

SPARC および Netra SPARC S7-2 シリーズ サーバーセキュリティガイド



Part No: E77180-01
2016 年 6 月

Part No: E77180-01

Copyright © 2016, 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.

このソフトウェアまた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。このソフトウェアまたはハードウェアは、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。このソフトウェアまた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。このソフトウェアまた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に起因して損害が発生しても、Oracle Corporation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はオラクル およびその関連会社の登録商標です。その他の社名、商品名等は各社の商標または登録商標である場合があります。

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。適用されるお客様とOracle Corporationとの間の契約に別段の定めがある場合を除いて、Oracle Corporation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。適用されるお客様とOracle Corporationとの間の契約に定めがある場合を除いて、Oracle Corporation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。

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	7
アクセス制限	7
シリアル番号	8
ハードドライブ	8
ソフトウェアのセキュリティーについて	9
▼ 不正アクセスを防止する (Oracle Solaris OS)	9
▼ 不正アクセスを防止する (Oracle ILOM)	9
▼ 不正アクセスを防止する (Oracle VM Server for SPARC)	10
アクセスの制限 (OpenBoot)	10
▼ パスワード保護を実装する	10
▼ セキュリティーモードを有効にする	10
▼ セキュリティーモードを無効にする	11
▼ 失敗したログインをチェックする	12
▼ 電源投入バナーを提供する	12
Oracle システムファームウェア	12
WAN ブートをセキュリティー保護する	13
検証済みブート	13

ハードウェアのセキュリティについて

物理的な分離とアクセス制御は、セキュリティアーキテクチャーを構築すべき基盤です。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。

これらのセクションでは、SPARC および Netra SPARC S7-2 シリーズサーバーのハードウェアの一般的なセキュリティガイドラインについて説明します。

- [7 ページの「アクセス制限」](#)
- [8 ページの「シリアル番号」](#)
- [8 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、改ざんや誤って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 (交換部品など) にセキュリティ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が、唯一の所有権証明になる場合があります。

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。これらのセクションでは、SPARC および Netra SPARC S7-2 シリーズサーバーのソフトウェアの一般的なセキュリティガイドラインについて説明します。

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

▼ 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。
使用しているバージョンの『Oracle Solaris セキュリティガイドライン』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)

- 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>

▼ 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。

- [10 ページの「パスワード保護を実装する」](#)
- [10 ページの「セキュリティモードを有効にする」](#)
- [11 ページの「セキュリティモードを無効にする」](#)
- [12 ページの「失敗したログインをチェックする」](#)
- [12 ページの「電源投入バナーを提供する」](#)

OpenBoot のセキュリティ変数の設定の詳細は、次の場所にある 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

- まだパスワードを設定していない場合は、この手順を実行してください。

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

パスワードの長さは 1 - 8 文字にできます。8 文字より多く入力した場合、最初の 8 文字のみが使用されます。すべての印刷可能な文字が受け入れられます。制御文字は使用できません。

注記 - パスワードをゼロ文字に設定すると、セキュリティがオフになり、`security-mode` パラメータは `none` に設定された場合を同じように処理されます。ただし、設定は変更されません。

▼ セキュリティ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 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。

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

2. セキュリティモードプロンプトを取得します。

前述したようにセキュリティモードを設定したあとで、セキュリティモードプロンプトを取得するには 2 つの方法があります。

■ 単語 logout および login 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
```

セキュリティモードを終了するには、例に示すように名前 logout および login を使用します。

■ 単語 reset-all を使用します。

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

この単語によってシステムがリセットされます。システムが再起動すると、OpenBoot はセキュリティモードプロンプトに移動します。コマンドプロンプトに再度ログインする (またはセキュリティモードからログアウトする) には、前述したように名前 logout および login を使用して、パスワードを入力します。

▼ セキュリティ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に Return を入力して、パスワードを長さゼロに設定します。

▼ 失敗したログインをチェックする

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。

```
{0} ok printenv security-#badlogins
```

このコマンドが 0 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. このコマンドを入力して、パラメータをリセットします。

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

▼ 電源投入バナーを提供する

これは直接の予防的コントロールまたは発見的コントロールではありませんが、次の理由でバナーを使用できます。

- 所有権を譲渡する。
 - サーバーの許容される用途をユーザーに警告する。
 - 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。
- 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
```

バナーメッセージは最大 68 文字です。すべての印刷可能な文字が受け入れられます。

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、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するほど、多くの管理が必要になりますが、システムデータをより広範に保護できます。

- 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保護に関する説明を参照してください。
- Oracle Solaris 11 OS の場合、『*Oracle Solaris 11.3 でのネットワークのセキュリティ保護*』を参照してください。

検証済みブート

検証済みブートを使用して、システムのブートブロックと Oracle Solaris カーネルモジュールをシステムにロードする前に検証できます。Oracle ILOM を使用して検証済みブートを有効にし、検証チェックの失敗時にシステムで対応すべき方法を指定します。検証済みブートを有効にすると、システムブートブロックへの有害な変更を防止したり、Oracle Solaris カーネルモジュールが影響を受けないようにしたりできます。

SPARC 検証済みブートプロパティの構成については、『*Oracle ILOM 構成および保守用管理者ガイド*』を参照してください。

