



## アプライアンスの設置

---

- [設置に関する警告およびガイドライン \(1 ページ\)](#)
- [ラックに関する要件 \(3 ページ\)](#)
- [ラックへのアプライアンスの設置 \(3 ページ\)](#)
- [初期設定 \(9 ページ\)](#)
- [Cisco IMC 設定ユーティリティを使用したシステムのセットアップ \(13 ページ\)](#)
- [BIOS および Cisco IMC のファームウェアの更新 \(15 ページ\)](#)
- [システム BIOS へのアクセス \(15 ページ\)](#)
- [スマート アクセス \(シリアル\) \(16 ページ\)](#)
- [HDD/SSD 交換後の RAID コントローラの設定 \(16 ページ\)](#)
- [SED のドライブセキュリティの有効化 \(18 ページ\)](#)

## 設置に関する警告およびガイドライン



---

### 警告 安全上の重要な注意事項

この警告マークは「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。機器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、一般的な事故防止対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。

ステートメント 1071

---



---

### 警告 システムの過熱を防ぐため、最大推奨周囲温度の 35°C (95°F) を超えるエリアで操作しないでください。

ステートメント 1047

---



**警告** いつでも装置の電源を切断できるように、プラグおよびソケットにすぐ手が届く状態にしておいてください。

ステートメント 1019



**警告** この製品は、設置する建物に短絡（過電流）保護機構が備わっていることを前提に設計されています。この保護装置の定格が 250 V、15 A 以下であることを確認します。

ステートメント 1005



**警告** 装置は地域および国の電気規則に従って設置する必要があります。

ステートメント 1074



**警告** この装置は、立ち入りが制限された場所への設置を前提としています。立ち入りが制限された場所とは、特殊な器具、錠と鍵、またはその他の保安手段を使用しないと入れない場所を意味します。

ステートメント 1017



**注意** 適切なエアフローを確保するためには、レールキットを使用してアプライアンスを取り付けてください。レールキットを使用せずに、ユニットを別のユニットの上に物理的に置く、つまり「積み重ねる」と、サーバーの上部にある通気口がふさがれ、過熱したり、ファンの回転が速くなったり、電力消費が増えたりすることがあります。サーバーをラックに取り付ける際には、サーバー間に必要な最小の間隔がレールによって提供されるので、レールキットにサーバーをマウントすることを推奨します。レールキットを使用してユニットをマウントする場合は、サーバー間の間隔を余分にとる必要はありません。

アプライアンスを設置するときは、次の注意事項に従ってください。

- アプライアンス周辺に、スムーズな作業や適切なエアフローを確保できるだけの十分なスペースがあることを確認します。
- 空調が、[環境仕様](#)に記載された温度要件に適合していることを確認します。
- キャビネットまたはラックが、[ラックに関する要件 \(3 ページ\)](#)に記載された要件に適合していることを確認します。
- 設置場所の電源が、[電力仕様](#)に記載された電源要件に適合していることを確認します。使用可能な場合は、電源障害に備えて無停電電源装置 (UPS) を使用してください。

## ラックに関する要件

次のタイプのラックを使用する必要があります。

- 標準 48.3 cm (19 インチ) 幅 4 支柱ラック、ANSI/EIA-310-D-1992 のセクション 1 に準拠した英国ユニバーサルピッチに適合するマウント支柱付き。
- 付属のシスコ製スライドレールを使用する場合、ラック支柱の穴は、9.6 mm (0.38 インチ) の正方形、7.1 mm (0.28 インチ) の丸形、#12-24 UNC、または #10-32 UNC になります。
- サーバーごとの縦方向の最小ラックスペースは、1 ラックユニット (RU)、つまり 44.45 mm (1.75 インチ) である必要があります。

### ラックの設置に必要な工具

このアプライアンス用にシスコが販売しているスライドレールは、取り付けに工具が必要ありません。

### スライドレールおよびケーブル マネジメント アームの寸法

アプライアンスのスライドレールの調整範囲は 610 ~ 914 mm (24 ~ 36 インチ) です。

オプションのケーブル マネジメント アーム (CMA) を使用する場合、長さの要件がさらに追加されます。

- サーバーの背面から CMA の背面までの距離は、137.4 mm (5.4 インチ) 追加されます。
- CMA を含むサーバーの全長は 35.2 インチ (894 mm) です。

## ラックへのアプライアンスの設置

ここでは、シスコが販売するサポートレールキットを使用して、アプライアンスをラックに設置する方法について説明します。



**警告** ラックにこの装置をマウントしたり、ラック上の装置の作業を行うときは、ケガをしないように、装置が安定した状態に置かれていることを十分に確認してください。安全を確保するために、次のガイドラインを守ってください。

ラックに設置する装置が1台だけの場合は、ラックの一番下に取り付けます。

ラックに複数の装置を設置する場合は、最も重い装置を一番下に設置して、下から順番に取り付けます。

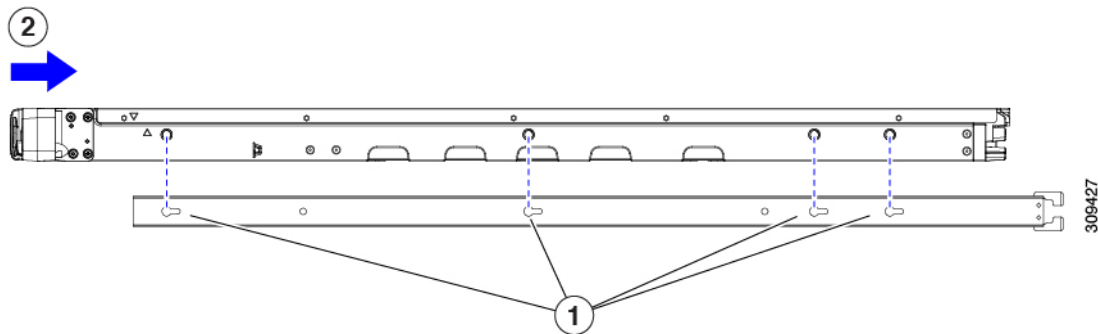
ラックにスタビライザが付いている場合は、スタビライザを取り付けてから、ラックに装置を設置したり、ラック内の装置を保守したりしてください。

ステートメント 1006

**ステップ1** アプライアンスの側面に内側レールを装着します。

- a) レール内の3つのキー付きスロットがアプライアンス側面の3個のペグの位置に合うように、内側レールをアプライアンスの一方の側の位置に合わせます。
- b) キー付きスロットをペグに設定し、レールを前面に向けてスライドさせて、ペグの所定の位置にロックします。
- c) 2つ目の内側レールをアプライアンスの反対側に取り付けます。

図1:アプライアンスの側面への内側レールの取り付け

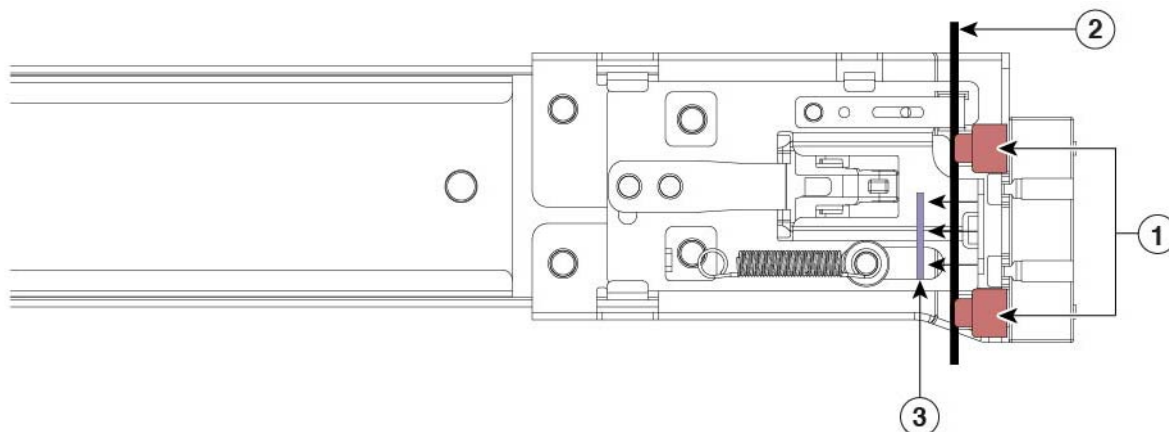


<b>1</b>	レールのキー付きスロット	<b>2</b>	アプライアンスの前面をキー付きスロットにスライドさせる
----------	--------------	----------	-----------------------------

**ステップ2** 両方のスライドレール部品で前面の固定プレートを開きます。スライドレール部品の前端に、バネ仕掛けの固定プレートがあります。取り付けペグをラック支柱の穴に挿入する前に、この固定プレートが開いている必要があります。

部品の外側で、背面を向いている緑の矢印ボタンを押して、固定プレートを開きます。

図 2: 前面の固定部分、前端の内側



1	前面側の取り付けペグ	3	開いた位置に引き戻された固定プレート
2	取り付けペグと開いた固定プレート の間のラック支柱	-	

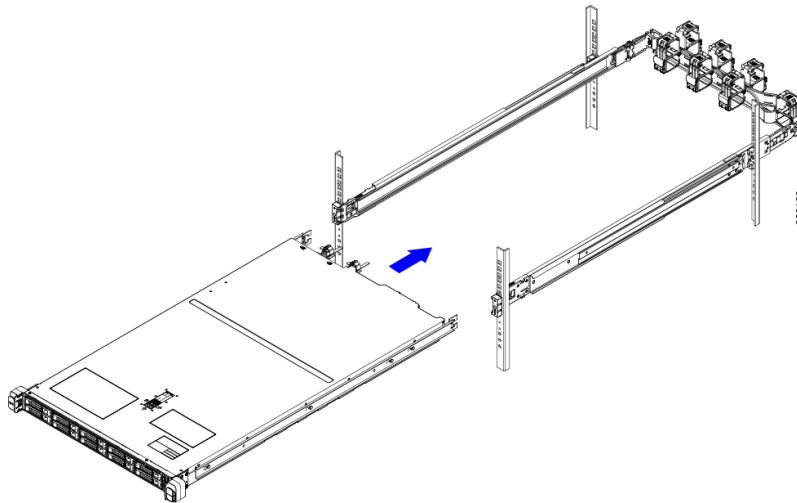
**ステップ 3** 外側のスライドレールをラックに取り付けます。

- a) 片側のスライドレール部品の前端を、使用する前面ラック支柱の穴の位置に合わせます。  
スライドレールの前部がラック支柱の外側を回り込むように配置され、取り付けペグが外側の前部からラック支柱の穴に入ります。  
(注) ラック支柱は、取り付けペグと開いた固定プレートの間にある必要があります。
- b) 取り付けペグを、外側前面からラック支柱の穴に押し込みます。
- c) 「Push」のマークが付いた固定プレートのリリースボタンを押します。ばね仕掛けの固定プレートが閉じて、ペグが所定の位置にロックされます。
- d) スライドレールの長さを調整したら、背面取り付けペグを対応する背面ラック支柱の穴に差し込みます。  
背面取り付けペグを、ラック支柱の内側から背面ラック支柱の穴に入れます。
- e) 2つ目のスライドレール部品の、ラックの反対側に取り付けます。2つのスライドレール部品が同じ高さであり、水平になっていることを確認します。
- f) 所定の位置に収まって留まるまで、各部品の内側のスライドレールをラック前方へ引き出します。

**ステップ 4** アプライアンスをスライドレールに装着します。

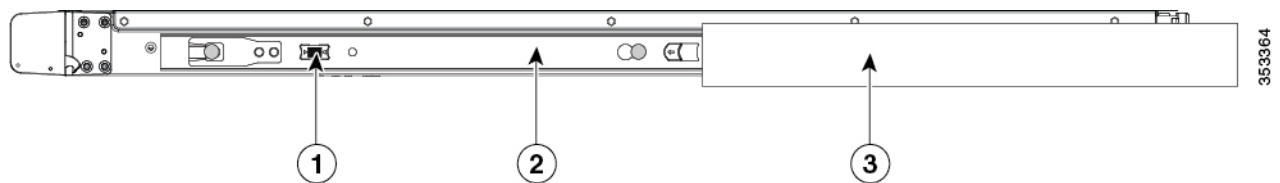
**注意** このアプライアンスは、コンポーネントがフルに搭載されている場合、最大で 27 kg (60 ポンド) の重量になります。アプライアンスを持ち上げるときは、2人以上で行うか、リフトを使用することを推奨します。この手順を 1人で実行しようとする、怪我や機器の損傷を招くおそれがあります。

- a) アプライアンスの側面に装着されている内側レールの後端を、ラック上の空のスライドレールの前端の位置に合わせます。
- b) 内部の停止位置で止まるまで、内側レールをラック上のスライドレールに押し込みます。



- c) 両方の内側レールで内側レールリリースクリップを背面に向けてスライドさせたら、前面のスラムラッチがラック支柱に収まるまで、アプライアンスをラックに押し込みます。

図 3:内側レールリリースクリップ



<b>1</b>	内側レール リリース クリップ	<b>3</b>	ラック支柱に装着されている外側スライドレール
<b>2</b>	アプライアンスに装着され、外側のスライドレールに挿入されている内側レール	-	

**ステップ 5** (任意) スライドレールに付属の2本のネジを使用して、アプライアンスをさらに確実にラックに固定します。アプライアンスを取り付けたラックを移動する場合は、この手順を実行します。

アプライアンスをスライドレールに完全に押し込んだ状態で、アプライアンス前面のヒンジ付きスラムラッチのレバーを開き、レバーの下にある穴からネジを挿入します。ネジがラック支柱のレールの静止部分に挿入され、アプライアンスが引き抜かれるのを防ぎます。反対のスラムラッチについても行ってください。

**ステップ 6** (任意) 該当する場合は、次の手順を実行します。

- a) ケーブルマネジメントアームを取り付けます。ケーブル マネジメント アームの取り付け (任意) (7 ページ) またはケーブル マネジメント アームを逆に取り付け (任意) (8 ページ) を参照してください。
- b) ロックベゼルを取り付けます。

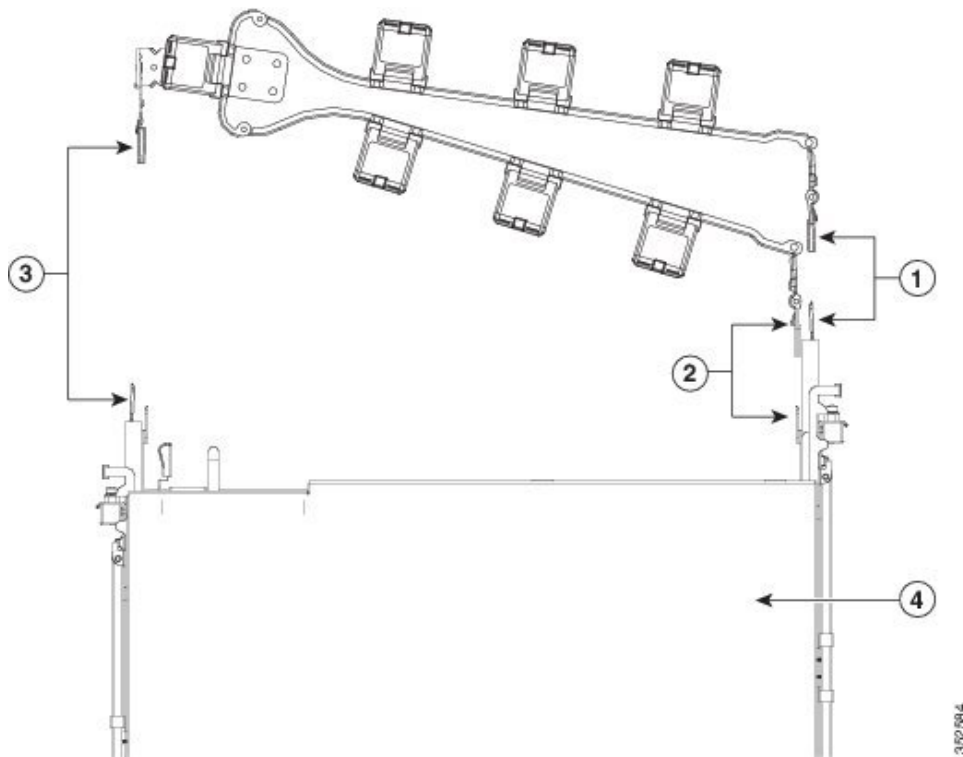
## ケーブル マネジメント アームの取り付け (任意)



(注) ケーブルマネジメントアーム (CMA) は、左右を逆にして取り付けることができます。CMA を逆に取り付けるには、取り付ける前に [ケーブル マネジメント アームを逆に取り付け \(任意\) \(8 ページ\)](#) を参照してください。

**ステップ 1** アプライアンスをラックに完全に押し込んだ状態で、アプライアンスから最も離れた CMA アームの CMA タブを、ラック支柱に装着された固定スライドレールの終端にスライドさせます。カチッと音がしてロックされるまで、タブをレールの終端にスライドさせます。

図 4: スライドレール後端への CMA の取り付け



ケーブル マネジメント アームを逆に取り付け（任意）

1	アプライアンスから最も離れたアームの CMA タブは、外側の固定スライドレールの終端に取り付けます。	3	幅調整スライダの CMA タブは、外側の固定スライドレールの終端に取り付けます。
2	アプライアンスに最も近いアームの CMA タブは、アプライアンスに装着された内側のスライドレールの終端に取り付けます。	4	アプライアンス背面

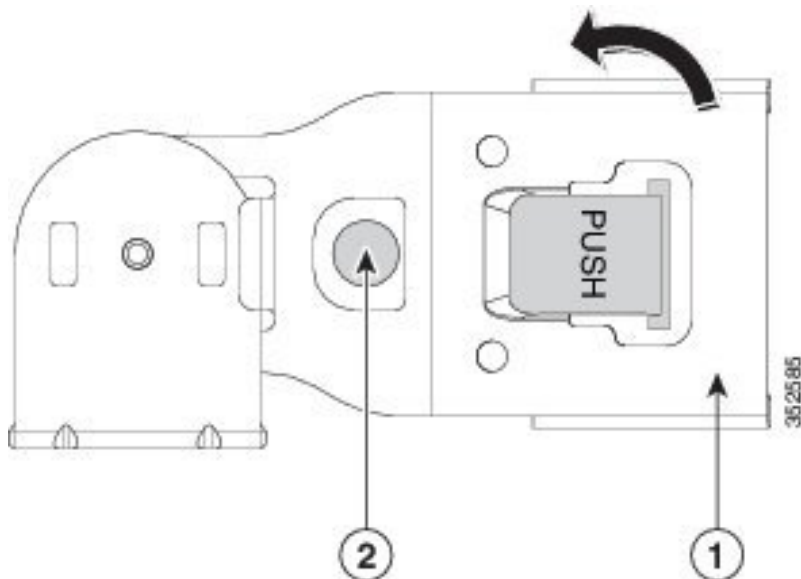
- ステップ 2** アプライアンスに最も近い CMA タブを、アプライアンスに装着された内側レールの終端にスライドさせます。カチッと音がしてロックされるまで、タブをレールの終端にスライドさせます。
- ステップ 3** CMA アセンブリの反対側の終端にある幅調整スライダを、ラックの幅まで引き出します。
- ステップ 4** 幅調整スライダの終端にある CMA タブを、ラック支柱に取り付けられている固定スライドレールの終端に押し込みます。カチッと音がしてロックされるまで、タブをレールの終端にスライドさせます。
- ステップ 5** 各プラスチック製ケーブルガイドの上部でヒンジ付きフラップを開き、必要に応じてケーブルガイドを通してケーブルを配線します。

## ケーブル マネジメント アームを逆に取り付け（任意）

- ステップ 1** CMA アセンブリ全体を、左から右へ 180 度回転させます。プラスチック製ケーブルガイドは、上を向いたままにしておく必要があります。
- ステップ 2** アプライアンスの背面を向くように、CMA アームの終端でタブを反転させます。
- ステップ 3** 幅調整スライダの終端にあるタブを回転させます。タブの外側の金属ボタンを長押しし、アプライアンスの背面を向くようにタブを 180 度回転させます。



図 5: CMA の反転



1	幅調整スライダの終端の CMA タブ	2	タブの外側の金属ボタン
---	--------------------	---	-------------

## 初期設定



(注) この項では、初期設定のためにシステムに接続する方法について説明します。

### アプライアンスのデフォルト設定

アプライアンスは次のデフォルト設定で出荷されます。

- NIC モードは *Shared LOM EXT* です。

Shared LOMEXT モードでは、1 Gb/10 Gb イーサネットポートおよび取り付け済みの Cisco 仮想インターフェイスカード (VIC) 上のすべてのポートが、Cisco Integrated Management Interface (Cisco IMC) にアクセスできます。10/100/1000 専用管理ポートを使用して Cisco IMC にアクセスする場合は、[Cisco IMC 設定ユーティリティを使用したシステムのセットアップ \(13 ページ\)](#) の説明に従い、アプライアンスに接続して NIC モードを変更できます。

- NIC の冗長性はアクティブ-アクティブです。すべてのイーサネットポートが同時に使用されます。
- DHCP は有効になっています。

- IPv4 は有効です。

### 接続方法

システムに接続して初期設定を行うには、次の2つの方法があります。

- ローカル設定：キーボードとモニターをシステムに直接接続して設定を行う場合は、この手順を使用します。この手順では、KVM ケーブル、またはアプライアンスの背面にあるポートを使用できます。
- リモート設定：専用管理 LAN 経由で設定を行う場合は、この手順を使用します。



- (注) システムをリモートで設定するには、システムと同じネットワーク上に DHCP サーバーが存在する必要があります。このサーバーノードの MAC アドレスの範囲を、DHCP サーバーにあらかじめ設定しておく必要があります。MAC アドレスは、前面パネルの引き抜きアセット タグにあるラベルに印字されています。このサーバー ノードでは、Cisco IMC に 6 つの MAC アドレスの範囲が割り当てられています。ラベルに印字されている MAC アドレスは、6 つの連続 MAC アドレスのうち最初のもので。

## 設定時のアプライアンスへのローカル接続

この手順には、次の機器が必要です。

- VGA モニタ
- USB キーボード
- サポートされている Cisco KVM ケーブル、または USB ケーブルと VGA DB-15 ケーブル

**ステップ 1** 電源コードをアプライアンスの各電源装置に接続し、次に、接地された電源コンセントに各コードを接続します。

初回のブートアップ時には、アプライアンスが起動してスタンバイ電源モードになるまでに約 2 分かかります。システムの電源ステータスは、前面パネルのシステムの電源ステータス LED で確認できます。LED がオレンジの場合、サーバーはスタンバイ電源モードです。

**ステップ 2** 次のいずれかの方法を使用して、USB キーボードと VGA モニターをアプライアンスに接続します。

- オプションの KVM ケーブルを前面パネルの KVM コネクタに接続します。USB キーボードと VGA モニタを KVM ケーブルに接続します。
- USB キーボードと VGA モニタを背面パネルの対応するコネクタに接続します。

**ステップ3** Cisco IMC 設定ユーティリティを開きます。

- a) 前面パネルの電源ボタンを 4 秒間長押しして、アプライアンスを起動します。
- b) ブートアップ時に、Cisco IMC 設定ユーティリティを開くよう求められたら **F8** を押します。

(注) Cisco IMC 設定ユーティリティを初めて開始すると、デフォルトのパスワードの変更を要求するプロンプトが表示されます。デフォルトパスワードは *password* です。強力なパスワード機能が有効になっています。

強力なパスワードの要件は、次のとおりです。

- パスワードは最小 8 文字、最大 14 文字とすること。
- パスワードにユーザー名を含めないこと。
- パスワードには次の 4 つのカテゴリの中から 3 つに該当する文字を含めること。
  - 大文字の英字 (A ~ Z)
  - 小文字の英字 (a ~ z)
  - 10 進数の数字 (0 ~ 9)
  - 非アルファベット文字 (!, @, #, \$, %, ^, &, \*, -, \_, =, ")。

**ステップ4** Cisco IMC 設定ユーティリティを使用したシステムのセットアップ (13 ページ) に進みます。

## 設定時のアプライアンスへのリモート接続

この手順には、次の機器が必要です。

- 管理 LAN に接続された RJ-45 イーサネット ケーブル X 1。

始める前に



(注) システムをリモートで設定するには、システムと同じネットワーク上に DHCP サーバーが存在する必要があります。このサーバー ノードの MAC アドレスの範囲を、DHCP サーバーにあらかじめ設定しておく必要があります。MAC アドレスは、前面パネルの引き抜きアセット タグにあるラベルに印字されています。このサーバー ノードでは、Cisco IMC に 6 つの MAC アドレスの範囲が割り当てられています。ラベルに印字されている MAC アドレスは、6 つの連続 MAC アドレスのうち最初のものです。

**ステップ1** 電源コードをアプライアンスの各電源装置に接続し、次に、接地された電源コンセントに各コードを接続します。

初回のブートアップ時には、アプライアンスが起動してスタンバイ電源モードになるまでに約2分かかります。システムの電源ステータスは、前面パネルのシステムの電源ステータスLEDで確認できます。LEDがオレンジの場合、サーバーはスタンバイ電源モードです。

**ステップ2** 管理イーサネット ケーブルを背面パネルの専用管理ポートに差し込みます。

**ステップ3** 事前設定された DHCP サーバーで、サーバー ノードに IP アドレスを割り当てられるようにします。

**ステップ4** 割り当てられた IP アドレスを使用して、サーバー ノードの Cisco IMC にアクセスし、ログインします。

(注) サーバのデフォルトのユーザ名は *admin* です。デフォルト パスワードは *password* です。

**ステップ5** Cisco IMC サーバーの [Summary] ウィンドウで、[Launch KVM Console] をクリックします。

別の KVM コンソール ウィンドウが開きます。

**ステップ6** Cisco IMC の [Summary] ウィンドウで、[Power Cycle Server] をクリックします。

システムがリブートします。

**ステップ7** KVM コンソール ウィンドウを選択します。

(注) 次のキーボード操作を有効にするには、KVM コンソール ウィンドウがアクティブ ウィンドウである必要があります。

**ステップ8** 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。

(注) Cisco IMC 設定ユーティリティを初めて開くと、デフォルトのパスワードの変更を要求するプロンプトが表示されます。デフォルトパスワードは *password* です。強力なパスワード機能が有効になっています。

強力なパスワードの要件は、次のとおりです。

- パスワードは最小 8 文字、最大 14 文字とすること。
- パスワードにユーザー名を含めないこと。
- パスワードには次の 4 つのカテゴリの中から 3 つに該当する文字を含めること。
  - 大文字の英字 (A ~ Z)
  - 小文字の英字 (a ~ z)
  - 10 進数の数字 (0 ~ 9)
  - 非アルファベット文字 (!, @, #, \$, %, ^, &, \*, -, \_, =, ")。

**ステップ9** Cisco IMC 設定ユーティリティを使用したシステムのセットアップ (13 ページ) に進みます。

# Cisco IMC 設定ユーティリティを使用したシステムのセットアップ

## 始める前に

システムに接続して Cisco IMC 設定ユーティリティを開いた後に、次の手順を実行します。



- (注) Cisco ISE ダウンロードサイトから入手した Cisco IMC ファームウェアのバージョン (SNS ハードウェアアプライアンスでの使用が認定されたバージョン) を使用する必要があります。UCS 用の Cisco IMC のバージョンには互換性がありません。Cisco IMC の新しいバージョンは、UCS 用に作成後、SNS ハードウェアアプライアンス用に作成されています。

**ステップ 1** NIC モードを設定して、サーバー管理用の Cisco IMC へのアクセスに使用するポートを選択します。

- [Shared LOMEXT] (デフォルト) : これは、工場出荷時設定の共有 LOM 拡張モードです。このモードでは、Shared LOM インターフェイスと Cisco Card インターフェイスの両方が有効です。このオプションを選択した場合は、次のステップで、NIC 冗長性設定にデフォルトの [アクティブ-アクティブ (Active-Active)] を選択する必要があります。
- [Shared LOM] : Cisco IMC へのアクセスに 1 Gb/10 Gb イーサネットポートを使用します。このオプションを選択した場合は、次のステップで、NIC 冗長性設定に [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)] を選択する必要があります。
- [Dedicated] : Cisco IMC へのアクセスに専用管理ポートを使用します。このオプションを選択した場合は、次のステップで、NIC 冗長性設定に [なし (None)] を選択する必要があります。
- [Cisco Card] : Cisco IMC へのアクセスに仮想インターフェイスカード (VIC) のポートを使用します。このオプションを選択した場合は、次のステップで、NIC 冗長性設定に [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)] を選択する必要があります。
- [VIC Slot] : Cisco Card NIC モードを使用する場合にのみ、VIC を取り付けた場所に合わせて、この設定を選択する必要があります。ライザー 1、ライザー 2、または Flex-LOM (mLOM スロット) を選択できます。
  - [Riser1] を選択した場合は、スロット 1 に VIC を取り付ける必要があります。
  - [Riser2] を選択した場合は、スロット 2 に VIC を取り付ける必要があります。
  - [Flex-LOM] を選択した場合は、mLOM スロットに mLOM タイプの VIC を取り付ける必要があります。

**ステップ 2** NIC 冗長性について、次のいずれかのオプションを選択します。

- [None] : イーサネットポートは個別に動作し、問題が発生した場合にフェールオーバーを行いません。この設定は、専用 NIC モードでのみ使用できます。
- [Active-standby] : アクティブなイーサネットポートに障害が発生した場合、スタンバイポートにトラフィックがフェールオーバーします。共有 LOM モードと Cisco カードモードでは、[アクティブ-スタンバイ (Active-standby)] または [アクティブ-アクティブ (Active-active)] の設定を使用できます。
- [Active-active] (デフォルト) : すべてのイーサネットポートが同時に使用されます。共有 LOM 拡張モードを選択した場合は、この NIC 冗長性設定のみを使用する必要があります。共有 LOM モードと Cisco カードモードでは、[アクティブ-スタンバイ (Active-standby)] または [アクティブ-アクティブ (Active-active)] の設定を使用できます。

**ステップ 3** ダイナミック ネットワーク設定用に DHCP をイネーブルにするか、スタティック ネットワーク設定を開始するかを選択します。

(注) DHCP をイネーブルにするには、DHCP サーバーにこのサーバーの MAC アドレスの範囲をあらかじめ設定しておく必要があります。MAC アドレスはサーバ背面のラベルに印字されています。このサーバでは、Cisco IMC に 6 つの MAC アドレスの範囲が割り当てられています。ラベルに印字されている MAC アドレスは、6 つの連続 MAC アドレスのうち最初のものです。

スタティック IPv4 および IPv6 設定には次が含まれます。

- [Cisco IMC IP address] : IPv6 の場合、有効な値は 1 ~ 127 です。
- [Gateway] : IPv6 の場合、ゲートウェイが不明な場合は、:: (コロン 2 つ) を入力して none として設定できます。
- [Preferred DNS Server Address] : IPv6 の場合、:: (コロン 2 つ) を入力して none として設定できます。

**ステップ 4** (任意) VLAN の設定を構成します。

**ステップ 5** (任意) サーバーのホスト名を設定します。

**ステップ 6** (任意) ダイナミック DNS をイネーブルにし、ダイナミック DNS (DDNS) ドメインを設定します。

**ステップ 7** (任意) [ファクトリデフォルト (Factory Default)] チェックボックスをオンにすると、サーバーは出荷時の初期状態に戻ります。

**ステップ 8** (任意) デフォルトのユーザー パスワードを設定します。

(注) サーバーのデフォルトのユーザー名は *admin* です。デフォルトパスワードは *password* です。

**ステップ 9** (任意) ポート設定の自動ネゴシエーションをイネーブルにするか、ポート速度およびデュプレックスモードを手動で設定します。

(注) 自動ネゴシエーションは専用 NIC モードを使用する場合にのみ使用できます。自動ネゴシエーションはサーバーが接続されているスイッチポートに基づいて自動的にポート速度およびデュプレックスモードを設定します。自動ネゴシエーションをディセーブルにした場合、ポート速度およびデュプレックスモードを手動で設定する必要があります。

**ステップ 10** (任意) ポートプロファイルとポート名をリセットします。

**ステップ 11** F5 を押して、行った設定に更新します。新しい設定が表示され、メッセージ「Network settings configured」が表示されるまでに約 45 秒かかる場合があります。その後、次の手順でサーバーを再起動します。

**ステップ 12** F10 を押して設定を保存し、サーバーを再起動します。

(注) DHCP のイネーブル化を選択した場合、動的に割り当てられた IP アドレスと MAC アドレスがブートアップ時にコンソール画面に表示されます。

## BIOS および Cisco IMC のファームウェアの更新



**注意** BIOS ファームウェアをアップグレードする場合、Cisco IMC ファームウェアも対応するバージョンにアップグレードする必要があります。アップグレードしないと、サーバーが起動しません。

シスコは、BIOS、Cisco IMC、およびその他のファームウェアを互換性のあるレベルに同時にアップグレードできるよう支援するために、*Cisco Host Upgrade Utility* を提供しています。

サーバーには、シスコが提供し、承認しているファームウェアが使用されています。シスコは、各ファームウェアイメージと共にリリース ノートを提供しています。

Cisco IMC の GUI または CLI インターフェイスを使用して Cisco IMC ファームウェアと BIOS ファームウェアをアップグレードできます。

## システム BIOS へのアクセス

**ステップ 1** ブート中にメッセージが表示されたら、F2 キーを押して BIOS セットアップユーティリティに切り替えます。

(注) このユーティリティの [Main] ページに、現在の BIOS のバージョンとビルドが表示されます。

**ステップ 2** 矢印キーを使って、BIOS メニュー ページを選択します。

**ステップ 3** 矢印キーを使って、変更するフィールドを反転表示にします。

**ステップ 4** Enter キーを押して変更するフィールドを選択し、そのフィールドの値を変更します。

**ステップ 5** Exit メニュー画面が表示されるまで右矢印キーを押します。

**ステップ 6** Exit メニュー画面の指示に従って変更内容を保存し、セットアップユーティリティを終了します（または、F10 を押します）。Esc キーを押すと、変更内容を保存せずにユーティリティを終了できます。

## スマート アクセス (シリアル)

このサーバーは、スマート アクセス (シリアル) 機能をサポートしています。この機能により、ホストのシリアルと Cisco IMC CLI を切り替えることができます。

- この機能には、次の要件があります。
  - サーバーの背面パネルの RJ-45 シリアルコネクタ、または前面パネルの KVM コンソールコネクタで DB-9 接続 (KVM ケーブルを使用する場合) を使用できるシリアルケーブル接続。
  - サーバーの BIOS でコンソール リダイレクションを有効にする必要があります。
  - 端末タイプは、VT100+ または VTUFT8 に設定する必要があります。
  - Serial over LAN (SOL) を無効にする必要があります。
- ホストのシリアルから Cisco IMC CLI に切り替えるには、Esc キーを押した状態で 9 キーを押します。  
接続を認証するために Cisco IMC クレデンシャルを入力する必要があります。
- Cisco IMC CLI からホストのシリアルに切り替えるには、Esc キーを押した状態で 8 キーを押します。



(注) Serial over LAN (SoL) 機能が有効になっている場合は、Cisco IMC CLI に切り替えることができません。

- セッションが作成されると、CLI または Web GUI に `serial` という名前が表示されます。

## HDD/SSD 交換後の RAID コントローラの設定

HDD または SSD の交換後に RAID コントローラカードを設定する場合は、次の手順を実行します。

**ステップ 1** 既存の HDD または SSD の交換 :

- a) Cisco SNS 3700 シリーズ アプライアンスにログインします。
- b) 左上隅にある [Menu] アイコンをクリックします。
- c) [Storage] > [Cisco RAID Controller] > [Controller Info] の順に選択します。
- d) [Clear Boot Drive] をクリックします。
- e) [OK] をクリックして、ブートドライブをクリアします。
- f) [Virtual Drive Info] をクリックします。



- g) [Virtual Drives] ウィンドウで仮想ドライブを選択し、[Delete Virtual Drive] をクリックします。
- h) [Physical Drive Info] をクリックします。
- i) [Physical Drives] ウィンドウで物理ドライブを選択し、[Prepare for Removal] をクリックします。

(注) ドライブを削除すると、Cisco ISE がアンインストールされます。HDD または SSD を交換したら、Cisco ISE を再インストールする必要があります。

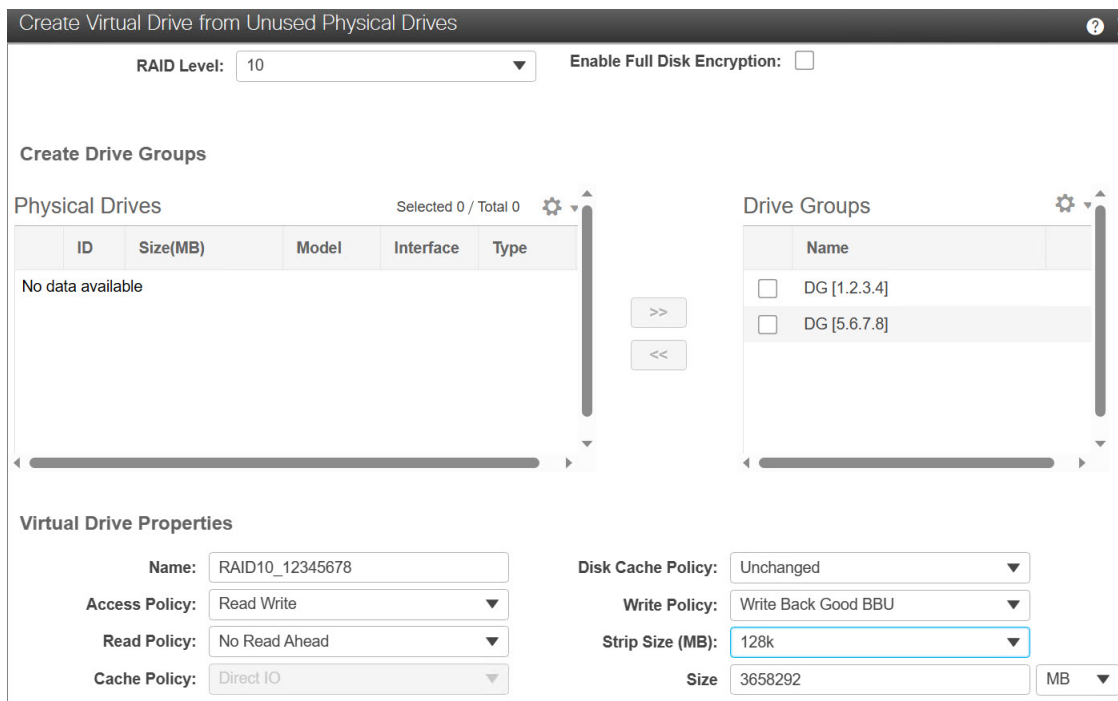
**ステップ2 RAID コントローラの設定 :**

- a) Cisco SNS 3700 シリーズ アプライアンスにログインします。
- b) 左上隅にある [Menu] アイコンをクリックします。
- c) [Storage] > [Cisco RAID Controller] > [Controller Info] の順に選択します。
- d) [Create Virtual Drive from Unused Physical Drives] をクリックします。

(注) ドライブを挿入すると、Just a Bunch Of Disks (JBOD) モードでドライブが構成されているように表示される場合があります。ドライブを仮想ディスクに追加する前に、ドライブ構成を解除する必要があります。

- e) [RAID Level] ドロップダウンリストから、SNS 3755 および SNS 3795 の場合は [RAID 10] を選択し、SNS 3715 の場合は [RAID 0] を選択します。
- f) [Create Drive Groups] セクションでグループ化するドライブを選択し、選択したドライブを [Drive Groups] ペインに移動します。要件に基づいてさまざまなグループを作成できます。
- g) [Virtual Drive Properties] セクションの [Write Policy] ドロップダウンリストで、[Write Back Good BBU] を選択します。

**図 6 : Virtual Drive Properties**



- h) [OK] をクリックします。  
[Virtual Drive Info] タブで、RAID 構成が成功したかどうかを確認できます。
- i) 新しく交換した HDD または SSD に Cisco ISE をインストールします。

詳細については、[Cisco UCS Server Configuration Utility ユーザーガイド \[英語\]](#) の「Configuring RAID Levels」の章を参照してください。

## SED のドライブセキュリティの有効化

SED のローカルキー管理やリモートキー管理を有効にできます。

### ローカルキー管理

SED のローカルキー管理を有効にするには、次の手順を実行します。

- ステップ 1 Cisco SNS 3700 シリーズ アプライアンスにログインします。
- ステップ 2 左上隅にある [Menu] アイコンをクリックします。
- ステップ 3 [Storage] > [Cisco 12G SAS RAID Controller] > [Controller Info] の順に選択します。
- ステップ 4 [Enable Drive Security] をクリックします。
- ステップ 5 [Local Key Management] オプションボタンをクリックします。
- ステップ 6 セキュリティ キーを入力します。
- ステップ 7 [Save] をクリックします。
- ステップ 8 [Virtual Drive Info] をクリックします。
- ステップ 9 [Virtual Drives] ウィンドウで仮想ドライブを選択し、[Secure Virtual Drive] をクリックします。

ドライブセキュリティが有効になっているドライブの [Virtual Drive Number] 列にロックアイコンが表示されます。

### リモート キー管理

SED のリモートキー管理を有効にするには、次の手順を実行します。

- ステップ 1 左上隅にある [Menu] アイコンをクリックします。
- ステップ 2 [Admin] > [Security Management] > [Secure Key Management] の順に選択します。
- ステップ 3 KPMI (暗号化ドライブのキー管理プロトコル) サーバーの詳細を入力します。
- ステップ 4 ルート CA 証明書、クライアント証明書、およびクライアント秘密キー証明書を割り当てます。

- ステップ 5 [Enable Secure Key Management] チェックボックスをオンにします。
- ステップ 6 [Storage] > [Cisco 12G SAS RAID Controller] > [Controller Info] の順に選択します。
- ステップ 7 [Enable Drive Security] をクリックします。
- ステップ 8 [Remote Key Management] オプションボタンをクリックします。
- ステップ 9 [Save] をクリックします。
- ステップ 10 [Virtual Drive Info] をクリックします。
- ステップ 11 [Virtual Drives] ウィンドウで仮想ドライブを選択し、[Secure Virtual Drive] をクリックします。

ドライブセキュリティが有効になっているドライブの [Virtual Drive Number] 列にロックアイコンが表示されます。

---



## 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。