

# SPARC M5-32 および SPARC M6-32 サー バー

セキュリティーガイド

---

Copyright © 2014 Oracle and/or its affiliates. All rights reserved.

このソフトウェアおよび関連ドキュメントの使用と開示は、ライセンス契約の制約条件に従うものとし、知的財産に関する法律により保護されています。ライセンス契約で明示的に許諾されている場合もしくは法律によって認められている場合を除き、形式、手段に関係なく、いかなる部分も使用、複写、複製、翻訳、放送、修正、ライセンス供与、送信、配布、発表、実行、公開または表示することはできません。このソフトウェアのリバース・エンジニアリング、逆アセンブル、逆コンパイルは互換性のために法律によって規定されている場合を除き、禁止されています。

ここに記載された情報は予告なしに変更される場合があります。また、誤りが無いことの保証はいたしかねます。誤りを見つけた場合は、オラクル社までご連絡ください。

このソフトウェアまたは関連ドキュメントを、米国政府機関もしくは米国政府機関に代わってこのソフトウェアまたは関連ドキュメントをライセンスされた者に提供する場合は、次の通知が適用されます。

#### U.S. GOVERNMENT END USERS:

Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

このソフトウェアもしくはハードウェアは様々な情報管理アプリケーションでの一般的な使用のために開発されたものです。このソフトウェアもしくはハードウェアは、危険が伴うアプリケーション(人的傷害を発生させる可能性があるアプリケーションを含む)への用途を目的として開発されていません。このソフトウェアもしくはハードウェアを危険が伴うアプリケーションで使用する際、安全に使用するために、適切な安全装置、バックアップ、冗長性(redundancy)、その他の対策を講じることは使用者の責任となります。このソフトウェアもしくはハードウェアを危険が伴うアプリケーションで使用したこと起因して損害が発生しても、オラクル社およびその関連会社は一切の責任を負いかねます。

OracleおよびJavaはOracle Corporationおよびその関連企業の登録商標です。その他の名称は、それぞれの所有者の商標または登録商標です。

Intel, Intel Xeonは、Intel Corporationの商標または登録商標です。すべてのSPARCの商標はライセンスをもとに使用し、SPARC International, Inc.の商標または登録商標です。AMD, Opteron, AMDロゴ, AMD Opteronロゴは、Advanced Micro Devices, Inc.の商標または登録商標です。UNIXは、The Open Groupの登録商標です。

このソフトウェアまたはハードウェア、そしてドキュメントは、第三者のコンテンツ、製品、サービスへのアクセス、あるいはそれらに関する情報を提供することがあります。オラクル社およびその関連会社は、第三者のコンテンツ、製品、サービスに関して一切の責任を負わず、いかなる保証もいたしません。オラクル社およびその関連会社は、第三者のコンテンツ、製品、サービスへのアクセスまたは使用によって損失、費用、あるいは損害が発生しても一切の責任を負いかねます。

---

# 目次

---

|  |   |
|--|---|
| 1. ハードウェアのセキュリティーについて .....                      | 5 |
| アクセス制限 .....                                     | 5 |
| シリアル番号 .....                                     | 6 |
| ハードドライブ .....                                    | 6 |
| 2. ソフトウェアのセキュリティーについて .....                      | 7 |
| ▼ 不正アクセスを防止する (Oracle Solaris OS) .....          | 7 |
| ▼ 不正アクセスを防止する (Oracle ILOM) .....                | 7 |
| ▼ 不正アクセスを防止する (Oracle VM Server for SPARC) ..... | 8 |
| アクセスの制限 (OpenBoot) .....                         | 8 |
| ▼ パスワード保護を実装する (OpenBoot) .....                  | 8 |
| ▼ 失敗したログインのチェック (OpenBoot) .....                 | 8 |
| ▼ 電源投入バナーを提供する (OpenBoot) .....                  | 9 |
| Oracle システムファームウェア .....                         | 9 |
| WAN ブートをセキュリティー保護する .....                        | 9 |



---

# 1

・・・ 第 1 章

## ハードウェアのセキュリティーについて

---

物理的な分離とアクセス制御は、セキュリティーアーキテクチャーを構築するための基盤です。物理サーバーを確実にセキュアな環境に設置することで、不正アクセスから保護します。同様に、すべてのシリアル番号を記録すると、盗難、転売、またはサプライチェーンの危険（つまり、偽造されたり危険にさらされたりしたコンポーネントが組織のサプライチェーンに流入されること）を防止するために役立ちます。

この章では、SPARC M5-32 および M6-32 サーバーのハードウェアの一般的なセキュリティーガイドラインについて説明します。

この章は、次のセクションで構成されています。

- [5 ページの「アクセス制限」](#)
- [6 ページの「シリアル番号」](#)
- [6 ページの「ハードドライブ」](#)

### アクセス制限

- サーバーと関連装置は、アクセスが制限された鍵の掛かった部屋に設置してください。
- 鍵付きのドアがあるラックに装置を設置する場合は、ラック内のコンポーネントの保守を行うとき以外はラックのドアに常に鍵を掛けておいてください。ドアに鍵を掛けることで、ホットプラグまたはホットスワップデバイスへのアクセスも制限されます。
- 予備の現場交換可能ユニット (FRU) または顧客交換可能ユニット (CRU) は、鍵の掛かったキャビネットに保管してください。鍵の掛かったキャビネットへのアクセスは承認された担当者に制限してください。
- ラックと予備のキャビネットの鍵のステータスと整合性を定期的に検証して、改ざんやドアの鍵が掛かっていないままなることを防止または検出します。
- キャビネットの鍵はアクセスが制限されたセキュアな場所に保管します。
- USB コンソールへのアクセスを制限します。システムコントローラ、配電盤 (PDU)、ネットワークスイッチなどのデバイスは、USB 接続が可能です。物理アクセスは、ネットワークベースの攻撃の影響を受けないため、よりセキュアにコンポーネントにアクセスできます。
- コンソールを外付けの KVM に接続して、リモートコンソールアクセスを有効にします。KVM デバイスでは多くの場合、ツーフアクタ認証、集中管理されたアクセス制御、および監査がサポート

されます。KVM のセキュリティーガイドラインとベストプラクティスの詳細は、KVM デバイスに付属のドキュメントを参照してください。

## シリアル番号

- すべてのハードウェアのシリアル番号を記録しておいてください。
- すべての主要なコンピュータハードウェア項目 (交換部品など) にセキュリティーのマークを付けます。専用の紫外線ペンまたはエンボスラベルを使用してください。
- ハードウェアのアクティベーションキーとライセンスは、緊急時にシステムマネージャーが簡単に取り出せるセキュアな場所に保管しておいてください。これらの印刷ドキュメントは、所有権を示す唯一の証明になります。

無線 RFID リーダーによってアセットの追跡がさらに容易になります。詳細は、次の場所にある RFID を使用して Oracle Sun システムのアセットを追跡する方法を参照してください。

<http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf>

## ハードドライブ

ハードドライブは多くの場合、機密情報を格納するために使用されます。この情報が不正に開示されないよう保護するため、ハードドライブを再利用、廃止、または廃棄する前にサニタイズする必要があります。

- Oracle Solaris の **format** (1M) コマンドなどのディスク抹消ツールを使用して、すべてのデータをディスクドライブから完全に消去します。または、該当し使用可能な場合は、物理消磁ツールを使用できます。
- ハードドライブに格納されている情報の機密性が高いと、粉碎や焼却などのハードドライブの物理的な廃棄が唯一の適切なサニタイズ方法である場合があります。

組織は、データ保護ポリシーを参照して、ハードドライブをサニタイズするために最適な方法を判別することをお勧めします。



### 注意

ディスク抹消ソフトウェアは、最新のハードドライブ (特に SSD) では、そのデータアクセスの管理方法のために一部のデータを削除できないことがあります。

---

---

## ・・・ 第 2 章

# ソフトウェアのセキュリティについて

---

ほとんどのハードウェアセキュリティは、ソフトウェア手段を通じて実装されます。この章では、SPARC M5-32 および SPARC M6-32 サーバーの一般的なソフトウェアセキュリティガイドラインについて説明します。

この章は、次のセクションで構成されています。

- ・ 7 ページの「不正アクセスを防止する (Oracle Solaris OS)」
- ・ 7 ページの「不正アクセスを防止する (Oracle ILOM)」
- ・ 8 ページの「不正アクセスを防止する (Oracle VM Server for SPARC)」
- ・ 8 ページの「アクセスの制限 (OpenBoot)」
- ・ 9 ページの「Oracle システムファームウェア」
- ・ 9 ページの「WAN ブートをセキュリティ保護する」

### ▼ 不正アクセスを防止する (Oracle Solaris OS)

- ・ Oracle Solaris OS コマンドを使用して、Oracle Solaris ソフトウェアへのアクセスの制限、OS の強化、セキュリティ機能の使用、およびアプリケーションの保護を行います。使用している OS バージョンの Oracle Solaris セキュリティガイドラインのドキュメントについては、次の場所で入手できます。  
<http://www.oracle.com/goto/Solaris11/docs>  
<http://www.oracle.com/goto/Solaris10/docs>

### ▼ 不正アクセスを防止する (Oracle ILOM)

1. Oracle ILOM コマンドを使用して、Oracle ILOM ソフトウェアへのユーザーアクセスの制限、出荷時に設定されたパスワードの変更、root スーパーユーザーアカウントの使用の制限、およびサービスプロセッサへのプライベートネットワークのセキュリティ保護を行います。『Oracle ILOM セキュリティガイド』は次の場所で入手できます。  
<http://www.oracle.com/goto/ILOM/docs>
2. 個々のドメインをセキュリティ保護するには、プラットフォーム固有の Oracle ILOM コマンドを使用して、特定の物理ドメインに適用される役割でユーザーアカウントを作成します。ユーザーの役割を物理ドメインに割り当てた場合、そのドメインの機能にはプラットフォームで割り当てられたユーザーの役割の機能が反映されますが、特定のコンポーネントに対して実行されるコマンドに制限されます。



## 注記

個々の物理ドメインで割り当てることができるのは、管理者 (**a**)、コンソール (**c**)、およびリセット (**r**) のユーザーの役割だけです。

『SPARC M5-32 and SPARC M6-32 サーバー管理ガイド』は次の場所で入手できます。  
<http://www.oracle.com/goto/M6-32/docs>

## ▼ 不正アクセスを防止する (Oracle VM Server for SPARC)

- Oracle VM for SPARC コマンドを使用して、Oracle VM for SPARC ソフトウェアへのアクセスを制限します。  
『Oracle VM for SPARC セキュリティーガイド』は次の場所で入手できます。  
<http://www.oracle.com/goto/VM-SPARC/docs>

## アクセスの制限 (OpenBoot)

これらのトピックでは、OpenBoot プロンプトでアクセスを制限する方法について説明します。

- [8 ページの「パスワード保護を実装する \(OpenBoot\)」](#)
- [8 ページの「失敗したログインのチェック \(OpenBoot\)」](#)
- [9 ページの「電源投入バナーを提供する \(OpenBoot\)」](#)

### 関連情報

- OpenBoot のセキュリティ変数の設定については、*OpenBoot 4.x コマンドのリファレンスマニュアル* (<http://download.oracle.com/docs/cd/E19455-01/816-1177-10/cfg-var.html#pgfId-17069>) を参照してください。

## ▼ パスワード保護を実装する (OpenBoot)

- `security-mode` パラメータを **full** または **command** のいずれかに設定します。  
**full** に設定すると、ブートなどの通常の操作を含むどのアクションの実行にもパスワードが必要になります。**command** に設定すると、**boot** または **go** コマンドにはパスワードは必要ありませんが、その他すべてのコマンドでパスワードが必要になります。事業継続のため、次の例に示すように `security-mode` パラメータを `command` に設定します。

```
ok password
ok setenv security-mode command
ok password
```

## ▼ 失敗したログインのチェック (OpenBoot)

- 次の例に示すように、`security-#badlogins` パラメータを使用して、ユーザーが OpenBoot 環境にアクセスしようとして失敗したかどうかを判別します。

```
ok printenv security-#badlogins
```



---

このコマンドがゼロより大きい値を返す場合、OpenBoot 環境にアクセスしようとして失敗したことが記録されています。

2. 次のコマンドを入力して、**security-#badlogins** パラメータをリセットします。

```
ok setenv security-#badlogins 0
```

## ▼ 電源投入バナーを提供する (OpenBoot)

- 次のコマンドを使用して、カスタムの警告メッセージを有効にします。

```
ok setenv oem-banner banner-message
ok setenv oem-banner? true
```

## Oracle システムファームウェア

Oracle システムファームウェアでは、制御された更新プロセスを使用して、無許可の変更を防止しています。スーパーユーザーまたは適切な権限を持つ認証済みユーザーのみが、更新プロセスを使用できます。

最新の更新またはパッチの取得については、サーバーのプロダクトノートを参照してください。

## WAN ブートをセキュリティー保護する

WAN ブートでは、さまざまなレベルのセキュリティーがサポートされています。WAN ブートでサポートされているセキュリティー機能を組み合わせて使用することで、ネットワークのニーズに対応できます。よりセキュアな構成では追加の管理が必要ですが、システムデータの保護がさらに強化されます。

- Oracle Solaris 10 OS の場合、『*Oracle Solaris インストールガイド (ネットワークベースのインストール)*』の「セキュアな WAN ブートインストール構成」を参照してください。

<http://www.oracle.com/goto/Solaris10/docs>

- Oracle Solaris 11 OS の場合、『*Oracle Solaris 11.1 でのネットワークのセキュリティー保護*』を参照してください。

<http://www.oracle.com/goto/Solaris11/docs>

---