりません（Upload Error - TFTP File Not Found） • アップロード エラー - 接続に失敗しました（Upload Error - Connection Failed） • アップロード エラー - アクセスが拒否されました（Upload Error - Access Denied） • アップロード エラー - ファイルが見つかりません（Upload Error - File Not Found） • アップロード エラー - ダウンロードに失敗しました（Upload Error - Download Failed） • アクティベーションに成功しました（Activation Successful） • エラー - 不明（Error - Unknown） • なし
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 ステータスを表示します。
[現在のアクティベーション ステータス（Current Activated Status）]	現在有効な PID カタログを表示します。

表 *81 : [PID* カタログの詳細（*PID Catalog Detail*）*]*

名前	説明
[PCI Slot] フィールド	PCIe デバイスが配置されているスロット。
[Vendor] フィールド	PCIe デバイスのベンダー。
[Product ID] フィールド	PCIe デバイスの製品 ID。

名前	説明
[Description] フィールド	PCIe デバイスのモデル番号。



第 6 章

センサーの表示

- 温度センサーの表示 （267 ページ）
- LED センサーの表示 （268 ページ）
- ストレージ センサーの表示 （268 ページ）
- 電源センサーの表示 （269 ページ）
- ファン センサーの表示 （270 ページ）

温度センサーの表示

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。

ステップ 2 **[センサー（Sensors）]** タブを選択します。

ステップ 3 [ナビゲーション（Navigation）] ペインから、 **[温度（Temperature）]**を選択します。

ステップ 4 次のプロパティを確認します。

名前	説明
[名前（Name）] フィールド	温度センサーの名前。
ステータス（Status）	温度センサーの動作ステータス。
[Temperature] フィールド	現在の温度（摂氏/華氏）。
[クリティカル最小しきい値（Critical Threshold Min）] フィールド	Critical の最小しきい値。
[クリティカル最大しきい値（Critical Threshold Max）] フィールド	Critical の最大しきい値。

名前	説明
[回復不能最小しきい値 Non-Recoverable Threshold Min）] フィールド	回復不可能な最小しきい値。
[回復不能最大しきい値（Non-Recoverable Threshold Max）] フィールド	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 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。
ステップ 2 **[センサー（Sensors）]** タブを選択します。
ステップ 3 [ナビゲーション（Navigation）] ペインから、**[LED]** を選択します。
ステップ 4 次のプロパティを確認します。

名前	説明
[Name] カラム	センサーの名前。
[Status] カラム	LED が点灯、点滅、または消灯しているかどうか。
[カラー（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 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。
ステップ 2 **[センサー（Sensors）]** タブを選択します。

ステップ 3 [ナビゲーション（Navigation）] ペインから、**[ストレージ（Storage）]** を選択します。
ステップ 4 次のプロパティを確認します。

名前	説明
[名前（Name）] フィールド	ストレージ デバイスの名前。
[Status] フィールド	ストレージ デバイスのステータスに関する簡単な説明。
[LED ステータス（LED Status）] フィールド	現在の LED の色（LED 付きの場合）。 ストレージ デバイスの物理 LED を点滅させるには、ドロップダウン リストから [点灯（Turn On）] を選択します。 LED の点滅をストレージ デバイスに制御させるには、[消灯（Turn Off）] を選択します。 **（注）** この情報は、一部の C シリーズ サーバのみで表示されます。

電源センサーの表示

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。
ステップ 2 **[センサー（Sensors）]** タブを選択します。
ステップ 3 [ナビゲーション（Navigation）] ペインから、**[電源（Power Supply）]** を選択します。
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。

名前	説明
[名前（Name）] フィールド	電源装置の名前。
[Type] フィールド	電源装置のタイプ。
ステータス（Status）	電源装置の動作ステータス。
[読み取り値（Reading）] フィールド	現在の電力使用量（ワット単位）。
[クリティカル最小しきい値（Critical Threshold Min）] フィールド	Critical の最小しきい値。

名前	説明
[クリティカル最大しきい値（Critical Threshold Max）] フィールド	Critical の最大しきい値。
[回復不能最小しきい値 Non-Recoverable Threshold Min）] フィールド	回復不可能な最小しきい値。
[回復不能最大しきい値（Non-Recoverable Threshold Max）] フィールド	回復不可能な最大しきい値。

ファン センサーの表示

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。

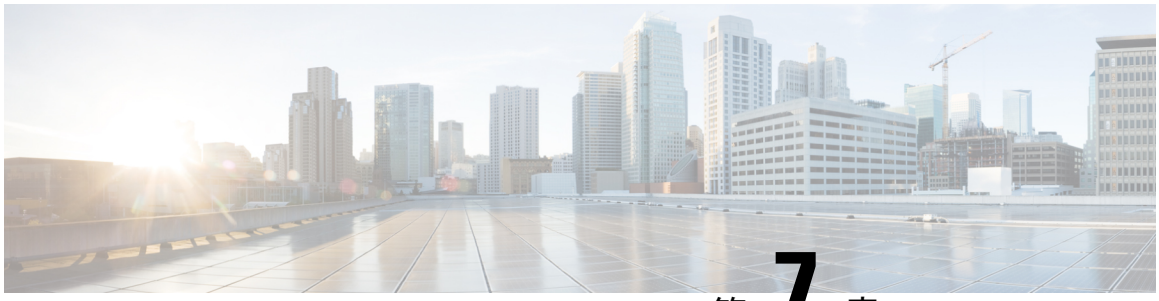
ステップ 2 **[センサー（Sensors）]** タブを選択します。

ステップ 3 [ナビゲーション（Navigation）] ペインから、**[fファン（Fan）]** を選択します。

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
[名前（Name）] フィールド	ファンの名前。
ステータス（Status）	ファンの動作ステータス。
[読み取り値（Reading）] フィールド	現在の電力使用量（ワット単位）。
[回復不能最小しきい値 Non-Recoverable Threshold Min）] フィールド	回復不可能な最小しきい値。
[PWM（%）]	パルス幅変調（PWM）は、速度を制御するためにファンのオン時間とオフ時間を変化させる絶対的な手段です。 オフタイムと比較したオンタイムの割合を **デューティサイクル**と呼びます。

名前	説明
[回復不能最大しきい値（Non-Recoverable Threshold Max）] フィールド	回復不可能な最大しきい値。



第 7 章

リモート プレゼンスの管理

•

• Serial over LAN の設定 （273 ページ）
• 仮想メディアの設定 （275 ページ）
• 仮想 KVM コンソール （283 ページ）
• KVM コンソールの起動 （284 ページ）
• 仮想 KVM コンソール - Cisco UCS C-Series M6 以降のサーバー （285 ページ）
• 仮想 KVM の設定 （302 ページ）

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。

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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[通信サービス（Communication Services）]** メニューをクリックします。

ステップ 3 [Serial over LAN Properties] 領域で、次のプロパティを更新します。

表 *82 : [Serial over LAN]* 領域

名前	説明
[有効（Enabled）] トグル ボタン	このサーバーで Serial over LAN（SoL）を有効または無効にすることができます。

名前	説明
[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 4 [保存（Save）] 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 **[アプリ（Apps）]** ドロップダウン リストから、**[コンピューティング（Compute）]** を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[リモート管理（Remote Management）]** メニューをクリックします。

ステップ 3 **[プロパティ（Properties）]** 領域で、次のプロパティを更新します。

表 *83* : プロパティ領域

名前	説明
[仮想KVMの有効化（Enable Virtual KVM）] トグル ボタン	仮想 KVM をイネーブルまたはディセーブルにできます。
[Max Sessions] ドロップダウン リスト	許可されている vKVM の同時セッションの最大数。選択できる数値は 1 ～ 4 です。
[リモートポート（Remote Port）] フィールド	vKVM 通信に使用するポート。
アクティブセッション	サーバーで実行されている vKVM セッションの数。
[仮想メディアの有効化（Enable Virtual Media）] トグル ボタン	オンにすると、サーバーは vKVM で送信されるすべてのビデオ情報を暗号化します。
[ローカル サーバー ビデオの有効化（Enable Local Server Video）] トグル ボタン	オンにすると、vKVM セッションはサーバーに接続されているすべてのモニタにも表示されます。
[低電力 USB の有効化（Lower Power USB Enabled）] トグル ボタン	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。

名前	説明
アクティブな仮想メディアセッション	アクティブな仮想メディア セッションを表示します。

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 **[アプリ（Apps）]** ドロップダウン リストから、**[コンピューティング（Compute）]** を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[リモート管理（Remote Management）]** メニューをクリックします。

ステップ 3 **[仮想メディア マッピング（Virtual Media 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 4 **[仮想メディアの追加（Add Virtual Media）]** 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
[仮想メディア タイプ（Virtual Media Type）] オプション ボタン	次のいずれかになります。 • [CDD] • [HDD]

名前	説明
[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。
[ファイルの場所] 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 5 [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 **[アプリ（Apps）]** ドロップダウン リストから、**[コンピューティング（Compute）]** を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[リモート管理（Remote Management）]** メニューをクリックします。

ステップ 3 **[仮想メディア マッピング（Virtual Media Mapping）]** 領域で、マッピング テーブルから行を選択します。

ステップ 4 [Properties] をクリックし、次の情報を確認します。

表 *84 :* 仮想メディアマッピング

名前	説明
[Add New Mapping] ボタン	新しいイメージを追加できます。
[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
[再マップ（Remap）] ボタン	保存済みのマッピングを変更します。
[Delete] ボタン	保存済みのマッピングを削除します。
[Volume] 列	イメージの ID。
[プロトコル（Protocol）] カラム	イメージのプロトコル。
[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。 • **[古い（Stale）]**： Cisco IMC はマッピングが古い理由を示すテキスト文字列を表示します。 • **[エラー（Error）]**： Cisco IMC はエラーの理由を示すテキスト文字列を表示します。
マッピングステータス	最後に試行されたマッピングのステータス。

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 **[アプリ（Apps）]** ドロップダウン リストから、**[コンピューティング（Compute）]** を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[リモート管理（Remote Management）]** メニューをクリックします。

ステップ 3 **[仮想メディア マッピング（Virtual Media Mapping）]** 領域で、マッピング テーブルから行を選択します。

ステップ 4 **[仮想メディア マッピング（Virtual Media Mappings）]** 領域で、**[マッピング解除Unmap）]** をクリックします。

マッピングを保存するように求められたら、 **[保存（Save）]**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 **[アプリ（Apps）]** ドロップダウン リストから、**[コンピューティング（Compute）]** を選択します。
ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[リモート管理（Remote Management）]** メニューをクリックします。
ステップ 3 **[仮想メディア マッピング（Virtual Media Mapping）]** 領域で、マッピング テーブルから行を選択します。
ステップ 4 **[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 **[アプリ（Apps）]** ドロップダウン リストから、**[コンピューティング（Compute）]** を選択します。
ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[リモート管理（Remote Management）]** メニューをクリックします。
ステップ 3 **[仮想メディア マッピング（Virtual Media Mapping）]** 領域で、マッピング テーブルから行を選択します。
ステップ 4 **[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 、**[ダッシュボード アプリ（Dashboard App）]** または **[アクション（Actions）]** から起動できます。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ダッシュボード（Dashboard）]** を選択します。

ステップ 2 **KVM コンソール**で、 **[KVM の起動（Launch KVM）]** ボタンをクリックします。

ステップ 3 または、**[アクション（Actions）]** > **[システム（System）]** > **[KVM の起動（Launch KVM）]**の任意のページから **KVM コンソール** を起動できます。

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。

コンソール（**Console**） メニュー

メニュー項目	説明
KVM	現用系のコンソールとして KVM（Keyboard Video and Mouse）を選択します。
SOL	現用系のコンソールとして 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、**[SQL を有効化（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 を有効化]** 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**）	**[クリップボード テキストの貼り付け（Paste Clipboard Text）]** ダイアログ ボックスには、次のオプションがあります。 • **[設定（Settings）]** ボタン：[設定（Settings）]ダイアログ ボックスを開きます。詳細については、表 85 : [設定（Settings）] ダイアログ ボックス （286 ページ）を参照してください。 • **[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（Send）]**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 *85 : [*設定（***Settings***）*]* ダイアログ ボックス

名前	説明
[貼り付けたテキストにサポートされていない文字がある場合：（When an unsupported character is found in pasted text:）] ドロップダウンリスト	サポートされていない文字が貼り付けられたテキストで見つかった場合のアクションを選択できます。 • 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（Unsupported Character）]** ダイアログ ボックスが開きます。 • 文字の処理方法を尋ねる—**[サポートされていない文字（Unsupported Character）]** ダイアログ ボックスを開きます。

名前	説明
[文字のマッピング（Character Mapping）] ボタン	**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 (文字長なし) に置き換えます。
[キーボード（Keyboard）] ドロップダウン リスト	文字の貼り付けに使用するキーボードのレイアウト。これは、ホストのキーボード レイアウトと同じである必要があります。
[**Save**] ボタン	設定を保存します。 （注） このオプションは、設定が更新された場合にのみ有効になります。

表 *86 : [*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。
[サポートされていない文字] ドロップダウン リストから操作方法を選択してください。	次の操作の 1 つを選択できます。 • 文字を無視する（Ignore the character(s)）- 無視するサポートされていない文字を判別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（Cancel the paste operation）—操作をキャンセルします。 文字を置き換える（Replace the character(s)） - 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（Replacement）] フィールド	（注） このオプションは、**[文字を置換（Replace the character(s)）]** 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に保存する（Store a mapping of this replacement to the unsupported character）] チェック ボックス	（注） このオプションは、**[文字を置換（Replace the character(s)）]** オプションでのみ表示されます。 文字マッピングを保存できるようになります。
[すべての*unsupported_character* 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に対してこのアクションを繰り返す（Repeat this action for all unsupported characters）]チェックボックス	（注） このオプションは、**[貼り付け操作をキャンセル（Cancel the paste operation）]** オプションの場合にのみ表示されません。 同じサポートされていない文字に対して、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。

メニュー項目	説明
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。
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 コンソールでのみがサポートされています。
全画面表示	画面全体になるように vKVM コンソールを拡大します。

マクロ画面

（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（受信合計バイト数）**—受信した合計バイト数。 • **合計送信バイト数（Total Bytes Sent）** —送信された合計バイト数。 • **受信待機幅（Rx Bandwidth）**—秒あたりの KB 数で測定された受信帯域幅。 • **送信帯域幅（Tx Bandwidth）—**秒あたりの KB 数で測定された送信帯域幅。 • **フレーム速度（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 タイル速度（Video Tile Rate）** —秒あたりにレンダリングされるビデオ タイル。 vMedia が有効化されると、**vKVM-Mapped vMedia Stats** エリアが次のとおり表示します。 • **Total Bytes Rec（受信合計バイト数）**—受信した合計バイト数。 • **合計送信バイト数（Total Bytes Sent）** —送信された合計バイト数。 • **デバイス（Device）**—ローカル デバイスのタイプ。 • **マップされたファイル（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。 • **期間（Duration）**—マップするデバイスの経過時間。 • **読み取りバイト数（Read Bytes）**—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（Write Bytes）** —vKVM メディアに書き込まれたバイト数。 • **所有者（Owner）**— メディアをブラウザにマップしたユーザー。

メニュー項目	説明
	[CIMC マップされた vMedia Stats（**CIMC-Mapped vMedia Stats**）]エリアには、次の情報が表示されます。

メニュー項目	説明
	• **デバイス（Device）**—ローカル デバイスのタイプ。 • **マップされたファイル（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。 • **デバイス ステータス（Device Status）** - 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 ステータスです • 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

メニュー項目	説明
	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
[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 **[セッション ユーザー リスト（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。

メニュー項目	説明
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。
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。
[ブートデバイス（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。[イメージの作成（Create Image）] ダイアログボックスに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。
vMedia を有効化（Activate vMedia）	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） **[vMedia を有効化]** 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 を有効化]** 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。

名前	説明
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。
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、表 87 : [Add New Mapping] ダイアログボックス （298 ページ） を参照してください。 （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、表 87 : [Add New Mapping] ダイアログボックス （298 ページ） を参照してください。 （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 *87 : [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。

名前	説明
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
[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）。

名前	説明
[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。
[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。

名前	説明
[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

[プロフィール 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（Role）]	ユーザ ロール名を表示します。
[サーバ（Server）]	ホスト名と IP アドレスを表示します。

名前	説明

[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（Maintain Aspect Ratio）** - 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（Absolute Positioning）** — 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（Relative Positioning）** — 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（Video Inactivity Timeout）]** 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。
	• **[端末のスクロールバック行数（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（Theme）** —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（Save）]** 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 **[アプリ（Apps）]** ドロップダウン リストから、**[コンピューティング（Compute）]** を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[リモート管理（Remote Management）]** メニューをクリックします。

ステップ 3 **[プロパティ（Properties）]** 領域で、次を更新します。

表 *88* : プロパティ領域

名前	説明
[仮想KVMの有効化（Enable Virtual KVM）] トグル ボタン	仮想 KVM をイネーブルまたはディセーブルにできます。
[Max Sessions] ドロップダウン リスト	許可されている vKVM の同時セッションの最大数。選択できる数値は 1 ～ 4 です。
[リモートポート（Remote Port）] フィールド	vKVM 通信に使用するポート。
アクティブセッション	サーバーで実行されている vKVM セッションの数。
[仮想メディアの有効化（Enable Virtual Media）] トグル ボタン	オンにすると、サーバーは vKVM で送信されるすべてのビデオ情報を暗号化します。
[ローカル サーバー ビデオの有効化（Enable Local Server Video）] トグル ボタン	オンにすると、vKVM セッションはサーバーに接続されているすべてのモニタにも表示されます。
[低電力 USB の有効化（Lower Power USB Enabled）] トグル ボタン	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。
アクティブな仮想メディアセッション	アクティブな仮想メディア セッションを表示します。

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 **[アプリ（Apps）]** ドロップダウン リストから、**[コンピューティング（Compute）]** を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[リモート管理（Remote Management）]** メニューをクリックします。

ステップ 3 **[プロパティ（Properties）]** 領域で、 **[仮想 KVM の有効化（Enabled Virtual KVM）]** チェックボックスをオンにします。

仮想 KVM のディセーブル化

始める前に

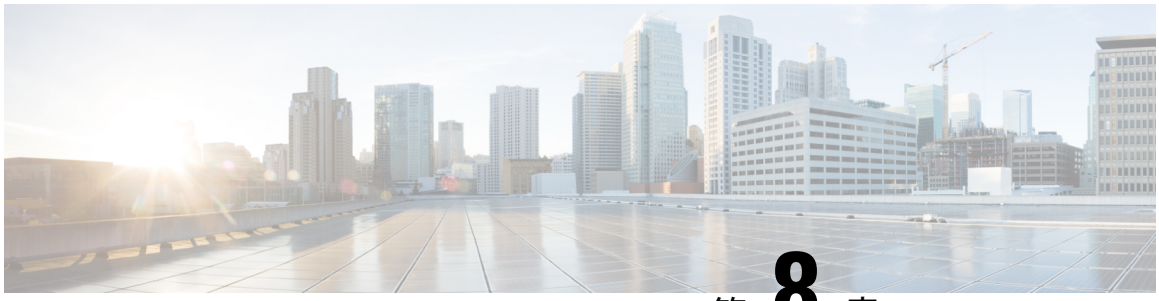
仮想 KVM をイネーブルにするには、admin 権限を持つユーザーとしてログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[コンピューティング（Compute）]** を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[リモート管理（Remote Management）]** メニューをクリックします。

ステップ 3 **[プロパティ（Properties）]** 領域で、 **[仮想 KVM の有効化（Enabled Virtual KVM）]** チェックボックスをオフにします。



第 8 章

ユーザー アカウントの管理

-
- 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 （305 ページ）
- 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 （309 ページ）
- ユーザ アカウントでの SSH キーの管理 （313 ページ）
- パスワードの有効期限切れ （319 ページ）
- 非管理者ユーザーとしてパスワードの変更 （321 ページ）
- アカウントロックアウトの詳細の構成 （322 ページ）
- ユーザー認証の優先順位の構成 （323 ページ）
- 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 （324 ページ）
- LDAP サーバ （325 ページ）
- LDAP 証明書の概要 （333 ページ）
- TACACS+ 認証 （337 ページ）
- ユーザー セッションの表示と終了 （340 ページ）

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 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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ユーザー管理（User Management）]** メニューをクリックします。

ステップ 3 **[ユーザー管理（User Management）]** タブを選択します。

ステップ 4 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。

ステップ 5 **[ローカル ユーザーの詳細（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。

表 ***89 :*** ユーザー名とロール

名前	説明
[ユーザ名（User Name）] フィールド	ユーザーのユーザー名を入力します。 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
[果たすロール（Role Played）]ドロップダウン リスト	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。 • [読み取りのみ（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。 • [ユーザ（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 • [管理者（admin）]：このロールのユーザは、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。
[有効（Enabled）] トグルボタン	オンにすると、ユーザは Cisco IMC でイネーブルになります。
[CIMC/IPMI/SNMP] トグル ボタン	次のタイプのユーザーを作成できます。 • CIMC • SNMP • IPMI

表 *90 : CIMC*

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。
[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。

名前	説明
[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 *91 : IPMI*

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。
[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。
[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 *92 : SNMP*

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。
[許可タイプ（Auth Type）] ドロップダウン リスト	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 リスト	プライバシー タイプ。次のいずれかになります。 • **CFB128_AES128**
[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。
プライバシーパスワードの確認	確認のための許可パスワードの再入力。

ステップ 6 [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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ユーザー管理（User Management）]** メニューをクリックします。

ステップ 3 **[ユーザー管理（User Management）]** タブを選択します。

ステップ 4 ローカル ユーザー アカウントを変更するには、で行をクリックし、**[ユーザーの変更（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。

表 *93 :* ユーザの詳細

名前	説明
ID	システムによって割り当てられるユーザーID。このID は編集できません
[ユーザ名（User Name）]フィールド	ユーザーのユーザー名を入力します。 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

[果たすロール（Role Played）]ドロップダウン リスト	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。
	• [読み取りのみ（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。
	• [ユーザ（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
	• [管理者（admin）]：このロールのユーザは、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。

[有効（Enabled）] トグルボタン	オンにすると、ユーザは Cisco IMC でイネーブルになります。
[CIMC/IPMI/SNMP] トグル ボタン	次のタイプのユーザーを作成できます。 • CIMC • SNMP • IPMI （注） 変更するユーザーのデフォルトのユーザー タイプをオフにすることはできません。
[パスワードの変更（Change Password）] トグル ボタン	ローカル ユーザー パスワードを変更できます。 （注） CIMC、IPMI、または SNMP のプロパティは、**[パスワードの変更（Change Password）]** が有効な場合にのみ表示されます。

表 *94 : CIMC*

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。
[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。
[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 *95 : IPMI*

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。
[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。
[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 *96 : SNMP*

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。

名前	説明
[許可タイプ（Auth Type）] ドロップダウン リスト	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**
[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 リスト	プライバシー タイプ。次のいずれかになります。 • **CFB128_AES128**
[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。
プライバシーパスワードの確認	確認のための許可パスワードの再入力。

ステップ 6 [保存（Save）] をクリックします。

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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ユーザー管理（User Management）]** メニューをクリックします。

ステップ 3 **[ユーザー管理（User Management）]** タブを選択します。

ステップ 4 アカウントの SSH キーの詳細を表示するには、ペインの行を選択し、**[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 (SSH Keys)]** ウィンドウで、次のプロパティを表示します。

表 *97 : SSH* キー

名前	説明
[ID] チェックボックス	SSH キーを選択できます。
[コメント（Comments ）] 列	キーを説明する内容を表示します。
[キー（Key）] カラム	キー テキストを表示します。
[追加（Add）] アイコン	新しい SSH キーを追加できます。 空の SSH キーの行の **[ID]** チェックボックスをオンにして、**[追加（Add）]**をクリックします。その後、キーを貼り付けるか、ローカルまたはリモートの場所からキーをアップロードできます。

名前	説明
[編集（Edit）] アイコン	SSH キーを編集できます。 編集する SSH キーの **[ID]** チェックボックスをオンにします。編集アイコンをクリックします。その後、キーを貼り付けるか、ローカルまたはリモートの場所からキーをアップロードできます。
[削除（Delete）] アイコン	SSH キーを削除できます。[OK] をクリックして続行します。

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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ユーザー管理（User Management）]** メニューをクリックします。

ステップ 3 **[ユーザー管理（User Management）]** タブを選択します。

ステップ 4 アカウントの SSH キーを追加するには、ペインの行を選択し、 **[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 キーを追加するには、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。

（注）
[キーの追加（Add Keys）] アイコンは、空のスロットに対してのみアクティブになります。

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 次のいずれかの情報を使用して、キーをアップロードします。

表 *98* : 貼り付け

名前	説明
[SSH キーの貼り付け（Paste SSH Key）] フィールド	キーの内容全体をコピーして、[貼り付け（Paste）] テキスト フィールドに貼り付けることができます。
[アップロード（Upload）] ボタン	キーをアップロードできます。

表 *99* : ローカル

名前	説明
[参照（Browse）] ボタン	**[参照 (Browse)]** をクリックして、アップロードするキーに移動します。
[アップロード（Upload）] ボタン	キーをアップロードできます。

表 *100* : リモート

名前	説明
[サーバIP/ホスト名（Server IP/Hostname）] フィールド	キーをアップロードするサーバーの詳細。
[Upload Protocol] ボタン	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。
[Path and Filename] フィールド	キー ファイルのサーバーでのファイル パスとファイル名。
[Username] フィールド	リモートサーバのユーザー名。
[パスワード（Password）] フィールド	リモート サーバのパスワードです。

名前	説明
[アップロード（Upload）] ボタン	キーをアップロードできます。

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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ユーザー管理（User Management）]** メニューをクリックします。

ステップ 3 **[ユーザー管理（User Management）]** タブを選択します。

ステップ 4 アカウントの SSH キーを変更するには、ペインの行を選択し、**[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 **[SSH キー（SSH Keys）]** ウィンドウの **[キーの編集（Edit Keys）]** アイコンをクリックして、SSH キーを追加します。

ステップ 7 次のいずれかの情報を使用して、キーをアップロードします。

表 *101* : 貼り付け

名前	説明
[SSH キーの貼り付け（Paste SSH Key）] フィールド	キーの内容全体をコピーして、[貼り付け（Paste）] テキスト フィールドに貼り付けることができます。
[アップロード（Upload）] ボタン	キーをアップロードできます。

表 *102 :* ローカル

名前	説明
[参照（Browse）] ボタン	**[参照 (Browse)]** をクリックして、アップロードするキーに移動します。
[アップロード（Upload）] ボタン	キーをアップロードできます。

表 *103 :* リモート

名前	説明
[サーバIP/ホスト名（Server IP/Hostname）] フィールド	キーをアップロードするサーバーの詳細。
[Upload Protocol] ボタン	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。
[Path and Filename] フィールド	キー ファイルのサーバーでのファイル パスとファイル名。
[Username] フィールド	リモートサーバのユーザー名。
[パスワード（Password）] フィールド	リモート サーバのパスワードです。
[アップロード（Upload）] ボタン	キーをアップロードできます。

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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ユーザー管理（User Management）]** メニューをクリックします。

ステップ 3 **[ユーザー管理（User Management）]** タブを選択します。

ステップ 4 アカウントの SSH キーを削除するには、ペインの行を選択し、 **[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 ウィンドウが表示されます。

ステップ 7 [OK] をクリックして、削除を実行します。

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有効化と設定

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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ユーザー管理（User Management）]** メニューをクリックします。

ステップ 3 **[アクション（Actions）]** ドロップダウン リストから、**[ユーザー管理（User Management）]** > **[パスワードの有効期限の詳細（Password Expiration Details）]**の順 に選択します。

[パスワード有効期限の詳細（Password Expiration Details）] ダイアログ ボックスが表示されます。

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、次のプロパティを更新します。

表 *104 :* パスワードの有効期限の詳細

名前	説明
[パスワード有効期限の有効化（Enable Password Expiry）] トグル ボタン	パスワード有効期限を有効または無効にできます。
[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。

名前	説明
[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。
[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。
[Reset] ボタン	値をリセットできます。
[Restore Defaults] ボタン	工場出荷時設定に戻せます。

ステップ 5 **[Save Changes]**をクリックします。

非管理者ユーザーとしてパスワードの変更

始める前に

パスワードを変更するには、非管理者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 Cisco IMC GUI の右上隅から、 **[Cisco IMC 情報（Cisco IMC info）]** パネルをクリックします。

ステップ 2 **[Cisco IMC 情報（Cisco IMC info）]** パネルで、 **[リセット（Reset）]**をクリックします。

（注）
このオプションは、管理者以外のユーザーのみが使用できます。

[パスワードの変更（Change Password）] ダイアログボックスが表示されます。

ステップ 3 **[パスワードの変更（Change Password）]** ダイアログ ボックスで、次のプロパティを更新します。

表 *105 :* パスワードを変更する

名前	説明
[ユーザ名（User Name）] フィールド	ユーザーの名前が表示されます。このフィールドは編集できません。
[ユーザー タイプ（User Type）] トグル ボタン	ユーザー タイプを表示します。これを無効にすると、パスワードを編集できません。
[現在のパスワード（Current Password）] フィールド	現在のパスワードを入力してください。
[新しいパスワード（New Password）] フィールド	新しいパスワードを入力します。
[Confirm New Password] フィールド	再度、新しいパスワードを入力します。
[**Save**] ボタン	クリックして新しいパスワードを保存します。

アカウントロックアウトの詳細の構成

手順

ステップ 1 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ユーザー管理（User Management）]** メニューをクリックします。

ステップ 3 **[アクション（Actions）]** ドロップダウン リストから、**[ユーザー管理（User Management）]** > **[アカウントロックアウトの詳細（Account Lockout Details）]**の順 に選択します。

[アカウント ロックアウトの詳細（Account Lockout Details）] ダイアログ ボックスが表示されます。

ステップ 4 **[ローカル ユーザーの詳細（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。

表 *106 :* アカウントロックアウトの詳細

名前	説明
[許可された試行（Allowed Attempts）] フィールド	誤ったパスワードでログイン試行が何回まで失敗できるかを設定できます。デフォルト値は 0 です（無効）。 0 ～ 20 の整数を入力します。

名前	説明
[ロックアウト期間（Lockout Period）] フィールド	ロックアウトする時間を分単位で設定できます。ロックアウトはログイン試行が許可される回数を超えた場合に発生します。デフォルト値は 0 です（無効）。 0 ～ 60 の整数を入力します。
[ロックアウト時にユーザーを無効化（Disable User on Lockout）] トグル ボタン	**[ロックアウト時にユーザーを無効化（Disable User on Lockout）]** チェックボックスがオンになっている場合、ユーザーアカウントはロックアウト時に無効になります。 （注） **ロックアウト時にユーザーを無効化は** 、デフォルトのユーザー（管理者）には適用されません。

リリース 6.0 以降、ユーザーが Cisco IMC にログインしようとしたときの、パスワードの入力の残りの試行回数は表示されなくなりました。また、ログイン時にアカウントがロックされているというメッセージも表示されなくなりました。管理者は、IMC 監査ログを参照して、試行回数とロックされたアカウントの詳細を知ることができます。

ユーザー認証の優先順位の構成

手順

ステップ 1 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ユーザー管理（User Management）]** メニューをクリックします。

ステップ 3 **[アクション（Actions）]** ドロップダウン リストから、**[ユーザー管理（User Management）]** > **[ユーザー認証の優先順位の設定（Configure User Authentication Precedence）]** の順に選択します。

[ユーザー認証の優先順位の設定（Configure User Authentication Precedence）] ダイアログ ボックスが表示されます。

ステップ 4 **[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。

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。

ステップ 5 次のプロパティを表示することができます：

表 *107* : ユーザー認証の優先順位

名前	説明
[データベース（Database）] チェックボックス	チェックボックスを使用して、目的のデータベースを選択します。
[Name] カラム	ユーザー データベース名。
[優先順位（Priority）] カラム	これにより、そのデータベースの優先順位が示されます。
上矢印ボタン	この矢印を使用して、データベースを優先順位リストの上に移動します。
下矢印ボタン	この矢印を使用して、データベースを優先順位リストの下に移動します。

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。

手順の概要

1. 管理者ユーザとしてログインします。
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。
3. [Chassis] メニューの [Summary] をクリックします。
4. ツールバーで、**[KVM の起動 (Launch KVM)]**をクリックします。
5. または、[Navigation] ペインの [Compute] メニューをクリックします。
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。
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。

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。
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。
10. F10 を押して設定を保存し、サーバを再起動します。

手順の詳細

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

Cisco CIMC 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 CIMC 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 Lightweight Directory Access Protocol（LDAP）をサポートします。さらに、Cisco CIMC 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 CIMC は LDAP での Kerberos ベースの認証サービスを利用します。

シスコ IMC で LDAP が有効になっている場合、ユーザ アカウントがローカル ユーザ データベース内に見つからないと、そのユーザ認証とロール許可は LDAP サーバ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 Settings] 領域で **[LDAP の有効化（Enable LDAP）]** チェックボックスをオンにすることで、LDAP サーバーへの送信データを暗号化するようサーバーに要求できます。

LDAP サーバの設定

Cisco IMC を設定して、LDAP をユーザーの認証と許可に使用できます。LDAP を使用するには、Cisco IMC のユーザー ロールとロケールを保持する属性を使用してユーザーを設定します。Cisco IMC のユーザー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 のユーザー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、LDAP 設定およびグループ承認の設定 （329 ページ） セクションに記載されている手順を実行します。

LDAP サーバー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 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 2 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（Value）]
共通名	**CiscoAVPair**
LDAP Display Name	**CiscoAVPair**
Unique X500 Object ID	**1.3.6.1.4.1.9.287247.1**

プロパティ	[値（Value）]
[説明（Description）]	**CiscoAVPair**
構文	**Case Sensitive String**

ステップ 3 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 4 Cisco IMC にアクセスできるようにするユーザーに対し、次のユーザー 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

LDAP サーバーを設定するには、Cisco IMC を使用します。

Cisco IMC 上の LDAP サーバーの設定

手順

ステップ 1 [Apps] ドロップダウンリストから、[Administration] を選択します。
ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ユーザー管理（User Management）]** メニューをクリックします。
ステップ 3 **[LDAP]** タブを選択します。
ステップ 4 **[LDAPサーバーの設定（Configure LDAP Servers）**] タブを選択します。
ステップ 5 次のいずれかの方法を使用して LDAP サーバーを構成できます。

- LDAPサーバの事前設定

- DNS を使用した LDAP サーバの設定

ステップ 6 **[LDAPサーバーの事前設定（Pre-Configure LDAP Servers）]** を使用して構成するには、ラジオ ボタンを選択して **[LDAPサーバーの追加（Add LDAP Server）]**をクリックします。

ステップ 7 次のプロパティを更新します。

表 *108 : LDAP* サーバーの構成：*LDAP* サーバーの事前構成

名前	説明
[LDAP サーバーの追加（Add LDAP Server）] ボタン	LDAP サーバーを追加できます。サーバーのリストに新しい行が追加されます。
[LDAP サーバー（LDAP Servers）] カラム	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。
[ポート（Port）] カラム	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。
[編集（Edit）] アイコン	LDAP サーバーの詳細を編集するには、それぞれの行のアイコンをクリックします。

ステップ 8 **[DNS を使用した LDAP サーバーの設定（Use DNS to Configure LDAP Servers）]**を使用して設定するには、ラジオ ボタンを選択して次のプロパティを更新します。

表 *109 : LDAP*サーバーの構成：*DNS*を使用して*LDAP*サーバーを構成する

名前	説明
[Source] ドロップダウンリスト	送信元を選択できます。次のいずれかを指定できます。 • 抽出済み • 設定済み（Configured） • 設定済み：抽出済み
[検索対象のドメイン（Domain to search for）] フィールド	この設定で、IMC が LDAP サーバーの検索に使用するドメイン名を指定します。設定すると、IMC は指定されたドメインの SRV レコードをドメイン ネーム システム（DNS）に照会して、LDAP サーバーを動的に検出します。
[検索するフォレスト（Forest to Search）] フィールド	この設定は、IMC が LDAP サーバーを検出するために検索する Active Directory（AD）フォレストを指定します。設定すると、IMC は DNS に指定されたフォレスト内の SRV レコードをクエリして、LDAP サーバーを動的に見つけます。

LDAP 設定およびグループ承認の設定

始める前に

この手順を実行するには、管理者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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ユーザー管理（User Management）]** メニューをクリックします。

ステップ 3 **[LDAP]** タブを選択します。

ステップ 4 **[LDAP 設定（LDAP Settings）]** タブを選択します。

ステップ 5 **[ユーザー設定（User Settings）]** 領域で、次のプロパティを更新します。

表 *110 : [*全般設定（*General Settings*）*]* 領域

名前	説明
[LDAP の有効化（Enable LDAP）] トグル ボタン	有効にすると、LDAPサーバによってユーザー認証とロール認可が最初に実行され、次にローカルユーザーデータベースにないユーザーアカウントについてこの認証と認可が実行されます。
[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。
[セキュア LDAP の有効化（Enable Secure LDAP）] トグル ボタン	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。 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。
[タイムアウト（サーバーごと）（Timeout（for each server））] ドロップダウン リスト	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した場合、Cisco IMCは、このタブにリストされている次のサーバへの接続を試みます(存在する場合)。 （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。

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。

表 *111* : *[*バインド パラメータ（***Binding Parameters***）*]*領域

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）]**：ユーザー名とパスワードを NULL にする必要があります。このオプションが選択され、LDAP サーバーで匿名ログインが設定されている場合は、ユーザー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、ユーザー名の識別名（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、ユーザーはアクセスを拒否されます。 • **[ログイン情報（Login Credentials）]**：ユーザーログイン情報が必要です。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。
[バインド DN（Bind DN）] フィールド	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。
[パスワード（Password）] フィールド	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。

表 *112 : [*検索パラメータ（*Search Parameters*）*]* 領域

名前	説明
[フィルタ属性（Filter Attribute）] フィールド	このフィールドは、LDAP サーバー上のスキーマの構成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）] フィールド	このフィールドは、LDAP サーバー上のスキーマの構成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、このフィールドには **[memberOf]** と表示されます。
[属性（Attribute）] フィールド	ユーザー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、ユーザー 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）。
[検索するグループのネスト レベル（Nested Group Search Depth）] フィールド	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） **[グループ承認（Group Authorization）]** エリアで、次のプロパティを更新します。

表 *113 : LDAP*グループ認証

名前	説明
[LDAP グループ認証（LDAP Group Authorization）] トグル ボタン	これを選択した場合、ローカル ユーザー データベースにない LDAP ユーザに関しても、グループ レベルでユーザー認証が実行されます。 このオプションをイネーブルにすると、Cisco IMC は **[グループの設定（Configure Group）]** ボタンをイネーブルにします。
[Group Name] カラム	サーバーへのアクセスが許可された LDAP サーバー データベース内のグループの名前。db 内のグループの名前

名前	説明
[Group Domain] カラム	グループを所属させる LDAP サーバ ドメイン。AD ドメイン

[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。これは、次のいずれかになります。[これらのユーザーのロール（Role for these users）]
	• [読み取りのみ（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。
	• [ユーザ（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
	• [管理者（admin）]：このロールのユーザは、GUI、CLI、IPMI で可能なすべてのアクションを実行できます。

[編集（Edit）] アイコン	新しい行を編集できます。設定が完了したら、**[保存（Save）]**をクリックします。
[削除（Delete）] ボタン	選択した LDAP グループを削除できます。

LDAP 証明書の概要

Cisco IMC では、LDAP クライアントが LDAP バインディング ステップでディレクトリ サーバーの証明書を、インストールされている CA 証明書またはチェーン CA 証明書と照合して検査できます。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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ユーザー管理（User Management）]** メニューをクリックします。

ステップ 3 **[LDAP]** タブを選択します。

ステップ 4 **[LDAP 設定（LDAP Settings）]** タブを選択します。

ステップ 5 **[LDAP CA 証明書ステータス（LDAP CA Certificate Status）]** 領域で、次のフィールドを確認します。

表 *114 : LDAP CA*証明書ステータス

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

この手順を実行するには、管理者ユーザー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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ユーザー管理（User Management）]** メニューをクリックします。

ステップ 3 **[アクション（Actions）]** ドロップダウンリストから、**[LDAP CA 証明書のエクスポート（Export LDAP CA Certificate）]** を選択します。

[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。

ステップ 4

ステップ 5 [エクスポート（Export）] をクリックします。

LDAP CA 証明書のアップロード

（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。

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。
- このアクションを実行するには、 **[セキュア LDAP の有効化（Enable Secure LDAP）]** を有効にする必要があります。

（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

ステップ 1 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ユーザー管理（User Management）]** メニューをクリックします。

ステップ 3 **[LDAP]** タブを選択します。

ステップ 4 **[LDAP 設定（LDAP Settings）]** タブを選択します。

ステップ 5 **[セキュアLDAPの有効化（Enable Secure LDAP）]** を有効にします。

[LDAP CA 証明書のアップロード（Upload LDAP CA Certificate）] ダイアログ ボックスが表示されます。

ステップ 6 **[LDAP CA 証明書のアップロード（Upload LDAP CA Certificate）]** ダイアログ ボックスで、次のプロパティを更新します。

表 *115* : リモート

名前	説明
リモート ボタン	このオプションは、証明書をリモート ロケーションからアップロードする場合に選択します。
サーバIP/ホスト名	証明書をアップロードする元のサーバーの詳細。
[Upload Protocol] ボタン	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。
[Path and Filename] フィールド	証明書ファイルのサーバーでのファイルパスとファイル名。
[Username] フィールド	リモートサーバのユーザー名。
[パスワード（Password）] フィールド	リモート サーバのパスワードです。
[アップロード（Upload）] ボタン	証明書をアップロードできます。

表 *116* : ローカル

名前	説明
[ローカル] ボタン	このオプションは、証明書をローカルマシンからアップロードする場合に選択します。 **[参照 (Browse)]** をクリックして、アップロードする証明書に移動します。
[アップロード（Upload）] ボタン	証明書をアップロードできます。

表 *117*: 貼り付け

名前	説明
[貼り付け（Paste）] ボタン	テキスト ボックスが開き、そこでルート CA 証明書の内容全体をコピーして、**[貼り付け（Paste）]** テキスト フィールドに貼り付けることができます。
[アップロード（Upload）] ボタン	証明書をアップロードできます。

LDAP バインディングのテスト

始める前に

この手順を実行するには、管理者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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ユーザー管理（User Management）]** メニューをクリックします。

ステップ 3 **[LDAP]** タブを選択します。

ステップ 4 **[LDAP 設定（LDAP Settings）]** タブを選択します。

ステップ 5 **[アクション（Actions）]** ドロップダウンリストから、**[ユーザー管理（User Management）]** > **[LDAP バインドのテスト（Test LDAP Binding）]**を選択します。

[LDAP バインドのテスト（Test LDAP Binding）] ダイアログ ボックスが表示されます。

ステップ 6 **[テスト（Test）]** をクリックします。

TACACS+ 認証

Cisco IMC は Terminal Access Controller Access-Control System Plus（TACACS+）認証をサポートしています。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 インターフェイスにも表示されます。

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も優先的にサポートします。

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+ サーバにー **[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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ユーザー管理（User Management）]** メニューをクリックします。

ステップ 3 **[TACACS+]** タブを選択します。

ステップ 4 **[TACACS+ プロパティ（TACACS+ Properties）]** 領域で、次のプロパティを更新します。

表 *118 : TACACS+*のプロパティ

名前	説明
[有効（Enabled）] トグル ボタン	有効にすると、TACACS+ベースのユーザー認証が行えます。

名前	説明
[接続がない場合にのみフォールバック（Fallback only on no connectivity）] トグル ボタン	有効になっている場合、Cisco IMCが設定済みのいずれのTACACS+サーバーにも接続できない場合、次の優先データベースへの認証のフォールバックが実行されます。
[タイムアウト（サーバーごと）：（5 ～ 30）秒（Timeout (for each server): (5 - 30) seconds）] ドロップダウン リスト	Cisco IMC が各 TACACS+ サーバーからの応答を待機する時間（秒単位）

ステップ 5 [保存（Save）] をクリックします。

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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ユーザー管理（User Management）]** メニューをクリックします。

ステップ 3 **[TACACS+]** タブを選択します。

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 ID の **[編集（Edit）]** アイコ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。

表 *119 :* サーバー リスト（*Server List*）

名前	説明
[ID] カラム	この TACACS+ サーバーに与える必要のある優先順位。サーバーの固有識別子でもあります。
[IPアドレスまたはホスト名（IP Address or Host Name）] カラム	TACACS+ サーバーが稼働している IP アドレス。
[ポート（Port）] カラム	TACACS+ サーバーが稼働しているポート。
[サーバー キー（Server key）] カラム	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）] カラム	サーバー キーを再度入力します。

ステップ 6 [保存（Save）] をクリックします。

ユーザー セッションの表示と終了

手順

ステップ 1 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ユーザー管理（User Management）]** メニューをクリックします。

ステップ 3 **[セッション管理（Sessions Management）]** タブを選択します。

ステップ 4 現在のユーザー セッションに関する次の情報が表示されます。

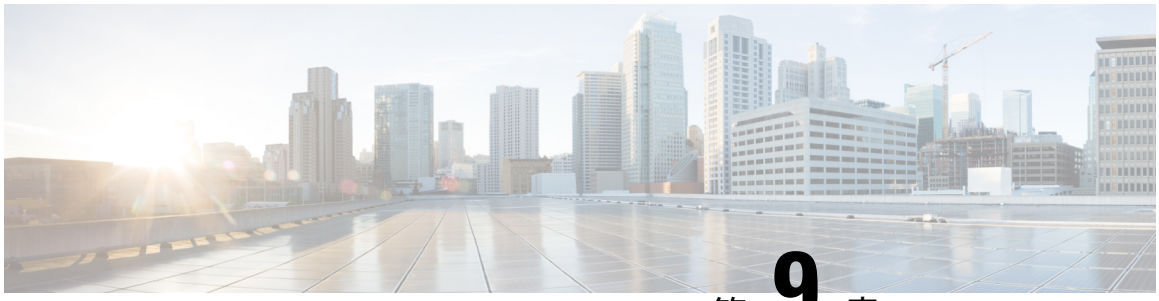
ヒント
カラムの見出しをクリックすると、そのカラムのエントリに従って表の行がソートされます。

表 *120 :* セッション管理

名前	説明
[Session ID] カラム	セッションの固有識別情報。
[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。
[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。

名前	説明
[Description] カラム	セッションの簡単な説明。
[セッションを終了（Terminate Session）] ボタン	ユーザーセッションを終了します、 テーブルからセッションを選択し、**[セッションを終了（Terminate Session）]**をクリックします。[OK] をクリックして続行します。

ステップ 5 セッションを終了するには、テーブルからセッションを選択し、**[セッションの終了（Terminate Session）]** をクリックします。[OK] をクリックして続行します。



第 9 章

シャーシ関連の設定の指定

•
• サーバの電源管理 （343 ページ）
• Web UI からのホスト名/IP アドレスの ping （344 ページ）
• ロケータ LED の切り替え （345 ページ）
• 時間帯の選択 （345 ページ）

サーバの電源管理

始める前に

この手順を実行するには、管理者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 **[アプリ（Apps）]** ドロップダウン リストから、**[ダッシュボード（Dashboard）]** を選択します。

ステップ 3 [アクション（Actions）] ドロップダウン メニューから、**[電源（Power）]** を選択します。

ステップ 4 電源オプションを選択し、次の詳細情報に従ってアクティビティを実行します。

表 *121* : 電源オプション

名前	説明
Power Off	サーバーの電源をオフにできます。**[電源オフ（Power Off）]** をクリックして続行します。
電源オン	サーバーの電源をオンにできます。
Power Cycle	サーバーの AC 電源のパワー サイクルを実行できます。**[パワー サイクル（Power Cycle）]** をクリックして続行します。

名前	説明
Hard Reset	サーバーを工場出荷時の設定にリセットできます。**[ハード リセット（Hard Reset）]** をクリックして続行します。
Shut Down	サーバーのグレースフル シャット ダウンを実行します。**[シャットダウン（Shut Down）]** をクリックして続行します。

Web UI からのホスト名/IP アドレスの ping

始める前に

この手順を実行するには、管理者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 **[アプリ（Apps）]** ドロップダウン リストから、**[ダッシュボード（Dashboard）]** を選択します。

ステップ 2 [アクション（Actions）] ドロップダウン メニューから、**[システム（System）]** > **[Ping]**を選択します。

ステップ 3 **[Ping の詳細（Ping Details）]** ダイアログ ボックスで、次の表に示す詳細に従ってアクティビティを実行します。

名前	説明
[Management IP Address] フィールド	到達するホスト名または IP アドレス。
[Number of Retries] ドロップダウン リスト	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（秒）（Timeout（in seconds））] ドロップダウン リスト	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。
Pingのステータス	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 アドレスの ping アクションを実行します。

ステップ 4 **[Ping]**をクリックします。

ロケータ LED の切り替え

始める前に

この手順を実行するには、管理者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 **[アプリ（Apps）]** ドロップダウン リストから、**[ダッシュボード（Dashboard）]** を選択します。

ステップ 2 [アクション（Actions）] ドロップダウン メニューから、**[システム（System）]** > **[LEDのオン/オフ（Turn On/Off LED）]**を選択します。

ステップ 3 操作に応じて、[Chassis Status] 領域の LED インジケータが点灯し、サーバーの物理ロケータ LED がオンまたはオフになり、点滅します。
[LED をオンにする（Turn On LED）] を選択すると、物理ドライブ上のロケータの LED がオンになります。

[LED をオフにする（Turn Off LED）] を選択すると、物理ドライブ上のロケータの LED がオフになります。

時間帯の選択

始める前に

このタスクを実行するには、admin 権限でログインする必要があります。

手順

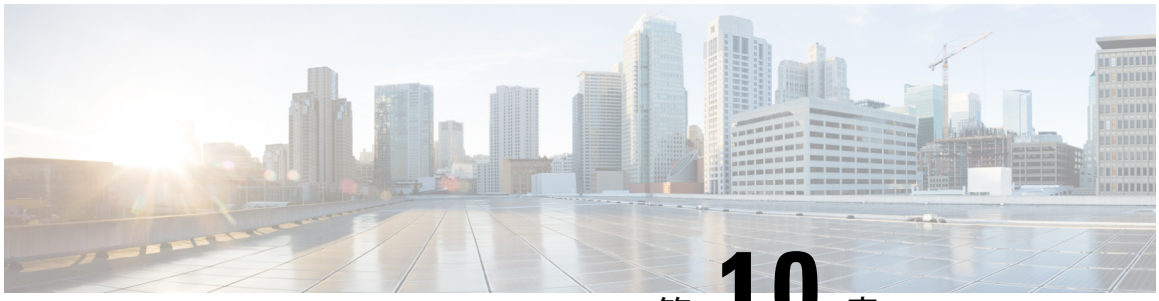
ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ダッシュボード（Dashboard）]** を選択します。

ステップ 2 **[CIMC 情報（CIMC Information）]** 領域で、**[タイムゾーン（Timezone）]** フィールドの下の値をクリックします。

[タイムゾーンの選択（Select Timezone）]画面が表示されます。

ステップ 3 **[タイムゾーンの選択（Select Timezone）]** ドロップダウン リストから必要なタイム ゾーンを選択するか、地図にマウスを合わせてクリックし、タイム ゾーンを選択します。

ステップ 4 [保存（Save）] をクリックします。



第 10 章

ネットワーク関連の設定

•
• ネットワーク関連の設定 （347 ページ）
• サーバー NIC （347 ページ）
• サーバ NIC の設定 （351 ページ）
• Cisco VIC mLOM および OCP カードの交換に関する考慮事項 （357 ページ）
• 単一 IP の設定 （359 ページ）
• 共通プロパティの設定 （360 ページ）
• IPv4 の設定 （362 ページ）
• IPv6 の設定 （363 ページ）
• VLAN への接続 （365 ページ）
• ネットワーク セキュリティの設定 （365 ページ）
• Network Time Protocol の設定 （367 ページ）

ネットワーク関連の設定

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：

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 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 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、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の、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、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の、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 M5 SD 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 2（Riser 2）]：スロット 2 が選択されます。
- **[mLOM]**：mLOM スロットの VIC カードが選択されています。

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 **[アプリ（Apps）]** ドロップダウン リストから、**[ネットワーキング（Networking）]** を選択します。
ステップ 2 [Apps] ドロップダウンリストから、[Administration] を選択します。
ステップ 3 **[管理（Administration）]** ページで、**[ネットワーキング（Networking）]** を選択します。
ステップ 4 **[ネットワーキング（Networking）]** タブで **[ネットワーク（Network）]**を選択します。
ステップ 5 [NIC Properties] 領域で、次のプロパティを更新します。

表 *122 : [NIC Properties]* 領域

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、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。 • **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。 **デフォルトのNICモード設定**： • UCS C シリーズ 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。

名前	説明
	• 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。
[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。 C240 M7 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 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 の場合、工場出荷時のデフォルト設定にリセットすると、スロットの優先順位は次のようになります。 **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 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 3 (Riser 3)]**：スロット 3 が選択されます。 • **mLOM** （注） C220 M7 の場合、工場出荷時のデフォルト設定にリセットすると、スロットの優先順位は次のようになります。 **1.** mLOM **2.** ライザー 1 ：スロット 1 **3.** ライザー 3 ：スロット 3

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。 • [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 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。
[Port Profile] フィールド	Cisco IMC など、サポートされているアダプタ カード上の管理インターフェイス、仮想イーサネット、VIF を設定するために Cisco UCS VIC 1223 仮想インターフェイスが使用するポート プロファイル。 最大 79 文字の英数字を入力します。-（ハイフン）と _（アンダースコア）を除き、スペースなどの特殊文字は使用できません。ポート プロファイル名をハイフンで始めることもできません。 （注） ポート プロファイルは、このサーバが接続されているスイッチに定義されている必要があります。

名前	説明
[自動ネゴシエーション（Auto Negotiation）] トグル ボタン	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。 • 有効にした場合、ネットワーク ポート速度とデュプレックス設定は無視され、Cisco IMC はスイッチに設定された速度を保持します。 • 無効にすると、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。
[ネットワーク ポート速度（Network Port Speed）] ドロップダウン リスト	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。

ステップ 6 [保存（Save）] 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 M8 および C245 M8 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 サーバの Cisco VIC mLOM または OCP カードを交換し、接続を失わないようにする場合は、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 で起動します。

     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 *123 :* 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
○	非対応	非対応	○	mLOM スロットのカードを使用する **Cisco Card** モード
非対応	○	非対応	○	**Shared OCP Extended**
非対応	○	○	○	**Shared OCP Extended**
非対応	非対応	○	○	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 M8 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 M8 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
非対応	非対応	非対応	○	**専用**

単一 IP の設定

単一 IP は、Cisco IMC 管理に IPv4 を割り当てるオプションの方法です。

（注） **[単一 IP モード（Single IP Mode）]** が有効になっている場合、次の IPv4 は設定に使用できません。

CMC および BMC

1 つの IP モードは、IPv4、IPv6 にのみ適用されるため、IPv6 は **1 つの IP モード**に関係なく設定できます。

IPv6 アドレスは、CMC1、CMC2、BMC1、および BMC2 などの個々のコンポーネントを割り当てることができます。

（注） 4.0.1x 以下にダウングレードする前に単一 IP 設定を無効にしてください。

単一 IP プロパティの設定

Cisco IMC 管理の IP を割り当てる場合は、単一 IP プロパティを設定します。

始める前に

単一 IP プロパティを設定するには、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 [単一IPプロパティ（Single IP Properties）] 領域で、次のプロパティを更新します。

名前	説明
単一 IP モード	単一 IP は、Cisco IMC 管理に IPv4 を割り当てるオプションの方法です。 （注） **[Single IP Mode]** が有効になっている場合、次の IPv4 は設定に使用できません。 CMC および BMC。 **1 つの IP モード**は、IPv4、IPv6 にのみ適用されるため、IPv6 は **1 つの IP モード**に関係なく設定できます。IPv6 アドレスは、CMC1、CMC2、BMC1、および BMC2 などの個々のコンポーネントを割り当てることができます。 デフォルト モード：**Disabled**
開始ポート	[単一IPモード（Single IP Mode）]が有効になっている場合、使用可能なポートの範囲は 9000 ~ 65529 です。 （注） Cisco IMC で KVM、SOL、および各コンポーネントの IPMI Over LAN にアクセスするために使用するポート番号を持つコンポーネントの一覧表を参照するには、**[Starting Port]** の隣にあるヘルプ アイコンをクリックします。

（注）
単一 IP モードでは、vkvm ポートは設定可能ではなく、デフォルトの **2068** からユーザに割り当てられたポートに変更されます。

ステップ 4 [Save Changes] をクリックします。

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、 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 [Apps] ドロップダウンリストから、[Administration] を選択します。
ステップ 2 **[管理（Administration）]** ページで、**[ネットワーキング（Networking）]** を選択します。
ステップ 3 **[ネットワーキング（Networking）]** タブで **[ネットワーク（Network）]**を選択します。
ステップ 4 右側ペインの **[VLAN のプロパティ（VLAN Properties）]** 領域で、次のプロパティを更新します。

表 *124 : [Common Properties]* 領域

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。
[ダイナミックDNS（Dynamic DNS）] トグルボタンを有効にします。	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。

ステップ 5 [保存（Save）] 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 [Apps] ドロップダウンリストから、[Administration] を選択します。
ステップ 2 **[管理（Administration）]** ページで、**[ネットワーキング（Networking）]** を選択します。
ステップ 3 **[ネットワーキング（Networking）]** タブで **[ネットワーク（Network）]**を選択します。
ステップ 4 [IPv4 Properties] 領域で、次のプロパティを更新します。

表 *125 : [IPv4 Properties]* 領域

名前	説明
[IPv4 の有効化（Enable IPv4）] トグル ボタン	オンにすると、IPv4 が有効になります。
DHCP トグル ボタン	有効にすると、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。BMC を管理する際に利用できる外部仮想 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。
[IPv4 ゲートウェイ（IPv4 Gateway）] フィールド	IP アドレスのゲートウェイ。
[DHCP から DNS サーバアドレスを取得（Obtain DNS Server Addresses from DHCP）] トグル ボタン	有効にすると、Cisco IMCはDNSサーバアドレスをDHCPから取得します。
[IPv4 優先 DNS サーバー（IPv4 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 5 [保存（Save）] 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 [Apps] ドロップダウンリストから、[Administration] を選択します。
ステップ 2 **[管理（Administration）]** ページで、**[ネットワーキング（Networking）]** を選択します。
ステップ 3 **[ネットワーキング（Networking）]** タブで **[ネットワーク（Network）]**を選択します。
ステップ 4 [**IPv6 Properties**] 領域で、次のプロパティを更新します。

表 *126 : [IPv6* プロパティ（*IPv4 Properties*）*]* 領域

名前	説明
[IPv6 の有効化（Enable IPv6）] トグル ボタン	オンにすると、IPv6 が有効になります。
[DHCP 使用（Use DHCP）] トグル ボタン	有効にすると、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。
[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。
[IPv6 ゲートウェイ（IPv6 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。
[DHCP から DNS サーバアドレスを取得（Obtain DNS Server Addresses from DHCP）] トグル ボタン	有効にすると、Cisco IMC は DNS サーバアドレスを 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。
[IPv6 優先 DNS サーバー（IPv6 Preferred DNS Server）] フィールド	プライマリ DNS サーバの IPv6 アドレス。
[IPv6 代替 DNS サーバー（IPv6 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。
[ステートレスアドレスの自動設定（Stateless Address Auto Configuration）] 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 5 [保存（Save）] 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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[管理（Administration）]** ページで、**[ネットワーキング（Networking）]** を選択します。

ステップ 3 **[VLAN のプロパティ（VLAN Properties）]** 領域で、次のプロパティを更新します。

表 *127 : [VLAN Properties]* 領域

名前	説明
[VLAN の有効化（Enable VLAN）] トグル ボタン	有効にすると、Cisco IMC 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 [保存（Save）] 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、サービス拒絶（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 **[アプリ（Apps）]** ドロップダウン リストから、**[ネットワーキング（Networking）]** を選択します。

ステップ 2 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 3 **[管理（Administration）]** ページで、**[ネットワーキング（Networking）]** を選択します。

ステップ 4 **[ネットワーキング（Networking）]** タブから、**[設定（Settings）]**を選択します。

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

表 *128 : [IP* ブロッキング プロパティ（*IP Blocking Properties*）*]* 領域

名前	説明
[IP ブロッキングの有効化（Enable IP Blocking）] トグル ボタン	IP ブロッキング機能を有効または無効にすることができます。
[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。
[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。

ステップ 6 **[IP フィルタリング（リスティング可能）（IP Filtering (Allow listing)）]** 領域で、次のプロパティを更新します。

表 *129 : [IP* フィルタリング（*IP Filtering*）*]* 領域

名前	説明
[IP フィルタリングの有効化（Enable IP Filtering）] トグル ボタン	IP フィルタリング機能を有効または無効にすることができます。
[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 7 [保存（Save）] 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 サーバーと時刻を同期することができます。デフォルトでは、Cisco IMC では NTP サーバーは動作しません。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 経由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

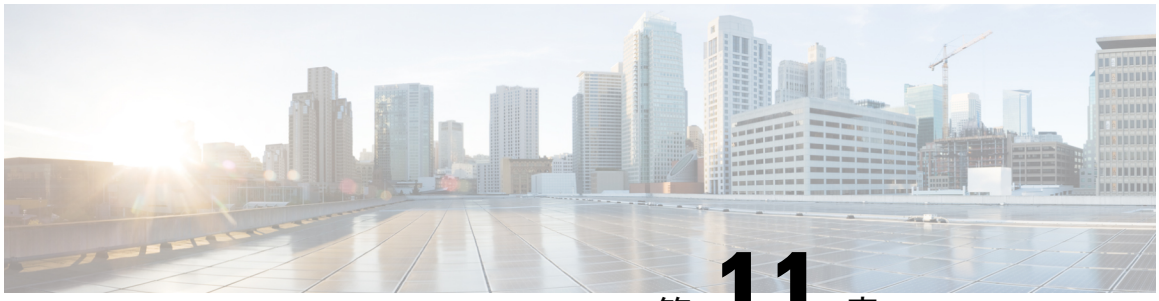
手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ネットワーキング（Networking）]** を選択します。
ステップ 2 [Apps] ドロップダウンリストから、[Administration] を選択します。
ステップ 3 **[管理（Administration）]** ページで、**[ネットワーキング（Networking）]** を選択します。
ステップ 4 **[ネットワーキング（Networking）]** タブから、**[設定（Settings）]**を選択します。
ステップ 5 **[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。

表 *130 : [NTP* プロパティ（*NTP Properties*）*]* エリア

名前	説明
[NTP の有効化（Enable NTP）] トグルボタン	NTP サービスを有効または無効にすることができます。
[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	NTP が有効の場合、このフィールドは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 6 [保存（Save）] をクリックします。



第 11 章

ネットワーク アダプタの管理

•
• Cisco UCS C シリーズ ネットワーク アダプタの概要 （369 ページ）
• Cisco UCS ネットワーク アダプタのプロパティの表示 （372 ページ）
• vHBA の管理 （382 ページ）
• vNIC の管理 （401 ページ）
• アダプタ設定のバックアップと復元 （444 ページ）

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 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 仮想インターフェイス カード

（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。ユーティリティは次の URL から入手できます。 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 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

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 サーバー専用に設計された、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、サーバー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 サーバーに提供します。

Cisco UCS P81E 仮想インターフェイス カード

Cisco UCS P81E 仮想インターフェイス カードは、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。

Cisco UCS ネットワーク アダプタ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。
- 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 **[アプリ（Apps）]** ドロップダウン リストから、**[ネットワーキング（Networking）]** を選択します。
ステップ 2 [全般（**General**）] タブを選択します。

ステップ 3 **[プロパティ（Properties）]** 領域で、次の情報を確認します。

表 *131 :* プロパティ領域

名前	説明
[PCI スロット（PCI Slot）]	アダプタが装着されている PCI スロット。
ベンダー	アダプタのベンダー。
製品名	アダプタの製品名。
製品ID	アダプタの製品 ID。
シリアル番号（Serial Number）	アダプタのシリアル番号。
バージョンID	アダプタのバージョン ID。
ハードウェアリビジョン	アダプタのハードウェア リビジョン。
[Cisco IMC 管理有効（Cisco IMC Management Enabled）]	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。
[設定保留中（Configuration Pending）]	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）]	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）]	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）]	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。
実行されているバージョン	現在有効なファームウェア バージョン。

名前	説明
バックアップ バージョン	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。
スタートアップ バージョン	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。
ブートローダーのバージョン	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。
ステータス（Status）	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。

[Settings] 領域で、次の情報を確認します。

表 *132 : [Settings]* 領域

名前	説明
[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。
[FIP モードの有効化（Enable FIP Mode）] トグルボタン	FCoE Initialization Protocol（FIP）を有効または無効にすることができます。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
[LLDP の有効化（Enable LLDP）] トグルボタン	（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。 有効にすると、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。
[VNTAG モードの有効化（Enable VNTAG Mode）] トグル ボタン	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。
[ポート チャネル（Port Channel] トグルボタン	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）] トグル ボタン	

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。 （注） リリース 4.3(6) 以降では、 **物理 NIC モード** が有効になっている場合、Cisco IMC ユーザー インター

名前	説明
	フェイスを使用してデフォルトの vLAN を作成することはできません。
[送信拡張モード（Transmit Enhanced Mode）] トグル ボタン	1500 バイトのパケットの場合に、送信側の TCP パフォーマンスを向上させます。

ステップ 4 **[DCE インターフェイス（DCE Interfaces）]** タブを選択します。

ステップ 5 次の情報を確認できます。

表 *133 : DCE*インターフェイス

名前	説明
[Port] カラム	アップリンク ポート ID。
[MAC Address] カラム	アップリンク ポートの MAC アドレス。
[リンクステータス（Status）] カラム	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]** • **アップ** • **ダウン** • **[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。

名前	説明
[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。
[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。 • **1 Gbps** • **10 Gbps** • **25Gbps** • **[40 Gbps]** • **50 Gbps** • **100 Gbps** • **[4 X 10 Gbps]** • **自動**

名前	説明
[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。 • **1 Gbps** • **10 Gbps** • **[40 Gbps]** • **[4 X 10 Gbps]** • **自動** （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。
[FECモードの管理（Admin FEC Mode）] カラム	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。

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 **[自動（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。

名前	説明
[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。 • QSFP-100G-LR4-S トランシーバの場合、値は**オフ**です。 • QSFP-40/100-SRBD トランシーバの場合、値は**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。
[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。

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 つの vHBA と4 つの vNIC 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と変更

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ネットワーキング（Networking）]** を選択します。

ステップ 2 **[vHBA インターフェイス（vHBA Interfaces）]** タブを選択します。

ステップ 3 vHBA のリストから、プロパティを表示または変更する vHBA をクリックします。

ステップ 4 **[全般設定（General Settings）]** タブで、次のプロパティを確認または変更します。

表 *134 :* 設定

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 WWWN（Initiator WWNN）] トグル ボタンとフィールド	vHBA に関連付けられた WWNN。 システムで WWNN を生成するには、**[イニシエータ WWWN（Initiator WWNN）]** を無効にします。WWNN を指定するには、**[イニシエータ WWWN（Initiator WWNN）]** を有効にし、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）] トグル ボタンとフィールド	vHBA に関連付けられた WWPN。 システムで WWPN を生成するには、**[イニシエータ WWPN（Initiator WWPN）]** を無効にします。WWPN を指定するには、**[イニシエータ WWPN（Initiator WWPN）]** を有効にし、対応するフィールドに WWPN を入力します。

名前	説明
[PCI Order] フィールド	この vHBA が使用される順序。 0 ～ 17 の整数を入力します。
[MAC アドレス（MAC Address）] トグルボタンとフィールド	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、**[MAC アドレス（MAC Address）]** を無効にします。MAC アドレスを指定するには、**[MAC アドレス（MAC Address）]** を有効にし、対応するフィールドに MAC アドレスを入力します。
[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。 • [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。
[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。
[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。
[デフォルト VLAN（Default VLAN）] トグル ボタンとフィールド	この vHBA のデフォルト VLAN がない場合は、**[デフォルト VLAN（Default VLAN）]** を無効にします。そうでなければ、**[デフォルト VLAN（Default VLAN）]** を有効にして、フィールドに 1 ～4094 の VLAN ID を入力します。
[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。
[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、Cisco UCS 14xx シリーズ VIC アダプタと Cisco UCS 15428 VIC 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
[PCI リンク（PCI Link）] フィールド	これは読み取り専用フィールドです。
[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。

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。
[レート制限（Rate Limit）] トグル ボタンとフィールド	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、**[レート制限（Rate Limit）]** を無効にします。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。

ステップ 5 **[詳細設定（Advanced Settings）]** タブで、次のプロパティを確認または変更します。

表 *135 : [Error Recovery]* 領域

名前	説明
[FCP エラー リカバリ（FCP Error Recovery）] トグル ボタン	有効になっている場合、FCP Sequence Level Error Recovery (FC-TAPE)プトロコルが使用されます。
[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
[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。
[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。
[FLOGI 再試行（FLOGI Retries）] トグルボタンとフィールド	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、**[FLOGI Retries]** を有効ににします。それ以外の場合は、**[FLOGI 再試行（FLOGI Retries）]** を無効にして、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。
[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。

表 *136 :* ファイバチャネルポート

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 ～ 1024 の整数を入力します。

名前	説明
[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。 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。 1 ～ 254 の整数を入力します。
[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。 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。
[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 6 **[ブート テーブル（Boot Table）**] タブで、次のプロパティを確認または変更します。

表 *137 :* ブートテーブル

名前	説明
[FC SAN ブート（FC SAN Boot）] トグル ボタン	オンにすると、vHBA を使用して SAN ブートを実行できます。
[Add Boot Entry] ボタン	ブート テーブルに新しいエントリを追加します。
[ブート エントリの削除（Delete Boot Entry）] ボタン	選択したブート テーブル行エントリを削除できます。
[ID] カラム	このフィールドのデフォルト値は **0** です。

名前	説明
[ターゲット WWPN（Target WWPN）] カラムとフィールド	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] カラムとフィールド	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。
[編集（Edit）] アイコン	選択したブート テーブル行の **[ターゲット WWPN（Target WWPN）]** および **[LUN ID]** を編集できます。

ステップ 7 **[永続バインド（Persistent Bindings）]** タブで、次のプロパティを確認または変更します。

表 *138* : 永続的バインディング

名前	説明
[永続的 LUN バインディング（Persistent LUN Bindings）] トグル ボタン	**永続的 LUN バインディング**を有効にできます。
[Reset] ボタン	工場出荷時の設定にリセットできます。
[**Save**] ボタン	**[永続的 LUN バインディング（Persistent LUN Bindings）**] の設定を変更した後、設定を保存します。
[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。
[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。

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 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 つの vHBA と4 つの vNIC 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

[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 **[アプリ（Apps）]** ドロップダウン リストから、**[ネットワーキング（Networking）]** を選択します。

ステップ 2 **[アクション（Actions）]** ドロップダウンリストから、**[vNIC]**>**[仮想 HBA インターフェイスの作成（Create Virtual NIC Interface）]**を選択します。

[vHBA の追加（Add vHBA）] ダイアログ ボックスが表示されます。

ステップ 3 **[Cisco vNIC Adapter の選択（Select Cisco vNIC Adapter）]** で、次のプロパティを更新し、**[次へ（Next）]** をクリックします。

表 *139 : Cisco VIC*アダプタの選択

名前	説明
[スロット（Slot）] ドロップダウン リスト	VIC スロットを選択できます。 （注） 使用可能なスロットが 1 つだけの場合、このオプションはグレー表示されます。
[次へ（Next）] ボタン	[次へ（Next）] をクリックして続行します。

ステップ 4 **[全般設定（General Settings）]** で、次のプロパティを更新し、**[次へ（Next）]**をクリックします。

表 *140 :* 一般設定

名前	説明
[名前（Name）] フィールド	ユーザー定義の名前を入力できます。
[PCIe 順序（PCIe Order）] フィールド	これは vHBA が使用される順序です。0 ～ 4 の整数を入力します。

名前	説明
[Uplink Port] ドロップダウン リスト	このvHBAに関連付けられているアップリンクポート。このvHBAの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。0 または 1 を選択します。
[Channel Number] フィールド	この vHBA に割り当てるチャネル番号を選択します。1 ～ 1000 の整数を入力します。
[詳細オプション（Advance Options）] トグル ボタン	詳細プロパティを更新するには、これを有効にします。 （注） 他のすべてのプロパティは、**[詳細オプション（Advance Options）]** が有効になっている場合にのみ表示されます。
[イニシエータ WWWN（Initiator WWNN）] トグル ボタンとフィールド	vHBA に関連付けられた WWNN。 システムで WWNN を生成するには、**[イニシエータ WWWN（Initiator WWNN）]** を無効にします。WWNN を指定するには、**[イニシエータ WWWN（Initiator WWNN）]** を有効にし、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）] トグル ボタンとフィールド	vHBA に関連付けられた WWPN。 システムで WWPN を生成するには、**[イニシエータ WWPN（Initiator WWPN）]** を無効にします。WWPN を指定するには、**[イニシエータ WWPN（Initiator WWPN）]** を有効にし、対応するフィールドに WWPN を入力します。
[FC SAN ブート（FC SAN Boot）] トグル ボタン	オンにすると、vHBA を使用して SAN ブートを実行できます。
[永続的 LUN バインディング（Persistent LUN Bindings）] トグル ボタン	有効になっている場合、手動でクリアするまで、LUN IDアソシエーションはメモリに保存されます。
[MAC アドレス（MAC Address）] トグルボタンとフィールド	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、**[MAC アドレス（MAC Address）]** を無効にします。MAC アドレスを指定するには、**[MAC アドレス（MAC Address）]** を有効にし、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
[デフォルト VLAN（Default VLAN）] トグル ボタンとフィールド	この vHBA のデフォルト VLAN がない場合は、**[デフォルト VLAN（Default VLAN）]** を無効にします。そうでなければ、**[デフォルト VLAN（Default VLAN）]** を有効にして、フィールドに 1 ～4094 の VLAN ID を入力します。
[レート制限（Rate Limit）] トグル ボタンとフィールド	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、**[レート制限（Rate Limit）]** を無効にします。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。
[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。

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、Cisco UCS 14xx シリーズ VIC アダプタと Cisco UCS 15428 VIC 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 • 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。
[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。

名前	説明
[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。
[PCI リンク（PCI Link）] フィールド	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 5 **[エラー リカバリ（Error Recovery）]**で次のプロパティを更新し、**[次へ（Next）]**をクリックします。

表 *141* : エラーリカバリ

名前	説明
[FCP エラー リカバリ（FCP Error Recovery）] トグル ボタン	有効になっている場合、FCP Sequence Level Error Recovery (FC-TAPE)プトロコルが使用されます。
[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。
[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。

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。

ステップ 6 **[ファイバ チャネル ポート（Fibre Channel Port）]**で、次のプロパティを更新し、**[次へ（Next）]**をクリックします。

表 *142 :* ファイバチャネルポート

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 ～ 1024 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。 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。 1 ～ 254 の整数を入力します。
[FLOGI 再試行（FLOGI Retries）] トグルボタンとフィールド	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、**[FLOGI Retries]** を有効ににします。それ以外の場合は、**[FLOGI 再試行（FLOGI Retries）]** を無効にして、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。
[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。

名前	説明
[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 7 **[I/O 送受信（I/O Receive & Transmit）]**で、次のプロパティを更新して **[次へ（Next）]**をクリックします。

表 *143 : I/O*受信および送信キュー

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。 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。
[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 8 **[サマリー（Summary）]** で、情報を確認し、**[保存（Save）]**をクリックします。

次のタスク

- サーバをリブートして vHBA を作成します。

vHBA の複製

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ネットワーキング（Networking）]** を選択します。

ステップ 2 **[vHBA インターフェイス（vHBA Interfaces）]** タブを選択します。

ステップ 3 複製する vHBA インターフェイスを選択し、 **[vHBA の複製（Clone vHBA）]** ボタンをクリックします。

[vHBA の複製（Clone vHBA）] ダイアログ ボックスが表示されます。

ステップ 4 **[vHBA の複製（Clone vHBA）]** ダイアログ ボックスで次のプロパティを更新します。

表 *144 :* クローン*vHBA*

名前	説明
[名前（Name）] フィールド	ユーザー定義の名前を入力できます。
[Uplink Port] ドロップダウン リスト	このvHBAに関連付けられているアップリンクポート。このvHBAの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。0 または 1 を選択します。
[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、Cisco UCS 14xx シリーズ VIC アダプタと Cisco UCS 15428 VIC 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 • 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
[PCIe 順序（PCIe Order）] フィールド	これは vHBA が使用される順序です。0 ～ 4 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を選択します。1 ～ 1000 の整数を入力します。

ステップ 5 **[[vHBA の複製（Clone vHBA）]]** をクリックして変更を保存します。

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 **[アプリ（Apps）]** ドロップダウン リストから、**[ネットワーキング（Networking）]** を選択します。

ステップ 2 **[vHBA インターフェイス（vHBA Interfaces）]** タブを選択します。

ステップ 3 削除する **vHBA インターフェイス** を選択し、**[vHBA の削除（Delete vHBA）]** ボタンをクリックします。

（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 4 [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 **[アプリ（Apps）]** ドロップダウン リストから、**[ネットワーキング（Networking）]** を選択します。

ステップ 2 **[vHBA インターフェイス（vHBA Interfaces）]** タブを選択します。

ステップ 3 vHBA のリストから、ブート テーブルを表示または変更する対象の vHBA をクリックします。

ステップ 4 **[ブート テーブル（Boot Tables）]** タブを選択します。

ステップ 5 **[ブート エントリの追加（Add Boot Entry）]** ボタンをクリックします。

これにより、ブート エントリ テーブルに新しいエントリが追加されます。

ステップ 6 **[ブート エントリの追加（Add Boot Entry）]** テーブルで編集アイコンをクリックし、次のプロパティを更新します。

名前	説明
[ターゲット WWPN（Target WWPN）] カラムとフィールド	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] カラムとフィールド	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。

ステップ 7 [保存（Save）] をクリックします。

ブート テーブル エントリの削除

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ネットワーキング（Networking）]** を選択します。
ステップ 2 **[vHBA インターフェイス（vHBA Interfaces）]** タブを選択します。
ステップ 3 vHBA のリストから、ブート テーブルを表示または変更する対象の vHBA をクリックします。
ステップ 4 **[ブート テーブル（Boot Tables）]** タブを選択します。
ステップ 5 ブート エントリ テーブルから、削除するエントリを選択します。
ステップ 6 **[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。

永続バインディングの表示と有効化

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ネットワーキング（Networking）]** を選択します。
ステップ 2 **[vHBA インターフェイス（vHBA Interfaces）]** タブを選択します。
ステップ 3 vHBA のリストから、ブート テーブルを表示または変更する対象の vHBA をクリックします。
ステップ 4 **[永続的バインディング（Persistent Binding）]** タブを選択します。

ステップ 5 **[永続バインディング（Persistent Bindings）]** タブで、次のプロパティを確認または変更します。

表 *145 :* 永続的バインディング

名前	説明
[永続的 LUN バインディング（Persistent LUN Bindings）] トグル ボタン	**永続的 LUN バインディング**を有効にできます。
[Reset] ボタン	工場出荷時の設定にリセットできます。
[**Save**] ボタン	**[永続的 LUN バインディング（Persistent LUN Bindings）**] の設定を変更した後、設定を保存します。
[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。
[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。

永続的なバインディングの再作成

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ネットワーキング（Networking）]** を選択します。
ステップ 2 **[vHBA インターフェイス（vHBA Interfaces）]** タブを選択します。
ステップ 3 vHBA のリストから、ブート テーブルを表示または変更する対象の vHBA をクリックします。
ステップ 4 **[永続的バインディング（Persistent Binding）]** タブを選択します。
ステップ 5 [Rebuild Persistent Bindings] ボタ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。

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 つの vHBA と4 つの vNIC 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 プロパティの表示と変更

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ネットワーキング（Networking）]** を選択します。

ステップ 2 **[vNIC インターフェイス（vNIC Interfaces）]** タブを選択します。

ステップ 3 vNIC のリストから、プロパティを表示または変更する vNIC をクリックします。

ステップ 4 **[全般設定（General Settings）]** タブで、次のプロパティを確認または変更します。

表 *146 : [Settings]* 領域

名前	説明
[名前（Name）] フィールド	仮想ネットワーク インターフェイス カード（vNIC）の名前。 デフォルトの vNIC の名前は変更できません。

名前	説明
[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。
[VLAN Mode] ドロップダウン リスト	関連付けられた VLAN のモード。次のいずれかになります。 • トランク • アクセス VLANトランキングを使用する場合は、[トランク（TRUNK）]を選択します。それ以外の場合は、[アクセス（ACCESS）]を選択します。 トランク（TRUNK）モード Cisco VIC アダプタ ポリシーの設定に加えて、パケットが正しく VLAN タグ付けされるように、ベアメタル RHEL Linux ホストで特定の VLAN を使用してサブインターフェイスを設定できます。 これは、ESXi ハイパーバイザで Vswitch を作成して VM に追加することによっても実現できます。適宜ホスト OS のベンダーと協力してください。
[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。
[MACアドレス（MAC Address）] ボタン	vNIC の自動 MAC アドレスを有効にできます。
[MAC Address] フィールド	MAC アドレスを手動で入力できます。
[Uplink Port] ドロップダウン リスト	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。
[Class of Service] フィールド	vNIC に関連付けられたサービス クラス。
[トラスト ホスト CoS（Trust Host CoS）] トグルボタン	ホスト オペレーティング システムが提供するサービス クラスを有効にできます。

名前	説明
[デフォルト VLAN (Default VLAN)] トグル ボタン	vNIC に関連付けられるデフォルト VLAN 番号を有効にすることができます。 （注） リリース 4.3(6) 以降では、**[物理 NIC モード（Physical NIC mode）]** が有効になっている場合、このオプションは無効になります。
[デフォルト VLAN 番号（Number of Default VLAN）] フィールド	デフォルト VLAN 番号を入力します。
[レート制限（Rate Limit）] トグル ボタン	無制限のデータ レートを有効または無効にすることができます。この vNIC に無制限のデータ レートを設定するには、[オフ（OFF）] を選択します。それ以外の場合は、トグルボタンを有効にして、関連するフィールドにレート制限を入力します。
[Rate Limit] フィールド	レート制限は 1 ～ 50000 の整数値である必要があります。
[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。
[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。
[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。 1 ～ 1000 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。

名前	説明
[Port Profile] フィールド	vNICに関連付けられているポートプロファイル（ある場合）。 （注） このオプションには VNTAG モードが必要です。:
[アップリンク フェールオーバーの有効化（Enable Uplink Failover）] トグル ボタン	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かどうかを選択できます。
[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ますが、その時間の長さをこの設定で制御します。 0 ～ 600 の整数を入力します。

表 *147 : [Resources]* 領域

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 ～ 256 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 ～ 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。
[Receive Queue 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。

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 ～ 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。
[Completion Queue Ring Size] フィールド	各完了キュー内の記述子の数。 この値は変更できません。
[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 5 **[機能（Feature）]** タブで、次のプロパティを確認または変更します。

表 *148 : [*オフロード機能（*Offload Feature*）*]* エリア

名前	説明
[TCP セグメンテーション オフロード（TCP Segmentation Offload）] オプション ボタン	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。
[NVGRE の有効化（Enable NVGRE）] トグルボタン	Generic Routing Encapsulation を有効化または無効化できるようにします。

名前	説明
[Geneve オフロード（Geneve Offload）] トグルボタン	

名前	説明
	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。 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するには、**Geneve オフロード**を無効にします。 **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 • 物理 NIC モード

名前	説明
	（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** 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、4.2(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。
[TCP 大規模受信（TCP Large Receive）] トグル ボタン	有効にすると、セグメント化されたすべてのパケットをハードウェアで再構成してから、CPUに送信します。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。
[aRFS] トグル ボタン	Accelerated Receive Flow steering (aRFS) を有効化または無効化します。
[高度なフィルタ（Advanced Filter）] トグル ボタン	vNIC の高度なフィルタ オプションを使用するには、このボックスをオンにします。
[TCP 送信オフロードチェックサム生成（TCP Tx Offload Checksum Generation）] トグル ボタン	有効にすると、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。

名前	説明
[PTP の有効化（Enable PTP）] トグルボタン	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。
[サイド スケーリング受信（Receive Side Scaling）] トグル ボタン	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。 イネーブルの場合、可能であれば、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。
[TCP 受信オフロード チェックサム検証（TCP Rx Offload Checksum Validation）] トグル ボタン	イネーブルの場合、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
[VXLAN] トグル ボタン	仮想拡張 LAN を有効化します。
[QinQ オフロード（QinQ Offload）] トグル ボタン	Cisco IMCは、Cisco UCS VIC 14xx シリーズおよび15xxx シリーズ VIC アダプタを搭載したCisco UCS M7 サーバーに VIC QinQ トンネリング サポートを提供します。 指定した vNIC で **[VIC QinQ トンネリング（VIC QinQ Tunneling）]** 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。 （注） VIC QinQ トンネリングは、13xx アダプタではサポートされていません。 Cisco VIC 14xx のセットアップで **QinQ オフロード** 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 usNIC • 同じ vNIC での Geneve オフロード • 同じ vNIC 上の VMMQ • 同じ vNIC 上の RDMA v2 • 同じ vNIC 上の SR-IOV • 同じ vNIC での iSCSI 起動 • 同じ vNIC での PXE 起動 Cisco VIC 15xxx のセットアップで **QinQ オフロード** 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 usNIC • 同じ vNIC 上の VMMQ • 同じ vNIC 上の RDMA v2 • 同じ vNIC 上の SR-IOV • 同じ vNIC での iSCSI 起動 • 同じ vNIC での PXE 起動
[QinQ VLAN] フィールド	フィールドに2～4094のQinQ VLAN IDを入力します。

リリース 4.3(6) 以降では、Receive Side Scaling（RSS）および複数の送信（Tx）および受信（Rx）キューを構成して、 VMware ESXi 8.0 U3 以降でネットワーク パフォーマンスを向上させることができます。

この構成は、以下でサポートされています。

- Cisco IMC リリース 4.3(6) 以降
- VMware ESXi：バージョン 8.0 U3 以降
- ESXi上の nenic ドライバ：最低限必要な nenic ドライバのバージョンは 2.0.17.0-1OEM.800.1.0.20613240（ ESXi 8.0U3 の場合）です。
- ハードウェア：Cisco UCS 1400、14000、および 15000 シリーズ アダプタでサポートされます。

[オフロード機能（Offload Feature）] エリアで、以下のオプションを設定します。

- 送信キュー = n（最大 16）
- 受信キュー = n (最大 16)
- 完了キュー = 送信キューの数 + 受信キューの数
- 割り込み =（完了キューの数 + 2）以上である 2 のべき乗の最小値

（注）
次の状態を確認してください。

- **[受信側スケーリング（Receive Side Scaling、RSS）]** オプションが有効であること。
- **[VMQ 接続ポリシー（VMQ Connection Policy）]** オプションが無効であること。

VMQ が無効になっている場合、RSS エンジンがキュー分散を処理するため、 ESXi コマンドの出力で Rx ネットキュー数が 1 として表示されることがあります。

VMQ が有効になっている場合、Rx キュー数は VMQ キューを反映し、RSS エンジンがアクティブとして報告されない場合があります。このため、複数の送信キューで RSS をサポートするには、VMQ を無効にして RSS を有効にする必要があります。

表 *149 : VMQ* のプロパティ

名前	説明
[VMQ の有効化（Enable VMQ）] トグル ボタン	仮想マシン キュー(VMQ)を有効にします。

名前	説明
[マルチキューの有効化（Enable Multi Queue）] トグル ボタン	vNICでマルチキューオプションを有効にします。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。
[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。 1 ～ 64 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 ～ 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。

表 *150 : RoCE*のプロパティ

名前	説明
[RDMA モード 1/2（RDMA Mode 1/2）] トグル ボタン	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 キュー有効化**を有効にする場合には、**RDMA モード 2** も有効になっていることを確認してください。
[Queue Pairs] フィールド	アダプタ当たりのキュー ペアの数。1 ～ 8192 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。
[Memory Regions] フィールド	アダプタ当たりのメモリ リージョンの数。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。
[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 ～ 256 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] ドロップダウン リスト	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。

表 *151 : SR-IOV*プロパティ

名前	説明
[SR-IOV の有効化（Enable SR-IOV）] トグル ボタン	SR-IOV 機能を有効または無効にすることができます。
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。

名前	説明
[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。
[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。
[VF あたりのインタラプト数（Interrupt Count Per VF）] 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 6 **[iSCSI ブート プロパティ（iSCSI Boot Properties）]** タブで、次のプロパティを確認または変更します。

表 *152 : PXE* ブート*/iSCSI* ブート

名前	説明
[PXE ブート（PXE Boot）] トグルボタン	有効にすると、BIOS のブート順の構成に PXE ブート デバイスが表示されます。
[iSCSI ブート（iSCSI Boot）] トグル ボタン	有効にすると、BIOS のブート順の構成に iSCSI ブート デバイスが表示されます。

表 *153 : iSCSI*設定

名前	説明
[DHCP ネットワーク（DHCP Network）] トグル ボタン	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] トグル ボタン	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。

名前	説明
[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）。
[LUN 再試行回数値の入力（LUN Busy Retry Count）] 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。

表 *154 : [イニシエータ（Initiator）]* 領域

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。
[優先度 (Priority)] ドロップダウン リスト	以下のうちのいずれかを選択できます。 • プライマリ • セカンダリ

名前	説明
[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。
[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。
[Secondary DNS] フィールド	セカンダリ DNS サーバー アドレス。

表 *155 :* 主なターゲット

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。

表 *156 :* セカンダリターゲット

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。

名前	説明
[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 7 **[usNIC プロパティ（usNIC Properties）]** タブで、次のプロパティを確認または変更します。

表 *157 : usNIC* プロパティ

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。
[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。
[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。
[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。

名前	説明
[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。
[大規模受信（Large Receive）] トグル ボタン	有効にすると、セグメント化されたすべてのパケットをハードウェアで再構成してから、CPUに送信します。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。

名前	説明
[TCP セグメント オフロード（TCP Segment Offload）] トグル ボタン	有効にすると、CPUは大きなTCPパケットをハードウェアに送信し、パケットがセグメント化されます。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。
[TCP 送信チェックサム（TCP Tx Checksum）] トグル ボタン	有効にすると、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 受信チェックサム（TCP Rx Checksum）] トグル ボタン	イネーブルの場合、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。

次のタスク

サーバをリブートして vHBA を作成します。

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 つの vHBA と4 つの vNIC 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） リリース 4.3(6) 以降、**物理 NIC モード** が有効になっている場合は vNIC を作成できません。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ネットワーキング（Networking）]** を選択します。

ステップ 2 **[アクション（Actions）]** ドロップダウンリストから、**[vNIC]**>**[仮想 NIC インターフェイスの作成（Create Virtual NIC Interface）]**を選択します。

[vNIC の追加 (Add vNIC)] ダイアログ ボックスが表示されます。

ステップ 3 **[Cisco vNIC Adapter の選択（Select Cisco vNIC Adapter）]** で、次のプロパティを更新し、**[次へ（Next）]** をクリックします。

表 *158 : Cisco VIC*アダプタの選択

名前	説明
[スロット（Slot）] ドロップダウン リスト	
[次へ（Next）] ボタン	[**次へ（Next）**] をクリックして続行します。

ステップ 4 **[全般設定（General Settings）]** で、次のプロパティを更新し、**[次へ（Next）]**をクリックします。

表 *159 :* 一般設定

名前	説明
[名前（Name）] フィールド	仮想ネットワーク インターフェイス カード（vNIC）の名前。
[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。
[Uplink Port] ドロップダウン リスト	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。

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。
[チャネル（Channel）] フィールド	vNICに関連付けられているチャネル（ある場合）。 （注） このオプションには VNTAG モードが必要です。:
[詳細オプション（Advance Options）] トグル ボタン	高度なプロパティを有効または無効にすることができます。
[MACアドレス（MAC Address）] ボタン	vNIC の自動 MAC アドレスを有効にできます。
[MAC Address] フィールド	MAC アドレスを手動で入力できます。
[NVGRE （NVGRE）] トグル ボタン	汎用ルーティング カプセル化を有効化または無効化できるようにします。
[VXLAN] トグル ボタン	仮想拡張 LAN を有効化します。

名前	説明
[PTP] トグル ボタン	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。
[aRFS] トグル ボタン	Accelerated Receive Flow steering (aRFS) を有効化または無効化します。

名前	説明
[Geneve オフロード（Geneve Offload）] トグルボタン	

名前	説明
	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。 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するには、**Geneve オフロード**を無効にします。 **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 • 物理 NIC モード

名前	説明
	（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** 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、4.2(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。
[高度なフィルタ（Advanced Filter）] トグル ボタン	vNIC の高度なフィルタ オプションを使用するには、このボックスをオンにします。
[PXE ブート（PXE Boot）] トグル ボタン	この vNIC に対して PXE ブートがイネーブルかどうか。
[アップリンク フェールオーバー（Uplink Failover）] トグル ボタン	プライマリ インターフェイスで障害が発生したときに、この vNIC 上のトラフィックがセカンダリ インターフェイスにフェールオーバーするかどうか。 （注） このオプションには VNTAG モードが必要です。:

名前	説明
[QinQ オフロード（QinQ Offload）] トグル ボタン	Cisco IMCは、Cisco UCS VIC 14xx シリーズおよび 15xxx シリーズ VIC アダプタを搭載したCisco UCS M7 サーバーに VIC QinQ トンネリング サポートを提供します。 指定した vNIC で **[VIC QinQ トンネリング（VIC QinQ Tunneling）]** 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。 （注） VIC QinQ トンネリングは、13xx アダプタではサポートされていません。 Cisco VIC 14xx のセットアップで **QinQ オフロード** 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 usNIC • 同じ vNIC での Geneve オフロード • 同じ vNIC 上の VMMQ • 同じ vNIC 上の RDMA v2 • 同じ vNIC 上の SR-IOV • 同じ vNIC での iSCSI 起動 • 同じ vNIC での PXE 起動 Cisco VIC 15xxx のセットアップで **QinQ オフロード**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 usNIC • 同じ vNIC 上の VMMQ • 同じ vNIC 上の RDMA v2 • 同じ vNIC 上の SR-IOV • 同じ vNIC での iSCSI 起動 • 同じ vNIC での PXE 起動
[QinQ VLAN] フィールド	フィールドに2～4094のQinQ VLAN IDを入力します。

名前	説明
[デフォルト VLAN (Default VLAN)] トグル ボタン	vNIC に関連付けられるデフォルト VLAN 番号を有効にすることができます。
[デフォルト VLAN 番号（Number of Default VLAN）] フィールド	デフォルト VLAN 番号を入力します。
[レート制限（Rate Limit）] トグル ボタン	無制限のデータ レートを有効または無効にすることができます。この vNIC に無制限のデータ レートを設定するには、[オフ（OFF）] を選択します。それ以外の場合は、トグルボタンを有効にして、関連するフィールドにレート制限を入力します。
[Rate Limit] フィールド	レート制限は 1 ～ 50000 の整数値である必要があります。
[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。
[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。
[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。
[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。

名前	説明
[Port Profile] フィールド	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。
[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。
[次へ（Next）] ボタン	[**次へ（Next）**] をクリックして続行します。

ステップ 5 **[イーサネットのインタラプト（Ethernet Interrupt）]** で、次のプロパティを更新し、**[次へ（Next）]** をクリックします。

表 *160* : イーサネット割り込み

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。

名前	説明
[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。
[次へ（Next）] ボタン	[**次へ（Next）**] をクリックして続行します。

ステップ 6 **[TCP オフロード（TCP Offload）]** で、次のプロパティを更新し、 **[次へ（Next）]**をクリックします。

表 *161 : TCP*オフロード

名前	説明
[TCP 大規模受信（TCP Large Receive）] トグル ボタン	有効にすると、セグメント化されたすべてのパケットをハードウェアで再構成してから、CPUに送信します。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 セグメンテーション オフロード（TCP Segmentation Offload）] オプション ボタン	有効にすると、CPUは大きなTCPパケットをハードウェアに送信し、パケットがセグメント化されます。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
[TCP 受信オフロード チェックサム検証（TCP Rx Offload Checksum Validation）] トグル ボタン	イネーブルの場合、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。
[TCP 送信オフロードチェックサム生成（TCP Tx Offload Checksum Generation）] トグル ボタン	有効にすると、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。
[次へ（Next）] ボタン	**[次へ（Next）]** をクリックして続行します。

ステップ 7 **[VMQ 設定（VMQ Settings）]** で、次のプロパティを更新し、 **[次へ（Next）]**をクリックします。

表 *162 : VMQ*の設定

名前	説明
[VMQ] トグル ボタン	仮想マシン キュー(VMQ)を有効または無効にします。
[マルチ キュー（Multi Queue）] トグル ボタン	vNICでマルチ キューオプションを有効にします。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。

名前	説明
[トラスト ホスト CoS（Trust Host CoS）] トグル ボタン	vNICが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場合、このオプションを有効にします。
[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。
[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。
[次へ（Next）] ボタン	**[次へ（Next）]** をクリックして続行します。

ステップ 8 **[RoCE のプロパティ（RoCE Properties）]** で、次のプロパティを更新し、**[次へ（Next）]** をクリックします。

表 *163 : RoCE*のプロパティ

名前	説明
[RoCEv2] トグル ボタン	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 キュー有効化**を有効にする場合には、**RDMA モード 2** も有効になっていることを確認してください。
[Queue Pairs] フィールド	アダプタ当たりのキュー ペアの数。1 ～ 8192 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。
[Memory Regions] フィールド	アダプタ当たりのメモリ リージョンの数。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。

名前	説明
[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 ～ 256 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] ドロップダウン リスト	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。
[次へ（Next）] ボタン	[**次へ（Next）**] をクリックして続行します。

ステップ 9 **[キュー設定（Queue Settings）]** で、次のプロパティを更新し、 **[次へ（Next）]**をクリックします。

表 *164* : キューの設定

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 ～ 256 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 ～ 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。
[Receive Queue 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。

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 ～ 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。
[Completion Queue Ring Size] フィールド	各完了キュー内の記述子の数。 この値は変更できません。
[次へ（Next）] ボタン	**[次へ（Next）]** をクリックして続行します。

ステップ 10 **[SR-IOV プロパティ（SR-IOV Properties）]** で、次のプロパティを更新し、**[次へ（Next）]**をクリックします。

表 *165 : SR-IOV*プロパティ

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。
[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。
[VF あたりのインタラプト数（Interrupt Count Per VF）] 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。
[次へ（Next）] ボタン	**[次へ（Next）]** をクリックして続行します。

ステップ 11 **[サマリー（Summary）]** で、情報を確認し、**[次へ（Next）]**をクリックします。

vNIC の複製

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ネットワーキング（Networking）]** を選択します。

ステップ 2 **[vNIC インターフェイス（vNIC Interfaces）]** タブを選択します。

ステップ 3 複製する vNIC インターフェイスを選択し、 **[vNIC の複製（Clone vNIC）]** ボタンをクリックします。

[vNIC の複製（Clone vNIC）] ダイアログ ボックスが表示されます。

ステップ 4 **[vNIC の複製（Clone vNIC）]** ダイアログ ボックスで次のプロパティを更新します。

表 *166 :* クローン*vNIC*

名前	説明
[名前（Name）] フィールド	ユーザー定義の名前を入力できます。
[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。0 または 1 を選択します。
[PCIe 順序（PCIe Order）] フィールド	この vNIC が使用される順序。0 ～ 4 の整数を入力します。
[VLAN Mode] ドロップダウン リスト	関連付けられた VLAN のモード。次のいずれかになります。 • トランク • アクセス VLANトランキングを使用する場合は、[トランク（TRUNK）]を選択します。それ以外の場合は、[アクセス（ACCESS）]を選択します。
[デフォルト VLAN（Default VLAN）] トグル ボタンとフィールド	この vNIC のデフォルト VLAN がない場合は、無効になります。そうでなければ、[デフォルト VLAN（Default VLAN）] を有効にして、フィールドに 1 ～4094 の VLAN ID を入力します。

名前	説明
[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。1 ～ 1000 の整数を入力します。
[vNIC のクローン（Clone vNIC）] ボタン	vNIC を複製できます。

ステップ 5 **[vNIC の複製（Clone vNIC）]** をクリックして変更を保存します。

vNIC の削除

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ネットワーキング（Networking）]** を選択します。

ステップ 2 **[vNIC インターフェイス（vNIC Interfaces）]** タブを選択します。

ステップ 3 削除する **vNIC インターフェイス** を選択し、**[vNIC の削除（Delete vNIC）]** ボタンをクリックします。

（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 4 [OK] をクリックして確定します。

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。

- この手順を実行するには、管理者ユーザー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

始める前に

この手順を実行するには、管理者ユーザーとしてログインする必要があります。

Cisco IMC リリース 6.0 以降では、vNIC で **IPv6** の iSCSI ブート機能を設定できます。

（注） vNIC で IPv6 の iSCSI ブート機能を設定するための要件は、次のとおりです。

- vNIC で IPv6 の iSCSI ブート機能を有効にするためにサポートされる最小バージョンは、Cisco IMC 6.0 リリースのコンポーネント（Cisco IMC、 BIOS、 VIC）です。
- サポートされているサーバー：Cisco UCS M6 サーバー以降（UEFI ブート モードのみ）。
- デフォルトの iSCSI ポート番号は、 iSCSI ブートの場合は 3260 である必要があります。
- iSCSI DHCP ベンダーオプション 43 および 17 は、IPv6 ではサポートされていません。
- iSCSI はプライマリおよびセカンダリ ターゲットの LUN ID フィールドでブート LUN ID <= 255 をサポートします。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ネットワーキング（Networking）]** を選択します。

ステップ 2 **[vNIC インターフェイス（vNIC Interfaces）]** タブを選択します。

ステップ 3 プロパティを変更する vNIC インターフェイスを選択し、[名前（Name）] カラムをクリックします。

[vNIC プロパティ（vNIC Properties）] ダイアログ ボックスが表示されます。

ステップ 4 **[iSCSI ブート プロパティ (iSCSI Boot Properties)]** タブを選択します。

次のプロパティを表示または変更できます。

表 *167 : PXE* ブート*/iSCSI* ブート

名前	説明
[PXE ブート（PXE Boot）] トグルボタン	有効にすると、BIOS のブート順の構成に PXE ブート デバイスが表示されます。
[iSCSI ブート（iSCSI Boot）] トグル ボタン	有効にすると、BIOS のブート順の構成に iSCSI ブート デバイスが表示されます。

表 *168 : iSCSI*設定

名前	説明
[DHCP ネットワーク（DHCP Network）]トグル ボタン	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] トグル ボタン	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）。
[LUN 再試行回数値の入力（LUN Busy Retry Count）] 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。

表 *169* : *[*イニシエータ（*Initiator*）*]* 領域

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。
[優先度 (Priority)] ドロップダウン リスト	以下のうちのいずれかを選択できます。 • プライマリ • セカンダリ
[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。
[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。
[Secondary DNS] フィールド	セカンダリ DNS サーバー アドレス。

表 *170* : 主なターゲット

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。

名前	説明
[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。

表 *171* : セカンダリターゲット

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 5 [保存（Save）] 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

この手順を実行するには、管理者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 **[アプリ（Apps）]** ドロップダウン リストから、**[ネットワーキング（Networking）]** を選択します。

ステップ 2 **[vNIC インターフェイス（vNIC Interfaces）]** タブを選択します。

ステップ 3 プロパティを変更する vNIC インターフェイスを選択し、[名前（Name）] カラムをクリックします。

[vNIC プロパティ（vNIC Properties）] ダイアログ ボックスが表示されます。

ステップ 4 **[iSCSI ブート プロパティ (iSCSI Boot Properties)]** タブを選択します。
ステップ 5 **[iSCSI ブート（iSCSI Boot）]** トグル ボタンをクリックして、iSCSI ブートを無効にします。

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

vNIC での Cisco usNIC の表示と設定

始める前に

この手順を実行するには、管理者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 **[アプリ（Apps）]** ドロップダウン リストから、**[ネットワーキング（Networking）]** を選択します。
ステップ 2 **[vNIC インターフェイス（vNIC Interfaces）]** タブを選択します。
ステップ 3 プロパティを変更する vNIC インターフェイスを選択し、[名前（Name）] カラムをクリックします。

[vNIC プロパティ（vNIC Properties）] ダイアログ ボックスが表示されます。

ステップ 4 **[usNICプロパティ（usNIC Properties）]** タブを選択します。
ステップ 5 **[usNIC プロパティ（usNIC Properties）]** 領域で、次のフィールドを確認して更新します。

表 *172 : usNIC* プロパティ

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。

名前	説明
[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。
[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。
[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。
[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。

名前	説明
[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。
[大規模受信（Large Receive）] トグル ボタン	有効にすると、セグメント化されたすべてのパケットをハードウェアで再構成してから、CPUに送信します。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 セグメント オフロード（TCP Segment Offload）] トグル ボタン	有効にすると、CPUは大きなTCPパケットをハードウェアに送信し、パケットがセグメント化されます。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。
[TCP 送信チェックサム（TCP Tx Checksum）] トグル ボタン	有効にすると、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。

名前	説明
[TCP 受信チェックサム（TCP Rx Checksum）] トグル ボタン	イネーブルの場合、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 6 **[Save Changes]**をクリックします。

変更内容は次回のサーバ リブート時に有効になります。

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

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 **[アプリ（Apps）]** ドロップダウン リストから、**[ネットワーキング（Networking）]** を選択します。

ステップ 2 **[アクション（Actions）]** ドロップダウン リストから、**[vNIC]** > **[vNIC のエクスポート（Export vNIC）]**を選択します。

[vNIC のエクスポート（Export vNIC）] ダイアログ ボックスが表示されます。

ステップ 3 **[vNIC のエクスポート（Export vNIC）]** ダイアログ ボックスで、次のプロパティを更新します。

表 *173 : vNIC*のエクスポート

名前	説明
[サーバーIP/ホスト名（Server IP/Hostname）] フィールド	ファイルのエクスポート先となるサーバーの IP アドレスまたはホスト名。

名前	説明
[Upload Protocol] ボタン	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]** （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。
[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（Username）] フィールド	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。

ステップ 4 [Export Configuration] 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 **[アプリ（Apps）]** ドロップダウン リストから、**[ネットワーキング（Networking）]** を選択します。

ステップ 2 **[アクション（Actions）]** ドロップダウン リストから、**[vNIC]** > **[vNIC のインポート（Import vNIC）]**を選択します。

[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 3 **[vNIC のインポート (Import vNIC)]** ダイアログ ボックスで、次のプロパティを更新します。

表 *174 : vNIC*のインポート

名前	説明
[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 IP アドレスまたはホスト名。
[Upload Protocol] ボタン	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]** （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。
[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（Username）] フィールド	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。

ステップ 4 **[Import Configuration]**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 **[アプリ（Apps）]** ドロップダウン リストから、**[ネットワーキング（Networking）]** を選択します。

ステップ 2 **[アクション（Actions）]** ドロップダウン リストから、**[VIC]** > **[デフォルトにリセット （Reset to Defaults）]** を選択します。

[デフォルトにリセット （Reset to Defaults）] ダイアログ ボックスが表示されます。

ステップ 3 確認のために [はい（Yes）] をクリックします。

アダプタのリセット

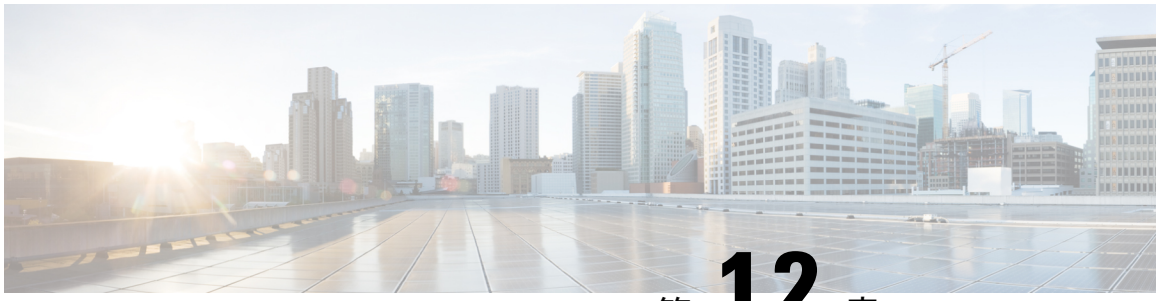
手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ネットワーキング（Networking）]** を選択します。

ステップ 2 **[アクション（Actions）]** ドロップダウン リストから、**[vNIC]** > **[リセット （Reset）]**を選択します。

[リセット（Reset）] ダイアログ ボックスが表示されます。

ステップ 3 [OK] をクリックして確定します。



第 12 章

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） （450 ページ）
• 未使用の物理ドライブからの仮想ドライブの作成 （454 ページ）
• 既存のドライブ グループからの仮想ドライブの作成 （458 ページ）
• 仮想ドライブを転送対応として設定 （461 ページ）
• 外部設定のインポート （462 ページ）
• 外部設定のクリア （463 ページ）
• ブート ドライブのクリア （464 ページ）
• JBOD の有効化 （465 ページ）
• JBOD の無効化 （465 ページ）
• コントローラの TTY ログの取得 （466 ページ）
• コントローラの設定のクリア （466 ページ）
• 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 （467 ページ）
• ドライブの削除のための準備 （467 ページ）
• 専用ホット スペアにする （468 ページ）
• グローバル ホット スペアにする （469 ページ）
• ホット スペア プールからのドライブの削除 （470 ページ）
• 物理ドライブのステータスの切り替え （471 ページ）
• 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 （471 ページ）
• 仮想ドライブの初期化 （472 ページ）
• ブート ドライブとして設定 （473 ページ）
• 仮想ドライブの編集 （474 ページ）
• 仮想ドライブの削除 （476 ページ）
• 仮想ドライブの非表示化 （477 ページ）
• バッテリ バックアップ ユニットの学習周期の開始 （477 ページ）
• ストレージ コントローラ ログの表示 （478 ページ）
• MegaRAID コントローラの SSD スマート情報の表示 （479 ページ）
• NVMe コントローラの詳細の表示 （481 ページ）
• NVMe 物理ドライブの詳細の表示 （483 ページ）

• PCI スイッチの詳細の表示 （486 ページ）
• コピーバック操作の開始 （491 ページ）
• Flexible Flash コントローラの管理 （491 ページ）
• FlexUtil コントローラの管理 （512 ページ）
• Cisco ブート最適化 M.2 Raid コントローラ （529 ページ）
• Cisco FlexMMC （547 ページ）

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

始める前に

このタスクを実行するには、admin 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**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 右側のペインの **[アクション（Actions）]** ドロップダウン リストで、**[ストレージ（Storage）]** > **[ドライブ セキュリティの有効化（Enable Drive Security）]** をクリックします。

[ドライブ セキュリティの有効化（Enable Drive Security）] ダイアログ ボックスが表示されます。

ステップ 4 **[ドライブ セキュリティの有効化（Enable Drive Security）]** ダイアログ ボックスで、次の情報を確認します。

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。 • [はい（True）]：コントローラ セキュリティが有効になっています。 • [いいえ（False）]：コントローラ セキュリティが無効になっています。

名前	説明
[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。
[提案（Suggest）] ボタン	使用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	操作をキャンセルします。

ステップ 5 [保存（Save）] をクリックします。

コントローラ セキュリティの変更

始める前に

このタスクを実行するには、admin 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]** 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 右ペインの **[アクション（Actions）]** ドロップダウンリストで、**[ストレージ（Storage）]** > **[ドライブ セキュリティの変更（Modify Drive Security）]** をクリックします。

[ドライブ セキュリティの変更（Modify Drive Security）] ダイアログ ボックスが表示されます。

ステップ 4 **[ドライブ セキュリティの変更（Modify Drive Security）]** ダイアログ ボックスで、次の情報を確認します。

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。 • [はい（True）]：コントローラ セキュリティが有効になっています。 • [いいえ（False）]：コントローラ セキュリティが無効になっています。
[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 キーを再入力します。
[提案（Suggest）] ボタン	使用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	操作をキャンセルします。

ステップ 5 [保存（Save）] をクリックします。

コントローラ セキュリティの無効化

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**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 右ペインの **[アクション（Actions）]** ドロップダウンリストで、**[ストレージ（Storage）]** > **[ドライブ セキュリティの無効化（Disable Drive Security）]** をクリックします。

プロンプトで **[はい（Yes）]** または **[いいえ（No）]** をクリックします。

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

このタスクによって、コントローラ 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たり、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 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]** 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 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、右側パネルの **[コントローラ情報（Controller Info）]** タブの **[アクション（Actions）]** ドロップダウン リストで、**[ローカル キー管理に切り替え（Switch to Local Key Management）]** を選択します。

（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、**[リモート キー管理に切り替え（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 権限でログインする必要があります。

一部の C シリーズ サーバーでのみ有効になります。

（注） Cisco IMC は、既存のデュアル ドライブ サポートに加えて、M.2 RAID コントローラでシングル ドライブをサポートするようになりました。

シングル ドライブのサポートでは、仮想ディスクを作成できません。

手順の概要

1. **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。
2. **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**メニューで、適切なLSI MegaRAIDコントローラをクリックします。
3. 右側ペインで **[仮想ドライブ情報（Virtual Drive Info）]** タブをクリックします。
4. 右側のペインの **[アクション（Actions）]** ドロップダウン リストから、**[ストレージ（Storage）]** > **[仮想ドライブの作成（Create Virtual Drive）]**をクリックします。
5. **[コントローラを選択（Select Controller）]**
6. **[範囲の作成（Create Ranges）]** ページで、次の情報を入力します。
7. **[RAID タイプおよび PD（RAID Type & PDs）]** ページで、次の情報を入力します。
8. **[VD のプロパティ（VD Properties）]** ページで、次の情報を入力します。
9. **[サマリー（Summary）]** ページで、情報を確認して **[作成（Create）]** をクリックします。

手順の詳細

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**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 右側ペインで **[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 右側のペインの **[アクション（Actions）]** ドロップダウン リストから、**[ストレージ（Storage）]** > **[仮想ドライブの作成（Create Virtual Drive）]**をクリックします。

[仮想ドライブの作成（Create Virtual Drive）] ペインが表示されます。

ステップ 5 **[コントローラを選択（Select Controller）]**

名前	説明
[MRAID] ドロップダウン リスト	ドロップダウン リストから [MRAID] を選択し、**[次へ（Next）]** をクリックします。

ステップ 6 **[範囲の作成（Create Ranges）]** ページで、次の情報を入力します。

名前	説明
[未使用の物理ドライブから（From Unused Physical Drives）] ラジオ ボタン	未使用の物理ドライブから VD を作成するには、このオプションを選択します
[既存のドライブ グループから（From Existing Drive Group）] ラジオ ボタン	既存のグループから VD を作成するには、このオプションを選択します。
[仮想ドライブ（Virtual Drive）] ドロップダウンリスト	このオプションは、**[既存のドライブグループから（From Existing Drive Group）]**でのみ使用できます。 リストから VDを選択し、**[次へ（Next）]** をクリックします。

ステップ 7 **[RAID タイプおよび PD（RAID Type & PDs）]** ページで、次の情報を入力します。

RAID タイプ

表 *175 : RAID* タイプ

名前	説明
[RAID タイプ（RAID Type）] ドロップダウン リスト	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。 • [Raid 00]：スパンされたストライピング。

（注）
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。

Physical Drives

表 *176 : Physical Drives*

名前	説明
[物理ドライブ（Physical Drives）] テーブル	ドライブ グループにまだ含まれていない物理ドライブのリスト。
[ID] カラム	物理ドライブの ID。
[Size (GB)] カラム	物理ドライブのサイズ（MB 単位）。
[Model] カラム	ドライブのベンダー名。
[インターフェイス タイプ（Interface Type] カラム	ドライブが SAS または SATA であるかどうか
[Type] カラム	ドライブ SSD または HDD のタイプ。
[>] ボタン	[物理ドライブ（Physical Drives）] テーブルで選択されたドライブをドライブ グループに追加します。
[<] ボタン	[ドライブ グループ（Drive Groups）] テーブルで選択されたドライブをドライブ グループから削除します。
[ドライブ/スパン（Drives/Span）] テーブル	ドライブ グループのリスト。
[Name] カラム	作成するドライブ グループの名前。

（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。

ステップ 8 **[VD のプロパティ（VD Properties）]** ページで、次の情報を入力します。

表 *177 : [*このグループの仮想ドライブ（*Virtual Drives in this Group*）*]*

名前	説明
[ID] カラム	仮想ドライブの ID。
[Name] カラム	仮想ドライブの名前。
[サイズ（MB）（Size (MB)）] 列	仮想ドライブのサイズ。

ステップ 9 **[サマリー（Summary）]** ページで、情報を確認して **[作成（Create）]** 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 権限でログインする必要があります。

手順の概要

1. **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。
2. **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**メニューで、適切な LSI MegaRAID コントローラをクリックします。
3. 右側ペインで **[仮想ドライブ情報（Virtual Drive Info）]** タブをクリックします。
4. 右側のペインの **[アクション（Actions）]** ドロップダウン リストから、 **[ストレージ（Storage）]** > **[仮想ドライブの作成（Create Virtual Drive）]**をクリックします。
5. **[コントローラを選択（Select Controller）]**
6. **[範囲の作成（Create Ranges）]** ページで、次の情報を入力します。
7. **[RAID タイプおよび PD（RAID Type & PDs）]** ページで、次の情報を入力します。
8. **[VD のプロパティ（VD Properties）]** ページで、次の情報を入力します。
9. **[サマリー（Summary）]** ページで、情報を確認して **[作成（Create）]** をクリックします。

手順の詳細

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**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 右側ペインで **[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 右側のペインの **[アクション（Actions）]** ドロップダウン リストから、 **[ストレージ（Storage）]** > **[仮想ドライブの作成（Create Virtual Drive）]**をクリックします。

[仮想ドライブの作成（Create Virtual Drive）] ペインが表示されます。

ステップ 5 **[コントローラを選択（Select Controller）]**

名前	説明
[MRAID] ドロップダウン リスト	ドロップダウン リストから [MRAID] を選択し、**[次へ（Next）]** をクリックします。

ステップ 6 **[範囲の作成（Create Ranges）]** ページで、次の情報を入力します。

名前	説明
[未使用の物理ドライブから（From Unused Physical Drives）] ラジオ ボタン	未使用の物理ドライブから VD を作成するには、このオプションを選択します
[既存のドライブ グループから（From Existing Drive Group）] ラジオ ボタン	既存のグループから VD を作成するには、このオプションを選択します。
[仮想ドライブ（Virtual Drive）] ドロップダウンリスト	このオプションは、**[既存のドライブグループから（From Existing Drive Group）]**でのみ使用できます。 リストから VDを選択し、**[次へ（Next）]** をクリックします。

ステップ 7 **[RAID タイプおよび PD（RAID Type & PDs）]** ページで、次の情報を入力します。

RAID タイプ

表 178 : RAID タイプ

名前	説明
[RAID タイプ（RAID Type）] ドロップダウン リスト	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。 • [Raid 00]：スパンされたストライピング。

（注）

- **[RAIDタイプの構成（Configure RAID Type）]** は、**[既存のドライブグループから（From Existing Drive Group）]** を選択した場合にのみ使用できます。
- 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。

Physical Drives

表 *179 : Physical Drives*

名前	説明
[物理ドライブ（Physical Drives）] テーブル	ドライブ グループにまだ含まれていない物理ドライブのリスト。
[ID] カラム	物理ドライブの ID。
[Size (GB)] カラム	物理ドライブのサイズ（MB 単位）。
[Model] カラム	ドライブのベンダー名。
[インターフェイス タイプ（Interface Type] カラム	ドライブが SAS または SATA であるかどうか
[Type] カラム	ドライブ SSD または HDD のタイプ。
[>] ボタン	[物理ドライブ（Physical Drives）] テーブルで選択されたドライブをドライブ グループに追加します。
[<] ボタン	[ドライブ グループ（Drive Groups）] テーブルで選択されたドライブをドライブ グループから削除します。
[ドライブ/スパン（Drives/Span）] テーブル	ドライブ グループのリスト。
[Name] カラム	作成するドライブ グループの名前。

（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。

[サイズ（Size）] は、**[既存のドライブグループから（From Existing Drive Group）]** を選択した場合にのみ使用できます。

表 *180 :* サイズ

名前	説明
[サイズ（Size）] ドロップダウン リスト	作成する仮想ドライブのサイズ。

ステップ 8 **[VD のプロパティ（VD Properties）]** ページで、次の情報を入力します。

表 *181 : [*このグループの仮想ドライブ（***Virtual Drives in this Group***）*]*

名前	説明
[ID] カラム	仮想ドライブの ID。
[Name] カラム	仮想ドライブの名前。
[サイズ（MB）（Size (MB)）] 列	仮想ドライブのサイズ。

このグループの仮想ドライブは、[既存のドライブグループから（From Existing Drive Group）] を選択した場合にのみ使用できます。

ステップ 9 **[サマリー（Summary）]** ページで、情報を確認して **[作成（Create）]** をクリックします。

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 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**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 右側ペインで **[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、**[転送準備完了に設定（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 5 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準備完了に設定すると、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。

外部設定のインポート

セキュアなドライブ グループをホストする物理ドライブのセットが別のサーバまたはコントローラ（または、それらが存在しない間にセキュリティ キーが変更された同じコントローラ）に挿入されると、それらは外部設定になります。これらは保護されているため、外部設定をインポートする前に、セキュリティ キー情報を確認してロックを解除する必要があります。

外部設定のセキュリティ キーを確認して設定をインポートするには、次の手順を実行します。

始める前に

このタスクを実行するには、admin 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**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 [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 4 右側ペインで **[コントローラ情報（Controller Info）]** タブをクリックします。

ステップ 5 右ペインの **[アクション（Actions）]** ドロップダウンリストで、**[ストレージ（Storage）]** > **[外部構成のインポート（Import Foreign Config）]** をクリックします。

[外部構成のインポート（Import Foreign Config）] ウィンドウに、次のメッセージが表示されます。

Are you sure you want import foreign config?（外部設定をインポートしますか?）

[OK] をクリックします。

このアクションにより、**[セキュア キーの確認（Secure Key Verification）]**ダイアログ ボックスが開きます。続行する前に、次の情報を確認してください。

表 *182 : [*セキュアキーの検証（***Secure Key Verification***）*]*領域

名前	説明
[セキュリティキー（Security Key）] フィールド	コントローラに割り当てられた一意のキー ID。
[検証（Verify）] ボタン	入力したキーが保存されているキー情報と一致するかどうかを検証します。 適切なセキュア キーであることが検証されると、要求したアクションが実行されます。
[Cancel] ボタン	操作をキャンセルします。

ステップ 6 [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 権限でログインする必要があります。

手順の概要

1. **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。
2. **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**メニューで、適切なLSI MegaRAIDコントローラをクリックします。

3. [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。
4. 右側ペインで **[コントローラ情報（Controller Info）]** タブをクリックします。
5. 右ペインの **[アクション（Actions）]** ドロップダウンリストで、**[ストレージ（Storage）]** > **[外部構成のクリア（Clear Foreign Config）]** をクリックします。
6. [OK] をクリックして確定します。

手順の詳細

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]** 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 [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 4 右側ペインで **[コントローラ情報（Controller Info）]** タブをクリックします。

ステップ 5 右ペインの **[アクション（Actions）]** ドロップダウンリストで、**[ストレージ（Storage）]** > **[外部構成のクリア（Clear Foreign Config）]** 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。

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 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]** 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 右側ペインの **[アクション（Actions）]** ドロップダウンリストで、**[ストレージ（Storage）]** > **[ブート ドライブのクリア（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 の有効化

（注） 一部の UCS C シリーズ サーバでのみ Just a Bunch of Disks（JBOD）をイネーブルにできます。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**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 右側ペインで **[コントローラ情報（Controller Info）]** タブをクリックします。

ステップ 4 右ペインの **[アクション（Actions）]** ドロップダウンリストで、**[JBOD の有効化（Enable JBOD）]** を選択します。

ステップ 5 [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 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**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 右側ペインで **[コントローラ情報（Controller Info）]** タブをクリックします。

ステップ 4 右ペインの **[アクション（Actions）]** ドロップダウンリストで、**[JBOD の無効化（Disable JBOD）]** を選択します。

ステップ 5 [OK] をクリックして確定します。

コントローラの TTY ログの取得

このタスクは、コントローラの TTY 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 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**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 右側ペインで **[コントローラ情報（Controller Info）]** タブをクリックします。

ステップ 4 [**Actions**] 領域で、[**Get TTY Log**] 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。

重要
コントローラの TTY 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 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]** 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 右側ペインの **[アクション（Actions）]** ドロップダウン リストで、**[ストレージ（Storage）]** > **[すべての構成のクリア（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 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]** 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 右ペインの **[アクション（Actions）]** ドロップダウン リストで、**[ストレージ（Storage）]** > **[デフォルトの復元（Restore 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 権限でログインする必要があります。

手順の概要

1. **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。
2. **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**メニューで、適切なLSI MegaRAIDコントローラをクリックします。
3. 右側ペインで **[物理ドライブ情報（Physical Drive Info）]** タブをクリックします。
4. 削除するドライブを選択します。
5. 選択したドライブの近くにある 3 つの水平のドットをクリックし、ドロップダウンリストから **[削除準備（Prepare for Removal）]** を選択します。
6. [OK] をクリックして確定します。

手順の詳細

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**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 右側ペインで **[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 削除するドライブを選択します。

ステップ 5 選択したドライブの近くにある 3 つの水平のドットをクリックし、ドロップダウンリストから **[削除準備（Prepare for Removal）]** を選択します。

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 権限でログインする必要があります。

手順の概要

1. **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。
2. **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**メニューで、適切なLSI MegaRAIDコントローラをクリックします。
3. 右側ペインで **[物理ドライブ情報（Physical Drive Info）]** タブをクリックします。
4. **[物理ドライブ（Physical Drives）]** 領域で、専用ホット スペアにする物理ドライブを選択します。
5. 横に並んだ 3 つのドットをクリックし、ドロップダウンリストから **[専用ホットスペアにする（Make Dedicated Hot Spare）]** を選択します。

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。
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。

手順の詳細

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**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 右側ペインで **[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、専用ホット スペアにする物理ドライブを選択します。

ステップ 5 横に並んだ 3 つのドットをクリックし、ドロップダウンリストから **[専用ホットスペアにする（Make Dedicated Hot Spare）]** を選択します。

[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。
[Physical Drive Number] フィールド	物理ドライブの番号。

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 権限でログインする必要があります。

手順の概要

1. **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。
2. **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**メニューで、適切なLSI MegaRAID コントローラをクリックします。
3. 右側ペインで **[物理ドライブ情報（Physical Drive Info）]** タブをクリックします。

4. **[物理ドライブ（Physical Drives）]** タブで、グローバル ホット スペアにする物理ドライブを選択します。
5. 3つの横にあるドットをクリックし、ドロップダウンリストから**[グローバルホットスペアにする（Make Global Hot Spare）]** を選択します。

手順の詳細

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**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 右側ペインで **[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）]** タブで、グローバル ホット スペアにする物理ドライブを選択します。

ステップ 5 3 つの横にあるドットをクリックし、ドロップダウンリストから **[グローバルホットスペアにする（Make Global Hot Spare）]** を選択します。

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 権限でログインする必要があります。

手順の概要

1. **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。
2. **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**メニューで、適切なLSI MegaRAID コントローラをクリックします。
3. 右側ペインで **[物理ドライブ情報（Physical Drive Info）]** タブをクリックします。
4. **[物理ドライブ情報（Physical Drives Info）]** タブで、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。
5. **[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。

手順の詳細

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**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 右側ペインで **[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 **[物理ドライブ情報（Physical Drives Info）]** タブで、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 **[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 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**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 右側ペインで **[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 **[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 選択されたドライブの近くにある 3 つの水平方向のドットをクリックし、ドロップダウン リストから **[状態を Unconfigured Good として設定する（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 権限で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 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**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 右側ペインで **[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 **[物理ドライブ情報（Physical Drives Info）]** 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 選択したドライブの近くにある 3 つの水平方向のドットをクリックし、ドロップダウン リストから **[ブート ドライブとして設定（Set as Boot Drive）]** を選択します。

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 権限でログインする必要があります。

手順の概要

1. **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。
2. **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**メニューで、適切な LSI MegaRAID コントローラをクリックします。
3. 右側ペインで **[仮想ドライブ情報（Virtual Drive Info）]** タブをクリックします。
4. **[仮想ドライブ情報（Virtual Drive Info）]** タブで、初期化するドライブを選択します。
5. 選択されたドライブの近くにある 3 つの水平のドットをクリックし、ドロップダウン リストから **[初期化（Initialize）]** をクリックします。
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。
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。
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。

手順の詳細

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**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 右側ペインで **[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 **[仮想ドライブ情報（Virtual Drive Info）]** タブで、初期化するドライブを選択します。

ステップ 5 選択されたドライブの近くにある 3 つの水平のドットをクリックし、ドロップダウン リストから **[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）。
[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 権限でログインする必要があります。

手順の概要

1. **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。
2. **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**メニューで、適切なLSI MegaRAIDコントローラをクリックします。
3. 右側ペインで **[物理ドライブ情報（Physical Drive Info）]** タブをクリックします。
4. **[物理ドライブ情報（Physical Drive Info）]** タブで、コントローラを起動する必要のあるドライブを選択します。
5. 選択されたドライブの近くにある 3 つの水平のドットをクリックし、**[ブートドライブとして設定（Set as Boot Drive）]** をクリックします。
6. [OK] をクリックして確定します。

手順の詳細

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**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 右側ペインで **[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 **[物理ドライブ情報（Physical Drive Info）]** タブで、コントローラを起動する必要のあるドライブを選択します。

ステップ 5 選択されたドライブの近くにある 3 つの水平のドットをクリックし、**[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 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**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 右側ペインで **[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 選択したドライブの近くにある 3 つの水平のドットをクリックし、**[仮想ドライブの編集（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 権限でログインする必要があります。

手順の概要

1. **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。
2. **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**メニューで、適切なLSI MegaRAIDコントローラをクリックします。
3. 右側ペインで **[仮想ドライブ情報（Virtual Drive Info）]** タブをクリックします。
4. **[仮想ドライブ情報（Virtual Drive Info）]** タブで、削除する仮想ドライブを選択します。
5. 選択されたドライブの近くにある3つの水平のドットをクリックし、**[仮想ドライブの削除（Delete Virtual Drive）]** をクリックします。
6. [OK] をクリックして確定します。

手順の詳細

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**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 右側ペインで **[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 **[仮想ドライブ情報（Virtual Drive Info）]** タブで、削除する仮想ドライブを選択します。

ステップ 5 選択されたドライブの近くにある 3 つの水平のドットをクリックし、**[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

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**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 右側ペインで **[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 **[仮想ドライブ情報（Virtual Drive Info）]** タブで、非表示にする仮想ドライブを選択します。

ステップ 5 選択されたドライブの近くにある 3 つの水平のドットをクリックし、**[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 権限でログインする必要があります。

手順の概要

1. **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

2. **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**メニューで、適切なLSI MegaRAIDコントローラをクリックします。
3. [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。
4. 右側ペインで**[バッテリ バックアップ ユニット（Battery Backup Unit）]**タブをクリックします。
5. [Actions] ペインで [Start Learn Cycle] をクリックします。
6. **[OK]** をクリックします。

手順の詳細

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**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 [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 4 右側ペインで**[バッテリ バックアップ ユニット（Battery Backup Unit）]**タブをクリックします。

ステップ 5 [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 6 **[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。

手順の概要

1. **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。
2. **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**メニューで、適切なLSI MegaRAIDコントローラをクリックします。
3. 右側ペインの **[ストレージ ログ（Storage Log）]** タブをクリックし、次の情報を確認します。

手順の詳細

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**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 右側ペインの **[ストレージ ログ（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） • 警告 • 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。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**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 右側ペインで **[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 カラム **[スロット ID（Slot ID）]** でドライブを選択します。

ドライブの詳細を含む新しいペインが表示されます。

ステップ 5 **[詳細（Detail）]** タブをクリックし、次の情報を確認します。

表 *183 :* 製品の詳細

名前	説明
電源の再投入回数	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）]	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)	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。
消耗状態 (日数)	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	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。
最大動作温度	ドライブがエラーなしで動作できる許容最高温度。
使用された予約済み容量の割合	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からのもの）。

ステップ 6 [閉じる（Close）] をクリックします。

NVMe 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 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**で、適切な NVMe コントローラをクリックします。

ステップ 3 右側のペインの **[コントローラ情報（Controller Info）]** タブで、**[一般（General）]** タブの下の次の情報を確認します。

名前	説明
製品名	MegaRAID コントローラの名前。
製品ID	RAID コントローラのシスコ製品番号。
[複合状態（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
コントローラステータス	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。

名前	説明
セキュリティ	現在の状態に応じてコントローラ ロック キーを表示します。 （注） • このオプションを使用できるのは一部の C シリーズ サーバだけです。 • ドライブ セキュリティを無効にすると、すべてのセキュア ドライブ上のデータを使用できなくなります。
[Serial Number] フィールド	MegaRAID コントローラのシリアル番号。
[RAID Chip Temperature] フィールド	コントローラの温度（摂氏）。
[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。
[Consistency Check Rate] フィールド	冗長データの不整合を検索して修正するために、コントローラが仮想ドライブをスキャンするレート。 このレートは、使用可能な帯域幅合計に対するパーセンテージで表示されます。
[PCI スロット（PCI Slot）]	コントローラが配置されている PCIe スロットの名前。
Vendor ID	PCI ベンダー ID（16 進）。
[サブベンダー ID（SubVendor ID）]	PCI サブベンダー ID（16 進）。
Device ID	PCI デバイス ID（16 進）。
サブ デバイス ID	PCI サブデバイス ID（16 進）。
[製造日（Manufactured Date）]	MegaRAID カードが製造された日付（yyy-mm-dd 形式）。
改定	ボードのリビジョン番号（存在する場合）。
ブートドライブ	ブート ドライブの番号。

名前	説明
インターフェイス タイプ	ドライブが SAS または SATA であるかどうか

NVMe 物理ドライブの詳細の表示

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 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**で、適切な NVMe コントローラをクリックします。

ステップ 3 **[物理ドライブ情報（Physical Drive Info）]** 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 ID（Slot ID）]	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。
Disk Type	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。

名前	説明
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。 • [Copyback]：ドライブはビジー状態で、コピーバック操作を実行しています。 • [Failed]：ドライブは使用中ですが、障害が発生しています。 • [Foreign configuration]：ドライブに外部設定が含まれます。 • [Global hot spare]：ドライブはグローバル スペア ドライブとして指定されています。 • [Dedicated hot spare]：ドライブは専用スペア ドライブとして指定されています。 • [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。 • [Ready to remove]：ドライブは削除の準備ができています。 • [Rebuild]：ドライブは現在再構築されています。 • [System]：ドライブはホストから見えますが、仮想ドライブに使用することはできません。 • [Unconfigured bad]：ドライブは障害が発生し、使用されていません。 • [Unconfigured good]：ドライブをドライブ グループまたはホット スペア プールに割り当てることができます。
容量(GB)	ドライブの容量（ギガバイト単位）。
モデル（**Model**）	ドライブのベンダー名。
ファームウェア	ドライブで実行されているファームウェア バージョン。

ステップ 4 カラム **[スロット ID（Slot ID）]** でドライブを選択します。

ドライブの詳細を含む新しいペインが表示されます。

[一般（General）] タブでドライブの詳細を表示します。

表 *184 : [*全般（*General*）*]* タブ

名前	説明
メディア タイプ	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。
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。
シーケンス番号	コントローラがドライブの変更を追跡するために使用するシーケンス番号。
セキュリティが有効	このフィールドに [はい（Yes）] が表示されている場合は、物理ドライブで完全なディスク暗号化が有効になっています。
物理ブロックサイズ	ドライブの物理ブロック サイズを示します。
スロット番号	物理ドライブが存在するスロット番号。
Device ID	ドライブのデバイス ID。
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。
UCS製品ID	
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。
ドライブのシリアル番号	ドライブのシリアル番号。
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）。
非強制サイズ	強制のために失われた領域を含む容量（MB単位）。
[強制サイズ（Coerced Size）]	強制的な丸め処理の実行後の容量（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。

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 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**メニューで、適切な **PCI Switch** コントローラをクリックします。

ステップ 3 次の情報を確認します。

[全般（General）] タブ

名前	説明
製品名	MegaRAID コントローラの名前。
製品ID	RAID コントローラのシスコ製品番号。
[複合状態（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
コントローラステータス	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。

名前	説明
セキュリティ	現在の状態に応じてコントローラ ロック キーを表示します。 （注） • このオプションを使用できるのは一部の C シリーズ サーバだけです。 • ドライブ セキュリティを無効にすると、すべてのセキュア ドライブ上のデータを使用できなくなります。
[Serial Number] フィールド	MegaRAID コントローラのシリアル番号。
[RAID Chip Temperature] フィールド	コントローラの温度（摂氏）。
[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。
[Consistency Check Rate] フィールド	冗長データの不整合を検索して修正するために、コントローラが仮想ドライブをスキャンするレート。 このレートは、使用可能な帯域幅合計に対するパーセンテージで表示されます。
[PCI スロット（PCI Slot）]	コントローラが配置されている PCIe スロットの名前。
Vendor ID	PCI ベンダー ID（16 進）。
[サブベンダー ID（SubVendor ID）]	PCI サブベンダー ID（16 進）。
Device ID	PCI デバイス ID（16 進）。
サブ デバイス ID	PCI サブデバイス ID（16 進）。
[製造日（Manufactured Date）]	MegaRAID カードが製造された日付（yyy-mm-dd 形式）。
改定	ボードのリビジョン番号（存在する場合）。
ブートドライブ	ブート ドライブの番号。
インターフェイス タイプ	ドライブが SAS または SATA であるかどうか

[Settings] 領域

表 *185 : [Settings]* 領域

名前	説明
物理ドライブステータス自動設定モード	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。
Rebuild Rate	低下した RAID ボリュームをコントローラが再ビルドするレート。 このレートは、使用可能な帯域幅合計に対するパーセンテージで表示されます。
[パトロール読み取りレート（Patrol Read Rate）]	整合性のないデータを検索するために、コントローラが物理ドライブのバックグラウンド読み取りを実行するレート。 このレートは、使用可能な帯域幅合計に対するパーセンテージで表示されます。
[整合性検査レート（Consistency Check Rate）]	冗長データの不整合を検索して修正するために、コントローラが仮想ドライブをスキャンするレート。 このレートは、使用可能な帯域幅合計に対するパーセンテージで表示されます。

名前	説明
[ECC バケット リーク レート（ECC Bucket Leak Rate）]	エラー訂正コード（ECC）の単一ビット エラー バケット リーク レート（分単位）。 ECCにより、コントローラは物理ドライブからの読み取り中に単一ビットエラーを検出したときに、エラーカウンタを増分します。このフィールドで定義された時間（分）が経過するたびに、コントローラはエラー カウンタを減少させます。 エラー カウンタがシステム定義の最大数に達すると、コントローラはイベント メッセージをシステムに送信します。
JBOD	このフィールドに [true] と表示される場合、JBOD は有効にされています。
[PD 失敗履歴の保持（Maintain PD Fail History）]	このフィールドに [true] と表示される場合、コントローラは不良と判断された物理ドライブをサーバの再起動間で記憶します。
バッテリー警告	このフィールドに [true] と表示される場合、バッテリ欠落警告は無効です。

表 *186 : [HW* 設定（*HW Configuration*）*]* エリア

名前	説明
[コントローラ SAS アドレス（Controller SAS Address）]	MegaRAID コントローラは、最大 16 個のシリアル接続 SCSI（SAS）アドレスを持つことができます。このフィールドには、最初の 8 個の SAS アドレス（使用中の場合）が表示されます。
[BBU あり（BBU Present）]	このフィールドに [true] と表示される場合、バッテリ バックアップ ユニットが存在します。
[メモリの有無（Memory Present）]	このフィールドに [true] と表示される場合、メモリが存在します。
フラッシュあり	このフィールドに [true] と表示される場合、フラッシュ メモリが存在します。

表 *187 : [Capabilities (*機能*)]* 領域

名前	説明
サポートされる RAID レベル	コントローラでサポートされる RAID レベル。これは次のいずれか、または複数の値になります。 • [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 1E]：統合オフセット ストライプ ミラーリング • [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。 • [Raid srl-03]：スパンされたセカンダリ RAID レベル • [Raid 00]：スパンされたストライピング。 • [Raid 1e-rlq0]：スパンを使用しない統合隣接ストライプ ミラーリング。 • [Raid 1e0-rlq0]：スパンを使用する統合隣接ストライプ ミラーリング。

表 *188 : [Error Counters]* 領域

名前	説明
メモリの修正可能なエラー数	コントローラ メモリ内の修正可能なエラーの数。

コピーバック操作の開始

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**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 右側のペインの **[物理ドライブ情報（Physical Drive Info）]** タブをクリックし、オンライン状態のドライブを選択します。

ステップ 4 **[アクション（Actions）]** ドロップダウン リストで、**[コピーバックの開始（Start Copyback）]** をクリックします。

ステップ 5 **[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 6 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 7 [コピーバックの開始（Start Copyback）] をクリックします。

ステップ 8 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 サーバーでは、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。

一部の C シリーズ 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として、内部 Secure Digital（SD）メモリ カードをサポートします。SD カードは、Cisco Flexible Flash ストレージ アダプタによってホストされます。

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 番目はユーザー 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 サーバー用の『Cisco UCS サーバー 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* シリーズ サーバー ドキュメンテーション ロードマップ』 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。

アクション	説明
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。
デュアル非ペア カード	サーバー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。 サーバーが稼働しているときにこのシナリオが検出された場合、ユーザーが新しい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。この状態は、Cisco IMC GUI または Cisco IMC CLI で確認できます。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 **[構成のリセット（Reset Configuration）]** オプションを使用するか、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、最新の Cisco IMC 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 権限で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 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[Cisco FlexFlash]**。

ステップ 3 右側ペインの **[コントローラ情報（Controller Info）]** タブの **[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 [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 *189 : Cisco UCS 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。
[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。

名前	説明
[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 にアクセスする際に、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読み取りエラーの数。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 5 [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 権限で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 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**で、適切な Cisco Flexible Flash コントローラをクリックします。

ステップ 3 **[アクション（Actions）]** ドロップダウン リストで、**[ファームウェア モードの設定（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 権限で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 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**で、**Cisco FlexFlash** をクリックします。

ステップ 3 **[アクション（Actions）]** ドロップダウン リストで、**[カードの設定（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
[Mode] フィールド	モード タイプをミラーとして表示します。
[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。

名前	説明
[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 5 [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

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。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 権限で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 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**で、**[FlexFlash]** をクリックします。

ステップ 3 **[アクション（Actions）]** 領域で、**[ブート オーバーライドの優先順位（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

通常の動作では、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 権限で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 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**で、適切な Cisco FlexFlash コントローラをクリックします。

ステップ 3 [Cisco FlexFlash] ペインの [Controller Info] タブをクリックします。

ステップ 4 右ペインの **[アクション（Actions）]** ドロップダウンリストで、**[FlexFlash コントローラのリセット（Reset FlexFlash Controller）]**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。

仮想ドライブの編集

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**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 右側ペインで **[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 選択したドライブの近くにある 3 つの水平のドットをクリックし、**[仮想ドライブの編集（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。

仮想ドライブの消去

始める前に

- このタスクを実行するには、admin 権限で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 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**で、適切な Cisco FlexFlash コントローラをクリックします。

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 権限で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 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]**>**[コントローラ（Controllers）]**で、適切な Cisco FlexFlash コントローラをクリックします。

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 権限で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 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**で、適切な Cisco Flexible Flash コントローラをクリックします。

ステップ 3 **[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 **[仮想ドライブ情報（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、[イメージの追加（Add Image）] をクリックします。

ステップ 5 [Add Image] をクリックします。

ステップ 6 [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。
[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。
[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`**

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**
[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。

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 権限で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 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**で、適切な Cisco Flexible Flash コントローラをクリックします。

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 権限で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 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**で、適切な Cisco Flexible Flash コントローラをクリックします。

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。
- ホストの接続が停止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 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**で、適切な Cisco Flexible Flash コントローラをクリックします。

ステップ 3 **[コントローラ情報（Controller Info）]** タブをクリックします。

ステップ 4 右ペインの [**アクション（Actions）]** ドロップダウンリストで、**[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 5 [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 6 [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 Cisco Flexible Flash カードがあります。
- 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 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**で、適切な Cisco Flexible Flash コントローラをクリックします。

ステップ 3 **[コントローラ情報（Controller Info）]** タブをクリックします。

ステップ 4 右側ペインの **[アクション（Actions）]** ドロップダウン リストの **[カード設定の同期（Synchronize Card Configuration）]** をクリックします。

ステップ 5 [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 6 [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 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**で、適切な Cisco Flexible Flash コントローラをクリックします。

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） • 警告 • 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。 [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 [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。
[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

Cisco UCS M5 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 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**で、適切な Cisco FlexUtil コントローラをクリックします。

ステップ 3 **[一般（General）]** タブの **[アクション（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。
[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。

名前	説明
[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 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**で、適切な FlexUtil コントローラをクリックします。

ステップ 3 **[一般（General）]** タブ > **[アクション（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 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**で、適切な FlexUtil コントローラをクリックします。

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。

名前	説明
[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 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**で、適切な FlexUtil コントローラをクリックします。

ステップ 3 右側のペインの **[物理ドライブ情報（Physical Drive Info）]** タブで、次のフィールドを確認します。

名前	説明
[スロット ID（Slot ID）]	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。
Disk Type	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。

名前	説明
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。 • [Copyback]：ドライブはビジー状態で、コピーバック操作を実行しています。 • [Failed]：ドライブは使用中ですが、障害が発生しています。 • [Foreign configuration]：ドライブに外部設定が含まれます。 • [Global hot spare]：ドライブはグローバル スペア ドライブとして指定されています。 • [Dedicated hot spare]：ドライブは専用スペア ドライブとして指定されています。 • [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。 • [Ready to remove]：ドライブは削除の準備ができています。 • [Rebuild]：ドライブは現在再構築されています。 • [System]：ドライブはホストから見えますが、仮想ドライブに使用することはできません。 • [Unconfigured bad]：ドライブは障害が発生し、使用されていません。 • [Unconfigured good]：ドライブをドライブ グループまたはホット スペア プールに割り当てることができます。
容量(GB)	ドライブの容量（ギガバイト単位）。
モデル（**Model**）	ドライブのベンダー名。
ファームウェア	ドライブで実行されているファームウェア バージョン。

ステップ 4 ドライブを選択し、新しいペインで次の情報を確認します。

表 *190 :* 製品の詳細

名前	説明
電源の再投入回数	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）]	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)	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。
消耗状態 (日数)	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	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。
最大動作温度	ドライブがエラーなしで動作できる許容最高温度。
使用された予約済み容量の割合	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からのもの）。

表 *191 : [*全般（*General*）*]* タブ

名前	説明
メディア タイプ	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。
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。
シーケンス番号	コントローラがドライブの変更を追跡するために使用するシーケンス番号。

名前	説明
セキュリティが有効	このフィールドに [はい（Yes）] が表示されている場合は、物理ドライブで完全なディスク暗号化が有効になっています。
物理ブロックサイズ	ドライブの物理ブロック サイズを示します。
スロット番号	物理ドライブが存在するスロット番号。
Device ID	ドライブのデバイス ID。
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。
UCS製品ID	
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。
ドライブのシリアル番号	ドライブのシリアル番号。
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）。
非強制サイズ	強制のために失われた領域を含む容量（MB単位）。
[強制サイズ（Coerced Size）]	強制的な丸め処理の実行後の容量（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。

表 *192 :* 正常性ステータス

名前	説明
[ロケータ LED（Locator LED）] トグル ボタン	ドライブ LED をオンまたはオフにできます。
[ヘルス（Health）]	このフィールドには、物理ドライブの状態が表示されます。

名前	説明
状態	ドライブのステータス。次のいずれかになります。 • [キャッシュ縮退（Cache degraded）]：BBU でキャッシュの一貫性を保証できないため、コントローラにより仮想ドライブの [書き込みポリシー（Write Policy）] 設定が [ライトバック（Write Back）] から [ライトスルー（Write Through）] に変更されました。 • [**Copyback**]：ドライブはビジー状態で、コピーバック操作を実行しています。 • [**Failed**]：ドライブは使用中ですが、障害が発生しています。 • [**Foreign configuration**]：ドライブに外部設定が含まれます。 • [**Global hot spare**]：ドライブはグローバル スペア ドライブとして指定されています。 • [**Dedicated hot spare**]：ドライブは専用スペア ドライブとして指定されています。 • [**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。 • [**Ready to remove**]：ドライブは削除の準備ができています。 • [**Rebuild**]：ドライブは現在再構築されています。 • [**System**]：ドライブはホストから見えますが、仮想ドライブに使用することはできません。 • [**Unconfigured bad**]：ドライブは障害が発生し、使用されていません。 • [**Unconfigured good**]：ドライブをドライブ グループまたはホット スペア プールに割り当てることができます。

名前	説明
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]：JBOD 状態のドライブ。 • [**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。 • [**Unconfigured bad**]：ドライブは障害が発生し、使用されていません。
コピーバックの操作ステータス	コピーバックの操作ステータス。次のいずれかになります。 • [不明（Unknown）]：完了した割合は不明です。 • [進行中（In Progress）]：[コピーバックの完了率（Copyback Percent Complete）] フィールドに表示される再構築プロセス。ホットスペアが設定され、RAID グループからディスクを削除した後、そのディスクを交換すると、ホットスペースを解放する再構築が行われます。 • [完了（Completed）]：コピーバック操作が完了しています。
コピーバックの完了率	コピーバック操作の完了率（パーセント値）。
[Power State] フィールド	現在の電源状態。次のいずれかになります。 • [active]：ドライブは正常に動作しています。 • [powersave]：ドライブはスピンダウンしています。 • [transitioning]：ドライブはスピンアップしています。

表 *193 : Error Count*

名前	説明
メディアエラー数	ドライブが最初に取り付けられた時点、またはホストが再起動された時点から発生したメディアエラーの数。

名前	説明
[他のエラー数（Other Error Count）] フィールド	ドライブが最初に取り付けられた時点、またはホストが再起動された時点から発生した非メディア エラーの数。
予測障害回数	ドライブで障害が発生した可能性があることをコントローラが予測した回数。

ステップ 5 [閉じる（Close）] をクリックします。

仮想ドライブのプロパティの表示

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**で、適切な FlexUtil コントローラをクリックします。

ステップ 3 右側のペインの **[仮想ドライブ情報（Virtual Drive Info）]** タブで、次のフィールドを確認します。

表 *194 : [*仮想ドライブ情報（***Virtual Drive Info***）*]*

名前	説明
ID	仮想ドライブの番号。詳細を確認するには、 をクリックします。
名前（Name）	仮想ドライブの名前。

名前	説明
ステータス（**Status**）	仮想ドライブの状態。次のいずれかになります。 • [キャッシュ縮退（Cache degraded）]：このドライブの要求時の書き込みキャッシュ ポリシーは [ライトバック（Write Back）] ですが、BBU に欠陥があるか、BBUの学習サイクルが進行中であるため、ドライブは現在、[ライトスルー（Write Through）] モードで動作しています。 • **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。 • [Partially Degraded]：ドライブは冗長性を多少失いましたが、まだ一部の冗長性が残っています。たとえば、3 方向の RAID 1 ミラー ドライブで 1 台のディスクを失っても、2 方向の冗長性は維持されます。 • [Optimal]：ドライブには完全な冗長性があります。
Size (GB)	ドライブの容量（MB 単位）。
[RAID レベル（RAID Level）]	仮想ドライブ上の RAID レベル。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]：パリティ付きストライピング。 • [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。 • [Raid 00]：スパンされたストライピング。

名前	説明
ブートドライブ	仮想ドライブがブート ドライブとして指定されているかどうか。

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 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**で、適切な FlexUtil コントローラをクリックします。

ステップ 3 右側ペインで **[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**

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 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**で、適切な FlexUtil コントローラをクリックします。

ステップ 3 右側ペインで **[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）] タブをクリックします。

ステップ 5 [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 6 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 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**で、適切な FlexUtil コントローラをクリックします。

ステップ 3 右側ペインで **[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 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 権限でログインする必要があります。

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**で、適切な FlexUtil コントローラをクリックします。

ステップ 3 右側ペインで **[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 **[仮想ドライブ情報（Virtual Drives Info）]** 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 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**から、適切な M.2 Raid コントローラをクリックします。

ステップ 3 右側のペインの **[コントローラ情報（Controller Info）]** タブ > **[一般（General）]** タブで、次の情報を確認します。

名前	説明
製品名	MegaRAID コントローラの名前。
製品ID	RAID コントローラのシスコ製品番号。

名前	説明
[複合状態（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**
コントローラステータス	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。
セキュリティ	現在の状態に応じてコントローラ ロック キーを表示します。 （注） • このオプションを使用できるのは一部の C シリーズ サーバだけです。 • ドライブ セキュリティを無効にすると、すべてのセキュア ドライブ上のデータを使用できなくなります。
[Serial Number] フィールド	MegaRAID コントローラのシリアル番号。
[RAID Chip Temperature] フィールド	コントローラの温度（摂氏）。
[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。

名前	説明
[Consistency Check Rate] フィールド	冗長データの不整合を検索して修正するために、コントローラが仮想ドライブをスキャンするレート。 このレートは、使用可能な帯域幅合計に対するパーセンテージで表示されます。
[PCI スロット（PCI Slot）]	コントローラが配置されている PCIe スロットの名前。
Vendor ID	PCI ベンダー ID（16 進）。
[サブベンダー ID（SubVendor ID）]	PCI サブベンダー ID（16 進）。
Device ID	PCI デバイス ID（16 進）。
サブ デバイス ID	PCI サブデバイス ID（16 進）。
[製造日（Manufactured Date）]	MegaRAID カードが製造された日付（yyy-mm-dd 形式）。
改定	ボードのリビジョン番号（存在する場合）。
ブートドライブ	ブート ドライブの番号。
インターフェイス タイプ	ドライブが SAS または SATA であるかどうか

ステップ 4 右側のペインの **[コントローラ情報（Controller Info）]** タブ > **[設定（Settings）]** タブで、次の情報を確認します。

表 *195 : [Settings]* 領域

名前	説明
物理ドライブステータス自動設定モード	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。

名前	説明
Rebuild Rate	低下した RAID ボリュームをコントローラが再ビルドするレート。 このレートは、使用可能な帯域幅合計に対するパーセンテージで表示されます。
[パトロール読み取りレート（Patrol Read Rate）]	整合性のないデータを検索するために、コントローラが物理ドライブのバックグラウンド読み取りを実行するレート。 このレートは、使用可能な帯域幅合計に対するパーセンテージで表示されます。
[整合性検査レート（Consistency Check Rate）]	冗長データの不整合を検索して修正するために、コントローラが仮想ドライブをスキャンするレート。 このレートは、使用可能な帯域幅合計に対するパーセンテージで表示されます。
[ECC バケット リーク レート（ECC Bucket Leak Rate）]	エラー訂正コード（ECC）の単一ビット エラー バケット リーク レート（分単位）。 ECC により、コントローラは物理ドライブからの読み取り中に単一ビットエラーを検出したときに、エラーカウンタを増分します。このフィールドで定義された時間（分）が経過するたびに、コントローラはエラー カウンタを減少させます。 エラー カウンタがシステム定義の最大数に達すると、コントローラはイベントメッセージをシステムに送信します。
JBOD	このフィールドに [true] と表示される場合、JBOD は有効にされています。
[PD 失敗履歴の保持（Maintain PD Fail History）]	このフィールドに [true] と表示される場合、コントローラは不良と判断された物理ドライブをサーバの再起動間で記憶します。
バッテリー警告	このフィールドに [true] と表示される場合、バッテリ欠落警告は無効です。

表 *196 : [HW* 設定（*HW Configuration*）*]* エリア

名前	説明
[コントローラ SAS アドレス（Controller SAS Address）]	MegaRAID コントローラは、最大 16 個のシリアル接続 SCSI（SAS）アドレスを持つことができます。このフィールドには、最初の 8 個の SAS アドレス（使用中の場合）が表示されます。
[BBU あり（BBU Present）]	このフィールドに [true] と表示される場合、バッテリ バックアップ ユニットが存在します。
[メモリの有無（Memory Present）]	このフィールドに [true] と表示される場合、メモリが存在します。
フラッシュあり	このフィールドに [true] と表示される場合、フラッシュ メモリが存在します。

表 *197 : [Capabilities (*機能*)]* 領域

名前	説明
サポートされる **RAID** レベル	コントローラでサポートされる RAID レベル。これは次のいずれか、または複数の値になります。 • [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 1E]：統合オフセット ストライプ ミラーリング • [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。 • [Raid srl-03]：スパンされたセカンダリ RAID レベル • [Raid 00]：スパンされたストライピング。 • [Raid 1e-rlq0]：スパンを使用しない統合隣接ストライプ ミラーリング。 • [Raid 1e0-rlq0]：スパンを使用する統合隣接ストライプ ミラーリング。

表 *198 : [Error Counters]* 領域

名前	説明
メモリの修正可能なエラー数	コントローラ メモリ内の修正可能なエラーの数。

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 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**から、適切な M.2 raid コントローラをクリックします。

ステップ 3 **[物理ドライブ情報（Physical Drive Info）]** タブをクリックし、[物理ドライブ（Physical Drives）] 領域で次の情報を確認します。

名前	説明
[スロット ID（Slot ID）]	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。
Disk Type	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。

名前	説明
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。 • [Copyback]：ドライブはビジー状態で、コピーバック操作を実行しています。 • [Failed]：ドライブは使用中ですが、障害が発生しています。 • [Foreign configuration]：ドライブに外部設定が含まれます。 • [Global hot spare]：ドライブはグローバル スペア ドライブとして指定されています。 • [Dedicated hot spare]：ドライブは専用スペア ドライブとして指定されています。 • [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。 • [Ready to remove]：ドライブは削除の準備ができています。 • [Rebuild]：ドライブは現在再構築されています。 • [System]：ドライブはホストから見えますが、仮想ドライブに使用することはできません。 • [Unconfigured bad]：ドライブは障害が発生し、使用されていません。 • [Unconfigured good]：ドライブをドライブ グループまたはホット スペア プールに割り当てることができます。
容量(GB)	ドライブの容量（ギガバイト単位）。
モデル（**Model**）	ドライブのベンダー名。
ファームウェア	ドライブで実行されているファームウェア バージョン。

ステップ 4 ドライブを選択し、新しいペインに表示される次の情報を確認します。

表 *199 :* [全般（*General*）] タブ

名前	説明
メディア タイプ	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。
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。
シーケンス番号	コントローラがドライブの変更を追跡するために使用するシーケンス番号。
セキュリティが有効	このフィールドに [はい（Yes）] が表示されている場合は、物理ドライブで完全なディスク暗号化が有効になっています。
物理ブロックサイズ	ドライブの物理ブロック サイズを示します。
スロット番号	物理ドライブが存在するスロット番号。
Device ID	ドライブのデバイス ID。
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。
UCS製品ID	
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。
ドライブのシリアル番号	ドライブのシリアル番号。
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）。
非強制サイズ	強制のために失われた領域を含む容量（MB 単位）。
[強制サイズ（Coerced Size）]	強制的な丸め処理の実行後の容量（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。

表 *200 :* 正常性ステータス

名前	説明
[ロケータ LED（Locator LED）] トグル ボタン	ドライブ LED をオンまたはオフにできます。

名前	説明
[ヘルス（Health）]	このフィールドには、物理ドライブの状態が表示されます。

名前	説明
状態	ドライブのステータス。次のいずれかになります。 • [キャッシュ縮退（Cache degraded）]：BBU でキャッシュの一貫性を保証できないため、コントローラにより仮想ドライブの [書き込みポリシー（Write Policy）] 設定が [ライトバック（Write Back）] から [ライトスルー（Write Through）] に変更されました。 • [**Copyback**]：ドライブはビジー状態で、コピーバック操作を実行しています。 • [**Failed**]：ドライブは使用中ですが、障害が発生しています。 • [**Foreign configuration**]：ドライブに外部設定が含まれます。 • [**Global hot spare**]：ドライブはグローバル スペア ドライブとして指定されています。 • [**Dedicated hot spare**]：ドライブは専用スペア ドライブとして指定されています。 • [**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。 • [**Ready to remove**]：ドライブは削除の準備ができています。 • [**Rebuild**]：ドライブは現在再構築されています。 • [**System**]：ドライブはホストから見えますが、仮想ドライブに使用することはできません。 • [**Unconfigured bad**]：ドライブは障害が発生し、使用されていません。 • [**Unconfigured good**]：ドライブをドライブ グループまたはホット スペア プールに割り当てることができます。

名前	説明
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]：JBOD 状態のドライブ。 • [**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。 • [**Unconfigured bad**]：ドライブは障害が発生し、使用されていません。
コピーバックの操作ステータス	コピーバックの操作ステータス。次のいずれかになります。 • [不明（Unknown）]：完了した割合は不明です。 • [進行中（In Progress）]：[コピーバックの完了率（Copyback Percent Complete）] フィールドに表示される再構築プロセス。ホットスペアが設定され、RAID グループからディスクを削除した後、そのディスクを交換すると、ホットスペースを解放する再構築が行われます。 • [完了（Completed）]：コピーバック操作が完了しています。
コピーバックの完了率	コピーバック操作の完了率（パーセント値）。
[Power State] フィールド	現在の電源状態。次のいずれかになります。 • [active]：ドライブは正常に動作しています。 • [powersave]：ドライブはスピンダウンしています。 • [transitioning]：ドライブはスピンアップしています。

表 *201 : Error Count*

名前	説明
メディアエラー数	ドライブが最初に取り付けられた時点、またはホストが再起動された時点から発生したメディアエラーの数。

名前	説明
[他のエラー数（Other Error Count）] フィールド	ドライブが最初に取り付けられた時点、またはホストが再起動された時点から発生した非メディア エラーの数。
予測障害回数	ドライブで障害が発生した可能性があることをコントローラが予測した回数。

表 *202 :* **製品の詳細**

名前	説明
電源の再投入回数	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）]	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)	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。
消耗状態 (日数)	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	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。
最大動作温度	ドライブがエラーなしで動作できる許容最高温度。
使用された予約済み容量の割合	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からのもの）。

ステップ 5 [閉じる（Close）] をクリックします。

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 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** > **[コントローラ（Controllers）]**から、適切な M.2 Raid コントローラをクリックします。

ステップ 3 **[仮想ドライブ情報（Virtual Drive Info）]** タブをクリックし、次の情報を確認します。

表 *203 : [*仮想ドライブ情報（***Virtual Drive Info***）*]*

名前	説明
ID	仮想ドライブの番号。詳細を確認するには、 をクリックします。
名前（Name）	仮想ドライブの名前。
ステータス（Status）	仮想ドライブの状態。次のいずれかになります。 • [キャッシュ縮退（Cache degraded）] : このドライブの要求時の書き込みキャッシュ ポリシーは [ライトバック（Write Back）] ですが、BBU に欠陥があるか、BBU の学習サイクルが進行中であるため、ドライブは現在、[ライトスルー（Write Through）] モードで動作しています。 • **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。 • [Partially Degraded] : ドライブは冗長性を多少失いましたが、まだ一部の冗長性が残っています。たとえば、3 方向の RAID 1 ミラー ドライブで 1 台のディスクを失っても、2 方向の冗長性は維持されます。 • [Optimal] : ドライブには完全な冗長性があります。
Size (GB)	ドライブの容量（MB 単位）。

名前	説明
[RAID レベル（RAID Level）]	仮想ドライブ上の RAID レベル。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]：パリティ付きストライピング。 • [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。 • [Raid 00]：スパンされたストライピング。
ブートドライブ	仮想ドライブがブートドライブとして指定されているかどうか。

ステップ 4 仮想ドライブを選択し、次の情報を確認します。

表 *204 : RAID* の詳細（*RAID Details*）

名前	説明
名前（**Name**）	仮想ドライブの名前。
ストリップ サイズ	各ストライプのサイズ（KB 単位）。
[スパンごとのドライブ数（Drives Per Span）]	各スパンに含まれるドライブの数。
スパンの深さ	仮想ドライブを構成するスパンの数。
専用ホットスペアドライブ	

名前	説明
[Access Policy] フィールド	ホスト オペレーティング システムで仮想ドライブへのアクセスに使用できる方法。次のいずれかになります。 • [Blocked]：ホストはドライブにアクセスできません。 • [Read-Write]：ホストはドライブにフル アクセスできます。 • [Read-Only]：ホストはドライブからデータの読み取りだけを行うことができます。
[Cache Policy] フィールド	キャッシュ ポリシー。次のいずれかになります。 • [Allow]：読み取りと書き込みがコントローラにキャッシュされます。 • [Allow Read]：読み取りのみがコントローラにキャッシュされます。 • [Allow Write]：書き込みのみがコントローラにキャッシュされます。 • [Direct]：読み取りも書き込みもコントローラにキャッシュされません。
[Read Ahead Policy] フィールド	コントローラによる先行読み出し機能の使用方法。次のいずれかになります。 • [Adaptive]：先行読み出しがイネーブルで、コントローラがパフォーマンスを向上させるときに使用されます。 • [Always]：先行読み出しがイネーブルで、常に使用されます。 • [なし（None）]：先行読み出しがディセーブルです。
セキュリティに対応	このフィールドに [はい（Yes）] が表示されている場合は、物理ドライブがセキュリティ対応であることを示します。
[整合性チェックの運用ステータス（Consistency Check Operation Status）]	

名前	説明
[要求時の書き込みキャッシュ ポリシー（Requested Write Cache Policy）]	コントローラによるキャッシングの処理方法。次のいずれかになります。 • [Write Through]：書き込まれたデータはキャッシュに格納され、物理ドライブにも書き込まれます。データが物理ドライブに書き込まれるまでは、トランザクションは完了としてマークされません。 • [Write Back]：書き込まれたデータはキャッシュに格納され、帯域幅が使用できる場合に物理ドライブに書き込まれます。このポリシーでは[ライトバック（Write Through）] モードよりも書き込みのパフォーマンスが向上しますが、BBU に欠陥がある場合、または BBU の学習サイクルが進行中の場合は、[ライトスルー（Write Through）] モードにフォールバックします。 • [不良 BBU でもライトバックを維持（Write Back Even If Bad BBU）]：BBU が不良であっても、キャッシングは [ライトバック（Write Back）] モードに維持されます。 電源障害が発生した場合、このモードではデータが失われる可能性があります。

名前	説明
[現在の書き込みキャッシュ ポリシー（Current Write Cache Policy）]	現在実行中のキャッシュ ポリシー。次のいずれかになります。 • [Write Through]：書き込まれたデータはキャッシュに格納され、物理ドライブにも書き込まれます。データが物理ドライブに書き込まれるまでは、トランザクションは完了としてマークされません。 • [Write Back]：書き込まれたデータはキャッシュに格納され、帯域幅が使用できる場合に物理ドライブに書き込まれます。このポリシーでは[ライトバック（Write Through）] モードよりも書き込みのパフォーマンスが向上しますが、BBU に欠陥がある場合、または BBU の学習サイクルが進行中の場合は、[ライトスルー（Write Through）] モードにフォールバックします。 • [不良 BBU でもライトバックを維持（Write Back Even If Bad BBU）]：BBU が不良であっても、キャッシングは [ライトバック（Write Back）] モードに維持されます。 電源障害が発生した場合、このモードではデータが失われる可能性があります。
ディスクキャッシュポリシー	コントローラによる物理ディスク キャッシングの処理方法。次のいずれかになります。 • [Disable]：キャッシングは物理ドライブでディセーブルです。 • [Enable]：キャッシングは物理ドライブでイネーブルです。 • [Unchanged]：物理ドライブに指定されているキャッシング ポリシーがコントローラによって使用されます。 （注） 複数の仮想ドライブでドライブ グループを共有する場合、すべてのドライブで同じディスク キャッシュ ポリシーを使用する必要があります。それ以外の場合、キャッシング ポリシーはランダムに物理ドライブに割り当てられることがあります。

名前	説明
ブート ドライブ	このフィールドに [true] と表示されている場合、仮想ドライブはブート ドライブとして指定されています。
セキュリティが有効	このフィールドに [はい（Yes）] が表示されている場合は、物理ドライブで完全なディスク暗号化が有効になっています。

ステップ 5 [閉じる（Close）] をクリックします。

Cisco FlexMMC

Cisco FlexMMC の詳細の表示

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** ページで、**[Cisco FlexMMC]** をクリックします。

ステップ 3 **[IMC イメージのストレージ（Storage for IMC Image）]** エリアで、次を表示します：

表 *205 : IMC*イメージ エリア用のストレージ

名前	説明
[IMC イメージのストレージ（Storage for IMC Images）] 円グラフ	Cisco IMC イメージの合計スペース、使用可能なスペース、および使用済みスペースを分析するのに役立ちます。
ファイル名 カラム	Cisco IMC イメージ ファイルの名前。
ファイル サイズカラム	Cisco IMC イメージ ファイルのサイズ。
ファイル タイプ カラム	Cisco IMC イメージ ファイルのタイプ。
[Status] カラム	Cisco IMCイメージ ファイルのステータス。

ステップ 4 **[ユーザー ファイル エリアのストレージ（Storage for User Files Area）]** エリアで、次を表示します：

表 *206 :* ユーザー ファイル エリアのストレージ

名前	説明
[ユーザーファイルのストレージ（Storage for User Files）] 円グラフ	ユーザーファイルの合計スペース、使用可能なスペース、および使用済みスペースを分析するのに役立ちます。
ファイル名 カラム	ユーザー ファイルの名前。
ファイル サイズカラム	ユーザー ファイルのサイズ。
ファイル タイプ カラム	ユーザー ファイルのタイプ。
[Status] カラム	ユーザー ファイルのステータス。

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。

手順の概要

1. **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。
2. **[ストレージ（Storage）]** ページで、**[Cisco FlexMMC]** をクリックします。
3. **[IMC イメージのストレージ（Storage for IMC Images）]** 領域で、**[ファイルのアップロード（Upload File）]**をクリックします。
4. **[IMC イメージ パーティションにファイルをアップロード（Upload File to IMC Images partition）]** ダイアログボックスで、次に値を入力します :
5. [保存（Save）] をクリックします。

手順の詳細

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** ページで、**[Cisco FlexMMC]** をクリックします。

ステップ 3 **[IMC イメージのストレージ（Storage for IMC Images）]** 領域で、**[ファイルのアップロード（Upload File）]** をクリックします。

[IMC イメージ パーティションにファイルをアップロード（Upload File to IMC Images partition）] ダイアログ ボックスが表示されます。

ステップ 4 **[IMC イメージ パーティションにファイルをアップロード（Upload File to IMC Images partition）]** ダイアログボックスで、次に値を入力します：

名前	説明
[ファイルの場所] 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。

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**
[Username] フィールド	（注） このフィールドは NFS マウントでは使用できません。 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	（注） このフィールドは NFS マウントでは使用できません。 選択されたユーザー名のパスワード（必要な場合）。
[Add] ボタン	システムにファイルを追加できます。

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

- 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。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がないことを確認してください。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。

手順の概要

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。
2. **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。
3. **[ストレージ（Storage）]** ページで、**[Cisco FlexMMC]** をクリックします。
4. **[IMC イメージのストレージ（Storage for IMC Images）**] エリア > **[コピーされたファイル（Files Copied）]** エリアで、イメージ ファイルを選択します。
5. **[ファイルの削除（Delete File）]** をクリックします。

手順の詳細

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 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 3 **[ストレージ（Storage）]** ページで、**[Cisco FlexMMC]** をクリックします。

ステップ 4 **[IMC イメージのストレージ（Storage for IMC Images）**] エリア > **[コピーされたファイル（Files Copied）]** エリアで、イメージ ファイルを選択します。

ステップ 5 **[ファイルの削除（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

手順の概要

1. **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。
2. **[ストレージ（Storage）]** ページで、**[Cisco FlexMMC]** をクリックします。
3. **[IMC イメージのストレージ（Storage for IMC Images）**] エリア > **[コピーされたファイル（Files Copied）]** エリアで、イメージ ファイルを選択します。
4. **[イメージのマップ（Map Image）]** または **[イメージのマップ解除（UnMap Image）]** をクリックします。

手順の詳細

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。

ステップ 2 **[ストレージ（Storage）]** ページで、**[Cisco FlexMMC]** をクリックします。

ステップ 3 **[IMC イメージのストレージ（Storage for IMC Images）]** エリア > **[コピーされたファイル（Files Copied）]** エリアで、イメージ ファイルを選択します。

ステップ 4 **[イメージのマップ（Map Image）]** または **[イメージのマップ解除（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。

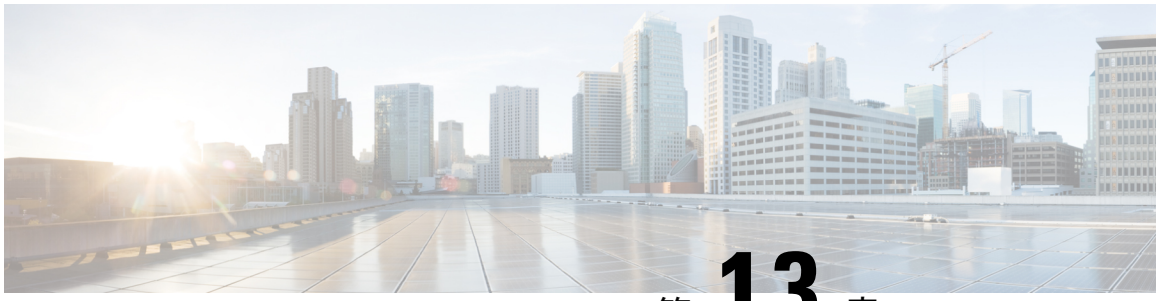
（注） この手順を実行すると、アップロードされたすべてのイメージが削除されます。

始める前に

- 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。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がないことを確認してください。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	**[アプリ（Apps）]** ドロップダウン リストから、**[ストレージ（Storage）]** を選択します。	
ステップ 2	**[ストレージ（Storage）]** ページで、**[Cisco FlexMMC]** をクリックします。	
ステップ 3	右ペインの **[アクション（Actions）]** ドロップダウンリストで、**[デフォルトへのリセット（Reset 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

•
• TLS v1.2 の有効化または無効化 （557 ページ）
• HTTP の設定 （559 ページ）
• SSH の設定 （561 ページ）
• XML API の設定 （562 ページ）
• Redfish のイネーブル化 （563 ページ）
• IPMI の設定 （564 ページ）
• SNMP の設定 （565 ページ）
• 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 （571 ページ）

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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[通信サービス（Communication Services）]** メニューをクリックします。

ステップ 3 [通信サービス（Communication Services）] タブを選択します。

ステップ 4 **[TLS 構成（TLS Configuration）]** エリアで、次のプロパティを更新します。

表 *207 : TLS* 構成 エリア

名前	説明
[TLS v1.2 有効化（Enabled TLS v1.2）] トグル ボタン	Cisco IMC で TLS v1.2 を有効または無効にすることができます。 （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バージョンの設定	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。 （注） FIPS が有効になっている場合、**カスタム** 暗号を設定することはできません。 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。 FIPS が有効になっている場合、**カスタム**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。

ステップ 5 [保存（Save）] をクリックします。

HTTP の設定

始める前に

この手順を実行するには、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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[通信サービス（Communication Services）]** メニューをクリックします。

ステップ 3 [通信サービス（Communication Services）] タブを選択します。

ステップ 4 [HTTP Properties] 領域で、次のプロパティを更新します。

表 *208 : [HTTP Properties]* 領域

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。 Cisco IMC にアクセスするための HTTPS サービスを有効または無効にすることができます。 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）] トグル ボタン	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。 HTTP サービスのみを有効/無効にして Cisco IMC にアクセスできます。 （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。
[HTTP から HTTPS へのリダイレクトの有効化（Redirect HTTP to HTTPS Enabled）] トグルボタン	（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。 HTTP 経由で試行される通信をすべて同等の HTTPS アドレスへリダイレクトする機能を有効/無効にします。 HTTP をイネーブルにする場合は、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。

名前	説明
[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。
[最大セッション数（Max Sessions）]	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を表示します。
アクティブセッション	Cisco IMC で現在実行されている HTTP および HTTPS セッションの数を表示します。

ステップ 5 [保存（Save）] 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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[通信サービス（Communication Services）]** メニューをクリックします。

ステップ 3 [通信サービス（Communication Services）] タブを選択します。

ステップ 4 [SSH Properties] 領域で、次のプロパティを更新します。

表 *209 : [SSH Properties]* 領域

名前	説明
[SSH 有効（SSH Enabled）] トグル ボタン	Cisco IMC で SSH を有効または無効にすることができます。
[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。

名前	説明
[最大セッション数（Max Sessions）]	Cisco IMC で許可されている SSH の同時セッションの最大数を表示します。
アクティブセッション	Cisco IMC で現在実行されている SSH セッションの数を表示します。

ステップ 5 [保存（Save）] をクリックします。

XML API の設定

Cisco IMC 用の XML API

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* ラックマウント サーバー *XML API* プログラマーズ ガイド』を参照してください。

XML API のイネーブル化

始める前に

この手順を実行するには、管理者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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[通信サービス（Communication Services）]** メニューをクリックします。

ステップ 3 [通信サービス（Communication Services）] タブを選択します。

ステップ 4 [XML API Properties] 領域で、次のプロパティを更新します。

表 210 : [XML API Properties] 領域

名前	説明
[XML API 有効（XML API Enabled）] トグル ボタン	このサーバー上の API アクセスを有効または無効にすることができます。

名前	説明
[最大セッション数（Max Sessions）]	Cisco IMC で許可されている API の同時セッションの最大数を表示します。
アクティブセッション	Cisco IMC で現在実行されている API セッションの数を表示します。

ステップ 5 [保存（Save）] 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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[通信サービス（Communication Services）]** メニューをクリックします。

ステップ 3 [通信サービス（Communication Services）] タブを選択します。

ステップ 4 [Redfishプロパティ（SSH Properties）] 領域で、次のプロパティを更新します。

表 *211 : [Redfish* のプロパティ（*Redfish Properties*****）]* 領域**

名前	説明
[Redfish 有効（Redfish Enabled）] トグル ボタン	Cisco IMC での Redfish アクセスを有効または無効にすることができます。
[最大セッション数（Max Sessions）]	Cisco IMC で許可されている Redfish の同時セッションの最大数を表示します。
アクティブセッション	Cisco IMC で現在実行されている Redfish セッションの数を表示します。

ステップ 5 [保存（Save）] 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

この手順を実行するには、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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[通信サービス（Communication Services）]** メニューをクリックします。

ステップ 3 [通信サービス（Communication Services）] タブを選択します。

ステップ 4 **[IPMI over LAN Properties]** 領域で、次のプロパティを更新します。

表 *212 : [IPMI over LAN Properties]* 領域

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 5 [保存（Save）] をクリックします。

SNMP の設定

SNMP

Cisco IMC は、サーバー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 v3 ユーザーは、DES セキュリティ プロトコルでは追加できません。

サポートされていないセキュリティ レベル、認証タイプ、またはプライバシー タイプの既存の v3 バージョンを選択すると、Cisco IMC GUI に警告が表示されます。ユーザーの詳細を選択して変更できます。

SNMP プロパティの設定

始める前に

この手順を実行するには、管理者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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[通信サービス（Communication Services）]** メニューをクリックします。

ステップ 3 **[SNMP]** タブを選択します。

ステップ 4 **[プロパティ（Properties）]** 領域で、次のプロパティを更新します。

表 *213:* プロパティ領域

名前	説明
[SNMP 有効（SNMP Enabled）] トグルボタン	サーバーが指定されたホストに SNMP トラップを送信する機能を有効/無効にします。 （注） SNMP を有効にするため、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、**[変更を保存（Save Changes）]** をクリックする必要があります。
[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。
[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。

名前	説明
[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。

ステップ 5 **[v2c プロパティ（v2c Properties）]** 領域で、次のプロパティを更新します。

表 *214 : [v2c* プロパティ（*v2c Properties*）*]* エリア

名前	説明
[SNMP v2c 有効（SNMP v2c Enabled）] トグル ボタン	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。
[Access Community String] フィールド	Cisco IMC が、任意の SNMP 操作を含める、デフォルトの SNMP v1 または v2c コミュニティ名。 最大 18 文字の文字列を入力します。
[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。

ステップ 6 **[v3 プロパティ（v3 Properties）]** 領域で、次のプロパティを更新します。

表 *215 : [v3* プロパティ（*v3 Properties*）*]* エリア

名前	説明
[SNMP v3 有効（SNMP v3 Enabled）] トグル ボタン	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 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。
[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。

ステップ 7 [保存（Save）] 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

この手順を実行するには、管理者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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[通信サービス（Communication Services）]** メニューをクリックします。

ステップ 3 **[SNMP]** タブを選択します。

ステップ 4 [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 5 [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。

表 *216:* トラップの追加/変更

名前	説明
[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**
[タイプ（Type）] 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。選択すると、確認応答が SNMP エンジンに送信されます。
[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。
[宛先アドレス（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。
[SNMP Port] フィールド	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。
[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。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 （任意） 加えて、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

この手順を実行するには、管理者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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[通信サービス（Communication Services）]** メニューをクリックします。

ステップ 3 **[SNMP]** タブを選択します。

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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[通信サービス（Communication Services）]** メニューをクリックします。

ステップ 3 **[SNMP]** タブを選択します。

ステップ 4 **[v3 ユーザー設定（v3 User Settings）]** 領域で、次のプロパティを更新します。

表 *217 : [v3* ユーザー設定（*v3 User Settings*）*]* エリア

名前	説明
[ID] カラム	SNMPユーザに対してシステムが割り当てる識別子。
[Name] カラム	SNMP ユーザ名。
[Auth Type] カラム	ユーザ認証タイプ。
[Privacy Type] カラム	ユーザ プライバシー タイプ。

ステップ 5 **[ユーザーの設定を変更するには、ここをクリックします（CLICK HERE to change the Users configurations）]** をクリックします。次を参照してください。 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 （305 ページ）

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

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

始める前に

この手順を実行するには、管理者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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[通信サービス（Communication Services）]** メニューをクリックします。

ステップ 3 **[メールアラート（Mail Alert）]** タブを選択します。

ステップ 4 [SMTP Properties] 領域で、次のプロパティを更新します。

表 *218 : [SMTP* プロパティ（*SMTP Properties*）*]* 領域

名前	説明
[SMTP 有効（SMTP Enabled）] トグルボタン	SMTP サービスを有効または無効にすることができます。

名前	説明
[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。

次のタスク

SMTP 電子メール受信者を追加するには、SMTP 電子メール受信者の追加 （572 ページ） を参照してください。

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

- この手順を実行するには、管理者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 （571 ページ）を参照してください。

手順

ステップ 1 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[通信サービス（Communication Services）]** メニューをクリックします。

ステップ 3 **[メールアラート（Mail Alert）]** タブを選択します。

ステップ 4 [SMTP Recipients] 領域で、次の手順を実行します。

- 受信者は追加できます。
- 受信者は削除できます。

ステップ 5 受信者を追加するには、**[+受信者を追加（+ Add Recipient）]**をクリックし、電子メール ID を入力して、**[レポートする最小シビラティ（Minimum Severity to Report）]** ドロップダウン リストからシビラティ（重大度）を選択します。

[レポートする最小シビラティ（Minimum Severity to Report）] ドロップダウン リストで、電子メール アラートが送られる最小シビラティ 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。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 [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）

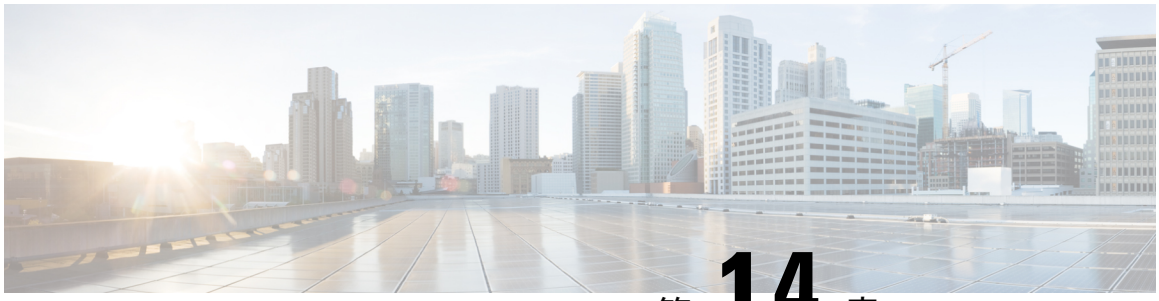
ステップ 8 （任意） 電子メール受信者を削除するには、電子メール受信者を選択し、**[行を削除（Delete Rows）]** をクリックします。

ステップ 9 （任意） [OK] をクリックして確認します。

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。



第 14 章

証明書とサーバー セキュリティの管理

•
• サーバ証明書の管理 （575 ページ）
• 外部証明書の管理 （588 ページ）
• SPDM セキュリティ：MCTP SPDM （593 ページ）
• キー管理相互運用性プロトコル （603 ページ）
• Cisco IMC での FIPS 140-2 の準拠 （618 ページ）

サーバ証明書の管理

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）

アップロードする証明書は、Cisco IMC によって生成された CSR から作成する必要があります。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。

証明書署名要求を生成する

（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

- この手順を実行するには、管理者ユーザー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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[セキュリティ管理（Security Management）]** メニューをクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]** メニューで **[証明書管理（Certificate Management）]** を選択します。

ステップ 4 **[アクション（Actions）]** ドロップダウンリストから、**[証明書署名要求の生成（Generate Certificate Signing Request）]** を選択します。

[証明書署名要求の生成（Generate Certificate Signing Request）] ダイアログボックスが表示されます。

ステップ 5 **[証明書署名要求の生成（Generate 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。

表 *219 :* 証明書署名要求の生成

名前	説明
共通名	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
Subject Alternate Name	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。 さまざまなタイプとして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。
[組織名（Organization Name）] フィールド	証明書を要求している組織。
[Organization Unit] フィールド	組織ユニット
[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。
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。 • 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。 （注） 署名アルゴリズム ECDSA および RSA は、Cisco UCS C シリーズ M7 サーバでのみ使用できます。

名前	説明
[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、Cisco UCS C シリーズ M7 サーバでのみ使用できます。 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、Cisco UCS C シリーズ M7 サーバでのみ使用できます。 • 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
[パスワードの変更（Change Password）] トグル ボタン	**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。

名前	説明
[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。
[自己署名証明書（Self Signed Certificate）] トグルボタン	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 6 [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 7 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。

証明書自己署名要求

（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

- この手順を実行するには、管理者ユーザー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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[セキュリティ管理（Security Management）]** メニューをクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]** メニューで **[証明書管理（Certificate Management）]** を選択します。

ステップ 4 **[アクション（Actions）]** 領域で、**[新規証明書署名要求の生成（Generate New Certificate Signing Request）]** リンクをクリックします。

[証明書署名要求の生成（Generate Certificate Signing Request）] ダイアログボックスが表示されます。

ステップ 5 **[アクション（Actions）]** ドロップダウンリストから、**[証明書署名要求の生成（Generate Certificate Signing Request）]** を選択します。

[証明書署名要求の生成（Generate Certificate Signing Request）] ダイアログボックスが表示されます。

ステップ 6 **[証明書署名要求の生成（Generate 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。

（注）
[自己署名証明書（Self Signed Certificate）] トグルボタンが有効になっていることを確認します。

表 *220 :* 証明書署名要求の生成

名前	説明
共通名	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
Subject Alternate Name	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。 さまざまなタイプとして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。
[組織名（Organization Name）] フィールド	証明書を要求している組織。
[Organization Unit] フィールド	組織ユニット
[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。
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。 • 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。 （注） 署名アルゴリズム ECDSA および RSA は、Cisco UCS C シリーズ M7 サーバでのみ使用できます。

名前	説明
[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、Cisco UCS C シリーズ M7 サーバでのみ使用できます。 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、Cisco UCS C シリーズ M7 サーバでのみ使用できます。 • 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
[パスワードの変更（Change Password）] トグル ボタン	**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。

名前	説明
[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。
[自己署名証明書（Self Signed Certificate）] トグルボタン	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。

ステップ 7 [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 8 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。

Linux を使用した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。

	コマンドまたはアクション	目的
		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。
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

- この手順を実行するには、管理者ユーザー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

- この手順を実行するには、管理者ユーザー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） Cusco IMC の [証明書管理（Certificate Management）] メニューを使用して、まず 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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[セキュリティ管理（Security Management）]** メニューをクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]** メニューで **[証明書管理（Certificate Management）]** を選択します。

ステップ 4 **[アクション（Actions）]** ドロップダウン リストから、**[サーバー証明書のアップード（Upload Server Certificate）]** を選択します。

[サーバー証明書のアップード（Upload Server Certificate）] ダイアログ ボックスが表示されます。

ステップ 5 **[サーバー証明書のアップード（Upload Server 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
[ローカル/貼り付け（Local/Paste）] トグルボタン	ローカルマシンから証明書ファイルを選択するか、証明書を貼り付けることができます。
[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。 **[ローカル（Local）]** オプションが選択されている場合にのみ適用されます。
[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。 **[貼り付け（Paste）]** オプションが選択されている場合にのみ適用されます。

名前	説明
[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。

外部証明書の管理

サーバー証明書に加えて、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

- この手順を実行するには、管理者ユーザー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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[セキュリティ管理（Security Management）]** メニューをクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]** メニューで **[証明書管理（Certificate Management）]** を選択します。

ステップ 4 **[アクション (Actions)]** ドロップダウン リストから、**[外部証明書のアップロード（Upload External Certificate）]** を選択します。

[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 5 **[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、証明書の適切なアップロード方法を選択し、関連する詳細情報を入力します。

表 *221 :* リモート

名前	説明
リモート ボタン	このオプションは、外部証明書をリモート ロケーションからアップロードする場合に選択します。
サーバIP/ホスト名	外部証明書をアップロードする元のサーバーの詳細。
[Upload Protocol] ボタン	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。
[Path and Filename] フィールド	外部証明書ファイルのサーバーでのファイルパスとファイル名。
[Username] フィールド	リモートサーバのユーザー名。
[パスワード（Password）] フィールド	リモート サーバのパスワードです。
[アップロード（Upload）] ボタン	外部証明書をアップロードできます。

表 *222 :* ローカル

名前	説明
[ローカル] ボタン	このオプションは、外部証明書をローカルマシンからアップロードする場合に選択します。 **[参照 (Browse)]** をクリックして、アップロードする証明書に移動します。
[アップロード（Upload）] ボタン	外部証明書をアップロードできます。

表 *223 :* 貼り付け

名前	説明
[貼り付け（Paste）] ボタン	テキストボックスが開くので、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。
[アップロード（Upload）] ボタン	外部証明書をアップロードできます。

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)]** アクションが有効になります。アップロードした外部証明書をアクティブにするには、**[アクション（Actionss）]** ドロップダウン リストで、**[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

- この手順を実行するには、管理者ユーザー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。

手順

ステップ 1 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[セキュリティ管理（Security Management）]** メニューをクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]** メニューで **[証明書管理（Certificate Management）]** を選択します。

ステップ 4 **[アクション（Actions）]** ドロップダウンリストで、**[外部秘密キーのアップロード（Upload External Private Key）]**を選択します。

[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 5 **[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、証明書の適切なアップロード方法を選択し、関連する詳細情報を入力します。

表 *224 :* リモート

名前	説明
リモート ボタン	このオプションは、外部秘密キーをリモート ロケーションからアップロードする場合に選択します。
[サーバIP/ホスト名（Server IP/Hostname）] フィールド	外部秘密キーをアップロードするサーバーの詳細
[Upload Protocol] ボタン	次のいずれかのプロトコルを選択します。 • SFTP • SCP
[Username] フィールド	リモートサーバのユーザー名。
[パスワード（Password）] フィールド	リモート サーバのパスワードです。
[アップロード（Upload）] ボタン	外部秘密キーをアップロードできます。

表 *225 :* ローカル

名前	説明
[ローカル] ボタン	ローカルマシンから外部秘密キーをアップロードする場合は、このオプションを選択します。 **[参照 (Browse)]** をクリックして、アップロードする秘密キー ファイルに移動します。
[アップロード（Upload）] ボタン	外部秘密キーをアップロードできます。

表 *226 :* 貼り付け

名前	説明
[貼り付け（Paste）] ボタン	テキスト ボックスが開くので、そこで外部秘密キーの内容全体をコピーして、**[外部秘密キーの内容を貼り付け（Paste External 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。
[アップロード（Upload）] ボタン	外部秘密キーをアップロードできます。

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)]** アクションが有効になります。アップロードした外部証明書をアクティブにするには、**[アクション（Actionss）]** ドロップダウン リストで、**[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

- この手順を実行するには、管理者ユーザー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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[セキュリティ管理（Security Management）]** メニューをクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]** メニューで **[証明書管理（Certificate Management）]** を選択します。

ステップ 4 **[アクション (Actions)]** ドロップダウン リストから、**[外部証明書のアクティブ化（Activate External Certificate）]** を選択します。

（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 UCS C シリーズ 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。

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

手順

ステップ 1 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[セキュリティ管理（Security Management）]** メニューをクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]** メニューから、**[MCTP SPDM]**を選択します。

ステップ 4 **[プロパティ（Properties）]** 領域で、次のプロパティを確認して更新します。

表 *227:* プロパティ領域

名前	説明
[障害アラート設定（Fault Alert Setting）] ドロップダウン リスト	ドロップダウン リストから障害アラート設定を選択します。 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。
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の進行状況が表示されます。
証明書のアップロードステータス	証明書のアップロードステータスが表示されます。
SPDMステータス	SDPM 認証ステータス全体を表示します。

次のタスク

デバイスの構成証明が失敗して障害が生成された場合、**[システム（System）]** アプリの **[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

手順

	コマンドまたはアクション	目的
ステップ 1	[Apps] ドロップダウンリストから、[Administration] を選択します。	
ステップ 2	**[ナビゲーション（Navigation）]** ペインで、**[セキュリティ管理（Security Management）]** メニューをクリックします。	
ステップ 3	**[セキュリティ管理（Security Management）]** メニューから、**[MCTP SPDM]**を選択します。	

	コマンドまたはアクション	目的
ステップ 4	**[プロパティ（Properties）]** 領域で、次のプロパティを確認します。	表 *228 :* プロパティ領域

名前	説明
[障害アラート設定（Fault Alert Setting）] ドロップダウン リスト	ドロップダウン リストから障害アラート設定を選択します。 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。
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の進行状況が表示されます。
証明書のアップロードステータス	証明書のアップロードステータスが表示されます。
SPDMステータス	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

手順

ステップ 1 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[セキュリティ管理（Security Management）]** メニューをクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]** メニューから、**[MCTP SPDM]** を選択します。

ステップ 4 **[証明書（Certificates）]** 領域で、 **[+ 証明書の追加（+ Add Certificate）]** をクリックします。
[認証局証明書の追加（Add Authorities Certificate）] ダイアログ ボックスが表示されます。

ステップ 5 **[認証局証明書の追加（Add Authorities Certificate）]** ダイアログ ボックスで、次の方法を使用して証明書を追加します。

表 *229:* リモート

名前	説明
リモート ボタン	このオプションは、認証局証明書をリモートロケーションから追加する場合に選択します。
サーバIP/ホスト名	認証局証明書を追加するサーバーの詳細。
[Upload Protocol] ボタン	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。
[Path and Filename] フィールド	ルート CA 証明書ファイルのサーバーでのファイルパスとファイル名。
[Username] フィールド	リモートサーバのユーザー名。
[パスワード（Password）] フィールド	リモート サーバのパスワードです。

名前	説明
[認証局証明書のアップロード（**Upload Authorities Certificate**）**]** ボタン	認証局証明書を追加できます。

表 *230 :* ローカル

名前	説明
[ローカル**]** ボタン	このオプションは、認証局証明書をローカルマシンから追加する場合に選択します。 **[**参照（**Browse**）**]** をクリックして、追加する認証局証明書に移動します。
[認証局証明書のアップロード（**Upload Authorities Certificate**）**]** ボタン	認証局証明書を追加できます。

表 *231 :* 貼り付け

名前	説明
[貼り付け（**Paste**）**]** フィールド	テキスト ボックスが開き、そこでルート CA 証明書の内容全体をコピーして、**[**認証局証明書の貼り付け（**Paste Authorities Certificate**）**]** テキスト フィールドに貼り付けることができます。
[認証局証明書のアップロード（**Upload Authorities Certificate**）**]** ボタン	認証局証明書を追加できます。

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。

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

手順

	コマンドまたはアクション	目的
ステップ 1	[Apps] ドロップダウンリストから、[Administration] を選択します。	

	コマンドまたはアクション	目的
ステップ 2	**[ナビゲーション（Navigation）]** ペインで、**[セキュリティ管理（Security Management）]** メニューをクリックします。	
ステップ 3	**[セキュリティ管理（Security Management）]** メニューから、**[MCTP SPDM]**を選択します。	
ステップ 4	**[証明書（Certificates）]** 領域で、**[エンドポイント（Endpoints）]** タブをクリックします。	
ステップ 5	次のプロパティを表示することができます：	**表 *232 :* エンドポイント** 名前 / 説明 **[共通名（Common Name）]** カラム / ルート CA 証明書の共通名を表示します。 **[エンドポイント ID（Endpoint ID）]** カラム / PCIe スロット ID を表示します。 [Status] カラム / 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。 **[証明書の詳細の表示（View Certificate Details）]** アイコン / エンドポイント証明書の詳細を表示します。
ステップ 6	**[証明書（Certificates ）]** 領域で、**[認証局（Authorities）]** タブをクリックします。	
ステップ 7	次のプロパティを表示することができます：	**表 *233 :* 認証局** 名前 / 説明 **[証明書の追加 +（Add Certificate +）]** ボタン / 認証局証明書を追加します。

<table>
<tr><th></th><th>コマンドまたはアクション</th><th>目的</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>名前</th><th>説明</th></tr>
<tr><td>[削除（Delete）] ボタン</td><td>認証局証明書を削除します。
テーブルの任意の行のチェックボックスを選択し、[削除（Delete）]ボタンをクリックします。
（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。</td></tr>
<tr><td>[共通名（Common Name）] カラム</td><td>認証局証明書の共通名を表示します。</td></tr>
<tr><td>[発行元（Issued by）] カラム</td><td>認証局証明書の発行者の詳細を表示します。</td></tr>
<tr><td>[有効期限（Expires）] カラム</td><td>認証局の証明書の有効性を表示します。</td></tr>
<tr><td>[証明書の詳細の表示（View Certificate Details）] アイコン</td><td>認証局の証明書の詳細を表示できます。</td></tr>
</table>
（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。</td></tr>
<tr><td>ステップ 8</td><td>特定の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。</td><td>[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。
<table>
<tr><th>名前</th><th>説明</th></tr>
<tr><td>名前（Name）</td><td>認証局証明書の共通名を表示します。</td></tr>
<tr><td>発行元（Issued By）</td><td>認証局証明書の発行者の詳細を表示します。</td></tr>
</table></td></tr>
</table>

	コマンドまたはアクション	目的

名前	説明
[シリアル番号（Serial Number）] フィールド	証明書のシリアル番号を表示します。
有効期限の開始	証明書の有効期間の開始日を表示します。
有効終了日	証明書の有効期間の終了日を表示します。

表 *234* : サブジェクト エリア

名前	説明
共通名	認証局証明書の共通名を表示します。
市区町村郡	証明書発行者が所在する市区町村郡を表示します。
[状態（State）] フィールド	証明書発行者が所在する都道府県を表示します。
Country Code	証明書発行者の国コードを表示します。
組織単位	証明書発行者の組織単位を表示します。
[組織（Organization）]	発行者の組織名を表示します。

表 *235* : 発行者エリア

名前	説明
共通名	証明書発行者の共通名を表示します。
市区町村郡	証明書発行者が所在する市区町村郡を表示します。
状態	証明書発行者が所在する都道府県を表示します。

	コマンドまたはアクション	目的
		名前 / 説明 **Country Code** / 証明書発行者の国コードを表示します。 **組織単位** / 証明書発行者の組織単位を表示します。 **[組織（Organization）]** / 発行者の組織名を表示します。

証明書の削除

手順

	コマンドまたはアクション	目的
ステップ 1	[Apps] ドロップダウンリストから、[Administration] を選択します。	
ステップ 2	**[ナビゲーション（Navigation）]** ペインで、**[セキュリティ管理（Security Management）]** メニューをクリックします。	
ステップ 3	**[セキュリティ管理（Security Management）]** メニューから、**[MCTP SPDM]**を選択します。	
ステップ 4	**[証明書（Certificates ）]** 領域で、**[認証局（Authorities）]** タブをクリックします。	
ステップ 5	**[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 6	エンドポイント証明書を削除するには、**[削除（Delete）]** 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。**
ステップ 7	**[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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[セキュリティ管理（Security Management）]** メニューをクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]** メニューから、**[セキュア鍵管理（Secure Key Management）]** を選択します。

ステップ 4 以下のプロパティを確認できます。

表 *236 :* セキュアなキー管理

名前	説明
[セキュア キー管理の有効化（Enable Secure Key Management）] トグル ボタン	セキュア キー管理機能を有効または無効にできます。

ステップ 5 **[KMIP サーバー（KMIP Servers）]** 領域で、次のフィールドを確認します。

表 *237 : KMIP*サーバ

名前	説明
[KMIP ログインの詳細（KMIP Login Details）] ボタン	[KMIP ログインの詳細（KMIP Login Details）] ダイアログボックスを表示します。

名前	説明
[+サーバーの追加（+ Add Server）] ボタン	サービスの詳細を含む行を追加できます。クリックして、新しい行にサーバーのプロパティを入力します。
[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 サーバー設定を削除できます。テーブルから VLAN を選択し、**[削除（Delete）]** をクリックします。 （注） 行を選択すると、**[削除（Delete）]** ボタンが表示されます。
[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。 （注） 行を選択すると、**[接続のテスト（Test Connection）]** ボタンが表示されます。

ステップ 6 **[証明書とキーのステータス（Certificate and Key Status）]** 領域で、次のフィールドを確認します。

表 *238 :* 証明書とキーのステータス

名前	説明
[Name] カラム	証明書/キーの名前を表示します。
[Status] カラム	証明書/キーの可用性を示します。
[ダウンロード（Download）]	証明書/キーのダウンロード ステータスを表示します。
[エクスポート（Export）] カラム	証明書/キーのエクスポート ステータスを表示します。

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。

手順の概要

1. **openssl genrsa -out** *Client_Privatekeyfilename keysize*
2. **openssl req -new -x509 -days** *numdays* **-key** *Client_Privatekeyfilename* **-out** *Client_certfilename*
3. KMIP サーバーから KMIP ルート CA 証明書を取得します。

手順の詳細

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。

	コマンドまたはアクション	目的
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。

ルート CA 証明書

ルート CA 証明書のダウンロード

手順

ステップ 1 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[セキュリティ管理（Security Management）]** メニューをクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]** メニューから、**[セキュア鍵管理（Secure Key Management）]** を選択します。

ステップ 4 **[アクション（Actions）]** ドロップダウン リストから、**[ルート CA 証明書のダウンロード（Download Root CA Certificate）]** を選択します。

ステップ 5 **[ルート CA 証明書のダウンロード（Download Root CA Certificate）]** ダイアログ ボックスで、次のいずれかの方法を使用してルート CA 証明書をダウンロードします。

表 *239 :* リモート

名前	説明
リモート ボタン	このオプションは、リモート ロケーションからルート CA 証明書をダウンロードする場合に選択します。
サーバIP/ホスト名	ルート CA 証明書をダウンロードする元のサーバーの詳細。

名前	説明
[Upload Protocol] ボタン	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。
[Path and Filename] フィールド	ルート CA 証明書ファイルのサーバーでのファイルパスとファイル名。
[Username] フィールド	リモートサーバのユーザー名。
[パスワード（Password）] フィールド	リモート サーバのパスワードです。
[ルート CA 証明書のダウンロード（Download Root CA Certificate）] ボタン	ルート CA 証明書をダウンロードできます。

表 *240 :* ローカル

名前	説明
[ローカル] ボタン	ローカルマシンからルート CA 証明書をダウンロードする場合は、このオプションを選択します。 **[参照（Browse）]** をクリックして、ダウンロードするルート CA 証明書に移動します。
[ルート CA 証明書のダウンロード（Download Root CA Certificate）] ボタン	ルート CA 証明書をダウンロードできます。

表 *241 :* 貼り付け

名前	説明
[貼り付け（Paste）] フィールド	テキスト ボックスが開き、そこでルート CA 証明書の内容全体をコピーして、**[ルート CA 証明書の内容を貼り付け（Paste root CA Certificate Content）]** テキスト フィールドに貼り付けることができます。

名前	説明
[ルート CA 証明書のダウンロード（Download Root CA Certificate）] ボタン	ルート CA 証明書をダウンロードできます。

ルート CA 証明書のエクスポート

手順

ステップ 1 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[セキュリティ管理（Security Management）]** メニューをクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]** メニューから、**[セキュア鍵管理（Secure Key Management）]** を選択します。

ステップ 4 **[アクション（Actions）]** ドロップダウンリストから、**[ルート CA 証明書のエクスポート（Export Root CA Certificate）]** を選択します。

ステップ 5 **[ルート CA 証明書のエクスポート（Export Root CA Certificate）]** ダイアログ ボックスで、次のいずれかの方法を使用してルート CA 証明書をエクスポートします。

表 *242 :* リモート

名前	説明
リモート ボタン	このオプションは、リモート ロケーションからルート CA 証明書をエクスポートする場合に選択します。
サーバIP/ホスト名	ルート CA 証明書をエクスポートするサーバーの詳細。
[Upload Protocol] ボタン	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。

名前	説明
[Path and Filename] フィールド	ルート CA 証明書ファイルのサーバーでのファイルパスとファイル名。
[Username] フィールド	リモートサーバのユーザー名。
[パスワード（Password）] フィールド	リモート サーバのパスワードです。
[ルート CA 証明書のエクスポート（Export Root CA Certificate）] ボタン	ルート CA 証明書をエクスポートできるようにします。

表 *243 :* ローカル

名前	説明
[ローカル] ボタン	ローカルマシンからルート CA 証明書をエクスポートする場合は、このオプションを選択します。 **[参照（Browse）]** をクリックして、エクスポートするルート CA 証明書の場所に移動します。
[ルート CA 証明書のエクスポート（Export Root CA Certificate）] ボタン	ルート CA 証明書を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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[セキュリティ管理（Security Management）]** メニューをクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]** メニューから、**[セキュア鍵管理（Secure Key Management）]** を選択します。

ステップ 4 **[アクション（Actions）]** ドロップダウン リストから、**[ルート CA 証明書の削除（Delete Root CA Certificate）]** を選択します。

ステップ 5 [OK] をクリックして確定します。

クライアント証明書のダウンロード

手順

ステップ 1 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[セキュリティ管理（Security Management）]** メニューをクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]** メニューから、**[セキュア鍵管理（Secure Key Management）]** を選択します。

ステップ 4 **[アクション（Actions）]** ドロップダウン リストから、**[クライアント証明書のダウンロード（Download Client Certificate）]** を選択します。

ステップ 5 **[クライアント証明書のダウンロード（Download Client Certificate）]** ダイアログボックスで、次のいずれかの方法を使用してクライアント証明書をダウンロードします。

表 *244 :* リモート

名前	説明
リモート ボタン	このオプションは、クライアント証明書をリモート ロケーションからダウンロードする場合に選択します。
サーバIP/ホスト名	クライアント証明書をダウンロードする元のサーバーの詳細。
[Upload Protocol] ボタン	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。
[Path and Filename] フィールド	クライアント証明書ファイルのサーバーでのファイルパスとファイル名。
[Username] フィールド	リモートサーバのユーザー名。
[パスワード（Password）] フィールド	リモート サーバのパスワードです。

名前	説明
[クライアント証明書のダウンロード（Download Client Certificate）] ボタン	クライアント証明書をダウンロードできます。

表 *245 :* ローカル

名前	説明
[ローカル] ボタン	このオプションは、クライアント証明書をローカルマシンからダウンロードする場合に選択します。 **[参照（Browse）]** をクリックして、ダウンロードするクライアント証明書に移動します。
[クライアント証明書のダウンロード（Download Client Certificate）] ボタン	クライアント証明書をダウンロードできます。

表 *246 :* 貼り付け

名前	説明
[貼り付け（Paste）] フィールド	テキストボックスが開き、そこでクライアント証明書の内容全体をコピーして、**[クライアント証明書の内容を貼り付け（Paste Client Certificate Content）]** テキスト フィールドに貼り付けることができます。
[クライアント証明書のダウンロード（Download Client Certificate）] ボタン	クライアント証明書をダウンロードできます。

Client Certificate

クライアント証明書のエクスポート

手順

ステップ 1 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[セキュリティ管理（Security Management）]** メニューをクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]** メニューから、**[セキュア鍵管理（Secure Key Management）]** を選択します。

ステップ 4 **[アクション（Actions）]** ドロップダウン リストから、**[クライアント証明書のエクスポート（Export Client Certificate）]** を選択します。

ステップ 5 **[クライアント証明書のエクスポート（Export Client Certificate）]** ダイアログボックスで、次のいずれかの方法を使用してクライアント証明書をエクスポートします。

表 *247 :* リモート

名前	説明
リモート ボタン	このオプションは、リモート ロケーションからクライアント証明書をエクスポートする場合に選択します。
サーバIP/ホスト名	クライアント証明書をエクスポートするサーバーの詳細。
[Upload Protocol] ボタン	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。
[Path and Filename] フィールド	クライアント証明書ファイルのサーバーでのファイルパスとファイル名。
[Username] フィールド	リモートサーバのユーザー名。
[パスワード（Password）] フィールド	リモート サーバのパスワードです。
[クライアント証明書のエクスポート（Export Client Certificate）] ボタン	クライアント証明書をエクスポートできます。

表 *248 :* ローカル

名前	説明
[ローカル] ボタン	ローカルマシンからクライアント証明書をエクスポートする場合は、このオプションを選択します。 **[参照（Browse）]** をクリックして、エクスポートするクライアント証明書に移動します。
[クライアント証明書のエクスポート（Export Client Certificate）] ボタン	クライアント証明書を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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[セキュリティ管理（Security Management）]** メニューをクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]** メニューから、**[セキュア鍵管理（Secure Key Management）]** を選択します。

ステップ 4 **[アクション（Actions）]** ドロップダウンリストから、**[クライアント証明書の削除（Delete Client Certificate）]** を選択します。

ステップ 5 [OK] をクリックして確定します。

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。 • [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 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。
[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。

名前	説明
[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

クライアント秘密キーのダウンロード

手順

ステップ 1 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[セキュリティ管理（Security Management）]** メニューをクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]** メニューから、**[セキュア鍵管理（Secure Key Management）]** を選択します。

ステップ 4 **[アクション（Actions）]** ドロップダウンリストで、**[クライアント秘密キーのダウンロード（Download Client Private Key）]**を選択します。

ステップ 5 **[クライアント秘密キーのダウンロード（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。

表 *249 :* リモート

名前	説明
リモート ボタン	リモートロケーションからクライアント秘密キーをダウンロードする場合は、このオプションを選択します。
サーバIP/ホスト名	クライアント秘密キーをダウンロードするサーバーの詳細。

名前	説明
[Upload Protocol] ボタン	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。
[Path and Filename] フィールド	クライアント秘密キー ファイルのサーバーでのファイル パスとファイル名。
[Username] フィールド	リモートサーバのユーザー名。
[パスワード（Password）] フィールド	リモート サーバのパスワードです。
[ルート CA 証明書のダウンロード（Download Root CA Certificate）] ボタン	クライアント秘密鍵をダウンロードできます。

表 *250* : ローカル

名前	説明
[ローカル] ボタン	ローカル マシンからクライアント秘密キーをダウンロードする場合は、このオプションを選択します。 **[参照（Browse）]** をクリックして、ダウンロードするクライアント秘密キーに移動します。
[クライアント秘密キーのダウンロード（Download Client Private Key）] ボタン	クライアント秘密鍵をダウンロードできます。

表 *251* : 貼り付け

名前	説明
[貼り付け（Paste）] フィールド	テキストボックスが開き、そこでクライアント秘密キーの内容全体をコピーして、**[クライアント秘密キーのダウンロード（Download Client Private Key）]** テキスト フィールドに貼り付けることができます。

名前	説明
[クライアント秘密キーのダウンロード（Download Client Private Key）] ボタン	クライアント秘密キーをダウンロードできます。

クライアント秘密キーの削除

手順

ステップ 1 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[セキュリティ管理（Security Management）]** メニューをクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]** メニューから、**[セキュア鍵管理（Secure Key Management）]** を選択します。

ステップ 4 **[アクション（Actions）]** ドロップダウンリストで、**[クライアント秘密キーの削除（Delete Client Private Key）]**を選択します。

ステップ 5 [OK] をクリックして確定します。

KMIP サーバー接続のテスト

手順

ステップ 1 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[セキュリティ管理（Security Management）]** メニューをクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]** メニューから、**[セキュア鍵管理（Secure Key Management）]** を選択します。

ステップ 4 **[KMIP サーバー（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、**[接続のテスト（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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[セキュリティ管理（Security Management）]** メニューをクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]** メニューから、**[セキュア鍵管理（Secure Key Management）]** を選択します。

ステップ 4 **[KMIP サーバー（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、**[削除（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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[セキュリティ管理（Security Management）]** メニューをクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]** メニューから、**[セキュア鍵管理（Secure Key Management）]** を選択します。

ステップ 4 **[アクション（Actions）]** ドロップダウン リストから、**[KMIP ログインの削除（Delete KMIP Logins）]** を選択します。

ステップ 5 [OK] をクリックして確定します。

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 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[セキュリティ管理（Security Management）]** メニューをクリックします。

ステップ 3 **[セキュリティ管理（Security Management）]** メニューから、**[セキュリティ設定（Security Configuration）]** を選択します。

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）]** ボタンを切り替えます。

（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

この手順を実行するには、管理者ユーザーとしてログインする必要があります。

（注） **[構成された TLS バージョン（Configured TLS Version）]** が **[カスタム（Custom）]** に設定されている場合、FIPS を有効にすることはできません。

手順

ステップ 1 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[セキュリティ管理（Security Management）]** メニューをクリックします。

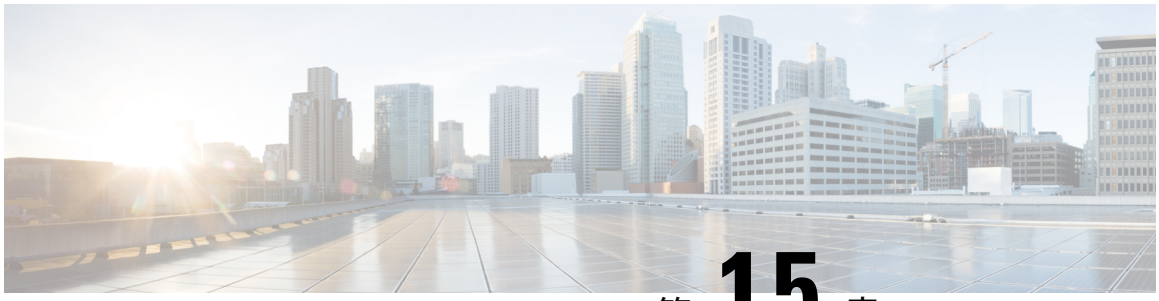
ステップ 3 **[セキュリティ管理（Security Management）]** メニューから、**[セキュリティ設定（Security Configuration）]** を選択します。

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、**[CC の有効化（Enable CC）]** ボタンを切り替えます。

ステップ 5 [保存（Save）] 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

- ファームウェア管理の概要 （621 ページ）
- ファームウェア コンポーネントの表示 （621 ページ）
- ファームウェアの更新 （623 ページ）
- ファームウェアのアクティブ化 （625 ページ）
- ファームウェアのアクティベーションのキャンセル （626 ページ）

ファームウェア管理の概要

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。

- CIMC
- BIOS
- RAID コントローラ
- Cisco UCS VIC

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。

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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 [Navigation] ペインで、[Firmware Management] をクリックします。

ステップ 3 **[Firmware Management]** 領域で、CIMC、BIOS、およびその他のコンポーネントに関する次の情報を確認します。

表 *252 :* ファームウェア管理

名前	説明
[コンポーネント（Component）] チェックボックス	1 つ以上のコンポーネントを選択できます。
[アップロード（Upload）] 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。 （注） **[アップロード]**ボタンは、コンポーネントを選択している場合にのみ表示されます。
[アクティブ化（Activate）] ボタン	選択したコンポーネントのファームウェアをアクティブ化できます。 （注） **[アクティブ化]**ボタンは、コンポーネントを選択している場合にのみ表示されます。
[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。
[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。

名前	説明
[Progress in %] カラム	操作の進行状況のパーセンテージ。

ファームウェアの更新

ローカルディスク、リモートサーバ、またはサーバに接続されているUSBストレージデバイス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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 [Navigation] ペインで、[Firmware Management] をクリックします。

ステップ 3 **[Firmware Management]** 領域で、**[コンポーネント（Component）]** カラムからコンポーネントを選択し、**[アップロード（Upload）]** をクリックします。

[ファームウェアの更新（Update Firmware）] ダイアログボックスが表示されます。

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

表 ***253:*** リモート

名前	説明
リモート ボタン	このオプションは、ファームウェアをリモートロケーションからアップロードする場合に選択します。
サーバIP/ホスト名	クライアント証明書をダウンロードする元のサーバーの詳細。

名前	説明
[Upload Protocol] ボタン	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。 • （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。 [前面パネル USB（Front Panel USB）] : サーバに接続されている USB ストレージ デバイスを介してファームウェアをインストールできます。 [イメージのパスとファイル名（Image Path and Filename）] フィールドに、ファームウェアのファイル名と場所を入力し、[ファームウェアのインストール（Install Firmware）] をクリックします。
[Path and Filename] フィールド	ファームウェアファイルがサーバー上にあるファイルパスとファイル名。
[Username] フィールド	リモートサーバのユーザー名。
[パスワード（Password）] フィールド	リモート サーバのパスワードです。

名前	説明
[アップロード（Upload）] ボタン	ファームウェア ファイルをアップロードできます。 （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。

表 *254 :* ローカル

名前	説明
[ローカル] ボタン	ローカルマシンからファームウェアを更新する場合はこのオプションを選択します。 [Browse] をクリックし、使用するファームウェアファイルに移動します。
[アップロード（Upload）] ボタン	ファームウェア ファイルをアップロードできます。

ファームウェアのアクティブ化

手順

ステップ 1 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 [Navigation] ペインで、[Firmware Management] をクリックします。

ステップ 3 [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 4 [Activate Firmware] ダイアログボックスで、次のプロパティを更新します。

表 *255 : Activate Firmware*

名前	説明
[Firmware Version] リスト	ファームウェアのアクティベートに使用可能なファームウェア バージョンのリストです。
[Activate Firmware] ボタン	選択したコンポーネントに応じて、選択したファームウェア バージョンをアアクティベートします。 **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 **（注）** ホストがオンの場合、BIOS ファームウェアをアクティブ化できます。この場合、 [Status] フィールドに [Activation Pending] と表示されます。次回のホストの起動後、保留状態にある BIOS がアクティブ化されます。

ファームウェアのアクティベーションのキャンセル

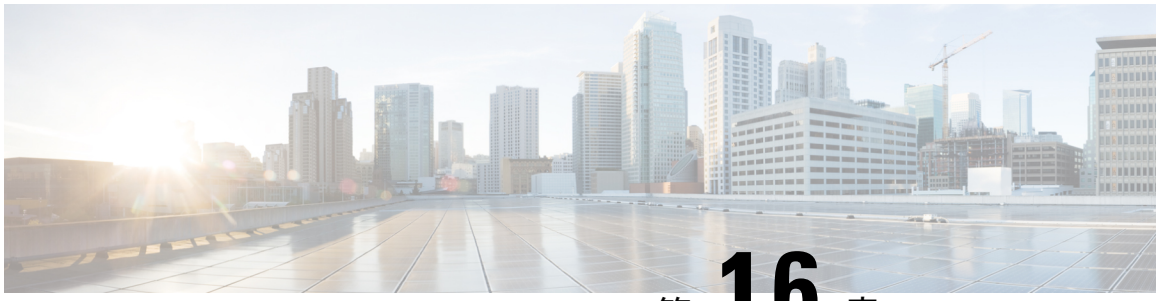
始める前に

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 [Apps] ドロップダウンリストから、[Administration] を選択します。
ステップ 2 [Navigation] ペインで、[Firmware Management] をクリックします。
ステップ 3 **[Firmware Management]** 領域で、アクティベーションをキャンセルするファームウェアを選択します。
ステップ 4 [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。

[Activation Pending] ステータスのファームウェアを選択した場合にのみ [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

- 障害サマリーの表示 （629 ページ）
- 障害履歴の表示 （630 ページ）
- システム イベント ログの表示 （631 ページ）
- Cisco IMC ログの表示 （632 ページ）
- ロギング制御 （633 ページ）

障害サマリーの表示

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。

ステップ 2 **[障害とログ（Faults and Logs）]** タブを選択します。

ステップ 3 **[ナビゲーション（Navigation）]** ペインで、**[障害サマリー（Fault Summary）]** メニューをクリックします。

ステップ 4 **[障害サマリー（Faults Summary）]** 領域で、次のプロパティを確認します。

（注）
正確なサマリーを表示するには、**[ログの検索（Search Logs）]** フィールドに障害に関連するテキストを入力します。または、**[シビラティ（Severity）]** ドロップダウン リストから特定のシビラティ（重大度）タイプを選択します。

名前	説明
[Time]	障害が発生した時刻。

名前	説明
シビラティ（重大度）（**Severity**）	次のいずれかになります。 • クリティカル（**Critical**） • **[Informational]** • 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。
Domain Name	識別名（ドメイン名）は、サーバー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。

障害履歴の表示

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。

ステップ 2 **[障害とログ（Faults and Logs）]** タブを選択します。

ステップ 3 **[ナビゲーション（Navigation）]** ペインで、**[障害履歴（Fault History）]** メニューをクリックします。

ステップ 4 **[生涯履歴（Faults History）]** 領域で、次のプロパティを確認します。

ヒント
正確な障害履歴を表示するには、**[ログの検索（Search Logs）]** フィールドに障害に関連するテキストを入力します。または、**[シビラティ（Severity）]** ドロップダウン リストから特定のシビラティ（重大度）タイプを選択します。

名前	説明
[Time]	障害が発生した時刻。

名前	説明
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**）
[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子
[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。

システム イベント ログの表示

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。

ステップ 2 **[障害とログ（Faults and Logs）]** タブを選択します。

ステップ 3 **[ナビゲーション（Navigation）]** ペインで、**[システム イベント ログ（System Event Log）]** メニューをクリックします。

ステップ 4 **[システム イベント ログ（System Event Log）]** エリアで、次の情報を確認します。

ヒント
正確なシステム イベント ログを表示するには、**[ログの検索（Search Logs）]** フィールドにシステム イベントに関連するテキストを入力します。または、**[シビラティ（Severity）]** ドロップダウン リストから特定のシビラティ（重大度）タイプを選択します。

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	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。
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、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。
[ログのクリア（Clear Log）] ボタン	システムのログ エントリをクリアできます。

Cisco IMC ログの表示

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。

ステップ 2 **[障害とログ（Faults and Logs）]** タブを選択します。

ステップ 3 **[ナビゲーション（Navigation）]** ペインで、**[Cisco IMC ログ（Cisco IMC Log）]** メニューをクリックします。

ステップ 4 [Cisco IMC Log] タブで、次の情報を確認します。

ヒント
正確な Cisco IMC ログを表示するには、**[ログの 検索（Search Logs）]** フィールドに Cisco IMC ログに関連するテキストを入力します。または、 **[シビラティ（Severity）]** ドロップダウン リストから特定のシビラティ（重大度）タイプを選択します。

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）]** • **[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。
[ログのクリア（Clear Log）] ボタン	Cisco IMC ログ エントリをクリアできます。

ロギング制御

ロギング制御の表示

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。

ステップ 2 **[障害とログ（Faults and Logs）]** タブを選択します。

ステップ 3 **[ナビゲーション（Navigation）]** ペインで、**[ロギング コントロール（Logging Controls）]** メニューをクリックします。

ステップ 4 **[ロギング制御（Logging Controls）]** 領域で、次の情報を確認します。

表 *256 : [Local Logging]* 領域

名前	説明
[報告する最小シビラティ（重大度）（Minimum Severity to Report）] ドロップダウン リスト	このドロップダウン リストで、ローカル ログに含まれるメッセージの最低レベルを指定できます。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）**

表 *257 :* アップロード ステータス エリア

名前	説明
証明書のアップロードステータス	証明書のアップロードのステータスが表示されます。 デフォルトでは、値は **[なし（NONE）]** です。 証明書のアップロードが完了すると、値は **COMPLETED** と表示されます。
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のプログレスが表示されます。 デフォルトでは、値は [なし（None）] です。 証明書のアップロードが完了すると、値は **100%** と表示されます。

表 *258 : [Remote Logging]* 領域

名前	説明
[+サーバーの追加（+Add Server）] ボタン	新しいサーバーの行を追加できます。**[+サーバーの追加（+Add Server）]**をクリックしたら、サーバーを作成するための値を入力して、**[保存（Save）]** をクリックします。

名前	説明
[削除（Delete）] ボタン	エントリを削除できます。削除するエントリを選択し、**[削除（Delete）]**をクリックします。
[セキュア Syslog（Secure Syslog）] トグルボタンまたは列	ステータスが **[有効（Enabled）]** の場合、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） ステータスが **[有効（Enabled）]** の場合、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。 このプロパティは、サーバーエントリを作成または編集するときにトグル ボタンとして機能します。
[ホスト名/IP アドレス（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。 このプロパティは、サーバー エントリを作成または編集するときにフィールドとして機能します。
[ポート（Port）] フィールドまたは列	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。 このプロパティは、サーバー エントリを作成または編集するときにフィールドとして機能します。
[プロトコル（Protocol）] ドロップダウンリストまたは列	Syslog メッセージの送信用のトランスポート層プロトコル。プロトコルは次のいずれかになります。 • TCP • UDP このプロパティは、サーバーエントリの作成または編集時にドロップダウン リストとして機能します。
[握手状態（Handshake Status）] フィールド	**[セキュア Syslog（Secure 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、証明書が正しい Syslog サーバー用であるかどうかを確認します。

名前	説明
[シビラティ（重大度）の最小値] ドロップダウン リストまたは列	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。これは、次のシビラティ（重大度）レベル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）** このプロパティは、サーバーエントリの作成または編集時にドロップダウン リストとして機能します。
[テスト SysLog を送信（Send Test SysLog）] ボタン	テスト Cisco IMC ログを設定済みのリモート Syslog サーバーに送信できます。
[編集（Edit）] アイコン	リモート Syslog サーバのプロパティを編集できます。 次のプロパティを編集して保存できます。 • ホスト名/IP アドレス（Host Name/IP Address） • ポート • プロトコル • 最小シビラティ（重大度）
[削除（Delete）] ボタン	Syslog サーバーを削除できます。

リモート サーバへの Cisco IMC ログの送信

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 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。

ステップ 2 **[障害とログ（Faults and Logs）]** タブを選択します。

ステップ 3 **[ナビゲーション（Navigation）]** ペインで、**[ロギング コントロール（Logging Controls）]** メニューをクリックします。

ステップ 4 **[リモートロギング（Remote Logging）]** 領域で、新しいサーバー エントリを作成するか、エントリを編集してセキュアな syslog を有効にできます。

ステップ 5 新しいサーバーを追加してセキュアな syslog を有効にするには、**[サーバーの追加（Add Server）]** をクリックします。または、既存のサーバー エントリを編集する場合には、行の末尾にある編集アイコンをクリックして、次のプロパティを更新します。

表 *259 : [Remote Logging]* 領域

名前	説明
[+サーバーの追加（+Add Server）] ボタン	新しいサーバーの行を追加できます。**[+サーバーの追加（+Add Server）]**をクリックしたら、サーバーを作成するための値を入力して、**[保存（Save）]** をクリックします。
[削除（Delete）] ボタン	エントリを削除できます。削除するエントリを選択し、**[削除（Delete）]**をクリックします。
[セキュア Syslog（Secure Syslog）] トグルボタンまたは列	ステータスが **[有効（Enabled）]** の場合、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） ステータスが **[有効（Enabled）]** の場合、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。 このプロパティは、サーバーエントリを作成または編集するときにトグル ボタンとして機能します。
[ホスト名/IP アドレス（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。 このプロパティは、サーバー エントリを作成または編集するときにフィールドとして機能します。

名前	説明
[ポート（Port）] フィールドまたは列	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。 このプロパティは、サーバー エントリを作成または編集するときにフィールドとして機能します。
[プロトコル（Protocol）] ドロップダウンリストまたは列	Syslog メッセージの送信用のトランスポート層プロトコル。プロトコルは次のいずれかになります。 • TCP • UDP このプロパティは、サーバーエントリの作成または編集時にドロップダウン リストとして機能します。
[握手状態（Handshake Status）] フィールド	**[セキュア Syslog（Secure 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、証明書が正しい Syslog サーバー用であるかどうかを確認します。
[シビラティ（重大度）の最小値] ドロップダウン リストまたは列	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。これは、次のシビラティ（重大度）レベル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）** このプロパティは、サーバーエントリの作成または編集時にドロップダウン リストとして機能します。
[テスト SysLog を送信（Send Test SysLog）] ボタン	テスト Cisco IMC ログを設定済みのリモート Syslog サーバーに送信できます。

名前	説明
[編集（Edit）] アイコン	リモート Syslog サーバのプロパティを編集できます。 次のプロパティを編集して保存できます。 • ホスト名/IP アドレス（Host Name/IP Address） • ポート • プロトコル • 最小シビラティ（重大度）
[削除（Delete）] ボタン	Syslog サーバーを削除できます。

ステップ 6 **[Save Changes]**をクリックします。

Cisco IMC ログしきい値の設定

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。

ステップ 2 **[障害とログ（Faults and Logs）]** タブを選択します。

ステップ 3 **[ナビゲーション（Navigation）]** ペインで、**[ロギング コントロール（Logging Controls）]** メニューをクリックします。

ステップ 4 **[ローカル ロギング（Local Logging）]** 領域で、**[レポートする最小シビラティ（Minimum Severity to Report）]** ドロップダウン リストを使用して、 ログに含まれるメッセージの最低レベルを指定します。

表 *260 : [Local Logging]* 領域

名前	説明
[報告する最小シビラティ（重大度）（Minimum Severity to Report）] ドロップダウン リスト	このドロップダウン リストで、ローカル ログに含まれるメッセージの最低レベルを指定できます。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のメッセージはログに記録されません。たとえば、**[エラー（Error）]**を選択した場合、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 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。

ステップ 2 **[障害とログ（Faults and Logs）]** タブを選択します。

ステップ 3 **[ナビゲーション（Navigation）]** ペインで、**[ロギング コントロール（Logging Controls）]** メニューをクリックします。

ステップ 4 **[リモート ロギング（Remote Logging）]** 領域の **[テスト Syslog の送信（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 ログが送信されます。

リモート Syslog 証明書の管理

ユーザーはリモート 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 Syslog 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。

始める前に

- この手順を実行するには、管理者ユーザーとしてログインする必要があります。
- **[ローカル（Local）]** オプションを選択する場合、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

	コマンドまたはアクション	目的
ステップ 1	**[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。	
ステップ 2	**[障害とログ（Faults and Logs）]** タブを選択します。	
ステップ 3	**[ナビゲーション（Navigation）]** ペインで、**[ロギング コントロール（Logging Controls）]** メニューをクリックします。	

<table>
<tr><th></th><th>コマンドまたはアクション</th><th>目的</th></tr>
<tr><td>ステップ 4</td><td>[リモート ロギング（Remote Logging）] 領域で、リモート Syslog 証明書をアップロードする必要がある Syslog サーバーを選択します。</td><td></td></tr>
<tr><td>ステップ 5</td><td>[証明書のアップロード（Upload Certificate）]ボタンをクリックします。</td><td>[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開きます。</td></tr>
<tr><td>ステップ 6</td><td>次のいずれかのオプションを選択して、証明書を選択します。</td><td>• リモート
• ローカル
• 貼り付け

表 261 : リモート
<table><tr><th>名前</th><th>説明</th></tr><tr><td>リモート ボタン</td><td>このオプションは、証明書をリモート ロケーションからアップロードする場合に選択します。</td></tr><tr><td>[サーバIP/ホスト名（Server IP/Hostname）] フィールド</td><td>証明書をアップロードする元のサーバーの詳細。</td></tr><tr><td>[Upload Protocol] ボタン</td><td>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。</td></tr><tr><td>[Path and Filename] フィールド</td><td>証明書ファイルのサーバーでのファイルパスとファイル名。</td></tr></table></td></tr>
</table>

	コマンドまたはアクション	目的

名前	説明
[Username] フィールド	リモートサーバのユーザー名。
[パスワード（Password）] フィールド	リモート サーバのパスワードです。
[アップロード（Upload）] ボタン	証明書をアップロードできます。

表 *262 :* ローカル

名前	説明
[ローカル] ボタン	このオプションは、証明書をローカルマシンからアップロードする場合に選択します。 **[参照 (Browse)]** をクリックして、アップロードする証明書に移動します。
[アップロード（Upload）] ボタン	証明書をアップロードできます。

表 *263 :* 貼り付け

名前	説明
[貼り付け（Paste）] ボタン	テキスト ボックスが開き、そこで Syslog 証明書の内容全体をコピーして、**[貼り付け（Paste）]** テキストフィールドに貼り付けることができます。
[アップロード（Upload）] ボタン	証明書をアップロードできます。

[アップロード ステータス（Upload Status）] 領域で、**[証明書のアップロード ステータス（Certificate Upload Status）]** と **[証明書のアップロードの進行状況（Certificate Upload Progress）]** を表示できます。

リモート Syslog 証明書の削除

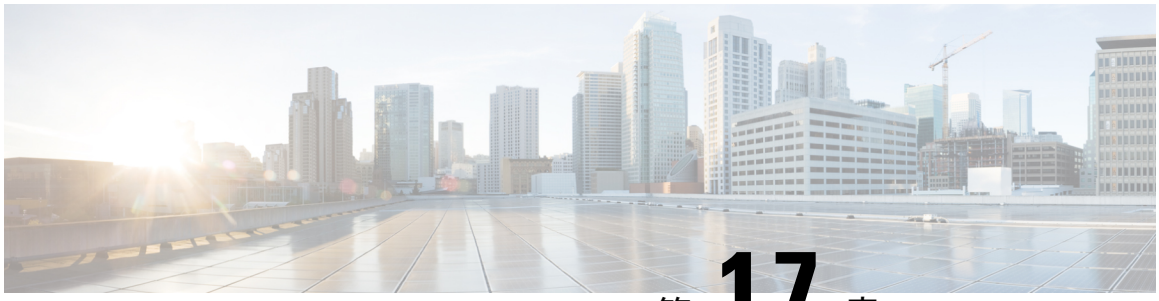
サーバーからリモート Syslog 証明書を削除できます。

始める前に

この手順を実行するには、管理者ユーザーとしてログイン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	**[**アプリ（**Apps**）**]** ドロップダウン リストから、**[**システム（**System**）**]** を選択します。	
ステップ 2	**[**障害とログ（**Faults and Logs**）**]** タブを選択します。	
ステップ 3	**[**ナビゲーション（**Navigation**）**]** ペインで、**[**ロギング コントロール（**Logging Controls**）**]** メニューをクリックします。	
ステップ 4	**[**リモート ロギング（**Remote Logging**）**]** 領域で、Syslog 証明書を削除する Syslog サーバーを選択します。	
ステップ 5	**[**証明書を削除（**Delete Certificates**）**]**をクリックします。	
ステップ 6	システム プロンプトに従って、削除を確認します。	



第 17 章

サーバ ユーティリティ

- テクニカル サポート データのエクスポート （645 ページ）
- 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 （650 ページ）
- 出荷時の初期状態へのリセット （652 ページ）
- Cisco IMC 設定のエクスポートとインポート （656 ページ）
- ホストへのマスク不可能な割り込みの生成 （660 ページ）
- Cisco IMC バナーの追加または更新 （661 ページ）
- Cisco IMC の最後のリセット理由の表示 （662 ページ）
- 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 （662 ページ）
- 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 （663 ページ）
- PIDカタログ （664 ページ）
- スマート アクセス USB の有効化 （668 ページ）
- デバイス コネクタの設定 （669 ページ）

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。

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、テクニカル サポート データをエクスポートしないでください。

手順

	コマンドまたはアクション	目的
ステップ 1	[Apps] ドロップダウンリストから、[Administration] を選択します。	

	コマンドまたはアクション	目的
ステップ 2	**[ナビゲーション（Navigation）]** ペインで、**[ユーティリティ（Utilities）]** メニューをクリックします。	
ステップ 3	[アクション（Actions）] ドロップダウンメニューから、**[管理ユーティリティ（Administration Utilities）]** > **[テクニカル サポート データのエクスポート（Export Technical Support Data）]** を選択します。	

	コマンドまたはアクション	目的
ステップ 4	**[**テクニカル サポート データのエクスポート（**Export Technical Support Data**）**]**ダイアログ ボックスで、次のプロパティを更新します。	表 *264* : テクニカル サポート データのエクスポート 名前 / 説明 [サーバ IP/ホスト名（Server IP/Hostname）] フィールド

	コマンドまたはアクション	目的	
		名前	説明
			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。 （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*

	コマンドまたはアクション	目的

名前	説明
	<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。 • [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。
[Path and Filename] フィールド	ファイルをリモート サーバ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。
[Username] フィールド	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。

	コマンドまたはアクション	目的
		名前 / 説明 [Password] フィールド / 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。 **[エクスポート（Export）]** ボタン / テクニカル サポート データをエクスポートできます。

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

	コマンドまたはアクション	目的
ステップ 1	[Apps] ドロップダウンリストから、[Administration] を選択します。	
ステップ 2	**[ナビゲーション（Navigation）]**ペインで、**[ユーティリティ（Utilities）]** メニューをクリックします。	
ステップ 3	[アクション（Actions）] ドロップダウンメニューから、**[管理ユーティリティ（Administration Utilities）]** > **[テクニカル サポート データをローカル ダウンロード用に生成（Generate Technical Support Data for Local Download）]**を選択します。	

	コマンドまたはアクション	目的
ステップ 4	**[ローカル ダウンロードのためのテクニカル サポート データの生成（Generate Technical Support Data for Local Download）]** ダイアログボックスで、次のオプションを選択します。	表 *265 :* ローカル ダウンロード用のテクニカル サポート データを生成（*Generate Technical Support Data for Local Download*）

名前	説明
[Generate Technical Support Data] オプション ボタン	Cisco IMC は、ダウンロードするテクニカル サポート データ ファイルがない場合、このオプション ボタンを無効にします。 **[Generate]** をクリックして、データ ファイルを作成します。
[Download to local file] オプション ボタン	Cisco IMC 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、このオプション ボタンを有効にします。 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。
[生成してダウンロード（Generate and Download）] ボタン	テクニカル サポート データ ファイルを生成してダウンロードできます。
[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。

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。

重要 他世代の C シリーズ サーバーから VIC アダプタを移動する際は、アダプタを出荷時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、管理者としてログイン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	[Apps] ドロップダウンリストから、[Administration] を選択します。	
ステップ 2	**[ナビゲーション（Navigation）]**ペインで、**[ユーティリティ（Utilities）]** メニューをクリックします。	
ステップ 3	[Actions] ドロップダウンメニューから、**[管理ユーティリティ（Administration Utilities）]**>**[工場デフォルトにリセット（Reset to Factory Default）]**を選択します。	

	コマンドまたはアクション	目的
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、次のオプションを選択します。	表 *266 :* 工場出荷時のデフォルトにリセット **名前**: **[**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 **説明**:

	コマンドまたはアクション	目的	
		名前	説明
			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。次のいずれかになります。 • [BMC]：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。 • [ストレージ コントローラ（Storage Controllers）]：オンにすると、特定のストレージアダプタを工場出荷時の設定にリセットします。 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。[展開して選択

<table>
<tr><th></th><th>コマンドまたはアクション</th><th>目的</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>名前</th><th>説明</th></tr>
<tr><td></td><td>（Expand to select）]
• [VIC]：オンにすると、特定の VIC を工場出荷時の設定にリセットします。
（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。</td></tr>
<tr><td>[Reset] ボタン</td><td>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。
（注）
工場出荷時の設定にリセットすると、ネットワーク構成モードはデフォルトで C125 M5 サーバに対して Cisco カード モードに設定されます。
その他の C シリーズ サーバでは、NIC のモードは、デフォルトで共有 LOM 拡張に設定されます。</td></tr>
</table>
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。
</td></tr>
</table>

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

（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。

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、Cisco IMC 設定をエクスポートしないでください。

手順

ステップ 1 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ユーティリティ（Utilities）]** メニューをクリックします。

ステップ 3 [アクション（Actions）] ドロップダウン メニューから、**[管理ユーティリティ（Administration Utilities）]** > **[設定のエクスポート（Export Configuration）]**を選択します。

ステップ 4 **[CIMC 設定のエクスポート（Export CIMC configuration）]** ダイアログボックスで、次のオプションのいずれかを選択して Cisco IMC 設定をエクスポートします。

- リモート
- ローカル

表 *267 :* リモート

名前	説明
リモート ボタン	JSON 設定ファイルをリモート サーバーにエクスポートするには、このオプションを選択します。
[サーバーIP/ホスト名（Server IP/Hostname）] フィールド	設定ファイルをエクスポートする必要があるサーバーの IP アドレスまたはホスト名。

名前	説明
[Upload Protocol] ボタン	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]** （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。
[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（Username）] フィールド	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。
[Password] フィールド	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。
[セキュア パスフレーズ（Secure Passphrase）] フィールド	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：! # $ & < > ? ; ' | ` ~ \ % ^ ( ) " （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エクスポートしようとすると、編集内容は無視され、エクス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。

表 *268 :* ローカル

名前	説明
[ローカル（Local）] ボタン	Cisco IMC を実行しているコンピュータのローカル ドライブに JSON 構成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。
[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：! # $ & < > ? ; ' | ` ~ \ % ^ ( ) " （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エクスポートしようとすると、編集内容は無視され、エクス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。

Cisco IMC 設定のインポート

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、Cisco IMC 設定をインポートしないでください。

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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ユーティリティ（Utilities）]** メニューをクリックします。

ステップ 3 [アクション（Actions）] ドロップダウン メニューから、**[管理ユーティリティ（Administration Utilities）]** > **[設定のインポート（Import Configuration）]**を選択します。

ステップ 4 **[CIMC 設定のインポート（Import CIMC configuration）**] ダイアログ ボックスで、Cisco IMC 設定をインポートするための次のオプションのいずれかを選択します。

- リモート

- ローカル

表 *269 :* リモート

名前	説明
リモート ボタン	JSON 設定ファイルをリモート サーバからインポートするには、このオプションを選択します。
[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 IP アドレスまたはホスト名。
[Upload Protocol] ボタン	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]** （注） このアクションを実行中にリモート サーバーのタイプとして 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 *[*サーバー（*RSA*）のキー 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。
[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（Username）] フィールド	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。
[Password] フィールド	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
[セキュア パスフレーズ（Secure Passphrase）] フィールド	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。

表 *270 :* ローカル

名前	説明
[ローカル（Local）] ボタン	Cisco IMC を実行しているコンピュータのローカル ドライブに JSON 構成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。 **[参照（Browse）]** をクリックして、インポート構成ファイルに移動します。
[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。

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。

始める前に

- この手順を実行するには、管理者ユーザー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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ユーティリティ（Utilities）]** メニューをクリックします。

ステップ 3 [アクション（Actions）] ドロップダウン メニューから、**[管理ユーティリティ（Administration Utilities）]** > **[ホストへの NMI の生成（Generate NMI to Host）]**を選択します。

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、**[OK]** をクリックして続行します。
ホストに NMI 信号が送信されます。OS が再起動される可能性があります。

Cisco IMC バナーの追加または更新

手順

ステップ 1 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ユーティリティ（Utilities）]** メニューをクリックします。

ステップ 3 [アクション（Actions）] ドロップダウン メニューから、**[管理（Administration）][ユーティリティ（Utilities）]** > **[Cisco IMC バナーの追加/更新（Add/Update Cisco IMC Banner）]**を選択します。

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、次のプロパティを更新します。

名前	説明
[Banner (80 Chars per line. Max 2K Chars.)] フィールド	Cisco IMC の 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）] トグルボタン	有効にすると、**[バナーの保存（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。
[バナーの保存（Save Banner）] ボタン	バナーの変更を保存します。**[OK]** をクリックして続行します。
[バナーのクリア（Clear Banner）] ボタン	バナー情報をクリアします。**[OK]** をクリックして続行します。

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 **[ユーティリティ（Utilities）]** ペインの **[操作（Operations）]** 領域で、**[Cisco IMC の最後のリセット（Cisco IMC Last Reset）]** 行の次の情報を確認します。

名前	説明
[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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ユーティリティ（Utilities）]** メニューをクリックします。

ステップ 3 [アクション（Actions）] ドロップダウン メニューから、**[管理ユーティリティ（Administration Utilities）]** > **[ハードウェア インベントリ データをローカルにダウンロード（Download Hardware Inventory Data to Local Download）]** を選択します。

ステップ 4 **[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（Download inventory data to local file）]** ダイアログ ボックスで、次のオプションを選択します。

名前	説明
[Generate Inventory Data] オプション ボタン	ダウンロードするインベントリ データ ファイルがない場合、Cisco IMC はこのオプション ボタンを無効にします。 [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、[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。
[インベントリ データをローカル ファイルにダウンロード（Download Inventory Data to Local File）] オプション ボタン	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、Cisco IMC はこのオプション ボタンを有効にします。 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。

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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 [アクション（Actions）] ドロップダウン メニューから、**[管理ユーティリティ（Administration Utilities）]** > **[ハードウェア インベントリ データをリモートにエクスポート（Export Hardware Inventory Data to Remote）]** を選択します。

ステップ 3 **[リモートへのハードウェア インベントリ データのエクスポート（Export Hardware Inventory Data to Remote）]** ダイアログ ボックスで、以下のプロパティを更新します。

表 *271 :* ハードウェア インベントリ データをリモートにダウンロード（*Export Hardware Inventory Data to Remote*）

名前	説明
[サーバーIP/ホスト名（Server IP/Hostname）] フィールド	データ ファイルのエクスポート先となるサーバーの IP アドレスまたはホスト名。

名前	説明
[Upload Protocol] ボタン	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]** （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。
[Path and Filename] フィールド	リモート サーバー上のデータ ファイルのパスとファイル名。
[Username] フィールド	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。
[Password] フィールド	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。
[エクスポート（Export）] ボタン	クリックしてデータ ファイルをエクスポートします。

PIDカタログ

PID カタログのアップロード

始める前に

この手順を実行するには、管理者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 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。

ステップ 2 **[インベントリ（Inventory）]** タブを選択します。

ステップ 3 [アクション（Actions）] ドロップダウン メニューから、**[PID カタログ（PID Catalog）]** > **[PID カタログのアップロード（Upload PID Catalog）]**を選択します。

ステップ 4 **[PID カタログのアップロード（Upload PID Catalog）]** ダイアログ ボックスで、次のオプションのいずれかを選択して PID カタログを選択します。

- リモート
- ローカル

表 *272 : [*リモート（*Remote***）*]* タブ**

名前	説明
[サーバ 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 Protocol] ボタン	次のいずれかのプロトコルを選択します。 • FTP • SFTP • SCP • TFTP • 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。
[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（Username）] フィールド	リモート サーバーのユーザー名。
[パスワード（Password）]フィールド	リモート サーバのパスワード。

名前	説明
[アップロード（Upload）] ボタン	PID カタログをアップロードできます。 （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。

[ローカル（Local）] : **[参照（Browse）]** をクリックし、ブラウザ クライアント上の更新する PID カタログ ファイルに移動します。ファイルを選択した後、[アップロード（Upload）] をクリックします。

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

この手順を実行するには、管理者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 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。

ステップ 2 **[インベントリ（Inventory）]** タブを選択します。

ステップ 3 [アクション（Actions）] ドロップダウン メニューから、**[PID カタログ（PID Catalog）]** > **[PID カタログのアクティベート（Activate PID Catalog）]**を選択します。

ステップ 4 **[PID カタログの有効化（Activate PID Catalog）]** ダイアログボックスで、 **[有効化（Activate）]** ボタンをクリックします。

（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 カタログ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す。PID は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

この手順を実行するには、管理者ユーザーとしてログインする必要があります。

手順の概要

1. **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。
2. **[インベントリ（Inventory）]** タブを選択します。
3. [アクション（Actions）] ドロップダウン メニューから、**[PID カタログ（PID Catalog）]** > **[PID カタログの削除（Delete PID Catalog）]**を選択します。
4. [OK] をクリックして確認します。

手順の詳細

手順

ステップ 1 **[アプリ（Apps）]** ドロップダウン リストから、**[システム（System）]** を選択します。

ステップ 2 **[インベントリ（Inventory）]** タブを選択します。

ステップ 3 [アクション（Actions）] ドロップダウン メニューから、**[PID カタログ（PID Catalog）]** > **[PID カタログの削除（Delete PID Catalog）]**を選択します。

ステップ 4 [OK] をクリックして確認します。

（注）
[PID カタログの削除（Delete PID Catalog）] オプションは、PID カタログがすでにアップロードされ、アクティブになっている場合にのみ表示されます。

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
- FAT32
- FAT16
- 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

この手順を実行するには、管理者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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ユーティリティ（Utilities）]** メニューをクリックします。

ステップ 3 [アクション（Actions）] ドロップダウン メニューから、**[管理ユーティリティ（Administration Utilities）]** > **[スマート アクセス USB の有効化（Enable Smart Access USB）]**を選択します。

ステップ 4 **[スマート アクセス USB の有効化（Enable Smart Access USB）]** ダイアログボックスで、**[OK]** をクリックして続行します。

デバイス コネクタの設定

Cisco Intersight 管理の有効化/無効化

Cisco Intersight の管理を有効または無効にできます。

Cisco Intersight 管理を有効にすると、Intersight クラウド アプリケーションと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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[デバイス コネクタ（Device Connector）]** メニューをクリックします。

ステップ 3 **[デバイス コネクタ（Device Connector）]** ウィンドウで、**[設定（Settings）]** アイコンをクリックします。**[一般（General）]** ページが表示されます。

ステップ 4 **[デバイスコネクタ（Device Connector）]** トグルボタンを有効または無効にします。

名前	説明
[有効化（Enable）]	Intersight の管理を有効にします。このシステムに対し要求を行って、Cisco Intersight の機能を活用できます。
無効（Disable）	Intersight 管理を無効にします。無効になっている場合、Cisco Intersightへの通信は許可されません。

Intersight デバイス コネクタのプロパティの表示

Intersight Infrastructure Service ライセンス

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。

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

[ヘルプ センター（Help Center）] 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。

手順

ステップ 1 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[デバイス コネクタ（Device Connector）]** メニューをクリックします。

ステップ 3 **[デバイス コネクタ（Device Connector）]** ウィンドウで、次のプロパティを確認して更新します。

表 *273 :* デバイス コネクタ

アクション	説明
[接続の再試行（Retry Connection）] または **[更新（Refresh）]** ボタン	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。
接続設定の **[設定を開く（Open Settiings）]** ボタン	接続設定を開きます。詳細を確認するには、接続をクリックします。
全般設定の **[設定を開く（Open Settiings）]** ボタン	全般設定を開きます。詳細を確認するには、全般をクリックします。

アクション	説明
[設定（Settings）] ボタン	次の設定を開きます。 • 総則：詳細については、「全般」を参照してください。 • DNS 構成。詳細については、「DNS の設定」を参照してください。 • NTP 構成。詳細については、「NTP の設定」を参照してください。 • プロキシ設定、詳細については、「プロキシ設定」を参照してください。 • 証明書マネージャ。詳細については、「証明書マネージャ」を参照してください。 • 接続。詳細については、「接続」を参照してください。
接続ステータス	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。
Device ID	Cisco IMC によって管理されるデバイスに割り当てられる一意の識別子。

アクション	説明
請求ID	デバイスを Cisco Intersight に登録して関連付けるために使用される、デバイスに割り当てられた一意の識別子。

表 *274* : 一般

名前	説明
[デバイス コネクタ（Device Connector）] トグル 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。
[アクセス モード（Access Mode）] ラジオ ボタン	次のいずれかになります。 • **[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。

名前	説明
[Intersight のみからの構成（Configuration from Intersight only）] トグル ボタン	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。
[トンネル化 vKVM（Tunneled vKVM）] トグル ボタン	この設定により、セキュアなトンネルを使用してサーバーの KVM インターフェイスにアクセスできるようになります。有効にすると、KVMトラフィックがセキュアトンネル経由でルーティングされ（通常はデバイス コネクタ経由）、クライアントとサーバー間で送信されるデータを暗号化することによってリモート管理セッションのセキュリティが強化されます。

表 *275 : DNS* の設定

名前	説明
[ドメイン名（Domain Name）] フィールド	Cisco IMC の完全修飾ドメイン名（FQDN）または、ホスト名。
[DNSサーバ（DNS Server）] フィールド	FQDN の IP アドレス。

表 *276 : NTP* の設定（*NTP Configuration*）

名前	説明
[NTP サーバ（NTP Server）] フィールド	NTP サーバーとして機能するサーバーのうちの 1 台の IP/DNS アドレス。

表 *277 :* プロキシ設定

名前	説明
[プロキシの有効化（Enable Proxy）] トグル ボタン	HTTPS プロキシ設定を有効または無効にすることができます。
[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	
[**Save**] ボタン	プロキシ設定を保存します。

表 *278 :* 証明書マネージャ

名前	説明
[インポート（Import）] ボタン	CA 署名付き証明書を選択して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。
[Name] カラム	CA 証明書の共通名。
[使用中（In Use）] カラム	トラスト ストアでリモート サーバーを正しく確認するため証明書を使用したかどうか。
[発行元（Issued by）] カラム	証明書の発行機関。
[有効期限（Expires）] カラム	証明書の有効期限日。
[証明書の表示（View Certificate）] アイコン	クリックして証明書の詳細を表示します。

名前	説明
[証明書の削除（Delete Certificate）] ボタン	証明書を削除できます。 （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。

表 *279 :* 証明書の詳細の表示

名前	説明
名前（Name）	証明書の名前。
発行元（Issued By）	組織の名前。
期限切れ	証明書の有効期限日。
フィンガープリント	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。
件名（Subject）	
国（Country）	会社が存在する国。
[組織（Organization）]	証明書を要求している組織。
共通名	証明書の発行対象サーバーの完全修飾（FQDN またはサーバーのドメイン名）ホスト名。
発行者	
国（Country）	証明書を発行した会社が存在している国
[組織（Organization）]	証明書を発行した会社内の組織
共通名	発行元の会社の完全修飾ホスト名

表 *280 :* 接続

名前	説明
接続の確認	接続を確認できます。**[接続の確認（Check Connection）]** をクリックして、続行します。
すべての詳細の表示	**[詳細の表示（View Details）]** ウィンドウを開きます。接続の完全な詳細を表示できます。

名前	説明
[詳細の表示（View Details）]	[DNS 解決（DNS Resolution）] の下で **アドレス（Addresses）]** と **[遅延（Latency）]** の値を表示できます。
修復を表示する	管理者は、サーバーで実行する必要がある修復アクションを表示できます。修復には、通常、サーバーをセキュリティポリシーまたは運用標準に準拠させるために必要な更新、パッチ、または設定変更が含まれます。

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 [Apps] ドロップダウンリストから、[Administration] を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[デバイス コネクタ（Device Connector）]** メニューをクリックします。

ステップ 3 **[デバイス コネクタ（Device Connector）]** ウィンドウで、**[設定（Settings）]** ボタンをクリックします。

ステップ 4 **[設定（Settings）]** 領域で、**[プロキシ設定（Proxy Configuration）]** を選択します。

ステップ 5 **[プロキシ設定の構成（Configure proxy settings）]** ダイアログ ボックスで、次のプロパティを更新します。

表 *281 :* プロキシ設定

名前	説明
[プロキシの有効化（Enable Proxy）] トグル ボタン	HTTPS プロキシ設定を有効または無効にすることができます。
[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	

名前	説明
[**Save**] ボタン	プロキシ設定を保存します。

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。