



# ロックダウンモード

## 概要

このセクションでは、ロックダウンモードの概要を説明します。ロックダウンモードは、ホストへのアクセス許可を制限することにより、ESXi ホストのセキュリティを強化するために使用されます。このモードを有効にすると、ESXi ホストには vCenter Server または Direct Console ユーザーインターフェイス (DCUI) からのみアクセスできます。ロックダウンモードの有効化は、どのユーザーがホスト サービスへのアクセスを認可されるかに影響します。



(注) ロックダウンモードを有効にする場合、`hxuser` アカウントを各 ESXi ホスト例外ユーザーリストに追加する必要があります。



(注) ロックダウンモードが有効になり、`root` または `administrator@vsphere.local`、またはその他のユーザーが例外ユーザーリストに含まれていない場合、これらのユーザーは ESX への SSH 接続が許可されません。同様に、何らかの理由によりホストが vCenter から削除された場合、vCenter にホストを再び追加することは許可されません。

表 1: ロックダウンモードの動作

サービス	通常モード	通常のロックダウンモード	厳密なロックダウンモード
vSphere Web サービス API	すべてのユーザー (権限に基づく)	vCenter (vpxuser) 例外にユーザーが含まれます (権限に基づく)。	vCenter (vpxuser) 例外にユーザーが含まれます (権限に基づく)。 vCloud Director (vsclouser、該当する場合)

サービス	通常モード	通常のロックダウンモード	厳密なロックダウンモード
CIM プロバイダ	ホスト上の管理者権限を持つユーザー。	vCenter (vpxuser) 例外にユーザーが含まれます (権限に基づく)。 vCloud Director (vslauser、該当する場合)	vCenter (vpxuser) 例外にユーザーが含まれます (権限に基づく)。 vCloud Director (vslauser、該当する場合)
Direct Console UI (DCUI)	ホスト上の管理者権限を持つユーザーおよび DCUI 内のユーザー。アクセスの詳細オプション。	DCUI アクセス詳細オプションで定義されたユーザー。 例外にホスト上の管理者権限を持つユーザーが含まれます。	DCUI サービスが停止します。
ESXi シェル (イネーブルな場合)	ホスト上の管理者権限を持つユーザー。	DCUI アクセス詳細オプションで定義されたユーザー。 例外にホスト上の管理者権限を持つユーザーが含まれます。	DCUI アクセス詳細オプションで定義されたユーザー。 例外にホスト上の管理者権限を持つユーザーが含まれます。
SSH (イネーブルな場合)	ホスト上の管理者権限を持つユーザー。	DCUI アクセス詳細オプションで定義されたユーザー。 例外にホスト上の管理者権限を持つユーザーが含まれます。	DCUI アクセス詳細オプションで定義されたユーザー。 例外にホスト上の管理者権限を持つユーザーが含まれます。

- [ロックダウンモードの有効化または無効化 \(2 ページ\)](#)
- [ロックダウンモードのトラブルシューティング \(3 ページ\)](#)

## ロックダウンモードの有効化または無効化

このセクションでは、DCUI から、または vSphere Web Client からロックダウンモードを有効または無効にする方法について説明します。



- (注) ロックダウンモードが有効になり、`root` または `administrator@vsphere.local`、またはその他のユーザーが例外ユーザーリストに含まれていない場合、これらのユーザーは ESX への SSH 接続が許可されません。同様に、何らかの理由によりホストが vCenter から削除された場合、vCenter にホストを再び追加することは許可されません。

## DCUI からのロックダウンモードの有効化または無効化 :

- ステップ 1 ESXi ホストに直接にログインします。
- ステップ 2 ホストで Direct Console ユーザー インターフェイス (DCUI) を開きます。
- ステップ 3 初期設定用の **F2** キーを押します。
- ステップ 4 [ロックダウンモードの設定 (Configure Lockdown Mode)] の設定を切り替えるには **Enter** を押します。
- ステップ 5 VSphere Web Client のインベントリでホストを特定します。

## vSphere Web Client からのロックダウンモードの有効化または無効化 :

- ステップ 1 VSphere Web Client のインベントリでホストを特定します。
- ステップ 2 [Manage] タブをクリックし、[Settings] をクリックします。
- ステップ 3 [System] で、[Security profile] を選択します。
- ステップ 4 [Lockdown Mode] パネルで、[Edit] をクリックします。
- ステップ 5 [例外ユーザー (Exception Users)] をクリックし、[+ ユーザーの追加 (+Add user)] を選択して、`hxuser` (すべて小文字) を追加します。
- ステップ 6 [ロックダウンモード (Lockdown Mode)] をクリックして、いずれかのロックダウンモードオプションを選択します。

## ロックダウンモードのトラブルシューティング

ロックダウンモードでエラーダイアログボックスが表示されたりソフトウェアのアップグレードが失敗したりする場合は、次のいずれかのシナリオに応じて以下の解決オプションを実行してください。

- 少なくとも 1 つのホストがロックダウンモードである。
- アップグレードの進行中にホストがロックダウンモードである。

少なくとも 1 つのホストがロックダウンモードである場合 :

1. アップグレード前の検証でホスト ロックダウン モードをチェックします。
2. 状態を検出し、エラーをスローしてクラスタのアップグレードを中止します。
3. ロックダウン モードを無効にして、アップグレードを再試行します。

アップグレードの進行中にホストがロックダウンモードである場合：

---

**ステップ 1** ホストをアップグレードする前に、ホスト ロックダウン モードをチェックします。

**ステップ 2** 状態を検出してエラーを送出し、アップグレードに失敗します。

**ステップ 3** ロックダウン モードを無効にして、アップグレードを再試行します。

---

## 展開フェーズでの vCenter へのホスト追加エラー

HX インストール中のロックダウンの検証は、「root」ユーザーを使用した ESXi ホストの SSH アクセシビリティチェックです。例外リストにルートユーザーを追加すると、ロックダウンモードの展開検証チェックがバイパスされます。この場合、展開フェーズで vCenter にホストが追加されると、そのホストは失敗し、HX のインストールも失敗します。

展開フェーズで vCenter にホストを追加すると失敗し、エラーメッセージ「**vCenter のホストを追加できません**」が表示されます。

---

ロックダウンモードのステータスを確認し、無効にして、「root」ユーザーを例外から削除します。

---

## 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。