SPARC M8 および SPARC M7 サーバーセキュリティーガイド

Part No: E63776-02
2017 年 9 月

ORACLE

Part No: E63776-02

ドキュメントのアクセシビリティについて

オラクルのアクセシビリティについての詳細情報は、Oracle Accessibility ProgramのWeb サイト(http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc)を参照してください。

Oracle Supportへのアクセス

サポートをご契約のお客様には、My Oracle Supportを通して電子支援サービスを提供しています。詳細情報は(http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info) か、聴覚に障害のあるお客様は (http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs)を参照してください。

目次

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、不正アクセスからサーバーを保護します。同様に、すべてのシリアル番号を記録しておくと、ハードウェアコンポーネントの未承認の使用の防止に役立ちます。

これらのセクションでは、それらの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。

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。
- 予備の交換部品はすべて、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、承認された人だけ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状態にならないよう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、ツーファクタ認証、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

コンポーネントを受領しインベントリに加えるときにすべてのシリアル番号を慎重に記録することで、ハードウェアコンポーネントの未承認の使用を防止します。すべてのコンポーネントを取り付けたり使用したりする前に、そのシリアル番号をコンポーネントの受領時に記録した番号と比較して信頼性を確認してください。ハードウェアをセキュリティー保護するには次の対策に従ってください。

- 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、システム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。

ワイヤレスの無線周波数識別 (Radio Frequency Identification、RFID) リーダーを使用すると、より簡単にアセットを追跡できます。『*RFID* を使用した *Oracle Sun* システムアセットの追跡方法』に関する Oracle のホワイトペーパー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 (ハードディスクドライブおよびソリッドステートドライブ) 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してください。

- 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。
- 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ライズするために最適な方法を判別してください。
- 必要に応じて、Oracle の Customer Data and Device Retention サービスを利用してください。

  `http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf`

ソフトウェアのセキュリティーについて

ハードウェアのほとんどのセキュリティーは、ソフトウェアを通じて実装されます。これらのセクションでは、それらのサーバーのソフト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。

▼ 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、セキュリティー機能の使用、およびアプリケーションの保護を実行します。**

  使用しているバージョンの『*Oracle Solaris* セキュリティーガイドライン』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ー保護を実行します。**

   『*Oracle ILOM* 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/ilom/docs`

2. **可能な場合は、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することにより、プラットフォーム固有の Oracle ILOM コマンドを使用して、個々のドメインをセキュリティー保護します。**
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 M8* および *SPARC M7* サーバー管理ガイド』は次の場所で入手できます。
`http://docs.oracle.com/cd/E55211_01/`

▼ 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 `http://www.oracle.com/goto/vm-sparc/docs` で入手できます。

アクセスの制限 (OBP)

これらのトピックでは、OBP 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。

- 10 ページの「パスワード保護を実装する」
- 11 ページの「セキュリティーモードを有効にする」
- 12 ページの「セキュリティーモードを無効にする」
- 12 ページの「失敗したログインを確認する (OBP)」
- 12 ページの「電源投入バナーを使用する」

OpenBoot のセキュリティー変数の設定についての詳細は、次の場所で公開されている OpenBoot のドキュメントを参照してください。

`http://www.oracle.com/goto/openboot/docs`

▼ パスワード保護を実装する

- **パスワードをまだ設定していない場合は、次の手順を実行します。**

```
{0} ok password
New password (8 characters max):
Retype new password: password
```

パスワードには 1-8 文字を使用できます。9 文字以上を入力した場合、最初の 8 文字だけが使用されます。出力可能な文字がすべて受け入れられます。制御文字は受け入れられません。

注記 - パスワードをゼロ文字に設定すると、セキュリティーはオフになり、security-mode パラメータは none に設定された場合と同じように扱われます。ただし、設定は変更されません。

▼ セキュリティーモードを有効にする

1. **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、boot 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 コマンドや go コマンドにはパスワードは必要ありませんが、その他のすべてのコマンドではパスワードが必要になります。ビジネス継続性の理由から、次の例に示すように security-mode パラメータを command に設定します。

   ```
   {0} ok setenv security-mode command
   {0} ok
   ```

2. **セキュリティーモードプロンプトを取得します。**

   上記のようにセキュリティーモードを設定したあと、2 つの方法のいずれかで、セキュリティーモードプロンプトを取得できます。

   - **logout および login コマンドを使用します。**

     ```
     {0} ok logout
     Type boot , go (continue), or login (command mode)
     >
     > login
     Firmware Password: password
     Type help for more information
     {0} ok
     ```

     セキュリティーモードを終了するには、logout および login 名を使用します。

   - **reset-all コマンドを使用します。**

     ```
     {0} ok reset-all
     ```

     このコマンドはシステムをリセットします。システムが再度稼働すると、OpenBoot はセキュリティーモードプロンプトになります。コマンドプロンプトに

再度ログイン (またはセキュリティーモードからログアウト) するには、上記のように `logout` 名と `login` 名を使用し、パスワードを入力します。

▼ セキュリティーモードを無効にする

1. **`security-mode` パラメータを `none` に設定します。**

```
{0} ok setenv security-mode none
```

2. **両方のパスワードプロンプトのあとで Return と入力することによって、パスワードの長さをゼロに設定します。**

▼ 失敗したログインを確認する (OBP)

1. **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 Ø 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. **次のように入力してパラメータをリセットします。**

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

▼ 電源投入バナーを使用する

直接防止したり検出を制御したりできませんが、次の目的にバナーを使用できます。

- 所有権を譲渡するため。
- サーバーの許容可能な使用についてユーザーに警告するため。
- OpenBoot パラメータへのアクセスまたは変更が、承認された人に制限されていることを示すため。

- **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。**

```
{0} ok setenv oem-banner banner-message
{0} ok setenv oem-banner? true
```

バナーメッセージには最大 68 文字使用できます。出力可能な文字がすべて受け入れられます。

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方法については、次の場所にあるプロダクトノートを参照してください。

http://docs.oracle.com/cd/E55211_01/

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にはさらに管理が必要ですが、システムデータの保護が強化されます。

- 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 WAN ブートインストール構成のセキュリティー保護に関する説明を参照してください。

  http://www.oracle.com/goto/solaris10/docs を参照してください。
- Oracle Solaris 11 OS の場合、『*Oracle Solaris* 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 を参照してください。