P3F1-1840-01

PRIMERGY

PRIMERGY SSLAccelerator 7117

取扱説明書

FUJITSU

ごあいさつ

このたびは、弊社の PRIMERGY（プライマジー）SSLAccelerator をお買い求めいただきまして、誠にありがとうございます。

PRIMERGY SSLAccelerator は、暗号化／復号化処理を Web サーバからオフロードし、セキュリティを保持したまま、Web サイトのパフォーマンスを向上させることができます。

本書は、PRIMERGY SSLAccelerator の取り扱い方法など、基本的なことがらを解説しています。

本書をご覧になり、PRIMERGY SSLAccelerator を正しくお使いいただきますよう、お願いいたします。

2002 年 5 月

本製品は、一般事務用、パーソナル用、家庭用、通常の産業用等の一般的用途を想定して設計・製造されているものであり、原子力施設における核反応制御、航空機自動飛行制御、航空交通管制、大量輸送システムにおける運行制御、生命維持のための医療用機器、兵器システムにおけるミサイル発射制御など、極めて高度な安全性が要求され、仮に当該安全性が確保されない場合、直接生命・身体に対する重大な危険性を伴う用途（以下「ハイセイフティ用途」という）に使用されるよう設計・製造されたものではございません。お客様は、当該ハイセイフティ用途に要する安全性を確保する措置を施すことなく、本製品を使用しないでください。ハイセイフティ用途に使用される場合は、弊社の担当営業までご相談ください。

当社のドキュメントには「外国為替および外国貿易管理法」に基づく特定技術が含まれていることがあります。特定技術が含まれている場合は、当該ドキュメントを輸出または非居住者に提供するとき、同法に基づく許可が必要となります。

本製品は、デジタル電子計算用の暗号機能を有するため、本製品を輸出又は非居住者に提供する際には、「外国為替及び外国貿易法」に基づく経済産業大臣の許可が必要となります。
また、仕向け地が EU+8ヵ国以外の国・地域であって、需要者が政府系機関である場合等は、米国政府の許可が必要となる場合があります。

注意
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。

本装置は、落雷などによる電源の瞬時電圧低下に対し不都合が生じることがあります。

PRIMERGY SSLAccelerator 7117 は「高調波ガイドライン適合品」です。

本書の読み方

本書は、PRIMERGY SSLAccelerator の基本的な取り扱い方法を解説しています。本書で解説していない周辺装置の取り扱い方法については、各周辺装置に添付されている取扱説明書をご覧ください。

■ 本書の構成

章	内容
第 1 章 本装置について	本装置の概要などを解説しています。 まず、最初にお読みください。
第 2 章 設置と初期設定	本装置の設置方法と、初期設定の手順を解説しています。本装置を設置するときにお読みください。
第 3 章 構成	本装置を使うときの構成、設定手順などを解説しています。本装置を初めて使うときにお読みください。
第 4 章 鍵と電子証明書	本装置を使用するために必要な基本的事項について解説しています。必要に応じてお読みください。
第 5 章 コマンドライン	コマンドラインについて説明し、コマンドの一覧とその機能を解説しています。必要に応じてお読みください。
第 6 章 リモート管理	リモート管理について解説しています。必要に応じてお読みください。
第 7 章 アラーム機能および監視機能	アラーム機能および監視機能について解説しています。必要に応じてお読みください。
第 8 章 トラブルシューティング	本装置にトラブルが発生したとき、どうすればよいのかを解説しています。本装置が思うように動かなかったり、画面にメッセージが表示されたりしたときにお読みください。
付録 A	本体仕様、用語集などを載せてあります。 必要に応じてお読みください。

安全にお使いいただくために

本書には、本装置を安全に正しくお使いいただくための重要な情報が記載されています。

本装置をお使いになる前に、本書を熟読してください。特に、本書の「安全上のご注意」をよくお読みになり、理解された上で本装置をお使いください。

また、本書は、本装置の使用中にいつでも参照できるよう大切に保管してください。

安全上のご注意

本装置およびそのオプション装置を安全にお使いいただくために、以降の記述内容を必ずお守りください。

本書では、いろいろな絵表示をしています。これは装置を安全に正しくお使いいただき、あなたや他の人々に加えられるおそれのある危害や損害を未然に防止するための目印となるものです。その表示と意味は次のようになっています。内容をよくご理解の上、お読みください。

⚠警告　**この表示を無視して、誤った取り扱いをすると、人が死亡する可能性または重傷を負う可能性があることを示しています。**

⚠注意　**この表示を無視して、誤った取り扱いをすると、人が傷害を負う可能性があること、および物的損害のみが発生する可能性があることを示しています。**

また、危害や損害の内容がどのようなものかを示すために、上記の絵表示と同時に次の記号を使用しています。

感電

△ で示した記号は、警告・注意を促す内容であることを告げるものです。記号の中やその脇には、具体的な警告内容（左図の場合は感電注意）が示されています。

分解

⃠ で示した記号は、してはいけない行為（禁止行為）であることを告げるものです。記号の中やその脇には、具体的な禁止内容（左図の場合は分解禁止）が示されています。

プラグ

● で示した記号は、必ず従っていただく内容であることを告げるものです。記号の中やその脇には、具体的な指示内容（左図の場合は電源プラグをコンセントから抜いてください）が示されています。

⚠警告

- **万一、装置から発熱や煙、異臭や異音がするなどの異常が発生した場合は、ただちに電源プラグをコンセントから抜いてください。**
  煙が消えるのを確認して、担当営業員または担当保守員に修理をご依頼ください。お客様自身による修理は危険ですから絶対におやめください。異常状態のまま使用すると、火災・感電の原因となります。
- **異物（水・金属片・液体など）が装置の内部に入った場合は、ただちに電源プラグをコンセントから抜いてください。その後、担当営業員または担当保守員にご連絡ください。そのまま使用すると、火災・感電の原因となります。特にお子様のいるご家庭ではご注意ください。**

■ 本体の取り扱いについて

⚠警告

- **装置を勝手に改造しないでください。火災・感電の原因となります。**
- **装置本体のカバーや差し込み口についているカバーは、オプション装置の取り付けなど、必要な場合を除いて取り外さないでください。**
  内部の点検、修理は担当営業員または担当保守員にご依頼ください。内部には電圧の高い部分があり、感電の原因となります。

禁 止

- **ディスプレイに何も表示できないなど、故障状態で使用しないでください。故障の修理は担当営業員または担当保守員にご依頼ください。そのまま使用すると火災・感電の恐れがあります。**
- **開口部（通風孔など）から内部に金属類や燃えやすいものなどの異物を差し込んだり、落とし込んだりしないでください。故障・火災・感電の原因となります。**
- **装置の上または近くに「花びん・植木鉢・コップ」などの水が入った容器、金属物を置かないでください。故障・火災・感電の原因となります。**
- **殺虫剤などを使って害虫駆除を行う場合には、サーバ本体を停止し、ビニールなどで保護してください。**
- **湿気・ほこり・油煙の多い場所、通気性の悪い場所、火気のある場所に置かないでください。故障・火災・感電の原因となります。**

水 気

- **本体に水をかけないでください。故障・火災・感電の原因となります。**
- **風呂場、シャワー室などの水場で使用しないでください。故障・火災・感電の原因となります。**

プラグ

近くで雷が発生したときは、電源ケーブルやモジュラケーブルをコンセントから抜いてください。そのまま使用すると、雷によって装置を破壊し、火災の原因となる場合があります。

禁 止

- **表示された電源電圧以外の電圧で使用しないでください。また、タコ足配線をしないでください。火災・感電の原因となります。**
- **濡れた手で電源プラグを抜き差ししないでください。感電の原因となります。**
- **電源ケーブルを傷つけたり、加工したりしないでください。重いものを載せたり、引っ張ったり、無理に曲げたり、ねじったり、加熱したりすると電源ケーブルを傷め、火災・感電の原因となります。**
- **電源ケーブルや電源プラグが傷んだとき、コンセントの差し込み口がゆるいときは使用しないでください。そのまま使用すると、火災・感電の原因となります。**

指 示

電源プラグの電極、およびコンセントの差し込み口にほこりが付着している場合は、乾いた布でよく拭いてください。そのまま使用すると、火災の原因となります。

アース

アース接続が必要な装置は、電源を入れる前に、必ずアース接続をしてください。アース接続ができない場合は、担当営業員または担当保守員にご相談ください。万一漏電した場合に、火災・感電の原因となります。

警 告

取り外したカバー、キャップ、ネジなどは、小さなお子様が誤って飲むことがないように、小さなお子様の手の届かないところに置いてください。万一、飲み込んだ場合は、直ちに医師と相談してください。

⚠注意

禁止

- 装置の開口部（通風孔など）をふさがないでください。通風孔をふさぐと内部に熱がこもり、火災の原因となります。
- 装置の上に重いものを置かないでください。また、衝撃を与えないでください。バランスが崩れて倒れたり、落下したりしてけがの原因となります。
- 振動の激しい場所や傾いた場所など、不安定な場所に置かないでください。落ちたり、倒れたりしてけがの原因となります。
- AC アダプタを使用する装置の場合は、マニュアルに記載されていない AC アダプタは使用しないでください。また、AC アダプタの改造・分解はしないでください。火災・けがの原因となります。
- サービスコンセントがある装置の場合は、マニュアルに記載されていない装置をサービスコンセントに接続しないでください。火災・けがの原因となります。
- フロッピィディスク・IC カードなどの差し込み口に指などを入れないでください。けがの原因となります。
- 電源プラグを抜くときは電源ケーブルを引っ張らず、必ず電源プラグを持って抜いてください。電源ケーブルを引っ張ると、電源ケーブルの芯線が露出したり断線したりして、火災・感電の原因となります。
- 携帯電話などを本体に近づけて使用しないでください。装置が正しく動かなくなります。

指示

- 転倒防止足のある装置は必ず使用してください。振動による転倒でけがをするおそれがあります。
- 電源プラグは、コンセントの奥まで確実に差し込んでください。火災・故障の原因となります。

プラグ

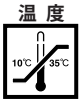
- 装置を移動する場合は、必ず電源プラグをコンセントから抜いてください。また、電源ケーブルなどもはずしてください。作業は足元に十分注意して行ってください。電源ケーブルが傷つき、火災・感電の原因となったり、装置が落ちたり倒れたりしてけがの原因となります。
- 長時間装置を使用しないときは、安全のため必ず電源プラグをコンセントから抜いてください。火災・感電の原因となります。

指 示

- 健康のため、1 時間ごとに 10 ～ 15 分の休憩をとり、目および手を休めてください。
- ディスプレイなど、重量のある装置を動かす場合は、必ず 2 人以上で行ってください。けがの原因となります。
- ヘッドホンを使用するときは、音量を上げすぎないように注意してください。耳を刺激するような大きな音量を長時間続けて聴くと、聴力に悪い影響を与える原因となります。

■ 温湿度について

⚠注意



- **本装置は、周囲温度が 10 ～ 35 ℃の環境を守ってご利用ください。**
  特に 24 時間運転をする場合には空調のスケジュールなどを十分考慮し（夜間や休日など）、周囲温度をはずれた温度のもとで運用されることの無いようにしてください。
  温度条件が守られないと、電子部品の誤動作や故障、寿命の短縮の原因となります。
  - **ー 特に夏場において 24 時間運用を行う場合、必要に応じて夜間・休日にも冷房を入れて、周囲温度が 35 ℃を超えないようにしてください。**
  - **ー 冬場など寒中での暖房時は、1 時間あたりの温度上昇が 15 ℃を超さないように室温調整を行い、結露を発生させないようにしてください。**

		室内温度（°C）							備考
		10	15	20	25	30	35	40	
相対湿度（%）	20	- 7	- 5	- 3	1	5	9	13	[見方] 温度 25° C で湿度 60% の場合、装置が 17° C 以下のとき、結露します。
	40	- 3	2	7	11	16	20	24	
	60	3	8	13	17	22	26	31	
	80	7	12	17	22	26	31	-	
	90	9	13	19	24	29	34	-	

■ 腐食性ガスや塵埃について

⚠注意

腐食性ガスや塩風は、装置を腐食させ誤動作、破損および、装置寿命を著しく短くする原因となりますので、空気清浄装置を設置するなどの対策が必要となります。
また、塵埃が多い場所についても、記憶媒体の破損、装置冷却の妨げなどにより、誤動作や装置寿命を著しく短くする原因となります。

- **腐食性ガスの発生源としては、化学工場地域、温泉／火山地帯などがあります。**
- **塩害地区の目安としては、海岸線から 500m 以内となります。**

■ 本装置を廃棄するとき

本装置を廃棄する場合には、産業廃棄物として処理する必要があります。廃棄する場合には、必ず担当営業または専門業者にご連絡ください。

保守サービスについて

■ 保守サポート期間

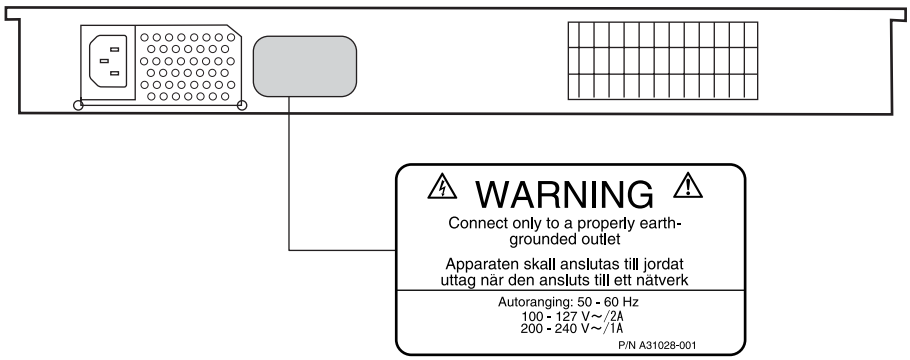
保守サポート期間は、お客様の購入後 6 年間です。

システムの安定稼動を目的に、保守サービス契約を結ばれることを推奨しております。
是非とも保守サービス契約を結ばれますようお願い申し上げます。

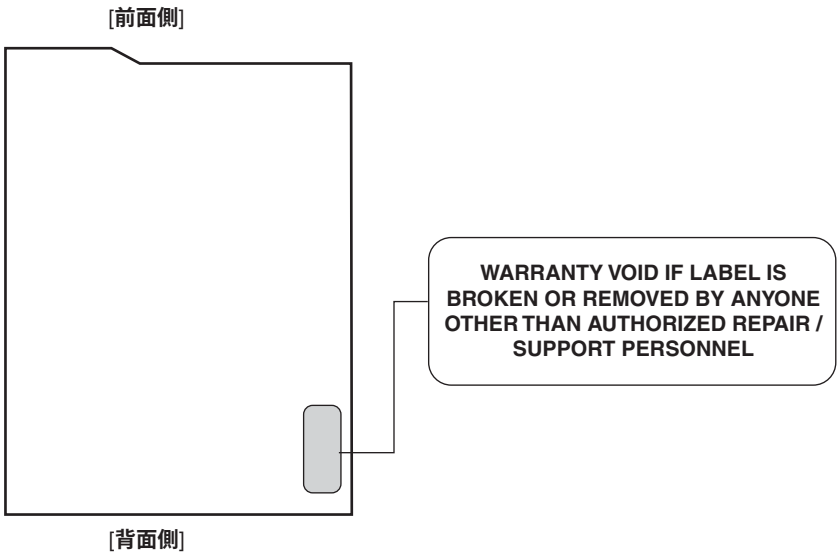
警告ラベル

本製品には、装置の上面および背面に警告ラベルが貼ってあります。警告ラベルは、絶対にはがさないでください。また、**その他のラベルもすべてはがさないでください**。

[装置背面]



[装置上面]



本書の表記について

■ キーの表記と操作方法

本文中のキーの表記は、キーボードに書かれているすべての文字を記述するのではなく、説明に必要な文字を次のように記述しています。

例：[Ctrl] キー、[Enter] キーなど

また、複数のキーを同時に押す場合には、次のように「+」でつないで表記しています。

例：[Ctrl] + [C] キーなど

■ コマンド入力での表記

本文中では、コマンドラインインタプリタで用いるコマンドの説明において、以下の規則に従って表記しています。

< >
: ユーザが入力するパラメタを意味します。

[ ]
: ユーザが選択するパラメタを省略します。パラメタはそれぞれ「|」で区切って表示されます。

{ }
: 省略可能なコマンドや省略可能なパラメタを意味します。

太字（ボールド体）
: コマンドラインインターフェースに対しユーザが入力する実際の文字列を示します。コマンド実行の結果表示される文字列は通常の字体で表記されます。

|
: [ ] 内の入力パラメタの区切りです。この記号で区切られている複数のパラメタのうち 1 つを選択します。実際の入力ではこの記号を入力しないでください。

#
: SSLAccelerator の標準コマンドラインプロンプトです。

■ 本文中の表記

本文中では、以下の表記を使用しています。

本装置、SSLAccelerator

PRIMERGY SSLAccelerator 7117 のことです。

ポイント

ハードウェアやソフトウェアを正しく動作させるために必要なことが書いてあります。

■ 画面例について

本書に記載されている画面は一例です。お使いのサーバに表示される画面やファイル名などが異なる場合があります。ご了承ください。

目　次

1 本装置について

この章では、本装置の概要および機能について説明します。

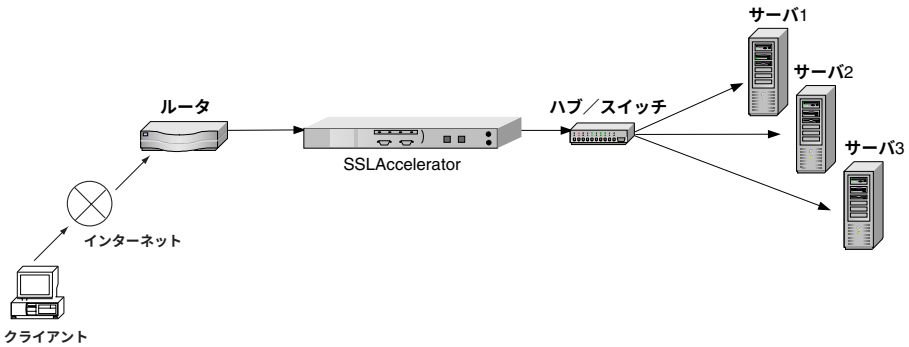
Contents

1.1 概要

PRIMERGY SSLAccelerator 7117（以降、特に明記しないかぎり、これを「本装置」または「SSLAccelerator」と記述）は、暗号化／復号化処理を Web サーバからオフロードし、セキュリティを保持したまま、Web サイトのパフォーマンスを向上させる装置です。

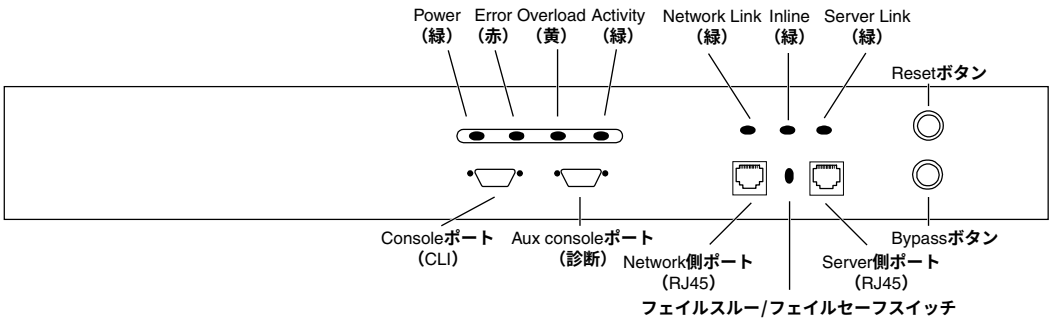
SSLAccelerator には以下の特長があります。

- SSL v2 と SSL v3 に対応しています。
- 多くの暗号アルゴリズムとハッシュ関数をサポートしています。
- 鍵や証明書、認証局の証明書発行に必要な CSR 作成機能があり、作成された鍵や証明書などを取り出すことができます。また、鍵や証明書を取り込むこともできます。
- ネットワーク側とサーバ側の RJ-45 ポートを SSLAccelerator 内部で直接接続する設定ができ、障害発生時にもサービスを提供し続けることができます。
- SSLAccelerator 7117 では、最大で毎秒 1000 コネクションの SSL リクエストを処理することができます。
- SSLAccelerator を直列にカスケード接続し、処理性能を向上しつつ障害発生に備えることができます。



1.2 名称と働き

ここでは、本装置の名称と働きを解説します。



■ ボタンとスイッチ

SSLAccelerator のフロントパネルには、ボタンが 2 個とスイッチが 1 個あります。

ボタン／スイッチ	機能
Reset ボタン	短い間押した場合、SSLAccelerator は再起動します。5 秒以上押した場合、SSLAccelerator の設定がリセットされ、出荷時のデフォルト設定に戻ります。
Bypass ボタン	バイパスモードとインラインモードを切り替えます。
フェイルスルー／フェイルセーフスイッチ	フェイルセーフ（スイッチ位置が上）に設定すると、SSLAccelerator に障害が発生している間、ネットワーク接続は切断されます。フェイルスルー（スイッチ位置が下）に設定すると、障害が発生してもネットワーク接続は維持されます。デフォルトはフェイルセーフです。 詳細は、「A.3 障害／バイパスモード」（→ 192 ページ）を参照してください。

■ フロントパネルの LED

LED は、SSLAccelerator の様々な情報を表しています。SSLAccelerator のフロントパネルには 7 個の LED があります。これらは、4 個のグループと 3 個のグループに分かれています。

LED	状態
Power	点灯 - 電源がオンになっています。
	消灯 - 電源がオフになっています。
Error	点灯 - エラーが検出されました。
	消灯 - 通常の状態です。
Overload	点灯 - 受信した SSL 要求の数が多すぎます。 過負荷の度合いが高くなるにつれて、暗い点滅状態から明るい点灯状態へと変化します。処理しきれない要求を別の SSLAccelerator に渡す方法については、「3.4 カスケード接続する場合」（→ 33 ページ）を参照してください。
	消灯 - 通常の状態です。
Activity	点灯 - SSL 処理が実行中です。 この LED は、処理の負荷が小さい場合は暗く、大量のトラフィックが処理されている場合は明るく点灯します。
	消灯 - SSL 処理は実行されていません。
Network Link	点灯 - ケーブルが接続されている場合、ネットワーク側機器との接続は正常です。
	消灯 - ケーブルが接続されている場合、ネットワーク側機器との接続は異常です。
Inline	点滅（緑）- フェイルセーフモードです（デフォルト）。SSLAccelerator に障害が発生した場合、トラフィックは遮断されます。
	点灯（緑）- フェイルスルーモードです。SSLAccelerator に障害が発生した場合、トラフィックはバイパスされます。
	消灯 - SSLAccelerator が動作していないか、バイパスモードになっています。
Server Link	点灯 - ケーブルが接続されている場合、サーバ側機器との接続は正常です。
	消灯 - ケーブルが接続されている場合、サーバ側機器との接続は異常です。

■ コネクタ

以下に、SSLAccelerator のコネクタを示します。

コネクタ	種類	目的
Network 側コネクタ	RJ45	ネットワーク（クライアント）への 100BASE-TX/10BASE-T 接続です。ホストポートになります（パソコンなどのホストと同じ極性のポート）。
Server 側コネクタ	RJ45	サーバ（複数可）への 100BASE-TX/10BASE-T 接続です。ハブポートになります（ハブ／スイッチと同じ極性のポート）。
Console ポート	DB9	RS-232 DTE コンソールポートです（9600、8、N、1）。
Aux console ポート	DB9	RS-232 DTE コンソールポートです（115200、8、N、1）。起動時にカーネルの診断を行います。

2 設置と初期設定

この章では、SSLAccelerator の設置と初期設定の方法について説明します。

Contents

2.1 梱包物

箱の中に次の品物がそろっているか確認してください。万一、欠品などがございましたら、担当営業員までお申しつけください。

SSLAccelerator 7117

名称	備考
□ SSLAccelerator **本体**	
□**シリアルケーブル**	
□**電源ケーブル**	
□**ラックマウント用キット**	**ブラケット**× 2、**ネジ**× 4
□**ラック固定用キット**	**ネジ**× 4、**ナット**× 4
□**フロッピィディスク**	
□**取扱説明書（本書）**	
□**保証書**	

その他、添付されているドキュメントがある場合には、サーバ設置前に必ずお読みください。

添付品はシステムの変更時やソフトウェアの再インストール時に必要となるため、大切に保管してください。

2.2 設定の準備

インストールを開始する前に、次の情報を確認してください。

- サーバの IP アドレスとポート番号
- 鍵／電子証明書：テスト用の鍵と電子証明書は、SSLAccelerator でも作成できます。鍵と電子証明書の入手方法については、「第 4 章 鍵と電子証明書」（→ 39 ページ）を参照してください。
- ネットワークケーブル（ストレートケーブルまたはクロスケーブルなど）
  使用するケーブルのタイプについては、「2.4 ケーブル接続」（→ 16 ページ）を参照してください。
  コネクタの極性については、「■ コネクタ」（→ 5 ページ）を参照してください。

SSLAccelerator をラックに設置する場合は、以下の工具が必要です。

- プラスドライバ

本体のカバーを外さないでください。
お客様に設定および設置していただく部品や部位はありません。

2.3 設置

ここでは、本装置を設置する場合の注意事項および設置条件などについて説明します。

2.3.1 設置場所に関する注意

本装置を設置するときは、以下の場所は避けてください。

⚠警告

湿気・ほこり・油煙の多い場所、通気性の悪い場所、火気のある場所に設置しないでください。
故障・火災・感電の原因となります。

- **本体に水をかけないでください。**
  故障・火災・感電の原因となります。
- **風呂場、シャワー室などの水場で使用しないでください。**
  故障・火災・感電の原因となります。

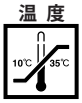
⚠注意

- **直射日光の当たる場所や、暖房器具の近くなど、高温になる場所には設置しないでください。また、10 ℃未満の低温になる場所には、設置しないでください。故障の原因となります。**
- **塩害地域では使用しないでください。故障の原因となります。**
- **電源ケーブルおよび各種ケーブル類に足がひっかかる場所には設置しないでください。故障の原因となります。**
- **テレビやスピーカの近くなど、強い磁界が発生する場所には設置しないでください。故障の原因となります。**
- **空気の吸排気口である装置前面部、背面部および左右側面部をふさがないでください。**
  これらをふさぐと内部に熱がこもり、火災の原因となります。
- **本体装置は、水平で安定した場所、および大きな振動の発生しない場所に設置してください。**
  振動の激しい場所や傾いた場所などの不安定な場所は、落ちたり倒れたりしてけがの原因になりますので、設置しないでください。
  また、通路の近くには、危険防止のため設置しないでください。通路の近くに設置すると、人の歩行などで発生する振動によって本体が故障したり誤動作する場合があります。
- **本装置の上に重いものを置かないでください。また、本装置の上に物を落としたり、衝撃を与えないでください。**
  バランスが崩れて倒れたり、落下したりしてけがの原因となります。また、本装置が故障したり誤動作する場合があります。
- **本装置を移動する場合は、必ず電源を切断し、ケーブル類を外してください。**

2.3.2 設置環境および設置条件

ここでは、設置環境および設置条件について説明します。

⚠注意



- **本装置は、周囲温度が 10 ～ 35 ℃の環境を守ってご利用ください。**
  特に 24 時間運転をする場合には空調のスケジュールなどを十分考慮し（夜間や休日など）、周囲温度をはずれた温度のもとで運用されることのないようにしてください。
  温度条件が守られないと、電子部品の誤動作や故障、寿命の短縮の原因となります。
  - **ー 特に夏場において 24 時間運用を行う場合、必要に応じて夜間・休日にも冷房を入れて、周囲温度が 35 ℃を超えないようにしてください。**
  - **ー 冬場など寒中での暖房時は、一時間あたりの温度上昇が 15 ℃を超さないように室温調整を行い、結露を発生させないようにしてください。**

■ 設置環境

本装置は、以下の環境条件を守ったうえで運用してください。環境条件をはずれた設置環境での運用は、本装置の故障や寿命を著しく短縮する原因となります。

温度（10 ～ 35 ℃）

直射日光の当たる場所、温度条件の厳しい場所を避けて設置してください。また、急激な温度変動は装置を構成する部品に悪影響を与え、故障の原因となるため、温度勾配は 10 ℃／時間以内が理想です。また、15 ℃／時間を超えるような環境は避けてください。

湿度（20 ～ 80%）

高湿度環境に設置すると、腐食性有害物質および塵埃との相乗作用による故障の原因となります。また、磁気媒体・帳票類へも悪影響を及ぼしますので、空調機などにより調整してください。

塵埃（オフィス環境：0.15mg ／ m^3 以下）

塵埃（ほこり、ちりなど）は磁気媒体やヘッドを傷つけたり、接触不良を起こす原因となります。また、腐食性有害物質および湿気との相乗作用により装置に悪影響を与えるため、空調機を装備したエアフィルタで塵埃を除去するなどの対策が必要です。

■ 本装置環境条件

項目		設置条件
温度	動作時	10 ～ 35 ℃
	休止時	0 ～ 50 ℃
湿度	動作時	20 ～ 80%RH（結露しないこと）
	休止時	
温度勾配	動作時	15 ℃ /hr 以下（結露しないこと）
	休止時	
AC 入力条件	電圧	AC100 ～ 120V
	周波数	50/60Hz
浮遊塵埃		0.15mg/m^3 以下

■ 設置スペース

本装置は、ラックに搭載して運用します。
ラックの設置スペースについては、ラックに添付の取扱説明書を参照してください。

⚠注意

**本装置の上に重いものを置かないでください。また、本装置の上に物を落としたり、衝撃を与えないでください。
バランスが崩れて倒れたり、落下したりしてけがの原因となります。また、本装置が故障したり誤動作する場合があります。**

2.3.3　ラックへの設置

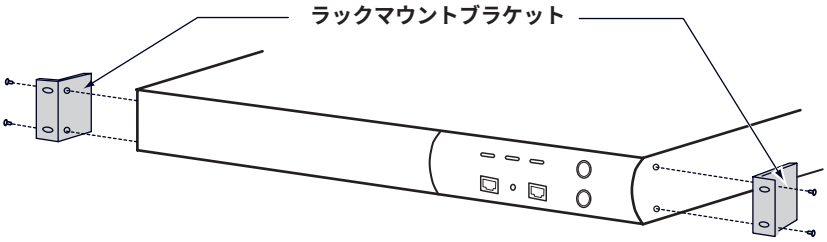
ここでは、本装置をラックに搭載する手順について説明します。

1　**本装置の両側面にラックマウントブラケットを 1 個ずつ取り付けます。手順は次のとおりです。**

1　**同梱されているラックマウントブラケット 2 個とネジ 4 本（短い銀色ネジ）を使用します。**

2　**ラックマウントブラケットには円形の取り付け孔と楕円形の取り付け孔がありますが、本装置への取り付けには円形、ラックには楕円形を使用します。**

3　**本装置の前面付近にある取り付け孔にラックマウントブラケットの取り付け孔を合わせ、ネジを締めつけます。**

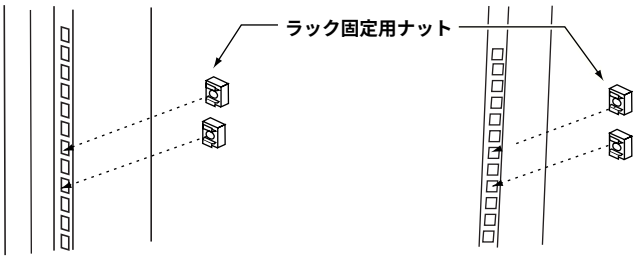


2　**本装置を 19 インチラック上に設置し、ラックマウントブラケットをラックに固定します。手順は次のとおりです。**

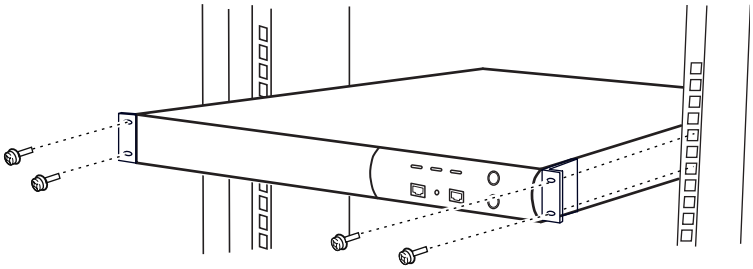
1　**同梱されているラック固定用ナット 4 個と、ネジ 4 本（長い銀色ネジ）を使用します。**

2　**ラックマウントブラケット前面にある楕円形の取り付け孔を使用します。**

3　**本装置を設置する位置の 19 インチラックの柱の裏側に、ラック固定用ナットを 4 個取り付けます。**



4 ラックマウントブラケット前面の楕円から、取り付け孔にラック固定用ネジを通し、手順 3 で取り付けたナット（4 個）と固定します。



⚠注意

本装置の前面に接続されるケーブルを背面側に配線する場合に備えて、ラックに設置した本装置の下側 1U（ラック柱穴 3 個分）は未設置とし、空けておくようにしてください。

2.4　ケーブル接続

SSLAccelerator は、次に示す どちらのモードでもネットワークに接続できます。

- インパス接続
  Network 側ポートがルータまたはスイッチに接続されて、Server 側ポートがサーバまたはサーバファームに接続されます。
- ワンアーム接続
  レイヤ -4（以降、L4 と略記）スイッチにサーバを接続しているシステムにおいて、SSLAccelerator を接続する場合にこの接続形態を利用することができます。
  この接続形態では、SSLAccelerator は Network 側ポートを L4 スイッチに接続することによって、L4 スイッチとサーバ間の接続を変更することなく、SSLAccelerator を導入することができます。

■ インパス接続によるネットワークの接続

1　次の表を参照して、インパス接続に適切なケーブルを選択して接続します。

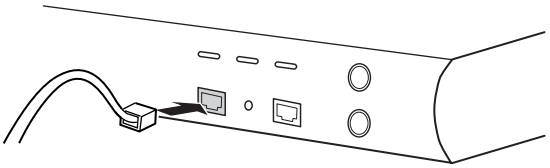
ケーブルはすべて、カテゴリ 5 UTP 以上のものを使用してください。

	SSLAccelerator **ネットワークコネクタ**	SSLAccelerator **サーバコネクタ**
ワークステーション またはサーバ	**クロスケーブル**	**ストレートケーブル**
スイッチまたはハブ	**ストレートケーブル**	**クロスケーブル**
ルータ	**クロスケーブル**	**推奨外**
SSLAccelerator **ネットワークコネクタ（*）**	**対象外**	**ストレートケーブル**
SSLAccelerator **サーバコネクタ（*）**	**ストレートケーブル**	**対象外**

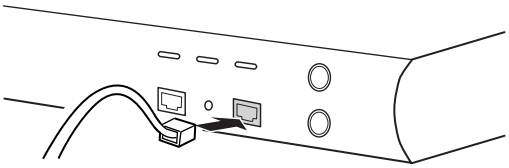
（*）複数の SSLAccelerator **をカスケード接続する場合のみ有効です。**

1　上記の表を参考に適切なケーブルを選択して、SSLAccelerator **の左側の** RJ-45 **コネクタをネットワークに接続します。**

接続が有効であれば、Network LED が点灯します。LED が点灯しない場合は、クロスケーブルを使用してもう一度接続してください。

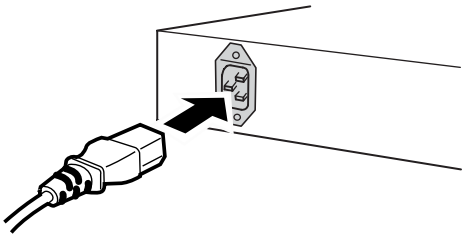


2 **表を参考に適切なケーブルを選択して、**SSLAccelerator **の右側の** RJ-45 **コネクタを他の** SSLAccelerator **（カスケード接続の場合）、またはサーバ側（ハブまたはサーバ）に接続します。**
接続が正常に行われていれば、Server LED が点灯します。LED が点灯しない場合は、クロスケーブルを使用してもう一度接続してください。



⚠注意 **両方のポートを同じネットワークセグメント（同じハブまたはスイッチ）に接続しないでください。同じネットワークセグメントに接続すると、フィードバックループが形成され、ネットワーク帯域幅に悪影響が生じます。**

2 **本装置に添付の電源ケーブルを** SSLAccelerator **本体背面の電源ソケットに接続します。**
普通の状態では、SSLAccelerator は、約 90 秒ほどの起動時間を必要とします。起動が完了すると、本体の Power LED が点灯します。また、インラインモードになると、Inline LED が点灯または点滅します。



3 Network LED **と** Server LED **の両方が点灯します。**
点灯しない場合は、「第 8 章 トラブルシューティング」（→ 181 ページ）を参照してください。

4 **同梱のシリアルケーブルで、本体のシリアルポート（左側の** Console **ポート）とターミナル（たとえば、ハイパーターミナルが動作している** Windows **ベースの パソコン）を接続します。**

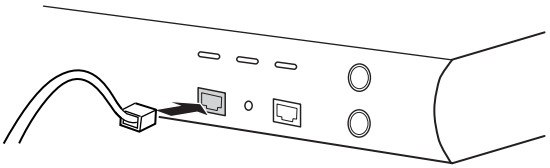
■ ワンアーム接続によるネットワークの接続

Network 側ポートと Server 側ポートの両方を使用して接続されるインパス接続とは異なり、ワンアーム接続では Network 側ポートだけを使用してスイッチに接続します。

⚠注意 ワンアーム接続には、Network 側ポートだけを使用してください。Server 側ポートを使用すると、この機能は働きません。

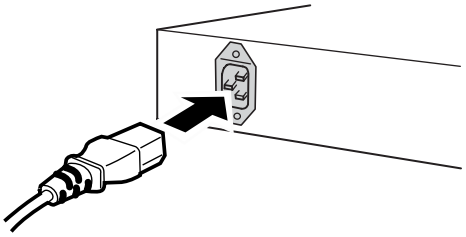
1 **ストレートケーブルを使用して、**SSLAccelerator **の** Network **側ポートとスイッチのポートを接続します。**

ケーブルは カテゴリ 5 UTP 以上のものを使用してください。



2 **本装置に添付の電源ケーブルを** SSLAccelerator **本体背面の電源ソケットに接続します。**

普通の状態では、SSLAccelerator は、約 90 秒ほどの起動時間を必要とします。起動が完了すると、本体の Power LED が点灯します。また、インラインモードになると、Inline LED が点灯または点滅します。



3 Network LED **が点灯します。**

点灯しない場合は、「第 8 章 トラブルシューティング」（→ 181 ページ）を参照してください。

4 **同梱のシリアルケーブルで、本体のシリアルポート（左側の** Console **ポート）とターミナル（たとえば、ハイパーターミナルが動作している** Windows **ベースの パソコン）を接続します。**

■ ステータスの確認

「2.5 初期設定」（→ 19 ページ）に進む前に、SSLAccelerator が正常に接続されているかどうか確認してください。

- Network LED と Server LED

  インパス接続を使用している場合は、Network LED と Server LED がどちらも点灯していることを確認してください。一方または両方の LED が点灯していない場合は、「第 8 章 トラブルシューティング」（→ 181 ページ）を参照してください。

  ワンアーム接続を使用している場合は、Network LED だけが点灯します。

- Inline LED

  インパス接続の場合、Inline LED が点滅している場合は、システムがフェイルセーフモードでオンラインになっていることを示します。Inline LED が点灯している場合は、システムがフェイルスルーモードでオンライン状態であることを示します。フェイルセーフモードとフェイルスルーモードについての詳細は、「第 8 章 トラブルシューティング」（→ 181 ページ）または「A.3 障害／バイパスモード」（→ 192 ページ）を参照してください。

  ワンアーム接続の場合、Inline LED が点灯または点滅していることを確認してください。

2.5 初期設定

■ 管理ターミナルの接続

パソコン上で、ハイパーターミナルなどの端末エミュレータを実行します。以下の手順は、ハイパーターミナルについて説明したものです。他の装置をご使用の場合は、手順が異なります。

1 **本体のシリアルポート（左側の「**Console **」と表記されている方）と、任意の端末（ここでは、**Windows **ハイパーターミナルを稼動するパソコン）のシリアルポートを** SSLAccelerator **に付属のシリアルケーブルを使用して接続します。**

2 **接続の設定ウィンドウの名前フィールドに適切な名前（ここでは** "SSL Configuration"**）を入力し、**［OK］**をクリックします。**
電話番号パネルが表示されます。

3 **接続方法フィールドの**［COM1］**を選択します。**
COM1 以外を使用する場合は、パソコンと SSLAccelerator 本体の接続に使用しているシリアルポートを選択します。

4 ［OK］**をクリックします。**
COM1 のプロパティパネルが表示されます。

5 **［標準に戻す］をクリックします。**
ビット／秒、データビット、パリティ、ストップビット、フロー制御の各フィールドの値が、それぞれ「9600」、「8」、「なし」、「1」、「なし」になります（［標準に戻す］ボタンをクリックしても、フロー制御が「なし」にならない場合は、手動で設定してください）。

6 ［OK］**をクリックします。**

■ ハイパーターミナルの貼り付け操作

設定を次のように変更すると、貼り付け操作が迅速に行えます。

1 **［ファイル］メニューで、［プロパティ］を選択します。**

2 **［設定］タブをクリックします。**

3 ［ASCII **設定**］**ボタンをクリックします。**

4 **「ディレイ（行）」および「ディレイ（文字）」の値を、**0 ～ 1msec **以上の値に変更します。**

5 ［OK］**をクリックして** ASCII **設定を終了します。**

6 ［OK］**をクリックして接続の設定を終了します。**

■ コマンドラインインターフェースへのアクセス

電源ケーブルの接続が完了して SSLAccelerator が起動すると、ハイパーターミナルに Password プロンプトが表示されます。表示されない場合は、［Enter］キーを押します。

1 **Password プロンプトに「admin」と入力し、［Enter］キーを押します。**
プロンプトが表示されます。

```
password: admin （プロンプトにはパスワードは表示されません）
Current date: 2000 03/01 15:59
#
```

これで、SSLAccelerator のコマンドラインインターフェース（CLI）から操作を行う準備ができました。
次に、一般的な操作の開始方法を示します。

⚠注意 **パスワードはコマンドライン上に表示されません。**

2 **パスワードを「admin」から別のものに変更します。**
変更には、password コマンドを使用します。

```
# password
```

設定したパスワードは、自動的にフラッシュメモリに保存されるため、装置の再起動後も有効です（config save コマンドを実行する必要はありません）。

3 **タイムゾーンを設定します。**

1 **使用可能なタイムゾーンを確認します。**
使用可能なタイムゾーンのリストを表示するには、list timezone コマンドを実行します。

```
# list timezone
```

2 set timezone **コマンドを実行して、適切なタイムゾーンを設定します。**

```
# set timezone Asia/Tokyo
```

4 **日付や時刻を変更する必要がある場合は、**set date **コマンドを実行します。**

ポイント

電子証明書の有効性は、日付と時刻によって決まります。

⚠注意

日付を設定すると、SSLAccelerator **が再起動します。**

```
# set date
```

5 **使用可能なコマンドを一覧表示する場合は、**help **コマンドを実行します。**
これらのコマンドは、「5.4 コマンド一覧」（→ 80 ページ）でも確認できます。

```
# help
```

6 **鍵と電子証明書のセットアップを行います。**
詳細については、「第 4 章 鍵と電子証明書」（→ 39 ページ）を参照してください。

■ 設定の続行

これで、SSLAccelerator の基本的な設定が完了しました。実際の構成に合わせてさらに SSLAccelerator を設定するには、「第 3 章 構成」（→ 23 ページ）に進んでください。

3 構成

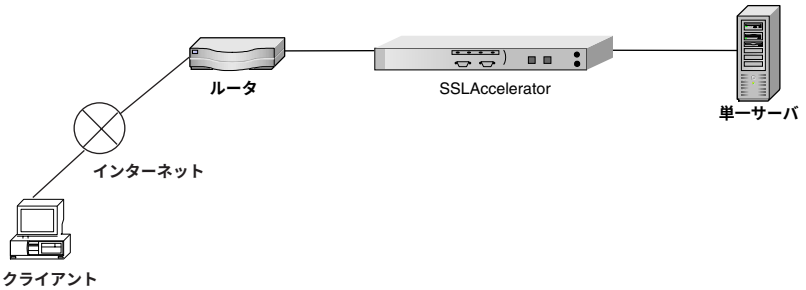
この章では、以下の構成例に対し SSLAccelerator の設定方法を図とともに示します。

- 単一サーバ構成
- 複数サーバ構成
- ITM デバイスを使用する構成
- 複数の SSLAccelerator をカスケード接続する構成
- 送信用ルータと受信用ルータが異なる構成

Contents

3.1 単一サーバの場合

SSLAccelerator は、単一のサーバでの SSL 処理の要求に対処する構成で使われる場合がよくあります。単一サーバ構成は、最も単純で一般的なサーバ構成です。このサーバ構成では、SSLAccelerator をルータとサーバの間にあるネットワークに接続します。設置においては、セキュリティを高め、管理をしやすくするために、SSLAccelerator とサーバを同じラックに配置する等、近距離に配置することを心がける必要があります。



以下に、SSLAccelerator を単一のサーバとともに使用する場合の一般的な設定について述べます。ここでは自動マッピングを用いる場合と、手動設定（手動マッピング）を用いる場合の両方について述べます。この例は、SSLAccelerator を使用する場合の最も簡単な例となります。

■ 自動マッピング

1 **SSLAccelerator をルータとサーバに接続します。**

2 **サーバへの** HTTPS **トラフィックを発生させます。**

SSLAccelerator は、トラフィックを監視して、初期マッピング（および対応するデフォルトの鍵と電子証明書）を使用して HTTPS トラフィックを復号化し、クリアテキスト HTTP トラフィックをサーバに渡します。

■ 手動設定

1 **「第 2 章 設置と初期設定」（→ 7 ページ）の手順に従って、SSLAccelerator 本体を設置します。**

次に、コマンドラインインターフェースにアクセスしプロンプトを表示させます。

2 **「第 4 章 鍵と電子証明書」（→ 39 ページ）の手順に従って、適切な鍵と電子証明書の設定を行います。**

3 **サーバに対するマッピングを作成します。**

create map コマンドを使用して、サーバの IP アドレスとポート番号、そして KeyID を関連づけます。

```
# create map
Server IP (0.0.0.0): 10.1.1.30
SSL (network) port [443]: <Enter>
Cleartext (server) port [80]: <Enter>
KeyID to use for mapping: myserver
```

4 **マッピングが正しく行われており、有効であることを確認します。**

マッピングを変更したい場合は、上記のコマンドを使用して作成し直してください。

```
# list map
Map                                  Net   Ser  Cipher          Re-     Client
ID  KeyID      Server IP             Port  Port  Suites         direct  Auth
== ======== ========== ==== ==== ========== ===== ====
1  default    Any        443   80   all(v2+v3)     n       n
2  myserver   10.1.1.30  443   80   med(v2+v3)     n       n
```

5 **デフォルトのマッピングを削除することが可能です。**

削除する場合は、マッピングを手動で作成したあとに、デフォルトのマッピングを削除します。この例の場合は MapID 1 のマッピング（デフォルトのマッピング）を削除します。デフォルトのマッピングを削除すると MapID 2 の MapID は 1 に変更されます。

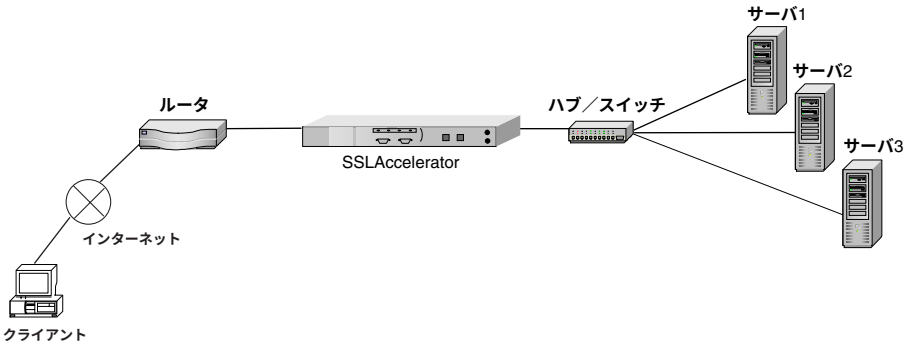
```
# delete map 1
# list map
Map                                  Net   Ser  Cipher          Re-     Client
ID  KeyID      Server IP             Port  Port  Suites         direct  Auth
==  ======== ========== ==== ==== ========== ===== ====
 1  myserver   10.1.1.30  443   80   med(v2+v3)     n       n
```

6 **サーバのマッピングが作成されたら、その設定を保存します。**

```
# config save
Saving configuration to flash...
Configuration saved to flash
```

3.2 複数サーバの場合

SSLAccelerator は、SSL 処理を複数サーバ構成で行うときにも使用できます。複数サーバ構成では、SSLAccelerator をルータとハブの間に接続します。サーバに向けて送信された SSL トラフィックを、SSLAccelerator がいったん取り込み、処理を行います。その他のトラフィックはそのまま通過していきます。



以下に、複数サーバ環境で設定する方法について説明します。

1 **「第 2 章 設置と初期設定」（→ 7 ページ）の手順に従って、SSLAccelerator 本体を設置します。**

次に、コマンドラインインターフェースにアクセスしプロンプトを表示させます。

2 **「第 4 章 鍵と電子証明書」（→ 39 ページ）の手順に従って、適切な鍵と電子証明書の設定を行います。**

3 **サーバ 1 に対するマッピングを作成します。**

create map コマンドを使用して、サーバの IP アドレスとポート番号、そして KeyID を関連づけます。

```
# create map
Server IP: 10.1.1.30
SSL (network) port [443]: <Enter>
Cleartext (server) port [80]: <Enter>
KeyID to use for mapping: myserver
```

4 **サーバ 2 に対するマッピングを作成します。**

create map コマンドを使用して、サーバの IP アドレスとポート番号、そして KeyID を関連づけます。

```
# create map
Server IP: 10.1.1.31
SSL (network) port [443]: <Enter>
Cleartext (server) port [80]: <Enter>
KeyID to use for mapping: myserver2
```

5 **サーバが** 3 **台以上ある場合は、サーバ** 3 **以降のサーバに対して、上記の手順** 4 **の処理を、**IP **アドレスをサーバの** IP **アドレスに変更して行います。**

6 list maps **コマンドを使用して、現在の作成されているマッピングを表示します。**

（複数の鍵と電子証明書をインポートし、それぞれのサーバに対してマップすることが可能です。）

```
# list map
Map                                  Net   Ser   Cipher              Re-       Client
ID  KeyID      Server IP             Port  Port  Suites              direct    Auth
==  ========== ========== ========== ====  ====  ==========          ======    ======
 1  default     Any                  443   80    all(v2+v3)          n         n
 2  myserver    10.1.1.30            443   80    med(v2+v3)          n         n
 3  myserver2   10.1.1.31            443   80    med(v2+v3)          n         n
```

7 **必要に応じて、デフォルトのマッピングを削除します。**

削除する場合は、マッピングを手動で作成したあとに、デフォルトのマッピングを削除します。この例では、MapID 1 のマッピング（デフォルトのマッピング）を削除します。デフォルトのマッピングを削除すると MapID 2 の MapID は 1 に変更されます。

```
# delete map 1
# list map
Map                                  Net   Ser   Cipher              Re-       Client
ID  KeyID      Server IP             Port  Port  Suites              direct    Auth
==  ========== ========== ========== ====  ====  ==========          ======    ======
 1  myserver    10.1.1.30            443   80    med(v2+v3)          n         n
 2  myserver2   10.1.1.31            443   80    med(v2+v3)          n         n
```

8 **サーバのマッピングが作成されたら、設定を保存します。**

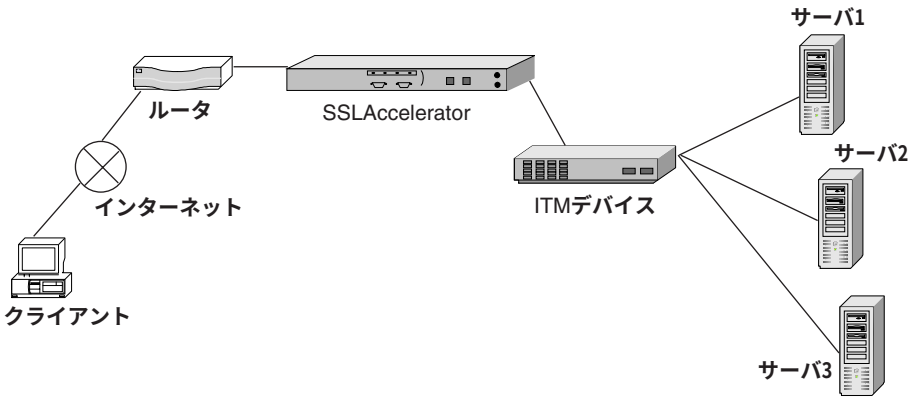
```
# config save
Saving configuration to flash...
Configuration saved to flash
```

3.3 ITM デバイスを使用する場合

SSLAccelerator には、ITM（Internet Traffic Management）デバイスとの互換性があります。ITM デバイスは、通信負荷を複数のサーバに分散させ、内容ごとにトラフィックを分類してリダイレクトします。

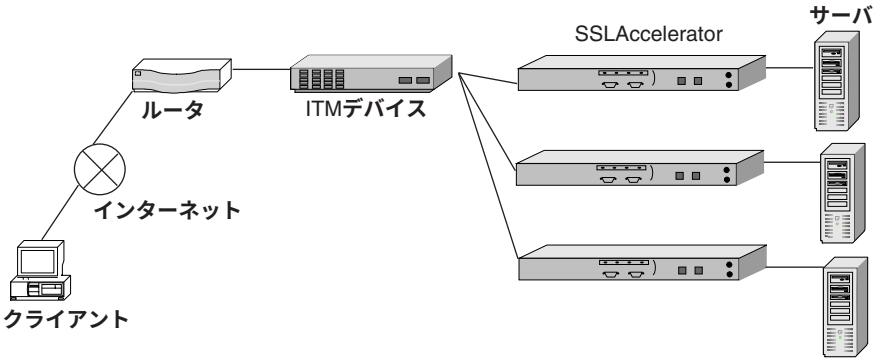
3.3.1 クライアントネットワーク側への配置

ITM デバイスが L7 のトラフィック管理をサポートしている場合は、トラフィック上の URL が読み取り可能（暗号化されていない）であることが必要です。このような環境では、SSLAccelerator を ITM デバイスとクライアントネットワークの間に配置することを推奨します。



3.3.2 サーバ側への配置

セキュリティ要件で、暗号化されていないデータによる通信を制限している場合は、SSLAccelerator を ITM デバイスとサーバの間に配置する必要があります。



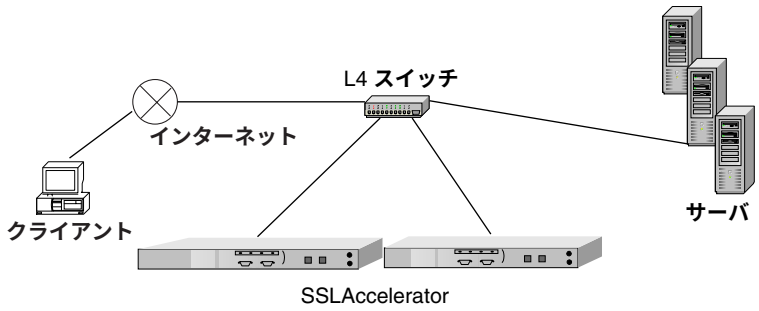
⚠注意

この構成を採用する場合は、L7 のロードバランシングを行うことができません。この構成では、ITM デバイスを通過するセキュアトラフィックは暗号化されているからです。

3.3.3 ワンアーム接続での配置

■ ワンアーム接続

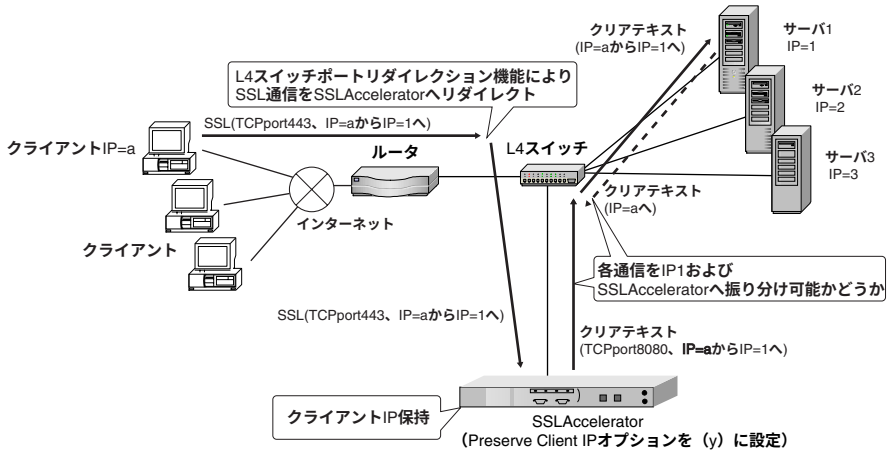
L4 スイッチにサーバを接続しているシステムにおいて、L4 スイッチとサーバ間の物理的接続を変更することなく、SSLAccelerator の導入および追加が可能です。



■ 推奨スイッチ

ワンアーム接続では、SSLAccelerator はポートリダイレクト機能をサポートしている L4 スイッチに接続する必要があります。また、set onearm コマンドで Preserved Client IP オプションを（y）に設定する場合には、フルキャッシュサーバトランスペアレンシ機能（Full Cache Server Transparency）をサポートしている L4 スイッチに接続する必要があります。

以下に、SSLAccelerator をワンアーム接続で使用した場合の構成例を示します。



クライアントからの SSL 通信は、L4 スイッチによってリダイレクトされ、SSLAccelerator で復号化されたあとに、サーバにクリアテキストの状態で送信されます。set onearm コマンドで Preserved Client IP オプションを（y）に設定した場合、この復号パケットの送信元 IP アドレスはクライアントの IP アドレスです。サーバからの戻りパケットに関して L4 スイッチが SSLAccelerator 側にリダイレクトさせ

るための処理ができない場合、サーバからの戻りパケットはクライアントに直接送信され、通信が成立しません。
通信を成立させるためには、L4 スイッチがサーバからの戻りパケットを SSLAccelarator にフォワードする必要があります。また、この SSL 通信と同時に、SSL 以外の通信は SSLAccelerator を経由することなく、クライアントとサーバの間で直接通信される必要があります。
本書ではこのような機能をフルキャッシュサーバトランスペアレンシ （Full Cache Server Transparency）と呼びます。

■ ワンアーム接続への変更

インパス接続からワンアーム接続へ変更する場合には、以下の作業が必要です。

- LAN ケーブルの接続変更
- ワンアーム接続に必要なコマンドの実行

ワンアーム接続の管理には、次の 2 つの CLI コマンドを使用します。

- show onearm コマンドは、SSLAccelerator の現在の状態（インパス接続またはワンアーム接続）を表示します。
- set onearm コマンドは、キーワード enable または disable とともに使用して、ワンアーム接続をオンまたはオフにします。

例：

```
# show onearm
Running Inpath Operation
# set onearm enable
Preserve client IP (y/n)? [n]: <Enter>
One-arm mode enabled.
# show onearm
Running One-arm Operation
```

ワンアーム接続の動作には、次の制限があります。

- 現在サポートされているスイッチで動作するための IP アドレスを、SSLAccelerator に割り当てる必要があります。
- SSLAccelerator は、サーバとの通信に独自の IP アドレスを使用します。
- SSLAccelerator をカスケード接続することができません。
- 状況監視機能には、ICMP だけがサポートされています。
- ワンアーム接続が機能するのは、SSLAccelerator の Network 側ポートが、対応している L4 スイッチに接続されている場合だけです。
- ブロック（block）と許可（permit）は使用できません。

SSLAccelerator がワンアーム接続で動作している場合は、ほかのプロセスや装置（ロードバランサなど）から ICMP（ping）クエリを発行しても、そのクエリからはサーバが見えないことがあります。map visible 機能を使用すると、SSLAccelerator の背後で動作するサーバに ICMP でアクセスできるようになります。この機能を有効にすると、SSLAccelerator のマップのインバウンド IP アドレスがスイッチに認識されるため、SSLAccelerator は arp 要求および ping 要求に応答できるようになります。set および show のコマンドサブセットを使用すると、map visible 機能のオン / オフの切り替えや現在の状態を確認できます。

例：

```
# show map_visible
map_visible: disabled
# set map_visible enable
map_visible is enabled.
# show map_visible
map_visible: enabled
```

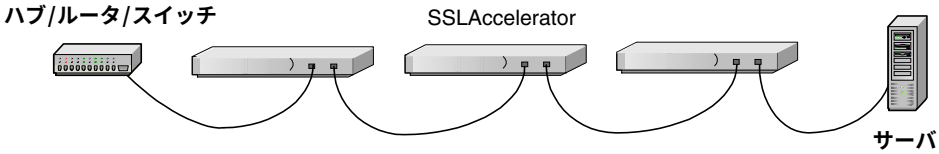
3.4 カスケード接続する場合

■ スケーラビリティとカスケード接続

複数の SSLAccelerator をカスケード接続することにより、SSLAccelerator の性能を拡張できます。カスケード接続では、前段の SSLAccelerator の Server 側コネクタと後段の SSLAccelerator の Network 側コネクタをケーブルで接続して、最後段に接続した SSLAccelerator の Server 側コネクタをスイッチやサーバまたは ITM デバイスに接続します。

■ Spill と Throttle

SSLAccelerator の「spill」（spill は「あふれ」と言う意味）オプションが有効になっている場合は、SSLAccelerator がある特定の時間内でリクエストを処理しきれなかった場合、そのリクエストは処理されずそのまま暗号化された状態で次段のインライン状態の SSLAccelerator に渡されます。また、最後段の SSLAccelerator でも「spill」が有効になっていれば、同様に、そこで処理できなかったリクエストはそのままサーバに渡されることとなります。この spill 機能は接続ごとに動的に動作します。つまり、各 SSLAccelerator ごとに単独で、他の SSLAccelerator と連携せずに動作状態が決定されます（spill コマンドについては「5.5.6 操作コマンド」（→ 105 ページ）を参照してください）。spill 機能が無効になっている場合は、SSLAccelerator は「throttle」状態になります。この場合、SSLAccelerator は、過負荷状態が解消されるまで、着信した要求を受け入れません。



SSLAccelerator による処理を待機している、SSL ハンドシェークの数をハードウェア待ち行列といいます。この数が最高点（hwq_hiwat_spill）を超えると、SSLAccelerator は spill モードになって、それ以降の SSL 接続をカスケードの次の SSLAccelerator に渡します。待ち行列内の SSL ハンドシェーク数が最低点（hwq_lowat_spill）より少なくなるまで spill モードを維持します。

ステータス画面に表示された IDLE CPU のパーセンテージが 5% 未満の場合は、ハードウェア待ち行列の長さを下方修正する必要があります。set hwq_hiwat_spill と set hwq_lowat_spill を入力して通常のトラフィック負荷で IDLE CPU が 5% を超えるまで、または最高点と最低点が最小値の 1 に達するまで、両水準点を下げてください。

IDLE CPU が非常に高く、システムがいつまでもあふれているように見える場合は、ハードウェア待ち行列の長さを上方修正する必要があります。set hwq_hiwat_spill と set hwq_lowat_spill を入力して最高点と最低点を引き上げ、望ましいタイミングで spill モードのオンとオフが切り替わるようにしてください。

ポイント

工場出荷時の最高点および最低点のデフォルト値は、ほとんどの環境に対応しています。
hwq_hiwat_spill および hwq_lowat_spill パラメタは、SSLAccelerator が希望どおりに spill モードに入らない場合にのみ使用してください。

■ 可用性（Availability）

フェイルスルーモードが有効になっているときに、SSLAccelerator に障害が発生した場合、またはバイパスモードに設定した場合、SSLAccelerator は、その機能がなんらかの原因によって停止したときに、2 つの RJ-45 コネクタを内部で直接接続し、停止状態が解除されるまで、トラフィックを何の処理もせずに通過させます。この機能により、単一の SSLAccelerator の故障がネットワーク全体に影響を与えるのを防止し、高いレベルの可用性を提供することが可能になります。また、前述したように、複数の SSLAccelerator を用いる場合は、後段にカスケードされるユニットによって暗号化／復号化処理能力を追加することができます。また、単一の SSLAccelerator を用いる場合でも、サーバに処理の一部を任せることができます。詳細については、「A.3 障害／バイパスモード」（→ 192 ページ）を参照してください。

以下に、複数の SSLAccelerator をカスケードに接続し、その処理能力と可用性を拡張する場合の設定方法を説明します。

仮定

- 2 つ以上の SSLAccelerator を同じネットワーク上に接続します。SSLAccelerator をカスケード接続するためには前段（ネットワーク側）の SSLAccelerator のサーバ用ポートを次段の SSLAccelerator のネットワーク用ポートに接続します。この接続を最終段まで繰り返し、最終段の SSLAccelerator のサーバ用ポートをサーバに接続します（より詳しい情報については「第 2 章 設置と初期設定」（→ 7 ページ）を参照してください）。
- 初段の SSLAccelerator 上で、set spill enable コマンドを使用して spill 処理を有効にします。これで、初段の SSLAccelerator が処理できなかったデータは、次段の SSLAccelerator が処理します。後段の SSLAccelerator についても、順番に spill 処理を有効にします（最終段の SSLAccelerator を除く）。サーバにあふれ出た処理を引き継がせたい場合は、同様に、最終段の SSLAccelerator で、set spill enable コマンドを実行します。
- 初段の SSLAccelerator はすべて設定済みであり、必要な鍵、電子証明書、およびマップが存在していなければなりません。この設定を初段の SSLAccelerator からエクスポートし、次段の SSLAccelerator にインポートします。後段の SSLAccelerator についても、順番にこの手順を繰り返します。

■ 手順

1 **初段の** SSLAccelerator **に対し必要な設定を行います。**
後段に接続される他の SSLAccelerator はこの設定をエクスポートして使用します。

2 **コマンドプロンプトから「**set spill enable**」と入力し、あふれ出た処理を後段に処理させるようにします。**

3 **設定を保存します。**

```
# config save
Saving configuration to flash...
Configuration saved to flash
```

4 **設定をエクスポートします。**
export config コマンドを使用し、XMODEM でエクスポートします。

```
# export config
Garble or encrypt all keys: (garble, encrypt) [encrypt]: <Enter>
Enter a pass phrase to encrypt all keys []: pass
Enter the pass phrase again to confirm []: pass
Export protocol: (xmodem, ascii) [ascii]: xmodem
Press Ctrl-X multiple times to kill transmission
Beginning export...
```

5 **ハイパーターミナルの［転送］メニューで［受信］を選択します。**

6 **ディレクトリ名を入力するか、または［参照］ボタンを使用して、受信したファイルを保存するディレクトリを指定します。**

7 **受信プロトコルとして［**XMODEM**］を選択します。**

8 **［受信］ボタンをクリックします。**

9 **受信したファイルのファイル名を指定し、［**OK**］をクリックします。**
処理は終了し、通常のプロンプトが再表示されます。

```
Export successful!
#
```

10 2 **段目の** SSLAccelerator **にシリアルケーブルを接続し直し、パスワードを入力してコマンドプロンプトを表示させておきます。**

11 2 **段目の** SSLAccelerator **のフロントパネルにある** Bypass **ボタンを押して、**2 **段目の** SSLAccelerator **をバイパスモードにします。**

12 **設定をインポートします。**

import config コマンドを使用して、処理を開始させます。まず、［XMODEM］を選びます。次に、［Enter］キーを押して、SSLAccelerator 本体へのインポート処理を開始させます。

```
# import config
Import protocol: (paste, xmodem) [paste]: xmodem
Start xmodem upload now
Press Ctl-X multiple times to cancel upload
```

13 **ハイパーターミナル の［転送］メニューで［送信］を選択します。**

14 **ファイル名を入力するか、または［参照］ボタンを使用して、送信するファイルを指定します。**

15 **送信プロトコルとして［XMODEM］を選択します。**

16 **［送信］ボタンをクリックします。転送が完了し、この設定をインストールするかどうか確認するプロンプトが表示されます。**

```
Do you want to install this config? [y]: <Enter>
```

17 **パスワードを入力すると、プロンプトが再表示されます。**

```
Enter a pass phrase to decrypt all encrypted keys []: pass
/keys/1/key.pem is encrypted and decrypted with the pass phrase.
/keys/default/key.pem is encrypted and decrypted with the pass phrase.
#
```

ポイント

間違ったパスワードを入力すると、次のようなメッセージが表示され、インポートに失敗します。
Imported configuration is invalid. Rollback to existing config...

18 **設定を保存します。**

```
# config save
Saving configuration to flash...
Configuration saved to flash
```

19 **2 段目 の** SSLAccelerator **のフロントパネルにある** Bypass **ボタンを押して、2 段目の** SSLAccelerator **をインラインモードにします。**

20 **上記の手順** 10 **〜** 20 **を 3 段目以降に接続した** SSLAccelerator **に対して繰り返します。**

21 **必要に応じて、最終段の** SSLAccelerator **で** set spill disable **コマンドによって、あふれ出た処理をサーバに引き渡さないように設定します。**

この設定を行った場合は、再度 config save コマンドで設定を保存してください。

⚠注意

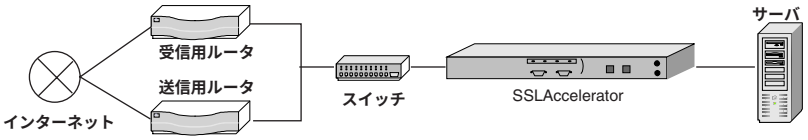
本装置をカスケード接続で使用する場合は、カスケードされる SSLAccelerator の IP アドレスをそれぞれ異なった IP アドレスにする必要があります。

3.5 送信用ルータと受信用ルータが異なる場合

SSLAccelerator に接続されたルータとして SSLAccelerator 側からの送信用ルータと受信用ルータが異なるものを使用する場合の構成について説明します。

仮定

- 単一または複数のサーバを接続します。
- 1 台以上の SSLAccelerator を使用します（複数の SSLAccelerator をカスケードすることも可能です）。
- 1 台以上の受信用ルータ（クライアント側からサーバ側へのトラフィックを扱うルータ）を使用します。
- 1 台の送信用ルータ（サーバ側からクライアント側へのトラフィックを扱うルータ）を使用します。



■ 手順

1 SSLAccelerator **の一般的な（送受信用のルータが同じ場合の）設定を行います。**
サイト構成に合わせて、前述の例で行った設定を行います。

2 SSLAccelerator **からクライアント側へ送るトラフィックを扱う送信用ルータの** MAC **アドレスを調べます。**

3 **コマンドラインから、デフォルトで用いる送信用ルータを指定し、設定を保存します。**

```
# set egress_mac 00:11:22:33:44:55
Egress MAC set to 00:11:22:33:44:55
# config save
Saving configuration to flash...
Configuration saved to flash
```

設定を無効にするためには以下のように入力します。

```
# set egress_mac none
```

⚠注意 **サーバのデフォルトゲートウェイとして、送信用ルータが設定されている場合は、**arp -a **コマンドをサーバから実行して、デフォルトゲートウェイの** MAC **アドレスを得ることができます。この** MAC **アドレスを使用してください。**

4 鍵と電子証明書

この章では、SSLAccelerator を使用するときに必要な鍵と電子証明書について説明します。

Contents

4.1 概要

SSLAccelerator を使用するには、鍵と電子証明書が必要です。鍵は、データの暗号化／復号化に使用される一連の数値です。また、電子証明書は、サーバやユーザを特定化する「書類」です。電子証明書には、ユーザの会社に関する情報のほか、ユーザの身元を証明する第三者の情報も含まれています。
鍵と電子証明書は、次の 3 とおりの方法で取得できます。

- VeriSign 社をはじめとする認証局から電子証明書を取得
- 既存の鍵／電子証明書を使用
- 新しい鍵／電子証明書を SSLAccelerator で作成

⚠警告 **SSLAccelerator ではテスト用に電子証明書を作成することができますが、実際に使用する電子証明書は、認知されている認証局から取得する必要があります。**

■ ハイパーターミナルでのカット & ペースト

次のいくつかの手順では、カット & ペースト機能を使用します。ここでは、ハイパーターミナルを使用するものとしてカット & ペーストの方法を説明します。これ以外のターミナルプログラムを使用する場合は、その製品のマニュアルに記載されている正しい手順を参照してください。
ハイパーターミナルからアイテム（鍵データ、署名要求、証明書等）をコピーするには、次のようにします。

1 **［ハイパーターミナル］ウィンドウを開きます。**
2 **アイテムを選択して、［編集］メニューを開き、［コピー］をクリックします** ［Ctrl］+［C］。
3 **データの貼り付け先のウィンドウを開き、適切な位置にカーソルを置きます。**
4 **［編集］メニューの［貼り付け］をクリックします** ［Ctrl］+［V］。

以上の操作は最初の 1 回のみ行います。

ハイパーターミナルにコピーしたアイテム（鍵データ、署名要求、証明書等）を貼り付ける（ペーストする）には、次のようにします。

1 **適切なアプリケーションウィンドウ内のアイテムを表示し、クリックとドラッグによってそのアイテムを選択します。**
2 **アイテムを選択して［編集］メニューをクリックし、［コピー］を選択します** ［Ctrl］+［C］。
3 **［ハイパーターミナル］ウィンドウに移動し、適切な位置にカーソルを置きます。**
4 **［編集］メニューの［ホスト側に貼り付け］を選択します** ［Ctrl］+［V］。

4.2 認証局からの電子証明書の取得

create key コマンドを使用して、鍵を作成します。create sign コマンドを使用して、署名要求（CSR）を作成します。作成した署名要求は、認証を受け署名をしてもらうために認証局（VeriSign 社など）に送ります。すると、1 ～ 5 日間程度で署名済みの電子証明書が返送されてきます。この電子証明書を SSLAccelerator にインポートするには、import cert コマンドを使用します。

署名要求を作成するとき、各フィールドに入力した情報のことを総称的に「DN（Distinguished Name ／識別名）」と呼びます。追加のセキュリティ機能を実現するために、DN が一意な値になるように、フィールドに入力した値の一部に変更が必要となる場合があります。

鍵を作成するには、次のようにします。

1 プロンプトに create key コマンドを入力します。

```
# create key
Key strength (512/1024) [512]: <Enter>
New keyID [001]: 001
Keypair was created for keyID: 001.
```

⚠注意

鍵を作成した場合は、必ず設定を保存してください。設定の保存には、config save コマンドを使用します。
また export key コマンドでバックアップを作ることを推奨します。鍵が保存されていないと、取得した電子証明書が使えません。
セキュリティ上、鍵の保管には十分注意してください。

2 署名要求を作成します。

```
# create sign 001
You are about to be asked to enter information
that will be incorporated into your certificate request.
The "common name" must be unique.
For other fields, you could use default values.
```

以下の説明に従って、要求される項目に入力していきます。

各認証局が持つ固有のガイドラインに従って、SSLAccelerator からの問い合わせに回答することが必要です。こうしたガイドラインは認証局によって異なっているため、CSR（Certificate Signing Request ／署名要求）の送付先として選択した認証局のガイドラインを参照する必要があります。署名要求（CSR）に組み込む情報を入力するときは、次のことに注意してください。

- Country Name：国名を表す 2 文字の略語。ISO 形式（日本の場合は JP）となります。
- State or Province Name：電子証明書を必要とする組織の本社がある州。州名を省略しないで入力してください（日本の場合は都道府県名）。

- Locality Name：組織の本社がある市。
- Organization name：ドメイン名を所有している組織名（企業名、大学名、政府機関名など）です。行政区画（国、州、市など）レベルで登録されている正式な名前を使用してください。組織名の省略や、次の特殊文字の使用は不可です。
：< > ~ ! @ # $ % ^ * / \ ( ) ?
- Organization Unit Name：電子証明書を使用する部門またはグループの名前です。
- Common Name：サーバの DNS ルックアップ処理で使用する「完全修飾ドメイン名（FQDN）」であり、URL とも呼ばれます（www.mycompany.xyz など）。ブラウザは、この情報を使って Web サイトを確認します。ブラウザによっては、サーバ名と電子証明書に組み込まれている Common Name が一致しないとき、安全な接続の確立を拒否するものもあります。Common Name には、プロトコル指定子「http://」やポート番号、パス名などを含めないでください。また、「*」、「?」などのワイルドカードや IP アドレスの使用は不可です。
- Email Address：電子証明書を管理する担当者の電子メールアドレス。

3 CSR をエクスポートします。

ここでは、Console ポートに接続されているパソコン に、Xmodem プロトコルを使用して CSR を送る例を示します。

```
# export sign 001
Export protocol: (xmodem, ascii) [ascii]: xmodem
Press Ctrl-X multiple times to kill transmission
Beginning export...
Export successful!
```

CSR を認証局に送る場合は、認証局が用意しているオンラインのフォームに、この結果表示される内容をコピーして貼り付けます。このときに、「-----BEGIN CERTIFICATE REQUEST -----」という行と「----- END CERTIFICATE REQUEST -----」という行も含めて貼り付けるようにしてください。CSR の一般的な例は以下のようになります。

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBnDCCAQUACQAwXjELMAkGA1UEBhMCQ0ExEDOABgNVBAgT
B09udGFayW8xEDAOBgNVBAcTB01vbnRyYWwxDDAKBgNVBAoT
A0tGQzEdMBsGA1UEAxMUd3d3Lmlsb3ZlY2hpY2tlbi5jb20w
gZ0wDQYJKoZIhvcNAQEBBQADgYsAMIGHAoGBALmJA2FLSGJ9
iCF8uwfPW2AKkyyKoe9aHnnwLLw8WWjhl[ww9pLietwX3bp6
Do87mwV3jrgQ1OIwarj9iKMLT6cSdeZ0OTNn7vvJaNv1iCBW
GNypQv3kVMMzzjEtOl2uGl8VOyeE7jImYj4HlMa+R168AmXT
82ubDR2ivqQwl7AgEDoAAwDQYJKoZIhvcNAQEEBQADgYEAn8
BTcPg4OwohGIMU2m39FVvh0M86ZBkANQCEHxMzzrnydXnvRM
KPSE208x3Bgh5cGBC47YghGZzdvxYJAT1vbkfCSBVR9GBxef
6ytkuJ9YnK84Q8x+pS2bEBDnw0D2MwdOSF1sBb1bcFfkmbpj
N2N+hqrrvA0mcNpAgk8nU=
-----END CERTIFICATE REQUEST-----
```

4 認証局から返送されてきた署名済みの電子証明書を SSLAccelerator にインポートします。

import cert コマンドに KeyID を指定して実行し、export コマンドと同様に鍵のインポートに使用するプロトコルを選択します。ここでは、デフォルトの［paste］を選択します。ペースト後、改行しピリオドを 3 つ入力して、コマンドラインに戻ります。

```
# import cert 001
import protocol (paste, xmodem) [paste]: <Enter>
Type or paste in data, end with ... alone on a line.
-----BEGIN CERTIFICATE-----
MIIDKDCCAtKgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBnDEL
MAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMQ4wDAYDVQQHEwVQ
b3dheTEaMBgGA1UEChMRQ29tbWVyY2Ug
.
.
.
-----END CERTIFICATE----- <Enter>
... <Enter>
Import successful!
```

5 サーバのマッピングを作成します。

create map コマンドを使用して、サーバの IP アドレス、ポート、KeyID を指定してください。

```
# create map
Server IP [0.0.0.0]: 10.1.1.30
SSL (network) port [443]: <Enter>
Cleartext (server) port [80]: <Enter>
KeyID to use for mapping: 001
```

6 マッピングの作成後、設定を保存します。

```
# config save
Saving configuration to flash...
Configuration saved to flash
```

4.3 既存の鍵／電子証明書の使用

■ 鍵／電子証明書を Web サーバからエクスポート

ここからは、既存の鍵と電子証明書を使用する方法について説明します。
鍵と電子証明書を Web サーバからエクスポートする方法の詳細については、サーバソフトウェアのマニュアルを参照してください。エクスポートが完了したら、import key コマンドと import cert コマンドを使用して、鍵と電子証明書を SSLAccelerator にインポートします。
次に、Apache Web Server 製品を使用する場合の一般的な処理方法を示します。
以下に示す手順は、システム構成の違い等によって、異なる場合があります。特に環境変数（$APACHEROOT）が設定されていないことがあり、その際は各システムの Apache ソフトウェアや SSL ソフトウェアのインストール情報から同等の情報を判別する必要があります。

⚠注意 **現時点では、Microsoft IIS または Netscape サーバから秘密鍵を抽出する方法は公表されていません。**

■ OpenSSL を用いた Apache（mod_ssl）の場合

鍵：

1. $APACHEROOT/conf/httpd.conf **ファイルを参照して、***.key **ファイル（鍵ファイル）の場所を調べます。**
2. **鍵データをコピー** & **ペーストします。**

電子証明書：

1. $APACHEROOT/conf/httpd.conf **ファイルを参照して、***.crt **ファイル（電子証明書ファイル）の場所を調べます。**
2. **電子証明書ファイルをコピー** & **ペーストします。**

■ Apache SSL の場合

鍵：

1. $APACHESSLROOT/conf/httpd.conf **ファイルを参照して、***.key **ファイル（鍵ファイル）の場所を調べます。**
2. **鍵データをコピー** & **ペーストします。**

電子証明書：

1. $APACHESSLROOT/conf/httpd.conf **ファイルを参照して、***.cert **ファイル（電子証明書ファイル）の場所を調べます。**
2. **電子証明書ファイルをコピー** & **ペーストします。**

■ stronghold の場合

鍵：

1 $STRONGHOLDROOT/conf/httpd.conf ファイルを参照して、*.key ファイル（鍵ファイル）の場所を調べます。

2 鍵データをコピー & ペーストします。

電子証明書：

1 $STRONGHOLDROOT/conf/httpd.conf ファイルを参照して、*.cert ファイル（電子証明書ファイル）の場所を調べます。

2 電子証明書ファイルをコピー & ペーストします。

4.4 SSLAccelerator へのインポート

1 import key コマンドに KeyID を指定して実行し、インポートに使用するプロトコルを選択します。

ここでは、デフォルトの［paste］を選択します。
秘密鍵を貼り付けたあと、改行しピリオドを 3 つ入力して、コマンドラインに戻ります。

```
# import key 001
import protocol (paste, xmodem) [paste]: <Enter>
Type or paste in data, end with ... alone on a line.
-----BEGIN RSA PRIVATE KEY-----
MIIBOgIBAAJBALGOlBH14vIdtfuA+UnyRIoKya13ey8mj3GD
QakdwoDJALu+jtcC
.
.
.
S9dPdwp6zctsZeztn/ewPeNamz3q8QoEhY8CawEA
-----END RSA PRIVATE KEY-----<Enter>
... <Enter>
The key is encrypted.
Enter a pass phrase to decrypt the key []: sesame
Import successful!
```

2 import cert コマンドに KeyID を指定して実行し、インポートに使用するプロトコルを選択します。

ここでは、デフォルトの［paste］を選択します。
証明書を貼り付けたあと、改行しピリオドを 3 つ入力して、コマンドラインに戻ります。

```
# import cert 001
import protocol (paste, xmodem) [paste]: <Enter>
Type or paste in data, end with ... alone on a line.
-----BEGIN CERTIFICATE-----
MIIDKDCCAtKgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBnDEL
MAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMQ4wDAYDVQQHEwVQ
b3dheTEaMBgGA1UEChMRQ29tbWVyY2Ug
.
.
.
-----END CERTIFICATE----- <Enter>
... <Enter>
Import successful!
```

3 サーバのマッピングを作成します。

create map コマンドを使用して、サーバの IP アドレス、ポート、KeyID を指定してください。

```
# create map
Server IP [0.0.0.0]: 10.1.1.30
SSL (network) port [443]: <Enter>
Cleartext (server) port [80]: <Enter>
KeyID to use for mapping: 001
```

4 マッピングの作成後、設定を保存します。

```
# config save
Saving configuration to flash...
Configuration saved to flash
```

4.5 SSLAccelerator での新しい鍵／電子証明書の作成

create key コマンドと create cert コマンドを使用して、SSLAccelerator での処理に使用する新しい鍵と電子証明書を作成します。この方法は、サーバ上に鍵や電子証明書がない場合に使用できます。この方法には、鍵と電子証明書をすぐに取得できるという利点がありますが、認証局による署名はありません。
電子証明書を作成するとき、各フィールドに入力した情報のことを総称的に「DN（Distinguished Name ／識別名）」と呼びます。

SSLAccelerator ではテスト用に電子証明書を作成することができますが、実際に使用する電子証明書は、認知されている認証局から取得する必要があります。

1 次のようにして鍵を作成します。

```
# create key
Key strength (512/1024) [512]: <Enter>
New keyID [001]: 001
Keypair was created for keyID: 001.
```

2 create cert コマンドに KeyID を指定して実行します。

```
# create cert 001
You are about to be asked to enter information…
```

電子証明書情報の入力を求めるプロンプトが表示されます。次の各情報を入力してください。

- Country Code（国コード）
- State or Province（都道府県）
- Locality（市町村名）
- Organization（ドメイン名を所有している組織名）
- Organization Unit（部署名等）
- Common name（例：www.mycompany.xyz）
- Email address（電子メールアドレス）

3 サーバのマッピングを作成します。

create map コマンドを使用して、サーバの IP アドレス、ポート、KeyID を指定してください。

```
# create map
Server IP [0.0.0.0]: 10.1.1.30
SSL (network) port [443]: <Enter>
Cleartext (server) port [80]: <Enter>
KeyID to use for mapping: 001
```

4　**マッピングの作成後、設定を保存します。**

config save
Saving configuration to flash...
Configuration saved to flash

4.6 グローバルサイト電子証明書

ここでは、以下の 4 種類の電子証明書について説明します。

- ルート CA 電子証明書
  VeriSign などの信頼できる認証局（CA）の電子証明書。
- サーバ電子証明書
  サーバ上にロードされる、自己生成された電子証明書または VeriSign などの認証局から受け取った電子証明書。要求の発信元のブラウザが持つルート CA 電子証明書との相互作用によって、暗号化通信のための認証が行われます。
- グローバルサイト電子証明書
  拡張されたサーバ電子証明書。米国国外への輸出向けに機能が制限されたブラウザでも 128 ビット暗号化を使用できるようにします。
- 中間認証局（中間 CA）電子証明書
  「他の CA によって署名された CA」の電子証明書。VeriSign などの公認の認証局によって認証され、グローバルサイト電子証明書の有効性の確認に使用されます。以下の説明では、「中間 CA 電子証明書」と呼びます。

⚠注意 **SSLAccelerator は、1 つのマッピングにつき 1 つのルート CA 電子証明書と、1 つのマッピングにつき複数の中間 CA 電子証明書をサポートします。**

Internet Explorer および Netscape Communicator の輸出向け版は、40 ビット暗号化を使用して SSL サーバに接続します。SSL サーバは、クライアントからの要求を受信すると、電子証明書を返信します。この電子証明書が従来のサーバ電子証明書である（つまり、グローバルサイト電子証明書ではない）場合は、ブラウザとサーバは、SSL ハンドシェークを完了し、40 ビット鍵を使用してアプリケーションデータを暗号化します。しかし、SSL サーバが要求の発信元のブラウザにグローバルサイト電子証明書を返信した場合は、クライアントは、自動的に再接続して 128 ビット暗号化を使用します。

グローバルサイト電子証明書は、それに対応する中間 CA 電子証明書とその中間 CA 電子証明書に署名をした CA のルート電子証明書よって有効性が確認されます（電子証明書の連鎖と呼びます）。中間 CA 電子証明書には、Microsoft SGC Root や VeriSign Class 3 CA などがあります。ブラウザは、サーバに対して証明書を要求します。サーバは、その要求に対してグローバルサイト電子証明書と対応する中間 CA 電子証明書を送ります。ブラウザは、受け取った中間 CA 電子証明書に署名しているルート CA の電子証明書をブラウザ内にあらかじめ登録されている電子証明書の中から探し、有効性を確認します。この結果、この中間 CA 証明書の有効性が確認され、そしてグローバルサイト電子証明書の有効性が確認されます。有効性が確認されると、128 ビット暗号化通信が使用可能になります。

■ グローバルサイト電子証明書の貼り付け手順

グローバルサイト電子証明書を使用する場合は、グローバルサイト電子証明書とそれに対応する中間 CA 電子証明書をインポートする必要があります。2 つの電子証明書は、1 つのファイルに結合されている必要があります。

⚠注意 SSLAccelerator **は、1 つのマッピングにつき 1 つのルート** CA **電子証明書と、1 つのマッピングにつき複数の中間** CA **電子証明書をサポートします。**

import cert コマンドを使用して、単一の電子証明書や連鎖した複数の電子証明書をインポートできます。2 つの連鎖した電子証明書を使用する場合は、最初にサーバのグローバルサイト電子証明書を貼り付け、次に中間 CA 電子証明書を貼り付けます。中間 CA 電子証明書の後に改行してピリオドを 3 つ入力します。

⚠注意 **電子証明書の前後や 2 つの電子証明書の間にスペース文字があってはいけません。**
また、"Begin..." **と** "End..." **を含む行は、すべてそのまま残しておかなければなりません。**

例：

```
# import cert 001
import protocol (paste, xmodem) [paste]: <Enter>
Type or paste in data, end with ... alone on a line.
-----BEGIN CERTIFICATE-----
MIIFZTCCBM6gAwIBAgIQCTN2wvQH2CK+rgZKcTrNBzANBgkq
hkiG9w0BAQQFADCBujEfMB0GA1UEChMWVmVyaVNpZ24gVHJ1
.
.
.
OTExMTEwMDAwMDBaFw0wMDExMTAyMzU5NTlaMIHHMQswCQYD
VQQGEwJVUzETMBEG
-----END CERTIFICATE-----<Enter>
-----BEGIN CERTIFICATE-----
MIIEMTCCA5qgAwIBAgIQI2yXHivGDQv5dGDe8QjDwzANBgkq
hkiG9w0BAQIFADBfMQswCQYDVQQGEwJVUzEXMBUGA1UEChMO
.
.
.
NlVBp4xZkZ9G3hg9FXUbFXIaWJwfE22iQYFm8hDjswMKNXRj
M1GUOMxImaSESQeSltLZI5lVR5fN5qu
-----END CERTIFICATE-----<Enter>
...<Enter>
Import successful!
```

4.7 クライアント認証

デフォルトでは、SSLAccelerator はクライアントの ID を認証しません。ただし、ID の確認のためにクライアント電子証明書を要求するように、特定の MapID を設定しておくことができます。この機能が有効になっている場合、SSLAccelerator は、確認済みの CA がクライアント電子証明書に署名しているかどうかを確認します。この機能は、import client_ca コマンドによって制御されます。

例：

最初に、list map コマンドを使用して、現在の MapID とそれらの設定を表示します。最後の項目は、クライアント認証機能が有効（y）になっているか無効（n）になっているかを示します。

```
# list map
Map                                  Net   Ser   Cipher        Re-     Client
ID  KeyID     Server IP              Port  Port  Suites        direct  Auth
== ======= ========== ==== ==== ========== ===== ====
1   default    Any          443  80    all(v2+v3)    n         n
2   sample   10.1.2.57      443  80    med(v2+v3)    n         n
```

次に、MapID 2 にクライアント認証用 CA の電子証明書をインポートします。

```
# import client_ca 2
import protocol (paste, xmodem) [paste]: <Enter>
Type or paste in data, end with ... alone on a line.
-----BEGIN CERTIFICATE-----
MIIDxzCCAzCgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBpDEL
MAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWExEjAQ
BgNVBAcTCVNhbiBEaWVnbzEUMBIGA1UE
.
.
.
XcCabZcfBRuYcZeUoNrGUl8tD80jp2YNG1vidgLEaD1YCli5
I9/mNrcB25mSfdAR/08ROTMxm4VKOSA=
-----END CERTIFICATE-----<Enter>
...<Enter>
Import successful!
```

list map コマンドをもう一度使用して、インポートの結果を確認します。ClientAuth の項目で、MapID 2 のクライアント認証機能が有効になっていることに注意してください。

```
# list map
Map                                  Net   Ser   Cipher          Re-      Client
ID   KeyID      Server IP            Port  Port  Suites          direct   Auth
==   ========   =========  ====  ====  ============  ======  ======
1    default    Any          443   80    all(v2+v3)      n        n
2    sample     10.1.2.57    443   80    med(v2+v3)      n        y
```

MapID 2 で指定されたサーバに接続するクライアントは、上記の手順でインポートされたクライアント認証用 CA の電子証明書の発行元の CA が署名したクライアント電子証明書を提示するように要求されます。正しい署名を持つクライアント電子証明書を提示しない場合は、接続は拒否されます。

■ OpenSSL を使用したクライアント電子証明書の作成

クライアント電子証明書を生成する際は、市販のソフトウェアパッケージを使用できます。以下の例は、OpenSSL を使用した手順を示しています。

ポイント **ユーザの環境に** OpenSSL **のコピーを取得するには、**OpenSSL **の** Web **サイト** (www.openssl.org) **にアクセスします。**

1 **クライアント認証用** CA **用の秘密鍵（**ca_key.pem**）を作成します。**

```
openssl genrsa -out ca_key.pem 1024
```

2 **クライアント認証用** CA **の電子証明書（**ca_cert.pem**）を作成します。**

```
openssl req -new -x509 -key ca_key.pem -days 365 -out ca_cert.pem
```

3 import client_ca **コマンドを使用して、クライアント認証用** CA **の電子証明書をインポートします。**

各クライアントについて、以下の手順を実行します。

1 **秘密鍵（**cl1key.pem**）を作成します。**

```
openssl genrsa -out key.pem 1024
```

2 **署名要求を作成します。**

```
openssl req -new -days 365 -key key.pem -out csr.pem
```

3 **クライアント認証用** CA **の電子証明書を使用して、署名要求に署名します。**

```
openssl x509 -req -CAcreateserial -CAkey ca_key.pem -CA
ca_cert.pem -days 365 -in csr.pem -out cert.pem
```

4 **署名済みのクライアント電子証明書の形式を** PEM **形式から** PKCS12 **形式に変換します。**

```
openssl pkcs12 -export -in cert.pem -inkey key.pem -name
"<Client ID>" -out cert.p12
```

5 **手順** 4 **で得られたクライアント電子証明書（**cert.p12**）をクライアントブラウザにインポートします。**

4.8 リダイレクション

■ サポートされない暗号方式に対するリダイレクト

選択された暗号方式をサポートしないクライアントが SSLAccelerator に接続しようとした場合、デフォルトの動作では、その接続が拒否されます。この場合、クライアントシステムは致命的エラーを報告します。しかし、SSLAccelerator では、管理者が「リダイレクトアドレス」を指定し、そのアドレスでクライアントに追加情報を提供することができます。set cipher_redir コマンドを使用して、任意の MapID に対してリダイレクト Web アドレスを指定できます。show cipher_redir コマンドは、現在設定されているリダイレクトアドレスをすべて表示します。

⚠注意

管理者は、リダイレクト URL を指定し、その URL が使用可能であることを確認してください。
また、リダイレクトページの内容を定義しておく必要があります。

⚠警告

クライアントが、リダイレクト URL に従って、リダイレクションを発生させた SSLAccelerator のマッピングと同じマッピングにアクセスした場合は、無限ループ状態が発生します。リダイレクト URL に HTTP プロトコルを指定することをお勧めします。

```
# list map
Map                                  Net   Ser   Cipher       Re-      Client
ID  KeyID    Server IP               Port  Port  Suites       direct   Auth
== ======= ========== ==== ==== ========== ====== ====
1   default   Any          443   80    all(v2+v3)    n        n
2   sample    10.1.2.5     443   80    med(v2+v3)    n        n
# set cipher_redir 2
Enter a weak cipher redirect URL at the following prompt
e.g. http://www.mycompany.xyz/weakbrowser.html

Enter a weak cipher redirect URL []: http://www.myco.xyz/cipher_info.html
# list map
Map                                  Net   Ser   Cipher       Re-      Client
ID  KeyID    Server IP               Port  Port  Suites       direct   Auth
== ======= ========== ==== ==== ========== ====== ====
1   default   Any          443   80    all(v2+v3)    n        n
2   sample    10.1.2.5     443   80    med(v2+v3)    ci       n
# show cipher_redir 2
cipher_redir for mapping 2 is set: http://www.myco.xyz/cipher_info.html
```

特定のマッピングのリダイレクト URL を無効にするには、次のようなコマンドを使用します。

```
# set cipher_redir 2 none
# show cipher_redir 2
cipher_redir for mapping 2 is not set
```

■ クライアント電子証明書が存在しない場合、または無効な場合のリダイレクト

この機能を使うことによって、クライアントにクライアント電子証明書がない場合、またはクライアントが無効な電子証明書を提示した場合は、SSLAccelerator はリダイレクションを行います。この機能を管理するコマンドは、set cert_redir コマンドと show cert_redir コマンド です。暗号リダイレクション機能の場合と同様に、クライアント電子証明書のリダイレクションの状態は、list map コマンドの出力データに反映されます。

```
# list map
Map                              Net   Ser   Cipher        Re-      Client
ID   KeyID     Server   IP       Port  Port  Suites        direct   Auth
==== ======== ========== ====== ===== ===== ========== ======= ====
1    default    Any              443   80    all(v2+v3)     n        n
2    sample   10.1.2.5           443   80    med(v2+v3)   n        v
# set cert_redir 2
Enter a none/bad client cert redirect URL at the following prompt
e.g. http://www.mycompany.xyz/clientcert.html

Enter a none/bad client cert redirect URL []: http://www.myco.xyz/
cert_info.html
# list map
Map                              Net   Ser   Cipher        Re-      Client
ID   KeyID     Server IP        Port  Port  Suites        direct   Auth
==== ======== ========== ====== ===== ===== ========== ======= ====
1    default    Any              443   80    all(v2+v3)     n        n
2    sample   10.1.2.5           443   80    med(v2+v3)   ce       y
# show cert_redir 2
cert_redir for mapping 2 is set: http://www.myco.xyz/cert_info.html
```

特定マッピングに対するクライアント電子証明書のリダイレクト URL を無効にするには、次のコマンドを使用します。

```
# set cert_redir 2 none
# show cert_redir 2
cert_redir for mapping 2 is not set
```

4.9 証明書失効リスト

通常、電子証明書はその有効期間を通して使用されます。ただし、名前の変更やサブジェクトと CA の関係が変わった場合などのように、有効期間の失効日より前に電子証明書が無効になる場合があります。SSLAccelerator は、証明書失効リスト（CRL）によってこれをサポートします。

CRL は認証局から取得できます。この CRL を使用して、無効とみなされる電子証明書を提示するクライアントからの要求をブロックするように SSLAccelerator を設定できます。CRL は、シリアル番号と発行者に基づいて無効な電子証明書を識別します。電子証明書を取り消さなければならない状況としては、間違って電子証明書を発行した場合や、不注意で非公開鍵を公開してしまった場合などがあります。SSLAccelerator では、以下の方法のいずれか使用して、CRL を取得することができます。

- FTP
- HTTP
- LDAP
- PEM 方式で符号化した ASCII を管理コンソールでペーストする方法
- Xmodem

CRL 処理を有効にしており、かつ SSLAccelerator が有効な CRL を取得している場合には、新しい SSL 接続ごとに提示される電子証明書は CRL と照合されます。CRL で証明書が検出されると、その接続は閉じられて、電子証明書が無効になっていることを知らせるメッセージが要求元に表示されます。このメッセージは、使用しているブラウザによって異なります。CRL を定期的に更新するように SSLAccelerator を設定することができます。

CRL を取得している間にエラーが発生するか、または CRL が 100 KB を超える場合には、CRL の取得は拒否されて、警告メッセージがログに記録されるか、または画面に表示されます。CRL を正常に受信するまで、指定の CRL 検索間隔で CRL の取得を再試行します。

CRL の管理には、次の各 CLI コマンドを使用します。

- show crl <mapID>
  指定した mapID について、現在の失効 URL ソース、および CRL を表示します。mapID を指定しない場合は、すべての CRL が表示されます。
- set crl_mode <mapID>
  指定した mapID の CRL のサーバタイプ、ファイル名、およびファイル位置を設定します（このコマンドは、クライアント電子証明書がインストールされて、IP が設定されている場合にのみ有効です）。
- set crl_refresh [now] | <0-1440 >
  CRL リフレッシュ間隔を分単位で設定するか、またはオプションで、現在指定されているリフレッシュ間隔に影響を与えずに新しい CRL をただちに要求します。

- import crl <mapID>
  指定したマッピングの CRL をコンソールに貼り付けたり、Xmodem によって送信することができます。このコマンドは、定期的な CRL 検索間隔に影響しません。定期的な更新が設定されている場合、インポートされた CRL は、一定の検索間隔で上書きされます。
- export crl <mapID>
  ASCII または Xmodem を使用して、指定したマッピングの有効な CRL を SSLAccelerator からコンソールへ転送できます。
- delete crl <mapID>
  指定したマッピングについて、現在の CRL を削除します。
- delete crl_mode <mapID>
  指定した mapID について、現在指定されているアップロードモードを無効にします。
- status crl [all | last]
  CRL のダウンロード状態を表示します。最終ダウンロード状態または現在のすべてのダウンロード状態のどちらかを指定できます。
- delete crl_status
  以前の CRL のダウンロード状態をすべて削除します。

⚠注意

大きな CRL ファイルをハイパーターミナルで貼り付けると、処理速度が低下して、CRL を取得できない場合があります。ハイパーターミナルの Xmodem を使用して CRL をインポートするか、または別のターミナルエミュレータを使用して貼り付けや Xmodem 操作を行うことをお勧めします。

■ OpenSSL による CRL の生成

以下の例は、OpenSSL を使用して証明書失効リスト（CRL）を生成する手順を示しています。
まず、クライアント認証用 CA の電子証明書を作成します。

1 **クライアント認証用 CA の秘密鍵（ca_key.pem）を作成します。**

```
openssl genrsa -out ca_key.pem 1024
```

2 **クライアント認証用 CA の電子証明書（ca_cert.pem）を作成します。**

```
openssl req -new -x509 -key ca_key.pem -out ca_cert.pem
```

3 import client_ca **コマンドを使用して、クライアント認証用 CA の電子証明書を SSLAccelerator にインポートします。**

次にクライアント電子証明書を作成します。

1 **秘密鍵（**cl1key.pem**）を作成します。**

```
openssl genrsa -out cl1key.pem 1024
```

2 **署名要求（**cl1csr.pem**）を作成します。**

```
openssl req -new -key cl1key.pem -out cl1csr.pem
```

3 **クライアント認証用** CA **の電子証明書を使用して、署名要求に署名します。**

```
openssl ca -keyfile ca_key.pem -cert ca_cert.pem -in cl1csr.pem -out
cl1cert.pem
```

4 cl1key.pem **と** cl1cert.pem **を結合して** 1 **つのファイルにします。**

```
cat cl1key.pem cl1cert.pem > cl1all.pem
```

5 **クライアント電子証明書の形式を** PEM **形式から** PKCS12 **形式へ変換します。**

```
openssl pkcs12 -export -in cl1all.pem  -out cl1cert.p12 -name "cl1"
```

6 **手順** 5 **で得られたクライアント電子証明書（**cl1cert.p12**）をクライアントブラウザにインポートします。**

⚠注意

クライアント電子証明書を作成する前に必ず openssl.cnf **ファイルを設定してください。**
このファイルで定義されたディレクトリ構造やデータベースファイル等が正しく設定されていない場合、クライアント電子証明書や CRL **が正しく作成できない場合があります。**

ポイント

OpenSSL **の取得方法と使用方法の詳細は** OpenSSL **の** Web **サイト（**www.openssl.org**）を参照してください。**

クライアント電子証明書の取り消しは以下の手順で行います。

1 **クライアント電子証明書（**cl1cert.pem**）を取り消します。**

```
openssl ca -revoke cl1cert.pem
```

2 **取り消されたクライアント電子証明書の情報を取り込み、新しい** CRL **（**crl.pem**）を作成します。**

```
openssl ca -gencrl -out crl.pem
```

3 import crl **コマンドを使用して** CRL **を** SSLAccelerator **にインポートします。**

4.10 SSL の処理

■ サーバの割り当て（マッピング）

鍵の組み合わせ（キーペア）と対応する電子証明書の識別には KeyID、サーバの識別にはサーバの IP アドレスと Network 側ポート番号の組み合わせを使用します。マッピングとは、この KeyID とサーバ（サーバの IP アドレス、ネットワーク側ポート番号、サーバ側ポート番号を使用）を対応付ける処理のことです。
SSLAccelerator では、次の 2 種類のマッピングを行うことができます。

- 自動マッピング
- 手動マッピング

ポイント　SSLAccelerator **は、最大** 1000 **までのマッピングをサポートします。**

■ 自動マッピング

自動マッピングを行う場合は、サーバの IP アドレスとして（0.0.0.0）を指定します。
このように指定すると、SSLAccelerator は全てのサーバに対する特定のポート番号（後述のデフォルト）へのパケットに割り込むようになります。マッピングエントリを作成するときは、サーバの IP アドレスとネットワーク側ポート番号の組み合わせが他のエントリと重複しないように注意してください。

⚠注意　**マッピングを変更した場合は、必ず設定を保存してください。設定の保存には、**config save **コマンドを使用します。**

SSLAccelerator の出荷時の設定では、ネットワーク側ポート 443 とサーバ側ポート 80 の自動マッピングエントリが用意されています。この自動マッピングエントリは、内部で生成されたデフォルトのキーペアと電子証明書（KeyID は「default」）に対応しています。この設定では、トラフィックが SSLAccelerator を介して送信されるとき、ネットワーク側ポート 443 のすべてのトラフィックについて自動マッピングが行われます。

ユーザ指定の鍵と電子証明書を使用して自動マッピングする場合には、以下のことに注意してください。

- 少なくとも 1 つのマッピングがある状態で、自動マッピングを削除した場合、装置は自動マッピング（0.0.0.0/443/80）を再作成しません。
- 複数の自動マッピングを持つことはできません。
- デフォルトの自動マッピングを削除するには、少なくとも 1 つのマッピングを作成しておく必要があります。

- 自動マッピングだけしかなく、他にマッピングがない場合に、自動マッピングを変更して異なる鍵と電子証明書を使用したいときは、以下の操作を行います。

  1 **まず新しいマッピングを 1 つ作成してください。**

  2 **元の自動マッピングを削除し、新しい** KeyID **を使用して新たに自動マッピングを作成します。**

  3 **最初に生成したマッピングを削除してください（自動マッピングが最後のマッピングである場合は、それを削除できません）。**
  自動マッピングと少なくとも 1 つのマッピングがある場合は、自動マッピングを削除して新しい自動マッピングを作成することができます。

■ 複数のポートを組み合わせた自動マッピング

ネットワーク側ポート番号が一意であれば、複数の自動マッピングエントリを指定できます。たとえば、初期設定時のネットワーク側ポート 443 とサーバ側ポート 80 のほかに、ネットワーク側ポート 8010 とサーバ側ポート 80 の組み合わせを指定できます。Network 側ポート 443 と Server 側ポート 81 に自動マッピングを追加することはできません。これは、デフォルトの自動マッピングが Network 側ポート 443 をすでに使用しているためです。

■ 手動マッピング

create map コマンドを使って、サーバごとに 1 つ以上のマッピングエントリを手動で作成できます。各サーバに一意の KeyID を指定するには、この方法を利用します。通常、手動マッピングを作成した場合は、デフォルトの自動マッピングエントリを削除します。ただし、この削除は必ずしも必要ではありません。

■ 自動マッピングと手動マッピングの組み合わせ

自動マッピングと手動マッピングで作成したエントリを組み合わせて、最大 1000 のエントリまで使用できます。ただし、この場合は、サーバ IP アドレス、ネットワーク側ポートの組み合わせが一意でなければなりません。実際のマッピング手順については、「第 3 章 構成」（→ 23 ページ）を参照してください。

手動マッピングと自動マッピングの両方を使用できる場合は、SSLAccelerator **は常に手動マッピングを使用します。**

4.11　ブロック機能

SSLAccelerator を使用すると、指定した IP アドレスとポートをブロックしたり、クライアント IP アドレスを指定して特定のサーバおよびポートへのアクセスを許可することができます。ブロック（Block）と許可（permit）は、TCP および UDP の両方のトラフィックに適用されます。

⚠注意　**SSLAccelerator がワンアーム接続のときは、ブロックと許可は使用できません。**

許可はブロックよりも優先されます。たとえば、すべての IP アドレスをブロックしてから、いくつかの IP アドレスを選択して許可を作成し、全体的なブロックを上書きすることができます。IP アドレスとポートの組み合わせは、次の情報に基づいてアクセスをブロックまたは許可することができます。

- 指定の IP アドレスの指定のポート
- サブネットの IP アドレス、指定のポート
- すべての IP アドレス、指定のポート

■ サーバポートマスク

サーバマスク（2 進法表記で表現）は、Server 側ポートに適用すると、フィルタにかけるポートを指定できます。デフォルト（0xffff）の場合には、サーバマスクのビット列は Server 側ポートのビット列に一致するので、フィルタにかけられるポートは 1 つだけです。

⚠注意　**マスクおよび 2 進数表現を完全に理解していない場合は、デフォルトのビットマスクを使用することをお勧めします。**

例 :

Server **側ポート** :1023 (0x03ff)
Server **側ポートマスク** :0xfc00
結果 :1024 **未満のポートをすべてブロックします。**

例 :

Server **側ポート** :127 (0x007f)
Server **側ポートマスク** :0xff80
結果 :128 **未満のポートをすべてブロックします。**

Server 側ポートと Server 側ポートマスクの設定値はともに、一連のビット列であり、かつポートのブロック範囲を補足するものでなければなりません。

■ 指定の IP アドレスの指定のポートに対するブロック

特定のサーバの IP アドレスとポートの組み合わせをブロックするには、次のようにします。

例：

```
# create block
Client IP to block [0.0.0.0]: 10.1.2.1
Client IP mask [255.255.255.255]: 255.255.255.255
Server IP to block [0.0.0.0]: 20.1.2.1
Server IP mask [255.255.255.255]: 255.255.255.255
Server Port to block (0-65535): 80
Server Port mask [0xffff]: <Enter>
```

確認には、show block コマンドを使用します。

```
# show block
--------
blocks :
---------
(1) block 10.1.2.1 255.255.255.255 20.1.2.1 255.255.255.255 80 0xffff
```

■ 指定のサブネットの指定のポートに対するブロック

特定のサブネットの IP アドレス、特定のポートの組み合わせをブロックするには、次のようにします（この設定では、特定のサブネット上のすべてのホストの特定のポートへのトラフィックをブロックします）。

例：

```
# create block
Client IP to block [0.0.0.0]: 10.1.2.0
Client IP mask [255.255.255.0]: 255.255.255.0
Server IP to block [0.0.0.0]: 20.1.2.0
Server IP mask [255.255.255.255]: 255.255.255.0
Server Port to block (0-65535): 80
Server Port mask [0xffff]: <Enter>
```

確認には、show block コマンドを使用します。

```
# show block
-----------
blocks :
-----------
(1) block 10.1.2.0 255.255.255.0 20.1.2.0 255.255.255.0 80 0xffff
-----------
```

■ IP アドレスの変更の指定のポートに対するブロック

すべての IP アドレスの指定のポートに対してブロックするには、次のようにします。

例：

```
# create block
Client IP to block [0.0.0.0]: <Enter>
Client IP mask [0.0.0.0]: <Enter>
Server IP to block [0.0.0.0]: <Enter>
Server IP mask [0.0.0.0]: <Enter>
Server Port to block (0-65535): 80
Server Port mask [0xffff]: <Enter>
```

確認には、show block コマンドを使用します。

```
# show block
-----------
blocks :
-----------
(1) block 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 80 0xffff
-----------
```

■ ブロックの削除

以下に、ブロックを削除する方法を示します。ブロックを削除するには、delete block コマンドにブロック ID を指定して実行します。この例の場合、ブロック ID は 1 です。

1 show block **コマンドを実行し、削除するブロックを特定します。**

```
# show block
-----------
blocks :
-----------
(1) block 10.1.2.1 255.255.255.255 20.1.2.1 255.255.255.255 80 0xffff
-----------
```

2 delete block **コマンドに、削除するブロック** ID **を指定して実行します。**

```
# delete block 1
```

■ 許可の作成

特定の IP アドレスからの SSLAccelerator の管理インターフェースへのアクセスを許可するには、次のようにします。先にブロックが指定されていても、許可のほうが優先されます。

```
# create permit
Client IP to permit [0.0.0.0]: 10.1.2.1
Client IP mask [0.0.0.0]: 255.255.255.255
Server IP to permit [0.0.0.0]: 20.1.2.2
Server IP mask [0.0.0.0]: 255.255.255.255
Server Port to permit (0-65535): 80
Server Port mask [0xffff]: <Enter>
```

確認には、show permit コマンドを使用します。

```
# show permit

--------
permits :
---------
(1) permit 10.1.2.1 255.255.255.255 20.2.1.22 255.255.255.255 80 0xffff
----------
```

4.12 SSL セッションのキャッシュ機能

SSLAccelerator では、セッション 機能を確立するたびにハンドシェーク処理を実行しなくても済むように、SSL セッション ID を保持するためのキャッシュ ID が用意されています。キャッシュの動作については次の 2 つの値で調整します。

⚠注意 **キャッシュサイズパラメタを 0 に設定して、キャッシュを無効にすることができます。**

値	説明
キャッシュサイズ	キャッシュに格納する SSL セッション ID の最大個数を指定します。0 ～ 20,000 個のセッション ID を指定できます。デフォルトは 18,000 個です。0 を指定した場合、キャッシュ機能は無効になります。
タイムアウト	何秒間隔でキャッシュを空にするかを指定します。指定できる値の範囲は 30 ～ 864,000 秒です。デフォルトは 180 秒です。

ほとんどの場合は、デフォルト値のままで問題ありません。マッピングの数が少ない場合（100 個未満の場合）は、上の 2 つの値を最大値に設定してもかまいません。また、以下の場合には、キャッシュの設定値を小さく設定する必要があります。

- マッピングを 100 個より多く設定した場合
- SSLAccelerator とサーバを結ぶ経路の情報転送能力に制約がある場合

マッピングが 100 個より多いときに、キャッシュサイズ値とタイムアウト値を最大値にすると、SSLAccelerator のメモリリソースが不足する可能性があります。上記の条件のいずれかに該当する場合は、キャッシュサイズとタイムアウト値を減らすことを考慮してください。メモリエラーが発生した場合は、これらの値をすぐに減らしてください。

SSL のキャッシュに関する値を設定するには、set cache コマンドを使用します。現在の値を表示するには show cache コマンドを使用します。

4.13　サーバ位置確認機能の無効化

デフォルトでは、SSLAccelerator はサーバの位置を確認してから SSL 接続を許可します。通常、この処理は自動的に行われ、外部からは透過的ですが、SSLAccelerator の背後にあるプロキシサーバがサーバ位置確認処理を妨げ、間違った結果が出る可能性があります。この問題を解決するために、SSLAccelerator では、ser_loc_trust コマンドを使用して、サーバ位置確認機能を無効にすることができます。

```
# set ser_loc_trust enable
Server locations will not be validated before accepting connections.
```

4.14 HTTP ヘッダ挿入データ

デフォルトでは、サーバが SSLAccelerator から受信した復号済みデータは、標準的な HTTP 形式で受信します。ただし、場合によっては、通常より多くの情報をサーバに渡す必要があります。たとえば、最新のトランザクションアクティビティに関するセキュリティ監査を行うには、ソース IP アドレスをサーバに保存する必要があります。このような処理をサポートするために、SSLAccelerator は、セッション最初のパケットのヘッダに以下の項目を埋め込むための設定ができます。

- 証明書
- クライアント IP アドレス
- 暗号方式
- セッション ID

⚠注意 **同一サーバに対して複数の SSLAccelerator を構成しており、ヘッダ挿入機能を有効にしている場合は、それらの SSLAccelerator をすべて同じ設定にする必要があります。**

set hdr_fields コマンドを入力して、各 mapID の各データ項目のヘッダ挿入機能を有効または無効にします。

ヘッダ情報の処理方法は、サーバによって異なります。このため、SSLAccelerator では、挿入された項目の識別に使用するヘッダ文字列を、以下の方法で編集または削除できます。

- マップごとのヘッダ文字列
  特定のマッピングと関連付けられた証明書、暗号方式、セッション ID、クライアント IP アドレス、およびユーザ指定のヘッダ文字列を定義するために使用します。
- すべてのマッピングで有効なデフォルトヘッダ文字列
  マッピング固有のヘッダ文字列が定義されていない場合に使用します。

⚠注意 **ヘッダ挿入機能を使用する場合は、サーバの HTTP keepalive 機能を無効にする必要があります。**

4.15 VLAN サポート

インパス接続で動作中の SSLAccelerator は、VLAN をサポートするスイッチ間における VLAN（仮想 LAN）環境での動作をサポートします。SSLAccelerator による VLAN サポートには、次のものがあります。

- 802.1Q タグの自動保存
- 管理ポートから発信されたパケットの優先順位の割り当て

⚠注意 **SSLAccelerator がワンアーム接続のときは、VLAN サポートを使用できません。**

以下のような VLAN に関連した設定ができます。

- 管理ポート QoS
  この値の範囲は 0 ～ 7 で、デフォルトは 0 です。この値により、管理ポートから発信されたパケットの優先順位を決定します。
- 管理ポート VLAN ID
  この値の範囲は 1 ～ 4094 で、デフォルトは 1 です。この値により、管理 VLAN を指定します。管理 VLAN に指定したい VLAN の ID を使用してください。VLAN 作動時には、正しい VLAN ID を持つパケットだけがリモート管理に受け入れられます。

⚠注意 **set vlan コマンドは、シリアル接続されたコンソールからのみ使用できます。**

例：

```
# set vlan
Enter the management port VLAN QoS (0-7) [0]: <Enter>
Enter the management port VLAN ID (1-4094) [1]: <Enter>

# show vlan
The management port VLAN QoS is set to 0
The management port VLAN ID is set to 1
```

VLAN サポートを無効にするには、set vlan none コマンドを入力してください。パラメタ「none」は、小文字でなければなりません。

4.16 NTP（Network Time Protocol）の設定

NTP を使用すると、ネットワーク上の複数の装置の時刻を同期化することができます。このプロトコルは、マスタ／スレーブ構成で動作中のタイムサーバの分散サブネットを使用して、そのサブネット内のローカルクロックを同期化して、国内標準時間に合わせます。SSLAccelerator では、NTP を有効または無効にすることができます。また、最大で 3 台の NTP サーバを指定することができます。同期化データは、UDP を介して各装置間でやりとりされます。

⚠注意

・SSLAccelerator は NTP サーバと同期化することができますが、ネットワーク上の他の装置を SSLAccelerator に同期させることはできません。
・本装置の時刻については、手動で NTP サーバの時刻にできるだけ合わせて設定することをお勧めします。

以下に、NTP 機能の例を示します。

1 SSLAccelerator に IP を設定します。

```
# set ip
Enter IP Address (’none’ to delete) [none]: 192.168.1.105
Enter Netmask (’none’ to delete) [255.255.255.0]: <Enter>
```

2 NTP サーバを設定します。

```
# set ntp_servers
Enter IP address of NTP server (q to quit) [q]: 192.168.1.2
Enter IP address of NTP server (q to quit) [q]: 192.168.1.21
Enter IP address of NTP server (q to quit) [q]: 192.168.1.22
Only three NTP servers are allowed. Saving entered servers.
```

3 NTP サーバを確認します。

```
# show ntp_servers
NTP servers: 192.168.1.2 192.168.1.21 192.168.1.22
```

4 NTP を有効にします。

```
# set ntp enable
An optional default route may be entered before starting the NTP service.
Enter a default route (’none’ to delete) [none]: <Enter>
NTP Service started.
```

5 NTP **サーバの有効／無効を確認します。**

show ntp

NTP: enabled

6 NTP **プロセスの現在の状態を確認します。**

show ntp_status

remote	local	st	poll	reach	delay	offset	disp
=192.168.1.2	192.168.1.105	3	64	1	0.00024	-0.000416	7.93752
=192.168.1.21	192.168.1.105	3	64	1	0.00026	-0.000096	7.93750
=192.168.1.22	192.168.1.105	3	64	1	0.00031	-0.000102	7.93750

4.17　障害発生時の処理 - フェイルセーフとフェイルスルー

SSLAccelerator で障害が発生した場合に未処理のデータパケットを通過させるかどうかは、フェイルセーフモードとフェイルスルーモードのどちらを使用しているかによって決定します。フェイルスルースイッチは、デフォルトでフェイルセーフモードに設定されています。このモードでは、障害が発生している間、データパケットは SSLAccelerator を通過しません。詳細については、「A.3 障害／バイパスモード」（→ 192 ページ）を参照してください。

5 コマンドライン

SSLAccelerator の設定は、すべてコマンドラインインターフェース（CLI）から行えます。CLI にアクセスするには、Console ポートまたは Aux console ポート（RS232）を使用します。

Contents

5.1 オンラインヘルプ

SSLAccelerator のオンラインヘルプには、次のいずれかの方法でアクセスできます。

- help：コマンド一覧を表示します。
- help <command>：コマンド（<command>）の説明を表示します。このコマンドにサブコマンドがある場合は、サブコマンドのリストも表示します。
- help usage：すべてのコマンドとその使用方法を表示します。
- tty_char：編集用特例文字の一覧を表示します。

5.2 コマンドラインインターフェース

使用者が Console や Aux console ポートを使って作業を行うときは、コマンドラインインターフェース（CLI）を使用します。コマンドラインインターフェースは、2 つのシリアルポートごとにそれぞれ常に動作しています。

■ ユーザ認証

ユーザが CLI にアクセスするには、パスワードを入力する必要があります。パスワードを入力すると、バージョン情報とシリアルナンバー表示されます。

■ コマンドラインプロンプト

SSLAccelerator 7117 の標準コマンドラインプロンプトは、次のような形式になっています。

```
#
```

プロンプトを変更するには、set prompt コマンドを使用します。

必ずしもコマンド全体を入力する必要はありません。CLI コマンドには、コマンド名を識別可能な最小文字数で表した省略形を使用できます。

■ 入力文字の省略

コマンドを入力する場合、必ず完全なコマンド名を指定しなければならないわけではありません。CLI コマンドは、他のコマンドと区別できる長さまで、コマンド名を短くすることができます。たとえば、delete コマンドを実行する場合は、以下のように「del 」と入力するだけで構いません。

```
# del
Usage: delete item [arg]
        alarms                  - delete all previous alarms
        block       blockID     - delete a block filter
        cert        keyID       - delete a cert
        client_ca   mapID       - delete a client CA
        crl         mapID       - delete a CRL for a mapping
        crl_mode    mapID       - delete a CRL automatic upload
        crl_status              - delete all previous CRL upload status
        key         keyID       - delete a key
        logs        logID|all   - delete a log or all logs
        map         mapID       - delete a mapping
        patch                   - delete the installed patch
        permit      permitID    - delete a permit filter
        sign        keyID       - delete a sign request
        snmp_community          - delete a SNMP community
        trap_community          - delete a SNMP trap community
```

ただし、以下のように、「ex 」を省略コマンド名として使用することはできません。「ex 」だけでは、「export 」と「exit 」を区別できないからです。

```
# ex
```

次の例において、「ssh 」の後に続く単一文字の「e 」は、「set ssh enable 」を示します。

```
# set ssh e
SSH Service started.
```

5.3 キー操作

5.3.1 カーソルの移動

コマンド	説明
ctrl-b	1 文字戻ります。
ctrl-f	1 文字進みます。
ctrl-a	行頭に移動します。
ctrl-e	行末に移動します。
ctrl-l	現在の行を再描画します。

5.3.2 コマンドヒストリ

最近実行したコマンドは、ヒストリバッファに格納されています。これらにアクセスするには、次のコマンド群を使用します。

コマンド	説明
ctrl-p	ヒストリリストの上方に移動します。
ctrl-n	ヒストリリストの下方に移動します。
ctrl-r	（後方ヒストリ検索）現在の行から後方検索を行い、コマンドヒストリを過去方向にさかのぼります。
ctrl-s	（前方ヒストリ検索）現在の行から前方検索を行い、コマンドヒストリを新しいほうに進めます。

5.3.3 カット & ペースト

コマンド	説明
ctrl-d	カーソル位置の文字を削除します。
ctrl-k	現在のカーソル位置から行末までの文字をすべて削除します。
ctrl-u	現在のカーソル位置から行頭までの文字をすべて削除します。
ctrl-w	カーソルの左側にある語を削除します。このとき、語と語の区切りは空白文字で判断されます。
ctrl-y	上記 4 つのコマンドのいずれかを使用してカットしたテキストをペーストします。
backspace/del	カーソルの左側にある 1 文字を削除します。

5.4 コマンド一覧

この節では、SSLAccelerator のコマンド構造の一覧を示します。各コマンドの詳細は、「5.5 コマンドリファレンス」（→ 85 ページ）に記載されています。

コマンド	コマンドオプション
bypass	
config	default compare reset save
create	block cert <keyID> key <keyID> map permit sign <keyID>
delete	alarms block <blockID> cert <keyID> client_ca <mapID> crl <mapID> crl_mode <mapID> crl_status key <keyID> logs <logID >| [all] map <mapID> patch permit <permitID> sign <keyID> snmp_community trap_community
exit	
export	cert <keyID> config crl <mapID> key <keyID> log <logID> sign <keyID>
factory_default	
help	<command> usage
import	cert <keyID> client_ca <mapID> config crl <mapID> key <keyID> patch upgrade

コマンド	コマンドオプション
inline	
list	blocks filters keys logs map monitoring permits procs snmp_community system trap_community timezone[continent]
nic	
password	
ping <ip>	
quit	
reboot	
set	alarms [all | esc | nls | none | ovl | rsc | utl] cache cert_redir <mapID> [none] cipher_redir <mapID> [none] ciphers <mapID> [default] client_tmo <5-36000> crl_mode <mapID> crl_refresh [now | <0-1440>] date defcert egress_mac [<mac> | none] ether hdr_cert <mapID> [none] hdr_cert_def hdr_cip <mapID> [none] hdr_cip_def hdr_cipher <mapID> [none] hdr_cipher_def hdr_fields <mapID> hdr_sid <mapID> [none] hdr_sid_def hdr_user <mapID> [none] hwq_hiwat_spill <1-256> hwq_lowat_spill <1-256> idleto <0-525600> ip <ip> <netmask> kstrength [512 | 1024]

コマンド	コマンドオプション
set	map_visible [enable | disable] max_remote_sessions<0-5> mgmt_if [network | server] monitoring [enable | disable] monitoring_interval <5-65000> monitoring_fields [all | cps | cpu | dec | enc | failmode | link | mode | ovrld] more ntp [enable | disable] ntp_servers onearm [enable | disable] ovl_window <5-65000> prompt route <ip> redir_change <mapID> [enable | disable | all] rsc_window <5-65000> serial ser_loc_trust [enable | disable] server_tmo <5-36000> snmp [enable | disable] snmp_community snmp_info snmp_port <port> spill [enable | disable] ssh [enable | disable] ssh_port <10-65535> sys_contact <contact name> sys_location <location information> sys_name <system name> telnet [enable | disable] telnet_port <10-65535> timezone [<tz> | none] trap_authen [enable | disable] trap community trap_port <port> utl_highwater <2-100> utl_lowwater <1-99> utl_window <5-65000> vlan [none]

コマンド	コマンドオプション
show	alarms
	blocks
	cache
	cert <keyID>
	cert_redir <mapID>
	cipher_redir <mapID>
	ciphers <mapID>
	client_ca <mapID>
	client_tmo
	config
	config default
	config saved
	crl <mapID>
	crl_mode <mapID>
	crl_refresh
	date
	defcert
	egress_mac
	ether
	filters
	hdr_cert <mapID>
	hdr_cert_def
	hdr_cipher <mapID>
	hdr_cipher_def
	hdr_fields <mapID>
	hdr_cip <mapID>
	hdr_cip_def
	hdr_sid <mapID>
	hdr_sid_def
	hdr_user <mapID>
	idleto
	info
	ip
	hwq_hiwat_spill
	hwq_lowat_spill
	key <keyID>
	kstrength
	logs
	map
	map_visible
	max_remote_sessions
	mgmt_if
	monitoring
	monitoring_interval
	monitoring_fields
	more
	ntp
	ntp_servers
	ntp_status
	redir_change <mapID>
	onearm
	ovl_window
	patch
	permits
	rsc_window
	route

コマンド	コマンドオプション
show	serial ser_loc_trust server_tmo snmp snmp_community snmp_info snmp_port ssh ssh_port sign <keyID> spill status <arg> sys_contact sys_location sys_name telnet telnet_port timezone trap_authen trap_community trap_port utl_highwater utl_lowwater utl_window vlan
status	alarms crl [all | last] line <log> realtime
tty_char	

5.5 コマンドリファレンス

5.5.1 ヘルプコマンド

コマンド	説明
help	使用可能なコマンドの一覧を表示します。
help <command>	コマンド <command> の使用方法を表示します。
help usage	すべてのコマンドとその使用方法を表示します。
tty_char	使用可能なキーボードのショートカットコマンドの一覧を表示します。

5.5.2 状態コマンド

コマンド	説明
status	統計情報を表示します。以下に示すように、いくつかのモードが指定できます。デフォルトは realtime です。 構文 : # **status [alarms | crl [all | last] | line | <logID> | realtime]** 「alarms」は、現在のアラームイベントを表示します。 「crl all」は、ダウンロードしたすべての CRL の状態を表示します。 「crl last」は、前回ダウンロードした CRL の状態を表示します。 「line」は、統計情報を項目ごとに行単位文字列として表示します。 「realtime」は、統計情報をリアルタイム表示します。 「logID」は、ログファイル内の統計情報およびアラームイベントを表示します。
show status	統計情報を表示します（status と同じ）。

5.5.3 SSL コマンド

コマンド	説明
create key	新しいキーペアを作成し、KeyID を割り当てます。 例 : # **create key** Key strength (512/1024) [512]: **<Enter>** New keyID [001]:**001** Keypair was created for keyID: 001.
delete key	指定した KeyID を持つキーペアを削除します。 構文 : # **delete key <keyID>** 「keyID」は、削除されるキーペアに対応する KeyID です。
import key	指定した KeyID を持つキーペアをインポートします。指定した鍵が暗号化されている場合は、import key コマンドを実行すると、暗号化パスワードを入力するようプロンプトが表示されます。 構文 : # **import key <keyID>** 「keyID」は、インポートされるキーペアの KeyID です。 設定の詳細は、「4.4 SSLAccelerator へのインポート」（→ 46 ページ）を参照してください。

コマンド	説明
export key	指定した KeyID を持つキーペアをエクスポートします（ascii、xmodem のいずれか）。セキュリティを確実にするため、このコマンドを実行すると、指定したキーが暗号化され、暗号化パスワードを入力するようプロンプトが表示されます。 注意 : 暗号化したキーを import key コマンドでインポートするとき、このコマンドで作成したパスワードが必要になります。 構文 : # **export key <keyID>** 例 : # **export key 001** Enter a pass phrase to encrypt the key []: **sesame** Enter the pass phrase again to confirm []: **sesame** Export protocol: (xmodem, ascii) [ascii]: **<Enter>** Press any key to start, then again when done... -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED DEK-Info: DES-EDE3-CBC,E7D86BD9EB1C9DEEcbV/ GpxBZZjBal5tkjh1lSMzMpD4Nl/kTf89lDzcVdy/ YKehgmLXvoTrPVy4pIMm . . ... 7FjciZrZh3ab4Yl/CkGsBClAvyMEHvu4cuNS0fE6nuw= -----END RSA PRIVATE KEY----- 「keyID」は、エクスポートされるキーペアの KeyID です。
show key	指定した KeyID に対応する、拡張されたキーペア（PEM 形式を含む）を表示します。KeyID を指定しない場合は、すべてのキーが表示されます。 構文 : # **show key <keyID>** 「keyID」は、表示されるキーペアに対応する KeyID です。
list keys	使用可能な KeyID を一覧表示します。 例 : # **list keys** 001 default

コマンド	説明
create cert	**指定した** KeyID **に対応する電子証明書を作成します。** **構文** : # **create cert <keyID>** **「**keyID**」は、電子証明書が作成される** KeyID **です。** **設定の詳細は、「**4.5 SSLAccelerator **での新しい鍵／電子証明書の作成」（→** 48 **ページ）を参照してください。**
delete cert	**指定した** KeyID **に対応する電子証明書を削除します。** **構文** : # **delete cert <keyID>** **「**keyID**」は、削除される電子証明書に対応する** KeyID **です。**
import cert	**指定した** KeyID **に対応する電子証明書をインポートします。** **構文** : # **import cert <keyID>** **「**keyID**」は、インポートされる電子証明書に対応する** KeyID **です。**
export cert	**指定した** KeyID **に対応する電子証明書をエクスポートします。** **構文** : # **export cert <keyID>** **「**keyID**」は、エクスポートされる電子証明書に対応する** KeyID **です。**
show cert	**指定した** KeyID **に対応する、拡張された電子証明書（**PEM **形式を含む）を表示します。**KeyID **を指定しない場合は、すべての電子証明書が表示されます。** **構文** : # **show cert <keyID>** **「**keyID**」は、表示される電子証明書に対応する** KeyID **です。**

コマンド	説明
set ciphers	**指定した** MapID **のマッピングによって認識される** SSL **のバージョンと暗号方式の強さを設定します。** **構文** : # **set ciphers <mapID> [default]** **例** : # **set ciphers 1** 1 - all 2 - high 3 - medium 4 - low 5 - export only 6 - Customized Ciphers Select cipher strength [1]: **1** 1 - SSLv2 2 - SSLv3 3 - SSLv2 and SSLv3 Select ciphers from SSL version [3]: **2** **「**mapID**」は、暗号方式を設定する** MapID **です。** **オプションパラメタ「**default**」を入力して、指定した** MapID **のマッピングで認識される** SSL **のバージョンと暗号方式の強さをデフォルトにします。** **サポートしている暗号方式については、「**A.4 **対応している暗号方式」（→** 194 **ページ）を参照してください。**
show ciphers	**指定した** MapID **のマッピングで認識される** SSL **のバージョンと暗号方式の強さの設定を表示します。** **構文** : # **show ciphers <mapID>** **「**mapID**」は、表示するマッピングの** MapID **です。**

コマンド	説明
set cert_redir	**クライアント電子証明書がないか、または無効な電子証明書を持つクライアントに対して、リダイレクト先のアドレスを設定します。** **構文** : **set cert_redir <mapID> [none]** **例** : **set cert_redir 1** Enter a none/bad client cert redirect URL at the following prompt e.g. http://www.mycompany.xyz/clientcert.html Enter a none/bad client cert redirect URL []: **http://www.yourcompany.xyz/clientcert.html** **「**mapID**」は、クライアント電子証明書のリダイレクト先のアドレスが定義される** mapID **です。** **オプションのパラメタ「**none**」を入力して、指定したマップ** ID **の既存のクライアント電子証明書のリダイレクト先のアドレスを無効にすることができます。**
show cert_redir	**クライアント電子証明書がないか、または無効な電子証明書を持つクライアントのリダイレクト先のアドレスを表示します (** 指定した MapID **についてリダイレクト先のアドレスが設定されている場合**)。 **構文** : # **show cert_redir <mapID>** **「**mapID**」は、リダイレクト先のアドレス が表示されるマッピングです。** **例** : # **show cert_redir 1** cert_redir for mapping 1 is set: http:// www.yourcompany.xyz/clientcert.html

コマンド	説明
set cipher_redir	**指定した** MapID **に対応する暗号方式をクライアントがサポートしていない場合に、そのクライアントのリダイレクト先のアドレスを設定します。** **構文** :**set cipher_redir <mapID> [none]** **例** : **set cipher_redir1** Enter a weak cipher redirect URL at the following prompt e.g. http://www.mycompany.xyz/weakbrowser.html Enter a weak cipher redirect URL []: **http://www.yourco.xyz/weakbrowser.html** **「**mapID**」は、暗号方式をサポートしていない場合のリダイレクト先のアドレスを定義する** MapID **です。** **オプションのパラメタ「**none**」を入力して、指定した** MapID **に対応する、既存の弱い暗号方式のリダイレクト先のアドレスを無効にすることができます。**
show cipher_redir	**指定した** MapID **に対応する暗号方式をクライアントがサポートしておらず、そのクライアントのリダイレクト先となるアドレスが設定されている場合に、そのアドレスを表示します。** **構文** : # **show cipher_redir <mapID>** **「**mapID**」は、リダイレクト先の** URL **を表示するマッピングです。** **例** : # **show cipher_redir 1** cipher_redir for mapping 1 is set: http://www.yourcompany.xyz/weakbrowser.html

コマンド	説明
set redir_change	指定した mapID ついて、リダイレクトヘッダを HTTP から HTTPS に変換するかどうかを設定します。 構文 : # **set redir_change <mapID>[enable | disable | all]** 例 : # **set redir_change 1 enable** Enter the URL domain name key word [all]: **www** Http redirection has www will be changed https. 「enable」は、リダイレクト先 URL についてキーワードで指定したヘッダ文字列が存在する場合、リダイレクト先 URL を HTTP から HTTPS に変換します。キーワードに「all」を指定すると、すべてのリダイレクト先 URL を HTTPS に変換します。 「disable」は、すべてのリダイレクト先 URL を HTTP から HTTPS に変換しません。 「all」は、すべてのリダイレクト先 URL を HTTPS に変換します。
show redir_change	指定した mapID について、HTTP から HTTPS に変換されるように設定されているリダイレクトヘッダの文字列のキーワードを表示します。 構文 : # **show redir_change <mapID>** 例 : # **show redir_change 1** Http redirection that has www will be changed https.
show client_ca	指定した MapID に対応する、クライアント認証用 CA の電子証明書の内容（PEM 形式を含む）を表示します。クライアント認証用 CA の電子証明書がインポートされていない場合は、このコマンドを実行すると、そのことを示すメッセージが表示されます。MapID を指定しない場合は、すべてのクライアント認証用 CA の電子証明書が表示されます。 構文 : **show client_ca <mapID>** 「mapID」は、表示されるインポートされたクライアント認証用 CA の電子証明書を持つキーの MapID です。

コマンド	説明
import client_ca	クライアントを認証する場合は、このコマンドを使用して、クライアント認証用 CA の電子証明書をインポートします。クライアント認証機能が有効になると、クライアント電子証明書を持たないクライアントや無効な電子証明書を持つクライアントは、接続を拒否されます。 **構文** : **import client_ca <mapID>** **例** : # **import client_ca 1** Import protocol (paste, xmodem) [paste]: **<Enter>** Type or paste in data, end with ... alone on a line. **（ここにクライアント認証用** CA **の電子証明書を貼り付けます）** ...**<Enter>** **「**mapID**」は、インポートされるクライアント認証用** CA **の電子証明書が関連付けられる** MapID **です。**
delete client_ca	**指定した** MapID **に対応するクライアント認証用** CA **の電子証明書を削除します。** **構文** : **delete client_ca <mapID>** **「**mapID**」は、削除されるクライアント認証用** CA **の電子証明書に対応する** MapID **です。**
create sign	**指定した** KeyID **の署名要求を作成します。** **構文** : # **create sign <keyID>** **「**keyID**」は、署名要求が作成されるキーの** KeyID **です。** **設定の詳細は、「**4.2 **認証局からの電子証明書の取得」（→** 41 **ページ）を参照してください。**
delete sign	**指定した** KeyID **の署名要求を削除します。** **構文** : # **delete sign <keyID>** **「**keyID**」は、署名要求が削除されるキーの** KeyID **です。**

コマンド	説明
export sign	指定した KeyID の署名要求（PEM 形式）をエクスポートします。 構文 : # **export sign <keyID>** 「keyID」は、署名要求がエクスポートされるキーの KeyID です。
show sign	指定した KeyID に対応する、拡張された署名要求（PEM 形式）を表示します。 KeyID を指定しない場合は、すべての署名要求が表示されます。 構文 : # **show sign <keyID>** 「keyID」は、署名要求が表示されるキーの KeyID です。
set defcert	電子証明書や署名要求の作成時に使用されるデフォルト値を設定します。デフォルト値には、国コード、州（県）、地区名、組織名、組織ユニット名、電子証明書を使用するサイト名、要求元の電子メールアドレスなどが含まれています。これらのフィールドをすべて変更する、一部を変更する、変更しない等の操作が可能です。[Enter] キーを押すと、デフォルト値が確定され、次のフィールドに移動します。 例 : # **set defcert** Country name [XX]: **<Enter>** State [MyState]: **<Enter>** City [MyCity]: **<Enter>** Organization [MyCompany]: **<Enter>** Organization unit [MyCompany Division]: **<Enter>** Issuer name [www.MyCompany.xyz]: **<Enter>** Issuer email address [support@MyCompany.xyz]: **<Enter>** Make changes [y]: **<Enter>** Changes applied
show defcert	電子証明書作成や署名要求の作成時に使用されるデフォルト値を表示します。 例 : # **show defcert** Country : XX State : MyState City : MyCity Organization : MyCompany Unit : MyCompany Division Name : www.MyCompany.xyz Email : support@MyCompany.xyz

コマンド	説明
set kstrength	公開／秘密鍵ペアの強さ（デフォルト）を設定します。設定可能な値は 512 または 1024 で、デフォルト値は 512 です。 構文 : # **set kstrength [512 | 1024]** 「512」は、鍵の強さを Low に設定します。 「1024」は、鍵の強さを High に設定します。
show kstrength	公開鍵と秘密鍵の強さを表す値を表示します。 例 : # **show kstrength** Default key strength: 512
set client_tmo	クライアント要求のあと、クライアントとサーバの間の接続がこの値を超えてアイドル状態になっていると（いずれの方向にもデータが送信されないと）、接続がタイムアウトになります。デフォルト値は 30（秒）です。 構文 : # **set client_tmo <secs>** 「secs」は、5 ～ 36000 の範囲の値（秒）です。
show client_tmo	現在指定されているクライアントタイムアウト値を表示します。 例 : # **show client_tmo** Client timeout [secs]: 30
set server_tmo	サーバとの接続が行われるまでの制限時間を指定します。指定した時間内に接続が行われないと、クライアント要求は拒否されます（接続要求 SYN に対しサーバが SYN+ACK を返すまでの時間を指定します）。 注意 : サーバがタイムアウトする一般的な原因には、サーバの電源がオフになっている、サーバにアクセスできない、指定したポート上でアプリケーションが使用できないなどがあります。 構文 : # **set server_tmo <secs>** 「secs」は、5 ～ 36000 の範囲の値（秒）です。

コマンド	説明
show server_tmo	**現在指定されているサーバのタイムアウト値を表示します。** **例** : # **show server_tmo** Server timeout [secs]: 5
set cache	SSL session **のキャッシュサイズ値とタイムアウト値を設定します。この機能の詳細については、「**4.12 SSL **セッションのキャッシュ機能」（→** 67 **ページ）を参照してください。キャッシュサイズ値の範囲は** 0 **〜** 20**（**K**）で、デフォルト値は** 18**（**K**）です。キャッシュサイズを** 0 **に設定すると、キャッシュ機能は無効になります。タイムアウト値の範囲は、**30 **〜** 86400**（秒）で、デフォルト値は** 180**（秒）です。** **例** : # **set cache** Enter SSL session cache size (0-20K) [18]: **18** Enter SSL session timeout (30-864000) [180]: **3600**
show cache	SSL session **のキャッシュ値として現在設定されている内容を表示します。** **例** : # **show cache** SSL Session Cache Size : 18K SSL Session Timeout : 3600 seconds

5.5.4 CRL コマンド

コマンド	説明
show crl	**指定した** MapID **について、現在の** CRL **を表示します。** MapID **を指定しない場合は、すべての** CRL **が表示されます。** **構文** : # **show crl <mapID>** **例** : # **show crl 1** ========== /keys/0.0.0.0_443_80_crl.pem========== Certificate Revocation List (CRL): Version 1 (0x0) Signature Algorithm: md5WithRSAEncryption Issuer: /C=XX/ST=CA/L=City/O=Company/OU=Unit QA/CN=broker/Email=broker@MyCompany.xyz Last Update: Mar 2 09:10:30 2001 GMT Next Update: Apr 1 09:10:30 2001 GMT Revoked Certificates: Serial Number: 1004 Revocation Date: Mar 2 09:10:29 2001 GMT Serial Number: 100E Revocation Date: Mar 2 09:10:29 2001 GMT Signature Algorithm: md5WithRSAEncryption 32:ed:12:5b:e4:fd:34:d2:86:68:08:e2:08:22:56:62:14:c0:9a: b2:83:f0:bf:d8:a1:aa:11:25:d0:15:a4:cf:d1:d1:6d:39:ad:6f:3f: 6d:d3:1a:05:41:4f:89:74:63:1e:58:cd:67:9d:04:51:eb:d2:93: fc:23:ed:ea:65:13:dc:9c:d1:90:c7:48:53:50:02:ad:5f:93:5d: 1e:a3:d8:b4:37:51:c0:e0:35:bf:bc:d1:42:66:83:99:0a:d1:c8: ff:02:a6:f4:a8:90:ba:29:58:59:28:8e:8f:e9:86:1b:4c:70:0d:c6: 47:4d:71:6e:02:e1:c7:29:6b:92:83:04 -----BEGIN X509 CRL----- MIIBczCB3TANBgkqhkiG9w0BAQQFADCBgTELMA...etc. ... -----END X509 CRL-------
delete crl	**指定したマッピングについて、現在の** CRL **を消去します。** **構文** : **delete crl <mapID>** **例** : # **delete crl 1** The CRL for mapping 1 is deleted.

コマンド	説明
set crl_mode	**指定したマッピングについて、サーバタイプ（**ftp、http、**または** ldap**）と** CRL **のファイル名（およびディレクトリの場所）を設定します。このコマンドは、クライアント電子証明書が取得されていて、かつ** IP **アドレスが設定されている場合のみ有効です。** **構文** : # **set crl_mode <mapID>** **例** : # **set crl_mode 1** Enter the CRL upload mode, (ftp ǀ http ǀ ldap) [ftp]:**http** Enter CRL server IP address []: **10.8.50.5** Enter CRL filename []: **directory\path\crl.pem** Enter username []: **username** Enter password []: **password** crld started.
show crl_mode	**指定したマッピングについて、**CRL **モード（サーバタイプ）、アップロードの場所、ファイル名、およびユーザ情報の最新の状態を表示します。** **構文** : # **show crl_mode <mapID>** **例** : # **show crl_mode 1** The crl auto upload mode is ftp. The crl auto upload location is 10.8.50.16. The crl auto upload filename is /usr/var/tmp/certs/crl.pem. The crl auto upload username is username. The crl auto upload password is password.
delete crl_mode	**指定した** MapID **について、現在のダウンロードモードを無効にします。** **構文** : **delete crl_mode <mapID>**
set crl_refresh	CRL **の更新間隔を分単位で設定するか、または現在指定されている更新間隔とは無関係に新しい** CRL **をただちに要求します。** **構文** : **set crl_refresh [now ǀ <0-1440>]**

コマンド	説明
show crl_refresh	**現在すべてのマッピングに適用されている** CRL **更新間隔を表示します。** **構文** : **show crl_refresh** **例** : # **show crl_refresh** CRL refresh period is set to 60 minutes.
import crl	**指定したマッピングについて、**CRL **をコンソールに貼り付けたり、**Xmodem **で送信できるようにします。このコマンドは、**CRL **の定期的な更新には影響しません。インポートされた** CRL **は、定期的な更新間隔で上書きされます。このコマンドを実行する前に、クライアント** CA **をインポートしておく必要があります。** **構文** : **import crl <mapID>** **例** : # **import crl 1** Import protocol (paste, xmodem) [paste]: **<Enter>** Type or paste in data, end with ... alone on a line. (**ここに** CRL **を貼り付けます**) ... **<Enter>** Import successful!

コマンド	説明
export crl	**指定したマッピングについて、有効な** CRL **を** SSLAccelerator **からコンソールへ** ASCII **または** Xmodem **で送信できるようにします。** **構文** : **export crl <mapID>** **例** : **export crl 1** Export protocol: (xmodem, ascii) [ascii]: **<Enter>** Press any key to start, then again when done... -----BEGIN X509 CRL----- MIIBczCB3TANBgkqhkiG9w0BAQQFADCBgTELMAkGA1U EBhMCVVMxCzAJBgNVBAgTAkNBMRIwEAYDVQQHEwlT . . . P8l+3qZRPcnNGQx0hTUAKtX5NdHqPYtDdRwOA1v7zRQ maDmQrRyP8CpvSokLopWFkojo/ phhtMcA3GR01xbgLhxylrkoME -----END X509 CRL-----
delete crl_status	**以前の** CRL **のダウンロード状態の情報を削除します。** **構文** : **delete crl_status**

5.5.5 マッピングコマンド

マッピングコマンドは、第 4 章の「■ サーバの割り当て（マッピング）」（→ 61 ページ）、「4.11 ブロック機能」（→ 63 ページ）で説明した処理を行うときに使用します。

コマンド	説明
create block	**指定の** IP **アドレスの指定のポート番号へのアクセスを拒否するブロックを作成します。単一の** IP **アドレスにつき、単一のポートまたはすべてのポートをブロックできます。**1 **部のポートだけをブロックする場合は、各ポートに対して** create block **コマンドを繰り返し使用する必要があります。** **注意** :255.255.255.255 **をブロックアドレスとして指定できません。** **注意** :SSLAccelerator **がワンアーム接続のときは、ブロックは作成できません。** **例** : # **create block** Client IP to block [0.0.0.0]: **10.1.2.1** Client IP mask [0.0.0.0]: **255.255.255.255** Server IP to block [0.0.0.0]: **20.1.2.1** Server IP mask [0.0.0.0]: **255.255.255.255** Server Port to block (0-65535): **80** Server Port mask [0xffff]: **<Enter>**
delete block	**指定したブロック番号のブロックを削除します。既存のブロックとその番号を表示するには、**show blocks **コマンド（以下を参照）を使用してください。** **構文** : # **delete block <blockID>** **例** : # **delete block 1**
show blocks	**現在設定されている全ブロックを表示します。** **例** : # **show blocks** -------- blocks : --------- (1) block 10.1.2.1 255.255.255.255 20.1.2.1 255.255.255.255 80 0xffff ----------
list blocks	**現在設定されている全ブロックを表示します（**show blocks **と同じ）。**

コマンド	説明
create permit	特定のサーバおよび特定のポートに対して、特定のユーザにアクセス権を与えるかどうかを設定します。 注意 :255.255.255.255 を許可アドレスとして指定できません。 注意 :SSLAccelerator がワンアーム接続のときは、許可を指定できません。 例 : # **create permit** Client IP to permit [0.0.0.0]:**10.1.2.1** Client IP mask [0.0.0.0]:**255.255.255.255** Server IP to permit [0.0.0.0]:**20.1.2.1** Server IP mask [0.0.0.0]:**255.255.255.255** Server Port to permit (0-65535): **443** Server Port mask [0xffff]: **<Enter>**
delete permit	指定した許可番号の許可を削除します。既存の許可とその番号を表示するには、show permits コマンド（以下を参照）を使用してください。 構文 : # **delete permit <permitID>** 例 : # **delete permit 1**
show permits	現在有効な許可を表示します。 例 : # **show permits** -------- permits : --------- (1) permit 10.1.2.1 255.255.255.255 20.1.2.1 255.255.0.0 443 0xffff ----------
list permits	現在有効な許可を表示します（show permits と同じ）。

コマンド	説明
show filters	**現在設定されているブロックと許可を表示します。** **例** : # **show filters** -------- blocks : --------- (1) block 10.1.2.1 255.255.255.255 20.1.2.1 255.255.255.255 80 0xffff ---------- -------- permits : --------- (1) permit 10.1.2.1 255.255.255.255 20.1.2.1 255.255.0.0 443 0xffff ----------
list filters	**現在設定されているブロックと許可を表示します（**show filters **と同じ）。**
create map	**サーバの** IP **アドレス（ワンアーム接続が有効なときは、** Inbound **と** Outbound **の** IP **アドレス）、**SSL **ポート、クリアテキストポート、**KeyID **の対応関係を示すマッピングを作成します。** **注意** :255.255.255.255 **をサーバ** IP **アドレスとして使用できません。** **例（インパス接続の場合）**: # **create map** Server IP [0.0.0.0]: **1.1.1.1** SSL (network) port [443]: **443** Cleartext (server) port [80]: **8080** KeyID to use for mapping: **001** **例（ワンアーム接続の場合）**: # **create map** Inbound IP [0.0.0.0]: **1.1.1.1** Outbound IP [1.1.1.1]: **1.1.1.2** SSL (network) port [443]: **443** Cleartext (server) port [80]: **8080** KeyID to use for mapping: **001** **注意** :create map **コマンドを実行する前に、新しいマッピングに使用される** KeyID **が作成されていなければなりません。** create key **コマンドを使用して、新しい** KeyID **を作成してください。また、マッピングを使用する前に、**KeyID **に電子証明書が関連付けられていなければなりません（詳細については、「第** 4 **章 鍵と電子証明書」（→** 39 **ページ）を参照）。**

コマンド	説明
delete map	**マッピングを削除します。** **注意** : **このコマンドを実行すると、削除するように指定した** MapID **より大きい** MapID **は、すべて** 1 **ずつデクリメントされます。** **構文** : # **delete map <mapID>** **「**mapID**」は、削除されるマッピングの** MapID **です。**
list map	**さまざまな設定を持つすべてのマッピングを一覧表示します（**show map **と同じ）。** **例（インパス接続の場合）** : # **list map** Map ID KeyID Server IP Net Port Ser Port Cipher Suites Re-direct Client Auth == ===== ======= ==== ==== ======== ===== ==== 1 default Any 443 80 all (v2+v3) n n 2 sample 1.1.2.5 443 80 med (v2+v3) n n **例（ワンアーム接続の場合）** : # **list map** Map ID KeyID Server IP Net Port Ser Port Cipher Suites Re-direct Client Auth == ===== ======= ==== ==== ======== ===== ==== 1 default Any 443 80 all (v2+v3) n n Any 2 sample 1.1.2.5 443 80 med (v2+v3) n n 1.1.2.6
show map	**すべてのマッピングを表示します（**list map **と同じ）。**
set map_visible	map visible **機能の有効／無効を切り替えます。サーバに送信される** ping **クエリが** SSLAccelerator **によって阻止される可能性のあるようなネットワーク構成になっている場合、ワンアーム接続ではこの機能を有効にするのが一般的です。** **構文** : # **set map_visible [enable | disable]**
show map_visible	map visible **機能の現在の状態（有効／無効）を表示します。** **例** : # **show map_visible** map_visible : disable

5.5.6 操作コマンド

コマンド	説明
bypass	バイパスモードを有効にします。バイパスモードの詳細は、「A.3 障害／バイパスモード」（→ 192 ページ）を参照してください。バイパスを取り消すモード（インラインモード）については、inline コマンドの項目を参照してください。 警告 : リモート管理セッション（Telnet または SSH）からは、bypass コマンドを発行しないでください。発行すると、SSLAccelerator との接続がただちに切断されます。 構文 : # **bypass** バイパスモードが有効になると、SSLAccelerator のフロントパネル上の Inline LED が消灯します。 注意 : Bypass ボタンと CLI の bypass コマンドを同時に使用して、SSLAccelerator をバイパスモードにすることができます。この場合、SSLAccelerator をインラインモードに戻すには、Bypass ボタンと CLI の inline コマンドの両方を使用する必要があります。
inline	インラインモードを有効にします。インラインモードでは、SSLAccelerator は通常の方法でトラフィックを処理します。 注意 : 何らかの要因でインラインモードを使用できないことがあります。これらについては、「A.3 障害／バイパスモード」（→ 192 ページ）を参照してください。 例 : # **inline** インラインモードが有効になると、SSLAccelerator のフロントパネル上の Inline LED が点灯します。

コマンド	説明
set onearm	**ワンアーム接続の有効／無効を切り替えます。** SSLAccelerator **の** Network **側ポートがスイッチに接続されており、**Server **側ポートを使用しない場合は、この値を「**enable**」に設定しないと、**SSLAccelerator **は正常に動作しません。物理的な接続方法の詳細については、「第** 2 **章 設置と初期設定」（→** 7 **ページ）と「第** 3 **章 構成」（→** 23 **ページ）を参照してください。** **注意** : **キャッシュサーバが完全に見えないようにする機能を持つスイッチに** SSLAccelerator **を接続している場合は、**Preserve client IP **オプションを有効にすることをお勧めします。** **注意** : **ワンアーム接続を有効にすると、**create map **コマンドおよび** list map **コマンド (または** show map **コマンド) の機能が変わります。** **例** : # **set onearm enable** Preserve client IP (y/n)? [n]:**y** One-arm mode enabled with client IP preservation.
show onearm	**ワンアーム接続の現在の状態（有効／無効）を表示します。** **注意** : **ワンアーム接続が無効になっているときに、このコマンドを実行すると、"** Running Inpath Operation. **"と表示されます。** **例** : # **show onearm** Running One-arm Operation (with client IP preserved) **注意** :Preserve Client IP **機能が無効な場合は、"** Running One-arm Operation **"とだけ表示されます。**
set route	SSLAccelerator **がインターネットと通信するときに経由するルータまたはゲートウェイのアドレスを指定します。** **注意** :IP **アドレス** 0.0.0.0 **は使用できません。** **構文** : # **set route <ip address>** **例** : # **set route 51.1.34.1**

コマンド	説明
show route	SSLAccelerator がインターネットと通信するときに経由するルータまたはゲートウェイとして現在指定されているアドレスを表示します。 構文 : # **show route** Default Route: 51.1.34.1
set ser_loc_trust	サーバ位置確認機能の有効／無効を切り替えます。デフォルトでは、SSLAccelerator は SSL 接続を許可する前にそのサーバの位置を確認しようとします。しかし、SSLAccelerator の後ろにプロキシサーバが配置されていると、このサーバ位置確認機能により一部の接続がブロックされてしまいます。そうした現象に対する配慮として、この機能を無効にするコマンドが用意されています。 注意 :SSLAccelerator がワンアーム接続で構成されている場合、この機能は使用できません。 構文 : # **set ser_loc_trust [enable | disable]** 例 : # **set ser_loc_trust enable** Server locations will not be validated before accepting connections.
show ser_loc_trust	サーバ位置確認機能の現在の状態（有効／無効）を表示します。 例 : # **show ser_loc_trust** ser_loc_trust: enabled
set spill	「spill」モードの有効／無効を切り替えます。「spill」モードでは、SSLAccelerator が受け取った要求の待ち行列の長さが一定の値に達すると、その値より上の要求は処理されずにそのまま次段に接続された（つまり server 側ポートに接続された）SSLAccelerator またはサーバに渡されます。 構文 : # **set spill [enable | disable]** 例 : # **set spill enable**

コマンド	説明
show spill	「spill」オプションのモードの現在の状態（有効／無効）を表示します。 例 : # **show spill** Spill on overload: disabled
set hwq_hiwat_spill	ハードウェア待ち行列の spill の最高点を設定します。この値は、ハードウェア待ち行列で待ち状態にある要求の数を示します。この値を超えると、SSLAccelerator は spill モードに入るか、またはカスケード接続されている次の SSLAccelerator に新しい要求を送ります。spill モードにある SSLAccelerator は、ハードウェア待ち行列の要求の数が、指定した最低点（set hwq_lowat_spill を参照）まで減少すると、処理を再開します。デフォルト値は 1 です。 構文 : **set hwq_hiwat_spill <1-256>**
show hwq_hiwat_spill	ハードウェア待ち行列の現在の spill の最高点を表示します。 例 : # **show hwq_hiwat_spill** HW spill high water mark: 1
set hwq_lowat_spill	ハードウェア待ち行列の spill の最低点を設定します。このコマンドは、SSLAccelerator のハードウェア待ち行列にある要求の数を指定します。この値に達すると、SSLAccelerator の spill モードが終了して、処理が再開されます（set hwq_hiwat_spill を参照）。デフォルト値は 1 です。 構文 : **set hwq_lowat_spill <1-256>**

コマンド	説明
show hwq_lowat_spill	**ハードウェア待ち行列の現在の** spill **の最低点を表示します。** **例** : # **show hwq_lowat_spill** HW spill low water mark: 1
reboot	SSLAccelerator **を再起動します。** **警告** : **再起動すると、現在の** CLI **セッションの間に行われた設定変更はすべて失われます。設定変更を保存する方法については、**config save **コマンドを参照してください。** **例** : # **reboot** Are you sure you want to reboot (y/n) ? [n]: **y** System rebooting...done **(システムが再起動され、パスワードの入力を求めるプロンプトが表示されます。)**

5.5.7 ヘッダ挿入コマンド

⚠注意

同一サーバに対して複数の SSLAccelerator を構成しており、ヘッダ挿入機能を有効にしている場合は、それらの SSLAccelerator をすべて同じ設定にする必要があります。
また、サーバの keepalive 機能は無効にする必要があります。

コマンド	説明
set hdr_fields	**補足用のデータ項目がある場合に、どの項目を復号済み HTTP トラフィックに挿入してサーバに送信するかをマッピングごとに指定します。** **構文** : # **set hdr_fields <mapID>** Enter the header insertion fields (cert cipher ip user all none) [all]: **[cert | cipher | ip | user | all | none]** **「**cert**」は、指定した** mapID **に対応する電子証明書です。** **「**cipher**」は、指定した** mapID **に対応する暗号です。** **「**ip**」は、クライアントのソース** IP **アドレスです。** **「**user**」を指定すると、ユーザ定義可能な** HTTP **ヘッダが有効になります。** **「**all**」を指定すると、すべてのフィールドが有効になります。** **「**none**」を指定すると、すべてのフィールドが無効になります。**
show hdr_fields	**指定したマッピングについて、挿入するヘッダ文字列の項目を表示します。** **例** : # **show hdr_fields 1** The hdr_fields for mapping 1 is set : cert
set hdr_cert	**指定したマッピングについて、クライアント電子証明書のヘッダ文字列を設定します。** **構文** : # **set hdr_cert <mapID> [none]** **例** : # **set hdr_cert 1** Enter the cert string ID [SSL_CLIENT_CERTIFICATE]: **HEADER_CERT** **オプションパラメタ「**none**」を入力して、指定した** MapID **に対するクライアント電子証明書のヘッダ文字列の定義を無効にすることができます。**

コマンド	説明
show hdr_cert	**指定したマッピングについて、現在定義されているクライアント電子証明書のヘッダ文字列を表示します。** **例** : # **show hdr_cert 1** hdr_cert for mapping 1 is set: HEADER_CERT
set hdr_cipher	**指定したマッピングについて、暗号方式のヘッダ文字列を設定します。** **構文** : # **set hdr_cipher <mapID> [none]** **例** : # **set hdr_cipher 1** Enter the cipher string ID [SSL_CIPHER_USED]: **HEADER CIPHER_IP** **オプションパラメタ「**none**」を入力して、指定した** MapID **に対する暗号方式のヘッダ文字列の定義を無効にすることができます。**
show hdr_cipher	**指定したマッピングについて、現在定義されている暗号方式のヘッダ文字列を表示します。** **例** : # **show hdr_cipher 1** hdr_cipher for mapping 1 is set: HEADER_CIPHER_IP
set hdr_cip	**指定したマッピングについて、クライアント** IP **アドレスのヘッダ文字列を設定します。** **構文** : # **set hdr_cip <mapID> [none]** **例** : # **set hdr_cip 1** Enter the client IP string ID [SSL_SOURCE_IP]:**HEADER CLIENT_IP** **オプションパラメタ「**none**」を入力して、指定した** MapID **に対するクライアント** IP **アドレスのヘッダ文字列の定義を無効にすることができます。**
show hdr_cip	**指定したマッピングについて、現在定義されているクライアント** IP **アドレスのヘッダ文字列を表示します。** **例** : # **show hdr_cip 1** hdr_cip for mapping 1 is set: HEADER_CLIENT_IP

コマンド	説明
set hdr_sid	**指定したマッピングについて、**SSL **セッション** ID **のヘッダ文字列を設定または削除します。** **構文** : # **set hdr_sid <mapID> [none]** **例** : # **set hdr_sid 1** Enter the SSL session ID string ID [SSL_SSL_SESSION_ID]:**HEADER SESSION_ID** **オプションパラメタ「**none**」を入力して、指定した** MapID **に対する** SSL **セッション** ID **のヘッダ文字列の定義を無効にすることができます。**
show hdr_sid	**指定したマッピングについて、現在定義されている** SSL **セッション** ID **のヘッダ文字列を表示します。** **例** : # **show hdr_sid 1** hdr_sid for mapping 1 is set: HEADER_SESSION_ID
set hdr_user	**指定したマッピングについて、ユーザが定義した** HTTP **ヘッダを設定します。** **構文** : # **set hdr_user <mapID> [none]** **例** : # **set hdr_user 1** Enter the user defined HTTP header []: **U-D Header**
show hdr_user	**指定したマッピングについて、ユーザが定義した** HTTP **ヘッダを表示します。** **構文** : # **show hdr_user <mapID>** **例** : # **show hdr_user 1** hdr_user for mapping 1 is set: U-D Header
set hdr_cert_def	**デフォルトのクライアント電子証明書のヘッダ文字列を設定します。** **例** : **set hdr_cert_def** Enter the default cert string ID [SSL_CLIENT_CERTIFICATE]: **CLIENT_CERT_DEF**

コマンド	説明
show hdr_cert_def	**現在定義されているデフォルトのクライアント電子証明書のヘッダ文字列を表示します。** **例** : # **show hdr_cert_def** The default cert ID string is: CLIENT_CERT_DEF
set hdr_cipher_def	**デフォルトの暗号方式のヘッダ文字列を設定します。** **例** : **set hdr_cipher_def** Enter the default SSL cipher string ID [SSL_CIPHER_USED]: **CIPHER_DEF**
show hdr_cipher_def	**現在定義されているデフォルトの暗号方式のヘッダ文字列を表示します。** **例** : # **show hdr_cipher_def** The default cipher ID string is: CIPHER_DEF
set hdr_cip_def	**デフォルトのクライアント** IP **ヘッダ文字列を設定します。** **例** : # **set hdr_cip_def** Enter the default client IP string ID [SSL_SOURCE_IP]: **IP_DEF**
show hdr_cip_def	**現在定義されているデフォルトのクライアント** IP **ヘッダ文字列を表示します。** # **show hdr_cip_def** The default SSL cipher ID string is: IP_DEF
set hdr_sid_def	**デフォルトの** SSL **セッション** ID **のヘッダ文字列を設定します。** **例** : # **set hdr_sid_def** Enter the default SSL session ID string ID [SSL_SSL_SESSION_ID]: **SESSION_ID_DEF**
show hdr_sid_def	**現在定義されているデフォルトの** SSL **セッション** ID **のヘッダ文字列を表示します。** # **show hdr_sid_def** The default SSL session ID string is: SESSION_ID_DEF

5.5.8 リモート管理コマンド

コマンド	説明
list procs	CLI コマンドおよびリモート管理コマンド（crld、inetd、telnetd、sshd2、および snmpd）に関連するプロセスの一覧をすべて表示します。 注意 : 一部のメンテナンスプロセス (crld など) と ntpd も、そのプロセスが有効になっている場合は作動しています。 例 : # **list procs** PID: 40 PROG: cli PID: 41 PROG: cli
set max_remote_sessions	同時に実行する Telnet セッションおよび SSH セッションの最大数を設定します。 構文 : # **set max_remote_sessions <0-5>** 「0-5」は、実行されるリモートセッションの最大数です。デフォルトは 5 です。
show max_remote_sessions	同時に実行する Telnet セッションおよび SSH セッションの最大数を表示します。 例 : # **show max_remote_sessions** Network of remote session(s) allowed: 5

コマンド	説明
set telnet	Telnet セッションの有効／無効を切り替えます。このコマンドに「enable」を指定して、IP アドレスを SSLAccelerator のネットワークインターフェースに割り当てると、リモート Telnet セッションを介して SSLAccelerator の CLI にアクセスすることができます。コマンドに「disable」を指定すると、SSLAccelerator は Telnet 接続を受け付けなくなります。不足しているパラメタがある場合は、コンソールがその入力を求めてきます。デフォルトは「disable」です。 **構文** : # **set telnet [enable | disable]** **例** : # **set telnet enable** An IP address is required to start Telnet service. Enter IP Address []: **10.1.2.124** A netmask is required to start Telnet service. Enter Netmask [255.255.255.0]: **<Enter>** An optional default route max to be entered before starting the Telnet service. Enter a default route (' none 'to delete) [none]: **<Enter>** Telnet Service started.
show telnet	Telnet の現在の状態（有効／無効）を表示します。 **例** : # **show telnet** Telnet: enabled
set telnet_port	Telnet 接続を受け入れるポートを設定します（デフォルトポートは 23 です）。 **構文** : # **set telnet_port <port>** <port> は、Telnet セッションを接続するポート番号です。
show telnet_port	Telnet セッションが現在接続されているポートを表示します。 **例** : # **show telnet_port** Telnet Port Number: 23

コマンド	説明
set ssh	SSH（Secure Shell）セッションの有効／無効を切り替えます。このコマンドに「enable」を指定して、IP アドレスを SSLAccelerator のネットワークインターフェースに割り当てると、リモート SSH セッションを介して SSLAccelerator の CLI にアクセスすることができます。コマンドに「disable」を指定すると、SSLAccelerator は SSH 接続を受け付けなくなります。パラメタが指定されていないと、プロンプトが表示されます。デフォルトは「disable」です。 **構文** : # **set ssh [enable | disable]** **例** : # **set ssh enable** An IP address is required to start SSH service. Enter IP Address []: **10.1.2.124** A netmask is required to start SSH service. Enter Netmask [255.255.255.0]: **<Enter>** An optional default route max to be entered before starting the SSH service. Enter a default route (' none 'to delete) [none]: **<Enter>** SSH Service started.
show ssh	SSH の現在の状態（有効／無効）を表示します。 **例** : # **show ssh** SSH: disabled
set ssh_port	SSH セッションを受け入れるポートを設定します（デフォルトポートは 22 です）。 **構文** : # **set ssh_port <port>** 「port」は、SSH セッションを接続するポート番号です。
show ssh_port	SSH セッションを受け入れるポートを表示します。 **例** : # **show ssh_port** SSH Port Number: 22
set snmp	SNMP エージェントの有効／無効を切り替えます。SNMP の情報およびパラメタ（set snmp_info 参照）を見ることができます。デフォルトは「disable」です。 **構文** : # **set snmp [enable|disable]**

コマンド	説明
show snmp	SNMP エージェントの現在の状態（有効／無効）を表示します。 例 : # **show snmp** SNMP: enabled
set snmp_info	以下に示す SNMP の情報およびパラメタを設定します。 • SNMP Port（デフォルトは 161） • SNMP Trap Port（デフォルトは 162） • Contact person • System location • System name 注意 : 上記の各パラメタはそれぞれ、set snmp_port、set trap_port、set sys_contact、set sys_name、set sys_location コマンドで個別に設定することができます。 例 : # **set snmp_info** SNMP Port [161]: **161** SNMP Trap Port [162]: **162** Contact Person []: **support** System Location []: **MyCity** System Name []: **SSL Accelerator v2.5**
show snmp_info	現在設定されている SNMP の情報およびパラメタを表示します。 例 : # **show snmp_info** SNMP Port Number : 161 SNMP Trap Port Number : 162 SNMP System Contact : “ support ” SNMP System Name : “ SSL Accelerator v2.5 ” SNMP System Location : “ MyCity ” System IP Address : 10.1.2.124 System Netmask : 255.255.255.0 Default Route : None
set snmp_port	SNMP ポートを設定します。 構文 : # **set snmp_port <port#>**
show snmp_port	現在設定されている SNMP ポートを表示します。 例 : # **show snmp_port** SNMP Port Number: 161

コマンド	説明
set trap_port	SNMP **のトラップポートを設定します。** **構文** : # **set trap_port <port#>**
show trap_port	**現在設定されている** SNMP **のトラップポートを表示します。** **例** : # **show trap_port** SNMP Trap Port Number: 162
set sys_contact	**管理者を設定します。** **構文** : # **set sys_contact**
show sys_contact	**現在設定されている管理者を表示します。** **例** : # **show sys_contact** SNMP System Contact: support
set sys_name	**システム名を設定します。** **構文** : # **set sys_name**
show sys_name	**現在設定されているシステム名を表示します。** **例** : # **show sys_name** SNMP System Name: SSLAccelerator v2.5
set sys_location	**システム位置を設定します。** **構文** : # **set sys_location <system location>**
show sys_location	**現在設定されているシステム位置を表示します。** **例** : # **show sys_name** SNMP System Name: MyCity

コマンド	説明
set snmp_community	SNMP コミュニティ文字列と SNMP マネージャの IP アドレスを設定します。IP アドレスとコミュニティ文字列の組み合わせによって SNMP 管理ステーションを定義します。定義された IP アドレスを使用しており、かつコミュニティ文字列に一致している SNMP 管理ステーションだけが SSLAccelerator の SNMP 情報にアクセスできます。管理ステーションは 10 台まで定義できます。 注意 :SNMP を使用する場合は、コミュニティ文字列を設定する必要があります。 注意 :IP アドレス 255.255.255.255 は使用できません。 例 : # **set snmp_community** SNMP Community String(s) Setting. Enter a SNMP Community IP (q to quit): **1.1.1.1** Enter a SNMP Community String (q to quit): **public** Enter a SNMP Community IP (q to quit): **q**
list snmp_community	現在設定されている SNMP コミュニティ文字列を表示します。 例 : # **list snmp_community** SNMP Community String(s) information. <2> Current SNMP Community String(s): 1.) IP: 1.1.1.1 => String: public => Rights: read 2.) IP: 1.1.1.2 => String: public => Rights: read
show snmp_community	現在設定されている SNMP コミュニティ文字列を表示します（list snmp_community と同じ）。

コマンド	説明
delete snmp_community	**現在設定されている** SNMP **コミュニティ文字列を削除します。** **例** : # **delete snmp_commmunity** SNMP Community String(s) Deletion. <2> Current Available SNMP Community String(s): 1.) IP: 1.1.1.2 => String: public => Rights: read 2.) IP: 1.1.1.1 => String: public => Rights: read Enter number (1 to 2) to delete (q to quit) [q]: **2** SNMP Community String(s) Deletion. <1> Current Available SNMP Community String(s): 1.) IP: 1.1.1.2 => String: public => Rights: read Enter number (1) to delete (q to quit) [q]: **q**
set trap_authen	**「**enable**」に設定すると、**SNMP **マネージャへ認証異常が発生したときにトラップを送ります。** **構文** : # **set trap_authen [enable|disable]**
show trap_authen	**認証トラップの現在の状態（有効／無効）を表示します。** **例** : # **show trap_authen** SNMP Authorization Trap: enable
set trap_community	SNMP **トラップコミュニティ文字列を設定します。**IP **アドレスとコミュニティ文字列によって、**SSLAccelerator **のトラップメッセージを受信できる** SNMP **管理ステーションを定義します。最大** 10 **台の管理ステーションを定義できます。** **注意** :IP **アドレス** 255.255.255.255 **は使用できません。** **例** : # **set trap_community** SNMP Trap Community String(s) Setting. Enter a SNMP Trap Community IP (q to quit): **0.0.0.0** Enter a SNMP Trap Community String (q to quit): **private** Enter a SNMP Trap Community IP (q to quit): **0.0.0.0** Enter a SNMP Trap Community String (q to quit): **public** Enter a SNMP Trap Community IP (q to quit): **q**

コマンド	説明
list trap_community	SNMP **トラップコミュニティ文字列を表示します。** **例** : # **list trap_community** SNMP Trap Community String(s) information. <2> Current SNMP Trap Community String(s): 1.) IP: 0.0.0.0 => String: private 2.) IP: 0.0.0.0 => String: public
show trap_community	SNMP **トラップコミュニティ文字列を表示します（**list trap_community **と同じ）。**
delete trap_community	SNMP **トラップコミュニティを削除します。** **注意** :SNMP **トラップを使用するには、コミュニティ文字列を設定する必要があります。** **例** : # **delete trap_community** SNMP Trap Community String(s) Deletion. <2> Current Available SNMP Trap Community String(s): 1.) IP: 0.0.0.0 => String: private 2.) IP: 0.0.0.0 => String: public Enter number (1 to 2) to delete (q to quit) [q]: **2** <1> Current Available SNMP Trap Community String(s): 1.) IP: 0.0.0.0 => String: private Enter number (1to 2) to delete (q to quit) [q]: **q**

コマンド	説明
set vlan	**管理ポートの** VLAN **タグの設定が指定できるようにします。** **注意** :set vlan **コマンドは、シリアル接続されたコンソールからしか使用できません。** **注意** : **ワンアーム接続のときは、**VLAN **サポートを使用できません。** **構文** : # **set vlan [none]** **例** : # **set vlan** Enter the management port VLAN QoS (0-7) [0]: **1** Enter the management port VLAN ID (1-4094) [1]: **2** **オプションパラメタ「**none**」を入力して、**VLAN **タグの設定を削除することができます。**
show vlan	**管理ポートの** VLAN **タグに現在設定されている値を表示します。** **例** : # **show vlan** The management port VLAN QoS is set to 1 The management port VLAN ID is set to 2

5.5.9 アラームコマンドおよび監視コマンド

コマンド	説明
set alarms	SSLAccelerator のアラームのすべてまたは一部を有効にします。 構文 : # **set alarms [all | esc | nls | none | ovl | rsc | utl]** 「all」は、SSLAccelerator の 5 つのアラームすべてを有効にします。 「esc」は、暗号状態の変更を通知するアラームを有効にします。 「nls」は、ネットワークのリンク状況を通知するアラームを有効にします。 「none」は、アラームをすべて無効にします。 「ovl」は、過負荷状態であることを通知するアラームを有効にします。 「rsc」は、SSL 接続が拒否されたことを通知するアラームを有効にします。 「utl」は、使用しきい値を超えたことを通知するアラームを有効にします。
show alarms	現在有効なアラームのリスト（esc, rsc, utl, ovl, nsl）を表示します。 注意 : アラームを 1 つも設定していない場合（set alarms に「none」を指定したとき）は、「Alarms set: 」のあとに「none」と表示されます。 例 : # **show alarms** Alarms set: none
delete alarms	アラームの履歴を削除します。
set monitoring	端末の監視機能の有効／無効を切り替えます。 構文 : # **set monitoring [enable | disable]**
show monitoring	端末の監視機能の現在の状態（有効／無効）を表示します。 例 : # **show monitoring** Monitoring for this terminal: enabled

コマンド	説明
list monitoring	**監視する端末の数を表示します。** **例** : # **list monitoring** 1.) /dev/ttyp0 --- Total of 1 device(s) with monitoring enabled. ---
set monitoring_fields	**指定したフィールドについて、監視レポートを記録するかしないかを設定します。** **構文** : # **set monitoring_fields [all | cps | cpu | dec | enc | failmode | link | mode | ovrld]** **「**all**」を指定すると、監視フィールドがすべて有効になります。** **「**cps**」は、**1 **秒あたりの** SSL **接続数です。** **「**cpu**」は、**CPU **の使用率です。** **「**dec**」は、復号化されたデータの処理量です。** **「**enc**」は、暗号化されたデータの処理量です。** **「**failmode**」は、フェイルセーフモードまたはフェイルスルーモードです。** **「**link**」は、ネットワークまたはサーバリンクのいずれかの状態です。** **「**mode**」は、インラインモードまたはバイパスモードです。** **「**ovrld spill**」は、**spill **機能が有効な場合は、**1 **秒あたりの** spill **の 個数です。**spill **機能が無効な場合は 、**1 **秒あたりのスロットルの個数です。**
show monitoring_fields	**監視レポートの記録機能が有効になっているフィールドを表示します。** **例** : # **show monitoring_fields** Monitoring report fields: mode failmode cpu cps ovrld
set monitoring_interval	**有効な監視フィールドについて、監視レポートの生成間隔を秒単位で設定します。** **構文** : # **set monitoring_interval <5-65000>**
show monitoring_interval	**有効な監視フィールドについて、監視レポートの生成間隔を表示します。** **例** : # **show monitoring_interval** Monitoring report interval [secs]: 15

コマンド	説明
set rsc_window	拒否された SSL 接続がないかどうかを検査する時間間隔（ウィンドウ）を設定します。拒否された SSL 接続が見つかった場合は、RSC アラームを発行します（指定範囲は 5 ～ 65000 秒。デフォルトは 15 です）。 構文 : # **set rsc_window <sec>** 「sec」は、検査間隔を示す秒数です。
show rsc_window	拒否された SSL 接続を検査する時間間隔の現在の設定値を表示します。 例 : # **show rsc_window** Check for refused SSL connections [secs]: **15**
set utl_window	使用しきい値（CPU 負荷、1 秒当たりの接続数、同時にオープンできる接続数など）を超えているかどうかを検査する時間間隔（ウィンドウ）を設定します。この値を超えているものが見つかった場合は、使用しきい値アラームが発行されます（指定範囲は 5 ～ 65000 秒。デフォルトは 15 です）。 注意 : 使用しきい値メトリックスについて集められたデータは、バースト性を持つ傾向があります。そのため、アラームが休みなく発行され続けることを防ぐため、スムージングアルゴリズムが使用されています。使用ウィンドウは、ユーザが指定するスライディング間隔と同じです。この間にデータが収集され、その平均値が計算されます。したがって、間隔を短くすると、まったく意味のないアラームが発行されることがあります。 注意 : このセクションの set utl_highwater コマンドおよび set utl_lowwater コマンドも参照してください。 構文 : # **set utl_window <secs>** 「secs」は、検査間隔を示す秒数です。
show utl_window	現在の使用しきい値アラームウィンドウを表示します。 例 : # **show utl_window** Utilization Window set [secs]: 10

コマンド	説明
set utl_highwater	使用しきい値アラームの最高点を設定します。最高点（%）は、CPU 使用率、1 秒当たりの接続数、または同時にオープンできる接続数の最大値を表します。この値を超えると、UTL アラームが発行されます（指定範囲は 2 ～ 100%、デフォルトは 90 です）。 注意 : このセクションの set utl_window コマンド および set utl_lowwater コマンドも参照してください。 構文 : # **set utl_highwater <%>** 「%」は、CPU 使用率、1 秒当たりの接続数、または同時にオープン可能な接続数に対する最高点を示します。この値を超えると、使用しきい値アラームが発行されます。
show utl_highwater	現在の使用しきい値アラームの最高点を表示します。 例 : # **show utl_highwater** Utilization High water mark [%]: 90
set utl_lowwater	使用しきい値アラームの最低点を設定します。最低点（%）は、CPU 使用率、1 秒当たりの接続数、または同時にオープンできる接続数の最小値を表します。この値を下回ると、UTL アラームが発行されます（指定範囲は 1 ～ 99%。デフォルトは 60 です）。 注意 : このセクションの set utl_window コマンドおよび set utl_highwater コマンド も参照してください。 構文 : **set utl_lowwater <%>** 「%」は、CPU 使用率、1 秒当たりの接続数、または同時にオープン可能な接続数に対する、最低点を示します。この値を下回ると、使用しきい値アラームが発行されます。
show utl_lowwater	現在の使用しきい値アラームの最低点を表示します。 例 : # **show utl_lowwater** Utilization Low water mark [%]: 60

コマンド	説明
set ovl_window	**過負荷のため** spill **や** throttle **が実行されていないかどうかを検査する時間間隔（ウィンドウ）を設定します。**spill **や** throttle **が実行されていると、過負荷アラームが発行されます（指定範囲は** 5 **〜** 65000 **秒。デフォルトは** 15 **です）。** **構文** : # **set ovl_window <secs>** **例** : # **set ovl_window 10**
show ovl_window	**現在の過負荷アラームウィンドウを表示します。** **例** : # **show ovl_window** Check for overload conditions [secs]: 10

5.5.10 設定コマンド

コマンド	説明
show config	**現在の設定内容を表示します。** **例** : # **show config** **（設定パラメタが表示されます）**
show config saved	**保存されている設定内容を表示します。** **注意** : **保存されている設定内容を呼び出すには、通常** 5 **～** 10 **秒かかります。** **例** : # **show config saved** Saved configuration ========== **（設定パラメタが表示されます）**

コマンド	説明
show config default	**デフォルトの設定を表示します。これらの値は、** factory_default **コマンドの実行時に使用される値です。** **例** : # **show config default** Default configuration ========== conlog 0xffffffcf ilog 0xffffffff trace 0xfffff3dd media auto logport tty01 cache 18 180 server_tmo 5 client_tmo 30 mgmt_if network map 0.0.0.0 443 80 default kpanic reboot monitoring_interval 15 monitoring_fields 0x1f alarm_mask 0x00000000 ovl_window 15 rsc_window 15 utl_window 15 utl_high 90 utl_low 60 idle 300 kstrength 512 con_speed 9600 con_bits 8 con_stop 1 con_parity n max_remote_sessions 5 trap_authen 1 crl_refresh 5 hdr_cert_def SSL_CLIENT_CERTIFICATE hdr_cip_def SSL_SOURCE_IP hdr_sid_def SSL_SSL_SESSION_ID hdr_cipher_def SSL_CIPHER_USED defcert_cname XX defcert_state MyState defcert_city MyCity defcert_orgname MyCompany defcert_orgunit MyCompany Division defcert_name www.MyCompany.xyz defcert_email support@MyCompany.xyz prompt # hwq_hiwat_spill 3 hwq_lowat_spill 1 #

コマンド	説明
config compare	保存されている設定と現在の設定の違いを表示します。設定とテストを簡単に行えるように、SSLAccelerator は、「現在の」（揮発性の）設定と「保存されている」（不揮発性の）設定をサポートしています。config compare コマンドは、現在の設定と保存されている設定の相違点を表示します。 例 : # **config compare** Only in /keys: 4
config reset	保存されている設定を現在の設定として復元します。 警告 : このコマンドを実行すると、システムが再起動されます。 注意 : 保存されている設定内容を呼び出すには、通常 5 ～ 10 秒かかります。 例 : # **config reset** Reverting to saved configuration, and unit will reboot automatically. Reset (y/n) [n]: **y** Reset to saved configuration System rebooting...
config default	現在の設定と保存されている設定をクリアして、出荷時の設定に戻します。 警告 : このコマンドを実行すると、システムが再起動されます。 注意 : 保存されている設定内容を呼び出すには、通常 5 ～ 10 秒かかります。 例 : # **config default** Reset to factory default configuration (y/n) ? [n]: **y** Reset to factory defaults System rebooting...
config save	現在の設定をフラッシュメモリ（不揮発性）に保存します。 注意 : 設定内容を保存するには、通常 5 ～ 10 秒かかります。 例 : # **config save** Saving configuration to flash... Configuration saved to flash

コマンド	説明
export config	すべての設定内容と鍵、電子証明書の情報を ASCII または Xmodem でエクスポートします。encrypt を指定して、エクスポートする鍵を暗号化する場合は、暗号化パスワードを入力するようプロンプトが表示されます。Garble を指定して、エクスポートするどの鍵も外部から読み取れないようにした場合は、鍵は xxxxxx... と表示されます。 警告 : エクスポートした設定ファイルは変更しないでください。 例 : # **export config** Garble or encrypt all keys: (garble, encrypt) [encrypt]: **<Enter>** Enter a pass phrase to encrypt all keys []: **sesame** Enter the pass phrase again to confirm []: **sesame** Export protocol: (xmodem, ascii) [ascii]: **<Enter>** Press any key to start, then again when done... （設定内容が表示れます）
import config	paste または Xmodem で設定をインポートします。指定した設定ファイルが暗号化されている場合は、import config コマンドを実行すると、暗号化パスワードを入力するようプロンプトが表示されます。 例 : # **import config** Import protocol (paste, xmodem) [paste]: **<Enter>** Type or paste in data, end with ... alone on line （ここに設定ファイルを貼り付けます） ...**<Enter>** Do you want to install this config? [y]: **y** Enter a pass phrase to decrypt all encrypted keys []: **sesame** /keys/001/key.pem is encrypted and decrypted with the pass phrase. /keys/default/key.pem is encrypted and decrypted with the pass phrase.

コマンド	説明
import upgrade	**ソフトウェアアップグレードをインポートします。ソフトウェアアップデートについての詳細は、「**A.2 **ソフトウェアのアップデート」（→** 189 **ページ）を参照してください。** **例** : # **import upgrade** import protocol (xmodem) [xmodem]: **<Enter>** Start xmodem upload now Use Ctl-X multiple times to cancel upload Verifying upgrade image... upgrade image valid version x.x, build xxx Continue with the upgrade? [n]:**y** **注意** : **アップデートが正常に終了すると、保存されているログがすべて削除され、システムが再起動されます。**
import patch	**一部修正ソフトウェアのアップグレードをインポートします。** **例** : # **import patch** import protocol (xmodem) [xmodem]: **<Enter>** Start xmodem upload now Press Ctrl-X multiple times to cancel upload Patch: Imported.
show patch	**現在パッチがインストールされているかどうかを確認します。** **例** : # **show patch** Patch is not installed.
delete patch	**現在インストールされているパッチを削除します。** **例** : # **delete patch** Patch: Deleted.
list system	CPU**、メモリ、暗号カードの情報を表示します。** **例** : # **list system** ========== | SYSTEM INFO | ========== * CPU : Intel Processor 852 MHz * Real MEM : 469762048 (448.00 MB) * Crypto : 1

コマンド	説明
factory_default	**出荷時の設定に戻します。** **例** : # **factory_default** Reset to default configuration [n]: **y** Reset to factory defaults System rebooting...done T944 V2.31 DXC. .. 868242+361188O/S running Generating 512 bit default key Generating default certificate Saving default key/cert to flash Restricted Rights Legend (**著作権情報とバージョン情報が表示されます**) Serial 0:a0:a5:11:4:9d password:

5.5.11 管理コマンド

コマンド	説明
password	SSLAccelerator **のパスワードを設定します（パスワードはプロンプトに影響しません）。** **構文** : # **password** Old password: **<old p/w>** Enter new admin password (5 characters min.): **<new p/w>** Retype new password: **<new p/w>**
ping	**指定した** IP **アドレスにパケットを送信して、応答時間（または応答なし）を表示します。** **注意** :0.0.0.0 **は使用できません。** **例** : # **ping 1.1.1.2** PING 1.1.2.5 (1.1.2.5): 56 data bytes 64 bytes from 1.1.2.5: icmp_seq=1 ttl=255 time=0.355 ms 64 bytes from 1.1.2.5: icmp_seq=2 ttl=255 time=0.178 ms 64 bytes from 1.1.2.5: icmp_seq=3 ttl=255 time=0.173 ms 64 bytes from 1.1.2.5: icmp_seq=4 ttl=255 time=0.174 ms --- 1.1.2.5 ping statistics --- 5 packets transmitted, 4 packets received, 20% packet loss round-trip min/avg/max = 0.173/0.219/0.355 ms
show info	**ソフトウェアのバージョン情報を表示します。** **例** : # **show info** ========== === SSL Accelerator === (c) Copyright 2001. All rights reserved. === === Version 2.5, Build xxx ==========

コマンド	説明
set date	**日付と時刻を設定します。** **警告** : **このコマンドを実行すると、**SSLAccelerator **の再起動が行われます。このコマンドを実行する前に** config save **コマンドを必ず実行してください。** **注意** : **このコマンドを** NTP **とともに使用する場合は、**SSLAccelerator **の時刻を 手動で** NTP **サーバの時刻にできるだけ近づけて設定することをお勧めします。** **例** : # **set date** Year [2001]: **<Enter>** Month [6]: **<Enter>** Day [7]: **<Enter>** Hour (24 hour clock) [19]: **<Enter>** Minute [55]: **<Enter>** The system must reboot immediately for new time to be set. Reboot? [y]: **y**
show date	**現在の日付と時刻を表示します。** **例** : # **show date** 2001 06/07 19:57:07
list timezone	SSLAccelerator **を設定するときに利用できるタイムゾーンオプションを表示します。デフォルトでは、どのタイムゾーンも設定されていません。** **例** : # **list timezone** Time zones of following continents are supported. Use command "list timezone <continent>" for detail. Africa/ Asia/ Etc/ US/ America/ Canada/ Europe/
set timezone	**現地時刻が表示されるようタイムゾーンを設定します。このコマンドで使用するタイムゾーン識別子は大文字と小文字が区別されます。** **注意** :set timezone **コマンドを実行したあとは、**set date **コマンドを実行して日時の再設定を行ってください。** **構文** : **set timezone [none]|<tz>** **例** : # **set timezone Asia/Tokyo**

コマンド	説明
show timezone	**現在設定されているタイムゾーンを表示します。** **例** : # **show timezone** Timezone is set to "Asia/Tokyo".
set egress_mac	**送信トラフィックと受信トラフィックのパスが異なる場合の** SSLAccelerator **の設定に使用します（「**3.5 **送信用ルータと受信用ルータが異なる場合」（→** 38 **ページ）を参照）。** **例** : # **set egress_mac aa:bb:cc:dd:ee:ff** Egress MAC set to aa:bb:cc:dd:ee:ff
show egress_mac	**送信トラフィックと受信トラフィックのパスが異なる場合の** SSLAccelerator **の設定を表示します。** **例** : # **show egress_mac** Egress MAC is aa:bb:cc:dd:ee:ff
set ether	**転送速度（**10baseT/100baseTX**）および、転送モード（**half duplex/full duplex**）を設定します。** **例** : # **set ether** 1 - auto 2 - 10baseT, half duplex 3 - 10baseT, full duplex 4 - 100baseTX, half duplex 5 - 100baseTX, full duplex Select media type [1]: **<Enter>** Media set to auto
show ether	**転送速度（**10baseT/100baseTX**）および、転送モード（**half duplex/full duplex**）を表示します。** **例** : # **show ether** Ethernet media set to auto
set idleto	**コンソールのアイドル状態の制限時間を設定します。「**min**」分間キーボード操作を行わない場合は、自動的にログオフされます。** **構文** : # **set idleto <min>** **「**min**」は制限時間の値（分）です（**0 ～ 525600**）。**0 **を指定した場合は、この自動ログオフがされないようになります。**

コマンド	説明
show idleto	コンソールのタイムアウト値を表示します。 例 : # **show idleto** Idle timeout is 5 minutes
set ip	Telnet セッションおよび SSH セッションを確立するために、SSLAccelerator のネットワークインターフェースに IP アドレスとネットマスクを割り当てます。現在設定されている IP アドレスを無効にするには、set ip のあとに「none」を入力します。 警告 :IP アドレスを割り当てると、セキュリティの問題を伴います。 注意 : • 0.0.0.0 と 255.255.255.255 は使用できません。 • set ip コマンドは、シリアル接続されたコンソール経由でのみ使用できます。 例 : # **set ip** Enter IP Address (' none 'to delete) [none] 10.1.2.124 **: <Enter>** Enter Netmask [255.255.255.0]: **<Enter>**
show ip	SSLAccelerator の IP アドレスを表示します。 例 : # **show ip** System IP Address : 10.1.2.124 System Netmask : 255.255.255.0
set mgmt_if	SSLAccelerator には、ネットワークインターフェースとサーバインターフェースがあります。このコマンドを使用すると、リモート管理でどちらのインターフェースを使用するかを指定できます。デフォルトでは、SSLAccelerator に割り当てた IP アドレスがネットワークインターフェースに適用されます。このコマンドを使用すると、リモート管理用インターフェースにサーバインターフェースを指定できます。デフォルトでは、「network」（ネットワークインターフェース）です。 注意 : このコマンドを使用すると、実行中のリモート管理セッションはすべて終了します。 構文 : # **set mgmt_if [network | server]**

コマンド	説明
show mgmt_if	**現在リモートマネジメントインターフェースとして指定されているインターフェースを表示します。** **例** : # **show mgmt_if** The remote management interface is set to: network
set more	**コンソールディスプレイの表示ページの長さを設定します。デフォルトではスクロールの自動停止機能は無効です。** **構文** : # **set more <n>** **「**n**」は希望の行数です。有効な入力値は、**0 **または** 23 **以上の値です。**0 **に設定すると、コンソール表示スクロールの自動停止機能は無効になります。**
show more	**現在設定されているコンソールディスプレイの表示ページの長さを表示します。** **例** : # **show more** Paging set [lines per page]: 23
nic	**転送速度（**10baseT/100baseTX**）および、転送モード（**half duplex/full duplex**）を設定します。** **例** : # **nic** 1 - auto 2 - 10baseT, half duplex 3 - 10baseT, full duplex 4 - 100baseTX, half duplex 5 - 100baseTX, full duplex Select media type [1]: **<Enter>** Media set tu auto
set ntp	**ネットワークタイムプロトコル（**NTP**）の有効／無効を切り替えます** NTP **を利用するには、**NTP **サーバを指定する必要があります。**set ntp **コマンド の実行時に** NTP **サーバが指定されていないと、**NTP **サーバを設定するように要求されます。**NTP **サーバがすでに設定されている場合は、**NTP **プロセスがただちに開始します。デフォルトは「**disable**」です。** **例** : # **set ntp enable** An optional default route may be entered before starting the NTP service. Enter a default route (’ none ’to delete) [none]: **<Enter>** NTP Service started.

コマンド	説明
show ntp	NTP の現在の状態（有効／無効）を表示します。 例 : # **show ntp** NTP : Disabled
show ntp_status	NTP プロセスの現在の状態を表示します。 注意 :show ntp_status コマンドは、NTP を有効にしてから約 1 分後に利用できます。 例 : # **show ntp_status** remote local st poll reach delay offset disp ======= ======== == === ===== ===== ======= ===== =1.1.1.2 10.1.8.34 2 64 77 0.0026 -0.1442 0.004 *1.1.2.3 10.1.8.34 2 64 77 0.0024 -0.1396 0.004 =1.1.3.4 10.1.8.34 2 64 77 0.0024 -0.1309 0.005
set ntp_servers	SSLAccelerator のクロックの同期化に使用する NTP サーバの IP アドレスを指定します。最大 3 台のサーバを指定できます。 注意 :0.0.0.0 と 255.255.255.255 は使用できません。 例 : # **set ntp_servers** Enter IP address of NTP server (q to quit) [q]: **10.12.30.1** Enter IP address of NTP server (q to quit) [q]: **10.12.30.2** Enter IP address of NTP server (q to quit) [q]: **q**
show ntp_servers	現在指定されている NTP サーバの IP アドレスを表示します。 例 : # **show ntp_servers** NTP servers: 10.12.30.1 10.12.30.2
set prompt	プロンプトの形式をデフォルトの 「#」から指定した文字列に変更します。 例 : # **set prompt** Prompt [#]: **Acclerator>** Acclerator>

コマンド	説明
set serial	Console ポートの伝送速度、データビット、ストップビット、パリティビットの設定を行います。Aux consol ポートの伝送速度、データビット、ストップビット、パリティビットの値は、115200、8、1、N の固定値になっています。Console ポートの設定を行うと、パスワードプロンプトが表示されます。 例 : # **set serial** Baud rate (9600/115200) [9600]: **<Enter>** Data bits (7/8) [8]: **<Enter>** Stop bits (1/2) [1]: **<Enter>** Parity (n/e/o) [n]: **<Enter>** Set serial parameters (y/n) ? [y]: **<Enter>**
show serial	Console ポートの通信パラメタを表示します。 例 : # **show serial** Speed: 9600 Bits: 8 Stop Bits: 1 Parity: n
exit	CLI からログアウトします。再起動したあとも維持するために保存する必要がある設定変更について通知があります。 例 : # **exi** Exiting CLI... . . . password:
quit	CLI からログアウトします（exit と同じ）。

5.5.12 ロギングコマンド

コマンド	説明
export log	**保存されているログファイルをエクスポートします。ログファイル名を表示するには、**list logs **コマンドを使用します。** **注意** : **このログファイルを直接読むことはできません。** **構文** : # **export log <logID>** **「**logID**」は、エクスポートされるログの** ID **です。** **例** : # **export log 20010814_110951** Export protocol: (xmodem) [xmodem]: **<Enter>** Use Ctrl-X multiple times to kill transmission Beginning export...
delete log	**保存されているログファイルを** /flash/logs **ディレクトリから削除します。** **構文** : # **delete log <logID>	[all]** **「**logID**」は、削除されるログの** ID **です。** **「**all**」を指定すると、すべてのログが削除されます。**
list logs	**すべてのログファイルを表示します。** **例** : # **list logs** 20010605_070027 20010605_070324
show logs	**すべてのログファイルを表示します（**list logs **と同じ）。**

6 リモート管理

この章では、リモート管理について説明しています。

Contents

6.1 概要

SSLAccelerator は、リモート管理できます。リモート管理機能は、次のプロトコルに対応しています。

- Telnet
- Secure Shell（SSH）
- SNMP

リモート管理機能を有効にすると、遠隔地のマシンで実行中の Telnet セッションまたは SSH セッションから、デバイスのコマンドラインインターフェース（CLI）にアクセスすることができます。リモートセッションは、Telnet セッションおよび SSH セッションを含めて、最大 5 つ設定することができます（デフォルトは 5）。デバイスのリモート管理機能を使用するには、ローカルのシリアルコンソールでリモート管理を有効にして、その設定を行う必要があります。リモート管理機能を使用するには、デバイスのネットワークインターフェースに IP アドレスを割り振る必要があります。SNMP のリモート管理機能については、MIB-II のシステムグループ管理までサポートされています。

リモート管理機能を有効にして、その設定を行うには、ローカルのシリアルコンソールが必要です。

6.1.1 リモート管理の制約

ローカルコンソールで使用可能な CLI 機能のいくつかは、リモートセッションでは使用できないことに注意してください。以下にそれらを示します。

- SSLAccelerator のネットワークインターフェースに対する IP アドレスの割り当て
- Telnet 、SSH 、または SNMP の有効／無効の切り替え
- Telnet 、SSH 、または SNMP のポートの変更
- Telnet セッション、または SSH セッションの数の変更
- ルートの設定
- リモート管理インターフェースの変更
- VLAN の設定値は、リモート変更が不可能

リモート管理用の CLI コマンドを使用すると、デバイスの設定ファイルに影響が及ぶことがあります。デバイスを再起動してもリモート管理の設定内容が失われないようにするためには、CLI コマンドの config save **コマンド** を使って、リモート管理の設定の変更を保存する必要があります。これにより、設定は起動時に復元されます。

6.1.2 リモート管理用 CLI コマンド

リモート管理機能は、ローカルのシリアルコンソールから一連の CLI コマンドを使用して、有効／無効を切り替えたり、設定を行ったりすることができます。正確なシーケンスは、有効にしたいリモートセッションのタイプや設定によりさまざまです。リモート管理コマンドの詳細については、「5.5 コマンドリファレンス」（→ 85 ページ）を参照してください。

共通 :

- set ip <ip> <netmask> は、SSLAccelerator のネットワークインターフェースに IP アドレスおよびネットマスクを割り当てます。
- set max_remote_sessions <0-5> は、同時に実行できる Telnet セッションおよび SSH セッションの最大数を設定します。

Telnet **用** :

- set telnet [enable | disable] は、Telnet セッションの有効／無効を切り替えます。
- show telnet は、Telnet の現在の状況が有効、無効のどちらであるのかを表示します。
- set telnet_port <port> は、Telnet のポートを設定します（デフォルトは 23 です）。
- show telnet_port は、Telnet の現在のポートを表示します。

SSH **用** :

- set ssh [enable | disable] は、SSH セッションの有効／無効を切り替えます。
- show ssh は、SSH の現在の状況が有効、無効のどちらであるのかを表示します。
- set ssh_port <port> は、SSH のポートを設定します（デフォルトは 22 です）。
- show ssh_port は、SSH の現在のポートを表示します。

SNMP **用** :

- set snmp [enable | disable] は、SNMP 管理機能の有効／無効を切り替えます。
- show snmp は、SNMP の現在の状況が有効、無効のどちらであるのかを表示します。
- set snmp_info は、以下に示す SNMP の情報およびパラメタを設定します。
    - SNMP port（デフォルトは 161）
    - SNMP trap port（デフォルトは 162）
    - Contact person
    - System name
    - System location
- show snmp_info は、SNMP の現在の情報およびパラメタを表示します。

- set snmp_community は、コミュニティ文字列を設定します。
- list snmp_community は、コミュニティ文字列を表示します。
- delete snmp_community は、コミュニティ文字列を削除します。
- set trap_community は、トラップコミュニティ文字列を設定します。
- list trap_community は、トラップコミュニティ文字列を表示します。
- delete trap_community は、トラップコミュニティ文字列を削除します。

⚠注意

Telnet や SSH 、SNMP で使用する IP/ ポート番号の組み合わせが互いに同じものにならないようにし、また、マップされた SSL 処理サービスに使用されるIP/ポート番号と同じにならないように注意してください。特にデフォルトのマッピングが使用されている場合は、telnet や SSH、SNMP にポート 443 を使用できないことに注意してください。

6.2 リモート Telnet セッション

このセクションでは、リモート Telnet セッションを介して、SSLAccelerator の CLI にアクセスする手順を説明します。

6.2.1 シリアルコンソールからの初期設定

以下の手順で、SSLAccelerator のネットワークインターフェースに IP アドレスおよびネットマスクを割り当てます。

1 **IP アドレスを設定します。**

```
# set ip
Enter IP [10.1.2.56]: 10.1.1.254
Enter Netmask [255.255.255.0]: <Enter>
```

2 **必要に応じて、IP アドレスおよびネットマスクを確認します。**

```
# show ip
System IP Address : 10.1.1.254
System Netmask : 255.255.255.0
```

3 **リモート Telnet セッションを有効にします。**

```
# set telnet enable
```

4 **ネットワークルートを設定します。**

```
# set route
Enter Default Route ( ’ none ’to delete) [10.1.1.1] : 10.1.1.253
```

5 **必要に応じて、ルート設定を確認します。**

```
# show route
Default Route : 10.1.1.253
```

削除するには以下のコマンドを使用します。

```
# set route none
```

以上で SSLAccelerator のリモート Telnet 管理機能が設定され、リモート Telnet セッションから CLI にアクセスすることができます。

⚠注意 **デバイスを再起動しても、リモート管理の設定内容が失われないようにするには、**config save **コマンドを実行します。**

6.2.2 Telnet の使用

リモート Telnet を SSLAccelerator 上で有効にしたあと、以下の手順で SSLAccelerator の CLI にアクセスします。

```
Client-prompt> telnet 10.1.1.1
Trying 10.1.1.1...
Connected to 10.1.1.1.
Escape character is '^]'.
.
.
.
Serial 0:a0:a5:11:4:2e
password: <password>
```

パスワードを入力すると、Telnet セッションは、SSLAccelerator の CLI を表示します。これ以降、ローカルのシリアルコンソールから行うのと同様に、デバイスを管理することができます（ただし、本章初めの「6.1.1 リモート管理の制約」（→ 145 ページ）に示したコマンドは使用できません）。

⚠注意 **他のリモートセッションがすでに実行されていて、新しいセッションを確立すると、セッション数が** setmax_remote_sessions **コマンドで設定した値を超えてしまう場合は、「**Max Remote Sesion Limit of (5)exceeded!**」というメッセージが表示されます。この場合は、ローカルコンソールからセッションを閉じて、新しいセッションを確立できるようにしてください。**

6.2.3 Telnet ポートの変更

Telnet ポートを設定または表示するには、CLI コマンドの set telnet_port <port> コマンドまたは show telnet_port コマンドを使用します。

これらのコマンドを実行できるのは、ローカルのシリアルコンソールからだけです。デフォルトでは、Telnet ポート番号は 23 です。

Telnet ポートを設定するには、次のようにします。

```
# set telnet_port 230
```

Telnet ポートを表示するには、次のようにします。

```
# show telnet_port
        Telnet Port Number: 230
```

6.2.4 Telnet の無効

Telnet は、SSLAccelerator のローカルのシリアルコンソールから無効にすることができます。Telnet を無効にするには、次のようにします。

```
# set telnet disable
```

Telnet が無効になったことを確認するには、次のようにします。

```
# show telnet
        Telnet: disable
```

デバイスを再起動しても、Telnet セッションを無効のままにしたい場合は、config save コマンドを実行します。

6.3 リモート SSH セッション

このセクションでは、リモート SSH（Secure Shell）セッションを介して、SSLAccelerator の CLI にアクセスする手順を説明します。サポートしている暗号の詳細については「A.4 対応している暗号方式」（→ 194 ページ）を参照してください。

6.3.1 シリアルコンソールからの初期設定

以下の手順で、SSLAccelerator のネットワークインターフェースに IP アドレスを割り当てます。

1 **IP アドレスを設定します。**

```
# set ip
Enter IP [10.1.2.56]: 10.1.1.254
Enter Netmask [255.255.255.0]: <Enter>
```

2 **必要に応じて、IP アドレスおよびネットマスクを確認します。**

```
# show ip
System IP Address: 10.1.1.254
System Netmask: 255.255.255.0
```

3 **リモート SSH セッションを有効にします。**

```
# set ssh enable
```

4 **ネットワークルートを設定します。**

```
# set route
Enter Default Route ( ’ none ’to delete) [10.1.1.1] : 10.1.1.253
```

5 **必要に応じて、ルート設定を確認します。**

```
# show route
Default Route : 10.1.1.253
```

削除するには以下のコマンドを使用します。

```
#  set route none
```

以上で SSLAccelerator のリモート SSH 管理機能が設定され、リモート SSH セッションから、CLI にアクセスすることができます。

⚠注意 **デバイスを再起動しても、リモート管理の設定内容が失われないようにするには、**config save **コマンドを実行します。**

6.3.2 SSH の使用

リモート SSH を SSLAccelerator 上で有効にしたら、以下の手順で SSLAccelerator の CLI にアクセスします。

```
Unix-prompt> ssh - l admin 10.1.1.1
.
.
.
Serial 0:a0:a5:11:4:2e

password: <password>
```

パスワードを入力すると、SSH セッションは、SSLAccelerator の CLI を表示します。これ以降、ローカルのシリアルコンソールから行うのと同様に、デバイスを管理することができます（ただし、本章初めの「6.1.1 リモート管理の制約」（→ 145 ページ）に示したコマンドは使用できません）。

⚠注意

- SSH **ユーザ名は、「**admin**」です。**
- **他のリモートセッションがすでに実行されていて、新しいセッションを確立すると、セッション数が** setmax_remote_sessions **コマンドで設定した値を超えてしまう場合は、「**Max Remote Sesion Limit of (5) exceeded!**」というメッセージが表示されます。この場合は、ローカルコンソールからセッションを閉じて、新しいセッションを確立できるようにしてください。**

6.3.3 SSH ポートの変更

SSH ポートを設定または表示するには、CLI コマンドの set ssh_port <port> コマンドまたは show ssh_port コマンドを使用します。

これらのコマンドを実行できるのは、ローカルのシリアルコンソールからだけです。デフォルトでは、SSH ポート番号は 22 です。

SSH ポートを設定するには、次のようにします。

```
# set ssh_port 220
```

SSH ポートを表示するには、次のようにします。

```
# show ssh_port
        SSH Port Number : 220
```

6.3.4 SSH の無効

SSLAccelerator のローカルのシリアルコンソールから、SSH を無効にすることができます。SSH を無効にするには、次のようにします。

1 SSH を無効にします。

```
# set ssh disable
```

2 SSH が無効になったことを確認するには、次のようにします。

```
# show ssh
SSH: disable
```

デバイスを再起動しても、SSH セッションを無効のままにしたい場合は、config save コマンドを実行します。

6.4 SNMP

SSLAccelerator は、業界標準に完全に準拠した組み込み式の SNMP エージェントです。SNMPv1 要求と SNMPv2 要求をサポートしています。プライベートエンタープライズ MIB は、標準 MIB-II の他にも、以下のような機能を提供しています。

- SSLAccelerator のハードウェアおよびネットワークリンク障害の監視
- アラーム機能および監視機能の有効／無効を示すフラグの監視
- CPU 使用率、接続総数、1 秒当たりの接続数などで示される SSLAccelerator の負荷の監視
- SSL の暗号化／復号化機能の状況およびパフォーマンスの監視
- 過負荷、1 秒当たりの spill、1 秒当たりの throttle の監視

SNMP を使用する場合は、コミュニティ文字列を作成する必要があります。

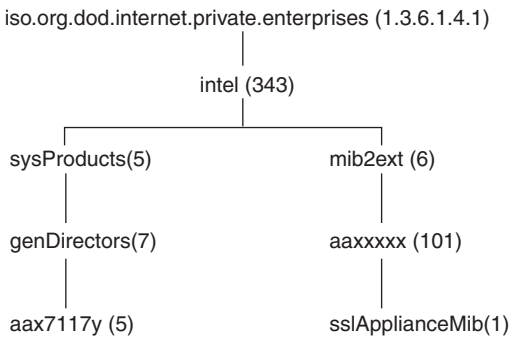
SNMP 管理機能として SNMP マネージャからの SET には対応していません。SNMP 情報は参照のみでリモートから変更をかけることはできません。

6.4.1 業界標準への準拠

SSLAccelerator の SNMP エージェントは、SNMPv1 要求および SNMPv2c 要求という、2 つの規格に対応しています。プライベートエンタープライズ MIB ファイルは、RFC1902 に規定されている SMIv2 に準拠しています。SSLAccelerator では、どの MIB オブジェクトに対しても、SET 操作を行うことはできません。ただし、CLI コマンドを使用すれば、MIB 変数値は反映されます。

6.4.2 Intel MIB ツリー

以下の図では、MIB ツリーの最上位を示しています。



エンタープライズ MIB および MIB オブジェクトはすべて、ツリーの mib2ext ブランチの下で定義されます。製品を識別する sysObjectId はすべて、ツリーの genDirectors ブランチの下で定義されます。

■ サポートされる MIB

管理情報ベース II（MIB-II）
以下のエンタープライズ MIB:

gen-header.my
ssl-appliance-mib.my

■ MIB ファイルの入手方法

本製品に同梱されている CD-ROM に、SSLAccelerator が使用する MIB ファイルのコピーが収録されています。
SNMP SET を介しての書き込みアクセスは、どの MIB 変数や SNMP グループに対しても行うことはできません。SNMP SET をグループに対して実行すると、エラーが戻されます。
標準 SNMP トラップとして、coldStart 、warmStart 、authenticationFailure 、linkUp 、および linkDown がサポートされています。

gen-header.my

gen-header.my には、システムオブジェクト ID が入っています。すべてのシステムオブジェクト ID は、ツリーの genDirectors ブランチの配下に定義されています。

6.4.3 エンタープライズプライベート MIB の一覧

以下に、SSLAccelerator プライベート MIB の一覧を示します。

mode
inline(1): Device is configured to accelerate SSL traffic
bypass(2): Device is configured to pass through all SSL traffic

failMode
safe(1): Fail-through switch is up, causing Ethernet segments to remain open when device fails. It stops traffic from reaching the server
through(2): Fail-through switch is down, causing Ethernet segments to remain closed when device fails. It allows traffic to reach the server

spillMode
throttle(1): Device will throttle SSL connections when utilization reaches 100%
spill(2): Device will spill SSL connections when utilization reaches 100%

sslSessionCache
enabled(1): SSL session caching is turned on
disabled(2): SSL session caching is turned off

restarts
Number of times the system has restarted

appLastRestart
The value of sysUpTime at the time the last restart of the application process happened

encryptionAlarm
enabled(1): Encryption status change alarm is turned on
disabled(2): Encryption status change alarm is turned off

sslConnectionAlarm
enabled(1): SSL connection alarm is turned on
disabled(2): SSL connection alarm is turned off

thresholdAlarm
enabled(1): Threshold alarm is turned on
disabled(2): Threshold alarm is turned off

overloadAlarm
enabled(1): Overload alarm is turned on
disabled(2): overload alarm is turned off

linkStatusAlarm
enabled(1): Network link status alarm is turned on
disabled(2): Network link status alarm is turned off

encryptProcessingState
on(1): SSL processing on
off(2):SSL processing halted

encryptProcessingStateReason
normal(1): Normal
hardware(2): Change caused by hardware fault
consoleBypass(3): Bypass mode enabled at console
consoleInline(4): Inline mode enabled at console
frontPanelBypass(5): Bypass mode enabled at front panel
frontPanelInline(6): Inline mode enabled at front panel

serverInterfaceState
State of the server-side interface

networkInterfaceState
State of the network-side interface

utilWindow
Sliding window (in seconds) to calculate average connections, CPU utilization, and active connnection rates

cpuUtil
CPU utilization percentage (0-100)

cpuUtilNetwork
CPU utilization percentage processing network traffic (0-100)

cpuUtilProxy
CPU proxy utilization percentage (0-100)

cpuUtilHiWater
CPU utilization high water mark (2-100)

cpuUtilLoWater
CPU utilization low water msrk (1-99)

cpuUtilState
When CPU utilization exceeds the high water mark, CPU utilization state is in alert and is not returned to normal until the low water threshold is crossed

sslCps
SSL connections per second

sslCpsMaximum
Maximum SSL connection rate in connections per second since (re)start

sslCpsHiWater
SSL connections per second high water mark

sslCpsLoWater
: SSL connections per second low water mark

sslCpsState
: When SSL connections per second exceeds the high water mark, sslCpsState is in alert and is not returned to normal until the low water threshold is crossed

sslConnCnt
: Current number of concurrent open SSL connections

sslConnCntMaximum
: Maximum number of concurrent open SSL connections since (re)start

sslConnTotal
: Total number of SSL connections processed

sslConnCntHiWater
: Concurrent open SSL connection count high water mark

sslConnCntLoWater
: Concurrent open SSL connection count low water mark

sslConnCntState
: When concurrent open SSL connection count exceeds the high water mark, sslConnCntState is in alert and is not returned to normal until the low water threshold is crossed

encryptedBps
: Encryption rate in bytes per second

encryptedBpsMaximum
: Maximum encryption rate in bytes per second since (re)start

encryptedBytesTotalMb
: Total number of megabytes of data encrypted

decryptedBps
: Decryption rate in bytes per second

decryptedBpsMaximum
: Maximum decryption rate in bytes per second since (re)start

decryptedBytesTotalMb
: Total number of megabytes of data decrypted

sslOverloadInterval
: The periodic interval (in seconds) used when counting the number of spilled or throttled SSL connections. If any SSLconnections were spilled or throttled in the last sslOverloadInterval, a trap is generated. If sslOverloadInterval is 0, no trap is generated

throttlesPerSec
: Number of throttles per second

throttlesPerSecMaximum
: Maximum number of throttles per second since (re)start

throttlesTotal
: Total number of throttles since (re)start

throttles
: Total number of throttles in the last sslOverloadInterval

spillsPerSec
: Number of spills per second

spillsPerSecMaximum
: Maximum number of spills per second since (re)start

spillsTotal
: Total number of spills since (re)start

spills
: Number of spills in the last sslOverloadInterval

refusedSslInterval
: The periodic interval (in seconds) used when counting the number of refused SSL connections.
If any SSL connections were refused in this time interval, a trap is generated.

cipherSuiteMismatch
: Number of refused SSL connections in the last refusedSslInterval which are due to inability of the client and server to agree upon a cipher suite

clientCertAuthFail
: Number of refused SSL connections in the last refusedSslInterval which are due to authentication failure of the client certificate

6.4.4 トラップの一覧

以下に、SSLAccelerator により生成されるトラップを一覧にして示します。各トラップの詳細については、前述した MIB の説明、または MIB ファイル内のドキュメントを参照してください。トラップは、SNMP が生成します。

■ 標準 SNMP トラップ

coldStart
warmStart
authenticationFailure
linkUp
linkDown

■ ssl-appliance-mib.my のプライベートトラップ

encryptionStopped
Alert issued whenever the device stops processing SSL traffic

encryptionResumed
Resumes processing traffic after having been stopped

serverInterfaceStateChanged
The server-side interface changed its state

networkInterfaceStateChanged
The network-side interface changed its state

cpuUtilAlert
The device has exceeded the CPU utilization high water threshold

cpuUtilNormal
CPU utilization back to normal levels

sslCpsAlert
The device has exceeded the SSL connections per second high water threshold

sslCpsNormal
The SSL connections per second processed by the device is back to normal levels

sslConnCntAlert
The device has exceeded the open SSL connection count high water threshold

sslConnCntNormal
The open SSL connection count of the device is back to normal levels

sslConnectionRefusedMismatch
: SSL connections were refused in the past sslRefusedInterval due to cipher suite negotiation failure

sslConnectionRefusedAuthFail
: SSL connections were refused in the past sslRefusedInterval due to authentication failure of the client certificate

sslOverloadSpills
: SSL connections were spilled in the past sslOverloadInterval

sslOverloadThrottles
: SSL connections were throttled in the past sslOverloadInterval

appRestartAlert
: SSL processing application has restarted

6.4.5 SNMP を有効にする

SNMP の有効／無効を切り替えるには、CLI コマンドの set snmp [enable|disable] コマンド を使用します。動作状況を調べるには、show snmp コマンドを使用します。

例 :

```
# set snmp enable
# show snmp
SNMP: enabled
# set snmp disable
# show snmp
SNMP: disabled
```

■ SNMP 情報の指定

設定可能な SNMP パラメタは、以下に示すように、set snmp_info コマンドを使用して、一度に設定することができます。

```
# set snmp_info
SNMP Port [161]: 161
SNMP Trap Port [162]: 162
Contact Person []: support
System Location []: MyCity
System Name []: SSL Accelerator
```

SNMP パラメタの値は、以下のように、show snmp_info コマンドを使用して表示することができます。

```
# show snmp_info
SNMP Port Number : 161
SNMP Trap Port Number: 162
SNMP System Contact : “ support ”
SNMP System Name : “ SSL Accelerator ”
SNMP System Location : “ MyCity ”
System IP Address : 10.1.1.254
System Netmask : 255.255.255.0
Default Route : 10.1.1.253
```

SNMP 情報の各項目は、以下のコマンドを使用して、個別に設定することもできます。

- set snmp_port ：SNMP ポートの設定
- set trap_port ：SNMP トラップポートの設定
- set sys_contact ：連絡先の設定
- set sys_name ：システム名の設定
- set sys_location：システム位置の設定

前記のコマンドで設定した値は、それぞれ以下のコマンドを使用して表示することができます。

- show snmp_port：SNMP ポートの表示
- show trap_port：SNMP トラップポートの表示
- show sys_contact ：連絡先の表示
- show sys_name：システム名の表示
- show sys_location：システム位置の表示

■ コミュニティ文字列

IP アドレスとコミュニティ文字列の組み合わせによって、SNMP 管理ステーションを定義します。定義された IP アドレスで、さらにコミュニティ文字列に一致している SNMP 管理ステーションだけが、SSLAccelerator の SNMP 情報にアクセスできます。管理ステーションは 10 台まで定義できます。

SNMP コミュニティ文字列を設定、表示、削除するには、CLI コマンドの set snmp_community コマンド 、list snmp_community コマンド、delete snmp_community コマンドを使用します。

```
# set snmp_community

SNMP Community String(s) Setting.

Enter a SNMP Community IP (q to quit): 1.1.1.1
Enter a SNMP Community String (q to quit): public
Enter a SNMP Community IP (q to quit): 1.1.1.2
Enter a SNMP Community String (q to quit): private
Enter a SNMP Community IP (q to quit): q

# list snmp_community

SNMP Community String(s) information.

<2> Current SNMP Community String(s):

1.) IP:    1.1.1.2 => String:    private => Rights: read
2.) IP:    1.1.1.1 => String:     public => Rights: read
```

delete snmp_community

SNMP Community String(s) Deletion.

<2> Current Available SNMP Community String(s):

1.) IP: 1.1.1.2 => String: private => Rights: read
2.) IP: 1.1.1.1 => String: public => Rights: read

Enter number (1) to delete (q to quit) [q]: **2**

SNMP Community String(s) Deletion.

<1> Current Available SNMP Community String(s):

1.) IP: 1.1.1.2 => String: private => Rights: read

Enter number (1) to delete (q to quit) [q]: **q**

⚠注意 **デフォルトでは、SNMP コミュニティが設定されていません。SNMP を使用する場合は SNMP Community String の設定を必ず行ってください。**

■ トラップコミュニティ文字列

IP アドレスとコミュニティ文字列の組み合わせによって、SSLAccelerator のトラップメッセージを受信できる SNMP 管理ステーションを定義します。管理ステーションは 10 台まで定義できます。

トラップコミュニティ文字列を設定、表示、削除するには、CLI コマンドの set trap_community コマンド、list trap_community コマンド、delete trap_community コマンドを使用します。

set trap_community

SNMP Trap Community String(s) Setting.

Enter a SNMP Trap Community IP (q to quit): **1.1.1.1**
Enter a SNMP Trap Community String (q to quit): **private**
Enter a SNMP Trap Community IP (q to quit): **2.2.2.2**
Enter a SNMP Trap Community String (q to quit): **public**
Enter a SNMP Trap Community IP (q to quit): **q**

list trap_community

SNMP Trap Community String(s) information.

<2> Current SNMP Trap Community String(s):

1.) IP: 1.1.1.1 => String: private
2.) IP: 2.2.2.2 => String: public

delete trap_community

SNMP Trap Community String(s) Deletion.

<2> Current Available SNMP Trap Community String(s):

1.) IP: 1.1.1.1 => String: private
2.) IP: 2.2.2.2 => String: public

Enter number (1 to 2) to delete (q to quit) [q]: **2**

SNMP Trap Community String(s) Deletion.

<1> Current Available SNMP Trap Community String(s):

1.) IP: 1.1.1.1 => String: private

Enter number (1) to delete (q to quit) [q]: **q**

プライベートトラップを送信させるためには、SSLAccelerator**のアラームを設定する必要があります。アラームの設定については、「第 7 章 アラーム機能および監視機能」（→ 167 ページ）を参照してください。**

7 アラーム機能および監視機能

この章では、アラーム機能および監視機能について説明します。

Contents

7.1 概要

SSLAccelerator は、事前に指定しておいたイベントが起きたときに、アラームをコンソールへ送ることができます。また、定期的に状況監視レポートを作成することもできます。アラームおよび監視レポートは、1 行のテキスト形式です。アラームは「A」で始まり、監視レポートは「M」で始まります。どちらにもタイムスタンプが付いています。アラームおよび監視レポートは、ローカルの管理コンソールまたはリモート管理セッション（Telnet または Secure Shell のみ）に対して作成することができます。

アラームを設定すると、以下の状況を即座にユーザへ通知することができます。

- 暗号状態の変更
- SSL 接続の拒否
- 使用（しきい値）アラーム
- 過負荷アラーム
- ネットワークのリンク状況

デフォルトでは、すべてのアラームが無効になっています。有効にするときは、任意の組み合わせが可能です。

アラームの形式は、次のようになっています。

```
A:yyyymmddhhmmss:ALARM_CODE:MODIFIER:EXTENDED_DATA:
/*message*/
```

- A：アラームであることを示します（モニタレポートには「M」が付きます）。
- yyyymmddhhmmss：アラームの発生した日時です。
- ALARM_CODE：アラームのタイプ [ESC|RSC|UTL|OVL|NLS] です。
- MODIFIER：アラームの発生源です。アラームをトリガしたイベントを示すコードです。
- EXTENDED_DATA：関連する情報です。
- /*message*/：どのようなアラームなのかを示す簡単な説明です。

暗号状態の変更アラーム（ESC）は、EXTENDED_DATA を表示しません。

アラームを設定するための CLI コマンドを以下に示します。

コマンド	パラメタ	デフォルト
set alarms	none, all, esc, rsc, utl, ovl, nls	未設定
show alarms		

コマンドの使用例を以下に示します。

```
# set alarms
Usage: set alarms [args] | none
all => All alarms turned on.
esc => Encryption status change alarm.
nls => Network link status alarm.
none => All alarms turned off (disabled).
ovl => Overload alarm.
rsc => Refused SSL connections alarm.
utl => Utilization threshold alarm.
# set alarms all
# show alarms
Alarms set: esc rsc utl ovl nls
# set alarms none
# show alarms
Alarms set: none
```

7.2 アラームのタイプ

設定可能なアラームのタイプを以下に詳しく説明します。

7.2.1 ESC：暗号状態の変更アラーム

このアラームを有効にすると、デバイスがインラインモード／バイパスモードの切り替えを行ったときに、アラームが発行されます。このモードの切り替えを行うには、inline コマンドまたは bypass コマンドを CLI から実行します。

フロントパネルの Bypass ボタンを押してもこのアラームが発行されます。

形式：

A:yyyymmddhhmmss: ESC:HDWR|CONB|CONI|FNTB| FNTI|APPR:/ *message*/

- A：アラームであることを示します。
- yyyymmddhhmmss：アラームの発生した日時です。
- ESC：暗号状態が変更されたことを示します。

■ アラームの修飾子およびメッセージ

アラームの修飾子は以下のとおりです。

- HDWR：暗号処理ハードウェアに問題がありました。
- CONB：コンソールからバイパスモードにされました。
- CONI：コンソールからインラインモードにされました。
- FNTB：フロントパネルからバイパスモードにされました。
- FNTI：フロントパネルからインラインモードにされましたす。
- APPR：アプリケーションが再起動しました。

7.2.2 RSC：SSL 接続の拒否

このアラームを有効にすると、現在指定されている期間（5 ～ 65000 秒、デフォルトは 15 秒）の間に、暗号群の不一致またはクライアント認証の失敗によって SSL 接続が拒否された場合に、アラームが発行されます。拒否された SSL 接続の総数は、拒否の理由とともに報告されます。このアラームは、CLI から有効／無効を切り替えることができます。

形式：

A:yyyymmddhhmmss:RSC:CSMM|CCAF:XXX:/*message*/

- A：アラームであることを示します。
- yyyymmddhhmmss：アラームの発生した日時です。
- RSC：SSL 接続が拒否されたことを示します。

■ アラームの修飾子およびメッセージ

アラームの修飾子は以下のとおりです。

- CSMM：対応する暗号方式が不一致です。
- CCAF：クライアント認証に失敗しました。

■ 詳細情報

XXX：ウィンドウ時間内に拒否されたコネクションの数です。

■ RSC アラーム用の CLI コマンド

SSL 接続の拒否アラームの発行間隔を設定するには、以下のコマンドを使用します。

```
set rsc_window <secs>
```

SSL 接続の拒否アラームの発行間隔を表示するには、以下のコマンドを使用します。

```
show rsc_window
```

使用例：

```
# set rsc_window 10
# show rsc_window
        Check for refused SSL connections [secs]: 10
```

7.2.3 UTL：使用しきい値アラーム

このアラームは、以下の 3 つの使用しきい値を監視します。

- CPU
- 1 秒当たりの接続数
- 同時にオープンできる接続数

このアラームを有効にすると、使用値のいずれかが所定の最高点を超えたとき、または、所定の最高点を超えたときや所定の最低点を下回ったときに、アラームが発行されます。最高点および最低点は、ユーザが定義します。デフォルトでは、最高点は 90%、最低点は 60%です。

⚠注意

使用しきい値メトリックスについて集められたデータは、バースト性を持つ傾向があります。そのため、アラームが休みなく発行され続けることを防ぐため、スムージングアルゴリズムが使用されています。使用ウィンドウは、ユーザが指定するスライディング間隔と同じです。この間にデータが収集され、その平均値が計算されます。したがって、間隔を短くすると、全く意味のないアラームが発行されることがあります。この間隔は、5 ～ 65000 秒の間で設定することができます（デフォルトは 15 です）。

形式：

A:yyyymmddhhmmss: UTL:ALRT|NRML:CPU|CON|SSLCS:/*message*/

- A：アラームであることを示します。
- yyyymmddhhmmss：アラームの発生した日時です。
- UTL：使用しきい値のアラームを示します。

■ アラームの修飾子およびメッセージ

アラームの修飾子と、修飾子が示すメッセージは以下のとおりです。

- ALRT：使用値のいずれかが最高点を超えました。
  Message: [CPU|Open connections|SSLCS] exceed high water mark
- NRML：使用値のいずれかが最低点を下回りました。
  Message: [CPU|Open connections|SSLCS] drop below low water mark

■ 詳細情報

- CPU：CPU 負荷率です。
- CON：アクティブになっているコネクション数です。
- SSLCS：1 秒あたりのコネクション数です。

■ UTL アラーム用の CLI コマンド

使用しきい値アラームの時間ウィンドウを設定するには、以下のコマンドを使用します。

```
set utl_window <secs>
```

使用しきい値アラームの最高点を設定するには、以下のコマンドを使用します。

```
set utl_highwater <%>
```

使用しきい値アラームの最低点を設定するには、以下のコマンドを使用します。

```
set utl_lowwater <%>
```

現在の設定を表示するには、以下のコマンドを使用します。

```
show utl_window
show utl_highwater
show utl_lowwater
```

例：

```
# set utl_window 10
# show utl_window
        Utilization Window set [secs]: 10
# set utl_highwater 80
# show utl_highwater
        Utilization High water mark [%]: 80
# set utl_lowwater 60
# show utl_lowwater
        Utilization Low water mark [%]: 60
```

7.2.4 OVL：過負荷アラーム

このアラームを有効にすると、過負荷が発生して、現在設定されているアラーム期間（5 ～ 65000 秒、デフォルトは 15 秒）の間に spill や throttle が実行された場合に、アラームが発行されます。

⚠注意 **このアラームは、暗号化／復号化機能が過負荷になっていることを示しています（SSL の通常動作は、アラームの原因となった条件がなくなると再開されます）。**

形式：

A:yyyymmddhhmmss: OVL:SPIL|THRT:XXX: /*message*/

- A：アラームであることを示します。
- yyyymmddhhmmss：アラームの発生した日時です。
- OVL：過負荷アラームであることを示します。

■ アラームの修飾子およびメッセージ

アラームの修飾子と、修飾子が示すメッセージは以下のとおりです。

- SPIL：過負荷によってスピルされました。
  Message: Spill mode.
- THRT：過負荷によってスロットリングされました。
  Message: Throttle mode.

■ 詳細情報

XXX：ウィンドウ時間内に発生した過負荷状態の数です。

■ OVL アラーム用の CLI コマンド

過負荷アラームの時間ウィンドウを設定するには、以下のコマンドを使用します。

 # set ovl_window <secs>

過負荷アラームの時間ウィンドウを表示するには、以下のコマンドを使用します。

show ovl_window

例：

set ovl_window 10
show ovl_window
Check for overload conditions [secs]: 10

7.2.5 NLS：ネットワークのリンク状況アラーム

ネットワークまたはサーバのリンク状況が変わると、アラームが発行されます。

形式：

A:yyyymmddhhmmss:
NLS:NETL|SVRL:NC|10HDX|10FDX|100HDX|100FDX: /*message*/

- A：アラームであることを示します。
- yyyymmddhhmmss：アラームの発生した日時です。
- NLS：ネットワークリンク状況アラームであることを示します。

■ アラームの修飾子およびメッセージ

アラームの修飾子と、修飾子が示すメッセージは以下のとおりです。

- NETL：Network 側ポートの状態です。
  Message: [No carrier|10Mb/s|100Mb/s][half duplex|full duplex]
- SVRL：Server 側ポートの状態です。
  Message: [No carrier|10Mb/s|100Mb/s] [half duplex|full duplex]

■ 詳細情報

- NC：キャリアなしですす。
- 10HDX：10Mb/s、半二重です。
- 10FDX：10Mb/s、全二重です。
- 100HDX：100Mb/s、半二重です。
- 100FDX：100Mb/s、全二重です。

7.3 アラームのログ

SSLAccelerator は、発行されたアラームの循環バッファを保持しています。最新のアラームや、例外発生により生成および保存された履歴ログは、コンソールや Telnet リモートセッション、SSH（Secure Shell）リモートセッションで参照することができます。最新のアラームを表示するときは、アラームバッファがただちにダンプされます。

履歴ログは、情報のスナップショットからなります。ここでいう情報とは、status line コマンドを実行してから、例外発生時に存在していたアラームバッファをダンプすることにより得られる情報のことです。

発行されたアラームは、CLI コマンドの status alarms コマンドを使用して、コンソールに表示することができます。また、例外発生により生成および保存されたログは、CLI コマンドの status <log filename> コマンドを使用して、表示することができます（list logs コマンドを使用すれば、参照可能なログファイルを表示できます）。

監視機能を有効にすることによって、アラームをコンソールに表示できます。監視レポートはデフォルトでは無効ですが、set monitoring [enable | disable] コマンドを使用して有効にできます。監視レポートは、監視機能を有効にしたコンソールと同一のコンソールに表示されます。

以下は、ログ表示を行うための CLI コマンドの例です。

list logs コマンドと status コマンドの使用例を示します。

```
# list logs
20000727_145544
# status 20000727_145544
====================== STATE ======================

Boot time:                    Thu Jul 27 14:54:21 2000
Curr time:                    Thu Jul 27 14:55:43 2000
Restarts:                     3
KTR Mask:                     0xFFFFF3DD
Total Connections:            0
Active Connections:           0, 0 (cur, max)
Connections/Second:           0, 0 (cur, max)

Util Status:
Secure Bytes Read:            0
Plain Bytes Read:             0
Secure Bytes Written:         0
Plain Bytes Written:          0
Bytes Allocated to dbufs:     0
Bytes Per dbuf:               0

Spill Mode:                   disable
Transactions Spilled:         0
Times Throttled:              0
Bypass Mode:                  disable
L&M board status:             RESPEND INLINE
(0x00000060)
Network NIC:                  100baseTX
```

```
                                Half Duplex
                                (0x00000026
                                 0x00000003
                                 0x0000026)
Server NIC:                     No carrier
                                (0x00000023
                                 0x00000001
                                 0x00000023)
Network LED:                    on
Server LED:                     off
SSL Caching:                    Enabled.

------------------ Configuration ------------------
conlog 0xffffffcf
ilog 0xffffffff
trace 0xfffff3dd
media auto
logport tty01
cache 3
server_tmo 5
client_tmo 30
serverif exp1
netif exp0
map 0.0.0.0 443 80 default
kpanic reboot
monitoring_interval 0
monitoring_fields 0x1f
alarm_mask 0x0000001f
ovl_window 15
rsc_window 15
utl_window 15
utl_high 90
utl_low 60
idle 300
kstrength 512
con_speed 9600
con_bits 8
con_stop 1
con_parity n
max_remote_sessions 5
trap_authen 1
crl_refresh 5
hdr_cert_def SSL_CLIENT_CERTIFICATE
hdr_cip_def SSL_SOURCE_IP
hdr_sid_def SSL_SSL_SESSION_ID
hdr_cipher_def SSL_CIPHER_USED
trap_authen
defcert_cname XX
defcert_state MyState
defcert_city MyCity
defcert_orgname MyCompany
defcert_orgunit MyCompany Division
defcert_name www.MyCompany.com
```

```
defcert_email support@MyCompany.xyz
prompt #
hwq_hiwat_spill 1
hwq_lowat_spill 1
trap_com0 1.1.1.1:private
snmp_com0 1.1.1.2:private
A:07/27/2000 14:54:47:NLS:SVRL:NC:/* Server port status, No carrier */
A:07/27/2000 14:54:41:NLS:SVRL:100FDX:/* Server port
status, 100Mb/s, full dupl/
A:07/27/2000 14:54:21:NLS:NETL:100HDX:/* Network port
status, 100Mb/s, half dup/
A:07/27/2000 14:54:21:NLS:SVRL:NC:/* Server port status, No carrier */
A:01/01/1970 00:00:00:ESC:APPR:3:/* Application Restarted */
```

status alarms コマンドの使用例を示します。

```
# status alarms
A:07/27/2000 14:57:05:ESC:CONI: /* Console inline */
A:07/27/2000 14:57:05:NLS:NETL:100HDX: /* Network port
status, 100Mb/s, half dup/
A:07/27/2000 14:57:01:ESC:CONB: /* Console bypass */
A:07/27/2000 14:57:01:NLS:NETL:NC: /* Network port status, No carrier */
A:07/27/2000 14:56:51:NLS:SVRL:NC: /* Server port status, No carrier */
A:07/27/2000 14:56:46:NLS:SVRL:100FDX: /* Server port
status, 100Mb/s, full dupl/
A:07/27/2000 14:56:30:ESC:CONI: /* Console inline */
A:07/27/2000 14:56:30:NLS:NETL:100HDX: /* Network port
status, 100Mb/s, half dup/
A:07/27/2000 14:56:29:NLS:NETL:NC: /* Network port status, No carrier */
A:07/27/2000 14:56:29:NLS:SVRL:NC: /* Server port status, No carrier */
```

7.4 監視

7.4.1 監視レポート

監視レポートは、ユーザが設定することのできる 1 行のテキストです。指定した 5 ～ 65000 秒の間隔で、コンソールに表示されます。間隔のデフォルト値は 15 秒です。

デフォルトでは、監視レポート機能は無効になっています。有効にするには、set monitoring [enable | disable] コマンドセットを使用します。監視アプリケーションは、これらのコマンドが届けられたポートを検知して、それと同じポートにレポートを送信します。そのため、監視レポートは、そのコマンドが出されたのと同じコンソールに表示されます。

7.4.2 レポートの設定

ユーザは、各レポートに表示するフィールドを指定することができます。レポートは「M」で始まり（監視レポートの場合。アラームレポートと区別するための文字です）、それに続いて、タイムスタンプが示されます。この他に表示するフィールドは、CLI コマンドを使用して選択することができます（「■ 監視レポート用の CLI コマンド」（→ 180 ページ）を参照してください）。標準のデフォルトフィールドは、SSLCS, CPU、DEC、ENC、FAILMODE、LINK、MODE、および OVR です。監視レポート機能は、デフォルトでは無効になっています。

監視レポートの形式は、次のようになっています。

形式：

M:yyyymmddhhmmss: mode:failmode:CPU;i,k,a:SSLCS;c,m,t:OVR;r,c,m,t:NetIF;s:SvrIF;s:BES;c,m,t;BDS;c,m,t

- M：監視レポートであることを示します（アラームには「A」が付きます）。
- yyyymmddhhmmss：レポートの生成された日時です。
- mode：バイパスモードの状態 [INLINE | BYPASS] です。
- failmode：フェイルモードの状態 [SAFE | THRU] です。
- CPU;i,k,a：「i」はアイドル、「k」はカーネル、「a」はアプリケーションです。
- SSLCS;c,m,t：SSL の 1 秒あたりのコネクション数です。「c」は現在の値、「m」は最大値、「t」合計値です。
- OVR;r,c,m,t：過負荷イベントです。「r」は応答 [SPIL | THRT]、「c」は現在の値、「m」は最大値、「t」合計値です。
- NetIF;s：ネットワーク側インターフェースの状態です。「s」は [NC | 10HDX | 10FDX | 100HDX | 100FDX] です。
- SvrIF;s：ネットワーク側インターフェースの状態です。「s」は [NC | 10HDX | 10FDX | 100HDX | 100FDX] です。

- BES;c,m,t：暗号処理速度です。「c」は 1 秒あたりの処理バイト数、「m」は 1 秒ごとの最大処理バイト数、「t」は起動してからの総処理バイト数です。
- BDS;c,m,t：復号処理速度です。「c」は 1 秒あたりの処理バイト数、「m」は 1 秒ごとの最大処理バイト数、「t」は起動してからの総処理バイト数です。

■ 監視レポート用の CLI コマンド

以下は、コンソールで監視を行うのための設定例です。コマンドの詳細については、「5.5.9 アラームコマンドおよび監視コマンド」（→ 123 ページ）を参照してください。

1 レポート間隔を設定します。

set monitoring_interval 15

2 監視フィールドを設定します。

set monitoring_fields all

3 レポート間隔、監視フィールドの設定を確認します。

show monitoring_interval
Monitoring report interval [secs]: 15
show monitoring_fields
Monitoring report fields: mode failmode cpu cps ovrld link enc dec

4 モニタリング機能を有効にします。

set monitoring enable

5 モニタリング機能の設定を確認します。

show monitoring
Monitoring for this terminal: enabled

モニタ機能を使用している場合、export/import **するデータがモニタ機能の出力によって乱れる場合があります。**
export/import **コマンドを使用する場合は、以下のコマンドを使用してモニタ機能を無効にしてください。**

set monitoring disable

8 トラブルシューティング

この章では、本装置を使っていて思うように動かないときに、どうすればいいかを説明しています。

Contents

8.1 トラブルシューティング

本装置を操作してみて、うまく動作しない場合など「故障かな？」と思ったときには、以下のことを確認してください。
ここでは主に、インパス接続を前提に説明します。

■ SSLAccelerator 導入時

現象	考えられる原因	処置
電源が入らない。	SSLAccelerator の電源ケーブルがコンセントに接続されていない。	電源ケーブルが SSLAccelerator に接続されていることを確認してから、コンセントに接続してください。
Power LED が点灯しない。	SSLAccelerator の電源ケーブルがコンセントに接続されていない。	電源ケーブルが SSLAccelerator に接続されていることを確認してから、コンセントに接続してください。
	SSLAccelerator が故障している。	SSLAccelerator が故障している可能性があります。担当保守員に連絡してください。

■ 導入時／運用中

現象	考えられる原因	処置
Error LED が継続的に点灯している。	SSLAccelerator が故障している。	SSLAccelerator が故障している可能性があります。担当保守員に連絡してください。
Power LED が継続的に点滅している。	SSLAccelerator が起動中である。または SSLAccelerator が故障している。	5 分間この状態が続いた場合、SSLAccelerator が故障している可能性があります。担当保守員に連絡してください。

■ 運用中

現象	考えられる原因	処置
Server LED または Network LED、あるいはその両方が点灯しない。	ケーブルが配線されていない。	SSLAccelerator とその接続先の機器にケーブルが接続されていることを確認してください。
	SSLAccelerator に接続されている機器の電源が入っていない。	SSLAccelerator に接続されている機器の電源が入っていることを確認してください。
	ケーブルの種類が不適当である。	SSLAccelerator が接続されている機器のタイプに応じて、Network 側ポート、Server 側ポートごとに、Cat-5 のストレートケーブルかクロスケーブルを選択して接続する必要があります。Network LED と Server LED が点灯するように、各ポートに接続されるケーブルのタイプを変えてみます。
	SSLAccelerator がバイパスモードになっている。（バイパスモードでかつフェイルセーフモードになっている場合、トラフィックはすべて遮断されます。）	Inline LED が点灯も点滅もしない場合は、本体のフロントパネル上の Bypass スイッチを押すか、または CLI の inline コマンドを使用して、SSLAccelerator をバイパスモードからインラインモードに切り替えます。 （「A.3 障害／バイパスモード」（→ 192 ページ）を参照。）
ケーブルを接続していないポートの LED が継続的に点灯または点滅している。	SSLAccelerator が故障している。	SSLAccelerator が故障している可能性があります。担当保守員に連絡してください。
HTTP 通信で、ブラウザに “ ページが表示できませんでした。” などのエラーメッセージが表示される。	SSLAccelerator 以外の機器の設定に誤りがある。または SSLAccelerator 以外の機器が故障している。	Network LED と Server LED が両方とも点灯している場合は、SSLAccelerator をフェイルスルーモード（「A.3 障害／バイパスモード」（→ 192 ページ）を参照）に設定して、本体をバイパスモードに切り替えます。これで、トラフィックは SSLAccelerator をそのまま通過します。この状態でデータが通過しない場合は、ネットワーク上の他の箇所に原因があります。

現象	考えられる原因	処置
HTTPS の通信で、ブラウザに “ ページが表示できませんでした。” などのエラーメッセージが表示される。	マッピングが不適当である。	第 4 章の「■ サーバの割り当て（マッピング）」（→ 61 ページ）を参照してください。
	SSLAccelerator とブラウザで利用できる暗号方式が一致していない。	• 暗号方式に関するブラウザ設定を変更してください。 • 以下のコマンドを使用して、SSLAccelerator が対応する暗号方式を変更することができます。 # **set ciphers <mapID>** <mapID> は暗号方式を設定する MapID です。 SSLAccelerator の対応する暗号方式については、「A.4 対応している暗号方式」（→ 194 ページ）を参照してください。
	電子証明書または秘密鍵、あるいはその両方が壊れている。	デフォルトの鍵と電子証明書を使用するか、または新しい鍵と署名なしの電子証明書を作成します。 これでエラーが表示されなくなった場合は、秘密鍵と署名要求 (CSR) をもう一度作成して認証局に再送信し新しい電子証明書を取得します。
HTTPS の通信で、Web ページの一部しか表示されない。 または、ブラウザに "Document Contains No Data（文書にデータが含まれていません）" や “ ページが表示できませんでした。” などのエラーメッセージが表示される。	クライアントタイムアウト値が小さすぎる。 クライアント要求の後、クライアントとサーバの間の接続が「クライアントタイムアウト」時間を超えてアイドル状態になっていると（すなわち、いずれの方向にもデータが送信されないと）、接続がタイムアウトになる。	以下のコマンドを使用して、タイムアウト時間を延長します。 # **set client_tmo <secs>** <secs> はタイムアウト値 (秒) です。 デフォルトは 30 秒です。推奨値は、最長サーバ応答時間の 1.5 倍です。
ブラウザがグローバルサーバ ID のロード後にこの電子証明書の署名者を認識できなかったことを示すエラーメッセージが表示される。	中間電子証明書が正しくインストールされていない。	正しい手順については、「4.6 グローバルサイト電子証明書」（→ 50 ページ）を参照してください。

現象	考えられる原因	処置
エラーメッセージ： Server/Network media mismatch	Server **側ポートと** Network **側ポートが、異なるメディア設定を自動認識している。**	**ネットワーク側とサーバ側の接続パラメタが一致することを確認してください。**status **コマンドを使用して、メディア設定を確認します。** # **status** . . Network port 100baseTX Full Duplex Server port 10baseT Half Duplex **次に、**nic **コマンドを使用して、強制的に共通のメディア属性に設定します。** **設定例：** # **nic** 1 - auto 2 - 10baseT, half duplex 3 - 10baseT, full duplex 4 - 100baseTX, half duplex 5 - 100baseTX, full duplex Select media type [1]: **2** **上記の例において、**2 **が正しい選択となります。**2 **つのポートが異なる速度／デュプレクスモードに自動設定された場合は、両方のポートを自動設定時に用いられた遅い方の設定に速度、デュプレクスモードを合わせるようにします（**10 Mbps **と** 100 Mbps **が、それぞれのポートに表われた時は** 10 Mbps **を、**half duplex **と** full duplex **の場合は** half **を選択する）。**
Overload LED **が継続的に点灯している。**	SSL **トラフィックが** SSLAccelerator **の処理能力を超えている。**	• SSLAccelerator **がカスケード接続されている場合は** show spill **コマンドを実行して、設定が** enable **になっていることを確認します。** enable **にするためには** set spill enable **コマンドを実行します。このとき、最終段（サーバに一番近い** SSLAccelerator**）以外の** SSLAccelerator **の** Overload LED **が継続的に点灯していても問題ありません。** **最終段の** SSLAccelerator **の** Overload LED **が継続的に点灯している場合はシステム構成の再検討が必要です。** • **カスケード接続されていない場合は、**SSL **のリクエストが** SSLAccelerator **の処理能力を超えていること示しています。システム構成の再検討が必要です（**SSLAccelerator **の増設で回避できます）。** SSL **トラフィックの処理の状態は** CLI **上で** status **コマンドを実行して確認します。**

付録 A

Contents

A.1　仕様

本装置の仕様は、次のとおりです。
他の周辺装置の仕様については、本装置に添付の取扱説明書をご覧ください。

装置名称	SSLAccelerator 7117
接続インタフェース	LAN (100BASE-TX/10BASE-T) × 2 、 **シリアル**× 2
外形寸法	424.9(W) × 44.5(H) × 469.9(D)mm
質量	**最大** 4.8Kg

本装置の仕様は、改善のため予告なしに変更することがあります。あらかじめ、ご了承ください。

A.2　ソフトウェアのアップデート

SSLAccelerator ソフトウェアの更新またはアップデートには、import upgrade コマンドを使用します。SSLAccelerator ソフトウェアをアップデートした場合、電子証明書、すべての鍵、電子証明書、マッピングを含む設定情報は保存されますが、ログファイルはすべて消去されます。ソフトウェアのファイルは、イメージファイル（*.IMG）です。

■ アップグレードの前に

- 出力データの監視を実行することよって、インポートまたはエクスポート処理に障害が生じる可能性があります。
  監視機能が有効な状態でインポートまたはエクスポートの処理を実行すると、その監視レコードの定期出力がインポートまたはエクスポート時のデータフローに挿入されます。このため、インポートまたはエクスポートを実行する前に、監視機能をすべてオフにしておくことをお勧めします。

  ```
  # set monitoring disable
  ```

  装置の監視機能の詳細については、「7.4 監視」（→ 179 ページ）を参照してください。

- ソフトウェアがアップグレードされると 、IP ブロックが無効になる可能性があります。
  ソフトウェアのアップグレードの完了後、装置が自動的に再起動すると、それまでに作成されていた IP ブロックを装置が再確立できないという問題が生じる場合があります。この場合、コンソールには、次のいずれかのメッセージが表示されます。

  ```
  Upgrading...
  System rebooting...09/20 13:41:43 Build 122 Tue
  Sep 19 02:40:36 PDT 2000 09/20 13:41:44 "block
  9.8.7.6 255.255.255.255 99 0xffff" is incomplete and ignored
  Warning: "ciphers ALL:!ADH:!EDH" at line # 11 ignored.
  Warning: "block 9.8.7.6 255.255.255.255 99 0xffff" at line # 30 ignored.
  Do you want to install this config? [y]:
  ```

  アップグレードの完了後、必要な IP ブロックを作成し直すには、create block コマンドを入力します。block コマンドの詳細については、「5.5.5 マッピングコマンド」（→ 101 ページ）を参照してください。

■ Windows ハイパーターミナルの使用方法

コマンド：import upgrade

伝送速度を大きくするには、SSLAccelerator の Aux console ポート（デフォルトの伝送速度は 115.2 kbps）を使用します。XMODEM を使用したインポート手続きには、およそ 9 分（115.2 kbps の場合）かかります。

1 **イメージファイル（.IMG）をローカルの** PC **にダウンロードします。**

2 COM1 **または** COM2 **と、**SSLAccelerator **の** Aux console **ポートをシリアルケーブルで接続します。「第** 2 **章 設置と初期設定」（→** 7 **ページ）を参照してください。**

3 SSLAccelerator **にログインします。**

4 import upgrade **コマンドを入力します。**XMODEM **の選択を求めるプロンプトが表示されます。**[Enter]**キーを押して、デフォルト（**XMODEM**）を選択します。**

```
# import upgrade
import protocol (xmodem) [xmodem]: <Enter>
Start xmodem upload now
Use Ctl-X multiple times to cancel upload
```

5 **ハイパーターミナルの［転送］メニューのファイルの送信をクリックし、ファイルを選択します。ファイル名は、直接入力するか、[参照]をクリックして検索します。次に、プロトコルフィールドをクリックして転送プロトコルとして** 1K XMODEM**（または** XMODEM**）を選択し、送信をクリックします。**

```
Verifying upgrade image...
Upgrade image valid
=== Release x.x
=== Load xx, Fri Aug 25 05:31:51 2001
```

6 Continue with upgrade? **というプロンプトが表示されたら、**[y]**キーを押します。**

```
Continue with upgrade? [n]: y
Upgrading...
System rebooting...done
```

正しくアップデートが完了すると、保存されているログがすべて削除され、システムが再起動します。

コマンド :import patch

伝送速度を大きくするには、SSLAccelerator の Aux console ポート（デフォルトの伝送速度は 115.2kbps）を使用します。

1 **パッチファイル（*.patch）をローカルのパソコン にダウンロードします。**

2 COM1 **または** COM2 **と、**SSLAccelerator **の** Aux console **ポートをシリアルケーブルで接続します。**

3 SSLAccelerator **にログインします。**

4 import patch **コマンドを入力します。**

XMODEM の選択を求めるプロンプトが表示されます。［Enter］キー を押してデフォルト（XMODEM）を選択します。

```
# import patch
import protocol (xmodem) [xmodem]: <Enter>
Start xmodem upload now
Use Ctl-X multiple times to cancel upload
```

5 **ハイパーターミナルの［転送］メニューの［ファイルの送信］をクリックし、ファイルを選択します。**

ファイル名は、直接入力するか、［参照］をクリックして検索します。次に、プロトコルフィールドをクリックして転送プロトコルとして 1K XMODEM（または XMODEM）を選択し、［送信］をクリックします。

```
Verifying patch image...
Patch successfully imported.
```

このパッチは、次回システムを再起動したときに有効になります。

A.3　障害／バイパスモード

SSLAccelerator には、インパス接続の場合、障害が発生すると自動的にトラフィックをバイパスする機能があります。Bypass ボタンを押すか、bypass コマンドを実行することで、バイパスモードに設定することもできます。

SSLAccelerator には、フェイルスルースイッチがあります。このスイッチは、デフォルトでフェイルセーフの位置に設定されています。この設定のときは障害が発生しても、トラフィックは伝送されません。手動でバイパスモードに設定している場合も、トラフィックは伝送されません。

ここからは、正しい CLI コマンドを入力して SSLAccelerator の処理を有効にし、SSLAccelerator が通常の状態で動作しているものとして、Bypass ボタンとフェイルスルースイッチについて説明します。

■ Bypass ボタン

一部のオフライン操作（設定内容の変更、証明書情報の入力、障害の切り分けなど）では、SSLAccelerator を強制的にバイパスモードに設定する必要があります。

SSLAccelerator の処理をバイパスする必要がある場合は、Bypass ボタンをオンにします（バイパスモード）。このとき、Network LED、inline LED および Server LED はすべて消灯します。バイパスモードに設定しているときは、トラフィックは処理されません。

インパス接続の場合、クライアントとサーバ間のトラフィックを未処理のまま伝送するかどうかは、フェイルスルースイッチで設定するモードによって決定します。

ワンアーム接続の場合、フェイルスルースイッチの設定にかかわらず、SSLAccelerator と L4 スイッチの通信は遮断されます。

フェイルスルースイッチについては、次の節を参照してください。

■ フェイルスルースイッチ

フェイルスルースイッチでは、障害発生時の動作を制御できます。このスイッチは、Network 側コネクタと Server 側コネクタの間にあります。スイッチを動かすには、ドライバやクリップを使用します。このスイッチの位置によって、障害発生時（または Bypass ボタンがオンになっているとき）にトラフィックの伝送を許可するか、またはブロックするかが決定されます。スイッチ位置が下（フェイルスルーモード）になっていると、障害が発生します。Bypass ボタンがオンになっていると、トラフィックは未処理のまま伝送されます。

正常動作中においては、SSLAccelerator は、通過するトラフィックが障害発生時に未処理のまま通過させるかどうかを、Inline LED（緑）の点滅状態によって表示します（障害発生時にトラフィックを通過させるかどうかの設定は、フェイルスルースイッチでなされます）。点滅状態の場合、SSLAccelerator は、正常にトラフィック処理を行っていることを意味します。点滅状態の場合は、障害発生時にトラフィックを通過させないモード（フェイルセーフモード）で動作していることを意味します。点灯状態の場合は、障害発生時にトラフィックを処理せずにそのまま通過させるモード（フェイルスルーモード）で動作していることを意味します。Inline LED が消灯している場合は、SSLAccelerator は SSL 処理を行っていません。このとき、フェイルセーフモードに設定されていると、トラフィックはそこで遮断されます。また、フェイルスルーモードに設定されていると、トラフィックは何も処理されずに次段に渡されます。

次に、インパス接続におけるフェイルスルースイッチと Bypass ボタンを使用したときの状態と Inline LED の動作を示します。

デバイスモード	Bypass ボタン	フェイルスルースイッチモード	トラフィックの状態	Inline LED
障害発生	N/A	フェイルセーフ（上方）	トラフィックの通過拒否（両方向）	消灯
障害発生	N/A	フェイルスルー（下方）	トラフィックは未処理のまま通過	消灯
N/A	オン（バイパス）	フェイルセーフ（上方）	トラフィックの通過拒否（両方向）	消灯
N/A	オン（バイパス）	フェイルスルー（下方）	トラフィックは未処理のまま通過	消灯
動作	オフ（インライン）	フェイルセーフ（上方）	トラフィックを処理	点滅（緑）
動作	オフ（インライン）	フェイルスルー（下方）	トラフィックを処理	点灯（緑）

⚠注意 **ワンアーム接続でバイパスモードの場合、フェイルスルースイッチの上、下にかかわらず、SSLAccelerator と L4 スイッチの通信は遮断されます。**

A.4　対応している暗号方式

SSLAccelerator は、公開鍵暗号方式として RSA 公開鍵暗号方式の鍵交換と認証のみをサポートしています。Diffie-Hellman（Anonymous、Ephemeral を含む）公開鍵方式の鍵交換／認証や、DSS 認証はサポートしていません。

暗号方式の指定には、set cipher コマンドを使用します。このコマンドを実行すると、暗号方式の強さと SSL のバージョンレベルの入力を求めるプロンプトが表示されます。

以下に、選択できる暗号方式の強さと SSL のバージョンレベルを示します。

■ 暗号方式の強さ

- All- サポートしているすべての暗号方式（輸出向けの暗号方式を含む）
- High-168 ビット暗号化を使用するすべての暗号方式（トリプル DES）
- Medium-128 ビット以上の暗号化を使用するすべての暗号方式（High を含む）
- Low-64 ビット以上の暗号化を使用するすべての暗号方式（Medium と High を含む）
- Export only- 輸出向けの暗号方式

■ SSL バージョンレベル

- SSLv2-SSL バージョン 2.0 のすべての暗号方式
- SSLv3-SSL バージョン 3.0 のすべての暗号方式
- SSLv2 と SSLv3-SSL バージョン 2.0 と 3.0 のすべての暗号方式

デフォルトでは、サポートされているすべての暗号方式が使用可能です（SSLv2 と SSLv3 の両方）。

次の表に、SSLAccelerator でサポートしている暗号化方式を示します。

名前	プロトコル	鍵交換	認証	暗号化（鍵のサイズ）	メッセージ認証	プロファイル（Hi/Medium/Low/Export）
DES-CBC3-SHA	SSLv3	RSA(1024)	RSA	3DES(168)	SHA1	H
RC4-SHA	SSLv3	RSA(1024)	RSA	RC4(128)	SHA1	M
RC4-MD5	SSLv3	RSA(1024)	RSA	RC4(128)	MD5	M
DES-CBC-SHA	SSLv3	RSA(1024)	RSA	DES(56)	SHA1	L
DES-CBC3-MD5	SSLv2	RSA(1024)	RSA	3DES(168)	MD5	H
RC2-CBC-MD5	SSLv2	RSA(1024)	RSA	RC2(128)	MD5	M
RC4-MD5	SSLv2	RSA(1024)	RSA	RC4(128)	MD5	M

名前	プロトコル	鍵交換	認証	暗号化（鍵のサイズ）	メッセージ認証	プロファイル（Hi/Medium/Low/Export）
RC4-64-MD5	SSLv2	RSA(1024)	RSA	RC4(64)	MD5	L
DES-CBC-MD5	SSLv2	RSA(1024)	RSA	DES(56)	MD5	L
EXP-DES-CBC-SHA	SSLv3	RSA(512)	RSA	DES(40)	SHA1	L
EXP-RC2-CBC-MD5	SSLv3	RSA(512)	RSA	RC2(40)	MD5	L
EXP-RC4-MD5	SSLv3	RSA(512)	RSA	RC4(40)	MD5	L
EXP-RC2-CBC-MD5	SSLv2	RSA(512)	RSA	RC2(40)	MD5	L
EXP-RC4-MD5	SSLv2	RSA(512)	RSA	RC4(40)	MD5	L

■ SSH のバージョン

以下の表に、SSLAccelerator が対応している暗号方式を示します。

	SSH2
暗号方式	3DES、Twofish、RC4、**なし**
MAC	MD5、**なし**

A.5　お手入れ

本装置のお手入れのしかたは、以下のとおりです。

⚠警告

お手入れをする前に、電源ケーブルをコンセントから取り外してください。また、本装置に接続してある周辺装置も電源を切り、本装置から取り外してください。
感電の原因となります。

柔らかい布で乾拭きします。乾拭きで落ちない汚れは、中性洗剤をしみ込ませ固くしぼった布で拭きます。汚れが落ちたら、水に浸して固くしぼった布で、中性洗剤を拭き取ります。拭き取りのときは、本装置に水が入らないようにご注意ください。

A.6　用語集

ここでは、SSLAccelerator ユーザーズガイドで使用する用語と略語の定義を示します。

● 暗号方式

共通鍵または公開鍵を使用した暗号化アルゴリズムです。ネットワーク経由で送信されるデータを暗号化することを目的として、データストリームの形式になっている場合と、ブロックに分割されている場合があります。

● インパス接続

SSLAccelerator が、Network 側ポートと Server 側ポートの両方を介してネットワークに接続されるネットワーク構成です。ワンアーム接続についての説明も参照してください。

● 鍵

メッセージの暗号化と復号化に使用する鍵です。

● 鍵の強さ

データの暗号化または認証で使用する鍵の長さ（ビット単位）です。（例：56、128、512）。

● カスケード接続

複数の SSLAccelerator を直列に接続することにより、より大量のトラフィック（CPS）の処理を可能とする構成です。

● キーペア

組となる公開鍵と秘密鍵のことです。

● 公開鍵

公開鍵暗号方式で使用する鍵のうち、広汎に配布される公開の鍵を指します。メッセージの暗号化や、電子署名の照合に使用します。

● サービス

ポート番号と組み合わせになっている IP アプリケーションです。たとえば、「HTTP:80」は、ポート 80 で待機しているサーバの HTTP アプリケーションで構成されるサービスを表します。このほか、「FTP:21」のような表記も考えられます。

● 実行サーバ

ユーザの要求を満たす内容を格納しているサーバです。

● 署名要求

認証局に電子証明書の認証を求める要求を送るときに必要です。CSR とも呼ばれます。

● **電子証明書**

SSL 暗号化トランザクションで使用する電子署名付きのトークンです。発行元（認証局）、電子証明書を所有する組織、公開鍵、電子証明書の有効期限、ホスト名などの情報が含まれています。

● **電子証明書取り消しリスト**

認証局が発行する、無効になった電子証明書を示すリスト。

● **バイパス**

トラフィックが SSLAccelerator の処理をバイパスするように設定するユーザーアクションです。実行するには、CLI の bypass コマンドか、SSLAccelerator のフロントパネルの Bypass ボタンを使用します。

● **秘密鍵**

公開鍵暗号方式で使用する鍵のうち、所有者のみが使用できる非公開の鍵を指します。メッセージの復号や、電子署名の作成に使用します。

● **フラッシュ**

設定内容の変更を格納する不揮発記憶装置です。

● **ポート**

TCP/IP セッションで使用するプロトコル固有のハンドルです。

● **リダイレクション**

クライアント電子証明書を持たない、クライアント電子証明書が無効である、またはサポートされていない暗号の使用を試みるクライアントに代替ページを表示できるようにする機能です。

● **ロードバランシング**

コンピュータネットワーク全体で処理と通信アクティビティを分散させ、特定のデバイスの負荷が大きくなり過ぎないようにすることです。サーバへの要求数の予測が難しいネットワークでは、この処理が特に重要になります。トラフィックの多い Web サイトでは、2 台以上の Web サーバを使用してロードバランシングを行うのが一般的です。

● **ワンアーム接続**

SSLAccelerator が、Network 側ポートのみを介してネットワークに接続するネットワーク構成です。インパス接続よりも拡張性に優れています。インパス接続についての説明も参照してください。

● DNS

ドメインネームサーバ（Domain Name Server）の略称です。ホストコンピュータの名前をアドレスに変換するメカニズムの一種であり、インターネットで使用されます。

● HTTP

Hypertext Transfer Protocol の略称です。Web ブラウザとサーバの間で、文書の要求とその内容の転送に使用されます。

● HTTPS

SSL 暗号化セッションで通信を行う HTTP です。

● Inline

SSLAccelerator が SSL トラフィックを処理できるときは、フロントパネル上の Inline LED が点灯または点滅します。

● IP

インターネットプロトコル（Internet Protocol）の略称です。

● IP **アドレス**

IP ネットワーク上のノードを識別する一意の識別子です。ドットで区切った 10 進数で表記されます（例：10.0.0.1）。

● IP **サービス**

ネットワークアクセス、IP アクセス可能なアプリケーションプロトコルです。HTTP や FTP などがあります。

● ITM（Internet Traffic Manager）

Intel NetStructure ™ 7140/7170 Traffic Director および Intel NetStructure ™ 7180 e-Commerce Director 製品です。ロードバランシングに使用します。

● SSL （Secure Socket Layer）

Netscape 社が開発したプロトコルです。TCP/IP ネットワークを介して暗号文を伝送するとき、セキュアなエンドツーエンドのリンクを張ります。

● VeriSign

一般的な認証局の 1 つです。

索引

せ

そ

た

て

と

に

ね

ひ

ふ

へ

ほ

ま

ゆ

ら

り

ろ

わ

C

S

T

PRIMERGY SSLAccelerator 7117

取扱説明書

P3F1-1840-01-00

発行日　2002 年 5 月

発行責任　富士通株式会社

Printed in Japan

Ⓟ0205-1

FUJITSU

このマニュアルは再生紙を使用しています。