Sun Flash Accelerator F40 PCIe カード

セキュリティーガイド

Part No: E39696-02
2013 年 10 月

目次

・・・第 1 章

Sun Flash Accelerator F40 PCIe カードのセキュリティー

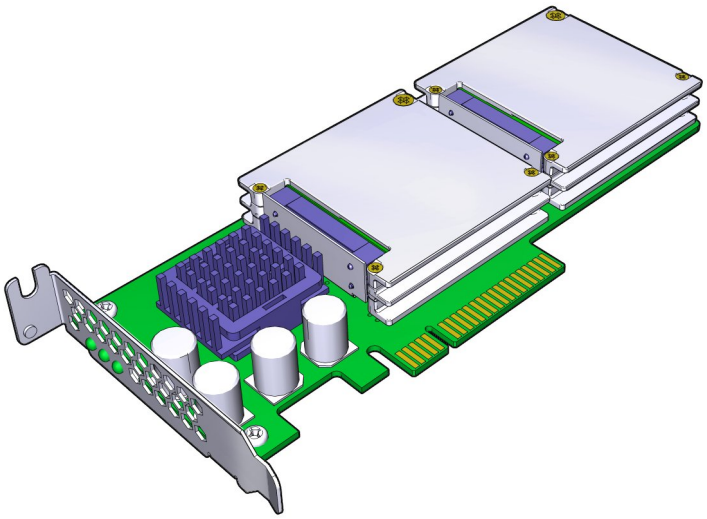
このドキュメントでは、Sun Flash Accelerator F40 PCIe カードなどの Oracle x86 ハードウェア製品の保護に役立つ一般的なセキュリティーガイドラインを示します。

次のセクションが含まれています。

Sun Flash Accelerator F40 PCIe カードの説明

次のセクションが含まれています。

Sun Flash Accelerator F40 PCIe カードは、ロープロファイルフォームファクタの、すぐに使える PCI-E 2.0 HBA フラッシュメモリーストレージカードです。次の図に、Sun Flash Accelerator F40 PCIe カードを示します。



詳細な製品情報については、*Sun Flash Accelerator F40 PCIe カードユーザーズガイド*を参照してください。

ハードウェアコンポーネント

Sun Flash Accelerator F40 PCIe カードには次のハードウェアコンポーネントが含まれています。

- 4 つの SSD フラッシュモジュール: 合計400G バイトの 32nm eMLC NAND フラッシュメモリーがカードに直接搭載されています。
- PCI-E 対 SAS プロトコルコントローラ: Sun Flash Accelerator F40 PCIe カードのプロトコルコントローラへの SATA インタフェースには、LSI 2008 SAS/SATA 2 x4 6G ビット/秒プロトコルコントローラに接続する PCI-E 2.0 x8 ホストインタフェースがあります。
- エネルギーストレージコンポーネント: システムまたは PCIe スロットの電源に障害が発生した場合は、未完了の書き込みをフラッシュメモリーにフラッシュします。

詳細については、*Sun Flash Accelerator F40 PCIe カードユーザーズガイド*を参照してください。

ソフトウェアおよびファームウェアコンポーネント

Sun Flash Accelerator F40 PCIe カードには次のモジュールが含まれています。

コンポーネント	参照先
MegaRAID Storage Manager (MSM)	7 ページの「MSM アプリケーションのセキュリティー」
診断サービス	8 ページの「診断サービスのセキュリティー」
Linux 診断ドライバ	9 ページの「Linux 診断サービスのセキュリティー」
SNMP	9 ページの「SNMP のセキュリティー」
WarpDrive コントローラファームウェア	10 ページの「Warp Drive コントローラファームウェアのセキュリティー」
SSDFW	10 ページの「SSDFW のセキュリティー」
DDCLI	11 ページの「DDCLI のセキュリティー」

詳細については、*Sun Flash Accelerator F40 PCIe カードユーザーズガイド*を参照してください。

セキュリティーの原則

基本的なセキュリティーの原則として、アクセス、認証、承認、およびアカウンティングの 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 Flash Accelerator F40 PCIe カードをインストールして構成するときは、実行前および実行時に次の点に注意してください。

次のセクションが含まれています。

- 8 ページの「ハードウェアのセキュリティー 」
- 8 ページの「ソフトウェアのセキュリティー 」
- 8 ページの「ファームウェアのセキュリティー」
- 9 ページの「Oracle ILOM ファームウェア」

- 9 ページの「システムログ」

ハードウェアのセキュリティー

物理的なハードウェアのセキュリティー保護方法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の 2 つです。

- **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は、承認された人だけがアクセスするように制限してください。
- **シリアル番号を記録する**
  - すべての Sun Flash Accelerator F40 PCIe カードにセキュリティーマークを付けます。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。
  - すべての Sun Flash Accelerator F40 PCIe カードのシリアル番号を記録しておいてください。
  - 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。

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てください。
- Sun Flash Accelerator F40 PCIe カード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。
- Sun Flash Accelerator F40 PCIe カード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

Sun Flash Accelerator F40 PCIe カード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、Oracle サポートに問い合わせてサポートを手配するか、Oracle サポートに製品の最新の更新と手順について確認してください。

  https://support.oracle.com
- Sun Flash Accelerator F40 PCIe カードのファームウェア管理ユーティリティー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、無許可のファームウェアの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、Sun Flash Accelerator F40 PCIe カードとともに提供されているプロダクトノート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 Command Reference Manual*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

- ロギングを有効にし、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

Sun Flash Accelerator F40 PCIe カードの初期インストールおよび設定が終了したら、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」
- 10 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

目録を追跡するには、シリアル番号を使用します。Oracle のシリアル番号は、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。
- 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.lsi.com 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、Sun Flash Accelerator F40 PCIe カードとともに提供されているプロダクトノー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ー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ー

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、セキュリティーポリシーに従って情報を保存してください。
- 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ー

次のソフトウェアおよびファームウェアモジュールがあります。

- 10 ページの「MSM アプリケーションのセキュリティー」
- 12 ページの「診断サービスのセキュリティー」
- 12 ページの「Linux 診断ドライバのセキュリティー」
- 13 ページの「SNMP のセキュリティー」
- 14 ページの「SSDFW のセキュリティー」
- 14 ページの「DDCLI のセキュリティー」

注記

テキストの WarpDrive という用語は Sun Flash Accelerator F40 PCIe カード を指します。

MSM アプリケーションのセキュリティー

MegaRAID Storage Manager (MSM) は、ドライバを通じて、WarpDrive ファームウェアを構成し、やりとりするためのグラフィカルユーザーインタフェースを提供するソフトウェアアプリケーショ

ンです。MSM は、LSI® MegaRAID、SAS、および WarpDrive コントローラのストレージ構成も監視し、保守します。

Sun Flash Accelerator F40 PCIe カードの MSM モジュールのセキュリティー考慮事項は次のとおりです。

- MegaRAID Storage Manager の互換性: Linux 64 ビット、Solaris X86。
- LSI によって提供されているユーザーガイド、MSM に組み込まれているオンラインヘルプ、インストーラに付属する readme ファイルを参照してください。http://www.lsi.com にアクセスしてください。
- アクセスが許可されるには、ユーザーが認証される必要があります。
  - ユーザーが root として認証されると、すべてのハードウェアアクセスが許可されます。
  - ユーザーとして認証されると、表示専用の権限が許可されます。
- 通常、ログファイルには書き込み権限があり、バイナリファイルには実行権限があり、その他のファイルは読み取り専用です。
- 管理権限を持つユーザーは一度に 1 人だけです。他のユーザーは表示専用権限を持ちます。クライアント/サーバーの認証時には、Java の組み込みの乱数ジェネレーターを使用して、セッション ID が生成されます。
- クライアントとサーバーは Java で実装されます。クライアントとサーバーは相互に TCP/IP を使用して通信します。サーバーは JNI を使用してライブラリと通信します。
- MSM はインターネットと通信しますが、IPv6 をサポートしていません。
- MSM は SSL を使用して、クライアントとサーバー間で通信します。
- システムのファイアウォール設定は、実行するインストールのタイプによって異なります。
  - ローカルを除くすべてのインストールで、MSM クライアントおよびサーバーへのアクセスを制御するように、ファイアウォールを構成する必要があります。
  - ローカルインストールでは、localhost IP を使用します。
- 設定の構成と変更には、root ユーザーアクセスが必要です。潜在的な攻撃者のアクセスを制限するには、次のガイドラインに従ってください。
  - セキュアなパスワードを選択します。
  - クライアントとサーバーの両方の、MSM コンポーネントを実行するすべてのシステムで異なるパスワードを使用します。
- オプションで、サーバーへのアクセスの認証に LDAP を使用できます。
- MegaRAID Storage Manager (MSM) は次の方法でインストールできます。
  - Complete: すべてのコンポーネントがインストールされます。
  - Client: リモートでのサーバーの表示と構成に必要なコンポーネントのみがインストールされます。ポート 3071 および 5571 が開いている必要があります。
  - Server: サーバーのリモート管理に必要なコンポーネントのみがインストールされます。

    MSM サーバーは、ユニキャストアドレスのほかに、マルチキャスト IP アドレス 229.111.112.12 と TCP/UDP ポート 3071 および 5571 も使用します。

    SNMP の場合、ポート 161 および 162 が開いている必要があります。LDAP が構成されている場合、ポート 389 が開いている必要があります。

- StandAlone: サーバーのローカル管理に必要なコンポーネントのみがインストールされます。
- Local: サーバーのローカル構成に必要なコンポーネントのみがインストールされます。

診断サービスのセキュリティー

診断サービスは、ドライバによって発行される WarpDrive 関連のトリガーイベントを待機する、サービスデーモンアプリケーションです。診断サービスは、報告されたイベントの発生時またはユーザーによるリクエスト時に、WarpDrive から診断情報を収集します。

Sun Flash Accelerator F40 PCIe カードの診断サービスモジュールのセキュリティー考慮事項は次のとおりです。

- 診断サービスデーモンは storelib ライブラリ API を使用して、関心のあるトリガーイベントを構成し、イベント通知を取得します。
- 診断サービスイベントおよびログ情報は、storelib ライブラリ API によって排他的に取得され、ログファイルに保存されます。
- 診断サービスは UDP ポート 162 を使用します。
- サンプルユーザーイベントスクリプトファイルはデフォルトでインストールされますが、デバッグ目的で構成しないかぎり使用されません。
- 診断サービスの構成ファイルとログファイルは、すべてのユーザーには読み取り専用で、root ユーザーには書き込み権限があります。バイナリファイルは、すべてのユーザーには読み取り専用ですが、root ユーザーには書き込みおよび実行権限があります。
- 診断サービスは、構成に応じて、イベントの発生時に SNMP トラップを送信できます。監視には、内部的にパイプが使用されます。

Linux 診断ドライバのセキュリティー

Linux 診断ドライバは、起動時に、自動的にホストトレースバッファー (2M バイト) をポストし、診断サービストリガーを実装し、管理インタフェースアプリケーションを使用して多くの機能をサポートできる MPT2SAS SAS2 6G バイトドライバです。ドライバは、トリガー属性に基づいてエラーを監視し、将来の参照用に新しい診断サービスイベントを追加します。

Sun Flash Accelerator F40 PCIe カードの Linux 診断ドライバのセキュリティー考慮事項は次のとおりです。

- Linux 診断ドライバはカーネル領域で実行します。OS が仮想化されている場合、ドライバは親で実行します。
- Linux 診断ドライバは、一連のトリガーイベントの発生時に、ファームウェアからトレースバッファーを取得します。これらのトリガーイベントは、システム管理者が指定し、カーネルの Sysfs インタフェース経由でドライバに送られます。
- 権限を持つ root ユーザーのみが Linux 診断ドライバの Sysfs 属性ファイルに書き込むことができます。
- Linux 診断ドライバの SAS2 世代製品は EEDP (End-to-end data protection) をサポートします。
- Linux 診断ドライバは、ハードウェア、ファームウェア、およびオペレーティングシステムの中間層の間にあります。Linux 診断ドライバは、下位では業界で確立された SAS2 および SATA プ

ロトコルと LSI Message Passing Technology を使用し、上位では OS 呼び出しを使用して、ストレージデータフローを処理します。

- Linux 診断ドライバソースはオープンソースで、Linux カーネルコミュニティーで入念に調査されています。
- Linux 診断ドライバは、それが管理するすべてのハードウェアのフルアクセス権を持ち、機能するために必要なすべてのカーネル構造にアクセスできます。Linux 診断ドライバは、SCSI IO の管理に使用されるすべてのカーネルインタフェースのフルアクセス権を持ちます。

SNMP のセキュリティー

SNMP エージェントにより、簡易ネットワーク管理プロトコル (SNMP) を使用して、LSI SAS コントローラを管理および監視できます。SNMP でサポートされるコントローラファミリーは LSI MR、IR、IR2、WarpDrive です。MIB ブラウザーを使用するか、独自のブラウザーを作成して、LSI SNMP エージェントによって表示されるトポロジーを監視および構成できます。

Sun Flash Accelerator F40 PCIe カードの SNMP モジュールのセキュリティー考慮事項は次のとおりです。

- SNMP サブエージェントは、簡易ネットワーク管理プロトコルを使用して、監視しているシステムの情報を SNMP クライアントに提供します。
- SNMP クライアントには、SNMPv1 をサポートする任意の MIB ブラウザーを使用できます。
- MR/IR SNMP サブエージェントは、storelib API を使用して storelib ライブラリから情報を取得します。storelib はその情報を取得するために、ドライバへの IOCTL (入出力制御) を行います。
- SNMP ログファイルには書き込み権限があり、バイナリファイルには実行権限があり、その他のファイルは読み取り専用です。
- すべての SNMP アクセスには、Net-SNMP をサポートする認証メカニズムを使用する認証が必要です。

WarpDrive コントローラファームウェアのセキュリティー

WarpDrive コントローラファームウェアは WarpDrive コントローラボード上で実行します。これは、WarpDrive コントローラボードに接続された SATA ソリッドステートドライブ (SSD) に対し、6G ビット/秒またはレガシーの 3G ビット/秒の転送速度を実現します。WarpDrive コントローラへのホスト接続は、PCIe 2.0 接続によってサポートされます。

Sun Flash Accelerator F40 PCIe カードの WarpDrive コントローラファームウェアのセキュリティー考慮事項は次のとおりです。

- WarpDrive コントローラファームウェアは、コントローラボード上にあるプロセッサで実行します。
- WarpDrive OS ドライバは、Warp Drive コントローラファームウェアの上位にあり、MPI (Message Passing Interface) を使用して PCIe 経由で通信します。
- Warp Drive コントローラファームウェアは、SAS/SATA インタフェースを使用して、その下位にある SSD ドライブモジュールとやりとりします。
- 正しい署名とチェックサムを持つ Warp Drive コントローラファームウェアイメージのみをボードにアップロードできます。

SSDFW のセキュリティー

SSDFW ファームウェアモジュールは、SF-2500 フラッシュストレージプロセッサファミリーのファームウェアを提供します。

Sun Flash Accelerator F40 PCIe カードの SSDFW モジュールのセキュリティー考慮事項は次のとおりです。

- SSDFW ファームウェアモジュールは、片方で NAND フラッシュインタフェースに接続し、もう一方で SATA AHCI インタフェースに接続します。
- ホスト側の通信は、シリアル ATA 規格および ATA コマンドセット (ACS-2) 規格に定義されている SATA インタフェース経由で接続します。
- SSDFW ファームウェアモジュールはデフォルトで admin 権限です。
- ログファイルは暗号化されます。ロギングはシリアルポートによってサポートされます。
- SSDFW モジュールは SF-2500 フラッシュストレージプロセッサ ASIC に存在する埋め込みファームウェアです。
- SSDFW ファームウェアモジュールはシステムデータ (ドライブ状態など) およびユーザーデータを格納し、それを NAND 不揮発性メディアに配置します。すべてのシステムデータはドライブの一意の鍵によって暗号化されます。
- 特権を取得するために、システムパスワードとユーザーパスワードが使用されます。
- SSDFW ファームウェアは、LSI-ASD サブシステム内に埋め込まれています。
- データ (プレーンテキスト) の暗号化には AES-128 または AES-256 が使用されます。SHA エンジンがファームウェアを認証します。キーおよびカウンタ値は、フラッシュメモリーに格納される前に暗号化されます。

DDCLI のセキュリティー

DDCLI はユーザーアプリケーションです。DDCLI は、システムに接続されている任意の WarpDrive を監視できるスタンドアロンの CLI です。WarpDrive の各種コンポーネントに関する重要な情報は、**ddcli** ユーティリティーを使用すると取得できます。

Sun Flash Accelerator F40 PCIe カードの DDCLI アプリケーションのセキュリティー考慮事項は次のとおりです。

- DDCLI は、初期状態では実行可能権限なしで出荷されています。root ユーザーはこの権限を追加する必要があります。
- 実行できるように、ファイル ddcli の権限を変更する必要があります。セキュリティーの問題を最小限に抑えるには、権限を 0744 に設定します。root が所有する必要があります。これにより、すべてのユーザーが表示できますが、実行できるのは root ユーザーだけです。
- MPT (Message Processing Technology) API をサポートするライブラリは、DDCLI に静的にリンクされます。このライブラリはドライバに IOCTL を送信して、必要な情報を取得します。
- DDCLI アプリケーションは、実行可能権限を持つバイナリファイルです。