SPARC M5-32 および SPARC M6-32 サーバー

セキュリティーガイド

Part No: E49758-02
2014 年 7 月

目次

・・・第 1 章

1 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。

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に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

- 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、粉砕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ラ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ラ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

2 ソフトウェアのセキュリティーについて

ほとんどのハードウェアセキュリティーは、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。

▼ 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 セキュリティー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ー保護を行います。
   『*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. 個々のドメインをセキュリティー保護するには、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 のセキュリティー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)

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