



Sun™ Crypto Accelerator 4000 ボードご使用にあたって

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No. 817-2348-10
2003 年 5 月, Revision A

コメントの宛先: docfeedback@sun.com

Copyright 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, CA 95054 U.S.A. All rights reserved.

米国 Sun Microsystems, Inc. (以下、米国 Sun Microsystems 社とします)は、本書に記述されている製品に採用されている技術に関する知的所有権を有しています。これら知的所有権には、<http://www.sun.com/patents>に掲載されているひとつまたは複数の米国特許、および米国ならびにその他の国におけるひとつまたは複数の特許または出願中の特許が含まれています。

本書およびそれに付随する製品は著作権法により保護されており、その使用、複製、頒布および逆コンパイルを制限するライセンスのもとにおいて頒布されます。サン・マイクロシステムズ株式会社の書面による事前の許可なく、本製品および本書のいかなる部分も、いかなる方法によっても複製することが禁じられます。

本製品のフォント技術を含む第三者のソフトウェアは、著作権法により保護されており、提供者からライセンスを受けているものです。

本製品のの一部は、カリフォルニア大学からライセンスされている Berkeley BSD システムに基づいていることがあります。UNIX は、X/Open Company Limited が独占的にライセンスしている米国ならびに他の国における登録商標です。

本製品は、株式会社モリサワからライセンス供与されたリュウミン L-KL (Ryumin-Light) および中ゴシック BBB (GothicBBB-Medium) のフォント・データを含んでいます。

本製品に含まれる HG 明朝 L と HG ゴシック B は、株式会社リコーがリョービマジクス株式会社からライセンス供与されたタイプフェースマスタをもとに作成されたものです。平成明朝体 W3 は、株式会社リコーが財団法人 日本規格協会 文字フォント開発・普及センターからライセンス供与されたタイプフェースマスタをもとに作成されたものです。また、HG 明朝 L と HG ゴシック B の補助漢字部分は、平成明朝体 W3 の補助漢字を使用しています。なお、フォントとして無断複製することは禁止されています。

Sun, Sun Microsystems, SunVTS, AnswerBook2, docs.sun.com, iPlanet, Sun Enterprise, Sun Enterprise Volume Manager は、米国およびその他の国における米国 Sun Microsystems 社の商標もしくは登録商標です。サン・ロゴマークおよび Solaris は、米国 Sun Microsystems 社の登録商標です。

すべての SPARC 商標は、米国 SPARC International, Inc. のライセンスを受けて使用している同社の米国およびその他の国における商標または登録商標です。SPARC 商標が付いた製品は、米国 Sun Microsystems 社が開発したアーキテクチャーに基づくものです。Netscape は、米国 Netscape Communications Corporation の商標または登録商標です。本製品では、OpenSSL Project が開発した OpenSSL Toolkit (<http://www.openssl.org/>) のソフトウェアを使用しています。本製品では、Eric Young (eay@cryptsoft.com) が開発した暗号化ソフトウェアを使用しています。本製品では、Ralf S. Engelschall <rse@engelschall.com> が開発した mod_ssl project (<http://www.modssl.org/>) のソフトウェアを使用しています。

OPENLOOK、OpenBoot、JLE は、サン・マイクロシステムズ株式会社の登録商標です。

ATOK は、株式会社ジャストシステムの登録商標です。ATOKS は、株式会社ジャストシステムの著作物であり、ATOKS にかかる著作権その他の権利は、すべて株式会社ジャストシステムに帰属します。ATOK Server/ATOK12 は、株式会社ジャストシステムの著作物であり、ATOK Server/ATOK12 にかかる著作権その他の権利は、株式会社ジャストシステムおよび各権利者に帰属します。

本書で参照されている製品やサービスに関しては、該当する会社または組織に直接お問い合わせください。

OPENLOOK および Sun Graphical User Interface は、米国 Sun Microsystems 社が自社のユーザーおよびライセンス実施権者向けに開発しました。米国 Sun Microsystems 社は、コンピュータ産業用のビジュアルまたはグラフィカル・ユーザーインタフェースの概念の研究開発における米国 Xerox 社の先駆者としての成果を認めるものです。米国 Sun Microsystems 社は米国 Xerox 社から Xerox Graphical User Interface の非独占的ライセンスを取得しており、このライセンスは米国 Sun Microsystems 社のライセンス実施権者にも適用されます。

Use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth in the Sun Microsystems, Inc. license agreements and as provided in DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013(c)(1)(ii) (Oct. 1998), FAR 12.212(a) (1995), FAR 52.227-19, or FAR 52.227-14 (ALT III), as applicable.

本書は、「現状のまま」をベースとして提供され、商品性、特定目的への適合性または第三者の権利の非侵害の黙示の保証を含みそれに限定されない、明示的であるか黙示的であるかを問わない、なんらの保証も行われぬものとします。

本書には、技術的な誤りまたは誤植のある可能性があります。また、本書に記載された情報には、定期的に変更が行われ、かかる変更は本書の最新版に反映されます。さらに、米国サンまたは日本サンは、本書に記載された製品またはプログラムを、予告なく改良または変更することがあります。

本製品が、外国為替および外国貿易管理法 (外為法) に定められる戦略物資等 (貨物または役務) に該当する場合、本製品を輸出または日本国外へ持ち出す際には、サン・マイクロシステムズ株式会社の事前の書面による承諾を得ることのほか、外為法および関連法規に基づく輸出手続き、また場合によっては、米国商務省または米国所轄官庁の許可を得ることが必要です。

原典: Sun Crypto Accelerator 4000 Board Release Notes
Part No: 817-0432-10
Revision A



Sun Crypto Accelerator 4000 ボード のご使用にあたって

このマニュアルでは、Sun™ Crypto Accelerator 4000 ボードの既知の問題について説明します。

パッチ 114795-01 は、Sun Crypto Accelerator 4000 ソフトウェアをインストールすると自動的にインストールされます。将来パッチが更新された場合には、`showrev -p` コマンドを使用してパッチのバージョンを確認できます。

Sun Crypto Accelerator 4000 ソフトウェアの既知の問題

サポートするプラットフォーム

現在、Sun Crypto Accelerator 4000 ボードは、Sun Fire™ 15K プラットフォームをサポートしていません。

バグ ID 4757594 vca.conf の変数

Solaris ソフトウェアでこのバグが修正されるまでの手動の回避策として、vca.conf の変数が提供されています。次のエントリを kernel/drv/vca.conf ファイルに追加します。

```
dma-mode=1;
```

この回避策は、Sun Blade™ 100、150 などのローエンドプラットフォームでのみ必要です。

バグ ID 4470196 Solaris 8 の必須パッチ

Solaris 8 オペレーティング環境では、Sun Crypto Accelerator 4000 ソフトウェアをインストールする前に、パッチ番号 112438-01 および 109234-09 をインストールする必要があります。これらのパッチは、製品 CD の patches サブディレクトリに収録されています。また、<http://sunsolve.sun.com> からダウンロードすることもできます。

注 – これらのパッチを適用したあと、Sun Crypto Accelerator 4000 ソフトウェアをインストールする前に、システムを再起動する必要があります。

バグ ID 4621453 鍵の抽出

鍵を抽出するためのソフトウェアツールは、Sun ONE Web Server 6.x で提供されるもので、Sun ONE Web Server 4.x では提供されていません。

注 – Sun ONE Web サーバーは、以前は iPlanet™ Web サーバーと呼ばれていたものです。

ソフトウェア (内部) データベースの鍵を抽出するための回避策として、次の 2 つの方法があります。

- NSPR 4.12 および NSS 3.3 (またはそれ以降のバージョン) を、次の Web サイトからダウンロードします。
<http://www.mozilla.org>

配布されたソフトウェアをインストールしたあと、データベース上で pk12util を実行して、ソフトウェア (内部) データベースから証明書および鍵を抽出します。

- Netscape Communicator 4.x または 6.x を使用して、ソフトウェア (内部) データベースから鍵を抽出します。

バグ ID 4630250 鍵および証明書の素材

このマニュアルの発行時点では、Sun Crypto Accelerator 4000 ボードから鍵および証明書の素材を抽出する機能は使用できません。http://sunsolve.sun.com の Web サイトでパッチのデータベースを確認して、この問題を解決するためのパッチが作成されているかどうかを確認してください。

バグ ID 4796664 内部ループバックテスト

Sun Crypto Accelerator 4000 MMF ボードでは、SunVTS™ の内部ループバックテスト netlbtst が異常終了する場合があります。その場合、次のエラーメッセージが表示されます。

```
"
12/19/02 17:20:03 username SunVTS4.5: VTSID 8003 netlbtst.
  FATAL vcal:      "Failed to get the link up.
  Probable_Cause(s):
    (1)Loopback cable not connected.
    (2)Faulty loopback cable.
  Recommended_Action(s):
    (1)Check and replace, if necessary, the loopback cable.
    (2)If problem persists, call your authorized Sun service
  provider.
```

バグ ID 4826508 シングルコマンドモードでのログイン

シングルコマンドモードで vcaadm を実行してログインに失敗すると、次のメッセージが出力されます。

```
Security Officer Login: so
Security Officer Password:
Login failed.

Error writing data: Bad file number
```

バグ ID 4816009 FIPS モードを有効にする

セキュリティー管理者がボードの所有権を取得して FIPS モードを有効にしているときに、所有していないボードを暗号化演算に使用すると、ボードがハングアップすることがあります。

回避策 : FIPS モードになっているボードの情報を消去 (zeroize) しないでください。また、ボードに暗号化を要求しているときに、カードを初期化して FIPS モードにしないでください。

バグ ID 4825721 Sun Fire 15K システムの診断

MMF および UTP ボードを使用したポイントツーポイント構成で、Sun Fire 15K の診断を実行すると、コンソールに次のエラーが表示されます。

```
Feb 27 11:39:04 xc15p13-b3 vca: [ID 732820 kern.warning] WARNING:
vca1: vce_link_stats_set: cant determine params
Feb 27 11:40:29 xc15p13-b3 vca: [ID 214153 kern.warning] WARNING:
vca1: Can't determine link paramaters!
Feb 27 11:40:29 xc15p13-b3 vca: [ID 702911 kern.notice] NOTICE:
vca1: link up 0 Mbps half duplex
Feb 27 11:40:29 xc15p13-b3 vca: [ID 732820 kern.warning] WARNING:
vca1: vce_link_stats_set: cant determine params
Feb 27 11:41:08 xc15p13-b3 vca: [ID 702911 kern.notice] NOTICE:
vca0: link down
Feb 27 12:01:07 xc15p13-b3 vca: [ID 702911 kern.notice] NOTICE:
vca0: link up 1000 Mbps full duplex
```

この場合、接続は数分後に回復されるため、通信への影響はありません。

RFE ID 4753295

Apache Web サーバーソフトウェアでは、デフォルトでバルク暗号化が使用可能になっており、使用不可にはできません。Sun ONE サーバーソフトウェアでは、デフォルトでバルク暗号化が使用不可になっているため、空のファイル (/etc/opt/SUNWconn/cryptov2/sslreg) を作成して Sun ONE サーバーソフトウェアを再起動することで、手動で使用可能にする必要があります。Sun ONE サーバーソフトウェアでバルク暗号化を使用可能にすると、サイズの大きいファイルの転送速度は大幅に向上しますが、サイズの小さいファイルの転送速度は若干低下することがあります。

回避策 : Sun ONE サーバーソフトウェアのバルク暗号化は、主にサイズの大きいファイルを転送する場合にのみ使用可能にします。

バグ ID 4822356 vcaadm によるマスター鍵の交換

rekey master コマンドを実行すると、vcaadm によって「Cannot get new modulus from firmware.」というメッセージが表示されます。これは、マスター鍵が生成されなかったことを示しているわけではありません。このエラーメッセージには意味はなく、実際にはコマンドは正しく実行されています。

```
vcaadm{vca0@localhost, sec_officer}> rekey master
WARNING: Rekeying the master key will render all old board backups
         useless with the new keystore file.  If other boards use
this
         keystore, you will need to back up this new key and
initialize
         the other boards to use the keystore, providing the backed
up
         master key in the process.

Rekey board? (Y/Yes/N/No) [No]: y
Rekeying crypto accelerator board.  This may take a few
minutes...Done.
Cannot get new modulus from firmware.
```

バグ ID 4852120 タイムアウトエラーの可能性

ネットワークトラフィックの過負荷状態の検出と、暗号化演算の実行が同時に発生したとき、次のようなエラーメッセージが表示される場合があります。

```
Apr 17 23:44:37 xc15p13-b0 vca: WARNING: stale job(s) found in ring 30000978718
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         request 0x7820aa68
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         =====
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         vr_key_id[0]: 0x00000000
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         vr_key_id[1]: 0x00000000
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         vr_cmd: 0x0013
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         vr_key_flags[0]: 0x0
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         vr_key_flags[1]: 0x0
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         vr_in_len: 192
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         vr_out_len: 192
Apr 17 23:44:37 xc15p13-b0 genunix: WARNING: vca1: fault detected in device;
service unavailable
Apr 17 23:44:37 xc15p13-b0 genunix: WARNING: vca1: crypto job timeout (device
hung?)
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE: vca1: Resetting board...
Apr 18 00:08:47 xc15p13-b0 vca: WARNING: vca1: Device is in failed state!
Apr 18 00:08:47 xc15p13-b0 last message repeated 1 time
```

回避策 : Sun Crypto Accelerator 4000 ボードをリセットします。

Sun ONE Web サーバーの既知の問題

バグ ID 4532645 管理サーバーのメッセージ

Sun ONE 4.x または 6.x の管理サーバーが動作していて、管理される Web サーバーが動作していない場合には、いくつかの状況でトークンパスワードの入力を求めるダイアログボックスが表示されます。非常に大きなフォントが使用されていたり、トークンが多いためにパスワード入力の行が多数表示されたりすると、ダイアログボックスの固定サイズが小さいために、パネルの下部にあるボタンが表示されません。ダイアログボックスのサイズは変更できないため、パネルの下部の「Accept」ボタンを選択して変更を受け入れることができません。

この問題には、次の 2 つの回避策があります。

- コマンド行から、または管理ウィンドウの GUI で「Preferences」の「On/Off」を実行して、最初に Web サーバーを起動しておきます。

- 「Apply」 → 「Load Configuration Files」 を実行して、Web サーバーを起動せずに設定を適用します。

バグ ID 4532941 および 4593111 複数のキーストア

Sun ONE Web サーバーは、複数のキーストアが存在する構成では正しく動作しません。この問題は、Sun ONE Web Server 6.0 Service Pack 5 (SP5) で修正されています。

回避策：すべての Web サーバーインスタンスに対して、1 つのキーストアを設定します。次に、Web サーバーインスタンスごとに異なるキーストアユーザーを設定します。これで、各 Web サーバーインスタンスに個別の鍵を設定できます。

バグ ID 4620283 pk12util ユーティリティー

Sun ONE では、pk12util ユーティリティーを使用して、証明書および鍵を内部 (ソフトウェア) データベースからエクスポートし、外部 (ハードウェア) データベースにインポートすることができます。ただし、外部データベースから証明書または鍵をエクスポートすることはできません。

```
% cd /usr/iplanet/servers/alias
% pk12util -o temp.p12 -n "Our Token:Server-Cert" -d .
Enter Password or Pin for "Our Token":
Enter password for PKCS12 file:
Re-enter password:
pk12util: add cert and key failed: Unable to export. Private Key
could not be located and exported.
```

バグ ID 4607112 「Cipher Default」 の設定

Sun ONE Web Server 6.0 の設定では、「Cipher Default」設定を選択し、証明書を選択し、「OK」ボタンをクリックしてから、右上の角にある「Apply」リンクを選択して暗号を適用しますが、『Sun Crypto Accelerator 4000 ボードインストールマニュアル』に記載されている順序でこの手順を実行しないと、`username:password` エントリが削除される場合があります。この問題は、Sun ONE Web Server 6.0 Service Pack 3 (SP3) で修正されています。

このエントリは、Sun Crypto Accelerator 4000 ボードを使用する Web サーバーを正しく起動するために必要なものです。この問題は、次の順序で Sun ONE Web Server 6.0 を設定したときに発生する可能性があります。

1. 「Cipher Default」または「SSL2」暗号、「SSL3」暗号のいずれかを選択します。
2. 「OK」をクリックします。
3. 「Apply」をクリックします。
4. 「Load Configuration」をクリックします。

この手順を実行した可能性があり、Web サーバーが正しく起動しない場合には、次の回避策を実行してください。

- 次のファイルを編集します。

```
/usr/iplanet/servers/https-hostname.domain/config/server.xml
```

- 次の文字列で始まる行を検出します。

```
<SSLPARAMS servercertnickname="Server-Cert". . .
```

- 検出した行の Server-Cert の前に *keystore_name*: を挿入して、次のように変更します。

```
<SSLPARAMS servercertnickname="keystore_name:Server-Cert". . .
```

- Web サーバーを再起動します。

サポートする Apache Web サーバーのバージョン

Sun Crypto Accelerator 4000 ソフトウェアの現在のバージョンは、Apache 1.3.26 をサポートします。

Apache Web サーバーの既知の問題

バグ ID 4766977 Solaris 8 の必須パッチ

Solaris 8 オペレーティング環境で、Apache Web サーバーで使用する Sun Crypto Accelerator 4000 ボードを構成するには、Sun Crypto Accelerator 4000 ソフトウェアをインストールする前に、パッチ番号 109234-09 をインストールする必要があります。このパッチは、製品 CD の patches サブディレクトリに収録されています。また、<http://sunsolve.sun.com> からダウンロードすることもできます。

注 - このパッチを適用したあと、Sun Crypto Accelerator 4000 ソフトウェアをインストールする前に、システムを再起動する必要があります。

Apache Web サーバーは、Sun Crypto Accelerator 1000 ボードと Sun Crypto Accelerator 4000 ボードを同時に使用するようには構成することはできません。Apache Web サーバーを両方のボードを同時に使用するようには構成すると、Apache は正しく動作しなくなります。

Apache Web Server 1.3.26 で Sun Crypto Accelerator 4000 ボードを使用する場合にのみ、このボードの SUNWkc12a ソフトウェアパッケージをインストールしてください。Apache Web サーバーのほかの構成またはバージョンを使用する場合は、SUNWkc12a パッケージをインストールしないでください。

起動ファイル

Apache の起動ファイル (/etc/rc3.d/S50apache) および dtlogin の起動ファイル (/etc/rc2.d/S99dtlogin) の順序によっては、マシンの起動時に順序に関する問題が発生します。このため、起動時に、コンソールが Apache のパスワードエントリにアクセスできない場合があります。

回避策：スーパーユーザーになって次のコマンドを実行し、Apache Web サーバーを起動する順序を元に戻します。

```
# mv /etc/rc3.d/S50apache /etc/rc2.d/S95apache
```

