



## Cisco IMC REST API の概要

---

この章は、次の内容で構成されています。

- [Introduction, on page 1](#)
- [新規および変更された API \(2 ページ\)](#)
- [Redfish™ アーキテクチャ \(3 ページ\)](#)
- [管理標準規格 \(5 ページ\)](#)
- [主なテクノロジー \(5 ページ\)](#)
- [運用モデル \(6 ページ\)](#)

### Introduction

Representational state transfer (REST) or RESTful web services allow you to provide interoperability between computer systems on the Internet. Using the REST-compliant web services you can request systems to access and manipulate textual representations of web resources using a uniform and predefined set of stateless operations. Cisco has now built capabilities of using RESTful APIs to configure the UCS C-series servers using the Redfish™ technology.

Redfish™ is an open industry standard specification and schema that specifies a RESTful interface and utilizes JSON and OData to help customers integrate solutions within their existing tool chains. It utilizes a range of scalable IT technologies that are widely used, and by using these accepted technologies, it makes the use of Redfish™ easier. Redfish™ is sponsored and controlled by the Distributed Management Task Force, Inc. (DMTF), a peer-review standards body recognized throughout the industry.



---

**Note** To determine which Cisco UCS rack-mount servers are supported by this firmware release, see the associated *Release Notes*. The release notes are available at the following URL: [http://www.cisco.com/en/US/products/ps10739/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps10739/prod_release_notes_list.html)

---

For more information on DMTF and Redfish™ standards, see [DMTF and Redfish™](#)

Beginning with release 4.2 (2a), you can use REST with Cisco UCS S-Series servers also.

# 新規および変更された API

## リリース 4.2(3d) の新規および変更された API

### 新規 API

- データの無害化 - リリース4.2(3d)以降、Cisco IMC はデータの無害化機能をサポートしています。データサニタイズプロセスを使用して、Cisco IMC はすべての機密データを消去し、お客様データの抽出または回復を不可能にします。ステータスレポートから個々のデバイス消去のデータサニタイズプロセスのステータスと進行状況を確認し、必要に応じて問題を修正することができます。
  - お客様データを含むコンポーネントでデータのサニタイズを実行する必要があります。
  - この機能は、次のサーバーでサポートされています。
    - Cisco UCS C220 M5、C240 M5、C480 M5、C125 M5 サーバー
    - Cisco UCS C220 M6、C240 M6、C225 M6、C245 M6 サーバー

## リリース 4.2(3b) の新規および変更された API

### 新規 API

- パスワード変更
- NULL アドレスを使用した LDAP サーバーの構成
- NIC での DDNS およびドメイン名プロパティのサポート
- 1 ~ 65535 の許容ポートで SMTP サービスを有効にする
- SSH プロトコルのセッションタイムアウトの設定
- シリアル オーバー LAN ポリシー用の COM ポートの設定




---

(注) この API は、C シリーズ サーバーと S シリーズ サーバーの両方で使用できます。

---

- 権限および暗号化キーの設定




---

(注) この API は、C シリーズ サーバーと S シリーズ サーバーの両方で使用できます。

---

### リリース 4.2 (2a) の新規および変更された API

- リリース 4.2 (2a) 以降、Cisco UCS S シリーズ サーバーで REST を使用できます。Cisco UCS S シリーズ サーバーの例については、[リリース 4.2 でサポートされる S シリーズ サーバーの Cisco IMC REST API の例](#) を参照してください。
- さまざまな認証方式の TACACS+ および優先順位の構成 : Redfish スキーマに従って、[優先順位 (Priority)] の値は Redfish API では [0] から始まりますが、他の Cisco IMC インターフェイスの場合、優先順位は [1] から始まります。
- 以下はリリース 4.2 (2a) では非推奨です。
  - /redfish/v1/Managers/CIMC URI の Oem/Cisco での [EncryptionStatus]
  - /redfish/v1/Managers/CIMC/NetworkProtocol URI の Oem/Cisco での [VideoEncryption]
  - /redfish/v1/Managers/CIMC/LogServices/CIMC URI の Oem/Cisco での [SyslogConnectionInfo]
- 新規 API
  - Cisco IMC Syslog 構成
  - FlexMMC 構成

### リリース 4.2 (1a) の新規および変更された API

#### 新規 API

- SNMP ユーザの設定
- MCTP 障害アラート設定の構成
- SPDM 認証局証明書の追加
- エンドポイント SPDM 証明書の表示

## Redfish™ アーキテクチャ

Redfish™ API は、「/redfish/」の Redfish ルートで始まるフォルダ構造で構成されます。C シリーズ サーバーの場合、ルートは URI `https://<Cisco IMC IP>/redfish/v1/` を介してアクセスされます。URI の末尾にある「v1」は、API のバージョンを示します。

URI は、リソースの主要な一意の識別子です。Redfish™ URI は、[RFC3986](#) で説明されている 3 つの部分で構成されます。パート 1 は URI のスキームとオーソリティを定義し、パート 2 はルート サービスとバージョンを指定し、パート 3 は一意のリソース識別子を定義します。

たとえば、次の URI : `https://mgmt.vendor.com/redfish/v1/Systems/SvrID:` で、

- `https://mgmt.vendor.com` はスキームと権限です。

- /redfish/v1 はルートとバージョンです。
- /Systems/SvrID はリソース識別子です。

### [Redfish™ ツリー構造 (Redfish™ Tree Structure) ]

Redfish ツリー構造は、RESTful インターフェースが分岐して多数の「コレクション」をカバーする最上位のルートで構成され、その後に複数のレベルが含まれ、ツリーのような構造が作成されます。この構造に移動して、情報と設定を見つけることができます。

たとえば、C シリーズ サーバー上のコントローラの Redfish™ 構造にアクセスするには、次のパスを使用してナビゲートします。

**https://10.10.10.10/redfish/v1/Systems/FCH2005V1EN/SimpleStorage/SLO T-HBA**



- (注) API パスの一部は、ハードウェア構成によって異なる場合があります。たとえば、管理対象サーバーに別の種類の RAID コントローラが搭載されている場合、「SLOT-HBA」は異なる場合があります。

### [Redfish™ 操作 (Redfish™ Operations) ]

Redfish™ は、HTTPS メソッドを使用して RESTful API の操作を実行します。作成するリクエストのタイプを指定できます。これは、標準の CRUD (作成、取得、更新、および削除) フォーマットに準拠しています。目的の結果に応じて、次のタイプのコマンドを発行できます。

- **GET** : データの表示
- **POST** : リソースの作成またはアクションの使用
- **PATCH** : リソースの 1 つ以上のプロパティの変更
- **DELETE** : リソースの削除



- (注) 現在、HEAD および PUT 操作は Redfish™ URI ではサポートされていません。

表 1: Redfish スキーマと仕様

リリース	Redfish スキーマ	Redfish 仕様
リリース 4.2 (1a)	<a href="https://www.dmtf.org/sites/default/files/standards/documents/DSP8010_2020.3.zip">https://www.dmtf.org/sites/default/files/standards/documents/DSP8010_2020.3.zip</a>	<a href="https://www.dmtf.org/sites/default/files/standards/documents/DSP0266_1.7.0.pdf">https://www.dmtf.org/sites/default/files/standards/documents/DSP0266_1.7.0.pdf</a>
リリース 4.2 (2a)	<a href="https://www.dmtf.org/sites/default/files/standards/documents/DSP8010_2021.1.zip">https://www.dmtf.org/sites/default/files/standards/documents/DSP8010_2021.1.zip</a>	<a href="https://www.dmtf.org/sites/default/files/standards/documents/DSP0266_1.13.0.pdf">https://www.dmtf.org/sites/default/files/standards/documents/DSP0266_1.13.0.pdf</a>

リリース	Redfish スキーマ	Redfish 仕様
リリース 4.2(3b)	<a href="https://www.dmtf.org/sites/default/files/standards/documents/DSP8010_2021.1.zip">https://www.dmtf.org/sites/default/files/standards/documents/DSP8010_2021.1.zip</a>	<a href="https://www.dmtf.org/sites/default/files/standards/documents/DSP0266_1.13.0.pdf">https://www.dmtf.org/sites/default/files/standards/documents/DSP0266_1.13.0.pdf</a>

## 管理標準規格

IT ソリューション モデルは何年にもわたって進化し、いくつかのアウトオブバンド (OOB) システム管理標準、つまり、新興のプログラミング標準内で機能し、組み込みシステムに実装できるライトアウト管理 (LOM) システムに取って代わられました。これは非常にうまく機能しましたが、IT ソリューションのさまざまな要求を確実に処理できる単一の管理標準が依然として必要でした。拡張されたスケール、より高いセキュリティ、およびマルチベンダーのオープン性は、同様に多様な DevOps ツールとプロセスを必要とします。

これらの要件を念頭に置いて、DMTF は新しい管理インターフェイス標準を作成する責任を負い、2015 年 7 月に正式にリリースされた Redfish™ バージョン 1.0 になりました。

Redfish™ 管理標準の主な機能は次のとおりです。

- 使用がシンプル、かつ安全性が高い
- 暗号化された接続と全体的に強化されたセキュリティ
- スクリプトを使用して簡単に管理できるシンプルなプログラム インターフェイス
- Open Compute Project のリモート マシン管理要件に適合
- Web API およびデータ形式の広く使用されている標準に基づいています。

Redfish™ は、モノリシック サーバーからコンバージドインフラストラクチャ、ハイパースケールアーキテクチャまで、あらゆる種類のサーバーアーキテクチャをサポートできます。Redfish™ データ モデルはベンダーに中立であり、サーバー ステータス、インベントリ、および既存の運用機能を含む独自の構造とデータ形式を定義します。管理者は、管理スクリプトを自動化して Redfish™ 準拠サーバーを管理できるため、異種サーバー群を効率的に運用できます。

セキュリティの面では、Redfish™ は、従来の管理プロトコルとは対照的に、HTTPS 暗号化を使用することで、非常に安全で信頼性の高い通信の機会を提供します。暗号化されたパケットでネットワーク全体のイベント通知を含む、すべての Redfish™ ネットワーク トラフィックを伝達できるため、脅威を大幅に削減できます。

## 主なテクノロジー

### [HTTPS 通信 (HTTPS Communications) ]

Hypertext Transfer Protocol または HTTP は、コラボレーションハイパーメディア分散情報システム用のアプリケーションプロトコルであり、World Wide Web のデータ通信の基盤を形成しています。セキュア HTTP または HTTPS は、TLS または SSL によって暗号化されたネット

ワーク接続内で HTTP を操作することにより、セキュアな通信を可能にする HTTP のセキュアバージョンです。HTTPS を利用することにより、Redfish™ は、特に従来のサーバー管理プロトコルと比較して、サーバー管理のセキュリティを大幅に強化します。

### [RESTful アプリケーション プログラム インターフェイス (RESTful Application Programming Interface) ]

Representational State Transfer (REST) または RESTful API は、HTTP リクエストを使用して、GET、POST、および DELETE データの助けを借りて情報を取得するプログラミングインターフェイスです。多くの IT 企業は RESTful アーキテクチャを使用しています。この標準化されたアプローチを利用して、Redfish™ は、管理情報にアクセスし、サーバーの構成または操作状態を変更するコマンドを発行するための RESTful API を実装します。

## 運用モデル

Redfish™ 操作は、GET、POST、PATCH、および DELETE 操作に HTTPS を使用してクライアントによって開始され、管理対象サーバーからの JSON 応答を解釈することができます。応答は、要求された情報と、要求された操作の成功または失敗の指示を提供します。

### [Redfish™ クライアント (Redfish™ Client) ]

RESTful API は、「すべてがリソースである」という原則に従っています。これは、すべての Uniform Resource Identifier または URI が特定のタイプのリソース（サービス、コレクション、または個々のエンティティ）を表すことを意味します。ただし、Redfish™ コンテキスト内では、リソースは、URI にアクセスするときに返される HTTPS メッセージのコンテンツと考えることができます。さまざまな REST クライアントを使用して、次のような Redfish™ リソースにアクセスできます。

- Google Chrome Web ストアの「Advanced REST Client」や「Postman」などのアプリケーション。
- Firefox ブラウザ用の「REST Easy」および「RESTClient」プラグイン。
- URI の処理と JSON ペイロードの解析をサポートする cURL、Python、およびその他のスクリプトまたはプログラミング言語。

## 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。