Sun™ Crypto Accelerator 4000 ボードバージョン 1.1 インストールマニュアル

Sun Microsystems, Inc.
www.sun.com

Part No. 817-5925-10
2004 年 1 月, Revision A

コメント送付: http://www.sun.com/hwdocs/feedback

原典: *Sun Crypto Accelerator 4000 Board Version 1.1 Installation and User's Guide*
Part No: 817-3693-10
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
- 台湾経済部標準検験局 (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

表目次

はじめに

このマニュアルでは、Sun Crypto Accelerator 4000 ボードの機能、プロトコル、およびインタフェースについて説明します。また、使用しているシステムでのボードの取り付け、構成、および管理方法について説明します。

このマニュアルは、Solaris™ オペレーティング環境、PCI I/O 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。

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、プロトコル、および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 診断コード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。
- 第 8 章では、PKCS#11 インタフェースを使用した、さまざまな構成のボードの操作について説明します。
- 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、インストールスクリプトを使用せずに、Sun Crypto Accelerator 4000 ソフトウェアを手動でインストールする方法について説明します。
- 付録 C 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 D 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 E では、サン以外のベンダーによる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 F 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 G 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。

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

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)	#

書体と記号について

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

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、印刷、または購入できます。

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

Sun の技術サポート

このマニュアルに記載されていない技術的な問い合わせについては、次の URL にアクセスしてください。

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

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。コメントは下記よりお送りください。

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

コメントにはマニュアルの Part No. (817-5925-10) とタイトルを記載してください。

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。

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。

取り付けたボードは、`vcaadm` ユーティリティーを使用して初期化および構成します。`vcaadm` ユーティリティーは、キーストアおよびユーザーの情報を管理し、ボードが動作するセキュリティーレベルを決定します。キーストアおよびセキュリティー管理者のアカウントを設定すると、`iplsslcfg` および `apsslcfg` スクリプトを使用して、Sun ONE Web サーバーおよびアプリケーションサーバー、または Apache Web サーバーを、このボードを使用して SSL を高速化するように構成できます。Sun ONE 管理コンソールと、`modutil` および `certutil` ユーティリティーを使用して、Sun ONE ディレクトリサーバー、メッセージングサーバー、およびポータルサーバーを、このボードを使用して SSL を高速化するように構成することもできます。また、キーストアおよび暗号化サービスに PKCS#11 インタフェースを必要とするアプリケーションの多くは、このボードと互換性があります。

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 33/66 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 Server 4.1 および 6.0

- Sun ONE Application Server 7.0
- Sun ONE Directory Server 5.2
- Sun ONE Messaging Server 5.2
- Sun ONE Portal Server 6.2
- Apache Web Server 1.3.x および 2.x

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 (Transmission Layer Security)

このボードは、次の IPsec 機能を高速化します。

- ESP (DES、3DES) 暗号化
- ESP (SHA1、MD5) 認証 *
- AH (SHA1、MD5) 認証 *

* IPsec のインライン高速化が構成されている場合 (5 ページの「ハードウェアによる IPsec のインライン高速化」を参照)

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

このボードは、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、現在のジョブの負荷、およびデータサイズに基づいて行われます。

このボードは、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
ハッシュ*	MD5、SHA1

* ハードウェアによる IPsec のインライン高速化が構成されている場合

このボードは、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

IPsec 高速化

ボードがサポートする IPsec 高速化には、2 つの形式 (帯域外およびインライン) があります。どちらの構成も、負荷の高い暗号化演算を SPARC® プロセッサからボードにオフロードします。詳細は、56 ページの「ハードウェアによる IPsec の高速化の構成」を参照してください。

表 1-3 IPsec アルゴリズムの高速化

アルゴリズム	帯域外	インライン
DES	X	X
3DES	X	X
MD5		X
SHA1		X

ハードウェアによる IPsec の帯域外高速化

ボードに IPsec の帯域外高速化を構成すると、Solaris 9 以降のシステムに取り付けたハードウェアによって、サポートされる暗号化および複号化処理が高速化されます。IPsec に固有のパケット処理はすべて、ホストの Solaris IPsec ソフトウェアによって行われます。詳細は、57 ページの「IPsec の帯域外高速化を使用可能にする方法」を参照してください。

注 – Solaris 9 で IPsec の帯域外高速化を行うボードを使用する場合、IPsec を構成または調整する必要はありません。Sun Crypto Accelerator 4000 パッケージのインストールおよび再起動のみを実行します。

ハードウェアによる IPsec のインライン高速化

IPsec のインライン高速化を構成すると、Solaris 9 12/03 以降のシステムに取り付けたハードウェアによって、サポートされる暗号化、複号化、および認証処理が高速化されます。IPsec に固有のパケット処理の一部は、ボードによって直接実行されます。IPsec のインライン高速化を行うようにボードを構成する手順については、57 ページの「IPsec のインライン高速化を使用可能にする方法」を参照してください。

SSL 高速化

表 1-4 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 1-4 サポートする SSL アルゴリズム

	Sun ONE Web サーバー		Apache Web サーバー	
アルゴリズム	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		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。

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。

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。

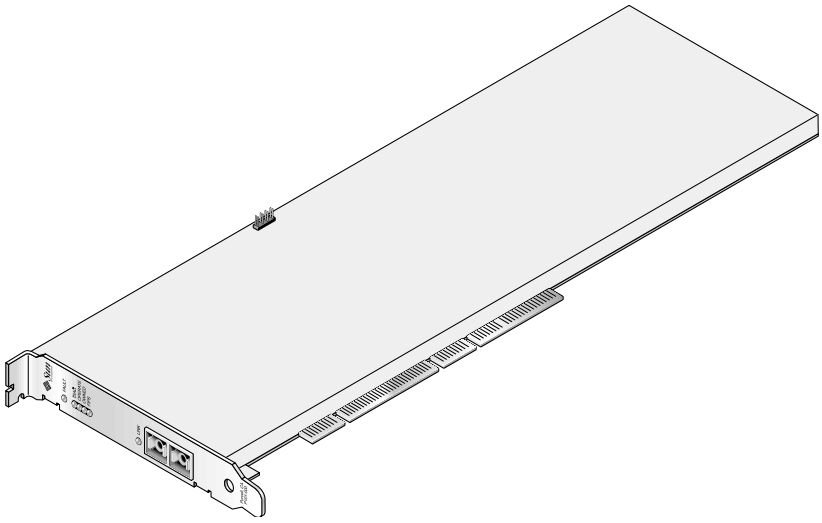

図 1-1　Sun Crypto Accelerator 4000 MMF アダプタ

LED 表示

表 1-5　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、DIAGNOSTICS、および 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、DIAGNOSTICS、および DISABLED (ドライバが組み込まれていない) 状態で点灯。 IDLE、OPERATIONAL、および FAILSAFE 状態で点滅。	緑
INIT	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、68 ページの「`vcaadm` によるボードの初期化」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	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、100、または 1000 Mbps の Ethernet ネットワークで動作するように設定できます。

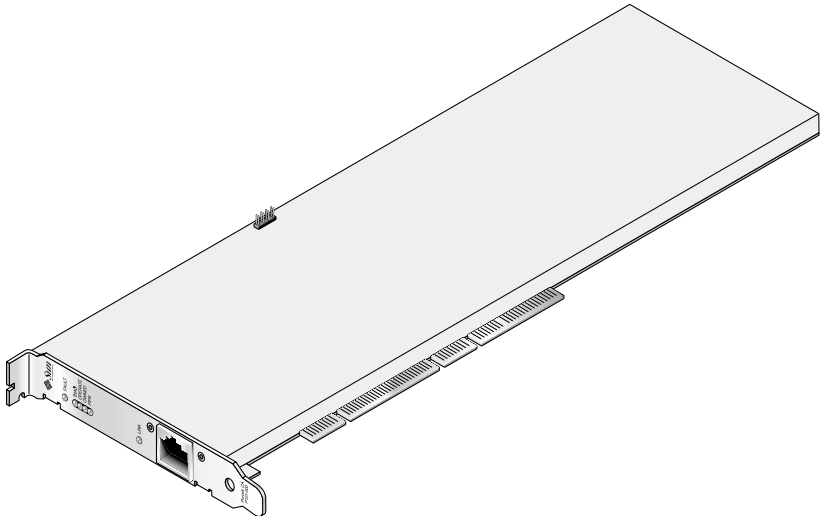

図 1-2　Sun Crypto Accelerator 4000 UTP アダプタ

LED 表示

表 1-6　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、DIAGNOSTICS、および 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、DIAGNOSTICS、および DISABLED (ドライバが組み込まれていない) 状態で点灯。 IDLE、OPERATIONAL、および FAILSAFE 状態で点滅。	緑
INIT	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、68 ページの「`vcaadm` によるボードの初期化」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	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。まれに 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 ソフトウェアは、ハードウェア資源の減少に合わせて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 1-7 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 1-7 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 ボードバージョン 1.1 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には、後述のパッチが必要です。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 SunSolve℠ の Web サイト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

Solaris 8 で Apache Web サーバーを使用する場合は、パッチ 109234-09 をインストールしてから Sun Crypto Accelerator 4000 ソフトウェアを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 Apache Web サーバー mod_ssl 1.3.26 が構成されます。

Solaris 8 のパッチ

表 1-8 に、Sun Crypto Accelerator 4000 ソフトウェアの Solaris 8 必須パッチを示します。

表 1-8 Solaris 8 必須パッチ

パッチ ID	説明
110383-01	`libnvpair`
108528-23	`KU-05` (`nvpair` サポート)
112438-01	`/dev/random`
110900-10	`pcifg`、Sun Fire 15K サポート、および DR
110824-04	DR

表 1-8　Solaris 8 必須パッチ (続き)

パッチ ID	説明
110842-11	バスの速度および DR
110839-04	マイナーノードおよび DLPI プロバイダの名前
109234-09	Apache サポート

Solaris 9 のパッチ

表 1-9 に、Sun Crypto Accelerator 4000 ソフトウェアの Solaris 9 必須パッチを示します。

表 1-9　Solaris 9 必須パッチ

パッチ ID	説明
113068-04	バスの速度、Sun Fire 15K サポート、および DR
112838-08	`pcifg`、DR、および Sun Fire 15K サポート
113218-08	Gigabit 性能および `vca` メモリーリーク
112904-08	Gigabit 性能
114758-01	マイナーノードおよび DLPI プロバイダの名前
112233-08	(Solaris 9 9/04 より前のバージョンの Solaris にのみ必要)

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と、自動スクリプトを使用した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。この章は、次の節で構成されます。

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、構成およびキーストア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、68 ページの「vcaadm によるボードの初期化」を参照してください。

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 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@8,600000/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         00 03 ba 0e 99 ca
version                   Sun PCI Crypto Accelerator 4000 1000Base-T FCode
FCode 2.11.13 03/03/04
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
max-latency               00000040
cache-line-size           00000010
max-latency               00000040
min-grant                 00000040
subsystem-vendor-id       0000108e
subsystem-id              00003de8
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、12 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には、2 通りの方法 (手動または `install` スクリプト) があります。この節では、`install` スクリプトを使用してソフトウェアをインストールする方法について説明します。ソフトウェアを手動でインストールする方法については、付録 B 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)	
install	Sun Crypto Accelerator 4000 ソフトウェアをインストールするスクリプト	
remove	Sun Crypto Accelerator 4000 ソフトウェアを削除するスクリプト	
Docs	『Sun Crypto Accelerator 4000 ボードバージョン 1.1 インストールマニュアル』(このマニュアル) 『Sun Crypto Accelerator 4000 ボードバージョン 1.1 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。	
	SUNWkcl2r	暗号化カーネルコンポーネント
	SUNWkcl2u	暗号化管理ユーティリティーおよびライブラリ
	SUNWkcl2a	Apache の SSL サポート (オプション)
	SUNWkcl2m	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
	SUNWvcafw	VCA ファームウェア
	SUNWvcamn	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)
	SUNWkcl2o	SSL 開発ツールおよびライブラリ (オプション)
	SUNWkcl2i.u	KCLv2 Crypto を使用する IPsec の高速化 (オプション)

このインストールスクリプトは、特定の順序で必須パッケージをインストールします。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 を使用する場合にかぎり、オプションの SUNWkcl2a パッケージをインストールします。

Apache Web サーバーのほかのバージョンと再接続する場合にかぎり、オプションの SUNWkcl2o 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かぎり、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 SUNWkcl2i.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 SUNWkcl2i 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、必須ソフトウェアをインストールします。

```
# cd /cdrom/cdrom0
# ./install
```

install スクリプトは、システムを分析してインストールする必要のある必須パッチを特定し、そのパッチと主要なソフトウェアをインストールし、任意でオプションのソフトウェアをインストールします。次に例を示します。

注 – 次の例では、著作権およびライセンス情報の表示を省略しています。著作権およびソフトウェアライセンスの詳細は、付録 E を参照してください。

```
# ./install
This program installs the software for the Sun Crypto Accelerator
4000, Version 1.1.

*** Checking if Sun Crypto Accelerator support is already installed...
*** Checking for required OS patch(es):
 113146-01 112838-07 113068-04 113449-02 113453-04 114758-01
*** Checking for incompatible OS patch(es) ...
*** Checking for optional package dependencies...

Do you wish to install the optional Crypto IPsec Acceleration software
(SUNWkcl2i.u)?  [y,n,?,q]

Do you wish to install the optional Crypto Apache Support (SSL) (SUNWkcl2a
SUNWkcl2o)?  [y,n,?,q] y

Do you wish to install the optional Crypto QA Tools (SUNWkcl2q SUNWvcaq)?
[y,n,?,q] n

Do you wish to install the optional VCA Crypto Accelerator/Gigabit Ethernet
SunVTS Diagnostics (SUNWvcav)?  [y,n,?,q] n

This script is about to take the following actions:
- Install Sun Crypto Accelerator 4000 support for Solaris 9
- Install Optional Crypto IPsec Acceleration software
- Install Optional Crypto Apache Support (SSL) software
```

```
To cancel installation of this software, press 'q' followed by a Return.
 **OR**
Press Return key to begin installation:

*** Installing Sun Crypto Accelerator 4000 software for Solaris 9...
Installing required packages:
 SUNWkcl2r SUNWkcl2u SUNWkcl2m SUNWvcar SUNWvcau SUNWvcaa SUNWvcamn SUNWvcafw

Installation of <SUNWkcl2u> was successful.
Installation of <SUNWkcl2m> was successful.
Installation of <SUNWvcar> was successful.
Installation of <SUNWvcau> was successful.
Installation of <SUNWvcaa> was successful.
Installation of <SUNWvcamn> was successful.
Installation of <SUNWvcafw> was successful.
*** Installing selected optional software for Solaris 9...
Installing optional package(s):
 SUNWkcl2i.u SUNWkcl2a SUNWkcl2o
Installation of <SUNWkcl2i> was successful.

Checking operating environment requirements...
Determining package requirements...
Verifying required packages are installed...
All required packages installed.
Determining patch requirements...
Verifying required patches are installed...
Requirement for 113146-01 met by 113146-01.
All required patches installed.

Installation of <SUNWkcl2a> was successful.

Installation of <SUNWkcl2o> was successful.
*** Installation complete.
```

インストールするオプションパッケージの選択

Apache Web サーバーの SSL サポートと、Sun Crypto Accelerator 4000 のオンライン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、`SUNWkcl2a` および `SUNWkcl2m` を選択します。

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、`SUNWkcl2a`、`SUNWkcl2m`、`SUNWvcamn`、`SUNWvcav`、`SUNWkcl2o`、および `SUNWkcl2i.u` を選択します。

これら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`	ユーティリティー
`/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。

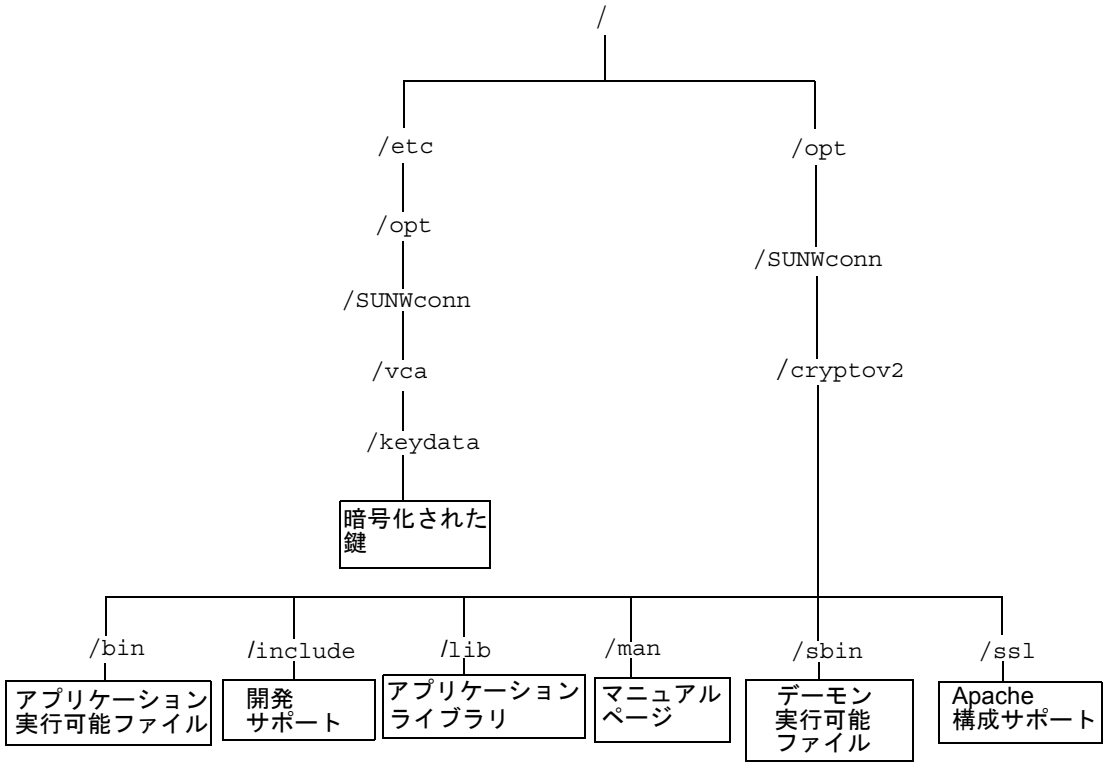

図 2-1 Sun Crypto Accelerator 4000 ディレクトリおよびファイル

注 – Sun Crypto Accelerator 4000 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、構成およびキーストア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、68 ページの「`vcaadm` によるボードの初期化」を参照してください。

Sun Crypto Accelerator 4000 ソフトウェアの削除

ソフトウェアを削除するには、3 通りの方法 (CD-ROM の `remove` スクリプト、サーバーの `/var/tmp/crypto_acc.remove` スクリプト、または `pkgrm` コマンド) があります。この節では、2 つの削除スクリプトを使用したソフトウェアの削除方法について説明します。`pkgrm` コマンドを使用したソフトウェアの削除方法については、付録 B を参照してください。

`install` スクリプトを使用してソフトウェアをインストールした場合は、`remove` スクリプトを使用してソフトウェアを削除します。手動でソフトウェアをインストールした場合 (付録 B) は、`/var/tmp/crypto_acc.remove` スクリプトを使用します。

▼ `remove` スクリプトを使用してソフトウェアを削除する

- Sun Crypto Accelerator 4000 CD-ROM を挿入して、次のように入力します。

```
# cd /cdrom/cdrom0
# ./remove
```

▼ `/var/tmp/crypto_acc.remove` スクリプトを使用してソフトウェアを削除する

この場合のインストールのログは、次のように存在します。

```
/var/tmp/crypto_acc.install.2003.10.13
```

- 次のように入力します。

```
# /var/tmp/crypto_acc.remove
```

第3章

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。

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、42 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」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、duplex、および 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 – 正常な接続を確立するには、speed、duplex、および 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、42 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、状態、および説明

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

表 3-1　vca ドライバのパラメタ、状態、および説明 (続き)

パラメタ	状態	説明
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
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
infinit-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	UTP アダプタ	MMF アダプタ
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)	X	X
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)		X
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)	X	X
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)	X	
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)	X	
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)	X	
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)	X	

表 3-2 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 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-asmpause-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-asmpause-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-asmpause-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。
	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、enable-ipg0 というプログラム可能な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 1	enable-ipg0 は有効 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 バイトより大きく 6,144 バイトより小さい場合の、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、8 パケットのうち最初のパケットがこの範囲でドロップされます (デフォルト = 0)。
`red-dv6to8k`	0 ～ 255	FIFO しきい値が 6,144 バイトより大きく 8,192 バイトより小さい場合の、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、8 パケットのうち最初のパケットがこの範囲でドロップされます (デフォルト = 0)。
`red-dv8to10k`	0 ～ 255	FIFO しきい値が 8,192 バイトより大きく 10,240 バイトより小さい場合の、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、8 パケットのうち最初のパケットがこの範囲でドロップされます (デフォルト = 0)。
`red-dv10to12k`	0 ～ 255	FIFO しきい値が 10,240 バイトより大きく 12,288 バイトより小さい場合の、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、8 パケットのうち最初のパケットがこの範囲でドロップされます (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。その他の値は、2 のべき乗として、負荷の大きいトラフィックに適用されます。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かぎり、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 ユーティリティーを使用
- vca.conf ファイルを使用

ndd ユーティリティー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、39 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 ユーティリティーを使用したパラメタの設定

ndd ユーティリティーを使用して、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 ユーティリティーを使用して、-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 ユーティリティーのデバイスインスタンスを指定する

ndd ユーティリティーを使用して 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ー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 ユーティリティーは、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、ユーティリティー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、ユーティリティーは終了します。対話型モードでは、ユーティリティーを使用して、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 ユーティリティーの使用

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 ユーティリティーを起動すると、ユーティリティーは *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
```

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。

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*N* 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? (パラメタ名を入力します。?を入力すると、すべてのパラメタを参照できます。)
```

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。

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*N* **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/vcaN
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-asmpause-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 ?
#
```

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。

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、その接続パラメタは強制モードになります。強制モードでは、speed パラメタ値を接続相手と一致させる必要があります。詳細は、42 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。

▼ 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、duplex、または link-clock パラメ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-asmpause-cap
   - adv-pause-cap

   これらのパラメ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 パラメタに 0 を設定します。**

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

ndd 接続パラメタを変更すると、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、duplex、および link-clock (1000 Mbps のみ) パラメ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、42 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。

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、26 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、親デバイス、および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、インスタンス番号、および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、デバイスノード名、および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
"/pci@8,600000/network@1"	/pci@8,600000	network	1
"/pci@8,700000/network@1"	/pci@8,700000	network	1

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、ノード名およびユニットアドレス) 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、vca 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、ノード名、およびユニットアドレス) を省略すると、すべての Sun Crypto Accelerator 4000 Ethernet デバイスの全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 2003 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
#ident  "@(#)vca.conf   1.3     03/10/13 SMI"

#
# Use the new Solaris 9 ddi-no-autodetach property to prevent the
# driver from being unloaded by the cleanup modunload -i 0.
#
ddi-no-autodetach=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 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、1000、100、または 10 を設定できます。構文は次のとおりです。 • speed=auto (デフォルト) • speed=1000 • speed=100 • speed=10
duplex	このパラメタには、auto、full、または half を設定できます。構文は次のとおりです。 • 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、slave、または auto を設定できます。構文は次のとおりです。 • link-clock=auto (デフォルト) • link-clock=master • link-clock=slave

正常な接続を確立するため、speed、duplex、および 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、duplex、および 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。OpenBoot PROM の ok 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 Mpbs 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、OpenBoot PROM の ok 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。

1000 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、OpenBoot PROM の ok 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、OpenBoot PROM の ok 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、OpenBoot PROM の ok 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。

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

パラメタ	説明	Stable/Unstable
vs-mode	FIPS、standard、または 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、faulted、または 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ーがないために、有効な着信パケットが破棄された回数 (long)	Stable
noxmtbuf	送信バッファーがビジー状態か、または送信パケットに割り当てるバッファーがないために、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、ネットワーク上の 1 つ以上のステーションが、ネットワークの最大許容時間に違反してい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 ビットの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ます。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	受信バッファー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　現在の Ethernet 接続属性

パラメタ	説明	Stable/Unstable
ifspeed	1000、100、または 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、29 ページの「フロー制御パラメタ」を参照してください。	Stable
link-asmpause	接続の現在のポーズ設定。詳細は、29 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
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

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-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 (29 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 (29 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 (29 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 (29 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-wsrv	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	メモリー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 パリティーエラーの検出数	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
```

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。

ハードウェアによる IPsec のインライン高速化の統計情報

表 3-19 に、ボードにハードウェアによる IPsec のインライン高速化を構成すると加算されるようになる、カーネルの統計情報を示します。IPsec のインライン構成を使用するようにボードを構成する手順については、57 ページの「IPsec のインライン高速化を使用可能にする方法」を参照してください。

表 3-19 IPsec のインライン高速化に関する暗号化ドライバの統計情報

パラメタ	説明	Stable/Unstable
ipsec_ierrrors	エラーが含まれるために処理できない IPsec の受信パケットの総数 (long)	Stable
ipsec_ipackets	IPsec の着信パケット数	Stable
ipsec_ipackets64	IPsec の着信パケット数 (64 ビット)	Stable
ipsec_obytes	インタフェースで送信が要求された IPsec のバイトの総数	Stable
ipsec_obytes64	インタフェースで送信が要求された IPsec のバイトの総数 (64 ビット)	Stable
ipsec_oerrors	エラーが原因で送信に失敗した IPsec パケットの総数 (long)	Stable
ipsec_opackets	インタフェースで送信が要求された IPsec パケットの総数	Stable
ipsec_opackets64	インタフェースで送信が要求された IPsec パケットの総数 (64 ビット)	Stable
ipsec_rbytes	インタフェースが正常に受信した IPsec のバイトの総数	Stable
ipsec_rbytes64	インタフェースが正常に受信した IPsec のバイトの総数 (64 ビット)	Stable
sadb_cache_misses	ファームウェアのキャッシュミス数	Stable
sadb_cache_overflows	ファームウェアのキャッシュのオーバーフロー数	Stable
sadb_entries	SADB ドライバのエントリ数	Stable
sadb_operations	Solaris IPsec からドライバへ送信される SADB 操作数	Stable

注 – 表 3-19 に示す IPsec のカーネル統計情報は、ハードウェアによって実際にインライン処理される IPsec パケットに対してのみ加算されます。256 バイト未満の受信パケットはインライン処理されないため、これらのパケットに対しては、IPsec のカーネル統計情報は加算されません。また、このカーネル統計情報は、IPsec の帯域外トラフィックにも適用されません (56 ページの「ハードウェアによる IPsec の高速化の構成」を参照)。`snoop` が使用可能になっている場合は、これらのカウンタは加算されません。帯域外パケットは、ネットワークに関する通常のカーネル統計情報と、該当する暗号化の統計情報 (`3desbytes` および `3desjobs`) に加算されます。

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.vca`*N* ファイルを作成する必要があります。ファイル名 `hostname.vca`*N* 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
```

   詳細は、ifconfig(1M) の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*.vca*N* 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*.vca*N* ファイルを作成して、ファイル名の *N* にデバイスのインスタンス番号 (この例では 0) 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*.vca*N* ファイルを作成しないでください。
   - /etc/*hostname*.vca*N* 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*.vca*N* 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
```

ハードウェアによる IPsec の高速化の構成

このボードには、ハードウェアによって IPsec を高速化するための 2 通りの構成 (インラインおよび帯域外) があります。どちらの構成も、IPsec の暗号操作を高速化します。ただし、それぞれの方法の利点は異なるため、システム全体の要件を考慮して適切な構成を決定する必要があります。

注 – IPsec の高速化は、Solaris 9 以降でサポートされます。Solaris 8 ではサポートされません。IPsec のインライン高速化は、Solaris 9 12/03 以降でのみサポートされます (表 3-20 を参照)。

表 3-20 IPsec の高速化に関する Solaris バージョンの要件

Solaris のバージョン	帯域外高速化	インライン高速化
Solaris 8 の全バージョン	サポートされない	サポートされない
Solaris 9 ～ Solaris 9 8/03	サポートされる	サポートされない
Solaris 9 12/03 以降	サポートされる	サポートされる

帯域外は、デフォルトの IPsec 構成で、マルチプロセッサシステムで最適な性能を実現します。この構成は、DES および 3DES 暗号化機能をボードにオフロードするもので、ホストの処理能力に問題のないマルチプロセッサシステムに推奨される構成です。

インラインの IPsec 構成は、認証サポート (MD5 および SHA1) によって帯域外の機能を補強するもので、ホストのパケット処理の一部をボードにオフロードします。追加のパケット処理に対処することによって、ボードはホスト CPU の使用率を大幅に削減します。

注 – DES または 3DES 暗号化アルゴリズムのみを必要とするマルチプロセッサシステムでは、帯域外の IPsec スループットの方がインラインより優れています。

IPsec の帯域外高速化を使用可能にする方法

Solaris 9 以降が必要です。帯域外は、ボードのデフォルトの構成です。Solaris 9 でこのボードを使用して IPsec の帯域外高速化を実現する場合、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。

IPsec のインライン高速化を使用可能にする方法

Solaris 9 12/03 以降が必要です。インライン高速化を構成するには、Solaris ソフトウェアと `vca` ドライバの両方の構成ファイルを変更する必要があります。

▼ ハードウェアによる IPsec のインライン高速化を使用可能にする

1. **`/etc/system` 構成ファイルに次のエントリを追加して、Solaris ソフトウェアのインライン高速化を使用可能にします。**

```
set ip:ip_use_dl_cap=1
```

`/etc/system` ファイルの変更を有効にするには、システムを再起動する必要があります。

2. **`/kernel/drv/vca.conf` 構成ファイルに次のエントリを追加して、`vca` ドライバのインライン高速化を使用可能にします。**

```
inline-ipsec=1;
```

`/kernel/drv/vca.conf` ファイルの変更を有効にするには、システムを再起動するか、`vca` ドライバを読み込み解除して、再読み込みする必要があります。

注 – Solaris ソフトウェアでインライン高速化が使用可能になっていない場合には、ドライバでインライン高速化を使用可能にしないでください。これを行うと、IPsec 以外の性能が低下する可能性があります。

インライン高速化を使用可能にしたあとは、通常の IPsec 構成手順によって、インタフェースに Solaris ソフトウェアの IPsec ポリシーを構成できます。Solaris の IPsec ポリシーの構成については、『IPsec と IKE の管理』を参照してください。このマニュアルは、`http://docs.sun.com` から入手できます。

インライン高速化を使用すると、AH および ESP の両方のアルゴリズムを高速化できます。ただし、複数の入れ子になった変換 (AH+ESP など) は、このボードでは実行できません。複数の変換が適用されていると、もっとも外側の変換のみがインラインで実行されます。その他の変換は、Solaris の IPsec 構成で実行されます。Solaris 9 システムに KCL IPsec 高速化パッケージ (`SUNWkcl2i.u`) がインストールされている場合は、これらの変換がハードウェア (帯域外) でも実行されます。

ボードに IPsec のインライン高速化を構成すると、`kstat`(1M) コマンドの表示に統計情報が追加されて、加算されるようになります。IPsec のインライン高速化の `kstat` 統計情報については、表 3-19 を参照してください。

第4章

Sun Crypto Accelerator 4000 ボードの管理

この章では、vcaadm、vcad、vcadiag、または pk11export 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。

vcaadm ユーティリティーの使用

vcaadm ユーティリティーは、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。vcaadm ユーティリティーを使用できるのは、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 ユーティリティー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 *hostname*] [-p *port*] [-d vca*N*] [-f *filename*]
- vcaadm [-y] [-h *hostname*] [-p *port*] [-d vca*N*] [-s *sec-officer*] *command*

注 – -d 属性を使用する場合の vca*N* 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 ユーティリティー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 vca*N*	*N* 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 vca1 を指定すると、デバイス vca1 に接続します。vca はこのボードのデバイス名を示す文字列で、1 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 vca0 です。必ず vca*N* の書式で、*N* にはデバイスインスタンス番号を指定してください。
-f *filename*	*filename* 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 *hostname*	*hostname* 上の Sun Crypto Accelerator 4000 ボードに接続します。*hostname* 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 *port*	*port* 上の Sun Crypto Accelerator 4000 ボードに接続します。*port* の値は、デフォルトでは 6870 になっています。
-s *sec-officer*	*sec-officer* という名前のセキュリティー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 yes と応答します。

注 – このマニュアルでは、セキュリティー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、ファイルモード、および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、指定したキースト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、キーストア内に *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、62 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、-p、および -d の各属性によってホスト、ポート、および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 ユーティリティーは、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
vca*N*	vca は、Sun Crypto Accelerator 4000 ボードを示す文字列です。*N* は、デバイスインスタンス番号 (ユニットアドレス) で、ボードのデバイスパ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、39 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。
hostname	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。*hostname* 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。
sec-officer	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、ホスト名、またはセキュリティー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タ

パラメタ	意味
dev vca*N*	ドライバインスタンス番号 *N* の Sun Crypto Accelerator 4000 ボードに接続します。たとえば、-d vca1 と入力すると、デバイス vca1 に接続します。デフォルトでは、vca0 デバイスになっています。
host *hostname*	*hostname* 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。*hostname* 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。
port *port*	*port* 上の Sun Crypto Accelerator 4000 ボードに接続します。デフォルトでは 6870 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 ユーティリティーには、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 (一意にほかのコマンドと識別できるだけの文字数) を使用して入力します。show の代わりに sh は使用できますが、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 ユーティリティーの終了

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、106 ページの「概念および用語」を参照してください。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ためのプロンプトを表示します。

▼ 新しいキーストアでボードを初期化する

1. 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
Please select an action:

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

Your Choice --> 2
This board is uninitialized.
You will now initialize the board. You may either
completely initialize the board and start with a new
keystore or initialize the board to use an existing
keystore, providing a backup file in the process.

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

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

2. キーストア名を作成します (72 ページの「名前の要件」を参照)。

```
Keystore Name: keystore-name
```

3. 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、ボードは FIPS 140-2 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
```

4. 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 (72 ページの「名前の要件」を参照)。

```
Initial Security Officer Name: sec-officer
Initial Security Officer Password:
Confirm Password:
```

注 – 重要なパラメ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、Yes、N、または 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... This may take a few
minutes...Done.
```

既存のキーストアを使用したボードの初期化

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、77 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。

名前の要件

セキュリティー管理者名、ユーザー名、およびキーストア名は、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、ユーザー名、および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、下線 (_)、ダッシュ (-)、およびドット (.)
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`、`med`、または `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` が入力を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、次の表に示す 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 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、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`、`med`、または `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もあります。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 (詳細は、72 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、Web サーバープロセスの 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 (詳細は、72 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 – 鍵にアクセスするには、パスワードを覚えておく必要があります。パスワードを忘れた場合に、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、79 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` を使用して変更できるのは、セキュリティー管理者のパスワードだけです。セキュリティー管理者は、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。ユーザーアカウントを無効にするには、disable user コマンドを実行します。

```
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.
```

アカウントを有効にするには、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、82 ページの「ボードのソフトウェア情報の消去」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

ここでは、`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

セキュリティー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ー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、1,440 分 (1 日) です。初期化した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、セキュリティー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、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のいずれか、速度、デュプレックスモードなど)、および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) ユーティリティーを使用して、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、44 ページの「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
```

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生じる場合があります。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 にふたたびログインして、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.
```

ボードの鍵の交換

セキュリティーポリシーが変更されると、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生じる場合があります。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。鍵を交換したら、マスター鍵のバックアップを作成してください。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.
```

ボードのソフトウェア情報の消去

ボードからすべての鍵素材を消去するには、2 つの方法があります。1 つ目は、ハードウェアジャンパ (シャント) を使用する方法です。この方法で情報を消去すると、ボードは出荷時の状態 (Failsafe モード) に戻ります。詳細は、259 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 コマンドは鍵素材を削除しますが、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、セキュリティー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ソフトウェア情報を消去するには、次のように入力して確認します。

```
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、vcaadm ユーティリティーおよび SunVTS ソフトウェアから実行できます。vcaadm の diagnostics コマンドは、Sun Crypto Accelerator 4000 ハードウェアの 3 つの主要なカテゴリ (一般的なハードウェア、暗号化サブシステム、およびネットワークサブシステム) 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、フラッシュメモリー、PCI バス、DMA コントローラ、および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
-----------------------------------------------------
```

vcad コマンドの使用

vcad コマンドは、vcad デーモンを構成して起動します。このデーモンは、vcaadm(1M) およびその他の暗号化アプリケーションに対して、暗号のキーストアサービスを提供します。また、vcad デーモンは、ドライバおよびハードウェアのキーストアデータの読み取りおよび書き込みも行います。

vcad コマンド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/cryptov2/sbin/
$ export PATH
```

次に、vcad コマンドのコマンド行構文を示します。

/opt/SUNWconn/cryptov2/sbin/vcad [-dFlV] [-f *config-file*]
[-h *host-address*] [-k *keystore-dir*] [-L *logfile*] [-p *port*] [-s *max-size*]
[-t *seconds*] [-u *username*]

表 4-7 に、vcad コマンドがサポートするオプションを示します。

表 4-7 vcad コマンドオプション

オプション	説明
-d	デバッグをオンに設定します。各メッセージには、実際のメッセージのほかに、vcad のプロセス ID、現在のスレッド ID、およびメッセージのカテゴリが含まれます。複数の -d オプションを指定すると、より詳細になります (2 つまで指定可)。複数の -d オプションを使用する場合、-d は構成ファイルの DebugLevel パラメタに INFO を設定するのと同じ意味になり、-dd は DEBUG を設定するのと同じ意味になります。
-f *config-file*	構成ファイルの位置を指定します。構成ファイルのデフォルトの位置は /etc/opt/SUNWconn/vca/vcad.conf です。このオプションを使用しているときに構成ファイルを開くことができないと、vcad は起動しません。
-F	フォアグラウンドで vcad を実行して、ログの出力を stderr に送信します。このオプションの動作は、-L フラグで選択した *logfile* より優先されます。
-h *host-address*	着信接続用に vcad がバインドおよび待機する IPv4 または IPv6 のホストアドレスを指定します。-h オプションを追加することによって、複数のホストまたは IP アドレスを指定できます。このオプションを使用しない場合は、デフォルトの動作として、vcad は着信接続用に使用できるすべてのインタフェースで待機します。特定のホストまたは IP アドレスにバインドするように指定すると、そのアドレスおよび localhost に応答するインタフェースでのみ接続が確立されます。-h フラグで指定したアドレスまたはホストより、-l オプションの方が優先されます。
-k *keystore-dir*	すべてのキーストアデータのディレクトリとして、*keystore-dir* を使用します。デーモンがスーパーユーザー以外のユーザーとして動作している場合、キーストアデータファイル自体だけでなく、このディレクトリも、そのユーザーから読み取りおよび書き込み可能である必要があります。キーストアデータのデフォルトのディレクトリは /etc/opt/SUNWconn/vca/keydata です。
-l	ローカルホストから送信される管理クライアントからの着信接続のみを受け入れます。このオプションは、デーモンにほかのインタフェースの待機を指示するコマンド行または .conf ファイルディレクティブより優先されます。
-L *logfile*	標準的なシステムログの出力先ではなく、*logfile* で指定した位置にログを送信します。
-p *port*	着信接続用に *port* に指定したポートを使用してバインドします。デフォルトで使用されるポートは 6870 です。

表 4-7　vcad コマンドオプション (続き)

オプション	説明
`-s` *max-size*	コマンドで *max-size* バイトまでの大きさのデータを Sun Crypto Accelerator に送信することを許可します。管理者は、この機能を使用して、1 回のコマンドで大容量のデータが送信されるのを防ぐことができます。1 回のコマンドのデフォルトの最大サイズは、4M バイト (4194304 バイト) です。
`-t` *seconds*	vcad がクライアントからのデータを待機する時間を、*seconds* に秒単位で設定します。ここで指定した時間が過ぎると、vcad とクライアント間の接続が切断されます。
`-u` *username*	*username* に指定したユーザー名で vcad を実行します。ユーザー名が指定されていない場合は、vcad を起動したユーザーで vcad を実行することを試みます。指定したユーザー名がシステム上に見つからない場合、vcad は実行されません。vcad がスーパーユーザー、またはユーザー ID が 0 のほかのアカウントで動作している場合、vcad は警告を出します。スーパーユーザー以外のユーザーで vcad を実行する際の推奨事項については、87 ページの「vcad デーモンのセキュリティー」を参照してください。
`-V`	vcad のバージョン情報を表示します。

vcad 構成ファイル

vcad デーモンは、動作パラメタを構成ファイルから取得します。デフォルトでは、デーモンは構成ファイル `/etc/opt/SUNWconn/vca/vcad.conf` を探します。ただし、vcad デーモンの起動時に vcad コマンドの `-f` フラグで別のファイルを指定することもできます。`-f` フラグが指定されておらず、またデフォルトの構成ファイルが存在しないか読み取れない場合には、vcad デーモンはすべてのパラメタをデフォルト値として起動を試みます。この場合、警告メッセージが標準エラー出力に送信されます。

構成ファイルには、1 行に 1 つのディレクティブを指定します。各ディレクティブには、関連する値が必要です。コメントを使用することもできます。コメントは、「#」文字で開始する必要があります。ディレクティブ名では、大文字と小文字は区別されません。ただし、ディレクティブの値は、大文字と小文字が区別される場合があります。詳細は、表 4-8 の各ディレクティブの説明を参照してください。

構成ファイルのディレクティブよりも、同じ動作パラメタに対するコマンド行オプションの方が優先される場合があります。たとえば、`-p` オプションは、構成ファイルディレクティブ `Port` より優先されます。コマンド行オプションまたは構成ファイルディレクティブで指定されない動作パラメタには、あらかじめ組み込まれているデフォルト値が使用されます。表 4-8 に、vcad コマンドがサポートするコマンド行ディレクティブを示します。

表 4-8　vcad コマンドのコマンド行ディレクティブ

ディレクティブ	説明
`DebugLevel` *level*	ユーザーは、構成ファイルで 3 つのデバッグレベルのうちの 1 つを設定できます。3 つのレベルとは、情報量の少ない順に Notice、Info、および Debug です。Notice レベルがデフォルトです。
`HostBind` *host/IP*	指定した IPv4 または IPv6 アドレス、あるいはホストが決定した IP アドレスにバインドして待機するように `vcad` に指示します。複数の `HostBind` ディレクティブを指定すると、`vcad` は複数のアドレスで待機できます。構成ファイルに `HostBind` エントリがない場合は、デフォルトで、接続できるすべてのインタフェースで待機します。コマンド行の `-l` フラグは、すべての `HostBind` エントリより優先されることに注意してください。
`KeyStoreDir` *directory*	管理者は、キーストアファイルの保管場所として代替ディレクトリを選択できます。`vcad` を実行するユーザーには、このディレクトリに対する読み取りおよび書き込み権限が必要です (`User` ディレクティブを参照)。デフォルトのキーストアディレクトリは `/etc/opt/SUNWconn/vca/keydata` です。
`LogFile` *logfile*	すべてのログデータが書き込まれる位置として *logfile* を使用します。デフォルトでは、ログデータは syslog に書き込まれます。コマンド行の `-F` フラグ (フォアグラウンドで実行) が使用されている場合、このディレクティブは無視され、`vcad` ログデータは標準エラーデバイスに送信されます。
`MaxData` *size*	1 回のコマンドで送信できるデータの最大量を、size に指定したバイト数に設定します。デフォルトでは、この値は 4M バイト (4194304 バイト) です。送信されたデータがこの値を超えると、`vcad` はクライアントにエラーを戻して接続を切断します。
`Port` *port*	待機ポートを設定します。`vcad` が待機するデフォルトのポートは 6870 です。特権ポート (通常は 1024 未満のポート) で `vcad` を待機させる必要がある場合は、`vcad` をスーパーユーザー特権を持つユーザーで実行する必要があります。セキュリティーに関する注意事項については、87 ページの「`vcad` デーモンのセキュリティー」を参照してください。
`Timeout` *seconds*	管理者は、コマンドデータの 1 バイト目を受信したあと待機する時間を設定できます。このタイムアウト値によって、ストールした読み取り操作が特定のカードへのアクセスをロックすることを防ぎます。`vcad` が、接続されたクライアントから新しいコマンドが送信されることを待っているときには、このタイムアウト値は適用されません。この状況には、ファームウェアのタイムアウト値が対応します (79 ページの「自動ログアウト時間の設定」を参照)。デフォルトのタイムアウト値は、300 秒 (5 分) です。

表 4-8　vcad コマンドのコマンド行ディレクティブ (続き)

ディレクティブ	説明
User *username*	vcad が username に指定したユーザー名で動作するように設定します。デーモンは、実際のユーザー ID を username に関連する UID に設定することを試みます。このディレクティブのデフォルト値は、vcad プロセスを開始したユーザーです。

vcad デーモンのセキュリティー

vcad デーモンは TCP ポートで待機するため、セキュリティーに関する特定の推奨事項について考慮する必要があります。

vcad を実行するときには、そのプロセスは、スーパーユーザー特権を持たないユーザー ID (UID0 アカウント以外) で実行する必要があります。ネットワークからこのユーザーアカウントに直接ログインできるようにしないでください。このアカウントのパスワードは存在しないかロックされていて、ログインシェルがありません。/etc/shadow ファイルのこのアカウントに対するエントリには、NP または *LK* と記されます。

デフォルトでは、vcad デーモンは、デーモンのユーザーアカウントで起動することを試みます。このアカウントが無効になっている場合でも vcad デーモンは正しく起動しますが、システムにはアカウントが存在する必要があります。次の手順を実行して、別のユーザー名で動作するように vcad を手動で構成します。

▼ 別のユーザー名で動作するように vcad デーモンを構成する

1. **/dev/vcactl への読み取りおよび書き込みアクセス権を設定します。**

   vcad デーモンは、/dev/vcactl と直接通信し、コマンドデータを中継して Sun Crypto Accelerator 4000 ファームウェアからキーストアの入出力コマンドを取得します。アクセス権および所有権は、vcad を実行しているユーザーアカウントのみが /dev/vcactl に対する読み取りおよび書き込みを行えるように設定されています。デフォルトでは、vcactl モジュールが追加され、マイナーノードの所有者はデーモンで、所有者の読み取りおよび書き込み権のみが設定されます。もっとも安全な方法でこれらのアクセス権を変更するには、rem_drv(1m) および add_drv(1m) を使用して vcactl モジュールを再登録します。

```
rem_drvvcactl
add_drv-m '* MODE USERGROUP' vcactl
```

USER および GROUP の位置には、デバイスのマイナーノードに必要なユーザーおよびグループの所有権を設定する必要があります。MODE に、デバイスのマイナーノードに対するファイルモードを指定します。vcactl モジュールに推奨されるモードは 0600 です。詳細は、add_drv(1m) のマニュアルページを参照してください。

2. **キーストアへの読み取りおよび書き込みアクセス権を構成します。**

   キーストアの入出力操作を実行する vcad デーモンが、構成ファイルで指定されたキーストアディレクトリにアクセスできるようにする必要があります。キーストアディレクトリには、vcad を実行しているユーザーアカウントだけが、読み取り、書き込み、および実行の権限を持つように設定する必要があります。このディレクトリのキーストアファイルは、このユーザーだけに読み取りおよび書き込み権限を許可する必要があります。

3. **特権のない TCP ポートで vcad デーモンを実行します。**

   vcad デーモンがスーパーユーザー特権を使用せずに動作している場合は、特権ポートにバインドすることはできません。通常、特権のないポートは 1024 以上です。使用するシステムの tcp_smallest_nonpriv_port パラメタの値が 1024 でない場合は、ndd を使用してこの値を設定します。デフォルトでは、vcad デーモンはポート 6870 を使用します。

例

例 1 : vcad デーモンを起動して、ポート 5525 で待機します。

```
# /opt/SUNWconn/cryptov2/sbin/vcad -p 5525
```

例 2 : 詳細なデバッグ情報を出力するように指定して vcad デーモンを起動し、その情報を画面に送信します。

```
# /opt/SUNWconn/cryptov2/sbin/vcad -Fdd
```

このように起動すると、起動時に次の出力が表示されます。

```
vcad[1679/1]: [debug] got exclusive lock
vcad[1679/1]: [info] Security daemon starting up
vcad[1679/1]: [debug] Starting file handling thread
vcad[1679/1]: [debug] Starting TCPserver
vcad[1679/1]: [debug] TCP socket bound on port 6870
vcad[1679/1]: [debug] fd is 6
```

また、vcad デーモンは、2 つのレベルのデバッグ出力で動作している場合、新しい接続の開始および切断時にも情報を通知します。

例 3 : vcad デーモンを起動して、代替構成ファイルを使用します。

```
# /opt/SUNWconn/cryptov2/sbin/vcad -f /etc/opt/SUNWconn/vca/alt-vcad.conf
```

vcadiag ユーティリティーの使用

vcadiag ユーティリティーは、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、セキュリティー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 ユーティリティー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] vca*N*
- vcadiag [-F] vca*N*
- vcadiag [-K] vca*N*
- vcadiag [-Q]
- vcadiag [-R] vca*N*
- vcadiag [-Z] vca*N*

注 – [-DFKRZ] オプションを使用する場合の vca*N* 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 4-9 に、vcadiag ユーティリティーがサポートするオプションを示します。

表 4-9 vcadiag オプション

オプション	意味
-D vca*N*	Sun Crypto Accelerator 4000 ボードの診断を実行します。
-F vca*N*	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 vca*N*	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、次の情報がコロンで区切って表示されます。 • デバイス • 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 このオプションを使用して、デバイスとキーストアの関係を判断できます。
-R vca*N*	ボードをリセットします。
-Z vca*N*	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 76fdcb2a 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.
```

pk11export ユーティリティーの使用

pk11export ユーティリティーは、鍵のデータベースから鍵および証明書を抽出して、インポート可能な PKCS#12 形式にします。このユーティリティーによってオブジェクトを抽出し、PKCS#12 ファイルに鍵および証明書を配置するには、PKCS#11 インタフェースが必要です。一度に抽出できるのは、1 組の鍵と証明書だけです。

PKCS#11 インタフェースが動的ライブラリに含まれている場合、このユーティリティーはさまざまな PKCS#11 プロバイダとともに動作します。次の要件が満たされていると、pk11export ユーティリティーは PKCS#11 プロバイダを介して鍵をエクスポートします。

- PKCS#11 インタフェースが、PKCS#11 関数 C_WrapKey を実装している
- PKCS#11 インタフェースが、PKCS#11 メカニズム CKM_DES3_CBC_PAD および CKM_SHA_1 を実装している
- エクスポートされる鍵に、CKA_EXTRACTABLE 属性が設定されている

次に、pk11export コマンドのコマンド行構文を示します。

- /opt/SUNWconn/cryptov2/bin/pk11export -V
- /opt/SUNWconn/cryptov2/bin/pk11export -l [-p *pkcs11-lib*]
- /opt/SUNWconn/cryptov2/bin/pk11export [-n *friendly-name*] [-o *filename*] [-p *pkcs11-lib*] *token-name*

表 4-10 に、pk11export ユーティリティーがサポートするオプションを示します。

表 4-10 pk11export オプション

オプション	説明
-l	特定の PKCS#11 ライブラリが認識する、使用可能なトークンをすべて表示します。
-n *friendly-name*	エクスポートする鍵および証明書の組を指定します。*friendly-name* には、文字列を指定します。
-o *filename*	作成された PKCS#12 ファイルを *filename* ファイルに書き込みます。出力先の *filename* が指定されていない場合、PKCS#12 ファイルは、pkcs12file という名前でカレントディレクトリに出力されます。
-p *pkcs11-lib*	鍵および証明書を抽出する PKCS#11 ライブラリを指定します。このオプションを使用するには、*pkcs11-lib* 変数に動的ライブラリへのフルパスを指定する必要があります。デフォルトでは、pk11export は、Sun Crypto Accelerator 1000 PKCS#11 ライブラリ (/opt/SUNWconn/crypto/lib/libpkcs11.so) を使用しますが、このオプションの *pkcs11-lib* 変数によって任意の PKCS#11 ライブラリを指定することができます。

表 4-10　pk11export オプション (続き)

オプション	説明
-V	pk11export のバージョン情報を表示します。

例

例 1 : PKCS#11 実装のトークンを表示します。

```
# pk11export -l -p /opt/SUNWconn/cryptov2/bin/libvpkcs11.so
0. SUNW acceleration only
1. arf
```

例 2 : PKCS#11 トークン nobody@webserv から Server-Cert 証明書をエクスポートし、/tmp/webserv-export.p12 ファイルに書き込みます。

```
example% pk11export -o /tmp/webserv-export.p12 nobody@webserv
Enter password for nobody@webserv:
Enter password for pkcs12 file:
Re-enter password for pkcs12 file:
/tmp/webserv-export.p12 was created successfully
```

iplsslcfg スクリプトの使用

iplsslcfg スクリプトのオプション 1 および 2 は、Sun ONE Web サーバーおよびアプリケーションサーバーソフトウェアを構成して登録するモジュールをインストールします。このスクリプトのオプション 3 および 4 は、Sun ONE Web サーバーの鍵の PKCS#12 形式へのエクスポートと、PKCS#12 形式からのインポートを行います。

▼ iplsslcfg スクリプトのオプション 1 を使用する (Sun ONE Web Server 4.1 の場合)

- 詳細は、115 ページの「Sun ONE Web Server 4.1 の構成」を参照してください。

▼ iplsslcfg スクリプトのオプション 1 を使用する (Sun ONE Web Server 6.0 の場合)

- 詳細は、125 ページの「Sun ONE Web Server 6.0 の構成」を参照してください。

▼ iplsslcfg スクリプトのオプション 2 を使用する

1. 次のように入力して、iplsslcfg スクリプトを実行します。

```
# /opt/SUNWconn/cryptov2/bin/iplsslcfg
```

2. Sun ONE アプリケーションサーバーの場合は 2 を入力して、バイナリおよびドメインのパスを入力します。

```
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): 2

You will now be prompted for four pieces of information:
 1. The location of the Sun ONE Application Server binaries
 2. The location where Sun ONE Server domains are stored
 3. The Application Server domain (e.g. domain1)
 4. The Application Server server name (e.g. server1)

Full path to Application Server binaries: [/opt/SUNWappserver7]:
/opt/SUNWappserver7
Full path to Application Server domains: [/var/opt/SUNWappserver7]:
/var/opt/SUNWappserver7
Application Server domain: domain1
Application Server server name: server1
This script will update your Sun ONE Application Server installation
```

```
in /opt/SUNWappserver7 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
/var/opt/SUNWappserver7/domains/domain1/server1/config...
Module "Sun Crypto Accelerator 4000" added to database.
/opt/SUNWappserver7 has been configured to use
the Sun Crypto Accelerator.

<Press ENTER to continue>
```

3. 0 を入力して処理を終了します。

▼ iplsslcfg スクリプトのオプション 3 を使用する

このオプションは、SSL 証明書および鍵を、Sun ONE Web サーバーの内部データベースから PKCS#12 形式にエクスポートします。エクスポートした証明書は、Sun Crypto Accelerator 4000 モジュールにふたたびインポートできます。

1. 次のように入力して、iplsslcfg スクリプトを実行します。

```
# /opt/SUNWconn/cryptov2/bin/iplsslcfg
```

2. Sun ONE Web サーバーの鍵を PKCS#12 形式にエクスポートするため、3 を入力して Return キーを押します。

```
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): 3
```

3. Sun ONE サーバーのディレクトリのパスを入力します。

   iplsslcfg ユーティリティーは、鍵をエクスポートできる可能性のあるすべての証明書および鍵のデータベースを探します。

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

4. 表示されたリストから名前を選択して入力します。

```
The following certificate databases were found:
https-machine.domain.com-webserv1-
https-machine.domain.com-webserv2-
Which certificate database do you wish to export from?
https-machine.domain.com-webserv1-
```

5. エクスポートするサーバー証明書のフレンドリ名を入力します。

   デフォルトの名前は Server-Cert です。

```
Please provide the name for the certificate you wish to export.
If you wish to export from a hardware device, you will need to
provide the token name followed by a ":" and the certificate name.
Not all external tokens will allow keys to be exported.
Certificate Name [Server-Cert]: Server-Cert
```

6. PKCS#12 ファイルのパスおよびファイル名を指定します。

```
Please specify the path where the PKCS#12 file will be stored:
/tmp/export.p12
```

7. パスワードを入力します。

   認証に成功すると、PKCS#12 ファイルのパスワードを設定するように求められます。このパスワードを作成すると、手順 6 で選択したファイル名で PKCS#12 ファイルが書き込まれます。

```
Enter Password or Pin for "NSS Certificate DB":
Enter password for PKCS12 file:
Re-enter password:
pk12util: PKCS12 EXPORT SUCCESSFUL
Successfully created the PKCS#12 file.
<Press ENTER to continue>
```

8. 0 を入力して処理を終了します。

▼ iplsslcfg スクリプトのオプション 4 を使用する

このオプションは、鍵および証明書を PKCS#12 形式からボードにインポートします。

1. 次のように入力して、iplsslcfg スクリプトを実行します。

```
# /opt/SUNWconn/cryptov2/bin/iplsslcfg
```

2. PKCS#12 形式から Sun ONE Web サーバーに鍵をインポートするため、4 を入力して Return キーを押します。

```
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): 4
```

3. Sun ONE サーバーのディレクトリのパスを入力します。

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

4. インポートする PKCS#12 ファイルのパスを入力します。

```
Enter the path to the PKCS#12 file: /tmp/export.p12
```

5. 次の質問に yes と答えます。

```
Will you be importing to a hardware device? [Y/N]: Y
```

6. 初期設定でボードに構成したキーストア名を入力します。

```
Enter the token name: vca0
```

7. 正しく認証される形式で *username:password* 文字列を入力します。詳細は、表 5-1 を参照してください。

```
Enter Password or Pin for "vca0":
```

8. PKCS#12 ファイルを保護するパスワードを入力します。

```
Enter password for PKCS12 file:
Import successful.

<Press ENTER to continue>
```

apsslcfg スクリプトの使用

apsslcfg スクリプトのオプション 1 は、Apache Web サーバーを SSL を使用できるように構成します。オプション 2 は、Apache Web サーバーの鍵を構成します。

注 – apsslcfg スクリプトは、Apache Web Server 1.3.26 のみをサポートします。

▼ apsslcfg スクリプトのオプション 1 を使用する

- 詳細は、180 ページの「Apache Web サーバー 1.3x の構成」を参照してください。

apsslcfg スクリプトのオプション 2 の使用

オプション 2 には、さらに次の 3 つのオプションがあります。

1. 鍵ペアを生成して Apache の証明書を要求する
2. Apache (PEM 符号化形式の X.509) 鍵を PKCS#12 形式でエクスポートする
3. PKCS#12 形式から Apache (PEM 符号化形式の X.509) に鍵をインポートする

▼ 鍵ペアを生成して Apache の証明書を要求する

このオプションは、認証局に提出できる RSA 鍵および証明書要求を生成します。

1. **このオプションを選択するには、`1` を入力します。**
2. **バイナリおよび Apache モジュールのパスと、構成ファイルのパスを入力します。**

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

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

3. **鍵のパスを入力します。**

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

4. **鍵および証明書要求のファイルの基本名を入力します。**

   ファイル名の前にこの名前が付加されます。たとえば、`cert1` を選択すると、鍵のファイル名は `cert1-key.pem` になり、証明書要求のファイル名は、`cert1-certreq.pem` になります。

```
Please choose a base name for the key and request file: cert1
```

5. **生成する RSA 鍵のサイズを選択します。**

   サイズをビット単位で指定すると、RSA 鍵が生成されます。

```
What size would you like the RSA key to be [1024]? 1024
```

6. **鍵ファイルを暗号化するパスワードを入力します。**

   強力なパスワードを使用してください。また、パスワードは忘れないでください。

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

7. **証明書要求に必要な各名称を入力します。**

   証明書要求は、認証局に提出できる形式でファイルに書き込まれます。

```
-----
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]: California
Locality Name (eg, city) []: San Diego
Organization Name (eg, company) []: Company
Organizational Unit Name (eg, section) []: Department
SSL Server Name (eg, www.company.com) []: www.company.com
Email Address []: admin@domain.com

The keyfile is stored in /etc/apache/keys/cert1-key.pem.
The certificate request is in /etc/apache/keys/cert1-certreq.pem.

<Press ENTER to continue>
```

▼ Apache (PEM 符号化形式の X.509) 鍵を PKCS#12 形式にエクスポートする

このオプションを使用すると、Apache Web サーバーの鍵および証明書を PKCS#12 ファイルに書き込むことができます。

1. **このオプションを選択するには、2 を入力します。**
2. **鍵および証明書のファイルのパスを入力します。**

   鍵および証明書のファイルが同じものである場合は、同じパスを 2 回入力します。

注 – 鍵および証明書のデータは、同じファイルまたは個別のファイルに格納されます。ただし、個別のファイルに格納されていても、ファイル名は同じである必要があります。

```
Enter the path to the key file:
Enter the path to the certificate file:
```

3. PKCS#12 ファイルの出力先のパスを入力します。

```
Please specify the path where the PKCS#12
file will be stored:
```

4. 証明書のフレンドリ名を入力します。

   この名前は、証明書および鍵を一意に識別します。

```
Please provide a friendly name for the PKCS#12 being
built.  This friendly name is necessary when
importing your PKCS#12 file for use by other web servers.
Friendly Name [Server-Cert]:
```

5. PCKS#12 ファイルに出力する鍵を保護しているパスワードを入力します。

```
Enter pass phrase for /etc/apache/keys/ap1-key.pem:
```

6. PKCS#12 ファイルの鍵データを保護するためのパスワードを入力します。

   PKCS#12 ファイルは、前の手順で指定したファイルに書き込まれます。

```
Enter Export Password:
Verifying - Enter Export Password:
Your PKCS#12 file has been created successfully and is in
/tmp/exp.p12

<Press ENTER to continue>
```

▼ PKCS#12 形式から Apache (PEM 符号化形式の X.509) に鍵をインポートする

このオプションを使用すると、鍵および証明書を PKCS#12 ファイルから抽出して、Apache Web サーバーで使用できるようになります。

1. このオプションを選択するには、3 を入力します。
2. PKCS#12 ファイルのパスとファイル名を入力します。

```
Enter the path to the PKCS#12 file:
```

3. 鍵および証明書の抽出先のパスを入力します。

```
Enter the directory where keys and certificates
will be stored:
```

4. 鍵および証明書ファイルのファイル名を入力します。

暗号化された鍵および証明書は、同じファイルに格納されます。

```
Please choose a name for the key and
Certificate file. This file will contain
both the encrypted key and the certificate:
```

5. PKCS#12 ファイルを保護するパスワードを入力します。

```
Enter Import Password:
MAC verified OK
```

6. 新しいパスワードを入力して、Apache が読み取ることのできる形式で抽出した鍵ファイルを保護します。

鍵および証明書のデータは、手順 4 で指定したファイルに書き込まれます。

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

The keys have been successfully extracted to the file
/etc/apache/key2/yakstuff.pem.

<Press ENTER to continue>
```

同じサーバーに取り付けた複数のボードへの異なる MAC アドレスの割り当て

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システムレベルで、2 つ目の方法は OpenBoot PROM 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. OpenBoot PROM の ok 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. オペレーティングシステムを起動します。

第5章

Sun ONE サーバーソフトウェアのインストールおよび構成

この章では、Sun ONE サーバーで Sun Crypto Accelerator 4000 ボードを使用するため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。

注 – このマニュアルで説明する Sun ONE サーバーは、以前は iPlanet™ 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。

注 – Apache Web サーバー (第 6 章) は、この章で説明するキーストアまたはユーザーアカウントの機能を使用しません。

Sun Crypto Accelerator 4000 ボードでは、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、3 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 *sca4000-ks-1* と、そのキーストア内の 3 人のユーザー *webserv*、*dirserv*、および *mailserv* によって 1 つの構成が作成されます。この場合、3 人のユーザーは、この 1 つのキーストア内でサーバーの鍵へのアクセス制御を所有し管理することができます。図 5-1 に、通常のインストールの概要を示します。

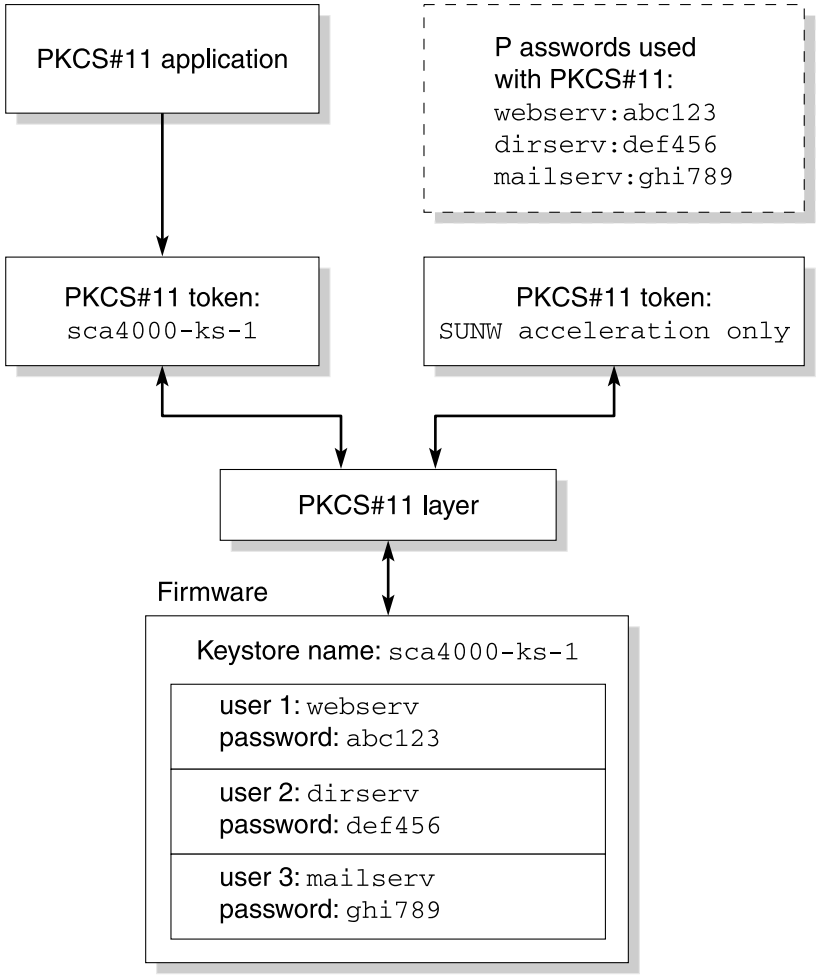

図 5-1　　キーストアおよびユーザーの概要

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、71 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。トークンファイルによって、Sun Crypto Accelerator 4000 の管理者は、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ことができます。

例

engineering、*finance*、および *legal* の 3 つのキーストアが作成されている場合、デフォルトでは、次の 3 つのトークンが 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 – コメントは「#」文字で開始します。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、108 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します。

```
# 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。

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。

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	セキュリティー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。
セキュリティー管理者	`vcaadm` の特権操作を行うときに必要なパスワードです。
username:password	セキュリティー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 (*keystore-name*) 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、`vcaadm` でキーストアのユーザーを作成するときに指定した *username* および *password* で構成されます。キーストアの *username* と *password* 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、68 ページの「vcaadm によるボードの初期化」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、59 ページの「vcaadm ユーティリティーの使用」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。

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

注意 – これらの手順は、記載されている順に実行してください。別の順番で実行すると、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、114 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、124 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。

再起動時のユーザーの操作をなくすための、Sun ONE Web サーバーの起動設定

Sun ONE 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 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 サーバーのインスタンスの `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
```

Sun ONE Web Server 4.1 のインストールおよび構成

この節では、ボードを使用するために Sun ONE Web Server 4.1 をインストールおよび構成する方法について説明します。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 サーバーのインストールおよび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。この節の内容は、次のとおりです。

▼ 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. インストールディレクトリに移動して、Web サーバーソフトウェアを解凍します。

3. コマンド行で `setup` スクリプトを使用して、Web サーバーをインストールします。

   サーバーのデフォルトのパス名は、`/usr/netscape/server4` です。

   この章では、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。

   ```
   # ./setup
   ```

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。

   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. 完全指定のドメイン名を入力します。

   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。

Sun ONE Web Server 4.1 の構成

以降の手順では、Web サーバーのインスタンスに対する認証データベースの作成、Web サーバーで使用するボードの登録、サーバーの証明書の生成とインストール、および Web サーバーでの SSL の有効化を行います。

構成処理中は、Sun ONE Web サーバーの管理サーバーが起動し、動作している必要があります。

▼ 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、次のコマンドを入力して 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フェース (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」タブをクリックします。

b. サーバーを選択して、「Manage」ボタンをクリックします。

c. ページの上部にある「Security」タブをクリックして、「Create Database」リンクをクリックします。

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。

▼ Web サーバーで使用するボードを登録する

1. 次のスクリプトを実行して、Web サーバーで使用するボードを登録します。

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

このスクリプトは、サーバーを選択するためのプロンプトを表示し、選択した Sun ONE 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。そのあと、構成ファイルを更新してボードを使用できるようにします。

2. `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。

注 – この手順では、このプロンプトでオプション 1 を選択することを想定しています。オプション 2、3、または 4 を選択する場合は、93 ページの「iplssslcfg スクリプトの使用」を参照してください。

```
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
```

3. 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
```

4. プロンプトが表示されたら、y および Return キーを押します。

```
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>
```

5. 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 5-2 を参照)。

「Create Trust Database」ページが表示されます。

5. 左側のパネルにある「Request a Certificate」リンクを選択します (図 5-2 を参照)。

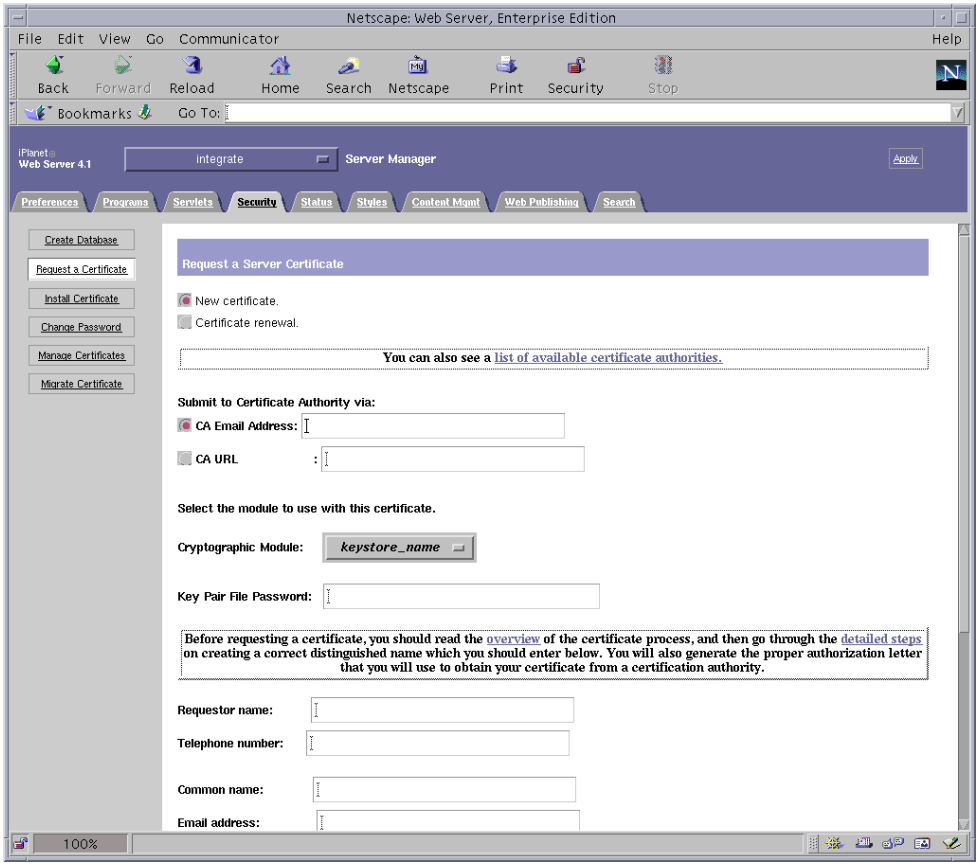

図 5-2　Sun ONE Web Server 4.1 管理サーバーの「Request a Server Certificate」ダイアログボックス

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」(認証局の 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、証明書要求の送信先の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、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。「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. 表 5-2 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
Organization	会社名
Organizational Unit	(任意) 会社の部門
Locality	(任意) 市区町村
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」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」タブをクリックします。

3. 左側のパネルにある「Install Certificate」リンクを選択します。

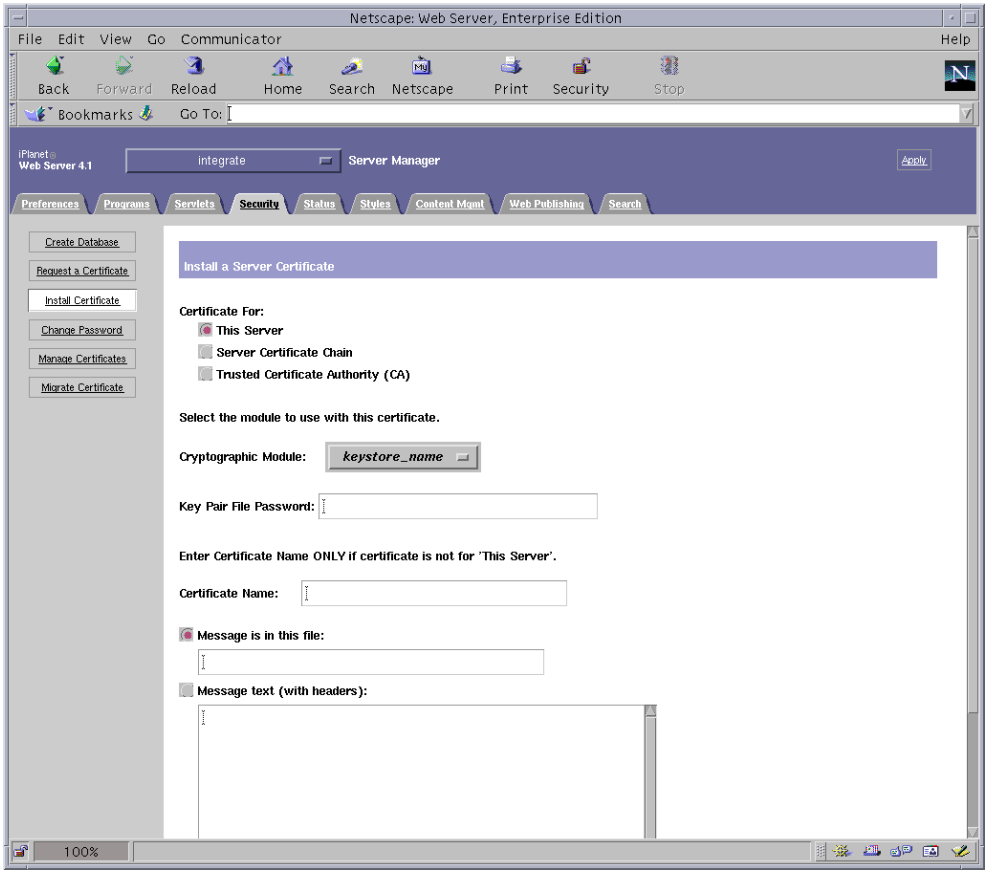

図 5-3　Sun ONE Web Server 4.1 管理サーバーの「Install a Server Certificate」ダイアログボックス

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。ボードを使用するには、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、*username:password* 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 (118 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. 「OK」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。

注 – テストのため、証明書に自己署名する方法については、mod_SSL および OpenSSL のマニュアルを参照してください。

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する必要があります。

▼ Web サーバーで SSL を使用可能にする

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」ボタンをクリックします。**

6. **「Save」ボタンをクリックして、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、ページの右上の角にある「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、ボードを使用するために Sun ONE Web Server 6.0 をインストールおよび構成する方法について説明します。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 サーバーのインストールおよび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。この節の内容は、次のとおりです。

▼ 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. **インストールディレクトリに移動して、Web サーバーソフトウェアを解凍します。**

3. コマンド行で setup スクリプトを使用して、Web サーバーをインストールします。

   サーバーのデフォルトのパス名は、/usr/iplanet/servers です。

   この章では、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。

```
# ./setup
```

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。

   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. 完全指定のドメイン名を入力します。

   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。

Sun ONE Web Server 6.0 の構成

以降の手順では、Web サーバーのインスタンスに対する認証データベースの作成、Web サーバーで使用するボードの登録、サーバーの証明書の生成とインストール、および Web サーバーでの SSL の有効化を行います。

構成処理中は、Sun ONE Web サーバーの管理サーバーが起動し、動作している必要があります。

▼ 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」をクリックします。

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 の管理サーバーのダイアログボックスで「Servers」タブをクリックします。

b. サーバーを選択して、「Manage」ボタンをクリックします。

c. ページの上部にある「Security」タブをクリックして、「Create Database」リンクをクリックします。

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。

▼ Web サーバーで使用するボードを登録する

1. 次のスクリプトを実行して、Web サーバーで使用するボードを登録します。

```
# /opt/SUNWconn/cryptov2/bin/iplsslcfg
```

このスクリプトは、サーバーを選択するためのプロンプトを表示し、選択した Sun ONE 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。そのあと、構成ファイルを更新してボードを使用できるようにします。

2. 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。

注 – この手順では、このプロンプトでオプション 1 を選択することを想定しています。オプション 2、3、または 4 を選択する場合は、93 ページの「iplsslcfg スクリプトの使用」を参照してください。

```
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
```

3. 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
```

4. 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>
```

5. 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」をクリックします。

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のパネルにある「Request a Certificate」リンクをクリックします。

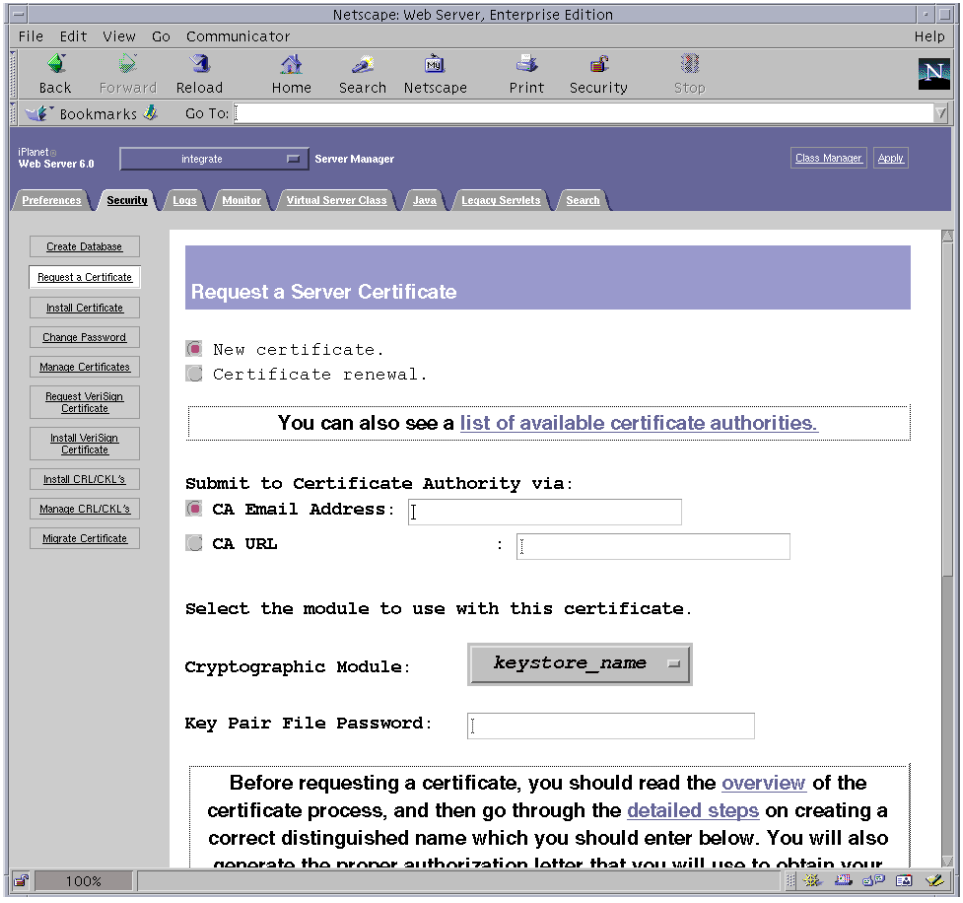

図 5-4　Sun ONE Web Server 6.0 管理サーバーの「Request a Server Certificate」ダイアログボックス

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、証明書要求の送信先の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、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。「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. 表 5-4 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
Organization	会社名
Organizational Unit	(任意) 会社の部門
Locality	(任意) 市区町村
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」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、131 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」タブをクリックします。

3. 左側のパネルにある「Install Certificate」リンクをクリックします。

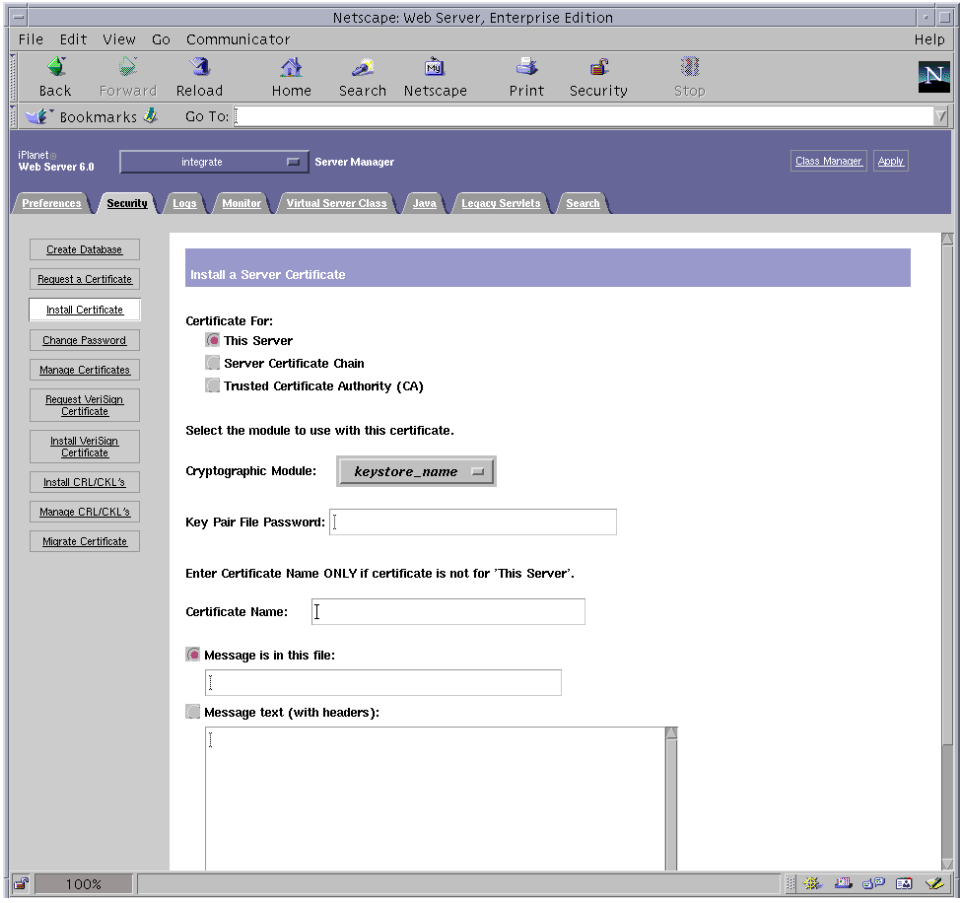

図 5-5　Sun ONE Web Server 6.0 管理サーバーの「Install a Server Certificate」ダイアログボックス

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。ボードを使用するには、*keystore-name* 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、*username:password* 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 (128 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. **「OK」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。

注 – テストのため、証明書に自己署名する方法については、mod_SSL および OpenSSL のマニュアルを参照してください。

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する必要があります。

▼ Web サーバーで SSL を使用可能にする

1. **ページの上部にある「Preferences」タブをクリックします。**

2. **左側のパネルにある「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」をクリックして、変更を適用します。

「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」、「SSL2」、または「SSL3/TLS」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」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」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」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。

Sun ONE Application Server 7 のインストールおよび構成

この節では、ボードを使用するために Sun ONE Application Server 7 をインストールおよび構成する方法について説明します。アプリケーションサーバーの追加ソフトウェアは、アプリケーションサーバーソフトウェアとは別にインストールする必要があります。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 アプリケーションサーバーのインストールおよび使用方法については、Sun ONE アプリケーションサーバーのマニュアルを参照してください。この節の内容は、次のとおりです。

▼ Sun ONE Application Server 7 をインストールする

1. Sun ONE Application Server 7 ソフトウェアをダウンロードします。

   アプリケーション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/`

   Sun ONE Application Server 7 にはさまざまな配布があり、それぞれに固有の機能があります。

2. インストールディレクトリに移動して、アプリケーションサーバーソフトウェアを解凍します。

   インストールディレクトリのデフォルトのパスは、Sun ONE Application Server 7 ソフトウェアの配布によって異なります。

3. `setup` プログラムを実行して、GUI ベースのインストールを開始します。

注 – 端末エミュレータから `setup -console` プログラムを実行して、コマンド行ベースのインストールを開始することもできます。この手順の例では、GUI ベースのインストールを使用することを想定しています。

```
# ./setup
```

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。

   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. JDK (Java™ Development Kit) の位置の入力を求めるプロンプトが表示されたら、「Use Existing Installation」(サポートされる場合)、または「Install From the Appserver Build」のいずれかを選択します。

   c. Sun ONE アプリケーションサーバーの管理サーバーのユーザー名を入力します (任意の名前を入力できます)。

   d. Sun ONE アプリケーションサーバーの管理サーバーのパスワードを 2 回入力します。

注 – Solaris 8 オペレーティング環境を使用している場合のみ、次の手順を実行します。

---

5. Solaris 8 を使用している場合は、Solaris 8 Sun ONE アプリケーションサーバーパッチ (109326-08) をインストールします。

   このパッチは、Solaris 9 には必要ありません。Solaris 8 Sun ONE アプリケーションサーバーパッチは、次の SunSolve Web サイトからダウンロードします。
   `http://sunsolve.sun.com`

   次のように実行して、パッチを追加します。

```
# cd patch-location/SUNWappserver7/patches
# cd patches/109326-08
# ./patchadd .
```

6. システムを再起動します。

▼ Sun ONE アプリケーションサーバーの追加ソフトウェアをインストールする

1. Sun ONE Application Server 7 の追加ソフトウェアをダウンロードします。

   アプリケーション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. Sun ONE アプリケーションサーバーの追加ソフトウェアを解凍します。

3. `./AddOns/SSLUtils` ディレクトリに移動します。

4. `iplsslcfg` スクリプトが `modutil` セキュリティーツールを起動するためのディレクトリを作成します。

```
# mkdir /usr/bin/mps
```

   `iplsslcfg` スクリプトは、このパスで `modutil` セキュリティーツールを検索します。

5. `modutil`、`certutil`、および `pk12util` のバイナリを `/usr/bin/mps/` パスにコピーします。

```
# cp modutil /usr/bin/mps/
# cp certutil /usr/bin/mps/
# cp pk12util /usr/bin/mps/
```

6. /usr/bin/mps/ ディレクトリのバイナリに実行権を設定します。

```
# chmod 544 /usr/bin/mps/*
```

Sun ONE Application Server 7 の構成

以降の手順では、アプリケーションサーバーのインスタンスに対する認証データベースの作成、アプリケーションサーバーで使用するボードの登録、サーバーの証明書の生成とインストール、およびアプリケーションサーバーでの SSL の有効化を行います。

構成処理中は、Sun ONE アプリケーションサーバーの管理サーバーが起動し、動作している必要があります。

▼ 認証データベースを作成する

1. Sun ONE アプリケーションサーバーおよび Sun ONE アプリケーションサーバーの管理サーバーを起動します。

```
# installation-directory/bin/asadmin start-appserv
```

注 – アプリケーションサーバーが動作していることを示すメッセージが表示されます。

2. Web ブラウザを開いて次の URL を入力し、管理用 GUI を起動します。

```
http://hostname:4848
```

認証ダイアログボックスが表示されるので、setup プログラムで作成した Sun ONE アプリケーション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 アプリケーション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 アプリケーションサーバー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」をクリックします。

4. **アプリケーション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 つ以上のアプリケーションサーバーの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、アプリケーションサーバーの各インスタンスで、手順 1 〜手順 4 を繰り返します。

注 – Sun ONE アプリケーションサーバーの管理サーバーで 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/source/816-6482/` の『Sun ONE Application Server 7 セキュリティ管理者ガイド』を参照してください。

---

   a. **管理 GUI の「Manage Database」セクションに移動します。**

      左側のパネルの「Security」リンクを選択して、右側のパネルの「Manage Database」タブをクリックします。

   b. **2 つのテキストボックスに 8 文字以上のパスワードを入力して、「OK」をクリックします。**

      このパスワードは、Sun ONE アプリケーションサーバーの認証データベースのパスワードです。このパスワードは、Sun ONE アプリケーション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。

▼ アプリケーションサーバーで使用するボードを登録する

1. **`iplsslcfg` スクリプトを実行して、アプリケーションサーバーで使用するボードを登録します。**

```
# /opt/SUNWconn/cryptov2/bin/iplsslcfg
```

   このスクリプトは、サーバーを選択するためのプロンプトを表示し、選択した Sun ONE 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。そのあと、構成ファイルを更新してボードを使用できるようにします。

2. **Sun ONE アプリケーションサーバーの場合は `2` を入力して、バイナリおよびドメインのパスを入力します。**

注 – この節の手順では、このプロンプトでオプション 2 を選択することを想定しています。オプション 3 または 4 を選択する場合は、93 ページの「iplsslcfg スクリプトの使用」を参照してください。

```
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): 2
```

3. バイナリおよびドメインの位置と、ドメインおよびサーバーの名前を入力します。

```
You will now be prompted for four pieces of information:
 1. The location of the Sun ONE Application Server binaries
 2. The location where Sun ONE Server domains are stored
 3. The Application Server domain (e.g. domain1)
 4. The Application Server server name (e.g. server1)

Full path to Application Server binaries: [/opt/SUNWappserver7]:
/opt/SUNWappserver7
Full path to Application Server domains:
[/var/opt/SUNWappserver7]: /var/opt/SUNWappserver7
Application Server domain: domain1
Application Server server name: server1
This script will update your Sun ONE Application Server
installation in /opt/SUNWappserver7 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
/var/opt/SUNWappserver7/domains/domain1/server1/config...
Module "Sun Crypto Accelerator 4000" added to database.
/opt/SUNWappserver7 has been configured to use
the Sun Crypto Accelerator.

<Press ENTER to continue>
```

注 – デフォルトのインストールディレクトリは、Sun ONE Application Server 7 配布によって異なる場合があります。

4. `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. 管理 GUI の「Certificate Management」セクションに移動します。

   左側のパネルの「Security」リンクを選択して、右側のパネルの「Certificate Management」タブを選択します。管理 GUI の「Certificate Management」セクションの「Request」サブメニューウィンドウが表示されます。

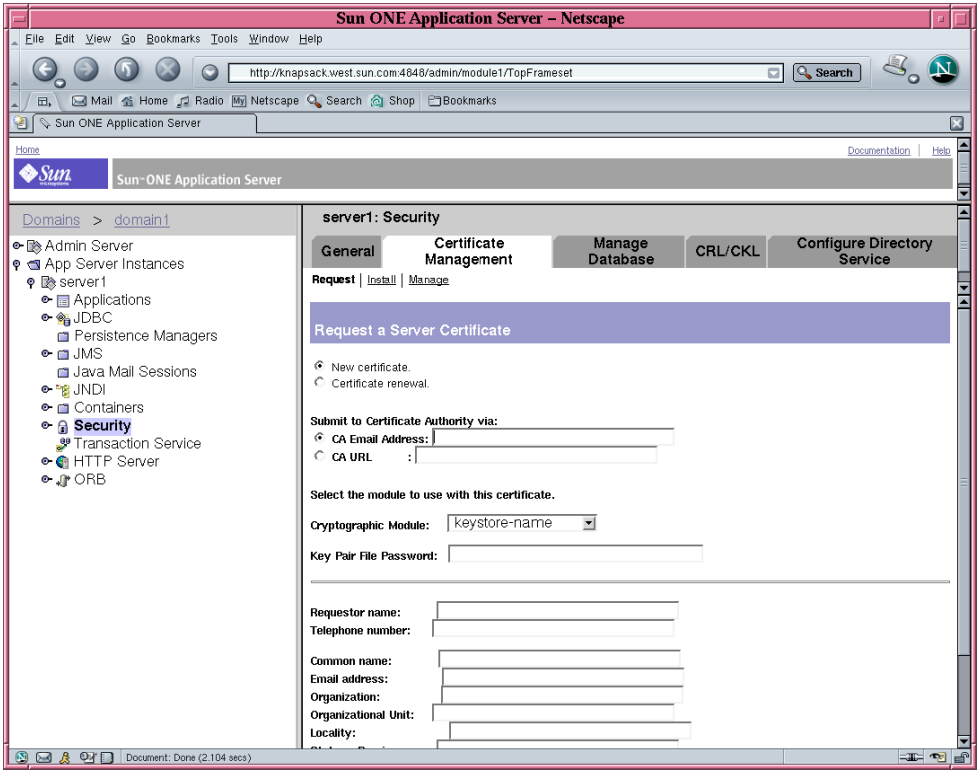

図 5-6　Sun ONE アプリケーションサーバーの管理サーバーの「Request a Server Certificate」ダイアログボックス

2. 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、証明書要求の送信先の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、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。「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. 表 5-6 の要求者情報フィールドに、適切な情報を入力します。

表 5-6　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
Organization	会社名
Organizational Unit	(任意) 会社の部門
Locality	(任意) 市区町村
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」をクリックして、情報を送信します。

3. 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。

4. 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、143 ページの「サーバーの証明書をインストールする」の手順 3 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. 管理 GUI の右側のパネルにある「Certificate Management」セクションの「Install」リンクを選択します。

   管理 GUI の「Certificate Management」セクションの「Install」サブメニューウィンドウが表示されます。

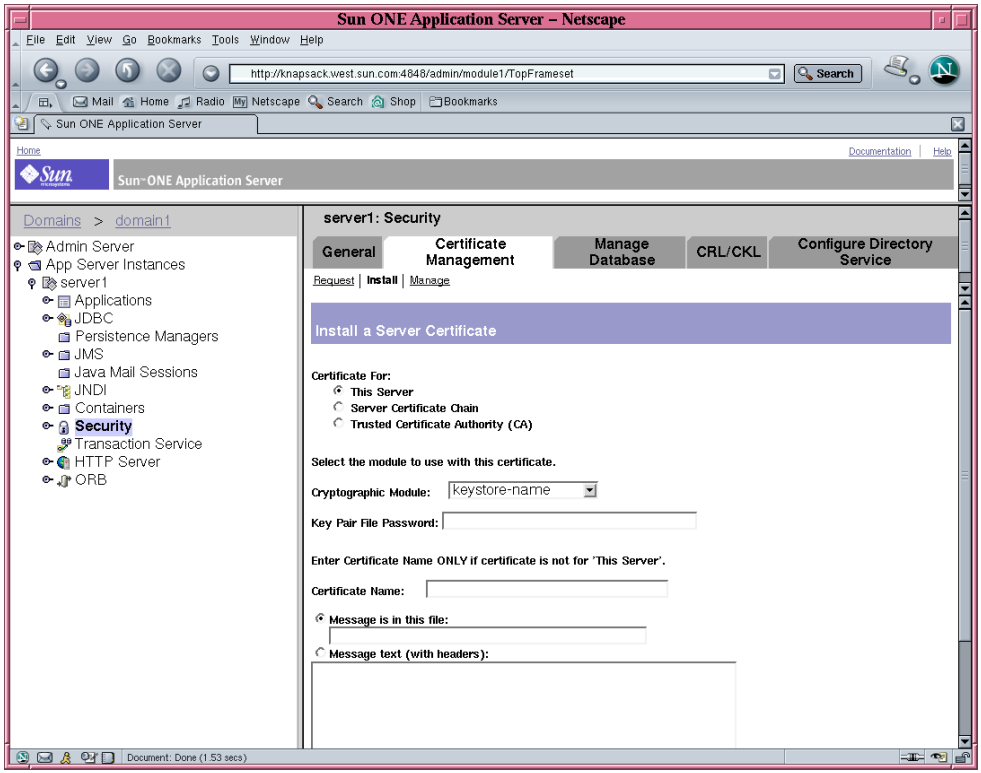

図 5-7　Sun ONE アプリケーションサーバーの管理サーバーの「Install a Server Certificate」ダイアログボックス

2. 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 5-7　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 ボードを使用するには、証明書を要求したときに選択し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、*username:password* です。
Certificate Name	ほとんどの場合、このフィールドは空白にします。ここに名前を指定すると、アプリケーションサーバーで 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。

3. 「Message text (with headers):」ラジオボタンをクリックして、認証局からコピーした証明書 (141 ページの「サーバーの証明書を生成する」の手順 4 を参照) をラジオボタンの下にあるテキストボックスにペーストします。

4. 「OK」をクリックします。

   証明書に関する基本的な情報が表示されます。

5. 表示された内容に誤りがなければ、「Add Server Certificate」をクリックします。

   アプリケーションサーバーの再起動を求めるプロンプトが表示されます。アプリケーションサーバーはまだ再起動しないでください。SSL の構成が完了したあとで再起動します。また、アプリケーションサーバーで 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。

▼ アプリケーションサーバーで SSL を使用可能にする

1. 端末エミュレータで次のコマンドを入力します。

   このコマンドを実行したあと、Sun ONE アプリケーションサーバーの管理サーバーのパスワードも入力する必要があります。

注 – デフォルトのポート 4848 を使用するように Sun ONE アプリケーションサーバーの管理サーバーが構成されている場合に、ローカルホストでこのコマンドを実行するときは、`--host` *hostname* `--port` *administration-server-port* の引数を省略できます。

```
# installation-directory/bin/asadmin create-ssl --user app-admin --host
hostname --port administration-server-port --type http-listener --certname
keystore-name:server-certificate-name --instance server-name http-listener
password>
```

2. 管理 GUI の左側のパネルで、「HTTP Server」リンクの左の拡張ボタンを選択します。

   「HTTP Server」のサブメニュー項目が表示されます。

3. 「HTTP Server」リンクの下にある「HTTP Listeners」サブメニュー項目を選択します。

4. 右側のパネルで、SSL/TLS を設定する HTTP リスナーを選択し、その HTTP リスナーの関連リンクを選択します。

   ウインドウが表示されます。このウィンドウで、HTTP リスナーの属性を編集できます。

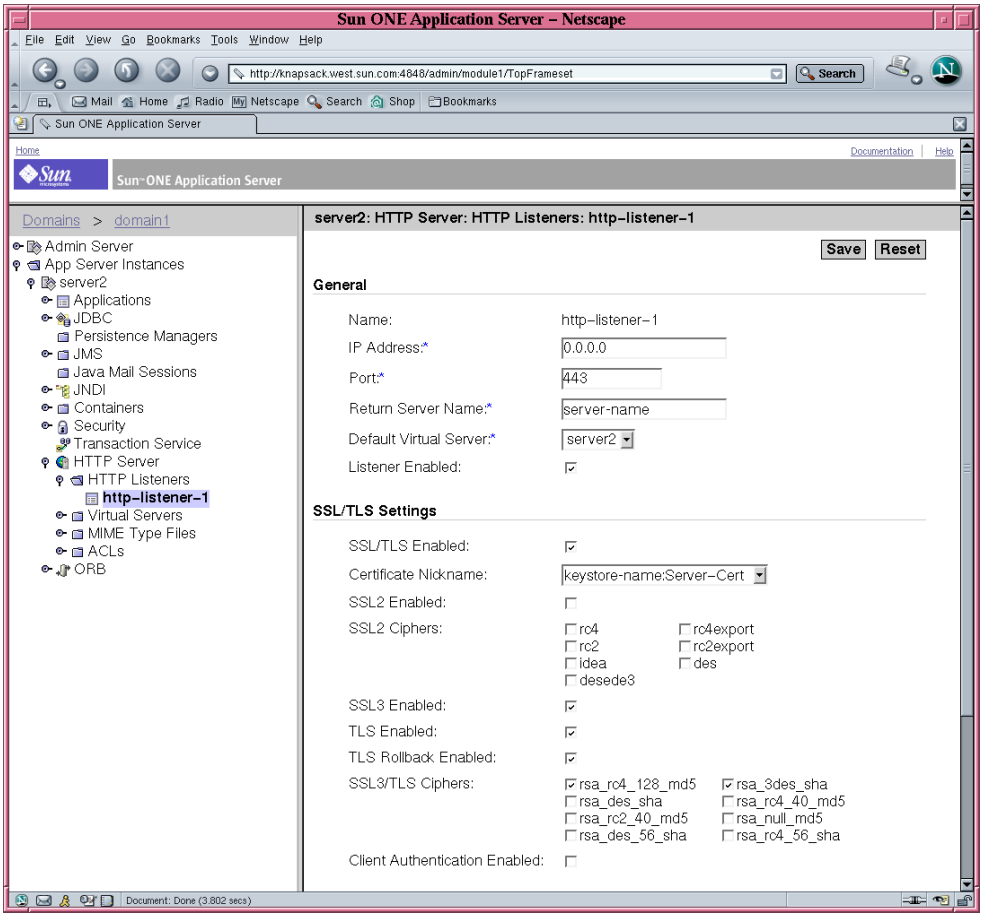

図 5-8　Sun ONE アプリケーションサーバーの管理サーバーの HTTP リスナー属性のダイアログボックス

5. 「SSL/TLS Settings」の「Certificate Nickname」の表示が、144 ページの「アプリケーションサーバーで SSL を使用可能にする」の手順 1 のコマンドオプション `--certname` で選択した証明書の名前と一致することを確認します。

6. 次のボックスには必ずチェックします。
   - SSL/TLS Enabled
   - SSL3 Enabled
   - TLS Enabled

- TLS Rollback Enabled
- SSL3/TLS Ciphers : `rsa_rc4_128_md5` および `rsa_3des_sha`

7. **ポートを設定します。通常は 443 です。**
8. **ロールバック用に、使用するサーバーへのアクセスを検索するブラウザでも TLS を有効にする必要があります。**
   - Netscape Navigator 6.0 では、TLS および SSL3 の両方にチェックします。
   - Microsoft Internet Explorer 5.0 および 5.5 では、TLS Rollback オプションを使用します。
   - TLS Rollback では、TLS にチェックし、SSL3 および SSL2 の両方を無効にします。
9. **「Save」をクリックします。**
10. **左側のパネルで「App Server Instances」を選択して、使用するサーバーのインスタンスを選択します。次に、右側のパネルで「Apply Changes」を選択します。**
11. **サーバーを停止して起動し、変更を有効にします。**

    `init.conf` ファイルが自動的に変更されて、セキュリティーが有効になったことを示します。すべての仮想サーバーに、デフォルトのセキュリティーパラメタが自動的に割り当てられます。

    サーバーで SSL を有効にすると、その URL には、`http` の代わりに `https` が使用されます。SSL が有効になっているサーバーのドキュメントであることを示す URL の形式は、次のとおりです。

```
https://server-name.domain.dom:port-number
```

    次に例を示します。

```
https://admin.sun.com:443
```

注 – セキュリティー保護されたデフォルトの HTTP ポート番号 (443) を使用する場合は、URL にポート番号を入力する必要はありません。

詳細は、『Sun ONE Application Server 7 セキュリティ管理者ガイド』の「SSL と TLS の有効化」の節を参照してください。次の URL で参照できます。
`http://docs.sun.com/source/816-6482/sgencryp.html#293273`

Sun ONE Directory Server 5.2 のインストールおよび構成

この節では、ボードを使用するために Sun ONE Directory Server 5.2 をインストールおよび構成する方法について説明します。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 ディレクトリサーバーのインストールおよび使用方法については、Sun ONE ディレクトリサーバーのマニュアルを参照してください。この節の内容は、次のとおりです。

Sun ONE Directory Server 5.2 のインストール

この手順では、ディレクトリサーバーのソフトウェアをコマンド行からインストールします。

▼ Sun ONE Directory Server 5.2 をインストールする

1. **Sun ONE Directory Server 5.2 ソフトウェアをダウンロードします。**

   ディレクトリ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. **インストールディレクトリに移動します。**

3. **`./idsktune` コマンドを実行して、推奨パッチがインストールされていることを確認します。**

4. **ディレクトリサーバーソフトウェアを解凍します。**

5. **`setup` スクリプトを実行して、ソフトウェアをインストールします。**

注 – `setup` スクリプトでは、すべてのパッケージがインストールされるため、個々のパッケージをインストールする必要はありません。

インストール後、Sun ONE ディレクトリサーバーと管理サーバーが自動的に起動されます。

手動でディレクトリサーバーを起動する方法

1. 起動ディレクトリに移動します。

```
# cd /var/Sun/mps
```

2. `start-admin` コマンドを実行します。

```
# ./start-admin
```

3. `slapd-`*servername* ディレクトリに移動します。

```
# cd slapd-servername
```

servername には、インスタンス名を指定します。

4. `start-slapd` コマンドを実行します。

```
# ./start-slapd
```

Sun ONE Directory Server 5.2 の構成

以降の手順では、ディレクトリサーバーのインスタンスに対する認証データベースの作成、ディレクトリサーバーで使用するボードの登録、ルート CA 証明書の確認とインストール、およびディレクトリサーバーでの SSL の有効化を行います。

構成処理中は、構成ディレクトリおよび Sun ONE ディレクトリサーバーの管理サーバーが起動し、動作している必要があります。

▼ 認証データベースを作成する

この手順では、Sun Crypto Accelerator 4000 モジュールを追加します。32 ビット版と 64 ビット版のインストール手順は同じです。

1. ディレクトリサーバーのコンソールを起動します。

2. 構成するディレクトリサーバーのインスタンスを選択して、メインコンソールウィンドウで「Open」を選択します。

3. 表示された新しいウィンドウで、「Console」→「Security」→「Manage Certificates」を選択します。

   この手順では、ディレクトリ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. パスワードを選択して 2 つのボックスに入力し、「OK」をクリックします (図 5-9 を参照)。

   b. 「Manage Certificates」ダイアログボックスが表示されるので、これを閉じます。

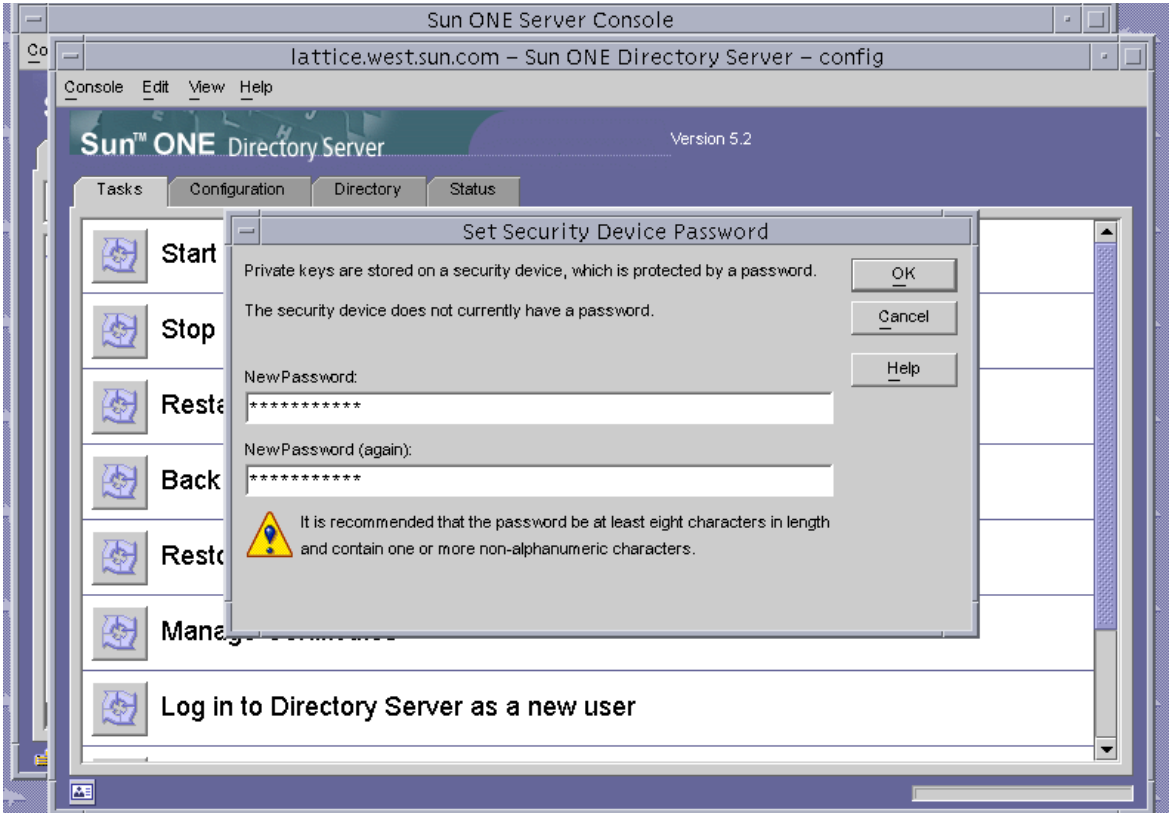

図 5-9　Sun ONE ディレクトリサーバーの「Set Security Device Password」ダイアログボックス

4. 表示された新しいウィンドウで、「Console」→「Security」→「Configure Security Modules」を選択します。

a. 「Install」をクリックします。

b. 「Enter the PKCS#11 module driver filename」エントリに次のパスを入力します。

```
/opt/SUNWconn/cryptov2/lib/libvpkcs11.so
```

5. 「Enter an identifying name for this module」エントリに名前を入力します。次に例を示します。

```
Sun Crypto Accelerator 4000
```

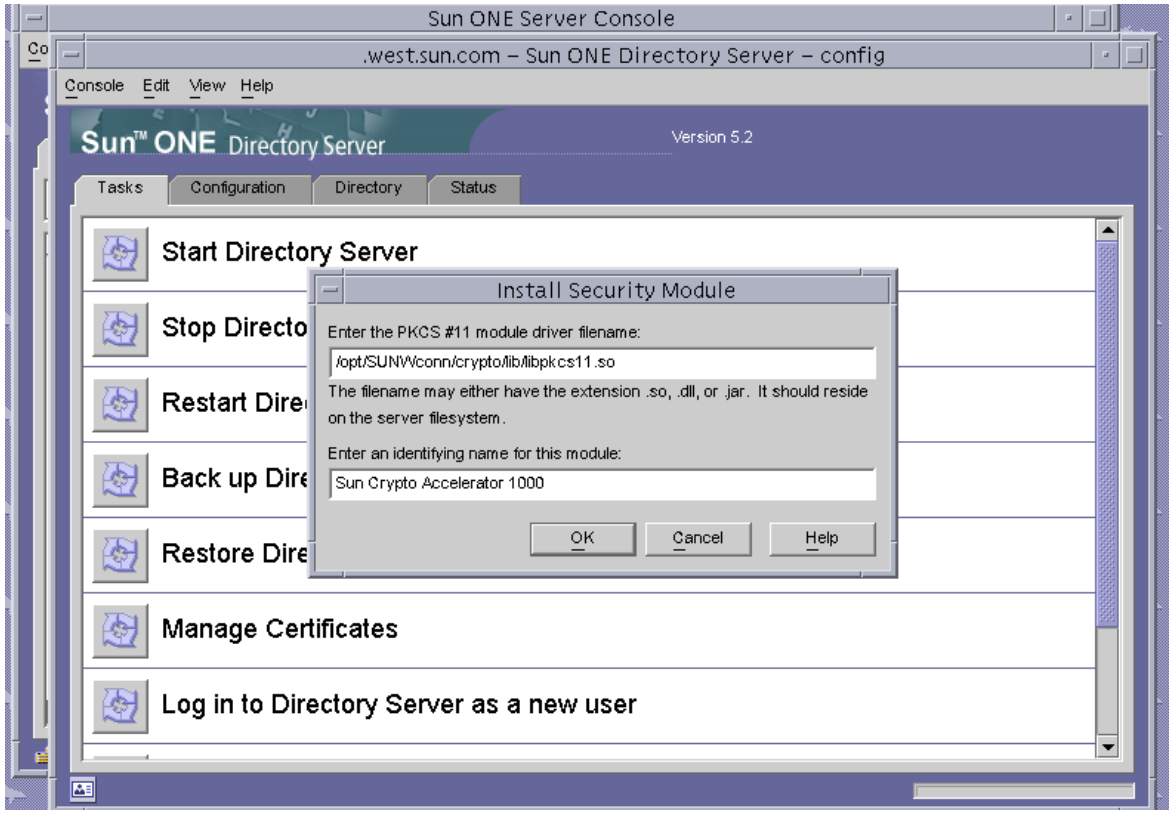

図 5-10　Sun ONE ディレクトリサーバーの「Install Security Module」ダイアログボックス

6. 「OK」をクリックします。

▼ ディレクトリサーバーで使用するボードを登録する (32 ビット版)

この手順では、32 ビット版のボードモジュールをコマンド行から追加します。

1. 次のコマンドを入力して、適切なパスを設定します。

```
# setenv LD_LIBRARY_PATH server-inst/lib:${LD_LIBRARY_PATH}
```

2. ボードを secmod.db データベースに追加します。

a. 次のディレクトリに移動します。

```
# cd server-inst/alias
```

b. modutil ユーティリティーを使用して、ライブラリを追加します。

```
# server-inst/shared/bin/modutil -dbdir . -nocertdb -add "Sun Crypto Acclerator
4000" -libfile /opt/SUNWconn/cryptov2/lib/libvpkcs11.so
```

▼ ディレクトリサーバーで使用するボードを登録する (64 ビット版)

この手順では、64 ビット版のボードモジュールをコマンド行から追加します。

1. 64 ビット版の Netscape Security Services (NSS) ユーティリティーを http://www.mozilla.org から取得します。

```
ftp://ftp.mozilla.org/pub/mozilla.org/security/nss/releases/NSS_3_3_2_RTM/SunO
S5.8_64_OPT.OBJ/
```

tar ファイル nss-3.3.2.tar.gz を保存します。

2. 次のコマンドを入力して、適切なパスを設定します。

注 – この節では、*server-inst* は製品のルートインストールディレクトリを指し、*nss64-inst* は 64 ビット版の NSS ツールをインストールした位置を指します。

```
# setenv LD_LIBRARY_PATH server-inst/lib/64:${LD_LIBRARY_PATH}
```

3. ボードを secmod.db データベースに追加します。

a. alias ディレクトリに移動します。

```
# cd server-inst/alias
```

b. ライブラリを追加します。

```
# nss64-inst/bin/modutil -dbdir . -nocertdb -add "Sun Crypto Acclerator 4000"
-libfile /opt/SUNWconn/cryptov2/lib/64/libvpkcs11.so
```

サーバーの証明書の生成およびインストール

表 5-8 に示すパスの変数が異なっていること以外は、32 ビット版と 64 ビット版の PKCS#11 ライブラリのインストール手順は同じです。

表 5-8　32 ビット版および 64 ビット版のパスの変数の違い

変数定義	32 ビット	64 ビット
LD_LIBRARY_PATH	*server-inst*/lib	*server-inst*/lib/64
NSS ツールの位置	*server-inst*/shared/bin	*nss64-inst* (NSS ツールをインストールした位置)

表 5-9 に、この手順で使用する certutil コマンドの変数を示します。

表 5-9　certutil の変数の説明

変数	説明
token-name	PKCS#11 トークンの名前。ボードを初期化したときに選択したキーストアの名前です。
subject-name	デジタル証明書に記載される名前。通常は、次の形式で記載されます。 CN=*Fully-Qualified-Domain-Name*,OU=*Organization-Unit*,O=*Organization*. 名前は、組織によって変わる場合があります。
output-file	証明書要求の位置
certfile	ASCII 符号化形式の証明書の位置
instname	ディレクトリサーバーのインスタンス名
nickname	ユーザーが選択した、サーバーの証明書のフレンドリ名

▼ サーバーの証明書を生成する

1. 次のディレクトリに移動します。

```
# cd server-inst/alias
```

2. 証明書を要求します。

```
# certutil -R -d . -h token-name -s "subject-name" -a -o output-file [-g key-size] -P
slapd-instname-
```

3. *output-file* の証明書要求を、選択した認証局に送信します。

   base64 符号化形式の証明書を、*certfile* という名前のテキストファイルに書き込みます。

▼ サーバーの証明書をインストールする

1. サーバーの証明書をインストールします。

```
# certutil -A -d . -h token-name -t "Pu,Pu,Pu" -P slapd-instname- -a -i certfile -n
nickname
```

ルート CA 証明書の確認およびインストール

Sun ONE ディレクトリサーバーには、現在認証されている、公知のルート認証局証明書がいくつか含まれています。使用するサーバーの証明書が既知のルート CA のいずれかによって発行されている場合は、この手順は省略してください。

▼ ディレクトリサーバーに認識されるルート CA 証明書を確認する

1. ディレクトリサーバーのコンソールウィンドウから、ボードのディレクトリサーバーインスタンスを開きます。
2. コンソールウィンドウの上部のメニューで、「Console」→「Security」→「Manage Certificates」を選択します。
3. 「Manage Certificates」ウインドウの上部にある「CA Certs」タブを選択します。

   Sun ONE ディレクトリサーバーのインスタンスが認識する CA 証明書のリストが表示されます。エントリを選択して、「Detail」ボタンをクリックすると、選択した CA 証明書の詳細情報を確認できます。

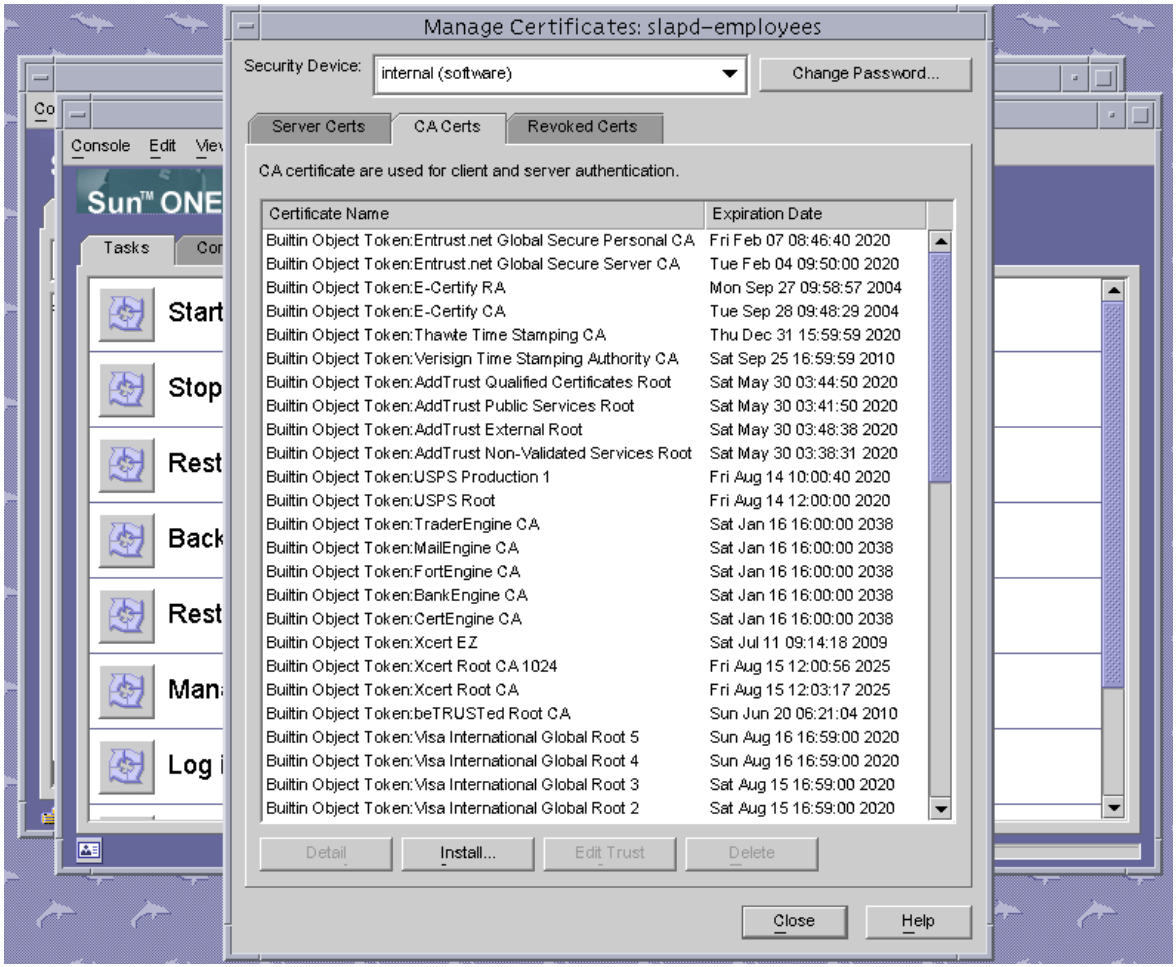

図 5-11　Sun ONE ディレクトリサーバーの「Manage Certificates」ダイアログボックス

▼ ルート CA 証明書をインストールする

次の手順は、専用の PKI から証明書を取得する場合にのみ実行します。したがって、VeriSign、Thawte、または GTE を使用する場合は、この手順を実行しないでください。主要ベンダーによって発行された証明書に、Sun ONE のデフォルトの認証 CA リストにインストールされていない中間 CA がある場合は、この手順が必要です。

1. alias ディレクトリに移動します。

```
# cd server-inst/alias
```

2. ルート CA 証明書をインストールします。

注 – 複数の CA 証明書をインストールする場合は、-n に異なる値を指定します。-n に同じ値を指定すると、証明書は相互に上書きされます。CA-Cert を、CA 証明書の対象者名の CommonName 構成要素の内容に置き換えてください。CommonName の内容は、SubjectName で CN= を検索すると参照できます。

```
# certutil -A -d . -P slapd-instname- -n "CA-Cert" -t "CT,CT,CT" -a -i path-to-ca-cert
```

▼ ディレクトリサーバーで SSL を使用可能にする

1. ディレクトリサーバーのコンソールをまだ起動してない場合は、起動します。

```
# ./cd server-root
# ./startconsole
```

2. メインコンソールウィンドウの左側のパネルにあるボードのディレクトリサーバーインスタンスをダブルクリックして、ディレクトリサーバーインスタンスを開きます。
3. メインコンソールウィンドウの「Directory」タブをクリックします。
4. 「Directory」タブの左側のパネルにある cn=config エントリを開いて、次のパラメタを変更します (図 5-12 を参照)

   a. nsslapd-security に on を設定します。

   b. nsslapd-secureport に適切なポート (デフォルトは 636) を設定します。

c. 「OK」をクリックします。

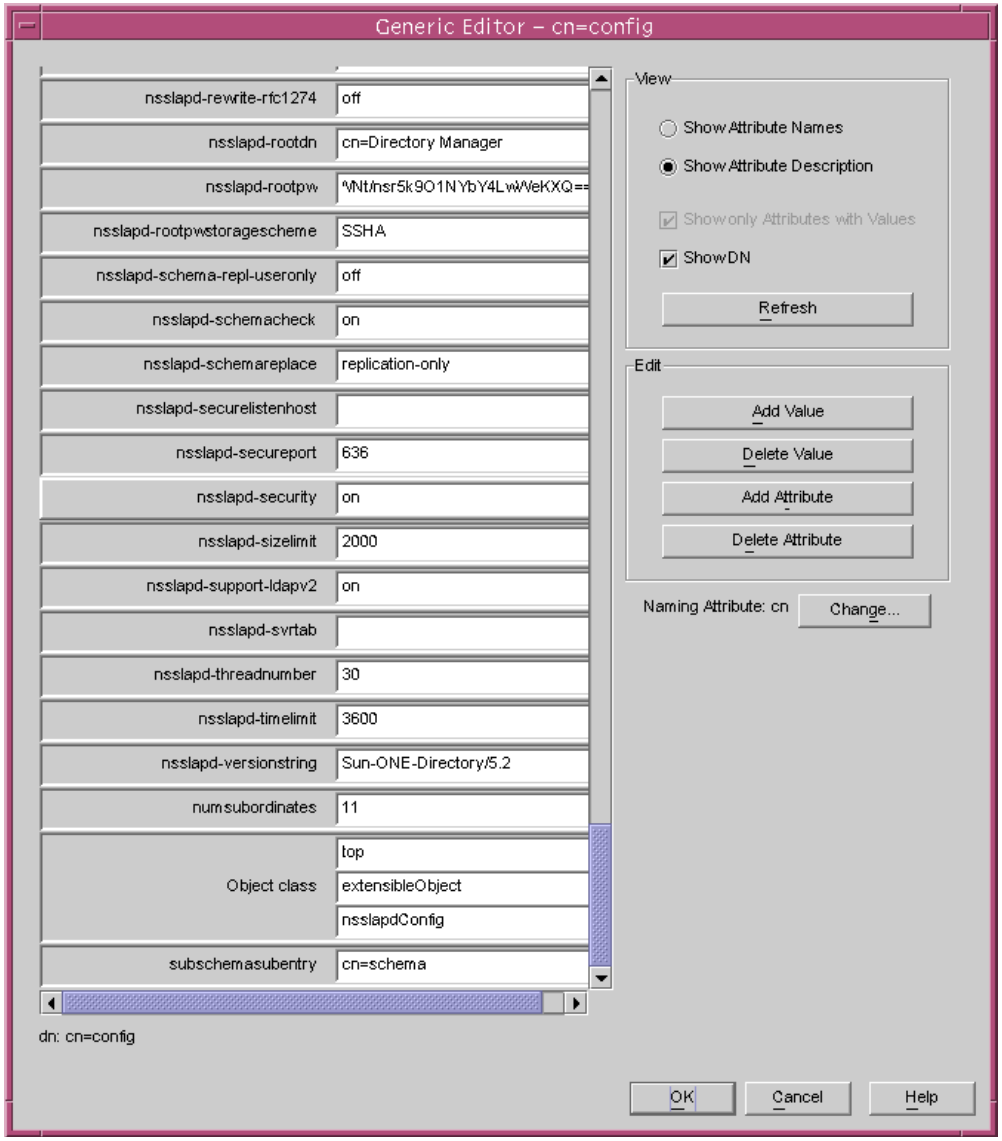

図 5-12　Sun ONE ディレクトリサーバーの `cn=config` の編集用ダイアログボックス

5. メインコンソールウィンドウの左側のパネルにある `cn=encryption,cn=config` エントリを開いて、次のパラメタを変更します (図 5-13 を参照)。

   a. `nsssl3` に on を設定します。

b. 「Add Attribute」ボタンを使用して、値に `alias/slapd-`*instname*`-cert8.db` を指定した `nsCertFile` を追加します。

c. 「Add Attribute」ボタンを使用して、値に `alias/slapd-`*instname*`-key3.db` を指定した `nsKeyFile` を追加します。

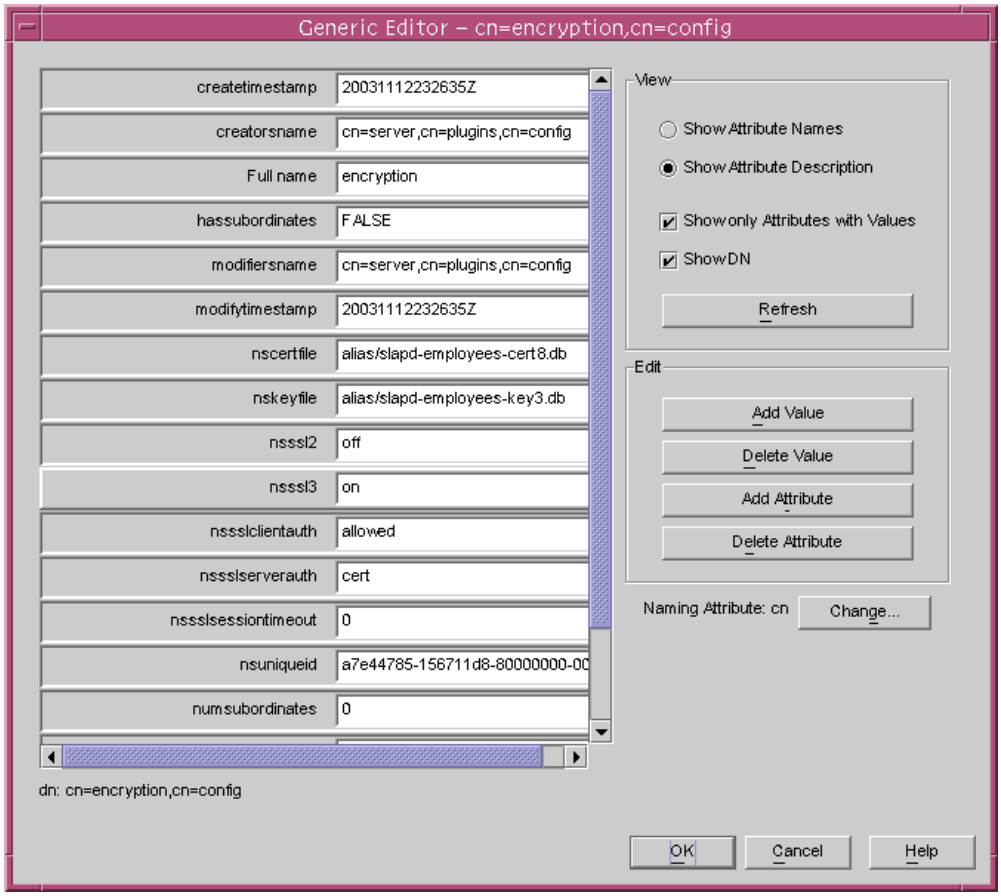

図 5-13　Sun ONE ディレクトリサーバーの `cn=encryption,cn=config` のダイアログボックス

d. 「OK」をクリックします。

6. データベースの `cn=encryption,cn=config` の下に新しいエントリを作成します。

a. メインウィンドウで暗号アイコンを右クリックし、メニューから「New」→「Other」を選択します。

b. `nsEncryptionModule` を選択します。

c. 「Full name」属性の値を、「New」から「RSA (Remote Security Access)」に変更します (図 5-14 を参照)。

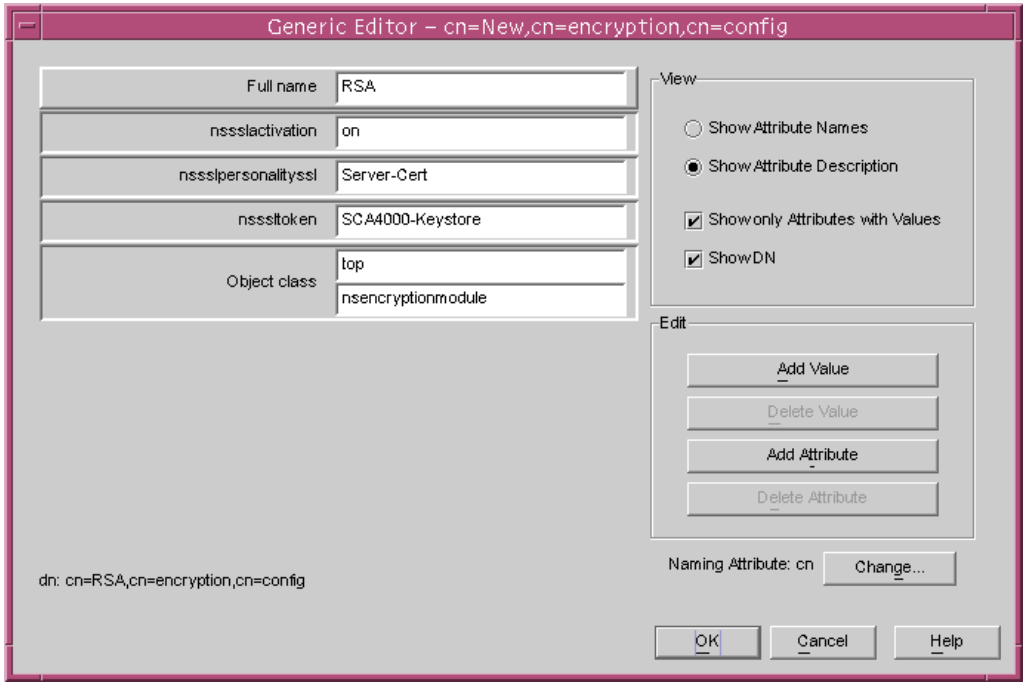

図 5-14　Sun ONE ディレクトリサーバーの nsEncryption モジュールのダイアログボックス

d. 「Add Attribute」ボタンを使用して、次の属性と値を追加します。

nsssltoken	*token-name*
nsslpersonalityssl	*nickname*
nssslactivation	on

e. 「OK」をクリックします。

Sun ONE Messaging Server 5.2 のインストールおよび構成

この節では、ボードを使用するために Sun ONE Messaging Server 5.2 をインストールおよび構成する方法について説明します。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 メッセージングサーバーのインストールおよび使用方法については、Sun ONE メッセージングサーバーのマニュアルを参照してください。この節の内容は、次のとおりです。

Sun ONE Messaging Server 5.2 のインストール

この手順では、Sun ONE Messaging Server 5.2 をコマンド行からインストールします。

▼ Sun ONE Messaging Server 5.2 をインストールする

1. Sun ONE Messaging Server 5.2 ソフトウェアをダウンロードします。

   メッセージング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. インストールディレクトリに移動して、メッセージングサーバーソフトウェアを解凍します。

3. `setup` スクリプトを使用して、メッセージングサーバーソフトウェアをインストールします。

   a. プロンプトが表示されたら、インストールパスを入力します。

   b. プロンプトが表示されたら、インストールするコンポーネントを入力します。

   c. `./setup` コマンドを実行して、コンポーネントをインストールします。

Sun ONE Messaging Server 5.2 の構成

以降の手順では、メッセージングサーバーのインスタンスに対する認証データベースの作成、メッセージングサーバーで使用するボードの登録、サーバーの証明書の生成とインストール、およびメッセージングサーバーでの SSL の有効化を行います。

構成処理中は、構成ディレクトリおよび Sun ONE メッセージングサーバーの管理サーバーが起動し、動作している必要があります。

▼ 認証データベースを作成する

1. メッセージングサーバーのコンソールを起動します。
2. Sun ONE メッセージングサーバーのインスタンスを開きます。

   図 5-15 に示すメニューが表示されます。

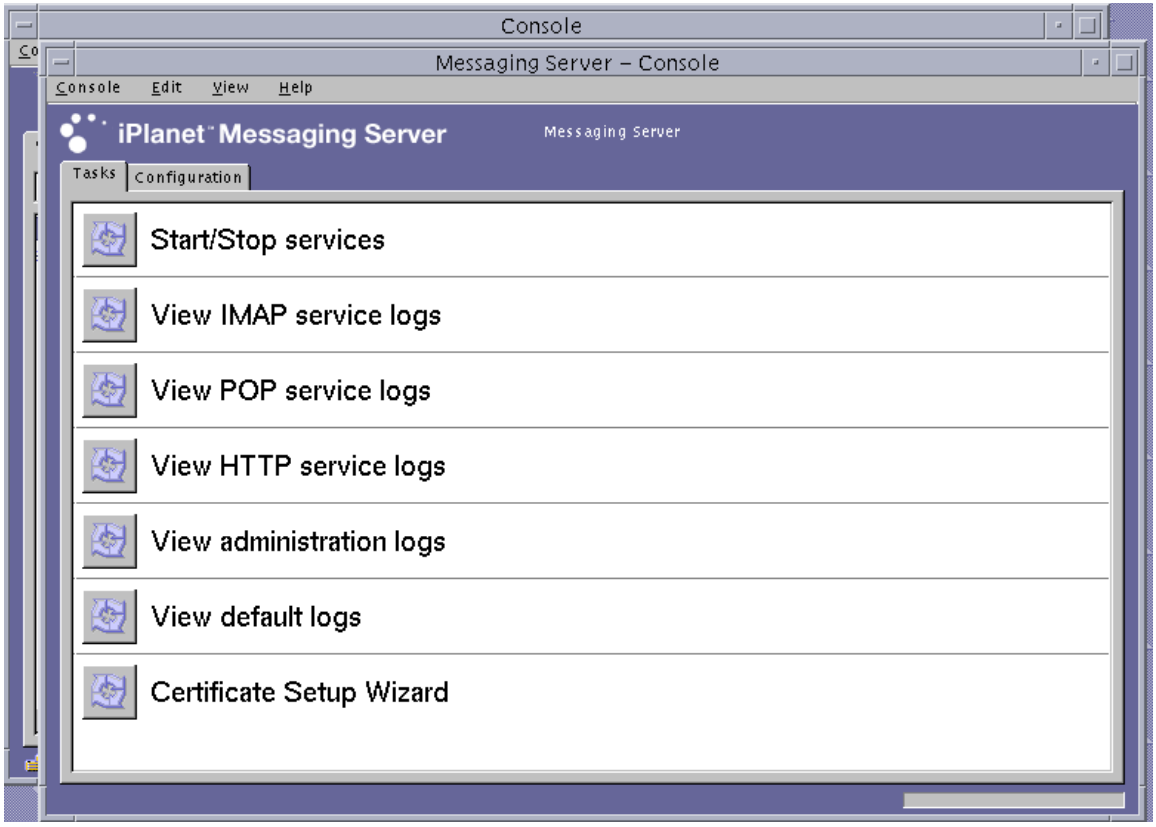

図 5-15　Sun ONE メッセージングサーバーのメインコンソールウィンドウ

3. 「Console」→「Certificate Setup Wizard」を選択します。

   「Certificate Setup Wizard」が表示されます。

   a. 「Next」をクリックします。

   b. 「internal (software)」トークンを選択します。

   c. 「Do not install a certificate」を選択して、「Next」をクリックします。

   d. 「Next」をクリックします。

   e. 内部データベースのパスワードを設定して、「Next」をクリックします。

   f. 「Done」をクリックします。

▼ メッセージングサーバーで使用するボードを登録する

1. 次のディレクトリに移動します。

```
# cd server-root/shared/bin
```

2. LD_LIBRARY_PATH 変数が正しく設定されていることを確認します。

```
# setenv LD_LIBRARY_PATH server-root/lib:${LD_LIBRARY_PATH}
```

3. ボードモジュールを secmod.db データベースに追加します。

```
# ./modutil -dbdir ../../admin-serv/config \
-nocertdb \
-add "Sun Crypto Accelerator 4000" \
-libfile "/opt/SUNWconn/cryptov2/lib/libvpkcs11.so"
```

▼ サーバーの証明書を生成する

1. メッセージングサーバーのコンソールから、「Certificate Setup Wizard」を開いて証明書を要求します。「Console」->「Certificate Setup Wizard」を選択します。

   a. 「Next」をクリックします。

   b. 鍵を保存する Sun Crypto Accelerator 4000 のトークンと一致するトークンを選択します (図 5-16 を参照)。

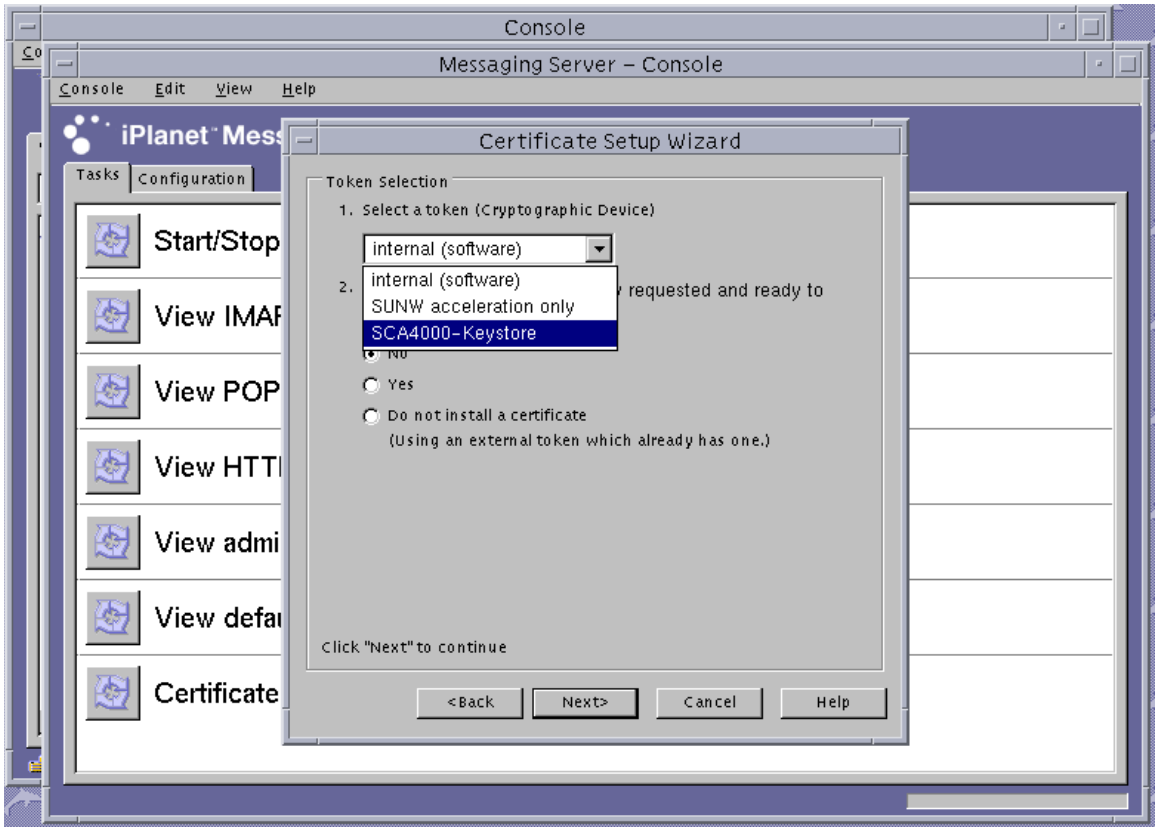

図 5-16　Sun ONE メッセージングサーバーの「Certificate Setup Wizard」の「Token Selection」ダイアログボックス

c. 「Is the certificate already requested and ready to install?」に「No」と答えて、「Next」をクリックします。

d. 「Next」をクリックします。

e. 「New Certificate」を選択し、証明書要求を認証局に送信する方法 (電子メールまたは HTTPS) を選択して (図 5-17)、「Next」をクリックします。

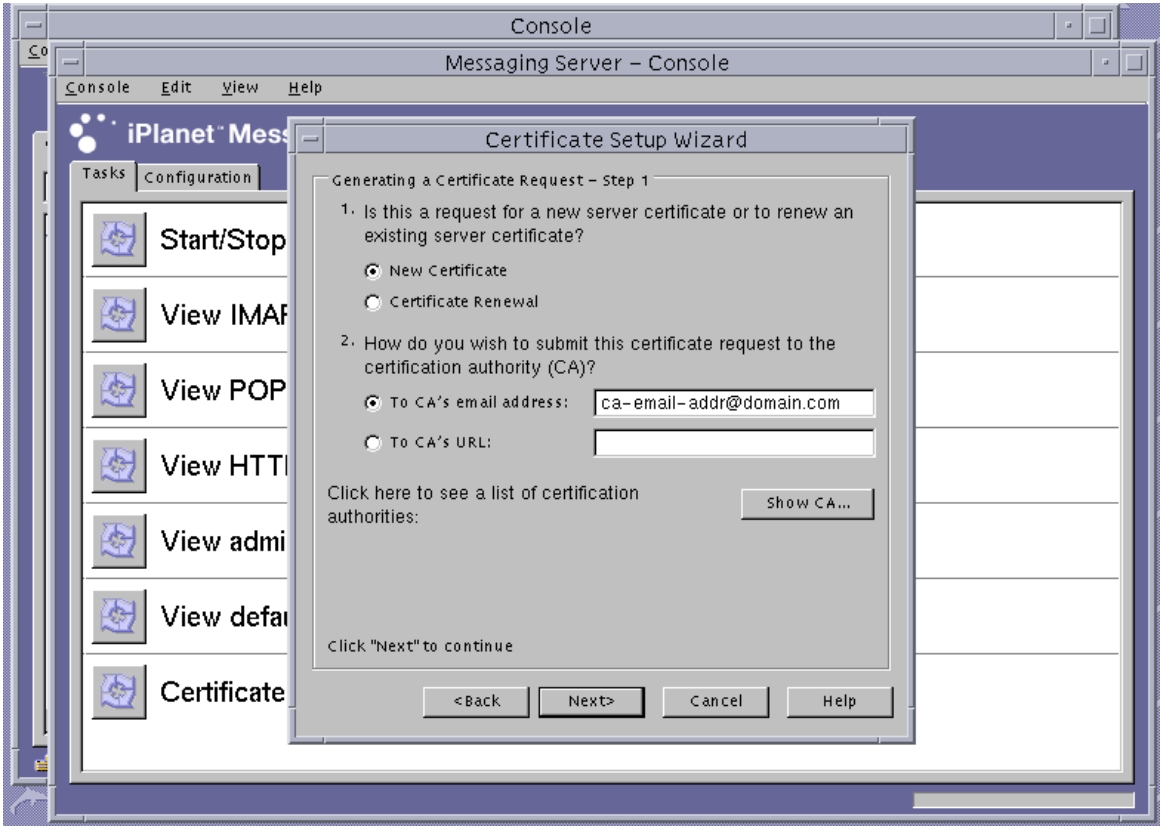

図 5-17　Sun ONE メッセージングサーバーの「Certificate Setup Wizard」の証明書要求ダイアログボックス

f. 表 5-10 に示す要求者情報フィールドに適切な情報を入力し、「Next」をクリックします。

表 5-10　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

表 5-10　要求者情報フィールド (続き)

フィールド	説明
Organization	会社名
Organizational Unit	(任意) 会社の部門
Locality	(任意) 市区町村
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)

g. **画面に、認証データベースの作成時に使用したパスワードの入力を要求するメッセージが表示されます。このパスワードの代わりに、キーストアユーザーのパスワード (*username:password*) を入力して、「Next」をクリックします。**

username:password の詳細は、表 5-1 を参照してください。

h. 手順 e で HTTPS を選択した場合は、すでに要求は CA に送信されています。手順 e で電子メールを選択した場合は、「Copy to Clipboard」をクリックしてから、「Next」をクリックします (図 5-18)。

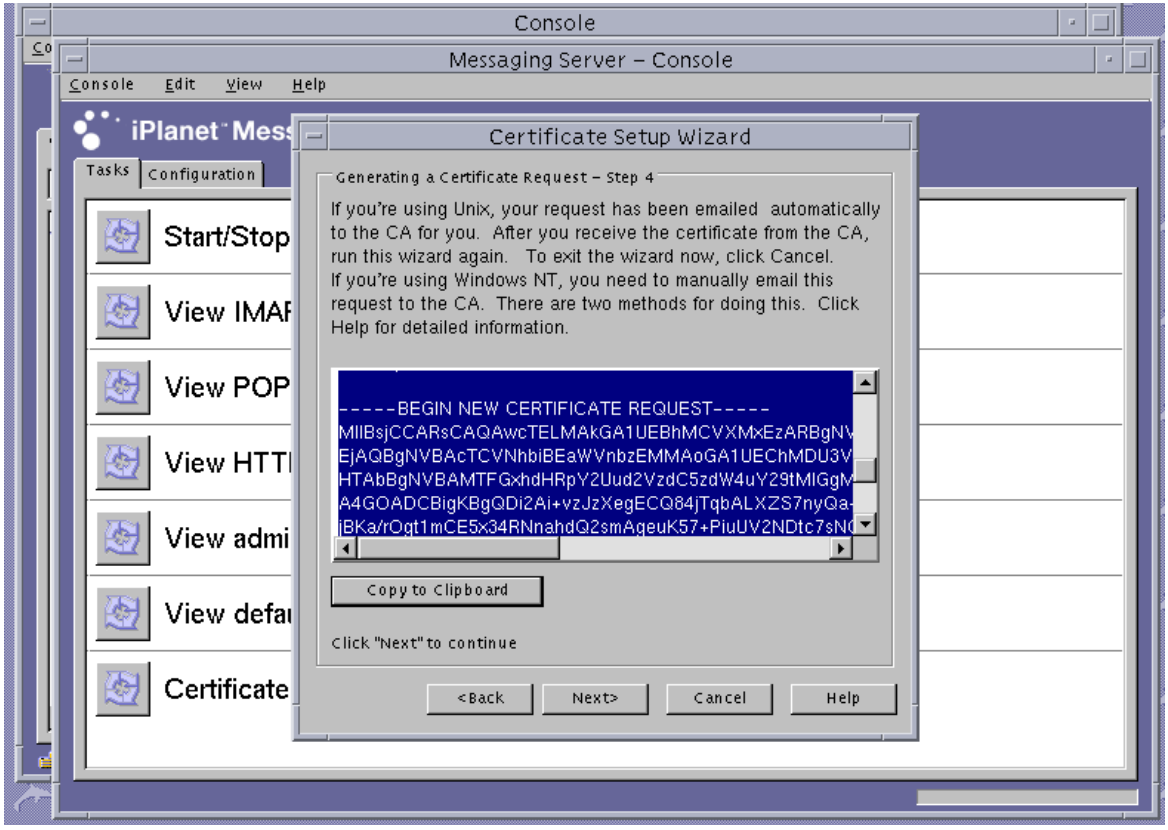

図 5-18　Sun ONE メッセージングサーバーの「Certificate Setup Wizard」の証明書送信ダイアログボックス

i. 「Next」をクリックします。

注 – 証明書を要求したあと、「Certificate Setup Wizard」を続けて使用して、発行された証明書を Sun Crypto Accelerator 4000 キーストアにインストールできます。生成された証明書をインストールする前に「Certificate Setup Wizard」を終了した場合は、「Certificate Setup Wizard」を再起動して、中止したところから操作を再開できます。

▼ サーバーの証明書をインストールする

1. サーバーの証明書を生成する手順の途中で「Certificate Setup Wizard」を終了した場合は、「Console」->「Certificate Setup Wizard」を選択してウィザードを再起動し、最初の画面で「Next」をクリックします。
2. 証明書をインストールする Sun Crypto Accelerator 4000 のトークンと一致するトークンを選択します。

   このトークンは、要求を生成したときと同じトークンである必要があります。
3. サーバーの証明書をインストールする準備ができているかどうかの質問に「Yes」と答えて、「Next」をクリックします。
4. 「Next」をクリックします。

5. 証明書のインストール先に「This Server」を選択し、ウィザードによって提供されていない場合はキーストアのパスワード (*username:password*) を入力して、「Next」をクリックします (図 5-19 を参照)。

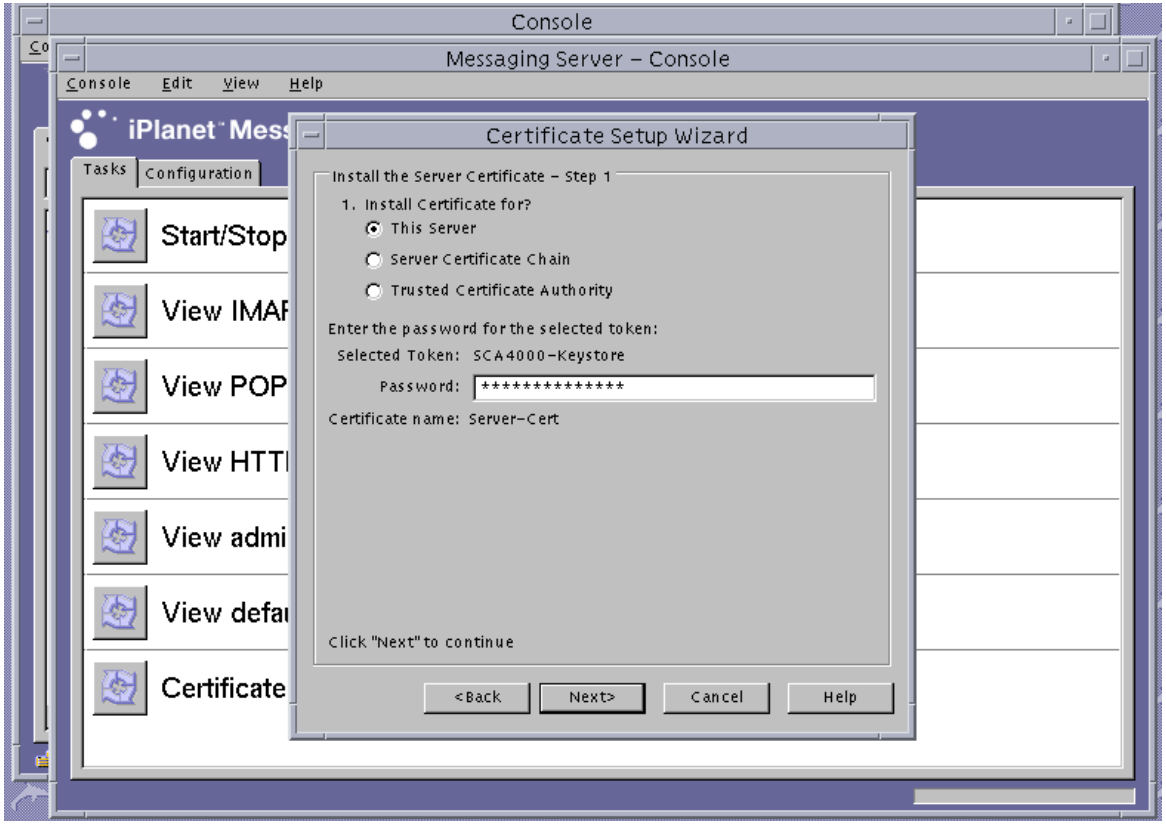

図 5-19　Sun ONE メッセージングサーバーの「Certificate Setup Wizard」のパスワードダイアログボックス

注 – 証明書のデフォルトの名前は `Server-Cert` です。

---

6. base64 符号化形式の証明書をクリップボードにコピーして、「The certificate is located in the following text field」のラベルの付いたテキストボックスにペーストします (図 5-20 を参照)。

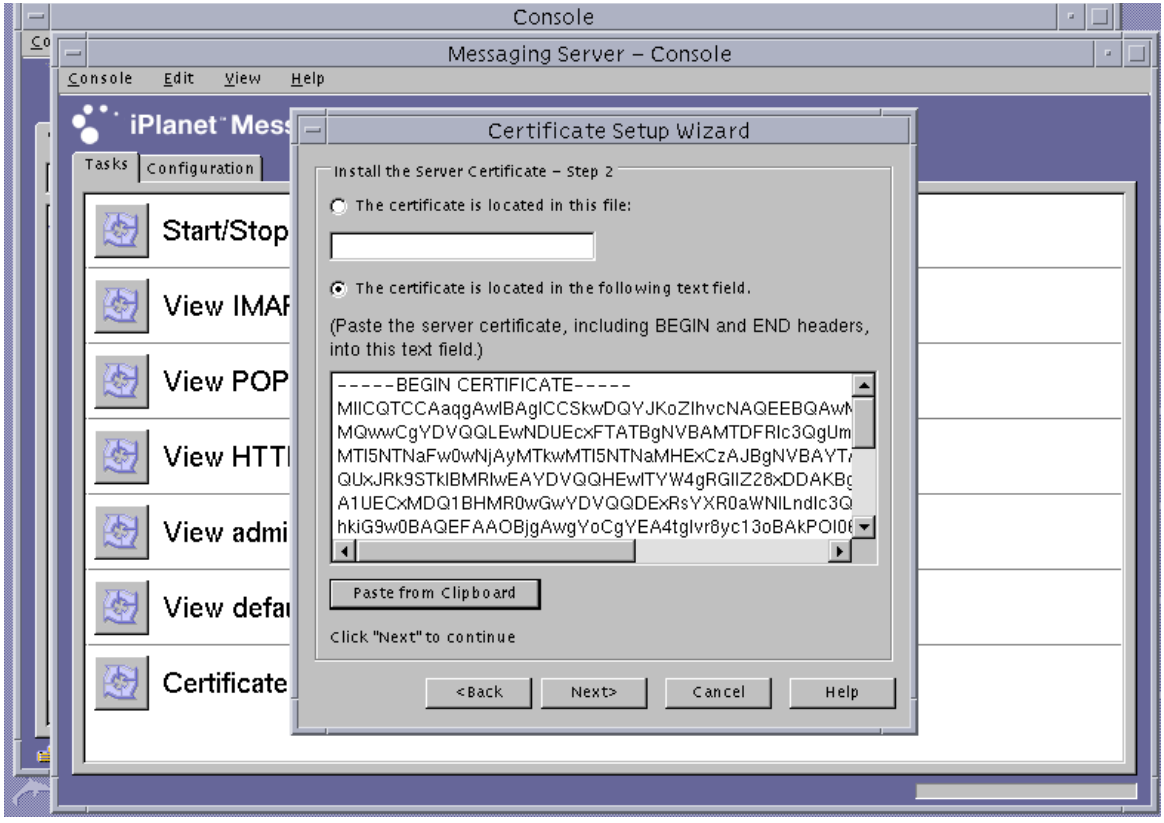

図 5-20　Sun ONE メッセージングサーバーの「Certificate Setup Wizard」の証明書入力ダイアログボックス

a. 「Add」をクリックして証明書を追加します。

b. 「Done」をクリックします。

7. ルート CA 証明書を追加します (メッセージングサーバーがすでに認証しているルート認証局の証明書ではない場合)。

この手順には、「Certificate Setup Wizard」を使用します。

a. メッセージングサーバーのコンソールから、「Console」→「Certificate Setup Wizard」を選択します。

b. 「Next」をクリックします。

c. トークンに「internal (software)」を選択して「Is the certificate already requested and ready to install?」で「Yes」をクリックし、「Next」をクリックします。

d. 「Next」をクリックします。

e. 「Trusted Certificate Authority」を選択して、「Next」をクリックします。

f. base64 符号化形式の CA 証明書をクリップボードにコピーして、「The certificate is located in the following text field」のラベルの付いたテキストボックスにペーストし、「Next」をクリックします。

g. 「Add」をクリックして証明書を追加します (図 5-21)。

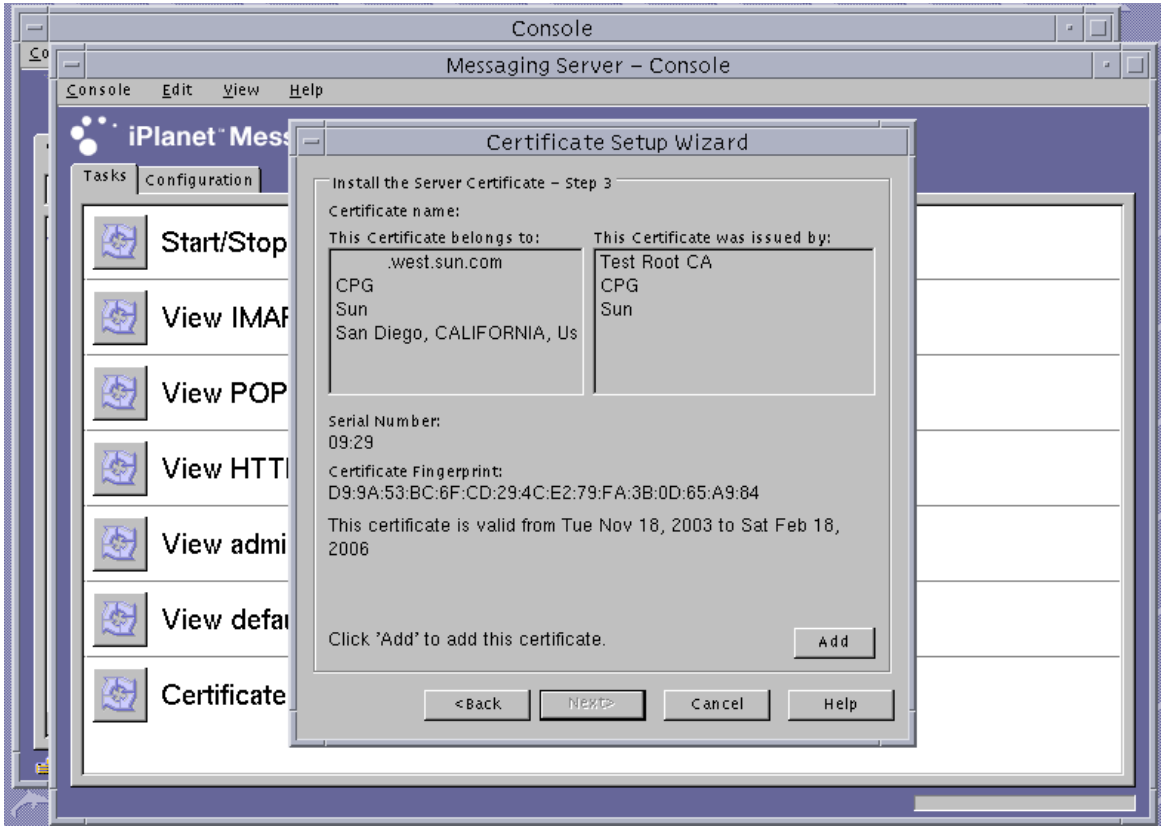

図 5-21　Sun ONE メッセージングサーバーの「Certificate Setup Wizard」のパスワードダイアログボックス

h. 「Done」をクリックします。

▼ メッセージングサーバーで SSL を使用可能にする

1. su コマンドを使用して、メッセージングサーバーの実行用に選択したユーザーになります。

   このユーザー名を忘れた場合は、*server-root*/msg-*instname*/config/msg.conf ファイルで local.serveruid プロパティーを検索すると、ユーザー名を確認できます。

```
# cd server-root/msg-instname
# su username
```

2. configutil ツールを使用して、メッセージングサーバーの SSL パラメタを設定します。

   表 5-11 に、configutil ツールで使用する変数の定義を示します。

表 5-11 configutil 変数

変数	定義
keystorename	手順 1 で使用したキーストア名
certname	使用する証明書のフレンドリ名。デフォルトは Server-Cert です。
portnumber	POP3 over SSL を実行するポート番号。通常は、995 です。

```
# ./configutil -o nsserversecurity -v on
# ./configutil -o encryption.rsa.nssslactivation -v on
# ./configutil -o encryption.rsa.nsssltoken -v keystorename
# ./configutil -o encryption.rsa.nssslpersonalityssl -v certname
# ./configutil -l -o service.pop.enablesslport -v yes
# ./configutil -l -o service.pop.sslport -v portnumber
```

3. メッセージングサーバーのコンソールで、Sun ONE メッセージングサーバーインスタンスの管理に使用するコンソールウィンドウの「Configuration」タブをクリックします。「Messaging Server」->「Services」->「IMAP」の順に選択し、「System」タブをクリックします。

4. 前述のウィンドウで、「Use separate port for IMAP over SSL」のポート番号を設定します。デフォルトでは、このポートは 993 です。

5. メッセージングサーバーインスタンスの sslpassword.conf ファイルを構成します。

```
# cd server-root/msg-instname/config
# vi sslpassword.conf
```

Internal (Software) token:netscape! の行を、*tokenname*:*username:password* に置き換えます。*tokenname* には、キーストア名を指定します。この *tokenname* は、手順 1 で鍵を生成するために選択したトークンの名前です。*username:password* は、このトークンを認証するために使用します。*username:password* の詳細は、表 5-1 を参照してください。

6. sslpassword.conf ファイルの所有権およびアクセス権を変更します。

sslpassword.conf ファイルには鍵素材の認証に使用されるパスワード情報が含まれているため、デーモンを実行するユーザーがこのファイルを所有して、そのユーザーのみがこのファイルを読み取ることができるように設定する必要があります。

```
# cd server-root/msg-instname/config
# chown msg-user sslpassword.conf
# chmod 0400 sslpassword.conf
```

7. コマンド行からサーバーを再起動します。

```
# cd server-root
# msg-instname/start-msg
```

Sun ONE Portal Server 6.2 のインストールおよび構成

この節では、ボードを使用するために Sun ONE Portal Server 6.2 をインストールおよび構成する方法について説明します。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 ポータルサーバーのインストールおよび使用方法については、Sun ONE ポータルサーバーのマニュアルを参照してください。この節の内容は、次のとおりです。

- 173 ページの「Sun ONE Portal Server 6.2 のインストール」
- 174 ページの「Sun ONE Portal Server 6.2 の構成」
- 174 ページの「ポータルサーバーで使用するボードを登録する」
- 118 ページの「サーバーの証明書を生成する」

- 120 ページの「サーバーの証明書をインストールする」
- 176 ページの「ポータルサーバーに認識されるルート CA 証明書を確認する」
- 176 ページの「ルート CA 証明書をインストールする」
- 177 ページの「ポータルサーバーで SSL を使用可能にする」

Sun ONE Portal Server 6.2 には、Sun ONE Web Server 6.0 が含まれています。ポータルサーバーをインストールおよび構成する前に、Sun ONE Web サーバーソフトウェアをインストールおよび構成する必要があります (124 ページの「Sun ONE Web Server 6.0 のインストールおよび構成」を参照)。

注 – ポータルサーバーと併用するために Sun ONE Web サーバーをインストールおよび構成する場合は、インストールパスに `/opt/SUNWam/servers` を使用してください。

Sun ONE Portal Server 6.2 のインストール

ここでは、Sun ONE Portal Server 6.2 をコマンド行からインストール方法について説明します。

▼ Sun ONE Portal Server 6.2 をインストールする

1. **Sun ONE Portal Server 6.2 ソフトウェアをダウンロードします。**

   ポータル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. **インストールディレクトリに移動して、ポータルサーバーソフトウェアを解凍します。**

3. **`setup` スクリプトを使用して、ポータルサーバーソフトウェアをインストールします。**

   a. **プロンプトが表示されたら、インストールパスを入力します。**

   b. **プロンプトが表示されたら、インストールするコンポーネントを入力します。**

   c. **`./setup` コマンドを実行して、コンポーネントをインストールします。**

注 – 認証データベースは、インストール時に自動的に作成されます。

Sun ONE Portal Server 6.2 の構成

以降の手順では、ポータルサーバーの Secure Remote Access (SRA) ゲートウェイの構成、ポータルサーバーで使用するボードの登録、サーバーの証明書の生成とインストール、およびポータルサーバーでの SSL の有効化を行います。

この手順を始める前に、SRA がインストールされていることと、ゲートウェイサーバーの証明書 (自己署名済または CA が発行したもの) がインストールされていることを確認してください。構成処理中は、Sun ONE ポータルサーバーの管理サーバーが起動し、動作している必要があります。

▼ ポータルサーバーで使用するボードを登録する

1. vcaadm ユーティリティーを使用して、ボードの新しいユーザーアカウントを作成します (59 ページの「vcaadm ユーティリティーの使用」を参照)。

```
vcaadm{vca0@localhost, sec-officer}> create user
New user name: username
Enter new user password:
Confirm password:
User crypta created successfully.
```

2. Sun Crypto Accelerator 4000 モジュールを読み込みます。

   LD_LIBRARY_PATH 変数が次のパスを指している必要があります。

```
/usr/lib/mps/secv2/
```

   a. モジュールを読み込みます。

```
# /usr/bin/mps/modutil -dbdir /etc/opt/SUNWps/cert/default -add "Sun Crypto
Accelerator 4000" -libfile /opt/SUNWconn/cryptov2/lib/libvpkcs11.so
```

   b. このモジュールが読み込まれていることを確認します。

```
# /usr/bin/mps/modutil -list -dbdir /etc/opt/SUNWps/cert/default -nocertdb
```

サーバーの証明書の生成およびインストール

この手順を実行するときは、LD_LIBRARY_PATH 環境変数が次のパスを指している必要があります。

```
/usr/lib/mps/secv1/
```

表 5-9 に、この手順で使用する certutil コマンドの変数を示します。

表 5-12　certutil の変数の説明

変数	説明
token-name	PKCS#11 トークンの名前。ボードを初期化したときに選択したキーストアの名前です。
subject-name	デジタル証明書に記載される名前。通常は、次の形式で記載されます。 CN=*Fully-Qualified-Domain-Name*,OU=*Organization-Unit*,O=*Organization*. 名前は、組織によって変わる場合があります。
output-file	証明書要求の位置
certfile	ASCII 符号化形式の証明書の位置
instname	ポータルサーバーのインスタンス名
nickname	ユーザーが選択した、サーバーの証明書のフレンドリ名

▼ サーバーの証明書を生成する

1. 次のディレクトリに移動します。

```
# cd /etc/opt/SUNWps/cert/default
```

2. 証明書を要求します。

```
# /usr/bin/mps/bin/certutil -R -d . -h token-name -s "subject-name" -a -o output-file
[-g key-size]
```

3. *output-file* の証明書要求を、選択した認証局に送信します。

   base64 符号化形式の証明書を、*certfile* という名前のテキストファイルに書き込みます。

▼ サーバーの証明書をインストールする

1. サーバーの証明書をインストールします。

```
# /usr/bin/mps/certutil -A -d . -h token-name -t "Pu,Pu,Pu" -a -i certfile -n nickname
```

ルート CA 証明書の確認およびインストール

Sun ONE ポータルサーバーには、現在認証されている、公知のルート認証局証明書がいくつか含まれています。使用するサーバーの証明書が既知のルート CA のいずれかによって発行されている場合は、この手順は省略してください。

▼ ポータルサーバーに認識されるルート CA 証明書を確認する

- 次のコマンドを入力します。

```
# /usr/bin/mps/certutil -L -d /etc/opt/SUNWps/cert/default
```

▼ ルート CA 証明書をインストールする

次の手順は、専用の PKI から証明書を取得する場合にのみ実行します。したがって、VeriSign、Thawte、または GTE を使用する場合は、この手順を実行しないでください。主要ベンダーによって発行された証明書に、Sun ONE のデフォルトの認証 CA リストにインストールされていない中間 CA がある場合は、この手順が必要です。

1. 証明書のデータベースのディレクトリに移動します。

```
# cd /etc/opt/SUNWps/cert/default
```

2. ルート CA 証明書をインストールします。

注 – 複数の CA 証明書をインストールする場合は、`-n` に異なる値を指定します。`-n` に同じ値を指定すると、証明書は相互に上書きされます。`CA-Cert` を、CA 証明書の対象者名の CommonName 構成要素の内容に置き換えてください。CommonName の内容は、SubjectName で CN= を検索すると参照できます。

```
# /usr/bin/mps/certutil -A -d . -n "CA-Cert" -t "CT,CT,CT" -a -i path-to-ca-cert
```

▼ ポータルサーバーで SSL を使用可能にする

1. /etc/opt/SUNWps/cert/default/.nickname ファイルを作成します。

```
# vi /etc/opt/SUNWps/cert/default/.nickname
```

ファイルには、空白文字を入れずに次の行だけを含めます。

```
keystore-name:server-cert
```

2. 暗号の高速化を選択します。

注 – Sun Crypto Accelerator 4000 ハードウェアで DES および 3DES アルゴリズムを高速化するには、/etc/opt/SUNWconn/cryptov2/sslreg ファイルが存在する必要があります。詳細は、109 ページの「バルク暗号化の使用可能および使用不可の切り替え」を参照してください。

ボードは RSA 関数を高速化しますが、DES および 3DES 暗号の高速化のみをサポートします。これらの暗号のいずれかを有効にするには、次のように入力します。

```
Gateway >> Security >> Enable SSL Cipher Selection: >> SSL3
Ciphers: >>
SSL3_RSA_WITH_3DES_EDE_CBC_SHA or
SSL3_RSA_WITH_DES_CBC_SHA
```

3. /etc/opt/SUNWps/platform.conf.*gateway-profile-name* を変更して、ボードを使用可能にします。

```
gateway.enable.accelerator=true
```

4. 端末エミュレータから、ゲートウェイを再起動します。

```
# InstallDir/SUNWps/bin/gateway -n gateway-profile-name start
```

ゲートウェイは、キーストアのパスワードの入力を求めるプロンプトを表示します。*sra-keystore*:*username*:*password* の形式のパスワードまたは PIN を入力してください。

第6章

Apache Web サーバーソフトウェアのインストールおよび構成

この章では、Apache Web サーバーでボードを使用するためのインストールおよび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。

- 180 ページの「Apache Web サーバー 1.3x の構成」
- 186 ページの「Apache Web サーバー 2.x の構築および構成」
- 190 ページの「再起動時のユーザーの操作をなくすための、Apache Web サーバーの設定」
- 191 ページの「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 Apache と使用するように構成する方法」

次に、Apache Web サーバーでボードを使用するために必要なソフトウェアを示します。

- Apache Web サーバー 1.3.26 以降。Sun Crypto Accelerator 4000 ソフトウェアには、バージョン 1.3.26 が付属します。
- Solaris 8 用のパッチ 109234-09。`http://sunsolve.sun.com` より入手できます。
- Solaris 9 用のパッチ 113146-02。`http://sunsolve.sun.com` より入手できます。
- `SUNWkcl2a` パッケージ。Sun Crypto Accelerator 4000 ソフトウェアに含まれています。

`SUNWkcl2a` パッケージを追加すると、システムに Apache Web サーバーおよび mod_ssl 1.3.26 が構成されます。

注 – Apache Web サーバーは、106 ページの「概念および用語」で説明するキーストアまたはユーザーアカウントの機能を使用しません。

注意 – Apache Web サーバーを、Sun Crypto Accelerator 1000 ボードと Sun Crypto Accelerator 4000 ボードを同時に使用するように構成しないでください。Apache サーバーが正しく動作しなくなります。

注 – Apache 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、使用不可にすることはできません。

Apache Web サーバー 1.3x の構成

この節では、`apsslcfg` スクリプトを使用して、ボードを使用するために Web サーバーを構成する方法について説明します。また、この節では、サーバーの証明書の作成およびインストール方法についても説明します。

▼ Apache Web サーバーを構成する

1. `httpd` 構成ファイルをまだ作成していない場合は、これを作成します。

   Solaris システムでは、通常、`/etc/apache` ディレクトリ内に `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、次のようにコピーして使用できます。

   ```
   # 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 を使用するように設定します。

注 – この手順では、このプロンプトでオプション 1 を選択することを想定しています。オプション 2 を選択する場合は、98 ページの「apsslcfg スクリプトの使用」を参照してください。

```
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 バイナリのパスを入力します。

   Solaris システムでは、通常、このパスは /usr/apache ディレクトリです。

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

6. Apache 構成ファイルのパスを入力します。

   Solaris システムでは、通常、このパスは /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 (Remote Security Access) 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]: Y
```

この質問に No と入力した場合は、182 ページの「サーバーの証明書を生成する」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、証明書要求ファイル、および証明書ファイルをそれぞれ識別できるように、異なる接尾辞が付加されます。

```
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。

▼ サーバーの証明書を生成する

1. **180 ページの「Apache Web サーバーを構成する」の手順 7 で作成した鍵を使用して、証明書要求を作成します。**

a. **パスワードを入力して、鍵にアクセスします。要求者情報フィールドに、適切な情報を入力します。**

表 6-1 に、要求者情報フィールドの説明を示します。

```
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) []: Company
Organizational Unit Name (eg, section) []: Department
SSL Server Name (eg, www.company.com) []:www.company.com
Email Address []:admin@company.com
```

表 6-1 要求者情報フィールド

フィールド	説明
Country Name	2 文字の ISO 国別記号 (たとえば、米国の場合は US)
State or Province Name	(任意) 組織の所在地の都道府県の正式名称を入力するか、ピリオドを入力することもできます。
Locality	市区町村
Organization Name	会社名
Organizational Unit Name	会社の部門
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

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と、`/etc/apache/httpd.conf` ファイルの変更方法が表示されます。

```
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、SSLCertificateFile、および 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>
```

180 ページの「Apache Web サーバーを構成する」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 を入力します。

▼ サーバーの証明書をインストールする

1. /etc/apache/keys/*base-name*-certreq.pem ファイル (*base-name* は、180 ページの「Apache Web サーバーを構成する」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、認証局に証明書要求を送信します。
2. 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。
3. Apache Web サーバーを起動します。

   次のパスは、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異なる場合は、正しいパスを入力してください。

```
# /usr/apache/bin/apachectl sslstart
```

4. プロンプトが表示されたら、PEM パスフレーズを入力します。
5. 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 であることに注意してください。

注 – テストのため、証明書に自己署名する方法については、mod_SSL および OpenSSL のマニュアルを参照してください。

Apache Web サーバー 2.x の構築および構成

Sun Crypto Accelerator 4000 ソフトウェアには、Apache Web サーバー 2.x 用の mod_ssl ライブラリは含まれていません。この節では、Web サーバーを構築する際に含める必要のあるオプションと、ボードを使用するために Apache 2.x を構成する方法について説明します。

Apache Web サーバー 2.x の構築

この処理を開始する前に、OpenSSL 実装にすべての必須パッチを適用しておく必要があります。ここでは、ボードに固有のオプションについてのみ説明します。Apache 2.x の全体を構築するための詳細な手順については説明していません。完全な手順については、`http://www.apache.org` から入手できるマニュアルを参照してください。

▼ Apache 2.x を構築する

1. `configure` スクリプトに適合するように、`SH_LIBS` 環境変数を設定しておきます。

```
sh:
# SH_LIBS="-lssl -lcrypto"
# export SH_LIBS
csh/tcsh:
# setenv SH_LIBS "-lssl -lcrypto"
```

2. インストールディレクトリに移動して、`configure` スクリプトを実行します。

   このスクリプトには、多くのコマンド行オプションがあります。次に、ボードを使用する Web サーバーを構成するために必要なオプションを示します。

```
# ./configure --enable-ssl --enable-mods-shared=ssl
--with-ssl=/opt/SUNWconn/cryptov2
```

3. スクリプトが終了したら、次の手順のいずれかを実行します。

   a. はじめて Apache 2.x を構築してインストールする場合は、次のコマンドを入力します。

```
# make
# make install
```

   b. 既存の Apache Web サーバー 2.x の mod_ssl 共有ライブラリを構築する場合は、次のように入力します。

```
# make shared-build
# cp modules/ssl/.libs/mod_ssl.so Apache-directory/modules
```

Apache Web サーバー 2.x の構成

ここでは、ボードを使用するために Web サーバーを構成する方法について説明します。これには、サーバーの証明書の生成とインストール、および Web サーバーでの SSL の有効化を行います。

▼ サーバーの証明書を生成する

1. 鍵および証明書要求を生成します。

```
# /opt/SUNWconn/cryptov2/bin/openssl req \
-new -newkey rsa:keysize -keyout key-output-file \
-out cert-request-output-file \
-config /opt/SUNWconn/cryptov2/ssl/openssl.cnf
Generating a 1024 bit RSA private key
.....................................................................
..........++++++
.......++++++
writing new private key to '/tmp/key1.pem'
```

2. 鍵ファイルを保護するパスワードを入力します。

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

3. 識別名 (Distinguished Name) の値を入力します (表 6-2 を参照)。

```
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]:California
Locality Name (eg, city) []:San Diego
Organization Name (eg, company) []: Company
Organizational Unit Name (eg, section) []: Company Division
SSL Server Name (eg, www.company.com) []:www.company.com
Email Address []: admin@domain.com
```

表 6-2　識別名フィールド

フィールド	説明
Country Name	2 文字の ISO 国別記号 (たとえば、米国の場合は US)
State or Province Name	(任意) 組織の所在地の都道府県の正式名称を入力するか、ピリオドを入力することもできます。
Locality Name	(任意) 市区町村
Organization Name	会社名
Organizational Unit Name	(任意) 会社の部門
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

▼ サーバーの証明書をインストールする

- 188 ページの「サーバーの証明書を生成する」の手順 1 で鍵ファイルを作成したディレクトリに、証明書要求とヘッダーをコピーします。

▼ SSL を使用可能にする

1. Apache Web サーバー 2.x のインストールディレクトリの `conf` サブディレクトリにある `ssl.conf` ファイルを編集します。

   `ssl.conf` ファイルには、いくつかのディレクティブがあります。このボードを使用するには、Web サーバーの次のディレクティブを設定する必要があります。

```
Listen port-number
ServerName fully-qualified-domain-name
SSLEngine on
SSLCertificateFile path-to-certificate-file
SSLCertificateKeyFile path-to-key-file
```

2. 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異なる場合は、正しいディレクトリを入力してください。

```
# /usr/apache/bin/apachectl sslstart
```

3. 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。

4. 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。

注 – テストのため、証明書に自己署名する方法については、mod_SSL および OpenSSL のマニュアルを参照してください。

再起動時のユーザーの操作をなくすための、Apache Web サーバーの設定

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ように設定できます。

▼ 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
```

パスワードファイルのアクセス権および所有者を次のように変更します。

```
# 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。

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 Apache と使用するように構成する方法

SUNWkcl2a 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 ボードを構成する場合は、次のパッチが必要になります。

SUNWkcl2a 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 を使用するように構成するには、次のパッチが必要です。

- Apache 1.3.26 用 ー 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 ー パッチ ID 112869-02
- Sun Crypto Accelerator 1000 バージョン 1.1 ソフトウェア用 ー パッチ ID 113355-01

SUNWkcl2a 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 ー 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 ー パッチ ID 113355-01

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。

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` とともに、Solaris 8 および 9 ソフトウェアのサプリメント 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 `netlbtest` 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 `vcatest` 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 netlbtest 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 netlbtest 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 netlbtest 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 ソフトウェアサプリメント 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 ソフトウェアサプリメント 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 パッケージを削除してください。以前にインストールした SunVTS パッケージは、インストールしたとき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てください。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 vcatest が含まれています。

SunVTS ソフトウェアによる vcatest、nettest、および netlbtest 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、ユーザーマニュアル、および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。

▼ vcatest 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、197 ページの「`vcatest` のテストパラメタオプション」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」ドロップダウンメイ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. 「Start」をクリックして、選択したテストを実行します。
11. 「Stop」をクリックして、すべてのテストを中止します。

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 バルク暗号化のテスト
DES	DES バルク暗号化のテスト
3DES	3DES バルク暗号化のテスト
RSA	RSA 公開鍵および非公開鍵のテスト
DSA	DSA シグニチャー検査のテスト
MD5	MD5 メッセージダイジェスト/デジタルシグニチャーのテスト
SHA1	SHA1 ダイジェスト鍵生成のテスト
RNG	乱数ジェネレータのテスト

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には、コマンド行の文字列にすべての引数を指定してください。

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、このパスは /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,tl=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、DSA、および MD5 テストが実行されます。

```
# /opt/SUNWvts/bin/sparcv9/vcatest -f -o dev=vca2,tl=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
dev=vca*N*	テストするデバイスのインスタンスを、vca0、vca2 のように指定します。指定しない場合のデフォルトは、vca0 です。*N* 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。
tl=*testlist*	実行するサブテストのリストを指定します。tl 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、DES、3DES、DSA、RSA、MD5、SHA1、および RNG です。したがって、tl=CDMF+DES+3DES+DSA+RSA+MD5+SHA1+RNG 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、tl=all 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 all です。

▼ netlbtest 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. 「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 vca*N*(netlbtest) 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。

   - vca*N*(netlbtest) が表示された場合は、手順 6 に進みます。
   - vca*N*(netlbtest) 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 vca*N*(netlbtest) 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。vca*N*(netlbtest) 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、netlbtest 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 vca*N*(netlbtest) 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 vca*N*(netlbtest) 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. vca*N*(netlbtest) 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」ドロップダウンメイ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. 「Start」をクリックして、選択したテストを実行します。

11. 「Stop」をクリックして、すべてのテストを中止します。

▼ 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。

注 – このあとの手順では、CDE ユーザーインタ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. 「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 `vca`*N*`(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。

   - `vca`*N*`(nettest)` が表示された場合は、手順 6 に進みます。
   - `vca`*N*`(nettest)` が表示されない場合は、`vca`*N* 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は、`nettest` プローブがデバイスをテスト対象として認識していません。`ifconfig` のオンラインマニュアルページの手順を参照して、インタフェースを接続してください。

`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. vca*N*(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 vca*N*(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 vca*N*(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. vca*N*(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」ドロップダウンメイ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. 「Start」をクリックして、選択したテストを実行します。

11. 「Stop」をクリックして、すべてのテストを中止します。

注 – nettest と netlbtest 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
        dsasign                 0
        dsaverify               0
        rngbytes                10592
        rngjobs                 187
        rngsha1bytes            16328
        rngsha1jobs             327
        rsaprivate              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 の ok プロンプトから 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

▼ 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、OpenBoot PROM の ok 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。**

   『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. **OpenBoot PROM の ok 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。PHY 接続が確立できなくなるため、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はなれません。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
```

6. アダプタのテストが完了したら、次のように入力して OpenBoot PROM の ok プロンプト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
```

7. auto-boot? 構成パラメタを true に設定します。

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

8. 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 OpenBoot PROM 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、OpenBoot PROM の `ok` 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、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、ok 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         00 03 ba 0e 99 ca
version                   Sun PCI Crypto Accelerator 4000 1000Base-T
FCode 2.11.13 03/03/04
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
max-latency               00000040
min-grant                 00000040
subsystem-vendor-id       0000108e
subsystem-id              00003de8
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、ok 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。

第8章

PKCS#11 インタフェース

この章では、ボードの PKCS#11 インタフェースの実装について説明します。この章では、Sun Crypto Accelerator 4000 ソフトウェアがデフォルトの位置にインストールされていることを前提としています。また、ユーザーに PKCS#11 インタフェースに関する知識があることも前提としています。PKCS#11 規格に関する情報と、ヘッダーファイル `pkcs11.h`、`pkcs11f.h`、および `pkcs11t.h` の元ファイルは、`http://www.rsasecurity.com/rsalabs/PKCS` から入手できます。

この章は、次の節で構成されます。

一般的な情報

Sun Crypto Accelerator 4000 ボードとこれに関連するソフトウェアは、PKCS#11 インタフェースを提供します。多くのアプリケーションに必要な PKCS#11 関数は、すべて Sun Crypto Accelerator 4000 ソフトウェアによって提供されます。

PKCS#11 は、シングルユーザーシステム用に設計されています。Solaris オペレーティングシステムはマルチユーザーシステムで、相互に信頼関係のない複数のユーザーに同時に対応する必要があります。そのため、このボードは、PKCS#11 を拡張することなく複数のユーザーを特定および認証する処理を追加しています。機密の PIN (Personal Identification Number) を受け取るすべての PKCS#11 関数では、*username:password* 形式の文字列を指定する必要があります (表 5-1 を参照)。この PIN 構造は、通常はアプリケーションを介して伝えられますが、このボード用に書かれたいくつかのアプリケーションは、ユーザー名と機密情報の部分を別々に要求する場合があります。

PKCS#11 の管理機能は、トークンを初期化する C_InitToken と、ユーザーの PIN を設定する C_InitPin の、2 つの関数に限定されています。ボードはこの機能を使用せずに、代わりに vcaadm ユーティリティーを使用します。

vcaadm のセキュリティー管理者 (SO) は、UNIX のスーパーユーザーとは関連がありません。また、SO が vcaadm を使用して作成するボードユーザーの userid も、UNIX ユーザー名または ID と関連がありません。

PKCS#11 では、スロットとトークンの概念が明確に区別されます。トークンは、スマートカードに類似したもので、スロットに差し込まれます。Sun Crypto Accelerator 4000 システムでは、スロットとトークンは区別されません。このマニュアルでは、通常「トークン」という用語を使用しますが、アプリケーションやほかのマニュアルでは、「スロット」という用語が使用される場合があります。

各ボードがサポートするキーストアは 1 つだけです。SO は、vcaadm を使用して、各キーストアに名前を付けます。各キーストアは、ボードによって PKCS#11 トークンとして提示されます。これには、関連するキーストアの名前に、32 文字になるように空白文字を追加したトークンラベルが付けられます。高可用性を実現するため、複数のボードで単一のキーストアをサポートすることもできます。

また、SUNW acceleration only というラベルの付いた特別なトークンが 1 つあります。このトークンは永続的な鍵を格納できず、アプリケーションはこのトークンにログインすることができません。このトークンに送信された要求は、使用可能なすべてのボードに配信されます。

アプリケーションの多くは、トークンの一覧を表示します。通常、トークンは、PKCS#11 トークンラベルによって識別されます。トークンラベルとは、SO が割り当てた関連キーストアに空白文字を追加した名前です。

PKCS#11 を使用したボードの管理

Sun Crypto Accelerator 4000 システムは、vcaadm ユーティリティーを使用して管理します (第 4 章を参照)。SO は、キーストアに名前を付けてユーザーアカウントを作成し、各アカウントに初期パスワードを設定します。また、SO は、ボードが FIPS モードで動作するかどうかの制御も行います (212 ページの「PKCS#11 および FIPS モード」を参照)。

ボードは、多くの PKCS#11 メカニズムをサポートします。ほとんどのメカニズムが、無条件で使用可能になっています。ただし、管理者は、次のメカニズムを提示することによって部分的に制御することができます。

- CKM_SSL3_SHA1_MAC
- CKM_SSL3_MD5_MAC
- CKM_SSL3_PRE_MASTER_KEY_GEN
- CKM_SSL3_MASTER_KEY_DERIVE

- CKM_SSL3_KEY_AND_MAC_DERIVE
- CKM_TLS_PRE_MASTER_KEY_GEN
- CKM_TLS_MASTER_KEY_DERIVE
- CKM_TLS_KEY_AND_MAC_DERIVE

これらのメカニズムは、常に、acceleration only トークンによって提示されます。/etc/opt/SUNWconn/cryptov2/sslreg ファイルが存在する場合にのみ、キーストアを持つトークンによって提示されます。このファイルを作成するには、スーパーユーザーで次のコマンドを入力します。

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

アプリケーションを再起動すると、変更が有効になります。

Network Security Services (NSS) は、これらのメカニズムが使用可能になったことを認識します。メカニズムが提供されると、NSS は、小さいバッファーで C_DigestUpdate に対して多数の呼び出しを発行するので、性能を低下させます。そのため、これらのメカニズムは、デフォルトでは提供されないようになっています。

暗号化サービスを使用するアプリケーションのインストールおよび管理

PKCS#11 ライブラリのデフォルトの位置は、/opt/SUNWconn/cryptov2/lib/libvpkcs11.so です。

ほとんどのアプリケーションには構成ファイルまたはデータベースがあり、そこに PKCS#11 ライブラリの位置を設定します。構成ファイルまたはデータベースには、GUI を使用してアクセスできる場合もあります。エディタまたは GUI を使用して、前述のデフォルトの位置を入力します。

鍵に CKA_SENSITIVE 属性が設定されている場合、その鍵に関する操作はハードウェアに限定されます。ただし、ハードウェアによって、すべての操作およびすべての形式の鍵がサポートされるわけではありません。アプリケーションがハードウェアで処理できない操作を要求した場合に、鍵の CKA_SENSITIVE 属性が true に設定されていると、その操作は失敗します。鍵、操作、およびメカニズムの組み合わせに関する規則の詳細は、213 ページの「ハードウェアの高速化と機密鍵」を参照してください。これらの規則が原因でアプリケーションが動作しない場合は、その鍵を機密 (sensitive) に指定しないように構成できる場合があります。

管理者は、SSL... および TLS... メカニズムを提示するかどうかを制御できます。アプリケーションにこれらのメカニズムが必要な場合、またはこれらのメカニズムを使用可能にすると性能にどのような影響を及ぼすかを調べる場合には、210 ページの「PKCS#11 を使用したボードの管理」を参照してください。

ボードが FIPS モードである場合は、FIPS で承認されているメカニズムのみが提供されます (212 ページの「PKCS#11 および FIPS モード」を参照)。

PKCS#11 および FIPS モード

SO が vcaadm を使用して Sun Crypto Accelerator 4000 ボードを FIPS モードに設定すると、ボードは FIPS (Federal Information Processing Standard) 140-2 レベル 3 に準拠するようになります。FIPS 140-2 の詳細は、http://www.nist.gov を参照してください。

FIPS モードでボードを操作すると、ボードの操作に次の変更が生じます。

- FIPS で承認されているメカニズムが、ボード自体で使用可能になります。
- すべての鍵および重要なセキュリティーパラメタは、暗号化された形式で PCI バスを通過するようになります。
- 起動時と、鍵および乱数の生成時に、特定の整合性チェックが追加して実行されるようになります。
- 乱数は、ハッシュおよび演算を使用して、保存された状態と温度ノイズベースジェネレータからの真性乱数データ (エントロピ) を結合する、FIPS で承認されているアルゴリズムによって生成されます。温度ノイズベースジェネレータからの 512 ビットは、出力データの 160 ビットごとに使用されます (FIPS 以外のモードでは、温度ノイズベースジェネレータからの 512 ビットは、160 ビットに SHA-1 ハッシュされます)。

FIPS モードは、Sun Crypto Accelerator 4000 ボード自体にのみ適用されます。前述のとおり、ボードが FIPS モードに設定されると、ボードは FIPS で承認されているメカニズムのみを提供するようになります。MD5、RC2、および RC4 は FIPS で承認されていないことに注意してください。ただし、FIPS の規定はハードウェアにのみ適用されるため、ソフトウェアは、通常提供するすべてのメカニズムを継続して提供できます。

FIPS モードで操作した場合の大きな違いは、FIPS で承認されていない操作がソフトウェアのみで実行されることで、その結果、次の 2 つの影響があります。

- FIPS で承認されていないメカニズムを使用する暗号化演算は、高速化されません。
- FIPS で承認されていないメカニズムを使用する暗号化演算が、CKA_SENSITIVE 属性が true に設定されている鍵を使用すると、その操作は失敗します。CKA_SENSITIVE 属性が true に設定された鍵は、ハードウェアでのみ使用できるためです。

ハードウェアの高速化と機密鍵

ボードは、ハードウェアの能力、セキュリティー要件、および性能に基づいて、操作を実行する場所を選択します。

PKCS#11 は多数の形式の鍵とメカニズムを定義していますが、これらのすべてがハードウェアでサポートされるわけではありません。アプリケーションがハードウェアで完全にサポートされていない操作、鍵およびメカニズムの組み合わせを要求すると、その要求はソフトウェアとハードウェアに分けて実行されるか、すべてソフトウェアで実行される可能性があります。

鍵の CKA_SENSITIVE 属性が true に設定されていると、その鍵を使用する操作は安全に、つまり鍵素材がハードウェアから出力されることなく実行されます。ハードウェアが操作を確実に実行することができない場合、その操作は失敗します。また、鍵の CKA_SENSITIVE 属性が false に設定されていると、ボードは、性能に基づいてハードウェアまたはソフトウェアのいずれかを選択します。この節では、操作をハードウェアで実行するか、ソフトウェアで実行するか、または実行しないかを決定する規則について説明します。

便宜上、次の鍵とメカニズムを定義します。

- hardware_key_set =
  - RSA (鍵のサイズは 2048 ビット未満)
  - DSA (鍵のサイズは 1024 ビット未満)
  - DES
  - 3DES
  - CDMF
- hardware_mechanism_set =
  - CKM_CDMF_... (CKM_CDMF_ECB を除く)
  - CKM_DES_... (CKM_DES_ECB を除く)
  - CKM_DES3_... (CKM_DES3_ECB を除く)
  - CKM_DSA
  - CKM_MD5 (FIPS モードを除く)
  - CKM_RSA_...
  - CKM_SHA_1
- hardware_wrap_mechanism_set =
  - CKM_AES_CBC_PAD
  - CKM_CDMF_CBC_PAD
  - CKM_DES_CBC_PAD
  - CKM_DES3_CBC_PAD
  - CKM_RC2_CBC_PAD (FIPS モードを除く)

操作が必ずハードウェアで実行されるようにするには、hardware_key_set に設定した鍵と、hardware_mechanism_set に設定したメカニズムを使用する必要があります。鍵が hardware_key_set に設定されていても、メカニズムが hardware_mechanism_set に設定されていなければ、ハードウェアによって操作は高速化されますが、ソフトウェアの支援が必要になります。

C_DeriveKey はハードウェアで高速化されますが、ソフトウェアの支援が必要です。したがって、ハードウェアレベルではセキュリティー保護されません。

次の表に、鍵を使用する操作の実行が可能かどうかと、その操作が実行される場所を示します。

表 8-1 鍵を使用する多くの Crypto 操作の処理

状況	CKA_SENSITIVE=False	CKA_SENSITIVE=True
ハードウェアレベルのセキュリティー保護	RSA、DSA、およびバッファーが大きい場合はハードウェア。その他の場合はソフトウェア。	ハードウェア
ソフトウェアの支援によってハードウェアの高速化が可能	RSA、DSA、およびバッファーが大きい場合はハードウェアとソフトウェア。その他の場合はソフトウェア。	失敗
ソフトウェアのみ	ソフトウェア	失敗

C_WrapKey および C_UnwrapKey は、2 つの鍵に対して 2 つの操作を実行します。C_Wrapkey は、ラップされる鍵を符号化する操作を実行してから、符号化された値をラップする鍵を使用して暗号化する操作を実行します。C_UnwrapKey は、この逆の順序で、暗号解読と復号化操作を実行します。

ラップされる鍵が RSA または DSA 鍵で、ラップするメカニズムが hardware_wrap_mechanism_set である場合、符号化および暗号化の手順はどちらもハードウェアで行われます。操作は、両方の鍵についてハードウェアレベルでセキュリティー保護されます。

前述の条件のいずれかが満たされない場合、符号化の手順はソフトウェアで行われます。ラップされる鍵については、操作がハードウェアレベルでセキュリティー保護されなくなります。暗号化の手順は、ラップする鍵およびメカニズムを使用する C_Encrypt 操作と同様に処理されます。詳細は、表 8-1 を参照してください。

次の表に、さまざまな状況の概要をまとめます。

表 8-2 C_WrapKey および C_UnwrapKey の失敗の条件

条件	ラップされる鍵が機密の場合	ラップする鍵が機密の場合
ラップされる鍵が RSA または DSA で、メカニズムが hardware_wrap_mechanism_set に設定されている場合	–	–
ラップする鍵が hardware_key_set、メカニズムが hardware_mechanism_set に設定されている場合	失敗	–
その他の場合	失敗	失敗

C_Digest は、ホストメモリー内のバッファー全体を整理します。C_DigestFinal は、バッファーが大きく、しかし 65532 バイト未満であれば、バッファー全体をハードウェアに送信します。これ以外の場合は、バッファー全体がソフトウェアで処理されます。

C_DigestKey は、鍵素材をホストメモリーに移して、通常のデータと同様に扱います。そのあと、この鍵素材は C_DigestUpdate で処理されます。鍵の CKA_SENSITIVE 属性が true の場合、この処理は失敗します。

PKCS#11 を使用したアプリケーションの開発

必要なヘッダーファイルは /opt/SUNWconn/cryptov2/include; にあります。このディレクトリをインクルードパスに追加して、cryptoki.h をインクルードします。下位レベルのインクルードファイル pkcs11.h、pkcs11f.h、および pkcs11t.h は、Sun Crypto Accelerator 4000 ソフトウェアに含まれています。これらのファイルは、PKCS#11 の Web サイト (http://www.rsasecurity.com/rsalabs/PKCS) で入手できるファイルと同じものです。pkcs11_preamble.h ファイルはインクルードディレクトリ内にあり、下位レベルのどのファイルより先にインクルードする必要があります。

pkcs11 ライブラリは、/opt/SUNWconn/cryptov2/lib/libvpkcs11.so です。

Sun Crypto Accelerator 4000 ライブラリは、通常のライブラリとしてリンクするか、dlopen (3DL) を使用して動的に開くことができます。

通常のライブラリとしてリンクする場合は、次のコマンドを使用します。

```
cc [flags] files... -L /opt/SUNWconn/cryptov2/lib \
-R /opt/SUNWconn/cryptov2/lib -l vpkcs11 [other libraries...]
```

次の例のように、コードは関数を直接呼び出す必要があります。

```
rv = C_Initialize(NULL);
```

動的にリンクする場合は、次のコマンドを使用します (エラー処理は省略しています)。

```
cc [flags] files... -ldl [ other libraries ... ]

#include "cryptoki.h"
#include <dlfcn.h>
#include <link.h>

void *cryptdlhandle;
CK_RV (*getfunctionlistp) (CK_FUNCTION_LIST_PTR *);
CK_FUNCTION_LIST *pk11funclist; /* may need to be globally
accessible */
CK_RV rv;
/* dlopen Sun Cryptoaccelerator 4000 library */
cryptodlhandle =
    dlopen("/opt/SUNWconn/cryptov2/lib/libvpkcs11.so",
    RTLD_NOW | RTLD_LOCAL | RTLD_GROUP);
if (cryptodlhandle == NULL) ...
/* Get pointer to C_GetFunctionList function */
getfunctionlistp = dlsym(cryptodlhandle, "C_getFunctionList");
if (getfunctionlistp == NULL) ...
/* Get libvpksc11's cryptki function list */
rv = (*getfunctionlistp) (&pk11funclist);
if (rv != CKR_OK) ...
```

次の例のように、コードは関数を間接的に呼び出す必要があります。

```
rv = pk11funclist -> C_Initialize(NULL);
```

Sun Crypto Accelerator 4000 ソフトウェアには、独自の制限はほとんどありません。資源の多くは、ホストメモリーによってのみ制限されます。トークン (acceleration only トークンを含む) の最大数は 1024 です。

カーネルのメモリーを極度に消費する障害または不正プログラムによるサービス不能攻撃を防ぐため、ソフトウェアは、1 人の Solaris ユーザー (プロセスではない) が消費するカーネルのメモリー量を 16M バイト以下に制限します。この制限値は、変更できません。

次の推奨事項を守ることによって、カーネルのメモリーの極度の消費を回避できます。

- 複数実行される操作を途中で放棄しないでください。終了する場合は、適切な終了処理関数 (C_EncryptFinal など) を呼び出すか、セッションを終了します。
- 必要のないオブジェクトを途中で放棄しないでください。終了する場合は、作成セッションを終了するか (揮発性のオブジェクトのみに有効)、C_DestroyObject を呼び出します。
- 極端に大容量のデータ (数M バイト) を一度に送信しないでください。通常、大きなダイジェスト操作はソフトウェアで行われるため、この推奨事項はダイジェスト操作には適用されません。

PKCS#11 の管理用の関数 C_InitToken および C_InitPin は実装されていません。CKU_SO (Security Officer) フラグを指定した C_Login 関数は、拒否されます。

PKCS#11 の *public token* オブジェクトは、認証なしで参照および削除できる永続オブジェクトです。Sun Crypto Accelerator 4000 ソフトウェアによって認識されるユーザーは Solaris ユーザーとは関連がなく、ソフトウェアは C_Login が成功するまでユーザーの識別情報を確認しないため、すべてのユーザーがこのオブジェクトをグローバルに参照できる必要があり、すべてのユーザーがこのオブジェクトを削除できます。このような動作は容認されず、そのため public token オブジェクトは許可されません。public token オブジェクトを作成する操作は失敗します。

揮発性の (セッション) オブジェクトの数は、仮想記憶によってのみ制限されます。永続オブジェクトは、すべてボードの RAM に収まる必要がありますが、これは具体的な制限事項ではありません。この概念に合わせて、CK_TOKEN_INFO 構造体 (C_GetTokenInfo 関数によって戻される) のメモリーの最大サイズを示すフィールドには、すべて CK_EFFECTIVELY_INFINITE が設定されます。C_GetObjectSize 関数は実装されていません。

オプションのデュアルオペレーション関数 (C_DigestEncryptUpdate、C_DecryptDigestUpdate、C_SignEncryptUpdate、および C_DecryptVerifyUpdate) は実装されていないため、C_GetTokenInfo によって戻されるフラグフィールド内の CKF_DUAL_OPERATIONS_FLAG は false になります。

C_GetOperationState と関連する関数 C_SetOperationState の実装は、制限されています。C_Digest の操作で、蓄積された入力データが 65532 バイト以下である場合にのみ、C_GetOperationState は成功します。

Sun Crypto Accelerator 4000 システムによって提供されるトークンは、削除不可とみなされます。したがって、CK_GetSlotInfo によって戻される CKF_REMOVABLE_DEVICE フラグは false になります。

C_WaitForSlotEvent 関数は実装されていないため、Sun Crypto Accelerator 4000 システムは、C_OpenSession への Notify パラメタとして渡されるコールバック関数を呼び出しません。ソフトウェアは、C_OpenSession の pApplication パラメタを使用して、呼び出しアプリケーションに制御を戻すことはありません。

Sun Crypto Accelerator 4000 ボードには、高品質の真性乱数ジェネレータが含まれています。乱数ジェネレータをシードする必要はなく、C_SeedRandom は、CKR_RANDOM_SEED_NOT_SUPPORTED というエラーで拒否されます。

ホストメモリー内に存在する重要なフィールドに依存する実装の関数は、CKA_SENSITIVE 属性を true に設定して作成した鍵を使用すると失敗します。具体的な規則は、次のとおりです。

- 鍵の CKA_SENSITIVE が true に設定されていると、C_DigestKey は失敗します。
- 基本となる鍵または派生する鍵の CKA_SENSITIVE が true に設定されていると、すべてのメカニズムの C_DeriveKey は失敗します。
- ラップされるまたはラップ解除される鍵の CKA_SENSITIVE が true に設定されていると、次の条件が適合した場合に、C_WrapKey および C_UnwrapKey は失敗します。
  - 鍵が RSA 鍵または DSA 鍵ではない
  - メカニズムが、CKM_DES_CBC_PAD、CKM_DES3_CBC_PAD、CKM_RC2_CBC_PAD、または CKM_AES_CBC_PAD ではない
- 鍵の CKA_SENSITIVE が true に設定されていると、次のメカニズムを使用する操作はすべての失敗します。
  - CKM_AES...
  - CKM_CDMF_ECB
  - CKM_DES_ECB
  - CKM_DES3_ECB
  - CKM_DH...
  - CKM_MD5_HMAC...
  - CKM_RC2...
  - CKM_RC4...
  - CKM_SHA_1_HMAC...
  - CKM_SSL3...
  - CKM_TLS...
- CKA_SENSITIVE が true に設定されていると、2048 ビットを超える RSA 鍵または 1024 ビットを超える DSA 鍵に関する操作は失敗します。

CKA_EXTRACTABLE 属性のデフォルトは true です。CKA_SENSITIVE 属性のデフォルトは、CKA_EXTRACTABLE の反対の false です。CKA_SENSITIVE および CKA_EXTRACTABLE の両方を false に設定しようとすると失敗して、CKR_TEMPLATE_INCONSISTENT というエラーが戻されます。

通常、属性の矛盾が検出されることはありません。たとえば、テンプレートに同じ属性が複数含まれている場合、その実装は、最後の値のみを使用します。鍵の形式に関連のない属性は無視されるだけです。すべての無効な属性が検出されるわけではありません。

CKA_LOCAL、CKA_ALWAYS_SENSITIVE、および CKA_NEVER_EXTRACTABLE 属性は、実装されていません。

ソフトウェアによって戻されるエラーコードは、予測されるコードと異なる場合があります。特に、CKR_MECHANISM_INVALID は、ほかの値の方が適しているような場合でも、多くのエラーに対して戻されます。リターンコード CKR_HOST_MEMORY は、通常、malloc(3c) コマンドへの内部呼び出しが失敗したことを意味します。このエラーが戻されたあとは、重要な状態が適切に保存されていない場合があり、C_Finalize 呼び出し以外は、処理を継続しても効果がありません。

負荷を低減するため、ソフトウェアの C_EncryptInit および同様の関数の実装は、実際にデータが暗号化されるまでボードへの鍵の送信を保留することがあります。この結果、PKCS#11 が C_EncryptInit (および同様の関数) が報告すべきであると表明している一部のエラーが、実際には、後続の C_EncryptUpdate (および同様の関数) への最初の呼び出しで報告されます。

次の PKCS#11 指示子によって認識されるメカニズムは、Sun Crypto Accelerator 4000 ソフトウェアで使用できます。CKM_SSL3... および CKM_TLS... メカニズムは、次のリストに示されていますが、/etc/opt/SUNWconn/cryptov2/sslreg ファイルが存在する場合にのみ、キーストアを持つトークンで使用できます (210 ページの「PKCS#11 を使用したボードの管理」を参照)。

- CKM_AES_CBC
- CKM_AES_CBC_PAD
- CKM_AES_ECB
- CKM_AES_KEY_GEN
- CKM_CDMF_CBC
- CKM_CDMF_CBC_PAD
- CKM_CDMF_ECB
- CKM_CDMF_KEY_GEN
- CKM_DES2_KEY_GEN
- CKM_DES3_CBC
- CKM_DES3_CBC_PAD
- CKM_DES3_ECB
- CKM_DES3_KEY_GEN
- CKM_DES_CBC
- CKM_DES_CBC_PAD
- CKM_DES_ECB
- CKM_DES_KEY_GEN
- CKM_DH_PKCS_DERIVE
- CKM_DH_PKCS_KEY_PAIR_GEN
- CKM_DSA
- CKM_DSA_KEY_PAIR_GEN
- CKM_MD5

- CKM_MD5_HMAC
- CKM_MD5_HMAC_GENERAL
- CKM_RC2_CBC
- CKM_RC2_CBC_PAD
- CKM_RC2_ECB
- CKM_RC2_KEY_GEN
- CKM_RC4
- CKM_RC4_KEY_GEN
- CKM_RSA_PKCS
- CKM_RSA_PKCS_KEY_PAIR_GEN
- CKM_RSA_X_509
- CKM_SHA_1
- CKM_SHA_1_HMAC
- CKM_SHA_1_HMAC_GENERAL
- CKM_SSL3_KEY_AND_MAC_DERIVE
- CKM_SSL3_MASTER_KEY_DERIVE
- CKM_SSL3_MD5_MAC
- CKM_SSL3_PRE_MASTER_KEY_GEN
- CKM_SSL3_SHA1_MAC
- CKM_TLS_KEY_AND_MAC_DERIVE
- CKM_TLS_MASTER_KEY_DERIVE
- CKM_TLS_PRE_MASTER_KEY_GEN

RSA、DSA、および Diffie-Hellman 鍵の最大サイズは次のとおりです。

表 8-3 鍵の最大サイズ

鍵	機密ではない鍵の最大サイズ	機密の鍵の最大サイズ
RSA	4096	2048
DSA	4096	1024
DH	2048	使用不可

オブジェクトハンドルまたはセッションハンドルは、常に small integer で連続して割り当てられるとはかぎりません。これらのハンドルは、unsigned long である場合があります。

C_Initialize に渡される相互排他 (mutex) のコールバック関数ポインタは無視されます。

多くの場合、小容量のデータの操作は、ボードではなくホストプロセッサで処理されます。これは、操作をボードに送信するコストが、ホストでその操作を実行するコストより大きいためです。ただし、CKA_SENSITIVE 属性が true に設定されているオブジェクトを使用する操作はすべてボードで実行されます。

すべての C_DigestUpdate バッファーの累積サイズが 65532 バイトを超えると、ホストのソフトウェアによってダイジェスト操作が実行されます。同じ特性が C_Digest にも適用されます。このようにして、小容量のデータと非常に大容量のデータは、どちらもソフトウェアによって処理されます。

永続オブジェクトに関する情報は、ユーザーが C_Login 関数を正常に実行したときにプロセスに渡されて、キャッシュされたまま残ります。そのあとの、別の処理による永続オプジェクトの作成、削除、または修正は見えない場合があります。ボードで実行される操作は、最新の状態の鍵を使用します (ボードが使用可能で鍵が機密である場合、またはボードが使用可能でバッファーの大きさが妥当である場合には、操作はボードで実行されます)。それ以外の操作と、C_FindObjects 関数は、キャッシュされた状態の鍵を使用してソフトウェアで処理されます。

注意 – 将来のリリースでは、この鍵のキャッシュの動作は変更される可能性があります。

PKCS#11 規格によって定められているとおり、ユーザが C_Logout 関数を呼び出すか、最後の PKCS#11 セッションを終了すると、すべての永続オブジェクトハンドルが無効になります。ソフトウェアは、ソフトウェアのキャッシュからトークンオブジェクトを消去します。次に C_Login 関数を正常に実行したときに、すべてのトークンオブジェクトはその時点で最新のものになります。別のユーザーがこのログインを実行した場合には、別のトークンオブジェクトのセットが使用されることに注意してください。ただし、同じユーザーがこのログインを実行した場合でも、トークンオブジェクトは以前とは異なるハンドルを取得することがあります。

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。

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 @ 5 V 12.75 W @ 3.3 V
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 ℃、+32 ～ +131 °F	-40 ～ +75 ℃、-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	1000 Mbps (全二重)
100 Mbps	100 Mbps (全二重および半二重)
10 Mbps	10 Mbps (全二重および半二重)

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 @ 5 V 12.75 W @ 3.3 V
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 ℃、+32 ～ +131 °F	-40 ～ +75 ℃、-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

付録B

インストールスクリプトを使用しないソフトウェアのインストール

この付録では、製品 CD で提供されるインストールスクリプト (`/cdrom/cdrom0/install`) を使用せずに、Sun Crypto Accelerator 4000 ソフトウェアを手動でインストールする方法について説明します。この付録は、次の節で構成されます。

手動によるソフトウェアのインストール

Sun Crypto Accelerator 4000 ソフトウェアは、製品 CD に収録されています。SunSolve Web サイト (`http://sunsolve.sun.com`) 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、12 ページの「必須パッチ」を参照してください。

▼ ソフトウェアを手動でインストールする

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 B-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)	
install	Sun Crypto Accelerator 4000 ソフトウェアをインストールするインストールスクリプト	
remove	Sun Crypto Accelerator 4000 ソフトウェアを削除する削除スクリプト	
Docs	『Sun Crypto Accelerator 4000 ボードバージョン 1.1 インストールマニュアル』(このマニュアル) 『Sun Crypto Accelerator 4000 ボードバージョン 1.1 ご使用にあたって』	
Packages	Sun Crypto Accelerator 4000 ソフトウェアパッケージ	
	SUNWkcl2r	暗号化カーネルコンポーネント
	SUNWkcl2u	暗号化管理ユーティリティーおよびライブラリ
	SUNWkcl2a	Apache の SSL サポート (オプション)
	SUNWkcl2m	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
	SUNWvcafw	VCA ファームウェア
	SUNWvcamn	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)
	SUNWkcl2o	SSL 開発ツールおよびライブラリ (オプション)
	SUNWkcl2i.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 を使用する場合にかぎり、オプションの SUNWkcl2a 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かぎり、オプションの SUNWkcl2o 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かぎり、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 SUNWkcl2i.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 SUNWkcl2i 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。

1. 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 SUNWkcl2m SUNWvcar SUNWvcau SUNWvcaa SUNWvcamn
SUNWvcafw
```

2. (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 SUNWvcafw
system      SUNWkcl2r      KCLv2 Crypto (Root)
system      SUNWkcl2u      KCLv2 Crypto Support Software
system      SUNWvcaa       VCA Crypto Accelerator/Gigabit Ethernet Admin
system      SUNWvcafw      VCA Crypto Accelerator/Gigabit Ethernet firmware
system      SUNWvcar       VCA Crypto Accelerator/Gigabit Ethernet Drivers
system      SUNWvcau       VCA Crypto Accelerator/Gigabit Ethernet Daemon
```

3. (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
```

4. (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  vcactl (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、Sun Crypto Accelerator 4000 のオンライン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 B-1 を参照してください。

ディレクトリおよびファイル

表 B-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 B-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	ユーティリティー
/opt/SUNWconn/cryptov2/lib	サポートライブラリ
/opt/SUNWconn/cryptov2/sbin	管理コマンド

図 B-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。

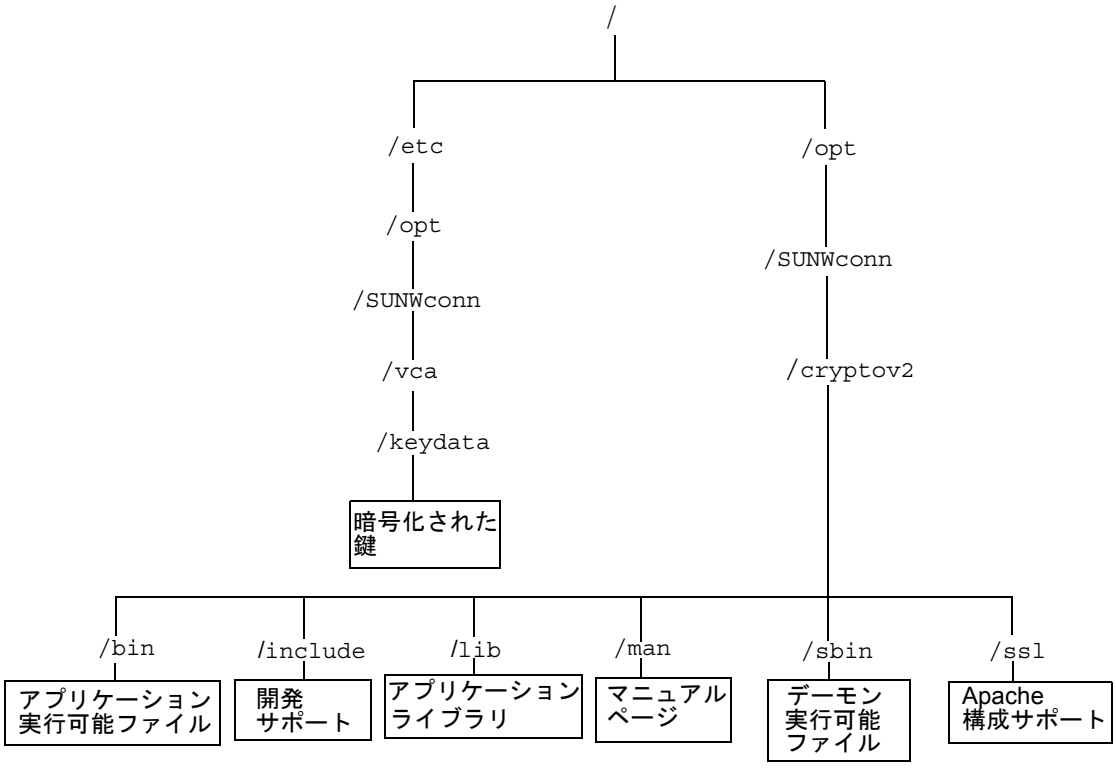

図 B-1 Sun Crypto Accelerator 4000 ディレクトリおよびファイル

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、構成およびキーストア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、68 ページの「`vcaadm` によるボードの初期化」を参照してください。

手動による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 (71 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、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、82 ページの「ボードのソフトウェア情報の消去」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用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。

▼ ソフトウェアを手動で削除する

- **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 SUNWvcafw SUNWvcau
```

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。

付録C

Apache Web サーバーの SSL 設定ディレクティブ

この付録では、Sun Crypto Accelerator 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* が 1 回実行されます (収集された各パスワードは、*program* をふたたび実行する前に試されます)。

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

注 – このプログラムはシステムの起動中に実行されるため、コンソールが `tty` デバイスでない場合 (`tty`(3c) が false を返す場合) に対処できる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 を使用するように設定しています。ディレクティブが設定されていない場合、このプロトコルはデフォルトでオフになります。

3. SSLProtocol [+-]*protocol*

   コンテキスト : グローバル、仮想ホスト

   このディレクティブでは、サーバーが SSL トランザクションで使用するプロトコルを設定します。表 C-1 に、使用可能なプロトコルとその説明を示します。

表 C-1　SSL プロトコル

プロトコル	説明
SSLv2	標準である Netscape の最初の SSL プロトコル
SSLv3	SSL プロトコルの更新バージョン。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 ハンドシェークで使用されます。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 C-2 に示す暗号を、コロンで区切って指定します。表 C-2 で、DH は Diffie-Hellman を、DSS は Digital Signature Standard を表します。

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

表 C-3　SSL の別名

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

暗号の優先順位は、表 C-4 に示す特殊文字を使用して設定できます。

表 C-4 暗号の優先順位を設定する特殊文字

文字	説明
指定なし	リストに暗号を追加
!	リストから完全に暗号を削除 (ふたたび追加できない)
+	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 (ふたた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 C-5 に、*level* の値を示します。

表 C-5 SSL のクライアントの検証レベル

レベル	説明
none	クライアントの証明書は必要なし
optional	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 C-6 に、*level* の値を示します。

表 C-6 SSL のログレベルの値

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

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

コンテキスト : グローバル、仮想ホスト、ディレクトリ、`.htaccess`

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

表 C-7 に、オプションを示します。

表 C-7 使用できる 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 `SSL_SERVER_CERT` および `SSL_CLIENT_CERT`、`SSL_CLIENT_CERT_CHAIN`*n* (*n* = 0, 1, ...) がエクスポートされます。これらの変数には、クライアントおよびサーバーに対する PEM 符号化形式の証明書が含まれます。
`FakeBasicAuth`	クライアント証明書の識別名 (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 `xxj31ZMTZzkVA` を使用する必要があります。これは、「password」を暗号化 (`crypt`(3c)) したものです。
`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 が使用されないかぎり、特定のディレクトリへのアクセスを禁止します。このディレクティブは、認証されていないアクセスまたは暗号化されていないアクセスによってディレクトリの内容を使用できる状態になっている場合などの、誤った構成を防止するために使用します。

付録D

ボードを使用するためのカスタムアプリケーションの構成

この付録では、ボードに付属するソフトウェアについて説明します。このソフトウェアを使用すると、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かぎりません。OpenSSL の標準ライブラリで構築した方が効果的なアプリケーションもあります。OpenSSL の標準ライブラリは、`http://www.openssl.org` からダウンロードできます。

ボードを使用するためのカスタムアプリケーションの構成

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。

▼ ボードを使用するためにカスタムアプリケーションを構成する

1. `SUNWkcl2o` パッケージをインストールします。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。

2. 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、アプリケーションを構成します。

```
-I/opt/SUNWconn/cryptov2/include
```

3. リンカーに適切なライブラリへの参照を指定します。

   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。サンの暗号化ライブラリを指定してください。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
```

付録E

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権を許諾します。

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。本契約の一部分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にあり、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 rouines 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F

マニュアルページ

この付録では、ボードのソフトウェアが提供する Sun Crypto Accelerator 4000 のコマンドおよびユーティリティーの説明と、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。

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 pagename
```

表 F-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 F-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)	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
vcad(1m)	キーストアサービスを提供するデーモン
vcaadm(1m)	ボードに関する構成、アカウント、鍵のデータベースを手動で操作するためのユーティリティー
vcadiag(1m)	スーパーユーザーに、ボードのリセット、鍵素材の消去、および基本的な診断の実行機能を提供するユーティリティー
kcl2(7d)	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
apsslcfg(1m)	Apache Web サーバー用の構成ユーティリティー
iplsslcfg(1m)	Sun ONE Web サーバー用の構成ユーティリティー
pk11export(1m)	PKCS#11 インタフェースを使用する鍵のエクスポートユーティリティー

付録 G

ハードウェアの情報の消去

この付録では、Sun Crypto Accelerator 4000 ボードのハードウェア上の情報を消去して、ボードを出荷時の状態に戻す方法について説明します。ボードは、出荷時の状態に戻ると Failsafe モードになります。

注意 – 必要な場合以外は、ハードウェア上の情報を消去しないでください。すべての鍵素材だけを削除する必要がある場合は、`vcaadm` プログラムの `zeroize` コマンドを使用して、ソフトウェアの情報を消去してください。`zeroize` コマンドの詳細は、82 ページの「ボードのソフトウェア情報の消去」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 – ボードのハードウェア上の情報を消去すると、Sun Crypto Accelerator 4000 ファームウェアが削除されます。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生じる場合があります。この作業は、標準的な SCSI ハードウェアジャンパ (シャント) を使用して行います。

注 – vcaadm プログラムの 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、82 ページの「ボードのソフトウェア情報の消去」を参照してください。また、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。

▼ 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 1 および 2 に、ジャンパを取り付けます。**

   ピン 1 および 2 は、留め具のもっとも近くにあります。2 つのピンが 4 組あります。図 G-1 に示すように、ピン 1 および 2 にジャンパを取り付けます。

注意 – ピン 1 および 2 にジャンパが取り付けられたボードは機能しません。

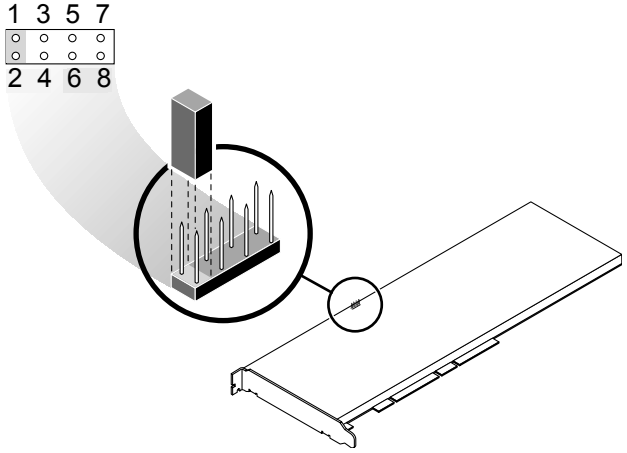

図 G-1　　ハードウェアのジャンパブロックのピン

4. **システムの電源を入れます。**

注意 – ハードウェア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、鍵素材、および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 1 および 2 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、68 ページの「vcaadm によるボードの初期化」を参照してください。

索引

T

U

V

W

Z

あ

い

え

お

す

せ

そ

つ

て

と

へ

ほ

ま

め

も

ゆ

よ

ら

れ

わ