



Sun™ Crypto Accelerator 4000 ボード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. 817-2329-10
2003 年 5 月, Revision A

コメントの宛先: docfeedback@sun.com

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

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

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

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

本製品の一部は、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, Sun ONE, Sun Enterprise, Sun Enterprise Volume Manager, Sun Fire, SunSolve, 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 (<http://www.modssl.org/>) のソフトウェアを使用しています。

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

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

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

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

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

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

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

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

原典: Sun Crypto Accelerator 4000 Board Installation and User's Guide
Part No: 817-0431-10
Revision A



Declaration of Conformity (Fiber MMF)

Compliance Model Number: Venus-FI
Product Family Name: Sun Crypto Accelerator 4000 - Fiber (X4012A)

EMC

USA - FCC Class B

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

- 1) This equipment may not cause harmful interference.
- 2) This equipment must accept any interference that may cause undesired operation.

European Union

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

As Telecommunication Network Equipment (TNE) in both Telecom Centers and Other Than Telecom Centers per (as applicable):

EN300-386 V.1.3.1 (09-2001) Required Limits:

EN55022/CISPR22	Class B
EN61000-3-2	Pass
EN61000-3-3	Pass
EN61000-4-2	6 kV (Direct), 8 kV (Air)
EN61000-4-3	3 V/m 80-1000MHz, 10 V/m 800-960 MHz and 1400-2000 MHz
EN61000-4-4	1 kV AC and DC Power Lines, 0.5 kV Signal Lines,
EN61000-4-5	2 kV AC Line-Gnd, 1 kV AC Line-Line and Outdoor Signal Lines, 0.5 kV Indoor Signal Lines > 10m.
EN61000-4-6	3 V
EN61000-4-11	Pass

As information Technology Equipment (ITE) Class B per (as applicable):

EN55022:1998/CISPR22:1997 Class B

EN55024:1998 Required Limits:

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 60950:2000, 3rd Edition

Evaluated to all CB Countries

UL 60950, 3rd Edition, CSA C22.2 No. 60950-00

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.
4150 Network Circle, MPK15-102
Santa Clara, CA 95054, USA
Tel: 650-786-3255
Fax: 650-786-3723

/S/

Pamela J Dullaghan
Quality Program Manager
Sun Microsystems Scotland, Limited
Springfield, Linlithgow
West Lothian, EH49 7LR
Scotland, United Kingdom
Tel: +44 1 506 672 395
Fax: +44 1 506 672 855

Declaration of Conformity (Copper UTP)

Compliance Model Number: Venus-CU

Product Family Name: Sun Crypto Accelerator 4000 - Copper (X4011A)

EMC

USA - FCC Class B

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

- 1) This equipment may not cause harmful interference.
- 2) This equipment must accept any interference that may cause undesired operation.

European Union

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

As Telecommunication Network Equipment (TNE) in both Telecom Centers and Other Than Telecom Centers per (as applicable):

EN300-386 V.1.3.1 (09-2001) Required Limits:

EN55022/CISPR22	Class B
EN61000-3-2	Pass
EN61000-3-3	Pass

EN61000-4-2	6 kV (Direct), 8 kV (Air)
EN61000-4-3	3 V/m 80-1000MHz, 10 V/m 800-960 MHz and 1400-2000 MHz
EN61000-4-4	1 kV AC and DC Power Lines, 0.5 kV Signal Lines,
EN61000-4-5	2 kV AC Line-Gnd, 1 kV AC Line-Line and Outdoor Signal Lines, 0.5 kV Indoor Signal Lines > 10m.
EN61000-4-6	3 V
EN61000-4-11	Pass

As information Technology Equipment (ITE) Class B per (as applicable):

EN55022:1998 / CISPR22:1997 Class B

EN55024:1998 Required Limits:

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 60950:2000, 3rd Edition

Evaluated to all CB Countries

UL 60950, 3rd Edition, CSA C22.2 No. 60950-00

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.
 4150 Network Circle, MPK15-102
 Santa Clara, CA 95054, USA
 Tel: 650-786-3255
 Fax: 650-786-3723

/S/

Pamela J Dullaghan
 Quality Program Manager
 Sun Microsystems Scotland, Limited
 Springfield, Linlithgow
 West Lothian, EH49 7LR
 Scotland, United Kingdom
 Tel: +44 1 506 672 395
 Fax: +44 1 506 672 855

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. 製品の概要	1
製品の機能	1
主なプロトコルおよびインタフェース	1
主な機能	2
サポートするアプリケーション	2
サポートする暗号化プロトコル	2
診断のサポート	3
暗号化アルゴリズムの高速化	3
サポートする暗号化アルゴリズム	3
バルク暗号化	4
ハードウェアの概要	5
IPsec ハードウェアの高速化	5
Sun Crypto Accelerator 4000 MMF アダプタ	6
LED 表示	6
Sun Crypto Accelerator 4000 UTP アダプタ	7
LED 表示	8
動的再構成 (DR) および高可用性 (HA)	9
負荷分散	9
ハードウェアおよびソフトウェアの要件	10
必須パッチ	10

Apache Web サーバーパッチ	10
Solaris 8 のパッチ	11
Solaris 9 のパッチ	11
2. Sun Crypto Accelerator 4000 ボードの取り付け	13
ボードの取り扱い	13
ボードの取り付け	14
▼ ハードウェアを取り付ける	14
Sun Crypto Accelerator 4000 ソフトウェアのインストール	16
▼ ソフトウェアをインストールする	16
オプションパッケージのインストール	18
ディレクトリおよびファイル	19
ソフトウェアの削除	21
▼ ソフトウェアを削除する	21
3. ドライバパラメタの設定	23
Sun Crypto Accelerator 4000 Ethernet デバイスドライバ (vca) のパラメタ	23
ドライバパラメタ値および定義	24
通知される接続パラメタ	25
フロー制御パラメタ	27
Gigabit 強制モードパラメタ	28
パケット間隔パラメタ	28
割り込みパラメタ	30
ランダム早期ドロップパラメタ	30
PCI バスインタフェースパラメタ	31
vca ドライバパラメタの設定	32
ndd ユーティリティを使用したパラメタの設定	32
▼ ndd ユーティリティのデバイスインスタンスを指定する	32
非対話型モードと対話型モード	33

自動ネゴシエーションモードまたは強制モードの設定	35
▼ 自動ネゴシエーションモードを使用不可にする	36
vca.conf ファイルを使用したパラメタの設定	37
▼ vca.conf ファイルを使用してドライバパラメタを設定する	37
vca.conf ファイルを使用したすべての Sun Crypto Accelerator 4000 vca デバイスのパラメタの設定	38
▼ vca.conf ファイルを使用してすべての Sun Crypto Accelerator 4000 vca デバイスのパラメタを設定する	39
vca.conf ファイルの例	39
OpenBoot PROM を使用した接続パラメタの自動ネゴシエーションモードおよび 強制モードの切り替え	40
Sun Crypto Accelerator 4000 暗号化ドライバおよび Ethernet ドライバの動作に関 する統計情報	42
暗号化ドライバの統計情報	42
Ethernet ドライバの統計情報	43
接続相手の機能の報告	47
▼ 接続相手の設定を確認する	50
ネットワーク構成	50
ネットワークホストファイルの構成	50
4. vcaadm および vcardiag ユーティリティによる Sun Crypto Accelerator 4000 ボードの管理	53
vcaadm の使用	53
動作モード	55
シングルコマンドモード	55
ファイルモード	56
対話型モード	56
vcaadm によるログインおよびログアウト	56
vcaadm によるボードへのログイン	57
新しいボードへのログイン	57
遠隔アクセス鍵が変更されたボードへのログイン	58

vcaadm プロンプト	59
vcaadm によるボードからのログアウト	59
vcaadm でのコマンドの入力	61
コマンドのヘルプの表示	62
対話型モードでの vcaadm プログラムの終了	63
vcaadm による Sun Crypto Accelerator 4000 ボードの初期化	63
▼ 新しいキーストアで Sun Crypto Accelerator 4000 ボードを初期化する	64
既存のキーストアを使用した Sun Crypto Accelerator 4000 ボードの初期化	65
▼ 既存のキーストアを使用して Sun Crypto Accelerator 4000 ボードを初期化する	66
vcaadm によるキーストアの管理	67
名前の要件	67
パスワードの要件	67
パスワードの要件の設定	68
キーストアのセキュリティー管理者の生成	68
キーストアのユーザーの生成	69
ユーザーおよびセキュリティー管理者の一覧表示	70
パスワードの変更	70
ユーザーの有効および無効の切り替え	71
ユーザーの削除	72
セキュリティー管理者の削除	72
マスター鍵のバックアップ	72
バックアップを防ぐためのキーストアのロック	73
vcaadm によるボードの管理	74
自動ログアウト時間の設定	74
ボードの状態の表示	75
新しいファームウェアのインストール	76
Sun Crypto Accelerator 4000 ボードのリセット	76

	Sun Crypto Accelerator 4000 ボードの鍵の交換	77
	Sun Crypto Accelerator 4000 ボードの情報の消去	78
	vcaadm diagnostics コマンドの使用	78
	vcadiag の使用	79
5.	Sun Crypto Accelerator 4000 ボードを使用するための Sun ONE サーバーソフトウェアの構成	83
	Sun ONE Web サーバーのセキュリティー管理	83
	概念および用語	84
	トークンおよびトークンファイル	85
	トークンファイル	85
	バルク暗号化の使用可能および使用不可の切り替え	86
	Sun ONE Web サーバーの構成	87
	パスワード	87
	キーストアのユーザーの生成	88
	▼ キーストアのユーザーを生成する	88
	Sun ONE Web サーバーを使用可能にする方法の概要	89
	Sun ONE Web Server 4.1 のインストールおよび構成	90
	Sun ONE Web Server 4.1 のインストール	90
	▼ Sun ONE Web Server 4.1 をインストールする	90
	▼ 認証データベースを作成する	91
	▼ サーバーの証明書を生成する	93
	▼ サーバーの証明書をインストールする	96
	Sun ONE Web Server 4.1 での SSL の構成	97
	▼ Sun ONE Web Server 4.1 を構成する	97
	Sun ONE Web Server 6.0 のインストールおよび構成	99
	Sun ONE Web Server 6.0 のインストール	99
	▼ Sun ONE Web Server 6.0 をインストールする	99
	▼ 認証データベースを作成する	100

- ▼ サーバーの証明書を生成する 103
- ▼ サーバーの証明書をインストールする 106
- Sun ONE Web Server 6.0 での SSL の構成 107
 - ▼ Sun ONE Web Server 6.0 を構成する 107
- 6. Sun Crypto Accelerator 4000 ボードを使用するための Apache Web サーバーの構成 111
 - Apache Web サーバーでボードを使用するための構成 112
 - Apache Web サーバーを使用可能にする方法 112
 - ▼ Apache Web サーバーを使用可能にする 112
 - 証明書の作成 114
 - ▼ 証明書を作成する 115
- 7. 診断および障害追跡 119
 - SunVTS 診断ソフトウェア 119
 - vca ドライバ用の SunVTS netlbttest および nettest のインストール 120
 - SunVTS ソフトウェアによる vcatest および nettest、netlbttest の実行 121
 - ▼ vcatest を実行する 121
 - vcatest のテストパラメタオプション 123
 - vcatest のコマンド行構文 123
 - ▼ netlbttest を実行する 124
 - ▼ nettest を実行する 126
 - kstat による暗号化の処理状況の確認 128
 - OpenBoot PROM の FCode 自己診断の使用 129
 - ▼ Ethernet FCode 自己診断を実行する 129
 - Sun Crypto Accelerator 4000 ボードの障害追跡 131
 - show-devs 132
 - .properties 132

watch-net 134

A. 仕様 135

Sun Crypto Accelerator 4000 MMF アダプタ 135

コネクタ 135

物理寸法 137

性能仕様 137

電源要件 137

インタフェース仕様 138

環境仕様 138

Sun Crypto Accelerator 4000 UTP アダプタ 138

コネクタ 138

物理寸法 140

性能仕様 140

電源要件 140

インタフェース仕様 141

環境仕様 141

B. Apache Web サーバーの SSL 設定ディレクティブ 143

C. Sun Crypto Accelerator 4000 ボードで使用するアプリケーションの構築 153

D. ソフトウェアライセンス 155

サン以外のベンダーのライセンス条項 158

E. マニュアルページ 163

F. ハードウェアの情報の消去 165

Sun Crypto Accelerator 4000 ハードウェアの情報の消去による出荷時状態への復帰 165

▼ ハードウェアジャンパを使用して Sun Crypto Accelerator 4000 ボード上の情報を消去する 166

G. よく受ける質問 169

再起動時のユーザーの操作をなくすには、Web サーバーをどのように設定すればよいのですか？ 169

▼ 再起動時に Apache Web サーバーを自動起動するために、暗号化された鍵を作成する 169

▼ 再起動時に Sun ONE Web サーバーを自動起動するために、暗号化された鍵を作成する 170

同じサーバーに取り付けた複数のボードに異なる MAC アドレスを割り当てるにはどのようにすればよいのですか？ 170

▼ 端末エミュレータから異なる MAC アドレスを割り当てる 171

▼ OpenBoot PROM レベルで異なる MAC アドレスを割り当てる 171

Apache に Sun Crypto Accelerator 4000 ソフトウェアをインストールしたあとで、Sun Crypto Accelerator 1000 を使用するにはどのようにすればよいのですか？ 171

テストのため、証明書に自己署名するにはどのようにすればよいのですか？ 172

表目次

表 1-1	IPsec の暗号化アルゴリズム	3
表 1-2	SSL の暗号化アルゴリズム	3
表 1-3	サポートする SSL アルゴリズム	4
表 1-4	MMF アダプタの正面パネルの LED 表示	6
表 1-5	UTP アダプタの正面パネルの LED 表示	8
表 1-6	ハードウェアおよびソフトウェアの要件	10
表 1-7	Sun Crypto Accelerator 4000 ソフトウェアの Solaris 8 必須パッチ	11
表 2-1	/cdrom/cdrom0 ディレクトリにあるファイル	17
表 2-2	Sun Crypto Accelerator 4000 のディレクトリ	19
表 3-1	vca ドライバのパラメタおよび状態、説明	24
表 3-2	動作モードパラメタ	26
表 3-3	読み取りおよび書き込みが可能なフロー制御キーワードの説明	27
表 3-4	Gigabit 強制モードパラメタ	28
表 3-5	enable-ipg0 および ipg0 を定義するパラメタ	29
表 3-6	読み取りおよび書き込みが可能なパケット間隔パラメタの値と説明	29
表 3-7	別名読み取り用の RX ブランキングレジスタ	30
表 3-8	RX ランダム早期検出 8 ビットベクトル	30
表 3-9	PCI バスインタフェースパラメタ	31
表 3-10	デバイスパス名	38
表 3-11	ローカル接続のネットワークデバイスパラメタ	40

表 3-12	暗号化ドライバの統計情報	42
表 3-13	Ethernet ドライバの統計情報	43
表 3-14	TX および RX MAC カウンタ	44
表 3-15	現在の Ethernet 接続属性	46
表 3-16	読み取り専用の vca デバイスの機能	46
表 3-17	読み取り専用の接続相手の機能	47
表 3-18	ドライバ固有のパラメタ	48
表 4-1	vcaadm オプション	54
表 4-2	vcaadm のプロンプト変数の定義	59
表 4-3	connect コマンドのオプションパラメタ	60
表 4-4	セキュリティー管理者名およびユーザー名、キーストア名の要件	67
表 4-5	パスワードの要件の設定	68
表 4-6	鍵の種類	77
表 4-7	vcadiag オプション	80
表 5-1	Sun ONE Web サーバーに必要なパスワード	87
表 5-2	要求者情報フィールド	95
表 5-3	証明書をインストールするためのフィールド	97
表 5-4	要求者情報フィールド	105
表 5-5	証明書をインストールするためのフィールド	107
表 7-1	vca ドライバ用の SunVTS netlbttest および nettest の必須ソフトウェア	120
表 7-2	vcatest サブテスト	123
表 7-3	vcatest のコマンド行構文	124
表 A-1	SC コネクタ接続の特性 (IEEE P802.3z)	136
表 A-2	物理寸法	137
表 A-3	性能仕様	137
表 A-4	電源要件	137
表 A-5	インタフェース仕様	138
表 A-6	環境仕様	138
表 A-7	Cat-5 コネクタ接続の特性	139
表 A-8	物理寸法	140

表 A-9	性能仕様	140
表 A-10	電源要件	140
表 A-11	インタフェース仕様	141
表 A-12	環境仕様	141
表 B-1	SSL プロトコル	145
表 B-2	使用できる SSL の暗号	146
表 B-3	SSL の別名	147
表 B-4	暗号の優先順位を設定する特殊文字	148
表 B-5	SSL のクライアントの検証レベル	149
表 B-6	SSL のログレベルの値	150
表 B-7	使用できる SSL オプション	151
表 E-1	Sun Crypto Accelerator 4000 のオンラインマニュアルページ	163

はじめに

このマニュアルでは、Sun™ Crypto Accelerator 4000 ボードの機能およびプロトコル、インタフェースについて説明します。また、システムへのボードの取り付けおよび構成、管理の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 入出力カードを取り付けたサンのプラットフォーム、Sun ONE および Apache Web サーバー、IPsec、SunVTS™ ソフトウェア、認証局からの証明書取得システムのうち、1 つ以上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 4000 ボードの機能およびプロトコル、インタフェースを示し、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 4000 ハードウェアの取り付けおよび取り外し方法と、ソフトウェアのインストールおよび削除方法について説明します。
- 第 3 章では、Sun Crypto Accelerator 4000 の調整可能なドライバパラメータを示し、`ndd` ユーティリティーおよび `vca.conf` ファイルを使用してパラメータを設定する方法について説明します。また、OpenBoot™ PROM インタフェースを使用して接続パラメータを自動ネゴシエーションまたは強制モードに設定する方法と、ネットワークの `hosts` ファイルを設定する方法についても説明します。
- 第 4 章では、Sun Crypto Accelerator 4000 ボードを構成する方法と、`vcaadm` および `vcadiag` ユーティリティーを使用してキーストアを管理する方法について説明します。
- 第 5 章では、Sun ONE Web サーバーで Sun Crypto Accelerator 4000 ボードを使用するための構成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 4000 ボードを使用するための構成方法について説明します。
- 第 7 章では、SunVTS 診断アプリケーションおよびオンボードの FCode 自己診断を使用して、Sun Crypto Accelerator 4000 ボードを診断する方法について説明します。また、OpenBoot PROM コマンドを使用した障害追跡方法についても説明します。
- 付録 A では、Sun Crypto Accelerator 4000 ボードの仕様を示します。
- 付録 B では、Sun Crypto Accelerator 4000 ソフトウェアを使用して Apache Web サーバーの 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 C では、Sun Crypto Accelerator 4000 ボードに付属するソフトウェアと、ボードの高速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方法について説明します。
- 付録 D では、サン以外のベンダーのソフトウェアを規定する注意およびライセンスについて説明します。Sun Crypto Accelerator 4000 ボードで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。
- 付録 E では、Sun Crypto Accelerator 4000 のコマンドの説明と、各コマンドに対応するオンラインマニュアルページを示します。
- 付録 F では、Sun Crypto Accelerator 4000 ボードを、出荷時の状態である failsafe モードに戻す (情報を消去する) 方法について説明します。
- 付録 G では、よく受ける質問 (FAQ) の回答を示します。

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。

- 『Solaris Sun ハードウェアマニュアル』
- Solaris オペレーティング環境についてのオンラインマニュアルは、下記の URL から入手できます。
<http://docs.sun.com>
- 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。	<code>.login</code> ファイルを編集します。 <code>ls -a</code> を実行します。 <code>% You have mail.</code>
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。	<code>rm filename</code> と入力します。 <code>rm ファイル名</code> 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

各言語対応版を含むサンの各種マニュアルは、次の URL から表示または印刷、購入できます。

<http://www.sun.com/documentation>

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. (817-2329-10) 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

製品の概要

この章では、Sun Crypto Accelerator 4000 ボードの概要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「製品の機能」
 - 5 ページの「ハードウェアの概要」
 - 10 ページの「ハードウェアおよびソフトウェアの要件」
-

製品の機能

Sun Crypto Accelerator 4000 ボードは、Gigabit Ethernet ベースのネットワークインタフェースカードで、サンのサーバー上で IPsec と SSL (対称型および非対称型) の暗号化処理を高速化する暗号ハードウェアが組み込まれています。暗号化されていないネットワークトラフィックを標準的な Gigabit Ethernet ネットワークインタフェースとして処理するとともに、暗号化された IPsec トラフィックを内蔵の暗号ハードウェアによって標準的なソフトウェアソリューションより高いスループットで処理します。

主なプロトコルおよびインタフェース

Sun Crypto Accelerator 4000 ボードは、Ethernet の標準的な最小および最大フレームサイズ (64 ~ 1518 バイト) およびフレーム形式を取り扱い、次の標準規格およびプロトコルに準拠する、既存の Ethernet デバイスとの相互運用が可能です。

- フルサイズ PCI 33/36 Mhz、32/64 ビット
- IEEE 802.3 CSMA/CD (Ethernet)
- IEEE 802.2 論理リンク制御
- SNMP (一部の MIB)
- 全二重モードおよび半二重モードの Gigabit Ethernet インタフェース (IEEE 802.z)
- 汎用のデュアル電圧信号 (3.3 V および 5 V)

主な機能

- 銅または光ファイバインタフェースの Gigabit Ethernet
- IPsec および SSL 暗号化機能を高速化
- セッション確立の速度は、最大で 1 秒あたり 4300 回
- バルクデータの暗号化速度は、最大で 800 Mbps
- 最大 2048 ビットの RSA 暗号化を提供
- 3DES によるバルク暗号化を、最大で 10 倍高速化
- Sun ONE Web サーバーに、安全性を強化し鍵の管理を簡素化するための、改ざん防止を保証するセキュリティー鍵および証明書の集中管理機能を提供
- FIPS 140-2 レベル 3 認証に対応した設計
- CPU 利用率が低いため、サーバーシステムが使用できるリソースおよび帯域幅が拡大
- 非公開鍵を安全に保存および管理
- サンのミッドフレームサーバーおよびハイエンドサーバーの、動的再構成 (DR) および冗長性/フェイルオーバーをサポート
- 複数 CPU 間の RX パケットの負荷を均衡化
- フロー制御を完全サポート (IEEE 802.3x)

Sun Crypto Accelerator 4000 ボードは、FIPS (Federal information Processing Standard) 140-2 のレベル 3 で規定された暗号化モジュールのセキュリティー要件に準拠するように設計されています。

サポートするアプリケーション

- Solaris 8 および Solaris 9 オペレーティング環境 (IPsec VPN)
- Sun ONE Web サーバー
- Apache Web サーバー

サポートする暗号化プロトコル

このボードは、次のプロトコルをサポートします。

- IKE を含む、IPv4 および IPv6 の IPsec
- SSLv2、SSLv3、TLSv1

このボードは、次の IPsec 機能を高速化します。

- ESP (DES、3DES) 暗号化

このボードは、次の SSL 機能を高速化します。

- クライアントとサーバー間の、一連の暗号化パラメタおよび秘密鍵の安全な構築
- 鍵のボード上での安全な保管と、ボードから出力する際の暗号化

診断のサポート

- OpenBoot PROM によるユーザー実行型自己診断
- SunVTS 診断テスト

暗号化アルゴリズムの高速化

Sun Crypto Accelerator 4000 ボードは、ハードウェアおよびソフトウェアの両方で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しているのは、暗号化アルゴリズムを高速化するための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するよう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するように設計されているものもあります。ハードウェアによる高速化では、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デバイスに移動し、結果をユーザーアプリケーションに戻すため、余分なコストがかかります。暗号化アルゴリズムの中には、高度に調整されたソフトウェアによって、専用のハードウェアで実行された場合と同様に高速に処理できるものもあります。

サポートする暗号化アルゴリズム

Sun Crypto Accelerator 4000 のドライバ (vca) は、最大のスループットが得られるように、各暗号要求を調べて、もっとも高速化できる場所 (ホストプロセッサまたは Sun Crypto Accelerator 4000) を決定します。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。

Sun Crypto Accelerator 4000 ボードは、次の IPsec アルゴリズムを高速化します。

表 1-1 IPsec の暗号化アルゴリズム

種類	アルゴリズム
対称型	DES、3DES

Sun Crypto Accelerator 4000 ボードは、次の SSL アルゴリズムを高速化します。

表 1-2 SSL の暗号化アルゴリズム

種類	アルゴリズム
対称型	DES、3DES、ARCFOUR
非対称型	Diffie-Hellman (Apache のみ) および RSA (最大 2048 ビットの鍵)、DSA
ハッシュ	MD5、SHA1

SSL 高速化

表 1-3 に、ハードウェアにオフロードされる SSL 高速化アルゴリズムと、Sun ONE Web サーバーおよび Apache Web サーバーで使用できるソフトウェアアルゴリズムを示します。

表 1-3 サポートする SSL アルゴリズム

アルゴリズム	Sun ONE 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
ARCFOUR		X		
Diffie-Hellman			X	X
DES	X	X	X	X
3DES	X	X	X	X
MD5	X	X		
SHA1	X	X		

バルク暗号化

Sun ONE サーバーソフトウェアの Sun Crypto Accelerator 4000 のバルク暗号化機能は、デフォルトでは使用不可になっています。この機能を手動で使用可能にするには、ファイルを作成して Sun ONE サーバーソフトウェアを再起動します。

Sun ONE サーバーソフトウェアで Sun Crypto Accelerator 4000 ボードのバルク暗号化機能を使用可能にするには、`/etc/opt/SUNWconn/cryptov2/` ディレクトリ内に `sslreg` という名前の空のファイルを作成して、サーバーソフトウェアを再起動します。

```
# touch /etc/opt/SUNWconn/cryptov2/sslreg
```

バルク暗号化機能を使用不可にするには、`sslreg` ファイルを削除して、サーバーソフトウェアを再起動します。

```
# rm /etc/opt/SUNWconn/cryptov2/sslreg
```

Apache Web サーバーソフトウェアのバルク暗号化機能は、デフォルトで使用可能であり、使用不可にはできません。

ハードウェアの概要

Sun Crypto Accelerator 4000 ハードウェアは、106.68 mm×312.00 mm (4.2 インチ×12.283 インチ) の、フルサイズ PCI Gigabit Ethernet アダプタタイプの暗号化アクセラレータで、サンのサーバーで IPsec および SSL の性能を向上させます。

IPsec ハードウェアの高速化

Sun Crypto Accelerator 4000 ボードは、ハードウェア内で IPsec パケットを暗号化および復号化することで、暗号化演算による高い負荷を SPARC™ プロセッサからオフロードします。また、この暗号ハードウェアは、ほかのアプリケーションが使用する一般的な非対称型および対称型の暗号化演算をサポートし、乱数を生成するハードウェアを備えています。

注 – Sun Crypto Accelerator 4000 ボードを使用して IPsec を高速化する場合に、IPsec を構成または調整する必要はありません。Sun Crypto Accelerator 4000 パッケージをインストールして再起動するだけです。

Sun Crypto Accelerator 4000 ボードおよびパッケージをインストールすると、既存の IPsec も、インストール後に導入する IPsec も、コア Solaris ソフトウェアに代わって Sun Crypto Accelerator 4000 ボードを使用するようになります。このボードは、表 1-1 に示す IPsec アルゴリズムを処理します。Sun Crypto Accelerator 4000 ボードがサポートしていない IPsec アルゴリズムは、引き続きコア Solaris 暗号化ソフトウェアで処理されます。IPsec の設定については、<http://docs.sun.com> の、Solaris System Administrator Collection に含まれている『Solaris のシステム管理』を参照してください。

Sun Crypto Accelerator 4000 MMF アダプタ

Sun Crypto Accelerator 4000 MMF アダプタは、シングルポートの Gigabit Ethernet 光ファイバー PCI バスカードで、1000 Mbps Ethernet ネットワークのみで動作します。

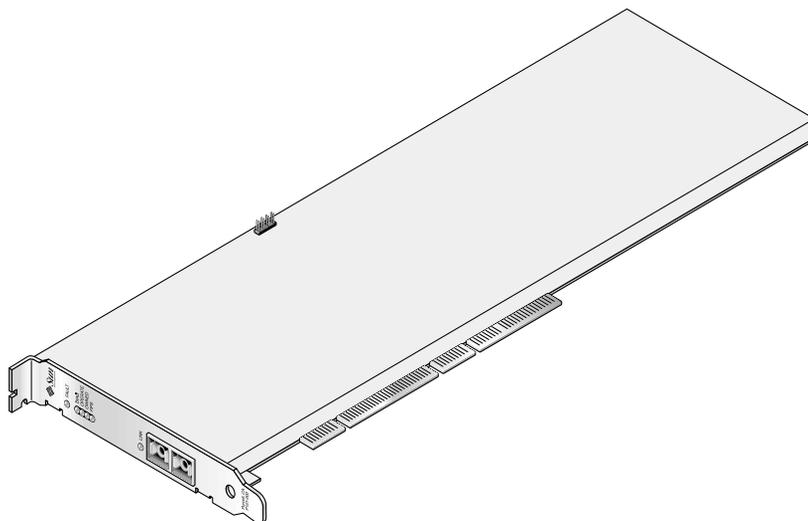


図 1-1 Sun Crypto Accelerator 4000 MMF アダプタ

LED 表示

表 1-4 を参照してください。

表 1-4 MMF アダプタの正面パネルの LED 表示

ラベル	点灯状態が示す意味	色
Fault	ボードが HALTED (致命的なエラー) 状態である場合、または下層のハードウェアの初期化で障害が発生した場合に点灯。 起動処理中にエラーが発生した場合に点滅。	赤
Diag	POST および DIAGNOSTICS、FAILSAFE (ファームウェアがアップグレードされていない) 状態で点灯。 診断の実行中に点滅。	緑

表 1-4 MMF アダプタの正面パネルの LED 表示 (続き)

ラベル	点灯状態が示す意味	色
Operate	POST および DIAGNOSTICS、DISABLED (ドライバが組み込まれていない) 状態で点灯。 IDLE および OPERATIONAL、FAILSAFE 状態で点滅。	緑
Owned	セキュリティー管理者が vcaadm でボードを初期化した場合に点灯。詳細は、63 ページの「vcaadm による Sun Crypto Accelerator 4000 ボードの初期化」を参照。 情報消去用のジャンパが取り付けられている場合に点滅。	緑
FIPS Mode	FIPS 140-2 レベル 3 認証モードで動作している場合に点灯。 FIPS モードでない場合に消灯。	緑
Link	接続を確立している場合に点灯。	緑

Sun Crypto Accelerator 4000 UTP アダプタ

Sun Crypto Accelerator 4000 UTP アダプタは、シングルポートの Gigabit Ethernet 銅ベース PCI バスカードで、10 または 100、1000 Mbps の Ethernet ネットワークで動作するように設定できます。

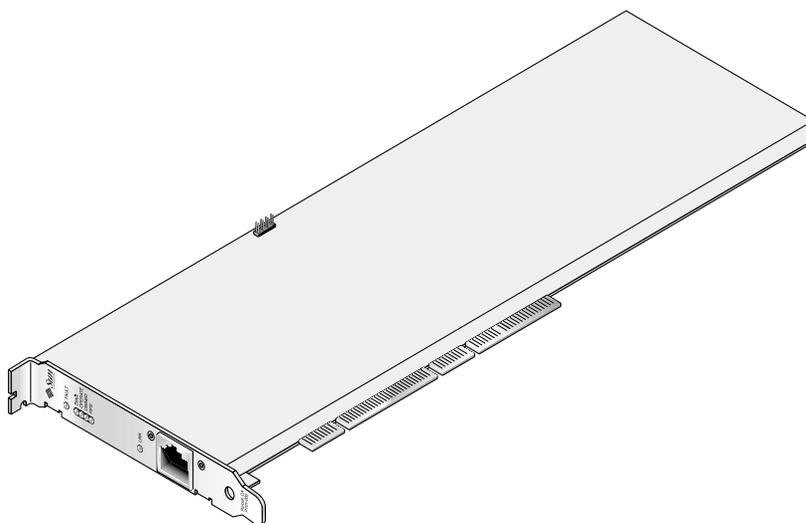


図 1-2 Sun Crypto Accelerator 4000 UTP アダプタ

LED 表示

表 1-5 を参照してください。

表 1-5 UTP アダプタの正面パネルの LED 表示

ラベル	点灯状態が示す意味	色
Fault	ボードが HALTED (致命的なエラー) 状態である場合、または下層のハードウェアの初期化で障害が発生した場合に点灯。 起動処理中にエラーが発生した場合に点滅。	赤
Diag	POST および DIAGNOSTICS、FAILSAFE (ファームウェアがアップグレードされていない) 状態で点灯。 診断の実行中に点滅。	緑
Operate	POST および DIAGNOSTICS、DISABLED (ドライバが組み込まれていない) 状態で点灯。 IDLE および OPERATIONAL、FAILSAFE 状態で点滅。	緑
Owned	セキュリティー管理者が vcaadm でボードを初期化した場合に点灯。詳細は、63 ページの「vcaadm による Sun Crypto Accelerator 4000 ボードの初期化」を参照。 情報消去用のジャンパが取り付けられている場合に点滅。	緑
FIPS Mode	FIPS 140-2 レベル 3 認証モードで動作している場合に点灯。 FIPS モードでない場合に消灯。	緑
1000 (ラベルなし)	Gigabit Ethernet を使用している場合に点灯。	緑
Activity (ラベルなし)	接続上での送信中または受信中に点灯。	オレンジ
Link	接続を確立している場合に点灯。	緑

注 – Sun ONE 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。

動的再構成 (DR) および高可用性 (HA)

Sun Crypto Accelerator 4000 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 4000 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よう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 4000 ボードを取り付けることができます。Sun Crypto Accelerator 4000 ハードウェアで障害が発生した場合には、ソフトウェア層が障害を検出し、使用できる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ボードを削除します。Sun Crypto Accelerator 4000 は、ハードウェア資源の減少に適応するよう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、残りのボードにスケジュールされます。

Sun Crypto Accelerator 4000 ハードウェアは、鍵長の長い鍵を生成するときに、高品質のエントロピ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 4000 ボードを取り外すと、鍵長の長い鍵は、それより低い品質のエントロピソースから生成されるようになります。

負荷分散

Sun Crypto Accelerator 4000 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、後続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次のボードのキューに入れられます。このキューイング機能は、ボードに要求をまとめることによって、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 1-6 に、Sun Crypto Accelerator 4000 アダプタの、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 1-6 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 Fire™ V120、V210、V240、280R、V480、V880、4800、4810、6800、12K、15K; Netra™ 20 (1w4); Sun Blade™ 100、150、1000、2000
オペレーティング環境	Solaris 8 2/02 以降の互換バージョン (IPsec の高速化には Solaris 9 が必要)

必須パッチ

必須パッチの詳細は、『Sun Crypto Accelerator 4000 ボードご使用にあたって』を参照してください。

システムで Sun Crypto Accelerator 4000 ボードを動作させるために、次のパッチが必要になる場合があります。Solaris アップデートには、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、後述の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。

パッチは、次の Web サイトからダウンロードできます。
<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。

Apache Web サーバーパッチ

Apache Web サーバーを使用する場合は、パッチ 109234-09 もインストールする必要があります。SUNWkcl2a パッケージを追加すると、システムには Apache Web サーバー用の mod_ssl 1.3.26 が構成されます。

Solaris 8 のパッチ

この製品が使用する Solaris 8 の必須パッチと推奨パッチを示します。表 1-7 に、必須パッチを示します。

表 1-7 Sun Crypto Accelerator 4000 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

Solaris 9 のパッチ

現在のところ、Solaris 9 の必須パッチはありません。

第2章

Sun Crypto Accelerator 4000 ボードの取り付け

この章では、Sun Crypto Accelerator 4000 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。

- 13 ページの「ボードの取り扱い」
- 14 ページの「ボードの取り付け」
- 16 ページの「Sun Crypto Accelerator 4000 ソフトウェアのインストール」
- 19 ページの「ディレクトリおよびファイル」
- 21 ページの「ソフトウェアの削除」

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 4000 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を記載しています。システム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する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する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、取り外したねじを保管しておきます。
5. Sun Crypto Accelerator 4000 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、背面側の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. OpenBoot PROM (OBP) の `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
.
/chosen
/packages
/upa@8,480000/SUNW,ffb@0,0
/pci@8,600000/network@1
/pci@8,600000/SUNW,qlc@4
/pci@8,600000/SUNW,qlc@4/fp@0,0
.
```

この例では、`/pci@8,600000/network@1` が Sun Crypto Accelerator 4000 ボードのデバイスパスになります。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 4000 のデバイス属性が正しく設定されているかどうかを確認するには、ok プロンプトからデバイスパスに進み、.properties を入力して属性の一覧を表示します。

```
ok cd /pci@8,60000/network@1
ok .properties
assigned-addresses      82000810 00000000 00102000 00000000 00002000
                        81000814 00000000 00000400 00000000 00000100
                        82000818 00000000 00200000 00000000 00200000
                        82000830 00000000 00400000 00000000 00100000
d-fru-len               00 00 00 00
d-fru-off               00 00 e8 00
d-fru-dev               eeprom
s-fru-len               00 00 08 00
s-fru-off               00 00 e0 00
s-fru-dev               eeprom
compatible              70 63 69 38 30 38 36 2c 62 35 35 35 2e 31 30 38
reg                     00000800 00000000 00000000 00000000 00000000
                        02000810 00000000 00000000 00000000 00002000
                        02000814 00000000 00000000 00000000 00000100
                        02000818 00000000 00000000 00000000 00200000
                        02000830 00000000 00000000 00000000 00100000
address-bits            00 00 00 30
max-frame-size          00 00 40 00
network-interface-type ethernet
device_type             network
name                    network
local-mac-address       08 00 20 aa bb cc
version                 Sun PCI Crypto Accelerator 4000 1000Base-T FCode
12.11.13 02/10/31
phy-type                mif
board-model             501-6039
model                   SUNW,pci-vca
fcode-rom-offset        00000000
66mhz-capable
fast-back-to-back
devsel-speed            00000001
class-code              00100000
interrupts              00000001
latency-timer           00000040
cache-line-size         00000010
max-latency             00000040
min-grant                00000040
subsystem-id            00003de8
subsystem-vendor-id     0000108e
revision-id             00000002
device-id               0000b555
vendor-id               00008086
```

Sun Crypto Accelerator 4000 ソフトウェアのインストール

Sun Crypto Accelerator 4000 ソフトウェアは、Sun Crypto Accelerator 4000 CD に収録されています。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、10 ページの「必須パッチ」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. システムに接続されている CD-ROM ドライブに、Sun Crypto Accelerator 4000 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 4000 ボードインストールマニュアル』(このマニュアル) 『Sun Crypto Accelerator 4000 ボードご使用にあたって』
Packages	次の Sun Crypto Accelerator 4000 のソフトウェアパッケージが含まれます。
SUNWkc12r	暗号化カーネルコンポーネント
SUNWkc12u	暗号化管理ユーティリティおよびライブラリ
SUNWkc12a	Apache の SSL サポート (オプション)
SUNWkc12m	暗号化管理マニュアルページ (オプション)
SUNWvcar	VCA Crypto アクセラレータ (ルート)
SUNWvcau	VCA Crypto アクセラレータ (ユーザー)
SUNWvcaa	VCA 管理
SUNWvcaw	VCA ファームウェア
SUNWvcamm	VCA Crypto アクセラレータマニュアルページ (オプション)
SUNWvcav	VCA Crypto アクセラレータの SunVTS テスト (オプション)
SUNWkc12o	SSL 開発ツールおよびライブラリ (オプション)
SUNWkc12i.u	KCLv2 Crypto を使用する IPsec の高速化 (オプション)

必須パッケージは、オプションパッケージをインストールする前に、特定の順序でインストールする必要があります。必須パッケージをインストールしたあとは、オプションパッケージを任意の順序でインストールおよび削除できます。

Web サーバーとして Apache を使用する場合に限り、オプションの SUNWkc12a 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、オプションの SUNWkc12o 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、オプションの SUNWvcav パッケージをインストールします。SUNWvcav パッケージをインストールする場合は、SunVTS 4.4 ~ 5.x をインストールしておく必要があります。

注 - オプションの SUNWkc12i.u パッケージには、Sun Crypto Accelerator 4000 CD 上でのみ .u 拡張子が付いています。このパッケージをインストールすると、名前は SUNWkc12i に変更されます。CD 上で .u 拡張子が付いているのは、パッケージが sun4u アーキテクチャー固有であることを示すためです。

2. 次のように入力して、必須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 . SUNWkcl2r SUNWkcl2u SUNWvcar SUNWvcau SUNWvcaa SUNWvcaw
```

3. (任意) 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 SUNWkcl2r SUNWkcl2u SUNWvcar SUNWvcau SUNWvcaa SUNWvcaw
system SUNWkcl2r   Cryptography Kernel Components
system SUNWkcl2u   Cryptographic Administration Utility and Libraries
system SUNWvcar    VCA Crypto Accelerator (Root)
system SUNWvcau    Crypto Accelerator/Gigabit Ethernet (Usr)
system SUNWvcaa    VCA Administration
system SUNWvcaw    VCA Firmware
```

4. (任意) prtdiag 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。詳細は、prtdiag(1m) のオンラインマニュアルページを参照してください。

```
# prtdiag -v
```

5. (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。

```
# modinfo | grep Crypto
62  1317f62  20b1f 198   1  vca (VCA Crypto/Ethernet v1.102)
63  13360e9  12510 200   1  kcl2 (Kernel Crypto Library v1.148)
197 136d5d6  19b0 199   1  vact1 (VCA Crypto Control v1.19)
```

オプションパッケージのインストール

Apache Web サーバーの SSL サポートと、暗号化管理マニュアルページを提供するオプションパッケージのみをインストールするには、次のように入力します。

```
# cd /cdrom/cdrom0/Packages
# pkgadd -d . SUNWkcl2a SUNWkcl2m
```

オプションのソフトウェアパッケージをすべてインストールするには、次のように入力します。

```
# cd /cdrom/cdrom0/Packages
# pkgadd -d . SUNWkcl2a SUNWkcl2m SUNWvcamn SUNWvcav SUNWkcl2o SUNWkcl2i.u
```

この例のオプションパッケージの内容の詳細は、表 2-1 を参照してください。

ディレクトリおよびファイル

表 2-2 に、Sun Crypto Accelerator 4000 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 4000 のディレクトリ

ディレクトリ	内容
/etc/opt/SUNWconn/vca/keydata	キーストアデータ (暗号化されている)
/opt/SUNWconn/cryptov2/bin	ユーティリティ
/opt/SUNWconn/cryptov2/lib	サポートライブラリ
/opt/SUNWconn/cryptov2/sbin	管理コマンド

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。

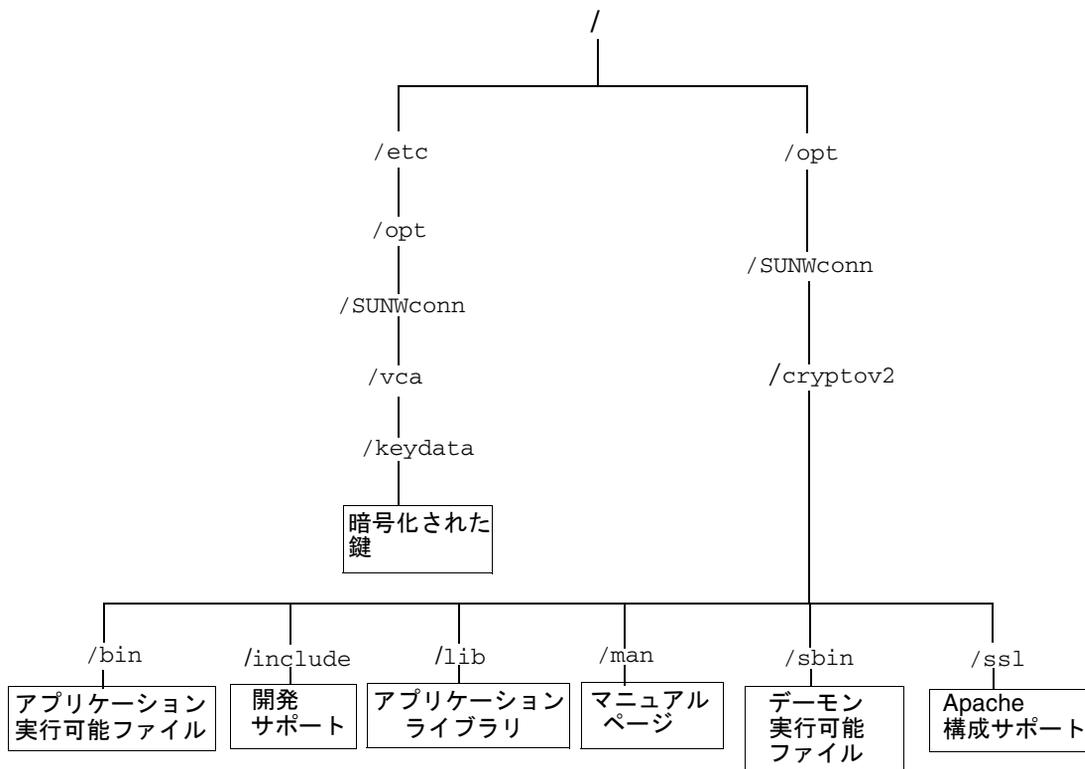


図 2-1 Sun Crypto Accelerator 4000 ディレクトリおよびファイル

注 - ボードのハードウェアを取り付けて、ソフトウェアをインストールしたあとは、構成およびキースタの情報によってボードを初期化する必要があります。ボードを初期化する方法については、63 ページの「vcaadm による Sun Crypto Accelerator 4000 ボードの初期化」を参照してください。

ソフトウェアの削除

すでにキーストアを作成していた場合は (67 ページの「vcaadm によるキーストアの管理」を参照)、ソフトウェアを削除する前に、Sun Crypto Accelerator 4000 ボードの構成に使用したキーストア情報を削除する必要があります。zeroize コマンドを実行するとすべての鍵素材が削除されますが、Sun Crypto Accelerator 4000 ボードを取り付けた物理ホストのファイルシステムに格納されているキーストアファイルは削除されません。zeroize コマンドの詳細は、78 ページの「Sun Crypto Accelerator 4000 ボードの情報の消去」を参照してください。システムに格納されたキーストアファイルを削除するには、スーパーユーザーになってキーストアファイルを削除します。キーストアを作成していない場合は、この手順を省略してください。



注意 – 使用中のキーストア、またはほかのユーザーおよびキーストアと共有しているキーストアは削除しないでください。キーストアを自由に参照するには、Web サーバーか管理サーバー、またはその両方の停止が必要になる場合があります。



注意 – Sun Crypto Accelerator 4000 ソフトウェアを削除する前に、Sun Crypto Accelerator 4000 ボードを使用する 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せずに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、前述の手順で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 – インストールしたパッケージは、次に示す順で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、カーネルモジュールがインストールされたままになります。

すべてのパッケージをインストールしていた場合は、次の順に削除します。

```
# pkgrm SUNWkcl2o SUNWvcav SUNWvcar SUNWkcl2a SUNWkcl2u SUNWkcl2r  
SUNWvcamn SUNWkcl2m SUNWkcl2i SUNWvcaa SUNWvcaw SUNWvcaw
```

注 – SunVTS が動作している状態で、Sun Crypto Accelerator 4000 ボードの SunVTS テスト (SUNWvcav) をインストールまたは削除した場合には、その作業のあと、使用できるテストを更新するためにシステムの再プローブの実行が必要になることがあります。詳細は、SunVTS のマニュアルを参照してください。

ドライバパラメタの設定

この章では、Sun Crypto Accelerator 4000 の UTP および MMF Ethernet アダプタが使用する vca デバイスドライバパラメタの設定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。

- 23 ページの「Sun Crypto Accelerator 4000 Ethernet デバイスドライバ (vca) のパラメタ」
- 32 ページの「vca ドライバパラメタの設定」
- 40 ページの「OpenBoot PROM を使用した接続パラメタの自動ネゴシエーションモードおよび強制モードの切り替え」
- 42 ページの「Sun Crypto Accelerator 4000 暗号化ドライバおよび Ethernet ドライバの動作に関する統計情報」
- 50 ページの「ネットワーク構成」

Sun Crypto Accelerator 4000 Ethernet デバイスドライバ (vca) のパラメタ

vca デバイスドライバは、Sun Crypto Accelerator 4000 の UTP および MMF Ethernet デバイスを制御します。vca ドライバは、Sun Crypto Accelerator 4000 用の UNIX の pci 名前属性である pci108e、3de8 に関連付けられています (108e はベンダー ID、3de8 は PCI デバイス ID)。

vca デバイスドライバパラメタを手動で設定することで、システムに合わせて各 Sun Crypto Accelerator 4000 デバイスをカスタマイズできます。この節では、ボードが使用する Sun Crypto Accelerator 4000 Ethernet デバイスの機能の概要について説明します。また、使用できる vca デバイスドライバパラメタの一覧を示し、それらのパラメタの設定方法についても説明します。

Sun Crypto Accelerator 4000 の Ethernet UTP および MMF PCI アダプタは、35 ページの「自動ネゴシエーションモードまたは強制モードの設定」に示す速度およびモードで動作できます。デフォルトでは、vca デバイスは接続先 (接続相手) と自動ネゴ

シエーションモードで動作し、speed および duplex、link-clock パラメタに共通する動作モードを設定します。link-clock パラメタは、ボードが 1000 Mbps で動作している場合にのみ有効です。vca デバイスでは、これらのパラメタに強制モードを設定することもできます。



注意 – 接続を正常に確立するには、speed および duplex、link-clock (1000 Mbps のみ) の各パラメタを、接続相手に合わせて自動ネゴシエーションモードまたは強制モードに設定して動作させる必要があります。これらのパラメタを接続相手と同じモードにして動作していないと、ネットワークエラーが発生します。詳細は、40 ページの「OpenBoot PROM を使用した接続パラメタの自動ネゴシエーションモードおよび強制モードの切り替え」を参照してください。

ドライバパラメタ値および定義

表 3-1 に、vca デバイスドライバのパラメタおよび設定を示します。

表 3-1 vca ドライバのパラメタおよび状態、説明

パラメタ	状態	説明
instance	読み取りおよび書き込み可	デバイスインスタンス
adv-autoneg-cap	読み取りおよび書き込み可	動作モードパラメタ
adv-1000fdx-cap	読み取りおよび書き込み可	動作モードパラメタ (MMF アダプタのみ)
adv-1000hdx-cap	読み取りおよび書き込み可	動作モードパラメタ
adv-100fdx-cap	読み取りおよび書き込み可	動作モードパラメタ (UTP アダプタのみ)
adv-100hdx-cap	読み取りおよび書き込み可	動作モードパラメタ (UTP アダプタのみ)
adv-10fdx-cap	読み取りおよび書き込み可	動作モードパラメタ (UTP アダプタのみ)
adv-10hdx-cap	読み取りおよび書き込み可	動作モードパラメタ (UTP アダプタのみ)
adv-asmpause-cap	読み取りおよび書き込み可	フロー制御パラメタ
adv-pause-cap	読み取りおよび書き込み可	フロー制御パラメタ
pause-on-threshold	読み取りおよび書き込み可	フロー制御パラメタ
pause-off-threshold	読み取りおよび書き込み可	フロー制御パラメタ
link-master	読み取りおよび書き込み可	1 Gbps の速度の強制モードパラメタ
enable-ipg0	読み取りおよび書き込み可	パケット送信前の追加遅延を有効に設定
ipg0	読み取りおよび書き込み可	パケット送信前の追加遅延
ipg1	読み取りおよび書き込み可	パケット間隔パラメタ

表 3-1 vca ドライバのパラメタおよび状態、説明 (続き)

パラメタ	状態	説明
ipg2	読み取りおよび書き込み可	パケット間隔パラメタ
rx-intr-pkts	読み取りおよび書き込み可	受信割り込みブランキング値
rx-intr-time	読み取りおよび書き込み可	受信割り込みブランキング値
red-dv4to6k	読み取りおよび書き込み可	ランダム早期検出およびパケットドロップベクトル
red-dv6to8k	読み取りおよび書き込み可	ランダム早期検出およびパケットドロップベクトル
red-dv8to10k	読み取りおよび書き込み可	ランダム早期検出およびパケットドロップベクトル
red-dv10to12k	読み取りおよび書き込み可	ランダム早期検出およびパケットドロップベクトル
tx-dma-weight	読み取りおよび書き込み可	PCI インタフェースパラメタ
rx-dma-weight	読み取りおよび書き込み可	PCI インタフェースパラメタ
infinite-burst	読み取りおよび書き込み可	PCI インタフェースパラメタ
disable-64bit	読み取りおよび書き込み可	PCI インタフェースパラメタ

通知される接続パラメタ

ここに示すパラメタは、speed および duplex 接続パラメタを送受信して vca ドライバから接続相手に情報を通知するかどうかを決定します。表 3-2 に、動作モードパラメタおよびそのデフォルト値を示します。

注 - パラメタの初期設定が 0 の場合は変更することができません。0 の初期設定を変更しようとしても、0 に戻ります。デフォルトでは、これらのパラメタはその vca デバイスの機能に応じて設定されています。

表 3-2 に示すように、Sun Crypto Accelerator 4000 UTP アダプタの通知される接続パラメタと、Sun Crypto Accelerator 4000 MMF アダプタの接続パラメタには違いがあります。

表 3-2 動作モードパラメタ

パラメタ	説明
次のパラメタは、Sun Crypto Accelerator 4000 の UTP および MMF アダプタに共通です。	
adv-autoneg-cap	ハードウェアが通知するローカルインタフェースの機能 0 = 強制モード 1 = 自動ネゴシエーション (デフォルト)
次のパラメタは、Sun Crypto Accelerator 4000 の MMF アダプタだけで有効です。	
adv-1000fdx-cap	ハードウェアが通知するローカルインタフェースの機能 0 = 1000 Mbps、全二重不可 1 = 1000 Mbps、全二重可 (デフォルト)
次のパラメタは、Sun Crypto Accelerator 4000 の UTP および MMF アダプタに共通です。	
adv-1000hdx-cap	ハードウェアが通知するローカルインタフェースの機能 0 = 1000 Mbps、半二重不可 1 = 1000 Mbps、半二重可 (デフォルト)
次のパラメタは、Sun Crypto Accelerator 4000 の UTP アダプタだけで有効です。	
adv-100fdx-cap	ハードウェアが通知するローカルインタフェースの機能 0 = 100 Mbps、全二重不可 1 = 100 Mbps、全二重可 (デフォルト)
adv-100hdx-cap	ハードウェアが通知するローカルインタフェースの機能 0 = 100 Mbps、半二重不可 1 = 100 Mbps、半二重可 (デフォルト)
adv-10fdx-cap	ハードウェアが通知するローカルインタフェースの機能 0 = 10 Mbps、全二重不可 1 = 10 Mbps、全二重可 (デフォルト)
adv-10hdx-cap	ハードウェアが通知するローカルインタフェースの機能 0 = 10 Mbps、半二重不可 1 = 10 Mbps、半二重可 (デフォルト)

前述のパラメタがすべて 1 に設定されている場合、自動ネゴシエーションは使用できる最高速度を選択します。パラメタがすべて 0 に設定されている場合は、次のエラーメッセージが表示されます。

```
NOTICE: Last setting will leave vca0 with no link capabilities.
WARNING: vca0: Restoring previous setting.
```

注 – この例では、vca0 が Sun Crypto Accelerator 4000 ボードのデバイス名です。vca の文字列は、すべての Sun Crypto Accelerator 4000 ボードに共通です。この文字列には、必ずボードのデバイスインスタンス番号が続きます。したがって、vca0 ボードのデバイスインスタンス番号は 0 です。

フロー制御パラメタ

vca デバイスは、IEEE 802.3x のフレームベースのリンクレベルフロー制御プロトコルに準拠するポーズフレームのソーシング (送信) およびターミネーティング (受信) に対応しています。vca デバイスは、受信したフロー制御フレームに応じて転送レートを落とすことができます。また、接続相手がこの機能をサポートしている場合には、フロー制御フレームを送信して、接続相手の転送レートを落とすこともできます。デフォルトでは、自動ネゴシエーション中に、ドライバはポーズフレームの送信および受信が可能であることを通知します。

表 3-3 に、フロー制御のキーワードおよびその機能を示します。

表 3-3 読み取りおよび書き込みが可能なフロー制御キーワードの説明

キーワード	説明
adv-asmppause-cap	MMF および UTP アダプタは、非対称方式のポーズをサポートします。したがって、vca デバイスは一方向でのみ一時停止することができます。 0 = オフ (デフォルト) 1 = オン
adv-pause-cap	このパラメタには、adv-asmppause-cap の値に応じて、2 つの意味があります。(デフォルト = 0)
	パラメタ値 + パラメタ値 = 説明
	adv-asmppause-cap= adv-pause-cap=
1	1 または 0 adv-pause-cap によって、どちらの方向のポーズフレームを有効にするかを決定します。

表 3-3 読み取りおよび書き込みが可能なフロー制御キーワードの説明 (続き)

キーワード	説明		
	1	1	ポーズフレームは受信されますが、送信されません。
	1	0	ポーズフレームは送信されますが、受信されません。
	0	1	ポーズフレームは送受信されます。
	0	1 または 0	adv-pause-cap によって、ポーズ機能のオンまたはオフを決定します。
pause-on-threshold	受信 (RX) FIFO での、64 バイトブロック数を設定します。この設定に応じて、ボードが XON-PAUSE フレームを生成します。		
pause-off-threshold	RX FIFO での、64 バイトブロック数を設定します。この設定に応じて、ボードが XOFF-PAUSE フレームを生成します。		

Gigabit 強制モードパラメタ

Gigabit 接続では、このパラメタによって link-master を決定します。通常は、スイッチを接続マスターとして使用可能にします。その場合は、このパラメタを変更する必要はありません。そうでない場合は、link-master パラメタによって、vca デバイスを接続マスターとして使用可能にすることができます。

表 3-4 Gigabit 強制モードパラメタ

パラメタ	説明
link-master	1 に設定した場合、接続相手がスレーブであれば、マスターの動作が有効になります。 0 に設定した場合、接続相手がマスターであれば、スレーブの動作が有効になります (デフォルト)。

パケット間隔パラメタ

vca デバイスは、プログラム可能な enable-ipg0 と呼ぶモードをサポートします。

enable-ipg0 を有効 (デフォルト) にしてパケットを送信すると、vca デバイスは追加の遅延時間を設定します。ipg0 パラメタで設定した遅延時間が、ipg1 および ipg2 パラメタで設定した遅延時間に追加されます。ipg0 で追加遅延を設定することによって衝突を低減できます。

enable-ipg0 が無効の状態では、ipg0 の値は無視され、追加遅延は設定されません。この場合は、ipg1 および ipg2 によって指定する遅延だけが使用されます。ほかのシステムから大量の連続パケットが継続して送信される場合は、enable-ipg0 を無効にしてください。enable-ipg0 を有効にしていると、ネットワーク上で時間が不足する場合があります。追加遅延は、ipg0 パラメタに 0 ~ 255 の値を設定することで追加できます。遅延は、メディアのバイト時間によって指定します。表 3-5 に、enable-ipg0 および ipg0 パラメタの説明を示します。

表 3-5 enable-ipg0 および ipg0 を定義するパラメタ

パラメタ	値	説明
enable-ipg0	0	enable-ipg0 は有効
	1	enable-ipg0 は無効 (デフォルト = 1)
ipg0	0 ~ 255	パケットを受信してから送信するまでの追加遅延時間 (間隔) (デフォルト = 8)

vca デバイスは、プログラム可能なパケット間隔 (InterPacket Gap : IPG) パラメタ ipg1 および ipg2 をサポートします。ipg1 と ipg2 を合計した値が、IPG 合計になります。接続速度が 1000 Mbps の場合の IPG 合計は 0.096 マイクロ秒です。

表 3-6 に、IPG パラメタのデフォルト値および許容値を示します。

表 3-6 読み取りおよび書き込みが可能なパケット間隔パラメタの値と説明

パラメタ	値 (バイト時間)	説明
ipg1	0 ~ 255	パケット間隔 1 (デフォルト = 8)
ipg2	0 ~ 255	パケット間隔 2 (デフォルト = 4)

デフォルトでは、ドライバは ipg1 を 8 バイト時間に、ipg2 を 4 バイト時間に設定します。これらの値は標準的な値です。バイト時間とは、接続速度が 1000 Mbps である場合に、接続上で 1 バイトを送信するのに要する時間です。

ネットワーク上にこれより長い IPG 値 (ipg1 と ipg2 の合計値) を使用するシステムが存在して、ネットワークにアクセスする速度が遅く感じられる場合は、ほかのマシンの長い IPG 値に合わせて ipg1 と ipg2 の値を大きくしてください。

割り込みパラメタ

表 3-7 に、受信割り込みブランキング値を示します。

表 3-7 別名読み取り用の RX ブランキングレジスタ

フィールド名	値	説明
rx-intr-pkts	0 ~ 511	最後のパケットの受信後、ここで指定する数のパケットを受信したら割り込みます。値が 0 の場合は、パケット数によるブランキングは行われません (デフォルト = 3)。
rx-intr-time	0 ~ 524287	最後のパケットの受信後、4.5 マイクロ秒 (μsec) が経過したら割り込みます。値が 0 の場合は、時間によるブランキングは行われません (デフォルト = 3)。

ランダム早期ドロップパラメタ

これらのパラメタを使用すると、受信 FIFO がいっぱいになった場合にパケットをドロップすることができます。デフォルトでは、この機能は使用不可になっています。FIFO の使用率が指定した値に達すると、あらかじめ設定された頻度でパケットがドロップされます。FIFO のレベルが上がったときには、頻度も大きくする必要があります。制御パケットはドロップされることがなく、統計情報にもカウントされません。

表 3-8 RX ランダム早期検出 8 ビットベクトル

フィールド名	値	説明
red-dv4to6k	0 ~ 255	FIFO しきい値が 4,096 ~ 6,144 バイトの場合の、ランダム早期検出およびパケットドロップベクトル。ドロップの頻度は、12.5% の粒度でプログラムできます。たとえば、ビット 0 を設定すると、このしきい値範囲では 8 パケットのうち最初のパケットがドロップされます (デフォルト = 0)。
red-dv6to8k	0 ~ 255	FIFO しきい値が 6,144 ~ 8,192 バイトの場合の、ランダム早期検出およびパケットドロップベクトル。ドロップの頻度は、12.5% の粒度でプログラムできます。たとえば、ビット 8 を設定すると、このしきい値範囲では 8 パケットのうち最初のパケットがドロップされます (デフォルト = 0)。

表 3-8 RX ランダム早期検出 8 ビットベクトル (続き)

フィールド名	値	説明
red-dv8to10k	0 ~ 255	FIFO しきい値が 8,192 ~ 10,240 バイトの場合の、ランダム早期検出およびパケットドロップベクトル。ドロップの頻度は、12.5% の粒度でプログラムできます。たとえば、ビット 16 を設定すると、このしきい値範囲では 8 パケットのうち最初のパケットがドロップされます (デフォルト = 0)。
red-dv10to12k	0 ~ 255	FIFO しきい値が 10,240 ~ 12,288 バイトの場合の、ランダム早期検出およびパケットドロップベクトル。ドロップの頻度は、12.5% の粒度でプログラムできます。たとえば、ビット 24 を設定すると、このしきい値範囲では 8 パケットのうち最初のパケットがドロップされます (デフォルト = 0)。

PCI バスインタフェースパラメタ

次のパラメタを使用すると、PCI インタフェース機能を変更して、特定のアプリケーションの PCI 性能を向上させることができます。

表 3-9 PCI バスインタフェースパラメタ

パラメタ	説明
tx-dma-weight	加重ラウンドロビン調停を行っているときに、送信 (TX) 側に付与する優先度の乗数を指定します。指定できる値は 0 ~ 3 です (デフォルト = 0)。0 は、加重しないことを意味します。そのほかの値は、2 のべき乗として、トラフィック上で加重されます。たとえば、tx-dma-weight が 0 で、rx-dma-weight が 3 の場合、RX トラフィックが連続して着信している限り、RX トラフィックが PCI にアクセスする優先順位は、TX トラフィックの 8 倍以上になります。
rx-dma-weight	加重ラウンドロビン調停の、RX 側に付与する優先度の乗数を指定します。指定できる値は 0 ~ 3 です (デフォルト = 0)。
infinite-burst	このパラメタを有効にすると、システムが無限バーストをサポートしている場合には、無限バースト機能を使用できます。アダプタは、バス上ですべてのパケットが送信されるまでバスを解放しません。指定できる値は 0 または 1 です (デフォルト = 0)。
disable-64bit	アダプタの 64 ビット機能を無効にします。

注 : UltraSPARC[®] III ベースのプラットフォームでは、このパラメタはデフォルトで 1 に設定されている場合があります。UltraSPARC II ベースのプラットフォームでは、デフォルトで 0 になっています。指定できる値は 0 または 1 です (デフォルト = 0、64 ビット機能は有効)。

vca ドライバパラメタの設定

vca デバイスドライバパラメタは、次の 2 つの方法で設定できます。

- ndd ユーティリティを使用
- vca.conf ファイルを使用

ndd ユーティリティを使用して設定したパラメタは、システムを再起動するまで有効です。この方法は、パラメタの設定をテストするのに適しています。

システムの再起動後もパラメタが有効であるように設定するには、`/kernel/drv/vca.conf` ファイルを作成して、システムのデバイスに設定する必要のあるパラメタ値をこのファイルに追加します。詳細は、37 ページの「vca.conf ファイルを使用してドライバパラメタを設定する」を参照してください。

ndd ユーティリティを使用したパラメタの設定

ndd ユーティリティを使用して、システムを再起動するまで有効なパラメタを設定します。

ここでは、vca ドライバおよび ndd ユーティリティを使用して、`-set` オプションを指定して各 vca デバイスのパラメタを変更する方法と、`-set` オプションを指定せずにパラメタを表示する方法について説明します。

▼ ndd ユーティリティのデバイスインスタンスを指定する

ndd ユーティリティを使用して vca デバイスのパラメタを表示または設定するには、事前にユーティリティのデバイスインスタンスを確認しておく必要があります。

1. `/etc/path_to_inst` ファイルで、特定のデバイスに対応するインスタンス番号を確認します。詳細は、`path_to_inst(4)` のオンラインマニュアルページを参照してください。

```
# grep vca /etc/path_to_inst
"/pci@8,600000/network@1" 0 "vca"
"/pci@8,700000/network@1" 1 "vca"
```

この例に表示されている 2 つの Sun Crypto Accelerator 4000 Ethernet インスタンスは、どちらも取り付けられたアダプタのものです。インスタンス番号は 0 および 1 です。

2. インスタンス番号を使用してデバイスを選択します。

```
# ndd -set /dev/vcaN
```

注 – このマニュアルの例では、*N* はデバイスのインスタンス番号を表します。

選択したデバイスは、選択を変更するまで有効です。

非対話型モードと対話型モード

ndd ユーティリティは、次の 2 つのモードで使用できます。

- 非対話型
- 対話型

非対話型モードでは、ユーティリティを起動して特定のコマンドを実行します。コマンドを実行したら、ユーティリティは終了します。対話型モードでは、ユーティリティを使用して、1 つ以上のパラメタ値を表示または設定できます。詳細は、ndd(1M) のオンラインマニュアルページを参照してください。

非対話型モードでの ndd ユーティリティの使用

ここでは、パラメタの変更方法および表示方法について説明します。

- パラメタ値を変更するには、`-set` オプションを使用します。

`-set` オプションを指定して ndd ユーティリティを起動すると、ユーティリティは *value* に指定された値をドライバに引き渡して、*parameter* に割り当てます。値は、指定した `/dev/vca` ドライバインスタンスに対して設定されます。

```
# ndd -set /dev/vcaN parameter value
```

adv パラメタを変更した場合は、次のようなメッセージが表示されます。

```
- link up 1000 Mbps half duplex
```

- パラメタ値を表示するには、パラメタ名を指定して値は省略します。
-set オプションを省略すると、ユーティリティーは照会の操作であると判断して、指定されたデバイスインスタンスを照会し、指定された *parameter* に対応する値を読み出して出力します。

```
# ndd /dev/vcaN parameter
```

対話型モードでの ndd ユーティリティーの使用

- 対話型モードでパラメタ値を変更するには、次に示すように ndd /dev/vca を実行します。

ndd ユーティリティーは、パラメタ名の入力を求めるプロンプトを表示します。

```
# ndd /dev/vcaN  
name to get/set? (Enter the parameter name or ? to view all  
parameters)
```

パラメタ名を入力すると、ndd ユーティリティーは、パラメタ値の入力を求めるプロンプトを表示します (表 3-1 ~ 表 3-9 を参照)。

- vca ドライバがサポートするパラメタの一覧を表示するには、`ndd /dev/vca` を実行します。

パラメタの詳細は、表 3-1 ～表 3-9 を参照してください。

```
# ndd /dev/vca
name to get/set ? ?
?                               (read only)
instance                        (read and write)
adv-autoneg-cap                 (read and write)
adv-1000fdx-cap                 (read and write)
adv-1000hdx-cap                 (read and write)
adv-100fdx-cap                  (read and write)
adv-100hdx-cap                  (read and write)
adv-10fdx-cap                   (read and write)
adv-10hdx-cap                   (read and write)
adv-asmppause-cap               (read and write)
adv-pause-cap                   (read and write)
pause-on-threshold              (read and write)
pause-off-threshold             (read and write)
link-master                     (read and write)
enable-ipg0                     (read and write)
ipg0                            (read and write)
ipg1                            (read and write)
ipg2                            (read and write)
rx-intr-pkts                    (read and write)
rx-intr-time                    (read and write)
red-p4k-to-6k                   (read and write)
red-p6k-to-8k                   (read and write)
red-p8k-to-10k                  (read and write)
red-p10k-to-12k                 (read and write)
tx-dma-weight                   (read and write)
rx-dma-weight                   (read and write)
infinite-burst                  (read and write)
disable-64bit                   (read and write)
name to get/set ?
#
```

自動ネゴシエーションモードまたは強制モードの設定

次の接続パラメタは、自動ネゴシエーションモードまたは強制モードで動作するように設定できます。

- speed
- duplex
- link-clock

デフォルトでは、これらの接続パラメータには自動ネゴシエーションモードが設定されています。これらのパラメータのいずれかが自動ネゴシエーションモードである場合、vca デバイスは接続相手と通信を行って、共通する値およびフロー制御機能のネゴシエーションを行います。これらのパラメータのいずれかに auto 以外の値が設定されている場合は、ネゴシエーションは行われず、その接続パラメータは強制モードになります。強制モードでは、speed パラメータ値を接続相手と一致させる必要があります。詳細は、40 ページの「OpenBoot PROM を使用した接続パラメータの自動ネゴシエーションモードおよび強制モードの切り替え」を参照してください。

▼ 自動ネゴシエーションモードを使用不可にする

ネットワークデバイスが自動ネゴシエーションをサポートしていない場合、またはネットワークに強制的に speed または duplex、link-clock パラメータを設定する場合は、vca デバイスの自動ネゴシエーションを使用不可にすることができます。

1. 次のドライバパラメータに、接続相手のデバイス (スイッチなど) に付属するマニュアルに記載されている値を設定します。

- adv-1000fdx-cap
- adv-1000hdx-cap
- adv-100fdx-cap
- adv-100hdx-cap
- adv-10fdx-cap
- adv-10hdx-cap
- adv-asmppause-cap
- adv-pause-cap

これらのパラメータの説明および設定できる値については、表 3-2 を参照してください。

2. adv-autoneg-cap パラメータに 0 を設定します。

```
# ndd -set /dev/vcaN adv-autoneg-cap 0
```

ndd 接続パラメータを変更すると、次のようなメッセージが表示されます。

```
link up 1000 Mbps half duplex
```

注 - 自動ネゴシエーションを使用不可にする場合は、speed および duplex、link-clock (1000 Mbps のみ) パラメータを強制モードで動作するように設定する必要があります。設定手順については、40 ページの「OpenBoot PROM を使用した接続パラメータの自動ネゴシエーションモードおよび強制モードの切り替え」を参照してください。

vca.conf ファイルを使用したパラメタの設定

/kernel/drv ディレクトリ内の vca.conf ファイルにエントリを追加することで、ドライバパラメタの属性を指定することもできます。指定するパラメタ名は、24 ページの「ドライバパラメタ値および定義」に示すパラメタ名と同一です。



注意 – /kernel/drv/vca.conf ファイル内のデフォルトのエントリは削除しないでください。

詳細は、prtconf(1) および driver.conf(4) のオンラインマニュアルページを参照してください。次の手順では、vca.conf ファイルにパラメタを設定する例を示します。

前述の手順では、システムで認識されたデバイスに対してパラメタを適用しました。vca.conf ファイルを使用して Sun Crypto Accelerator 4000 ボードの変数を設定するには、デバイス名および親デバイス、デバイスユニットアドレスの 3 つのデバイス情報を把握しておく必要があります。

▼ vca.conf ファイルを使用してドライバパラメタを設定する

1. デバイスツリー内の、vca デバイスのハードウェアパス名を取得します。
 - a. /etc/driver_aliases ファイルで特定のデバイスに対応する名前を確認します。

```
# grep vca /etc/driver_aliases
vca "pci108e,3de8"
```

この例では、Sun Crypto Accelerator 4000 ソフトウェアドライバ (vca) に対応するデバイス名は "pci108e,3de8" です。

- b. /etc/path_to_inst ファイルで親デバイス名およびデバイスユニットアドレスを探します。

詳細は、path_to_inst(4) のオンラインマニュアルページを参照してください。

```
# grep vca /etc/path_to_inst
"/pci@8,600000/network@1" 0 "vca"
"/pci@8,700000/network@1" 1 "vca"
```

この例には、デバイスパス名およびインスタンス番号、ソフトウェアドライバ名の、3列の情報が出力されています。

この例の最初の行に表示されているデバイスパス名は、`"/pci@8,600000/network@1"` です。デバイスパス名は、親デバイス名およびデバイスノード名、デバイスユニットアドレスの3つの情報で構成されます。詳細は、表 3-10 を参照してください。

表 3-10 デバイスパス名

デバイスパス名全体	親デバイス名	ノード名	ユニットアドレス
<code>"/pci@8,600000/network@1"</code>	<code>/pci@8,600000</code>	<code>network</code>	<code>1</code>
<code>"/pci@8,700000/network@1"</code>	<code>/pci@8,700000</code>	<code>network</code>	<code>1</code>

`vca.conf` ファイル内に PCI デバイスを明確に指定するには、そのデバイスのデバイスパス名全体 (親デバイス名およびノード名、ユニットアドレス) を使用します。PCI デバイスの仕様の詳細は、`pci(4)` のオンラインマニュアルページを参照してください。

2. `/kernel/drv/vca.conf` ファイルに、前の手順で確認したデバイスのパラメタを設定します。

次のエントリでは、指定した Sun Crypto Accelerator 4000 Ethernet デバイスの `adv-autoneg-cap` パラメタを無効にしています。

```
name="pci108e,3de8" parent="/pci@8,700000" unit-address="1" adv-autoneg-cap=0;
```

3. `vca.conf` ファイルを保存します。
4. すべてのファイルとプログラムを保存して閉じ、ウィンドウシステムを終了します。
5. システムを停止して再起動します。

`vca.conf` ファイルを使用したすべての Sun Crypto Accelerator 4000 `vca` デバイスのパラメタの設定

デバイスパス名 (親デバイス名およびノード名、ユニットアドレス) を省略すると、すべての Sun Crypto Accelerator 4000 Ethernet デバイスのすべてのインスタンスに対してパラメタが設定されます。

▼ vca.conf ファイルを使用してすべての Sun Crypto Accelerator 4000 vca デバイスのパラメタを設定する

1. vca.conf ファイルに 1 行追加して *parameter=value;* の形式で値を入力し、すべてのインスタンスのパラメタ値を変更します。

次の例では、すべての Sun Crypto Accelerator 4000 Ethernet デバイスの、すべてのインスタンスの *adv-autoneg-cap* パラメタに 1 を設定しています。

```
adv-autoneg-cap=1;
```

vca.conf ファイルの例

次に、vca.conf ファイルの例を示します。

```
#
# Copyright 2002 Sun Microsystems, Inc. All rights reserved.
# Use is subject to license terms.
#
#ident "@(#)vca.conf 1.2 02/06/26 SMI"

#
# Use the new Solaris 9 properties to ensure that the driver is attached
# on boot, to get us to register with KCL2. This also prevents us from
# being unloaded by the cleanup modunload -i 0.
#
ddi-forceattach=1 ddi-no-autodetach=1;
name="pci108e,3de8" parent="/pci@8,700000" unit-address="1" adv-autoneg-cap=0;
adv-autoneg-cap=1;
```

OpenBoot PROM を使用した接続パラメタの自動ネゴシエーションモードおよび強制モードの切り替え

次の接続パラメタには、OpenBoot PROM (OBP) インタフェースから、自動ネゴシエーションモードまたは強制モードの動作を設定できます。

表 3-11 ローカル接続のネットワークデバイスパラメタ

パラメタ	説明
speed	このパラメタには、auto または 1000、100、10 を設定できます。構文は次のとおりです。 <ul style="list-style-type: none">• speed=auto (デフォルト)• speed=1000• speed=100• speed=10
duplex	このパラメタには、auto または full、half を設定できます。構文は次のとおりです。 <ul style="list-style-type: none">• duplex=auto (デフォルト)• duplex=full• duplex=half
link-clock	このパラメタは、speed パラメタに 1000 を設定した場合、または 1000 Mbps MMF の Sun Crypto Accelerator 4000 ボードを使用している場合にのみ有効です。このパラメタの値は、接続相手の値に対応している必要があります。たとえば、ローカル接続に master の値を設定した場合、接続相手は slave の値である必要があります。このパラメタには、master または slave、auto を設定できます。構文は次のとおりです。 <ul style="list-style-type: none">• link-clock=auto (デフォルト)• link-clock=master• link-clock=slave

接続を正常に確立するため、speed および duplex、link-clock (1000 Mbps のみ) パラメタは、ローカル接続と接続相手との間で正しく設定してください。speed および duplex、link-clock (1000 Mbps のみ) の各パラメタを、接続相手に合わせて自動ネゴシエーションモードまたは強制モードを指定して動作させる必要があります。これらのパラメタに auto を指定すると、そのパラメタが自動ネゴシエーションモードで動作するように接続が設定されます。OBP プロンプトでパラメタを指定しなければ、そのパラメタはデフォルトの auto に設定されます。auto 以外の値を指定すると、ローカル接続のそのパラメタは強制モードで動作するように設定されます。

ローカル接続が、100 Mbps 以下の全二重および半二重モードに対応し、speed および duplex パラメタに自動ネゴシエーションモードを設定している場合、接続相手は、100 Mbps または 10 Mbps で、全二重または半二重モードを使用することになります。

speed パラメタに強制モードを設定して動作している場合、その値は接続相手の speed 値と一致している必要があります。duplex パラメタがローカル接続と接続相手との間で一致していなくても接続される可能性はありますが、トラフィック衝突が発生します。

ローカル接続の speed パラメタに自動ネゴシエーションモードを設定し、接続相手の speed パラメタに強制モードを設定している場合には、ローカル接続と接続相手との間で speed 値をネゴシエーションできれば接続が成立することがあります。自動ネゴシエーションモードが設定されたインタフェースは、速度が一致していれば、常にデフォルトの半二重モードで接続の確立を試みます。もう一方のインタフェースが自動ネゴシエーションモードになっていないため、自動ネゴシエーションモードであるインタフェースは speed パラメタしか検出せず、duplex パラメタは検出しません。この方法を、並列検出 (Parallel Detection) と呼びます。



注意 – duplex が競合する接続を確立すると、トラフィック衝突が発生します。

ローカル接続のパラメタを強制モードで動作させるには、auto 以外の値に設定する必要があります。たとえば、100 Mbps の半二重モードで強制モード接続を確立するには、OBP プロンプトで次のように入力します。

```
ok boot net:speed=100,duplex=half
```

注 – この節の例では、net はデフォルトの統合ネットワークインタフェースデバイスパスの別名です。net ではなくデバイスパスを指定することで、ほかのネットワークデバイスを設定できます。

100 Mbps の半二重モードで、クロックマスターとして強制モード接続を設定するには、OBP プロンプトで次のコマンドを入力します。

```
ok boot net:speed=1000,duplex=half,link-clock=master
```

注 – link-clock パラメタには、接続相手の link-clock 値に対応する値を設定する必要があります。たとえば、ローカル接続の link-clock 値に master を指定する場合、接続相手の link-clock 値は slave に設定されている必要があります。

speed に 10 Mbps の強制モード、duplex に自動ネゴシエーションモードを設定するには、OBP プロンプトで次のように入力します。

```
ok boot net:speed=10,duplex=auto
```

また、OBP プロンプトで次のように入力しても、前の例と同じローカル接続パラメータを設定できます。

```
ok boot net:speed=10
```

詳細は、IEEE 802.3 に関するドキュメントを参照してください。

Sun Crypto Accelerator 4000 暗号化ドライバおよび Ethernet ドライバの動作に関する統計情報

この節では、kstat(1M) コマンドで表示される統計情報について説明します。

暗号化ドライバの統計情報

表 3-12 に、暗号化ドライバの統計情報を示します。

表 3-12 暗号化ドライバの統計情報

パラメータ	説明	Stable/Unstable
vs-mode	FIPS または standard、unitialized が表示されます。FIPS は、ボードが FIPS モードであることを示します。standard は、ボードが FIPS モードでないことを示します。unitialized は、ボードが初期化されていないことを示します。	Stable
vs-status	ready または faulted、failsafe が表示されます。ready は、ボードが正常に動作していることを示します。faulted は、ボードが動作していないことを示します。failsafe は、ボード出荷時の状態の failsafe モードであることを示します。	Stable

Ethernet ドライバの統計情報

表 3-13 で、Ethernet ドライバの統計情報について説明します。

表 3-13 Ethernet ドライバの統計情報

パラメタ	説明	Stable/Unstable
ipackets	着信パケット数	Stable
ipackets64	ipackets の 64 ビット版	Stable
ierrors	エラーが含まれるために処理できない受信パケットの総数 (long)	Stable
opackets	インタフェースで送信が要求されたパケットの総数	Stable
opackets64	インタフェースで送信が要求されたパケットの総数 (64 ビット)	Stable
oerrors	エラーが原因で送信に失敗したパケットの総数 (long)	Stable
rbytes	インタフェースが正常に受信したバイトの総数	Stable
rbytes64	インタフェースが正常に受信したバイトの総数 (64 ビット)	Stable
obytes	インタフェースで送信が要求されたバイトの総数	Stable
obytes64	インタフェースで送信が要求されたバイトの総数 (64 ビット)	Stable
multircv	グループアドレスおよび機能アドレスを含む、正常に受信したマルチキャストパケット数 (long)	Stable
multixmt	グループアドレスおよび機能アドレスを含む、送信が要求されたマルチキャストパケット数 (long)	Stable
brdcstrcv	正常に受信したブロードキャストパケット (long)	Stable
brdcstxmt	送信が要求されたブロードキャストパケット (long)	Stable
norcvbuf	受信パケットに割り当てるバッファがないために、有効な着信パケットが破棄された回数 (long)	Stable
noxmtbuf	送信バッファがビジー状態か、または送信パケットに割り当てるバッファがないために、出力時に破棄されたパケット数 (long)	Stable

表 3-14 に、送受信の MAC カウンタに関する説明を示します。

表 3-14 TX および RX MAC カウンタ

パラメタ	説明	Stable/Unstable
tx-collisions	衝突が発生したフレーム送信を試行するたびに加算される 16 ビットのロード可能カウンタ	Stable
tx-first-collisions	1 回目は衝突が発生したが 2 回目に正常に実行されたフレーム送信があるたびに加算される 16 ビットのロード可能カウンタ	Unstable
tx-excessive-collisions	試行回数限度を超えたフレーム送信があるたびに加算される 16 ビットのロード可能カウンタ	Unstable
tx-late-collisions	衝突が発生したフレーム送信があるたびに加算される 16 ビットのロード可能カウンタ。最小フレームサイズ (バイト数) 以上を送信したあとに発生した衝突が原因で、TxMAC がドロップしたフレームの数を示します。通常は、ネットワーク上に、ネットワークの最大許容時間に違反するステーションが 1 つ以上存在することを意味します。	Unstable
tx-defer-timer	フレーム送信の試行中に TxMAC がネットワーク上のトラフィックを保留にした時間を計測する 16 ビットロード可能タイマー。このタイマーの単位は、メディアバイトクロックを 256 で割った値です。	Unstable
tx-peak-attempts	送信に成功したフレームあたりの最大連続衝突回数を示す 8 ビットレジスタ。このレジスタが最後に読み取られたあとに発生した回数を示します。このレジスタがカウントできるのは 255 回までです。送信に成功したフレームあたりの連続衝突回数が 255 を超えると、ソフトウェアに対するマスク可能割り込みが発生します。このレジスタを読み取ると、自動的に 0 にクリアされます。	Unstable
tx-underrun	有効なフレームをネットワークから受信するたびに加算される 16 ビットのロード可能カウンタ	Unstable

表 3-14 TX および RX MAC カウンタ (続き)

パラメタ	説明	Stable/Unstable
rx-length-err	最大フレームサイズレジスタにプログラムされた値より長いフレームをネットワークから受信するたびに加算される 16 ビットのロード可能カウンタ	Unstable
rx-alignment-err	受信フレームで整合エラーが検出された場合に加算される 16 ビットのロード可能カウンタ。整合エラーは、受信フレームの巡回冗長検査 (CRC) アルゴリズムでエラーが検出されて、かつフレームのバイト数が整数にならない場合 (フレームサイズのビット数の余りが 0 にならない場合) に報告されます。	Unstable
rx-crc-err	受信フレームの巡回冗長検査 (CRC) アルゴリズムでエラーが検出されて、かつフレームのバイト数が整数になる場合 (フレームサイズのビット数の余りが 0 になる場合) に加算される 16 ビットのロード可能カウンタ	Unstable
rx-code-violations	フレーム受信中に MII 上の XCVR によって Rx_Err が生成された場合に加算される 16 ビットのロード可能カウンタ。これは、受信されたデータストリーム中に無効なコードが検出された場合に、トランシーバによって表示されず、受信コード違反は FCS エラーまたは整合エラーとしてカウントされません。	Unstable
rx-overflows	リソース不足のためにドロップされた Ethernet フレーム数	Unstable
rx-no-buf	受信バッファの容量が足りないためにハードウェアがデータを受信できなかった回数	Unstable
rx-no-comp-wb	ハードウェアが受信データのエントリ完了を通知できなかった回数	Unstable
rx-len-mismatch	表明された長さが実際のフレームの長さとは一致しない受信フレーム数	Unstable

次に示す Ethernet 属性 (表 3-15) は、デバイスと接続相手の機能の共通部分から導出されます。

表 3-15 に、現在の Ethernet 接続属性に関する説明を示します。

表 3-15 現在の Ethernet 接続属性

パラメタ	説明	Stable/Unstable
ifspeed	1000 または 100、10 Mbps	Stable
link-duplex	0 = 半二重、1 = 全二重	Stable
link-pause	接続の現在のポーズ設定。詳細は、27 ページの「フロー制御パラメタ」を参照してください。	Stable
link-asmopause	接続の現在のポーズ設定。詳細は、27 ページの「フロー制御パラメタ」を参照してください。	Stable
link-up	1 = 接続確立、0 = 接続未確立	Stable
link-status	1 = 動作中、0 = 停止中	Stable
xcvr-inuse	使用しているトランシーバの種類: 1 = 内部 MII、2 = 外部 MII、3 = 外部 PCS	Stable

表 3-16 に、読み取り専用のメディア独立インタフェース (MII) 機能に関する説明を示します。これらのパラメタはハードウェアの機能を規定します。Gigabit メディア独立インタフェース (GMII) は、次のすべての機能をサポートします。

表 3-16 読み取り専用の vca デバイスの機能

パラメタ	説明	Stable/Unstable
cap-autoneg	0 = 自動ネゴシエーション不可 1 = 自動ネゴシエーション可	Stable
cap-1000fdx	ローカルインタフェースの全二重機能 0 = 1000 Mbps、全二重不可 1 = 1000 Mbps、全二重可	Stable
cap-1000hdx	ローカルインタフェースの半二重機能 0 = 1000 Mbps、半二重不可 1 = 1000 Mbps、半二重可	Stable
cap-100fdx	ローカルインタフェースの全二重機能 0 = 100 Mbps、全二重不可 1 = 100 Mbps、全二重可	Stable
cap-100hdx	ローカルインタフェースの半二重機能 0 = 100 Mbps、半二重不可 1 = 100 Mbps、半二重可	Stable

表 3-16 読み取り専用の vca デバイスの機能 (続き)

パラメタ	説明	Stable/Unstable
cap-10fdx	ローカルインタフェースの全二重機能 0 = 10 Mbps、全二重不可 1 = 10 Mbps、全二重可	Stable
cap-10hdx	ローカルインタフェースの半二重機能 0 = 10 Mbps、半二重不可 1 = 10 Mbps、半二重可	Stable
cap-asm-pause	ローカルインタフェースのフロー制御機能 0 = 非対称ポーズ不可 1 = ローカルデバイスからの非対称ポーズ可 (27 ページの「フロー制御パラメタ」を参照)	Stable
cap-pause	ローカルインタフェースのフロー制御機能 0 = 対称ポーズ不可 1 = 対称ポーズ可 (27 ページの「フロー制御パラメタ」を参照)	Stable

接続相手の機能の報告

表 3-17 に、接続相手の機能を示す読み取り専用パラメタに関する説明を示します。

表 3-17 読み取り専用の接続相手の機能

パラメタ	説明	Stable/Unstable
lp-cap-autoneg	0 = 自動ネゴシエーション不可 1 = 自動ネゴシエーション可	Stable
lp-cap-1000fdx	0 = 1000 Mbps、全二重送信不可 1 = 1000 Mbps、全二重送信可	Stable
lp-cap-1000hdx	0 = 1000 Mbps、半二重送信不可 1 = 1000 Mbps、半二重送信可	Stable
lp-cap-100fdx	0 = 100 Mbps、全二重送信不可 1 = 100 Mbps、全二重送信可	Stable
lp-cap-100hdx	0 = 100 Mbps、半二重送信不可 1 = 100 Mbps、半二重送信可	Stable
lp-cap-10fdx	0 = 10 Mbps、全二重送信不可 1 = 10 Mbps、全二重送信可	Stable

表 3-17 読み取り専用の接続相手の機能 (続き)

パラメタ	説明	Stable/Unstable
lp-cap-10hdx	0 = 10 Mbps、半二重送信不可 1 = 10 Mbps、半二重送信可	Stable
lp-cap-asm-pause	0 = 非対称ポーズ不可 1 = 接続相手に対する非対称ポーズ可 (27 ページの「フロー制御パラメタ」を参照)	Stable
lp-cap-pause	0 = 対称ポーズ不可 1 = 対称ポーズ可 (27 ページの「フロー制御パラメタ」を参照)	Stable

接続相手が自動ネゴシエーション不可 (lp-cap-autoneg が 0) の場合は、表 3-17 に示すその他の情報は無効で、パラメタ値は 0 になります。

接続相手が自動ネゴシエーション可 (lp-cap-autoneg が 1) の場合は、自動ネゴシエーションおよび接続相手の機能を使用したときに、速度とモードの情報が表示されます。

表 3-18 に、ドライバ固有のパラメタに関する説明を示します。

表 3-18 ドライバ固有のパラメタ

パラメタ	説明	Stable/Unstable
lb-mode	デバイスがループバックモードになっていれば、このパラメタに反映されます。	Unstable
promisc	有効にすると、デバイスは無差別 (promiscuous) モードになります。無効にすると、デバイスは無差別モードになりません。	Unstable
Ethernet 送信カウンタ		
tx-wsrsv	送信リングがいっぱいになった回数	Unstable
tx-msgdup-fail	パケットの複製を試行して失敗した回数	Unstable
tx-allocb-fail	メモリの割り当てを試行して失敗した回数	Unstable
tx-queue0	1 台目のハードウェアの送信キューに入れられた送信パケット数	Unstable
tx-queue1	2 台目のハードウェアの送信キューに入れられた送信パケット数	Unstable
tx-queue2	3 台目のハードウェアの送信キューに入れられた送信パケット数	Unstable
tx-queue3	4 台目のハードウェアの送信キューに入れられた送信パケット数	Unstable

表 3-18 ドライバ固有のパラメタ (続き)

パラメタ	説明	Stable/Unstable
Ethernet 受信カウンタ		
rx-hdr-pkts	256 バイト未満のサイズの受信パケット数	Unstable
rx-mtu-pkts	256 バイト以上 1514 バイト未満のサイズの受信パケット数	Unstable
rx-split-pkts	2 ページに分割されたパケット数	Unstable
rx-nocanput	IP スタックへの配信で障害が発生したためにドロップされたパケット数	Unstable
rx-msgdup-fail	複製できなかったパケット数	Unstable
rx-allocb-fail	ブロックの割り当てに失敗した回数	Unstable
rx-new-pages	受信中に置き換えられたページ数	Unstable
rx-new-hdr-pages	受信中に置き換えられた、256 バイト未満のパケットを格納したページ数	Unstable
rx-new-mtu-pages	受信中に置き換えられた、256 バイト以上 1514 バイト未満のパケットを格納したページ数	Unstable
rx-new-nxt-pages	受信中に置き換えられた、複数ページに分割されたパケットを含むページ数	Unstable
rx-page-alloc-fail	ページの割り当てに失敗した回数	Unstable
rx-mtu-drops	ドライバが新しいページを割り当てて置き換えることができなかったために、256 バイト以上 1514 バイト未満のパケットを格納したページ全体がドロップした回数	Unstable
rx-hdr-drops	ドライバが新しいページを割り当てて置き換えることができなかったために、256 バイト未満のパケットを格納したページ全体がドロップした回数	Unstable
rx-nxt-drops	ドライバが新しいページを割り当てて置き換えることができなかったために、分割されたパケットを含むページがドロップした回数	Unstable
rx-rel-flow	ドライバがフローを解放するように指示された回数	Unstable
Ethernet PCI 属性		
rev-id	現場で使用されているデバイスを識別するための Sun Crypto Accelerator 4000 Ethernet デバイスのバージョン ID	Unstable
pci-err	PCI エラーの総数	Unstable

表 3-18 ドライバ固有のパラメタ (続き)

パラメタ	説明	Stable/Unstable
pci-rta-err	ターゲット側の中断を受信した回数	Unstable
pci-rma-err	マスター側の中断を受信した回数	Unstable
pci-parity-err	PCI パリティエラーの検出数	Unstable
pci-drto-err	遅延トランザクション再試行がタイムアウトになった回数	Unstable
dma-mode	Sun Crypto Accelerator 4000 ドライバ (vca) が使用	Unstable

▼ 接続相手の設定を確認する

- スーパーユーザーで、`kstat vca:N` コマンドを実行します。

```
# kstat vca:N
module: vca                instance: 0
name:   vca0               class:   misc
```

注 - この例では、*N* は *vca* デバイスのインスタンス番号を表します。この番号には、`kstat` コマンドの実行の対象になるボードのインスタンス番号を指定する必要があります。

ネットワーク構成

この節では、アダプタをシステムに取り付けたあとで、ネットワークホストファイルを編集する方法について説明します。

ネットワークホストファイルの構成

ドライバソフトウェアをインストールしたら、アダプタの **Ethernet** インタフェース用の `hostname.vcaN` ファイルを作成する必要があります。ファイル名 `hostname.vcaN` の *N* は、使用する *vca* インタフェースのインスタンス番号に対応することに注意してください。また、`/etc/hosts` ファイルにも、この **Ethernet** インタフェースの IP アドレスおよびホスト名を設定する必要があります。

1. `/etc/path_to_inst` ファイルで、該当する `vca` インタフェースおよびインスタンス番号を探します。

詳細は、`path_to_inst(4)` のオンラインマニュアルページを参照してください。

```
# grep vca /etc/path_to_inst
"/pci@8,600000/network@1" 0 "vca"
```

この例では、インスタンス番号は 0 です。

2. `ifconfig(1M)` コマンドを使用して、アダプタの `vca` インタフェースを設定します。

`ifconfig` コマンドを使用して、ネットワークインタフェースに IP アドレスを割り当てます。コマンド行に次のように入力します。`ip_address` の部分は、アダプタの IP アドレスに置き換えてください。

```
# ifconfig vcaN plumb ip_address up
```

注 – この節の例では、`N` はデバイスのインスタンス番号を表します。

詳細は、`ifconfig(1M)` のオンラインマニュアルページおよび Solaris のマニュアルを参照してください。

- 再起動後も設定が変わらないようにするには、`/etc/hostname.vcaN` ファイルを作成します。ファイル名の `N` は、使用する `vca` インタフェースのインスタンス番号になります。

手順 1 で示した `vca` インタフェースを使用する場合は、`/etc/hostname.vcaN` ファイルを作成して、ファイル名の `N` に、この例で 0 と表示されたデバイスのインスタンス番号を指定します。インスタンス番号が 1 の場合、ファイル名は `/etc/hostname.vca1` になります。

- 使用する予定のない Sun Crypto Accelerator 4000 インタフェースには、`/etc/hostname.vcaN` ファイルを作成しないでください。
- `/etc/hostname.vcaN` ファイルには、適切な `vca` インタフェースのホスト名を設定する必要があります。
- ホスト名に固有の IP アドレスを割り当て、`/etc/hosts` ファイルに設定する必要があります。
- ホスト名は、ほかのインタフェースのホスト名とは異なる名前にする必要があります。たとえば、`/etc/hostname.vca0` および `/etc/hostname.vca1` は、同じホスト名を共有できません。

次に、Sun Crypto Accelerator 4000 ボード (zardoz-11) を搭載する zardoz という名前のシステムに必要な `/etc/hostname.vcaN` ファイルの例を示します。

```
# cat /etc/hostname.hme0
zardoz
# cat /etc/hostname.vca0
zardoz-11
```

3. `/etc/hosts` ファイル内に、有効な各 vca インタフェースに対応する適切なエントリを作成します。

次に例を示します。

```
# cat /etc/hosts
#
# Internet host table
#
127.0.0.1    localhost
129.144.10.57 zardoz    loghost
129.144.11.83 zardoz-11
```

第4章

vcaadm および vcadiag ユーティ リティーによる Sun Crypto Accelerator 4000 ボードの管理

この章では、vcaadm および vcadiag ユーティリティーの概要について説明します。この章は、次の節で構成されます。

- 53 ページの「vcaadm の使用」
- 56 ページの「vcaadm によるログインおよびログアウト」
- 61 ページの「vcaadm でのコマンドの入力」
- 63 ページの「vcaadm による Sun Crypto Accelerator 4000 ボードの初期化」
- 67 ページの「vcaadm によるキーストアの管理」
- 74 ページの「vcaadm によるボードの管理」
- 79 ページの「vcadiag の使用」

vcaadm の使用

vcaadm プログラムは、Sun Crypto Accelerator 4000 ボードのコマンド行インタフェースを提供します。この vcaadm ユーティリティーを使用することができるのは、セキュリティー管理者に指定されたユーザーだけです。最初に vcaadm を使用して Sun Crypto Accelerator 4000 ボードに接続するときには、初期セキュリティー管理者およびパスワードを作成するためのプロンプトが表示されます。

vcaadm 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 4000 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/bin
$ export PATH
```

次に、vcaadm コマンド行構文を示します。

- vcaadm [-H]
- vcaadm [-y] [-h *host*] [-p *port*] [-d *vcaN*] [-f *filename*]
- vcaadm [-y] [-h *host*] [-p *port*] [-d *vcaN*] [-s *sec_officer*] *command*

注 – -d 属性を使用する場合の *vcaN* はボードのデバイス名で、*N* は Sun Crypto Accelerator 4000 デバイスのインスタンス番号です。

表 4-1 に、vcaadm ユーティリティのオプションを示します。

表 4-1 vcaadm オプション

オプション	意味
-H	vcaadm コマンドのヘルプファイルを表示して終了します。
-d <i>vcaN</i>	<i>N</i> をドライバインスタンス番号とする Sun Crypto Accelerator 4000 ボードに接続します。たとえば、-d <i>vca1</i> を指定すると、デバイス <i>vca1</i> に接続します。 <i>vca</i> はこのボードのデバイス名を示す文字列で、 <i>1</i> はデバイスのインスタンス番号です。この値のデフォルトは <i>vca0</i> です。必ず <i>vcaN</i> の書式で、 <i>N</i> にはデバイスインスタンス番号を指定してください。
-f <i>filename</i>	<i>filename</i> 内に指定された 1 つ以上のコマンドを解釈および実行して終了します。
-h <i>host</i>	<i>host</i> 上の Sun Crypto Accelerator 4000 ボードに接続します。 <i>host</i> は、ホスト名または IP アドレスで指定できます。デフォルトではループバックアドレスになっています。
-p <i>port</i>	<i>port</i> 上の Sun Crypto Accelerator 4000 ボードに接続します。 <i>port</i> の値は、デフォルトでは 6870 になっています。
-s <i>sec_officer</i>	<i>sec_officer</i> という名前のセキュリティ管理者としてログインします。
-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 <i>yes</i> と応答します。

注 – このマニュアルでは、セキュリティ管理者名の例として *sec_officer* を使用します。

動作モード

vcaadm は、3つのモードのいずれかで実行できます。モードは、主に vcaadm へのコマンドの渡し方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。

注 - vcaadm を使用するには、セキュリティー管理者としての認証が必要です。セキュリティー管理者としての認証を受ける回数は、使用する動作モードによって異なります。

シングルコマンドモード

シングルコマンドモードでは、コマンドを実行するたびにセキュリティー管理者としての認証が必要です。コマンドを実行すると、セキュリティー管理者は vcaadm からログアウトされます。

シングルコマンドモードでコマンドを入力する場合は、すべてのコマンド行スイッチを指定したあとで、実行するコマンドを指定します。たとえば、シングルコマンドモードでは、次のコマンドを実行すると、指定したキースタア内のすべてのユーザーが表示されてコマンドのシェルプロンプトに戻ります。

```
$ vcaadm show user
Security Officer Name: sec_officer
Security Officer Password:
```

次のコマンドを実行すると、*sec_officer* に指定したセキュリティー管理者としてログインして、キースタア内に *web_admin* に指定したユーザーを作成できます。

```
$ vcaadm -s sec_officer create user web_admin
Security Officer Password:
Enter new user password:
Confirm password:
User web_admin created successfully.
```

注 - 最初のパスワードはセキュリティー管理者のもので、そのあと新しいユーザー *web_admin* のパスワード入力およびパスワード確認が続きます。

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 シェルの機能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、使用するファイルごとにセキュリティー管理者としての認証が必要です。コマンドファイル内のコマンドを実行したあと、セキュリティー管理者は `vcaadm` からログアウトされます。

ファイルモードでコマンドを入力するには、ファイルを指定します。`vcaadm` はそのファイルから 1 つ以上のコマンドを読み込みます。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。コメントは、それぞれ「#」文字で開始します。ファイルモードのオプションを指定すると、`vcaadm` 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` ファイル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。

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

対話型モード

対話型モードでは、ボードに接続するたびにセキュリティー管理者としての認証が必要です。これは、`vcaadm` のデフォルトの動作モードです。対話型モードで `vcaadm` からログアウトするには、`logout` コマンドを使用します。詳細は、56 ページの「`vcaadm` によるログインおよびログアウト」を参照してください。

対話型モードは、`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、一度に 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。

vcaadm によるログインおよびログアウト

コマンド行から `vcaadm` を使用して、`-h` および `-p`、`-d` の各属性によってホストおよびポート、デバイスを指定すると、正常なネットワーク接続が確立していれば、すぐにセキュリティー管理者としてログインするためのプロンプトが表示されます。

`vcaadm` プログラムは、`vcaadm` アプリケーションと指定したボード上で動作する Sun Crypto Accelerator 4000 ファームウェアとの間に、暗号化ネットワーク接続 (チャンネル) を確立します。

暗号化チャネルの設定中、ボードはハードウェア Ethernet アドレスおよび RSA 公開鍵を使用して自己確認を行います。vcaadm が最初にボードに接続したときには、認証データベース (\$HOME/.vcaadm/trustdb) が作成されます。このファイルには、セキュリティー管理者が現在管理しているボードがすべて含まれています。

vcaadm によるボードへのログイン

セキュリティー管理者が新しいボードに接続すると、vcaadm はセキュリティー管理者に通知して、次のオプションを表示します。

1. Abort the connection
2. Trust the connection one time only (no changes to trust database)
3. Trust this board forever (adds the hardware ethernet address and RSA public key to the trust database).

セキュリティー管理者が遠隔アクセス鍵が変更されたボードに接続すると、vcaadm はセキュリティー管理者に通知して、次の 3 つのオプションを表示します。

1. Abort the connection
2. Trust the connection one time only (no changes to trust database)
3. Replace the old public key bound to this hardware ethernet address with the new public key.

新しいボードへのログイン

注 - この章のこれ以降の例では、vcaadm の対話型モードを使用する例を示します。

新しいボードに接続するとき、vcaadm は認証データベースに新しいエントリを作成する必要があります。新しいボードにログインする例を次に示します。

```
# vcaadm -h hostname
Warning: MAC ID and Public Key Not Found
-----
The MAC ID and public key presented by this board were
not found in your trust database.

MAC ID: 08:00:20:EE:EE:EE
Key Fingerprint: 29FC-7A54-4014-442F-7FD9-5FEA-8411-CFB4
-----
Please select an action:

1. Abort this connection
2. Trust the board for this session only.
3. Trust the board for all future sessions.

Your Choice -->
```

遠隔アクセス鍵が変更されたボードへのログイン

遠隔アクセス鍵が変更されたボードに接続するとき、vcaadm は認証データベースのそのボードに対応するエントリを変更する必要があります。遠隔アクセス鍵が変更されたボードにログインする例を次に示します。

```
# vcaadm -h hostname
Warning: Public Key Conflict
-----
The public key presented by the board you are connecting
to is different than the public key that is trusted for
this MAC ID.

MAC ID: 08:00:20:EE:EE:EE
New Key Fingerprint: 29FC-7A54-4014-442F-7FD9-5FEA-8411-CFB4
Trusted Key Fingerprint: A508-38D1-FED8-8103-7ACC-0D19-C9C9-11F2
-----
Please select an action:

1. Abort this connection
2. Trust the board for this session only.
3. Replace the current trusted key with the new key.

Your Choice -->
```

vcaadm プロンプト

対話型モードの vcaadm プロンプトは、次のように表示されます。

```
vcaadm{vcaN@hostname, sec_officer}> command
```

次の表に、vcaadm のプロンプト変数の説明を示します。

表 4-2 vcaadm のプロンプト変数の定義

プロンプト変数	定義
<i>vcaN</i>	vca は、Sun Crypto Accelerator 4000 ボードを示す文字列です。 <i>N</i> は、デバイスインスタンス番号 (ユニットアドレス) で、ボードのデバイスバス名に含まれています。デバイスインスタンス番号の確認方法については、37 ページの「vca.conf ファイルを使用してドライバパラメタを設定する」を参照してください。
<i>hostname</i>	Sun Crypto Accelerator 4000 ボードが物理的に接続されているホストの名前。 <i>hostname</i> には、物理ホストの IP アドレスを指定することもできます。
<i>sec_officer</i>	現在ボードにログインしているセキュリティー管理者の名前

vcaadm によるボードからのログアウト

対話型モードで操作しているときに、vcaadm を完全に終了せずに、あるボードから接続を切り離してほかのボードに接続したい場合があります。ボードから接続を切り離してログアウトしたあとも対話型モードを継続するには、logout コマンドを使用します。

```
vcaadm{vcaN@hostname, sec_officer}> logout  
vcaadm>
```

この例で、`vcaadm>` プロンプトに、デバイスインスタンス番号またはホスト名、セキュリティ管理者名が表示されなくなったことに注意してください。ほかのデバイスにログインするには、次のオプションパラメータを使用して `connect` コマンドを入力します。

表 4-3 `connect` コマンドのオプションパラメータ

パラメータ	意味
<code>dev vcaN</code>	ドライバインスタンス番号 <i>N</i> の Sun Crypto Accelerator 4000 ボードに接続します。たとえば、 <code>-d vca1</code> と入力すると、デバイス <code>vca1</code> に接続します。デフォルトでは、 <code>vca0</code> デバイスになっています。
<code>host hostname</code>	<i>hostname</i> 上の Sun Crypto Accelerator 4000 ボードに接続します。デフォルトではループバックアドレスになっています。 <i>hostname</i> には、物理ホストの IP アドレスを指定することもできます。
<code>port port</code>	<i>port</i> 上の Sun Crypto Accelerator 4000 ボードに接続します。デフォルトでは <code>6870</code> になっています。

例：

```
vcaadm{vcaN@hostname, sec_officer}> logout
vcaadm> connect host hostname dev vca2
Security Officer Login: sec_officer
Security Officer Password:
vcaadm{vcaN@hostname, sec_officer}>
```

すでに Sun Crypto Accelerator 4000 ボードに接続している場合は、`vcaadm` で `connect` コマンドを実行することはできません。この場合は、一度ログアウトしてから `connect` コマンドを実行する必要があります。

新しく接続するたびに、`vcaadm` と対象の Sun Crypto Accelerator 4000 ファームウェアは、送られてくる管理データを保護するための新しいセッション鍵の再ネゴシエーションを行います。

vcaadm でのコマンドの入力

vcaadm プログラムには、Sun Crypto Accelerator 4000 ボードと対話するために必要なコマンド言語が組み込まれています。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 は使用できませんが、re は reset または rekey の可能性があるため不明確です。

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。

```
vcaadm{vcaN@hostname, sec_officer}> show user
User                                     Status
-----
web_admin                                enabled
Tom                                       enabled
-----
```

この例では、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。

```
vcaadm{vcaN@hostname, sec_officer}> re
Ambiguous command: re
```

コマンドのヘルプの表示

vcaadm 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せずに入力し、その行のどこかに「?」を指定すると、コマンドの構文が表示されます。次に例を示します。

```
vcaadm{vcaN@hostname, sec_officer}> create ?
Sub-Command          Description
-----
so                    Create a new security officer
user                  Create a new user

vcaadm{vcaN@hostname, sec_officer}> create user ?
Usage: create user [<username>]

vcaadm{vcaN@hostname, sec_officer}> set ?
Sub-Command          Description
-----
passreq              Set password requirements
password             Change an existing security officer password
timeout              Set the auto-logout time
```

また、vcaadm プロンプトで「?」を入力すると、すべての vcaadm コマンドおよびその説明の一覧を見ることができます。次に例を示します。

```
vcaadm{vcaN@hostname, sec_officer}> ?
Sub-Command          Description
-----
backup                Backup master key
connect              Begin admin session with firmware
create                Create users and accounts
delete                Delete users and accounts
diagnostics           Run diagnostic tests
disable               Disable a user
enable                Enable a user
exit                  Exit vcaadm
loadfw                Load new firmware
logout                Logout current session
quit                  Exit vcaadm
rekey                 Generate new system keys
reset                 Reset the hardware
set                   Set operating parameters
show                  Show system settings
zeroize               Delete all keys and reset board
```

vcaadm が対話型モードでない場合は、「?」を入力すると操作中のシェルが解釈を行います。この場合は、「?」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。

対話型モードでの vcaadm プログラムの終了

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

vcaadm による Sun Crypto Accelerator 4000 ボードの初期化

Sun Crypto Accelerator 4000 ボードを構成する最初の手順は、ボードの初期化です。ボードを初期化するときには、キーストアを作成する必要があります。詳細は、84 ページの「概念および用語」を参照してください。Sun Crypto Accelerator 4000 ボードは、新しいキーストアで初期化するか、バックアップファイルの既存のキーストアを使用して初期化することができます。

vcaadm で最初に Sun Crypto Accelerator 4000 ボードに接続すると、新しいキーストアでボードを初期化するか、またはバックアップファイルに格納されている既存のキーストアでボードを初期化するかを確認するプロンプトが表示されます。vcaadm は、ボードの初期化方法に応じて、必要な情報を入力するプロンプトを表示します。

▼ 新しいキーストアで Sun Crypto Accelerator 4000 ボード を初期化する

1. Sun Crypto Accelerator 4000 ボードを取り付けたシステムのコマンドプロンプトで `vcaadm` を入力するか、システムが遠隔にある場合は `vcaadm -h hostname` を入力し、1 を選択してボードを初期化します。

```
# vcaadm -h hostname
This board is uninitialized.
You will now initialize the board.  You may
either completely initialize the board and
start with a new keystore or restore the board
using a backup file.

1. Initialize the board with a new keystore
2. Initialize the board to use an existing keystore

Your Choice (0 to exit) --> 1
```

2. 初期セキュリティー管理者名およびパスワードを作成します (67 ページの「名前の要件」を参照)。

```
Initial Security Officer Name: sec_officer
Initial Security Officer Password:
Confirm Password:
```

3. キーストア名を作成します (67 ページの「名前の要件」を参照)。

```
Keystore Name: keystore_name
```

4. FIPS 140-2 モードまたは FIPS でないモードを選択します。

FIPS モードの場合、Sun Crypto Accelerator 4000 ボードは FIPS 140-2 のレベル 3 に準拠します。FIPS 140-2 は、FIPS (Federal Information Processing Standard) が規定する標準で、改ざん防止機能と、高レベルのデータの完全性および安全性に関する要件を定めています。FIPS 140-2 の詳細は、次の Web ページを参照してください。
<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

```
Run in FIPS 140-2 mode? (Y/Yes/N/No) [No]: y
```

注 – 重要なパラメータを変更または削除する前、または重大な影響を及ぼす可能性のあるコマンドを実行する前には、`vcaadm` が確認のプロンプトを表示するので、`Y` または `Yes`、`N`、`No` を入力して確認してください。大文字と小文字は区別されません。デフォルトでは、`No` になります。

5. 構成情報を確認します。

```
Board initialization parameters:
-----
Initial Security Officer Name: sec_officer
Keystore name: keystore_name
Run in FIPS 140-2 Mode: Yes
-----

Is this correct? (Y/Yes/N/No) [No]: y
Initializing crypto accelerator board...
```

既存のキーストアを使用した Sun Crypto Accelerator 4000 ボードの初期化

1 つのキーストアに複数のボードを追加するため、同じキーストア情報ですべてのボードを初期化したい場合があります。また、Sun Crypto Accelerator 4000 ボードを元のキーストア設定に復元したい場合もあります。ここでは、バックアップファイルに保存されている既存のキーストアを使用してボードを初期化する方法について説明します。

この手順を行う前に、既存のボード設定のバックアップファイルを作成する必要があります。バックアップファイルを作成および復元するには、バックアップファイルのデータを暗号化および復号化するためのパスワードが必要です。詳細は、72 ページの「マスター鍵のバックアップ」を参照してください。

▼ 既存のキーストアを使用して Sun Crypto Accelerator 4000 ボードを初期化する

1. Sun Crypto Accelerator 4000 ボードを取り付けたシステムのコマンドプロンプトで `vcaadm` を入力するか、システムが遠隔にある場合は `vcaadm -h hostname` を入力し、2 を選択してバックアップからボードを復元します。

```
# vcaadm -h hostname
This board is uninitialized.
You will now initialize the board.  You may
either completely initialize the board and
start with a new keystore or restore the board
using a backup file.

1. Initialize the board with a new keystore
2. Initialize the board to use an existing keystore

Your Choice (0 to exit) --> 2
```

2. バックアップファイルのパスおよびパスワードを入力します。

```
Enter the path to the backup file: /tmp/board-backup
Password for restore file:
```

3. 構成情報を確認します。

```
Board restore parameters:
-----
Path to backup file: /tmp/board-backup
Keystore name: keystore_name
-----

Is this correct? (Y/Yes/N/No) [No]: y
Restoring data to crypto accelerator board...
```

vcaadm によるキーストアの管理

キーストアとは、鍵素材のリポジトリです。キーストアには、セキュリティー管理者およびユーザーが関連付けられています。キーストアは、記憶領域を提供するだけでなく、ユーザーアカウントによって鍵オブジェクトを所有する手段を提供します。これによって、鍵の所有者として認証されていないアプリケーションに対して鍵を隠すことができます。キーストアは、次の3つの情報で構成されます。

- 鍵オブジェクト : Sun ONE 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。
- セキュリティー管理者アカウント : vcaadm を使用して鍵管理機能にアクセスする手段を提供します。

注 - 1つの Sun Crypto Accelerator 4000 ボードには、1つのキーストアが必要です。複数の Sun Crypto Accelerator 4000 ボードが同じキーストアを共有するように構成して、性能および耐障害性を向上させることもできます。

名前の要件

セキュリティー管理者名およびユーザー名、キーストア名は、次の要件を満たす必要があります。

表 4-4 セキュリティー管理者名およびユーザー名、キーストア名の要件

名前の要件	説明
最小の長さ	1 文字以上
最大の長さ	ユーザー名は 63 文字、キーストア名は 32 文字
有効な文字	英数字および下線 (_)、ダッシュ (-)、ドット (.)
最初の文字	英字であること

パスワードの要件

パスワードの要件は、現在の set passreq の設定 (low または med、high) によって異なります。

パスワードの要件の設定

Sun Crypto Accelerator 4000 ボードのパスワードを設定するには、`set passreq` コマンドを使用します。このコマンドによって、`vcaadm` が入力に要求するすべてのパスワードの文字に関する要件を設定します。パスワードの要件には、次の 3 つの設定があります。

表 4-5 パスワードの要件の設定

パスワード設定	要件
low	パスワードの制限はありません。これは、ボードが FIPS モードでないときのデフォルト設定です。
med	6 文字以上で、そのうち 1 文字は英字以外にする必要があります。これは、ボードが FIPS 140-2 モードであるときのデフォルト設定で、FIPS 140-2 モードで最低限必要なパスワード要件です。
high	8 文字以上で、そのうち 3 文字は英字、1 文字は英字以外にする必要があります。これはデフォルト設定ではないので、手動で設定する必要があります。

パスワードの要件を変更するには、`set passreq` コマンドを入力し、続けて `low` または `med`、`high` を入力します。次のコマンド例では、Sun Crypto Accelerator 4000 ボードのパスワード要件を `high` に設定しています。

```
vcaadm{vcaN@hostname, sec_officer}> set passreq high

vcaadm{vcaN@hostname, sec_officer}> set passreq
Password security level (low/med/high): high
```

キーストアのセキュリティー管理者の生成

1 つのキーストアに複数のセキュリティー管理者を登録する場合があります。このセキュリティー管理者名は、Sun Crypto Accelerator 4000 ボードの範囲内だけで認識されるものなので、ホストシステムのユーザー名と同一にする必要はありません。

セキュリティー管理者を作成する場合、名前のパラメタはコマンド行から省略できます。セキュリティー管理者名を省略すると、vcaadm は名前の入力を求めます (67 ページの「名前の要件」を参照)。

```
vcaadm{vcaN@hostname, sec_officer}> create so Alice
Enter new security officer password:
Confirm password:
Security Officer Alice created successfully.

vcaadm{vcaN@hostname, sec_officer}> create so
New security officer name: Bob
Enter new security officer password:
Confirm password:
Security Officer Bob created successfully.
```

キーストアのユーザーの生成

作成するユーザー名は、Sun Crypto Accelerator 4000 ボードの範囲内だけで認識されるものなので、動作している Web サーバプロセスの UNIX ユーザー名と同一にする必要はありません。

ユーザーを作成する場合、ユーザー名のパラメタはコマンド行から省略できます。ユーザー名を省略すると、vcaadm はユーザー名の入力を求めます (67 ページの「名前の要件」を参照)。

```
vcaadm{vcaN@hostname, sec_officer}> create user web_admin
Enter new user password:
Confirm password:
User web_admin created successfully.

vcaadm{vcaN@hostname, sec_officer}> create user
New user name: Tom
Enter new user password:
Confirm password:
User Tom created successfully.
```

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 – パスワードを忘れないようにしてください。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に、これを確認する方法はありません。

注 - 5分以上コマンドを入力しないと、そのユーザーアカウントはログアウトされます。これは変更可能なオプションです。詳細は、74 ページの「自動ログアウト時間の設定」を参照してください。

ユーザーおよびセキュリティー管理者の一覧表示

キーストアに関連するユーザーおよびセキュリティー管理者の一覧を表示するには、`show user` または `show so` コマンドを実行します。

```
vcaadm{vcaN@hostname, sec_officer}> show user
User                                     Status
-----
web_admin                               Enabled
Tom                                     Enabled
-----

vcaadm{vcaN@hostname, sec_officer}> show so
Security Officer
-----
sec_officer
Alice
Bob
-----
```

パスワードの変更

`vcaadm` を使用してパスワードを変更できるのはセキュリティー管理者だけで、自身のパスワードだけを変更できます。セキュリティー管理者のパスワードを変更するには、`set password` コマンドを使用します。

```
vcaadm{vcaN@hostname, sec_officer}> set password
Enter new security officer password:
Confirm password:
Security Officer password has been set.
```

ユーザーのパスワードは、Sun ONE Web サーバーの `modutil` ユーティリティーの PKCS#11 インタフェースを使用して変更できます。詳細は、Sun ONE Web サーバーのマニュアルの `modutil` に関する説明を参照してください。

ユーザーの有効および無効の切り替え

注 – セキュリティー管理者を無効にすることはできません。セキュリティー管理者を作成すると、削除するまで有効になります。

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。ユーザーは無効にすることができます。無効になったユーザーは、PKCS#11 インタフェースを使用して鍵素材にアクセスできなくなります。無効になったユーザーを有効にすると、ユーザーのすべての鍵素材にアクセスできる状態に戻ります。

ユーザーを有効または無効にする場合、ユーザー名のパラメタはコマンド行から省略できます。ユーザー名を省略すると、vcaadm はユーザー名の入力を求めます。

```
vcaadm{vcaN@hostname, sec_officer}> disable user Tom
User Tom disabled.
vcaadm{vcaN@hostname, sec_officer}> disable user
User name: web_admin
User web_admin disabled.
```

アカウントを無効にするには、enable user コマンドを実行します。

```
vcaadm{vcaN@hostname, sec_officer}> enable user Tom
User Tom enabled.

vcaadm{vcaN@hostname, sec_officer}> enable user
User name: web_admin
User web_admin 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。ユーザーを削除する場合、ユーザー名のパラメータはコマンド行から省略できます。ユーザー名を省略すると、`vcaadm` はユーザー名の入力を求めます

```
vcaadm{vcaN@hostname, sec_officer}> delete user web_admin
Delete user web_admin? (Y/Yes/N/No) [No]: y
User web_admin deleted successfully.

vcaadm{vcaN@hostname, sec_officer}> delete user
User name: Tom
Delete user Tom? (Y/Yes/N/No) [No]: y
User Tom deleted successfully.
```

セキュリティー管理者の削除

削除するセキュリティー管理者を指定して、`delete so` コマンドを実行します。セキュリティー管理者を削除する場合、セキュリティー管理者名のパラメータはコマンド行から省略できます。セキュリティー管理者名を省略すると、`vcaadm` はセキュリティー管理者名の入力を求めます。

```
vcaadm{vcaN@hostname, sec_officer}> delete so Bob
Delete Security Officer Bob? (Y/Yes/N/No) [No]: y
Security Officer Bob deleted.

vcaadm{vcaN@hostname, sec_officer}> delete so
Security Officer name: Alice
Delete Security Officer Alice? (Y/Yes/N/No) [No]: y
Security Officer Alice deleted.
```

マスター鍵のバックアップ

キーストアはディスクに格納され、マスター鍵で暗号化されます。このマスター鍵は、`Sun Crypto Accelerator 4000` ファームウェアに格納されていて、セキュリティー管理者はバックアップを作成することができます。

マスター鍵をバックアップするには、`backup` コマンドを使用します。`backup` コマンドを実行するには、バックアップを格納するファイルへのパス名が必要です。このパス名はコマンド行で指定することも、省略することもできます。省略すると、`vcaadm` はパス名の入力を求めます。

バックアップデータには、パスワードを設定する必要があります。このパスワードは、バックアップファイルのマスター鍵を暗号化するために使用されます。

```
vcaadm{vcaN@hostname, sec_officer}> backup /opt/SUNWconn/vca/backups/bkup.data
Enter a password to protect the data:
Confirm password:
Backup to /opt/SUNWconn/vca/backups/bkup.data successful.
```



注意 – バックアップファイルを作成するときに指定するパスワードは、キーストアのマスター鍵を保護するものであるため、推測されにくいパスワードを選択する必要があります。また、入力したパスワードは覚えておく必要があります。パスワードを忘れると、マスター鍵のバックアップファイルにアクセスできなくなります。パスワードを忘れた場合に、保護されているデータを確認する方法はありません。

バックアップを防ぐためのキーストアのロック

Sun Crypto Accelerator 4000 ボードのマスター鍵がハードウェア外に出力されることを許さない、厳しいセキュリティーポリシーで運用されているサイトもあります。この場合は、`set lock` コマンドを使用してセキュリティーを強化できます。



注意 – このコマンドを実行すると、マスター鍵をバックアップできなくなります。このロックは、マスター鍵を交換しても保持されます。この設定を消去する唯一の方法は、`zeroize` コマンドを使用して Sun Crypto Accelerator 4000 ボード上の情報を消去することです。詳細は、78 ページの「Sun Crypto Accelerator 4000 ボードの情報の消去」を参照してください。

```
vcaadm{vcaN@hostname, sec_officer}> set lock
WARNING: Issuing this command will lock the
         master key. You will be unable to back
         up your master key once this command
         is issued. Once set, the only way to
         remove this lock is to zeroize the board.
Do you wish to lock the master key? (Y/Yes/N/No) [No]: y
The master key is now locked.
```

vcaadm によるボードの管理

この節では、vcaadm ユーティリティーを使用して Sun Crypto Accelerator 4000 ボードを管理する方法について説明します。

自動ログアウト時間の設定

セキュリティ管理者が自動的にボードからログアウトされるまでの時間をカスタマイズするには、`set timeout` コマンドを使用します。自動ログアウト時間を変更するには、`set timeout` コマンドを入力し、続けてセキュリティ管理者が自動的にログアウトされるまでの時間を分単位で入力します。0 を設定すると、自動ログアウト機能は無効になります。設定できる最大値は、1 日あたり 1,440 分です。初期化した Sun Crypto Accelerator 4000 ボードのデフォルトは、5 分になっています。

次のコマンドを実行すると、セキュリティ管理者の自動ログアウト時間を 10 分に変更できます。

```
vcaadm{vcaN@hostname, sec_officer}> set timeout 10
```

ボードの状態の表示

Sun Crypto Accelerator 4000 ボードの現在の状態を表示するには、`show status` コマンドを実行します。このコマンドで、ボードのハードウェアバージョンおよびファームウェアバージョン、ネットワークインタフェースの MAC アドレス、ネットワークインタフェースの状態 (接続中または停止中、速度、デュプレックスモードなど)、キーストアの名前と ID を表示することができます。

```
vcaadm{vcaN@hostname, sec_officer}> show status
Board Status
-----
Hardware Version: 1.0
Firmware Version: 1.0
Bootstrap Firmware Version: VCA Crypto Accelerator 1.0 March 2003
Current Firmware Version: VCA Crypto Accelerator 1.0 March 2003
MAC Address: 00:03:ba:0e:96:aa
Interface information: Link up, 1000Mbps, Full Duplex
Keystore Name: keystore_name
Keystore ID: 832aece03e654790
Login Session Timeout (in minutes): 10
Password policy security level: HIGH
Number of master key backups: 0
* Device is in FIPS 140-2 Mode
-----
```

ボードが FIPS 140-2 モードで動作しているかどうかの確認

Sun Crypto Accelerator 4000 ボードが FIPS 140-2 モードで動作している場合は、`show status` コマンドを実行すると次の行が出力されます。

```
* Device is in FIPS 140-2 Mode
```

ボードが FIPS 140-2 モードで動作していない場合は、`show status` コマンドによって FIPS 140-2 モードを示す行は出力されません。

また、`kstat(1M)` ユーティリティを使用して、ボードが FIPS 140-2 モードで動作しているかどうかを確認することもできます。ボードが FIPS 140-2 モードで動作している場合は、`kstat(1M)` のパラメタ `vs-mode` に FIPS と表示されます。詳細は、42 ページの「Sun Crypto Accelerator 4000 暗号化ドライバおよび Ethernet ドライバの動作に関する統計情報」および `kstat(1M)` のオンラインマニュアルを参照してください。

新しいファームウェアのインストール

新機能が追加されたときには、Sun Crypto Accelerator 4000 ボードのファームウェアを更新できます。ファームウェアをインストールするには、ファームウェアファイルへのパスを指定して `loadfw` コマンドを実行します。

ファームウェアを正常に更新するには、`reset` コマンドを使用して、手動でボードをリセットする必要があります。ボードをリセットすると、現在ログインしているセキュリティー管理者はログアウトされます。

```
vcaadm{vcaN@hostname, sec_officer}> loadfw /opt/SUNWconn/cryptov2/firmware/sca4000fw
Security Officer Login: sec_officer
Security Officer Password:
WARNING: This command will load new firmware onto the
         the target device.  You must issue a reset
         command and log back into the target device in
         order to use the new firmware.

Proceed with firmware update? (Y/Yes/N/No) [No]: y
```

Sun Crypto Accelerator 4000 ボードのリセット

状況によっては、ボードをリセットする必要がある場合があります。リセットするには、`reset` コマンドを実行する必要があります。コマンドを実行すると、リセットするかどうかの確認が求められます。Sun Crypto Accelerator 4000 ボードをリセットすると、ほかに負荷を引き継ぐことができる動作中の Sun Crypto Accelerator 4000 ボードがなければ、システムの暗号化の高速化は一時的に無効になります。また、このコマンドを実行すると自動的に `vcaadm` からログアウトされるので、管理作業を継続する場合は、`vcaadm` に再びログインして、デバイスに再接続する必要があります。

```
vcaadm{vcaN@hostname, sec_officer}> reset
WARNING: Issuing this command will reset the
         the board and close this connection.

Proceed with reset? (Y/Yes/N/No) [No]: y
Reset successful.
```

Sun Crypto Accelerator 4000 ボードの鍵の交換

時間の経過とともに、セキュリティーポリシーに応じて、マスター鍵または遠隔アクセス鍵に新しい鍵を使用する必要がある場合があります。rekey コマンドを使用すると、これらの鍵のいずれかまたは両方を再生成できます。

マスター鍵を交換すると、新しい鍵によってキーストアも再暗号化されるので、以前にバックアップしたマスター鍵ファイルは、新しいキーストアファイルによって無効になります。鍵を交換するときは、マスター鍵のバックアップを作成することをお勧めします。複数の Sun Crypto Accelerator 4000 ボードで同じキーストアを使用している場合は、新しいマスター鍵をバックアップしてほかのボードに対して復元する必要があります。

遠隔アクセス鍵を交換すると、セキュリティー管理者はログアウトされて、新しい遠隔アクセス鍵を使用する接続が強制的に確立されます。

rekey コマンドを実行するときには、次の 3 種類のいずれかの鍵を指定する必要があります。

表 4-6 鍵の種類

鍵の種類	動作
master	マスター鍵を交換します。
remote	遠隔アクセス鍵を交換します。セキュリティー管理者はログアウトされます。
all	マスター鍵および遠隔アクセス鍵を交換します。

rekey コマンドで、鍵の種類に all を選択する例を次に示します。

```
vcaadm{vcaN@hostname, sec_officer}> rekey

Key type (master/remote/all): all
WARNING: Rekeying the master key will render all old board backups
useless with the new keystore file. If other boards use this
keystore, they will need to have this new key backed up and
restored to those boards. Rekeying the remote access key will
terminate this session and force you to log in again.

Rekey board? (Y/Yes/N/No) [No]: y
Rekey of master key successful.
Rekey of remote access key successful. Logging out.
```

Sun Crypto Accelerator 4000 ボードの情報の消去

状況によっては、ボードのすべての鍵素材の消去が必要になる場合があります。これを行うには、2つの方法があります。1つ目は、ハードウェアジャンパを使用する方法です。この方法で情報を消去すると、Sun Crypto Accelerator 4000 ボードは出荷時の状態 (failsafe モード) に戻ります。詳細は、165 ページの「Sun Crypto Accelerator 4000 ハードウェアの情報の消去による出荷時状態への復帰」を参照してください。2つ目は、zeroize コマンドを使用する方法です。

注 – zeroize コマンドは、鍵素材だけを削除し、更新されたファームウェアはそのまま残します。また、このコマンドが正常に実行されると、セキュリティ管理者はログアウトされます。

zeroize コマンドを使用してボード上の情報を消去するには、次のように入力します。

```
vcaadm{vcaN@hostname, sec_officer}> zeroize
WARNING: Issuing this command will zeroize all keys
         on the board. Once zeroized, these keys
         cannot be recovered unless you have
         previously backed up your master key.

Proceed with zeroize? (Y/Yes/N/No) [No]: y
All keys zeroized successfully.
```

vcaadm diagnostics コマンドの使用

診断は、SunVTS のほか、vcaadm ユーティリティから実行することもできます。vcaadm の diagnostics コマンドは、Sun Crypto Accelerator 4000 ハードウェアの、一般的なハードウェアおよび暗号化サブシステム、ネットワークサブシステムの3つの主要なカテゴリの診断に対応しています。一般的なハードウェアの診断では、DRAM およびフラッシュメモリー、PCI バス、DMA コントローラ、ハードウェアの

その他の内蔵部品が対象になります。暗号化サブシステムの診断では、乱数ジェネレータおよび暗号化アクセラレータが対象になります。ネットワークサブシステムの診断では、vca デバイスが対象になります。

```
vcaadm{vcaN@hostname, sec_officer}> diagnostics
```

```
Performing diagnostic tests...Done.
```

```
Diagnostic Results
```

```
-----  
General Hardware:                PASS
```

```
Cryptographic Subsystem:        PASS
```

```
Network Subsystem:              PASS  
-----
```

vcadiag の使用

vcadiag プログラムは、Sun Crypto Accelerator 4000 ボードへのコマンド行インタフェースを提供します。このインタフェースによって、スーパーユーザーは、セキュリティ管理者として認証されていなくても管理作業を行うことができます。

vcadiag が実行する作業は、コマンド行オプションによって指定します。

vcadiag 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 4000 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/bin
```

```
$ export PATH
```

次に、vcadiag のコマンド行構文を示します。

- vcadiag [-D] vcaN
- vcadiag [-F] vcaN
- vcadiag [-K] vcaN
- vcadiag [-Q]
- vcadiag [-R] vcaN
- vcadiag [-Z] vcaN

注 - [-DFKRZ] 属性を使用する場合の vcaN はボードのデバイス名で、N は Sun Crypto Accelerator 4000 デバイスのインスタンス番号です。

表 4-1 に、vcadiag ユーティリティーのオプションを示します。

表 4-7 vcadiag オプション

オプション	意味
-D vcaN	Sun Crypto Accelerator 4000 ボードの診断を実行します。
-F vcaN	Sun Crypto Accelerator 4000 ボードがセキュリティー管理セッションに使用する公開鍵の指紋を表示します。
-K vcaN	Sun Crypto Accelerator 4000 ボードがセキュリティー管理セッションに使用する公開鍵およびその鍵指紋を表示します。
-Q	Sun Crypto Accelerator 4000 デバイスおよびソフトウェアコンポーネントの情報を表示します。出力には、デバイスおよび内部機能、キーストア名、キーストアのシリアル番号、キーストアの参照回数 の情報が、コロンで区切って表示されます。このコマンドを使用して、デバイスとキーストア の関係を判断できます。
-R vcaN	Sun Crypto Accelerator 4000 ボードをリセットします。
-Z vcaN	Sun Crypto Accelerator 4000 ボード上の情報を消去します。

次に、-D オプションの例を示します。

```
# vcadiag -D vca0
Running vca0 on-board diagnostics.
Diagnostics on vca0 PASSED.
```

次に、-F オプションの例を示します。

```
# vcadiag -F vca0
5f26-b516-83b4-d254-a75f-c70d-0544-4de6
```

次に、-K オプションの例を示します。

```
# vcadiag -K vca0
Device: vca0
Key Length: 1024 bits
Key Fingerprint: 5f26-b516-83b4-d254-a75f-c70d-0544-4de6
Modulus:
    b7215a99 8bb0dfe9 389363a0 44dac2b0 7c884161
    20ee8c8b d751437d 4e6a5cdb 76fdc2ba ad353c0b
    248edc1d 3c76591d dbca5997 f6ee8022 e8bb5a6d
    465a4f8c 601d46be 573e8681 506e5d8d f240a0db
    11d5c095 2d237061 df27b2de c353900f f531092b
    7d9a755b c5d79782 95a1180b e17303bb aca939ef
    006c73f7 74469031
Public Exponent:
    00010001
```

次に、-Q オプションの例を示します。

```
# vcadiag -Q
vca0:cb
vca0:cb:keystore_name:83097c2b3e35ef5b:1
vca0:ca
vca0:ca:keystore_name:83097c2b3e35ef5b:1
kcl2pseudo
vca0:om
vca0:om:keystore_name:83097c2b3e35ef5b:1
libkcl
```

次に、-R オプションの例を示します。

```
# vcadiag -R vca0
Resetting device vca0, this may take a minute.
Please be patient.
Device vca0 reset ok.
```

次に、-Z オプションの例を示します。

```
# vcadiag -Z vca0
Zeroizing device vca0, this may take a few minutes.
Please be patient.
Device vca0 zeroized.
```


第5章

Sun Crypto Accelerator 4000 ボード を使用するための Sun ONE サー バーソフトウェアの構成

この章では、Sun ONE Web サーバーで使用する Sun Crypto Accelerator 4000 ボードを設定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。

- 83 ページの「Sun ONE Web サーバーのセキュリティー管理」
- 87 ページの「Sun ONE Web サーバーの構成」
- 90 ページの「Sun ONE Web Server 4.1 のインストールおよび構成」
- 99 ページの「Sun ONE Web Server 6.0 のインストールおよび構成」

注 – このマニュアル中の Sun ONE Web サーバーは、以前は iPlanet™ Web サーバーと呼ばれていたものです。

Sun ONE Web サーバーのセキュリ ティー管理

この節では、Sun ONE Web サーバーによって管理する Sun Crypto Accelerator 4000 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 – キーストアを管理するには、ご使用のシステム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。

概念および用語

キーストアおよびユーザーは、PKCS#11 インタフェースを介して Sun Crypto Accelerator 4000 ボードと通信する、Sun ONE 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 4000 では、ユーザーとは、暗号化鍵素材の所有者を指します。鍵は、それぞれ 1 人のユーザーが所有します。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」鍵などのユーザーの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ができます。

注 - 「ユーザー」または「ユーザーアカウント」という用語は、通常の UNIX ユーザーアカウントではなく、vcaadm で作成された Sun Crypto Accelerator 4000 のユーザーを指します。UNIX のユーザー名と Sun Crypto Accelerator 4000 のユーザー名には、一定の関連付けはありません。

キーストアとは、鍵素材のリポジトリです。キーストアには、セキュリティー管理者およびユーザーが関連付けられています。キーストアは、記憶領域を提供するだけでなく、ユーザーアカウントによって鍵オブジェクトを所有する手段を提供します。これによって、鍵の所有者として認証されていないアプリケーションに対して、鍵を隠すことができます。キーストアは、次の 3 つの情報で構成されます。

- 鍵オブジェクト : Sun ONE 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。
- セキュリティー管理者アカウント : vcaadm を使用して鍵管理機能にアクセスする手段を提供します。

注 - 1 つの Sun Crypto Accelerator 4000 ボードには、1 つのキーストアが必要です。複数の Sun Crypto Accelerator 4000 ボードが同じキーストアを共用するように構成すると、性能および耐障害性を向上させることができます。

標準的なインストールでは、1 人のユーザーを指定した 1 つのキーストアが作成されます。たとえば、1 つのキーストアである `web_server` と、そのキーストア内の 1 人のユーザーである `web_admin` によって 1 つの構成が作成されます。この場合、ユーザー `web_admin` は、この 1 つのキーストア内でサーバーの鍵へのアクセスを制御し、管理することができます。

Sun Crypto Accelerator 4000 のキーストアおよびユーザーの管理には、管理ツール vcaadm を使用します。詳細は、67 ページの「vcaadm によるキーストアの管理」を参照してください。

トークンおよびトークンファイル

Sun ONE Web サーバーは、キーストアをトークンとして認識します。トークンファイルは、Sun Crypto Accelerator 4000 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。

例

engineering および finance、legal の 3 つのキーストアがある場合は、次のトークンが Sun ONE Web サーバーに渡されます。

- engineering
- finance
- legal

トークンファイル

デフォルトの設定を無効にして優先指定を行う場合は、トークンファイルが必要です。アプリケーションによっては、複数のトークンを扱えない場合があります。トークンファイルは、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。

注 - トークン名とキーストア名は同一になります。

Sun ONE Web サーバーは、トークン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、トークンファイルの指定方法を優先度の高い順に示します。

1. 環境変数 `SUNW_PKCS11_TOKEN_FILE` に指定されたファイル

アプリケーションソフトウェアには、環境変数を抑制するものがあります。その場合、この方法は実行できません。

2. ファイル `$HOME/.SUNWconn_cryptov2/tokens`

このファイルは、Sun ONE 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。Sun ONE Web サーバーは、ホームディレクトリを持たない UNIX ユーザーによって実行されることもあります。その場合、この方法は実行できません。

3. ファイル `/etc/opt/SUNWconn/cryptov2/tokens`

トークンファイルが存在しない場合、Sun Crypto Accelerator 4000 ソフトウェアは、すべてのトークンを Sun ONE Web サーバーに渡します。

次に、トークンファイルの内容の例を示します。

```
=====  
# This is an example token file  
  
engineering # Comments are acceptable on the same line  
  
legal  
  
# Because the finance keystore is not listed, the Sun Crypto  
# Accelerator will not present it to the Sun ONE Web Server.  
  
...  
=====
```

注 - 「#」のあとの文字列はコメントです。また、空行を設けることができます。

前述のトークンファイルが存在しない場合には、85 ページの「トークンおよびトークンファイル」で説明するデフォルトの方法が使用されます。

バルク暗号化の使用可能および使用不可の切り替え

Sun ONE サーバーソフトウェアのバルク暗号化機能は、デフォルトでは使用不可になっています。大規模なファイルを送信することが多い場合には、この機能を使用可能にします。

Sun Crypto Accelerator 4000 ボード上で Sun ONE サーバーソフトウェアのバルク暗号化機能を使用可能にするには、`/etc/opt/SUNWconn/cryptov2/` ディレクトリ内に `sslreg` という名前の空のファイルを作成して、サーバーソフトウェアを再起動します。

```
# touch /etc/opt/SUNWconn/cryptov2/sslreg
```

バルク暗号化機能を使用不可にするには、`sslreg` ファイルを削除して、サーバーソフトウェアを再起動する必要があります。

```
# rm /etc/opt/SUNWconn/cryptov2/sslreg
```

Sun ONE Web サーバーの構成

この節では、次の項目について説明します。

- 87 ページの「パスワード」
- 88 ページの「キーストアのユーザーの生成」
- 89 ページの「Sun ONE Web サーバーを使用可能にする方法の概要」
- 90 ページの「Sun ONE Web Server 4.1 のインストールおよび構成」
- 97 ページの「Sun ONE Web Server 4.1 での SSL の構成」
- 99 ページの「Sun ONE Web Server 6.0 のインストールおよび構成」
- 107 ページの「Sun ONE Web Server 6.0 での SSL の構成」

パスワード

Sun ONE Web サーバーを使用できるように設定する過程では、いくつかのパスワードの入力が要求されます。表 5-1 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、この章全体で使用します。使用するパスワードが不明な場合は、表 5-1 を参照してください。

表 5-1 Sun ONE Web サーバーに必要なパスワード

パスワードの種類	説明
Sun ONE Web サーバーの管理サーバー	Sun ONE Web サーバーの管理サーバーを起動するために必要なパスワードです。このパスワードは、Sun ONE Web サーバー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なパスワードです。このパスワードは、Sun ONE 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、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。
セキュリティ管理者 <i>username:password</i>	<i>vcaadm</i> の特権操作を行うときに必要なパスワードです。 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 4000 モジュールを起動するために必要なパスワードです。また、内部の暗号化モジュール (<i>keystore_name</i>) 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。このパスワードは、 <i>vcaadm</i> でキーストアのユーザーを作成するときに指定した <i>username</i> および <i>password</i> で構成されます。キーストアの <i>username</i> と <i>password</i> を、コロン (;) で区切った形式です。

キーストアのユーザーの生成

Sun ONE Web サーバーでボードを使用するには、まずボードを初期化して、ボードのキーストアに 1 人以上のユーザーを生成する必要があります。ボードのキーストアは初期化処理中に作成されます。また、既存のキーストアを使用して Sun Crypto Accelerator 4000 ボードを初期化することもできます。詳細は、63 ページの「vcaadm による Sun Crypto Accelerator 4000 ボードの初期化」を参照してください。

注 - 1 つの Sun Crypto Accelerator 4000 ボードに構成できるキーストアは 1 つだけで、各ボードには 1 つのキーストアが必要です。複数の Sun Crypto Accelerator 4000 ボードが同じキーストアを共用するように構成して、性能および耐障害性を向上させることもできます。

▼ キーストアのユーザーを生成する

1. Sun Crypto Accelerator 4000 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、次のようにコマンドを実行して、検索パスにディレクトリを指定します。

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

2. vcaadm コマンドを実行して vcaadm ユーティリティーにアクセスするか、vcaadm -h *hostname* を実行して vcaadm を遠隔ホストのボードに接続します。詳細は、53 ページの「vcaadm の使用」を参照してください。

```
$ vcaadm -h hostname
```

3. ボードのキーストアにユーザーを作成します。

作成するユーザー名は、Sun Crypto Accelerator 4000 ボードの範囲内だけで認識されるものなので、Web サーバープロセスが使用している UNIX のユーザー名と同一にする必要はありません。ユーザーを作成する前に、まず vcaadm セキュリティー管理者でログインする必要があります。

4. create user コマンドでユーザーを作成します。

```
vcaadm{vcaN@hostname, sec_officer}> create user username
Initial password:
Confirm password:
User username created successfully.
```

ここで作成した *username* および *password* は、*username:password* の形式でまとめられます (表 5-1 を参照)。Web サーバーの起動時の認証では、このパスワードを使用する必要があります。これはシングルユーザーのためのキーストアパスワードです。



注意 – この *username:password* を忘れないようにしてください。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に、これを確認する方法はありません。

5. vcaadm を終了します。

```
vcaadm{vcaN@hostname, sec_officer}> exit
```

Sun ONE Web サーバーを使用可能にする方法の概要

Sun ONE Web サーバーを使用するには、次の手順を完了する必要があります。このあとの 2 つの節では、これらの手順の詳細を説明します。

- Sun ONE Web サーバーのインストール
- 認証データベースの作成
- 証明書の要求
- 証明書のインストール
- Sun ONE Web サーバーの構成



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、Sun ONE Web サーバーが正しく構成されないことがあります。

- Sun ONE Web Server 4.1 を使用している場合は、90 ページの「Sun ONE Web Server 4.1 のインストールおよび構成」に進みます。
- Sun ONE Web Server 6.0 を使用している場合は、99 ページの「Sun ONE Web Server 6.0 のインストールおよび構成」に進みます。

Sun ONE Web Server 4.1 のインストールおよび構成

この節では、Sun ONE Web Server 4.1 のインストール方法および構成方法について説明します。この節の内容は、次のとおりです。

- 90 ページの「Sun ONE Web Server 4.1 のインストール」
- 97 ページの「Sun ONE Web Server 4.1 での SSL の構成」

Sun ONE 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。Sun ONE Web サーバーの使用方法については、Sun ONE Web サーバーのマニュアルを参照してください。

▼ Sun ONE Web Server 4.1 をインストールする

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

Web サーバーのソフトウェアは、次の URL から入手できます。
<http://www.sun.com/>

2. Web サーバーをインストールします。

ここでは、1 つの例を挙げて各手順を説明しますが、この例とは異なる設定で Sun ONE 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。

Sun ONE Web サーバーのインストール時に、デフォルトのパスを受け入れてください。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。Web サーバーのソフトウェアを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が表示す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. Sun ONE Web Server 4.1 の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. Sun ONE Web Server 4.1 の管理サーバーを起動します。

setup 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て Sun ONE Web Server 4.1 の管理サーバーを起動します。

```
# /usr/netscape/server4/https-admserv/start
SunONE-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、管理用のグラフィカルユーザーインターフェイス (GUI) を起動します。

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

認証ダイアログボックスが表示されるので、`setup` の実行時に選択した Sun ONE Web Server 4.1 の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 – Sun ONE 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 Sun ONE Web Server 4.1 の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」を選択します。
Sun ONE Web Server 4.1 の管理サーバーのウィンドウが表示されます。
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。
 - a. Sun ONE Web Server 4.1 の管理サーバーのウィンドウで「Servers」タブを選択します。
 - 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 (表 5-1 を参照) 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、Sun ONE 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します。

1 つ以上の Web サーバーインスタンスでセキュリティーを有効にしたい場合があります。その場合は、各 Web サーバーインスタンスで、手順 1 ～手順 4 を繰り返します。

注 – Sun ONE Web Server 4.1 の管理サーバーで SSL (Secure Socket Layer) を実行する場合も、認証データベースの設定手順は同様です。詳細は、<http://docs.sun.com> の『iPlanet Web Server, Enterprise Edition Administrator's Guide』を参照してください。

5. 次のスクリプトを実行して、Sun Crypto Accelerator 4000 ボードを使用可能にします。

```
# /opt/SUNWconn/bin/iplsslcfg
```

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ます。このスクリプトは、Sun ONE Web サーバー用の Sun Crypto Accelerator 4000 暗号化モジュールをインストールします。次に、構成ファイルを更新して、Sun Crypto Accelerator 4000 ボードを使用できるようにします。

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

```
Sun Crypto Accelerator Sun ONE Installation
-----
This script will install the Sun Crypto Accelerator
cryptographic modules for Sun ONE Products.

Please select what you wish to do:
-----
1. Configure Sun ONE Web Server for SSL
2. Configure Sun ONE Application Server for SSL
3. Export Sun ONE Web Server keys to PKCS#12 format
4. Import keys from PKCS#12 format for Sun ONE Web Server

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て、Return キーを押します。

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

8. **y** を入力して Return キーを押すと、処理が実行されます。

```
This script will update your Sun ONE 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 4000" added to database.
/usr/netscape/server4 has been configured to use
the Sun Crypto Accelerator.

<Press ENTER to continue>
```

9. **0** を入力して処理を終了します。

▼ 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、Sun ONE Web Server 4.1 の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
```

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、管理用 GUI を起動します。

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

認証ダイアログボックスが表示されるので、`setup` の実行時に選択した Sun ONE Web Server 4.1 の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 – Sun ONE 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 Sun ONE Web Server 4.1 の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」を選択します。
Sun ONE Web Server 4.1 の管理サーバーのウィンドウが表示されます。
4. サーバーの証明書を要求するには、Sun ONE Web Server 4.1 の管理サーバーのウィンドウの上部にある「Security」タブを選択します (図 5-1 を参照)。
「Create Trust Database」ページが表示されます。
5. ページの左側にある「Request a Certificate」リンクを選択します (図 5-1 を参照)。

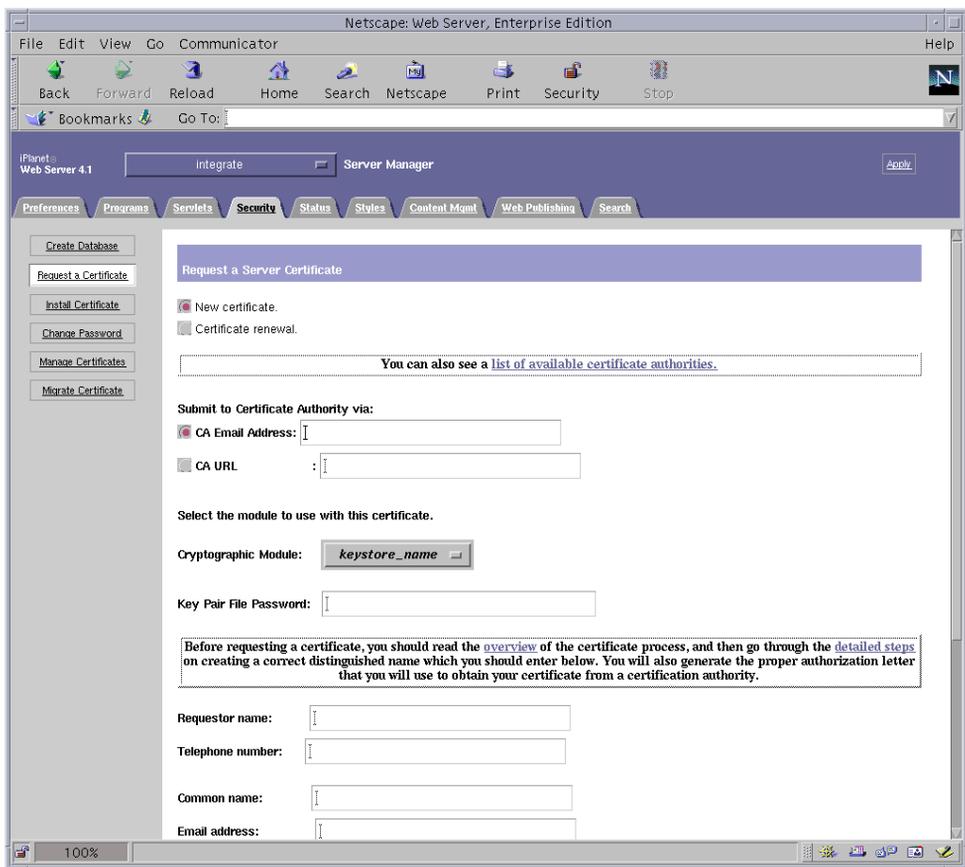


図 5-1 Sun ONE Web Server 4.1 管理サーバーのサーバー証明書要求の画面

6. 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、各キーストアごとに固有のエントリがあります。正しいキーストアを選択していることを確認してください。「SUNW acceleration only」は選択しないでください。

c. 「Key Pair File Password」ダイアログボックスに、鍵を所有するユーザーのパスワードを入力します。

このパスワードは、*username:password* です (表 5-1 を参照)。

d. 次の要求者情報フィールドに、適切な情報を入力します。

表 5-2 要求者情報フィールド

フィールド	説明
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 <i>hostname.domain</i> 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。

7. 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。

8. 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。

注 - 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。このデータは、このあとの手順 5 で必要になるので、クリップボード上に保持しておいてください。

▼ サーバーの証明書をインストールする

1. Sun ONE Web Server 4.1 の管理サーバーのウィンドウの左側にある「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、Sun ONE 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. ページの左側にある「Install Certificate」リンクを選択します。

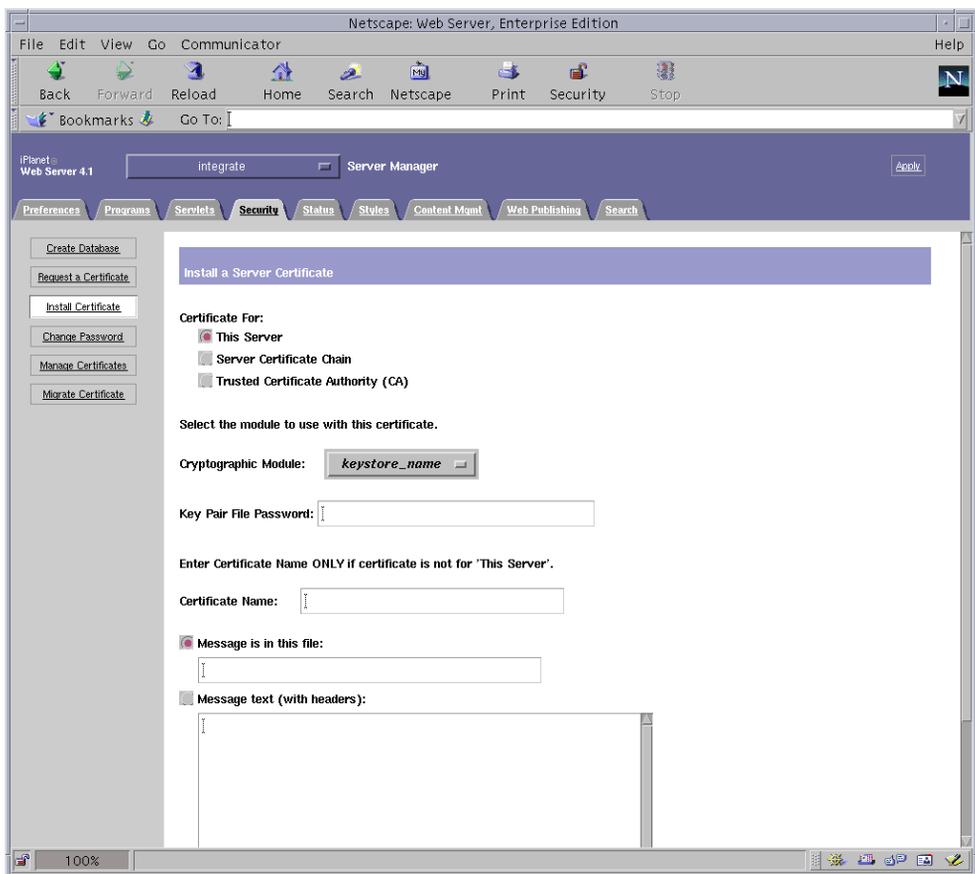


図 5-2 Sun ONE Web Server 4.1 管理サーバーのサーバー証明書インストールの画面

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。

表 5-3 証明書をインストールするためのフィールド

フィールド	説明
Certificate For	「This Server」を選択します。
Cryptographic Module	このプルダウンメニューには、キーストアごとの固有のエントリが表示されます。正しいキーストア名を選択してください。Sun Crypto Accelerator 4000 を使用するには、キーストアに割り当てた名前と同じ名前のモジュールを選択する必要があります。
Key Pair File Password	このパスワードは、 <i>username:password</i> です (表 5-1 を参照)。
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。このフィールドのデフォルト設定は、Server-Cert です。

5. 認証局からコピーした証明書 (93 ページの「サーバーの証明書を生成する」の手順 8 を参照) 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。

6. ページの下部にある「OK」ボタンをクリックします。

7. 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。

Sun ONE Web Server 4.1 での SSL 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。

▼ Sun ONE Web Server 4.1 を構成する

1. Sun ONE Web Server 4.1 の管理サーバーのメインページで、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、「Preferences」タブをクリックします。

3. ページの左側にある「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」ボタンを選択します。
6. 「Save」ボタンを選択して、この変更内容を適用します。

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 (hostname は Web サーバーの名前) を編集して、次の行を追加します。

```
CERTDefaultNickname keystore_name:Server-Cert
```

デフォルトでは、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 の代わりに選択した名前を使用してください。

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。

この操作によって、Sun ONE Web Server 4.1 の管理サーバーに変更内容を適用します。
9. 「Load Configuration Files」ボタンをクリックして、magnus.conf ファイルに加えられた変更を適用します。

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。

Web サーバーが起動していないときに「Apply Changes」ボタンをクリックすると、*username:password* の入力を求める認証ダイアログボックスが表示されます。この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」を選択します。
 - 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. Sun ONE Web Server 4.1 の管理サーバーのウィンドウで、左側にある「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。

モジュールの *keystore_name* プロンプトで、そのキーストアの *username:password* を入力します。

プロンプトが表示されたら、ほかのキーストアの *username:password* を入力します。

12. 次の URL で、新しい Web サーバーが SSL に対応していることを確認します。

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

注 – デフォルトの *server_port* は、443 です。

Sun ONE Web Server 6.0 のインストールおよび構成

この節では、Sun ONE Web Server 6.0 で Sun Crypto Accelerator 4000 ボードを使用するための構成方法について説明します。この節の内容は、次のとおりです。

- 99 ページの「Sun ONE Web Server 6.0 のインストール」
- 107 ページの「Sun ONE Web Server 6.0 での SSL の構成」

Sun ONE 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。Sun ONE Web サーバーの使用方法については、Sun ONE Web サーバーのマニュアルを参照してください。

▼ Sun ONE Web Server 6.0 をインストールする

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

Web サーバーのソフトウェアは、次の URL から入手できます。

`http://www.sun.com/`

2. Web サーバーをインストールします。

ここでは、1 つの例を挙げて手順を説明しますが、この例とは異なる設定で Sun ONE 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/iplanet/servers` です。

Sun ONE Web サーバーのインストール時に、デフォルトのパスを受け入れてください。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。ソフトウェアを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が表示す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. Sun ONE Web Server 6.0 の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. Sun ONE Web Server 6.0 の管理サーバーを起動します。
setup 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て Sun ONE Web Server 6.0 の管理サーバーを起動します。

```
# /usr/iplanet/servers/https-admserv/start
SunONE-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、管理用 GUI を起動します。

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

認証ダイアログボックスが表示されるので、setup の実行時に選択した Sun ONE Web Server 6.0 の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 – Sun ONE 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 Sun ONE Web Server 6.0 の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」を選択します。
Sun ONE Web Server 6.0 の管理サーバーのウィンドウが表示されます。

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。

1 つ以上の Web サーバーインスタンスでセキュリティーを有効にしたい場合があります。その場合は、各 Web サーバーインスタンスで、手順 1 ～手順 4 を繰り返します。

注 – Sun ONE Web Server 6.0 の管理サーバーで SSL を実行する場合も、認証データベースの設定手順は同様です。詳細は、<http://docs.sun.com> の『iPlanet Web Server, Enterprise Edition Administrator's Guide』を参照してください。

- a. Sun ONE Web Server 6.0 の管理サーバーのウィンドウで「Servers」タブを選択します。
 - 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 (表 5-1 を参照) 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、Sun ONE 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します。
5. 次のスクリプトを実行して、Sun Crypto Accelerator 4000 ボードを使用可能にします。

```
# /opt/SUNWconn/crypto/bin/iplsslcfg
```

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ます。このスクリプトは、Sun ONE Web サーバー用の Sun Crypto Accelerator 4000 暗号化モジュールをインストールします。次に、構成ファイルを更新して、Sun Crypto Accelerator 4000 ボードを使用できるようにします。

6. 1 を入力して Return キーを押し、Sun ONE Web サーバーで SSL を使用するよう
構成します。

```
Sun Crypto Accelerator Sun ONE Installation
-----
This script will install the Sun Crypto Accelerator
cryptographic modules for Sun ONE Products.

Please select what you wish to do:
-----
1. Configure Sun ONE Web Server for SSL
2. Configure Sun ONE Application Server for SSL
3. Export Sun ONE Web Server keys to PKCS#12 format
4. Import keys from PKCS#12 format for Sun ONE Web Server

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て、
Return キーを押します。

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

8. y を入力して Return キーを押すと、処理が実行されます。

```
This script will update your Sun ONE 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 4000" added to database.
/usr/iplanet/servers has been configured to use
the Sun Crypto Accelerator.

<Press ENTER to continue>
```

9. 0 を入力して処理を終了します。

▼ 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、Sun ONE Web Server 6.0 の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
```

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、管理用 GUI を起動します。

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

認証ダイアログボックスが表示されるので、setup の実行時に選択した Sun ONE Web Server 6.0 の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 – Sun ONE 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 Sun ONE Web Server 6.0 の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」を選択します。
Sun ONE Web Server 6.0 の管理サーバーのウィンドウが表示されます。
4. サーバーの証明書を要求するには、Sun ONE Web Server 6.0 の管理サーバーのウィンドウの上部にある「Security」タブを選択します。
「Create Trust Database」ウィンドウが表示されます。

5. Sun ONE Web Server 6.0 の管理サーバーのウィンドウの左側にある「Request a Certificate」リンクを選択します。

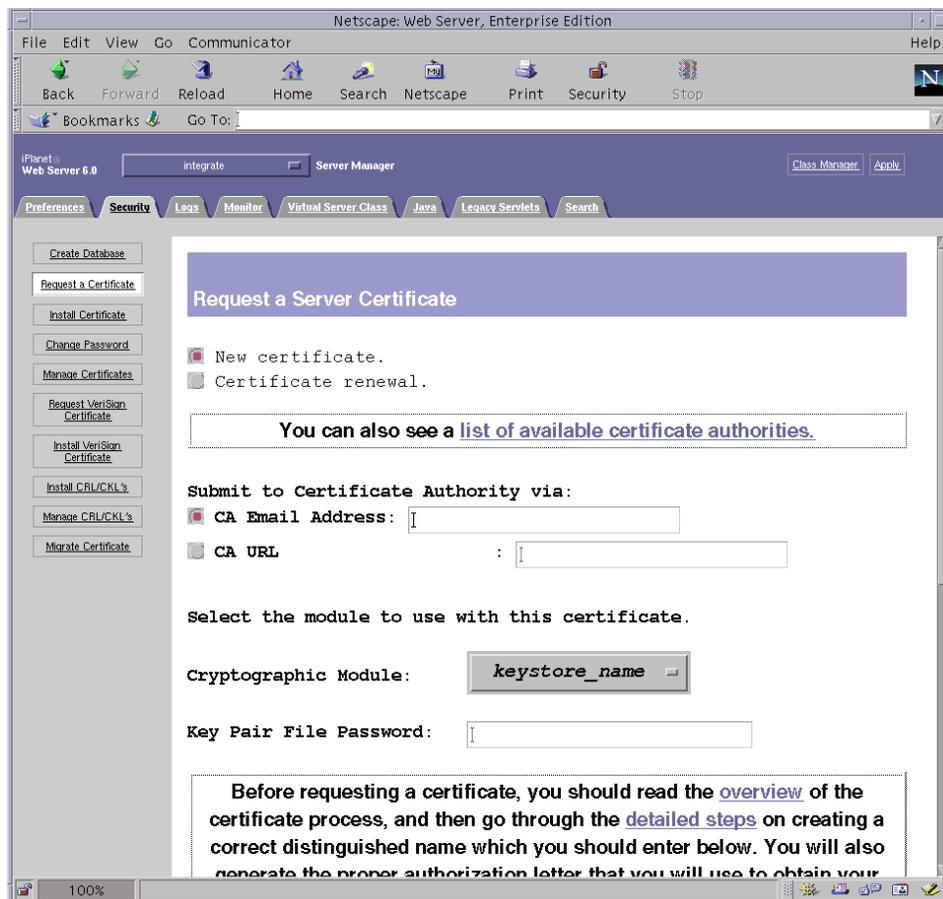


図 5-3 Sun ONE Web Server 6.0 管理サーバーのサーバー証明書要求の画面

6. 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、各キーストアごとに固有のエントリがあります。正しいキーストアを選択してください。「SUNW acceleration only」は選択しないでください。

- c. 「Key Pair File Password」ダイアログボックスに、鍵を所有するユーザーのパスワードを入力します。

このパスワードは、*username:password* です (表 5-1 を参照)。

- d. 次の要求者情報フィールドに、適切な情報を入力します。

表 5-4 要求者情報フィールド

フィールド	説明
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 <i>hostname.domain</i> 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。

7. 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。

8. 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。

注 – 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。このデータは、106 ページの「サーバーの証明書をインストールする」の手順 5 で必要になるので、クリップボード上に保持しておいてください。

▼ サーバーの証明書をインストールする

1. Sun ONE Web Server 6.0 の管理サーバーのウィンドウの左側にある「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、Sun ONE 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. ページの左側にある「Install Certificate」リンクを選択します。

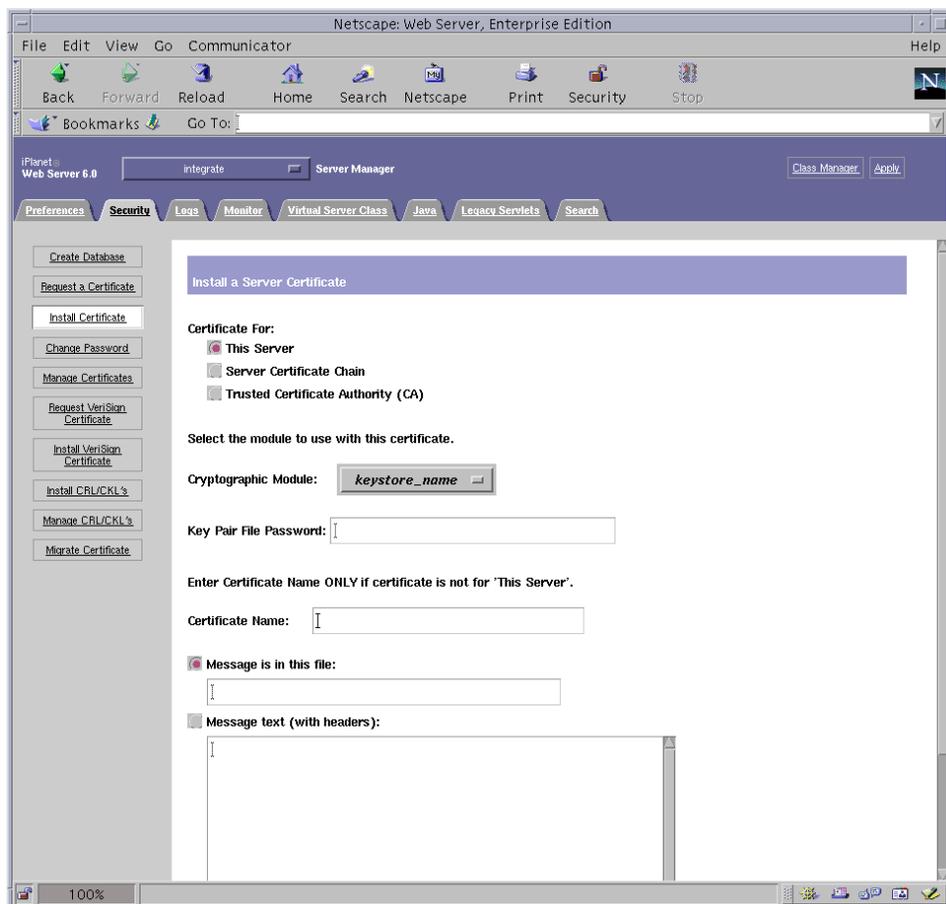


図 5-4 Sun ONE Web Server 6.0 管理サーバーのサーバー証明書インストールの画面

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。

表 5-5 証明書をインストールするためのフィールド

フィールド	説明
Certificate For	「This Server」を選択します。
Cryptographic Module	このプルダウンメニューには、キーストアごとの固有のエントリが表示されます。正しいキーストアを選択してください。Sun Crypto Accelerator 4000 を使用するには、 <i>keystore_name</i> の形式のモジュールを選択する必要があります。
Key Pair File Password	このパスワードは、 <i>username:password</i> です (表 5-1 を参照)。
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。このフィールドのデフォルト設定は、Server-Cert です。

5. 認証局からコピーした証明書 (103 ページの「サーバーの証明書を生成する」の手順 8 を参照) を「Message」テキスト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。

6. ページの下部にある「OK」ボタンをクリックします。

7. 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。

Sun ONE Web Server 6.0 での SSL 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。

▼ Sun ONE 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. ページの左側にある「Edit Listen Sockets」リンクを選択します。

中央部分に、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. *username:password* を入力して、システムでキーストアを認証します。
5. デフォルトの暗号設定を変更する場合は、「Ciphers」という見出しの下の暗号設定を選択します。

暗号設定を変更するためのダイアログボックスが表示されます。「Cipher Default」または「SSL2」、「SSL3/TLS (Transmission Layer Security)」を選択します。

「Cipher Default」を選択した場合、デフォルト設定は表示されません。「SSL2」または「SSL3/TLS」を選択した場合は、ポップアップダイアログボックスで、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。詳細は、暗号選択に関する Sun ONE マニュアルを参照してください。
6. キーストアのあとに : Server-Cert (または実際に選択した証明書の名前) を付けた形式で証明書を選択します。

「Certificate Name」 フィールドには、該当するキーストアユーザーが所有する鍵だけが表示されます。このキーストアユーザーは、*username:password* で認証されるユーザーです。
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、右上の角にある「Apply」 リンクをクリックして変更内容を有効にします。
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。

Web サーバーが起動していないときに「Apply Changes」 ボタンをクリックすると、*username:password* の入力を求める認証ダイアログボックスが表示されます。この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」を選択します。
 - 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. Sun ONE Web Server 6.0 の管理サーバーのウィンドウで、左側にある「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。

モジュールの *keystore_name* プロンプトで、*username:password* を入力します。

プロンプトが表示されたら、ほかのキーストアの *username:password* を入力します。

12. 次の URL で、新しい Web サーバーが SSL に対応していることを確認します。

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

注 – デフォルトの *server_port* は、443 です。

第6章

Sun Crypto Accelerator 4000 ボード を使用するための Apache Web サー バーの構成

この章では、Apache Web サーバーで使用する Sun Crypto Accelerator 4000 ボードを設定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。

- 112 ページの「Apache Web サーバーでボードを使用するための構成」
- 112 ページの「Apache Web サーバーを使用可能にする方法」
- 114 ページの「証明書の作成」



注意 – Sun Crypto Accelerator 1000 ボードと Sun Crypto Accelerator 4000 を使用する Apache Web サーバーを、同時に構成しないでください。両方のボードを同時に構成すると、Apache は正しく動作しません。

Apache Web サーバーを使用する場合は、パッチ 109234-09 もインストールする必要があります。SUNWkcl2a パッケージが追加されたら、システムは Apache Web サーバー mod_ssl 1.3.26 を使用して構成されます。

注 – Apache Web サーバーソフトウェアのバルク暗号化機能は、デフォルトで使用可能になっており、使用不可にはできません。

Apache Web サーバーでボードを使用するための構成

この節では、Apache Web サーバーで Sun Crypto Accelerator 4000 ボードを使用可能にする方法の概要を説明します。

Apache Web サーバーを使用可能にする方法

Sun Crypto Accelerator 4000 ボードを使用するには、Apache Web サーバーのバージョン 1.3.26 以降が必要です。この節では、Apache Web サーバーバージョン 1.3.26 での手順を説明します。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、`/etc/apache` ディレクトリに `httpd.conf-example` ファイルがあります。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. `httpd.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. `apsslcfg` を起動します。

```
# /opt/SUNWconn/cryptov2/bin/apsslcfg
```

4. 1 を選択して、Apache Web サーバーで SSL を使用するよう設定します。

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

Please select what you wish to do:
-----
1. Configure Apache for SSL
2. Work with Apache keys

Your selection (0 to quit): 1
```

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 `apsslcfg` 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、115 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。
指定したディレクトリが存在しなければ、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: base_name
```

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
Using configuration from /opt/SUNWconn/cryptov2/ssl/openssl.cnf
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to /etc/apache/keys/base_name
```

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 – 入力したパスフレーズを覚えておく必要があります。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。パスフレーズを忘れた場合に、これを確認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 4000 ボードを使用できるよう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. 112 ページの「Apache Web サーバーを使用可能にする」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。そのあと、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、ドット (.) 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。入力すると、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、証明書要求の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 4000 ソフトウェアを使用するために `/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、使用している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する必要があります。

```
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/cryptov2/bin/apgetpass
```

```
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>
```

112 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 Sun ONE and Apache keys" from the
apsslcfg main menu.
```

4. apsslcfg を終了するには 0 を選択します。
5. /etc/apache/keys/base_name-certreq.pem (base_name は、112 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これとは異なる場合は、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、新しい Web サーバーが SSL に対応していることを確認します。

```
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 4000 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。

- 119 ページの「SunVTS 診断ソフトウェア」
- 128 ページの「kstat による暗号化の処理状況の確認」
- 129 ページの「OpenBoot PROM の FCode 自己診断の使用」
- 131 ページの「Sun Crypto Accelerator 4000 ボードの障害追跡」

SunVTS 診断ソフトウェア

コア SunVTS ラッパーは、テストを制御し、一連のテストへのユーザーインタフェースを提供します。テストのいくつかは、パッケージ SUNWvts および SUNWvtsx として、コアとともにまとめて Solaris 8 および 9 ソフトウェアのサブリメント CD に収録されています。SunVTS コアを使用する、ほかの個別のテストは、テスト対象のデバイスのドライバソフトウェアとともに提供されます。

Sun Crypto Accelerator 4000 ボードは、3 つの SunVTS テストによって診断できます。そのうち、nettest および net1btest の 2 つのテストは、SunVTS 5.1 Patch Set (PS) 2 以降のコア SunVTS ソフトウェアに含まれています。これらのテストは、ボードの Ethernet 回路上で動作します。

3 つ目の SunVTS テスト vcatetest は、Sun Crypto Accelerator 4000 CD にパッケージ SUNWvcav として収録されていて、コア SunVTS ラッパーとともに動作して、ボードの暗号化回路を診断します。

vca ドライバ用の SunVTS netlbttest および nettest のインストール

表 7-1 に、既存の SunVTS ソフトウェアを更新して、vca ドライバ用の SunVTS netlbttest および nettest を導入する方法を示します。

表 7-1 vca ドライバ用の SunVTS netlbttest および nettest の必須ソフトウェア

基本 Solaris ソフトウェア	基本 SunVTS ソフトウェア	必須交換 パッケージ	必須オーバー レイパッチ
Solaris 8 7/01	SunVTS4.4		111854-04
Solaris 8 10/01	SunVTS4.5		112250-04
Solaris 8 2/02	SunVTS4.6	SunVTS5.1ps2	
Solaris 9 5/02	SunVTS5.0	SunVTS5.1ps2	
Solaris 9 9/02	SunVTS5.1		113614-11
Solaris 8 HW 12/02	SunVTS5.1ps1		113614-11
Solaris 9 12/02	SunVTS5.1ps1		113614-11
Solaris 8 HW 5/03	SunVTS5.1ps2		
Solaris 9 4/03	SunVTS5.1ps2		

SunVTS ソフトウェアは、Solaris の各バージョンに付属する Solaris ソフトウェアサプレメント CD に収録されています。表 7-1 の「基本 SunVTS ソフトウェア」欄に示す SunVTS ソフトウェアの各バージョンは、同じ行に示す Solaris に付属する Solaris ソフトウェアサプレメント CD に収録されています。

表 7-1 の「SunVTS」で始まるエントリは、SunVTS パッケージセットのバージョンを示しています。各 SunVTS パッケージセットに含まれている SUNWvts および SUNWvtsx パッケージをインストールする必要があります。

表 7-1 の「必須交換パッケージ」欄は、既存の SunVTS パッケージセットを、その SunVTS パッケージセットに交換する必要があることを示しています。SunVTS 交換パッケージを追加する前に、既存の SunVTS パッケージを削除する必要があります。以前にインストールした SunVTS パッケージは、それをインストールした方法と同じ方法で削除します。たとえば、pkgadd コマンドを使用してパッケージをインストールした場合は、pkgrm コマンドを使用してパッケージを削除します。

表 7-1 の「必須オーバーレイパッチ」欄にパッチが示されている場合には、patchadd コマンドを使用して、「基本 SunVTS ソフトウェア」欄の SunVTS パッケージにそのパッチを上書きインストールします。必須パッチを追加する前に、既存の SunVTS パッケージを削除しないでください。

patchadd コマンドを使用してパッチ 113614-11 をインストールすると、既存の SunVTS パッケージを SunVTS5.1ps2 パッケージと交換した場合と同じ結果が得られます。

交換パッケージは、次の URL から入手できます。
<http://www.sun.com/oem/products/vts/>

オーバーレイパッチは、次の URL から入手できます。
<http://sunsolve.sun.com/>

注 – 必須 SunVTS パッケージおよび必須パッチは、SUNWvcav パッケージをインストールする前にインストールしておく必要があります。SUNWvcav パッケージには、SunVTS テスト vctest が含まれています。

SunVTS ソフトウェアによる vctest および nettest、netlbttest の実行

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 のテストリファレンスマニュアルおよびユーザーマニュアル、リファレンスカードを参照してください。これらのマニュアルは、<http://docs.sun.com> の Solaris on Sun Hardware Documentation Set から入手できます。これらのマニュアルは、使用する Solaris リリースに付属する Solaris ソフトウェアサブプリメント CD でも提供されています。

注 – SunVTS は、必須 SunVTS パッケージおよび必須 SunVTS パッチをインストールした場合にだけ使用できます。

▼ vctest 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にしています。

2. SunVTS Diagnostic 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 `vcatest` 以外のチェックボックスのチェックを外します。
 - `vcatest` が表示された場合は、手順 6 に進みます。
 - `vcatest` が表示されない場合は、「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検索します。具体的な手順については、SunVTS のユーザーマニュアルを参照してください。プローブが終了して `vcatest` が表示されたら、手順 6 に進みます。
6. `vcatest` のインスタンスを 1 つ選択し、右クリックおよびドラッグして「Test Parameter Options」ダイアログボックスを表示します。

このオプションは、`vcatest` にのみ関連します。詳細は、123 ページの「`vcatest` 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 `vcatest` 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 `vcatest` のチェックしたインスタンスをすべて変更します。

この操作によって、ダイアログボックスが閉じられ、SunVTS Diagnostic のメインウィンドウに戻ります。
8. `vcatest` のインスタンスを 1 つ選択し、右クリックおよびドラッグして「Test Execution Options」ダイアログボックスを表示します。

「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」ダイアログボックスを表示できます。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 のユーザー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」をクリックしてダイアログボックスを閉じ、SunVTS 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。

vcatest のテストパラメタオプション

表 7-2 に、vcatest サブテストの説明を示します。

表 7-2 vcatest サブテスト

テスト名	説明
CDMF	CDMF バルク暗号化をテストします。
DES	DES バルク暗号化をテストします。
3DES	3DES バルク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。
MD5	MD5 メッセージダイジェスト/デジタルシグニチャーをテストします。
SHA1	SHA1 ダイジェスト鍵生成をテストします。
RNG	乱数ジェネレータをテストします。

vcatest のコマンド行構文

vcatest を CDE インタフェースではなく、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、vcatest へのパスは /opt/SUNWvts/bin/ です。64 ビットモードでは、vcatest 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 vcatest 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。vcatest 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 vcatest を起動する例を示します。次のコマンドにより、vca0 のすべてのサブテストが実行されます。

```
# /opt/SUNWvts/bin/vcatest -f -o dev=vca0,t1=all
```

次に、SunVTS インフラストラクチャーから 64 ビットモードの `vcatest` を起動する例を示します。次のコマンドにより、`vca2` の RSA および DSA、MD5 テストが実行されます。

```
# /opt/SUNWvts/bin/sparcv9/vcatest -f -o dev=vca2,t1=RSA+DSA+MD5
```

コマンド行から `vcatest` 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表 7-3 に示すデフォルトの動作になります。

表 7-3 `vcatest` のコマンド行構文

オプション	説明
<code>dev=vcaN</code>	テストするデバイスのインスタンスを、 <code>vca0</code> 、 <code>vca2</code> のように指定します。指定しない場合のデフォルトは、 <code>vca0</code> です。 <code>N</code> には、テストするデバイスのインスタンス番号を指定することに注意してください。
<code>t1=testlist</code>	実行するサブテストのリストを指定します。 <code>t1</code> には、サブテストをプラス (+) の文字で区切って指定します。サポートするサブテストは、CDMF および DES、3DES、DSA、RSA、MD5、SHA1、RNG です。したがって、 <code>t1=CDMF+DES+3DES+DSA+RSA+MD5+SHA1+RNG</code> を指定すると、すべてのサブテストを実行することになります。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のデフォルトは <code>a11</code> です。

▼ netlbttest 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
```

起動方法の詳細は、SunVTS の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 Diagnostic 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. 「Network」のチェックボックスを選択し、「Network」の「+」ボタンをクリックして、Network グループのすべてのテストを表示します。
5. Network グループの `vcaN(net1btest)` 以外のチェックボックスのチェックを外します。N には、テスト中のデバイスのインスタンス番号が表示されていることに注意してください。
 - `vcaN(net1btest)` が表示された場合は、手順 6 に進みます。
 - `vcaN(net1btest)` が表示されない場合は、「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検索します。

具体的な手順については、SunVTS のユーザーマニュアルを参照してください。プローブが終了して `vcaN(net1btest)` が表示されたら、手順 6 に進みます。

6. 「Intervention Mode」ボタンを選択します。`vcaN(net1btest)` のインスタンスを 1 つ選択し、右クリックおよびドラッグして「Test Parameter Options」ダイアログボックスを表示します。

このオプションは、`net1btest` にのみ関連します。詳細は、SunVTS のテストリファレンスマニュアル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 `vcaN(net1btest)` 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 `vcaN(net1btest)` のチェックしたインスタンスをすべて変更します。

この操作によって、ダイアログボックスが閉じられ、SunVTS Diagnostic のメインウィンドウに戻ります。

8. `vcaN(net1btest)` のインスタンスを 1 つ選択し、右クリックおよびドラッグして「Test Execution Options」ダイアログボックスを表示します。

「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」ダイアログボックスを表示できます。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 のユーザー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」をクリックしてダイアログボックスを閉じ、SunVTS 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。

▼ nettest 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
```

起動方法の詳細は、SunVTS の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 Diagnostic 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. 「Network」のチェックボックスを選択し、「Network」の「+」ボタンをクリックして、Network グループのすべてのテストを表示します。
5. Network グループの `vcaN(nettest)` 以外のチェックボックスのチェックを外します。 N には、テスト中のデバイスのインスタンス番号が表示されることに注意してください。
 - `vcaN(nettest)` が表示された場合は、手順 6 に進みます。
 - `vcaN(nettest)` が表示されない場合は、`vcaN` ボードを含むサーバーのほかのウィンドウで `ifconfig -a` と入力します。エントリは次のように表示されます。

```
vcaN up inet ip-address plumb
```

前述の `ifconfig` エントリが表示されない場合、`nettest` プロブはデバイスがテスト不可であると判断します。インターフェースをオンラインにするには、`ifconfig` のオンラインマニュアルページの指示に従ってください。

`ifconfig -a` が前述のエントリを表示したら、SunVTS Diagnostic のメインウィンドウに戻り、「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 `vca` を検索します。

具体的な手順については、SunVTS のユーザーマニュアルを参照してください。プローブが終了して `vca0(nettest)` が表示されたら、手順 6 に進みます。

6. `vcaN(nettest)` のインスタンスを 1 つ選択し、右クリックおよびドラッグして「Test Parameter Options」ダイアログボックスを表示します。

このオプションは、nettest にのみ関連します。詳細は、SunVTS のテストリファレンスマニュアル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 vcaN(nettest) 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 vcaN(nettest) のチェックしたインスタンスをすべて変更します。

この操作によって、ダイアログボックスが閉じられ、SunVTS Diagnostic のメインウィンドウに戻ります。

8. vcaN(nettest) のインスタンスを 1 つ選択し、右クリックおよびドラッグして「Test Execution Options」ダイアログボックスを表示します。

「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」ダイアログボックスを表示できます。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 のユーザー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」をクリックしてダイアログボックスを閉じ、SunVTS 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。

注 - nettest と netlbttest を選択して同時に実行しないでください。

kstat による暗号化の処理状況の確認

Sun Crypto Accelerator 4000 ボードには、暗号化の処理状況を示す 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 vca:0
module: vca                instance: 0
name:    vca0              class:    misc
        3desbytes          3040
        3desjobs           5
        crtime              65.342725895
        dsassign            0
        dsverify            0
        rngbytes            10592
        rngjobs             187
        rngshalbytes        16328
        rngshaljobs         327
        rsapivate           9
        rsapublic           0
        snaptime            106956.467004482
```

注 - この例で、0 は `vca` デバイスのインスタンス番号です。この番号は、`kstat` コマンドの実行の対象に指定したボードのインスタンス番号を反映しています。

`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 4000 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 4000 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/vca.conf` ファイルに `nostats` 属性を指定すると、統計情報の取得および表示は実行できなくなります。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。

OpenBoot PROM の FCode 自己診断の使用

このテストは、システムが起動していない場合にアダプタの問題を特定するのに役立ちます。

FCode 自己診断を起動するには、OpenBoot PROM (OBP) の `test` または `test-all` コマンドを使用します。診断中にエラーが検出された場合には、適切なメッセージが表示されます。`test` および `test-all` コマンドの詳細は、『OpenBoot コマンド・リファレンスマニュアル』を参照してください。

FCode 自己診断では、ほとんどの機能を細部ごとに動作させて、次のことを確認します。

- アダプタボードを取り付けているときの接続性
- システム起動に必要な部品がすべて機能していることの確認

▼ Ethernet FCode 自己診断を実行する

Ethernet 診断を実行するには、まずシステムをリセットして、OBP プロンプトが表示されるまで起動する必要があります。システムをリセットしないと、診断テストでシステムがハングアップする場合があります。

ここで実行する OpenBoot コマンドの詳細は、『OpenBoot コマンド・リファレンスマニュアル』を参照してください。

1. システムを停止します。

停止は、『Sun 周辺機器使用の手引き』に記載されている標準的な停止手順を実行してください。

2. OBP プロンプトで、`auto-boot?` 構成変数を `false` に設定します。

```
ok setenv auto-boot? false
```

3. システムをリセットします。

```
ok reset-all
```

4. `show-nets` を実行してデバイスの一覧を表示し、デバイスを選択します。

次に示すような、アダプタに関するデバイスの一覧が表示されます。

```
ok show-nets
a) /pci@8,600000/network@1
b) /pci@8,700000/network@5,1
q) NO SELECTION
Enter Selection, q to quit: a
/pci@8,600000/network@1 has been selected.
Type ^Y ( Control-Y ) to insert it in the command line.
e.g. ok nvalias mydev ^Y for creating devalias mydev for
/pci@8,600000/network@1
```

注 – 次の手順で `test` コマンドによる自己診断を実行する前に、Ethernet ポートをネットワークに接続しておく必要があります。

5. `test` コマンドを使用して、自己診断を実行します。

`test` コマンドを実行すると、次の自己診断が行われます。

- vca レジスタのテスト (diag-switch? に true が設定されている場合のみ)
- 内部ループバックテスト
- 接続状態の確認テスト

注 – 1000 Mbps 接続の Sun Crypto Accelerator 4000 UTP アダプタの自己診断では、link-clock パラメータを調整できないため、外部ループバックケーブルを使用するテストはサポートされません。この診断では、ローカルおよび遠隔のポートが、それぞれクロックマスターおよびクロックスレーブになるように調整する必要があります。外部ループバックケーブルを使用すると、ローカルと遠隔のポートが同一になります。1つのポートはクロックマスターおよびクロックスレーブの両方になれないので、PHY 接続は確立できません。Sun Crypto Accelerator 4000 UTP アダプタの自己診断を 1000 Mbps 接続で実行するには、遠隔の 1000Base-T ポートに接続する必要があります。

次のように入力します。

```
ok test device_path
```

test に合格すると、次のメッセージが表示されます。

```
ok test /pci@8,600000/network@1
Testing /pci@8,600000/network@1
Register tests: passed
Internal loopback test: passed
/pci@8,600000/network@1: 100 Mbps half duplex link up
```

ボードがネットワークに接続できなかった場合は、次のメッセージが表示されます。

```
ok test /pci@8,600000/network@1
Testing /pci@8,600000/network@1
Register tests: passed
Internal loopback test: passed
/pci@8,600000/network@1: link down
```

- アダプタをテストしたあとは、次のように入力して OBP インタフェースを標準の動作モードに戻します。

```
ok setenv diag-switch? false
```

- auto-boot? 構成パラメタを true に設定します。

```
ok setenv auto-boot? true
```

- システムをリセットして再起動します。

Sun Crypto Accelerator 4000 ボードの障害追跡

この節では、ボードの障害追跡に使用できる OBP レベルのコマンドについて説明します。ここで説明するコマンドの詳細は、『OpenBoot コマンド・リファレンスマニュアル』を参照してください。

show-devs

Sun Crypto Accelerator 4000 デバイスがシステムに認識されているかどうかを確認するには、OBP プロンプトから `show-devs` を入力して、デバイスの一覧を表示します。次の例に示すように、Sun Crypto Accelerator 4000 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
.
.
/chosen
/packages
/upa@8,480000/SUNW,ffb@0,0
/pci@8,600000/network@1
/pci@8,600000/SUNW,qlc@4
/pci@8,600000/SUNW,qlc@4/fp@0,0
.
.
```

この例では、`/pci@8,600000/network@1` エントリが Sun Crypto Accelerator 4000 ボードのデバイスパスです。このようなエントリが、システム内のボードごとに 1 行表示されます。

.properties

Sun Crypto Accelerator 4000 のデバイスの属性が正しく設定されているかどうかを確認するには、OBP プロンプトから `.properties` を入力して、属性の一覧を表示します。

```

ok .properties
assigned-addresses      82000810 00000000 00102000 00000000 00002000
                        81000814 00000000 00000400 00000000 00000100
                        82000818 00000000 00200000 00000000 00200000
                        82000830 00000000 00400000 00000000 00100000
d-fru-len               00 00 00 00
d-fru-off                00 00 e8 00
d-fru-dev                eeprom
s-fru-len                00 00 08 00
s-fru-off                00 00 e0 00
s-fru-dev                eeprom
compatible              70 63 69 38 30 38 36 2c 62 35 35 35 2e 31 30 38
reg                      00000800 00000000 00000000 00000000 00000000
                        02000810 00000000 00000000 00000000 00002000
                        02000814 00000000 00000000 00000000 00000100
                        02000818 00000000 00000000 00000000 00200000
                        02000830 00000000 00000000 00000000 00100000
address-bits             00 00 00 30
max-frame-size           00 00 40 00
network-interface-type  ethernet
device_type              network
name                     network
local-mac-address        08 00 20 aa bb cc
version                  Sun PCI Crypto Accelerator 4000 1000Base-T Code
2.11 02/10/31
phy-type                 mif
board-model              501-6039
model                    SUNW,pci-vca
fcode-rom-offset         00000000
66mhz-capable
fast-back-to-back
devsel-speed             00000001
class-code                00100000
interrupts                00000001
latency-timer             00000040
cache-line-size           00000010
max-latency                00000040
min-grant                  00000040
subsystem-id              00003de8
subsystem-vendor-id       0000108e
revision-id                00000002
device-id                  0000b555
vendor-id                  00008086

```

watch-net

ネットワーク接続を監視するには、OBP プロンプトから `apply watch-net` コマンドとデバイスパスを入力します。

```
ok apply watch-net /pci@8,600000/network@1
/pci@8,600000/network@1: 1000 Mbps full duplex link up
Watch ethernet packets
'.' is a good packet and 'X' is a bad packet
Press any key to stop
.....X...X.....X.....
```

システムはネットワークトラフィックを監視します。正常なパケットを受信すると「.」を表示し、受信したパケットにネットワークハードウェアインタフェースが検出したエラーが含まれていると「X」を表示します。

付録 A

仕様

この付録では、Sun Crypto Accelerator 4000 の MMF および UTP アダプタの仕様について説明します。この付録は、次の節で構成されます。

- 135 ページの「Sun Crypto Accelerator 4000 MMF アダプタ」
 - 138 ページの「Sun Crypto Accelerator 4000 UTP アダプタ」
-

Sun Crypto Accelerator 4000 MMF アダプタ

この節では、Sun Crypto Accelerator 4000 MMF アダプタの仕様について説明します。

コネクタ

図 A-1 に、Sun Crypto Accelerator 4000 MMF アダプタのコネクタを示します。



図 A-1 Sun Crypto Accelerator 4000 MMF アダプタのコネクタ

表 A-1 に、SC コネクタ (850 nm) の特性を示します。

表 A-1 SC コネクタ接続の特性 (IEEE P802.3z)

特性	62.5 ミクロン MMF	50 ミクロン MMF
動作範囲	最長 260 m	最長 550 m

物理寸法

表 A-2 物理寸法

寸法	測定値	メートル表記
長さ	12.283 インチ	312.00 mm
幅	4.200 インチ	106.68 mm

性能仕様

表 A-3 性能仕様

機能	仕様
PCI クロック	最大 33/66 MHz
PCI データバースト転送	最大 64 バイトのバースト
PCI データ/アドレス幅	32/64 ビット
PCI モード	マスター/スレーブ
1 Gbps、850 nm	1000 Mbps (全二重)

電源要件

表 A-4 電源要件

仕様	測定値
最大電力消費量	6.25 W @ 5V 12.75 W @ 3.3V
電圧許容範囲	5 V +/- 5% 3.3 V +/- 5%

インタフェース仕様

表 A-5 インタフェース仕様

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	PCI 2.1、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
PCI バス幅	32 ビットまたは 64 ビット

環境仕様

表 A-6 環境仕様

条件	動作時の仕様	保管時の仕様
温度	0 ~ +55°C、 +32 ~ +131°F	-40 ~ +75°C、 -40 ~ +167°F
相対湿度	5 ~ 85% 結露のないこと	0 ~ 95% 結露のないこと

Sun Crypto Accelerator 4000 UTP アダプタ

この節では、Sun Crypto Accelerator 4000 UTP アダプタの仕様について説明します。

コネクタ

図 A-2 に、Sun Crypto Accelerator 4000 UTP アダプタのコネクタを示します。



図 A-2 Sun Crypto Accelerator 4000 UTP アダプタのコネクタ

表 A-7 に、Sun Crypto Accelerator 4000 UTP アダプタが使用する Cat-5 コネクタの特性を示します。

表 A-7 Cat-5 コネクタ接続の特性

特性	説明
動作範囲	最長 100 m

物理寸法

表 A-8 物理寸法

寸法	測定値	メートル表記
長さ	12.283 インチ	312.00 mm
幅	4.200 インチ	106.68 mm

性能仕様

表 A-9 性能仕様

機能	仕様
PCI クロック	最大 33/66 MHz
PCI データバースト転送	最大 64 バイトのバースト
PCI データ/アドレス幅	32/64 ビット
PCI モード	マスター/スレーブ
1 Gbps、850 nm	1000 Mbps (全二重)

電源要件

表 A-10 電源要件

仕様	測定値
最大電力消費量	6.25 W @ 5V 12.75 W @ 3.3V
電圧許容範囲	5 V +/- 5% 3.3 V +/- 5%

インタフェース仕様

表 A-11 インタフェース仕様

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	PCI 2.1、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
PCI バス幅	32 ビットまたは 64 ビット

環境仕様

表 A-12 環境仕様

条件	動作時の仕様	保管時の仕様
温度	0 ~ +55°C、 +32 ~ +131°F	-40 ~ +75°C、 -40 ~ +167°F
相対湿度	5 ~ 85% 結露のないこと	0 ~ 95% 結露のないこと

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 4000 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 사용되는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/cryptov2/bin/apgetpass` は、 *program* の実行可能ファイルとして使用できます。このプログラムは自動的にパスワードの入力を求めるプロンプトを表示します。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。この機能は、Web サーバーの起動時のユーザーの操作をなくしたい場合に使用します。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だけが入っています。

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。システム起動時のユーザーの操作をなくすには、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、仮想ホストで使用します。通常は、次のような書式が使用されます。

```
<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 B-1 に、使用可能なプロトコルとその説明を示します。

表 B-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。多くの一般的な Web ブラウザでサポートされています。
TLSv1	SSLv3 を更新したもの。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で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は、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、設定された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 B-2 に示す暗号を、コロンで区切って指定します。表 B-2 で、DH は Diffie-Hellman を、DSS は Digital Signature Standard を表します。

表 B-2 使用できる 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 B-2 使用できる 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 B-3 に、マクロのように暗号をグループ化するために使用する別名を示します。

表 B-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 B-4 に示す特殊文字を使用して設定できます。

表 B-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) を使用する場合、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 B-5 に、*level* の値を示します。

表 B-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	有効な証明書が必要な場合がある
require	有効な証明書が必要
optional_no_ca	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では、SSL 固有の情報を記録す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する情報のレベルを指定します。表 B-6 に、*level* の値を示します。

表 B-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 B-7 に、オプションを示します。

表 B-7 使用できる SSL 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 <code>SSL_SERVER_CERT</code> および <code>SSL_CLIENT_CERT</code> 、 <code>SSL_CLIENT_CERT_CHAIN<i>n</i></code> ($n = 0, 1, \dots$) 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 (Distinguished Name : 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 <code>xxj31ZMTZzkVA</code> 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。
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。

Sun Crypto Accelerator 4000 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 4000 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 4000 ボードの高速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。OpenSSL の標準ライブラリで構築した方が効果的な場合もあります。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 – ここで説明する Sun Crypto Accelerator 4000 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。この製品の一部分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、保証はいたしません。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 SUNWkcl2o 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/cryptov2/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/cryptov2/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` ライブラリのいずれかまたは両方を参照します。また、サンの暗号化ライブラリも指定する必要があります。それには、リンカー属性を次のように指定します。

```
-L/opt/SUNWconn/cryptov2/lib -R/opt/SUNWconn/cryptov2/lib \  
-lcrypto -lssl -lkcl
```


ソフトウェアライセンス

この付録では、サンのバイナリコードライセンス契約書 (Sun Binary Code License Agreement)、およびサン以外のベンダーが規定す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。

注 – この付録のサン以外のベンダーのライセンスおよび注意は、そのソフトウェアの所有者が提供するライセンスおよび注意をそのまま記載したものです。

Sun Microsystems, Inc.

バイナリコードライセンス契約書

このソフトウェア製品のパッケージを開封する前に、この契約書の条項と補足ライセンス条項 (以下「本契約」といいます) をよくお読みください。ソフトウェア製品のパッケージを開封すると、本契約の条項を同意したものとみなされます。電子的な手段でこのソフトウェアにアクセスしている場合は、本契約の末尾にある「同意する」ボタンを選択して同意してください。これらの条項に同意できない場合は、未使用のソフトウェアを購入店にただちに返却し、代金の払い戻しを受けてください。電子的な手段でソフトウェアにアクセスしている場合は、本契約の末尾の「キャンセル」ボタンを選択してください。

1. 使用の許諾。Sun は、お客様に対して、使用料が支払われているユーザー数およびコンピュータハードウェアのクラスに応じて、Sun が提供する付随するソフトウェア、文書、および修正プログラム (以下「本ソフトウェア」といいます) を内部でのみ使用するための非独占的で譲渡不能な使用权を許諾します。

2. 制限。本ソフトウェアには秘密情報が含まれており、著作権は保護されています。本ソフトウェアの権限および付随するすべての知的財産権は、Sun およびそのライセンサー (またはそのいずれか) が保有しています。補足ライセンス条項において特に許諾されていない限り、本ソフトウェアの複製物を作成することは禁止されています。ただし、本ソフトウェアの複製物を保存用に1部だけ作成することは許可されています。適用のある法令によってかかる制限禁じられている場合を除き、本ソフトウェアを変更、逆コンパイル、もしくはリバースエンジニアリングすることは禁止されています。お客様は、本ソフトウェアが、核施設の設計、建設、運転または保守で

使用するように設計、ライセンス、および意図されていないことを認識するものとします。Sun は、そのような目的の適合性に関して、明示的、黙示的を問わずいかなる保証も致しません。本契約では、Sun またはそのライセンサーの商標、サービスマーク、ロゴまたは商号の権利、権限、または所有権は一切与えられません。

3. 限定保証。Sun は、領収証に記入された購入日から90 日間、本ソフトウェアが正常に使用された場合に限り、本ソフトウェアが保存されている媒体 (存在する場合) の材質上および製造上の瑕疵がないことを保証します。上記のことを除いて、本ソフトウェアは「現状のまま」で提供されます。この限定保証では、お客様に対する全面的な補償と Sun の全責任は、本ソフトウェア製品の交換または本ソフトウェアに対してお客様が支払った代金の払い戻しに限られます。

4. 保証の否認。本契約に明記されていない限り、商品性、特定目的への適合性、または権利の非侵害性に関する黙示の保証を含む、すべての明示的または黙示的な条件、表明および保証を否認します。ただし、これらの否認が法令で認められていない場合はこの限りではありません。

5. 責任の限度。Sun またはそのライセンサーは、たとえ損害の可能性を知らされていたとしても、本ソフトウェアの使用または使用不能を原因とする、またはそれに関連する、収益、利益、データの喪失、その他一切の損害 (特別損害、間接損害、偶発的損害、付随的損害、懲罰的損害を問いません) に対して、法令が認める範囲で、その責任内容に関わらず一切責任を負いません。契約に定められた行為、または定められていない行為 (過失を含めて) によるものであるかに関わらず、お客様に対する Sun の責任は、いかなる場合も本契約に基づいてお客様が本ソフトウェアに対して支払った金額を超えることはありません。上記の制限は、前述の保証内容よりも優先されるものとします。

6. 終了。本契約は終了するまで有効です。お客様は、本ソフトウェアの複製物をすべて破棄することにより、本契約をいつでも終了することができます。お客様が本契約の条項に従わなかった場合、Sun から通知されることなく、本契約はただちに終了するものとします。終了時には、お客様はソフトウェアの複製物をすべて破棄しなければなりません。

7. 輸出規制。本契約で提供されるすべてのソフトウェアおよび技術的データは、米国輸出管理法の対象となっています。また、他国においても輸出入管理法規の対象となっている場合があります。お客様は、それらのすべての法令および規制を厳守することに同意し、納品後に輸出、再輸出、または輸入の許可が必要となった場合には、お客様にそれらを取得する責任があるものとします。

8. アメリカ合衆国連邦政府の制限された権利。本ソフトウェアが米国連邦政府やその代理機関、また米国連邦政府と直接的あるいは間接的に契約を結んだ機関によって取得された場合、ソフトウェアおよび付随する文書に対する米国連邦政府の権限は、48 CFR 227.7201、227.7202-4 (米国国防総省による取得) および 48 CFR 2.101、12.212 (米国国防総省以外による取得) に従って、この契約書に記載されている内容に制限されます。

9. 準拠法。本契約は、カリフォルニア州法およびそれを統括している米国連邦法を準拠法とします。法域や法令を選択することはできません。

10. 可分性。本契約の一部が強制力を持たないと判明した場合でも、残りの部分は引き続き有効になります。ただし、その条項を除くことで当事者の目的が達成されなくなる場合は、本契約はただちに終了するものとします。

11. 完全性。本契約は、お客様とSun における、その契約内容に関する完全な合意であり、事前または同時になされた口頭または書面による協議、提案、表明、および保証よりも優先されます。また、本契約期間中に当事者間で交わされた、契約内容に関する見積り、注文、承認、その他一切の協議との間で、矛盾や追加条項がある場合、本契約が優先されます。本契約は、各当事者の権限のある代表者が署名した書面によってのみ、その内容を変更することができます。

ご質問がある場合は、Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, California 95054 までお問い合わせ下さい。

(Form ID#011801)

Sun Microsystems, Inc.

Sun Crypto Accelerator 4000 補足ライセンス条項

本補足ライセンス条項 (以下「補足条項」とする) はバイナリコードライセンス契約書 (以下集合的に「本契約書」とする) の条項に追加または修正を加えるものです。本補足条項に定義されていない大文字の用語は、本契約書における定義と同義です。本補足条項は、本契約書またはソフトウェアに含まれるライセンス条項における矛盾する条項、または相反する条項のすべてに優先します。

1. Sun 以外のベンダーのライセンス条項。本ソフトウェアの一部は、Sun 以外のベンダーによって、その部分の使用を規定する注意およびライセンス (またはそのいずれか) とともに提供されています。

サン以外のベンダーのライセンス条項

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 aheared 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.

付録 E

マニュアルページ

この付録では、Sun Crypto Accelerator 4000 ボードでのコマンドの説明と、各コマンドに対応するオンラインマニュアルページを示します。この付録に記載するコマンドは、すべて Sun Crypto Accelerator 4000 ソフトウェアに含まれています。

オンライン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 E-1 に、参照できるオンラインマニュアルページを示します。

表 E-1 Sun Crypto Accelerator 4000 のオンラインマニュアルページ

マニュアルページ	説明
vca(7d)	vca デバイスドライバは、それに属す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。 アプリケーションおよびカーネルクライアントが vca ドライバのサービスにアクセスするには、階層化されたソフトウェアが必要です。
vca(1m)	vca(1m) デーモンは、キースタアサービスを提供します。
vcaadm(1m)	vcaadm は、Sun Crypto Accelerator 4000 の管理プログラムです。 vcaadm コマンドは、Sun Crypto Accelerator 4000 ボードに関連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。 vcaadm は、重要な暗号化鍵情報を取り扱います。
vcadiag(1m)	vcadiag は、root ユーザーに Sun Crypto Accelerator 4000 ボードのリセットおよび鍵素材の消去の機能を提供するユーティリティです。また、root ユーザーは、このユーティリティを使用して基本的な診断を実行することもできます。
kc12(7d)	kc12 は、暗号化ハードウェアドライバをサポートするカーネルモジュールです。

表 E-1 Sun Crypto Accelerator 4000 のオンラインマニュアルページ (続き)

マニュアルページ	説明
kc12(7d)	kc12 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、サンの暗号化ドライバをサポートします。 アプリケーションおよびカーネルクライアントが kc12 ドライバが提供するサービスにアクセスするには、階層化されたソフトウェアが必要です。
apsslcfg(1m)	apsslcfg は、Apache Web サーバー用の構成ユーティリティーです。
iplsslcfg(1m)	iplsslcfg は、Sun ONE Web サーバー用の構成ユーティリティーです。

付録F

ハードウェアの情報の消去

この付録では、Sun Crypto Accelerator 4000 ボードを、出荷時の状態である failsafe モードに戻す (情報を消去する) 方法について説明します。



注意 – この付録に記載されている手順は、必要な場合以外には行わないでください。vcaadm の zeroize コマンドは、すべての鍵素材を削除する必要がある場合にのみ使用できます。zeroize コマンドの詳細は、78 ページの「Sun Crypto Accelerator 4000 ボードの情報の消去」を参照してください。また、すべての鍵素材の削除方法については、vcadiag(4) のオンラインマニュアルページも参照してください。

注 – この付録で説明する手順を行うと、Sun Crypto Accelerator 4000 ファームウェアは削除されます。この手順を行った場合は、Sun Crypto Accelerator 4000 ソフトウェアに付属するファームウェアを再インストールする必要があります。

Sun Crypto Accelerator 4000 ハードウェアの情報の消去による出荷時状態への復帰

状況によっては、ボードを failsafe モードに戻し、すべての鍵素材および構成情報を消去する必要がある場合があります。この作業は、ボードに付属するハードウェアジャンパを使用して行います。

注 - vcaadm ユーティリティの zeroize コマンドを使用して、Sun Crypto Accelerator 4000 ボードからすべての鍵素材を削除することもできます。ただし、zeroize コマンドは、更新したファームウェアはそのまま残します。詳細は、78 ページの「Sun Crypto Accelerator 4000 ボードの情報の消去」を参照してください。また、vcadiag のオンラインマニュアルページも参照してください。

▼ ハードウェアジャンパを使用して Sun Crypto Accelerator 4000 ボード上の情報を消去する

1. システムの電源を切断します。

注 - システムによっては、電源を切断する代わりに動的再構成 (DR) を使用して、この手順に必要なボードを取り外し交換することができます。DR の正しい手順については、システムに付属のマニュアルを参照してください。



注意 - ジャンパを調整している間は、ボードに電源を供給しないでください。

2. コンピュータのカバーを取り外して、ボードの上部中央にあるジャンパを探します。
3. ジャンパブロックのピン 0 および 1 に、ジャンパを取り付けます。

ピン 0 と 1 は、留め具にもっとも近いところにあるピンで、「Z」のラベルが付いています。図 F-1 に示すように、ジャンパブロックには 2 つで 1 組のピンが 4 組あり、ピン 0 と 1 の組にジャンパを取り付ける必要があります。



注意 – ピン 0 と 1 にジャンパが取り付けられた Sun Crypto Accelerator 4000 ボードは使用できません。

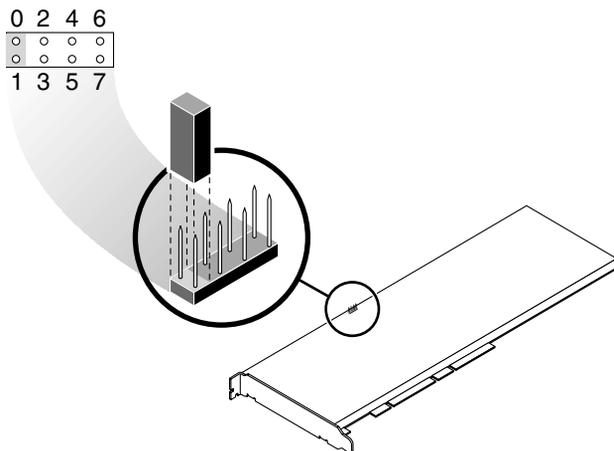


図 F-1 Sun Crypto Accelerator 4000 ボードのジャンパブロックのピン

4. システムの電源を入れます。



注意 – Sun Crypto Accelerator 4000 ボードのジャンパを調整してシステムの電源を入れると、すべてのファームウェアおよび鍵素材、構成情報が削除されます。この手順を行うと、ボードは出荷時の状態の failsafe モードに戻ります。

5. システムの電源を切断します。
6. ジャンパブロックのピン 0 および 1 からジャンパを取り外し、元の位置に戻します。
7. システムの電源を入れます。
8. `vcaadm` を使用して、Sun Crypto Accelerator 4000 ボードに接続します。
`vcaadm` は、ファームウェアをアップグレードするためのパスの入力を求めます。
9. ファームウェアをインストールするためのパスとして、
`/opt/SUNWconn/cryptov2/firmware/sca4000fw` を入力します。
ファームウェアが自動的にインストールされて、ユーザーは `vcaadm` からログアウトされます。

10. `vcaadm` を使用して、Sun Crypto Accelerator 4000 ボードに再接続します。

`vcaadm` は、新しいキーストアと既存のキーストアのどちらを使用してボードを初期化するかを指定するプロンプトを表示します。詳細は、63 ページの「`vcaadm` による Sun Crypto Accelerator 4000 ボードの初期化」を参照してください。

よく受ける質問

再起動時のユーザーの操作をなくすには、Web サーバーをどのように設定すればよいのですか？

Sun ONE および Apache Web サーバーは、再起動したとき、暗号化された鍵を使用して自動的に起動することができます。

▼ 再起動時に Apache Web サーバーを自動起動するために、暗号化された鍵を作成する

1. 次のエントリが `httpd.conf` ファイルに存在するかどうかを確認します。

```
SSLPassPhraseDialog exec:/opt/SUNWconn/cryptov2/bin/apgetpass
```

このディレクティブは、`/etc/apache` ディレクトリ内の保護されたパスワードファイルからパスワードを 1 つ取り出します。

2. 前の手順で取り出した `/etc/apache` ディレクトリ内のパスワードだけを含むパスワードファイルを作成します。ファイルには、次の命名規則に従って名前を付けます。

```
server_name:port.KEYTYPE.pass
```

- *server_name* - `httpd.conf` ファイルの「`ServerName`」ディレクティブに設定した値
- *port* - この SSL サーバーが動作しているポート (たとえば、443)
- *KEYTYPE* - RSA または DSA

たとえば、RSA 鍵を使用してポート 443 で SSL を実行している webserv101 という名前のサーバーの場合、/etc/apache に次のファイルを作成します。

```
webserv101:443.RSA.pass
```

パスワードのアクセス権および所有者を次のように変更することをお勧めします。

```
# chmod 400 server_name:port.KEYTYPE.pass  
# chown root server_name:port.KEYTYPE.pass
```

詳細は、mod_SSL および OpenSSL のマニュアルを参照してください。

▼ 再起動時に Sun ONE Web サーバーを自動起動するために、暗号化された鍵を作成する

1. Sun ONE Web サーバーインスタンスの config サブディレクトリ (/usr/iplanet/servers/https-webserver_instance_name/config など) に移動します。
2. 次の行だけを含む password.conf ファイルを作成します (パスワードの定義の詳細は、表 5-1 を参照してください)。

```
internal:trust_db_password  
keystore_name:username:password
```

3. パスワードファイルの所有者を、Web サーバーを実行する UNIX ユーザー ID とし、ファイルの所有者だけが読み取ることができるようにアクセス権を設定します。

```
# chown web_server_UNIX_user_ID password.conf  
# chmod 400 password.conf
```

同じサーバーに取り付けた複数のボードに異なる MAC アドレスを割り当てるにはどのようにすればよいのですか？

1 つのサーバーの複数のボードに異なる MAC アドレスを割り当てる方法は 2 つあります。1 つ目の方法はオペレーティング環境レベルで、2 つ目の方法は OpenBoot PROM (OBP) レベルで行います。

▼ 端末エミュレータから異なる MAC アドレスを割り当てる

1. 次のコマンドを実行します。

```
# eeprom "local-mac-address?"=true
```

注 - "local-mac-address?" パラメタが true に設定されていると、統合されていないネットワークインタフェースデバイスはすべて、製造時に製品に割り当てられたローカルの MAC アドレスを使用します。

2. システムを再起動します。

▼ OpenBoot PROM レベルで異なる MAC アドレスを割り当てる

1. OBP プロンプトで、次のコマンドを実行します。

```
ok setenv local-mac-address? true
```

注 - "local-mac-address?" パラメタが true に設定されていると、統合されていないネットワークインタフェースデバイスはすべて、製造時に製品に割り当てられたローカルの MAC アドレスを使用します。

2. オペレーティング環境を起動します。

Apache に Sun Crypto Accelerator 4000 ソフトウェアをインストールしたあとで、Sun Crypto Accelerator 1000 を使用するにはどのようにすればよいのですか？

SUNwkc12a ソフトウェアパッケージをインストールすると、システムには Apache Web サーバー mod_ssl 1.3.26 が構成されます。

Apache で Sun Crypto Accelerator 1000 を構成する場合は、次のパッチが必要になります。

SUNwkc12a パッケージをインストールした Solaris 8 システムで、Apache 1.3.26 とともに Sun Crypto Accelerator 1000 を使用するよう構成するには、次のパッチが必要です。

- Apache 1.3.26 用 - パッチ ID 109234-09 以降

- Sun Crypto Accelerator 1000 バージョン 1.0 ソフトウェア用 – パッチ ID 112869-02
- Sun Crypto Accelerator 1000 バージョン 1.1 ソフトウェア用 – パッチ ID 113355-01

SUNWkc12a パッケージをインストールした Solaris 9 システムで、Apache 1.3.26 とともに Sun Crypto Accelerator 1000 を使用するように構成するには、次のパッチが必要です。

- Apache 1.3.26 用 – パッチ ID 113146-01 以降
- Sun Crypto Accelerator 1000 バージョン 1.1 ソフトウェア用 – パッチ ID 113355-01

テストのため、証明書に自己署名するにはどのようにすればよいのですか？

この手順については、mod_SSL および OpenSSL のマニュアルを参照してください。

索引

記号

`$HOME/.vcaadm/trustdb`, 57
`.properties` コマンド, 132
`.u` 拡張子, 17
`/etc/apache/default.pass`, 144
`/etc/apache/servername.port.keytype.pas`
`ss`, 144
`/etc/driver_aliases` ファイル, 37
`/etc/hostname.vcaN` ファイル, 51
`/etc/hosts` ファイル, 52
`/etc/opt/SUNWconn/vca/keydata`, 19
`/etc/path_to_inst` ファイル, 37
`/kernel/drv/vca.conf` ファイル, 128
`/opt/SUNWconn/crypto/bin/sslpassword`, 1
43
`/opt/SUNWconn/cryptov2/firmware/sca400`
`0fw`, 167
`/opt/SUNWconn/cryptov2/include`, 153
`/opt/SUNWconn/cryptov2/lib`, 19
`/opt/SUNWconn/cryptov2/sbin`, 19

数字

16 ビットのロード可能カウンタ, 44
8 ビットベクトル, 30

A

`adv-asmopause-cap`, 27
`adv-asmopause-cap` パラメタ, 27
`adv-autoneg-cap`, 24
`adv-autoneg-cap` パラメタ, 24
`adv-pause-cap`, 27
`adv-pause-cap` パラメタ, 27
Apache SSL ディレクティブ, 143
Apache Web サーバー, 17
使用するための設定, 112
証明書の作成, 114
ディレクティブ, 143, 144, 145, 146, 147, 148,
149, 150, 151
`.htaccess`, 145
SSL の別名, 147
`SSLCACertificateFile`, 148
`SSLCARevocationFile`, 149
`SSLCertificateChainFile`, 148
`SSLCertificateFile`, 148
`SSLCertificateKeyFile`, 148
`SSLCipherSuite`, 145, 148
`SSLEngine`, 144
`SSLLog`, 149
`SSLLogLevel`, 149
`SSLOptions`, 150
`SSLPassPhraseDialog`, 143
`sslpassword`, 144
`SSLProtocol`, 144
`SSLRequireSSL`, 151
`SSLVerifyClient`, 149
`SSLVerifyDepth`, 149

- 暗号の優先順位, 148
- 使用可能な SSL の暗号, 146
- 特殊文字, 148
- ボードを使用するための設定, 112

auto-boot? 構成変数, 129, 131

D

dcatest, 122

- サブテスト, 123

diag-switch? 構成変数, 130

Diffie-Hellman, 146

Digital Signature Standard, 146

driver.conf ファイル, 37

driver_aliases ファイル, 37

DSS, 146

E

enable-ipg0, 28

enable-ipg0 パラメタ, 28

etc/apache/default.pass, 144

etc/apache/servername.port.keytype.pas
s, 144

etc/hostname.vcaN ファイル, 51

etc/hosts ファイル, 52

etc/path_to_inst ファイル, 37

Ethernet

- FCode 自己診断, 129
- MMF, 24
- PCI 属性, 49
- UTP, 24
- 受信カウンタ, 49
- 接続属性, 46
- 送信カウンタ, 48
- 属性, 46
 - ドライバの統計情報, 43
 - ドライバの動作に関する統計情報, 42

Ethernet の標準的なフレームサイズ, 1

F

failsafe モード, 165

FCode 自己診断, 129

FIFO 使用率, 30

FIPS 140-2 モード, 64

G

Gigabit 強制モードパラメタ, 28

Gigabit メディア独立インタフェース (GMII), 46

H

hostname.vcaN ファイル, 51

hosts ファイル, 52

I

IEEE 802.3x, 27

ifconfig コマンド, 51

infinet-burst, 25

infinet-burst パラメタ, 25

IP アドレスの割り当て, 51

ipg0, 28

ipg0 パラメタ, 28

ipg1, 28

ipg1 パラメタ, 28

ipg2, 28

ipg2 パラメタ, 28

K

kernel/drv/vca.conf ファイル, 128

kstat コマンド, 42, 50, 128

L

libcrypto.a パラメタ, 153

libssl.a パラメタ, 153

link-master, 24
link-master パラメタ, 24

M

MMF, 24
modinfo コマンド, 18

N

ndd ユーティリティー, 32
nostats 属性, 128

O

OBP PROM, 129, 132
OBP 構成変数
 auto-boot?, 129, 131
 diag-switch?, 130
OBP コマンド
 .properties, 132
 reset-all, 129
 setenv auto-boot?, 129
 setenv diag-switch?, 131
 show-devs, 132
 show-nets, 130
 test device_path, 130
 watch-net, 134

OpenBoot PROM, 40, 129, 132
OpenBoot PROM FCode 自己診断, 129
OpenSSL 互換アプリケーション, 153
opt/SUNWconn/crypto/bin/sslpassword, 14
 3
opt/SUNWconn/cryptov2/firmware/sca4000
 fw, 167
opt/SUNWconn/cryptov2/include, 153

P

path_to_inst ファイル, 37
pause-off-threshold, 24

pause-off-threshold パラメタ, 24
PCI アダプタ, 24
pci 名前属性, 23
PCI バスインタフェースパラメタ, 31
PKCS#11 インタフェース, 70
pkgadd コマンド, 18
pkginfo コマンド, 18
prtconf コマンド, 37
prtdiag コマンド, 18

R

RSA 鍵ペア, 113
RX MAC カウンタ, 44
RX 消去レジスタ、別名読み取り用, 30
RX ランダム早期検出 8 ビットベクトル, 30
rx-intr-pkts, 25, 30
rx-intr-pkts パラメタ, 25, 30
rx-intr-time, 30
rx-intr-time パラメタ, 30

S

setenv auto-boot?, 129
show-devs コマンド, 132
show-nets コマンド, 130
Solaris 8 のパッチ, 11
Solaris 9 のパッチ, 11
Solaris オペレーティング環境, 10
speed=
 10, 40
 100, 40
 1000, 40
 auto, 40
SSL アルゴリズム, 3
SSL の高速化, 4
Sun ONE Web サーバー
 Sun ONE Web Server 4.1
 インストール, 90
 構成, 96

- サーバーの証明書の生成, 91
- サーバーの証明書のインストール, 96
- 認証データベースの作成, 91

Sun ONE Web Server 6.0

- インストール, 99
- 構成, 107
- サーバーの証明書の生成, 103
- サーバーの証明書のインストール, 106
- 認証データベースの作成, 100

管理, 83

- キーストアおよびユーザーの作成, 88
- 構成, 87
- 使用するための設定, 89
- トークン, 85
- トークンファイル, 85
- パスワード, 87

Sun ONE Web サーバーを使用するための設定, 89

SunVTS, 120, 121

- netlbttest, 124
- nettest, 126
- vca ドライバ, 120
- vcatest
 - コマンド行構文, 123
 - テストパラメタオプション, 123
- vcatest, 121
- ソフトウェア, 119
- 必須ソフトウェア, 120

SunVTS 4.4, 17

SunVTS 5.1 Patch Set (PS) 2, 119

SunVTS 5.x, 17

T

TX MAC カウンタ, 44

TX および RX MAC カウンタ, 44

U

UNIX pci 名前属性, 23

URL

- OpenSSL, 153

- Sun ONE ソフトウェア, 90, 99

UTP, 24

V

vca ドライバ, 120

- 必須ソフトウェア, 120

vca ドライバパラメタ

- 値および定義, 24

- 強制モード, 24

- 設定, 23

- パラメタおよび設定, 24

vca ドライバパラメタの設定

- ndd を使用, 32, 37

- vca.conf を使用, 32, 37

vca インタフェース, 51

vca.conf ファイル, 37

vca.conf ファイルの例, 39

vcaadm

- キーストアの生成

 - セキュリティー管理者, 68

 - ユーザー, 69

vcaadm

- 新しいファームウェアのインストール, 76

- オプション, 54

- コマンド行構文, 54

- コマンドの入力, 61

- 自動ログアウトの設定, 74

- 終了, 63

- 使用方法, 53

- 診断コマンド, 78

- セキュリティー管理者の一覧表示, 70

- 対話型モード, 56

- 動作モード, 55

- 名前の要件, 67

- パスワードの変更, 70

- パスワードの要件, 67

- バックアップ, 72

- バックアップを防ぐためのキーストアのロック, 73

- ファイルモード, 56

- プロンプト, 59

- ヘルプの表示, 62

- ボード上の情報の消去, 78

- ボードの鍵の交換, 77

- ボードの管理, 74

- ボードの初期化, 63

- ボードのリセット, 76
- 文字の要件, 67
- ユーザーの一覧表示, 70
- ユーザーの削除, 72
- ユーザーの有効および無効の切り替え, 71
- ユーザー名の要件, 67
- ユーティリティー, 53
- ログインおよびログアウト, 56

vcadiag

- オプション, 80
- コマンド行構文, 79
- 使用方法, 79
- ユーティリティー, 79
- 例, 80, 81

W

- watch-net コマンド, 134

Z

- zeroize コマンド, 166

あ

- 値および定義, 24
- アプリケーションの構築
 - libcrypto.a, 153
 - libssl.a, 153
- アルゴリズム, 4
- 暗号化アルゴリズムの高速化, 3
- 暗号化ドライバおよび Ethernet ドライバの動作に関する統計情報, 42
- 暗号化ドライバの統計情報, 42
- 暗号化ドライバの動作に関する統計情報, 42
- 暗号化の処理状況, 128
- 暗号化ライブラリ, 153

い

- インストール
 - ソフトウェアパッケージ, 18
 - ディレクトリおよびファイル, 19
 - ファイルおよびディレクトリ, 17
- インストール、オプションパッケージ, 18
- インタフェース、Gigabit メディア独立, 46
- インタフェース、vca インタフェース, 51
- インタフェース、メディア独立, 46

お

- オプションパッケージ, 17
 - インストール, 18
 - 説明, 17
- オペレーティング環境, 10
- オンラインマニュアルページ, 163
 - apsslcfg(1m), 164
 - iplsslcfg(1m), 164
 - kc12(7d), 163, 164
 - vca(7d), 163
 - vcaadm(1m), 163
 - vcad(1m), 163
 - vcadiag(1m), 163

か

- カーネルの統計値, 128
- 鍵オブジェクト, 67
- 鍵長, 114
- 鍵長の長い鍵, 9
- 確認、暗号化の処理状況, 128
- カスタムアプリケーション, 153
- 間隔パラメタ, 28
- 管理、Sun ONE Web サーバー, 83
- 管理コマンド, 19

き

- キーストア, 64, 65, 84
 - vcaadm による管理, 67

キーストアダプター, 19
強制モードパラメータ, 28

け

現在の Ethernet 接続属性, 46
検出 8 ビットベクトル, 30

こ

高可用性 (HA), 9
構成、Sun ONE Web サーバー, 87
構成、ネットワーク, 50
構築、アプリケーション, 153
高品質のエントロピ, 9
コマンド
 .properties, 132
 driver.conf, 37
 ifconfig, 51
 kstat, 42, 50, 128
 modinfo, 18
 pkgadd, 18
 pkginfo, 18
 prtconf, 37
 prtdiag, 18
 setenv auto-boot?, 129
 show-devs, 132
 show-nets, 130
 watch-net, 134
 zeroize, 166

さ

サーバーの証明書, 94, 103
サポート
 Solaris オペレーティング環境, 10
 SSL アルゴリズム, 4
 アルゴリズム, 4
 暗号化アルゴリズム, 3
 オペレーティング環境, 10
 ソフトウェア, 10
 ハードウェア, 10

プラットフォーム, 10
サポートライブラリ, 19
サンの暗号化ライブラリ, 153

し

自己診断, 129
自動ネゴシエーション, 24, 27
 設定, 24, 36
 送受信, 27
 ポーズ機能, 27
 無効に切り替え, 36
終了、vcaadm, 63
受信 MAC カウンタ, 44
受信カウンタ, 49
受信割り込みブランキング値, 25, 30
出荷時の状態, 165
仕様, 136, 137, 138, 139, 140, 141
 MMF アダプタ, 136, 137, 138
 インタフェース仕様, 138
 環境仕様, 138
 性能仕様, 137
 電源要件, 137
 特性, 136
 UTP アダプタ, 138, 139, 140, 141
 インタフェース仕様, 141
 環境仕様, 141
 コネクタ, 138
 性能仕様, 140
 電源要件, 140
 特性, 139
 物理寸法, 140
障害追跡, 131
消去レジスタ、別名読み取り用, 30
使用するための設定
 Apache Web サーバー, 112
 Sun ONE Web サーバー, 87
情報の消去、ハードウェア, 165
使用率、FIFO, 30
診断テスト, 121
診断のサポート, 3

す

スループロットの最適化, 9

せ

製品の機能, 1

セキュリティー管理者, 68

セキュリティー管理者アカウント, 67

セキュリティー管理者の削除, 72

接続相手, 24, 27, 46, 50

 確認, 50

 設定, 50

接続機能, 27

接続属性, 46

接続パラメタ, 25

そ

早期検出 8 ビットベクトル, 30

早期ドロップパラメタ, 30

送受信、ポーズ機能, 27

送信 MAC カウンタ, 44

送信カウンタ, 48

属性

 Ethernet, 46

 接続, 46

 Ethernet PCI, 49

 nostats, 128

 現在の Ethernet 接続, 46

 接続, 46

ソフトウェアパッケージ, 18

つ

通知される接続パラメタ, 25

て

ディレクトリおよびファイル, 19

 階層, 19

デバイスドライバパラメタの設定, 23

デバイスパス名, 38

と

統計値, 128

動作の強制モード, 24

動作モードパラメタ, 25, 26

動的再構成, 9

トークン, 85

トークンファイル, 85

動作に関する統計情報, 42

ドライバ固有のパラメタ, 48

ドライバの統計情報, 42, 43

ドライバの統計値, 128

ドライバパラメタ, 23

 値および定義, 24

 強制モード, 24

 設定, 23

 パラメタおよび設定, 24

ドロップパラメタ, 30

な

名前属性, 23

名前の要件, 67

に

認証データベース

 作成

 Sun ONE Web Server 4.1, 91

 Sun ONE Web Server 6.0, 100

 vcaadm, 57

ね

ネットワーク構成, 50

ネットワークホストファイル, 50

ネットワークホストファイルの構成, 50

ネットワークホストファイルの編集, 50

は

ハードウェア, 10

ハードウェアおよびソフトウェアの要件, 10

ハードウェア上の情報の消去, 165

パケット間隔パラメタ, 28

パス名, 38

パスワード

Sun ONE Web サーバーに必要なパスワードの一覧, 87

vcaadm, 67, 88

システム管理者, 88

パスワードの要件, 67

バックアップを防ぐためのキーストアのロック, 73

パッケージ

オプション, 17

必須, 17

パッチ, 11

Solaris 8, 11

Solaris 9, 11

必須, 11

パラメタ, 25

8ビットベクトル, 30

adv-asm-pause-cap, 27

adv-autoneg-cap, 24

adv-pause-cap, 27

enable-ipg0, 28

Gigabit 強制モードパラメタ, 28

infinet-burst, 25

ipg0, 28

ipg1, 28

ipg2, 28

libcrypto.a, 153

libssl.a, 153

link-master, 24

pause-off-threshold, 24

PCI バスインタフェース, 31

RX ランダム早期検出 8 ビットベクトル, 30

rx-intr-pkts, 25, 30

rx-intr-time, 30

vca.conf ファイルによる設定, 37, 39

強制モード, 28

すべての vca デバイスに設定, 39

接続, 25

接続機能, 27

早期検出 8 ビットベクトル, 30

早期ドロップ, 30

動作モード, 26

ドライバ固有, 48

パケット間隔, 28

フロー制御, 27

割り込み, 30

パラメタおよび設定, 24

パラメタ値

変更方法および表示方法, 33

ひ

必須パッケージ, 17

必須パッチ, 10

標準規格およびプロトコル, 1

ふ

ファームウェア, 167

ファイルおよびディレクトリ
インストール, 17

負荷均衡, 9

負荷分散, 9

プラットフォーム, 10

ブランキング値, 25, 30

フレームベースのリンクレベルフロー制御プロトコル, 27

フロー制御, 27

キーワード, 27

フレーム, 27

プロトコルおよびインタフェース, 1

へ

並列検出, 41

ベクトル, 30
別名読み取り, 30

ほ

ポーズ機能, 27
ボード状態の表示, 75
ボードの初期化, 20
ホストファイル, 50
ホットプラグ, 9

ま

マニュアルページの説明, 163

め

メディア独立インタフェース (MII), 46

も

モード、FIPS 140-2, 64

ゆ

ユーザーアカウント, 67
ユーザーの PKCS#11 インタフェース定義, 84
ユーザーの概念および用語, 84
ユーティリティー, 19

よ

要求をまとめることによる最適化, 9
読み取り/書き込みが可能なフロー制御, 27
読み取り専用の vca デバイス機能, 46
読み取り専用の接続相手の機能, 47

ら

ライブラリ、暗号化, 153
ランダム早期検出 8 ビットベクトル, 30
ランダム早期検出 8 ビットベクトルの受信, 30
ランダム早期ドロップパラメタ, 30

れ

例、vca.conf ファイル, 39
レジスタ、別名読み取り用, 30

わ

割り込みパラメタ, 30
割り込みブランキング値, 25, 30

