



# Sun™ Crypto Accelerator 1000 ボードバージョン 1.1 ご使用にあたって

---

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

Part No. 816-4572-10  
2002 年 7 月, Revision A

コメントの宛先: [docfeedback@sun.com](mailto:docfeedback@sun.com)

Copyright 2002 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・のロゴマークおよび 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 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らに限定されない、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 1000 Board Version 1.1 Release Notes Part No: 816-2451-11 Revision A
-----	---



# Sun Crypto Accelerator 1000 ボードバージョン 1.1 のご使用にあたって

---

このマニュアルでは、『Sun Crypto Accelerator 1000 ボードバージョン 1.1 インストールマニュアル』を発行した時点では記載できなかった情報について説明します。

---

## iPlanet Web サーバーの既知の問題

1. iPlanet 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、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る状況がいくつかあります。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、または管理用 GUI で「Preferences」の「On/Off」を設定して、最初に Web サーバーを起動します。
- Web サーバーを起動せずに設定を適用します。「Apply」->「Load Configuration Files」を実行します。

参照バグ : 4532645

2. 複数の領域が存在する場合、または各サーバーに異なるユーザーが設定されている場合は、iPlanet Web サーバーは動作しません。

この問題には、次の 2 つの回避策があります。

- 各 Web サーバーに 1 つの領域と 1 人のユーザーだけを設定します。

- 別々の UNIX ユーザーとして iPlanet Web サーバーの異なるインスタンスを実行すると、それぞれのユーザーに \$HOME/.SUNWconn\_crypto\_slots を設定できます。スロットファイルの詳細は、『Sun Crypto Accelerator 1000 ボードバージョン 1.1 インストールマニュアル』を参照してください。

参照バグ : 4532941 および 4593111

3. iPlanet では、ユーティリティ pk12util 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て外部 (ハードウェア) データベースにインポートします。ただし、外部データベースからは証明書および鍵はエクスポートされません。

```
% 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.
```

参照バグ : 4620283

4. iPlanet Web Server 6.0 の設定で、「Cipher Default」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たあとに、『Sun Crypto Accelerator 1000 ボードバージョン 1.1 インストールマニュアル』で指示されている順番に手順を実行しないと、`user@realm-name` エントリが削除される場合があります。

このエントリは、Sun Crypto Accelerator 1000 ボードを使用して Web サーバーを正しく起動するために必要です。次の順番で iPlanet Web Server 6.0 を設定すると、エントリが作成されます。

- 「Cipher Default」または「SSL2」暗号、「SSL3」暗号のいずれかを選択
- 「OK」をクリック
- 「Apply」をクリック
- 「Load Configuration Files」をクリック

この手順を実行しても Web サーバーが正しく起動しない場合は、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 `user@realm-name:` を挿入して、次のように変更します。

```
<SSLPARAMS servercertnickname="user@realm-name:Server-Cert" . . .
```

- Web サーバーを再起動します。

参照バグ : 4607112

---

## サポートされる Apache Web サーバーのバージョン

このバージョンの Sun Crypto Accelerator 1000 ソフトウェアは、Solaris 8 では Apache 1.3.12 および Apache 1.3.26 をサポートします。また、Solaris 9 では Apache 1.3.22 および Apache 1.3.26 をサポートします。このサポート情報は、オペレーティングシステムに含まれていた Apache のバージョンか、サンの正式なパッチとして提供された Apache のバージョンに適用されます。

---

## Apache Web サーバーの既知の問題

1. 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、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、コンソールは起動時に 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。この問題を回避するには、スーパーユーザーになって次のコマンドを実行して、Apache Web サーバーの起動順を元に戻します。

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

---

# Sun Crypto Accelerator 1000 バージョン 1.1 ソフトウェアの既知の問題

1. Solaris 8 オペレーティング環境では、Crypto Accelerator 1000 バージョン 1.1 ソフトウェアをインストールする前に、パッチ番号 112438-01 のパッチをインストールする必要があります。このパッチは、製品の CD の patches サブディレクトリに収録されています。また、このパッチを <http://sunsolve.sun.com> からダウンロードすることもできます。

参照バグ : 4470196

2. 鍵を抽出するためのソフトウェアツールは、iPlanet Web Server 6.x では提供されていますが、iPlanet Web Server 4.x では提供されていません。

ソフトウェア (内部) データベースの鍵を抽出するには、次の 2 つの回避策があります。

- 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.ipplanet.com/downloads>

配布されたソフトウェアをインストールし、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。

現在のところ、Sun Crypto Accelerator 1000 ボードが管理している鍵を抽出するための回避策は存在しません。

参照バグ : 4621453

3. prtdiag(1M) を使用したときに、Sun Crypto Accelerator 1000 ボードの表示が異なったり、まったく表示されなかったりする場合があります。これは、prtdiag ユーティリティおよび Open Boot PROM を実行するプラットフォームが異なっているためです。たとえば、Sun Enterprise 450 では、Sun Crypto Accelerator 1000 ボードは次のように表示されます。

SYS	PCI	66	4	pciclass,100000
-----	-----	----	---	-----------------

参照バグ : 4343467 および 4526901

4. このマニュアルを発行する時点では、**Sun Crypto Accelerator I** から鍵および証明書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。

参照バグ : 4630250

5. **Solaris 9** オペレーティング環境が動作している **Sun Fire™ V880** システムの場合、**66 MHz** スロットでの **PCI** ホットプラグ機能は、**Sun Crypto Accelerator 1000** ボードではサポートされていません。これは、**Solaris 8** オペレーティング環境が動作しているシステムには関係ありません。この問題は、将来のパッチで修正される予定です。

**Solaris 9** システムでは、システムの電源が切断されている間に、**66 MHz** スロットにボードを取り付けて、そのまま使用することができます。また、**Solaris 9** システムの **33 MHz** スロットでは、ボードのホットプラグが可能です。

参照バグ : 4698278

