



SIOC 管理

- [SIOC 管理 Cisco UCS Manager](#) (1 ページ)
- [SIOC の認識](#) (2 ページ)
- [PCIe サポートがある SIOC に移行する](#) (3 ページ)
- [CMC のリセット](#) (4 ページ)
- [CMC セキュア ブート](#) (5 ページ)

SIOC 管理 Cisco UCS Manager

Cisco UCS Manager を使用して Cisco UCS ドメイン 内のすべてのシステム I/O コントローラ (SIOC) を管理およびモニタできます。

SIOC の削除または交換

シャーシから SIOC の取り外しや交換ができます。SIOC の取り外しと交換はサービスに影響する操作であるため、シャーシ全体の電源をオフにする必要があります。

SIOC の取り外しのガイドライン

- アクティブな SIOC または両方の SIOC を取り外すには、シャーシ全体をシャットダウンして電源を切ります。完全に電源を切るためには、すべての電源コードを抜く必要があります。
- シャーシから SIOC を削除すると、シャーシ全体が Cisco UCS Manager から切断されます。

SIOC の取り外し

SIOC をシステムから取り外すには、次の手順を実行してください。

1. シャットダウンして、シャーシ全体の電源を切ります。完全に電源を切るためには、すべての電源コードを抜く必要があります。
2. SIOC をシステムに接続しているケーブルを取り外します。

3. システムから SIOC を取り外します。

SIOC の交換

SIOC をシステムから取り外し、別の SIOC に置き換えるには、次の手順を実行してください。

1. シャットダウンして、シャーシ全体の電源を切ります。完全に電源を切るためには、すべての電源コードを抜く必要があります。
2. SIOC をシステムに接続しているケーブルを取り外します。
3. システムから SIOC を取り外します。
4. 新しい SIOC をシステムに接続します。
5. ケーブルを SIOC に接続します。
6. 電源コードを接続し、システムの電源をオンにします。
7. 新しい SIOC を認識させます。

置き換えられた SIOC に接続されているサーバを再度検出します。



- (注) 置き換えられた SIOC のファームウェアのバージョンがピア SIOC と異なる場合、シャーシプロファイルの関連付けを再度トリガーして、置き換えられた SIOC のファームウェアを更新することが推奨されます。

SIOC の認識

Cisco UCS Manager にはシャーシの特定の SIOC を認識する機能もあります。シャーシの SIOC を交換したときには、次の手順を実行します。



- 注意** この操作では、SIOC とその接続先ファブリック インターコネクトとの間に、ネットワーク接続が再構築されます。この SIOC に対応するサーバは到達不能になり、トラフィックは中断されます。

手順の概要

1. UCS-A# **scope chassis chassis-num**
2. UCS-A /chassis # **acknowledge sioc {1 | 2}**
3. UCS-A /chassis* # **commit-buffer**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	UCS-A# scope chassis <i>chassis-num</i>	指定したシャーシでシャーシモードを開始します。
ステップ 2	UCS-A /chassis # acknowledge sioc {1 2}	シャーシで指定した SIOC を認識します。
ステップ 3	UCS-A /chassis* # commit-buffer	トランザクションをシステムの設定にコミットします。

例

次の例では、SIOC 1 を認識し、トランザクションをコミットします。

```
UCS-A# scope chassis 3
UCS-A /chassis # acknowledge sioc 1
UCS-A /chassis* # commit-buffer
UCS-A /chassis #
```

PCIe サポートがある SIOC に移行する

始める前に

Cisco UCS Manager がリリース 4.0(1a) 以上であることを確認してください。

手順の概要

1. シャーシとサーバのファームウェアを 4.0(1) リリースにアップデートします。
2. シャーシの稼働を中止します。
3. シャットダウンして、シャーシ全体の電源を切ります。完全に電源を切るためには、すべての電源コードを抜く必要があります。
4. SIOC をシステムに接続しているケーブルを取り外します。
5. システムから SIOC を取り外します。
6. 新しい SIOC をシステムに接続します。
7. ケーブルを SIOC に接続します。
8. 電源コードを接続し、システムの電源をオンにします。
9. 新しい SIOC を認識させます。

手順の詳細

ステップ 1 シャーシとサーバのファームウェアを 4.0(1) リリースにアップデートします。

ステップ 2 シャーシの稼働を中止します。

- ステップ3 シャットダウンして、シャーシ全体の電源を切ります。完全に電源を切るためには、すべての電源コードを抜く必要があります。
- ステップ4 SIOC をシステムに接続しているケーブルを取り外します。
- ステップ5 システムから SIOC を取り外します。
- ステップ6 新しい SIOC をシステムに接続します。
- ステップ7 ケーブルを SIOC に接続します。
- ステップ8 電源コードを接続し、システムの電源をオンにします。
- ステップ9 新しい SIOC を認識させます。

CMC のリセット

手順の概要

1. UCS-A# **scope chassis chassis-num**
2. UCS-A /chassis # **scope sioc {1 | 2}**
3. UCS-A /chassis/sioc # **scope cmc**
4. UCS-A /chassis/sioc/cmc # **reset**
5. UCS-A /chassis/sioc/cmc* # **commit-buffer**

手順の詳細

	コマンドまたはアクション	目的
ステップ1	UCS-A# scope chassis chassis-num	指定したシャーシでシャーシモードを開始します。
ステップ2	UCS-A /chassis # scope sioc {1 2}	シャーシで指定した SIOC を入力します。
ステップ3	UCS-A /chassis/sioc # scope cmc	選択した SIOC スロットの CMC を入力します。
ステップ4	UCS-A /chassis/sioc/cmc # reset	CMC をリセットします。
ステップ5	UCS-A /chassis/sioc/cmc* # commit-buffer	トランザクションをシステムの設定にコミットします。

例

次に、SIOC1のCMCをリセットし、トランザクションをコミットする例を示します。

```
UCS-A# scope chassis 1
UCS-A /chassis # scope sioc 1
UCS-A /chassis/sioc # scope cmc
UCS-A /chassis/sioc/cmc # reset
UCS-A /chassis/sioc/cmc* # commit-buffer
```

CMC セキュア ブート

Chassis Management Controller (CMC) のセキュア ブートにより、シスコの署名が付加されたファームウェア イメージのみインストールでき、CMC で実行できます。CMC が更新されると、イメージは、ファームウェアがフラッシュされる前に認証されます。認証に失敗すると、ファームウェアはフラッシュされません。これにより、CMC ファームウェアへの不正アクセスを防止します。

CMC セキュア ブートの注意事項と制約事項

- CMC セキュア ブートは、Cisco UCS S3260 シャーシ上でのみサポートされます。
- シャーシの関連付けの実行中、1 つの SIOC でセキュア ブートを有効にすると、操作は失敗します。
- CMC セキュア ブートを有効にした後で、無効にすることはできません。
- CMC セキュア ブートはそれが有効にされた SIOC に固有です。CMC セキュア ブートが有効になっている SIOC を置き換えると、[Secure boot operational state] フィールドには新しい SIOC のセキュア ブートのステータスが表示されます。
- CMC セキュア ブートがシャーシで有効にされると、そのシャーシをスタンドアロンモードに戻すことはできず、CMC のファームウェア イメージを Cisco IMC リリース 2.0(13) 以前にダウングレードできなくなります。
- [Secure boot operational state] フィールドには、セキュア ブートのステータスが表示されます。次のいずれかになります。
 - Disabled : CMC セキュア ブートが有効ではありません。これは、デフォルトの状態です。
 - Enabling : CMC セキュア ブートが有効化されています。
 - Enabled : CMC セキュア ブートが有効化されました。
- 4.0(1)以降では、**セキュア ブート動作状態**がデフォルトで **[Enabled]** の状態になっており、ユーザーは設定できません。オプションがグレー表示されます。

CMC セキュア ブートの有効化

Cisco UCS Manager リリース 3.1(2) には、Cisco が署名したファームウェア イメージのみをシャーシ管理コントローラ (CMC) にインストールして実行できるように、CMC のセキュア ブートを有効にするための機能が追加されています。

手順の概要

1. UCS-A# **scope chassis chassis-num**

2. UCS-A /chassis # **scope sioc** {1 | 2}
3. UCS-A /chassis/sioc # **scope cmc**
4. UCS-A /chassis/sioc/cmc # **enable secure-boot**
5. UCS-A /chassis/sioc/cmc* # **commit-buffer**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	UCS-A# scope chassis <i>chassis-num</i>	指定したシャーシでシャーシモードを開始します。
ステップ 2	UCS-A /chassis # scope sioc {1 2}	シャーシで指定した SIOC を入力します。
ステップ 3	UCS-A /chassis/sioc # scope cmc	選択した SIOC スロットの CMC を入力します。
ステップ 4	UCS-A /chassis/sioc/cmc # enable secure-boot	CMC セキュア ブートを有効にします。 セキュア ブートの状態が enabled のときにこのコマンドを実行すると、Cisco UCS Manager はエラーメッセージを表示して、操作は失敗します。 (注) この操作は、元に戻すことができません。 CMC セキュア ブートを無効にすることはできません。
ステップ 5	UCS-A /chassis/sioc/cmc* # commit-buffer	トランザクションをシステムの設定にコミットします。

例

次に、SIOC 1 上で CMC セキュア ブートを有効にし、トランザクションをコミットする例を示します。

```
UCS-A# scope chassis 1
UCS-A /chassis # scope sioc 1
UCS-A /chassis/sioc # scope cmc
UCS-A /chassis/sioc/cmc # enable secure-boot
Warning: This is an irreversible operation.
Do you want to proceed? [Y/N] Y
UCS-A /chassis/sioc/cmc* # commit-buffer
```