

# Sun Storage 16 Gb Fibre Channel PCIe Universal Host Bus Adapter

HBA Model 7101674 用セキュリティーガイド

---

Copyright © 2013, 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場合、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

---

<b>1. Sun Storage 16 Gb FC PCIe Universal HBA セキュリティー</b> .....	5
Universal HBA の概要 .....	5
セキュリティーの原則 .....	6
セキュアな環境の計画 .....	7
ハードウェアのセキュリティー .....	7
ソフトウェアのセキュリティー .....	8
ファームウェアのセキュリティー .....	8
Oracle ILOM ファームウェア .....	8
システムログ .....	8
セキュアな環境の保守 .....	9
アセットの追跡 .....	9
ファームウェアの更新 .....	9
ソフトウェアの更新 .....	9
ログのセキュリティー .....	10
モジュールのセキュリティー .....	10



---

# 1

・・・ 第 1 章

## Sun Storage 16 Gb FC PCIe Universal HBA セキュリティ

---

このドキュメントでは、Sun Storage 16 Gb FC PCIe Universal HBA を使用するときを考慮するセキュリティの原則とガイドラインについて説明します。

このドキュメントには、次のセキュリティ情報は記載されていません。

- BIOS、Open Boot Prom (OBP)、および Hypervisor など、個々のプラットフォームファームウェアのセキュリティ
- オペレーティングシステムのセキュリティに関する注意事項
- ハードウェアシステムの物理的なセキュリティ
- 外部ネットワーク基盤のネットワークセキュリティ
- Trusted Platform Module の情報

これらのセキュリティ領域に関する情報については、個々の製品に付属のセキュリティドキュメントを参照してください。

このドキュメントには、次のトピックが含まれています。

- [5 ページの「Universal HBA の概要」](#)
- [6 ページの「セキュリティの原則」](#)
- [7 ページの「セキュアな環境の計画」](#)
- [9 ページの「セキュアな環境の保守」](#)

### Universal HBA の概要

Oracle の Sun Storage 16 Gb Fibre Channel PCIe Universal HBA (パーツ番号 7101674) は、QLogic テクノロジを使用した、スタンドアロンの PCIe ロープロファイル Universal Host Bus Adapter です。HBA は動作プロトコルモードを 2 ポートの 16 Gb ファイバチャネル HBA から 2 ポートの 10 GbE ファイバチャネルオーバーイーサネット (FCoE) コンバージドネットワークアダプタに変更できる構成可能ボードであるため、汎用とみなされます。Universal HBA では、次の 4 つの構成が可能です。

- **10 GbE FCoE 銅** – この構成では、Twinax 銅ケーブル接続と 10 GbE FCoE Universal HBA 機能が提供されます。この Universal HBA 構成では、光モジュールの取り付けも装着も行いません。
- **16 Gb FC SW (短波長) 光** – この構成では、Universal HBA の SFP+ コネクタに 16 Gb FC 短波長の光トランシーバモジュールを取り付けて、16 Gb ファイバチャネル HBA 機能を有効にする必要があります。
- **10 GbE FCoE SR (短距離) 光** – この構成では、Universal HBA の SFP+ コネクタに 10 GbE 短距離の光トランシーバモジュールを取り付けて、10 GbE FCoE コンバーズドネットワークアダプタ機能を有効にする必要があります。
- **16 Gb FC LW (長波長) 光** – この構成では、Universal HBA の SFP+ コネクタに 16 Gb FC 長波長の光トランシーバモジュールを取り付けて、16 Gb ファイバチャネル HBA 機能を有効にする必要があります。

次の画像は、Sun Storage 16 Gb FC PCIe Universal HBA を示しています。



## セキュリティの原則

基本的なセキュリティの原則として、アクセス、認証、承認、およびアカウントの 4 つがあります。

- **アクセス**

物理的な制御とソフトウェアの制御によって、ハードウェアやデータを侵入から保護します。

- ハードウェアの場合、アクセス制限とは、通常は物理的なアクセス制限を意味します。
- ソフトウェアの場合、物理的な手段と仮想的な手段の両方でアクセスが制限されます。
- ファームウェアは、Oracle の更新プロセス以外では変更できません。

- **認証**

ユーザーが本人であることを保証するには、プラットフォームのオペレーティングシステムにパスワードシステムなどの認証機能を設定します。

担当者がコンピュータ室に入室する際に、従業員バッジを適切に付けていることを確認してください。

- **承認**

トレーニングを受けて使用を認定されたハードウェアとソフトウェアの操作のみを担当者に許可します。読み取り/書き込み/実行のアクセス権を設定して、コマンド、ディスク領域、デバイス、およびアプリケーションへのユーザーアクセスを制御します。

- **アカウントティング**

Oracle のソフトウェアおよびハードウェア機能を使用して、ログイン操作を監視したりハードウェアインベントリを管理したりします。

- ユーザーログインを監視するには、システムログを使用します。特にシステム管理者アカウントとサービスアカウントは強力なコマンドにアクセスできるため、これらのアカウントを監視してください。
- システムアセットを追跡するには、コンポーネントのシリアル番号を使用します。すべてのカード、モジュール、およびマザーボードには、Oracle パーツ番号が電子的に記録されています。

## セキュアな環境の計画

サーバーおよび Sun Storage 16 Gb Fibre Channel Express Module Universal HBA の設置と構成の前および最中に、このセクションの情報を参照してください。

このセクションには、次のトピックが含まれています。

- [7 ページの「ハードウェアのセキュリティ」](#)
- [8 ページの「ソフトウェアのセキュリティ」](#)
- [8 ページの「ファームウェアのセキュリティ」](#)
- [8 ページの「Oracle ILOM ファームウェア」](#)
- [8 ページの「システムログ」](#)

### ハードウェアのセキュリティ

物理的なハードウェアのセキュリティ保護は非常にシンプルで、ハードウェアへのアクセスを制限すること、およびシリアル番号を記録することです。

- **アクセスを制限する**
  - 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を保守する必要があるとき以外はドアの鍵は掛けたままにしてください。
  - 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。
- **シリアル番号を記録する**

すべての Universal HBA カードのシリアル番号を記録しておいてください。

## ソフトウェアのセキュリティー

ソフトウェアコンポーネントのセキュリティー考慮事項は次のとおりです。

- ソフトウェアに付属のドキュメントを参照して、ソフトウェアで使用可能なセキュリティー機能を有効にします。
- Universal HBA ドライバを設定および更新するには、スーパーユーザーアカウントを使用します。
- 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。
- Universal HBA をサポートするソフトウェアコンポーネントは、セキュアなアクセスを実現するために、システムのセキュリティー機能に依存しています。

## ファームウェアのセキュリティー

Universal HBA は出荷時にすべてのファームウェアがインストールされています。更新を除き、現場でファームウェアのインストールは必要ありません。

- ファームウェアの更新が必要になった場合は、QLogic Web サイトの Oracle サポート領域 ([http://www.driverdownloads.qlogic.com/QLogicDriverDownloads/Oracle\\_Search.aspx](http://www.driverdownloads.qlogic.com/QLogicDriverDownloads/Oracle_Search.aspx)) からファームウェアの更新を入手してください。

また、Oracle サポートに問い合わせサポートを手配したり、Oracle サポートに製品の最新の更新と手順について確認したりすることもできます。

<https://support.oracle.com>

- Universal HBA ファームウェア管理ユーティリティを設定および更新するには、スーパーユーザーアカウントを使用します。通常のユーザーアカウントでは、ファームウェアを表示することはできますが、編集できません。Oracle Solaris OS ファームウェア更新プロセスでは、未承認のファームウェア変更を防止しています。
- 最新ニュース、ファームウェア更新要件に関する情報、またはその他のセキュリティー情報については、Oracle の Web サイトにある Universal HBA のインストールガイドを参照してください。
- SPARC OpenBootPROM (OBP) セキュリティー変数の設定については、*OpenBoot 4.x のコマンドリファレンスマニュアル*を参照してください。

## Oracle ILOM ファームウェア

x86 サーバーにプリインストールされている Oracle Integrated Lights Out Manager (Oracle ILOM) ファームウェアを使用すると、システムコンポーネントをアクティブにセキュリティー保護、管理、および監視できます。このファームウェアを使用したパスワードの設定、ユーザーの管理、およびセキュリティー関連機能 (Secure Shell (SSH)、Secure Socket Layer (SSL)、RADIUS 認証など) の適用に関する詳細は、Oracle ILOM のドキュメントを参照してください。

<http://www.oracle.com/pls/topic/lookup?ctx=ilom31>

## システムログ

- ログインを有効にし、専用のセキュアなログホストにログを送信してください。

- NTP およびタイムスタンプを使用して正確な時間情報を含めるようにロギングを構成してください。

## セキュアな環境の保守

Universal HBA の初期インストールおよび設定のあと、Oracle ハードウェアおよびソフトウェアのセキュリティー機能を使用して、ハードウェアの制御およびシステムアセットの追跡を続行してください。

次のセクションが含まれています。

- [9 ページの「アセットの追跡」](#)
- [9 ページの「ファームウェアの更新」](#)
- [9 ページの「ソフトウェアの更新」](#)
- [10 ページの「ログのセキュリティー」](#)
- [10 ページの「モジュールのセキュリティー」](#)

### アセットの追跡

インベントリを追跡するには、シリアル番号を使用します。シリアル番号は、オプションのカードやシステムのマザーボード上のファームウェアに組み込まれています。これらのシリアル番号は、ローカルエリアネットワーク接続で読み取ることができます。

また、ワイヤレスの無線周波数識別 (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* を使用して Oracle Sun システムアセットを追跡する方法に関する Oracle のホワイトペーパーを参照してください。

### ファームウェアの更新

装置のファームウェアのバージョンを最新に維持してください。

- 更新を定期的にチェックしてください。
- カードを管理したり、ドライバやファームウェアをアップグレードしたりするには、一般にすべてのオペレーティングシステム、特に Oracle Solaris では、root 資格情報でログインする必要があります。
- 常に、最新のリリースバージョンのファームウェアをインストールしてください。

### ソフトウェアの更新

装置のソフトウェアは最新バージョンを維持してください。

- Oracle Solaris ドライバのソフトウェアの更新は、Oracle Solaris のパッチおよび更新を通じて入手できます。
- その他のオペレーティングシステムのドライバのソフトウェア更新は、[http://www.driverdownloads.qlogic.com/QLogicDriverDownloads/Oracle\\_Search.aspx](http://www.driverdownloads.qlogic.com/QLogicDriverDownloads/Oracle_Search.aspx) から入手できる場合があります。
- 最新ニュース、ソフトウェア更新要件に関する情報、またはその他のセキュリティー情報については、Oracle の Web サイトにある Universal HBA のドキュメントを参照してください。

- 常に、最新のリリースバージョンのソフトウェアをインストールしてください。
- ソフトウェアに必要なセキュリティパッチをインストールしてください。
- デバイスにはファームウェアも搭載されており、ファームウェアの更新が必要な場合があります。

## ログのセキュリティ

ログファイルは定期的に検査および保守してください。

- 可能性がある問題をログで確認し、セキュリティポリシーに従ってアーカイブしてください。
- ログファイルが適切なサイズを超えたら、定期的に回収してください。あとで参照したり、統計的に分析したりできるように、回収したファイルのコピーを保守してください。

## モジュールのセキュリティ

Universal HBA は、QLogic QConvergeConsole のコマンド行インタフェース (CLI) またはグラフィカルユーザーインタフェース (GUI) ユーティリティで管理されます。これらのユーティリティでは次のことが可能です。

- Universal HBA の動作を監視します。
- Universal HBA の動作プロトコルモード構成を変更します。
- Universal HBA ファームウェアを更新します。

QConvergeConsole ユーティリティにアクセスできるのは、**root** 資格情報を持つユーザーのみです。したがって、特権のないユーザーは、これらのユーティリティを使用して SAN 環境を変更することができません。

QConvergeConsole の CLI および GUI については、Web サイト (<http://www.qlogic.com>) で QLogic QConvergeConsole のドキュメントを参照してください。