



## Cisco ベースボード管理コントローラ コンフィギュレーションガイド

最終更新：2025年3月28日

### シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター  
0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>





## 目次

---

はじめに :

[はじめに](#) **vii**  
[対象読者](#) **vii**  
[表記法](#) **vii**

---

第 1 章

[はじめに](#) **1**  
[Cisco UCS C885A M8 ラック サーバ の概要](#) **1**  
[はじめに](#) **2**  
[要件](#) **4**  
[Cisco BMC にログインします。](#) **4**  
[ナビゲーションとメニュー](#) **5**  
[\[概要 \(Overview\)\] ページ](#) **7**

---

第 2 章

[ログ](#) **11**  
[イベントログ](#) **11**  
[イベント ログの表示](#) **11**  
[イベント ログのエクスポート](#) **12**  
[イベント ログの削除](#) **13**  
[POST ログ](#) **13**  
[POST コードログの表示](#) **13**  
[POST コード ログのエクスポート](#) **14**  
[テクニカル サポート ログ](#) **14**  
[テクニカル サポート ログのダウンロード](#) **14**

---

第 3 章

[ハードウェアステータス](#) **15**

インベントリと LED の表示	15
CPU のモニタリングと管理	23
冷却管理	23
ファンの障害状態を管理	24
センサー ステータスの表示	25
システム識別 LED のオン/オフ	26

---

**第 4 章****操作 27**

Cisco BMC とサーバー工場設定をリセット	27
KVM コンソールの起動	28
BMC のファームウェア	29
BMC ファームウェアの表示	29
BMC ファームウェアの更新	29
OEM ファームウェアのアップデート	30
BMC をリブート	30
Serial over LAN (SOL) の表示	31
サーバーの電源操作	32
サーバーの電源状態の表示	32
サーバの再起動	32
サーバーのシャットダウン	33
ブート ソースのオーバーライド	33
仮想メディア イメージの追加	33

---

**第 5 章****設定 35**

日付と時刻の構成	35
Cisco BMC のネットワーク管理	36
ネットワーク設定の表示または構成	36
IPv4 アドレスの表示または追加	37
静的 DNS IP アドレスの表示、追加、または削除	39
電源復元ポリシーの設定	39

---

第 6 章	<b>セキュリティとアクセス</b>	<b>41</b>
	ユーザセッション	41
	ユーザセッションの表示	41
	セッションの切断	42
	LDAP 設定	42
	LDAP 認証のイネーブル化	42
	ロールグループの追加	43
	ユーザ管理	44
	ユーザーの追加	44
	ユーザの編集	45
	ユーザーの有効化または無効化	46
	アカウントポリシー設定を管理	47
	ユーザの削除	47
	ポリシーを更新しています	48
	SSH を通じて BMC シェルの有効化または無効化	48
	ネットワーク IPMI を有効化または無効化	48
	証明書の管理	49
	証明書の詳細の表示	49
	新しい証明書の追加	50
	証明書署名要求を生成する	50

---

第 7 章	<b>リソース管理</b>	<b>53</b>
	電力構成の表示	53
	電力制限の適用	54

---

第 8 章	<b>GPU 管理</b>	<b>55</b>
	GPU 管理	55
	日付と時刻の構成	56
	GPU FRU 情報の表示	56
	GPU 電源および温度センサーの表示	57

GPU 電力構成の表示	58
GPU 電力制限の適用	58
イベント ログ	59
GPU イベント ログの表示	59
GPU イベント ログのエクスポート	60
GPU ファームウェアのアップデート	60

---

付録 A :

<b>REST API</b>	<b>63</b>
HTTP メソッド (HTTP Methods)	63
ステータス コード	64
認証	68
利用可能な API	69



## 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](#) (vii ページ)
- [表記法](#) (vii 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、 <b>[GUI 要素]</b> 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、 <b>[メインタイトル]</b> 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 ( <i>italic</i> ) 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、 <b>this font</b> 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。

---





# 第 1 章

## はじめに

- [Cisco UCS C885A M8 ラック サーバの概要 \(1 ページ\)](#)
- [はじめに \(2 ページ\)](#)
- [要件 \(4 ページ\)](#)
- [Cisco BMC にログインします。 \(4 ページ\)](#)
- [ナビゲーションとメニュー \(5 ページ\)](#)
- [\[概要 \(Overview\) \] ページ \(7 ページ\)](#)

## Cisco UCS C885A M8 ラック サーバの概要

Cisco UCS C885A M8 ラック サーバは、大規模なディープ ラーニング/Large Language Model (LLM) トレーニング、モデル調整、大規模モデル推論、および取得拡張生成 (RAG) を含む、最も要求の厳しい AI ワークロードに対処する大規模でスケーラブルな高速コンピューティング機能を提供するように設計された高密度 GPU サーバーです。

シングル サーバー内に高速コンピューティング パフォーマンスを届けるためにサーバーは、次のタイプの 8 つの GPU から選択できます：

- NVIDIA® H100 SXM または NVIDIA® H200 サーバー PCI Express モジュール (SXM) GPU。SXM は、NVIDIA GPU に使用されているソケットベースの GPU インターコネクタメソッドです。
- AMD MI300X OCP アクセラレータ モデル (OAM) GPU。OAM は、GPU ベンダーの縛りを防ぐオープン コンピュータ GPU インターコネクタ標準規格です。

ノースサウストラフィックではサーバーは、AI モデル トレーニングを高密度 GPU サーバーのクラスター全体に拡張するために NVIDIA Bluefield-3 B3220 DPU を 1 つサポートします。GPU の間のイーストウェストトラフィックのために NVIDIA ConnectX-7 または、Bluefield-3 B3140H SuperNIC を 8 つまでサポートします。

# はじめに

Cisco ベースボード管理コントローラ (Cisco BMC) ウェブ GUI は、HTML5 ベースで SSL (HTTPS) によってセキュリティが追加されています。これは、Cisco UCS C885A M8 ラックサーバの管理を次のオプションで助けます：

## ハードウェアとコンポーネント管理

インベントリ機能は、管理者がハードウェア デバイスと各サーバーの CPU、メモリ モジュール、ハードドライブ、ネットワーク カード、などのコンポーネントを有効します。

## ステータスと確認

インベントリ機能は、ハードウェアとソフトウェアデバイスのステータスとチェックを提供します。この情報はデバイス正常性のステータス、温度、電圧、接続ステータスなど含むことがあります。

機能	説明
ログインします。	ユーザー名 パスワード
概要	BMC 日付と時刻 SOL コンソール システムの情報 ステータス情報
ログ	ダウンロードした ポスト コード ログ テクニカル サポート ログ
ハードウェアのステータス	インベントリと LED センサー

機能	説明
操作	工場出荷時の状態へのリセット KVM ファームウェア OEM ファームウェア リブート BMC SOL コンソール サーバー電源の運用 仮想メディア
設定	Date and time Network 電力復元ポリシー
セキュリティとアクセス	セッション LDAP ユーザ管理 ポリシー 証明書
リソース管理	電源
GPU 管理	情報 センサー 電力 イベント ログ ファームウェア 日時 (注) このオプションは、一部のCisco UCS C885A M8 ラック サーバ構成でのみ利用可能です。

# 要件

表 1: オペレーティングシステムとブラウザの要件

推奨されるブラウザ	テスト済みバージョン	推奨される最小オペレーティングシステム
Mozilla Firefox	132.0.2 (AArch64)	macOS 15.1 (24B83)
	132.0 (64 ビット)	Ubuntu 20.04.3 LTS
	132.0.2 (64 ビット)	Microsoft Windows 11 Enterprise
Apple Safari	バージョン 18.1 (20619.2.8.11.10)	macOS 15.1 (24B83)
Google Chrome	131.0.6778.71 (64 ビット)	Microsoft Windows 11 Enterprise
Microsoft Edge	131.0.2903.51 (64 ビット)	Microsoft Windows 11 Enterprise

## Cisco BMC にログインします。

### 始める前に

ログインを試みる前に、すべての前提条件が満たされていることを確認します。

### 手順

**ステップ 1** Web ブラウザで、Cisco BMC 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。

(注)

未設定のシステムに初めてログインする場合は、ユーザ名に **[ルート (root)]**、パスワードに **[パスワード (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。

- Web UI または CLI でデフォルトのログイン情報を変更するまでは、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 [パスワード (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。

## ナビゲーションとメニュー

Cisco BMCにログインすると、[概要 (Overview) ] ページが表示されます。次のオプションが使用可能であることがわかります：

### メニューバー

上部のメニューバーには、次のオプションがあります：

名前	説明
正常性	イベント ログの表示 を表示できます。
電源	サーバの再起動を表示および構成できます。
更新	BMC センサーの値を更新できます。
root	プロファイル設定からログアウトしたり、パスワードを変更したりできます。

### [Navigation] ペイン

左側のナビゲーションペインには、次のオプションがあります：

名前	説明
ログ	ダウンロードした ポストコードログ テクニカルサポートログ
ハードウェアのステータス	インベントリと LED センサー

名前	説明
操作	工場出荷時の状態へのリセット KVM ファームウェア OEM ファームウェア リブート BMC SOL コンソール サーバー電源の運用 仮想メディア
設定	Date and time Network 電力復元ポリシー
セキュリティとアクセス	セッション LDAP ユーザ管理 ポリシー 証明書
リソース管理	電源
GPU 管理	情報 センサー 電力 イベントログ ファームウェア 日時  (注) このオプションは、一部のCisco UCS C885A M8 ラック サーバ構成でのみ利用可能です。

## [概要 (Overview) ] ページ

Cisco BMC GUI にログインすると、[概要 (Overview) ] ページが表示されます。このページから、重要な機能や情報にすばやくアクセスできます。次に、[概要 (Overview) ] ページの主要なプロパティとセクションを示します。

### BMC の日付と時刻

表 2: BMC の日付と時刻

名前	説明
[BMC の日付と時刻 (BMC date and time) ] フィールド	このフィールドでは、BMC システムの日時を表示および設定できます。
SOL ボタン	このボタンは、リモート管理およびトラブルシューティングのための Serial over LAN (SOL) セッションを開始します。詳細については、「 <a href="#">Serial over LAN (SOL) の表示 (31 ページ)</a> 」を参照してください。

### システム情報

表 3: サーバ情報

名前	説明
[モデル (Model) ] フィールド	このフィールドは、サーバーのモデルを表示します。
[シリアル番号 (Serial Number) ] フィールド	このフィールドには、サーバーに割り当てられた一意のシリアル番号が表示されます。
[サーバー メーカー (Server Manufacturer) ] フィールド	このフィールドは、サーバーの製造元を識別します。
[詳細を表示 (View more) ] リンク	詳細については、クリックしてください。 <a href="#">インベントリと LED の表示 (15 ページ)</a> 。

表 4: ファームウェア情報

名前	説明
[稼働 (Running) ] フィールド	このフィールドは、システムで実行されているファームウェアの現在のバージョンを示します。

名前	説明
[詳細を表示 (View more) ] リンク	詳細については、クリックしてください。 <a href="#">BMC ファームウェアの表示 (29 ページ)</a> 。

表 5: ネットワーク情報

名前	説明
[Hostname] フィールド	このフィールドサーバーに割り当てられたネットワーク ホスト名を表示します。
[リンク ステータス (Link Status) ] フィールド	このフィールドには、ネットワーク リンクの現在のステータス (LinkUp など) が表示されます。
[静的 IPv4 (Static IPv4) ] フィールド	このフィールドは、サーバーのスタティック IPv4 アドレス (設定されている場合) を示します。
[DHCPv4] フィールド	このフィールドには、DHCP を介してサーバーに割り当てられた IPv4 アドレスが表示されます。
[詳細を表示 (View more) ] リンク	詳細については、クリックしてください。 <a href="#">Cisco BMCのネットワーク管理 (36 ページ)</a> 。

表 6: 電源について

名前	説明
[CPU 0 電力 (CPU 0 Power) ] フィールド	このフィールドには、CPU 0 の消費電力が表示されます。
[CPU 1 電力 (CPU 1 Power) ] フィールド	このフィールドには、CPU 1 の消費電力が表示されます。
[詳細を表示 (View more) ] リンク	詳細については、クリックしてください。 <a href="#">電力構成の表示 (53 ページ)</a> 。

**[Status Information]**

表 7: イベント ログ

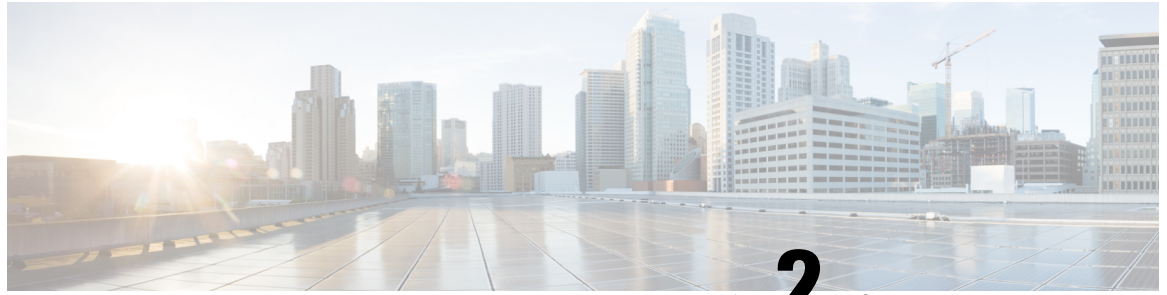
名前	説明
[重大 (Critical) ] フィールド	このフィールドには、システムに記録されたクリティカル イベントの数が表示されます。

名前	説明
[警告 (Warning) ] フィールド	このフィールドは、システムに記録された警告イベントの数を示します。
すべてのリンクをエクスポート	ログをエクスポートするには、クリックします。 ブラウザ設定によって、JSON ログ ファイルを開くまたは、保存することをプロンプトされる場合があります。
[詳細を表示 (View more) ] リンク	詳細については、クリックしてください。 <a href="#">イベント ログの表示 (11 ページ)</a> 。

表 8: インベントリと LED

名前	説明
[システム識別 LED (System identify LED) ] フィールド	このフィールドには、システム識別 LED のステータスが表示されます。この LED は、システムを物理的に識別するためにオンまたはオフに切り替えることができます。
[詳細を表示 (View more) ] リンク	詳細については、クリックしてください。 <a href="#">インベントリと LED の表示 (15 ページ)</a> 。





## 第 2 章

# ログ

---

- イベント ログ (11 ページ)
- POST ログ (13 ページ)
- テクニカル サポート ログ (14 ページ)

## イベント ログ

### イベント ログの表示

ロギングおよびコールアウト機能は、システムイベントの管理と追跡に不可欠であり、警告、エラー、異常な状態などのさまざまなイベントをログに記録して報告することで、動作ステータスの包括的なビューを提供します。

- **[ロギング (Logging)]** : システムイベントと異常状態を記録し、システムイベントログに保存します。イベントには、ハードウェア障害、システムエラー、温度異常、電源装置の問題などが含まれます。
- **[コールアウト (Callouts)]** : 特定のイベントが発生したときに、事前定義されたアクションをトリガーします。たとえば、ハードウェア障害やその他の重大なイベントが検出された場合、コールアウトは自動的にアラートをトリガーしたり、遠隔管理システムに通知したり、指定されたコマンドを実行したりできます。

#### 手順

---

**ステップ 1** [ナビゲーション ペイン (Navigation Pane)] で、[ログ (Logs)] > [イベント ログ (Event Logs)] を選択します。

**ステップ 2** 次のオプションに基づいてイベント ログをフィルタ処理できます。

- 開始と終了の日付
- 重要度に基づく : (OK、Warning、および Critical)

- 検索フィールドを使用して検索キーワード

次のログ 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	各ログ エントリの一意の識別子を表示します。
[Severity] カラム	ログ エントリの重要度または影響のレベルを示します。次のいずれかになります。 <ul style="list-style-type: none"> <li>• <b>[OK]</b> : ログ エントリが正常または成功した操作を表していることを示します。</li> <li>• <b>[クリティカル (critical)]</b> : すぐに対処が必要な重大な問題があることを示します。</li> <li>• <b>[注意 (Warning)]</b> : モニターする必要がある潜在的な問題を示します。</li> </ul>
[日付 (Date) ] カラム	ログ エントリが記録された日時を表示します。
[Description] カラム	ログ エントリに関する簡単な概要または詳細を提供します。

## イベント ログのエクスポート

### 手順

**ステップ 1** [ナビゲーション ペイン (Navigation Pane) ]で、[ログ (Logs) ]>[イベント ログ (Event Logs) ]を選択します。

**ステップ 2** すべてのログ エントリをエクスポートするには、[すべてエクスポート (Export all) ]をクリックします。ブラウザ設定によって、ログ ファイルを開くまたは、保存することをプロンプトされる場合があります。

## イベント ログの削除

### 手順

**ステップ 1** [ナビゲーション ペイン (Navigation Pane)] で、[ログ (Logs)] > [イベント ログ (Event Logs)] を選択します。

**ステップ 2** すべてのログ エントリを削除するには、[すべて削除 (Delete all)] をクリックします。

**ステップ 3** [ログを削除 (Delete Log)] ダイアログ ボックスで [削除 (Delete)] をクリックします。

## POST ログ

### POST コードログの表示

### 手順

**ステップ 1** [ナビゲーション ペイン (Navigation Pane)] で、[ログ (Logs)] > [POST コード ログ (POST code Logs)] を選択します。

**ステップ 2** 次のオプションに基づいてログをフィルタ処理できます。

- 開始と終了の日付
- 検索フィールドを使用して検索キーワード

次のログ プロパティを表示することができます：

名前	説明
[作成日時 (Created)] カラム	POST コードログが生成された日時を表示します。
[タイム スタンプ オフセット (Time stamp offset)] カラム	POST コードがログに記録されたときのシステム開始からの時間オフセットを示します。
[ブート カウント (Boot count)] カラム	システムが起動した回数を表示します。
[ポスト コード (Post Code)] カラム	電源投入時セルフテスト (POST) コードを表示します。

名前	説明
[Description] カラム	POST コード ログ エントリに関する詳細を提供します。

## POST コード ログのエクスポート

### 手順

**ステップ 1** [ナビゲーションペイン (Navigation Pane)] で、[ログ (Logs)] > [POST コード ログ (POST code Logs)] を選択します。

**ステップ 2** すべてのログエントリをエクスポートするには、[すべてエクスポート (Export all)] をクリックします。  
ブラウザ設定によって、ログファイルを開くまたは、保存することをプロンプトされる場合があります。

## テクニカル サポート ログ

### テクニカル サポート ログのダウンロード

### 手順

**ステップ 1** [ナビゲーションペイン (Navigation Pane)] で、[ログ (Logs)] > [POST コード ログ (POST code Logs)] を選択します。

**ステップ 2** [ダウンロード (Download)] をクリックして、ダウンロードプロセスを開始します。

**ステップ 3** [確認 (Confirm)] をクリックして続行し、ログファイルを保存します。

ブラウザ設定によって、ログファイルを開くまたは、保存することをプロンプトされる場合があります。



## 第 3 章

# ハードウェアステータス

- [インベントリと LED の表示 \(15 ページ\)](#)
- [CPU のモニタリングと管理 \(23 ページ\)](#)
- [冷却管理 \(23 ページ\)](#)
- [ファンの障害状態を管理 \(24 ページ\)](#)
- [センサー ステータスの表示 \(25 ページ\)](#)
- [システム識別 LED のオン/オフ \(26 ページ\)](#)

## インベントリと LED の表示

### 手順

**ステップ 1** [ナビゲーション ペイン (Navigation Pane)] で、[ハードウェア ステータス > インベントリと LED (Hardware Status Inventory and LED)] を選択します。

**ステップ 2** 次のプロパティを表示することができます：

表 9: LED 照明制御

名前	説明
[電源ステータス (Power Status)] フィールド	当該システムの現在の電力ステータスを表示します。
[システム ID LED (System identity LED)] トグル ボタン	システムの特定に役立つように、システム ID LED のオンとオフを切り替えます。

表 10: システム

名前	説明
[ID] カラム	各システムの一意の識別子を表示します。

名前	説明
[ハードウェア タイプ (Hardware type) ] カラム	各システムのハードウェアのタイプを示します。
[Health] カラム	各システムの現在のヘルス ステータスを表示します。
[LED 識別 (Identify LED) ] カラム	各システムの識別LEDがオンかオフかを示します。
[シリアル番号 (Serial Number) ] フィールド	システムのシリアル番号を表示します。
[モデル (Model)] フィールド	システムのモデルを表示します。
[アセット タグ (Asset tag) ] フィールド	システムのアセット タグを表示します。
[ステータス (状態) (Status (State)) ] フィールド	システムの現在の状態を示します。
[Power] フィールド	当該システムの現在の電力ステータスを表示します。
[正常性ロールアップ (Health rollup) ] フィールド	システムの全体的な正常性ステータスを表示します。
[メーカー (Manufacturer) ] フィールド	システムのメーカーを表示します。
[説明 (Description) ] フィールド	システムの簡単な説明を提供します。
[サブモデル (Sub model) ] フィールド	システムのサブモデルを表示します。
[システム タイプ (System Type) ] フィールド	システムのタイプを示します。
[メモリの概要 (Memory Summary) ]	システム メモリの概要を表示します。
[ステータス (State)] フィールド	メモリの現在の状態を示します。
[状態 (Health) ] フィールド	メモリの現在の正常性ステータスを表示します。
[正常性ロールアップ (Health rollup) ] フィールド	メモリの全体的な正常性ステータスを表示します。
[総メモリ (Total Memory) ] フィールド	システムで使用可能な総メモリを表示します。
[プロセッサの概要 (Processor Summary) ]	システム プロセッサの概要を示します。
[ステータス (State)] フィールド	プロセッサの現在の状態を示します。
[正常性 (Health) ] フィールド	プロセッサの現在の正常性ステータスを示します。
[正常性ロールアップ (Health rollup) ] フィールド	プロセッサの現在の正常性ステータスを示します。
[Count] フィールド	システム内のプロセッサの数を表示します。
[数 (Count) ] フィールド	プロセッサあたりのコア数を表示します。

表 11: BMC マネージャ

名前	説明
[ID] カラム	各 BMC マネージャ エントリの一意の識別子を表示します。
[正常性 (Health) ] カラム	BMC マネージャの現在の正常性ステータスを表示します。
[名前 (Name) ] フィールド	Cisco Integrated Management Controller
[モデル (Model)] フィールド	BMC マネージャのモデルを表示します。
[UUID] フィールド	BMC マネージャの UUID を表示します。
[サービス エントリ ポイント UUID (Service entry point UUID) ] フィールド	BMC マネージャのサービス エントリ ポイント UUID を表示します。
[ステータス (State)] フィールド	BMC マネージャの現在の状態を示します。
[電源 (Power) ] フィールド	BMC マネージャの現在の電源ステータスを表示します。
[正常性ロールアップ (Health rollup) ] フィールド	BMC マネージャの全体的な正常性ステータスを表示します。
[BMC 日付と時刻 (BMC date and time) ] フィールド	BMC の現在の日時を表示します
[最終リセット時刻 (Last Reset Time) ] フィールド	BMC の最終リセット時刻を表示します。
[説明 (Description) ] フィールド	BMC マネージャの簡単な説明を提供します。
[マネージャ タイプ (Manager type) ] フィールド	BMC マネージャのタイプを示します。
[ファームウェア バージョン (Firmware Version) ] フィールド	BMC マネージャのファームウェア バージョンを表示します。
<b>[OEM Firmware Version (OEM ファームウェア バージョン) ]</b>	
[BIOS] フィールド	BIOS バージョンを表示します。
[SCM FPGA] フィールド	SCM FPGA のバージョンを表示します。
[MB FPGA] フィールド	MB FPGA バージョンを表示します。
[HIB FPGA] フィールド	HIB FPGA バージョンを表示します。
[RoT] フィールド	RoT バージョンを表示します。
グラフィカルコンソール	

名前	説明
[サポートされている接続タイプ (Connect types supported)] フィールド	グラフィカルコンソールでサポートされている接続タイプを表示します。
[最大同時セッション数 (Max concurrent sessions)] フィールド	グラフィカルコンソールの同時セッションの最大数を表示します。
[有効化されたサービス (Service enabled)] フィールド	グラフィカルコンソールのサービスが有効化されているかどうかを示します。
シリアル コンソール	
[サポートされている接続タイプ (Connect types supported)] フィールド	シリアルコンソールでサポートされている接続タイプを表示します。
[最大同時セッション数 (Max concurrent sessions)] フィールド	シリアルコンソールの同時セッションの最大数を表示します。
[有効化されたサービス (Service enabled)] フィールド	シリアルコンソールのサービスが有効化されているかどうかを示します。

表 12: シャーシ

名前	説明
[ID] カラム	各シャーシエントリの一意の識別子を表示します。
[正常性 (Health)] カラム	シャーシの現在の正常性ステータスを示します。
<b>FRU_CHASSIS</b> 、 <b>FRU_CPUSLED</b> 、 <b>FRU_SCN</b> 、および <b>FU_SYS</b> の次のプロパティが表示されます。	
[ボード作成日 (Board build date)] フィールド	ボードの作成日を表示します。
[ボード メーカー (Board Manufacturer)] フィールド	ボードのメーカーを表示します。
[ボード製品 (Board product)] フィールド	ボードの製品の名前を表示します。
[ボードの部品番号 (Board Part Number)] フィールド	ボードの部品番号を表示します。
[ボードシリアル番号 (Board Serial Number)] フィールド	ボードのシリアル番号を表示します。
[ボード エキストラ (Board extra)] フィールド	ボードに関する追加情報を表示します。
[製品のメーカー (Product manufacturer)] フィールド	製品のメーカーを表示します。

名前	説明
[製品名 (Product Name) ] フィールド	製品名を表示します。
[製品の部品型番 (Product part number) ] フィールド	製品の部品番号を表示します。
[製品シリアル番号 (Product Serial Number) ] フィールド	製品のシリアル番号を表示します。
[製品バージョン (Product Version) ] フィールド	製品のバージョンを表示します。
[製品追加 (Product extra) ] フィールド	製品に関する追加情報を表示します。
[製品アセット タグ (Product Asset tag) ] フィールド	製品のアセット タグを表示します。
[シャーシ タイプ (Chassis Type) ] フィールド	シャーシのタイプを示します。
[シャーシの部品番号 (Chassis part number) ] フィールド	シャーシの部品番号を表示します。
[シャーシのシリアル番号 (Chassis serial number) ] フィールド	シリアル番号の部品番号を表示します。
[追加シャーシ (Chassis extra) ] フィールド	シャーシに関する追加情報を表示します。
[正常性ロールアップ (Health rollup) ] フィールド	シャーシの全体的な正常性ステータスを表示します。

表 13: DIMM スロット

名前	説明
[ID] カラム	各 DIMM スロット エントリの一意の識別子を表示します。
[Health] カラム	DIMM スロットの現在のヘルスステータスを表示します。
[ロケーション番号 (Location number) ] カラム	DIMM スロットの位置番号を示します。
[部品番号 (Part Number) ] フィールド	DIMM の部品番号を表示します。
[シリアル番号 (Serial Number) ] フィールド	DIMM のシリアル番号を表示します。
[容量 MiB (Capacity MiB) ] フィールド	DIMM の容量を MiB で表示します。
[ステータス (状態) (Status (State)) ] フィールド	DIMM スロットの現在の状態を示します。
[有効 (Enabled) ] フィールド	DIMM スロットが有効かどうかを示します。

名前	説明
[説明 (Description) ] フィールド	DIMM の簡単な説明を提供します。
[メモリ タイプ (Memory type) ] フィールド	DIMM のメモリのタイプを表示します。
[ベース モジュール タイプ (Base Module Type) ] フィールド	DIMM の基本モジュール タイプを示します。
[バス幅ビット (Bus width bits) ] フィールド	DIMM のバス幅をビット単位で表示します。
[データ幅ビット (Data width bits) ] フィールド	DIMM のデータ幅をビット単位で表示します。
[メモリスピードを運用 (Operating Memory Speed) ] フィールド	DIMM の動作速度を MHz で表示します。

表 14: ストレージ

名前	説明
[ID] カラム	各ストレージ エントリの一意の識別子を表示します。
[Health] カラム	ストレージの現在の正常性ステータスを表示します。
[StorageControllers (名前) (StorageControllers (Name)) ] フィールド	ストレージ コントローラの名前を表示します。
[StorageControllers (FirmwareVersion) ] フィールド	ストレージコントローラのファームウェアバージョンを表示します。
[説明 (Description) ] フィールド	ストレージの簡単な説明を提供します。
[SpeedGbps] フィールド	ストレージの速度を Gbps 単位で表示します。
[モデル (Model) ] フィールド	ストレージのモデルを表示します。
[ステータス (状態) (Status (State)) ] フィールド	ストレージの現在の状態を示します。
[SerialNumber] フィールド	ストレージのシリアル番号を表示します。

表 15: Fans

名前	説明
[ID] カラム	各ファン エントリの一意の識別子を表示します。
[Health] カラム	ファンの現在の正常性ステータスを表示します。
[名前 (Name) ] フィールド	ファンの名前を表示します。

名前	説明
[部品番号 (Part Number) ] フィールド	ファンの部品番号を表示します。
[ファン回転速度 (Fan speed) ] フィールド	ファンの速度を RPM で表示します。
[ステータス (状態) (Status (State)) ] フィールド	ファンの現在の状態を示します。
[ステータス (正常性ロールアップ) (Status (Health rollup)) ] フィールド	ファンの全体的な正常性ステータスを表示します。

表 16: 電源モジュール

名前	説明
[ID] カラム	各電源エントリの一意の識別子を表示します。
[Health] カラム	電源の現在の正常性ステータスを表示します。
[名前 (Name) ] フィールド	電源装置の名前を表示します。
[部品番号 (Part Number) ] フィールド	電源装置の製品番号を表示します。
[シリアル番号 (Serial Number) ] フィールド	電源装置のシリアル番号を表示します。
[スペア部品番号 (Spare part number) ] フィールド	電源装置のスペア部品番号を表示します。
[モデル (Model)] フィールド	電源のモデルを表示します。
[ステータス (状態) (Status (State)) ] フィールド	電源装置の現在の状態を示します。
[メーカー (Manufacturer) ] フィールド	電源装置の製造元が表示されます。

表 17: プロセッサ

名前	説明
[ID] カラム	各プロセッサ エントリの一意の識別子を表示します。
[Health] カラム	プロセッサの現在の正常性ステータスを示します。
[名前 (Name) ] フィールド	プロセッサの名前を表示します。
[部品番号 (Part Number) ] フィールド	プロセッサの部品番号を表示します。
[シリアル番号 (Serial Number) ] フィールド	プロセッサのシリアル番号を表示します。
[モデル (Model)] フィールド	プロセッサのモデルを表示します。
[アセット タグ (Asset tag) ] フィールド	プロセッサのアセット タグを表示します。

名前	説明
[ステータス (状態) (Status (State))] フィールド	プロセッサの現在の状態を示します。
[メーカー (Manufacturer)] フィールド	プロセッサの製造元が表示されます。
[プロセッサ タイプ (Processor Type)] フィールド	プロセッサのタイプを示します。
[プロセッサ アーキテクチャ (Processor architecture)] フィールド	プロセッサのアーキテクチャを表示します。
[手順セット (Instruction set)] フィールド	プロセッサでサポートされている命令セットを表示します。
[速度 (MHz) (Speed (MHz))] フィールド	プロセッサの最大速度 (MHz) を表示します。
[合計コア (Total cores)] フィールド	プロセッサのコアの総数を表示します。
[合計スレッド (Total Threads)] フィールド	プロセッサ内のスレッドの総数を表示します。

表 18: ネットワーク アダプタ

名前	説明
[ID] カラム	各ネットワーク アダプタ エントリの一意の識別子を表示します。
[Health] カラム	ネットワーク アダプタの現在の正常性ステータスを表示します。
[名前 (Name)] フィールド	ネットワーク アダプタの名前を表示します。
[Vendor] フィールド	ネットワーク アダプタのベンダーを表示します。
[シリアル番号 (Serial Number)] フィールド	ネットワーク アダプタのシリアル番号を表示します。
[部品番号 (Part Number)] フィールド	ネットワーク アダプタの部品番号を表示します。
[メーカー (Manufacturer)] フィールド	ネットワーク アダプタの製造元が表示されます。
[ファームウェアバージョン (Firmware Version)] フィールド	ネットワーク アダプタのファームウェアバージョンを表示します。
[ステータス (状態) (Status (State))] フィールド	ネットワーク アダプタの現在の状態を示します。

# CPU のモニタリングと管理

## 概要

CPU は、すべての計算タスクを実行するシステムの中心的なコンポーネントです。BMC は、温度や電力消費などの CPU の側面をモニターし、正常な範囲内で動作することを確認します。これにより、過熱やハードウェア障害を防ぎ、システムの安定性と信頼性を確保できます。さらに、管理者はシステムのワークロードを把握し、必要に応じてリソース割り当てを調整して、パフォーマンスと応答時間を最適化できます。

## 異常の検出と対応

CPU に異常（過度の高温など）が発生した場合、BMC は監視して警告を発することができるため、管理者は問題に迅速に対応し、トラブルシューティングを行うことができます。

## モニター対象および制御対象の機能

BMC は、次の CPU 機能をモニターおよび制御します。

- CPU 温度を取得
- 現在の CPU 電力消費量を取得
- CPU の最大電力制限の取得
- CPU の現在の電力制限の取得
- CPU 電力制限の設定

# 冷却管理

BMC は、温度センサーを監視し、熱エンジニアリングチームによって作成されたファンアルゴリズムに基づいてファン速度を調整することで、冷却システムを管理します。

## BMC ブート プロセスとデフォルトのファン制御

BMC の起動プロセス中に、コンポーネントからの温度測定値が正常に取得されなかった場合、BMC はデフォルトのファン制御を実装します。このシナリオでは、すべてのシステムセンサーからの温度データにアクセスできるようになるまで、すべてのファンが 80% のデューティ サイクルで動作します。

## ファンアルゴリズムのアクティブ化

ファンアルゴリズムがアクティブな場合、BMC はファン速度を管理するか、特定の条件下でシステムのシャットダウンを開始します。

- フルスピードファン動作の条件：

- コンポーネントの温度が指定されたしきい値を超えています。
  - 温度の読み取りが 60 秒を超えて失敗する。
  - ファームウェアの更新を開始されました。
  - GPU がシステム仕様と一致していません。
- システムをシャットダウンする条件：
- 温度がクリティカルしきい値を 60 秒以上超えています。
  - 温度が指定されたしきい値（UNR）を超えています。

## ファンの障害状態を管理

システムファンは3つのファンゾーンに分かれており、それぞれが特定の冷却機能を果たします。

- **ファン ゾーン #1**：GPU スレッドの冷却に使用されます。
- **ファン ゾーン #2**：CPU スレッドの冷却に使用されます。
- **ファン ゾーン #3**：SSD 冷却に使用されます。

### ファン障害応答

ファン障害状態が発生すると、BMC は残りのすべてのファンをフルスピードで動作するように設定するか、システムをシャットダウンします。ファンの障害状態が解消されると、BMC はファン制御アルゴリズムに従ってファン速度を復元します。ファンの障害は、次のシナリオに分類されます：

- **ファン ゾーン #1 の障害状態**：
  - 同じファンの一方または両方のファンローターが指定されたしきい値（LC）を下回っている場合、ファンゾーン #1 の残りのすべてのファンがフルスピードで動作します。
  - 異なるファンで2つのファンローターがしきい値（LC）を下回っている場合、または3つ以上のファンローターがしきい値（LC）を下回っている場合、システムはシャットダウンします。
- **ファン ゾーン #2 の障害状態**：
  - 1つのファンローターが指定されたしきい値（LC）を下回っている場合、ファンゾーン #2 の残りのすべてのファンがフルスピードで動作します。
  - 2つのファンローターがしきい値（LC）を下回ると、システムがシャットダウンします。

• ファンゾーン #3 の障害状態 :

- 1つのファンローターが指定されたしきい値 (LC) を下回っている場合、ファンゾーン #3 の残りのすべてのファンがフルスピードで動作します。
- 2つのファンローターがしきい値 (LC) を下回ると、システムがシャットダウンします。

## センサーステータスの表示

BMC は、温度、電力、ファン速度、論理センサーなどの主要なシステム センサーをモニターします。これらのセンサーは、GUIからアクセスできるリアルタイムの値とステータスを提供します。

### 手順

**ステップ 1** [ナビゲーション ペイン (Navigation Pane) ]で、[ハードウェア ステータス > センサー (Hardware Status Sensors) ]を選択します。

**ステップ 2** 次のプロパティを表示することができます :

表 19: センサー

名前	説明
[Name] カラム	センサーの名前を表示します。
[Status] カラム	センサーの現在のステータスを表示します。
[下限クリティカル (Lower critical) ] フィールド	センサーの下限クリティカルしきい値を表示します。
[下限警告 (Lower warning) ] フィールド	センサーの下限警告しきい値を表示します。
[現在の値 (Current Value) ] フィールド	センサーによって測定された現在の値を表示します。
[上限警告 (Upper warning) ] フィールド	センサーの警告しきい値の上限を表示します。
[クリティカルの上限 (Upper critical) ] フィールド	センサーの上限しきい値を表示します。

# システム識別 LED のオン/オフ

## 手順

---

ステップ1 [ナビゲーション ペイン (Navigation Pane) ]で、[ハードウェア ステータス > インベントリと LED (Hardware Status Inventory and LED) ]を選択します。

ステップ2 [LED 照明制御 (LED Light control) ]で、システムの位置を特定しやすいように [システム アイデンティティ LED (System identity LED) ] ボタンのオンとオフを切り替えます。

---



## 第 4 章

### 操作

- Cisco BMC とサーバー工場設定をリセット (27 ページ)
- KVM コンソールの起動 (28 ページ)
- BMC のファームウェア (29 ページ)
- OEM ファームウェアのアップデート (30 ページ)
- BMC をリブート (30 ページ)
- Serial over LAN (SOL) の表示 (31 ページ)
- サーバーの電源操作 (32 ページ)
- 仮想メディア イメージの追加 (33 ページ)

## Cisco BMC とサーバー工場設定をリセット

Cisco BMC システムには、BMC を元の製造元の設定に復元する工場出荷時設定へのリセットインターフェイスが含まれています。このインターフェイスは広く定義されており、さまざまな Cisco BMC サービス間でさまざまな実装が可能です。この柔軟性により、必要に応じて個々のサービスを工場出荷時のデフォルトにリセットできます。

サーバーの電源がオフの場合、次のメッセージが表示されることがあります。

BMC とサーバーの両方の設定をリセットしますか？

#### 始める前に

BMC をリセットする前に、次の点を考慮してください。

- すべての手動設定が削除されます。
- バックアップが存在する場合は、パーティション構成とプラットフォームキーストアを回復できます。
- すべての BMC ログが削除されます。
- すべてのネットワークインターフェイスで現在アクティブなセッションが切断されます。
- BMC のデフォルトのアカウントとパスワードの設定が復元されます。

## 手順

---

ステップ 1 [ナビゲーション ペイン (Navigation Pane)] から、[操作 (Operations)] > [工場出荷時の状態にリセット (Factory reset)] を選択します。

ステップ 2 [システムをシャットダウンせずに続行 (Continue without shutdown the system)] チェックボックスをクリックします。

ステップ 3 [BMCとサーバーの設定のリセット (Reset BMC and server settings)] をクリックします。

ホストが ON ステートの場合、次の警告メッセージが表示されます：

```
Reset BMC and server settings
```

```
Do you want to reset both the BMC and server settings?
```

```
All manual settings will be deleted.
```

```
Partition configurations and the platform keystore may be recovered if backups exist.
```

```
All BMC logs will be removed.
```

```
Currently active sessions on all network interfaces will be disconnected.
```

```
The BMC default account and password settings will be restored.
```

```
Resetting without shutting down the system might cause an unrecoverable error.
```

```
Continue without shutting down the system
```

ステップ 4 [はい (Yes)] をクリックして続行します。

---

## KVM コンソールの起動

## 手順

---

ステップ 1 [ナビゲーション ペイン (Navigation Pane)] から、[操作 (Operations)] > [KVM] を選択します。

ステップ 2 [Launch KVM] をクリックします。

[KVM] 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。

---

# BMC のファームウェア

## BMC ファームウェアの表示

### 手順

**ステップ 1** [ナビゲーション ペイン (Navigation Pane)] から、[操作 (Operations)] > [Firmware (ファームウェア)] を選択します。

**ステップ 2** [BMC とサーバー (BMC and server)] セクションの [実行中のイメージ (Running image)] で、[バージョン (Version)] を確認できます。

BMC ファームウェア バージョンは XYZ として表されます。X はメジャーバージョン、Y はマイナーバージョン、Z は BMC Aux ファームウェア バージョンを表します。たとえば、BMC ファームウェアのバージョン番号は 1.1.4 です。

## BMC ファームウェアの更新



(注) 更新プロセス中は、HTTPS サービスが一時的に使用できなくなります。この期間中は、WebUI、Redfish、またはその他の関連サービスにアクセスできません。サービスが完全に復元されるまで待ってから、技術情報にアクセスしてください。

### 始める前に

この手順を始める前にクライアントにファームウェアファイルが利用可能だということを確認します。

### 手順

**ステップ 1** [ナビゲーション ペイン (Navigation Pane)] から、[操作 (Operations)] > [Firmware (ファームウェア)] を選択します。

**ステップ 2** [ファイルを追加 (Add File)] をクリックしてファームウェア ファイルの場所を探すために参照します。  
ファームウェア ファイルを選択します。

**ステップ 3** ファームウェアアップデートを開始するために [アップデートを開始 (Start Update)] をクリックします。

# OEM ファームウェアのアップデート

## 始める前に

この手順を始める前にクライアントにファームウェアファイルが利用可能だということを確認します。



- (注) アップグレードするファームウェアのタイプに応じて、OEM ファームウェアのアップグレードでは、AC 電源の再投入またはホストの電源再投入が必要になる場合があります。
- **BIOS ファームウェア**：アクティブ化にはホストの電源の再投入が必要です。アップグレード後にこの手順を実行できることを確認します。
  - **FPGA ファームウェア**：アクティベーションにはサーバーの AC 電源の再投入が必要です。アップグレード後にこのアクションを完了する準備をしてください。

## 手順

ステップ 1 [ナビゲーション ペイン (Navigation Pane)] から、[操作 (Operations)] > [OEM Firmware (OEM ファームウェア)] を選択します。

ステップ 2 ドロップダウン リストからアップデートする特定のデバイスを選択します。

ステップ 3 [ファイルを追加 (Add File)] をクリックしてファームウェア ファイルの場所を探すために参照します。  
ファームウェア ファイルを選択します。

ステップ 4 [更新の開始 (Start Update)] をクリックして、ファームウェアの更新を開始します。

# BMC をリブート



- (注) BMC をリブートすると、Web ブラウザと BMC との接続が数分間失われます。BMC がオンラインに戻ったら、再度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 ペイン (Navigation Pane)] から、[操作 (Operations)] > [リブート BMC (Reboot BMC)] を選択します。
- ステップ 2** [BMC をリブート (Reboot BMC)] をクリックします。
- [確認 (Confirm)] をリブートに続きます。
- 

## Serial over LAN (SOL) の表示

Serial over LAN (SOL)、または BMC シリアル トラフィック リダイレクションは、シリアル コントローラ トラフィックをベースボードから IPMI セッションにリダイレクトします。この プロトコルは、BMC との接続を介して、オペレーティング システム (OS) 内およびプレ OS フェーズ中に非同期通信を可能にします。SOL は、IPMI LAN セッションを介して、OS コマンドライン インターフェイス、シリアル リダイレクト BIOS インターフェイス、その他のシリアル テキスト ベースのアプリケーションなどのシリアル テキスト ベースのインターフェイスを操作する場合に特に役立ちます。

SOL は、IPMI プラットフォーム管理への LAN ベースのアクセスとシリアル テキスト リダイレクションを統合 インターフェイスで統合し、単一のリモート コンソール アプリケーションで両方の機能をサポートできるようにします。SOL の許可とアクセス制御は、IPMI 管理に使用されるのと同じユーザー構成 インターフェイスを介して管理されます。この統合により、さまざまなプラットフォーム間で連携して動作する構成ソフトウェア、リモート管理アプリケーション、および構成ユーティリティの開発が合理化されます。

## 手順

- 
- ステップ 1** [ナビゲーション ペイン (Navigation Pane)] から、[操作 (Operations)] > [SOL コンソール (SOL console)] を選択します。
- ステップ 2** 画面に表示されるインターフェイスを使用して、サーバのシリアルポート出力を直接接続されているかのようにモニタおよび管理します。
-

# サーバーの電源操作

## サーバーの電源状態の表示

### 手順

ステップ1 [ナビゲーション ペイン (Navigation Pane)] から、[操作 (Operations)] > [サーバー電源オペレーション (Server power operations)] を選択します。

ステップ2 [現在のステータス (Current status)] で、次のプロパティを表示できます。

名前	説明
Server status	サーバーの電源が現在オンかオフかを示します。
最後の電源操作	サーバーの最新の電源再投入またはシャットダウンイベントの日時を記録します。

## サーバの再起動

### 始める前に

[再起動 (Reboot)] オプションは、サーバーの電源が入っている場合にのみ使用できます。サーバーの電源がオフの場合、[再起動 (Reboot)] オプションは表示されず、代わりに [電源オン (Power On)] と表示されます。

### 手順

ステップ1 [ナビゲーション ペイン (Navigation Pane)] から、[操作 (Operations)] > [サーバー電源オペレーション (Server power operations)] を選択します。

ステップ2 [サーバーの再起動 (Reboot server)] では、1つのオプションのみが使用可能で、デフォルトではが選択されています：

- [整頓された (Orderly)] : オペレーティングシステムがシャットダウンした後、サーバーがリブートします

ステップ3 [再起動 (Reboot)] をクリックして、再起動プロセスを開始します。

## サーバーのシャットダウン

### 始める前に

[シャットダウン (Shut down)] オプションは、サーバーの電源が入っている場合にのみ使用できます。サーバーの電源がオフの場合、[シャットダウン (Shut down)] オプションは表示されず、代わりに [電源オン (Power On)] と表示されます。

### 手順

---

ステップ 1 [ナビゲーション ペイン (Navigation Pane)] から、[操作 (Operations)] > [サーバー電源オペレーション (Server power operations)] を選択します。

ステップ 2 シャットダウン オプションから、次のいずれかを選択します。

- [Orderly] : オペレーティング システムがシャットダウンし、サーバーが再起動します。
- [即時 (Immediate)] : オペレーティング システムをシャットダウンせずにサーバーをシャットダウンします。データが破損する可能性があります

ステップ 3 [シャットダウン (Shut down)] をクリックして、シャットダウン プロセスを開始します。

---

## ブート ソースのオーバーライド

### 手順

---

ステップ 1 [ナビゲーション ペイン (Navigation Pane)] から、[操作 (Operations)] > [サーバー電源オペレーション (Server power operations)] を選択します。

ステップ 2 [Boot Source Override] ドロップダウン リストから、目的のブート ソースを選択します。

ステップ 3 デフォルトのブート順序を変更せずに、次のシステム起動時にブート デバイスを一時的に変更するには、[ワンタイム ブートを有効にする (Enable one time boot)] を選択します。

ステップ 4 [保存 (Save)] をクリックして、変更内容を保存します。

---

## 仮想メディア イメージの追加

仮想メディアを使用すると、BMC を介してサーバー ホストに ISO/IMG ドライブ イメージをリモートでマウントできます。リモート ドライブは、USB ストレージ デバイスとしてホストに表示され、コンテナの制限と書き込み保護スイッチを考慮して、読み取り専用モードまたは

読み取り/書き込みモードで動作します。この機能を使用して、ベアメタル システムに OS をインストールできます。

#### 始める前に

この手順を開始する前に、クライアントでイメージファイルが使用可能であることを確認します。



---

(注) ローカル イメージのみがサポートされます。リモート ファイル共有からのイメージのマッピングまたはクライアント外部の仮想メディア (vMedia) のマッピングはサポートされていません。適切に機能させるために、すべてのイメージがローカルに保存されていることを確認します。

---

#### 手順

---

**ステップ 1** [ナビゲーション ペイン (Navigation Pane)] から、[操作 (Operations)] > [仮想メディア (Virtual media)] を選択します。

**ステップ 2** [ファイルの追加 (Add file)] をクリックし、追加するイメージを参照します。  
イメージ ファイルを選択します。

**ステップ 3** [スタート (Start)] をクリックします。

---



## 第 5 章

# 設定

- [日付と時刻の構成 \(35 ページ\)](#)
- [Cisco BMCのネットワーク管理 \(36 ページ\)](#)
- [電源復元ポリシーの設定 \(39 ページ\)](#)

## 日付と時刻の構成

### 手順

ステップ 1 [ナビゲーション ペイン (Navigation Pane)] で、[設定 (Settings)] [> 日付と時刻 (Date and time)] を選択します。

ステップ 2 [構成設定 (Configure Settings)] で、次のオプションのいずれかを選択します：

- 手動
- NTP

ステップ 3 [マニュアル (Manual)] は、次のプロパティを更新します：

名前	説明
[日付 (Date)] フィールド	YYYY-MM-DD 形式で入力します。
[24時間表記 (UTC) (24-hour time (UTC))] フィールド	HH:MM フォーマットで時間を入力します。

ステップ 4 [NTP] は、次のプロパティを更新します：

名前	説明
[サーバ 1 (Server 1)] フィールド	最初の NTP サーバーを指定します。
[サーバ 2 (Server 2)] フィールド	2 番目の NTP サーバーを指定します。

名前	説明
[サーバ 3 (Server 3)] フィールド	3 番目の NTP サーバーを指定します。

ステップ 5 [設定の保存 (Save Settings)] をクリックします。

## Cisco BMCのネットワーク管理

Cisco BMC は、Web GUI、Redfish、IPMI コマンドなどのさまざまなインターフェイスを提供し、BMC ネットワークの包括的な管理を容易にします。ネットワーク構成には、IP アドレス、IP アドレス送信元、ゲートウェイの構成などのタスクが含まれます。

基本的なネットワーク構成機能は次のとおりです：

- IP アドレス送信元
- IP アドレス
- [ゲートウェイ (Gateways)]
- サブネット マスク

## ネットワーク設定の表示または構成



(注) 共有 NIC (eth1) は、X710 OCP カードに関連付けられます。接続とパフォーマンスを最適化するためにネットワークインターフェイスを設定するときに、この構成が考慮されていることを確認します。

### 手順

ステップ 1 [ナビゲーション ペイン (Navigation Pane)] で、[設定 (Settings)]、> [ネットワーク (Network)] の順に選択します。

ステップ 2 [ネットワーク設定 (Network Settings)] で、次のプロパティを更新します：

名前	説明
[Hostname] フィールド	BMC の完全修飾ドメイン名 (FQDN) を指定します。  編集ボタンをクリックして、ドメイン名を更新します。

名前	説明
[ドメイン名を使用 (Use domain name) ] トグルボタン	ネットワーク通信にドメイン名を使用するオプションを有効または無効にします。
[DNSサーバーを使用 (Use DNS servers) ] トグルボタン	ホスト名を IP アドレスに解決するために DNS サーバーを使用するオプションを有効または無効にします。
[NTPサーバーを使用 (Use NTP servers) ] トグルボタン	ネットワーク タイム プロトコル サーバーを使用して BMC のクロックを同期するオプションを有効または無効にします。
[共有NIC (eth1) を使用 (Use Shared NIC (eth1)) ] トグル ボタン	ネットワーク接続に共有ネットワーク インターフェイス カード (NIC) eth1 を使用するオプションを有効または無効にします。

ステップ 3 eth0/eh1 では、次のプロパティを表示できます。

名前	説明
[リンク ステータス (Link Status) ] フィールド	ネットワーク リンクの現在のステータスを示し、アクティブ (LinkUp) か非アクティブかを示します。
[速度 (mbps) (Speed (mbps)) ] フィールド	ネットワーク接続の現在の速度をメガビット/秒 (Mbps) で表示します。
インターフェイス設定	
[FQDN] フィールド	インターフェイスに割り当てる完全修飾ドメイン名 (FQDN) を指定します。
[MAC アドレス (MAC Address) ] フィールド	ネットワーク インターフェイスに割り当てられた一意の Media Access Control (MAC) アドレスを表示します。

## IPv4 アドレスの表示または追加

### 手順

ステップ 1 [ナビゲーション ペイン (Navigation Pane) ] で、[設定 (Settings) ]、> [ネットワーク (Network) ] の順に選択します。

ステップ 2 [IPv4] で、次のプロパティを更新します。

名前	説明
DHCP トグル ボタン	自動 IP アドレス割り当てに Dynamic Host Configuration Protocol (DHCP) をイネーブル化またはディセーブル化します。  DHCP を有効にすると、[静的 IPv4 アドレスの追加 (Add static IPv4 address)] ウィンドウが表示されます。
[IP Address] フィールド	ネットワーク上でデバイスを一意に識別する、デバイスに割り当てられたインターネットプロトコル (IP) アドレスを指定します。
[ゲートウェイ (Gateway)] フィールド	ネットワーク ゲートウェイの IP アドレスを入力します。ネットワーク ゲートウェイは、ローカルネットワークと他のネットワークまたはインターネットとの間でトラフィックを渡すアクセスポイントまたはルータとして機能します。
[サブネットマスク (Subnet mask)] フィールド	IP アドレスのどの部分がネットワークを参照し、どの部分がデバイスを参照するかを指定して、ネットワーク アドレスの範囲を入力します。

ステップ 3 [IPv4 アドレス (IPv4 addresses)] で、次のプロパティを表示できます：

名前	説明
[IP アドレス (IP Address)] カラム	ネットワーク上でデバイスを一意に識別する、デバイスに割り当てられたインターネットプロトコル (IP) アドレスを指定します。
[ゲートウェイ (Gateway)] カラム	ローカルネットワークと他のネットワークまたはインターネットとの間でトラフィックを渡すアクセスポイントまたはルータとして機能するネットワークゲートウェイの IP アドレスを指します。
[サブネットマスク (Subnet mask)] カラム	IP アドレスのどの部分がネットワークを参照し、どの部分がデバイスを参照するかを指定して、ネットワーク アドレス範囲を定義します。
[発信元アドレス (Address origin)] カラム	IP アドレスの取得方法を示します。DHCP によって動的に割り当てられるか、ユーザーによって静的に設定されます。

## 静的 DNS IP アドレスの表示、追加、または削除

### 手順

ステップ 1 [ナビゲーション ペイン (Navigation Pane)] で、[設定 (Settings)]、> [ネットワーク (Network)] の順に選択します。

ステップ 2 [静的 DNS (Static DNS)] で、[IP アドレスの追加 (Add IP address)] をクリックします。

[IP アドレスの追加 (Add IP address)] ウィンドウが表示されます。

ステップ 3 [IP アドレスの追加 (Add IP address)] ウィンドウで、次のプロパティを更新します。

名前	説明
[静的 DNS (Static DNS)] フィールド	DHCP が無効の場合にドメイン名解決に使用する静的 DNS サーバー アドレスを入力します。

ステップ 4 [Add] をクリックします。

ステップ 5 (任意) IP アドレスを削除するには、削除する行に対応する削除アイコンをクリックします。

## 電源復元ポリシーの設定

### 手順

ステップ 1 [ナビゲーション ペイン (Navigation Pane)] で、[設定 (Settings)] > [電源の復元 (Power restore policy)] を選択します。

ステップ 2 [電源復元ポリシー (Power Restore Policies)] で、次のいずれかを選択します：

- [常時オン (Always on)] : 電源が投入されるたびにシステムの電源がオンになります。
- [常にオフ (Always off)] : 電源が投入されると、システムの電源はオフのままになります。
- [最終状態 (Last state)] : 電源が投入されると、システムは前回の電源状態 (オンまたはオフ) に戻ります。

ステップ 3 [保存設定 (Save settings)] をクリックします。





## 第 6 章

# セキュリティとアクセス

- ユーザ セッション (41 ページ)
- LDAP 設定 (42 ページ)
- ユーザ管理 (44 ページ)
- ポリシーを更新しています (48 ページ)
- 証明書の管理 (49 ページ)

## ユーザ セッション

### ユーザ セッションの表示

手順

**ステップ 1** [ナビゲーション ペイン (Navigation Pane)] から、[セキュリティ (Security)] を選択し、> [セッション (Sessions)] にアクセスします。

**ステップ 2** 次のプロパティを表示することができます :

名前	説明
[Session ID] カラム	トラッキングおよび管理の目的で、各アクティブな Web ユーザーセッションに割り当てられる一意の識別子。
[Username] カラム	サーバー ログイン セッションに関連付けられているアカウント名。
[IP アドレス (IP Address)] カラム	セッション中にサーバーにアクセスするデバイスのネットワーク アドレス。

## セッションの切断

### 手順

ステップ1 [ナビゲーションペイン (Navigation Pane)]から、[セキュリティ (Security)]を選択し、>[セッション (Sessions)]にアクセスします。

ステップ2 セッションを切断するには、切断するセッションの行に対応する[切断 (Disconnect)]をクリックします。

## LDAP 設定

### LDAP 認証のイネーブル化

Cisco BMCでは、SSH、Redfish、Web サーバー、およびホスト コンソール インターフェイスにより、LDAP ディレクトリに対する認証が許可されます。ただし、IPMI インターフェイスは、セッションのセットアップ時にクリアテキストのパスワードを要求するため、LDAP に対して認証できません。PAM ベースの認証が実装されているため、LDAP ユーザーとローカルユーザーの両方で認証フローが同じになります。

LDAP ユーザー アカウントの場合、Cisco BMC 権限ロールに対応する LDAP 属性タイプはありません。推奨される方法は、LDAP ユーザーアカウントをLDAPグループにグループ化することです。その後、Redfish と GUI を使用して、特権ロールをLDAPグループに割り当てることができます。

### 手順

ステップ1 [ナビゲーションペイン (Navigation Pane)]で、[セキュリティ (Security)]を選択し、>LDAPにアクセスします。

ステップ2 [LDAP 認証 (LDAP authentication)]で、次のプロパティを更新します：

名前	説明
[有効化 (Enable)] チェックボックス	[有効 (Enable)] チェックボックスをオンにして、LDAP 認証オプションをアクティブにします。

名前	説明
[サービス タイプ (Service Type) ] オプション ボタン	オプション ボタンを選択して、適切なサービス タイプを選択します。  <ul style="list-style-type: none"> <li>ディレクトリ サービスとして OpenLDAP を使用するには、<b>[OpenLDAP]</b> オプション ボタンを選択します。</li> <li>Microsoft のアクティブ ディレクトリ サービスを使用するには、<b>[アクティブ ディレクトリ サービス (Active Directory) ]</b> オプション ボタンを選択します。</li> </ul>
[サーバー URI (Server URI) ] フィールド	サーバーの URI を入力します。
[Bind DN] フィールド	ベース識別名を入力します。
[バインドパスワード (Bind Password) ] フィールド	バインド DN のパスワードを入力します。
[ベース DN (Base DN) ] フィールド	ベース識別名を入力します。
[ユーザー ID 属性 (User ID Attribute) ] : (オプション) フィールド	ユーザーの識別の属性を入力します。
[グループ ID 属性 (Group ID Attribute) ] : (オプション) フィールド	グループの識別の属性を入力します。
[SSL 証明書の管理 (Manage SSL Certificate) ]	詳細については、 <a href="#">新しい証明書の追加 (50 ページ)</a> をクリックしてください。

ステップ 3 [保存設定 (Save settings) ] をクリックします。

## ロールグループの追加

グループロールは、ユーザの第1レベルの許可を決定し、必要なインターフェイスへのアクセスが許可されるかどうかを確立します。たとえば、ユーザーが Web サーバー グループにのみ属し、SSH グループに属していない場合、ユーザーは SSH にログインできません。共通のユーザー管理内にグループロールがあると、異なるアプリケーションが相互にロールを作成できます。たとえば、管理ユーザーは Web サーバーを介して新しいユーザーを作成し、Web サーバー、Redfish、IPMI、およびその他のインターフェイスにログインする機能を付与できます。

### 始める前に

LDAP 認証が有効になっていることを確認します。

## 手順

ステップ1 [ナビゲーション ペイン (Navigation Pane)] で、[セキュリティ (Security)] を選択し、>LDAP にアクセスします。

ステップ2 [ロール グループの追加 (Add Role Group)] をクリックします。

ステップ3 次の項目を更新します。

名前	説明
[グループ名 (Group Name)] フィールド	システム内で識別するために、役割グループの名前を入力します。
[グループ 特権 (Group Privilege)] フィールド	ドロップダウンリストからグループに適切なレベルのアクセスを選択します： <ul style="list-style-type: none"> <li>• 管理者</li> <li>• 演算子</li> <li>• ReadOnly</li> </ul>

## ユーザ管理

### ユーザの追加

Cisco BMC は、ユーザー アカウントの効果的な管理を容易にする Web GUI を提供します。これには、ユーザー名の定義、パスワードの設定と変更、特権レベルとチャネルアクセスの構成などのタスクが含まれます。これらの設定は、個々のユーザIDにリンクされ、管理コントローラに関連付けられた不揮発性ストレージフレームワーク内に構造化アレイとして保存されます。

## 手順

ステップ1 [ナビゲーション ペイン (Navigation Pane)] で、[セキュリティ (Security)] を選択し、>[ユーザー管理 (User Management)] にアクセスします。

ステップ2 [ユーザの追加 (Add User)] をクリックします。

[ユーザの追加 (Add user)] ウィンドウが表示されます。

ステップ3 [ユーザーを追加 (Add user)] ウィンドウで、次のプロパティを更新します：

名前	説明
[アカウントの状態 (Account status) ]ラジオ ボタン	アカウントを即時に <b>Activate</b> するために[有効 (Enabled) ]ラジオ ボタンを選択します。  アクティベーション無しでアカウントを作成するには、[無効化 (Disabled) ]ラジオ ボタンを選択します。
[Username] フィールド	ユーザー名を入力します。  ユーザー名 ルールの UI 手順に従ってください。
[ユーザー パスワード (User password) ] フィールド	ユーザのパスワードを入力します。  パスワード ルールの UI 手順に従ってください。
[ユーザー パスワードを確認 (Confirm user Password) ] フィールド	確認のためにパスワードを再入力します。
[特権 (Privilege) ] ドロップダウン リスト	[特権 (Privilege) ] ドロップダウン リストから、適切なロールを選択します：  <ul style="list-style-type: none"> <li>• [管理者 (Administrator) ] : フルアクセスとコントロール</li> <li>• [オペレータ (Operator) ] : 制限された操作アクセス</li> <li>• [読み取り専用 (ReadOnly) ] : 読み取り専用アクセス</li> </ul>

ステップ 4 [ユーザの追加 (Add User) ] をクリックします。

## ユーザの編集

### 手順

ステップ 1 [ナビゲーション ペイン (Navigation Pane) ]で、[セキュリティ (Security) ] を選択し、 >[ユーザー管理 (User Management) ] にアクセスします。

ステップ 2 ユーザーを編集するには、編集するユーザーレイヤに該当する編集アイコンをクリックします。

[AP を編集 (Edit AP) ] ウィンドウが表示されます。

ステップ 3 [ユーザーを編集 (Edit user) ] ウィンドウで、次のプロパティを更新します：

名前	説明
[アカウントの状態 (Account status) ]ラジオ ボタン	アカウントを即時に <b>Activate</b> するために[有効 (Enabled) ] ラジオ ボタンを選択します。  アクティベーション無しでアカウントを作成するには、[無効化 (Disabled) ] ラジオ ボタンを選択します。
[Username] フィールド	ユーザー名を入力します。  ユーザー名 ルールの UI 手順に従ってください。
[ユーザー パスワード (User password) ] フィールド	ユーザのパスワードを入力します。  パスワードルールの UI 手順に従ってください。
[ユーザー パスワードを確認 (Confirm user Password) ] フィールド	確認のためにパスワードを再入力します。
[特権 (Privilege) ] ドロップダウン リスト	[特権 (Privilege) ] ドロップダウン リストから、適切なロールを選択します：  <ul style="list-style-type: none"> <li>• [管理者 (Administrator) ] : フルアクセスとコントロール</li> <li>• [オペレータ (Operator) ] : 制限された操作アクセス</li> <li>• [読み取り専用 (ReadOnly) ] : 読み取り専用アクセス</li> </ul>

ステップ 4 [保存 (Save) ] をクリックします。

## ユーザーの有効化または無効化

### 手順

ステップ 1 [ナビゲーション ペイン (Navigation Pane) ] で、 [セキュリティ (Security) ] を選択し、 > [ユーザー管理 (User Management) ] にアクセスします。

ステップ 2 ユーザーを有効または無効にするには、有効または無効にするユーザーの行に対応するチェックボックスをオンにします。

チェック ボックスをオンにする時、追加オプションを含む新しいヘッダー行がテーブルの上に現れます。

ステップ3 [有効 (Enable) ] / [無効 (Disable) ] をクリックします。

## アカウントポリシー設定を管理

### 手順

ステップ1 [ナビゲーションペイン (Navigation Pane) ]で、[セキュリティ (Security) ]を選択し、>[ユーザー管理 (User Management) ]にアクセスします。

ステップ2 [アカウントポリシー設定 (Account Policy Settings) ] をクリックします。

[アカウントプロフィール設定 (Account Profile Settings) ] ウィンドウが表示されます。

ステップ3 [アカウントポリシー設定 (Account policy settings) ] ウィンドウで、次のプロパティを更新します：

名前	説明
[ログイン試行の最大失敗回数 (Max failed login attempts) ] フィールド	0 から 65535 までの値を入力してください。
[ユーザーのロック解除方法 (User unlock method) ] ラジオ ボタン	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• [手動 (Manual) ] : ロック解除のために手動による介入を要求するには、[手動 (Manual) ] オプション ボタンを選択します。</li> <li>• [タイムアウト後に自動 (Automatic After Timeout) ] : 指定したタイムアウト後に自動的にロックを解除するには、[タイムアウト後に自動 (Automatic After Timeout) ] オプション ボタンを選択します。</li> </ul>
[タイムアウト時間 (秒) (Timeout duration (seconds)) ] フィールド	[タイムアウト後に自動 (Automatic After Timeout) ] を選択した場合は、[タイムアウト期間 (秒) (Timeout Duration (seconds)) ] から期間を入力します。

ステップ4 [保存 (Save) ] をクリックします。

## ユーザの削除

ルート ユーザーは削除できません。

## 手順

---

ステップ1 [ナビゲーションペイン (Navigation Pane)] で、[セキュリティ (Security)] を選択し、> [ユーザー管理 (User Management)] にアクセスします。

ステップ2 ユーザーを削除するには、削除するユーザーの行に対応するチェックボックスをオンにします。  
チェックボックスをオンにする時、追加オプションを含む新しいヘッダー行がテーブルの上に現れます。

ステップ3 [削除 (Delete)] をクリックします。

---

## ポリシーを更新しています

### SSH を通して BMC シェルの有効化または無効化

Cisco BMC 内の BMC ヘルス モニターは、BMC のヘルス ステータスを追跡および報告し、その動作ステータスに関するリアルタイムの更新を提供します。この機能は、温度、電圧、ファン速度、ハードウェア ヘルス イベントなどの主要なインジケータをモニターします。必要なモニタリングおよびアラートメカニズムを提供することで、管理者が BMC の適切な機能を確保するのを支援します。包括的なリアルタイムの正常性レポートを提供することで、管理者は問題を迅速に特定して解決し、システムのメンテナンスと信頼性を向上させることができます。

## 手順

---

ステップ1 [ナビゲーションペイン (Navigation Pane)] で、[セキュリティとアクセス>ポリシー (Security and access Policies)] を選択します。

ステップ2 BMC シェル (SSH 経由) トグルボタンを使用して、BMC のポート 22 を介したシェルセッションへのアクセスを有効または無効にします。

---

### ネットワーク IPMI を有効化または無効化

## 手順

---

ステップ1 [ナビゲーションペイン (Navigation Pane)] で、[セキュリティとアクセス>ポリシー (Security and access Policies)] を選択します。

ステップ2 [Network IPMI] (アウトオブバンドIPMI) トグルボタンを使用して、IPMI を介したリモート管理を有効または無効にします。

## 証明書の管理

### 証明書の詳細の表示

証明書管理により、既存の証明書ファイルと秘密キーファイルを、認証局 (CA) によって発行された代替ファイルに簡単に置き換えることができます。この機能により、サーバー証明書とクライアント証明書の両方をシームレスに展開できます。GUI では、暗号化されていない .pem 形式の証明書と秘密キーファイルを使用して証明書を更新し、秘密キーを対応する署名付き証明書と統合できます。

#### 手順

ステップ1 [ナビゲーションペイン (Navigation Pane)] で、[セキュリティ (Security)] を選択し、> [証明書 (Certificates)] にアクセスします。

ステップ2 [証明書 (Certificates)] で、次のプロパティを表示できます：

名前	説明
[証明書 (Certificates)] カラム	証明書の名前または、識別子を表示します。
[発行元 (Issued by)] 列	証明書を発行した認証または、エンティティを表示します。
[発行先 (Issued to)] 列	証明書が発行された受信者または、エンティティを示します。
[有効開始日 (Valid from)] 列	証明書の有効期間の開始日。
[有効期限 (Valid until)] 列	証明書の有効期間の終了日。

## 新しい証明書の追加

### 手順

ステップ1 [ナビゲーションペイン (Navigation Pane)]で、[セキュリティ (Security)]を選択し、>[証明書 (Certificates)]にアクセスします。

ステップ2 [新しい証明書の追加 (Add new certificate)]をクリックします。

[新しい証明書の追加 (Add new certificate)]ウィンドウは、表示されます。

ステップ3 [新しい証明書の追加 (Add new certificate)]ウィンドウで、次のプロパティを更新します：

名前	説明
[証明書タイプ (Certificate Type)] ドロップダウンリスト	次のいずれかを選択します。 <ul style="list-style-type: none"> <li>LDAP 証明書：LDAP 関連の認証に使用します。</li> <li>Certificate Authority (CA) 証明書：認証局の目的で使用します。</li> </ul>
[ファイルを追加 (Add File)] ボタン	[ファイルの追加 (Add file)]をクリックして、クライアントから証明書ファイルを参照して選択します。

ステップ4 [追加 (Add)]をクリックします。

## 証明書署名要求を生成する

### 手順

ステップ1 [ナビゲーションペイン (Navigation Pane)]で、[セキュリティ (Security)]を選択し、>[証明書 (Certificates)]にアクセスします。

ステップ2 [CSR の作成 (Generate CSR)]をクリックします。

[証明書署名要求 (CSR) を生成 (Generate a Certificate Signing Request (CSR))]ウィンドウを表示します。

ステップ3 [証明書署名要求 (CSR) の生成 (Generate a Certificate Signing Request (CSR))]ウィンドウで、次のプロパティを更新します：

名前	説明
[証明書タイプ (Certificate Type) ] ドロップダウンリスト	ドロップダウンメニューから、次のいずれかのオプションを選択します： <ul style="list-style-type: none"> <li>• HTTPS 証明書：Web 通信を保護するために使用します。</li> <li>• LDAP 証明書：LDAP 関連の認証に使用します。</li> </ul>
[国/地域 (Country/Region) ] ドロップダウンリスト	ドロップダウンメニューを国または、地域から選択します。
[状態 (State) ] フィールド	都道府県名を入力します。
[市区町村 (City) ] フィールド	市区町名を入力します。
[会社名 (Company Name) ] フィールド	会社名を入力します。
[会社名ユニット (Company Unit) ] フィールド	社内のユニットを入力します。
[Common Name] フィールド	証明書の一般名を入力します。
[連絡先担当者 (Contact Person) ] (オプション) フィールド	担当者の名前を入力してください。
[電子メールアドレス (オプション) (Email Address (optional)) ] フィールド	メールアドレスを入力します。
[代行ユーザ名 (オプション) (Alternate Name (optional)) ] フィールド	スペースで区切ると、代替の名を入力できます。
[秘密キー (Private Key) ] [キー ペア アルゴリズム (Key Pair Algorithm) ] ドロップダウンリスト	ドロップダウンメニューから、次のいずれかを選択します： <ul style="list-style-type: none"> <li>• EC：短いキーでより高いセキュリティを実現する楕円曲線暗号化。</li> <li>• RSA：広く使用されている暗号化方式の Rivest-Shamir-Adleman アルゴリズム。</li> </ul>

ステップ 4 [CSR の作成 (Generate CSR) ] をクリックして、証明書署名要求を作成します。





## 第 7 章

# リソース管理

- [電力構成の表示 \(53 ページ\)](#)
- [電力制限の適用 \(54 ページ\)](#)

## 電力構成の表示

### 手順

**ステップ 1** [ナビゲーション ペイン (Navigation Pane)] で、[リソース管理 (Resource Management)] > [電力 (Power)] を選択します。

**ステップ 2** 次のプロパティを表示することができます：

名前	説明
[Name] カラム	コンポーネントまたはデバイスを識別します。
[消費電力 (Power Consumption)] カラム	現在の電力の使用状況を表示します。
[パワー キャッピング (Power Cap)] カラム	コンポーネントに設定されている最大電力制限を示します。
[最小制限 (Cap Minimum)] カラム	最小許容電力制限を表示します。
[最大制限 (Cap Maximum)] カラム	最大許容電力制限を表示します。

## 電力制限の適用

### 手順

---

**ステップ 1** [ナビゲーション ペイン (Navigation Pane) ]で、[リソース管理 (Resource Management) ]>[電力 (Power) ] を選択します。

**ステップ 2** 電力制限オプションを有効にするには、[電力制限の適用 (Apply power cap) ]チェックボックスをオンにします。

**ステップ 3** [Power cap value (in watts)]で、必要な電力制限値をワット単位で入力します。  
値が最小キャップ制限と最大キャップ制限の間にあることを確認します。

**ステップ 4** [保存 (Save) ] をクリックしてパワーキャップ設定を適用します。

---



## 第 8 章

# GPU 管理

---

- GPU 管理 (55 ページ)
- 日付と時刻の構成 (56 ページ)
- GPU FRU 情報の表示 (56 ページ)
- GPU 電源および温度センサーの表示 (57 ページ)
- GPU 電力構成の表示 (58 ページ)
- イベント ログ (59 ページ)
- GPU ファームウェアのアップデート (60 ページ)

## GPU 管理

### 概要

GPUは、さまざまなアプリケーションの高性能コンピューティングおよびグラフィック処理に広く使用されています。BMCは、温度などのGPUの正常性ステータスをモニターして、計算負荷が高いときの過熱や誤動作を防ぎ、ハードウェアの信頼性と寿命を確保します。

### モニター対象および制御対象の機能

BMCは、次のGPU機能をモニターおよび制御します：

- GPU 温度をモニターする
- 現在の GPU 電力消費量をモニターする
- GPU ボード上のコンポーネントの温度をモニターする
- GPU ボード上のコンポーネントの電力消費をモニターする
- GPU ボード上のコンポーネントのバージョンを表示する
- GPU ボード上の GPU ファームウェアおよびコンポーネントファームウェアをリモートで更新する

## 日付と時刻の構成



(注) このオプションは、一部のCisco UCS C885A M8 ラック サーバ構成でのみ利用可能です。

### 手順

ステップ 1 [ナビゲーション ペイン (Navigation Pane)] で、[設定 (Settings)] [> 日付と時刻 (Date and time)] を選択します。

ステップ 2 [構成設定 (Configure Settings)] で、次のオプションのいずれかを選択します：

- 手動
- GPU 日時を BMC 日時と同じに設定する

ステップ 3 [マニュアル (Manual)] は、次のプロパティを更新します：

名前	説明
[日付 (Date)] フィールド	YYYY-MM-DD 形式で入力します。
[24 時間表記 (UTC) (24-hour time (UTC))] フィールド	HH:MM フォーマットで時間を入力します。

ステップ 4 BMC から設定を自動的にインポートするには、[GPU 日時を BMC 日時と同じにする (Set GPU Datetime to be the BMC Datetime)] を選択します。

ステップ 5 [設定 (Set)] をクリックします。

## GPU FRU 情報の表示

### 手順

ステップ 1 [ナビゲーション ペイン (Navigation Pane)] で、[GPU 管理 (GPU Management)] > [情報 (Information)] を選択します。

ステップ 2 [FRU アセンブリ (FRU Assembly)] で、次のプロパティを表示できます：

名前	説明
モデル (Model)	GPU モデルを表示します。
名前	GPU 名を表示します。
製品番号	GPUに関連付けられている製品番号を一覧表示します。
物理コンテキスト	GPUの物理的なコンテキストまたは配置を記述します。
シリアル番号 (Serial Number)	GPU のシリアル番号を表示します。
ベンダー	GPU のベンダーまたは製造元を識別します。

ステップ 3 [バージョン (Versions) ]で、次のプロパティを表示できます：

名前	説明
[Name] カラム	GPUに関連するコンポーネントまたはソフトウェアを識別します。
[バージョン (Version) ]カラム	コンポーネントまたはソフトウェアに関連付けられているバージョン番号を表示します。

## GPU 電源および温度センサーの表示

### 手順

ステップ 1 [ナビゲーションペイン (Navigation Pane) ]で、[GPU 管理 (GPU Management) ]>[センサー (Sensors) ]を選択します。

ステップ 2 [電力 (Power) ]で、次のプロパティを表示できます。

名前	説明
[Name] カラム	パワー センサーを識別します。
[現在の値 (Current Value) ]カラム	現在の電力測定値を表示します。
[最小の値 (Current Value) ]カラム	記録された最小電力値を表示します。
[最大の値 (Current Value) ]カラム	記録された最大電力値を表示します。

ステップ3 [温度 (Temperature)] では、次のプロパティを表示できます：

名前	説明
[Name] カラム	温度センサーを識別します。
[現在の値 (Current Value)] カラム	現在の温度測定値を表示します。
[最小の値 (Current Value)] カラム	記録された最小温度値を表示します。
[現在の値 (Current Value)] カラム	記録された最大温度値を表示します。
[クリティカル上限 (Critical High)] カラム	温度センサーのクリティカル上限しきい値を示します。
[クリティカル下限 (Critical Low)] カラム	温度センサーの重大な下限しきい値を示します。

## GPU 電力構成の表示

### 手順

ステップ1 [ナビゲーション ペイン (Navigation Pane)] で、[GPU 管理 (GPU Management)] > [電力 (Power)] を選択します。

ステップ2 次のプロパティを表示することができます：

名前	説明
[Name] カラム	GPU を識別します。
[消費電力 (Power Consumption)] カラム	現在の電力の使用状況を表示します。
[パワーキャッピング (Power Cap)] カラム	GPU に設定されている最大電力制限を示します。

## GPU 電力制限の適用

### 手順

ステップ1 [ナビゲーション ペイン (Navigation Pane)] で、[GPU 管理 (GPU Management)] > [電力 (Power)] を選択します。

ステップ2 [電力制限の適用 (Apply power cap)] チェックボックスを選択します。

ステップ3 [電力制限値 (ワット) (Power cap value (in watts))] フィールドに、200 ~ 750 の値を入力します。

ステップ4 [保存 (Save)] をクリックします。

## イベント ログ

### GPU イベント ログの表示

#### 手順

ステップ1 ナビゲーション ウィンドウから、[GPU 管理 (GPU Management)] > [イベント ログ (Event logs)] を選択します。

ステップ2 次のオプションに基づいてイベント ログをフィルタ処理できます。

- 開始と終了の日付
- 重要度に基づく：(OK、Warning、および Critical)
- 検索フィールドを使用して検索キーワード

次のログ 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	各ログ エントリの一意の識別子を表示します。
[シビラティ (重大度) (Severity)] カラム	ログ エントリの重要度または影響のレベルを示します。次のいずれかになります。 <ul style="list-style-type: none"> <li>• [OK]：ログ エントリが正常または成功した操作を表していることを示します。</li> <li>• [クリティカル (critical)]：すぐに対処が必要な重大な問題があることを示します。</li> <li>• [注意 (Warning)]：モニターする必要がある潜在的な問題を示します。</li> </ul>
[日付 (Date)] カラム	ログ エントリが記録された日時を表示します。

名前	説明
[Description] カラム	ログエントリに関する簡単な概要または詳細を提供します。

## GPU イベント ログのエクスポート

### 手順

- ステップ 1** ナビゲーションウィンドウから、[GPU 管理 (GPU Management)] > [イベント ログ (Event logs)] を選択します。
- ステップ 2** 1 つのログ エントリをエクスポートするには、エクスポートする行に対応するエクスポートアイコンをクリックします。
- ステップ 3** (任意) すべてのログ エントリをエクスポートするには、[すべてエクスポート (Export all)] をクリックします。  
ブラウザ設定によって、JSON ログ ファイルを開くまたは、保存することをプロンプトされる場合があります。

## GPU ファームウェアのアップデート

### 始める前に

この手順を始める前にクライアントにファームウェアファイルが利用可能だということを確認します。

### 手順

- ステップ 1** [ナビゲーションペイン (Navigation Pane)] で、[GPU 管理 (GPU Management)] > [Firmware (ファームウェア)] を選択します。
- ステップ 2** [ファイルを追加 (Add File)] をクリックしてファームウェア ファイルの場所を探すために参照します。  
ファームウェア ファイルを選択します。
- ステップ 3** ファームウェアアップデートを開始するために [アップデートを開始 (Start Update)] をクリックします。

### 次のタスク

ファームウェアの更新が完了したら、AC 電源の再投入を実行して GPU のアップグレードをアクティブ化して完了します。





## 付録 **A**

### REST API

- [HTTP メソッド \(HTTP Methods\)](#) (63 ページ)
- [ステータス コード](#) (64 ページ)
- [認証](#) (68 ページ)
- [利用可能な API](#) (69 ページ)

### HTTP メソッド (HTTP Methods)

以下で説明するように、次のHTTPメソッドを使用してさまざまなアクションを実装します。

HTTP メソッド	説明
POST	<p>最初の方法は、新しい技術情報を作成するために使用されます。POST 要求は、新しい技術情報が属する技術情報コレクションに送信されます。コレクションを表す技術情報にPOST 要求を送信することは、その技術情報のメンバズ プロパティに同じ要求を送信することと同じです。</p> <p>最後のメソッドは、オブジェクトに対する操作（アクションなど）を開始するために使用されます。サービスは、アクションを送信するための POST メソッドをサポートする必要があります。POST 操作はべき等ではない場合があります。</p>
GET	<p>GET メソッドは、技術情報の表現を取得するために使用されます。その表現は、単一の技術情報またはコレクションのいずれかです。</p>

HTTP メソッド	説明
PUT	PUT メソッドは、技術情報を完全に置き換えるために使用されます。要求本文から省略されたプロパティは、デフォルト値にリセットされます。
PATCH	PATCH 方式は、既存の技術情報で更新を実行するために使用される推奨方式です。技術情報への変更は、要求本文で送信されます。要求本文で指定されていないプロパティは、PATCH 要求によって直接変更されません。応答は、更新が行われた後の空または技術情報の表現のいずれかです。実装は、独自のポリシーに基づいて特定のフィールドの更新操作を拒否する場合があります、その場合は、要求された更新を適用しません。
DELETE	DELETE メソッドは、技術情報を取り除くために使用されます。サービスは、削除できる技術情報の DELETE メソッドをサポートする必要があります。

## ステータスコード

HTTP は、応答メッセージで返されるステータスコードを定義します。

ステータスコード	ステータス名	説明
200	OK	要求が正常に完了し、本文に表現が含まれています。
201	Created	新しいリソースを作成した要求が正常に完了しました。 Location ヘッダーは、新しく作成されたリソースの正規 URI に設定されます。新しく作成されたリソースの表現は、応答本文に含まれる場合があります。

ステータスコード	ステータス名	説明
202	Accepted	要求の処理は受け入れられましたが、処理が完了していません。Location ヘッダーは、後で操作のステータスを判断するために照会できるタスクリソースの URI に設定する必要があります。タスクリソースの表現は、応答本文に含めることができます。
204	コンテンツなし	要求は成功しましたが、応答の本文にコンテンツが返されません。
301	完全に移動	要求されたリソースは、別の URI にあります。
302	検出済み	要求されたリソースは一時的に別の URI にあります。
304	未変更	サービスは、アクセスが許可されている条件付き GET 要求を実行しましたが、リソースの内容は変更されていません。条件付き要求は、ヘッダー If-Modified-Since および/または If-None-Match を使用して開始され、変更がない場合はネットワーク帯域幅を節約します。
401	Unauthorized	この要求に含まれる認証クレデンシャルが欠落しているか、無効です。
403	Forbidden	サーバーは要求内のクレデンシャルを認識しましたが、それらのクレデンシャルにはこの要求を実行する権限がありません。
404	Not Found	要求で、存在しないリソースの URI が指定されました。

ステータスコード	ステータス名	説明
405	Method Not Allowed	リクエストで指定されたHTTP動詞(DELETE、GET、HEAD、POST、PUT、PATCHなど)は、このリクエストURIではサポートされていません。応答には、Request-URIで識別されるリソースでサポートされるメソッドのリストを提供するAllowヘッダーが含まれます。
406	Not Acceptable	要求でAcceptヘッダーが指定されましたが、この要求で識別されるリソースは、Acceptヘッダーのメディアタイプの1つに対応する表現を生成できません。
409	競合	プラットフォームでサポートされているリソースの現在の状態で競合が発生する可能性があるため(たとえば、互換性のない値を使用してリンクされた方法で機能する複数の属性を設定しようとした場合)、作成要求または更新要求を完了できませんでした。

ステータスコード	ステータス名	説明
410	Gone	要求されたリソースがサーバーで使用できず、転送アドレスが不明なことを示しています。この状態は永続的であると見なされます。リンク編集機能を持つクライアントは、ユーザーの承認後に Request-URI への参照を削除する必要があります。サーバーが状態が永続的であるかどうかを認識していない場合、または決定する機能がない場合は、代わりにステータスコード404 (Not Found) を使用する必要があります (SHOULD)。この応答は、特に明記されていない限りキャッシュ可能です。
411	必須となる長さ	要求は、Content-Length ヘッダーを使用してコンテンツの長さを指定しませんでした (代わりに Transfer-Encoding : chunked が使用された可能性があります)。アドレス指定されたリソースには、Content-Length ヘッダーが必要です。
412	必須条件に失敗しました	前提条件 (OData-Version、If Match、If Not Modified ヘッダーなど) のチェックに失敗しました。
415	Unsupported Media Type	要求で、サポートされていない本文の Content-Type が指定されています。
500	Internal Server Error	サーバーで、要求の処理を妨げる予期しない状態が発生しました。

ステータスコード	ステータス名	説明
501	Not Implemented	サーバーは要求を処理するために必要な機能を（現在）サポートしていません。これは、サーバーが要求メソッドを認識せず、リソースのメソッドをサポートできない場合に適切な応答です。
503	Service Unavailable	サーバーの一時的な過負荷またはメンテナンスのため、サーバーは現在リクエストを処理できません。

## 認証

BMC は、認証を使用して特定の Redfish 技術情報アクセスする必要があります。Redfish は、RFC7617 で定義されている HTTPS 基本認証と呼ばれるアクセス方法を提供し、ユーザーが Redfish 技術情報にアクセスできるようにします。この方法では、TLS に準拠した接続のみを使用して、サードパーティの認証サービスとクライアント間でデータを転送します。ローカル BMC 認証またはLDAPや現用系ディレクトリなどのリモート認証を使用してログインします。

curl を使用した HTTPS 基本認証の適用例：

```
#
#UCS-Server: /logs$ curl -k -X GET https://<username>:<password>@<BMC IP>/redfish/v1 |
jq.
%Total %Received %xferd Average Speed      Time      Time      Time      Current
           Dload  Upload  Total      Spend    Left     Speed
100 1532 100 1532 0 0   10281           0--:--:--:--:--:--:--:  :--:  :--:  10281{
  "@odata.id": "/redfish/v1",
  "@odata.type": "#ServiceRoot.v1_11_0.ServiceRoot",
  "AccountService": {
    "@odata.id": "/redfish/v1/AccountService"
  },
  "Cables": {
    "@odata.id": "/redfish/v1/Cables"
  },
  "CertificateService": {
    "@odata.id": "/redfish/v1/CertificateService"
  },
  "Chassis": {
    "@odata.id": "/redfish/v1/Chassis"
  },
  "EventService": {
    "@odata.id": "/redfish/v1/EventService"
  },
  "Id": "RootService",
  "JsonSchemas": {
    "@odata.id": "/redfish/v1/JsonSchemas"
  },
  "Links": {
```

```

    "Sessions": {
      "@odata.id": "/redfish/v1/SessionService/Sessions"
    },
    "Managers": {
      "@odata.id": "/redfish/v1/Managers"
    },
    "Name": "Root Service",
    "ProtocolFeaturesSupported": {
      "DeepOperations": {
        "DeepPATCH": false,
        "DeepPOST": false
      },
      "ExcerptQuery": false,
      "ExpandQuery": {
        "ExpandAll": false,
        "Levels": false,
        "Links": false,
        "NoLinks": false
      },
      "FilterQuery": false,
      "OnlyMemberQuery": true,
      "SelectQuery": true
    },
    "RedfishVersion": "1.9.0",
    "Registries": {
      "@odata.id": "/redfish/v1/Registries"
    },
    "SessionService": {
      "@odata.id": "/redfish/v1/SessionService"
    },
    "Systems": {
      "@odata.id": "/redfish/v1/Systems"
    },
    "Tasks": {
      "@odata.id": "/redfish/v1/TaskService"
    },
    "TelemetryService": {
      "@odata.id": "/redfish/v1/TelemetryService"
    },
    "UUID": "1b187d13-66a7-4429-8496-b497d28931ba",
    "UpdateService": {
      "@odata.id": "/redfish/v1/UpdateService"
    }
  }
}

```

## 利用可能な API

次の Redfish 定義の URI がサポートされています：

Resource	リソース URI
サービス ルート	/redfish/v1/
アカウント サービス	/redfish/v1/AccountService
マネージャ アカウント の収集	/redfish/v1/AccountService/Accounts

Resource	リソース URI
マネージャアカウント	/redfish/v1/AccountService/Accounts/{{account_instance}}
ロールコレクション	/redfish/v1/AccountService/Roles
ロール	/redfish/v1/AccountService/Roles/{{role_instance}}
シャーシ収集	/redfish/v1/Chassis
シャーシ	/redfish/v1/Chassis/{{chassis_instance}}
マネージャ収集	/redfish/v1/Managers
マネージャ	/redfish/v1/Managers/{{manager_instance}}
マネージャネットワーク プロトコル	/redfish/v1/Managers/{{manager_instance}}/NetworkProtocol
ログサービスの収集	/redfish/v1/Managers/{{manager_instance}}/LogServices
ログサービスの収集 (シャーシ)	/redfish/v1/Chassis/{{chassis_instance}}/LogServices
ログサービス	/redfish/v1/Managers/{{manager_instance}}/LogServices/ {{manager_log_instance}}
ログエントリ収集	/redfish/v1/Managers/{{manager_instance}}/LogServices/ {{manager_log_instance}}/Entries
ログエントリの収集 (シャーシ)	/redfish/v1/Chassis/{{chassis_instance}}/LogServices/ {{chassis_log_instance}}/Entries
ログエントリ	/redfish/v1/Chassis/{{chassis_instance}}/LogServices/{{chassis_log_instance}}/ /Entries/{{chassis_logentry_instance}}
ログエントリ (マネージャ)	/redfish/v1/Managers/{{manager_instance}}/LogServices/{{manager_log_instance}}/ /Entries/{{manager_logentry_instance}}
イーサネットインター フェイスの収集	/redfish/v1/Managers/{{manager_instance}}/EthernetInterfaces
イーサネットインター フェイス	/redfish/v1/Managers/{{manager_instance}}/EthernetInterfaces/{{manager_ethifc_instance}}
イベントサービス	/redfish/v1/EventService
セッションサービス	/redfish/v1/SessionService
セッション収集	/redfish/v1/SessionService/Sessions

Resource	リソース URI
セッション	/redfish/v1/SessionService/Sessions/{{session_id}}
サービスの更新	/redfish/v1/UpdateService
FirmwareInventory 収集	/redfish/v1/UpdateService/FirmwareInventory
FirmwareInventory	/redfish/v1/UpdateService/FirmwareInventory/{{firmwareinventory_instance}}



## 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。