



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

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

Part No. 816-4567-11
2002 年 7 月, Revision A

コメントの宛先: 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, Sun VTS, AnswerBook2, docs.sun.com, iPlanet, Sun Enterprise, Sun Enterprise Volume Manager, Sun Fire, Sun Solve, Netra 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 1000 Board Version 1.1 Installation and User's Guide Part No: 816-2450-11 Revision A
-----	---



Declaration of Conformity

EMC

Compliance Model Number: DEIMOS
Product Family Name: Sun Crypto Accelerator 1000 (X6762A)

European Union

This equipment complies with the following requirements of the EMC Directive 89/336/EEC:

EN55022:1998/CISPR22:1997	Class A
EN55024:1998	Required Limits (as applicable):
EN61000-4-2	4 kV (Direct), 8 kV (Air)
EN61000-4-3	3 V/m
EN61000-4-4	1 kV AC Power Lines, 0.5 kV Signal and DC Power Lines
EN61000-4-5	1 kV AC Line-Line and Outdoor Signal Lines 2 kV AC Line-Gnd, 0.5 kV DC Power Lines
EN61000-4-6	3 V
EN61000-4-8	1 A/m
EN61000-4-11	Pass
EN61000-3-2:1995 + A1, A2, A14	Pass
EN61000-3-3:1995	Pass

Safety

This equipment complies with the following requirements of the Low Voltage Directive 73/23/EEC:

EC Type Examination Certificates:
EN 60950:2000, 3rd Edition
IEC 60950:1999, 3rd Edition

Supplementary Information

This product was tested and complies with all the requirements for the CE Mark.

/S/

Dennis P. Symanski
Manager, Compliance Engineering
Sun Microsystems, Inc.
901 San Antonio Road, MPK15-102
Palo Alto, CA 94303-4900 U.S.A.
Tel: 650-786-3255
Fax: 650-786-3723

DATE

/S/

Peter Arkless
Quality Manager
Sun Microsystems Scotland, Limited
Springfield, Linlithgow
West Lothian, EH49 7LR
Scotland, United Kingdom
Tel: 0506-670000 Fax: 0506-760011

DATE

Regulatory Compliance Statements

サンの製品には、次の適合規制条件のクラスが明記されています。

- 米連邦通信委員会 (FCC) — アメリカ合衆国
- カナダ政府通産省デジタル機器工業規格 (ICES-003) — カナダ
- 情報処理装置等電波障害自主規制協議会 (VCCI) — 日本
- 台湾經濟部標準檢驗局 (BSMI) — 台湾

本装置を設置する前に、装置に記載されているマークに従って、該当する節をよくお読みください。

FCC Class A Notice

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Shielded Cables: Connections between the workstation and peripherals must be made using shielded cables to comply with FCC radio frequency emission limits. Networking connections can be made using unshielded twisted-pair (UTP) cables.

Modifications: Any modifications made to this device that are not approved by Sun Microsystems, Inc. may void the authority granted to the user by the FCC to operate this equipment.

FCC Class B Notice

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/television technician for help.

Shielded Cables: Connections between the workstation and peripherals must be made using shielded cables in order to maintain compliance with FCC radio frequency emission limits. Networking connections can be made using unshielded twisted pair (UTP) cables.

Modifications: Any modifications made to this device that are not approved by Sun Microsystems, Inc. may void the authority granted to the user by the FCC to operate this equipment.

ICES-003 Class A Notice - Avis NMB-003, Classe A

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

ICES-003 Class B Notice - Avis NMB-003, Classe B

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.


VCCI 基準について

クラス A VCCI 基準について

クラス A VCCI の表示があるワークステーションおよびオプション製品は、クラス A 情報技術装置です。これらの製品には、下記の項目が該当します。

この装置は、情報処理装置等電波障害自主規制協議会 (VCCI) の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

クラス B VCCI 基準について

クラス B VCCI の表示  があるワークステーションおよびオプション製品は、クラス B 情報技術装置です。これらの製品には、下記の項目が該当します。

この装置は、情報処理装置等電波障害自主規制協議会 (VCCI) の基準に基づくクラス B 情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをしてください。

BSMI Class A Notice

The following statement is applicable to products shipped to Taiwan and marked as Class A on the product compliance label.

警告使用者：

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

目次

1. 製品概要 1
 - ハードウェアの概要 1
 - 製品の機能 2
 - 動的再構成 (DR) および高可用性 (HA) に関する考慮事項 3
 - 負荷分散 4
 - ハードウェアおよびソフトウェアの要件 4
 - 必要なパッチ 5
 - Solaris 8 のパッチ 5
 - Solaris 9 のパッチ 6
2. Sun Crypto Accelerator 1000 ボードの取り付け 7
 - ボードの取り扱い 7
 - ボードの取り付け 8
 - ▼ ハードウェアを取り付ける 8
 - Sun Crypto Accelerator 1000 ソフトウェアのインストール 9
 - ▼ ソフトウェアをインストールする 9
 - ディレクトリおよびファイル 12
 - ソフトウェアの削除 13
 - ▼ ソフトウェアを削除する 14

- 3. iPlanet Web サーバーでのボードの使用可能化 15
 - パスワード 15
 - 領域およびユーザーの作成 16
 - ▼ 領域およびユーザーを作成する 16
 - iPlanet Web サーバーの使用可能化の概要 18

- 4. iPlanet Web Server 4.1 のインストールおよび構成 19
 - iPlanet Web Server 4.1 のインストール 19
 - ▼ iPlanet Web Server 4.1 をインストールする 19
 - ▼ 認証データベースを作成する 20
 - ▼ サーバーの証明書を生成する 22
 - ▼ サーバーの証明書をインストールする 24
 - iPlanet Web Server 4.1 の構成 26
 - ▼ iPlanet Web Server 4.1 を構成する 26

- 5. iPlanet Web Server 6.0 のインストールおよび構成 29
 - iPlanet Web Server 6.0 のインストール 29
 - ▼ iPlanet Web Server 6.0 をインストールする 29
 - ▼ 認証データベースを作成する 30
 - ▼ サーバーの証明書を生成する 33
 - ▼ サーバーの証明書をインストールする 34
 - iPlanet Web Server 6.0 の構成 36
 - ▼ iPlanet Web Server 6.0 を構成する 36

- 6. Apache Web サーバーの使用可能化 39
 - Apache Web サーバーの使用可能化 39
 - ▼ Apache Web サーバーを使用可能にする 39
 - 証明書の作成 42
 - ▼ 証明書を作成する 42

7.	診断および障害追跡	47
	SunVTS 診断ソフトウェア	47
	▼ dcatetest を実行する	48
	dcatetest のテストパラメタオプション	49
	dcatetest コマンド行構文	49
	Sun Crypto Accelerator 1000 の障害追跡	50
A.	iPlanet Web サーバーでの Sun Crypto Accelerator 1000 ボードの管理	53
	概念および用語	53
	領域およびユーザー、iPlanet Web サーバー	54
	トークンおよびスロットファイル	54
	スロットファイル	55
	secadm の使用	56
	動作モード	57
	secadm へのコマンドの入力	58
	secadm を使用した認証	59
	コマンドのヘルプの表示	61
	secadm プログラムの終了	62
	領域の設定および管理	62
	領域の作成	62
	現在の作業領域の設定	63
	領域でのユーザーの生成	64
	領域の一覧表示	65
	領域のクラスの一覧表示	65
	領域の削除	65
	ユーザーアカウントの設定および管理	66
	ユーザーの作成	66
	ユーザーの一覧表示	67
	ユーザーパスワードの変更	67

- ユーザーの有効化または無効化 67
- ユーザーの削除 68

- B. マニュアルページ 69

- C. Apache Web サーバーの SSL 設定ディレクティブ 71

- D. Sun Crypto Accelerator 1000 ボードで使用するアプリケーションの構築 81

- E. Sun Crypto Accelerator 1000 ボードの仕様 83
 - 物理的な寸法 83
 - インタフェースの仕様 84
 - 電源要件 84
 - 環境仕様 85

- F. サン以外のライセンス 87

表目次

表 1-1	サポートされる SSL アルゴリズム	3
表 1-2	ハードウェアおよびソフトウェアの要件	4
表 1-3	Sun Crypto Accelerator 1000 ソフトウェアの Solaris 8 必須パッチ	5
表 1-4	Sun Crypto Accelerator 1000 ソフトウェアの Solaris 8 推奨パッチ	6
表 2-1	/cdrom/cdrom0 ディレクトリにあるファイル	10
表 2-2	Sun Crypto Accelerator 1000 のディレクトリ	12
表 3-1	iPlanet Web サーバーに必要なパスワード	16
表 7-1	dcatest サブテスト	49
表 7-2	dcatest コマンド行構文	50
表 A-1	secadm オプション	56
表 A-2	管理コマンドマトリックス	59
表 B-1	Sun Crypto Accelerator 1000 のマニュアルページ	69
表 C-1	SSL プロトコル	73
表 C-2	使用可能な SSL の暗号	74
表 C-3	SSL の別名	75
表 C-4	暗号の優先順位を設定する特殊文字	76
表 C-5	SSL のクライアントの検証レベル	77
表 C-6	SSL のログレベルの値	78
表 C-7	使用可能な SSL のオプション	78
表 E-1	物理的な寸法	83

表 E-2	インタフェースの仕様	84
表 E-3	電源要件	84
表 E-4	環境仕様	85

はじめに

このマニュアルでは、Sun™ Crypto Accelerator 1000 ボードの機能について説明します。また、システムにボードを取り付けて使用方法についても説明します。

このマニュアルは、Solaris™ オペレーティング環境、PCI 入出力カードが取り付けられたサンのプラットフォーム、iPlanet および Apache Web サーバー、SunVTS™ ソフトウェア、認証局からの証明書取得システムを構成した経験のあるネットワーク管理者を対象にしています。

このマニュアルの構成

このマニュアルは、次の章で構成されています。

- 第 1 章では、Sun Crypto Accelerator 1000 ボードの概要とハードウェアおよびソフトウェアの要件について説明します。
- 第 2 章では、Sun Crypto Accelerator 1000 ハードウェアの取り付け方法およびソフトウェアのインストール方法について説明します。
- 第 3 章では、iPlanet Web サーバーで Sun Crypto Accelerator 1000 ボードを使用可能にする方法について説明します。
- 第 4 章では、iPlanet Web Server 4.1 で Sun Crypto Accelerator 1000 ボードを使用可能にする方法について説明します。
- 第 5 章では、iPlanet Web Server 6.0 で Sun Crypto Accelerator 1000 ボードを使用可能にする方法について説明します。
- 第 6 章では、Apache Web サーバーで Sun Crypto Accelerator 1000 ボードを使用可能にする方法について説明します。

- 第7章では、Sun Crypto Accelerator 1000 ソフトウェアの診断テストおよび障害追跡について説明します。
- 付録 A では、iPlanet Web サーバーで管理される Sun Crypto Accelerator 1000 ボードのセキュリティー機能の概要について説明します。
- 付録 B では、Sun Crypto Accelerator 1000 ソフトウェアに付属するマニュアルページについて説明します。
- 付録 C では、Sun Crypto Accelerator 1000 ソフトウェアを使用する Apache Web サーバーで SSL サポートを設定するためのディレクティブを示します。
- 付録 D では、Sun Crypto Accelerator 1000 バージョン 1.1 に付属するソフトウェアについて説明します。このソフトウェアは、Sun Crypto Accelerator 1000 ボードの強化された暗号化機能を利用する OpenSSL 互換のアプリケーションを構築するために使用します。
- 付録 E では、Sun Crypto Accelerator 1000 ボードに関するさまざまな仕様の概要について説明します。
- 付録 F では、サン以外のベンダーによる注意およびライセンスが適用されるソフトウェアについて説明します。

UNIX コマンド

このマニュアルには、UNIX[®]の基本的なコマンド、およびシステムの停止、システムの起動、デバイスの構成などの基本的な手順の説明は記載されていません。

基本的なコマンドや手順についての説明は、次のマニュアルを参照してください。

- 『Sun 周辺機器 使用の手引き』
- Solaris[™] オペレーティング環境についてのオンライン AnswerBook2[™]
- 本システムに付属している他のソフトウェアマニュアル

書体と記号について

書体または記号	意味	例
AaBbCc123	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力、コード例。	.login ファイルを編集します。 ls -a を実行します。 % You have mail.
AaBbCc123	ユーザーが入力する文字を、画面上のコンピュータ出力と区別して表します。	マシン名 % su Password:
AaBbCc123 またはゴシック	コマンド行の変数部分。実際の名前や値と置き換えてください。	rm <i>filename</i> と入力します。 rm ファイル名 と入力します。
『』	参照する書名を示します。	『Solaris ユーザーマニュアル』
「」	参照する章、節、または、強調する語を示します。	第 6 章「データの管理」を参照。 この操作ができるのは「スーパーユーザー」だけです。
\	枠で囲まれたコード例で、テキストがページ行幅をこえる場合に、継続を示します。	% grep '^#define \ XV_VERSION_STRING'

シェルプロンプトについて

シェル	プロンプト
UNIX の C シェル	マシン名%
UNIX の Bourne シェルと Korn シェル	\$
スーパーユーザー (シェルの種類を問わない)	#

Sun のオンラインマニュアル

サンの各種システムマニュアルは下記 URL より参照できます。

<http://www.sun.com/products-n-solutions/hardware/docs>

Solaris およびその他のマニュアルは下記 URL より参照できます。

<http://docs.sun.com>

コメントをお寄せください

弊社では、マニュアルの改善に努力しており、お客様からのコメントおよびご忠告をお受けしております。コメントは下記宛に電子メールでお送りください。

docfeedback@sun.com

電子メールの表題にはマニュアルの Part No. (816-4567-11) を記載してください。

なお、現在日本語によるコメントには対応できませんので、英語で記述してください。

第1章

製品概要

この章では、Sun Crypto Accelerator 1000 ボードについて説明します。この章は、次の節で構成されます。

- 1 ページの「ハードウェアの概要」
- 4 ページの「ハードウェアおよびソフトウェアの要件」

ハードウェアの概要

Sun Crypto Accelerator 1000 ボードはハーフサイズの PCI ボードで、公開鍵暗号処理および対称鍵暗号処理を高速化するために、暗号化コプロセッサとして機能します。この製品には、外部インタフェースはありません。ボードは内蔵 PCI バスインタフェースを使用してホストと通信します。e コマースアプリケーションで使用されるセキュリティープロトコルでは、多数の暗号化アルゴリズムの計算処理が大量に集中して行われます。この処理を高速化するのが、このボードの目的です。

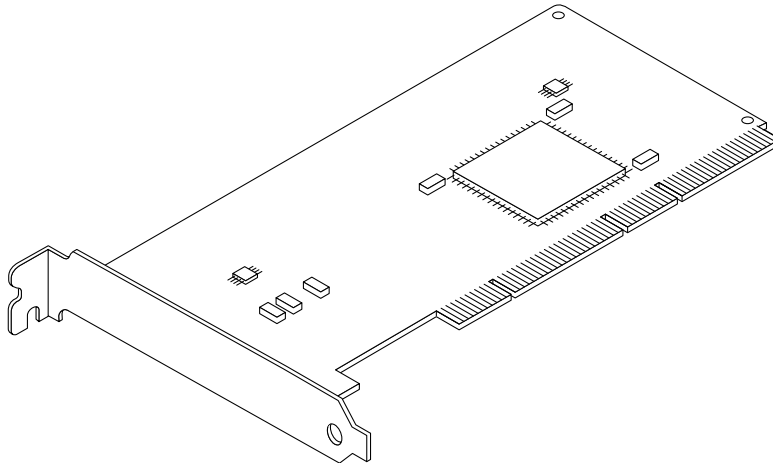


図 1-1 Sun Crypto Accelerator 1000 ボード

製品の機能

Sun Crypto Accelerator 1000 は、サンのプラットフォーム上で SSL の性能を向上させる暗号化アクセラレータボードです。Sun Crypto Accelerator 1000 は、ハードウェアおよびソフトウェアの両方における暗号化アルゴリズムを高速化します。ハードウェアとソフトウェアの両方の高速化に対応するのは、暗号化アルゴリズムの高速化にかかるコストがアルゴリズムによって異なるためです。暗号化アルゴリズムによっては、ハードウェアで実装されるように特別に設計されているものがあります。また、ソフトウェアで実装されるように設計されているものもあります。ハードウェアの高速化では、データをユーザーのアプリケーション空間からハードウェアの高速化装置に移動し、結果をユーザーアプリケーションに戻すため、余分な時間がかかります。暗号化アルゴリズムには、専用のハードウェアで実行された場合と同じように高度に調整されたソフトウェアで高速に処理されるもの (ARCFOUR など) があります。

Sun Crypto Accelerator 1000 ボードは、最大のスループットが得られるように、各暗号化要求を調べて、高速化のために最適な場所 (ホストプロセッサまたは Sun Crypto Accelerator 1000) を判定します。負荷分散は、暗号化アルゴリズムおよび現在のジョブの負荷、データサイズに基づいて行われます。

表 1-1 に、iPlanet および Apache Web サーバーで使用できる、ソフトウェアアルゴリズムとハードウェアにオフロードされる暗号化アルゴリズムを示します。

表 1-1 サポートされる SSL アルゴリズム

アルゴリズム	iPlanet Web サーバー		Apache Web サーバー	
	ハードウェア	ソフトウェア	ハードウェア	ソフトウェア
RSA	X	X	X	X
DSA	X	X	X	X
Diffie-Hellman			X	X
DES	X	X	X	X
3DES			X	X
ARCFOUR				X

動的再構成 (DR) および高可用性 (HA) に関する考慮事項

Sun Crypto Accelerator 1000 ハードウェアおよび関連するソフトウェアは、動的再構成 (DR) およびホットプラグをサポートするサンのプラットフォーム上で効果的に動作します。DR またはホットプラグ処理の実行中に、Sun Crypto Accelerator 1000 ソフトウェア層は、追加または取り外されたボードを自動的に検出し、ハードウェア資源の変更に適応するために、スケジューリングアルゴリズムを調整します。

高可用性 (HA) 構成では、ハードウェアの高速化を継続して使用できるように、1 つのシステムまたはドメインに複数の Sun Crypto Accelerator 1000 ボードを取り付けることができます。Sun Crypto Accelerator 1000 ハードウェアに障害が発生した場合は、ソフトウェア層が障害を検出し、使用可能なハードウェア暗号化アクセラレータのリストから障害の発生したカードを削除します。Sun Crypto Accelerator 1000 は、ハードウェア資源の減少に適応するために、スケジューリングアルゴリズムを調整します。それ以降の暗号化要求は、残りのカードにスケジュールされます。

また、Sun Crypto Accelerator 1000 ソフトウェアライブラリは、ソフトウェアですべての暗号化の演算を実行する機能を提供します。これによって、機能に悪影響を与えることなく、システムドメイン内のすべての Sun Crypto Accelerator 1000 ボードを DR またはホットプラグによって取り外すことができます。ただし、Sun Crypto Accelerator 1000 ハードウェアをサポートされる構成に復元するまでの間、性能には重大な悪影響を与えることとなります。

Sun Crypto Accelerator 1000 ハードウェアは、鍵長の長い鍵の生成に対して、高品質のエントロピを持つソースを提供します。ドメインまたはシステム内のすべての Sun Crypto Accelerator 1000 ボードが取り外された場合、鍵長の長い鍵は低品質のエントロピで生成されます。

負荷分散

Sun Crypto Accelerator 1000 ソフトウェアは、Solaris のドメインまたはシステムに取り付けられているボードの数だけ負荷を分散します。入ってくる暗号化要求は、固定長の作業キューに基づいてボードに分散されます。暗号化要求が最初のボードに送信されると、そのボードのキューがいっぱいになるまでは、そのあとの暗号化要求も最初のボードに送信されます。最初のボードのキューがいっぱいになると、そのあとの要求は、暗号化要求を受け取ることができる使用可能な最初のボードのキューに入れます。このキューイング機能は、ボードでの要求の処理を効率化することによって、スループットを最適化するように設計されています。

ハードウェアおよびソフトウェアの要件

表 1-2 に、Sun Crypto Accelerator 1000 ボードのハードウェアおよびソフトウェアの要件の概要を示します。

表 1-2 ハードウェアおよびソフトウェアの要件

ハードウェアおよびソフトウェア	要件
ハードウェア	Sun Blade™ 1000 Sun Enterprise™ 220R、250、420R、450 Sun Fire™ 280R、V480、V880、4800、4810、6800 Sun Netra™ T1 AC200/DC200、20、t 100/105、t 1120/1125、t 1400/1405 Sun Ultra™ 5、10、30、60、80
オペレーティング環境	Solaris 8 7/01 またはそれ以降の互換性のあるリリース Solaris 9 またはそれ以降の互換性のあるリリース
PCI スロット	32 ビットまたは 64 ビット 33 MHz または 66 MHz
ソフトウェア	iPlanet Web Server 4.1 SP9、6.0 SP1 または Apache Web Server 1.3.12、1.3.22 iPlanet または Apache Web サーバーの実行に必要なパッチ

注 – iPlanet Web Server 4.1 または 6.0 と記述されている場合は、サービスパック番号 SP9 または SP1 を指します。

必要なパッチ

システムで Sun Crypto Accelerator 1000 ボードを動作させるために、後述のパッチが必要になる場合があります。Solaris Update には、以前のリリースに対するパッチが含まれています。showrev -p コマンドを使用して、この節の表に記載されているパッチがすでにインストールされているかどうかを確認してください。

必要に応じて、次の Web サイトからパッチをダウンロードすることができます。
<http://sunsolve.sun.com>

最新のバージョンのパッチをインストールしてください。パッチのバージョンが新しくなると、ハイフン以降の数字 (-01 など) が大きくなります。Web サイトにあるパッチのバージョンが次の表に記載されているバージョンより大きい数字の場合は、Web サイトのパッチが最新のバージョンです。

必要なパッチが SunSolveSM から入手できない場合は、ご購入先にお問い合わせください。

Solaris 8 のパッチ

次の各表に、この製品で使用する Solaris 8 の必須パッチと推奨パッチを示します。表 1-3 に、必須パッチを示します。

表 1-3 Sun Crypto Accelerator 1000 ソフトウェアの Solaris 8 必須パッチ

パッチ ID	説明
110383-01	libnvpair
108528-05	KU-05 (nvpair サポート)
112438-01	/dev/random

注 – Apache 1.3.12 Web サーバーを使用する予定がある場合は、パッチ番号 109234-02 もインストールする必要があります。

表 1-4 に、Solaris 8 の推奨パッチを示します。

表 1-4 Sun Crypto Accelerator 1000 ソフトウェアの Solaris 8 推奨パッチ

パッチ ID	説明
108528-13	KU-13 (nvpair セキュリティー修正)

Solaris 9 のパッチ

現在のところ、Solaris 9 の必須パッチまたは推奨パッチはありません。

第2章

Sun Crypto Accelerator 1000 ボード の取り付け

この章では、Sun Crypto Accelerator 1000 ハードウェアの取り付け方法およびソフトウェアのインストール方法について説明します。この章は、次の節で構成されます。

- 7 ページの「ボードの取り扱い」
 - 8 ページの「ボードの取り付け」
 - 12 ページの「ディレクトリおよびファイル」
-

ボードの取り扱い

各ボードは、出荷時および保管時の保護のために、特別な静電気防止袋に入っています。ボード上の静電気に弱い部品の損傷を防ぐため、次のいずれかの方法で、ボードに触れる前に身体の静電気を取り除いてください。

- コンピュータの金属枠に触れる
 - 静電気防止用リストストラップを手首とアースされた金属面に装着する
-



注意 – ボード上の静電気に弱い部品の損傷を防ぐために、ボードを扱うときは静電気防止用リストストラップを装着して、ボードの端の部分だけを持ってください。ボードは常に静電気防止面 (ボードが入っていたビニール袋など) に置いてください。

ボードの取り付け

Sun Crypto Accelerator 1000 ボードの取り付け手順では、ボードのシステムへの挿入およびソフトウェアツールのインストールを行います。ハードウェアの取り付けについては、ボードの一般的な取り付け手順だけが記載されています。固有の取り付け手順については、ご使用のシステムに付属のマニュアルを参照してください。

▼ ハードウェアを取り付ける

1. スーパーユーザーで、ご使用のシステムに付属のマニュアルの指示に従ってシステムを停止します。次に、コンピュータの電源を切り、電源コードを外してコンピュータのカバーを取り外します。
2. 使用されていない PCI スロット (64 ビット、66 MHz のスロットを推奨) を探します。
3. 手首に静電気防止用リストストラップを装着し、もう一方の端をアースされた金属面に接続します。
4. プラスのねじ回しを使用して、PCI スロットのカバーからねじを取り外します。
手順 5 で留め具を固定するために、取り外したねじをとっておきます。
5. Sun Crypto Accelerator 1000 ボードの端の部分だけを持ってビニール袋から取り出し、PCI スロットに挿入して、背面留め具をねじで固定します。
6. コンピュータのカバーを元の位置に取り付け、電源コードを接続してシステムの電源を入れます。
7. `ok` プロンプトで `show-devs` コマンドを実行して、ボードが正しく取り付けられていることを確認します。

```
ok show-devs
. . .
/pci@1f,2000/pci108e,5455@1
/pci@1f,4000/pci108e,5455@5
. . .
```

`/pci@1f,2000/pci108e,5455@n` の行は、ボードが取り付けられ、システムによって認識されていることを示します。システムのボードごとに 1 つの行が表示されます。

Sun Crypto Accelerator 1000 ソフトウェアのインストール

Sun Crypto Accelerator 1000 ソフトウェアは、Sun Crypto Accelerator 1000 CD に含まれています。SunSolve Web サイトからパッチをダウンロードする必要がある場合があります。詳細は、5 ページの「必要なパッチ」を参照してください。

▼ ソフトウェアをインストールする

1. Sun 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、バージョン 1.0 ソフトウェアをすべて削除します。次のコマンドを使用して、バージョン 1.0 パッケージをすべて削除します。

```
# pkgrm SUNWcrys1 SUNWdcav SUNWdcar SUNWcrysu SUNWcrypu SUNWcrypr  
SUNWdcamn SUNWcrypm
```

2. システムに接続されている CD-ROM ドライブに、Sun Crypto Accelerator 1000 CD を挿入します。
 - システムで Sun Enterprise Volume Manager™ を実行している場合、CD-ROM は /cdrom/cdrom0 ディレクトリに自動的にマウントされます。
 - システムで Sun Enterprise Volume Manager を実行していない場合は、次のように入力して CD-ROM をマウントします。

```
# mount -F hsfs -o ro /dev/dsk/c0t6d0s2 /cdrom
```

/cdrom/cdrom0 ディレクトリには、次のファイルおよびディレクトリがあります。

表 2-1 /cdrom/cdrom0 ディレクトリにあるファイル

ファイルまたはディレクトリ	内容
Copyright	著作権ファイル (英語)
FR_Copyright	著作権ファイル (フランス語)
Docs	『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』 (このマニュアル)
Packages	次の Sun Crypto Accelerator 1000 のソフトウェアパッケージが含まれます。 SUNWcrypr 暗号化カーネルコンポーネント SUNWcrypu 暗号化管理ユーティリティおよびライブラリ SUNWcrysu Apache の SSL サポート (オプション) SUNWcrypm 暗号化管理マニュアルページ SUNWdcar DCA Crypto アクセラレータ (ルート) SUNWdcamn DCA Crypto アクセラレータマニュアルページ SUNWdcav DCA Crypto アクセラレータの SunVTS テスト (オプション) SUNWcrys1 SSL 開発ツールおよびライブラリ (オプション)

Web サーバーとして Apache を使用する場合に限り、SUNWcrysu パッケージをインストールします。

Apache Web サーバーのほかの (サポートされていない) バージョンと再接続する場合に限り、SUNWcrys1 パッケージをインストールします。

SunVTS テストを実行する場合に限り、SUNWdcav パッケージをインストールします。SUNWdcav パッケージをインストールする場合は、SunVTS 4.4 または 4.5、4.6、5.0 がインストールされている必要があります。

3. 次のように入力して、ソフトウェアパッケージをインストールします。

```
# cd /cdrom/cdrom0/Packages
# pkgadd -d .
```

4. `pkginfo` コマンドを実行して、ソフトウェアが適切にインストールされたことを確認します。

```
# pkginfo SUNWcrypr SUNWcrypu SUNWcrysl SUNWcrysu SUNWcrypm SUNWdcar SUNWdcamn
SUNWdcav
system SUNWcrypr   Cryptography Kernel Components
system SUNWcrypu   Cryptographic Administration Utility and Libraries
system SUNWcrysl   SSL Development Tools and Libraries
system SUNWcrysu   SSL Support for Apache
system SUNWcrypm   Cryptographic Administration Manual Pages
system SUNWdcar    DCA Crypto Accelerator (Root)
system SUNWdcamn   DCA Crypto Accelerator Manual Page
system SUNWdcav    SunVTS Test of DCA Crypto Accelerator
```

5. (任意) `prtconf` コマンドを実行して、ドライバが組み込まれたことを確認します。複数の Sun Crypto Accelerator 1000 ボードが取り付けられている場合は、次の例に示すように、複数の行が表示されます。

```
# prtconf
pci108e,5455, instance #0
pci108e,5455, instance #1
```

6. (任意) `modinfo` コマンドを実行して、読み込まれたモジュールを確認します。

ただし、`kcl` および `cryptio` は、実際に Sun Crypto Accelerator 1000 ボードで暗号化演算を実行するまで読み込まれないため表示されません。

```
# modinfo | grep Crypto
130 1033e946 6df0 79 1 cryptio (Cryptographic IOCTL v1.58)
131 1030240c 2d93 - 1 kcl (Cryptographic Library v1.64)
132 10313ac8 131e - 1 kcp_i (Crypto Provider Interface v1.27)
135 103178be 8684 82 1 dca (PCI Crypto Accelerator v1.156)
```

ディレクトリおよびファイル

表 2-2 に、Sun Crypto Accelerator 1000 ソフトウェアのインストール時に、デフォルトで作成されるディレクトリを示します。

表 2-2 Sun Crypto Accelerator 1000 のディレクトリ

ディレクトリ	内容
/etc/opt/SUNWconn/crypto/realms	領域およびユーザーデータ
/opt/SUNWconn/crypto/bin	アプリケーション実行可能ファイル
/opt/SUNWconn/crypto/lib	アプリケーションライブラリ
/opt/SUNWconn/crypto/sbin	静的にリンクされた実行可能ファイル

図 2-1 に、これらのディレクトリおよびファイルの階層を示します。

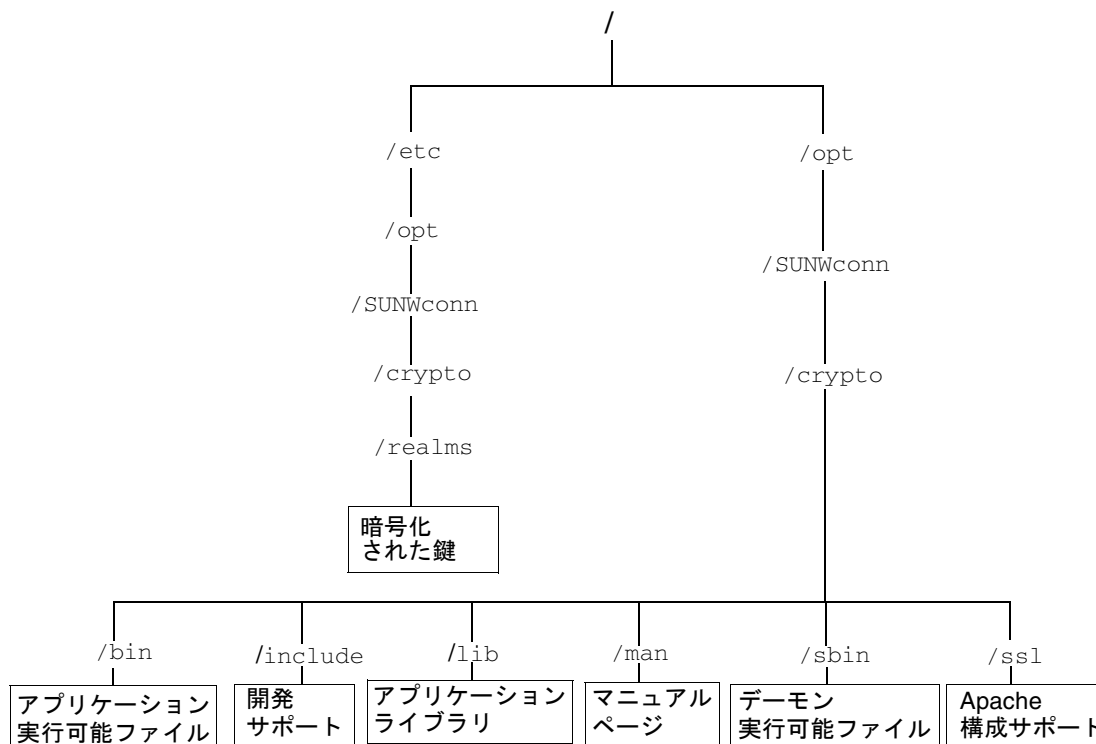


図 2-1 Sun Crypto Accelerator 1000 ディレクトリおよびファイル

ソフトウェアの削除

領域を作成した場合は、ソフトウェアを削除する前にその領域を削除する必要があります。詳細は、66 ページの「領域を削除する」を参照してください。領域を作成しなかった場合は、領域を削除する手順を省略できます。現在使用中の領域は削除できません。領域への参照を解放するには、Web サーバーか管理サーバー、またはその両方を停止する必要がある場合があります。



注意 – Sun Crypto Accelerator 1000 ソフトウェアを削除する前に、Sun Crypto Accelerator 1000 ボードで使用可能にした Web サーバーを使用不可にする必要があります。Web サーバーを使用不可にしないでソフトウェアを削除すると、Web サーバーが機能しなくなります。

▼ ソフトウェアを削除する

- スーパーユーザーで `pkgrm` コマンドを使用して、ユーザーがインストールしたソフトウェアパッケージだけを削除します。



注意 – インストールされているパッケージは、次に示す順に削除する必要があります。この順にパッケージを削除しないと、依存警告が発生し、カーネルのモジュールが読み込まれたままになります。

すべてのパッケージがインストールされている場合は、次の順に削除します。

```
# pkgrm SUNWcrys1 SUNWdcav SUNWdcar SUNWcrys2 SUNWcrypu SUNWcrypr
SUNWdcamn SUNWcrypm
```

注 – Sun Crypto Accelerator 1000 ボード用の SunVTS テスト (SUNWdcav) をインストールまたは削除したあとで、これまでも SunVTS を実行していた場合は、システムを再プローブして、使用可能なテストを更新する必要がある場合があります。詳細は、SunVTS のマニュアルを参照してください。

第3章

iPlanet Web サーバーでのボードの使用可能化

この章では、iPlanet Web サーバーで Sun Crypto Accelerator 1000 ボードを使用可能にする方法について説明します。この章は、次の節で構成されます。

- 15 ページの「パスワード」
- 16 ページの「領域およびユーザーの作成」
- 18 ページの「iPlanet Web サーバーの使用可能化の概要」

パスワード

iPlanet Web サーバー (iWS) を使用可能にする過程では、いくつかのパスワードの入力が要求されます。表 3-1 に、各パスワードに関する説明を示します。これらのパスワードは、この章全体で使用されます。使用するパスワードが不明な場合は、表 3-1 を参照してください。

表 3-1 iPlanet Web サーバーに必要なパスワード

パスワードの種類	説明
iWS 管理サーバー	iPlanet 管理サーバーを起動するために必要です。このパスワードは、iPlanet の設定中に割り当てられます。
Web サーバーの認証データベース	セキュリティ保護されたモードで動作しているとき、内部の暗号化モジュールを起動するために必要です。このパスワードは、iPlanet Web サーバーの管理サーバーを使用して認証データベースを作成するときに割り当てられます。また、このパスワードは、内部の暗号化モジュールで証明書を要求およびインストールするときにも必要です。
システム管理者	secadm の特権操作を行うときに必要です。このパスワードは、root (または Solaris ホストのもう 1 つの UID ゼロアカウント) 用の、UNIX ホストのパスワードです。
<i>user@realm-name</i>	セキュリティ保護されたモードで動作しているとき、Sun Crypto Accelerator 1000 モジュールを起動するために必要です。このパスワードは、secadm を使用して領域にユーザーを作成するときに割り当てられます。また、このパスワードは、 <i>user@realm-name</i> 暗号化モジュールで証明書を要求およびインストールするときにも必要です。

領域およびユーザーの作成

iPlanet Web サーバーでボードを使用可能にする前に、まず領域を設定して生成する必要があります。まだ領域の作成および設定を行っていない場合は、1 つ以上の領域および 1 人以上のユーザーを設定する必要があります。領域については、付録 A を参照してください。

▼ 領域およびユーザーを作成する

1. Sun Crypto Accelerator 1000 ツールのディレクトリが検索パスに指定されていない場合は、たとえば次のように、検索パスにディレクトリを指定します。

```

$ PATH=$PATH:/opt/SUNWconn/crypto/bin
$ export PATH

```

2. `secadm` ユーティリティーにアクセスします。

```
$ secadm
```

3. `secadm` ユーティリティーを使用して、新しい領域を作成します。

```
secadm> create realm=realm-name
System Administrator Login Required
Login: root
Password:
Realm realm-name created successfully.
```

4. 領域にユーザーを作成します。

作成するユーザー名は、Sun Crypto Accelerator 1000 のドメイン内だけで認識されます。Web サーバードプロセスが使用している UNIX のユーザー名と同一である必要はありません。ユーザーを作成する前に、まず現在の作業領域を設定して、システム管理者でログインする必要があります。

ユーザーを作成する前に、ユーザーを作成する領域を設定する必要があります。

```
secadm> set realm=realm-name
secadm{realm-name}> su
System Administrator Login Required
Login: root
Password:
secadm{root@realm-name}#
```

5. 領域にユーザーが 1 人だけ必要な場合は、ユーザー名 `nobody` を使用してスロットファイルの設定を省略できます。詳細は、55 ページの「スロットファイル」を参照してください。

```
secadm{root@realm-name}# create user=nobody
Initial password:
Confirm password:
User nobody created successfully.
```

Web サーバードの起動時に認証を行う際に、このパスワードを使用する必要があります。このパスワードの形式は、`user@realm-name` です。



注意 – 入力したパスワードを覚えておく必要があります。パスワードを忘れると、鍵にアクセスできなくなります。パスワードを忘れた場合、これを検索する方法はありません。

6. `secadm` を終了します。

```
secadm{root@realm-name}# exit
```

iPlanet Web サーバーの使用可能化の概要

iPlanet Web サーバーを使用可能にするには、次の手順を完了する必要があります。これらの手順の詳細は、このあとの 2 つの章で説明します。

1. iPlanet Web サーバーをインストールします。
2. 認証データベースを作成します。
3. 証明書を要求します。
4. 証明書をインストールします。
5. iPlanet Web サーバーを構成します。



注意 – これらの手順は、記載されている順に実行してください。別の順番で実行すると、iPlanet Web サーバーが正しく構成されないことがあります。

- iPlanet Web Server 4.1 を使用している場合は、第 4 章に進みます。
- iPlanet Web Server 6.0 を使用している場合は、第 5 章に進みます。

第4章

iPlanet Web Server 4.1 のインストールおよび構成

この章では、iPlanet Web Server 4.1 のインストールおよび構成方法について説明します。この章は、次の節で構成されます。

- 19 ページの「iPlanet Web Server 4.1 のインストール」
 - 26 ページの「iPlanet Web Server 4.1 の構成」
-

iPlanet Web Server 4.1 のインストール

ここで説明する手順は、記載されている順に実行する必要があります。iPlanet Web サーバーの使用方法については、iPlanet Web サーバーのマニュアルを参照してください。

▼ iPlanet Web Server 4.1 をインストールする

1. iPlanet Web Server 4.1 ソフトウェアをダウンロードします。

次の URL から、Web サーバーのソフトウェアを入手できます。

<http://www.iplanet.com>

2. Web サーバーをインストールします。

各手順には例が 1 つ示されていますが、例とは異なる設定で Web サーバーを構成することもできます。サーバーのデフォルトのパス名は、`/usr/netscape/server4` です。

iPlanet Web サーバーのインストール時には、デフォルトのパスを使用します。このマニュアルでは、このデフォルトのパスを使用します。異なる場所にインストールする場合は、インストール先を控えておいてください。

3. setup プログラムを実行します。
4. インストールスクリプトで表示されるプロンプトに応答します。

手順を簡単にするために、次のプロンプト以外はデフォルトの設定を使用することができます。

 - a. 使用許諾条件に同意する場合は、yes と入力します。
 - b. 完全指定の *hostname.domain* を入力します。
 - c. iWS 管理サーバーのパスワードを 2 回入力します。
 - d. プロンプトが表示されたら、Return キーを押します。

▼ 認証データベースを作成する

1. 管理サーバーを起動します。

iPlanet Web Server 4.1 を起動するには、設定要求として startconsole を実行する代わりに、次のコマンドを実行します。

```
# /usr/netscape/server4/https-admserv/start
iPlanet-WebServer-Enterprise/4.1SP9 BB1-08/23/2001 05:50
startup: listening to http://hostname.domain, port 8888 as root
```

応答メッセージに、サーバーに接続するための URL が表示されます。

2. Web ブラウザを開いて次のように入力し、iPlanet 管理サーバーを起動します。

```
http://hostname.domain:admin_port
```

ポップアップウィンドウが表示されるので、setup の実行時に選択した iWS 管理サーバーのユーザー名およびパスワードを入力します。

注 – iPlanet Web サーバーの設定時にデフォルトの設定を使用した場合は、ユーザー ID または iWS 管理サーバーのユーザー名に admin と入力してください。

3. 「OK」をクリックします。
4. Web サーバーのインスタンスに対する認証データベースを作成します。

複数の Web サーバーのインスタンスでセキュリティーを有効にする場合は、各 Web サーバーのインスタンスで、手順 1 ~ 4 を繰り返します。

注 - 管理サーバーで SSL を実行する場合も、認証データベースの設定処理は同様です。詳細は、iPlanet のマニュアルを参照してください。

- a. 管理サーバーの「Servers」タブをクリックします。
 - b. サーバーを選択して、「Manage」ボタンをクリックします。
 - c. ページの上部にある「Security」タブをクリックして、「Create Database」リンクを選択します。
 - d. 2 つのダイアログボックスに Web サーバーの認証データベースのパスワードを入力して、「OK」をクリックします。
8 文字以上のパスワードを選択してください。このパスワードは、iPlanet Web サーバーがセキュリティー保護されたモードで動作するときに、内部の暗号化モジュールを起動するために使用されます。
5. 次のスクリプトを実行して、Sun Crypto Accelerator 1000 ボードを使用可能にします。

```
# /opt/SUNWconn/crypto/bin/sslconfig
```

このスクリプトでは、Web サーバーを選択するためのプロンプトが表示され、iPlanet Web サーバーまたは Apache Web サーバー用の Sun Crypto Accelerator 1000 暗号化モジュールがインストールされます。その後、構成ファイルが更新され、Sun Crypto Accelerator 1000 ボードが使用可能になります。

6. 1 を入力して Enter を押し、iPlanet Web サーバーで SSL を使用するように構成します。

```
Sun Crypto Accelerator Installation
-----
This script will install the Sun Crypto Accelerator
cryptographic modules for iPlanet Web Server
or Apache.

Please select the type of web server you wish to configure
to use the Sun Crypto Accelerator:
-----
1. Configure iPlanet Web Server for SSL
2. Configure Apache for SSL
3. Work with iPlanet and Apache keys
Your selection (0 to quit): 1
```

7. プロンプトが表示されたら Web サーバーのルートディレクトリのパスを入力し、Enter を押します。

```
Please enter the full path of the web server
root directory [/usr/netscape/server4]: /usr/netscape/server4
```

8. 次の処理に進む場合は、y を入力して Enter を押します。

```
This script will update your iPlanet Web Server installation
in /usr/netscape/server4 to use the Sun Crypto Accelerator
You will need to restart your admin server after this has
completed.
Ok to proceed? [Y/N]: y

Using database directory /usr/netscape/server4/alias...
Module "Sun Crypto Accelerator" added to database.
/usr/netscape/server4 has been configured to use
the Sun Crypto Accelerator.

<Press ENTER to continue>
```

9. 処理を終了する場合は、0 を入力します。

▼ サーバーの証明書を生成する

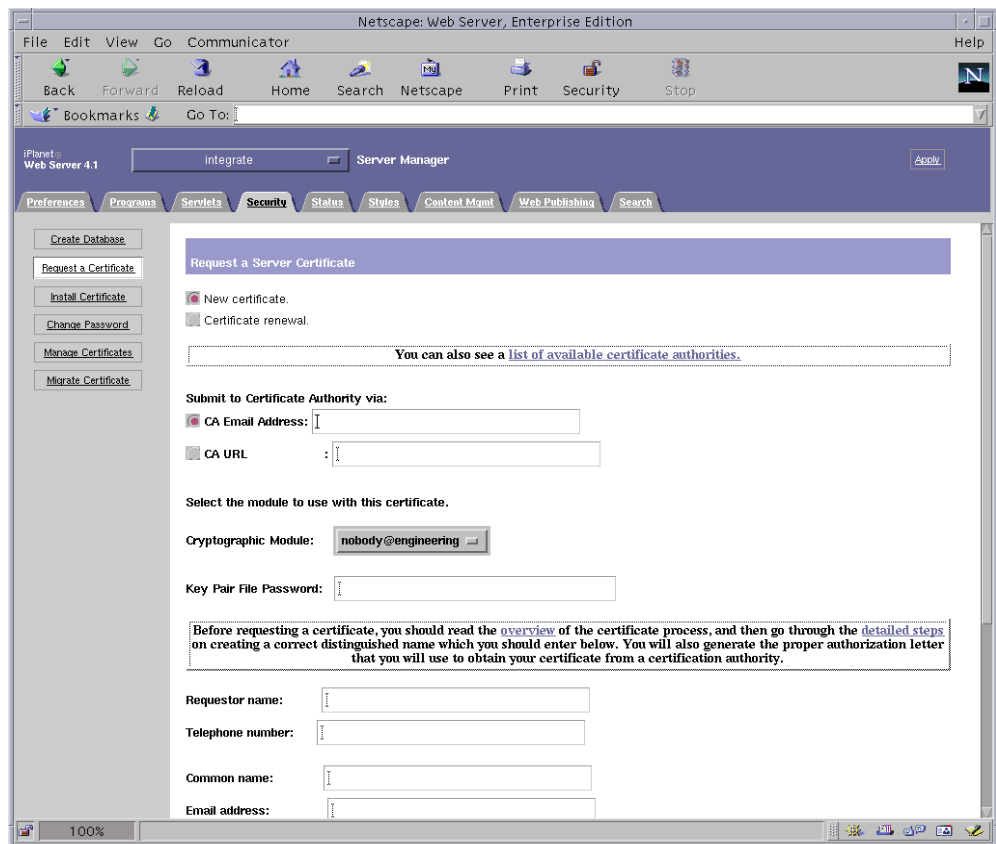
1. 次のコマンドを入力して、管理サーバーを再起動します。

```
# /usr/netscape/server4/https-admserv/stop
# /usr/netscape/server4/https-admserv/start
```

2. サーバーの証明書を要求するには、ページの上にある「Security」タブをクリックします。

「Create Trust Database」ウィンドウが表示されます。

3. ページの左側の「Request a Certificate」リンクを選択します。



4. 証明書要求を生成するための書式に、次の情報を入力します。

a. 「New Certificate」を選択します。

証明書要求を Web から利用できる認証局または登録機関に直接送信できる場合は、「CA URL」リンクを選択します。それ以外の場合は、「CA Email Address」を選択し、証明書要求を受け取る電子メールアドレスを入力します。

b. 使用する「Cryptographic Module」を選択します。

このプルダウンメニューには、各領域ごとに固有のエントリがあります。正しい領域を選択していることを確認してください。Sun Crypto Accelerator 1000 を使用するには、`user@realm-name` の形式のモジュールを選択する必要があります。

c. 「Key Pair File Password」ダイアログボックスに、鍵を所有する `user@realm-name` に対するパスワードを入力します。

d. 次の各フィールドに、適切な情報を入力します。

- Requestor Name : 証明書の要求者の連絡先
- Telephone Number : 証明書の要求者の連絡先
- Common Name : ブラウザで *hostname.domain* 形式で入力する Web サイトのドメイン名
- Email Address : 証明書の要求者の連絡先
- Organization : 証明書に記載される組織の名称
- Organizational Unit : (任意) 証明書に記載される部門の名称
- Locality : (任意) 組織の所在地の市区町村。入力されている場合は、証明書に記載されます。
- State : (任意) 組織の所在地の都道府県の正式名称
- Country : 2 文字の ISO 国別記号 (たとえば、米国の場合は US)

e. 「OK」 ボタンをクリックして、情報を送信します。

5. 認証局を使用して、証明書を生成します。

- 証明書要求を「CA URL」に送信するように選択した場合は、証明書要求は自動的に認証局に送信されます。
- 「CA Email Address」を選択した場合は、受け取った証明書要求のメールのヘッダーと本文をコピーして、認証局に提出します。

6. 証明書が生成されたら、ヘッダーと本文をクリップボードにコピーします。

証明書は証明書要求とは異なります。通常はテキスト形式で提供されます。

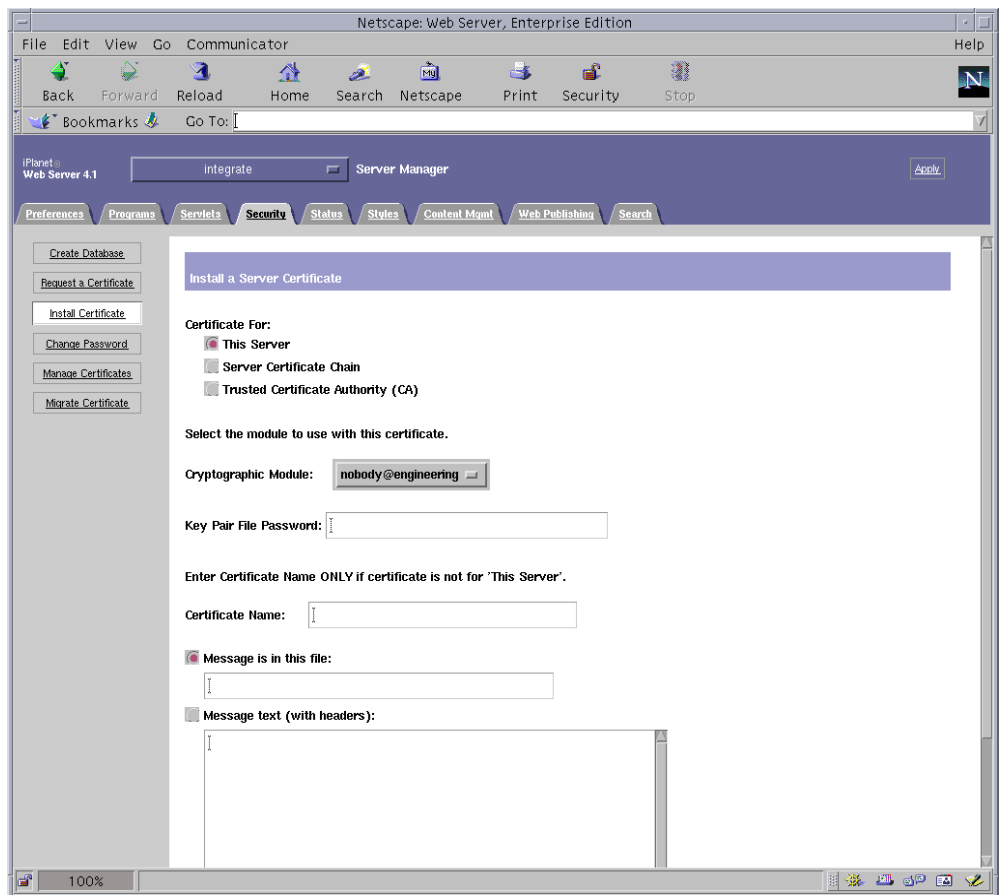
▼ サーバーの証明書をインストールする

1. ページの左側の「Install Certificate」リンクを選択します。

認証局によって証明書要求が承認され証明書が発行されたら、iPlanet Web サーバーに証明書をインストールする必要があります。

2. 「Security」タブを選択します。

3. ページの左側の「Install Certificate」リンクを選択します。



4. 証明書をインストールするための書式に、次のように入力します。

- Certificate For : 「This Server」を選択します。
- Cryptographic Module : 適切な `user@realm-name` を選択します。
- Key Pair File Password : 事前に生成した鍵を所有する `user@realm-name` に対するパスワードを入力します。
- Certificate Name : ほとんどの場合、この部分は空白にします。ここに名前を指定すると、Web サーバーで SSL サポートを有効にしたときに、証明書および鍵へのアクセスに使用する名前が、この名前に変更されます。

5. 「Message Text (with headers)」を選択し、あらかじめコピーしておいた証明書のヘッダーと本文をペーストします。

6. ページの下部にある「OK」ボタンをクリックします。

7. 認証局からコピーした証明書を「Message」ボックスにペーストします。
証明書に関する基本的な情報が表示されます。
8. 表示された内容に誤りがなければ、「Add Server Certificate」ボタンをクリックします。
サーバーの再起動を求めるメッセージが画面に表示されます。Web サーバーのインスタンスが完全に停止していた場合は、再起動は必要ありません。また、Web サーバーで SSL を使用するように構成する必要があることも通知されます。次の手順に従って、Web サーバーを構成します。

iPlanet Web Server 4.1 の構成

Web サーバーおよびサーバーの証明書のインストールが完了しました。Web サーバーで SSL を使用できるように構成する必要があります。

▼ iPlanet Web Server 4.1 を構成する

1. メイン管理ページで、使用する Web サーバーのインスタンスを選択して、「Manage」をクリックします。
2. ページの上部にある「Preferences」タブが選択されていない場合は、このタブをクリックします。
3. ページの左側の「Encryption On/Off」リンクを選択します。
4. 暗号化をオンに設定します。
ダイアログボックスの「Port」フィールドが、SSL のデフォルトのポート番号である 443 に更新されます。必要に応じて、ポート番号を変更します。
5. 「OK」ボタンをクリックします。
6. 「Save」ボタンをクリックすると、この変更内容が適用されます。
Web サーバーが、セキュリティー保護されたモードで動作するように構成されました。

7. `/usr/netscape/server4/https-hostname/config/magnus.conf` ファイルを編集して、次の行を追加します。

```
CERTDefaultNickname user@realm-name:Server-Cert
```

hostname には、Web サーバーの名前が入ります。

デフォルトでは、手順 2 および手順 4 で生成した証明書の名前は、Server-Cert になります。名前が異なる場合は、Server-Cert の部分を実際の証明書の名前で置き換えます。

8. 管理するサーバーを選択して、ページの右上角にある「Apply」ボタンをクリックします。

これによって、管理サーバーに変更内容が適用されます。

9. 「Load Configuration Files」ボタンをクリックして、`magnus.conf` ファイルに加えた変更を適用します。

サーバーの電源が入っていないときに「Apply Changes」ボタンをクリックすると、パスワードの入力を求めるポップアップウィンドウが表示されます。このポップアップウィンドウのサイズは変更できないため、変更内容を適用するときに問題がある場合があります。この問題には、次の 2 つの回避策があります。

- 代わりに「Load Configuration Files」をクリックします。
- Web サーバーを起動してから「Apply Changes」ボタンをクリックします。

10. Web サーバーのページの左側で「On/Off」リンクを選択します。

11. サーバーのパスワードを入力して、「OK」ボタンをクリックします。

1 つ以上のパスワードの入力を求めるプロンプトが表示されます。「Module Internal」プロンプトで、Web サーバーの認証データベースのパスワードを入力します。

「Module *user@realm-name*」プロンプトには、`secadm` コマンドを使用して *realm-name* に *user* を作成したときに設定したパスワードを入力します。

12. 次の URL で、SSL 対応の新しい Web サーバーを確認します。

`https://hostname.domain:server_port/`

デフォルトの *server_port* は、443 です。

第5章

iPlanet Web Server 6.0 のインストール および構成

この章では、iPlanet Web Server 6.0 で Sun Crypto Accelerator 1000 ボードを使用可能にする方法について説明します。この章は、次の節で構成されます。

- 29 ページの「iPlanet Web Server 6.0 のインストール」
 - 36 ページの「iPlanet Web Server 6.0 の構成」
-

iPlanet Web Server 6.0 のインストール

ここで説明する手順は、記載されている順に実行する必要があります。iPlanet Web サーバーの使用方法については、iPlanet Web サーバーのマニュアルを参照してください。

▼ iPlanet Web Server 6.0 をインストールする

1. iPlanet Web Server 6.0 ソフトウェアをダウンロードします。

次の URL から、Web サーバーのソフトウェアを入手できます。

<http://www.iplanet.com>

2. Web サーバーをインストールします。

各手順には例が 1 つ示されていますが、例とは異なる設定で Web サーバーを構成することもできます。サーバーのデフォルトのパス名は、`/usr/ipplanet/servers` です。

iPlanet Web サーバーのインストール時には、デフォルトのパスを使用します。このマニュアルでは、このデフォルトのパスを使用します。異なる場所にインストールする場合は、インストール先を控えておいてください。

3. setup プログラムを実行します。
4. インストールスクリプトで表示されるプロンプトに応答します。
手順を簡単にするために、次のプロンプト以外はデフォルトの設定を使用することができます。
 - a. 使用許諾条件に同意する場合は、yes と入力します。
 - b. 完全指定の *hostname.domain* を入力します。
 - c. iWS 管理サーバーのパスワードを 2 回入力します。
 - d. プロンプトが表示されたら、Return キーを押します。

▼ 認証データベースを作成する

1. 管理サーバーを起動します。
iPlanet Web サーバーを起動するには、設定要求として startconsole を実行する代わりに、次のコマンドを実行します。

```
# /usr/iplanet/servers/https-admserv/start
iPlanet-WebServer-Enterprise/6.0SP1 B08/20/2001 00:58
warning: daemon is running as super-user
[LS ls1] http://hostname.domain/port 8888 ready to accept requests
startup: server started successfully
```

応答メッセージに、サーバーに接続するための URL が表示されます。

2. Web ブラウザを開いて次のように入力し、iPlanet 管理サーバーを起動します。

```
http://hostname.domain:admin_port
```

ポップアップウィンドウが表示されるので、setup の実行時に選択した iWS 管理サーバーのユーザー名およびパスワードを入力します。

注 – iPlanet Web サーバーの設定時にデフォルトの設定を使用した場合は、ユーザー ID または iWS 管理サーバーのユーザー名に admin と入力してください。

3. 「OK」をクリックします。

4. Web サーバーのインスタンスに対する認証データベースを作成します。

複数の Web サーバーのインスタンスでセキュリティーを有効にする場合は、各 Web サーバーのインスタンスで、この手順を繰り返します。

注 – 管理サーバーで SSL を実行する場合も、認証データベースの設定処理は同様です。詳細は、iPlanet のマニュアルを参照してください。

- a. 管理サーバーの「Servers」タブをクリックします。
- b. サーバーを選択して、「Manage」ボタンをクリックします。
- c. ページの上部にある「Security」タブをクリックして、「Create Database」リンクを選択します。
- d. 2 つのダイアログボックスに Web サーバーの認証データベースのパスワードを入力して、「OK」をクリックします。
8 文字以上のパスワードを選択してください。このパスワードは、iPlanet Web サーバーがセキュリティー保護されたモードで動作するときに、内部の暗号化モジュールを起動するために使用されます。

5. 次のスクリプトを実行して、Sun Crypto Accelerator 1000 ボードを使用可能にします。

```
# /opt/SUNWconn/crypto/bin/sslconfig
```

このスクリプトでは、Web サーバーを選択するためのプロンプトが表示され、iPlanet Web サーバーまたは Apache Web サーバー用の Sun Crypto Accelerator 1000 暗号化モジュールがインストールされます。その後、構成ファイルが更新され、Sun Crypto Accelerator 1000 ボードが使用可能になります。

6. 1 を入力して Enter を押し、iPlanet Web サーバーで SSL を使用するよう構成します。

```
Sun Crypto Accelerator Installation
-----
This script will install the Sun Crypto Accelerator
cryptographic modules for iPlanet Web Server
or Apache.

Please select the type of web server you wish to configure
to use the Sun Crypto Accelerator:
-----
1. Configure iPlanet Web Server for SSL
2. Configure Apache for SSL
3. Work with iPlanet and Apache keys
Your selection (0 to quit): 1
```

7. プロンプトが表示されたら Web サーバーのルートディレクトリのパスを入力し、Enter を押します。

```
Please enter the full path of the web server
root directory [/usr/iplanet/servers]: /usr/iplanet/servers
```

8. 次の処理に進む場合は、y を入力して Enter を押します。

```
This script will update your iPlanet Web Server installation
in /usr/iplanet/servers to use the Sun Crypto Accelerator
You will need to restart your admin server after this has
completed.
Ok to proceed? [Y/N]: y

Using database directory /usr/iplanet/servers/alias...
Module "Sun Crypto Accelerator" added to database.
/usr/iplanet/servers has been configured to use
the Sun Crypto Accelerator.

<Press ENTER to continue>
```

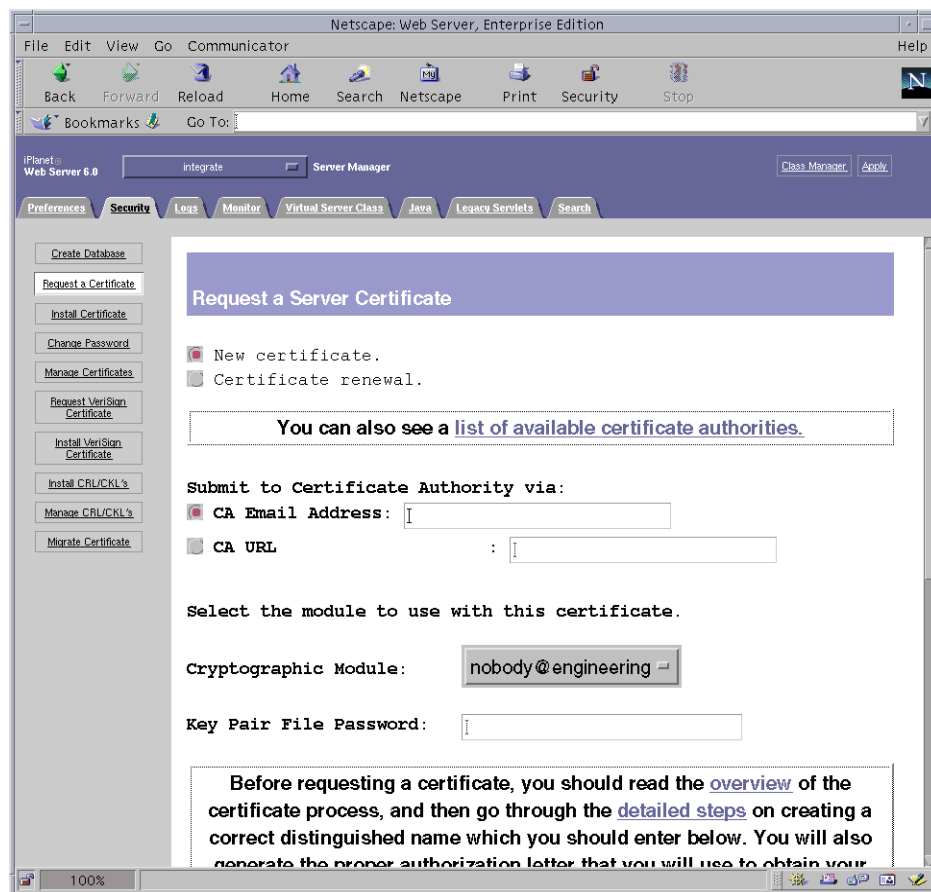
9. 処理を終了する場合は、0 を入力します。

▼ サーバーの証明書を生成する

1. 次のコマンドを入力して、管理サーバーを再起動します。

```
# /usr/iplanet/servers/https-admserv/stop  
# /usr/iplanet/servers/https-admserv/start
```

2. サーバーの証明書を要求するには、ページの上にある「Security」タブをクリックします。
「Create Trust Database」ウィンドウが表示されます。
3. ページの左側の「Request a Certificate」リンクを選択します。



4. 証明書要求を生成するための書式に、次の情報を入力します。

a. 「New Certificate」を選択します。

証明書要求を Web から利用できる認証局または登録機関に直接送信できる場合は、「CA URL」リンクを選択します。それ以外の場合は、「CA Email Address」を選択し、証明書要求を受け取る電子メールアドレスを入力します。

b. 使用する「Cryptographic Module」を選択します。

このプルダウンメニューには、各領域ごとに固有のエントリがあります。正しい領域を選択していることを確認してください。Sun Crypto Accelerator 1000 を使用するには、*user@realm-name* の形式のモジュールを選択する必要があります。

c. 「Key Pair File Password」ダイアログボックスには、鍵を所有する *user@realm-name* に対するパスワードを入力します。

d. 次の各フィールドに、適切な情報を入力します。

- Requestor Name : 証明書の要求者の連絡先
- Telephone Number : 証明書の要求者の連絡先
- Common Name : ブラウザで *hostname.domain* 形式で入力する Web サイトのドメイン名
- Email Address : 証明書の要求者の連絡先
- Organization : 証明書に記載される組織の名称
- Organizational Unit : (任意) 証明書に記載される部門の名称
- Locality : (任意) 組織の所在地の市区町村。入力されている場合は、証明書に記載されます。
- State : (任意) 組織の所在地の都道府県の正式名称
- Country : 2 文字の ISO 国別記号 (たとえば、米国の場合は US)

e. 「OK」ボタンをクリックして、情報を送信します。

5. 認証局を使用して、証明書を生成します。

- 証明書要求を「CA URL」に送信するように選択した場合は、証明書要求は自動的に認証局に送信されます。
- 「CA Email Address」を選択した場合は、受け取った証明書要求のメールのヘッダーと本文をコピーして、認証局に提出します。

6. 証明書が生成されたら、ヘッダーと本文をクリップボードにコピーします。

証明書は証明書要求とは異なります。通常はテキスト形式で提供されます。

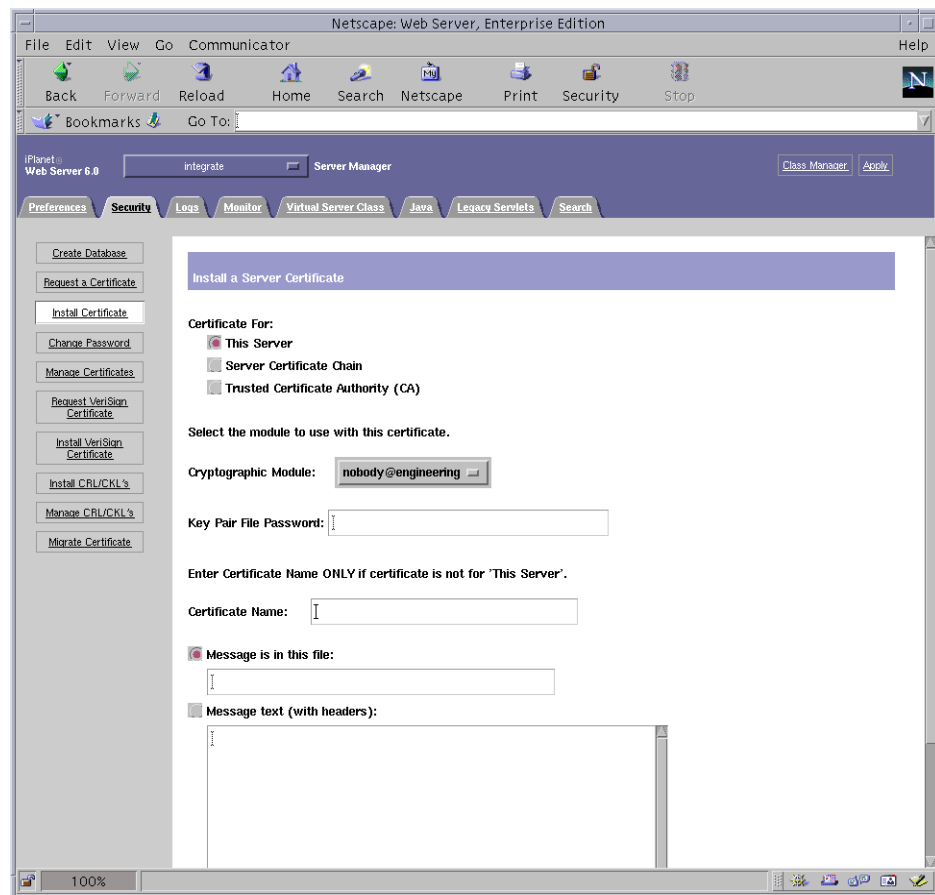
▼ サーバーの証明書をインストールする

1. ページの左側の「Install Certificate」リンクを選択します。

認証局によって証明書要求が承認され証明書が発行されたら、iPlanet Web サーバーに証明書をインストールする必要があります。

2. 「Security」タブを選択します。

3. ページの左側の「Install Certificate」リンクを選択します。



4. 証明書をインストールするための書式に、次のように入力します。

- Certificate For : 「This Server」を選択します。
- Cryptographic Module : 適切な `user@realm-name` を選択します。
- Key Pair File Password : 事前に生成した鍵を所有する `user@realm-name` に対するパスワードを入力します。
- Certificate Name : ほとんどの場合、この部分は空白にします。ここに名前を指定すると、Web サーバーで SSL サポートを有効にしたときに、証明書および鍵へのアクセスに使用する名前が、この名前に変更されます。

5. 「Message Text (with headers)」を選択し、あらかじめコピーしておいた証明書のヘッダーと本文をペーストします。

6. ページの下部にある「OK」ボタンをクリックします。

7. 認証局からコピーした証明書を「Message」ボックスにペーストします。
証明書に関する基本的な情報が表示されます。
8. 表示された内容に誤りがなければ、「Add Server Certificate」ボタンをクリックします。
サーバーの再起動を求めるメッセージが画面に表示されます。Web サーバーのインスタンスが完全に停止していた場合は、再起動は必要ありません。また、Web サーバーで SSL を使用するように構成する必要があることも通知されます。次の手順に従って、Web サーバーを構成します。

iPlanet Web Server 6.0 の構成

Web サーバーおよびサーバーの証明書のインストールが完了しました。Web サーバーで SSL を使用できるように構成する必要があります。

▼ iPlanet Web Server 6.0 を構成する

1. ページの上部にある「Preferences」タブをクリックします。
2. ページの左側の「Edit Listen Sockets」リンクを選択します。
中央の枠に、その Web サーバーインスタンスに設定されているすべての待機ソケットが一覧表示されます。
 - a. 次のフィールドを変更します。
 - Port : SSL 対応 Web サーバーを実行するポートを設定します。通常は、ポート 443 です。
 - Security : オンに設定します。
 - b. 「OK」ボタンをクリックして、変更内容を適用します。
「Edit Listen Sockets」ページのセキュリティーフィールドに、「Attributes」リンクが表示されます。
3. 「Attributes」リンクをクリックします。
4. *user@realm-name* パスワードを入力して、システムで *user@realm-name* を認証します。

5. ポップアップウィンドウで、SSL の設定を選択します。

「Cipher Default」または「SSL2」、「SSL3/TLS」を選択できます。「Cipher Default」を選択した場合、デフォルトの設定は表示されません。「SSL2」または「SSL3/TLS」を選択した場合は、使用可能にするアルゴリズムを選択する必要があります。
6. `user@realm-name` のあとに `:Server-Cert` (または実際に選択した証明書の名前) が付いた形式で証明書を選択します。

「Certificate Name」フィールドには、該当する `user@realm-name` が所有する鍵だけが表示されます。
7. 証明書を選択し、セキュリティーに関する設定をすべて確認したら、「OK」ボタンをクリックします。
8. サーバーを起動する前に、変更内容を有効にする場合は、右上の角にある「Apply」リンクをクリックします。
9. 「Load Configuration Files」リンクをクリックして、変更内容を適用します。

Web サーバーのインスタンスを起動できるページに切り替わります。

サーバーの電源が入っていないときに「Apply Changes」ボタンをクリックすると、パスワードの入力を求めるポップアップウィンドウが表示されます。このポップアップウィンドウのサイズは変更できないため、変更内容を適用するときに問題がある場合があります。

この問題には、次の 2 つの回避策があります。

 - 代わりに「Load Configuration Files」をクリックします。
 - Web サーバーを起動してから「Apply Changes」ボタンをクリックします。
10. 要求されたパスワードをダイアログボックスに入力して、サーバーを起動します。

1 つ以上のパスワードの入力を求めるプロンプトが表示されます。「Module Internal」プロンプトで、Web サーバーの認証データベースのパスワードを入力します。
11. 「Module `user@realm-name`」プロンプトには、`secadm` コマンドを使用して `realm-name` に `user` を作成したときに設定したパスワードを入力します。
12. 次の URL で、SSL 対応の新しい Web サーバーを確認します。

`https://hostname.domain:server_port/`

デフォルトの `server_port` は、443 です。

第6章

Apache Web サーバーの使用可能化

この章では、Apache Web サーバーで Sun Crypto Accelerator 1000 ボードを使用可能にする方法について説明します。この章は、次の節で構成されます。

- 39 ページの「Apache Web サーバーの使用可能化」
- 42 ページの「証明書の作成」

Apache Web サーバーの使用可能化

Apache Web Server 1.3.12 は、Solaris 8 7/01 オペレーティング環境に付属しています。Apache Web Server 1.3.22 は、Solaris 9 オペレーティング環境に付属しています。この章では、Apache Web サーバーのこれらのリリースについて説明します。Apache Web サーバーの使用方法については、Apache Web サーバーのマニュアルを参照してください。

▼ Apache Web サーバーを使用可能にする

1. httpd 構成ファイルを作成します。

Solaris システムでは、通常、httpd.conf-example ファイルが /etc/apache ディレクトリにあります。このファイルをテンプレートとして使用できます。次のように、ファイルをコピーします。

```
# cp /etc/apache/httpd.conf-example /etc/apache/httpd.conf
```

2. http.conf ファイルの ServerName の部分を、使用するサーバー名で置き換えます。

3. `sslconfig` を開始します。

```
# /opt/SUNWconn/crypto/bin/sslconfig
```

4. 2 を選択して、Apache Web サーバーで SSL を使用するよう構成します。

```
Sun Crypto Accelerator Installation
-----
This script will install the Sun Crypto Accelerator
cryptographic modules for iPlanet Web Server
or Apache.

Please select the type of web server you wish to configure
to use the Sun Crypto Accelerator:
-----
1. Configure iPlanet Web Server for SSL
2. Configure Apache for SSL
3. Work with iPlanet and Apache keys

Your selection (0 to quit): 2
```

5. Apache のバイナリファイルが存在するディレクトリを指定します。
Solaris システムでは、通常、`/usr/apache` ディレクトリにあります。

```
Please enter the directory where the Apache
binaries and libraries exist [/usr/apache]: /usr/apache
```

6. Apache の構成ファイルの位置を指定します。
Solaris システムでは、通常、`/etc/apache` ディレクトリです。

```
Please enter the directory where the Apache
configuration files exist [/etc/apache]: /etc/apache
```

7. システムに RSA 鍵ペアを作成します。

ここで鍵ペアを作成しない場合は、あとで `sslconfig` を使用して鍵を生成する必要があります。

```
Do you wish to create a new RSA keypair and certificate request?
[Y/N]:
```

この質問に `No` と入力した場合は、42 ページの「証明書を作成する」に進みます。

8. 鍵を格納するディレクトリを指定します。

そのディレクトリが存在しない場合は、作成されます。

```
Where would you like the keys stored? [/etc/apache/keys]:
/etc/apache/keys
```

9. 鍵素材の基本名を選択します。

この名前には、鍵ファイルおよび証明書要求ファイル、証明書ファイルをそれぞれ区別できるように、異なる接尾辞が付けられます。

```
Please choose a base name for the key and request file:
```

10. 512 ~ 2048 ビットの範囲で鍵長を指定します。

ほとんどの Web サーバーアプリケーションでは、1024 ビットで十分に強力ですが、必要に応じて、より強力な鍵を選択することもできます。

```
What size would you like the RSA key to be [1024]? 1024
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
```

11. PEM パスフレーズを作成します。

このパスフレーズは、鍵素材を保護します。強力なパスフレーズを選択する必要がありますが、忘れないようにしてください。パスフレーズを忘れると、鍵にアクセスできなくなります。

```
Enter PEM pass phrase:
Verifying password - Enter PEM pass phrase:
```



注意 – 入力したパスワードを覚えておく必要があります。パスワードを忘れると、鍵にアクセスできなくなります。パスワードを忘れた場合、これを検索する方法はありません。

証明書の作成

この節では、Apache Web サーバーで Sun Crypto Accelerator 1000 ボードを使用可能にするために必要な、証明書の作成方法について説明します。

▼ 証明書を作成する

1. 前述の節で作成した鍵を使用して、証明書要求を作成します。

まずパスワードを入力して、鍵にアクセスする必要があります。その後、次の各フィールドに適切な情報を入力します。

- **Country Name** : 2 文字の ISO 国別記号 (たとえば、米国の場合は US)。この情報は証明書に記載されます。入力必須です。
- **State or Province Name** : (任意) 組織の所在地の都道府県の正式名称を入力するか、ピリオド「.」を入力して **Return** キーを押します。
- **Locality** : (任意) 組織の所在地の市区町村。入力されている場合は、証明書に記載されます。
- **Organization Name** : 証明書に記載される組織の名称
- **Organizational Unit Name** : (任意) 証明書に記載される部門の名称
- **SSL Server Name** : ブラウザで入力する Web サイトのドメイン
- **Email Address** : 証明書の要求者の連絡先

次に、証明書フィールドの入力例を示します。

```
Enter PEM pass phrase:
You are about to be asked to enter information that will be incorporated into
your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:US
State or Province Name (full name) [Some-State]:.
Locality Name (eg, city) []:.
Organization Name (eg, company) []:Fictional Company, Inc.
Organizational Unit Name (eg, section) []:Online Sales Division
SSL Server Name (eg, www.company.com) []:www.fictional-company.com
Email Address []:admin@fictional-company.com
```

2. 指示に従って、`/etc/apache/httpd.conf` ファイルを変更します。

鍵および証明書ファイルに関する情報が表示されます。また、Sun Crypto Accelerator 1000 ソフトウェアで使用するために `/etc/apache/httpd.conf` ファイルを変更する方法も表示されます。

```
The keyfile is stored in /etc/apache/keys/base_name-key.pem.
The certificate request is in /etc/apache/keys/base_name-certreq.pem.

You will need to edit /etc/apache/httpd.conf for the following items:

You must specify the ports that Apache will listen to for
SSL connections, as well as for non-SSL connections. One
way to accomplish this is to add the following lines in
the Listen section:

Listen 80
Listen 443

In the LoadModule section, add the following:

LoadModule ssl_module /usr/apache/libexec/mod_ssl.so.version-number

In the AddModule section, add the following:

AddModule mod_ssl.c
```

注 - *version-number* には、ご使用の構成の正しいバージョン番号が表示されます。

3. VirtualHost の設定を選択しなかった場合は、SSLEngine および SSLCertificateFile、SSLCertificateKeyFile の各ディレクティブを httpd.conf ファイルの SSLPassPhraseDialog ディレクティブのすぐ上に指定します。

```
You may need a virtual host directive similar to
what is shown below:

<VirtualHost _default_:443>
    SSLEngine on
    SSLCertificateFile /etc/apache/keys/base_name-cert.pem
    SSLCertificateKeyFile /etc/apache/keys/base_name-key.pem
</VirtualHost>

You must add the following line after all of your VirtualHost
definitions:

SSLPassPhraseDialog exec:/opt/SUNWconn/crypto/bin/sslpassword

Other SSL-related directives and their explanations
can be found in the Sun Crypto Accelerator documentation.

Other Apache-related directives may need to be configured
in order to start your Apache Web Server. Please refer
to your Apache documentation.

<Press ENTER to continue>
```

39 ページの「Apache Web サーバーを使用可能にする」の手順 7 で No と入力した場合は、次に鍵素材を生成する方法が表示されます。

```
Since you did not create keys, you will need to
make sure that you have a key file and a certificate
file in place before enabling SSL for Apache.

You can create a new key file and certificate request
by selecting the "Generate a keypair and request a
certificate for Apache" option after choosing
"Work with iPlanet and Apache keys" from the
sslconfig main menu.
```

4. sslconfig を終了する場合は、0 を選択します。
5. /etc/apache/keys/*base_name*-certreq.pem (*base_name* は、39 ページの「Apache Web サーバーを使用可能にする」の手順 9 で指定した基本名) から証明書要求とヘッダーをコピーして、認証局に提出します。

6. 証明書が生成されたら、証明書ファイル

`/etc/apache/keys/base_name-cert.pem` を生成して、証明書をペーストします。

7. Apache Web サーバーを起動します。

ここでは、Apache のバイナリディレクトリが `/usr/apache/bin` であることを前提としています。実際のバイナリディレクトリが異なる場合は、正しいディレクトリ名を入力してください。

```
# /usr/apache/bin/apachectl start
```

8. PEM パスフレーズの入力を求めるプロンプトに対して、PEM パスフレーズを入力します。

9. ブラウザで次の URL を表示して、SSL 対応の新しい Web サーバーを確認します。

`https://server_name:server_port/`

デフォルトの `server_port` は、443 です。

第7章

診断および障害追跡

この章では、Sun Crypto Accelerator 1000 ソフトウェアの診断テストおよび障害追跡について説明します。この章は、次の節で構成されます。

- 47 ページの「SunVTS 診断ソフトウェア」
- 50 ページの「Sun Crypto Accelerator 1000 の障害追跡」

SunVTS 診断ソフトウェア

SunVTS テスト `dcatetest` は、SunVTS テストのコア制御部とユーザーインタフェースで動作し、Sun Crypto Accelerator 1000 ボードの診断を行います。`dcatetest` は、Sun Crypto Accelerator 1000 CD にパッケージ `SUNWdcav` として収録されています。また、SunVTS のコア制御部とユーザーインタフェースは、Solaris のサブリメント CD にパッケージ `SUNWvts` および `SUNWvtsx` として収録されています。

これらの診断テストの実行方法および監視方法については、SunVTS のマニュアルを参照してください。SunVTS のマニュアルは、ご使用のリリースの Solaris サプリメント CD の Solaris on Sun Hardware AnswerBook に収録されています。

注 – SunVTS は、Solaris のサブリメント CD から SunVTS パッケージをインストールした場合にだけ使用できます。

▼ dcatetest を実行する

1. スーパーユーザーで、SunVTS を起動します。

```
# /opt/SUNWvts/bin/sunvts
```

SunVTS の起動方法については、『SunVTS ユーザーマニュアル』を参照してください。

このあとの手順では、CDE ユーザーインターフェースを使用して SunVTS が起動されていることを前提としています。

2. SunVTS 診断のメインウィンドウで、「System Map」を「Logical」モードに設定します。

注 - 「Physical」モードもサポートされていますが、この手順では「Logical」モードを使用することを前提とします。

3. チェックボックスのチェックを外して、すべてのテストを使用不可にします。
4. 「Cryptography」のチェックボックスを選択し、「Cryptography」の「+」ボタンをクリックして、Cryptography グループのすべてのテストを表示します。
5. Cryptography グループの dcatetest 以外のチェックボックスのチェックを外します。
 - dcatetest が表示されている場合は、手順 6 に進みます。
 - dcatetest が表示されていない場合は、「Commands」ドロップダウンメニューから「Reprobe system」を選択して、システムをプローブして dcatetest を検索します。

具体的な手順については、SunVTS のマニュアルを参照してください。プローブが終了して dcatetest が表示されたら、手順 6 に進みます。

6. dcatetest のインスタンスを 1 つクリックし、右クリックおよびドラッグして「Test Parameter Options」を表示します。

このオプションは、dcatetest にだけ関係しています。詳細は、49 ページの「dcatetest のテストパラメータオプション」を参照してください。

7. 選択がすべて完了したら、「Within Instance」ドロップダウンメニューから「Apply」をクリックして dcatetest の選択したインスタンスを変更するか、「Across All Instances」ドロップダウンメニューから「Apply」をクリックして dcatetest のチェックしたインスタンスをすべて変更します。

これによって、ポップアップウィンドウが閉じられ、Sun Diagnostic のメインウィンドウに戻ります。

8. `dcatest` のインスタンスを1つクリックし、右クリックおよびドラッグして「Test Execution Options」を表示します。
「Options」ドロップダウンメニューをクリックしてから「Test Executions」をクリックする方法でも、「Test Execution Options」を表示できます。このオプションは、すべてのテストに影響する一般的な SunVTS 制御です。詳細は、SunVTS のマニュアルを参照してください。
9. 選択がすべて完了したら、「Apply」をクリックしてポップアップウィンドウを閉じ、Sun Diagnostic のメインウィンドウに戻ります。
10. 選択したテストを実行する場合は、「Start」をクリックします。
11. すべてのテストを中止する場合は、「Stop」をクリックします。

dcatest のテストパラメタオプション

表 7-1 に、`dcatest` サブテストの説明を示します。

表 7-1 `dcatest` サブテスト

テスト名	説明
3DES	3DES による大量データの暗号化をテストします。
RSA	RSA 公開鍵および非公開鍵をテストします。
DSA	DSA シグニチャー検査をテストします。
RNG	ランダム番号の生成をテストします。

dcatest コマンド行構文

`dcatest` を CDE 環境からではなく、コマンド行から実行する場合は、コマンド行の文字列にすべての引数を指定する必要があります。

32 ビットモードでは、`dcatest` へのパスは `/opt/SUNWvts/bin/` です。64 ビットモードでは、`dcatest` へのパスは `/opt/SUNWvts/bin/sparcv9/` です。

SunVTS の標準的なオプションは、すべて `dcatest` のコマンド行インタフェースでサポートされます。テスト固有のオプションは、`-o` 引数で指定します。

標準的なコマンド行引数の定義については、『SunVTS テストリファレンスマニュアル』を参照してください。`dcatest` は機能モードのテストであるため、`-f` を指定する必要があります。使用法のメッセージを表示する場合は `-u` を、VERBOSE (詳細) メッセージを表示する場合は `-v` を指定します。角括弧で囲まれている項目は、オプションのエントリを示します。

次に、スタンドアロンプログラムとして 32 ビットモードの `dcatest` を起動する例を示します。次のコマンドにより、`dca0` のすべてのサブテストが実行されます。

```
# /opt/SUNWvts/bin/dcatest -f -o dev=dca0,t1=3DES+RSA+DSA+RNG
```

次に、SunVTS インフラストラクチャーから 64 ビットモードの `dcatest` を起動する例を示します。次のコマンドにより、`dca2` の RSA テストが実行されます。

```
# /opt/SUNWvts/bin/sparcv9/dcatest -f -o dev=dca2,t1=RSA
```

コマンド行から `dcatest` を実行したときに、オプションの項目を省略した場合、その項目についてはデフォルトの動作になります (表 7-2 を参照)。

表 7-2 `dcatest` コマンド行構文

オプション	説明
<code>dev=dcan</code>	テストする装置のインスタンスを <code>dca0</code> 、 <code>dca2</code> などのように指定します。指定しない場合は、 <code>dca0</code> にデフォルト設定されます。
<code>t1=testlist</code>	実行するサブテストのリストを指定します。t1 には、サブテストをプラス (+) の文字で区切って指定します。サポートされているサブテストは、3DES および RSA、DSA、RNG のみです。そのため、 <code>t1=3DES+RSA+DSA+RNG</code> を指定すると、すべてのサブテストが実行されることとなります。また、 <code>t1=all</code> を入力して、すべてのテストを実行することもできます。サブテストを指定しない場合は、 <code>all</code> にデフォルト設定されます。

Sun Crypto Accelerator 1000 の障害追跡

Sun Crypto Accelerator 1000 がシステムのデバイス一覧に記載されているかどうかを判断する場合は、OpenBoot PROM (OBP) プロンプトで `show-devs` コマンドを入力してデバイス一覧を表示します。次の例のような Sun Crypto Accelerator 1000 ボードに関する行が、デバイス一覧に表示されます。

```
ok show-devs
. . .
/pci@1f,0/pci@1/pci108e,5455@2
. . .
```

この例では、pci108e,5455 が Sun Crypto Accelerator 1000 ボードのデバイスパスになります。このボードにはファームウェアがないため、OBP レベルの診断は使用できません。

Sun Crypto Accelerator 1000 ボードには、暗号化の活動を示す LED またはその他のインジケータはありません。ボード上で暗号化作業要求が実際に処理されているかどうかを確認する場合は、kstat(1M) コマンドを使用してデバイスの使用状況を表示します。

```
# kstat -m dca -i 0 -n dca0

module: dca                instance: 0
name:   dca0                class:   misc
3desbytes      3040
3desjobs       5
crttime        65.342725895
dsassign       0
dsaverify      0
rngbytes       10592
rngjobs        187
rngshalbytes   16328
rngshaljobs    327
rsapivate      9
rsapublic      0
snaptime       106956.467004482
```

kstat 情報を表示することによって、「jobs」と表示される暗号化要求が Sun Crypto Accelerator 1000 ボードに送信されているかどうかを確認できます。時間の経過とともに「jobs」の値が変化すれば、Sun Crypto Accelerator 1000 ボードに送信された暗号化作業要求はボードで高速処理されています。ボードに暗号化作業要求が送信されていない場合は、Web サーバーの具体的な構成を確認してください。

kstat(1M) によって返されたカーネルおよびドライバの統計値を解釈する必要はありません。これらの値は、フィールドサポートを容易にするためにドライバに保持されます。意味および実際の名称は、変更される可能性があります。

注 - /kernel/drv/dca.conf ファイルに nostats 属性が定義されている場合、統計情報の取得および表示は使用不可になります。この属性は、トラフィック分析を防止するために使用できます。

付録 A

iPlanet Web サーバーでの Sun Crypto Accelerator 1000 ボードの 管理

この付録では、iPlanet Web サーバーで管理される Sun Crypto Accelerator 1000 ボードのセキュリティー機能の概要について説明します。

注 – 領域を管理するには、ご使用のマシンのシステム管理者のアカウントを使用する必要があります。

この付録は、次の節で構成されます。

- 53 ページの「概念および用語」
- 62 ページの「領域の設定および管理」
- 66 ページの「ユーザーアカウントの設定および管理」

概念および用語

領域およびユーザーは、PKCS#11 インタフェースを介して Sun Crypto Accelerator 1000 ボードと通信する iPlanet Web サーバーなどのアプリケーションに対して作成する必要があります。

Sun Crypto Accelerator 1000 の説明では、ユーザーとは、暗号化鍵素材の一意の所有者のことです。各ユーザーは複数の鍵を所有できます。1 人のユーザーが、「本番用の」鍵と「開発用の」鍵などの (さまざまな職務を反映する) 複数の鍵を所有して、異なる構成を使用することもできます。また、高可用性 (HA) 構成のために複数の鍵が必要になる場合もあります。「ユーザー」または「ユーザーアカウント」という用

語が、通常の UNIX ユーザーアカウントではなく、Sun Crypto Accelerator 1000 のユーザーを指すことに注意してください。UNIX のユーザー名と Sun Crypto Accelerator 1000 のユーザー名には、一定の関連付けはありません。

領域はユーザーとその鍵素材の論理パーティションです。領域には、複数のユーザーを含めることができます。領域によってユーザーをパーティションに分割する利点は、各領域で一意的な名前空間を保持できるということです。これにより、領域の内容は別々に管理されます。

標準的なインストールでは、1人のユーザーが指定された1つの領域が作成されます。たとえば、1つの領域 `webserver` とその領域内の1人のユーザー `nobody` となる構成が作成されます。この場合、ユーザー `nobody` はこの1つの領域内でサーバー鍵のアクセスを制御し、管理することができます。

追加の領域を構築して、ユーザーおよび鍵素材をパーティションに分割することにも、柔軟に対応できます。より複雑な構成では、`finance`、`legal`、`engineering` などの、複数の領域が構成されます。各領域では一意的な名前空間が保持されます。たとえば、領域 `finance` のユーザー `webserv` は、領域 `engineering` の `webserv` とは異なるユーザーアカウントです。

Sun Crypto Accelerator 1000 の領域およびユーザーの管理には、管理ツール `secadm` を使用します。

領域およびユーザー、iPlanet Web サーバー

iPlanet Web サーバーで Sun Crypto Accelerator 1000 ボードが管理する鍵を参照する必要がある場合、鍵が内部ソフトウェアデータベースではなくハードウェアで管理されることを示すために「トークン名」が使用されます。

Sun Crypto Accelerator 1000 ボードでは、ユーザーアカウントと領域名を「@」マークで結び付けてトークン名が作成されます。標準的なインストールでは、1つの領域 `webserver` と1人のユーザー `nobody` が作成されます。iPlanet Web サーバーは、領域 `webserver` のユーザー `nobody` が所有する鍵を参照するために、`nobody@webserver` というトークン名を使用します。secadm を使用してユーザーを作成したときに設定するユーザー `nobody` のパスワードは、証明書の要求または証明書のインストール、iPlanet Web サーバーを起動するための認証に使用する必要があります。

トークンおよびスロットファイル

iPlanet Web サーバーは、トークンを使用して鍵素材にアクセスします。トークンは、スロットとも呼ばれます。スロットファイルは、Sun Crypto Accelerator 1000 の管理者が、指定されたアプリケーションに特定のトークンだけを選択して渡すための手段です。

スロットファイルが存在しない場合、Sun Crypto Accelerator 1000 ソフトウェアは、一組のデフォルトのトークンを iPlanet Web サーバーに渡します。この場合、nobody@realm-name という名前の 1 つのトークンが、領域ごとに渡されます。

例

engineering および finance、legal という 3 つの領域があります。次のトークンが iPlanet Web サーバーに渡されます。

- nobody@engineering
- nobody@finance
- nobody@legal

ただし、これらのトークン名を有効にするには、各領域にユーザー nobody が存在する必要があります。

スロットファイル

デフォルトの設定を無効にし優先指定を行う場合は、スロットファイルが必要です。スロットファイルは、1 つ以上のトークン名が 1 行ずつ指定されたテキストファイルです。iPlanet Web サーバーは、このファイルに指定されているトークンだけを渡します。次に、スロットファイルの指定方法を優先度の高い順に示します。

1. ファイル \$HOME/.SUNWconn_crypto_slots

このファイルは、iPlanet Web サーバーを実行する UNIX ユーザーのホームディレクトリに存在する必要があります。iPlanet Web サーバーは、ホームディレクトリを持たない UNIX ユーザーで実行されることもあります。この場合、この方法は実行できません。

2. ファイル /etc/opt/SUNWconn/crypto/slots

/etc/opt/SUNWconn/crypto/slots ファイルはグローバルデフォルトで、ユーザーのホームディレクトリに .SUNWconn_crypto_slots ファイルが存在しない場合に使用されます。

次に、スロットファイルの内容の例を示します。

```
webserv@engineering  
webserv@finance
```

この 2 つのファイルが存在しない場合には、54 ページの「トークンおよびスロットファイル」で説明したデフォルトの方法が使用されます。

iPlanet Web サーバー構成のトークン名の詳細は、第 3 章を参照してください。

secadm の使用

secadm プログラムは、Sun Crypto Accelerator 1000 ボードのコマンド行インタフェースを提供します。

secadm プログラムへのアクセスを容易にするには、検索パスに Sun Crypto Accelerator 1000 ツールのディレクトリを指定します。次に例を示します。

```
$ PATH=$PATH:/opt/SUNWconn/crypto/bin
$ export PATH
```

次に、secadm コマンドの構文を示します。

```
secadm [-h]
```

```
secadm [-y] [-f filename]
```

```
secadm [-y] [-r realm-name] [-u username | -s admin-name] command
```

このコマンドは、/opt/SUNWconn/crypto/bin/ ディレクトリにあります。

表 A-1 に、secadm ツールのオプションを示します。

表 A-1 secadm オプション

オプション	意味
-h	secadm のコマンドヘルプの表示および終了
-f filename	filename からの 1 つ以上のコマンドの読み込みおよび終了
-r realm-name	シングルコマンドモードだけで使用します。-r オプションを使用すると、secadm は指定されたコマンドを領域 <i>realm-name</i> で実行します。
-s admin-name	シングルコマンドモードだけで使用します。-s オプションを使用すると、secadm はログイン名に <i>admin-name</i> を使用して、システム管理者としてログインします。 <i>admin-name</i> は、UID 0 (ゼロ) の UNIX ユーザー (root など) である必要があります。指定されたコマンドが実行される前に、ログインが行われます。
-u username	シングルコマンドモードだけで使用します。-u オプションを使用すると、secadm は <i>username</i> でログインします。指定されたコマンドが実行される前に、ログインが行われます。
-y	通常はプロンプトを表示して確認を要求するすべてのコマンドに対して、強制的に「yes」と応答します。

動作モード

secadm は、3 種類のモードで実行できます。これらのモードは、主にコマンドがどのように secadm に渡されるかによって区別されます。モードには、シングルコマンドモードおよびファイルモード、対話型モードがあります。各モードには別々のパスワードが必要です。

シングルコマンドモード

シングルコマンドモードでは、すべてのコマンド行スイッチを指定したあとに secadm が実行するコマンドを指定します。たとえば、次のコマンドは、存在するすべての領域を表示したあとに、コマンドのシェルプロンプトに戻ります。

```
$ secadm show realm
```

次の例のコマンドは、システム管理者でログインし、領域 engineering にユーザー webserv を作成します。

```
$ secadm -r engineering -s root create user=webserv
Password:
Initial password:
Confirm password:
User webserv created successfully.
```

Password: のプロンプトでは、システム管理者のパスワードを入力する必要があります。Initial password: および Confirm password: プロンプトには、新しく作成するユーザーのパスワードを入力する必要があります。

シングルコマンドモードでの出力は、すべて標準の出力ストリームに出力されます。この出力は、標準の UNIX シェルベースの方法を使用して、リダイレクトできます。

ファイルモード

ファイルモードでは、secadm が 1 つ以上のコマンドを読み込むファイルを指定します。このファイルは、1 行につき 1 つのコマンドが指定されたテキストファイルである必要があります。各コメントは、「#」文字で開始します。ファイルモードのオブ

ションが設定されると、secadm は、最後のオプションよりあとに指定したすべてのコマンド行引数を無視します。次に、deluser.scr 内のコマンドを実行し、すべてのプロンプトに対して **yes** と応答する例を示します。

```
$ secadm -f deluser.scr -y
```

対話型モード

対話型モードでは、ftp(1) と同様のインタフェースを提供します。このインタフェースでは、1 度に 1 つのコマンドを入力できます。対話型モードでは、**-y** オプションはサポートされていません。

secadm へのコマンドの入力

secadm プログラムには、Sun Crypto Accelerator 1000 ボードと対話するために使用する必要のあるコマンド言語があります。コマンドは、文字列の全部または一部（一意に識別できるだけの文字数）を使用して入力します。show の代わりに sh は使用できますが、lo は login または logout の可能性があるため、明確ではありません。

次に、文字列を省略しない場合のコマンド入力の例を示します。

```
secadm{root@engineering}# show user
User                               Status
-----
webserv                             enabled
alice                               enabled
bob                                 enabled
-----
```

sh us のように、コマンドの文字列の一部を入力しても、同じ情報を取得することができます。

あいまいなコマンドを使用すると、そのコマンドが不明確であるという説明が表示されます。

```
secadm{root@engineering}# lo
Ambiguous command: lo
```

secadm を使用した認証

多くのコマンド (特にユーザーアカウントや鍵を扱うコマンド) では、システム管理者またはユーザーとしての認証が必要です。領域の作成、ユーザーアカウントの作成、ユーザーアカウントの有効化および無効化、領域とユーザーアカウントの削除を行う場合は、Sun Crypto Accelerator 1000 に対してシステム管理者としての認証が必要です。ユーザーのパスワードを変更したり、ユーザーが所有している鍵オブジェクトを一覧表示したりする場合は、ユーザーとしての認証が必要です。表 A-2 に、システム管理者およびユーザーが使用できるコマンドを示します。

表 A-2 管理コマンドマトリックス

コマンド	認証	資格	認証ユーザー
create user= <i>username</i>	なし	あり	システム管理者
create realm= <i>realm-name</i>	あり	なし	システム管理者
delete user= <i>username</i>	なし	あり	システム管理者
delete realm= <i>realm-name</i>	あり	なし	システム管理者
disable user= <i>username</i>	なし	あり	システム管理者
enable user= <i>username</i>	なし	あり	システム管理者
exit	なし	なし	すべて
login	あり	なし	ユーザー
logout	なし	なし	すべて
passwd	あり	あり	ユーザー
set realm= <i>realm-name</i>	なし	なし	すべて
show class	なし	なし	すべて
show key	なし	あり	ユーザー
show realm	なし	なし	すべて
show user	なし	あり	システム管理者
su	あり	なし	システム管理者
quit	なし	なし	すべて
unset realm	なし	なし	すべて

システム管理者として認証するには、UID 0 (root など) の UNIX ユーザー名を入力し、プロンプトに対してそのパスワードを入力する必要があります。ユーザーには、ユーザーを作成したときに設定したパスワードが必要です。システム管理者またはユーザーでログインすると、まず領域を選択する必要があります。

ユーザーでログインする場合は、次のように入力します。

```
secadm{realm-name}> login user=username
```

システム管理者でログインする場合は、次のように入力します。

```
secadm{realm-name}> su
```

ユーザーまたはシステム管理者でログインすると、secadm プロンプトに現在ログインしているユーザーが表示されます。ユーザーでログインしているか、システム管理者でログインしているかは、プロンプトの最後の文字で区別されます。ユーザーの場合は山括弧 (>) が表示され、システム管理者アカウントの場合はハッシュ記号 (#) が表示されます。現在、ユーザーまたはシステム管理者でログインしていて、ほかのユーザーまたはシステム管理者でログインすると、新しいログインに成功した時点で現在の資格は失われます。次に例を示します。

```
secadm> set realm=engineering
secadm{engineering}> login user=webserv
Password:
secadm{webserv@engineering}> su
System Administration Login Required
Login: root
Password:
secadm{root@engineering}# logout
secadm{engineering}>
```

コマンドのヘルプの表示

secadm には、ヘルプ機能が組み込まれています。ヘルプを表示するには、コマンドに続けて「?」文字を入力する必要があります。コマンドの文字列を省略しないで入力し、その行のどこかに「?」が存在すると、コマンドの構文が表示されます。次に、例を示します。

```
secadm> create ?
Usage: create {user=<username> | realm=<realm-name>}

secadm> show ?
Sub-Command          Description
-----
class                 Show all realm classes
key                   Show all key objects in a realm
realm                 Show all realms
user                  Show all system accounts
```

「?」を入力すると、次のように、有効なコマンドの文字列が一覧で表示されます。

```
secadm> ?
Sub-Command          Description
-----
create               Create users and accounts
delete               Delete users and accounts
disable              Disable a user
enable               Enable a user
exit                 Exit secadm
login                Login as a user
logout               Logout current session
passwd               Change password for a user
set                  Set current working realm
show                 Show system settings
su                   Authenticate as the System Administrator
quit                 Exit secadm
unset                Unset secadm operating parameters
```

コマンド行モードでヘルプを表示する場合、作業しているシェルによっては「?」文字が解釈されてしまうことがあります。「?」文字の前に、コマンドシェルのエスケープ文字を入力してください。

secadm プログラムの終了

secadm を終了するには、quit および exit の 2 つのコマンドが使用できます。Ctrl-D キーシーケンスでも secadm を終了することができます。

領域の設定および管理

領域は、鍵素材のリポジトリです。領域には、管理者およびユーザーが関連付けられています。領域は、記憶領域を提供するだけでなく、ユーザーアカウントが鍵オブジェクトを所有するための手段になります。これによって、鍵の所有者で認証されていないアプリケーションに対して、鍵を見えなくすることができます。領域には、次の 2 つのコンポーネントがあります。

- 鍵オブジェクト : iPlanet Web サーバーなどのアプリケーション用に格納されている鍵長の長い鍵です。
- ユーザーアカウント : 特定の鍵に対する認証およびアクセスを行う手段をアプリケーションに提供します。

必須の領域は 1 つだけですが、複数の領域を作成して、各領域に独自の一組のユーザーアカウントを設定することもできます。たとえば、アプリケーションがユーザー webserv で認証され、ある領域の鍵にアクセスする必要がある場合、その領域にユーザーアカウント webserv が存在する必要があります。

領域の作成

領域の作成では、鍵長の長い鍵オブジェクトの格納に必要なディレクトリおよびファイル、その他の資源を作成します。領域を作成する場合は、管理者が create realm コマンドを使用して、作成する領域の名前を指定する必要があります。現在保持している資格にかかわらず、コマンドを正常終了するには、システム管理者の認証が必要です。パスワードの入力を求めるプロンプトが表示されたら、UNIX のシステム管理者のパスワードを入力します。次に例を示します。

```
secadm> create realm=engineering
System Administrator Login Required
Login: root
Password:
Realm engineering successfully created.
```


領域には、用途に合わせた名前を付けることができます。たとえば、財務や技術などのさまざまな部門の領域を設定することも可能です。この場合、領域には `finance` および `engineering` という名前を付けます。次に例を示します。

```
secadm> create realm=finance
System Administrator Login Required
Login: root
Password:
Realm finance successfully created
```

現在の作業領域の設定

`secadm` では、1 度に 1 つの領域の鍵およびユーザーアカウントだけを管理できません。領域およびユーザーアカウントを扱うほとんどのコマンドでは、最初に領域を選択する必要があります。次の例に示すように、`set realm` コマンドを実行して、領域を選択します。

```
secadm> set realm=finance
secadm{finance}>
```

領域を選択すると、`secadm` プロンプトに中括弧で囲まれた領域名が表示されます。

現在の領域での作業を終了する場合は、現在の作業領域に新しい値を設定するか、領域の設定を解除します。現在の作業領域を変更または解除することによって、その領域で現在認証されているユーザーまたはシステム管理者は自動的にログアウトされます。次に例を示します。

```
secadm{finance}> set realm=engineering
secadm{engineering}> unset realm
secadm>
```

領域でのユーザーの生成

作成するユーザー名は、Sun Crypto Accelerator 1000 ボードのドメイン内だけで認識されます。動作している Web サーバープロセスの UNIX ユーザー名と同一である必要はありません。ユーザーを作成する前に、まず適切な領域を選択して、システム管理者でログインする必要があります。次に例を示します。

```
secadm> set realm=engineering
secadm(engineering)> su
System Administrator Login Required
Login: root
Password:
secadm(root@engineering)#
```

領域にユーザーが 1 人だけ必要な場合は、領域名 nobody を使用すると、スロットファイルの設定を省略できます。次の例では、領域 engineering にユーザー nobody を作成し、表 3-1 の *user@realm-name* の定義に従って nobody@engineering に対するパスワードを設定します。

```
secadm(root@engineering)# create user=nobody
Initial password:
Confirm password:
User nobody successfully created.
```

Web サーバーの起動時に認証を行う際に、このパスワードを使用する必要があります。



注意 – 入力したパスワードを覚えておく必要があります。パスワードを忘れると、鍵にアクセスできなくなります。パスワードを忘れた場合、これを検索する方法はありません。

領域の一覧表示

`show realm=realm-name` コマンドを実行すると、領域に関する情報が一覧で表示されます。

```
secadm> show realm
Realm Name
-----
engineering
finance
-----
```

領域のクラスの一覧表示

領域のクラスは、領域が鍵オブジェクトおよびユーザーアカウント、認証データを管理する方法を制御する鍵管理モジュールです。現在、Sun Crypto Accelerator 1000 でサポートされている領域のクラスは、SUNW_filesys だけです。サポートされているすべての領域のクラスを一覧で表示するには、`show class` コマンドを使用します。

```
secadm> show class
Realm Class
-----
SUNW_filesys
-----
```

領域の削除

`delete realm` コマンドに、削除する領域の名前を指定して実行すると、領域を削除できます。このコマンドを実行すると、領域の削除を確認するために、`yes/no` 形式の `secadm` プロンプトが表示されます。領域の作成時と同様に、このコマンドを実行する前に、システム管理者アカウントでの認証が必要です。また、使用中の領域は削除できません。領域への参照を解放するには、Web サーバーが管理サーバー、またはその両方を停止する必要がある場合があります。

▼ 領域を削除する

1. secadm ユーティリティを使用して、各領域を削除します。

```
secadm> delete realm=realm-name
Delete realm realm-name? [Y/N]: Y
System Administrator Login Required
Login: root
Password:
Realm realm-name deleted successfully.
```

これによって、鍵素材など、サイト固有のすべての領域データが削除されます。

ユーザーアカウントの設定および管理

ユーザーアカウントは、アプリケーションが Sun Crypto Accelerator 1000 に認証されるための方法です。また、これによって、1つの領域内で鍵を区別することもできます。1つのユーザーアカウントで所有される鍵は、そのユーザーが領域に対して認証されていないアプリケーション、またはほかのユーザーで認証されたアプリケーションからはアクセスできません。ここで使用するコマンドを実行するには、領域を選択し、システム管理者が secadm su コマンドでその領域にログインしている必要があります。

ユーザーの作成

- create user コマンドを実行して、ユーザーを作成します。

このコマンドには、create user=username の形式でユーザー名を指定する必要があります。

```
secadm{root@engineering}# create user=username
Initial password:
Confirm password:
User username created successfully.
```



注意 – 入力したパスワードを覚えておく必要があります。パスワードを忘れると、鍵にアクセスできなくなります。パスワードを忘れた場合、これを検索する方法はありません。

ユーザーの一覧表示

システム管理者だけが、領域内のユーザーを一覧で表示できます。システム管理者は、`show user` コマンドを実行する必要があります。このコマンドでは、現在選択されている領域のユーザーだけが一覧で表示されます。

- `show user` コマンドを実行します。

```
secadm{root@engineering}# show user
User                               Status
-----
webserv                             enabled
alice                               enabled
bob                                 enabled
-----
```

ユーザーパスワードの変更

`secadm login` コマンドを使用してログインしているユーザーだけが、そのユーザーのパスワードを変更できます。新しいパスワードを設定するには、現在のパスワードを知っている必要があります。

- `passwd` コマンドを実行します。

```
secadm{username@realm-name}> passwd
Enter current password:
Enter Password:
Confirm Password:
Password successfully changed for user username.
```



注意 – 入力したパスワードを覚えておく必要があります。パスワードを忘れると、鍵にアクセスできなくなります。パスワードを忘れた場合、これを検索する方法はありません。

ユーザーの有効化または無効化

システム管理者アカウントだけが、ユーザーを有効または無効にすることができます。デフォルトでは、各ユーザーは有効な状態で作成されます。

- ユーザーアカウントを無効にする場合は、`disable user=username` コマンドを入力します。

```
secadm{root@engineering}# disable user=username  
User is now disabled.
```

無効なユーザーアカウントでの認証は、すべて失敗します。ただし、鍵に対する変更は行われません。ユーザーアカウントが再び有効になると、そのユーザーが所有するすべての鍵は、認証されたアプリケーションによって再びアクセス可能になります。

- ユーザーアカウントを有効にする場合は、`enable user=username` コマンドを入力します。

```
secadm{root@engineering}# enable user=username  
User is now enabled.
```

ユーザーの削除

- 削除するユーザーを指定して `delete user` コマンドを実行します。

システム管理者が、削除するユーザーアカウント名を指定する必要があります。

このコマンドを実行すると、ユーザーに関連する鍵は削除されます。ユーザーを削除する前に、システム管理者に対して、確認のための `yes/no` 形式の `secadm` プロンプトが表示されます。

```
secadm{root@engineering}# delete user=username  
Delete user webserv? [Y/N]: y  
User username deleted successfully.
```

付録 B

マニュアルページ

この付録では、Sun Crypto Accelerator 1000 ソフトウェアに付属のマニュアルページについて説明します。

マニュアルページは、次のコマンドを使用して表示できます。

```
man -M /opt/SUNWconn/man page
```

表 B-1 に、使用可能なマニュアルページを示します。

表 B-1 Sun Crypto Accelerator 1000 のマニュアルページ

マニュアルページ	説明
cryptio(7d)	cryptio デバイスドライバは、構成されているハードウェア暗号化アクセラレータへのアクセスを制御します。 cryptio ドライバには、アプリケーションおよびカーネルクライアントが決められたサービスにアクセスするための階層化されたソフトウェアが必要です。
dca(7d)	dca デバイスドライバは、構成されているハードウェア暗号化アクセラレータへのアクセスを制御するリーフドライバです。 dca ドライバには、アプリケーションおよびカーネルクライアントが決められたサービスにアクセスするための階層化されたソフトウェアが必要です。
kcl(7d)	kcl デバイスドライバは、マルチスレッド化されたロード可能なカーネルモジュールで、サンの暗号化プロバイダドライバをサポートします。 kcl ドライバには、アプリケーションおよびカーネルクライアントが決められたサービスにアクセスするための階層化されたソフトウェアが必要です。

表 B-1 Sun Crypto Accelerator 1000 のマニュアルページ (続き)

マニュアルページ	説明
kcpi (7d)	<p>kcpi デバイスドライバは、マルチスレッド化されたロード可能なカーネルモジュールで、サンの暗号化プロバイダのドライバをサポートします。</p> <p>kcpi ドライバには、アプリケーションおよびカーネルクライアントが決められたサービスにアクセスするための階層化されたソフトウェアが必要です。</p>
secadm (1m)	<p>secadm は、Sun Crypto Accelerator 1000 の管理ユーティリティです。secadm コマンドは、Sun Crypto Accelerator 1000 に関する構成およびアカウント、鍵のデータベースを手動で操作する場合に使用します。</p> <p>secadm は、注意が必要な暗号化鍵情報を扱います。</p>
secd (1m)	<p>secd デーモンは、secadm アプリケーションに対して、管理アクセスサービスを提供します。</p>
sslconfig (1m)	<p>sslconfig は、Sun Crypto Accelerator 1000 の構成ユーティリティです。</p>

付録 C

Apache Web サーバーの SSL 設定 ディレクティブ

この付録では、Sun Crypto Accelerator 1000 ソフトウェアを使用して Apache Web サーバーで SSL サポートを設定するためのディレクティブを示します。ディレクティブは `http.conf` ファイルに設定します。詳細は、Apache Web サーバーのマニュアルを参照してください。

1. SSLPassPhraseDialog `exec:program`

コンテキスト：グローバル

このディレクティブは、指定した `program` を実行して鍵ファイルのパスワードを収集することを Apache Web サーバーに通知します。`program` は、収集したパスワードを標準出力へ出力します。

複数の鍵ファイルが存在し、それらが共通のパスワードを持つ場合は、`program` は一度だけ実行されます (収集された各パスワードは、`program` を再び実行する前に試されます)。

`program` は、2 つの引数を指定して実行されます。1 つ目の引数はサーバー名で、`servername:port` の形式で指定します。たとえば、`www.fictional-company.com:443` のように指定します (ポート 443 は、SSL ベースの Web サーバーで使用される一般的なポートです)。2 つ目の引数は、鍵ファイルの鍵の種類 (`keytype`) です。`keytype` には、RSA または DSA のいずれかを指定できます。

注 - このプログラムはシステムの起動中に実行されるため、コンソールが tty デバイスでない場合に対処できる (tty(3c) の場合は、偽を返す) ように設計してください。

提供されているプログラム `/opt/SUNWconn/crypto/bin/sslpasword` は、`program` の実行可能ファイルとして使用できます。このプログラムでは自動的にパスワードの入力を求めるプロンプトが表示されます。入力したパスワードの表示は抑止されます。

また、この `sslpassword` プログラムでは、ファイルからパスワードを自動的に検索することもできます。これは、Web サーバーの起動時にユーザーとの対話を回避する場合に使用されます。鍵ファイルのパスワードは、`/etc/apache/servername:port.keytype.pass` という名前のファイル内で検索されます。このファイルが存在しない場合は、ファイル `/etc/apache/default.pass` が使用されます。これらのパスワードファイルには、暗号化されていないパスワードが入っています。

注 – Web サーバーを実行する UNIX ユーザーだけがパスワードファイルを読み込めるように、アクセス権でファイルを保護してください。このユーザーは、標準の Apache の User ディレクティブで設定されているユーザーと同じである必要があります。

このディレクティブが指定されていない場合は、デフォルトで、内部のプロンプト機構が使用されます。システム起動時の対話に関する問題を回避するには、デフォルトではなく、提供されている `sslpassword` プログラムの使用をお勧めします。

2. SSLEngine (on|off)

コンテキスト：グローバル、仮想ホスト

このディレクティブは、SSL プロトコルを使用可能にします。通常は、このディレクティブは、一部のサーバーで SSL を使用可能にするために、仮想ホストで使用されます。次の書式が、一般的に使用されます。

```
<VirtualHost _default_:443>
SSLEngine on
</VirtualHost>
```

この文は、ポート 443 (標準の HTTPS ポート) で待機するすべてのサーバーで、SSL を使用するように設定しています。ディレクティブが設定されていない場合、このプロトコルはデフォルトでオフになります。

3. SSLProtocol [+*-*]protocol

コンテキスト：グローバル、仮想ホスト

このディレクティブでは、サーバーが SSL トランザクションで使用するプロトコルを設定します。表 C-1 に、使用可能なプロトコルを一覧で表示して説明します。

表 C-1 SSL プロトコル

プロトコル	説明
SSLv2	標準である Netscape の最初の SSL プロトコル
SSLv3	SSL プロトコルの更新バージョン。よく知られているほとんどの Web ブラウザでサポートされています。
TLSv1	SSLv3 に更新を加えたもの。現在 IETF で標準化が進められています。ごく限られたブラウザによってサポートされています。
all	すべてのプロトコルを使用可

プラス (+) またはマイナス (-) 符号を使用して、プロトコルを追加または削除できます。たとえば、SSLv2 のサポートを使用不可にする場合、次のようにディレクティブを指定します。

```
SSLProtocol all -SSLv2
```

この文は、次のように指定するのと同じ意味です。

```
SSLProtocol +SSLv3 +TLSv1
```

4. SSLCipherSuite cipher-spec

コンテキスト：グローバル、仮想ホスト、ディレクトリ、.htaccess

SSLCipherSuite ディレクティブは、使用可能な SSL の暗号および優先順位を設定するために使用します。グローバルコンテキストまたは仮想ホストコンテキストでは、このディレクティブは最初の SSL ハンドシェイクで使用されます。ディレクトリごとのコンテキストでは、名前付き暗号を使用するために、SSL の再ネゴシエーションが強制的に行われます。再ネゴシエーションは、要求が読み込まれたあとで、応答が送信される前に実行されます。

cipher-spec には、表 C-2 に示す暗号を、コロンで区切って指定します。表 C-2 で、DH は Diffie-Hellman を、DSS は Digital Signature Standard を表します。

表 C-2 使用可能な SSL の暗号

暗号タグ	プロトコル	鍵の交換	認証	暗号化	MAC	種類
DES-CBC3-SHA	SSLv3	RSA	RSA	3DES (168 ビット)	SHA1	
DES-CBC3-MD5	SSLv2	RSA	RSA	3DES (168 ビット)	MD5	
RC4-SHA	SSLv3	RSA	RSA	ARCFOUR (128 ビット)	SHA1	
RC4-MD5	SSLv3	RSA	RSA	ARCFOUR (128 ビット)	MD5	
RC4-MD5	SSLv2	RSA	RSA	ARCFOUR (128 ビット)	MD5	
RC2-CBC-MD5	SSLv2	RSA	RSA	ARCTWO (128 ビット)		
DES-CBC-SHA	SSLv3	RSA	RSA	DES (56 ビット)	SHA1	
RC4-64-MD5	SSLv2	RSA	RSA	ARCFOUR (64 ビット)	MD5	
DES-CBC-MD5	SSLv2	RSA	RSA	DES (56 ビット)	MD5	
EXP-DES-CBC-SHA	SSLv3	RSA (512 ビット)	RSA	DES (40 ビット)	SHA1	輸出
EXP-RC2-CBC-MD5	SSLv2	RSA (512 ビット)	RSA	ARCTWO (40 ビット)	SHA1	輸出
EXP-RC2-CBC-MD5	SSLv3	RSA (512 ビット)	RSA	ARCTWO (40 ビット)	SHA1	輸出
EXP-RC4-MD5	SSLv3	RSA (512 ビット)	RSA	ARCFOUR (40 ビット)	MD5	輸出
EXP-RC4-MD5	SSLv2	RSA (512 ビット)	RSA	ARCFOUR (40 ビット)	MD5	輸出
NULL-SHA	SSLv3	RSA	RSA	なし	SHA1	
NULL-MD5	SSLv3	RSA	RSA	なし	MD5	
ADH-DES-CBC3-SHA	SSLv3	DH	なし	3DES (168 ビット)	SHA1	
ADH-DES-CBC-SHA	SSLv3	DH	なし	DES (56 ビット)	SHA1	
ADH-RC4-MD5	SSLv3	DH	なし	ARCFOUR (128 ビット)	MD5	
EDH-RSA-DES-CBC3-SHA	SSLv3	DH	RSA	3DES (168 ビット)	SHA1	
EDH-DSS-DES-CBC3-SHA	SSLv3	DH	DSS	3DES (168 ビット)	SHA1	

表 C-2 使用可能な SSL の暗号 (続き)

暗号タグ	プロトコル	鍵の交換	認証	暗号化	MAC	種類
EDH-RSA-DES-CBC-SHA	SSLv3	DH	RSA	DES (56 ビット)	SHA1	
EDH-DSS-DES-CBC-SHA	SSLv3	DH	DSS	DES (56 ビット)	SHA1	
EXP-EDH-RSA-DES-CBC-SHA	SSLv3	DH (512 ビット)	RSA	DES (40 ビット)	SHA1	輸出
EXP-EDH-DSS-DES-CBC-SHA	SSLv3	DH (512 ビット)	DSS	DES (40 ビット)	SHA1	輸出
EXP-ADH-DES-CBC-SHA	SSLv3	DH (512 ビット)	なし	DES (40 ビット)	SHA1	輸出
EXP-ADH-RC4-MD5	SSLv3	DH (512 ビット)	なし	ARCFOUR (40 ビット)	MD5	輸出

表 C-3 に、マクロのように暗号をグループ化するために使用される別名を示します。

表 C-3 SSL の別名

別名	説明
SSLv2	SSL バージョン 2.0 のすべての暗号
SSLv3	SSL バージョン 3.0 のすべての暗号
EXP	輸出用グレードのすべての暗号
EXPORT40	40 ビットのすべての輸出用暗号
EXPORT56	56 ビットのすべての輸出用暗号
LOW	強度の低い暗号 (DES、40 ビット RC4)
MEDIUM	128 ビットのすべての暗号
HIGH	Triple DES を使用するすべての暗号
RSA	RSA 鍵交換を使用するすべての暗号
DH	Diffie-Hellman 鍵交換を使用するすべての暗号
EDH	Ephemeral Diffie-Hellman 鍵交換を使用するすべての暗号
ADH	匿名の Diffie-Hellman 鍵交換を使用するすべての暗号
DSS	DSS 認証を使用するすべての暗号
NULL	暗号化を使用しないすべての暗号

暗号の優先順位は、表 C-4 に示す特殊文字を使用して設定できます。

表 C-4 暗号の優先順位を設定する特殊文字

文字	説明
指定なし	リストに暗号を追加
!	リストから完全に暗号を削除 (再び追加できない)
+	リストに暗号を追加し、現在の位置に移動 (優先順位が下がる可能性あり)
-	リストから暗号を削除 (再びリストに追加できる)

cipher-spec のデフォルト値を次に示します。

```
SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP
```

デフォルトでは、匿名の (認証されていない) Diffie-Hellman 以外のすべての暗号が設定されています。この中で、まず ARCFOUR および RSA に優先権が与えられ、高いグレードから低いグレードの順に暗号が設定されています。

5. SSLCertificateFile *file*

コンテキスト: グローバル、仮想ホスト

このディレクティブは、サーバーの PEM 符号化形式の X.509 証明書ファイルの位置を指定します。

6. SSLCertificateKeyFile *file*

コンテキスト: グローバル、仮想ホスト

このディレクティブは、SSLCertificateFile ディレクティブで設定された証明書に対応する、サーバーの PEM 符号化形式の非公開鍵ファイルの位置を指定します。

7. SSLCertificateChainFile *file*

コンテキスト: グローバル、仮想ホスト

このディレクティブは、サーバーの証明書パスを構成する、PEM 符号化形式の証明書が指定されたファイルの位置を指定します。このディレクティブを使用すると、サーバーの証明書がクライアントが認識する認証局によって直接署名されたものでない場合に、クライアントによるサーバーの証明書の検証を助けることができます。

クライアント認証 (SSLVerifyClient) が使用される場合、連鎖内の証明書は、クライアント認証としても有効とみなされます。

8. SSLCACertificateFile *file*

コンテキスト: グローバル、仮想ホスト

このディレクティブは、認証局 (CA) の証明書リストが指定されたファイルの位置を指定します。クライアント認証に使用されます。

9. SSLCARevocationFile *file*

コンテキスト：グローバル、仮想ホスト

このディレクティブは、CA の証明取り消しリストが指定されたファイルの位置を指定します。クライアント認証に使用されます。

10. SSLVerifyClient *level*

コンテキスト：グローバル、仮想ホスト、ディレクトリ、.htaccess

このディレクティブは、サーバーに対するクライアントの認証を指定します (通常、e コマースアプリケーションでは必要ありませんが、ほかのアプリケーションで使用されます)。

表 C-5 に、*level* の値を示します。

表 C-5 SSL のクライアントの検証レベル

レベル	説明
none	クライアントの証明書は必要なし
optional	クライアントは有効な証明書が必要な場合がある
require	クライアントは有効な証明書が必要
optional_no_ca	クライアントは証明書が必要な場合があるが、有効である必要はない

通常、none または require が使用されます。デフォルトの設定は、none です。

11. SSLVerifyDepth *depth*

コンテキスト：グローバル、仮想ホスト、ディレクトリ、.htaccess

このディレクティブは、クライアントの証明書に対してサーバーが許可する証明書連鎖の最大の深さを指定します。値 0 は、自己署名付き証明書だけが有効であることを意味し、値 1 は、クライアント証明書が SSLCACertificateFile を介してサーバーが直接認識している CA によって署名される必要があることを意味します。値 2 以上が指定された場合は、CA の委任を許可します。

12. SSLLog *filename*

コンテキスト：グローバル、仮想ホスト

このディレクティブは、SSL 固有の情報が記録されるログファイルを指定します。このディレクティブを指定しないと、デフォルトでは、SSL 固有の情報は記録されません。

13. SSLLogLevel *level*

コンテキスト：グローバル、仮想ホスト

このディレクティブは、SSL ログファイルに記録される情報の詳細さを指定します。表 C-6 に、*level* の値を示します。

表 C-6 SSL のログレベルの値

値	説明
none	記録しない。ただし、エラーメッセージは標準の Apache エラーログに送信される。
warn	警告メッセージを含む
info	情報メッセージを含む
trace	追跡メッセージを含む
debug	デバッグメッセージを含む

14. SSLOptions [*+-*] *option*

コンテキスト：グローバル、仮想ホスト、ディレクトリ、.htaccess

このディレクティブでは、ディレクトリごとに SSL 実行時のオプションを設定します。オプションの前にプラス (+) 符号を付けると現在の設定に追加され、マイナス (-) 符号を付けると現在の設定から削除されます。複数のオプションをディレクトリに適用すると、もっとも限定的なオプションが使用されます (これらのオプションはマージされません)。

表 C-7 に、オプションを示します。

表 C-7 使用可能な SSL のオプション

オプション	説明
StdEnvVars	SSL に関連する標準的な CGI/SSI 環境変数の組が作成されます。このオプションは、性能に影響を与えます。
ExportCertData	環境変数 SSL_SERVER_CERT および SSL_CLIENT_CERT、SSL_CLIENT_CERT_CHAIN <i>n</i> (<i>n</i> = 0, 1, ...) がエクスポートされます。これらの変数には、クライアントおよびサーバーに対する PEM 符号化形式の証明書が含まれます。
FakeBasicAuth	クライアント証明書の識別名 (DN) が HTTP の基本認証ユーザー名に変換され、「擬似的」に認証が行われます。これによって、SSL クライアント認証を使用して、ユーザーにパスワードの入力を求めずに、標準の Apache アクセス制御機構を使用できます。 Apache パスワードファイル内のこれらのユーザーのエントリには、暗号化されたパスワード xxj31ZMTZzkVA を使用する必要があります。これは、「password」を暗号化 (crypt(3c)) したものです。

表 C-7 使用可能な SSL のオプション (続き)

オプション	説明
StrictRequire	SSLRequireSSL より優先される Satisfy Any などのほかのディレクティブがある場合でも、SSLRequireSSL によって拒否されたアクセスを禁止します。

15. SSLRequireSSL

コンテキスト: ディレクトリ、.htaccess

このディレクティブは、HTTPS が使用されない場合に限り、特定のディレクトリへのアクセスを禁止します。このディレクティブは、認証されていないアクセスまたは暗号化されていないアクセスによってディレクトリの内容を使用できる状態になっている場合などの、誤った構成を防止するために使用します。

付録 D

Sun Crypto Accelerator 1000 ボード で使用するアプリケーションの構築

この付録では、Sun Crypto Accelerator 1000 に付属するソフトウェアについて説明します。このソフトウェアは、Sun Crypto Accelerator 1000 ボードの強化された暗号化機能を利用する OpenSSL 互換のアプリケーションを構築するために使用できます。このコンパイル方法が、すべての OpenSSL アプリケーションに対して効果的であるとは限りません。これとは対照的に、OpenSSL の標準ライブラリで構築する方法もあります。OpenSSL の標準ライブラリは、www.openssl.org からダウンロードできます。

注 – Sun Crypto Accelerator 1000 ソフトウェアおよびハードウェアを使用するアプリケーションの構築に関する情報は、現状のまま無保証で提供されています。この製品の一部として正式にサポートされるものではありません。この情報は、参考のために記載していますが、保証はありません。サンがサポートするソリューションが必要な場合は、ご購入先にお問い合わせください。

最初に SUNWcrys1 パッケージをインストールする必要があります。このパッケージには、必要なヘッダーファイルおよびライブラリが含まれています。

アプリケーションは、コンパイラフラグなどで、
`/opt/SUNWconn/crypto/include` の OpenSSL ヘッダーを指定して構成する必要があります。

```
-I /opt/SUNWconn/crypto/include
```

また、リンカーには適切なライブラリへの参照を指定する必要があります。ほとんどの OpenSSL 互換のアプリケーションは、libcrypto.a および libssl.a ライブラリのどちらかまたは両方を参照します。サンの暗号化ライブラリも指定する必要があります。リンカーフラグには、次のように指定します。

```
-L/opt/SUNWconn/crypto/lib -R/opt/SUNWconn/crypto/lib \  
-lcrypto -lssl -lcryptography -lnvpair
```

付録 E

Sun Crypto Accelerator 1000 ボード の仕様

この付録では、Sun Crypto Accelerator 1000 ボードに関するさまざまな仕様の概要について説明します。この付録は、次の節で構成されます。

- 83 ページの「物理的な寸法」
- 84 ページの「インタフェースの仕様」
- 84 ページの「電源要件」
- 85 ページの「環境仕様」

物理的な寸法

表 E-1 物理的な寸法

寸法	米国表記	メートル表記
長さ	6.875 インチ	174.625 mm
幅	4.2 インチ	106.680 mm

インタフェースの仕様

表 E-2 インタフェースの仕様

機能	仕様
PCI クロック	33 MHz または 66 MHz
ホストインタフェース	33 MHz または 66 MHz のクロックレートおよび 3.3 V または 5 V の電力をサポートする PCI 2.1
PCI のバス幅	32 ビットまたは 64 ビット

電源要件

表 E-3 電源要件

仕様	測定値
最大電力消費量	10 W @ 5 V
	700 mW @ 3.3 V
電圧許容範囲	5 V +/- 5 %
	3.3 V +/- 5 %
動作時電流	2 A @ 1.8 V
	150 mA @ 3.3 V

環境仕様

表 E-4 環境仕様

条件	動作時の仕様	保管時の仕様
温度	0 ~ 70°C (32 ~ 160°F)	-65 ~ +150°C (-85 ~ 300°F)
相対湿度	5 ~ 85 % 結露のないこと	0 ~ 95 % 結露のないこと

付録F

サン以外のライセンス

この付録では、サン以外のベンダーによるソフトウェアの注意およびライセンスについて説明します。該当するソフトウェアを使用する際は、これに従う必要があります。

OpenSSL のライセンスの問題

OpenSSL のツールキットは、2つのライセンスの制約下であり、OpenSSL ライセンスおよびオリジナルの **SSLeay** ライセンスの両方の条件が適用されます。このあとに、実際のライセンス文書を記載します。この2つのライセンスは、実際には BSD 形式のオープンソースライセンスです。OpenSSL のライセンスに関する問題がある場合は、`openssl-core@openssl.org` にお問い合わせください。

OpenSSL License

Copyright (c) 1998-2001 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact `openssl-core@openssl.org`.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

``Ian Fleming was a UNIX fan!
How do I know? Well, James Bond
had the (license to kill) number 007,
i.e. he could execute anyone."
-- Unknown

MOD_SSL のライセンス

mod_ssl パッケージは、BSD 形式のライセンスの制約下で配布されるので、オープンソースソフトウェアに分類されます。詳細なライセンス情報は、次のとおりです。

Copyright (c) 1998-2000 Ralf S. Engelschall. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>)."
4. The names "mod_ssl" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.
5. Products derived from this software may not be called "mod_ssl" nor may "mod_ssl" appear in their names without prior written permission of Ralf S. Engelschall.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>)."

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RALF S. ENGELSCHALL OR HIS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

索引

A

- Apache SSL ディレクティブ, 71
- Apache Web サーバー
 - 使用可能化, 39
 - 証明書の作成, 42

D

- dcatest, 48
 - コマンド行構文, 49
 - サブテスト, 49
 - テストパラメタオプション, 49

I

- iPlanet Web サーバー
 - iPlanet Web Server 4.1
 - インストール, 19
 - 構成, 24
 - サーバーの証明書のインストール, 24
 - 証明書の生成, 20
 - 認証データベースの作成, 20
 - iPlanet Web Server 6.0
 - インストール, 29
 - 構成, 36
 - サーバーの証明書のインストール, 34
 - サーバーの証明書の生成, 33
 - 認証データベースの作成, 30
- 使用可能化, 15
- 領域およびユーザーの作成, 16

- iPlanet Web サーバーの管理, 53

K

- kstat コマンド, 51

O

- OpenBoot PROM, 50

R

- RSA 鍵ペア, 41

S

- secadm ユーティリティー, 56
- SunVTS, 47
 - dcatest, 48

U

- URL
 - iPlanet ソフトウェア, 19, 29
 - OpenSSL, 81

あ

アルゴリズム, 3

か

鍵長, 41

こ

高可用性 (HA), 3

コマンド

 kstat, 51

さ

サーバーの証明書, 22, 33

し

障害追跡, 50

使用可能化

 Apache Web サーバー, 39

 iPlanet Web サーバー, 15

診断テスト, 47

す

スロットファイル, 55

そ

ソフトウェアパッケージ, 10

て

ディレクトリ

 階層, 12

と

統計値, 51

動的再構成 (DR), 3

に

認証データベース

 作成

 iPlanet Web Server 4.1, 20

 iPlanet Web Server 6.0, 30

は

パスワード

 iPlanet Web サーバーで必要なリスト, 15

 secadm, 17

 システム管理者, 17

パッチ

 Solaris 8, 5

 Solaris 9, 6

 推奨, 6

 必須, 5

ふ

ファイルおよびディレクトリ

 インストール, 10

負荷分散, 4

ほ

ホットプラグ, 3

ゆ

ユーザー, 53

 一覧表示, 67

 削除, 68

 作成, 66

 有効化または無効化, 67

ユーザーパスワード
変更, 67

よ

要件
ソフトウェア, 4
ハードウェア, 4

ら

ライセンス
サン以外, 87

り

領域, 53
一覧表示, 65
削除, 65
作成, 62
設定, 63

